HITACHI
Inspire the Next

Hitachi IT Operations Analyzer

Handbuch „Erste Schritte“: Ergänzung „Gerätekonfiguration“

DIREKTLINKS

Hitachi Data Systems

MK-90IOS006GE-12

Inhalt

Informationen zu diesem Handbuch

Dieses Handbuch ist eine Ergänzung zum Handbuch „Erste Schritte“ für Hitachi IT Operations Analyzer. Es unterstützt Sie im Vorfeld der Installation bei der Einrichtung von Netzwerkkomponenten, die von Ihrem Standort überwacht werden sollen.

In diesem Abschnitt finden Sie folgende Informationen:

Zielgruppe

Dieses Dokument ist an Systemadministratoren gerichtet und andere Benutzer, die für Konfiguration und Betrieb des Hitachi IT Operations Analyzer verantwortlich sind.

Produktversion

Diese Dokumentversion gilt für IT Operations Analyzer Version 3.3.1.

Dokumentenversionen

Dieser Abschnitt enthält eine Übersicht über die verschiedenen Versionen dieses Dokuments.

Version	Datum	Beschreibung
MK-90IOS006GE-00	März 2010	Erstveröffentlichung
MK-90IOS006GE-01	Oktober 2010	Version 1, ersetzt MK-90IOS006GE-00
MK-90IOS006GE-02	April 2011	Version 2, ersetzt MK-90IOS006GE-01
MK-90IOS006GE-03	Januar 2012	Version 3, ersetzt MK-90IOS006GE-02
MK-90IOS006GE-04	März 2013	Version 4, ersetzt MK-90IOS006GE-03
MK-90IOS006GE-12	Juli 2013	Version 12, ersetzt MK-90IOS006GE-04

Ergänzende Dokumentation

- *Hitachi IT Operations Analyzer – Erste Schritte: Ergänzung „Gerätekonfiguration*", MK-90IOS006GE
- Hilfe für Hitachi IT Operations Analyzer
- Versionshinweise, RN-99IOS004

Konventionen in diesem Handbuch

Die folgenden Symbole kennzeichnen wichtige Informationen.

Symbol	Bedeutung	Beschreibung
	Tipp	Tipps enthalten hilfreiche Informationen, Richtlinien oder Vorschläge für eine effizientere Ausführung von Aufgaben.
	Hinweis	Hinweise kennzeichnen wichtige Punkte im Haupttext oder ergänzen diese.

In diesem Dokument werden die folgenden typografischen Konventionen verwendet.

Konvention	Beschreibung
Fett	Kennzeichnet Text in einem Fenster (abgesehen vom Fenstertitel), z. B. Menüs, Menüoptionen, Schaltflächen, Felder und Beschriftungen. Beispiel: Klicken Sie auf **OK**.
Kursiv	Heben Variablen hervor, die vom Benutzer oder vom System durch entsprechende Texteingaben ersetzt werden. Im Fall von Versionsinformationen steht das kursive „x" für alle darauffolgenden Versionen. Beispiele: • Kopieren Sie *Quelldatei Zieldatei*. • Kernel-Version 2.6.*x.* **Hinweis**: Spitze Klammern (< >) werden ebenfalls verwendet, um Variablen anzugeben.
Bildschirm/ Code	Kennzeichnet Text, der auf dem Bildschirm angezeigt oder vom Benutzer eingegeben wird. Beispiel: `# pairdisplay -g oradb`
Spitze Klammern	Heben Variablen hervor, die vom Benutzer oder vom System durch entsprechende Texteingaben ersetzt werden. Beispiel: `# pairdisplay -g` <Gruppe> **Hinweis**: Kursive Schrift wird ebenfalls verwendet, um Variablen anzugeben.

Produktverweise

In diesem Handbuch wird auf VMware®-Produkte verwiesen.
Diese Verweise werden folgendermaßen behandelt:

- Verweise auf spezifische Produktversionen, z. B. VMware ESX 3, VMware ESX 3i, VMware ESX 4.0 usw.
- Verweise auf den Produktserver ohne spezifische Versionsangabe: ESX-Server

Hilfe

Wenn Sie dieses Produkt gekauft haben und über eine gültige Support-Vereinbarung verfügen, stellen Sie bitte die folgenden Informationen zusammen:

- Produktname und Versionsnummer
- Name und Version des Betriebssystems oder Service-Pack-Nummer
- Seriennummer der Lizenz, auf die sich Ihre Anfrage bezieht
- Text aller angezeigten Fehlermeldungen
- Die Bedingungen, unter denen der Fehler bzw. das Problem aufgetreten ist
- Eine Beschreibung des Problems und welche Maßnahmen zu seiner Behebung getroffen wurden

Wenn Ihnen sämtliche Details vorliegen, setzen Sie sich mit dem Kundendienstzentrum von Hitachi Data Systems in Verbindung.

Eine Aufstellung der aktuellen Telefonnummern und andere Kontaktinformationen für das Kundendienstzentrum von Hitachi Data Systems finden Sie auf der Hitachi Data Systems-Website unter:

https://portal.hds.com

HINWEIS: Falls Sie mit einer Testversion des Produkts arbeiten, lesen Sie die Selbstbedienungsmaterialien im IT Operations-Softwareportal unter: http://www.itoperations.com

Anmerkungen

Senden Sie Ihre Hinweise und Anmerkungen zu diesem Dokument an: doc.comments@hds.com. Alle Mitteilungen sollten den Dokumenttitel, die Nummer und die Version enthalten. Geben Sie nach Möglichkeit auch an, auf welche Abschnitte und Absätze sich Ihre Anmerkungen beziehen.

Vielen Dank! (Alle Kommentare werden Eigentum von Hitachi Data Systems Corporation.)

1

Übersicht

Es ist wichtig, dass Sie vor der Installation von IT Operations Analyzer oder der Verwendung des Ermittlungsassistenten die Umgebung überprüfen. Dazu gehört die Überprüfung der Einstellungen, die in Ihrer Umgebung gelten, und das Sammeln von Informationen, die Sie später im Rahmen der Einrichtung benötigen.

- Vorbereiten der Umgebung

Vorbereiten der Umgebung

Tabelle 1-1 enthält eine Übersicht über die erforderlichen Aufgaben sowie über die Aufgaben, die je nach Umgebung und Zweck der Überwachung empfehlenswert oder optional sind.

Bei jeder Aufgabe wird auf das Kapitel verwiesen, das diesbezügliche Einzelheiten enthält.

Tabelle 1-1: Vorbereitung der Umgebung

Erforderliche Aufgaben	
Aufgabe	**Details**
Prüfen Sie beim Verwaltungsserver (dem Gerät, auf dem IT Operations Analyzer installiert wird) die DCOM-Einstellungen für WMI.	Verhindern Sie WMI-Remote-Verbindungsfehler, weil die Remote-Ausführung von DCOM unzulässig ist. Siehe Kapitel 2, Vorbereiten von WMI für Windows-Server.
Falls Ihr Standort eines oder mehrere der folgenden Überwachungsziele verwendet, müssen Sie diese einrichten:	Überwachungsziele sind die Server, Speichergeräte und Switches, die überwacht werden sollen.
• IP-Switches	IT Operations Analyzer verwendet SNMP zur Überwachung von IP-Switches. • Aktivieren Sie SNMP. • Bringen Sie den SNMP Community String in Erfahrung. • Bringen Sie die IP-Adresse in Erfahrung. Siehe Kapitel 5, Vorbereiten von SNMP für IP-Switches.
• Hitachi 9500V	IT Operations Analyzer überwacht Hitachi 9500V über den SMI-S Agent von Device Manager. Die Leistung wird nicht überwacht. Installieren Sie Device Manager 5.9 oder höher, und aktivieren Sie SMI-S. Siehe Kapitel 6, Vorbereiten von Hitachi Storage.
• Hitachi USP VM	IT Operations Analyzer überwacht Hitachi USP VM über den SMI-S-Agent von Device Manager. Installieren Sie Device Manager 6.2 oder höher, und aktivieren Sie SMI-S. Siehe Kapitel 6, Vorbereiten von Hitachi Storage.

• Sonstige Speichergeräte, FC-Switches	IT Operations Analyzer verwendet SMI-S zur Ermittlung und Überwachung anderer Speichergeräte und von FC-Switches. Installieren Sie SMI-S Agent, und bringen Sie dann Folgendes in Erfahrung:
	• IP-Adresse
	  • SMI-S-Agent (Proxy): Geben Sie eine IP-Adresse des SMI-S-Servers für den Switch an.
	  • SMI-S-Agent (integriert): Geben Sie für den FC-Switch dieselbe IP-Adresse an.
	• Benutzer-ID und Kennwort
	• Port-Nummer
	• Namespace
	Überprüfen Sie auch den SSL-Status.
	Siehe Kapitel 7, Prüfen der SMI-S-Vorbereitungen.
	Bei der Angabe von Zugangsdaten für NetApp FAS Serie oder bei der Verwaltung von Linux-Versionen unter Verwendung eines SMI-S-Agent empfehlen wir die Angabe von **http** für den **SSL** im Dialogfeld **Zugangsdaten hinzufügen**.

Tabelle 1-1: Vorbereitung der Umgebung

Empfohlene Aufgaben	
Aufgabe	**Details**
Prüfen der Überwachungsziele: • Windows-Server	IT Operations Analyzer verwendet WMI zur Überwachung von Windows-Servern. Für den Remote-Zugriff auf WMI muss DCOM auf dem Windows-Server und dem Verwaltungsserver aktiviert sein. Ist DCOM nicht aktiviert, kann die Software die Windows-Server ggf. nicht ermitteln oder überwachen. Installieren Sie außerdem den Integrationsservice auf einer virtuellen Maschine, wenn an Ihrem Standort eine virtuelle Hyper-V-Maschine überwacht werden soll. Siehe Kapitel 2, Vorbereiten von WMI für Windows-Server.
• Linux/Solaris-Server	IT Operations Analyzer verwendet SSH zur Ermittlung von Linux- und Solaris-Servern. Die Überwachung der Server erfolgt außerdem über Kennwortauthentifizierung (nicht Zertifikatsauthentifizierung). Überprüfen Sie Folgendes: • SSH-Service ist installiert und wird ausgeführt. • SSH2-Verbindung ist aktiviert. • Kennwortauthentifizierung ist zulässig. Siehe Kapitel 3, Vorbereiten von SSH für Linux-/Solaris-Server.
• VMware ESX-Server	IT Operations Analyzer kann Windows- oder Linux-Server auf virtuellen Maschinen nur richtig überwachen, wenn VMware-Tools installiert sind. Überprüfen Sie die unterstützte Version: • VMware ESX 3 • VMware ESX 3.5 • VMware ESX 3i • VMware ESX 3.5i • VMware ESX 4 • VMware ESX 4i • VMware ESX 4.1 • VMware ESX 4.1i • VMware ESX 5 • VMware ESX 5i • VMware ESX 5.1 • VMware ESX 5.1i Installieren Sie außerdem VMware Tools auf virtuellen Computern. Siehe Kapitel 4, Vorbereiten von VMware für ESX-Server.
• Hitachi AMS/WMS/SMS-Serie und Hitachi Unified Storage-Serie	Prüfen Sie, ob Kontoauthentifizierung oder Kennwortschutz aktiviert sind. Falls Kontoauthentifizierung oder Kennwortschutz aktiviert sind, benötigt IT Operations Analyzer die Benutzer-ID und das Kennwort. Siehe Kapitel 6, Vorbereiten von Hitachi Storage.

Tabelle 1-1: Vorbereitung der Umgebung

Empfohlene Aufgaben	
Aufgabe	**Details**
• Dell-Server	Mit dem integrierten Plug-In für Dell-Chassis können spezifische Informationen für Dell-Server abgerufen werden. „Dell Chassis (Windows)" wird als Plug-in für Windows und „Dell Chassis (Linux)" wird als Plug-in für Linux installiert. Im Folgenden werden die Systemanforderungen für Dell-Server, die mit IT Operations Analyzer überwacht werden, beschrieben: • Dell OpenManage Server Administrator (OMSA) Versionen 6.1.0 oder 6.2.0 müssen auf dem/den überwachten Dell-Server(n) laufen. • SNMP-Agent ist auf den überwachten Dell-Servern installiert und wird ausgeführt. • „Dell Chassis (Windows)" erfordert, dass DSM SA Data Manager Service auf dem Microsoft Windows Server ausgeführt wird. • „Dell Chassis (Linux)" erfordert, dass der Prozess dsm_sa_datamgrd oder dsm_sa_datamgr32d auf Red Hat Enterprise Linux Server läuft. Die Betriebssystemvoraussetzungen für Linux-basierte und Windows-basierte Dell-Server finden Sie in den Einrichtungsschritten für Linux-Server und Microsoft Windows-Server.
Optionale Aufgaben	
Aufgabe	**Details**
Prüfen der Überwachungsziele: • Windows-Server	IT Operations Analyzer verwendet WMI zur Überwachung von Windows-Servern. Unter Windows 2003 muss FCInfo installiert sein, damit FC HBA-Daten über WMI bereitgestellt werden. Falls die Windows-Server einen FC HBA verwenden, installieren Sie FCInfo. Siehe Kapitel 2, Vorbereiten von WMI für Windows-Server.
• IP-Switches	Aktivieren Sie das Senden von SNMP-Traps. IT Operations Analyzer kann SNMP-Traps von IP-Switches empfangen. Diese Aufgabe ist optional, da IT Operations Analyzer zur Überwachung von IP-Switches anstelle von Traps auch Abfragen verwenden kann. Siehe Kapitel 5, Vorbereiten von SNMP für IP-Switches.

2

Vorbereiten von Hyper-V und WMI für Windows-Server

IT Operations Analyzer verwendet WMI zur Überwachung von Windows-Servern. Für den Remote-Zugriff auf WMI muss DCOM auf dem Windows-Server und dem Verwaltungsserver aktiviert sein. Ist DCOM nicht aktiviert, kann die Software die Windows-Server ggf. nicht ermitteln oder überwachen. In diesem Kapitel wird die Vorbereitung der Hyper-V- und WMI-Umgebung beschrieben.

Vorbereiten von Hyper-V

Wenn an Ihrem Standort ein Windows- oder Linux-Server überwacht werden soll, der auf einer virtuellen Maschine unter Hyper-V installiert ist, müssen Sie im Betriebssystem der virtuellen Maschine den „Integrationsservice" installieren. Wenn der Integrationsservice nicht installiert ist, wird weder der Status der virtuellen Maschine noch die Beziehung zwischen Hostrechner und Gast-Betriebssystem in IT Operations Analyzer richtig angezeigt.

HINWEIS: Die Einrichtung des Hyper-V-Hostrechners entspricht im Wesentlichen den Vorbereitungsschritten für den Windows-Server. Weitere Informationen finden Sie im nächsten Abschnitt.
Außerdem ist es möglicherweise nicht möglich, sich mit dem Gast-Betriebssystem des Verwaltungszielgeräts Hyper-V zu verbinden, wenn KB2264080 nicht auf Windows Server 2008 R2 für das Host-Betriebssystem des Verwaltungsziels angewendet wurde:
- es laufen viele Sitzungen auf dem VM des Hyper-V.
- eine große Menge von Daten wird auf das VM des Hyper-V übertragen.

Vorbereiten von WMI für Windows-Server

IT Operations Analyzer ermittelt und überwacht Windows-Server über WMI (Windows Management Instrumentation). In den folgenden Abschnitten werden die Aufgaben im Zusammenhang mit der Aktivierung des Remote-Zugriffs auf WMI sowie die Konfiguration der Windows 2003/2003 R2-Server mit FC HBA beschrieben.

HINWEIS:

- Für Microsoft Hyper-V-Knoten und Windows-Server-Knoten können Sie Leistungsdaten zur Festplatte über FC-Verbindung, iSCSI-Verbindung und lokale Verbindung abrufen. Leistungsdaten zum CD-ROM-Laufwerk und USB-Speicher können nicht abgerufen werden. Wenn Leistungsdaten nicht abgerufen werden können, zeigt in der Registerkarte **Leistung** des **Überwachungsmoduls** das Symbol für die Leistungsmetrik den Status „Unbekannt" an.
- Für Windows Server 2003 wenden Sie bitte KB953955 an. Andernfalls können für den CPU-Namen falsche Werte berichtet werden.

Vorbereiten des Verwaltungsservers

Zur Überwachung von Windows-Computern oder Windows Storage Servern muss DCOM auf dem Verwaltungsserver aktiviert sein. Siehe Zulassen der Remote-Ausführung für DCOM siehe Seiten 2-4.

Vorbereiten der Windows-Computer und Windows Storage Server

Tabelle 2-1 enthält eine Aufstellung der Informationen, die für die Überwachung benötigt werden.

Tabelle 2-1: Informationen für die Verbindung zu Windows-Servern

Element	Details
IP-Adresse	IP-Adresse des zu überwachenden Windows-Servers
Benutzername	Benutzerkonto mit Administratorrechten für den zu überwachenden Windows-Server
Domänenname	Domänenname des Benutzers (wenn es sich bei dem o. g. Benutzerkonto um das eines Domänenbenutzers handelt)
Kennwort	Kennwort für den entsprechenden Benutzernamen

Um Windows-Server zu überwachen, müssen DCOM geprüft und alle WMI-Ausnahmen zur Windows-Firewall hinzugefügt werden. Wenn Sie FC HBA-Informationen mit Windows Server 2003 oder 2003 Windows Server R2 abrufen möchten, installieren Sie das Tool „Fibre Channel Information" (fcinfo).

