



# Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

[Einführung des Dell OpenManage™ IT Assistant](#)  
[Zum Einstieg mit Dell OpenManage™ IT Assistant](#)  
[Was ist neu in Version 8.0 des Dell OpenManage™ IT Assistant?](#)  
[Installationsplan für Dell OpenManage™ IT Assistant](#)  
[Dell OpenManage™ IT Assistant installieren, deinstallieren und erweitern](#)  
[Dell OpenManage™ IT Assistant zur Überwachung von Systemen konfigurieren](#)  
[Leistungsüberwachung](#)

[Softwareaktualisierungen](#)  
[Berichterstattung und Task-Verwaltung](#)  
[Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten](#)  
[Häufig gestellte Fragen](#)  
[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)  
[Dienstprogramme des Dell OpenManage™ IT Assistant](#)

---

## Anmerkungen und Hinweise

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit deren Hilfe Sie den Computer besser einsetzen können.
-  **HINWEIS:** Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder Datenverlust und zeigt, wie diese vermieden werden können.

---

**Irrtümer und technische Änderungen vorbehalten.**  
© 2006 Dell Inc. Alle Rechte vorbehalten.

Nachdrucke jeglicher Art ohne die vorherige schriftliche Genehmigung der Dell Inc. sind strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, das *DELL*-Logo, *OpenManage*, *OptiPlex*, *PowerEdge*, *PowerVault* und *PowerConnect* sind Marken von Dell Inc.; *Microsoft*, *Windows*, *Windows NT*, *Windows Server*, *Active Directory* und *Excel* sind eingetragene Marken der Microsoft Corporation; *Novell*, *NetWare* und *SUSE* sind eingetragene Marken von Novell, Inc. in den Vereinigten Staaten und anderen Ländern; *Red Hat* ist eine eingetragene Marke von Red Hat, Inc.; *Intel* ist eine eingetragene Marke der Intel Corporation; *EMC*, *FLARE* und *Navisphere* sind eingetragene Marken der EMC Corporation.

Alle anderen in dieser Dokumentation genannten und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. verzichtet auf alle Besitzrechte an Markenzeichen und Handelsbezeichnungen, die nicht ihr Eigentum sind.

Juni 2006

[Zurück zum Inhaltsverzeichnis](#)

# Dell OpenManage™ IT Assistant zur Überwachung von Systemen konfigurieren

## Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [IT Assistant in authentischen Benutzerszenarien](#)
- [Sicherstellen, dass Agenten und Instrumentation installiert sind und ausgeführt werden](#)
- [IT Assistant starten](#)
- [SNMP für eine verbesserte Systemverwaltung konfigurieren](#)
- [CIM für verbesserte Verwaltung konfigurieren](#)
- [Die besten Methoden zur Einstellung von Ermittlungszielen](#)
- [IPMI für Verwaltungsfunktionen des Systems konfigurieren](#)
- [IT Assistant zur Ermittlung neuer Speichergeräte konfigurieren](#)
- [Ermittlung in Sabines Geschäft \(kleine bis mittlere Größe\)](#)
- [Warnungsmaßnahmenfilter und Warnungsmaßnahmen für Sabines Firma \(kleine bis mittlere Größe\) erstellen](#)
- [Ermittlung in Christians Firma \(Unternehmensgröße\)](#)
- [Warnungsmaßnahmenfilter und Warnungsmaßnahmen für Christians großes Unternehmen erstellen](#)
- [IPMI-Ermittlung in Christians Geschäft der Unternehmensgröße verwenden](#)
- [Zusammenfassung](#)

Dell OpenManage IT Assistant kann für alle Systeme Ihres Unternehmens Ermittlung, Bestandsaufnahme und eine Reihe von Änderungsverwaltungs-Tasks ausführen. Zu den verwalteten Systemen können eine Mischung von Client-Systemen (Desktops, portable Komponenten und Workstations), Servern, Druckern, Bandgeräten, Speichergeräten, Systemen mit Remote-Zugriffskarten, Dell™ PowerConnect™-Schaltern und digitalen KVM-Schaltern (Digitaltastatur/Video/Maus), die bei Systemen mit dicht gefüllten Racks verwendet werden, gehören.


## IT Assistant in authentischen Benutzerszenarien

In diesem Abschnitt wird beschrieben, wie IT Assistant in zwei verschiedenen Kundenszenarien eingesetzt werden kann:

1. Eine kleine bis mittelgroße Firma
1. Eine Umgebung in größeren Unternehmen

Obwohl es sich bei den beiden in diesem Abschnitt präsentierten Szenarien nicht um authentische Fälle handelt, illustrieren sie, wie Administratoren, die für die Verwaltung von Netzwerkumgebungen verantwortlich sind, IT Assistant konfigurieren könnten. Während ein Großteil der Konfigurationskonzepte für beide Szenarios gleich sind, hängen andere von Typ und Anzahl der verwalteten Systeme ab. Verwenden Sie das Szenario, das Ihrer Situation am besten entspricht, als einen allgemeinen Leitfaden zur Konfiguration des IT Assistant.

Unabhängig von der Größe Ihres Netzwerks ist es nützlich, beide Szenarios durchzulesen, um eine vollständigere Vorstellung der IT Assistant-Verfahren und -Konzepten zu gewinnen.

 **ANMERKUNG:** Es ist nicht beabsichtigt, das die beiden Szenarios in diesem Abschnitt, die gesamten Fähigkeiten des IT Assistant illustrieren. Je nach der Situation Ihres Unternehmens entscheiden Sie sich eventuell, Optionen und Funktionen des IT Assistant zu verwenden, die hier nicht gezeigt sind. Weitere Informationen zum vollen Umfang der Fähigkeiten von IT Assistant finden Sie in der *IT Assistant-Onlinehilfe*.

## Mehrere Java-Laufzeitumgebungen auf dem System besitzen

IT Assistant verwendet die Java-Laufzeitumgebung (JRE) Version 5.0. Sie möchten jedoch eventuell eine andere Version der JRE verwenden, um z. B. eine Drittanwendung auszuführen. Sie können eine ältere Version von JRE in Verbindung mit Version 5.0 verwenden.


### Zwischen verschiedenen JRE-Versionen umschalten

 **ANMERKUNG:** Weitere Informationen finden Sie in der J2SE 5.0-Dokumentation von Sun Microsystems unter <http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>. Wechseln Sie dort zum Java-Abschnitt **Applet-Laufzeit-Einstellungen**.

Wenn das System, das Sie zur Ausführung der IT Assistant-Konsole verwenden auch zur Ausführung von Applets verwendet wird, die eine andere Version der JRE benutzen, führen Sie folgende Schritte aus. Diese Schritte ermöglichen Ihnen, zwischen zwei Versionen der JRE umzuschalten.

1. Machen Sie die Datei **jpicip132.exe** der JRE-Version ausfindig, die Sie verwenden und ausführen möchten.

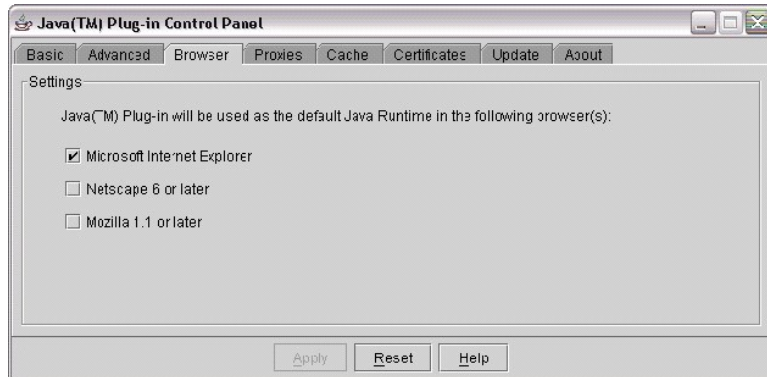
Wenn Sie z. B. die JRE-Version 1.4.2 verwenden möchten, können Sie `jpclip32.exe` unter `C:\Programme\Java\j2re1.4.2_05\bin` finden.

 **ANMERKUNG:** Diese Datei ist für alle JRE-Versionen verfügbar, die älter als Version 5.0 sind.

Das Java Plug-in Bedienungsfeld erscheint.

2. Im Register **Browser** heben Sie die Markierung von Microsoft Internet Explorer auf und klicken auf **Übernehmen**.
3. Wählen Sie jetzt Microsoft Internet Explorer, und klicken Sie auf **Übernehmen** (siehe [Abbildung 6-1](#)). Hierdurch wird JRE 1.4.2 mit Internet Explorer integriert.

**Abbildung 6-1. Java Plugin Bedienungsfeld für JRE 1.4.2**




4. Starten Sie Internet Explorer.
5. Führen Sie einen der folgenden Punkte aus, um die Java Plug-in-Versionsnummer zu überprüfen:
  1. Wählen Sie **Sun Java Konsole** vom Menü **Extras** aus. Die Java Plug-in-Versionsnummer wird 1.4.2\_05 sein.
  1. Wechseln Sie zu [www.java.com/en/download/faq/top\\_issues.jsp](http://www.java.com/en/download/faq/top_issues.jsp), und machen Sie das Thema **Test your Java Voirtual Machine (JVM) (Virtuelle Java-Maschine (JVM) testen)** ausfindig. Dieser Test überprüft die Java Plug-in-Version auf dem System und zeigt sie als 1.4.2\_05 an.

Sie können jetzt Applets ausführen, die diese Version der JRE verwenden.

Wenn Sie die JRE-Version 5.0 verwenden möchten, führen Sie folgende Schritte aus:

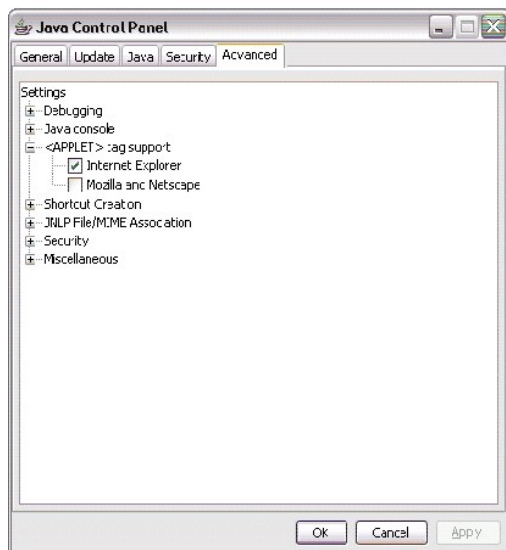
1. Im **Java Bedienungsfeld** (für JRE 5.0) unter dem Register **Erweitert** erweitern Sie die Komponente **<Applet>-Tag-Unterstützung** in der Struktur **Einstellungen**. Siehe [Abbildung 6-2](#).

 **ANMERKUNG:** Das Java-Bedienungsfeld steht unter **Einstellungen** → **Systemsteuerung** → **Java** zur Verfügung.

 **ANMERKUNG:** Auf unterstützten Linux-Systemen führen Sie die ausführbare Datei `ControlPanel` im **bin-Ordner** der JRE-Installation auf dem Linux-System aus.

2. Heben Sie die Markierung von **Internet Explorer** auf, und klicken Sie auf **Anwenden**.
3. Wählen Sie jetzt **Internet Explorer** aus dem **Java Bedienungsfeld** aus, und klicken Sie auf **Übernehmen** (siehe [Abbildung 6-2](#)). Hierdurch wird JRE 1.5.0 mit Internet Explorer integriert.

**Abbildung 6-2. Java Bedienungsfeld für JRE 5.0**



4. Starten Sie Internet Explorer.
5. Führen Sie einen der folgenden Punkte aus, um die Java Plug-in-Versionsnummer zu überprüfen:
  1. Wählen Sie **Sun Java Konsole** vom Menü **Extras** aus. Die Java Plug-in-Versionsnummer wird 1.5.0. sein.
  1. Wechseln Sie zu [www.java.com/en/download/faq/top\\_issues.jsp](http://www.java.com/en/download/faq/top_issues.jsp), und machen Sie das Thema **Test your Java Virtual Machine (JVM) (Virtuelle Java-Maschine (JVM) testen)** ausfindig. Dieser Test überprüft die Java Plug-in-Version auf dem System und zeigt sie als 1.5.0. an.


---

## Sicherstellen, dass Agenten und Instrumentation installiert sind und ausgeführt werden

Für verwaltete Systeme notwendige Dell-Agenten sind im *Dell OpenManage Server Administrator* enthalten; für Client-Systeme (Workstations, Desktops und portable Komponenten) notwendige Dell-Agenten sind in *Dell OpenManage Client Instrumentation* enthalten.


Diese Agenten sammeln Statusinformationen vom BIOS oder anderer Firmware auf den Systemen, auf denen sie installiert sind, und geben diese Informationen dann an den IT Assistant weiter. Durch IT Assistant überwachte Systeme werden allgemein als *verwaltete Systeme* bezeichnet - die Systeme, von denen sie verwaltet werden, werden als *Netzwerkverwaltungsstationen* oder *IT Assistant-Systeme* bezeichnet.

Wenn einer dieser beiden Agenten nicht installiert ist, sollten Sie sich die Dokumentation zu *Dell OpenManage Server Administrator* und *Dell OpenManage Client Instrumentation* ansehen, bevor Sie mit der IT Assistant-Konfiguration fortfahren. Wenn der entsprechende Agent installiert ist und ordnungsgemäß ausgeführt wird, starten Sie IT Assistant und lesen Sie weiter.

 **ANMERKUNG:** Beginnend mit IT Assistant Version 8.0 können Sie mit der IPMI-Ermittlungs-Unterstützungsfunktion Geräte ermitteln. Weitere Informationen finden Sie unter "[IPMI für System-Verwaltungsfunktionen konfigurieren](#)".


---


## IT Assistant starten

 **ANMERKUNG:** IT Assistant unterstützt funktionsbasierte Access Control (RBAC), um die spezifischen Vorgänge zu definieren, die jeder Benutzer durchführen kann. Um RBAC-Benutzer einzurichten, lesen Sie "[Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten](#)".


So melden Sie sich beim IT Assistant an:


1. Doppelklicken Sie auf dem Desktop des Systems auf das Symbol **IT Assistant**.
2. Das Dialogfeld **Anmelden** wird eingeblendet. (Wenn die Option Einfache Anmeldung so konfiguriert ist, wie in "[Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten](#)" beschrieben, wird das Dialogfeld **Anmelden** nicht eingeblendet.)
3. Geben Sie einen Benutzernamen und ein Kennwort ein.
4. Wählen Sie **Active Directory-Anmeldung**, wenn Sie Benutzerinformationen mit dem Microsoft® Active Directory®-Plugin konfiguriert haben. Die Berechtigungen, die Sie im IT Assistant haben, hängen von den definierten Benutzereinstellungen ab.

 **ANMERKUNG:** Weitere Informationen zur Errichtung eines funktionsbasierten Zugriffs erhalten Sie unter "[Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten](#)". Informationen zur Installation des Active Directory-Plugin und zur Erweiterung des Active Directory-Schemas für IT Assistant erhalten Sie unter *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

 **ANMERKUNG:** Um auf IT Assistant im Remote-Zugriff zuzugreifen, müssen Sie `https://<Host-Name>:<Schnittstellenummer>` eingeben. Die Standardschnittstellenummer ist 2607.

5. Geben Sie das Kennwort ein.

 **ANMERKUNG:** Bei Inbetriebnahme des IT Assistant wird ein Authentifizierungszertifikat-Popupfeld eingeblendet. Sie müssen innerhalb von 5 Minuten auf **OK** klicken, um diese Zertifikate anzunehmen. Andernfalls wird IT Assistant nicht richtig geladen und bestimmte kritische Funktionen werden nicht funktionieren.

 **ANMERKUNG:** Sie sehen eventuell mehrere Popups während der Inbetriebnahme des IT Assistant. Popups, die Sie auffordern, ein Autorisierungszertifikat anzunehmen, können vermieden werden, indem Sie **Zertifikat anzeigen** → **Zertifikat installieren** auswählen (falls verfügbar) oder indem Sie **Immer** als Antwort wählen, wenn Sie aufgefordert werden, das Zertifikat anzunehmen.

---

## SNMP für eine verbesserte Systemverwaltung konfigurieren

Lassen Sie uns zunächst die zwei Anwendungsbeispiele ansehen, die in diesem Abschnitt (Konfiguration von SNMP für eine verbesserte Systemverwaltung) zur Illustration von IT Assistant verwendet werden:

Zwei Systemadministratoren - nennen wir sie Sabine und Christian - sind für die Verwaltung zweier separater Netzwerkumgebungen verantwortlich. Sabine repräsentiert eine kleine bis mittelgroße Firma (50 Server, plus mehr als 200 Client-Systeme), während Christian ein viel größeres Unternehmen (1,000 Server) repräsentiert. Obwohl sowohl Sabine als auch Christian IT Assistant zur Ermittlung und Verwaltung ihrer Systeme verwenden, ist die Art, wie sie IT Assistant konfigurieren und verwenden sehr unterschiedlich. Bevor jedoch die Unterschiede weiter hervorgehoben werden, wollen wir uns einige grundlegende Schritte ansehen, die beide ausführen müssen.

Sowohl Sabine als auch Christian müssen das SNMP (einfaches Netzwerkverwaltungsprotokoll) -Systems Management-Protokoll) konfigurieren: zur Ermittlung ihrer Systeme sowie zum Empfangen von Traps (asynchron, Warnungsbenachrichtigungen), die den Status der jeweiligen Komponenten berichten. Der Agent des Server Administrators erzeugt auf verwalteten Systemen SNMP-Traps bei Statusänderungen der Sensoren und anderer auf einem verwalteten System überwachter Parameter. Um diese Traps richtig zu senden, muss der SNMP-Dienst des Betriebssystems mit einem oder mehreren Trap-Zielen konfiguriert sein, die dem System entsprechen, auf dem IT Assistant installiert ist.

### Details zur Konfiguration des SNMP-Dienstes

Detaillierte Informationen zur SNMP-Konfiguration für das IT Assistant-System und für alle unterstützten Betriebssysteme der verwalteten Systeme finden Sie unter "[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)".

### SNMP auf zu verwaltenden Systemen konfigurieren

Zusätzlich zum auf dem IT Assistant-System installierten und ausgeführten SNMP-Dienst muss der SNMP-Dienst oder Daemon auf jedem Betriebssystem des verwalteten Systems konfiguriert werden.

### Empfohlene Verfahren für SNMP


Die folgenden Anforderungen sollten bei der Konfiguration von SNMP eingehalten werden:


- 1 Verwendung eines Host-Namens oder einer statischen IP-Adresse für das IT Assistant-System.
- 1 Konfiguration der statischen IP-Adresse bzw. des Host-Namens als SNMP-Trap-Ziel auf allen verwalteten Systemen. Wenn ein Host-Name als SNMP-Trap-Ziel verwendet wird (der IT Assistant-Systemname), muss Namensauflösung im Netzwerk richtig konfiguriert sein.
- 1 Stellen Sie sicher, dass sich die **Get** und **Set** Community-Namen für SNMP unterscheiden.
- 1 Bei der Zuweisung von Community-Namen für verwaltete Systeme muss die Gesamtanzahl verschiedener Community-Namen niedrig sein. Je weniger Community-Namen vorhanden sind, desto leichter ist die Verwaltung des Netzwerks.

### Für die optimale SNMP Konfiguration benötigte Informationen zum verwalteten System

Für jedes mit dem SNMP-Protokoll zu ermittelnde und zu verwaltende System (auf dem das Windows-Betriebssystem ausgeführt wird), ist sicherzustellen, dass SNMP installiert und korrekt konfiguriert ist.

Die beiden einzurichtenden Community-Namen sind der **Get** (bzw. Lesen) -Community-Name und der **Set** (bzw. Schreiben) -Community-Name. Mithilfe des Community-Namens Lesen, auch als *Nur-Lesen* bezeichnet, kann der IT Assistant Informationen vom verwalteten System lesen, während der IT Assistant mittels des Community-Namens Schreiben, auch als *Lesen-Schreiben* bezeichnet, Informationen vom bzw. auf das verwaltete System lesen bzw. schreiben kann.

 **ANMERKUNG:** Bei Community-Namen muss Groß-/Kleinschreibung beachtet werden.

 **ANMERKUNG:** Obwohl für einen Community-Namen gleichzeitig Lese- und Lese-/Schreibrechte vergeben werden können, sollte für jedes Recht jeweils ein eigener Name vergeben werden, da so ein eingeschränkter Schreibzugriff möglich ist.

Die Community-Namen, die Sie dem SNMP für verwaltete Systeme im Betriebssystem zuweisen, müssen auch in IT Assistant eingetragen werden, wenn Sie SNMP-Ermittlungsbereiche einrichten.

Im Dialogfeld **Ermittlungsbereich** unterhalb des Abschnitts **Protokolle** müssen die **Get** (bzw. Lesen) und **Set** (bzw. Schreiben) -Community-Namen aller verwalteten Systeme eingegeben werden. Bei mehr als einem Community-Namen pro Feld trennen Sie die Community-Namen durch Kommas.

Weitere Informationen finden Sie unter "[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)".

---

## CIM für verbesserte Verwaltung konfigurieren


Abhängig von der Netzwerkumgebung stellt die Konfiguration von CIM eine erforderliche Aufgabe dar. CIM ist das bevorzugte Systemverwaltungsprotokoll für neuere Client-Instrumentation und ist für Dell Systeme erforderlich, die mit OMCI Version 7.x instrumentiert sind. CIM wird auch zur Ausführung von Remote-Windows-Software-Aktualisierungen verwendet.


In ihrem kleinen bis mittelgroßen Netzwerk muss Sabine CIM installieren, aktivieren und konfigurieren, um Client-Systeme zu verwalten, auf denen die neueste Client-Instrumentation (OMCI 7.x) ausgeführt wird. Obwohl Christians Gruppe von verwalteten Systemen nur aus Servern besteht, wird er auch CIM installieren und aktivieren. Im Allgemeinen sollte CIM aktiviert sein, wenn das Unternehmen ein verwaltetes System besitzt, das ein Microsoft Windows®-Betriebssystem ausführt.

## CIM im Betriebssystem konfigurieren

IT Assistant verwendet zur Herstellung von CIM-Verbindungen den WMI (Windows Management Interface) -Kern. Der WMI-Kern verwendet Microsoft Netzwerksicherheit, um CIM-Instrumentierung vor unberechtigtem Zugriff zu schützen.

Weitere Informationen zur Betriebssystem-CIM-Konfiguration finden Sie unter "[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)".

 **ANMERKUNG:** IT Assistant erfordert den CIM-Benutzernamen und das Kennwort mit Administratorrechten, der/das auf den verwalteten Systemen eingerichtet wurde. Stellen Sie bei der Verwendung eines Domänenbenutzers sicher, dass im Feld Benutzername die richtige Domäne angegeben wird. Ein Benutzername muss immer mit einer Domäne gekennzeichnet sein, oder mit lokaler Host, wenn keine Domäne vorhanden ist. Das Format ist entweder `<Domäne>\<Benutzer>` oder `<LokalerHost>\<Benutzer>`.

 **ANMERKUNG:** Zur CIM-Ermittlung sind korrekte Benutzer-ID und Kennwort erforderlich. Bei falscher Angabe dieser Informationen auf einem zur CIM-Ermittlung konfigurierten Subnetz könnte das Konto ausgeschlossen werden.

---

## Die besten Methoden zur Einstellung von Ermittlungszielen

Die folgende Tabelle zeigt unabhängig von der Größe des Netzwerks Dells Empfehlungen, wie Ermittlungsziele am besten einzustellen sind. IT Assistant-Benutzer definieren Ermittlungszielsysteme und -bereiche in einem Netzwerk, um die Systeme zu identifizieren, die sie suchen und in ihrer Datenbank eintragen wollen. Bei der Einrichtung eines Ermittlungsziels und -bereichs im IT Assistant besteht die Möglichkeit, einen Host-Namen, eine IP-Adresse oder einen Subnetzbereich zur Identifizierung der Systeme auszuwählen, die vom IT Assistant ermittelt werden sollen. In diesem Abschnitt wird veranschaulicht, welcher Ermittlungstyp sich für Ihre Netzwerkumgebung am besten eignet.


Tabelle 6-1. Empfehlungen zu den besten Methoden zur Einrichtung von Ermittlung

Bevorzugter Ermittlungsbereichstyp	DHCP	Primär statische IP-Adressen
Host-Name	Empfohlen	Empfohlen, falls DNS vorhanden ist und IP-Adressen über viele verschiedene Netzwerksegmente verteilt sind
IP-Adresse	Nicht empfohlen	Empfohlen, falls IP-Adressen über viele verschiedene Netzwerksegmente verteilt sind
IP-Bereich	Empfohlen, falls auf einem oder wenigen Netzwerksegmenten vorhanden	Empfohlen, falls auf einem oder wenigen Netzwerksegmenten vorhanden

## IPMI für Verwaltungsfunktionen des Systems konfigurieren

Damit Sie in der Lage sind, die Ermittlungsfunktion des Intelligenten Schnittstellenverwaltungsprotokolls (IPMI) zu verwenden, sind folgende Voraussetzungen zu erfüllen:

- 1 Dell PowerEdge™ x8xx-System und höher. Diese Funktion funktioniert für andere Systeme nicht.
- 1 Alle Systeme sind mit einem Baseboard-Verwaltungs-Contoller (BMC) ausgestattet.
- 1 BMC mit IPMI-Version 1.5 und höher.
- 1 BMC aller verwalteten Systeme ist konfiguriert.

 **ANMERKUNG:** Weitere Informationen zur Konfiguration des BMC finden Sie im Abschnitt "Veraltetes System konfigurieren" in *Dell OpenManage Baseboard Management Controller-Dienstprogramme: Benutzerhandbuch* auf Dells Support-Website unter [support.dell.com](http://support.dell.com) oder auf der Dokumentations-CD.

## Microsoft-IPMI-Anbieter verwenden

Microsoft Windows Server® 2003 R2 ist mit einem IPMI-Treiber und einem IPMI-CIM-Anbieter (Allgemeines Informationsmodell) ausgestattet. Der CIM-Anbieter zeigt Systeminformationen auf, die von BMC über die IPMI-Schnittstelle aufgezeigt werden. IT Assistant verwendet diese Funktion zum Extrahieren von Informationen. Mit IT Assistant können Sie BMC durch IPMI ermitteln und klassifizieren.

Stellen Sie jedoch sicher, dass folgende Voraussetzungen erfüllt werden, damit Sie Microsoft-IPMI-Anbieter zur Sendung von Informationen über Ihre Systeme verwenden können:

- 1 Windows Server 2003 R2-Betriebssystem auf den verwalteten Systemen
- 1 Alle verwalteten Systeme haben BMC mit IPMI-Version 1.5 oder höher
- 1 CIM ist auf den verwalteten Systemen konfiguriert


Weitere Informationen finden Sie in [Schritt 6](#) unter "[Ermittlungskonfigurationseinstellungen konfigurieren](#)".

- 1 IPMI-Treiber sind geladen
- 1 MSI zur Hardwareverwaltung

Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.


## Optimale Verfahren zum Verwenden der IPMI-Ermittlungsfunktion

IPMI-Ermittlung bietet Ihnen Informationen über ein System, selbst wenn das System heruntergefahren ist. IPMI verwendet das Protokoll der Remote-Verwaltungssteuerungspakete (RMCP), um mit dem BMC der verwalteten Systeme zu kommunizieren.

 **ANMERKUNG:** RMCP ist ein UDP-basiertes Protokoll, das über die Schnittstelle 623 kommuniziert. Die IPMI-Meldungen sind in den RMCP-Paketen verkapselt. Das RMCP-Protokoll aktiviert die Remote-Serversteuerung in allen Zuständen, in denen das System eingeschaltet ist.


- 1 Konfigurieren Sie den BMC auf verwalteten Systemen, die mit der IPMI-Ermittlungs-Unterstützungsfunktion ermittelt werden.
- 1 Schließen Sie die BMC-Netzwerkschnittstellenkarte (NIC) an das Netzwerk an.

Wenn sich auf Ihren Systemen ein Dell Remote Access Controller (DRAC) 5 befindet, sollte der RAC ans Netzwerk angeschlossen werden.

 **ANMERKUNG:** Bei x8xx-Systemen sollten Sie DRAC 4 und BMC aktivieren, wenn Sie die Funktionalität von beiden nutzen möchten. Bei x9xx-Systemen übernimmt jedoch DRAC 5 die volle Funktionalität des BMC. Deshalb müssen Sie nur DRAC 5 aktivieren.

- 1 In den Ermittlungsbereichen geben Sie die SNMP/CIM-IP-Adresse und -Anmeldeinformationen (Benutzername und Kennwort) für das Gerät sowie die BMC-IP-Adresse und -Anmeldeinformationen an.

Aufgrund des RMCP-Protokolls ist die Konnektivität unter Verwendung von IPMI gegebenermaßen langsam. Es wird daher empfohlen, dass Sie einen separaten Ermittlungsbereich für Geräte erstellen, auf denen kein Dell-Agent installiert ist. Für diesen Ermittlungsbereich allein können Sie die IPMI-Ermittlungsfunktion aktivieren.


 **ANMERKUNG:** Systeme, die nur durch das IPMI-Protokoll ermittelt werden, lassen sich auf der IT Assistant-Benutzeroberfläche durch die BMC-IP-Adresse identifizieren. Deshalb können Tasks wie Softwarebereitstellung und Leistungsüberwachung auf solchen Systemen nicht ausgeführt werden.

---

## IT Assistant zur Ermittlung neuer Speichergeräte konfigurieren

Beginnend mit IT Assistant Version 8.0 können Sie Dell|EMC-Speichergeräte ermitteln und überwachen.

Sie können den Status der ermittelten Dell|EMC-Speicher-Arrays in der Kategorie **Dell|EMC-Arrays** unter der Gruppe **Speichergeräte** anzeigen. Der Status der Dell|EMC-Speicher-Arrays wird rot für fehlerhaft/kritisch und grün für normal sein. Die Dell|EMC-Speicher-Arrays erkennen alle SNMP-Traps des Geräts einschließlich Protokollierungs-, Filter- und Maßnahmeninformationen.

 **ANMERKUNG:** Verwenden Sie das Ereignisverwaltungssystem von IT Assistant um Maßnahmen (wie z. B. das Senden einer E-Mail an einen Administrator oder das Erstellen einer Problembenachrichtigung in einem Helpdesk-System durch einen Anwendungsstart) kritischen Ereignisquellen zuzuordnen, die mit den Arrays assoziiert werden. Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.

## Voraussetzungen


Sie sollten die folgende Softwarekonfiguration haben, um die Speicherintegrationsfunktion zu aktivieren:

- 1 EMC® Navisphere® Secure CLI auf demselben System, das IT Assistant ausführt
- 1 SNMP aktiviert auf Ihrem Dell|EMC-Array
- 1 FLARE®-Betriebsumgebung Version 19 oder höher auf Ihrem Dell|EMC-Array

## Navisphere Secure CLI

IT Assistant verwendet Navisphere Secure CLI, um Bestandsaufnahme-Informationen von den Speichergeräten zu erhalten. Das IT Assistant-Installationsprogramm erkennt, wenn Navisphere Secure CLI auf der Verwaltungsstation nicht installiert ist und gibt Ihnen die Möglichkeit, sie zu installieren.

 **ANMERKUNG:** EMC gibt periodisch neue Versionen von Navisphere Secure CLI heraus, und es ist eventuell erforderlich, die CLI-Version auf der IT Assistant-Verwaltungsstation zu aktualisieren.

 **ANMERKUNG:** Die Navisphere Secure CLI-Version wird mit jeder neuen Version von IT Assistant aktualisiert.

Wenn Sie Speicher-Arrays in Ihrer Speicherumgebung haben, können Sie zum Elemente-Manager wechseln, um das Dell|EMC-Gerät zu verwalten.


Unter *Dell OpenManage IT Assistant-Onlinehilfe* finden Sie Informationen dazu, wie Sie eine Verbindung zum Remote-Array herstellen können, um Probleme mit dem Navisphere Agent zu beheben.


Details zur Überwachung von SNMP-Warnungen finden Sie in der Onlinehilfe zu EMC Navisphere.

## Setup und Konfiguration




- 1 IT Assistant unterstützt die Ermittlung auf Dell|EMC-Speicher-Arrays (z. B. AX100- oder AX150-Arrays), die auf Navisphere Manager erweitert wurden.

 **ANMERKUNG:** IT Assistant verwaltet Arrays nicht, auf denen Navisphere Express ausgeführt wird.


 **ANMERKUNG:** Wenn Sie ein AX100i-Speicher-Array ermitteln, können Sie aktuelle Informationen dazu in der IT Assistant-Infodatei nachlesen.


- 1 IT Assistant verwendet SNMP zum Ermitteln der Dell|EMC-Arrays. Verwenden Sie Navisphere Manager, um SNMP auf Ihrem Dell|EMC-Array zu aktivieren. Erst dann kann es in IT Assistant ermittelt werden. Setzen Sie SNMP in Navisphere unter die Netzwerkeinstellungen der Speicherprozessoreigenschaften.

 **ANMERKUNG:** Die Speicherprozessoren auf den Produkten Dell|EMC CX3-20, CX3-40 und CX3-80 haben jeweils eine Verwaltungsschnittstelle und eine Service-LAN-Schnittstelle (lokales Netzwerk). Verbinden Sie zum allgemeinen Gebrauch die Serviceschnittstellen nicht mit dem Netzwerk. Ein Verbinden dieser Schnittstellen mit dem Netzwerk kann innerhalb von IT Assistant zu unvorhersehbaren Status- und Ereignisreporten führen.

- 1 Stellen Sie sicher, dass die folgenden Schnittstellen auf der Firewall offen sind:

- o TCP 80/443 (Web und SSL)
- o TCP 6389 (Navisphere-CLI)
- o UDP 161/162 (SNMP und bidirektional)


 **ANMERKUNG:** Es handelt sich hierbei um Standardschnittstellen. Sollten Sie die Schnittstellenkonfiguration geändert haben, ist sicherzustellen, dass die richtigen Schnittstellen geöffnet sind.

 **ANMERKUNG:** Weitere Informationen zu Schnittstellen, die von IT Assistant verwendet werden, finden Sie im *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

- 1 IT Assistant ermittelt die Informationen für den im Ermittlungsbereich gespeicherten Speicherprozessorwert und zeigt diese an. Da die Speicherprozessoren redundant sind, müssen Sie für Ermittlungs- und Bestandsaufnahmewecke nur die IP-Adresse eines der Speicherprozessoren eingeben.

## Fehlerbehebungshilfsprogramm verwenden

Der EMV-Konnektivitätstest kann verwendet werden, um die Kommunikation zwischen der IT Assistant-Verwaltungsstation und dem Navisphere Agent auf dem Speichergerät zu testen. Der Test erfordert die IP-Adresse des Speicherprozessors sowie die Navisphere-Anmeldeinformationen.

 **ANMERKUNG:** Die Navisphere-Anmeldeinformationen sollten über eine globale Reichweite verfügen.

## Reporte erstellen

Sie können für die Dell|EMC-Arrays benutzerdefinierte Reporte erstellen. Der Report-Assistent von IT Assistant ermöglicht Ihnen, Felder aus einer Vielfalt von Tabellen auszuwählen, einschließlich Geräte, NIC, physische Festplatte, virtuelle Festplatte, Gehäuse und Controller.

Die Reporte können im Format HTML und XML sowie im kommagetrennten Werteformat (CSV) erstellt werden.

 **ANMERKUNG:** IT Assistant hat Controller- und Gehäuse-Reporte für die Dell|EMC-Arrays vordefiniert.

---

## Ermittlung in Sabines Geschäft (kleine bis mittlere Größe)

Sabine möchte alle Systeme in ihrem Netzwerk ermitteln. Bei der Ermittlung handelt es sich um ein Verfahren, bei dem IT Assistant jedes System identifiziert und diese Informationen für das System in der IT Assistant-Datenbank einträgt.

Wie zuvor erwähnt, ist Sabine der alleinige Systemadministrator eines gemischten Netzwerks von Systemen, einschließlich:

- 1 50 Dell PowerEdge-Systemen
- 1 200 Dell OptiPlex™-Desktops
- 1 10 Dell PowerConnect-Schaltern

Sabine verwendet den IT Assistant um den globalen Status der Systeme zu überwachen sowie um eine Benachrichtigung zu erhalten, sobald ein PowerEdge-System oder ein PowerConnect-Schalter im Netzwerk den Status Warnung oder Kritisch besitzt. Sabine setzt den IT Assistant nicht zur Benachrichtigung ein, wenn eines ihrer Desktop-Systeme eine Warnung erzeugt.

## Anforderungen für ein gemischtes Server-Client-System bestimmen

Vor dem Einsatz von IT Assistant zur Konfiguration der Ermittlung, muss Sabine einige grundlegende Entscheidungen über ihr Netzwerk treffen. Insbesondere muss sie folgendes entscheiden:

- 1 Systemverwaltungsprotokolle, die zur Verwaltung der Systeme und Geräte in ihrem Netzwerk erforderlich sind
- 1 Community-Namen und Trap-Ziele für Systeme, die durch SNMP verwaltet werden sollen
- 1 SNMP-Anforderungen für PowerConnect-Schalter
- 1 CIM-Anmeldeinformationen zur Authentifizierung
- 1 Host-Namen, IP-Adressen oder IP-Subnetzbereiche der Systeme, die sie überwachen möchte

## Für Sabines Netzwerk benötigte Systemverwaltungsprotokolle

Bei der Planung zur Konfiguration der Ermittlung muss Sabine eine Mischung verschiedener Systemtypen (Server, Clients und Schalter) berücksichtigen. Sabine benötigt zur Verwaltung dieser Netzwerksysteme und Geräte die folgenden Systemverwaltungsprotokolle:

- 1 SNMP für ihre PowerEdge-Systeme und PowerConnect-Schalter
- 1 CIM für die Systeme, die Windows ausführen, vorausgesetzt, dass auf Sabines Client-Systemen eine neuere, CIM-kompatible Client-Instrumentation installiert ist

Einen Überblick von Protokollanforderungen finden Sie unter "[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)".

## Community-Namen und Trap-Ziele

Die Größe des Betriebs beeinflusst nicht Sabines Anforderungen an die Konfiguration der **Get** und **Set** Community-Namen sowie an die Trap-Ziele für SNMP auf den verwalteten Systemen. Anforderungen an die SNMP-Konfiguration im Zusammenhang mit Servern finden Sie unter "[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)" beschrieben.

## SNMP für PowerConnect-Schalter konfigurieren

Mithilfe des IT Assistant kann Sabine ihre zehn PowerConnect-Schalter überwachen. Zu jedem Modell der PowerConnect-Schalter ist Dokumentation verfügbar, in der die folgenden Informationen zur Einrichtung des SNMP-Dienstes für diesen Schalter enthalten sind:

- 1 Community-Namen
- 1 Trap-Ziele
- 1 Die Hosts, von denen der Schalter SNMP-Pakete annimmt

## Anfängliche Tasks für das Finden von Systemen auf Sabines Netzwerk

Nachdem Sabine die Voraussetzungen für ihre Ermittlungskonfiguration zusammengetragen hat, kann sie eine erstmalige Ermittlungskonfiguration durchführen. Dazu muss Sabine die folgenden Aufgaben durchführen:

- 1 Kommunikationsprotokolle auf den verwalteten Systemen konfigurieren.
- 1 Einstellungen für die Ermittlung konfigurieren.
- 1 Alle Ermittlungsbereiche eingeben.

## IT Assistant verwenden, um Sabines Netzwerksysteme zu finden und zu verwalten

Wenn IT Assistant jetzt zum ersten Mal seit der Installation gestartet wird, sieht Sabine einen Willkommens-Bildschirm, der anzeigt, dass IT Assistant noch nicht konfiguriert worden ist. Die vier grundlegenden Schritte der Konfiguration sind hier aufgeführt:

Schritt 1 - Ermittlungskonfiguration - kontrolliert, wie oft IT Assistant das Netzwerk nach hinzugefügten neuen Systemen abfragt

Schritt 2 - Bestandsaufnahme Konfiguration - kontrolliert, wie oft IT Assistant eine detaillierte Bestandsaufnahme aller ermittelten Systeme abrufen

Schritt 3 - Statusabfrage - kontrolliert, wie oft IT Assistant den Funktionszustand und den Netzwerkverbindungsstatus ermittelter Systeme abrufen

Schritt 4 - Bereiche - identifiziert spezifische Bereiche für IT Assistant, um die Ermittlungs-, Bestandsaufnahme- oder Abfrage-Tasks entweder einzuschränken oder zu erweitern

Sobald Sabine einen dieser Schritte anklickt, wechselt sie zum entsprechenden Dialogfeld unter der Menüleiste **Ermittlung und Überwachung** in IT Assistant. Die Schritte 1 bis 3 sind Dialogfelder mit einem einzigen Fenster; Schritt 4 ist ein Assistent-basiertes Verfahren zum Definieren von Ermittlungsbereichen.

## Ermittlungseinstellungen konfigurieren

Sabine beginnt damit, die Ermittlungseinstellungen für ihre Systeme mit dem Dialogfeld **Ermittlungskonfigurationseinstellungen** zu konfigurieren. Dieser Dialog wird automatisch angezeigt, wenn sie auf *Schritt 1: Ermittlungskonfiguration* im IT Assistant klickt oder wenn sie **Ermittlungskonfiguration** aus der Menüleiste auswählt. Hier gibt Sabine Informationen ein, die IT Assistant für die Ermittlung verwenden wird. Diese Werte bleiben unverändert und werden auf die entsprechenden Ermittlungsbereiche angewendet, die sie später im Verfahren erstellt. Sie kann diese Werte jedoch jederzeit ändern.


Um Ermittlungseinstellungen in IT Assistant zu konfigurieren, führt Sabine folgende Schritte aus:

1. Sabine wählt von der IT Assistant-Menüleiste **Ermittlung und Überwachung** → **Ermittlungskonfiguration** aus.

Das Dialogfeld **Ermittlungskonfigurationseinstellungen** wird eingeblendet. **Geräteermittlung aktivieren** ist standardmäßig ausgewählt.

2. Im Dialogfeld unter **Geräteermittlung einleiten** wählt Sabine die Zeitspanne aus, während der IT Assistant die Ermittlung ausführen soll.

Sabine wählt 6:00:00 Uhr an allen sieben Tagen der Woche aus, da die Daten eventuell dynamisch sind. Sie möchte jedoch einen Zeitraum auswählen, der sich außerhalb der Spitzenzeiten befindet.

 **ANMERKUNG:** Dell empfiehlt, die Ermittlung zu Zeiten geringer Netzwerkbelastung durchzuführen.

3. Sabine bestimmt über den Schieberegler unter **Ermittlungsgeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die sie für die Ermittlung zuweisen möchte.

 **ANMERKUNG:** Je höher Sie die Ermittlungsgeschwindigkeit einstellen, desto mehr Netzwerk-Ressourcen wird die Ermittlung verbrauchen. Schnellere Ermittlungsgeschwindigkeiten können die Netzwerkleistung beeinflussen.

4. Sabine kann unter **Ermittlung** auswählen, ob **Alle Geräte** oder **Nur instrumentierte Geräte** ermittelt werden sollen.

Sie wählt **Nur instrumentierte Geräte**, da sie möchte, dass IT Assistant nur Geräte mit SNMP- oder CIM-Instrumentierung ermittelt. Wenn sie jedes Gerät ermitteln wollte, das auf einen Ping-Befehl reagiert, hätte sie **Alle Geräte** gewählt. Eine Liste mit unterstützten Agenten erhalten Sie unter "[Von IT Assistant unterstützte Agenten](#)".

 **ANMERKUNG:** Dell empfiehlt die Wahl der Standard-DNS-Namensauflösung, falls Domänenname-System (DNS) im Netzwerk konfiguriert ist.

5. Unter **Namensauflösung** wählt Sabine **DNS-Namensauflösung** oder **Instrumentationsnamensauflösung** aus.

DNS-Namensauflösung stimmt die IP-Adresse eines Systems mit dem Host-Namen ab. Instrumentationsnamensauflösung fragt den Namen der Agenten-Instrumentation des verwalteten Systems ab. Weitere Informationen zur Konfiguration der Instrumentationsnamensauflösung finden Sie in der Dokumentation des Gerätes oder des Systems.

 **ANMERKUNG:** Dell empfiehlt die Wahl der Standard-DNS-Namensauflösung, falls DNS im Netzwerk konfiguriert ist.

6. Sabine klickt auf **OK**.

## Bestandsaufnahmeinstellungen konfigurieren

Als nächstes muss Sabine sie Bestandsaufnahmeinstellungen eingeben. IT Assistant sammelt Bestandsaufnahmeinformationen zu Software- und Firmware-Versionen, sowie Geräteinformationen über Speicher, Prozessoren, Netzteile, PCI-Karten und integrierte Geräte sowie Speicherplatz. Diese Informationen werden in der IT Assistant-Datenbank gespeichert und können zur Erstellung von benutzerspezifischen Reports verwendet werden.

Um Bestandsaufnahme-Einstellungen einzustellen, führt Sabine folgende Schritte aus:


1. Sabine wählt aus der Menüleiste **Ermittlung und Überwachung** → **Bestandsaufnahmekonfiguration** aus.

Das Dialogfeld **Einstellungen der Bestandsaufnahmeabfrage** wird angezeigt. **Bestandsaufnahme aktivieren** ist standardmäßig ausgewählt.


2. Unter **Bestandsaufnahme einleiten** wählt Sabine aus, wann IT Assistant die Bestandsaufnahme ausführen soll.

Sabine wählt 6:00:00 Uhr für alle sieben Tage der Woche aus, da sich dieser Zeitraum außerhalb der Spitzenzeiten des Netzwerk-Datenverkehrs befindet.

3. Sabine bestimmt über den Schieberegler unter **Bestandsaufnahmegewindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die sie für die Bestandsaufnahme zuweisen möchte.

 **ANMERKUNG:** Je höher Sie die Bestandsaufnahmegewindigkeit einstellen, desto mehr Netzwerk-Ressourcen wird die Ermittlung verbrauchen. Höhere Bestandsaufnahmegewindigkeiten können die Netzwerkleistung beeinflussen.

4. Sabine klickt auf **OK**.

 **ANMERKUNG:** IT Assistant Version 8.0 kann jetzt die Bestandsaufnahme-Informationen für Drucker, Bänder und Speichergeräte anzeigen. Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.

## Statusabfrage-Einstellungen konfigurieren


Als nächstes definiert Sabine die Statusabfrageeinstellungen für ihre Systeme. IT Assistant führt eine Überprüfung des Strom- und Konnektivitätsfunktionszustands für ermittelte Geräte aus, und legt fest, ob ein Gerät normal funktioniert, sich in einem nichtnormalen Zustand befindet oder heruntergefahren ist. Die Statusmeldungen im IT Assistant umfassen *Funktionsfähig*, *Warnung*, *Kritisch* und *Heruntergefahren*. Statussymbole zeigen auch an, ob ein System nicht instrumentiert ist, ob es keine Informationen zum System gibt, oder sie zeigen den Zustand des Systems an, bevor es das letzte Mal heruntergefahren wurde.

Um Statusabfrage-Einstellungen einzustellen, führt Sabine folgende Schritte aus:

1. Sabine wählt aus der Menüleiste **Ermittlung und Überwachung** → **Statusabfragekonfiguration** aus.

Das Dialogfeld **Statusabfrage-Konfigurationseinstellungen** wird angezeigt. **Statusabfrage aktivieren** ist standardmäßig ausgewählt.

2. Unter **Statusabfrageintervall** wählt Sabine das Intervall aus, das IT Assistant zur Ausführung der Statusabfrage verwenden soll.
3. Sabine bestimmt über den Schieberegler unter **Statusabfragegeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die sie für die Statusabfrage zuweisen möchte.

 **ANMERKUNG:** Je höher Sie die Statusabfragegeschwindigkeit einstellen, desto mehr Netzwerk-Ressourcen wird die Ermittlung verbrauchen. Höhere Geschwindigkeiten können die Netzwerkleistung beeinflussen.

4. Sabine klickt auf **OK**.

## Ermittlungsbereiche konfigurieren

IT Assistant führt ein Register von Netzwerksegmenten, das zur Ermittlung von Geräten verwendet wird. Ein Ermittlungsbereich kann ein Subnetz, eine Reihe von IP-Adressen auf einem Subnetz, eine individuelle IP-Adresse oder ein individueller Host-Name sein.

Um ihre Systeme für IT Assistant festzulegen, muss Sabine einen Ermittlungsbereich definieren.


Um einen *Einschlussbereich* zu definieren, führt Sabine folgende Schritte aus:

1. Sabine wählt **Ermittlung und Überwachung** → **Bereiche** aus der Menüleiste aus.

Die Navigationsstruktur **Ermittlungsbereiche** wird auf der linken Seite des IT Assistant-Fenster angezeigt.

2. Sabine erweitert **Ermittlungsbereiche**, klickt mit der rechten Maustaste auf **Einschlussbereiche** und wählt **Neuer Einschlussbereich** aus.


Der **Assistent Neue Ermittlung** startet.


 **ANMERKUNG:** Um ein bestimmtes System oder einen bestimmten Host-Namen von der Ermittlung *auszuschließen* klicken Sie mit der rechten Maustaste auf **Ausschlussbereich** in der Navigationsstruktur **Ermittlungsbereich** und geben den Namen oder die IP-Adresse des Systems ein. In den meisten kleinen bis mittelgroßen Firmen wird, wie in Sabines Firma, diese Option nicht verwendet.

3. In Schritt 1 des Assistenten gibt Sabine eine IP-Adresse (oder einen IP-Bereich) oder einen Host-Namen ein.


Sie klickt auf **Hinzufügen**, um verschiedene Bereiche von IP-Adressen oder Host-Namen hinzuzufügen.

Sie klickt auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

 **ANMERKUNG:** Gültige Werte für den Einschlussbereich sind Subnetzbereich, Host-Name und IP-Adresse eines einzelnen Systems. Sabine hält sich an die IP-Subnetzbereiche, die sie für ihre Server, Desktop-Systeme und Schalter notiert hat. Z. B. hat Sabine auf ihrer Liste 192.166.153.\* und 192.166.154.\* eingetragen, wobei der erste Subnetzbereich für Sabines Server, der zweite Subnetzbereich für Sabines Desktops bestimmt ist und die Schalter auf beide Subnetze verteilt sind.

 **ANMERKUNG:** Das Dienstprogramm Import Node List bietet eine praktische Methode zur Festlegung einer Liste von Host-Namen, IP-Adressen und Subnetzbereichen, die IT Assistant ermitteln soll. Anleitungen zur Ausführung des Dienstprogramms von der Befehlszeile aus finden Sie in der *IT Assistant-Onlinehilfe*. Die Datei **importnodelist.exe** befindet sich im **bin**-Verzeichnis des IT Assistant-Basisverzeichnisses.

4. In Schritt 2 des Assistenten verwendet Sabine die Standardwerte für die Internetsteuerungs-Meldungsprotokoll (ICMP) -Zeitüberschreitung und versucht den Bereich erneut. Sie verwendet das Fehlerbehebungshilfsprogramm, um diese Werte zu bestimmen.

 **ANMERKUNG:** IT Assistant bietet ein Fehlerbehebungshilfsprogramm an, das für die Erfassung von Systeminformationen und Subnetzbereichen nützlich sein kann. Sie können auf das Hilfsprogramm zugreifen, indem Sie **Hilfsprogramme** → **Fehlerbehebungshilfsprogramm** aus der Menüleiste auswählen. Weitere Informationen erhalten Sie, wenn Sie das Dialogfeld Fehlerbehebungshilfsprogramm öffnen und auf **Hilfe** klicken.

5. In Schritt 3 des Assistenten konfiguriert Sabine die SNMP-Parameter, die während der Ermittlung verwendet werden sollen:


- 1 Sabine stellt sicher, dass die Option **SNMP-Ermittlung aktivieren** ausgewählt ist.
- 1 Sie gibt einen Wert für den **Get-Community-Namen** ein (Groß- und Kleinschreibung beachten).

Sabines Überlegungen:

Sabine verwaltet 50 Server, sie möchte also SNMP konfigurieren. Der **Get-Community**-Name ist ein Nur-Lesen-Kennwort, das SNMP-Agenten auf verwalteten Systemen zur Authentifizierung installieren. Folgendes zieht Sabine bei der Auswahl des **Get-Community**-Namens in Betracht:

Jedes SNMP-aktivierte verwaltete System besitzt einen **Get-Community**-Namen. Sabine stellt daher sicher, dass sie jeden Community-Namen auf allen zu verwaltenden Systemen auflistet. Wenn Sabines verwaltete Systeme mehr als einen Community-Namen aufweisen, gibt sie im Namensfeld **Get-Community** mehrere durch Kommas getrennte Community-Namen ein.


Obwohl der **Get-Community**-Name die Nur-Lese-Informationen beeinflusst, die IT Assistant von den verwalteten Systemen erhalten hat, wie z. B. Ermittlungsergebnisse, Statusabfragen und Warnungsprotokolle, möchte Sabine den Zugriff auf diese Daten einschränken. Sie ändert deshalb den Standard-**Get-Community**-Namen **öffentlich** zu einem Namen, der nur ihr und ihrer ernannten Vertretung bekannt ist.


 **ANMERKUNG:** Die in den Feldern SNMP-Get- und Set-Community-Name eingegebenen Community-Namen für das Betriebssystem des verwalteten Systems müssen mit den Get- und Set-Community-Namen übereinstimmen, die in IT Assistant zugewiesen wurden.

- 1 Sabine gibt einen Wert für den **Set-Community**-Namen ein (Groß- und Kleinschreibung beachten).


Sabines Überlegungen:

Der **Set-Community**-Name ist ein Lesen-Schreiben-Kennwort, das Zugriff auf ein verwaltetes System ermöglicht. SNMP-Agenten, die auf dem verwalteten System ausgeführt werden, verwenden dieses Kennwort zur Authentifizierung, wenn Maßnahmen auf dem System versucht werden. SNMP-Sätze werden nur bei Aus- und Einschaltungs-Tasks verwendet.

 **ANMERKUNG:** Obwohl die Dell Server-Instrumentation über eine Authentifizierungsebene oberhalb des SNMP-Set-Community-Namens (der einen Host-Namen und ein Kennwort erfordert) verfügt, besitzen viele SNMP-Agenten diese Ebene nicht. Agenten ohne diese zusätzliche Sicherheitsebene können allen Benutzern, die den SNMP-Set-Community-Namen kennen, ermöglichen, Kontrolle über das verwaltete System zu erlangen.

 **ANMERKUNG:** IT Assistant verwendet SNMP-Sätze nur, um Systeme aus- und einzuschalten, wenn die Remote-Befehlszeile von Server Administrator nicht verfügbar ist. Wenn SNMP-Sätze zu diesem Zweck nicht erforderlich sind, geben Sie keinen SNMP-Set-Community-Namen im Ermittlungsassistenten ein.


Sabine wählt einen **Set-Community**-Namen, der mit dem SNMP-Set-Community-Wert auf dem von ihr verwalteten System übereinstimmt. Sie stellt auch sicher, dass der ausgesuchte Name den Standards für sichere Kennworte entspricht, die in ihrem Unternehmen gelten.

 **ANMERKUNG:** Wenn mehr als ein SNMP Get oder Set Community-Name in einem einzelnen Ermittlungsbereich angegeben werden soll (z. B. ein Community-Name für jeden IP-Subnetzbereich), müssen die Community-Namen durch Kommas getrennt werden.

- 1 Sabine gibt die SNMP-Zeitüberschreitungs- und Wiederholungswerte für den Ermittlungsbereich ein. Für Sabines Netzwerktyp sind die Standardwerte gewöhnlich eine gute Wahl.
- 1 In Schritt 4 des Assistenten konfiguriert Sabine die CIM-Parameter, die während der Ermittlung verwendet werden sollen.

Da Sabine in Ihrer verwalteten Gruppe eine Mischung von Servern und Client-Systemen hat, die Windows ausführen, wird sie CIM konfigurieren.

- 1 Sabine stellt sicher, dass **CIM-Ermittlung aktivieren** ausgewählt ist.
- 1 Unter **Domäne\Benutzername** gibt sie denselben Namen ein, den Sie zur CIM-Konfiguration auf dem verwalteten System verwendet hat.
- 1 Sie gibt dasselbe Kennwort ein, das Sie als CIM-Kennwort auf dem verwalteten System verwendet hat.

 **ANMERKUNG:** Sie sollten die CIM- Ermittlungsoption aktivieren, wenn Sie den Microsoft-Hardwareagenten für IPMI in Microsoft Windows Server 2003 R2 verwenden möchten.

7. In Schritt 5 des Assistenten wählt Sabine **Dell/EMC-Array-Ermittlung aktivieren** nicht aus, weil sich auf ihrem Netzwerk keine Dell|EMC-Speichergeräte befinden.
8. In Schritt 6 des Assistenten konfiguriert Sabine die IPMI-Parameter nicht, da sie ihre Systeme über IPMI überwachen möchte.
9. In Schritt 7 des Assistenten wählt Sabine, welche Maßnahme IT Assistant nach Beendigung des Assistenten ausführen wird.
10. In Schritt 8 des Assistenten prüft Sabine ihre Auswahl und klickt auf **Fertig stellen**, um den Assistenten abzuschließen.

 **ANMERKUNG:** Sie können auf **Zurück** klicken, um Ihre Auswahl zu ändern.

## Ermittlungs-, Bestandsaufnahme- und Statusabfrageeinstellungen nach dem Original-Setup ändern

Sie können jederzeit zur Bearbeitung der eingegebenen Einstellungen zum Menü **Ermittlung und Überwachung** zurückkehren. Die neu eingegebenen Einstellungen werden wirksam, wenn sie das nächste Mal die entsprechende Maßnahme ausführen.

## Warnungsmaßnahmenfilter und Warnungsmaßnahmen für Sabines Firma (kleine bis mittlere Größe) erstellen

Sabine erstellt einen *Warnungsmaßnahmenfilter* im IT Assistant, indem Sie eine Reihe von Bedingungen festlegt. Bei Anbindung an eine *Warnungsmaßnahme* wird IT Assistant automatisch jede beliebige Maßnahme ausführen, die Sabine definiert hat.