Installieren des fcinfo-Tools (Fibre Channel Information)

Das fcinfo-Tool ist erforderlich, wenn Sie einen Host Bus Adapter (HBA) für die Verbindung zwischen Fibre-Channel-SAN-Festplattengeräten und dem zu überwachenden Server nutzen. Es unterstützt die HBA-API für Fibre Channel unter Windows und stellt mit WMI kompatible Funktionen bereit. Siehe Microsoft Download Center unter: http://www.microsoft.com/downloads/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

Hinzufügen einer WMI-Ausnahme zur Windows-Firewall

Sie können die Berechtigungen entweder über die Windows-Eingabeaufforderung oder den Gruppenrichtlinien-Editor ändern. Die folgenden Anweisungen gelten für Windows Server 2003. Einzelheiten zu Windows Server 2008 und Windows Server 2012 finden Sie unter Anwenden der Konfigurationseinstellungen für Windows Server 2008 oder Windows Server 2012 siehe Seiten 2-5.

Verwenden der Windows-Eingabeaufforderung:

1. Melden Sie sich beim Server an, und klicken Sie auf **Start** und **Ausführen**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zu den Befehlen Start und Ausführen zu navigieren, anders.

2. Geben Sie an der Eingabeaufforderung **cmd** ein, und klicken Sie auf **OK**.
3. Geben Sie an der Eingabeaufforderung Folgendes ein, und drücken Sie die **Eingabetaste**:

```
netsh firewall set service RemoteAdmin enable
```

Verwenden des Gruppenrichtlinien-Editors:

1. Melden Sie sich beim Server an, und klicken Sie auf **Start** und **Ausführen**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zu den Befehlen Start und Ausführen zu navigieren, anders.

2. Zum Starten des **Gruppenrichtlinien-Editors** geben Sie **gpedit.msc** ein und klicken auf **OK**.
3. Erweitern Sie unter **Richtlinie für „Lokaler Computer"** den Ordner **Administrative Vorlagen**.
4. Erweitern Sie die Ordner: **Netzwerk**, **Netzwerkverbindungen** und **Windows-Firewall**, und wählen Sie **Domänenprofil**.
5. Klicken Sie in der Einstellungsliste mit der rechten Maustaste auf **Windows-Firewall: Remoteverwaltungsausnahme zulassen** und anschließend auf **Eigenschaften**.
6. Klicken Sie auf **Aktiviert** und dann auf **OK**.

HINWEIS: Details finden Sie im Microsoft Developer Center unter: http://msdn2.microsoft.com/en-us/library/aa389286(VS.85).aspx

Zulassen der Remote-Ausführung für DCOM

Wenn Sie dcomcnfg.exe über die Windows-Eingabeaufforderung ausführen, können Sie das Fenster Komponentendienste öffnen und den DCOM-Status überprüfen.

1. Melden Sie sich beim Server an, und klicken Sie auf **Start** und **Ausführen**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zu den Befehlen **Start** und **Ausführen** zu navigieren, anders.

2. Zum Starten der **Komponentendienste** geben Sie **dcomcnfg.exe** ein und klicken auf **OK**.
3. Wählen Sie unter **Komponentendienste** die Optionen **Computer** und **Arbeitsplatz**.
4. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und wählen Sie **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Standardeigenschaften**.
6. Aktivieren Sie das Kontrollkästchen **DCOM (Distributed COM) auf diesem Computer aktivieren**, und klicken Sie auf die Registerkarte **COM-Sicherheit**.
7. Zum Anzeigen des Dialogfelds **Startberechtigung** klicken Sie unter **Start- und Aktivierungsberechtigungen** auf **Limits bearbeiten**. Wenn ein Benutzername oder eine Gruppe nicht im Feld **Gruppen- oder Benutzernamen** angezeigt wird, gehen Sie folgendermaßen vor:
   a. Klicken Sie auf **Hinzufügen**.
   b. Fügen Sie im Dialogfeld **Benutzer oder Gruppen auswählen** unter **Geben Sie die zu verwendenden Objektnamen ein** den Benutzernamen und die Gruppe hinzu. Klicken Sie auf **OK**.
   c. Klicken Sie im Dialogfeld **Startberechtigung** im Bereich **Gruppen- oder Benutzernamen** auf den Benutzer und die Gruppe. Aktivieren Sie im Bereich der **Benutzerberechtigungen** unter **Remoteaktivierung** in der Spalte **Zulassen**. Klicken Sie auf **OK**.

Anwenden der Konfigurationseinstellungen für Windows Server 2008 oder Windows Server 2012

Wenn Sie Windows Server 2008 oder Windows Server 2012 verwenden, ist neben den in den vorherigen Abschnitten beschriebenen Windows-Servereinstellungen eine der folgenden Bedingungen erforderlich:

- Verwenden des integrierten Administratorkontos
- Verwenden eines Domänen-Benutzerkontos
- Aktivieren der WMI-Remote-Verbindung über das lokale Administratorkonto

Aktivieren von lokalen Administratorkonten für die WMI-Remote-Verbindung

Sie können die Einstellung der Benutzerkontensteuerung (UAC) entweder von der Systemsteuerung des überwachenden Zielcomputers oder durch Anwenden der Einstellungsmethoden von der Registry aus ändern.

So wechseln Sie von der Systemsteuerung aus die UAC:

1. Klicken Sie im Menü **Start** auf **Systemsteuerung**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zum Startmenü zu navigieren, anders.

2. Wählen Sie **Benutzerkonten** und dann **Einstellung der Benutzerkontensteuerung ändern**.
3. Setzen Sie die UAC-Ebene auf **Nie benachrichtigen**.
4. Starten Sie den Computer neu.

Eine andere Methode zur Überwachung eines Zielcomputers besteht darin, den Schlüssel **LocalAccountTokenFilterPolicy** in der Registry zu registrieren und ihn auf dem überwachenden Zielcomputer als **1** einzustellen. Deaktivieren Sie anschließend **Filtern nach Benutzerkontensteuerung**, wodurch lokale Administratorrechte während der WMI-Remote-Verbindung unterdrückt werden.

Über das lokale Administratorkonto können Sie Windows Server 2003 und Windows Server 2008 oder Windows Server 2012 verwalten. Wenn Sie die Registry bearbeiten, kann ein schwerwiegender Fehler auftreten, der sich möglicherweise auf das gesamte System auswirkt. Es wird empfohlen, die Registry vor der Bearbeitung zu sichern.

Details erhalten Sie unter der folgenden Adresse. Dort finden Sie eine Beschreibung der UAC und der Remotebeschränkungen unter Windows Vista: http://support.microsoft.com/kb/951016/en-us

Nutzen Sie für die Konfiguration der Registry eine der folgenden Methoden:

- Registry-Editor
- Befehl reg

Verwenden des Registry-Editors:

1. Klicken Sie auf **Start** und **Ausführen**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zu den Befehlen **Start** und **Ausführen** zu navigieren, anders.

2. Geben Sie an der Eingabeaufforderung **regedit** ein, und klicken Sie auf **OK**.

   Der **Registry-Editor** wird angezeigt.

3. Suchen Sie nach dem folgenden Unterschlüssel:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
4. Wenn der Schlüssel **LocalAccountTokenFilterPolicy** nicht vorhanden ist, fügen Sie ihn hinzu:
   a. Wählen Sie im Menü **Bearbeiten** die Optionen **Neu** und **DWORD** aus.
   b. Geben Sie **LocalAccountTokenFilterPolicy** ein, und betätigen Sie die **Eingabetaste**.
5. Wenn der Wert für **LocalAccountTokenFilterPolicy** nicht **1** beträgt, ändern Sie ihn in **1**:
   a. Klicken Sie mit der rechten Maustaste auf **LocalAccountTokenFilterPolicy**, und wählen Sie **Bearbeiten**.
   b. Geben Sie in das Eingabefeld **1** ein, und klicken Sie auf **OK**.
6. Schließen Sie den **Registry-Editor**.

Verwenden des reg-Befehls:

1. Klicken Sie auf **Start** und **Ausführen**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zu den Befehlen **Start** und **Ausführen** zu navigieren, anders.

2. Geben Sie an der Eingabeaufforderung Folgendes ein:
   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0x1 /f
3. Klicken Sie auf **OK**.

Überprüfen, ob in der Gerätemanager-Struktur des Knotens doppelte Netzwerkadapternamen vorhanden sind

Wenn in der Gerätemanager-Struktur des Knotens doppelte Netzwerkadapternamen vorhanden sind, kann IT Operations Analyzer die folgenden Leistungsdaten nicht korrekt darstellen:

- Netzwerk durchschnittliche Paket-Empfangsmenge [Pakete/Sekunde]
- Netzwerk durchschnittliche Paket-Sendemenge [Pakete/Sekunde]

So überprüfen Sie im Gerätemanager, ob doppelte Netzwerkadapternamen vorhanden sind:

1. Klicken Sie auf **Start** > **Computer** > **Systemeigenschaften**.
   Das Pop-up-Menü **Systemeigenschaften** wird angezeigt.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zum **Startmenü** zu navigieren, anders.

2. Klicken Sie auf die Registerkarte **Hardware**.
3. Klicken Sie auf **Device Manager**.
4. Überprüfen Sie die Struktur des **Device Manager**, um zu sehen, ob im Abschnitt **Netzwerkadapter** doppelte Namen angezeigt werden.

HINWEIS: Wenn doppelte Netzwerkadapternamen aufgelistet sind, können Sie die genauen Leistungsdaten über Netzwerk durchschnittliche Paket-Sendemenge [Pakete/Sekunde] nicht anzeigen. Zwischen dem tatsächlichen Wert und den angezeigten Leistungsdaten besteht ein Unterschied. Es wird empfohlen, dass Sie Ihre IT-Services-Gruppe davon in Kenntnis setzen, dass die Netzwerkadapter umbenannt werden müssen, um Verdopplungen zu vermeiden.

3

Vorbereiten von SSH für Linux-/Solaris-Server

IT Operations Analyzer verwendet SSH zur Ermittlung von Linux- und Solaris-Servern. Die Überwachung der Server erfolgt außerdem über Kennwortauthentifizierung (nicht Zertifikatsauthentifizierung). In diesem Kapitel wird das Konfigurieren der Linux- und Solaris-Server beschrieben.

- Installieren der benötigen Pakete
- Ermitteln von Verbindungseinstellungen basierend auf der Anmeldemethode
- Anwenden von SSH-Server-Sicherheitseinstellungen

Installieren der benötigen Pakete

Für CentOS müssen erforderliche Pakete installiert werden.

Tabelle 3-1: Beispielpakete, die für CentOS hinzugefügt werden müssen

Paket	Im Paket, das IT Operations Analyzer ausführt, enthaltene Befehle
smartmontools	/usr/sbin/smartctl
nfs-utils	/usr/sbin/exportfs
pciutils	/sbin/lspci
iscsi-initiator-utils	/sbin/iscsid

Für SUSE Linux 11 SP1 und SP2 müssen erforderliche Pakete installiert werden.

Tabelle 3-2: Beispielpaket, das für SUSE Linux 11 SP1 und SP2 hinzugefügt werden muss

Paket	Im Paket, das IT Operations Analyzer ausführt, enthaltene Befehle
nfs-kernel-server	/usr/sbin/exportfs

Ermitteln von Verbindungseinstellungen basierend auf der Anmeldemethode

Es gibt verschiedene SSH-Anmeldemethoden, wenn Informationen vom Linux- oder Solaris-Server abgerufen werden sollen:

- Als **root-Benutzer** können Sie sich direkt mit SSH anmelden.
- Als **normaler Benutzer** führen Sie nach der Anmeldung mit SSH folgende Befehle aus:
  - `su`-Befehl für root-Berechtigungen
  - `sudo-/pfexec`-Befehl für root-Berechtigungen.

Für jede der Anmeldemethoden sind bestimmte Verbindungseinstellungen erforderlich. Diese Einstellungen werden in den folgenden Abschnitten beschrieben.

HINWEIS: Für Linux-/Solaris-Knoten können Leistungsdaten zum Mount-Point mit Lese-/Schreibberechtigung abgerufen werden. Leistungsdaten zu Windows-Partition und CD-ROM-Laufwerk können nicht mit Leseberechtigung abgerufen werden. Wenn Leistungsdaten nicht abgerufen werden können, zeigt in der Registerkarte **Leistung** des **Überwachungsmoduls** das Symbol für die Leistungsmetrik den Status „Unbekannt" an.

Einstellungen der Verbindungsmethode für root-Benutzer

Die folgende Konfiguration ist erforderlich:

- Aktivieren der Verbindung mit SSH2
- Zulassen der SSH-Kennwortauthentifizierung
- Zulassen der root-Anmeldung mit SSH

Tabelle 3-3: Verbindungseinstellungen für Linux-/Solaris-Server (root-Benutzer)

Einstellung	Details
IP-Adresse	Geben Sie die IP-Adresse des zu überwachenden Linux-/Solaris-Servers an.
Port-Nummer	Geben Sie die SSH-Port-Nummer des zu überwachenden Linux-/Solaris-Servers an.
Benutzername	Geben Sie `root` an.
Kennwort	Geben Sie das root-Kennwort an.
root-Kennwort	Lassen Sie dieses Feld leer.

Einstellungen der Verbindungsmethode für normale Benutzer (su-Befehl)

Die folgende Konfiguration ist erforderlich:

- Aktivieren der Verbindung mit SSH2
- Zulassen der SSH-Kennwortauthentifizierung

Tabelle 3-4: Verbindungseinstellungen für Linux-/Solaris-Server (su-Befehl)

Einstellung	Details
IP-Adresse	Geben Sie die IP-Adresse des zu überwachenden Linux-/Solaris-Servers an.
Port-Nummer	Geben Sie die SSH-Port-Nummer des zu überwachenden Linux-/Solaris-Servers an.
Benutzername	Geben Sie die Benutzer-ID an, die Sie für die Anmeldung verwendet haben.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.
root-Kennwort	Geben Sie das root-Kennwort an.

Einstellungen der Verbindungsmethode für normale Benutzer (sudo-Befehl)

Die folgende Konfiguration ist erforderlich:

- Aktivieren der Verbindung mit SSH2
- Zulassen der SSH-Kennwortauthentifizierung
- Fügen Sie Definitionen für die Einstellungen von sudo/pfexec hinzu. Weitere Informationen finden Sie in Hinzufügen der Definition der sudo-Einstellungen (Linux) siehe Seiten 3-7.
- Fügen Sie Definitionen für das Profil für Solaris hinzu. Weitere Informationen finden Sie in Hinzufügen des Profils für pfexec (Solaris) siehe Seiten 3-9.

Tabelle 3-5: Verbindungseinstellungen für Linux-/Solaris-Server (sudo-Befehl)

Einstellung	Details
IP-Adresse	Geben Sie die IP-Adresse des zu überwachenden Linux-/Solaris-Servers an.
Port-Nummer	Geben Sie die SSH-Port-Nummer des zu überwachenden Linux-/Solaris-Servers an.
Benutzername	Geben Sie die Benutzer-ID an, die Sie für die Anmeldung verwendet haben.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.
root-Kennwort	Lassen Sie dieses Feld leer.

HINWEIS: Bei der Verwendung von SSH ist in puncto Sicherheit Folgendes zu beachten:

- Das Zulassen der root-Anmeldung ist die einfachste Konfigurationsmöglichkeit. Die öffentliche Weitergabe des root-Kennworts kann jedoch zu Verfälschungen der Servereinstellungen führen. Diese Methode sollte nur zugelassen werden, wenn nicht autorisierte Zugriffe auf die Umgebung verhindert werden können.
- Einem normalen Benutzer die Berechtigung zum Ausführen des Befehls `su root` mit untersagter root-Anmeldung zu erteilen, ist sicherer, als die root-Anmeldung zuzulassen, sofern die Benutzer-ID und das Kennwort des Benutzers geheim bleiben.
- Da die Gefahr des Ausspionierens beim SSH1-Protokoll größer ist als beim SSH2-Protokoll, wird das SSH2-Protokoll empfohlen.
- Wenn die Kennwortauthentifizierung zugelassen wird, stellt dies ein größeres Sicherheitsrisiko dar, als wenn nur die Authentifizierung über einen öffentlichen Schlüssel zulässig ist. Da IT Operations Analyzer die Authentifizierung über einen öffentlichen Schlüssel nicht abwickeln kann, bietet die Verwendung von Ports (mit Ausnahme von Port 22) ein höheres Maß an Sicherheit bei der Kennwortauthentifizierung.