IT Assistant besitzt drei Arten von Warnungsfiltern:

**Warnungsmaßnahmenfilter** - werden verwendet, um Maßnahmen auszulösen, wenn eine Warnungsbedingung eintritt

**Ignorieren/Ausschließen-Filter** - werden verwendet, um SNMP-Traps und CIM-Hinweise zu ignorieren, wenn sie empfangen werden.

**Warnungsansichtsfilter** - werden verwendet, um die Warnungsprotokollansicht an die eigenen Bedürfnisse anzupassen

Sabine beschließt, einen Warnungsmaßnahmenfilter im IT Assistant zu verwenden, um *Warnungs-* und *kritische* Ereignisse für ihre Server und PowerConnect-Schalter zu filtern. Auf diese Weise wird sie imstande sein, eine Warnungsmaßnahme zu erstellen, die ihr automatisch eine E-Mail-Benachrichtigung sendet, wenn die Server- und Schalterkomponenten diese Zustände erreichen. Dann kann sie selbst Maßnahmen ergreifen, um ein ernsteres Ereignis wie eine Systemstörung zu verhindern. Da sie der einzige Systemadministrator ihres Netzwerks ist, muss Sabine gezielt entscheiden, welche Systeme sie überwachen und welche Warnungsmaßnahmenfilter sie erstellen will. Sie entscheidet sich dafür, diese Filter und Maßnahmen für die Geräte vorzubehalten, die für die Firmenaufträge am wichtigsten sind, sowie für die schwerwiegendsten Ereignisse.

## Warnungsmaßnahmenfilter erstellen

1. Wählen Sie **Warnungen**→**Filter** aus der Menüleiste.

Das Fenster **Warnungsfilter** wird eingeblendet.

2. Erweitern Sie die Warnungsfilter in der Navigationsstruktur und klicken Sie mit der rechten Maustaste auf **Warnungsmaßnahmenfilter**. Wählen Sie **Neuer Warnungsmaßnahmenfilter** aus.

Der **Assistent Filter hinzufügen** wird eingeblendet.

3. Geben Sie einen beschreibenden Namen für den Filter ein. Zum Beispiel *Sabines Netzwerkwarnung und kritisch*.
4. Wählen Sie unter **Schweregrad** den Schweregrad der Ereignisse aus, für die Warnungen und Protokolle empfangen werden sollen.

Sabine wählt **Warnung** und **Kritisch** aus.

Klicken Sie auf **Weiter**.

5. Unter **Warnungskategorie-Konfiguration** wählen Sie entweder **Alle auswählen** oder wählen Sie die Ereigniskategorien aus, die im Warnungsfilter enthalten sein sollen.

Sabine wählt **Alle auswählen** aus, da sie über alle Warnungsereignisse bzw. kritischen Ereignisse unterrichtet werden möchte, die ihre Netzwerkschalter oder Server beeinflussen.

Klicken Sie auf **Weiter**.

6. Unter **Geräte-/Gruppenkonfiguration** wählen Sie die Geräte oder Gruppen aus, die dem neuen Maßnahmenwarnungsfilter zugeordnet werden sollen.

Sabine wählt **Server und Netzwerkgeräte** aus.

Klicken Sie auf **Weiter**.

7. Unter **Datum/Uhrzeit-Bereichskonfiguration** geben Sie die Werte für einzelne oder alle optionalen Kategorien ein.

Sabine wählt keine dieser Optionen, da sie will, dass der Filter jeder Zeit angewendet wird.

Klicken Sie auf **Weiter**.

8. Unter **Warnungsmaßnahmenverbindung** wählen Sie, ob das durch den Filter erfasste Ereignis eine Warnung auslösen oder ob es zu einer Protokolldatei geschrieben werden soll.

Sabine wählt **Warnung** aus, damit Sie eine Konsolenbenachrichtigung erhält.

- Die **Zusammenfassung für Neuer Filter** zeigt Ihre Auswahl. Klicken Sie auf **Fertig stellen**, um anzunehmen oder auf **Zurück**, um Änderungen vorzunehmen.
- Überprüfen Sie, ob der Filtername, den Sie in [Schritt 3](#) des Assistenten erstellt haben, im Fenster **Zusammenfassung der Warnungsmaßnahmenfilter** erscheint.

## Warnungsmaßnahme erstellen


Jetzt will Sabine eine Warnungsmaßnahme erstellen, die durch den Warnungsmaßnahmenfilter ausgelöst wird, den sie gerade eingerichtet hat.

So wird eine Warnungsmaßnahme erstellt:

- Sabine wählt **Warnungen** → **Maßnahmen** aus der Menüleiste aus.
- Sabine klickt in der Navigationsstruktur mit der rechten Maustaste auf **Warnungsmaßnahmen** und wählt **Neue Warnungsmaßnahme** aus.


Der **Assistent Warnungsmaßnahme hinzufügen** wird eingeblendet.


- Sabine gibt der Maßnahme einen logischen Namen im Feld **Name**.
- Wählen Sie im **Typ**-Pull-down-Menü **E-Mail** aus.

 **ANMERKUNG:** Sabine könnte auch **Trap-Weiterleitung** oder **Anwendungsstart** aus der Pull-Down-Liste **Maßnahmentyp** auswählen. **Trap-Weiterleitung** ermöglicht den Managern von Großunternehmen, SNMP-Traps an eine spezifische IP-Adresse oder einen spezifischen Host zu senden. **Anwendungsstart** ermöglicht einem Administrator, eine ausführbare Datei zu bestimmen, die ausgeführt werden soll, wenn der Warnungsmaßnahmenfilter erfüllt wird.

 **ANMERKUNG:** Jeder von IT Assistant weitergeleitete Trap wird nicht die Enterprise OID, Allgemeine Trap-ID bzw. Spezifische Trap-ID des Original-Trip haben. Diese Werte werden in der Beschreibung des weitergeleiteten Traps erscheinen.

- Im Dialog **E-Mail-Konfiguration** gibt Sabine eine gültige E-Mail-Adresse an (innerhalb der SMTP-Servergruppe Ihres Unternehmens), um die automatische Benachrichtigung zu erhalten.

 **ANMERKUNG:** Sabine kann die E-Mail-Konfiguration, die sie angibt, mit der Schaltfläche **Testmaßnahme** testen. Eine Erfolgs- bzw. Fehlermeldung wird ausgegeben werden. Ein Erfolg bedeutet, dass IT Assistant die Nachricht gesendet hat und nicht, dass der Empfänger sie erhielt. Weitere Informationen zum Verwenden der Schaltfläche **Testmaßnahme** finden Sie unter dem Thema Fehlerbehebung in der *IT Assistant-Onlinehilfe*.

 **ANMERKUNG:** Um E-Mail durch den IT Assistant zu senden, muss der SMTP-Server des Unternehmens richtig konfiguriert werden. Um den SMTP-Server zu konfigurieren, wechseln Sie auf der oberen Navigationsleiste zu **Einstellungen** → **Web Server**, und konfigurieren **SMTP-Servername (oder IP-Adresse)** und **DNS-Suffix für SMTP-Server**.

- In **Warnungsfilterverbindungen** legt Sabine den Warnungsmaßnahmenfilter fest, der diese E-Mail auslösen wird.

Sie wählt *Sabines Netzwerk - Warnung und Kritisch* aus - den Namen, den sie dem zuvor eingerichteten Warnungsmaßnahmenfilter gegeben hat.

- Ein Zusammenfassungs-Dialogfeld zeigt Sabines Auswahl an.

Sabine überprüft, ob der Name der Warnungsmaßnahme, den Sie in [Schritt 3](#) zugewiesen hat, im Fenster **Zusammenfassung der Warnungsmaßnahmen** erscheint.

Sabine klickt auf **Fertig stellen**, um die Änderungen anzunehmen.

Je nach dem, wie Sabine die Warnungsmaßnahmenfilter und die Warnungsmaßnahmen in IT Assistant konfiguriert hat, passiert folgendes:

- IT Assistant wird alle Server und alle Netzwerkschalter auf Sabines Netzwerk ständig überwachen.
- Wenn einer der Server- oder Netzwerkschalter einen Warnungszustand oder einen kritischen Zustand erreicht, wird der Warnungsmaßnahmenfilter, den Sabine im IT Assistant eingerichtet hat, automatisch die begleitende Warnungsmaßnahme auslösen.
- Die Warnungsmaßnahme wird Sabine eine E-Mail-Benachrichtigung an die festgelegte Adresse senden.
- Sabine entscheidet dann, welche Maßnahme auf dem betroffenen System getroffen werden soll, wie z. B. das Aus- und Einschalten bzw. Herunterfahren des Systems oder die Ausführung eines Remote-Befehls unter Verwendung anderer IT Assistant-Fähigkeiten.

Weit mehr Funktionen als die hier dargestellten stehen im IT Assistant zur Verfügung. Klicken Sie auf die Schaltfläche **Hilfe** im entsprechenden IT Assistant-



Dialogfeld, um ausführliche Online-Hilfe zu dieser Funktion zu erhalten.

Lassen Sie uns jetzt sehen, wie ein wesentlich größeres Unternehmen IT Assistant einsetzen könnte, um mehr oder weniger die gleichen Tasks zu bewältigen, die Sabine für ihr kleines Unternehmen durchgeführt hat.

---

## Ermittlung in Christians Geschäft (Unternehmensgröße)

In einem größeren Geschäftsunternehmen ist Christian der Systemadministrator für ein Netzwerk von 1 000 Servern. Christian unterstehen auch vier Techniker, die ihn bei Korrekturmaßnahmen für Server unterstützen, falls ein kritisches oder Warnungsereignis eintritt. Christians vier Techniker haben folgende Zuständigkeitsbereiche:

- 1 Ein Administrator ist für alle Remote-Systeme verantwortlich
- 1 Ein Techniker in der ersten Schicht (12 Stunden)
- 1 Ein Techniker in der zweiten Schicht (12 Stunden)
- 1 Ein Techniker an Wochenenden, der 24-Stunden-Schichten arbeitet, aber nur nach Benachrichtigung auf kritische und Warnungsereignisse reagiert

## Ermittlungseinstellungen konfigurieren


Da Christian ein Servernetzwerk überwacht und keine Clients, ist SNMP die erste Wahl für das Systemverwaltungsprotokoll. Da er jedoch auch Systeme verwaltet, die Windows ausführen, wird er (wie Sabine) auch CIM aktivieren.

Zur Konfiguration der Ermittlungseinstellungen für seinen Server muss er die folgenden Tasks ausführen:

- 1 Subnetzbereiche, IP-Adressen und/oder Host-Namen für die zu überwachenden Server festlegen.
- 1 Die Subnetzbereiche, Host-Namen oder IP-Adressen festlegen, die nicht überwacht werden sollen.
- 1 Community-Namen des Typs schreibgeschützt (Get) und Lese-/Schreibzugriff (Set) für SNMP festlegen, die für das Netzwerk verwendet werden sollen.
- 1 SNMP-Agenten und SNMP-Dienst des Betriebssystems auf jedem zu überwachenden System installieren und konfigurieren.
- 1 Geeignete Zeitüberschreitungswerte für die Ermittlung im Netzwerk festlegen.

## IP-Subnetzbereiche für Server

Christian muss als erstes entscheiden, welche der 1,000 Server mit dem IT Assistant überwacht werden sollen. Er möchte eventuell den IP-Subnetzbereich jedes in der Ermittlung enthaltenen Subnetzes, alle von der Ermittlung ausgeschlossenen Systeme oder Bereiche, die in jedem Subnetz verwendeten entsprechenden Community-Namen sowie alle weiteren für das Netzwerk relevanten Daten aufzeichnen. Ein Beispiel für die Erfassung dieser Daten wird in [Tabelle 6-2](#) gezeigt. Zu beachten ist, dass Christian Systeme auf Basis des Subnetzbereichs, Host-Namens oder der IP-Adresse überwacht. Obwohl es ratsam ist, die Anzahl der in einem Netzwerk verwendeten Community-Namen zu begrenzen, kann Christian auch mehrere schreibgeschützte und Lese-/Schreibzugriff-Community-Namen in der Netzwerkumgebung definieren. Zum Beispiel kann Christian entscheiden, dass er einen gemeingültigen Get-Community-Namen für alle Systeme in diesem Netzwerk, jedoch eindeutige Set-Community-Namen für bestimmte Datenzentren einrichten möchte.

 **ANMERKUNG:** IT Assistant bietet ein Fehlerbehebungshilfsprogramm an, das für die Erfassung von Systeminformationen und Subnetzbereichen nützlich sein kann. Sie können auf das Hilfsprogramm zugreifen, indem Sie **Hilfsprogramme** → **Fehlerbehebungshilfsprogramm** aus der Menüleiste auswählen. Weitere Informationen erhalten Sie, wenn Sie das Dialogfeld Fehlerbehebungshilfsprogramm öffnen und auf Hilfe klicken.

## SNMP auf jedem verwalteten System konfigurieren

Vor der Konfiguration der Ermittlung muss Christian die Get- und Set-Community-Namen festlegen, die er für das Netzwerk verwenden will. Außerdem muss er den SNMP-Agenten sowie den SNMP-Dienst des Betriebssystems jedes zu verwaltenden Servers installieren und konfigurieren. Siehe "SNMP für Serververwaltungsfunktionen konfigurieren (beide Szenarien)".

[Tabelle 6-2](#) enthält Informationen zu den von Christian überwachten Remote-Systemen.

**Tabelle 6-2. Beispiele für Subnetzbereiche, IP-Adressen oder Host-Namen sowie entsprechende Informationen zu Datenzentrums- und Remote-Servern**

---

Systemgruppenname	Subnetzbereich einschließen	Hosts oder Subnetzbereich ausschließen	Schreibgeschützte/Lese-/Schreibzugriff-Community-Namen	Anzahl der Geräte im Subnetz	Längste im Subnetz beobachtete Ping-Antwortzeit (Millisekunden)
Datenzentrum-Server 1	192.166.153.*	192.166.153.2	dcp123/dcsecure01	100	64
Datenzentrum-Server 2	192.166.154.*	examplehost	dcp123/dcsecure01	100	128
Datenzentrum-Server 3	192.166.155.*	192.166.155.10-25	dcp123/dcxprivall	100	78
Datenzentrum-Server 4	192.166.156.*		dcp123/dcxprivall	100	32
Datenzentrum-Server 5	192.166.157.*		dcp123/dcxprivall	100	146
Datenzentrum-Server 6	192.166.158.*		dcp123/dcxprivall	100	148
Datenzentrum-Server 7	192.166.159.*		dcp123/dcxprivall	100	132
Datenzentrum-Server 8	192.166.160.*		dcp123/dcxprivall	100	59
Datenzentrum-Server 9	192.166.161.*		dcp123/dcxprivall	50	128
Remote-Server 1	10.9.72.*		dcp123/dcxprivrem	50	5600
Remote-Server 2	10.9.73.*		dcp123/dcxprivrem	100	2400
Dell EMC-Speichergeräte	192.166.162.1-10		dcp123/NA	5	32
Drucker	192.166.163.51-100		dcp123/NA	25	32
Bandgeräte	192.166.163.1-20		dcp123/NA	10	59

## Geeigneten Zeitüberschreitungswert für die Ermittlung im Netzwerk auswählen

Da Christian Remote-Systeme in einem WAN überwacht, können die Zeitüberschreitungswerte des lokalen Systems erheblich von denen der weiter entfernten abweichen. In diesem Fall sollte Christian ein geeignetes Zeitlimit für die Ermittlung der Systeme im WAN festlegen und einstellen.

In Umgebungen mit hohen Netzwerklatenzzeiten, wie z. B. globalen WANs, sollte Christian eventuell erwägen, die Ping-Zeitlimits im gesamten Unternehmen zu erhöhen. Er kann die Ping-Zeiten der Systeme festlegen, die die größte Latenz auf dem Netzwerk aufweisen, indem er zu **Hilfsprogramme** → **Fehlerbehebungshilfsprogramm** wechselt und das Register **Gerätekonnektivität** wählt. Dann kann Christian die Verbindung von Systemen mit hoher Latenz prüfen, um zu sehen, ob er spezifische Ping-Zeiten für eine bessere WAN-Leistung erhöhen sollte.

## Ermittlungseinstellungen im Unternehmensnetzwerk erstmalig konfigurieren

Wenn IT Assistant jetzt zum ersten Mal seit der Installation gestartet wird, sieht Christian wie Sabine einen Willkommens-Bildschirm, der anzeigt, dass IT Assistant noch nicht konfiguriert worden ist. Die vier grundlegenden Schritte der Konfiguration sind hier aufgeführt:

Schritt 1: Ermittlungskonfiguration

Schritt 2: Bestandsaufnahmekonfiguration

Schritt 3: Statusabfrage

Schritt 4: Bereiche

Sobald Christian einen dieser Schritte anklickt, wechselt er zum entsprechenden Dialogfeld unter der Menüleiste **Ermittlung und Überwachung** in IT Assistant. Die Schritte 1 bis 3 sind Dialogfelder mit einem einzigen Fenster; Schritt 4 ist ein Assistent-basiertes Verfahren zum Definieren von Ermittlungsbereichen.

## Ermittlungs-Konfigurationseinstellungen konfigurieren

Christian beginnt ebenfalls damit, die Ermittlungseinstellungen für seine Systeme mit dem Dialogfeld **Ermittlungskonfigurationseinstellungen** zu konfigurieren. Dieser Dialog wird automatisch angezeigt, wenn er auf *Schritt 1: Ermittlungskonfiguration* im Willkommens-Bildschirm des IT Assistant klickt oder wenn er **Ermittlungskonfiguration** aus der Menüleiste auswählt. Hier gibt Christian Informationen ein, die IT Assistant für die Ermittlung verwenden wird. Diese Werte bleiben unverändert und beziehen sich auf alle Ermittlungsbereiche, die er später im Verfahren erstellt. Er kann diese Werte jedoch jederzeit mit diesem Dialogfeld ändern.

Um in IT Assistant Ermittlungseinstellungen für ein großes Unternehmen zu konfigurieren, führt Christian folgende Schritte aus:

1. Christian wählt von der IT Assistant-Menüleiste **Ermittlung und Überwachung** → **Ermittlungskonfiguration** aus.

Das Dialogfeld **Ermittlungskonfigurationseinstellungen** wird eingeblendet. **Geräteermittlung aktivieren** ist standardmäßig ausgewählt.

2. Unter **Geräteermittlung einleiten** wählt Christian aus, wann IT Assistant die Ermittlung ausführen soll.


Christian will die Ermittlung jeden Tag ausführen, deshalb wählt er **Jede Woche um**, jeden Tag der Woche und 2:00 vormittags für die Startzeit. Sein Netzwerk-Datenverkehr weist zu diesem Zeitpunkt die geringste Dichte auf.

3. Christian bestimmt über den Schieberegler unter **Ermittlungsgeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die er für die Ermittlung zuweisen möchte.

Christian stellt die Ermittlungsgeschwindigkeit auf **Schnell** (ganz rechts) ein. Christian möchte alle mit dem IT Assistant zu verwaltenden Systeme schnell ermitteln und in die Datenbank aufnehmen. Wenn Christian feststellt, dass diese Einstellung die Netzwerkleistung drastisch beeinflusst, während er versucht, andere Tasks im Netzwerk auszuführen, kann er die **Ermittlungsgeschwindigkeit** für nachfolgende Ermittlungen so ändern, dass weniger Netzwerkressourcen verbraucht werden.

4. Christian kann unter **Ermittlung** wählen, ob alle Geräte oder nur instrumentierte Geräte ermittelt werden sollen.
5. Unter **Namensauflösung** kann Christian **DNS-Namensauflösung** oder **Instrumentationsnamensauflösung** auswählen.

DNS (Domänenname-System) -Namensauflösung stimmt die IP-Adresse eines Systems mit einem Host-Namen ab. Instrumentationsnamensauflösung fragt den Namen der Agenten-Instrumentation des verwalteten Systems ab. Weitere Informationen zur Konfiguration der Instrumentationsnamensauflösung finden Sie in der Dokumentation des Gerätes oder des Systems.

 **ANMERKUNG:** Wenn Sie einen Cluster verwalten, können Sie alle unabhängigen Knoten (Systeme) nur wahrnehmen wenn Sie Instrumentationsnamensauflösung verwenden, andernfalls wird die Verwendung der DNS-Namensauflösung empfohlen.

6. Christian klickt auf **OK**.

## Bestandsaufnahme-einstellungen konfigurieren

Als nächstes gibt Christian die Einstellungen der Bestandsaufnahme ein. IT Assistant sammelt Bestandsaufnahmeinformationen zu Software- und Firmware-Versionen, sowie Geräteinformationen über Speicher, Prozessoren, Netzteile, PCI-Karten und integrierte Geräte sowie Speicherplatz. Diese Informationen werden in der IT Assistant-Datenbank gespeichert und können zur Erstellung von benutzerspezifischen Reports verwendet werden.

Um Bestandsaufnahme-Einstellungen einzustellen, führt Christian folgende Schritte aus:


1. Christian wählt aus der Menüleiste **Ermittlung und Überwachung** → **Bestandsaufnahme-konfiguration** aus.

Das Dialogfeld **Einstellungen der Bestandsaufnahmeabfrage** wird angezeigt. **Bestandsaufnahme aktivieren** ist standardmäßig ausgewählt.


2. Im Dialogfeld unter **Bestandsaufnahme einleiten** wählt Christian aus, wann IT Assistant die Bestandsaufnahme ausführen soll.

Christian stellt die Bestandsaufnahme so ein, dass sie wöchentlich am Samstag um 3:00 vormittags ausgeführt wird.

3. Christian bestimmt über den Schieberegler unter **Bestandsaufnahme-geschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die er für die Bestandsaufnahme zuweisen möchte.

 **ANMERKUNG:** Je höher Sie die Bestandsaufnahme-geschwindigkeit einstellen, desto mehr Netzwerk-Ressourcen wird die Ermittlung verbrauchen. Höhere Bestandsaufnahme-geschwindigkeiten können die Netzwerkleistung negativ beeinflussen.

4. Christian klickt auf **OK**.

 **ANMERKUNG:** IT Assistant Version 8.0 kann jetzt die Bestandsaufnahme-Informationen für Drucker, Bänder und Speichergeräte anzeigen. Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.

## Statusabfrage-Einstellungen konfigurieren


Als nächstes definiert Christian die Statusabfrageeinstellungen für seine Systeme. IT Assistant führt eine Überprüfung des Strom- und Konnektivitätsfunktionszustands für ermittelte Geräte aus, und legt fest, ob ein Gerät normal funktioniert, sich in einem nichtnormalen Zustand befindet oder heruntergefahren ist. Die Statusmeldungen im IT Assistant umfassen *Funktionsfähig*, *Warnung*, *Kritisch* und *Heruntergefahren*. Statussymbole zeigen auch an, ob ein System nicht instrumentiert ist, ob es keine Informationen zu dem System gibt, oder sie zeigen den Zustand des Systems, indem es sich beim letzten Herunterfahren befand.

Um Statusabfrage-Einstellungen einzustellen, führt Christian folgende Schritte aus:

1. Christian wählt aus der Menüleiste **Ermittlung und Überwachung** → **Statusabfragekonfiguration** aus.

Das Dialogfeld **Statusabfrage-Konfigurationseinstellungen** wird angezeigt. **Statusabfrage aktivieren** ist standardmäßig ausgewählt.

2. Unter **Statusabfrageintervall** wählt Christian das Intervall aus, das IT Assistant zur Ausführung der Statusabfrage verwenden soll.
3. Christian bestimmt über den Schieberegler unter **Statusabfragegeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die er für die Statusabfrage zuweisen möchte.

 **ANMERKUNG:** Je höher Sie die Statusabfragegeschwindigkeit einstellen, desto mehr Netzwerk-Ressourcen wird die Ermittlung verbrauchen. Höhere Geschwindigkeiten können die Netzwerkleistung beeinflussen.

4. Christian klickt auf **OK**.

## Ermittlungsbereiche konfigurieren

IT Assistant führt ein Register von Netzwerksegmenten, das zur Ermittlung von Geräten verwendet wird. Ein Ermittlungsbereich kann ein Subnetz, ein Bereich von IP-Adressen auf einem Subnetz, eine individuelle IP-Adresse oder ein individueller Host-Name sein.

Christians Unternehmensnetzwerk ist in eine Reihe von Subnetzen unterteilt. Es sind 850 Server im Datenzentrum und 150 Remote-Server vorhanden. Christian bezieht sich auf die IP-Subnetzbereiche, die er für seine Server notiert hat (siehe [Tabelle 6-2](#)).

Christians Datenzentrumsserver sind in acht separate Subnetze unterteilt, seine Remote-Server sind in zwei Subnetze unterteilt.

Um seine Systeme für IT Assistant festzulegen, muss Christian einen Ermittlungsbereich definieren.

Um einen *Einschlussbereich* zu identifizieren, führt Christian folgende Schritte aus:

1. Christian wählt **Ermittlung und Überwachung** → **Bereiche** aus der Menüleiste aus.

Die Navigationsstruktur **Ermittlungsbereiche** wird auf der linken Seite des IT Assistant-Fenster angezeigt.

2. Christian erweitert **Ermittlungsbereiche**, klickt mit der rechten Maustaste auf **Einschlussbereiche** und wählt **Neuer Einschlussbereich** aus.

Der **Assistent Neue Ermittlung** startet.

3. In Schritt 1 des Assistenten kann Christian eine IP-Adresse, einen IP-Adressbereich oder einen Host-Namen eingeben.

Basierend auf den Informationen zu Christians Systemen in [Tabelle 6-2](#) muss er unterschiedliche IP-Adressbereiche hinzufügen. Christian kann die Bereiche kombinieren, die die gleichen Einstellungen haben (Community-Name, Zeitüberschreitung, Wiederholungsintervalle, Wahl des Ermittlungsprotokolls sowie Benutzeranmeldeinformationen). Er kann z. B. die Gruppen des Datenzentrumsservers 3 bis Datenzentrumsservers 9 kombinieren.


Er gibt den IP-Adressbereich ein als:

192.166.155.\*

Anstatt diesen Assistenten mehrmals mit denselben Einträgen in allen Assistentenfenstern durchzuführen, um alle diese Systeme einzuschließen, klickt Christian auf **Hinzufügen**, um mehrere IP-Adressbereiche hinzuzufügen. Das zweite Mal gibt er folgendes ein:

192.166.156.\*

usw.

 **ANMERKUNG:** Stellen Sie sicher, dass für Dell|EMC-Geräte ein separater Bereich vorhanden ist. Der Grund hierfür ist, dass für Dell|EMC-Geräte neben SNMP-Anmeldeinformationen auch Navisphere-Anmeldeinformationen erforderlich sind.

Christian klickt auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

 **ANMERKUNG:** Das Dienstprogramm Import Node List bietet eine praktische Methode zur Festlegung einer Liste von Host-Namen, IP-Adressen und Subnetzbereichen, die IT Assistent ermitteln soll. Anleitungen zur Ausführung des Dienstprogramms von der Befehlszeile aus finden Sie in der *IT Assistant-Onlinehilfe*. Die Datei **importnodelist.exe** befindet sich im Verzeichnis **/bin**.


4. In Schritt 2 des Assistenten gibt Christian die Zeitüberschreitungs- und Wiederholungswerte des Internetsteuerungs-Meldungsprotokolls (ICMP) für den Bereich ein. Christian wählt den höchsten Zeitüberschreitungs-Wiederholungswert für die Bereiche, die er kombiniert. In [Tabelle 6-2](#) für Datenzentrumsserver 3 bis Datenzentrumsserver 9 wählt Christian z. B. 148 Millisekunden, was das höchste Zeitüberschreitungs-Intervall dieses Bereichs darstellt.
5. In Schritt 3 des Assistenten konfiguriert Christian die **SNMP-Parameter**, die während der Ermittlung verwendet werden sollen:
  - 1 Christian stellt sicher, dass die Option **SNMP-Ermittlung aktivieren** ausgewählt ist.
  - 1 Christian gibt einen Wert für den **Get-Community-Namen** ein (Groß- und Kleinschreibung beachten). Der **Get-Community-Name** ist ein Nur-Lesen-Kennwort, das SNMP-Agenten auf verwalteten Systemen zur Authentifizierung installieren.

Christians Überlegungen:

Folgendes zieht Christian bei der Auswahl des **Get-Community**-Namens in Betracht:

Jedes SNMP-verwaltete System besitzt einen **Get-Community**-Namen. Christian stellt daher sicher, dass er jeden Community-Namen auf allen zu verwaltenden Systemen auflistet. Wenn Christians verwaltete Systeme mehr als einen Community-Namen aufweisen, kann er im Feld **Get-Community-Name** mehrere durch Kommas getrennte Community-Namen eingeben.

Obwohl der **Get-Community**-Name die Nur-Lese-Informationen beeinflusst, die IT Assistent von den verwalteten Systemen erhalten hat, wie z. B. Ermittlungsergebnisse, Statusabfragen und Warnungsprotokolle, möchte Christian den Zugriff auf diese Daten einschränken. Er ändert deshalb den Standard-**Get-Community**-Namen **öffentlich** zu einem Namen, der nur ihm und seinem Systemadministrator bekannt ist.

 **ANMERKUNG:** Die in den Feldern SNMP-Get- und Set-Community-Name eingegebenen Community-Namen für das Betriebssystem des verwalteten Systems müssen mit den Get- und Set-Community-Namen übereinstimmen, die in IT Assistent zugewiesen wurden.


- 1 Christian gibt einen Wert für den **Set-Community-Namen** ein (Groß- und Kleinschreibung beachten).


Christians Überlegungen:

Der **Set-Community**-Name ist ein Lesen-Schreiben-Kennwort, das Zugriff auf ein verwaltetes System ermöglicht. SNMP-Agenten, die auf dem verwalteten System ausgeführt werden, verwenden dieses Kennwort zur Authentifizierung, wenn Maßnahmen auf dem System versucht werden, einschließlich Herunterfahren, Konfigurieren von Warnungsmaßnahmen und Aktualisieren von Software.

 **ANMERKUNG:** Obwohl die Dell Server-Instrumentation über eine Authentifizierungsebene oberhalb des SNMP-Set-Community-Namens (der einen Host-Namen und ein Kennwort erfordert) verfügt, besitzen viele SNMP-Agenten diese Ebene nicht. Agenten ohne diese zusätzliche Sicherheitsebene ermöglichen allen Benutzern, die den SNMP-Set-Community-Namen kennen, Kontrolle über das verwaltete System zu erlangen.

Christian wählt einen **Set-Community**-Namen, der mit dem SNMP-Set-Community-Wert auf dem von ihm verwalteten System übereinstimmt. Er stellt auch sicher, dass der ausgesuchte Name den Standards für sichere Kennworte entspricht, die in seinem Unternehmen gelten.


 **ANMERKUNG:** Wenn mehr als ein SNMP Get oder Set Community-Name in einem einzelnen Ermittlungsbereich angegeben werden soll (z. B. ein Community-Name für jeden IP-Subnetzbereich), müssen die Community-Namen durch Kommas getrennt werden.

 **ANMERKUNG:** IT Assistant verwendet SNMP-Sätze nur, um Systeme aus- und einzuschalten, wenn die Remote-Befehlszeile von Server Administrator nicht verfügbar ist. Wenn SNMP-Sätze zu diesem Zweck nicht erforderlich sind, geben Sie keinen SNMP-Set-Community-Namen im Ermittlungsassistenten ein.

- 1 Christian gibt Zeitüberschreitungs- und Wiederholungswerte für den SNMP-Ermittlungsbereich ein.
- 1 In Schritt 4 des Assistenten konfiguriert Christian die CIM-Parameter, die während der Ermittlung verwendet werden sollen.

Da Christian auch Systeme hat, die Windows ausführen, muss er CIM konfigurieren.


- 1 Christian stellt sicher, dass **CIM-Ermittlung aktivieren** ausgewählt ist.
- 1 Unter **Domäne\Benutzername** gibt Christian denselben Namen ein, den er zur CIM-Konfiguration auf dem verwalteten System verwendet hat.
- 1 Christian gibt dasselbe **Kennwort** ein, das er als CIM-Kennwort auf dem verwalteten System verwendet hat.

 **ANMERKUNG:** Sie können die CIM-Ermittlungsoption aktivieren, wenn Sie die IPMI-Ermittlungsunterstützungs-Funktion verwenden möchten. Diese Option ist nur auf x8xx- und x9xx-Systemen verfügbar, auf denen Windows Server 2003 R2 oder andere Versionen ausgeführt werden, die den Microsoft-Hardwareverwaltungsanbieter unterstützen.

7. In Schritt 5 des Assistenten wählt Christian **Dell/EMC-Array-Ermittlung aktivieren** aus.

In diesem Bildschirm gibt Christian die folgenden Details an:


- 1 Navisphere-Benutzername
- 1 Navisphere-Kennwort

 **ANMERKUNG:** Sie können dieses Feld nur verwenden, wenn sich im Ermittlungsbereich Dell|EMC-Geräte befinden.

8. In Schritt 6 des Assistenten konfiguriert Christian die folgenden IPMI-Parameter des BMC seiner verwalteten Systeme.

- 1 Benutzername
- 1 Kennwort
- 1 KG-Schlüssel


 **ANMERKUNG:** KGKey ist nur auf x9xx-Systemen anwendbar, die IPMI Version 2.0 unterstützen. Standardmäßig ist KGKey auf dem BMC deaktiviert.

 **ANMERKUNG:** Wenn sich in Ihrem Netzwerk sowohl x8xx- als auch x9xx-Systeme befinden und Sie KGKey auf x9xx-Systemen aktivieren, werden Sie zwei separate Bereiche festlegen müssen, um diese Systeme zu ermitteln.

Da Christian PowerEdge-x9xx-Systeme besitzt, die nicht instrumentiert sind (auf denen kein Dell-Agent installiert ist), kann er diese Systeme anhand von IPMI-Ermittlung ermitteln.

Weitere Informationen finden Sie unter "[IPMI-Ermittlung in Christians Geschäft der Unternehmensgröße verwenden](#)".

9. In Schritt 7 des Assistenten kann Christian wählen, welche Maßnahme IT Assistant nach Beendigung des Assistenten ausführen wird.
10. In Schritt 8 des Assistenten prüft Christian seine Auswahl und klickt auf **Fertig stellen**, um den Assistenten abzuschließen.

 **ANMERKUNG:** IT Assistant Version 8.0 kann jetzt Drucker, Bänder und Speichergeräte ermitteln. Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.

## Systeme von der Ermittlung ausschließen

IT Assistant bietet auch die Fähigkeit, bestimmte Systeme von der Ermittlung auszuschließen. Diese Funktion wird normalerweise in der Umgebung in größeren Unternehmen verwendet, um die Geschwindigkeit zu erhöhen, ein System mit einem problematischen Agenten zu isolieren oder um Sicherheit und Benutzerfreundlichkeit zu verbessern.

Christian hat ein System in seinem Unternehmen, das hoch empfindliche Informationen enthält. In der Tat so empfindlich, dass er sogar möchte, dass das System nicht von seinen Systemadministratoren wahrgenommen werden kann. Deshalb richtet er einen **Ausschlussbereich** ein, der dieses System von der alltäglichen Netzwerkermittlung ausschließt.

1. Christian wählt **Ermittlung und Überwachung** → Bereiche aus der Menüleiste aus.

Die Navigationsstruktur **Ermittlungsbereiche** wird auf der linken Seite des IT Assistant-Fenster angezeigt.

- Christian erweitert **Ermittlungsbereiche**, klickt mit der rechten Maustaste auf **Ausschlussbereiche** und wählt **Neuer Ausschlussbereich**.

Das Dialogfeld **Neuer Ausschlussbereich** wird eingeblendet.

- Christian gibt die IP-Adresse für das System ein und klickt auf **OK**.

Infolgedessen kann dieses System nicht während der alltäglichen Ermittlung durch IT Assistant gefunden werden.

## Ermittlungs-, Bestandsaufnahme- und Statusabfrageeinstellungen nach dem Original-Setup ändern

Christian kann zur Bearbeitung der eingegebenen Einstellung zum Menü **Ermittlung und Überwachung** zurückkehren. Die neuen Einstellungen werden wirksam, wenn er das nächste Mal die entsprechende Maßnahme ausführt.

---

## Warnungsmaßnahmenfilter und Warnungsmaßnahmen für Christians großes Unternehmen erstellen

IT Assistant bietet Christian die Möglichkeit, Warnungsmaßnahmenfilter einzurichten, die eine Reihe von Systembedingungen festlegen. Wenn diese Bedingungen eintreten, kann Christian auch eine Warnungsmaßnahme im IT Assistant erstellen, die durch den Warnungsmaßnahmenfilter ausgelöst wird. Die Warnungsmaßnahme führt die Maßnahme aus, die Christian definiert hat.

IT Assistant besitzt drei Arten von Filtern:

**Warnungsmaßnahmenfilter** - werden verwendet, um Maßnahmen auszulösen, wenn eine Warnungsbedingung eintritt

**Ignorieren/Ausschließen-Filter** - werden verwendet, um SNMP-Traps und CIM-Hinweise zu ignorieren, wenn sie empfangen werden.

**Warnungsansichtsfilter** - werden verwendet, um die Warnungsprotokollansicht an die eigenen Bedürfnisse anzupassen

Bevor Christian Warnungsmaßnahmenfilter bzw. Warnungsmaßnahmen für seine Umgebung von 1 000 Servern erstellt, legt er zur Erleichterung der Ereignisbenachrichtigung zwei benutzerdefinierte Gruppen an. Gemäß dem zuvor beschriebenen Szenario befinden sich die meisten von Christians Servern in einem Datenzentrum, einige sind jedoch entfernt aufgestellt. Christian wählt diese Strategie für den IT Assistant-Setup.

Er entschließt sich:

- Eine benutzerdefinierte Gruppe für die Datenzentrumsserver sowie eine benutzerdefinierte Gruppe für die Remote-Server zu erstellen.
- Einen Warnungsmaßnahmenfilter für jeden der vier Administratoren, die Christian bei den Remote- und Datenzentrumsservern an verschiedenen Tagen und in verschiedenen Schichten unterstützen, zu erstellen.
- Eine Warnungsmaßnahme zu erstellen, die durch den entsprechenden Warnungsmaßnahmenfilter dazu veranlasst wird, automatisch eine E-Mail an den zuständigen Administrator am zutreffenden Tag und zur zutreffenden Zeit zu schicken.

## Christians Administratoren

Christian hat drei Administratoren; alle drei sind verantwortlich für den ordnungsgemäßen Betrieb der Server des Datenzentrums und arbeiten zu folgenden Zeiten:

- Thomas arbeitet im Unternehmen in der ersten Schicht Montag bis Freitag (7 bis 19 Uhr)
- Sven arbeitet im Unternehmen in der zweiten Schicht Montag bis Freitag (19 bis 7 Uhr)

- 1 Bettina hat an Wochenenden von Freitags 19 Uhr bis Montags 7 Uhr Bereitschaft

Deshalb will Christian IT Assistant so konfigurieren, dass:

- 1 Thomas, Sven und er selbst jedes Mal durch E-Mail benachrichtigt werden, wenn Warnungs- oder kritische Ereignisse bei Datenzentrumsservern eintreten
- 1 Bettina durch E-Mail benachrichtigt wird, wenn Warnungs- oder kritische Ereignisse eintreten, aber nur wenn diese während ihrer Bereitschaft eintreten

## Benutzerdefinierte Gruppen erstellen

Christian benötigt zwei benutzerdefinierte Gruppen zur Verwaltung der Benachrichtigungen seiner vier Administratoren, die bei kritischen und Warnungsereignissen seiner 1 000 Server Maßnahmen ergreifen. Bei den benutzerdefinierten Gruppen handelt es sich um Remote-Server und Datenzentrumsserver.

1. Christian wählt **Ansicht**→ **Geräte** aus der Menüleiste des IT Assistant aus.
2. Christian klickt mit der rechten Maustaste auf den Stamm der obersten Ebene in der IT Assistant-Navigationsstruktur und wählt **Neue Gruppe** aus.

Der **Assistent Gruppe hinzufügen** wird eingeblendet.

3. Christian gibt einen Namen und eine Beschreibung für die Gruppe ein, die er hinzufügen möchte.

Christian nennt seine Gruppe **Datenzentrumsserver**.

4. Im Dialog **Gruppenmitgliedschaft** kann Christian entweder die Geräte auswählen, die in der neuen Gruppe eingeschlossen sein sollen, oder, wenn es sich um eine abfragebasierte Gruppe handelt, wählt er die Abfrage aus dem Pulldown-Menü aus.
5. Christian prüft seine Auswahl im Zusammenfassungsbildschirm und klickt auf **Fertig stellen**, um den Assistenten abzuschließen.
6. Christian wiederholt die vorherigen Schritte, um eine zweite Gruppe mit dem Namen **Remote-Server** zu erstellen.

## Warnungsmaßnahmenfilter erstellen

Jetzt wird Christian einen Warnungsmaßnahmenfilter erstellen, der alle vier Administratoren einschließt, die für ihn arbeiten. Im folgenden Verfahren wird beschrieben, wie die Erstellung benutzerdefinierter Gruppen für die zwei verschiedenen Server die Erstellung von Ereignisfiltern erleichtert.

Um einen Warnungsmaßnahmenfilter zu erstellen, führt Christian folgende Schritte aus:

1. Christian wählt **Warnungen**→ **Filter** aus der Menüleiste aus.

Das Fenster **Warnungsfilter** wird eingeblendet.

2. Christian erweitert die Warnungsfilter in der Navigationsstruktur und klickt mit der rechten Maustaste auf **Warnungsmaßnahmenfilter**. Er wählt **Neuer Maßnahmenwarnungsfilter** aus.

Der **Assistent Filter hinzufügen** wird eingeblendet.

Christian plant die Erstellung von drei Ereignisfiltern, einen für jede Benachrichtigungsereignismaßnahme, die er für seine Administratoren erzeugt. Christian muss die drei Ereignisfilter nacheinander erstellen. Christian erstellt Filter für die folgenden Zeiten:

- 1 Datenzentrum erste Schicht (M-F, 7-19 Uhr)
  - 1 Datenzentrum zweite Schicht (M-F, 19-7 Uhr)
  - 1 Wochenendadministrator (19:00 Freitag bis 7:00 Montag)
- 1 Christian gibt einen beschreibenden Namen für den Filter ein.

Christian wählt **DZ 1. Schicht** als Namen für den ersten Filter. Die Namen, die er für die anderen zwei Filter wählt, sind **DZ 2. Schicht** und **Wochenende Admin**.

4. Christian wählt unter **Schweregrad** den Schweregrad der Ereignisse aus, für die er Warnungen und Protokolle empfangen möchte.



Für den Filter der 1. Schicht des DZ wählt Christian **Warnung** und **Kritisch** aus und klickt auf **Weiter**.

5. Unter **Warnungskategorie-Konfiguration** wählt Christian **Alle auswählen** aus, da er alle Server seines Unternehmens überwachen möchte, und klickt auf **Weiter**.
6. Unter **Geräte-/Gruppenkonfiguration** wählt Christian den Namen des Geräts oder der Gruppe aus, das/die dem neuen Maßnahmenwarnungsfilter zugeordnet werden sollen.

Christian wählt **Datenzentrumserver** aus, der Name einer der benutzerdefinierten Gruppen, die er zuvor erstellt hat, und klickt auf **Weiter**.

7. Unter **Datum/Uhrzeit-Bereichskonfiguration** gibt Christian Werte für einzelne oder alle optionale(n) Kategorien ein.

Christian wählt für jeden der drei Filter verschiedene Uhrzeit- und Tageswerte. Christian wählt keine Datumfilter aus, er könnte diesen Wert jedoch angeben, wenn er einen Filter und eine Maßnahme für die Urlaubszeit, für einen externen Dienstleister oder für eine andere besondere Situation erstellen möchte.

Für den DZ 1. Schichtfilter aktiviert Christian den Zeitbereich 7:00:00 Uhr bis 19:00:00 Uhr sowie die Tage Montag bis Freitag.

Für den DZ 2. Schichtfilter aktiviert Christian den Zeitbereich 19:00:00 Uhr bis 7:00:00 Uhr sowie die Tage Montag bis Freitag.

Für den **Wochenend-Admin-Filter** legt Christian zwei Filter fest (WA1 und WA2):

- 1 Für WA1 aktiviert Christian den Zeitbereich 19:00:00 Uhr bis 7:00:00 Uhr und wählt die Tage Freitag bis Montag.
- 1 Für WA2 aktiviert er den Zeitbereich 7:00:00 Uhr bis 19:00:00 Uhr und wählt die Tage Samstag und Sonntag aus.

Christian klickt auf **Weiter**.

8. Unter **Warnungsmaßnahmenverbindung** entscheidet Christian, ob das durch den Filter erfasste Ereignis eine Warnung auslösen oder zu einer Protokolldatei geschrieben werden soll.

Christian wählt **Warnung**, da er will, dass IT Assistant die ausgewählten Administratoren durch E-Mail benachrichtigt, wenn das System in einen kritischen oder einen Warnungszustand übergeht.

Klicken Sie auf **Weiter**.

9. Die **Zusammenfassung für Neuer Filter** zeigt Christians Auswahl.

Er überprüft, ob der Name des Filters, den er in [Schritt 3](#) zugewiesen hat, im Fenster **Zusammenfassung der Warnungsmaßnahmenfilter** erscheint.


Christian klickt auf **Fertig stellen**, um die Änderungen anzunehmen.

## Benachrichtigungs-Warnungsmaßnahmen in der Unternehmensumgebung

Christians Warnungsmaßnahmenfilter und -gruppen sind jetzt so konfiguriert, dass er E-Mail- und Funkrufwarnungsmaßnahmen so einrichten kann, dass er und seine drei Administratoren automatisch Benachrichtigungen erhalten. Christians Strategie lautet folgendermaßen:

- 1 IT Assistant so einrichten, dass eine E-Mail an seine Administratoren gesendet wird, wenn ein Warnungsereignis oder ein kritisches Ereignis eintritt, je nach Bereitschafts- bzw. Schichtstatus
- 1 selbst eine Kopie aller Meldungen bekommen, so dass er im Großen und Ganzen über Serverereignisse Bescheid weiß

Christian konfiguriert E-Mail sowohl für sich selbst, als auch für die Datenzentrums-Administratoren der ersten und zweiten Schicht sowie für seinen Wochenendadministrator. Deshalb wird er das folgende Verfahren viermal wiederholen - für sich selbst, für Thomas, Sven und Bettina.

 **ANMERKUNG:** Um über IT Assistant E-Mail zu senden, wechseln Sie auf der oberen Navigationsleiste zu **Einstellungen** → **Web Server** und konfigurieren den **SMTP-Servernamen** (oder die **IP-Adresse**) und das **DNS-Suffix für den SMTP-Server**.

## Warnungsmaßnahme erstellen

So wird eine Warnungsmaßnahme erstellt:


1. Christian wählt **Warnungen**→ **Maßnahmen** aus der Menüleiste aus.
2. Christian klickt mit der rechten Maustaste in der Navigationsleiste auf **Warnungsmaßnahmen** und wählt **Neue Warnungsmaßnahme** aus.

Der **Assistent Warnungsmaßnahme hinzufügen** wird eingeblendet.

3. Christian gibt der Maßnahme einen logischen Namen im Feld **Name**.

Christian konfiguriert eine **gesonderte** Warnungsmaßnahme für sich selbst, Thomas, Sven und Bettina. Jedes Mal wenn er dieses Verfahren wiederholt, verwendet er die folgenden Namen im Feld **Name**:

- 1 Christian ADMIN MGR E-Mail
  - 1 DZ 1. Schicht Thomas E-Mail
  - 1 DZ 2. Schicht Sven E-Mail
  - 1 Wochenende Admin Bettina E-Mail
- 1 Im Pulldown-Menü **Typ** wählt Christian **E-Mail** aus.
  - 1 Im Dialog **E-Mail-Konfiguration** gibt Christian eine **gültige** E-Mail-Adresse an (innerhalb der SMTP-Servergruppe Ihres Unternehmens), um die automatische Benachrichtigung zu erhalten.

 **ANMERKUNG:** Christian kann die E-Mail-Konfiguration, die er angibt, mit der Schaltfläche **Testmaßnahme** testen. Eine Erfolgs- bzw. Fehlermeldung wird ausgegeben werden. Christian kann mehrere durch Komma oder Semikolon getrennte E-Mail-Adressen festlegen.

6. In **Warnungsfilterverbindungen** legt Christian den Warnungsmaßnahmenfilter fest, der diese E-Mail auslösen wird.

Jedes Mal, wenn er diesen Schritt ausführt, gibt Christian die Namen der Warnungsfilter an, die er im vorhergehenden Verfahren eingerichtet hat - entweder **DZ 1. Schicht**, **DZ 2. Schicht** oder **Admin Wochenende**.

7. Ein Zusammenfassungs-Dialogfeld zeigt Christians Auswahl an. Er klickt auf **Fertig stellen**, um die Änderungen anzunehmen.

Er überprüft, ob die Warnungsmaßnahme, die er in [Schritt 3](#) definiert hat, im Fenster **Zusammenfassung der Warnungsmaßnahmen** erscheint.

Je nach dem, wie Christian die Warnungsmaßnahmenfilter und die Warnungsmaßnahmen in IT Assistant konfiguriert hat, passiert folgendes:

- 1 IT Assistant wird **unaufhörlich** alle Server auf Christians Netzwerk **überwachen**.
- 1 Wenn einer der Server einen Warnungszustand oder kritischen Zustand erreicht, wird IT Assistant automatisch eine E-Mail-Benachrichtigung an die E-Mail-Adresse **senden**, die Christian im **Warnungsmaßnahmen-Assistent** angegeben hat.
- 1 Wenn einer der Server einen Warnungszustand oder kritischen Zustand erreicht, wird IT Assistant automatisch eine E-Mail-Benachrichtigung an **Thomas, Sven oder Bettina** senden, je nach dem welcher Datumsbereich im **Warnungsmaßnahmenfilter-Assistent** angegeben wurde.

---

## IPMI -Ermittlung in Christians Geschäft der Unternehmensgröße verwenden


Nehmen wir an, dass Christian 100 Dell PowerEdge-x9xx-Systeme für sein Unternehmen erworben hat. Diese Systeme sind mit den **BMC** ausgestattet, die die IPMI-Versionen 1.5 oder höher unterstützen. Diese neuen Systeme sind nicht instrumentiert, d. h. es sind keine Dell-Agenten auf ihnen installiert.

IT Assistant Version 8.0 kommuniziert direkt mit dem BMC oder über den Windows-IPMI-Anbieter auf einem Windows Server 2003 R2-System. Hierbei klassifiziert er diese Systeme unter der Kategorie **Server** in der **Gerätestruktur**.

Anhand der IPMI-Ermittlungsfunktion kann Christian Folgendes tun:


- 1 Seine nicht instrumentierten Dell-Geräte **klassifizieren**
- 1 Informationen zu den nicht instrumentierten Geräten **anzeigen**
- 1 Den SOL-Proxy (Seriell über LAN) **starten**

- 1 Die IPMI-Shell (IPMISH) starten und auf den verwalteten Systemen Remote-Stromsteuerungs-Tasks ausführen


 **ANMERKUNG:** Sie sollten beim System angemeldet sein, bevor Sie es ausschalten. Microsoft Windows lässt nicht zu, dass Sie ein System ausschalten, auf dem Sie nicht angemeldet sind.

## Klassifizierung und Anzeige von Nicht-Dell-Systemen


Durch IPMI ermittelte Geräte werden unter **Bandexterne nicht klassifizierte Geräte** → **Nicht klassifizierte IPMI-Geräte** angezeigt.

 **ANMERKUNG:** Dies gilt für Nicht-Dell-Geräte.

Jedes Gerät wird in der Struktur als `<Server-Host-Name>` angezeigt.

 **ANMERKUNG:** Wenn der Host-Name nicht verfügbar ist, zeigt das Gerät die Geräte-IP-Adresse an.

Geräte der Version IPMI 1.5 unterstützen den Funktionszustand des Systems nur in begrenztem Maße, einschließlich Eingriff, Lüftern, Netzteilen und Laufwerken (nur interne Rückwandplatine). Dieser Funktionszustand ist eine gelbe oder grüne Anzeige. Geräte mit IPMI Version 2.0 unterstützen alle Funktionszustände, einschließlich normal, Warnung und kritisch.

 **ANMERKUNG:** PowerEdge x8xx-Systeme unterstützen IPMI Version 1.5, und x9xx-Systeme unterstützen IPMI Version 2.0.

## Hardwareprotokolle

Geräte unter der Gruppe **IPMI-ermittelte Geräte** haben ein Register zum Anzeigen der Hardwareprotokolle. Jedes Mal, wenn die Ansicht aktualisiert wird, wird eine Verbindung des IT Assistant-Verwaltungssystems zum Zielsystem hergestellt, um die aktuellen Protokolle abzurufen. Die Verbindung wird geschlossen, sobald alle Datensätze abgerufen wurden, um Ressourcen freizustellen und die Inanspruchnahme der Verbindung zu minimieren, da dem BMC in Bezug auf offene Verbindungen ein Limit gesetzt ist.

Das Register **Hardwareprotokolle** wird für den Protokollabruf durch alle unterstützten Protokolle verwendet.

## Start-URLs

Christian klickt mit der rechten Maustaste auf jedes Gerät unter **IPMI-ermittelte Geräte**, um auf den Start-URL für Seriell über LAN (SOL) zuzugreifen. SOL ist die einzige vorkonfigurierte Anwendung, die von der Gruppe **IPMI-ermittelte Geräte** aus gestartet werden kann.

 **ANMERKUNG:** Der Dell Remote Access Controller (DRAC) hat auch einen Telnet-Start-URL, um eine Verbindung zu DRAC herzustellen.

## IPMISH-Tasks

Christian kann IPMI-Shell-Tasks (IPMISH) auf den Geräten ausführen, die durch IPMI ermittelt wurden. Wenn er Geräte aus der Gruppe **IPMI-aktivierte Geräte** auswählt, kann er entweder `$IP` oder `$BMC_IP` verwenden.

 **ANMERKUNG:** Verwenden Sie den `-k`-Parameter auf der Befehlszeile des Baseboard-Verwaltungsdienstprogramms (BMU), um den IPMI-Verschlüsselungsschlüssel einzugeben.

## Informationen auf einem Nicht-Dell-System anzeigen

Christian kann sowohl die integrierten Protokolle auf einem Nicht-Dell-Gerät mit Windows Server 2003 R2 (mit installiertem System Management-MSI) anzeigen, als auch Informationen, die durch die Standard-Betriebssystem-Instrumentation zur Verfügung stehen.

Er hätte unter Verwendung des privilegierten Administrator-Benutzerkontos für CIM-Ermittlung die CIM-Ermittlung für den dem Gerät entsprechenden Einschussbereich aktivieren sollen.

 **ANMERKUNG:** Auf Nicht-Administrator-Benutzerkonten wird der Hardwareverwaltungsagent nicht ermittelt.

Klicken Sie in der Gerätestruktur auf ein Gerät, um Geräteinformationen anzuzeigen. Das Register Hardwareprotokolle enthält Informationen, die sich auf die integrierten Protokolle beziehen.

Das Register Gerätezusammenfassung enthält Informationen, die durch die Standardinstrumentation des Betriebssystems abgerufen werden. Diese Daten enthalten Informationen zu NIC, Betriebssystem, BIOS, Kontakt, Speicher und Prozessor. Das Gerät wird unter der Kategorie **Unbekannt** aufgeführt, da über die Standardinstrumentation des Betriebssystems keine Informationen zu Gerätetypen zur Verfügung stehen.

---

## Zusammenfassung

In diesem Kapitel wurden die IT Assistant-Konfigurationen für kleine bis mittelgroße Betriebe sowie für große Unternehmensnetzwerkumgebungen behandelt. Folgen Sie den hier gezeigten Beispielen, um IT Assistant mit größtmöglichem Erfolg zu konfigurieren.

Weit mehr Funktionen als die hier dargestellten stehen im IT Assistant zur Verfügung. Klicken Sie auf die Schaltfläche **Hilfe** im entsprechenden IT Assistant-Dialogfeld, um ausführliche Online-Hilfe zu dieser Funktion zu erhalten.

---

[Zurück zum Inhaltsverzeichnis](#)

## Häufig gestellte Fragen

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Zum IT Assistant häufig gestellte Fragen](#)
- [Umfang und Fähigkeiten von IT Assistant](#)
- [IT Assistant-Benutzeroberfläche](#)
- [Warnungsverwaltung](#)
- [IT Assistant-Dienste](#)
- [IT Assistant-Ermittlung](#)
- [Leistungsüberwachung](#)
- [Support für IPMI-Ermittlung](#)
- [Verschiedenes](#)

### Zum IT Assistant häufig gestellte Fragen

Die folgende Tabelle führt häufig gestellte Fragen und Antworten auf.