Anwenden von SSH-Server-Sicherheitseinstellungen

Dieser Abschnitt enthält Anweisungen für folgende Aufgaben:

- Aktivieren der SSH2-Verbindung
- Zulassen der SSH-Kennwortauthentifizierung
- Zulassen der root-Anmeldung mit SSH
- Hinzufügen der Definition der sudo-Einstellungen (Linux)
- Hinzufügen des Profils für pfexec (Solaris)

Vorbereitung

- Vergewissern Sie sich, dass der SSH-Service (sshd daemon) installiert und aktiv ist.
- Wenn Sie andere SSH-Software verwenden, konfigurieren Sie anhand des zugehörigen Softwarehandbuchs die entsprechenden Einstellungen. Linux enthält OpenSSH.
- Bereiten Sie die Umgebung so vor, dass Sie sich beim Zielserver für die Überwachung anmelden und die Systemshell bedienen können.
- Melden Sie sich von der Serverkonsole aus an, oder melden Sie sich per Remote-Zugriff mit SSH oder Telnet an. Die Anmeldung von einer lokalen Konsole aus wird empfohlen, um Probleme beim Wiederherstellen der Verbindung zu vermeiden (für den Fall, dass die Konfigurationseinstellungen nicht fehlerfrei sind).
- Bereiten Sie das root-Kennwort vor (root-Berechtigung ist erforderlich).
- Aktivieren Sie nach der Anmeldung als root-Benutzer oder normaler Benutzer die root-Berechtigung mithilfe des `su root`-Befehls.

Aktivieren der SSH2-Verbindung

1. Öffnen Sie die Datei **/etc/ssh/sshd_config** in einem Editor.
2. Durchsuchen Sie die Datei **sshd_config** nach dem Schlüsselwort **Protocol** (Protokoll).
   - Wenn keine Beschreibung vorhanden oder der Eintrag **Protocol** auskommentiert ist, sind die Protokolle SSH1 und SSH2 aktiviert. Es sind keine Änderungen erforderlich.
   - Wenn der Eintrag **Protocol 1** gefunden wird, ist nur das Protokoll SSH1 aktiviert. Ändern Sie diesen Eintrag in **Protocol 1, 2**.
   - Wenn der Eintrag **Protocol 2** gefunden wird, ist nur das Protokoll SSH2 aktiviert. Es sind keine Änderungen erforderlich.
   - Wenn der Eintrag **Protocol 1, 2** oder **Protocol 2, 1** gefunden wird, sind beide Protokolle, SSH1 und SSH2, aktiviert. Es sind keine Änderungen erforderlich.
3. Speichern Sie die Datei, und schließen Sie den Editor. Führen Sie zum Überprüfen von Einstellungsfehlern den entsprechenden Befehl aus:

   Linux: `/usr/sbin/sshd -t`

   Solaris: `/usr/lib/ssh/sshd -t`

- Wenn keine Meldung angezeigt wird, bedeutet dies, dass die Syntax oder der Bereich fehlerfrei ist.
- Es wird eine Fehlermeldung angezeigt, wenn die Syntax oder der Bereich fehlerhaft ist.

Beispiel für eine fehlerhafte Protokoll-Einstellung (Protocol 2, 3):

```
[root@linuxhost ssh]# /usr/sbin/sshd -t
ignoring bad proto spec: '3'.
```

4. Starten Sie den SSH-Service erneut, indem Sie den entsprechenden Befehl ausführen:
   - Linux: `service sshd restart`
   - Solaris 9: `/etc/init.d/sshd restart`
   - Solaris 10: `svcadm restart ssh`
5. Wenn **OK** für die Einträge **Stopping/Starting** (Anhalten/Starten) angezeigt wird, wird der Service ordnungsgemäß ausgeführt. Beispiel: `Stopping sshd: [ OK ]`

Zulassen der SSH-Kennwortauthentifizierung

HINWEIS: Informationen zum Bearbeiten der Datei **/etc/ssh/sshd_config** und zum Neustart des SSH-Services enthält der vorherige Abschnitt, Aktivieren der SSH2-Verbindung.

Durchsuchen Sie die Datei **/etc/ssh/sshd_config** nach dem Schlüsselwort **PasswordAuthentication** (Kennwortauthentifizierung).

- Wenn keine Beschreibung vorhanden oder der Eintrag **PasswordAuthentication** auskommentiert ist, ist die Kennwortauthentifizierung aktiviert. Es sind keine Änderungen erforderlich.
- Wenn der Eintrag **PasswordAuthentication no** gefunden wird, ist die Kennwortauthentifizierung nicht zulässig (es ist nur die Authentifizierung über einen öffentlichen Schlüssel aktiviert). Ändern Sie den Eintrag in **PasswordAuthentication yes**.
- Wenn der Eintrag **PasswordAuthentication yes** gefunden wird, ist die Kennwortauthentifizierung zulässig. Es sind keine Änderungen erforderlich.

Zulassen der root-Anmeldung mit SSH

HINWEIS: Informationen zum Bearbeiten der Datei **/etc/ssh/sshd_config** und zum Neustart des SSH-Services enthält der vorherige Abschnitt, Aktivieren der SSH2-Verbindung.

Durchsuchen Sie die Datei **/etc/ssh/sshd_config** nach dem Schlüsselwort **PermitRootLogin** (root-Anmeldung zulassen).

- Wenn keine Beschreibung vorhanden oder der Eintrag **PermitRootLogin** auskommentiert ist, ist die root-Anmeldung standardmäßig aktiviert. Es sind keine Änderungen erforderlich.
- Wenn der Eintrag **PermitRootLogin no** gefunden wird, ist die root-Anmeldung nicht zulässig (es sind nur normale Benutzer zulässig). Ändern Sie den Eintrag in **PermitRootLogin yes**.
- Wenn der Eintrag **PermitRootLogin yes** gefunden wird, ist die root-Anmeldung zulässig. Es sind keine Änderungen erforderlich.

Hinzufügen der Definition der sudo-Einstellungen (Linux)

Die Einstellungen für den Befehl **sudo** sind in der Datei **/etc/sudoers** beschrieben. Bearbeiten Sie die Datei ausschließlich mit dem Befehl **visudo**, weil dieser eine Ausschlusssteuerung und Syntaxüberprüfung ermöglicht.

1. Führen Sie den Befehl **visudo** aus. Bei normaler Ausführung des Befehls wird ein Editor geöffnet.

HINWEIS: Wenn der Befehl **visudo** gleichzeitig an verschiedenen Stellen ausgeführt wird, wird der Editor nicht geöffnet und stattdessen eine Fehlermeldung angezeigt:

```
[root@linuxhost ssh]# visudo
visudo: sudoers file busy, try again later
```

Wenn die Fehlermeldung angezeigt wird, obwohl der Befehl nicht gleichzeitig mehrfach ausgeführt wurde, dann wurde möglicherweise bei der vorherigen Ausführung des Befehls die Verbindung unterbrochen, aber der Prozess ist noch aktiv. Brechen Sie in diesem Fall den Prozess **visudo** ab.

2. Fügen Sie der Datei Zeilen hinzu, um Benutzern die Ausführung der Befehle ohne Kennwort zu ermöglichen.

   RedHat Linux 5.x:

   ```
   /usr/sbin/dmidecode
   /usr/sbin/smartctl
   /sbin/ethtool
   ```

   RedHat Linux 6.x:

   ```
   /usr/sbin/dmidecode
   /usr/sbin/smartctl
   /sbin/ethtool
   /usr/sbin/exportfs
   ```

   SUSE Linux 10:

   ```
   /usr/sbin/dmidecode
   /usr/sbin/smartctl
   /bin/cat
   /usr/sbin/ethtool
   ```

   SUSE Linux 11:

   ```
   /usr/sbin/dmidecode
   /usr/sbin/smartctl
   /bin/cat
   /sbin/ethtool
   ```

   SUSE Linux 11 SP 1 und SP 2:

   ```
   /usr/sbin/dmidecode
   /usr/sbin/smartctl
   /bin/cat
   /sbin/ethtool
   /usr/sbin/exportfs
   ```

CentOS und Oracle Linux 6.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
/usr/sbin/exportfs
```

Beispiel: Wenn ein Benutzername, der für die Verbindung verwendet wird, **sshconn** lautet und der betreffende Servername **linuxhost** ist, geben Sie in /etc/sudoers in SUSE Linux 11 folgendes Script ein:

```
sshconn linuxhost=NOPASSWD: /usr/sbin/dmidecode
sshconn linuxhost=NOPASSWD: /usr/sbin/smartctl
sshconn linuxhost=NOPASSWD: /bin/cat
sshconn linuxhost=NOPASSWD: /sbin/ethtool
```

3. Speichern Sie die Datei, und schließen Sie den Editor.

   Wenn ein Syntaxfehler vorliegt, wird eine Fehlermeldung angezeigt und der Speichervorgang zurückgestellt.

   - Wenn Sie **e** eingeben, wird der Editor erneut geöffnet. Nehmen Sie die Änderung vor, und speichern Sie die Datei.
   - Wenn Sie **x** eingeben, wird die Änderung verworfen, und Sie können zum Status vor der Ausführung des Befehls visudo zurückkehren.
   - Wenn Sie **Q** eingeben, wird die Speicherung der Änderung erzwungen, obwohl sie Fehler enthält. Wenn Ihnen beispielsweise beim Eingeben von NOPASSWD ein Tippfehler unterläuft, wird folgende Fehlermeldung angezeigt:

     ```
     Warning: undeclared Cmnd_Alias `NOPASSWD' referenced
     near line 92
     >>> sudoers file: syntax error? line 91 <<<
     What now?
     ```

HINWEIS: Lassen Sie Vorsicht walten, wenn Sie das Speichern von Änderungen erzwingen, deren Ergebnis Ihnen nicht bekannt ist. Wenn Sie nicht sicher sind, welches Ergebnis eine Änderung haben wird, sollten Sie deren Speicherung nicht erzwingen.

Hinzufügen des Profils für pfexec (Solaris)

Um eine root-Berechtigung mithilfe von pfexec zu vergeben, fügen Sie das Profil **/etc/security/prof_attr** und **/etc/security/exec_attr** hinzu, und weisen Sie anschließend das Profil dem Benutzer zu.

1. Führen Sie `vi /etc/security/prof_attr` aus.
   - Bei korrektem Start wird der Editor geöffnet.
   - Falls eine Fehlermeldung angezeigt wird, aber nicht gleichzeitig ein Befehl ausgeführt wird, könnte die Verbindung bei einer früheren Ausführung des Befehls eingeschränkt worden sein, wodurch der Prozess aufrechterhalten wurde. Brechen Sie in diesem Fall den Prozess **vi** ab.
2. Registrieren Sie das Profil. Wenn der Profilname beispielsweise HITOA lautet, wird er wie folgt angegeben: **HITOA::::**
3. Speichern Sie die Datei, und schließen Sie den Editor.
4. Führen Sie `vi/etc/security/exec_attr` aus. Bei korrektem Start wird der Editor geöffnet.
5. Fügen Sie die folgenden vier Zeilen hinzu, um den Befehl ohne Kennwort auszuführen:

   ```
   /sbin/ifconfig
   /usr/sbin/prtvtoc
   /usr/sbin/luxadm
   /usr/sbin/iscsiadm
   ```

   Wenn der Profilname beispielsweise **HITOA** lautet, sieht die Beschreibung folgendermaßen aus:

   ```
   HITOA:suser:cmd:::/sbin/ifconfig:euid=0
   HITOA:suser:cmd:::/usr/sbin/prtvtoc:euid=0
   HITOA:suser:cmd:::/usr/sbin/luxadm:euid=0
   HITOA:suser:cmd:::/usr/sbin/iscsiadm:euid=0
   ```
6. Speichern Sie die Datei, und schließen Sie den Editor.
7. Weisen Sie das Profil dem Benutzer zu. Wenn der Benutzername beispielsweise **sshconn** lautet, wird der folgende Befehl ausgeführt: `usermod –P HITOA sshconn`

4

Vorbereiten von VMware für ESX-Server

IT Operations Analyzer kann Windows- oder Linux-Server auf virtuellen Maschinen nur richtig überwachen, wenn VMware-Tools installiert sind. In diesem Kapitel wird die Vorbereitung der ESX-Server beschrieben.

- Ermitteln der Verbindungsinformationen für ESX-Server
- Installieren von VMware-Tools auf virtuellen Maschinen

Ermitteln der Verbindungsinformationen für ESX-Server

In der folgenden Tabelle sind die Informationen angegeben, die für die Verbindung zu einem ESX-Server erforderlich sind. Für die Ermittlung sind keine zusätzlichen Zugangsdaten erforderlich (nur der Benutzername und das Kennwort, wie in Tabelle 4-1 angegeben).

Tabelle 4-1: Informationen für die Verbindung zu VMware ESX-Servern

Element	Details
IP-Adresse	Verwenden Sie die IP-Adresse des ESX-Servers.
Port-Nummer	Geben Sie die vom ESX-Server verwendete Port-Nummer an.
Protokoll	Verwenden Sie basierend auf der Konfiguration des ESX-Servers entweder das HTTP- oder HTTPS-Protokoll.
Benutzername	Verwenden Sie den Benutzernamen des Administrators für den ESX-Server.
Kennwort	Verwenden Sie das Kennwort für den ESX-Server.

Installieren von VMware-Tools auf virtuellen Maschinen

Wenn ein Windows- oder Linux-Server als virtuelle Maschine überwacht werden soll, müssen VMware-Tools unter jedem Gast-Betriebssystem der virtuellen Maschine installiert werden, damit Sie Informationen vom ESX-Server abrufen können.

Wenn keine VMware-Tools installiert sind, wird weder der Status der virtuellen Maschine noch die Beziehung zwischen Hostrechner und Gast-Betriebssystem richtig angezeigt.

Beachten Sie, dass das Gast-Betriebssystem als separater Knoten verwaltet wird.

Weitere Informationen zur Installation dieser Tools finden Sie im Produkthandbuch für ESX-Server, *Basic System Administration*, das unter folgender URL verfügbar ist:

http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_admin_guide.pdf

Wenn eine kostenlose Version von ESX zur Verwaltung angezielt wird, ist es möglich, dass IT Operations Analyzer den Zustand des Laufwerks nicht genau abfragt.

HINWEIS: IT Operations Analyzer unterstützt nicht die Überwachung von VMware ESX-Servern, die als aktivierter verteilter virtueller Switch fungieren. Wenn IT Operations Analyzer die Konfigurationsinformationen eines aktivierten verteilten virtuellen Switches entsprechend des Ablaufplans erneut erfasst oder aktualisiert, werden jedoch Informationen zu nderungsereignissen in der VMKernel-NIC, die dem verteilten virtuellen Switch zugewiesen ist, und der Service Console-NIC protokolliert.

5

Vorbereiten von SNMP für IP-Switches

IT Operations Analyzer kann SNMP-Traps von IP-Switches empfangen. In diesem Kapitel wird das Konfigurieren der IP-Switches beschrieben.

Übersicht

IT Operations Analyzer kann die IP-Switches in Ihrer Umgebung überwachen, wenn folgende Bedingungen erfüllt sind:

- SNMP Version 1 ist installiert und aktiv.
- MIB-II ist unter Ihrem Community-Namen für den Lesezugriff freigegeben.
- Bridge MIB ist unter Ihrem Community-Namen für den Lesezugriff freigegeben.

Zur Überwachung von IP-Switches werden die in Tabelle 5-1 und Tabelle 5-2 angegebenen Daten benötigt.

Tabelle 5-1: Informationen für die Verbindung zu IP-Switches: SNMP-Version 1 oder 2C

Element	Details
IP-Adresse	Adresse des SNMP-IP-Switch-Knotens
Port-Nummer	Port-Nummer, an der der SNMP-IP-Switch auf Verbindungen wartet (Port 161)
Community-Name	Für SNMP-IP-Switches verwendeter Community-Name

Tabelle 5-2: Informationen für die Verbindung zu IP-Switches: SNMP-Version 3

Element	Details
IP-Adresse	Adresse des SNMP-IP-Switch-Knotens
Port-Nummer	Port-Nummer, an der der SNMP-IP-Switch auf Verbindungen wartet (Port 161)
Benutzername	Für SNMP-IP-Switches verwendeter Benutzername
Sicherheitsstufe	Die zur Kommunikation in SNMPv3 benötigte Sicherheitsstufe. Optionen: noAuthNoPriv, authNoPriv, authPriv
Authentifizierungsmethode	Die zur Kommunikation in SNMPv3 benötigte Authentifizierungsmethode. Optionen: MD5, SHA
Authentifizierungskennwort	Das zur Kommunikation in SNMPv3 benötigte Authentifizierungskennwort.
Verschlüsselungsmethode	Die zur Kommunikation in SNMPv3 benötigte Verschlüsselungsmethode. Optionen: DES, AES128
Verschlüsselungskennwort	Das zur Kommunikation in SNMPv3 benötigte Verschlüsselungskennwort.

Mithilfe dieser optionalen Einstellungen kann die Genauigkeit der erfassten Daten sichergestellt werden:

- Virtual Bridge MIB ist unter Ihrem Community-Namen für den Lesezugriff freigegeben.
- Cisco VTP MIB ist unter Ihrem Community-Namen für den Lesezugriff freigegeben.
- Extreme FDB MIB ist unter dem Community-Namen für den Lesezugriff freigegeben.
- SNMP Version 1, 2c oder Version 3 ist installiert und läuft.

- Interfaces Group MIB ist unter dem Community-Namen für den Lesezugriff freigegeben.

HINWEIS: Der zu überwachende IP-Switch muss die beiden folgenden Bedingungen erfüllen:
-RFC1213: SNMP V1 MIB-II wird unterstützt.
-RFC1493: SNMP V1 Bridge MIB wird unterstützt
Um sicherzustellen, dass die Funktionen RCA und Topologieansicht richtig funktionieren, überprüfen Sie, ob entweder RFC2674 (Virtual Bridge MIB) (oder RFC4363 (Virtual Bridge MIB)) oder Cisco VTP MIB unterstützt wird. Wenn Sie IP-Switches von Extreme Networks® überwachen, verwenden Sie ExtremeXOS® (Version 12.1.2 oder höher).

Beispiel für die Konfiguration eines Cisco IP-Switches (IOS)

Für SNMPv1 oder v2c:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `enable` ein. Geben Sie bei entsprechender Aufforderung Ihr Kennwort ein.
   b. Geben Sie `configure terminal` ein.
   c. Geben Sie `snmp-server community public RO` ein. (Wobei `public` der Community-Name ist und nach Bedarf geändert werden kann.)
   d. Geben Sie `end` ein.
   e. Geben Sie `show running-config` ein, und bestätigen Sie anschließend die Einstellungen.
2. Trennen Sie die Telnet-Verbindung.

Für SNMPv3:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `enable` ein. Geben Sie bei entsprechender Aufforderung Ihr Kennwort ein.
   b. Geben Sie `configure terminal` ein.
   c. Geben Sie `snmp-server view allView` ein. (Wobei `allView` der Ansichtsname ist und nach Bedarf geändert werden kann.)
   d. Erzeugen Sie eine Ansicht.
   e. Geben Sie `snmp-server group privGroup v3 priv read allView notify allView` ein. (Wobei `privGroup` der Gruppenname ist und nach Bedarf geändert werden kann, und `allView` der Anzeigename ist, den Sie in Schritt c angegeben haben.)
   f. Erzeugen Sie eine Gruppe.

g. Geben Sie `snmp-server user Md5DesUser privGroup v3 auth md5 password1 priv des password2` ein. (Dabei gilt:
`Md5DesUser` ist ein Benutzername und kann nach Bedarf geändert werden.
`privGroup` ist der Gruppenname, den Sie in Schritt e angegeben haben.
`md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
`password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.
`des` ist die Verschlüsselungsmethode und kann nach Bedarf geändert werden.
`password2` ist das Verschlüsselungskennwort und kann nach Bedarf geändert werden.)
Legen Sie das Kennwort und die Authentifizierungsmethode/ Verschlüsselung/Kennwort entsprechend der Sicherheitsstufe fest.

h. Erzeugen Sie einen Benutzer.

i. Geben Sie `end` ein.

2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines Cisco (Catalyst) IP-Switches (IOS)

Für SNMP v3:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `enable` ein. Geben Sie bei entsprechender Aufforderung Ihr Kennwort ein.
   b. Geben Sie `configure terminal` ein.
   c. Geben Sie `snmp-server view allView iso included` ein. (Wobei `allView` der Ansichtsname ist und nach Bedarf geändert werden kann.)
   d. Erzeugen Sie eine Ansicht.
   e. Geben Sie `snmp-server group authGroup v3 auth read allView notify allView` ein. (Wobei `authGroup` der Gruppenname ist und nach Bedarf geändert werden kann, und `allView` der Anzeigename ist, den Sie in Schritt c angegeben haben.)
   f. Erzeugen Sie eine Gruppe.
   g. Geben Sie `snmp-server user Md5NoneUser authGroup v3 auth md5 password1` ein. (Dabei gilt:
   `Md5NoneUser` ist ein Benutzername und kann nach Bedarf geändert werden.
   `authGroup` ist der Gruppenname, den Sie in Schritt e angegeben haben.
   `md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
   `password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.
   `des` ist die Verschlüsselungsmethode und kann nach Bedarf geändert werden.)
   Legen Sie das Kennwort und die Authentifizierungsmethode/ Verschlüsselung/Kennwort entsprechend der Sicherheitsstufe fest.

h. Erzeugen Sie einen Benutzer.

i. Geben Sie `show vlan` ein, und bestätigen Sie die VLAN-Liste. In diesem Fall geben Sie `refrains from the one of enet(ethernet)` ein.

j. Geben Sie `snmp-server group authGroup v3 auth context vlan-1 read allView notify allView` ein, und legen Sie fest, dass der Kontext zugelassen wird. Beachten Sie, dass ein Autorisierungsfehler auftreten kann, wenn die Einstellung nicht auf alle VLAN angewendet wird.
`authGroup` ist ein Gruppenname und kann nach Bedarf geändert werden.
`vlan-1` ist der VLAN-Name. Legen Sie ihn auf „all refrained VLAN" fest.
`allView` ist der Anzeigename, den Sie in Schritt c angegeben haben.

k. Geben Sie `end` ein.

2. Trennen Sie die Telnet-Verbindung.

Beispielkonfiguration für einen HP-IP-Switch

Für SNMPv1 oder v2c:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `configure terminal` ein.
   b. Geben Sie `snmp-server community public manager restricted` ein. (Dabei gilt:
   `public` ist der Community-Name und kann nach Bedarf geändert werden).
   c. Geben Sie `show snmp-server` ein, und bestätigen Sie anschließend die Einstellungen.
2. Trennen Sie die Telnet-Verbindung.

Für SNMPv3:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `configure terminal` ein.
   b. Geben Sie `snmpv3 user Md5DesUser auth md5 password1 priv password2` ein. (Dabei gilt:
   `Md5DesUser` ist ein Benutzername und kann nach Bedarf geändert werden.
   `md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
   `password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.
   `password2` ist ein Verschlüsselungskennwort und kann nach Bedarf geändert werden.
   Legen Sie das Kennwort und die Authentifizierungsmethode/ Verschlüsselung/Kennwort entsprechend der Sicherheitsstufe fest.
   c. Erzeugen Sie einen Benutzer.

d. Geben Sie `snmpv3 group managerpriv user Md5DesUser sec-model ver3` ein, (wobei `managerpriv` ein Gruppenname ist, der nach Bedarf geändert werden kann, und `Md5DesUser` der Benutzername ist, den Sie in Schritt b eingegeben haben.)

e. Verbinden Sie die Gruppe mit dem Benutzer.

2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines Juniper IP-Switches

Für SNMPv1 oder v2c:

1. Greifen Sie über den Web-Browser auf den Juniper-Gerätemanager zu.
   a. Melden Sie sich an.
   b. Wählen Sie im Navigationsbereich **System**, **Management**, **SNMP** und anschließend **Community Config**.
   c. Fügen Sie im Panel **Community Config** die SNMP-Community hinzu, auf die der Verwaltungsserver von IT Operations Analyzer zugreifen kann, oder aktualisieren Sie sie.
2. Schließen Sie den Web-Browser.

Für SNMPv3:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `cli` ein, und wechseln Sie dann zum cli-Modus.
   b. Geben Sie `configure` ein.
   c. Geben Sie `set snmp view allView oid .1 include` ein, (wobei `allView` ein Anzeigename ist und nach Bedarf geändert werden kann.)
   d. Erzeugen Sie eine Ansicht.
   e. Geben Sie `set snmp v3 vacm access group privGroup default-context-prefix security-model usm security-level privacy read-view allView notify-view allView` ein, (wobei `privGroup` ein Gruppenname ist und nach Bedarf geändert werden kann, und `allView` ein Anzeigename ist, den Sie in Schritt c angegeben haben.)
   f. Erzeugen Sie eine Gruppe.
   g. Geben Sie `set snmp v3 usm local-engine user Md5DesUser authentication-md5 authentication-password password1` ein. (Dabei gilt:
   `Md5DesUser` ist ein Benutzername und kann nach Bedarf geändert werden.
   `authentication-md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
   `password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.)
   Legen Sie Authentifizierungsmethode/Kennwort entsprechend der Sicherheitsstufe fest.
   h. Erzeugen Sie einen Benutzer.

i. Geben Sie `set snmp v3 usm local-engine user Md5DesUser privacy-des privacy-password password2` ein, (wobei: `Md5DesUser` der Benutzername ist, den Sie in Schritt g angegeben haben.
`privacy-des` ist eine Verschlüsselungsmethode und kann nach Bedarf geändert werden.
`password2` ist ein Verschlüsselungskennwort und kann nach Bedarf geändert werden.
Legen Sie Verschlüsselungsmethode/Kennwort entsprechend der Sicherheitsstufe fest.

j. Geben Sie `set snmp v3 vacm security-to-group security-model usm security-name Md5DesUser group privGroup` ein, (wobei „Md5DesUser" der Benutzername ist, den Sie in Schritt g eingegeben haben.
„privGroup" ist der Gruppenname, den Sie in Schritt e angegeben haben.)
Benutzer und Gruppe gehören zusammen.

k. Geben Sie „commit" ein.

2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines Enterasys-IP-Switches

Für SNMPv1 oder v2c:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her. Melden Sie sich mit Administratorrechten an, und führen Sie die folgenden Befehle aus:
   a. `set snmp community public`.
   b. `set snmp group groupRW user public security-model v1`, (wobei `groupRW` und `public` Namen sind, die geändert werden können).
   c. `show snmp access groupRW`, und bestätigen Sie anschließend die Einstellungen.

2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines Extreme-IP-Switches

Für SNMPv1 oder v2c:

1. Greifen Sie mit dem Browser auf ExtremeXOS ScreenPlay zu.
   a. Melden Sie sich an.
   b. Wählen Sie im Navigationsbereich **System**, **Management**, **SNMP** und anschließend **Community Config**.
   c. Fügen Sie im Panel **Community Config** die SNMP-Community hinzu, auf die der Verwaltungsserver von IT Operations Analyzer zugreifen kann, oder aktualisieren Sie sie.
2. Schließen Sie den Web-Browser.

Für SNMPv3:

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `configure snmpv3 add mib-view allView subtree 1 type included` ein, (wobei `allView` ein Anzeigename ist und nach Bedarf geändert werden kann.)
   b. Erzeugen Sie eine Ansicht.
   c. Geben Sie `configure snmpv3 add access authGroup sec-model usm sec-level authnopriv read-view allView notify-view allView` ein, (wobei `authGroup` ein Gruppenname ist und nach Bedarf geändert werden kann, und `allView` ein Anzeigename ist, den Sie in Schritt a angegeben haben.)
   d. Erzeugen Sie eine Gruppe.
   e. Geben Sie `configure snmpv3 add user Md5NoneUser authentication md5 password1` ein. (Dabei gilt:
   `Md5NoneUser` ist ein Benutzername und kann nach Bedarf geändert werden.
   `md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
   `password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.)
   Legen Sie Authentifizierungsmethode/Kennwort entsprechend der Sicherheitsstufe fest.
   f. Erzeugen Sie einen Benutzer.
   g. Geben Sie `configure snmpv3 add group authGroup user Md5NoneUser sec-model usm` ein, (wobei `authGroup` der Gruppenname ist, den Sie in Schritt c, und `Md5NoneUser` der Benutzer ist, den Sie in Schritt e eingegeben haben.)
   h. Stellen Sie die Verbindung zwischen Benutzer und Gruppe her.
2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines NETGEAR-Switches

Für SNMPv1 oder v2c:

1. Greifen Sie über den Web-Browser auf den NETGEAR-Switch zu:
   a. Melden Sie sich an.
   b. Wählen Sie im Navigationsbereich **System**, **Management**, **SNMP** und anschließend **Community Config**.
   c. Fügen Sie im Panel **Community Config** eine SNMP-Community hinzu, auf die der Verwaltungsserver von IT Operations Analyzer zugreifen kann, oder aktualisieren Sie eine solche.

2. Schließen Sie den Web-Browser.

Beispiel für die Konfiguration eines DELL IP-Switches

Für SNMPv1 oder v2c:

1. Greifen Sie über den Web-Browser auf den DELL OpenManage Switch
2. Administrator zu:
   a. Melden Sie sich an.
   b. Wählen Sie vom Navigationsgbereich **System**, **SNMP** und anschließend **Global Parameters**.
   c. Im Panel **Global Parameters** setzen Sie **SNMP Notifications** auf **Enable**.
   d. Wählen Sie im Navigationsmenü **Communities**.
   e. Fügen Sie im Fenster **Communities** (Communitys) eine SNMP-Community hinzu, auf dem vom Verwaltungsserver des IT Operations Analyzer zugegriffen werden soll, bzw. aktualisieren Sie diese.
3. Schließen Sie den Web-Browser.

Für SNMPv3

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `configure` ein.
   b. Geben Sie `snmp engineid local default` ein, und konfigurieren Sie die Engine ID.
   c. Geben Sie `snmp view allView 1 included` ein, (wobei `allView` ein Anzeigename ist und nach Bedarf geändert werden kann.)
   d. Erzeugen Sie eine Ansicht.
   e. Geben Sie `snmp group authGroup v3 auth read allView notify allView` ein, (wobei `authGroup` ein Gruppenname ist und nach Bedarf geändert werden kann, und `allView` ein Anzeigename ist, den Sie in Schritt c angegeben haben.)
   f. Erzeugen Sie eine Gruppe.
   g. Geben Sie `snmp user Md5NoneUser authGroup auth-md5 password1` ein. (Dabei gilt:
      `Md5NoneUser` ist ein Benutzername und kann nach Bedarf geändert werden.
      `authGroup` ist der Gruppenname, den Sie in Schritt e angegeben haben.
      `auth-md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
      `password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.)
      Legen Sie Authentifizierungsmethode/Kennwort entsprechend der Sicherheitsstufe fest.
   h. Erzeugen Sie einen Benutzer.
2. Trennen Sie die Telnet-Verbindung.

Beispielkonfiguration für einen Allied-Telesis-Switch (AT-9424T)

Für SNMPv3

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `enable snmp` ein, und aktivieren Sie SNMP.
   b. Geben Sie `create snmpv3 view allView Subtree=1 Type=Included` ein, (wobei `allView` ein Anzeigename ist und nach Bedarf geändert werden kann.)
   c. Erzeugen Sie eine Ansicht.
   d. Geben Sie `create snmpv3 access authGroup SecurityModel=V3 SecurityLevel=Authentication ReadView=allView NotifyView=allView` ein, (wobei `authGroup` ein Gruppenname ist und nach Bedarf geändert werden kann, und `allView` ein Anzeigename ist, den Sie in Schritt b angegeben haben.)
   e. Erzeugen Sie eine Gruppe.
   f. Geben Sie `add snmpv3 user Md5NoneUser Authentication=Md5 AuthPassword=password1` ein. (Dabei gilt:
   `Md5NoneUser` ist ein Benutzername und kann nach Bedarf geändert werden.
   `Md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
   `password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.)
   Legen Sie Authentifizierungsmethode/Kennwort entsprechend der Sicherheitsstufe fest.
   g. Erzeugen Sie einen Benutzer.
   h. Geben Sie `create snmpv3 group UserName=Md5NoneUser SecurityModel=V3 GroupName=authGroup` ein, (wobei `Md5NoneUser` der Benutzername ist, den Sie in Schritt f, und `authGroup` der Gruppenname ist, den Sie in Schritt d angegeben haben.)
2. Trennen Sie die Telnet-Verbindung.

Beispielkonfiguration für einen ALAXALA-Switch (AX3600)

Für SNMPv3

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `configure terminal` ein.
   b. Geben Sie `snmp-server view allView 1 included` ein, (wobei `allView` ein Anzeigename ist und nach Bedarf geändert werden kann.)
   c. Erzeugen Sie eine Ansicht.
   d. Geben Sie `snmp-server group authGroup v3 auth read allView notify allView` ein, (wobei `authGroup` ein Gruppenname ist und nach Bedarf geändert werden kann, und `allView` ein Anzeigename ist, den Sie in Schritt b angegeben haben.)
   e. Erzeugen Sie eine Gruppe.

f. Geben Sie `snmp-server user Md5NoneUser authGroup v3 auth md5 password1` ein. (Dabei gilt:
`Md5NoneUser` ist ein Benutzername und kann nach Bedarf geändert werden.
`authGroup` ist der Gruppenname, den Sie in Schritt d angegeben haben.
`md5` ist eine Authentifizierungsmethode und kann nach Bedarf geändert werden.
`password1` ist ein Authentifizierungskennwort und kann nach Bedarf geändert werden.)
Legen Sie Authentifizierungsmethode/Kennwort entsprechend der Sicherheitsstufe fest.

g. Erzeugen Sie einen Benutzer.

h. Geben Sie `write` ein.

2. Trennen Sie die Telnet-Verbindung.

Aktivieren von SNMP-Traps

IT Operations Analyzer kann bei jedem Auf- und Abbau von IP-Switch-Verbindungen SNMP-Traps empfangen. Um den optionalen Trap-Empfang einzurichten, wenden Sie die folgenden Einstellungen an:

- Aktivieren Sie **Trap senden** (es muss die Version SNMP V1 sein).
- Geben Sie als **Zieladresse für die Trapsendung** die IP-Adresse des Verwaltungsservers für IT Operations Analyzer und als **Ziel-Port für die Trapsendung** den **Trapping-Port** für IT Operations Analyzer auf dem Verwaltungsserver ein (die Port-Nummer lautet 162).

HINWEIS: Informationen über die von IT Operations Analyzer standardmäßig verwendeten Port-Nummern finden Sie in Kapitel 2 des *Handbuchs „Erste Schritte" für Hitachi IT Operations Analyzer*.

Beispiel für die Konfiguration eines Cisco IP-Switches (IOS)

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her. Geben Sie folgenden Befehl ein:

   a. `enable`. Geben Sie bei entsprechender Aufforderung Ihr Kennwort ein.

   b. `configure terminal`.

   c. `snmp-server enable traps`.

   d. `snmp-server host 192.168.1.1 version 1 public`, (wobei `192.168.1.1` das Ziel der Trapsendung und `public` der Community-Name ist und beide Werte nach Bedarf geändert werden können).

   e. `end`.

   f. `Geben Sie show running-config` ein, und bestätigen Sie anschließend die Einstellungen.

2. Trennen Sie die Telnet-Verbindung.

Beispielkonfiguration für einen HP-IP-Switch

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her.
   a. Geben Sie `configure` ein.
   b. Geben Sie `snmp-server host 192.168.1.1 public all` ein. (Wobei `192.168.1.1` die Zieladresse für das Senden von Traps und `public` der Community-Name ist. Beide Werte können nach Bedarf geändert werden.)
   c. Geben Sie `show snmp-server` ein, und bestätigen Sie anschließend die Einstellungen.
2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines Juniper IP-Switches (EX)

1. Greifen Sie über den Web-Browser auf den Juniper-Gerätemanager zu:
   a. Melden Sie sich an.
   b. Klicken Sie auf **Configure** (Konfigurieren).
   c. Klicken Sie auf **Service**, und wählen Sie anschließend **SNMP**.
   d. Klicken Sie in den **Trap-Gruppen** auf **Add** (Hinzufügen).
   e. Legen Sie einen Trap-Gruppennamen fest.
   f. Wählen Sie im Bereich **Categories** (Kategorien) die Option **Link** oder **None** (Keine).
   g. Fügen Sie die IP-Adressen des Verwaltungsservers zu den Zielen hinzu.
   h. Klicken Sie auf **OK**.

2. Schließen Sie den Web-Browser.

Beispiel für die Konfiguration eines Enterasys-IP-Switches

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her. Melden Sie sich mit Administratorrechten an, und führen Sie die folgenden Befehle aus:
   a. `set snmp targetparams testParams user public security-model v1 message-processing v1`.

      Beachten Sie, dass **testParams** ein Name ist, der nach Bedarf geändert werden kann.
   b. `set snmp notify testNotify tag testTag trap`.

      Beachten Sie, dass **testNotify** und **testTag** Namen sind, die nach Bedarf geändert werden können.
   c. `set snmp targetaddr testTargetAddr 192.168.55.11 param testParams udpport 162 mask 255.255.255.0 taglist testTag`.

      Beachten Sie, dass **testTargetAddr** ein optionaler Name, **192.168.55.11** die IP-Adresse des Trap-Ziels, **162** die Port-Nummer des Trap-Ziels und **255.255.255.0** eine Subnetzmaske des Trap-Ziels ist. Sie können diese Daten nach Bedarf ändern.
   d. `Geben Sie show running-config` ein, und bestätigen Sie anschließend die Einstellungen.

2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines Extreme-IP-Switches

1. Stellen Sie über Telnet eine Verbindung zum IP-Switch her. Melden Sie sich mit Administratorrechten an, und führen Sie die folgenden Befehle aus:
   a. `configure snmpv3 add target-params testTargetParam user v1v2c_ro mp-model snmpv1 sec-model snmpv1 sec-level noauth`.

      Beachten Sie, dass **testTargetParam** ein willkürlicher Name ist und **v1v2c_ro** ein Sicherheitsname. Beide Namen können nach Bedarf geändert werden. Sie können den Sicherheitsnamen durch Ausführen von `show snmpv3 community` bestätigen.

   b. `configure snmpv3 add target-addr 192.168.55.11 param testTargetParam ipaddress 192.168.55.11/FFFFFF00 transport-port 162 from 192.168.55.7`.

      Beachten Sie, dass **191.168.55.11** die IP-Adresse des Trap-Ziels ist, **FFFFFF00** eine Subnetzmaske des Trap-Ziels, **162** die Port-Nummer des Trap-Ziels und **192.168.55.7** eine IP-Adresse der Trap-Quelle. Sie können diese Daten nach Bedarf ändern.

   c. `Geben Sie show running-config` ein, und bestätigen Sie anschließend die Einstellungen.

2. Trennen Sie die Telnet-Verbindung.

Beispiel für die Konfiguration eines NETGEAR IP-Switches

1. Greifen Sie über den Web-Browser auf den NETGEAR-Switch zu:
   a. Melden Sie sich an.
   b. Wählen Sie im Navigationsbereich **System**, **Management**, **SNMP** und anschließend **Trap Config**.
   c. Im Panel **Trap Config** können Sie eine Trap-Konfiguration zum Senden einer SNMP-Trap an den IT Operations Analyzer Verwaltungsserver hinzufügen oder aktualisieren. Für die **SNMP Version** geben Sie **SNMP V1** an.
   d. Vom Navigationsbereich wählen Sie **Trap Flags**.
   e. Vom Panel **Trap Flags** setzen Sie **Link Up/Down** auf **Enable**.

2. Schließen Sie den Web-Browser.

Beispiel für die Konfiguration eines DELL IP-Switches

1. Greifen Sie über den Web-Browser auf den DELL **OpenManage Switch Administrator** zu:
   a. Melden Sie sich an.
   b. Wählen Sie vom Navigationsgbereich **System**, **SNMP** und anschließend **Global Parameters**.
   c. Im Panel **Global Parameters** setzen Sie **SNMP Notifications** auf **Enable**.
   d. Vom Navigationsbereich wählen Sie **Notification Recipients**.
   e. Im Panel **Notification Recipients** können Sie eine Trap-Konfiguration zum Senden einer SNMP-Trap an den Verwaltungsserver von IT Operations Analyzer hinzufügen oder aktualisieren. Zur Konfiguration wählen Sie **SNMPv1.2**.

2. Schließen Sie den Web-Browser.

6

Vorbereiten von Hitachi Storage

IT Operations Analyzer kann die Hitachi AMS/WMS/SMS-Serie und die Hitachi Unified Storage-Serie überwachen. Es kann außerdem Hitachi 9500V und Hitachi USP VM über den SMI-S-Provider von Device Manager überwachen. Es überwacht jedoch nicht die Leistung von Hitachi 9500V.

In diesem Kapitel werden die Informationen beschrieben, die für eine Verbindung mit dem Knoten der Hitachi AMS/WMS/SMS-Speichergeräte, Hitachi Unified Storage, Hitachi 9500V und Hitachi USP VM zu erfassen sind. Ebenso werden die Vorbereitungsschritte zum Erhalt der Leistungsdaten für die Hitachi AMS/WMS/SMS-Serie, die Hitachi Unified Storage-Serie und Hitachi USP VM beschrieben.

- Vorbereitungsschritte für die Verbindung zur Hitachi AMS/WMS/SMS-Serie und Hitachi Unified Storage-Serie
- Vorbereitungen für den Erhalt von Leistungsinformationen für die Hitachi AMS/WMS/SMS-Serie und Hitachi Unified Storage-Serie
- Vorbereitungen für den Anschluss an Hitachi 9500V und Hitachi USP VM
- Vorbereitungen für den Erhalt von Leistungsinformationen für Hitachi USP VM

Vorbereitungsschritte für die Verbindung zur Hitachi AMS/ WMS/SMS-Serie und Hitachi Unified Storage-Serie

IT Operations Analyzer kann die Hitachi AMS/WMS/SMS-Serie und die Hitachi Unified Storage-Serie überwachen. Wenn eine Verbindung zur Hitachi AMS/WMS/SMS-Serie und Hitachi Unified Storage-Serie hergestellt werden soll, werden die Informationen aus Tabelle 6-1 benötigt.

Tabelle 6-1: Informationen zur Verbindung mit der Hitachi AMS/WMS/ SMS-Serie und Hitachi Unified Storage-Serie

Element	Details
IP-Adresse	Die IP-Adresse, die für die Verbindung zum Speichergerät verwendet wird
Benutzer-ID	Wenn die **Kontoauthentifizierung** oder der **Kennwortschutz** aktiviert ist, geben Sie die ID des Benutzers an, der sich beim Speichergerät anmelden kann.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an. Das Kennwort ist erforderlich, wenn die **Kontoauthentifizierung** oder der **Kennwortschutz** aktiviert ist.

HINWEIS: Wenn der **Kennwortschutz** verwendet wird, können Fehler auftreten. Dies ist z. B. der Fall, wenn mehrere Verwaltungsserver gleichzeitig versuchen, auf ein Hitachi Speichergerät mit konfiguriertem **Kennwortschutz** zuzugreifen. Um Fehler zu vermeiden, wird empfohlen, den **Kennwortschutz** zu deaktivieren.

Ändern der Port-Nummer

Wenn die Nummer des Verwaltungs-Ports für Hitachi Speichergeräte geändert wird, registrieren Sie die geänderte Port-Nummer in der Services-Datei. Diese Services-Datei befindet sich im folgenden Windows-Verzeichnis:

<*Windows-Verzeichnis*>\system32\drivers\etc\services

- Der Service-Name der **normalen** Port-Nummer ist: df-damp-snm
- Service-Name der Nummer des **sicheren Ports**: df-damp-snm-ssl

Im folgenden Beispiel ist der **normale Port** auf 2300 und der **sichere Port** auf 25000 gesetzt:

df-damp-snm 2300/tcp #normal port

df-damp-snm-ssl 25000/tcp #secure port - SSL

HINWEIS: Die Port-Nummer des Hitachi Speichers, der von IT Operations Analyzer überwacht wird, sollte passend sein. Wenn die Services-Datei geändert wird, betrifft die Änderung Produkte, die HSNM2-API nutzen, wie etwa Hitachi Storage Navigator Modular 2, HiCommand Serie usw.

Vorbereitungen für den Erhalt von Leistungsinformationen für die Hitachi AMS/WMS/SMS-Serie und Hitachi Unified Storage-Serie

Zum Erhalt von Leistungsinformationen führen Sie die folgenden Schritte durch.

1. Öffnen Sie das Fenster **Performance Statistics** (Leistungsstatistiken) für das Speichergerät, dessen Leistung in Hitachi Storage Navigator Modular 2 überwacht werden soll.
2. Schließen Sie Aufgaben ab, je nachdem, ob der Management-Dialog in einem neuen Fenster anzeigt wird:

   - **Wenn der Management-Dialog in einem neuen Fenster anzeigt wird:**

   a. Melden Sie sich bei Hitachi Storage Navigator Modular 2 an.

   b. Klicken Sie auf den Namen des Ziel-Arrays, und öffnen Sie den Management-Dialog.

   c. Klicken Sie in der Menüleiste auf **Tool**, **Performance** und dann auf **Setting**.

   - **Wenn der Management-Dialog in demselben Fenster anzeigt wird:**

   a. Melden Sie sich bei Hitachi Storage Navigator Modular 2 an.

   b. Klicken Sie auf den Namen des Ziel-Arrays, und öffnen Sie die Management-Anzeige.

   c. Aus der Strukturansicht öffnen Sie **Performance** und klicken dann auf **Monitoring**.

   d. Klicken Sie auf **Acquisition item change**.

3. Bestätigen Sie, dass Folgendes ausgewählt ist: **RAID Group/Logical Unit Information** (RAID-Gruppe/LU-Informationen), **Cache Information** (Cache-Informationen), **Processor Information** (Prozessorinformationen) und **Drive Operating Information** (Laufwerksbetriebsinformationen). Klicken Sie dann auf **OK**.

Vorbereitungen für den Anschluss an Hitachi 9500V und Hitachi USP VM

IT Operations Analyzer dient zum Überwachen von:

- Hitachi 9500V über den SMI-S-Provider von Device Manager. Installieren Sie Device Manager 5.9 oder höher, und aktivieren Sie die Nutzung des SMI-S-Providers.
- Hitachi USP VM über den SMI-S-Provider von Device Manager. Installieren Sie Device Manager 6.2 oder höher, und aktivieren Sie die Nutzung des SMI-S-Providers.

Es folgt eine allgemeine Verfahrensübersicht für den Erhalt von Anschlussinformationen für Hitachi 9500V und Hitachi USP VM. Spezifische Details entnehmen Sie den Anwendungshandbüchern:

- Hitachi Device Manager, Provisioning Manager und Tiered Storage Manager Software-Installationshandbuch
- Hitachi Device Manager und Provisioning Manager Software System-Konfigurationshandbuch
- Hitachi Device Manager Software Web Client-Benutzerhandbuch

1. Installieren Sie **Device Manager** auf einem beliebigen Server. Da Sie während der Installation angeben können, dass ein SMI-S-Agent vorhanden ist, aktivieren Sie diese Option.
2. Melden Sie sich bei **Device Manager** an, und klicken Sie auf **Subsystems** (Subsysteme), dann auf **Add Subsystem** (Subsystem hinzufügen), und registrieren Sie die Speichergeräte.