Frage	Antwort
Welche UDP/TCP-Schnittstellen (Protokoll für Benutzerdatagramme/Übertragungssteuerungsprotokoll) verwendet IT Assistant?	Siehe "Von IT Assistant verwendete Schnittstellen und assoziierte Agenten-Anwendung" im <i>Dell OpenManage-Sicherheits- und Installationshandbuch</i> .
Ich habe gerade eine Systemaktualisierung durchgeführt; warum kann ich die aktualisierte Version nicht in der IT Assistant-Bestandsaufnahme sehen?	Alle vom IT Assistant in der Systemliste angezeigten Daten werden im Daten-Repository gespeichert, das immer während des Bestandsaufnahmezyklus aktualisiert wird. Wenn eine Aktualisierung durchgeführt wird, meldet IT Assistant die Änderung nach dem nächsten Bestandsaufnahmezyklus. Zur Aktualisierung der Bestandsaufnahme des Gerätes vor dem nächsten geplanten Bestandsaufnahmezyklus klicken Sie mit der rechten Maustaste auf das Gerät mit der veralteten Version in der <b>Gerätestruktur</b> -Ansicht und klicken Sie auf <b>Bestandsaufnahme aktualisieren</b> .  <b>ANMERKUNG:</b> Es kann eventuell einige Minuten dauern, bis die Bestandsaufnahme die aktualisierte Version anzeigt. Es wird daher empfohlen, 5 - 10 Minuten vor der Anforderung einer Bestandsaufnahme des Geräts zu warten.
Ich habe gerade ein System heruntergefahren. Warum wird es von IT Assistant immer noch als aktiv angezeigt?	IT Assistant aktualisiert den Status Hochgefahren/Heruntergefahren eines Systems nur während einer Statusabfrage bzw. Ermittlung des Systems oder wenn IT Assistant ein Ereignis vom System empfängt.
Warum kann ich auf der IT Assistant-Benutzeroberfläche (UI) die Statusaktualisierung eines Geräts nicht sehen?	Falls IT Assistant feststellt, dass der globale Status eines Geräts bei einer geplanten Statusabfrage NICHT geändert wurde, wird er keine Meldung zur Benutzeroberfläche senden. IT Assistant wird auch dann keine Meldung zur Benutzeroberfläche senden, wenn der Status nach einem eingehenden Ereignis für dieses Gerät geprüft wird. Dieses Verhalten wird zum optimalen Einsatz der Ressourcen angewendet sowie zur Erhöhung der Verarbeitungsgeschwindigkeit der anderen Meldungen, die dem Benutzer gesendet werden.  Falls Sie zur gleichen Zeit die Gerätezusammenfassung oder die Gerätedetails ansehen, werden die Informationen zur letzten Statuszeit bzw. zum individuellen Agentenstatus nicht automatisch aktualisiert werden. Aktualisieren Sie die Ansicht oder klicken Sie auf ein anderes Gerät, um die neuesten Informationen automatisch von der Datenbank zu laden.
Woher weiß ich, wann IT Assistant die Ermittlung von Systemen abgeschlossen hat?	IT Assistant bietet Ermittlungszyklus-Fortschrittsinformationen. In der IT Assistant-Benutzeroberfläche wechseln Sie zu <b>Ermittlung und Überwachung</b> → <b>Protokolle</b> . Siehe auch "Ermittlungs- und Überwachungsprotokolle - Ermittlungsprobleme lösen" in der <i>Dell OpenManage IT Assistant-Onlinehilfe</i> .
Ich habe eine Meldung erhalten, die besagt, dass IT Assistant nicht mit dem Remote-Gerät kommunizieren kann. Was verursacht dieses Problem?	IT Assistant konnte keine Verbindung zum Remote-Agenten oder dem Gerät herstellen. Verwenden Sie das Fehlerbehebungshilfsprogramm, um das Problem mit den Tests Ping-, CIM- und SNMP-Konnektivität sowie dem Namensauflösungstest zu lösen. In der IT Assistant-Benutzeroberfläche wechseln Sie zu <b>Hilfsprogramme</b> → <b>Fehlerbehebungshilfsprogramm</b> . Siehe "Fehlerbehebungshilfsprogramme - Ermittlungsprobleme auffindig machen und lösen" in der <i>Dell OpenManage IT Assistant-Onlinehilfe</i> .
Warum erhalte ich eine Fehlermeldung, wenn ich Anwendungen durch Klicken mit der rechten Maustaste auf die <b>Gerätestruktur</b> starte?	Bestimmte Anwendungen (z. B. Dell OpenManage Server Administrator Storage Management-Dienste und Digital-KVM-Konsole) müssen auf dem System, auf dem die IT Assistant-Benutzeroberfläche ausgeführt wird, installiert sein, bevor sie von IT Assistant aus gestartet werden können.
Warum erhalte ich die Ausnahme Nicht genügend Speicher für Java vorhanden?	Wenn Sie eine Umgebung mit mehr als 2000 Geräten verwalten, vergrößern Sie die dem JRE-Heap (Java-Laufzeitumgebung) zugewiesene Speichergröße.  <b>ANMERKUNG:</b> Der Speicher sollte auf dem System vergrößert werden, von dem aus sie auf die IT Assistant Management Station zugreifen.  Dazu schließen Sie die IT Assistant-Browser-Sitzung und wechseln zur Java-Systemsteuerung. Das Feld befindet sich unter der Microsoft® Windows®-Systemsteuerung oder der ausführbaren Datei ControlPanel im bin-Ordner der JRE-Installation auf dem Linux-System.  Klicken Sie auf das Register Java und im Abschnitt Java-Applet-Laufzeit auf Anzeigen... Klicken Sie an eine beliebige Stelle im Java-Laufzeitparameter-Bereich und geben Sie

	ein:  -Xmx256M
Warum erhalte ich eine Host-Namenswarnung bzgl. einer fehlerhaften Übereinstimmung, wenn ich versuche, auf die Benutzeroberfläche von IT Assistant zuzugreifen?	Diese Warnung wird eingeblendet, wenn der Host-Name der Webadresse, die Sie verwendet haben, um die Verbindung zu IT Assistant herzustellen, und der zur Installation von IT Assistant verwendete Host-Name nicht übereinstimmen. Wenn Sie z. B. IT Assistant mit dem Host-Namen <b>sysadmin3</b> und der IP-Adresse <b>133.143.157.30</b> installiert haben, wird die Warnung eingeblendet, wenn Sie sich bei IT Assistant mit der IP-Adresse anmelden. Wenn Sie sich jedoch mit dem Systemnamen <b>sysadmin3</b> am Remote-Gerät anmelden, wird die Warnung nicht eingeblendet.
Warum erhalte ich keine Anmeldungsaufforderung, wenn ich mich von einem Desktop aus bei IT Assistant anmelde?	IT Assistant verwendet die Betriebssystem-Anmeldeinformationen des zurzeit angemeldeten Benutzers und meldet Sie automatisch bei IT Assistant an. Zusätzliche Informationen dazu finden Sie im Abschnitt über die Einmalige Anmeldung im <i>IT Assistant-Benutzerhandbuch</i> .
Warum schlägt die Windows NT@ LAN Manager-Authentifizierung (NTLM) fehl, wenn ich versuche, mich bei IT Assistant anzumelden?	Stellen Sie sicher, dass die Einmalige Anmeldung im Internet Explorer-Browser aktiviert ist.  Starten Sie den Internet Explorer, um die Einmalige Anmeldung zu aktivieren. Klicken Sie auf das Register <b>Extras</b> → <b>Internetoptionen</b> → <b>Sicherheit</b> . Wählen Sie <b>Vertrauenswürdige Sites</b> . (Das IT Assistant-System wird durch diese Sicherheitszone abgedeckt.)  Klicken Sie auf Stufe anpassen. Scrollen Sie nach unten zu Benutzerauthentifizierung, und wählen Sie <b>Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort</b> aus.
Wie kann ich Java-Zwischenspeichern deaktivieren?	Um Java-Zwischenspeicherung auf einem Windows-System zu deaktivieren, wechseln Sie zur <b>Windows-Systemsteuerung</b> , klicken Sie auf das <b>Java</b> -Symbol, um das <b>Java-Bedienungsfeld</b> anzuzeigen und stellen Sie sicher, dass das Kontrollkästchen <b>Zwischenspeicherung aktivieren</b> im Dialogfeld <b>Java Applet Cache Viewer</b> nicht ausgewählt ist.  Um die Zwischenspeicherung auf einem Linux-System zu deaktivieren, führen Sie die ausführbare Datei <b>ControlPanel</b> im <b>bin-Ordner</b> der JRE-Installation auf dem Linux-System aus, und stellen Sie sicher, dass das Kontrollkästchen <b>Zwischenspeicherung aktivieren</b> im Dialogfeld des <b>Java Applet Cache Viewer</b> nicht ausgewählt ist.
Welche Vorkehrungen muss ich treffen, wenn ich auf eine ältere Version von IT Assistant zurückgreife?	Wenn auf den Systemen, von denen Sie auf die IT Assistant-Benutzeroberfläche zugegriffen haben, Java-Applet-Zwischenspeicherung aktiviert ist, löschen Sie die von IT Assistant verwendeten jar-Dateien vom jeweiligen Cache der einzelnen Systeme. Wechseln Sie zu <b>Java Bedienungsfeld</b> , und klicken Sie unter <b>Temporary Internet Files</b> auf <b>Einstellungen</b> . Dieses Fenster befindet sich unter der Microsoft Windows-Systemsteuerung oder der Linux-Systemsteuerung im Ordner <b>bin</b> . Klicken Sie auf <b>Applets anzeigen</b> . Wählen Sie die zwischengespeicherten Dateien aus, und klicken Sie auf <b>Löschen</b> .  <b>ANMERKUNG:</b> Ein Nichtlöschen des Java-Applet-Cache führt eventuell zu inkonsistentem Verhalten der älteren IT Assistant-Version.

## Umfang und Fähigkeiten von IT Assistant

Diese häufig gestellten Fragen befassen sich mit den allgemeinen Fähigkeiten von IT Assistant, der Optimierung der Benutzeroberflächenumgebung und der Ermittlungskonfiguration.

Frage	Antwort
Warum zeigt IT Assistant an, dass das ermittelte System während einer Statusabfrage nicht betriebsbereit ist, obwohl es betriebsbereit ist?	Auf Netzwerken, auf denen das Dynamische Host-Konfigurationsprotokoll (DHCP) durchgeführt wird, kann IT Assistant ein System als nicht betriebsbereit anzeigen wenn es in Wirklichkeit betriebsbereit ist, wenn ein anderes System dessen IP-Adresse erhalten hat. Während eines Ermittlungszyklus, wenn IT Assistant ein bestimmtes verwaltetes System ermittelt, sucht IT Assistant in seiner Datenbank nach anderen Systemen, deren IP-Adresse die gleiche ist, wie die des Systems unter Ermittlung. Wenn ein anderes System die gleiche Adresse besitzt, wird dessen IP-Adresse als ungültig markiert. Wenn das System, dessen IP-Adresse als ungültig markiert wurde, schließlich neu ermittelt wird, werden dessen IP-Adresseinträge aktualisiert und wieder als gültig markiert. Bis diese IP-Adresseinträge aktualisiert sind, zeigt jede durchgeführte Statusabfrage das System als nicht-betriebsbereit an, da es keine gültigen IP-Adresseinträge besitzt, die geprüft werden könnten.
Warum zeigt IT Assistant mein System nicht als aktiv, nachdem ich den Namen geändert habe?	Wenn IT Assistant während eines Ermittlungszyklus ein bestimmtes verwaltetes System durch die IP-Adresse ermittelt, versucht er die Adresse des verwalteten Systems auf einen Namen aufzulösen, entweder durch Instrumentation oder durch DNS. Wenn DNS die bevorzugte Namensauflösungsmethode ist und der Name des zu ermittelnden verwalteten Systems vor kurzer Zeit geändert wurde, kann es eventuell mehrere Ermittlungszyklen dauern, bis der Name im IT Assistant aktualisiert wird, da Windows DNS-Einträge im Cache-Speicher des lokalen Systems ablegt sind. Weitere Informationen zur schnelleren Leerung des Cache finden Sie in der Microsoft-Dokumentation Ihres Betriebssystems.
Warum kann ich mein Desktop-System nicht ermitteln?	Lösen Sie dieses Problem mithilfe des Fehlerbehebungshilfsprogramms von IT Assistant. In der Benutzeroberfläche wechseln Sie zu <b>Hilfsprogramme</b> → <b>Fehlerbehebungshilfsprogramm</b> . Siehe "Fehlerbehebungshilfsprogramm - Ermittlungsprobleme ausfindig machen und lösen" in der <i>Dell OpenManage IT Assistant-Onlinehilfe</i> .
Verwaltet IT Assistant nur Dell Systeme?	Ja. IT Assistant verwaltet nur Dell-Systeme, auf denen Dell-Instrumentation installiert ist und ausgeführt wird. Beginnend mit IT Assistant 8.0 können Geräte, die mit IPMI 1.5 oder höher konfiguriert sind, jedoch auch mit IT Assistant ermittelt werden.
Muss IT Assistant auf einem Dell System installiert werden?	Nein. Obwohl IT Assistant für die Installation auf Dell Systemen getestet wurde, ist die IT Assistant-Benutzeroberfläche für den Betrieb auf Systemen entwickelt, die unterstützte Betriebssysteme ausführen. Daher sollte IT Assistant problemlos auf Nicht-Dell-Systemen funktionieren, auf denen diese Betriebssysteme ausgeführt werden und die den Mindest-Hardwarespezifikationen entsprechen.  Weitere Details finden Sie unter " <a href="#">Installationsplan für Dell OpenManage™ IT Assistant</a> ".

	Dell bietet jedoch keine Garantie und keinen kostenlosen Support für Systeme, die nicht von Dell sind.
Wie viele Benutzer können IT Assistant gleichzeitig ausführen?	Mehrere Benutzer können IT Assistant ausführen, um eine Verbindung mit den IT Assistant-Diensten herzustellen. Die Anzahl der Benutzer wird durch die Anzahl der verfügbaren Ressourcen auf der Verwaltungsstation begrenzt.
Kann IT Assistant zusätzlich zu Client Administrator installiert werden?	Client Administrator-Konfiguration wird zurzeit nicht auf demselben System wie IT Assistant unterstützt.
Wie viele Systeme können verwaltet werden?	IT Assistant ist so ausgelegt und getestet, dass er bis zu mehreren tausend Systemen auf einem entsprechend konfigurierten System <i>verwalten</i> kann.  <b>ANMERKUNG:</b> CPU-intensive Tasks wie z. B. Leistungsüberwachung können jedoch nur auf 100 Systemen ausgeführt werden, und Softwarebereitstellung kann nur auf etwa 20 Systemen gleichzeitig versucht werden.
Kann IT Assistant über das Internet verwendet werden?	IT Assistant ist ein LAN (Lokales Netzwerk) -orientiertes Hilfsprogramm zum Überwachen und Verwalten von Systemen in einem IP-Netzwerk. Sie können mit dem IT Assistant Systeme über das Internet überwachen und verwalten; Dell empfiehlt dies jedoch nur dann, wenn Sie selbst Ihre Daten sichern können. Der IT Assistant bietet Sicherheitsfunktionen, die zur Verwendung in einem Firmennetzwerk geeignet sind.

## IT Assistant-Benutzeroberfläche

Frage	Antwort
Ich weiß, dass die IT Assistant-Benutzeroberfläche so eingestellt ist, dass ich nach einer Leerlaufzeit von 30 Minuten automatisch abgemeldet werde. Warum kann ich dann weiterhin Menüs und Ansichten ändern, wenn ich länger als 30 Minuten bei IT Assistant angemeldet bin?	IT Assistant speichert einige Daten und bestätigt die Zeitüberschreitung nur, wenn die Sammlung neuer Daten erforderlich ist.
Warum sind nicht alle Warnungen auf dem Register <b>Warnungen</b> sichtbar?	Die Benutzeroberfläche von IT Assistant zeigt Warnungen in der <b>Warnungsprotokoll</b> -Ansicht an. Durch Auswahl von <b>Alle Warnungen</b> im Drop-Down-Menü <b>Filter</b> können Sie festlegen, dass Sie alle Warnungen anzeigen möchten. Siehe "Warnungsprotokolle - mit Warnungen arbeiten" in der <i>Dell OpenManage IT Assistant-Onlinehilfe</i> .
Warum wird der Stromzustand für ein heruntergefahrenes System in IT Assistant nicht als heruntergefahren angezeigt?	Der Stromzustand ist abhängig von der letzten Statusabfrage, die wiederum vom Statusabfrageintervall abhängig ist. Der Stromzustand wird aktualisiert, wenn die nächste Statusabfrage stattfindet.
Was mache ich, wenn sich das System nicht aktivieren lässt?	Zur Aktivierung dieses Geräts verwendet IT Assistant die MAC-Adressen und Subnetzmasken, die für das Gerät ermittelt wurden. Wenn das Gerät für NIC-Teaming konfiguriert wurde, wird nur ein MAC vom Betriebssystem angekündigt. Wake-on-LAN (WOL) funktioniert nur, wenn es für alle NICs in diesem Team aktiviert wurde.  Damit ein WOL-Paket sein beabsichtigtes Ziel erreicht, muss auf den Zwischen-Routern gezieltes Broadcasting (auch als Subnetz-Broadcasting bezeichnet) aktiviert sein. Direkt-Broadcasting ist meistens auf den Routern deaktiviert. Deshalb ist es notwendig, diese Funktion auf dem Router zur Aktivierung zu konfigurieren.
Warum werden in der <b>Warnungsprotokoll</b> -Ansicht keine neuen Warnungen angezeigt?	Zur Anzeige neuer Warnungen klicken Sie im <b>Warnungsprotokoll</b> fenster auf <b>Neue Warnungen zeigen</b> .
Warum sehe ich keine detaillierte Beschreibung meines Netzwerkadapter-Herstellers auf der Seite <b>Gerät-Details - Zusammenfassung</b> des IT Assistant?	Aufgrund der Einführung von MIB2 auf Red Hat Linux, hat der Abschnitt <b>Netzwerk</b> der Seite <b>Gerät-Details - Zusammenfassung</b> des IT Assistant keine detaillierte Beschreibung des Netzwerkadapter-Herstellers. "eth0" oder eine ähnliche Zeichenkette erscheint z. B. unter <b>Produktname</b> .
Warum wird die IP-Adresse auf der Seite NIC-Informationen in der falschen Reihe angezeigt?	Dieses Problem wurde durch ein Red Hat-Patch für das net-snmp-Paket gelöst.
Wenn ich meinen Report in das CSV-Format exportiere, zeigt Excel den Report nicht in einer korrekten Ansicht an. Wie kann das Problem gelöst werden?	Das Reportsystem erstellt alle Ausgaben im Unicode-Format ( <a href="http://www.unicode.org">www.unicode.org</a> ). Zum Öffnen der CSV-Reporte starten Sie Microsoft Excel und führen den Befehl <b>Datei   Öffnen</b> aus, der den Import-Assistenten aufruft. Wählen Sie die Option <b>Komma getrennt</b> , um den Report so zu öffnen, dass die Daten in den korrekten Spalten sind.
Warum erhalte ich einen Registrierungsfehler, wenn ich versuche, die IT Assistant-Benutzeroberfläche zu öffnen?	Ein Fehler des Registrierungs-Editors tritt auf, wenn die IT Assistant-Benutzeroberfläche auf einem System geöffnet wird, das nicht genügend Speicherplatz hat. Der IT Assistant-Client benötigt 25 MB verfügbaren Festplattenspeicher.

## Warnungsverwaltung

Frage	Antwort
Warum ist das Warnungsprotokoll eines verwalteten Systems leer, wenn ich Warnungen erhalte und diese in der <b>Warnungsprotokoll</b> -Ansicht angezeigt werden?	Wenn IT Assistant ein Ereignis mit einer in dem Ereignis gespeicherten IP-Adresse erhält, löst er das Ereignis in einen entsprechenden Namen auf, mithilfe der Datenbank der ermittelten Systeme des IT Assistant (wenn <b>Instrumentationsnamensauflösung bevorzugt wird</b> ) oder mithilfe von DNS (wenn <b>DNS-Auflösung bevorzugt wird</b> ). SNMP-Traps und CIM-Angaben besitzen immer eine IP-Adresse zur Auflösung.  Wenn die IP-Adresse bereits in einen Namen aufgelöst wurde, versucht IT Assistant nicht, sie noch einmal aufzulösen. Diese Maßnahme könnte zu Unterschieden zwischen dem im Ereignis gespeicherten Namen und dem Namen führen, mit dem IT Assistant das System ermittelte und das Ereignis sendete, wenn

	<p>Instrumentationsnamensauflösung im IT Assistant bevorzugt wurde. Dieses Problem könnte dazu führen, dass Ereignismaßnahmen nicht durchgeführt werden, wenn die Auswahl von Systemnamen im Erstellungs-Dialogfeld Ereignisfilter, die nicht mit dem im Ereignis enthaltenen Namen übereinstimmt.</p> <p>Außerdem kann es sein, das im IT Assistant nicht alle von diesem System empfangenen Ereignisse in der <b>Warnungen</b>-Ansicht des Systems angezeigt werden. Um dieses Verhalten zu vermeiden, wird empfohlen, die DNS-Auflösung dann als <b>bevorzugte Auflösung</b> im IT Assistant auszuwählen, wenn DNS oder WINS in der Netzwerkumgebung, in der IT Assistant Ermittlungen ausführt, vorhanden sind.</p>
--	---

## IT Assistant-Dienste

Frage	Antwort
Wie löst der IT Assistant die Namen ermittelter Systeme auf?	Siehe "Namensauflösung" in der <a href="#">Dell OpenManage IT Assistant-Onlinehilfe</a> .
Warum dauert das Anmeldeverfahren nach einem Neustart des Systems so lange? Verursachen die IT Assistant-Dienste diese Leistungsprobleme?	Stellen Sie sicher, dass Ihr System die minimalen Systemanforderungen erfüllt, wie unter <a href="#">"Installationsplan für Dell OpenManage™ IT Assistant"</a> beschrieben.
Warum sieht es so aus, als ob das SQL Server-Verfahren eine große Menge des Speichers der Verwaltungsstation verbraucht, wenn der Speicherverbrauch vom Task-Manager aus angesehen wird?	Der Task-Manager berichtet eventuell nicht die tatsächlich verbrauchte Speichermenge. Zur besseren Einschätzung des Speicherverbrauchs des SQL-Servers wechseln Sie zu <a href="http://www.microsoft.com">www.microsoft.com</a> und suchen Sie nach dem Knowledge Base-Artikel KB321363, der beschreibt, wie SQL-Server Speicher verbrauchen und freigeben.

## IT Assistant-Ermittlung

Frage	Antwort
Ich habe ein System ermittelt, das CIM-Anzeigen unterstützt. In der Vergangenheit konnte ich Anzeigen vom System empfangen, jetzt kann ich sie nicht mehr über den IT Assistant empfangen. Die Anzeigen sehe ich lokal auf dem verwalteten System.	Damit CIM-Anzeigen an die Verwaltungsstation gesendet werden können, muss die Verwaltungsstation bei dem verwalteten System registriert werden. Die Registrierung wird jedes Mal unterbrochen, wenn die Verwaltungsstation oder das verwaltete System neu gestartet werden. Wenn IT Assistant ein System ermittelt, wird das System beim CIM-Anzeigeanbieter registriert. Nach einem Neustart des verwalteten Systems, registriert der IT Assistant es erst beim nächsten Ermittlungszyklus. So erzwingen Sie eine Neuregistrierung beim Anzeigeanbieter: Erzwingen Sie eine Ermittlung des verwalteten Systems in IT Assistant, indem Sie mit der rechten Maustaste in der <b>Gerätestruktur</b> -Ansicht auf das System und dann auf <b>Status aktualisieren</b> klicken.
Wie kann ich CIM-Benutzernamen qualifizieren?	CIM ist nur durch den Ermittlungsbereich aktiviert/deaktiviert und setzt voraus, dass jeder CIM-Benutzer durch eine Domäne oder einen lokalen Host qualifiziert ist, wenn keine vertrauenswürdige Domäne konfiguriert wurde.  Es ist sehr wichtig, dass diese Qualifizierung vorliegt, wenn CIM durch einen Ermittlungsbereich (z. B. <Domäne>\<Benutzername> oder localhost\<Benutzername>) zur Authentifizierung und Verwendung des CIM-Protokolls konfiguriert werden soll.  Nehmen Sie von IT Assistant Version 6.x ein Upgrade zu Version 7.x vor, indem Sie Ihren Benutzernamen durch die Bearbeitung der Ermittlungsbereiche korrekt qualifizieren.
Wie bestimmt die IT Assistant-Benutzeroberfläche die angezeigten Uhrzeiten?	Datum und Uhrzeit werden gemäß der auf der Verwaltungsstation konfigurierten Zeitzone ausgegeben.
Warum kann IT Assistant keine Systeme auf dem konfigurierten Ermittlungsbereich ermitteln?	Lösen Sie dieses Problem mithilfe des Fehlerbehebungshilfsprogramms von IT Assistant. In der Benutzeroberfläche wechseln Sie zu <b>Hilfsprogramme -&gt; Fehlerbehebungshilfsprogramm</b> . Siehe auch "Fehlerbehebungshilfsprogramm - Ermittlungsprobleme ausfindig machen und lösen" in der <a href="#">Dell OpenManage IT Assistant-Onlinehilfe</a> .
Warum meldet IT Assistant einige Attributwerte als nicht angegebene bzw. leere Werte?	IT Assistant wird nicht angegebene bzw. leere Datenwerte für die Attribute zeigen, die vom Agenten abgefragt, jedoch nicht von ihm zurückgegeben wurden. Diese nicht angegebenen Felder sind eventuell ein Zeichen dafür, dass die Funktion vom Gerät nicht unterstützt wird bzw. vom Geräte-Agenten nicht berichtet wird, oder dass die Funktion durch die aktuelle Gerätekonfiguration deaktiviert wird. Zusätzlich können nicht angegebene Werte auch ein Zeichen für leere Felder sein, die vom Agenten zurückgegeben wurden.
Über welche Schnittstellen kommunizieren die IT Assistant-Dienste? Wie können die Schnittstellenzuweisungen geändert werden?	Schnittstelle 2607 ermöglicht die Kommunikation zwischen der IT Assistant-Benutzeroberfläche und dem IT Assistant-Verbindungsdienst. Schnittstelle 2606 ermöglicht die Kommunikation zwischen dem IT Assistant-Verbindungsdienst und dem Netzwerküberwachungsdienst des IT Assistant. Sie können diese Schnittstellenzuweisungen bei der Installation des IT Assistant ändern, indem Sie benutzerdefinierte Einstellungen verwenden. Wenn Sie die Schnittstellenzuweisungen während der benutzerdefinierten Installation nicht ändern, können die Schnittstellennummern nur über die Registrierung neu zugewiesen werden. Siehe auch "Von IT Assistant verwendete Schnittstellen und assoziierte Agenten-Anwendung" im <a href="#">Dell OpenManage-Sicherheits- und Installationshandbuch</a> .
Wenn ich mehrere Protokolle an eine Netzwerkkarte gebunden habe, zeigt der IT Assistant im Register Zusammenfassung des Fensters Systeme unter Netzwerkdaten mehrere Einträge für diese Netzwerkkarte an. Dies führt dazu, dass ich annehme, ich hätte mehr Netzwerkkarten als tatsächlich im System installiert sind. Warum zeigt der IT Assistant diese mehrfachen Einträge an?	Diese Situation tritt vor allem dann ein, wenn die Kommunikation mit dem verwalteten System ausschließlich über SNMP erfolgt. Die Mehrheit der angezeigten Zusammenfassungen-Informationen werden aus den Tabellen innerhalb der entsprechenden MIB-Datei entnommen. In diesem Fall werden Netzwerkinformationen aus der Tabelle MIB2 Interfaces bezogen. Durch die Bindung mehrerer Protokolle an eine einzelne Netzwerkkarte wird für jedes Protokoll eine Zeile zur Schnittstellentabelle der MIB-Datei hinzugefügt. Der IT Assistant zieht dann alle Zeilen aus dieser Tabelle. Da nur eine physische Adresse pro Netzwerkkarte vorhanden ist, können Sie über die physische Medienzugriffssteuerung (MAC) -Adresse feststellen, wie viele Netzwerkkarten tatsächlich installiert sind.
Warum erzeugt DCOM Ereignisprotokollmeldungen, wenn	Hierbei handelt es sich um ein bekanntes Problem mit der Microsoft WBEM-Implementierung.



keine Kommunikation mit den verwalteten Systemen aufgebaut werden kann?	DCOM protokolliert jedes Mal einen Fehler, wenn keine Remote-Verbindung aufgebaut werden kann. Bei aktiviertem CIM versucht IT Assistant, eine Verbindung zu jedem CIM-Agent herzustellen, dessen Adresse mit dem Befehl <b>ping</b> erreicht werden kann. Wenn Benutzername und -kennwort nicht funktionieren oder wenn kein CIM-Agent vorhanden ist, fügt DCOM eine Fehlermeldung zum Ereignisprotokoll hinzu.
Warum sind IT Assistant-Dienste auf meinem Windows 2000-System nicht stabil?	IT Assistant-Dienste können Instabilität auf Systemen mit Windows 2000 SP3 zeigen. Lesen Sie dazu den Microsoft Knowledge Base-Artikel 813648: "Random Access Violations When Multithreaded Applications Call the setlocale Function" (Random Access-Verletzungen, wenn Multithread-Anwendungen die Funktion setlocale aufrufen).
Warum tritt eine Verzögerung bei der Anzeige des Ermittlungs-Feedbacks im Fenster <b>Ermittlungs- und Überwachungsprotokolle</b> auf?	Wenn ein Ermittlungs-Task bereits ausgeführt wird während ein anderer Ermittlungsbereich eingegeben wird, kann es sein, dass der neue Bereich eventuell nicht sofort im Fenster <b>Ermittlungs- und Überwachungsprotokolle</b> angezeigt wird. Dieses Verhalten ist auch von der Anzahl der Systeme abhängig, die ermittelt werden.
Warum hängt die Ermittlung bei meiner CIM-aktivierten IT Assistant-Installation?	Wenn IT Assistant CIM aktiviert hat und die Ermittlung von verwalteten Systemen, die für CIM konfiguriert sind, mit Dell OpenManage Server Agent Version 4.4 oder früher durchgeführt, kann die Ermittlung hängen. Sie müssen die Instrumentation für diese Systeme aktualisieren. Wechseln Sie in der IT Assistant-Benutzeroberfläche zu <b>Ermittlung und Überwachung</b> → <b>Ermittlungskonfiguration</b> , um dieses Problem zu lösen. Siehe "Ermittlungskonfiguration - IT Assistant zum Ermitteln neuer Geräte konfigurieren" in der <i>Dell OpenManage IT Assistant-Onlinehilfe</i> .
Der gesamte reservierte Speicher im IT Assistant-Netzwerküberwachungsdienst wird nicht freigegeben. Was verursachte das Problem?	Wenn IT Assistant auf einem Gerät installiert ist, das Windows 2000 SP4 ausführt, verursacht ein bekanntes Problem mit dem Microsoft WMI API, dass bei Verwendung des CIM-Protokolls nicht der gesamte reservierte Speicher im IT Assistant-Netzwerküberwachungsdienst freigegeben wird. Das Leck tritt auf, wenn das Remote-Gerät falsche Authentifizierungs-Anmeldeinformationen während eines Ermittlungszyklus oder einer Statusabfrage erhält.
Warum kann ich mein ERA/MC-Gerät nicht ermitteln?	Bevor Sie den ERA/MC ermitteln können, muss er richtig konfiguriert sein. (Konfigurationsinformationen finden Sie in der ERA/MC-Dokumentation.) Nach Konfiguration des ERA/MC, sollten Sie sicherstellen, dass die dem Gerät zugeteilte IP-Adresse im IT Assistant-Ermittlungsbereich eingeschlossen ist.
Warum wird im Gerätestatus <b>Unbekannt</b> angezeigt, wenn ich ihn anhand der SNMP- und CIM-Protokoll-Kombinationen zu ermitteln versuche?	Verschiedene Bereiche werden von IT Assistant nicht gleichzeitig ermittelt, und ein Bereich wird von einem anderen überschrieben werden. Geben Sie zur Geräteermittlung konsistente Anmeldeinformationen an. Wenn Sie z. B. SNMP und CIM für den ersten Bereich mit bestimmten Anmeldeinformationen aktiviert haben, geben Sie dieselben SNMP- und CIM-Anmeldeinformationen für den zweiten Bereich bzgl. des zu ermittelnden Geräts ein.
Ich habe durch Bestimmen der IP-Adresse im Bereich ein Gerät ermittelt. Das System wurde neu gestartet und erhielt eine neue IP-Adresse. Warum zeigt der Status das System als ausgeschaltet an, obwohl sich die IP-Adresse im Bereich befindet?	IT Assistant verwendet die bereitgestellte IP-Adresse nur während der Ermittlung aller Vorgänge wie z. B. Status, Fehlerbehebung, Tasks usw.. Wenn die zur Ermittlung verwendeten IP-Adressen nicht verfügbar sind oder sich geändert haben (aufgrund der Neuuzuordnung des Dynamischen Host-Konfigurationsprotokolls), zeigt der Status das System als ausgeschaltet an.  Ermitteln Sie das Gerät nochmals von dem Bereich aus, der die aktualisierte IP-Adresse des Geräts enthält.

## Leistungsüberwachung

Frage	Antwort
Ich habe meine Leistungsüberwachungs-Tasks mit einem Intervall von zwei Minuten geplant. Der Task holt jedoch nicht alle Proben zu gleichen Intervallen ein.	Die Verzögerung beim Einholen von Proben kann auf verschiedenen Gründen beruhen, wie z. B. niedriger Speicher oder hoher Prozessorgebrauch auf der IT Assistant-Verwaltungsstation.
Ich bin nicht in der Lage, die Informationen über das Speicherattribut im Fenster der Ausführungsergebnisse des Tasks zu sehen.	Wenn ein Attribut auf dem Remote-Gerät (verwalteten System) nicht unterstützt ist, werden Attributinformationen im Task-Fenster <b>Ausführungsergebnisse</b> und im Register <b>Leistung</b> in der <b>Geräte</b> -Ansicht nicht angezeigt. Außerdem ist zu beachten, dass dieses Attribut für Statusberechnungen nicht in Betracht gezogen wird.
Ich habe den Windows Management Interface-Dienst (WMI) angehalten. Warum sehe ich, wenn ich diesen Dienst neu starte, die Meldung "Verbindung zum Gerät kann anhand von CIM/SSH nicht hergestellt werden"?	Hierbei handelt es sich um eine normale Situation. Die Datenerfassung wird nach fünfzehn bis dreißig Minuten beginnen, da die Verbindungen einmal alle fünfzehn Minuten freigegeben werden.

## Support für IPMI-Ermittlung

Frage	Antwort
Ich habe die IP-Adresse meines Systems sowie die Anmeldeinformationen für die Ermittlung der Verwaltungsschnittstelle der intelligenten Plattform (IPMI) angegeben, doch die Ermittlung schlägt immer noch fehl.	Geben Sie die BMC-IP-Adresse und die BMC-Anmeldeinformationen (Benutzername, Kennwort und KG-Schlüssel) des verwalteten Systems an.  <b>ANMERKUNG:</b> Der KG-Schlüssel steht nur auf PowerEdge x9xx-Systemen zur Verfügung.
Ich habe auf meinen verwalteten Systemen BMC konfiguriert. Ich kann diese Systeme jedoch immer noch nicht ermitteln.	Stellen Sie sicher, dass eine LAN-Verbindung zum BMC besteht.
Ich verwende die IPMI-Ermittlungsfunktion zum Ermitteln meiner x9xx-Systeme. Ich kann jedoch die Software- und Hardware-Bestandsaufnahmen dieser Systeme nicht erhalten.	Die IPMI-Ermittlungsfunktion kommuniziert mit dem BMC dieser verwalteten Systeme, um Informationen zum Status dieser Systeme einzuholen. Der BMC stellt Daten zur Verfügung wie:  <ul style="list-style-type: none"> <li>1 Strom- und Gehäusestatus</li> <li>1 Hardwareprotokoll</li> <li>1 Service-Tag-Nummer</li> </ul>

	<ul style="list-style-type: none"> <li>1 Host-Name</li> <li>1 Betriebssystem</li> <li>1 Systemtyp</li> </ul> <p>BMC stellt zu den verwalteten Systemen keine anderen Informationen zur Verfügung.</p> <p><b>ANMERKUNG:</b> Sollten Sie weitere Informationen zu den verwalteten Systemen benötigen, können Sie die Software-Bereitstellungsfunktion von IT Assistant verwenden, um den Dell-Agenten (Server Administrator) auf Ihren verwalteten Systemen bereitzustellen. Weitere Informationen finden Sie unter "<a href="#">Server-Softwarebereitstellung verwenden</a>".</p>
--	--

## Verschiedenes

Frage	Antwort
Ich möchte auf der Schnittstelle, auf der IT Assistant Netmon Service installiert ist, eine andere Anwendung ausführen. Muss ich IT Assistant deinstallieren und wieder neu installieren?	Die Schnittstellenummer für den DSM-IT Assistant-Netzwerküberwachungsdienst wird anhand des Microsoft Windows-Registrierungsschlüssels <code>HKLM\Dell Computer Corporation\Dell OpenManage IT Assistant\Network Monitoring Service\PortNumber</code> definiert. Ändern Sie den Wert dieses Schlüssels, und starten Sie den DSM-IT Assistant-Verbindungsdienst und die DSM-IT Assistant-Netzwerküberwachungsdienste neu.
Welche sind die Namen der verschiedenen IT Assistant-Dienste?	Die Namen der IT Assistant-Dienste sind: <ul style="list-style-type: none"> <li>1 DSM-IT Assistant-Netzwerküberwachung</li> <li>1 DSM-IT Assistant-Verbindungsdienst</li> </ul>
Ich sehe redundante Einträge für die Dell™ PowerConnect™-Schalter - einen unter der Kategorie <b>Unbekannt</b> , und den anderen unter <b>Netzwerkgeräte</b> als Schalterobjekt.	Wenn IT Assistant den PowerConnect-Schalter mit konfigurierter IP-Adresse ermittelt, SNMP jedoch nicht konfiguriert ist, klassifiziert er dieses Objekt unter der Gruppe <b>Unbekannt</b> als ein Gerät, das <b>Unbekannt</b> ist. Wenn Sie SNMP jedoch auf dem Schalter konfigurieren und auf <b>Bestandsaufnahme aktualisieren</b> klicken, klassifiziert IT Assistant den Schalter neu als ein <b>Schalterobjekt</b> unter der Kategorie <b>Netzwerkgeräte</b> , löscht jedoch den Eintrag <b>Unbekannt</b> nicht. Der redundante Eintrag <b>Unbekannt</b> muss manuell gelöscht werden.
Der Anwendungsstart der RAC-Konsole steht für meine Systeme nicht zur Verfügung.	Wenn Sie Ihre Systeme anhand von CIM statt SNMP ermittelt haben, steht der Anwendungsstart für die RAC-Konsole nicht zur Verfügung.
Ich kann von meinen Linux-Systemen keine Traps vom Dell OpenManage Server Administrator-Speicherverwaltungsdienst empfangen.	Stellen Sie sicher, dass die Datei <code>snmpd.conf</code> nicht so eingestellt ist, dass sie SNMP-Traps im Format der Version 2 sendet. IT Assistant kann das SNMP-Format der Version 2 nicht erkennen.  Stellen Sie sicher, dass das Trap-Format auf <code>Trapsink-Host-Name &lt;Community-Zeichenkette&gt;</code> eingestellt ist.  <b>ANMERKUNG:</b> <code>trapsink</code> sendet SNMP-Traps der Version 1, und <code>trap2sink</code> sendet SNMP-Traps der Version 2.
Ich kann keine Ereignisbenachrichtigungen bzgl. Array Manager und Storage Management-Dienst empfangen.	CIM wird von den Storage Management-Diensten und Array Manager nicht unterstützt. Deshalb empfängt IT Assistant von Speichergeräten, die CIM verwenden, keine Ereignisbenachrichtigungen.  Sie können Benachrichtigungen zu Speicherereignissen empfangen, indem Sie Array Manager und den Storage Management-Dienst so konfigurieren, dass sie Benachrichtigungen zu SNMP-basierten Ereignissen senden.
Ich bin nicht in der Lage, die neusten Daten in der <b>Tasks</b> -Struktur zu sehen.	Wenn Sie veraltete Daten sehen, oder wenn die Daten fehlen, drücken Sie auf F5, um die IT Assistant-Benutzeroberfläche manuell zu aktualisieren.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Zum Einstieg mit Dell OpenManage™ IT Assistant

### Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

Sie können Dell OpenManage IT Assistant zum Überwachen und Verwalten von Systemen auf einem lokalen Netzwerk (LAN) oder einem Weitverkehrsnetz (WAN) verwenden, als auch zur Identifikation der Systemgruppen, die im Fernzugriff verwaltet werden sollen sowie zur Konsolidierung der Ansicht aller Systeme, wodurch Sie einen zentralen Start-URL zum Verwalten dieser Systeme erhalten.

Um IT Assistant verwenden zu können, ist Folgendes notwendig:

1. [Planen Sie Ihre IT Assistant-Installation](#) - Planung ist wichtig, da Sie IT Assistant abhängig von Ihren Netzwerkverwaltungszielen eventuell folgendermaßen einsetzen möchten:
  - o als Hilfsprogramm zur Ermittlung oder Statusabfrage.
  - o zur Leistungsüberwachung der verschiedenen Geräte auf Ihrem Netzwerk und zum Ausführen von Softwareaktualisierungen.
  - o zum ausschließlichen Erhalt von Warnungen zu Problemen auf Ihren verwalteten Systemen.
1. [IT Assistant installieren](#) - IT Assistant ist erhältlich auf:
  - o Der CD *Dell Systems Management Consoles*. Weitere Informationen zu den Systems Management Software-Komponenten finden Sie unter *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.
  - o Dells Support-Website unter [support.dell.com](http://support.dell.com).

Um IT Assistant herunterzuladen, führen Sie folgende Schritte aus:

1. Stellen Sie eine Verbindung zu Dells Support-Website unter [support.dell.com](http://support.dell.com) her.


In der Suchleiste in der oberen rechten Ecke wählen Sie **Technical Support (Technischer Support)** aus und geben Sie als Suchtext **OMI-50-MgmtStat-WIN\_A00.exe** ein.


 **ANMERKUNG:** Im Suchtext zeigt **50** die Version von Dell OpenManage an, die die Verwaltungsstationskomponenten einschließlich IT Assistant zusammenfügt.

2. Klicken Sie auf **Search (Suche)**.
3. Klicken Sie auf den Hyperlink, der auf der Suchergebnisseite erscheint. Die Seite **Drivers and Downloads (Treiber und Downloads)** erscheint.
4. Wählen Sie **OMI-50-MgmtStat-WIN\_A00.exe** aus. Die Download-Seite für **OMI-50-MgmtStat-WIN\_A00.exe** erscheint.
5. Klicken Sie auf **Download now (Jetzt herunterladen)** und speichern Sie die Datei zu einem Speicherort auf der Verwaltungsstation.

Die Verwaltungsstation ist das System, auf dem IT Assistant installiert ist. Eine Verwaltungsstation kann dazu verwendet werden, ein verwaltetes System bzw. mehrere verwaltete Systeme im Remote-Zugriff von einer zentralen Stelle aus zu verwalten. Systeme, die von IT Assistant überwacht werden, werden als verwaltete Systeme bezeichnet.

Stellen Sie vor der Installation von IT Assistant sicher, dass der Windows-SNMP-Dienst installiert ist.

 **ANMERKUNG:** Alle anderen Voraussetzungen, außer dem Windows-SNMP-Dienst, können anhand des IT Assistant-Installationsprogramms installiert werden.

 **ANMERKUNG:** Stellen Sie sicher, dass die CD zur Installation des Betriebssystems verfügbar ist, damit Sie die SNMP-Komponenten auf der Verwaltungsstation installieren können. Die IT Assistant-Installation wird fehlschlagen, wenn die SNMP-Komponenten nicht verfügbar sind.

Um den SNMP-Dienst auf der Verwaltungsstation zu installieren, führen Sie folgende Schritte aus:


1. Klicken Sie auf die **Start**-Schaltfläche. Zeigen Sie auf **Einstellungen** → **Systemsteuerung** → **Software** → **Windows-Komponenten hinzufügen/entfernen**.
2. Wählen Sie **Verwaltungs- und Überwachungs-Hilfsprogramme** aus.
3. Wenn Sie dazu aufgefordert werden, einen Installationsort anzugeben, wählen Sie die Betriebssystem-CD aus, die die SNMP-Dienstkomponenten enthält.

Um den Windows-SNMP-Dienst auf der Verwaltungsstation zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf dem Desktop mit der rechten Maustaste auf das Symbol **Arbeitsplatz**, und wählen Sie **Verwalten** aus. Das Fenster **Computerverwaltung** wird eingeblendet.
2. Erweitern Sie die Struktur **Dienste und Anwendungen**.
3. Klicken Sie auf **Dienste**. Die Dienstliste wird im rechten Fenster angezeigt.
4. Machen Sie **SNMP-Dienst** ausfindig und doppelklicken Sie darauf. Das Eigenschaftfenster **SNMP-Dienst** wird angezeigt.
5. Wählen Sie das Register **Sicherheit** aus, und klicken Sie unter **Zugelassene Community-Namen** auf **Hinzufügen**. Das Fenster **Konfiguration SNMP-Dienst** wird eingeblendet.
6. Wählen Sie im Drop-Down-Menü **Community-Rechte** **SCHREIBGESCHÜTZT** aus, und geben Sie in das Feld **Community-Name** eine Zeichenkette ein (Groß- und Kleinschreibung beachten).

 **ANMERKUNG:** Die Zeichenkette **Community-Name** dient als Kennwort für SNMP-Kommunikationen.

7. Klicken Sie auf **Hinzufügen**.
8. Wählen Sie **SNMP-Pakete von diesen Hosts annehmen** aus, und klicken Sie **erneut** auf **Hinzufügen**.
9. Im Dialogfeld der **SNMP-Dienstkonfiguration** geben Sie localhost oder die IP-Adresse der Verwaltungsstation unter **Host-Name, IP- oder IPX-Adresse** ein.
10. Klicken Sie auf **Hinzufügen**.
11. Klicken Sie auf das Register **Traps**. Geben Sie im Feld **Community-Name** eine Zeichenkette ein (Groß- und Kleinschreibung beachten), und klicken Sie auf **Zur Liste hinzufügen**.

 **ANMERKUNG:** Sie können dieselbe Zeichenkette eingeben, die Sie in [Schritt 6](#) eingegeben haben.


12. Klicken Sie unter dem Feld **Trap-Ziele** auf **Hinzufügen**, und geben Sie localhost oder die IP-Adresse der Verwaltungsstation unter **Host-Name, IP- oder IPX-Adresse** ein, und klicken Sie auf **Hinzufügen**.
13. Klicken Sie auf **OK**.
14. Klicken Sie mit der rechten Maustaste auf **SNMP-Dienst**, und wählen Sie **Neustarten** aus.
15. Wählen Sie **SNMP-Trap-Dienst** aus, und stellen Sie sicher, dass der Status als **Gestartet** und der Starttyp als **Automatisch** angezeigt wird.

Um den Windows-SNMP-Dienst auf dem verwalteten System zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf die **Start-Schaltfläche**. Zeigen Sie auf **Einstellungen** → **Systemsteuerung** → **Software** → **Windows-Komponenten hinzufügen/entfernen**.
2. Wählen Sie **Verwaltungs- und Überwachungs-Hilfsprogramme** aus.
3. Wenn Sie dazu aufgefordert werden, einen Installationsort anzugeben, wählen Sie die Betriebssystem-CD aus, die die SNMP-Dienstkomponenten enthält.


Um den Windows-SNMP-Dienst auf der Verwaltungsstation zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf dem Desktop mit der rechten Maustaste auf das Symbol **Arbeitsplatz**, und wählen Sie **Verwalten** aus. Das Fenster **Computerverwaltung** wird eingeblendet.
2. Erweitern Sie die Struktur **Dienste und Anwendungen**.
3. Klicken Sie auf **Dienste**. Die Dienstliste wird im rechten Fenster angezeigt.
4. Machen Sie **SNMP-Dienst** ausfindig und doppelklicken Sie darauf. Das Eigenschaftfenster **SNMP-Dienst** wird angezeigt.
5. Wählen Sie das Register **Sicherheit** aus, und klicken Sie unter **Zugelassene Community-Namen** auf **Hinzufügen**. Das Fenster **Konfiguration SNMP-Dienst** wird eingeblendet.
6. Wählen Sie im Drop-Down-Menü **Community-Rechte** **SCHREIBGESCHÜTZT** aus, und geben Sie in das Feld **Community-Name** eine Zeichenkette ein (Groß- und Kleinschreibung beachten).

 **ANMERKUNG:** Die Zeichenkette **Community-Name** dient als Kennwort für SNMP-Kommunikationen.

7. Klicken Sie auf **Hinzufügen**.
8. Wählen Sie **SNMP-Pakete von diesen Hosts annehmen** aus, und klicken Sie **erneut** auf **Hinzufügen**.
9. Im Dialogfeld der **SNMP-Dienstkonfiguration** geben Sie localhost oder die IP-Adresse der Verwaltungsstation unter **Host-Name, IP- oder IPX-Adresse** ein.
10. Klicken Sie auf **Hinzufügen**.
11. Klicken Sie auf das Register **Traps**. Geben Sie im Feld **Community-Name** eine Zeichenkette ein (Groß- und Kleinschreibung beachten), und

Klicken Sie auf **Zur Liste hinzufügen**.

 **ANMERKUNG:** Sie können dieselbe Zeichenkette eingeben, die Sie in [Schritt 6](#) eingegeben haben.

12. Klicken Sie unter dem Feld **Trap-Ziele** auf **Hinzufügen**, und geben Sie localhost oder die IP-Adresse der Verwaltungsstation unter **Host-Name, IP- oder IPX-Adresse** ein, und klicken Sie auf **Hinzufügen**.
13. Klicken Sie auf **OK**.
14. Klicken Sie mit der rechten Maustaste auf **SNMP-Dienst**, und wählen Sie **Neustarten** aus.

Wenn Sie IT Assistant von Dells Support-Website unter [support.dell.com](http://support.dell.com) heruntergeladen haben, führen Sie folgende Schritte aus:

1. Doppelklicken Sie auf **OMI-50-MgmtStat-WIN\_A00.exe**. Hierbei handelt es sich um ein selbstextrahierendes Winzip-Paket.
2. Geben Sie einen temporären Ordner an, um die extrahierten Dateien zu speichern.
3. Machen Sie den temporären Ordner ausfindig, und doppelklicken Sie auf **setup.exe**.

Das Installationsprogramm führt zuerst die Voraussetzungsprüfung aus, um zu überprüfen, ob alle Voraussetzungen installiert sind. Wenn nicht bereits eine Voraussetzung installiert ist, kann diese installiert werden, indem Sie im Installationsfenster auf den entsprechenden Hyperlink klicken und dann die Anleitungen auf den Setup-Bildschirmen befolgen.

Wenn alle Voraussetzungen installiert sind, installieren Sie IT Assistant, indem Sie auf **Verwaltungsstation installieren, modifizieren, reparieren oder entfernen** klicken und dann die Anleitungen der Setup-Bildschirme befolgen.


Nachdem IT Assistant installiert ist, folgen Sie einer der beiden nachfolgenden Anleitungen, um IT Assistant auszuführen:

1. Doppelklicken Sie auf dem Desktop auf das IT Assistant-Symbol.
1. Öffnen Sie einen unterstützten Internet-Browser und stellen Sie eine Verbindung zur IT Assistant-Verwaltungsstation her, indem Sie Folgendes in die Adressleiste eingeben:

`<IT Assistant-Host-Name>:<Schnittstellenummer>`

 **ANMERKUNG:** Die Standardschnittstellenummer von IT Assistant ist 2607.

Wenn Sie auf die IT Assistant-Benutzeroberfläche von einem System aus zugreifen, auf dem ein unterstütztes Windows-Betriebssystem ausgeführt wird, das keine unterstützte JRE-Mindestversion (Java-Laufzeitumgebung) von 5.0, Aktualisierung 6, besitzt, würde IT Assistant die Installation von JRE auf diesem System automatisch starten.

 **ANMERKUNG:** Wenn das System, das auf die IT Assistant-Benutzeroberfläche zugreift, JRE Version 5.0, Aktualisierung 1 bis 5 besitzt, aktualisiert IT Assistant die JRE nicht automatisch zu Version 5.0, Aktualisierung 6. Aktualisieren Sie in diesem Falle die JRE-Version manuell, indem Sie den Browser auf folgende Adresse lenken: [https://<Host-Name>:<Schnittstellenummer>/jre-1\\_5\\_0\\_06-windows-i586-p.exe](https://<Host-Name>:<Schnittstellenummer>/jre-1_5_0_06-windows-i586-p.exe).

Wenn Sie jedoch von einem System aus auf IT Assistant zugreifen, auf dem ein unterstütztes Linux-Betriebssystem ausgeführt wird, führen Sie folgende Schritte aus:

1. Speichern Sie das JRE-Installationsprogramm (**jre-1\_5\_0\_06-linux-i586-rpm.bin**) am Speicherort Ihrer Wahl.
  2. Extrahieren Sie den RPM, und installieren Sie JRE.
  3. Erstellen Sie im Browser-Ordner **Plugins** einen Softlink zu dieser JRE.
  4. Schließen Sie den Internet-Browser, und führen Sie IT Assistant erneut aus.
1. [Protokolle einrichten](#) - Sie müssen die entsprechenden Protokolle (SNMP, CIM und IPMI) konfigurieren, um die Systeme in Ihrem Netzwerk zu ermitteln und um Warnungen zu erhalten, die über den Status Ihrer Komponenten berichten. Weitere Informationen finden Sie unter "[Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren](#)".
  1. [Konfigurieren Sie IT Assistant zur Überwachung Ihrer Systeme](#) - IT Assistant kann für jedes System in Ihrem Netzwerk verschiedene Tasks ausführen. Damit IT Assistant in der Lage ist, diese Tasks auszuführen, konfigurieren Sie ihn folgendermaßen:
    - o Zur Ermittlung von Systemen, Druckern, Schaltern und Speichergeräten. Weitere Informationen finden Sie unter "[Ermittlungseinstellungen konfigurieren](#)".
    - o Zum Zusammentragen von Bestandsaufnahme-Informationen über Speicher, Prozessor, Netzteil, integrierte Geräte sowie Software- und Firmware-Versionen. Weitere Informationen finden Sie unter "[Bestandsaufnahme-Einstellungen konfigurieren](#)".
    - o Zur Definition von Statusabfrage-Einstellungen, um für alle ermittelten Geräte eine Strom- und Konnektivitätsfunktionszustands-Prüfung auszuführen. Dies bestimmt, ob ein Gerät normal funktioniert, sich in einem nichtnormalen Zustand befindet oder heruntergefahren ist. Weitere Informationen finden Sie unter "[Statusabfrage-Einstellungen konfigurieren](#)".

- Definieren Sie einen Ermittlungsbereich. Ein Ermittlungsbereich ist ein Netzwerksegment (Subnetz, Bereich von IP-Adressen in einem Subnetz, individuelle IP-Adressen oder ein individueller Host-Name), das IT Assistant zur Ermittlung von Geräten verwendet. Weitere Informationen finden Sie unter "[Ermittlungsbereiche konfigurieren](#)".
  - 1 Führen Sie verschiedene Tasks aus, wie z. B. :
    - [Warnungsmaßnahme erstellen](#)
    - [Leistungsüberwachungs-Task erstellen](#)
    - [Softwarebereitstellungs-Task erstellen](#)
    - [Neuen Report erstellen](#)
- 

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)


# Dell OpenManage™ IT Assistant installieren, deinstallieren und erweitern

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Voraussetzungen für die Installation](#)
  - [Protokolle zur Kommunikation mit Agenten einrichten oder aktivieren](#)
  - [RBAC-Benutzerinformationen einrichten](#)
  - [IT Assistant installieren](#)
  - [Eine vorherige Version des IT Assistant aktualisieren](#)
  - [IT Assistant deinstallieren](#)
- 

## Voraussetzungen für die Installation

Bei der Installation von Dell OpenManage IT Assistant sollte unbedingt die neueste Infodatei **readme.txt** auf der CD *Dell Systems Management Consoles* oder auf Dells Support-Website unter [support.dell.com](http://support.dell.com) gelesen werden. In dieser Datei werden die derzeit unterstützten Betriebssysteme und Hardwareanforderungen für IT Assistant angegeben. Zusätzlich zu diesen Anforderungen bestehen noch weitere Voraussetzungen für die IT Assistant-Installation sowie für die Systeme, die mit dem IT Assistant verwaltet werden. Weitere Informationen finden Sie unter "[Installationsplan für Dell OpenManage™ IT Assistant](#)".

 **ANMERKUNG:** Die CD *Systems Management Consoles* steht als Web-Paket und als ISO-Image zum Download zur Verfügung.

## Unterstützung für TCP/IP-Protokoll

Für die fehlerfreie Funktion des IT Assistant muss das TCP/IP-Protokoll vom Netzwerk unterstützt werden.

---

## Protokolle zur Kommunikation mit Agenten einrichten oder aktivieren

Vor der Installation des IT Assistant muss der einfache Netzwerkverwaltungsprotokoll (SNMP) -Dienst des Betriebssystems installiert sein. Damit Systeme für die IT Assistant-Ermittlungs- und Bestandsaufnahmefunktionen sichtbar sind, ist außerdem sicherzustellen, dass die Agenten und die Instrumentation auf verwalteten Systemen über die Protokolle des allgemeinen Informationsmodells (CIM), des einfachen Netzwerk-Verwaltungsprotokolls (SNMP) oder der intelligenten Plattform-Verwaltungsschnittstelle (IPMI) zugänglich sind.

 **ANMERKUNG:** CIM ist auf Microsoft® Windows® 2000, Windows Server® 2003 und Windows XP Professional standardmäßig installiert.

## SNMP auf dem IT Assistant-System installieren

Der SNMP-Dienst muss auf dem IT Assistant-System installiert und ausgeführt werden. SNMP (oder CIM) muss auch auf den Systemen installiert sein, die Sie entdecken und verwalten wollen.

 **ANMERKUNG:** Im folgenden Beispiel wird Windows 2000 Advanced Server verwendet.

1. Klicken Sie auf die Schaltfläche **Start**, zeigen Sie auf **Einstellungen** und doppelklicken Sie auf **Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Software**.

Hierdurch wird das Fenster **Software** eingeblendet.

3. Klicken Sie in der linken Menüleiste auf das Symbol **Windows-Komponenten hinzufügen/entfernen**.

Das Fenster **Assistent für Windows-Komponenten** wird eingeblendet.