   Geben Sie bei der Registrierung der Geräte die IP-Adressen, Benutzer-IDs und Kennwörter der Speicher-Controller an. Tabelle 6-2 enthält einen Überblick über die Informationen, die für die Verbindung zu einem Speichergerät von Hitachi erforderlich sind.
3. Wenn Sie entsprechend der Beschreibung in diesem Handbuch einen SMI-S-Agent verwenden, müssen Sie die Speicher-Heapgröße des Device Manager-Servers erhöhen. Im folgenden Beispiel wird das entsprechende Verfahren unter Microsoft Windows beschrieben:
   a. Berechnen Sie die Speicher-Heapgröße.
   b. Öffnen Sie die Datei **Server.ini** in einem Texteditor:

      <Installationsverzeichnis des Device Manager-Servers>\HiCommandServer\Server.ini
   c. Ändern Sie den Wert von **JVM_XOPT_HEAP_MAX** entsprechend den Berechnungen in Schritt a. Beispiel:

      JVM_XOPT_HEAP_MAX=Xmx<*Einstellungswert*>m
   d. Starten Sie den Device Manager-Server neu.

Tabelle 6-2: Informationen für den Anschluss an Hitachi 9500V und Hitachi USP VM

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem Device Manager installiert ist.
Namespace	Geben Sie für Device Manager 5.9 oder höher Folgendes an: root/smis/smis12 Geben Sie für Device Manager 6.2 oder höher Folgendes an: root/smis/smis13 Geben Sie für Device Manager 7.0 oder höher Folgendes an: root/smis/smis14
Vorhandensein von SSL	Wenden Sie die Einstellungen an, die während der Installation von Device Manager konfiguriert wurden.
Port-Nummer	Wenden Sie die Einstellungen an, die während der Installation von Device Manager konfiguriert wurden. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Geben Sie die Benutzer-ID für Device Manager an.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.

HINWEIS: Wenn an Ihrem Standort Hitachi Storage mit Hitachi Device Manager überwacht wird, wird für die folgenden Komponenten im **Überwachungsmodul** immer ein normaler Betriebszustand gemeldet:
-Speicher-Controller
-Speicher-FC-Port
-Speicher-Festplattenlaufwerk
-Speichervolume
-LUN
Auftretende Fehler werden daher nicht erkannt.

Vorbereitungen für den Erhalt von Leistungsinformationen für Hitachi USP VM

Nachfolgend sind allgemeine Richtlinien für das Abrufen von Leistungsdaten zu Hitachi USP VM aufgelistet. Weitere Informationen finden Sie in den Handbüchern zu Hitachi Device Manager.

1. Bereiten Sie das Speicher-Subsystem vor.

   Bereiten Sie das Befehlsgerät in jedem Speicher-Subsystem vor, von dem aus Leistungsdaten abgerufen werden sollen. (Das Befehlsgerät ist ein Steuerungsgerät, das den Steuerungsbefehl an das Disk-Array übermittelt.) Weisen Sie dann den Pfad zum Host zu, der Leistungsdaten erfasst, und konfigurieren Sie den Host so, dass er das Befehlsgerät erkennt.

2. Bereiten Sie den Host vor, der Leistungsdaten erfasst.

   Installieren Sie den Device Manager-Agent, und konfigurieren Sie das Befehlsgerät.

3. Bereiten Sie den Device Manager-Server vor.

   Tragen Sie in der Eigenschaftsdatei des Device Manager-Servers den Hostnamen für den Host ein, der Leistungsdaten erfasst.

7

Vorbereiten von SMI-S für FC-Switches und Speichergeräte

IT Operations Analyzer verwendet SMI-S zur Ermittlung und Überwachung anderer Speichergeräte und von FC-Switches. In diesem Kapitel werden SMI-S und die zur Einrichtung der FC-Switches und Speichergeräte erforderlichen Aufgaben beschrieben.

Prüfen der SMI-S-Vorbereitungen

SMI-S ist der SNIA-Standard (Storage Networking Industry Association), der eine offene Management-API (Application Programming Interface) bereitstellt. Er unterstützt die interoperable Verwaltung von Speichernetzwerken und Speichergeräten, wozu auch virtueller Speicher, Switches und Hosts zählen.

Wenn in Ihrer Umgebung Speichergeräte von Drittanbietern eingesetzt werden (d. h. andere Geräte als Hitachi Speichergeräte oder FC-Switches), kann IT Operations Analyzer diese mithilfe eines SMI-S-Agent ermitteln und überwachen.

In einer Umgebung mit Speichergeräten von Drittanbietern, die über einen SMI-S-Agent eingebunden sind, können zwei Modelle genutzt werden: ein integriertes Modell und ein Proxy-Modell.

- In einem **integrierten Modell** wird der SMI-S-Agent auf einem Gerät ausgeführt. Das wird SMI-S Agent (integriert) genannt.
- In einem **Proxy-Modell** ist der SMI-S-Agent auf einem Computer installiert. Das wird SMI-S Agent (Proxy) genannt.

Abbildung 7-1 zeigt ein Beispiel einer SMI-S-Umgebung, die aus einem Server (SMI-S-Server) und einem Client besteht. IT Operations Analyzer fungiert als Client und erfasst in diesem Beispiel Informationen zu FC-Switches (Fibre Channel). Der blau schattierte Bereich, der das integrierte Modell und das Proxy-Modell umfasst, muss vorbereitet werden, bevor Sie die erste Ermittlung durchführen.

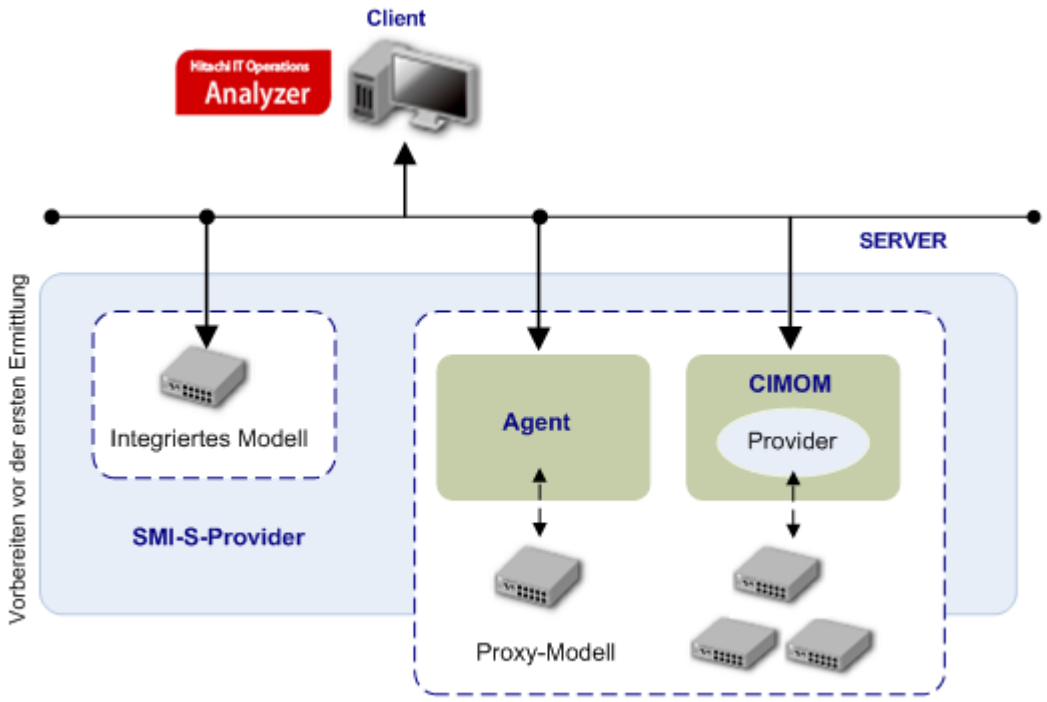

Abbildung 7-1: Beispiel für eine SMI-S-Umgebung

In den folgenden Abschnitten wird erläutert, welche Vorbereitungen Sie für die FC-Switches und Speichergeräte in Ihrer Umgebung treffen müssen.

Vorbereiten von SMI-S für Fibre Channel-Switches (FC)

Geräte, die als Überwachungsziele angegeben werden sollen, müssen SMI-S-Version 1.0 - 1.3 unterstützen, und der Service zur Verwaltung dieser Geräte muss aktiv sein. In diesem Abschnitt werden die Einstellungen des SMI-S-Agent für folgende Elemente beschrieben:

- Brocade® FC-Switches
- Brocade Sphereon FC-Switches
- QLogic® FC-Switches
- Cisco® FC-Switches

Konfigurieren von Brocade FC-Switches (außer Sphereon-Serie)

Konfigurieren Sie die Einstellungen des SMI-S-Agent gemäß den folgenden Richtlinien. Einzelheiten erfahren Sie in der Brocade SMI Agent Dokumentation auf folgender Website: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

Sie können in den Versionshinweisen enthaltene Installationsanforderungen, Installationsverfahren, Einstellungen nach der Installation und Aktualisierungen wie folgt bestätigen:

- Installationsanforderungen

  Brocade SMI Agent v120.6.0a Installationshandbuch, Kapitel 1 „Installationsanforderungen"
- Installationsverfahren

  Brocade SMI Agent v120.6.0a Installationshandbuch, Kapitel 2 „Installation des SMI Agent"
- Einstellungen nach der Installation

  Brocade SMI Agent v120.6.0a Benutzerhandbuch
- Versionshinweise

  Brocade SMI Agent v120.6.0a Versionshinweise v1.1

Anforderungen vor der Installation

- Brocade SMI-S Agent-Version: Brocade SMI Agent v120.6.0a
- Betriebssystem: Microsoft Windows Server 2003 (32 Bit)

Wenn eine vorangegangene Version des Brocade SMI-S-Agent installiert ist, führen Sie die folgenden Installationsaufgaben durch.

Installation eines Brocade SMI Agent:

1. Laden Sie den SMI-S-Agent v120.6.0a von folgender Website herunter, und starten Sie anschließend **install.exe**: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

2. Führen Sie alle im Installationsassistenten geforderten Schritte durch. Bei bestimmten Schritten richten Sie sich nach folgenden Vorgaben:
   a. **HTTP Port Configuration**. Die Standard-Port-Nummer ist 5988. Achten Sie darauf, dass die Port-Nummer, die Sie angeben, zur Verbindung mit IT Operations Analyzer verwendet wird.
   b. **HTTPS Port Configuration**. Die Standard-Port-Nummer ist 5988. Achten Sie darauf, dass die Port-Nummer, die Sie angeben, zur Verbindung mit IT Operations Analyzer verwendet wird.
   c. **Proxy Connections Configuration**. Geben Sie folgende Werte ein:

      Proxy IP: IP-Adresse des FC-Switches

      User name: Benutzername des FC-Switches

      Password: Kennwort des FC-Switches

      Geben Sie die anderen Einstellung entsprechend Ihrer Umgebung ein.
3. Um Ihre Einstellungen am Ende der Installation des Brocade Agent zu speichern, klicken Sie auf **Done**.

   Jetzt können Sie den FC-Switch registrieren.

So registrieren Sie den FC-Switch:

1. Starten Sie das **Brocade SMI Agent Configuration Tool**:
   a. Wählen Sie im Menü **Start** die Option **All Programs**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zum Startmenü zu navigieren, anders.

   b. Wählen Sie **SMIAgent120.6.0a** und dann **Brocade SMI Agent Configuration Tool**.
2. Klicken Sie auf **Add**, um den Dialog **Proxy Configuration** aufzurufen.
3. Geben Sie die erforderlichen Informationen ein, und klicken Sie dann auf **OK**, um Ihre Einstellungen zu speichern, und schließen Sie den Dialog **Proxy Configuration**.
4. In dem **Brocade SMI Agent Configuration Tool** ändern Sie den Proxy-Status von **Not Connected** zu **Connected**, indem Sie auf **Apply** klicken.

Tabelle 7-1 enthält einen Überblick über die Informationen, die für die Verbindung zu einem Brocade FC-Switch erforderlich sind.

Tabelle 7-1: Informationen für die Verbindung zu einem Brocade FC-Switch

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem Brocade SMI Agent installiert ist.
Namespace	Geben Sie `root/brocade1` an.
Vorhandensein von SSL	Wenden Sie die Einstellungen für Brocade SMI Agent an, die während der Installation konfiguriert wurden.

Tabelle 7-1: Informationen für die Verbindung zu einem Brocade FC-Switch

Element	Details
Port-Nummer	Wenden Sie die Einstellungen für Brocade SMI Agent an, die während der Installation konfiguriert wurden. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Geben Sie die Benutzer-ID für Brocade SMI Agent an.
Kennwort	Geben Sie ein Kennwort für die Benutzer-ID ein.

HINWEIS: Wenn ein FC-FC Routing-Port den Status „Verbindung getrennt" hat, ändert sich der Status des Phantom-Switches in „Nicht erreichbar".
Der Switch-Status „Nicht erreichbar" bleibt bestehen, auch wenn der Port-Status wieder normal ist.

Um den Switch-Status von „Nicht erreichbar" in „Normal" zu ändern, muss IT Operations Analyzer den Switch erneut ermitteln. Dies ist erforderlich, da der SMI-S-Provider des Phantom-Switches nicht antwortet, wenn der Port den Status „Verbindung getrennt" hat. Auch wenn der Port-Status wieder normal ist, protokolliert der SMI-S-Provider den Status des Switches als „Nicht erreichbar".

Weitere Informationen zum Ermitteln von Switches, Knoten und anderen Geräten finden Sie in der Onlinehilfe.

Konfigurieren von Brocade Sphereon FC-Switches

Konfigurieren Sie die Einstellungen des SMI-S-Agent gemäß den folgenden Richtlinien. Einzelheiten erfahren Sie in der Brocade SMI Agent for EOS Dokumentation auf folgender Website:
http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

Sie können in den Versionshinweisen enthaltene Installationsanforderungen, Installationsverfahren, Einstellungen nach der Installation und Aktualisierungen wie folgt bestätigen:

- Installationsanforderungen

  Brocade SMI Agent for EOS Products User Guide 2.0, Kapitel 1 „Systemanforderungen"

- Installationsverfahren

  Brocade SMI Agent for EOS Products User Guide 2.0, Kapitel 2 „Installation von Brocade SMI Agent für EOS Produkte"

- Einstellungen nach der Installation

  Brocade SMI Agent for EOS Products Benutzerhandbuch 2.0, Kapitel 3 „Benutzung des SMI Agent für EOS Produkte Serverkonfigurationsprogramm", und Kapitel 4 „Server Setup für Client Operations"

- Versionshinweise

  Brocade SMI Agent for EOS Products 2.0 Versionshinweise

Anforderungen vor der Installation

- Brocade SMI-S Agent-Version: Brocade SMI Agent for EOS Products 2.0 for Windows
- Betriebssystem: Microsoft Windows Server 2003 (32 Bit)

Installation eines Brocade SMI Agent:

1. Laden Sie den Brocade SMI Agent für Windows von folgender Website herunter, und starten Sie anschließend **install.exe**: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. Führen Sie alle im Installationsassistenten geforderten Schritte durch.
3. Um Ihre Einstellungen am Ende der Installation des Brocade Agent zu speichern, klicken Sie auf **Done**.

   Jetzt können Sie den FC-Switch registrieren.

So registrieren Sie den FC-Switch:

1. Öffnen Sie die Datei **Switch.properties**, die sich in folgendem Pfad befindet: <*Installationsverzeichnis*>\agent\server\jserver\bin
2. Geben Sie folgende Parameter ein:
   - **cimserver**

     Den URL des Servers, z. B.: https://localhost/root/mcdata
   - **cimserverusername**

     Den Benutzernamen für die Anmeldung beim CIM Server, z. B.: Administrator
   - **cimserverpassword**

     Das Kennwort für die Anmeldung beim CIM Server, z. B.: Kennwort
   - **switchip**

     Die IP-Adresse des Switches, z. B.: 172.26.24.180
   - **switchtype**

     Den Produkt-Typ-Code des Switches. Informationen hierzu finden Sie in der Anmerkung (siehe unten).
   - **switchusername**

     Der Benutzername für die Anmeldung beim Switch.

- **switchpassword**

  Das Kennwort für die Anmeldung beim Switch.

HINWEIS: Die Produkt-Typ-Codes der FC-Switches lauten wie folgt:

Sphereon 3016: Code 2

Sphereon 3032: Code 3

Sphereon 3216: Code 4

Sphereon 3232: Code 5

Sphereon 4300: Code 6

Sphereon 4400: Code 12

Sphereon 4500: Code 7

Sphereon 4700: Code 13

3. Verschieben Sie mithilfe der Eingabeaufforderung Informationen in den folgenden Pfad: <*Installationsverzeichnis*>\agent\server\jserver\bin
4. Führen Sie folgenden Befehl aus: ManageSwitch Add

Tabelle 7-2 enthält einen Überblick über die Informationen, die für die Verbindung zu einem Brocade Sphereon FC-Switch erforderlich sind.

Tabelle 7-2: Informationen für die Verbindung zu einem Brocade FC-Switch

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem Brocade SMI Agent for EOS installiert ist.
Namespace	Geben Sie `root/mcdata` an.
Vorhandensein von SSL	Wenden Sie die Einstellungen für Brocade SMI Agent an, die während der Installation konfiguriert wurden.
Port-Nummer	Wenden Sie die Einstellungen für Brocade SMI Agent for EOS an, die während der Installation konfiguriert wurden.
Benutzer-ID	Geben Sie die Benutzer-ID für Brocade SMI Agent for EOS an.
Kennwort	Geben Sie ein Kennwort für die Benutzer-ID ein.

Konfigurieren von QLogic FC-Switches

Der SMI-S-Provider ist im QLogic FC-Switch integriert. Das Verfahren in diesem Abschnitt beschreibt, wie man eine Verbindung zum Verwaltungs-Port des QLogic FC-Switches mithilfe eines Web-Browsers herstellt.

Details zur Konfiguration der SMI-S-Provider-Einstellungen mithilfe der Befehlszeilenschnittstelle (CLI) finden Sie in der Dokumentation für den QLogic FC-Switch. Die Dokumentation ist von folgender Website erhältlich:

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/NewDefault.aspx

Konfigurieren von QLogic FC-Switches:

1. Stellen Sie in Ihrem Web-Browser eine Verbindung zum Verwaltungsanschluss des QLogic FC-Switches her (Beispiel: http://10.208.113.46). Das Fenster **Switch Manager** (Switch-Verwaltung) wird angezeigt.
2. Wählen Sie in der Menüleiste für **Switch Manager** (Switch-Verwaltung) die Option **Switch** und anschließend **Services** aus. Das Dialogfeld **System Services** (Systemservices) wird angezeigt.
3. Überprüfen Sie, ob der SMI-S-Provider-Service aktiviert ist:
   - Wenn **CIM service** (CIM-Service) ausgewählt ist, bedeutet dies, dass der SMI-S-Provider-Service aktiviert ist. Klicken Sie auf **Schließen**.
   - Wenn **CIM service** (CIM-Service) nicht ausgewählt ist, wählen Sie ihn jetzt aus, und klicken Sie auf **OK**.
4. Wenn im Dialogfeld **System Services** (Systemservices) eine Option zum Angeben des **SSL service (SSL-Service)** vorhanden ist, können Sie den SSL-Port **5989** verwenden.

Tabelle 7-3 enthält einen Überblick über die Informationen, die für die Verbindung zu einem QLogic FC-Switch erforderlich sind.

Tabelle 7-3: Informationen für die Verbindung zu einem QLogic FC-Switch

Element	Details
IP-Adresse	IP-Adresse des QLogic FC-Switches
Namespace	Geben Sie `root/switch` ein.
Vorhandensein von SSL	Wenden Sie die Einstellungen für den QLogic FC-Switch an.
Port-Nummer	Wenden Sie die Einstellungen für den QLogic FC-Switch an, die während der Installation konfiguriert wurden. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Geben Sie die Benutzer-ID für den QLogic FC-Switch an.
Kennwort	Geben Sie ein Kennwort für die Benutzer-ID ein.

Konfigurieren von Cisco MDS 9000 Family FC-Switches

Der SMI-S-Provider ist im Cisco FC-Switch integriert. In den folgenden Schritten wird beschrieben, wie der Server aktiviert und mithilfe des HTTP-Protokolls verbunden wird (Port 5988). Wenn an Ihrem Standort das HTTPS-Protokoll (Port 5989) verwendet wird, wenden Sie die SSL-Authentifizierung (Secure Socket Layer) als Verschlüsselungsmethode für die Anmeldedaten an. Aktivieren Sie anschließend den HTTPS- und SMI-S-Agent (Proxy). Einzelheiten zu dieser Vorgehensweise finden Sie unter dem Link in Tabelle 7-4.

Einzelheiten finden Sie in den Programmierhinweisen für Cisco MDS 9000 Family SMI-S. Das Dokument ist von folgender Website erhältlich:

http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html

Konfigurieren von Cisco MDS 9000 Family FC-Switches

Ein Beispiel für die Befehlsausführung, die im folgenden Verfahren beschrieben wird, wird nach Schritt 8 beschrieben.

1. Greifen Sie über Telnet auf den FC-Switch zu, und melden Sie sich anschließend an.
2. Geben Sie `show cimserver` ein, und überprüfen Sie, dass cimserver Http aktiviert ist.
3. Geben Sie `config terminal` ein, und starten Sie den Konfigurationsmodus.
4. Standardmäßig ist HTTP aktiviert. Ist das nicht der Fall, aktivieren Sie HTTP, indem Sie `cimserver enableHttp` eingeben.
5. Geben Sie `cimserver enable` ein, um den CIM-Server zu aktivieren.
6. Geben Sie `end` ein, um den Konfigurationsmodus zu beenden.
7. Geben Sie `show cimserver` ein, und überprüfen Sie die Einstellungen:
   - cimserver is enabled
   - cimserver Http is enabled
8. Geben Sie `exit` ein, um Telnet zu trennen.

Befehlsbeispiel