4. Rollen Sie im Fenster **Assistent für Windows Komponenten** unter **Komponenten zu Verwaltungs- und Überwachungsprogramme**.

5. Wählen Sie **Verwaltungs- und Überwachungshilfsprogramme** aus, klicken Sie auf **Details**, wählen Sie **Einfaches Netzwerkverwaltungsprotokoll** und klicken Sie auf **OK**.
6. Klicken Sie im Fenster **Assistent für Windows Komponenten** auf **Weiter**.

SNMP wird vom **Assistenten für Windows Komponenten** installiert.

7. Klicken Sie nach der Installation auf **Fertig stellen**.
8. Schließen Sie das Fenster **Software**.

SNMP ist jetzt auf Ihrem System installiert.

IT Assistant kann nur auf Systemen installiert werden, auf denen Windows 2000, Windows XP Professional oder Windows Server 2003 ausgeführt wird. Informationen zur Installation und Konfiguration von SNMP auf verwalteten Systemen, auf denen die Betriebssysteme Microsoft Windows, Red Hat® Linux oder SUSE® Linux Enterprise Server ausgeführt werden, finden Sie unter ["Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren"](#).

## CIM aktivieren

Der CIM/WMI (Windows Management Instrumentation) -Dienst ist unter Windows 2000, Windows Server 2003 und Windows XP Professional standardmäßig installiert. Zur CIM-Ermittlung sind korrekte Anmeldeinformationen (Benutzer-ID und Kennwort) erforderlich. Bei falscher Angabe dieser Informationen auf einem zur CIM-Ermittlung konfigurierten Subnetz könnte das Konto ausgeschlossen werden.

Beispiele zur Einrichtung von CIM finden Sie unter ["Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren"](#).

---

## RBAC-Benutzerinformationen einrichten

IT Assistant unterstützt funktionsbasierte Access Control (RBAC), um die spezifischen Vorgänge zu definieren, die jeder Benutzer durchführen kann. Für das IT Assistant-Installationsverfahren ist es jedoch nicht erforderlich, dass diese Benutzerfunktionen vor der Installation eingerichtet werden. Um RBAC-Benutzer entweder vor oder nach der Installation von IT Assistant einzurichten, lesen Sie ["Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten"](#).

---

## IT Assistant installieren

Wenn Sie IT Assistant zum ersten Mal installieren, folgen Sie den hier gezeigten Schritten. Wenn Sie von einer vorherigen Version aktualisieren, lesen Sie ["Eine vorherige Version des IT Assistant aktualisieren"](#).

IT Assistant kann von der CD *Dell Systems Management Consoles* installiert oder von der Dell Support-Website unter [support.dell.com](http://support.dell.com) heruntergeladen und installiert werden. Das Dell OpenManage Management Station-Installationsprogramm wird zur Installation des IT Assistant und anderer Dell OpenManage-Software verwendet. Um ein anderes Produkt als den IT Assistant zu installieren, lesen Sie die Installationsanleitungen für dieses Produkt.

Erste Installation des IT Assistant:

1. Legen Sie die CD *Dell Systems Management Consoles* in das CD-Laufwerk ein.

Wenn das Installationsprogramm nicht automatisch startet, wechseln Sie zum Verzeichnis `/windows` und klicken auf `setup.exe`. Der Bildschirm **Dell OpenManage Management Station** wird angezeigt.

Das Installationsprogramm scannt Ihr System automatisch nach allen Abhängigkeiten (z. B., ob Sie SNMP installiert haben oder ob Sie eine unterstützte Datenbankanwendung haben). Wenn eine fehlende Abhängigkeit gefunden wurde, wird ein Informationsfenster eingeblendet, und Sie werden eventuell dazu aufgefordert, das erforderliche Paket zu installieren.

2. Wenn keine fehlenden Abhängigkeiten gefunden wurden, klicken Sie auf **Management Station installieren, modifizieren, reparieren oder entfernen**.



Der Installationsassistent von Dell OpenManage Management Station wird angezeigt. Klicken Sie auf **Weiter**.

3. Wenn Sie den Dell Inc. Softwarelizenzvereinbarung annehmen, klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster **Setup-Typ** die Installationsart **Typisch** oder **Benutzerdefiniert** aus.


Die Auswahl von **Benutzerdefiniert** ermöglicht Ihnen, spezifische Dell OpenManage-Anwendungen zur Installation auszuwählen und den Installationsverzeichnispfad sowie die Schnittstelleneinstellungen für den IT Assistant zu ändern.


Die Auswahl von **Typisch** installiert alle Dell OpenManage-Anwendungen (einschließlich IT Assistant), die die Abhängigkeitsüberprüfung mit vorausgewählten Standardeinstellungen bzgl. Standort und Schnittstelle bestanden haben. Wenn Sie **Typisch** wählen, fahren Sie mit dem letzten Schritt fort.


5. Stellen Sie sicher, dass **IT Assistant** in der Liste installierbarer Komponenten ausgewählt ist, und klicken Sie dann auf **Weiter**.
6. Wenn Sie die Installationsoption **Benutzerdefiniert** ausgewählt haben, geben Sie Schnittstelleneinstellungen ein oder akzeptieren die Standardeinstellungen. Wenn Sie die Installationsoption **Typisch** ausgewählt haben, erscheint dieses Dialogfeld nicht.
7. Klicken Sie auf **Weiter**.
8. Stellen Sie sicher, dass **IT Assistant** im Installationszusammenfassungsfenster aufgenommen ist und klicken Sie dann auf **Installieren**, um mit der Installation zu beginnen.

---

## Eine vorherige Version des IT Assistant aktualisieren

 **ANMERKUNG:** Nur die IT Assistant-Versionen 6.2 und höher unterstützen die Aktualisierung vorhergehender Versionen. Das Installationsprogramm der Dell OpenManage Management Station entdeckt, ob Sie zurzeit eine aktualisierbare Version von IT Assistant auf Ihrem System haben.

 **ANMERKUNG:** IT Assistant unterstützt ein direktes Upgrade von Version 6.x zu Version 8.0 nicht. Es ist erforderlich, zuerst IT Assistant Version 6.x zu Version 7.0 zu erweitern und dann zu IT Assistant Version 8.0.

 **ANMERKUNG:** Wenn Sie während dem Upgrade zu IT Assistant Version 8.0 auch planen, den Microsoft SQL Server zu erweitern, finden Sie Informationen zur entsprechenden Kombination von Betriebssystem und SQL Server unter "[SQL Server 2005 Express-Standarddatenbank oder SQL 2005 Server auswählen](#)".


Aktualisierung des IT Assistant:

1. Legen Sie die CD *Dell Systems Management Consoles* in das CD-Laufwerk ein.

Wenn das Installationsprogramm nicht automatisch startet, wechseln Sie zum Verzeichnis `/windows` und klicken auf `setup.exe`. Der Bildschirm **Dell OpenManage Management Station** wird angezeigt.

2. Das Installationsprogramm scannt Ihr System automatisch nach fehlenden Abhängigkeiten, z. B. ob SNMP installiert ist oder ob Sie eine unterstützte Datenbankanwendung haben. Wenn eine fehlende Abhängigkeit gefunden wurde, wird ein Informationsfenster eingeblendet, und Sie werden eventuell dazu aufgefordert, die erforderlichen Pakete zu installieren.

Das IT Assistant 8.0-Installationsprogramm entfernt alle vorhergehenden Management Station Applications und installiert die von Ihnen ausgewählten Anwendungen erneut. Alle Dell OpenManage Server Administrator-Anwendungen werden ebenfalls entfernt.

 **ANMERKUNG:** Wenn Sie IT Assistant Version 6.x haben, installieren Sie IT Assistant 7.0, bevor Sie Version 8.0 installieren.

3. Wenn keine fehlenden Abhängigkeiten gefunden wurden, klicken Sie auf **Management Station installieren, modifizieren, reparieren oder entfernen**.

Der Installationsassistent von Dell OpenManage Management Station wird angezeigt. Klicken Sie auf **Weiter**.


4. Wenn Sie den Dell Inc. Softwarelizenzvereinbarung annehmen, klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster **Setup-Typ** die Installationsart **Typisch** oder **Benutzerdefiniert** aus.

Die Auswahl von **Benutzerdefiniert** ermöglicht Ihnen, spezifische Dell OpenManage-Anwendungen zur Installation auszuwählen und den Installationsverzeichnispfad sowie die Schnittstelleneinstellungen für den IT Assistant zu ändern.


Die Auswahl von **Typisch** installiert alle Dell OpenManage-Anwendungen (einschließlich IT Assistant) mit vorausgewählten Standardeinstellungen bzgl. Standort und Schnittstelle.


6. Stellen Sie sicher, dass **IT Assistant** in der Liste installierbarer Komponenten ausgewählt ist, und klicken Sie dann auf **Weiter**.
7. Wenn Sie die Installationsoption **Benutzerdefiniert** ausgewählt haben, geben Sie Schnittstelleneinstellungen ein oder akzeptieren die Standardeinstellungen. Wenn Sie die Installationsoption **Typisch** ausgewählt haben, erscheint dieses Dialogfeld nicht.

8. Wenn Sie ein Upgrade von IT Assistant 6.x zu 7.0 vornehmen, wird standardmäßig **IT Assistant-Datenbankeinstellungen migrieren** ausgewählt. Bei Auswahl dieser Option, werden die folgenden Datenbankeinstellungen der vorhandenen IT Assistant-Installation in der neuen Installation erhalten:
  - 1 Globale Konfiguration
  - 1 Nach Ereignissen gespeicherte Maßnahmen
  - 1 Ermittlungskonfiguration

 **ANMERKUNG:** IT Assistant-Datenbankeinstellungen migrieren ist nicht verfügbar, wenn ein Upgrade von IT Assistant Version 7.x zu Version 8.0 vorgenommen wird.

9. Klicken Sie auf **Weiter**.
10. Stellen Sie sicher, dass **IT Assistant** im Installationszusammenfassungsfenster aufgenommen ist und klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

 **ANMERKUNG:** Bei der Aktualisierung von IT Assistant Version 6.x auf Version 7.2, müssen die CIM-Benutzernamen qualifiziert werden. Diese Qualifizierung ist notwendig, da CIM nur durch den Ermittlungsbereich aktiviert/deaktiviert ist und voraussetzt, dass jeder CIM-Benutzer durch eine Domäne oder einen lokalen Host qualifiziert ist, wenn keine vertrauenswürdige Domäne konfiguriert wurde. Es ist sehr wichtig, dass diese Qualifizierung vorliegt, wenn CIM durch einen Ermittlungsbereich (z. B. <Domäne\Benutzername> oder <lokaler Host\Benutzername->) zur Authentifizierung und Verwendung des CIM-Protokolls konfiguriert werden soll.


 **ANMERKUNG:** IT Assistant kann nicht in einer Remote-Datenbankumgebung erweitert werden. Details finden Sie im Abschnitt "[Microsoft SQL Server und IT Assistant im Fernzugriff](#)".

---

## IT Assistant deinstallieren

Deinstallation des IT Assistant:

1. Klicken Sie auf die Schaltfläche **Start**, zeigen Sie auf **Einstellungen** und doppelklicken Sie auf **Systemsteuerung**.
2. Doppelklicken Sie auf **Software**.
3. Wählen Sie **Dell OpenManage Management Station** von der Liste der derzeit installierten Programme aus, und klicken Sie auf die Schaltfläche **Ändern**.

 **ANMERKUNG:** Um die gesamte Management Station-Produktserie (einschließlich IT Assistant) zu deinstallieren, wählen Sie **Entfernen** im vorhergehenden Schritt. Bei Auswahl von **Entfernen**, kann die Deinstallation eventuell einige Minuten unempänglich erscheinen, wenn IT Assistant gerade eine Ermittlung oder eine Abfrage ausführt.

Der Management Station-Installationsassistent wird eingeblendet. Klicken Sie auf **Weiter**.

4. Im Fenster **Programmpflege** wählen Sie **Modifizieren** und klicken Sie dann auf **Weiter**.
5. Im Bildschirm **Benutzerdefiniertes Setup** wählen Sie IT Assistant ab und klicken dann auf **Weiter**.
6. Stellen Sie im Zusammenfassungsbildschirm sicher, dass IT Assistant in der Liste der zu entfernenden Anwendungen aufgeführt ist. Klicken Sie auf **Installieren**.
7. Klicken Sie nach Abschluss der Deinstallation auf **Fertig stellen**.
8. Starten Sie Ihr System neu (optional).

## Microsoft SQL Server und IT Assistant im Fernzugriff

Dieser Abschnitt beschreibt, wie IT Assistant Version 8.0 und höher konfiguriert wird, um Microsoft SQL Server 2005 zu verwenden, der auf einem Remote-Server als IT Assistant-Datenbank ausgeführt wird.

### IT Assistant zur Verwendung einer Remote-Datenbank konfigurieren

IT Assistant wird mit der SQL Server-konformen Standarddatenbank geliefert - SQL Server 2005 Express. Der IT Assistant-Netzwerküberwachungsdienst und der IT Assistant-Verbindungsdienst greifen auf die SQL Server-konforme Standarddatenbank zu - SQL Server 2005 Express, der mit IT Assistant geliefert wird.

Wenn sich die Datenbank außerhalb der IT Assistant-Verwaltungsstation befindet, wie dies bei einer Remote-Datenbank der Fall ist, ist es notwendig, den IT Assistant-Netzwerküberwachungsdienst und den IT Assistant-Verbindungsdienst auf der Verwaltungsstation zu veranlassen, auf die Remote-Datenbank zuzugreifen.

Stellen Sie hierzu Folgendes sicher:

- 1 Der SQL Server-Dienst (MSSQLServer) wird über das Dienstbedienungsfeld auf der Verwaltungsstation sowie über die Remote-Datenbank ausgeführt. Die SQL Server 2005-Dienste können entweder durch den SQL Server Service Manager auf der Taskleiste oder durch die SQL Server-Gruppe des SQL Server Enterprise Manager gestartet werden.
- 1 Die SQL Server-konformen Datenbankversionen auf der Verwaltungsstation und der Remote-Datenbank sind identisch.
- 1 SQL Server 2005 verwendet dieselbe Authentifizierung, die auf SQL Server 2005 Express auf der Verwaltungsstation verwendet wird.
- 1 Die Verwaltungsstation und die Remote-Datenbank verwenden dieselbe Authentifizierung mit Administratorrechten und sind über dasselbe Konto angemeldet, und die SQL Server-Datenbanken auf beiden Systemen sind zur Verwendung dieses Kontos konfiguriert. Dies ist der Fall, weil sich die IT Assistant-Dienste unter Verwendung der Windows NT@-Authentifizierung bei SQL Server 2005 Express anmelden.

Nehmen wir bzgl. dieses Beispiels an, dass auf beiden Servern der Benutzername Administrator ist und die Kennwörter identisch sind, und dass sich beide Systeme in derselben NT-Domäne befinden.

## Bereitstellung der IT Assistant-Datenbank für die Remote-Datenbank

Auf der Verwaltungsstation halten Sie den IT Assistant-Verbindungsdiens und den IT Assistant-Netzwerküberwachungsdiens vom Service Control Manager aus an. Dies hält die IT Assistant-Dienste davon ab, auf die lokale IT Assistant-Datenbank zuzugreifen. Stellen Sie sicher, dass kein anderes Programm auf die lokale IT Assistant-Datenbank zugreift. Wenn ein Datenbankprogramm wie der Enterprise Manager des SQL Server und/oder Query Analyzer ausgeführt werden, schließen Sie das Programm, oder stellen Sie sicher, dass das Programm nicht auf die lokale IT Assistant-Datenbank zugreift.

Auf der Verwaltungsstation trennen Sie die IT Assistant-Datenbank vom lokalen SQL Server, indem Sie das IT Assistant-Datenbankverwaltungs-Dienstprogramm auf der Befehlszeile ausführen.

Führen Sie den folgenden Befehl vom IT Assistant-bin-Verzeichnis aus:

```
dcdbmngg /r
```

Wenn die IT Assistant-Datenbank erfolgreich abgetrennt wurde, wird das Dialogfeld **Datenbank abtrennen** angezeigt.

Um sicherzustellen, dass die Datenbank abgetrennt wurde, führen Sie folgende Schritte aus:

1. Starten Sie den ODBC-Datenquellen-Administrator, indem Sie auf die Schaltfläche **Start** klicken. Wählen Sie **Einstellungen** → **Systemsteuerung** → **Verwaltung** → **Datenquellen (ODBC)** aus.
2. Wählen Sie das Register **System-DSN** aus.


Stellen Sie sicher, dass keine Systemdatenquelle mit dem Namen **ITAssist** (lokale IT Assistant-Datenbank) vorhanden ist.

Sollte eine solche Systemdatenquelle vorhanden sein, klicken Sie auf **Entfernen**, um diese Datenquelle zu löschen.

Auf der Verwaltungsstation wechseln Sie unter dem SQL Server-Installationsverzeichnis zum Ordner **Daten**. Standardmäßig wird der Installationspfad als **C:\Programme\Microsoft SQL Server\MSSQL** angegeben. Kopieren Sie die IT Assistant-Datenbankdatei **ITAssist\_Data.mdf** zu einem Speicherort auf dem Remote-Datenbanksystem. Bzgl. dieses Beispiels nehmen wir an, der gewünschte Pfad lautet **DB\_PATH**.

Auf dem Remote-Datenbanksystem verbinden Sie die Datenbankdatei **ITAssist\_Data.mdf**, die sich unter **DB\_PATH** befindet, mit dem lokalen SQL Server. Sie können dies tun, indem Sie den folgenden SQL-Befehl gegen die lokale übergeordnete Datenbank ausführen:

```
exec sp_attach_single_file_db @dbname='ITAssist',@physname='DB_PATH\ITAssist_Data.mdf'
```

 **ANMERKUNG:** Das erste Argument **@dbname** gibt den Namen der Datenbank an und sollte immer **ITAssist** sein. Das zweite Argument **@physname** gibt an, wo sich die Datenbankdatei befindet. Hierbei sollten Sie immer den korrekten Dateispeicherort **ITAssist\_Data.mdf** verwenden.

Wenn sich auf dem Remote-Datenbanksystem mehrere Instanzen des SQL Server befinden, können Sie den oben aufgeführten SQL-Befehl ausführen und **ITAssist** mit einer beliebigen Instanz des SQL Server verbinden. Es wird jedoch empfohlen, **ITAssist** mit der Standardinstanz der lokalen übergeordneten Datenbank zu verbinden. Dies kann in der SQL Server-Gruppe des SQL Enterprise Manager angezeigt werden. Alle nichtstandardmäßigen Instanzen des SQL Server werden mit dem Instanznamen in Verbindung stehen. Bzgl. dieses Beispiels werden **MYINST1** und **MYINST2** als die beiden nichtstandardmäßigen

Instanzen des SQL Server betrachtet. Diese SQL Server-Instanzen werden folgende sein: **REMOTE\_DB\_SERVER\MYINST1** und **REMOTE\_DB\_SERVER\MYINST2**. Dies kann auch in der SQL Server-Gruppe des SQL Enterprise Manager angezeigt werden. Wenn der SQL Enterprise Manager des Remote-Datenbanksystems keine vollständige Liste aller SQL Server-Instanzen auf dem System hat, registrieren Sie diese nichtstandardmäßigen Instanzen, damit sie in der SQL Server-Gruppe angezeigt werden.

## IT Assistant mit der Remote-Datenbank verbinden

1. Auf der Verwaltungsstation wechseln Sie zum IT Assistant-Installationsverzeichnis und bearbeiten die Konfigurationsdatei **dconfig.ini**, indem Sie jede (loka1e) Zeichenkette mit dem Namen des SQL Server ersetzen, der sich auf dem Remote-Datenbanksystem befindet. Sie können die Zeichenkette unter den Abschnitten [ITAssist\_Odbc\_Attributes] und [Master\_Odbc\_Attributes] finden].
2. Wenn sich die IT Assistant-Datenbank in der Standardinstanz des SQL Server befindet, wird die IT Assistant-Datenbank <Name des Datenbankservers> lauten. Wenn sich die IT Assistant-Datenbank in einer nichtstandardmäßigen Instanz des SQL Server (z. B. **MYINST1**) befindet, wird die IT Assistant-Datenbank <Name des Datenbankservers>/MYINST1 lauten. Mit anderen Worten

Attribute3=Server, <Name/IP-Adresse des Datenbankservers> -- im Falle einer standardmäßigen Instanz

Attribute3=Server, <Name des Datenbankservers>/MYINST1 -- im Falle einer benannten Instanz

3. Auf der Verwaltungsstation ändern Sie die Anmeldeinformationen des IT Assistant-Diensts von **Konto des lokalen Systems** zum allgemeinen Konto, das sowohl bei der Verwaltungsstation als auch beim Remote-Datenbanksystem zur Anmeldung beim lokalen SQL Server verwendet wird. Nehmen wir an, dass es sich in diesem Falle um das Konto des lokalen Administrators handelt.
4. Sie sollten die Anmeldeinformationen für den IT Assistant-Verbindungsdienst und den IT Assistant-Netzwerküberwachungsdienst ändern. Um dies zu tun, klicken Sie im **Service Control Manager** mit der rechten Maustaste auf die individuellen Dienste und wählen **Eigenschaften** aus. Wählen Sie das Register **Anmeldung** aus, um die Anmeldeinformationen zu ändern.

Wenn Sie diese Dienste konfigurieren, um unter einem unterschiedlichen Benutzerkonto ausgeführt zu werden, muss das für **Anmeldung** verwendete Benutzerkonto die folgenden Benutzerberechtigungen aufweisen:

- 1 Sich als Teil des Betriebssystems verhalten (diese Berechtigung ist auf dem Windows 2000-System erforderlich)
- 1 Ein Token auf Verfahrensebene ersetzen
- 1 Sich als Dienst anmelden

Um diese Berechtigungen einzustellen, führen Sie folgende Schritte aus:

- 1 Führen Sie im Eingabeaufforderungs-Dialogfeld `secpol.msc` aus.
  - 1 Wählen Sie **Sicherheitseinstellungen** → **Lokale Richtlinien** → **Zuweisen von Benutzerrechten** aus.
  - 1 Klicken Sie mit der rechten Maustaste auf die Regel, und wählen Sie **Eigenschaften** (oder für Windows 2000 **Sicherheit**) aus.
  - 1 Fügen Sie dieser Regel den Benutzernamen hinzu.
  - 1 Starten Sie das System neu, um die Einstellungen anzuwenden.
5. Dieser Schritt ist optional und ist nur dann erforderlich, wenn Sie planen, das Ausführen des SQL Server-Diensts auf der Verwaltungsstation zu unterbrechen.

Während der IT Assistant-Installation werden IT Assistant-Dienste erstellt, um vom SNMP-Dienst und dem MSSQLServer-Dienst des SQL Server abzuhängen. Sie können die Abhängigkeit der IT Assistant-Dienste auf dem MSSQLServer-Dienst des SQL Server entfernen, indem Sie die Registrierung für die IT Assistant-Dienste auf der Verwaltungsstation bearbeiten.

Vor dem Bearbeiten der Registrierung stellen Sie sicher, dass Sie eine Kopie der Registrierung speichern und verstehen, wie man eine Wiederherstellung durchführt, falls ein Problem auftreten sollte.

Auf der Verwaltungsstation öffnen Sie den Microsoft Windows-Registrierungs-Editor, indem Sie an der Eingabeaufforderung `regedit` eingeben. Wechseln Sie zu **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\dcnetmon**

Doppelklicken Sie auf den Wertenamen **DependOnService**, um seine Eigenschaften zu bearbeiten. Dieser Registrierungswert ist eine mehrfache UNICODE-Zeichenkette, und seine Anfangswertdaten lauten `SNMP, MSSQLServer`.


Löschen Sie **MSSQLServer**, und speichern Sie die Änderungen. Hierdurch wird die Abhängigkeit des IT Assistant-Netzwerküberwachungsdienstes auf dem SQL Server-Dienst entfernt.

Wechseln Sie daraufhin zu **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\dcconnsv**. Doppelklicken Sie auf den Wertenamen **DependOnService**, um seine Eigenschaften zu bearbeiten. Dieser Registrierungswert ist eine mehrfache UNICODE-Zeichenkette, und seine Anfangswertdaten lauten `SNMP, MSSQLServer, dcnetmon`.

Löschen Sie **MSSQLServer**, und speichern Sie die Änderungen. Hierdurch wird die Abhängigkeit des IT Assistant-Verbindungsdienstes auf dem SQL Server-Dienst entfernt.

Überprüfen Sie die Abhängigkeiten IT Assistant-Netzwerküberwachungsdienstes und des IT Assistant-Verbindungsdienstes auf der Verwaltungsstation, indem Sie im **Service Control Manager** mit der rechten Maustaste auf die einzelnen Dienste klicken. Wählen Sie dann **Eigenschaften** aus. Wählen Sie das Register **Abhängigkeiten** aus. Auf dem MSSQLServer-Dienst sollte keine Abhängigkeit vorliegen. Starten Sie die Verwaltungsstation neu, um diese Änderungen wirksam werden zu lassen.

6. Starten Sie auf der Verwaltungsstation den IT Assistant-Verbindungsdienst und den IT Assistant-Netzwerküberwachungsdienst. IT Assistant stellt jetzt eine Verbindung zu der auf dem SQL Server des Remote-Datenbanksystems bereitgestellten IT Assistant-Datenbank her.

 **ANMERKUNG:** Wenn die Abhängigkeit der IT Assistant-Dienste auf dem lokalen SQL Server-Dienst nicht, wie im vorhergehenden Schritt beschrieben, entfernt wurde, muss der SQL Server-Dienst auf der Verwaltungsstation ausgeführt werden, damit die IT Assistant-Dienste gestartet werden können, auch wenn die SQL Server-Datenbank nicht wirklich durch IT Assistant verwendet wird.

7. Um nachzuprüfen, ob die Verwaltungsstation erfolgreich mit der IT Assistant-Datenbank auf dem Remote-Datenbanksystem verbunden wurde, starten Sie den ODBC-Datenquellen-Administrator auf der Verwaltungsstation über **Systemsteuerung** → **Verwaltung**. Wählen Sie das Register **System-DSN** aus. Die **ITAssist**-Systemdatenquelle wird angezeigt.
8. Auf der Verwaltungsstation öffnen Sie die IT Assistant-Benutzeroberfläche. Die IT Assistant-Dienste auf der Verwaltungsstation sind jetzt bereit, die IT Assistant-Datenbank zu verwenden, die sich auf dem Remote-Datenbanksystem befindet.

## IT Assistant zur Erweiterung der Remote-Datenbank konfigurieren

IT Assistant erweitert die Datenbank nicht, die auf einem Remote-System konfiguriert wird. In diesem Abschnitt werden die Schritte besprochen, die zum Erweitern der IT Assistant-Datenbank (Version 7.0 und höher) erforderlich sind.

### IT Assistant-Datenbank für ITA\_STATION bereitstellen

1. Auf ITA\_STATION halten Sie den IT Assistant-Verbindungsdienst und den IT Assistant-Netzwerküberwachungsdienst über den **Service Control Manager** an. Dies hält die IT Assistant-Dienste davon ab, auf die Remote-IT Assistant-Datenbank zuzugreifen. Stellen Sie außerdem sicher, dass kein anderes Programm auf die IT Assistant-Datenbank **ITAssist** von **REMOTE\_DB\_SERVER** zugreift. Wenn ein Datenbankprogramm wie Enterprise Manager von SQL Server und/oder Query Analyzer ausgeführt wird, schließen Sie das Programm oder stellen Sie sicher, dass das Programm nicht auf die ITAssist genannte IT Assistant-Datenbank zugreift.
2. Auf dem **REMOTE\_DB\_SERVER** trennen Sie die IT Assistant-Datenbank vom lokalen SQL Server ab, indem Sie den folgenden SQL-Befehl gegen die lokale übergeordnete Datenbank ausführen:

```
exec sp_detach_db @dbname='ITAssist'
```

3. Um sicherzustellen, dass die Datenbank abgetrennt ist, wechseln Sie zum **ITA\_STATION**-System, starten Sie den **ODBC-Datenquellen-Administrator** über **Start** → **Einstellungen** → **Systemsteuerung** → **Verwaltung** → **Datenquellen (ODBC)**. Klicken Sie auf das Register **System-DSN**. Stellen Sie sicher, dass keine Systemdatenquelle mit dem Namen **ITAssist** vorliegt. Liegt eine vor, entfernen Sie diese Datenquelle, indem Sie auf das Register **Entfernen** klicken.
4. Auf dem **REMOTE\_DB\_SERVER** wechseln Sie zum Datenordner unter dem Speicherort, an dem **MSDE** oder **SQL Server** installiert sind. Standardmäßig ist dies **C:\Programme\Microsoft SQL Server\MSSQL**. Kopieren Sie die IT Assistant-Datenbankdatei **ITAssist\_Data.mdf** zum gewünschten Pfad auf der **ITA\_STATION**. Bzgl. dieses Beispiels nehmen wir an, der gewünschte Pfad lautet **DB\_PATH**.
5. Auf **ITA\_STATION** verbinden Sie die Datenbankdatei **ITAssist\_Data.mdf**, die sich unter **DB\_PATH** befindet, mit dem lokalen SQL Server. Sie können dies tun, indem Sie den folgenden SQL-Befehl gegen die lokale übergeordnete Datenbank ausführen:

```
exec sp_attach_single_file_db @dbname='ITAssist', @physname='DB_PATH\ITAssist_Data.mdf'
```

 **ANMERKUNG:** Stellen Sie sicher, dass sich auf dem **ITA\_STATION**-System keine **ITAssist\_Data**- und **ITAssist\_Log**-Dateien befinden.