```
FCGS03 login: ********

Kennwort:

FCGS03# show cimserver

 cimserver is not enabled

 cimserver Http is enabled

 cimserver Https is not enabled

 cimserver certificate file is not installed

FCGS03# config terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
FCGS03(config)# cimserver enable

FCGS03(config)# end

FCGS03# show cimserver

 cimserver is enabled

 cimserver Http is enabled

 cimserver Https is not enabled

 cimserver certificate file is not installed

 Current value for the property logLevel in CIMServer is
'WARNING'.

FCGS03# exit
```

Tabelle 7-4: Informationen für die Verbindung zu einem Cisco FC-Switch

Element	Details
IP-Adresse	IP-Adresse des Cisco FC-Switches
Namespace	Geben Sie `root/cimv2` ein.
Vorhandensein von SSL	Wenden Sie die Einstellungen für den Cisco FC-Switch an. Einzelheiten finden Sie in den Programmierhinweisen für Cisco MDS 9000 Family SMI-S: http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html
Port-Nummer	Wenden Sie die Einstellungen für den Cisco FC-Switch an, die während der Installation konfiguriert wurden. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Geben Sie die Benutzer-ID für den Cisco FC-Switch an.
Kennwort	Geben Sie ein Kennwort für die Benutzer-ID ein.

Vorbereiten von SMI-S auf die Speicherung

Speichergeräte, die als Überwachungsziele angegeben werden sollen, müssen SMI-S-Version 1.0 - 1.3 unterstützen, und der Service zur Verwaltung dieser Speichergeräte muss aktiv sein. In diesem Abschnitt werden die Einstellungen des SMI-S für folgende Elemente beschrieben:

- EMC-Speichergeräte
- HP EVA-Speichergeräte
- HP MSA-Speichergeräte
- Engenio OEM Sun-Speichergeräte und IBM-Speichergeräte
- NetApp-Speichergeräte

HINWEIS: Informationen zur Konfiguration von Hitachi Speichergeräten und zum Abrufen von Leistungsdaten zu Hitachi Storage (USP VM) finden Sie unter Chapter 6, Vorbereiten von Hitachi Storage.

Hinweise zur maximalen Anzahl überwachter Volumes für ein Speichergerät

Für ein Speichergerät können maximal 2000 Volumes (logische Geräte) überwacht werden. Wenn dieser Wert überschritten wird, gibt das Speichervolume (Komponententyp), das auf der Registerkarte **Komponenten** des **Überwachungsmoduls** angezeigt wird, die folgenden Informationen aus, und das Volume kann nicht überwacht werden:

- Komponentenname: Volumes (Anzahl der Volumes)
- Komponentenstatus: Das Volume kann nicht überwacht werden, da die Anzahl der Volumes größer als 2000 ist.

Außerdem werden die folgenden Informationen zum Volume nicht erfasst. Im **Überwachungsmodul** werden folgende Informationen angezeigt:

- **Komponenten** (Registerkarte) Für die folgenden Komponententypen werden keine Daten angezeigt: „LUN", „Speicher für exportierte Dateifreigabe", „Speicher für Dateifreigabe-Port", „Speichervolume"
- **Leistung** (Registerkarte) Der Status von Cache-Trefferverhältnis (Schreiben) lautet Unbekannt, und die Leistung wird nicht abgerufen.

Konfigurieren von EMC-Speichergeräten

Konfigurieren Sie die Einstellungen des SMI-S-Agent gemäß den folgenden Richtlinien. Weitere Informationen finden Sie in der Dokumentation zum EMC SMI-S-Agent:

- EMC SMI-S-Provider Versionshinweise

  Übersicht: Installationsmethode und Einstellungsmethode nach der Installation

  http://Powerlink.EMC.com

  Support > **Technical Documentation and Advisories** > **Software ~ S ~ Documentation** > **SMI-S-Provider** > **Release Notes**

- EMC Support-Matrix

  Übersicht: Support-Ziel des EMC SMI-S-Providers

  http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

Anforderungen vor der Installation

- EMC SMI-S-Provider Version: V3.2.3, V3.3.1
- Betriebssystem: Microsoft Windows 2003 [x86] R2, SP1
- Speicher-Array: CLARiiON

Über folgenden Link finden Sie Informationen über die EMC Support Matrix für die Anforderungen an die Speicherbetriebsumgebung:

http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

HINWEIS: Der Wert für die Leistungs-Metrik, **WriteHitIOs**, wird in EMC CLARiiON nicht erfasst.

So wird der EMC SMI-S-Provider installiert:

Bitte beachten Sie, dass falls installiert, EMC SMI-S-Provider der vorangegangenen Version oder der Solutions Enabler deinstalliert werden müssen.

1. Sie können den EMC SMI-S-Provider unter folgender URL herunterladen:

   http://Powerlink.EMC.com
2. Navigieren Sie zu folgendem Speicherort: **Support** > **Software Downloads and Licensing** > **Downloads S** > **SMI-S Provider**
3. Schließen Sie vor dem Starten der Installation alle Anwendungen.
4. Laden Sie **se6430-WINDOWS-x86-SMI.msi** oder **se65132-WINDOWS-x86-SMI.msi** herunter.
5. Starten Sie die Installationsdatei, um den Installationsassistenten für **EMC Solutions Enabler with SMI** zu starten.
6. Führen Sie alle Schritte in dem Assistenten durch, zu denen Sie aufgefordert werden. Klicken Sie zum Abschluss auf **OK**.

   Jetzt können Sie die Speicherinformationen registrieren.

So registrieren Sie die Speicherinformationen:

Das folgende Verfahren stellt sicher, dass Sie unter Verwendung des EMC SMI-S-Provider Speicher verwalten können.

1. Wenn das EMC-Speichervolumen nicht auf einen Server angewendet wird, auf dem EMC SMI-S-Provider installiert ist, führen Sie die folgenden band-externen Schritte durch. Ein Beispiel für die Befehlsausführung, die im folgenden Verfahren beschrieben wird, wird nach Schritt j beschrieben.
   a. Führen Sie die Datei **TestSmiProvider.exe** aus, die sich in folgendem Pfad befindet: *<Installationsverzeichnis>*\SYMCLI\storbin\TestSmiProvider.exe

b. Bei all Hosts, Connection Type, Logfile path, Port, Username und Password klicken Sie auf Enter, um die Standardinformationen zu behalten.

c. Geben Sie **addsys** ein, und klicken Sie auf **Enter**.

d. Geben Sie **y** ein, und klicken Sie auf **Enter**.

e. Wählen Sie den Typ des Speicher-Arrays. Für CLARiiON geben Sie **1** ein, und klicken Sie auf **Enter**.

f. Geben Sie die IP-Adresse von **Processor A** ein, und klicken Sie auf **Enter**. Geben Sie außerdem die IP-Adresse von **Processor** B ein, und klicken Sie auf **Enter**.

g. Wählen Sie den in Schritt f angegebenen Adresstyp aus. Geben Sie **2** ein, und klicken Sie auf **Enter**.

h. Geben Sie die mit der Administrator-Autorität verbundene Benutzer-ID und das Kennwort für den Speicher, den Sie registrieren, ein.

i. Wenn die Registrierung erfolgreich ist, wird **OUTPUT : 0** angezeigt. Schreiben Sie die Seriennummer auf, die in dem jeweiligen Bereich des Befehls angezeigt wird, z. B. CK200080001000.

j. Geben Sie **dv** ein, und klicken Sie auf **Enter**. Überprüfen Sie, ob die Seriennummer, die Sie in Schritt **i** notiert haben, in den Informationen zur **Firmware-Version** angezeigt wird.

Befehlsbeispiel

```
Host [localhost]:
Connection Type (ssl,no_ssl) [no_ssl]:
Logfile path [Testsmiprovider.log]:
Port [5988]:
Username []:
Password []:
Connecting to localhost: 5988
(localhost:5988) ? addsys
Add System {y|n} [n]: y
ArrayType (1=Clar, 2=Symm) [1]: 1
One or more IP address or Hostname or Array ID
Elements for Addresses
IP address or hostname or array id 0 (blank to quit):
192.168.10.31
IP address or hostname or array id 1 (blank to quit):
192.168.10.32
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]: 2
Address Type (1) [default=2]: 2
```

```
User [null]: analyzer

Password [null]: analyzerpass

++++ EMCAddSystem ++++

OUTPUT : 0

Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout,
4=Failed

       5=Invalid Parameter

       4096=Job Queued, 4097=Size Not Supported

System: //kaede/root/
emc:Clar_StorageSystem.CreationClassName="Clar_StorageSys
tem",Name="CLARiiON+CK200080001000"

(localhost:5988) ? dv

++++ Display version information ++++

CIM ObjectManager Name: PG:5B48A8C4-682F-4FCB-AE98-
F0687C31225F

CIMOM Version: Pegasus CIM Server Version 2.6.1

SMI-S spec version: 1.3.0

SMI-S Provider version: V3.3.1.0

Solutions Enabler version: V6.5-883 1.32

Firmware version information:

CLARiiON Array CK200080001000 (Rack Mounted CX3_10_C) :
3.26.10.5.019
```

2. Wenn das EMC-Speichervolumen auf einen Server angewendet wird, auf dem EMC SMI-S-Provider installiert ist, führen Sie die folgenden band-internen Schritte durch. Ein Beispiel für die Befehlsausführung, die im folgenden Verfahren beschrieben wird, wird nach Schritt f beschrieben.
   a. Bestätigen Sie, dass mindestens ein CLARiiON LUN registriert ist. Führen Sie den folgenden Befehl von dem Server aus, auf dem der EMC SMI-S-Provider installiert ist:

      <*Installation folder*>\SYMCLI\bin> syminq -cids

   b. Bestätigen Sie, dass der Wert für folgende Einstellung auf **true** gesetzt ist:
      OslProv/com.emc.se.osls.osl.StorApi.database.discover
      Diese Einstellung befindet sich in der Konfigurationsdatei von **emcprovider.conf**:
      <*Installationsordner*>\SYMCLI\storbin**TestSmiProvider.exe**

      Wenn der Wert **false** ist, ändern Sie ihn zu **true**.

   c. Führen Sie folgenden Befehl aus, um den EMC SMI-S-Provider-Service zu unterbrechen:

      <*Installation folder*>\SYMCLI\strobin> cimserver -stop EMC_SMI_Provider

d. Führen Sie folgenden Befehl aus, um die Authentifizierungsinformation zu registrieren:

   <*Installation folder*>\SYMCLI\bin>symcfg authorization add -host <*Storage IP address*> -Username <Storage User ID> -Password <*Storage Password*>

   Die folgenden Befehle würden beispielsweise ausgeführt, wenn das Kennwort von IT Operations Analyzer **analyzerpass** ist, die IP-Adresse von **Processor A 192.168.10.31** ist und die IP-Adresse von **Processor B** für CLARiiON **192.168.10.32** ist. Processor A wird zuerst registriert:

   <*Installation folder*>\SYMCLI\bin>symcfg authorization add -host

   192.168.10.31 -username analyzer -password analyzerpass

   <*Installation folder*>\SYMCLI\bin>symcfg authorization add -host

   192.168.10.32 -username analyzer -password analyzerpass

e. Führen Sie folgenden Befehl aus, um den EMC SMI-S-Provider-Service zu starten: Anschließend dauert es einige Zeit, bis Sie von IT Operations Analyzer aus suchen können:

   <*Installation folder*>\SYMCLI\strobin> cimserver -start EMC_SMI_Provider

f. Führen Sie folgenden Befehl aus, um die Registrierungsinformationen zu bestätigen:

   <*Installation folder*>\SYMCLI\bin> symcfg list auth

Befehlsbeispiel

```
C:\Program Files\EMC\SYMCLI\bin>syminq -cids

Device                 Clariion               Device

------------------------ --------------------- ---------

Name               Type   ID Rev  Ser Num      Cap (KB)

------------------------ --------------------- ---------
\\.\PHYSICALDRIVE2      CK200080001000  0326 070000B5
1048576

C:\Program Files\EMC\SYMCLI\storbin>cimserver -stop
EMC_SMI_Provider

Pegasus wurde als Windows-Dienst angehalten

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.31 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.32 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\storbin>cimserver -start
EMC_SMI_Provider
```

```
Pegasus wurde als Windows-Dienst gestartet
C:\Program Files\EMC\SYMCLI\bin>symcfg list auth
Hostname            Username          Namespace     Port
192.168.10.31         analyzer
192.168.10.32         analyzer
```

Abrufen von Leistungsdaten des EMC-Speichergeräts

Führen Sie folgende Schritte aus, um die Leistungsdaten des EMC-Speichergeräts abzurufen.

1. Rufen Sie die Leistungsdaten mit der Verwaltungssoftware für das EMC-Speichergerät ab. Folgen Sie dabei den Anweisungen für **EMC Navisphere Management Suite**:
   a. Öffnen Sie über die Menüleiste von **EMC Navisphere Management Suite** das Fenster **Data Logging** (Datenprotokollierung). Wählen Sie im Menü **Extras** die Option **Analyzer** und dann **Data Logging** (Datenprotokollierung).
   b. Wählen Sie im Bereich **Target** (Ziel) das Speichergerät aus, dessen Leistungsdaten abgerufen werden sollen, und prüfen Sie den Wert im Feld **Status** für Logging (Protokollierung):

      Wenn **Status** den Wert **Stopped** (Angehalten) hat, klicken Sie auf **Start** (Starten).

      Wenn **Status** den Wert **Running. Started on date time** (Aktiv. Gestartet am [Datum] um [Uhrzeit]) hat, klicken Sie auf **Cancel** (Abbrechen). Es ist nicht notwendig, den SMI-S-Agent erneut zu starten.
2. Starten Sie den SMI-S-Provider erneut. Wenn Sie die Befehlszeilenschnittstelle (CLI) verwenden, führen Sie den Befehl `cimserver` aus. Halten Sie anschließend den SMI-S-Provider an, und starten Sie ihn dann erneut:

```
<Installation folder>\SYMCLI\strobin> cimserver -stop
EMC_SMI_Provider
Pegasus wurde als Windows-Dienst angehalten
<Installation folder>\SYMCLI\strobin> cimserver -start
EMC_SMI_Provider
Pegasus wurde als Windows-Dienst gestartet
```

Tabelle 7-5: Informationen für die Verbindung zu EMC-Speichergeräten

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem der EMC SMI-S-Provider installiert ist.
Namespace	Geben Sie `root/emc` ein.
Vorhandensein von SSL	Geben Sie die Einstellungen für den EMC-Provider an.
Port-Nummer	Geben Sie die Einstellungen für den EMC SMI-S-Provider an. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Geben Sie die Benutzer-ID für den EMC-Provider an. Standardeinstellung ist leer.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an. Standardeinstellung ist leer.

Konfigurieren von HP EVA-Speichergeräten

Konfigurieren Sie die Einstellungen des SMI-S-Providers gemäß den folgenden Richtlinien. Weitere Informationen finden Sie in den Handbüchern zu Command View EVA.

HINWEIS: Die Funktion zum Abrufen von Leistungsinformationen wird vom HP EVA SMI-S-Agent nicht unterstützt.

Anforderungen vor der Installation

- Unterstützte Version: HP StorageWorks Command View EVA 8.0
- Betriebssystem: Microsoft Windows Server 2003
- Speicher: HP StorageWorks 4400 Enterprise Virtual Array

Installation von HP StorageWorks Command View EVA 8.0:

1. Starten Sie die ausführbare Datei HP StorageWorks Command View EVA Software Suite.exe.
2. Klicken Sie auf **OK**, um den Installationsassistenten zu starten.
3. Wählen Sie im Installations-Fenster **Choose Install Set**, und stellen Sie sicher, dass **SMI-S CIMOM** ausgewählt ist.

   Der HP SMI-S EVA verwendet die Standard-Port-Nummern 5988 oder 5989.

   Wenn die Benutzung der Standard-Ports nicht möglich ist, wird eine Meldung angezeigt, welche Ports nicht verfügbar sind. Wenn Sie eine solche Meldung erhalten, geben Sie eine verfügbare Port-Nummer an (von 60000 bis 65536). Setzen Sie dann die Installation fort.
4. Das letzte Fenster des Installationsassistenten zeigt **Install Complete** an. Zum Abschluss klicken Sie auf **Done**.

   Jetzt können Sie die HP Command View EVA Einstellungen anwenden.

Zur Anwendung der Einstellungen von HP Command View EVA:

1. Konfigurieren Sie den CIMOM Server:
   a. Modifizieren Sie die folgende Datei, um die Port-Nummer und HTTP/HTTPS, die für den CIMOM Server verwendet werden, zu ändern:

      <*Installationsverzeichnis*>\SMI-S\CXWSCimom\config\cxws.properties

   b. Die Standardwerte lauten wie folgt:

      enableHttp: true

      enableHttps: true

      cxws.http.port: 5988

      cxws.https.port: 5989

      Geben Sie **False** an, wenn Sie enableHttp (Https) annullieren und die zu verwendende Port-Nummer angeben.

c. Nach Änderung der Einstellungen starten Sie HP StorageWorks CIM Object Manager Service (Objektmanager-Service) neu:

   Wählen Sie im Menü **Start** die Option **Einstellung**, **Systemsteuerung**, **Verwaltungstools** und dann **Dienst**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zum Startmenü zu navigieren, anders.

2. Registrieren Sie Ihren Speicher:
   a. Starten Sie Ihren Browser, und geben Sie folgende URL ein:

      https://host_name:2372

      Geben Sie **Server name** oder **IP Address** für den **host_name** ein.

   b. Melden Sie sich am **HP Command View EVA prompt** an.

      Verwenden Sie beim Anmelden die Benutzerkontoinformationen des Servers, auf dem Sie die HP Command View EVA installiert haben. Stellen Sie sicher, dass das Benutzerkonto der **HP Storage Admin group** gehört.

   c. Nach dem Anmelden bestätigen Sie, dass Ihr Speicher im Fenster **Storage System** angezeigt wird. Wenn er nicht angezeigt wird, klicken Sie auf **Discover** (Ermitteln), um Ihren Speicher zu registrieren.

HINWEIS: Damit der Speicher registriert werden kann, muss der Server, auf dem HP Command View EVA installiert ist, direkt an den FS-Switch angeschlossen werden.

Tabelle 7-6: Informationen für die Verbindung zu HP EVA-Speichergeräten

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem Command View EVA installiert ist.
Namespace	Geben Sie `root/eva` ein.
Vorhandensein von SSL	Geben Sie die Einstellungen für Command View EVA an.
Port-Nummer	Geben Sie die Einstellungen für Command View EVA an. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Geben Sie die Benutzer-ID für Command View EVA an.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.

Konfigurieren von HP MSA-Speichergeräten

Konfigurieren Sie die Einstellungen des SMI-S-Agent gemäß den folgenden Anweisungen. Weitere Informationen finden Sie in der Dokumentation zum MSA SMI-S-Agent.

HINWEIS: Die Funktion zum Abrufen von Leistungsinformationen wird vom HP MSA SMI-S-Agent nicht unterstützt.

1. Sie können den **MSA SMI-S-Provider** unter folgender URL herunterladen:

   http://h18006.www1.hp.com/storage/smis.html

2. Installieren Sie den **MSA SMI-S-Provider** auf einem beliebigen Server.

Tabelle 7-7: Informationen für die Verbindung zu HP MSA-Speichergeräten

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem der MSA SMI-S-Provider installiert ist.
Namespace	Geben Sie `root/hpmsa` ein.
Vorhandensein von SSL	Geben Sie die Einstellungen für den MSA SMI-S-Provider an.
Port-Nummer	Geben Sie die Einstellungen für den MSA SMI-S-Provider an.
Benutzer-ID	Geben Sie die Benutzer-ID für den MSA SMI-S-Provider an.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.

Konfigurieren von Engenio OEM Sun-Speichergeräten und IBM-Speichergeräten

Konfigurieren Sie die Einstellungen des SMI-S-Providers gemäß den folgenden Anweisungen. Weitere Informationen finden Sie in der Dokumentation zum Engenio SMI-S-Provider. Um die Dokumente herunterzuladen, ist ein Anmeldekonto für die NetApp-Website erforderlich:

http://support.netapp.com/NOW/apbu/oemcp/protcd/

Anforderungen vor der Installation

- Unterstützte Version: Engenio SMI Provider 09.19.G0.07
- Betriebssystem: Microsoft Windows Server 2003 (32 Bit)

Installation des Engenio SMI-S-Providers:

1. Starten Sie die ausführbare Datei zur Installation des Engenio SMI Provider 09.19.G0.07.
2. Führen Sie alle Schritte in dem Installationsassistenten durch, zu denen Sie aufgefordert werden.
3. Wenn Sie die Installation abgeschlossen haben, klicken Sie auf **Done**.

So registrieren Sie das Speichergerät:

Das folgende Verfahren registriert das Speichergerät, das Sie mit dem Engenio SMI-Provider verwalten wollen.

1. Starten Sie die Befehlszeile.
2. Navigieren Sie zu folgendem Verzeichnis:

   <*Installation directory*>\SMI_SProvider\bin
3. Starten Sie den Befehl `ProviderUtil`, und geben Sie folgende Informationen ein:
   - **Input CIMOM Username**

     Geben Sie optional den CIMOM-Benutzernamen ein, z. B.: any
   - **Input CIMOM Password**

     Geben Sie optional das CIMOM-Kennwort ein, z. B.: any
   - **Input Port [5988]**

     Geben Sie optional eine Port-Nummer ein. Der Standardwert ist 5988.
   - **Input Operation**

     1) add Device

     2) remove Device

     3) Add credentials for an array

     Please Input 1, 2, or 3

     Geben Sie **1** ein, um ein Speichergerät zu registrieren.
   - **Input device DNS-resolvable hostname or IP address**

     Geben Sie die IP-Adresse oder den Hostnamen für das Speichergerät ein.
   - **Input Array Password** (default is blank)

     Geben Sie das Kennwort des Speichergeräts ein.

   Das Speichergerät ist erfolgreich registriert, wenn die Meldung **The extrinsic call succeeded** (Eingehender Anruf erfolgreich) angezeigt wird.

Tabelle 7-8 enthält einen Überblick über die Informationen, die für die Verbindung zu dem zu überwachenden Speicherknoten erforderlich sind.

Tabelle 7-8: Informationen für die Verbindung zu Sun- und IBM-Speichergeräten

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem der Engenio SMI-S-Provider installiert ist.
Namespace	Geben Sie `root/lsissi11` ein.
Vorhandensein von SSL	Geben Sie die Einstellungen für den Engenio SMI-S-Provider an.
Port-Nummer	Geben Sie die Einstellungen für den Engenio SMI-S-Provider an. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989

Tabelle 7-8: Informationen für die Verbindung zu Sun- und IBM-Speichergeräten

Element	Details
Benutzer-ID	Geben Sie die Benutzer-ID für den Engenio SMI-S-Provider an.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.

Konfigurieren von NetApp-Speicher

Konfigurieren Sie die Einstellungen des SMI-S-Providers für NetApp-Speicher gemäß den folgenden Anweisungen. Weitere Informationen finden Sie in der Dokumentation zum NetApp SMI-S-Provider. Um die Dokumente herunterzuladen, ist ein Anmeldekonto für die NetApp-Website erforderlich:

http://support.netapp.com/NOW/apbu/oemcp/protcd/

Anforderungen vor der Installation

- Unterstützte Version von NetApp Data ONTAP SMI-S Agent: Data ONTAP SMI-S Agent 3.0
- Betriebssystem: Microsoft Windows Server 2003 (32 Bit)

JDK 1.5.0 oder höher und JRE 1.5.0 sind zur Benutzung von NetApp Data ONTAP SMI-S-Agent erforderlich. Bestätigen Sie, ob auf dem Windows-Server, auf dem Sie den SMI-S-Agent installieren, die Informationen installiert sind.

Installation von Data ONTAP SMI-S-Agent 3.0:

1. Laden Sie die Data ONTAP SMI-S-Agent Installationsdatei herunter.
2. Wählen Sie **Windows** von **Select Platform** unter **Data ONTAP SMI-S-Agent**, und klicken Sie dann auf **Go**.
3. Klicken Sie auf **View & Download**.
4. Klicken Sie auf **CONTINUE** auf der Seite **Software download Instructions**.
5. Klicken Sie auf **Accept**, um fortzufahren. Laden Sie SMI-S-Agent und die entsprechenden Handbücher herunter.
6. Starten Sie die ausführbare Datei zur Installation des Data ONTAP SMI-S-Agent 3.0.
7. Wählen Sie je nach Bedarf **Typical** oder **Custom**.
8. Führen Sie alle Schritte in dem Installationsassistenten durch, zu denen Sie aufgefordert werden.
9. Wenn Sie die Installation abgeschlossen haben, klicken Sie auf **Done**.

Konfigurieren der SMI-S-Provider-Einstellungen:

1. Im Dialog **Edit System Variable** geben Sie **JAVA_HOME** als Systemumgebungsvariable oder Benutzerumgebungsvariable an. Wenn Sie einen Pfad angeben, der ein Leerzeichen enthält, schließen Sie den Pfad mit doppelten Anführungszeichen ein (").

2. Verwenden Sie für die Verbindung mit dem SMI-S-Provider die Port-Nummer **5989** und das **HTTPS**-Protokoll. Bearbeiten Sie die Datei **WEBSconfig.ini**, um die Port-Nummer zu ändern oder um die Verbindung mit dem HTTP-Protokoll zu aktivieren. Diese Datei befindet sich im folgenden Verzeichnis: **C:\Program\ws\server\ cserver\bin** Die folgenden Einstellungen sind die Standardvorgaben in der Datei **WEBSconfig.ini**. Wenn Sie sie ändern, setzen Sie **enableOverride** auf **True**.

   enableOverride=False (muss in **True** geändert werden, wenn Sie Änderungen an den folgenden Einstellungen vornehmen.)

   HTTPPort=5988

   HTTPSPort=5989

   enableSSL=True

   enableHTTP=False

So registrieren Sie das Speichergerät:

1. Wechseln Sie von der Befehlszeile auf den folgenden Pfad:

   C:\Program Files\ws\server\cserver\bin

2. Geben Sie an: **C:\Program Files\ws\bin**
3. Um das Speichergerät zu registrieren, führen Sie folgenden Befehl aus:

   `smis.bat <User ID> <Password> add <Storage IP address> <Storage User ID> <Storage Password> [-p http]*`

   *Nur angeben, wenn Sie das http-Protokoll verwenden.

   < UserID > und < Password > verwenden das Windows-Management-Autoritäts-Konto des Servers, auf dem SMI-S installiert ist. Die IP-Adresse des Gerätes < Storage_UserID > und < Storage_Password > spezifizieren die Authentifizierungsinformationen auf dem Speicher für < StorageIP >.

4. Um zu überprüfen, ob die Informationen registriert wurden, führen Sie die Datei **smis.bat** aus:

   `smis.bat <User ID> <Password> list`

5. Führen Sie das natest-Skript aus, das sich im Verzeichnis **ws\bin** befindet, um zu überprüfen, ob SMI-S-Provider die Speicherinformationen erhalten konnte. Im folgenden Beispiel werden Datenträgerinformationen des Speichergeräts ausgegeben:

   `natest.bat <User ID> <Password> disks`

Tabelle 7-9 enthält einen Überblick über die Informationen, die für die Verbindung zu den NetApp-Speichergeräten erforderlich sind.

Tabelle 7-9: Informationen für die Verbindung zu NetApp-Speichergeräten

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Servers an, auf dem der ONTAP SMI-S-Agent installiert ist.
Namespace	Geben Sie `root/ontap` an.
Vorhandensein von SSL	Verwenden Sie die Einstellungen für Data ONTAP SMI-S Agent.
Port-Nummer	Verwenden Sie die Einstellungen für Data ONTAP SMI-S Agent. Standardwerte: • Nicht-SSL-Kommunikation: 5988 • SSL-Kommunikation: 5989
Benutzer-ID	Verwenden Sie die Benutzer-ID des Servers, auf dem der ONTAP SMI-S Agent installiert ist.
Kennwort	Geben Sie das Kennwort für die entsprechende Benutzer-ID an.

HINWEIS: Wenn Sie einen NetApp-Speicherknoten auswählen, zeigt ein Symbol im **Überwachungsmodul** an, ob IT Operations Analyzer die Statusinformationen verarbeitet oder wenn das Programm Informationen für die Komponente sammelt. Außerdem wird möglicherweise innerhalb von 15 Minuten die folgende Fehlermeldung angezeigt:

KAZZ20087-E Die Aktualisierung der Konfiguration ist fehlgeschlagen. Name des Knotens, bei dem der Fehler aufgetreten ist: <Gerätename>

Diese Fehlermeldung wird angezeigt, wenn alle folgenden Bedingungen vorliegen:

1. Das NetApp-Speichergerät wird überwacht.
2. Das NetApp-Speichergerät wird auf einem Linux-Server unter Verwendung einer Linux-Version eines SMI-S-Agent verwaltet.
3. Eine HTTPS-Verbindung besteht zwischen dem Verwaltungsserver von IT Operations Analyzer und der Linux-Version des SMI-S-Agent, der überwacht wird.

Führen Sie einen der folgenden Schritte aus:

- Registrieren Sie die IP-Adresse und den Hostnamen der Linux-Version des SMI-S-Agent in der Host-Datei des Servers, auf dem IT Operations Analyzer installiert ist: den Verwaltungsserver.
- Ändern Sie die aktuelle HTTPS-Verbindungsmethode, die zwischen dem Verwaltungsserver von IT Operations Analyzer und der Linux Version des SMI-S-Agent besteht, auf HTTP.
- Ändern Sie die Linux-Version des SMI-S-Agent auf die Windows-Version des SMI-S-Agent.

8

Vorbereiten von Dell-Servern

In diesem Kapitel werden die zur Einrichtung Ihres Dell-Servers erforderlichen Aufgaben beschrieben.

Übersicht

Es müssen jeweils zwei der folgenden Protokolle eingerichtet werden:

- WMI/SNMP für Windows-basierte Dell-Server (Zugangsdaten).
- SSH/SNMP für Linux-basierte Dell-Server (Zugangsdaten).

Tabelle 8-1 enthält einen Überblick über die Informationen, die für die Verbindung zu einem Dell-Server erforderlich sind.

Tabelle 8-1: Informationen zum Anschluss auf einen Dell-Server

Element	Details
IP-Adresse	Geben Sie die IP-Adresse des Dell-Servers ein.
Port-Nummer	Der SNMP-Port, an dem der Dell-Server auf Verbindungen wartet (Port 161).
Community-Name	Der für SNMP-Dell-Server verwendete Community-Name.

Aktivieren der SNMP-Service- und -Trap-Kommunikation

Der SNMP-Agent muss auf jedem überwachten Dell-Server so konfiguriert werden, dass SNMP-Traps an den Verwaltungsserver von Hitachi IT Operations Analyzer gesendet werden.

Wenn ein Dell OMSA-Trap vom Server empfangen wird, aktualisiert IT Operations Analyzer den Status der Dell OMSA-Trap-Komponente basierend auf dem Schweregrad des empfangenen Traps.

Konfigurieren eines SNMP-Agents in einer Microsoft Windows-Umgebung

So konfigurieren Sie den SNMP-Agent des Dell-Servers in einer Microsoft Windows-Umgebung:

1. Öffnen Sie das **Startmenü** auf Ihrem Desktop, und wählen Sie die **Systemsteuerung**.

HINWEIS: Unter Windows Server 2012 sind die Schritte, um zum Startmenü zu navigieren, anders.

2. Öffnen Sie **Verwaltung**.
3. Öffnen Sie **Dienste**.
4. Klicken Sie mit der rechten Maustaste auf **SNMP-Dienst**, und wählen Sie **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Sicherheit**, um das Dialogfeld **Sicherheit** zu öffnen.
6. Wählen Sie **SNMP-Pakete von jedem Host annehmen**, oder wählen Sie **SNMP-Pakete von diesen Hosts annehmen**, und klicken Sie anschließend auf **Hinzufügen**.

   Das Feld **SNMP-Dienstkonfiguration** wird angezeigt.
7. Geben Sie den Hostnamen oder die IP-Adresse des Verwaltungsservers von IT Operations Analyzer ein, und klicken Sie anschließend auf **Hinzufügen**.

8. Klicken Sie auf die Registerkarte **Traps**, um das Dialogfeld **Traps** zu öffnen.
9. Wählen Sie in der Drop-down-Liste **Community Name** den entsprechenden SNMP-Community-Namen aus, und klicken Sie anschließend unter dem Listenfeld **Trapziele** auf **Hinzufügen**.

   Das Feld **SNMP-Dienstkonfiguration** wird angezeigt.
10. Geben Sie den Hostnamen oder die IP-Adresse des Verwaltungsservers von IT Operations Analyzer ein, und klicken Sie anschließend auf **Hinzufügen**.
11. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Konfigurieren eines SNMP-Agents in einer Linux-Umgebung

So konfigurieren Sie den SNMP-Agent des Dell-Servers in einer Red Hat Enterprise Linux-Umgebung:

1. Fügen Sie die folgende Zeile zur Konfigurationsdatei **/etc/snmp/snmpd.conf** hinzu:

   trapsink IP_address community_name

   Der Wert der Variablen **IP_address** stellt die IP-Adresse des Verwaltungsservers von IT Operations Analyzer dar. Der Wert der Variablen **community_name** stellt den SNMP-Community-Namen dar.

2. Starten Sie den SNMP-Agent mithilfe des folgenden Befehls neu:

   /sbin/service snmpd restart

Index

V

Hitachi Data Systems

Unternehmenszentrale
2845 Lafayette Street
Santa Clara, California 95050-2639
USA
www.hds.com

Kontaktinformationen nach Regionen

Amerika
+1 408 970 1000
info@hds.com

Europa, Mittlerer und Naher Osten und Afrika
+44 (0)1753 618000
info.emea@hds.com

Asien-Pazifik
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90IOS006GE-12