Das erste Argument **@dbname** gibt den Namen der Datenbank an und muss als **ITAssist** beibehalten werden. Das zweite Argument **@physname** gibt an, wo sich die Datenbankdatei befindet. Hierbei sollten Sie eine Anpassung an Ihre Bedürfnisse vornehmen, um den korrekten Speicherort von **ITAssist\_Data.mdf** widerzuspiegeln. Stellen Sie sicher, dass sich in demselben Pfad keine **ITAssist\_log.ldf**-Datei befindet. Wenn eine Datei desselben Namens besteht, löschen Sie sie vor der Ausführung dieses Befehls.

### IT Assistant mit Datenbank auf ITA\_STATION verbinden

1. Auf der **ITA\_STATION** wechseln Sie zum Konfigurationsverzeichnis, in dem IT Assistant installiert ist. Bearbeiten Sie die Konfigurationsdatei **dconfig.ini**, indem Sie jede **REMOTE\_DB\_SERVER**-Zeichenkette (Name der Datenbank) unter den Abschnitten **[ITAssist\_Odbc\_Attributes]** und **[Master\_Odbc\_Attributes]** mit **(lokal)** ersetzen.
2. Auf der **ITA\_STATION** ändern Sie die Anmeldeinformationen für die IT Assistant-Dienste von "allgemeines" Konto zu Konto des "lokalen Systems". Dieser Vorgang sollte sowohl für den IT Assistant-Verbindungsdienst als auch für den IT Assistant-Netzwerküberwachungsdienst vorgenommen werden. Um diese Maßnahmen auszuführen, klicken Sie mit der rechten Maustaste vom **Service Control Manager** aus auf jeden Dienst und wählen **Eigenschaften**

aus. Wählen Sie jetzt das Register **Anmeldung** aus, um die Anmeldeinformationen zu ändern. Speichern Sie die Änderungen, und starten Sie die IT Assistant-Dienste.

3. Starten Sie IT Assistant.

## **IT Assistant erweitern**

Erweitern Sie IT Assistant anhand der neusten CD *Dell OpenManage Installation and Server Management*. Nachdem das Upgrade abgeschlossen ist, starten Sie IT Assistant.

## **Stellen Sie die IT Assistant-Datenbank für REMOTE\_DB\_SERVER bereit**

Informationen zum Verschieben der IT Assistant-Datenbank zum Remote-System finden Sie unter "[Bereitstellung der IT Assistant-Datenbank für die Remote-Datenbank](#)".

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Einführung des Dell OpenManage™ IT Assistant

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Systemverwaltung vereinfachen](#)
- [Funktionen der IT Assistant-Komponenten verstehen](#)
- [Integrierte Funktionen](#)
- [Weitere nützliche Informationen](#)

Dell OpenManage IT Assistant bietet einen zentralen Zugriffspunkt, um Systeme in einem lokalen Netzwerk (LAN) oder einem Weitverkehrsnetz (WAN) zu überwachen und zu verwalten. IT Assistant gibt Administratoren eine umfassende Ansicht des gesamten Unternehmens und kann so die Systembetriebszeit vergrößern, sich wiederholende Tasks automatisieren und eine Unterbrechung kritischer Geschäftsvorgänge verhindern.

---

### Systemverwaltung vereinfachen

Mit dem IT Assistant können Sie:

- 1 Systemgruppen zur Remote-Verwaltung identifizieren.
- 1 Die Ansicht aller Systeme konsolidieren und einen zentralen Startpunkt zur Verwaltung der Systeme bekommen.
- 1 Warnungsfilter und Maßnahmen erstellen, die Sie automatisch benachrichtigen, wenn die Systembetriebszeit betroffen ist.
- 1 Benutzerspezifische unternehmensweite Reporte erstellen, die eine ausführliche Bestandsaufnahme jedes Systems bieten.
- 1 Benutzerspezifische Tasks erstellen, die Ihnen ermöglichen, Konfigurationsverwaltung im gesamten Unternehmen zu koordinieren, einschließlich der Softwareaktualisierung, Gerätesteuerung (Herunterfahren/Hochfahren), und Befehlszeilenausführung.
- 1 Die Leistung von Systemen in Ihrem Netzwerk messen.

### Systemgruppen zur Remote-Verwaltung identifizieren

IT Assistant führt eine Ermittlung und eine Statusabfrage aus und ermöglicht Systemadministratoren, Systeme und Geräte auf einem Netzwerk durch den Host-Namen, die IP-Adresse oder den IP-Subnetzbereich zu identifizieren. Während einer Statusabfrage fragt IT Assistant den Funktionszustand bzw. den Status eines Systems und seiner Komponenten ab. Die während der Ermittlung und Statusabfrage erfassten Informationen werden in der Verwaltungskonsolle angezeigt und in der IT Assistant-Datenbank eingetragen. Die IT Assistant standardmäßig zugehörige Datenbank ist Microsoft® SQL Server 2005 Express. Benutzer, für die eine leistungsstärkere Datenbank erforderlich ist, können Microsoft SQL 2005 Server oder SQL Server 2000 verwenden.

### Anzeige aller Systeme konsolidieren

Mit dem IT Assistant können Systemadministratoren von der Verwaltungskonsolle aus Maßnahmen auf verwalteten Systemen durchführen. Mit IT Assistant können Sie Tasks erstellen, die auf ein einzelnes System oder alle Systeme in einer Gruppe angewendet werden. Sie können dynamische Systemgruppen erstellen, um die Verwaltung zu erleichtern und Bestandsaufnahmen auf Systemen durchzuführen. Außerdem bietet IT Assistant einen konsolidierten Start-URL für die folgenden Dell Systems Management-Anwendungen und Geräte: Dell OpenManage Server Administrator, Dell OpenManage Array Manager, Remote Access Console, Dell OpenManage Switch Administrator, Digital-KVM (Tastatur/Video/Maus), Drucker, Bänder, Speichergeräte sowie Geräte der intelligenten Plattform-Verwaltungsschnittstelle (IPMI).

### Warnungsfilter und -maßnahmen erstellen

Sie können IT Assistant verwenden, um *Warnungsfilter* zu erstellen, um Warnungen zu isolieren, die für einen Systemadministrator am wichtigsten sind. Systemadministratoren können dann entsprechende *Warnungsmaßnahmen* erstellen, die ausgelöst werden, wenn die Kriterien, die zur Definition des Warnungsfilters verwendet wurden, erfüllt werden. IT Assistant kann z. B. einen Systemadministrator benachrichtigen, wenn sich ein Serverlüfter in einem Warnungs- oder kritischen Zustand befindet. Durch die Erstellung eines Filters mit einer entsprechenden E-Mail-Maßnahme, wird dem Administrator eine E-Mail geschickt, wenn ein Lüfter den definierten Status erreicht. Der Administrator kann dann aufgrund der Benachrichtigung handeln, indem er das System, falls notwendig, mit IT Assistant herunterfährt oder Server Administrator zur Behebung des Problems startet.

### Benutzerspezifische Ermittlungs- und Bestandsaufnahme-Reporte erstellen

Mit dem Report-Assistent von IT Assistant können Sie benutzerspezifische Reports für alle Geräte und Gruppen im ganzen Unternehmen erstellen. Diese Reports können Gerätebestandsaufnahme-Informationen enthalten, die auf einer umfassenden Auswahl an Attributen basieren. Zum Beispiel können Sie einen Report erstellen, der Details für alle Add-On-Karten in allen Systemen einer Gruppe aufführt, darunter die Bustaktrate und -breite, Hersteller sowie Steckplatzlänge und/oder -nummer. IT Assistant bietet auch eine Sammlung vorformatierter Reports, die allgemeine Informationen vom Unternehmen sammeln.

## Tasks erstellen, die Konfigurationsverwaltung von einer Zentralkonsole aus aktivieren

IT Assistant ermöglicht Ihnen auch, allgemeine Konfigurationsverwaltungs-Tasks im gesamten Unternehmen von einer einzelnen Konsole aus zu steuern. Durch die Einrichtung einfacher Tasks mithilfe der assistentenbasierten Benutzeroberfläche (UI) von IT Assistant können Sie Gerätesteuerungs-Tasks (Herunterfahren/Hochfahren) und Softwareaktualisierungen ausführen, Agenten bereitstellen oder Befehlszeilen-Tasks auf allen Systemen der verwalteten Gruppe ausführen. IT Assistant ermöglicht Ihnen, Dell Update Packages (DUP) und Systemaktualisierungssätze in ein Zentral-Repository zu laden und deren Übereinstimmung mit Systemen im Unternehmen zu überprüfen. Der Systemadministrator kann dann IT Assistant beauftragen, die Aktualisierungen sofort oder nach einem festgelegten Plan auszuführen.

**ANMERKUNG:** Um eine Softwareaktualisierung auszuführen, muss die entsprechende Agent-Software auf dem Zielgerät installiert sein. Weitere Informationen zu Agenten finden Sie unter "[Agenten auf den zu überwachenden Systemen](#)".

## Die Leistung von Systemen in Ihrem Netzwerk messen

IT Assistant hilft Ihnen, über einen festgelegten Zeitraum hinweg die Leistung eines Geräts oder einer Gruppe von Geräten mit unterstützten Betriebssystemen zu überwachen. Leistung wird mithilfe eines Satzes von Leistungsindikatoren überwacht, die dazu konfiguriert werden können, Warnungen auszusenden, wenn Schwellen überschritten werden.

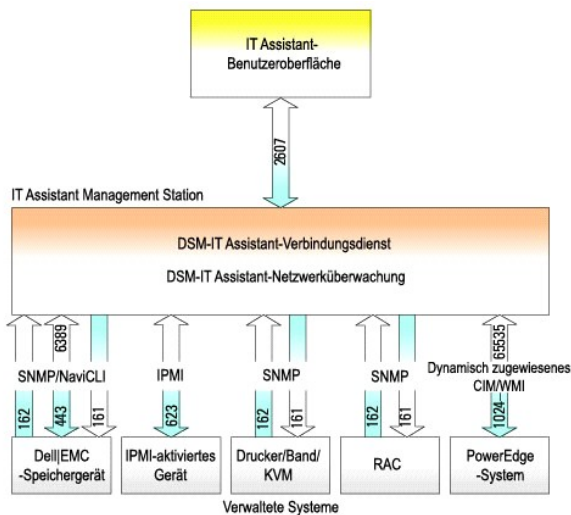
## Funktionen der IT Assistant-Komponenten verstehen

Für ein Verständnis der anderen Abschnitte in diesem Dokument müssen Sie auch die Funktionen der folgenden Komponenten des IT Assistant verstehen:


- 1 IT Assistant-Benutzeroberfläche (UI)
- 1 IT Assistant-Dienststufe (Netzwerküberwachungsdienst, Verbindungsdienst und Datenbank)
- 1 Verwaltetes System


Die IT Assistant-UI bietet eine graphische Benutzersicht der durch die IT Assistant-Dienststufe gesammelten Informationen. Diese Informationen zeigen den Gesamtfunktionszustand und Konfigurationsdetails aller Systeme in der verwalteten Gruppe. Die durch den IT Assistant überwachten Systeme in der verwalteten Gruppe, werden als *verwaltete Systeme* bezeichnet; das System, das die IT Assistant-UI ausführt, wird allgemein *Netzwerkverwaltungsstation* genannt.

Abbildung 1-1. IT Assistant - Benutzeroberfläche, Dienstesystem und verwaltetes System





 **ANMERKUNG:** Die Zahlen in [Abbildung 1-1](#) sind die von IT Assistant zur Kommunikation mit den verwalteten Systemen verwendeten Schnittstellennummern.

 **ANMERKUNG:** Weitere Informationen zu den von IT Assistant verwendeten Schnittstellen finden Sie im *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

## Benutzeroberfläche

Die IT Assistant-UI ermöglicht Ihnen die Durchführung einer großen Auswahl von Konfigurations- und Verwaltungs-Tasks, wie das Spezifizieren von Systemen zur Ermittlung, die Erstellung von Warnungsfiltren und -maßnahmen sowie das Aus- und Einschalten von Systemen.

Die IT Assistant-Benutzeroberfläche basiert auf der Java-Technologie von Sun Microsystems. Remote-Zugriff erfolgt entweder über einen Internet-Browser (Internet Explorer, Mozilla oder Firefox) oder eine Terminal-Dienstsitzung.

## IT Assistant-Dienste

Die IT Assistant-Dienststufe ist Teil der Standardinstallation. Rein technisch besteht die Dienststufe aus dem Netzwerküberwachungsdienst, dem Verbindungsdienst und der Datenbank. Bei im hohen Grade benutzerspezifischen Installationen können Benutzer eine eigene Datenbank auf einem separaten System installieren. Wenn Sie den Agenten des einfachen Netzwerkverwaltungsprotokolls (SNMP) auf einem verwalteten System konfigurieren, müssen Trap-Ziele für den SNMP-Dienst zum Host-Namen oder zur IP-Adresse des Systems hinweisen, wo IT Assistant installiert ist.

## Terminologie: Verwaltetes System und IT Assistant-System

Für die Zwecke des IT Assistant handelt es sich bei einem *verwalteten System* um ein System, auf dem unterstützte Instrumentation oder Agenten installiert sind, die es ermöglichen, dass das System ermittelt und nach seinem Status abgefragt werden kann. IT Assistant vereinfacht die Systemverwaltung auf vielen verwalteten Systemen, da Administratoren sie von einer Verwaltungskonsole aus überwachen können. Weitere Informationen zu Agenten finden Sie unter "[Agenten auf den zu überwachenden Systemen](#)".

In diesem Handbuch, werden die Begriffe *IT Assistant-System* und *Netzwerkverwaltungsstation* verwendet, um das System zu identifizieren, auf dem die IT Assistant-Software installiert ist.

---

## Integrierte Funktionen

### Systemeigene Installation

Die Softwareprodukte von Dell OpenManage Systems Management sind mithilfe eines betriebssystemeigenen Installationsverfahrens installiert.

### Benutzeroberflächendesign und Online-Hilfe

Die Benutzeroberfläche (UI) von IT Assistant umfasst assistentenbasierte Dialoge zur Ausführung zahlreicher Standard-Tasks. Die Menüleiste von IT Assistant Version 8.0 enthält neue Menüoptionen für die neuen Funktionen. Nehmen Sie sich etwas Zeit, um sich mit dem neuen Layout vertraut zu machen.

Es gibt eine umfassende Onlinehilfe, die sowohl über das Link **Hilfe** oben rechts im IT Assistant-Fenster als auch inhaltsspezifisch über die **Hilfe**-Schaltflächen innerhalb der einzelnen Dialoge verfügbar ist.

Die Benutzeroberfläche ist ausschließlich webbasiert, verwendet die Java-Technologie von Sun Microsystems und unterstützt auch Linux-Systeme.

## DMI-Support


IT Assistant unterstützt das DMI-Protokoll (Desktop-Verwaltungsschnittstelle) nicht mehr. Infolgedessen können Systeme, auf denen DMI unter Verwendung von Dell OpenManage Server Agent 4.5.1 (und früher) und Dell OpenManage Client Instrumentation 6.0 (und früher) ausgeführt wird, von IT Assistant nicht ermittelt werden.

## Topologieansicht

Auf der Benutzeroberfläche können Sie **Ansichten**→ **Topologie** auswählen, um sich eine graphische Darstellung der Geräte im Netzwerk anzeigen zu lassen. Wenn Sie auf das Symbol der Gruppe klicken, die Sie sich ansehen möchten, gehen Sie nach unten durch die Hierarchie. Zusätzlich können Sie detaillierte Geräteinformationen anzeigen, indem Sie den Cursor über die einzelnen Symbole führen. Sie können auch Tasks an den Geräten in dieser Ansicht ausführen, z. B. Starten einer Anwendung, Aktualisieren der Bestandsaufnahme und des Status und Beheben von Störungen.


## Dynamische Gruppen

Sie können dynamische Gerätegruppen erstellen, mit denen Sie Geräte effektiver verwalten und überwachen können. Weitere Informationen finden Sie unter dem Thema Gruppenkonfiguration in der *Dell OpenManage IT Assistant-Onlinehilfe*.

 **ANMERKUNG:** Sie können die in einem Modul von IT Assistant erstellten Geräteauswahlabfragen auch in anderen Modulen wiederverwenden. Eine vom Suchgerätemodul erstellte Abfrage wird auch verfügbar sein, wenn Sie einen Report, einen Warnungsfiler oder einen Task erstellen bzw. bearbeiten.

## Anwendungsstart

IT Assistant bietet die Möglichkeit einer gemeinsamen Start-URL für die folgenden Dell Systems Management-Anwendungen: Server Administrator, Array Manager, Remote Access Console, Dell OpenManage Switch Administrator und Digital-KVM (Tastatur/Video/Maus), Drucker, Bänder, Speichergeräte sowie Geräte der Intelligenten Plattform-Verwaltungsschnittstelle (IPMI). Weitere Informationen finden Sie unter dem Thema Anwendungsstart in der *IT Assistant-Onlinehilfe*.

 **ANMERKUNG:** Netzwerkadressübersetzung (NAT) ist keine unterstützte Konfiguration auf IT Assistant. Deshalb arbeitet der Anwendungsstart in Verbindung mit NAT nicht, obwohl IT Assistant die verwalteten Systeme erfolgreich ermittelt. Sie sollten IT Assistant nur dazu verwenden, eine Verbindung zu der IP-Adresse herzustellen, mit der ein System ermittelt wurde. Andere auf dem System vorhandene IP-Adressen sind für IT Assistant eventuell nicht zugänglich. In vielen Anwendungen, wie z. B. einer Server-Farm oder einer Lastenausgleichsanwendung, wird das System hinter einer NAT sein. In solchen Umgebungen kann IT Assistant keine Verbindung zum Server Administrator herstellen, der auf solchen Systemen ausgeführt wird.

## Bericht

IT Assistant bietet eine benutzerdefinierbare Report-Funktion, über die Daten der SQL Serverdatenbank gesammelt werden können. Reportergebnisse beruhen auf den Daten, die im letzten Ermittlungs- und/oder Bestandsaufnahmezyklus gesammelt wurden.

Das Design des Report-Schnittstellen-Assistenten ermöglicht die Auswahl der tatsächlichen Felder in der IT Assistant-Datenbank. Sie können einen Report mit Informationen wie den folgenden erstellen:

- 1 Details zu den Hardwaregeräten, die von IT Assistant verwaltet werden, einschließlich Systeme, Schalter und Speichergeräte
- 1 BIOS-, Firmware- und Treiberversionen
- 1 Daten zu austauschbaren Funktionseinheiten (FRU)
- 1 Andere Details zum Bestand oder den Betriebskosten

Sie können auch das Ausgabeformat, wie HTML, XML oder von Komma getrennte Werte (CSV), angeben. CSV wird normalerweise in einem Tabellenkalkulationsprogramm wie Microsoft Excel® verwendet. IT Assistant speichert die Reportdefinitionen für späteren Gebrauch und Abruf.

Um den Report-Assistenten von IT Assistant zu verwenden, wählen Sie **Ansichten**→ **Reporte**. Eine ausführliche Beschreibung der Fähigkeiten und Schritte zur Verwendung des Report-Assistenten steht in der *IT Assistant-Onlinehilfe* zur Verfügung.

## Softwareaktualisierungen

Mit IT Assistant können Sie Dell Update Packages und Systemaktualisierungssätze in ein zentrales Repository laden und dann die Pakete mit den derzeit auf

dem System ausgeführten Versionen der Software vergleichen. Sie können dann entscheiden, ob Sie die Systeme, die nicht mehr übereinstimmen, sofort oder entsprechend einem von Ihnen festgelegten Zeitplan aktualisieren möchten.

Sie können die Ansicht der Paketinformationen auch anpassen, und zwar nach Betriebssystem, Systemtyp, Komponentename und Softwaretyp.

Um die Softwareaktualisierungsfunktion zu verwenden, wählen Sie **Verwalten**→ **Softwareaktualisierungen**. Weitere Informationen finden Sie unter dem Thema Softwareaktualisierung in der *IT Assistant-Onlinehilfe*.

## Tasks verwalten

IT Assistant bietet eine aktualisierte Task-Verwaltungsfunktion, mit der bestimmte Tasks auf allen Systemen Ihres Unternehmens eingestellt und im Remote-Zugriff ausgeführt werden können, einschließlich Gerätesteuerung (Herunterfahren und Hochfahren), Softwareaktualisierung, Softwarebereitstellung und Befehlszeilenausführung.

Um diese Task-Verwaltungsfunktion zu nutzen, wählen Sie **Verwalten**→ **Tasks** aus. Weitere Informationen finden Sie unter dem Thema Task in der *IT Assistant-Onlinehilfe*.

## Fehlerbehebungshilfsprogramm

Unter **Hilfsprogramme**→ **Fehlerbehebungshilfsprogramm** steht ein graphisches Fehlerbehebungshilfsprogramm zur Verfügung, mit dem Ermittlungs- und Konfigurationsprobleme, u. a. Probleme mit SNMP und dem Allgemeinen Informationsmodell (CIM), diagnostiziert und gelöst werden können. Sie können das Hilfsprogramm auch dazu verwenden, Geräte und eine E-Mail-Konnektivität zu testen.

Weitere Informationen finden Sie in der *IT Assistant-Onlinehilfe*.

## Benutzerauthentifizierung

**Benutzer früherer IT Assistant-Versionen** sollten wissen, dass das IT Assistant 6.x Lesen/Schreiben-Kennwort nicht mehr verwendet wird. IT Assistant verwendet jetzt Betriebssystem- oder domänenbasierte Authentifizierung. Informationen zum Microsoft Active Directory®-Schema und wie man es für die Verwendung mit IT Assistant konfigurieren kann (einschließlich der Installation des erforderlichen Snap-In) finden Sie im *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

## Verbesserter Bestandsaufnahmezyklus

IT Assistant sammelt Bestandsaufnahmeinformationen wie Software und Firmware-Versionen, sowie Geräteinformationen über Speicher, Prozessoren, Netzteile, PCI-Karten und integrierte Geräte sowie Speicherplatz. In der Onlinehilfe finden Sie unter "Report hinzufügen - IT Assistant-Reportsystem verwenden" Details zu den Bestandsaufnahmeinformationen, die IT Assistant sammelt und in seiner Datenbank speichert. Informationen zur Konfiguration der Bestandsaufnahmeinstellungen finden Sie unter "Einstellungen der Bestandsaufnahmeabfrage - IT Assistant zur Ausführung von Bestandsaufnahmen konfigurieren" in der Onlinehilfe.

## Einmalige Anmeldung

Einmalige Anmeldung wird auf Windows-Systemen unterstützt. Mit der Option **Einfache Anmeldung** können Sie die Anmeldungsseite umgehen und durch Klicken auf das **IT Assistant**-Symbol auf dem Desktop direkt auf IT Assistant zugreifen. Das Desktop-Symbol erfragt bei der Registrierung, ob die Option **Automatische Anmeldung** mit aktuellem Benutzernamen und aktuellem Kennwort in Internet Explorer aktiviert ist. Wenn diese Option aktiviert ist, wird die **einfache Anmeldung** ausgeführt; andernfalls wird die normale Anmeldeseite angezeigt. Weitere Informationen zur Einstellung dieser Optionen finden Sie unter "[Einfache Anmeldung](#)".

## Benutzereinstellungen

Benutzereinstellungen sind unabhängig von Benutzerberechtigungen. Mit dieser Funktion können Sie die Ansicht der Gerätegruppen individuell einstellen. Diese Funktion ist zugänglich über **Hilfsprogramme**→ **Benutzereinstellungen**. Weitere Informationen zur Verwendung dieser Funktion finden Sie unter

"Benutzereinstellungen - IT Assistant-Benutzeroberfläche individuell einstellen" in der Onlinehilfe.

Informationen über die neuen Funktionen in IT Assistant Version 8.0 finden Sie unter "[Was ist neu in Version 8.0 des Dell OpenManage™ IT Assistant?](#)"

---

## Weitere nützliche Informationen

Das *Benutzerhandbuch* beabsichtigt eine Ansicht des IT Assistant auf höchster Ebene zu präsentieren. Nicht alle Funktionen und Fähigkeiten werden in diesem Dokument gezeigt. Alle Funktionen sind jedoch in der Online-Hilfe, die von der IT Assistant-UI aus verfügbar ist, vollkommen erklärt.

Zusätzlich stehen die folgenden Ressourcen sowohl auf Dells Support-Website unter [support.dell.com](http://support.dell.com) als auch auf der Dokumentations-CD zur Verfügung:

- 1 Im *Dell OpenManage Server Administrator: Benutzerhandbuch* werden die Funktionen, die Installation und die Dienste dokumentiert, aus denen sich die primäre Suite von Dells Serververwaltungshilfsprogrammen (eins-zu-eins) zusammensetzt.
- 1 Das *Dell OpenManage-Server Administrator-SNMP-Referenzhandbuch* dokumentiert die Server Administrator-SNMP-Verwaltungsinformationsbasis (MIB). Die MIB definiert Variablen, die über die Standard-MIB hinausgehen, um die Fähigkeiten von Systemverwaltungsagenten abzudecken.
- 1 Das *Dell OpenManage Server Administrator-CIM-Referenzhandbuch* beschreibt den Server Administrator-CIM-Anbieter, eine Erweiterung der Standard-MOF-Datei (Verwaltungs-Objektformat). Die von den MOF-Dokumenten des CIM-Anbieters unterstützten Klassen von Verwaltungsobjekten.
- 1 Das *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch* dokumentiert, wie man die Systems Management-Software von Dell OpenManage auf dem System installiert, wie man Active Directory konfiguriert und das Schema für den IT Assistant erweitert.

Sie können an zwei Stellen auf die *IT Assistant-Onlinehilfe* zugreifen: entweder indem Sie auf den **Hilfe**-Link im oberen rechten Teil des Browser-Fensters klicken, oder indem Sie auf die Schaltfläche **Hilfe** innerhalb des Dialogs oder des Assistenten klicken, den Sie verwenden.

---

[Zurück zum Inhaltsverzeichnis](#)

## Protokolle zum Senden von Informationen an Dell OpenManage™ IT Assistant konfigurieren

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [SNMP-Dienst konfigurieren](#)
- [SNMP-Agent auf Systemen konfigurieren, auf denen unterstützte Linux-Betriebssysteme ausgeführt werden](#)
- [CIM einrichten](#)

Dell OpenManage IT Assistant verwendet zwei Systemverwaltungsprotokolle - das einfache Netzwerkverwaltungsprotokoll (SNMP) und das allgemeine Informationsmodell (CIM). Dieser Anhang enthält Konfigurationsinformationen zu SNMP und CIM. Über diese Systemverwaltungsprotokolle kann IT Assistant den Status von Dell™ PowerEdge™-Systemen mithilfe von Serveragenten oder der Dell OpenManage Client Instrumentation (OMCI) abfragen. Dieser Anhang umfasst Verfahren zur Konfiguration von SNMP und CIM, die die Ermittlungs-, Status- und Trap-Informationen unterstützen. In der folgenden Tabelle werden die unterstützten Betriebssysteme sowie die entsprechenden SNMP- und CIM-Protokolle für Systeme aufgeführt, die vom IT Assistant verwaltet werden können.

Tabelle A-1. Auf verwalteten Systemen unterstützte Betriebssysteme und Systemverwaltungsprotokolle

Betriebssystem	SNMP	CIM
Microsoft® Windows®-Betriebssystem	Auf dem Installationsdatenträger des Betriebssystems verfügbar.	Auf dem Installationsdatenträger des Betriebssystems verfügbar
Red Hat® Linux-Betriebssystem	Das mit dem Betriebssystem gelieferte SNMP-Paket muss installiert werden.	Nicht verfügbar
Betriebssystem SUSE® Linux Enterprise Server	Das mit dem Betriebssystem gelieferte SNMP-Paket muss installiert werden.	Nicht verfügbar

### SNMP-Dienst konfigurieren

Damit der IT Assistant richtig installiert und betrieben werden kann, müssen die Dienste auf einem unterstützten Microsoft-Betriebssystem installiert sein, auf dem der SNMP-Dienst installiert und ausgeführt wird. Der SNMP-Dienst des Microsoft-Betriebssystems sollte keine weitere Konfiguration erfordern, es sei denn, der Dienst wurde nach der Installation geändert. Obwohl für den SNMP-Dienst auf dem IT Assistant-System keine besondere Konfiguration erforderlich ist, müssen die SNMP-Dienste auf den verwalteten Systemen besonders konfiguriert werden. Während IT Assistant nur auf unterstützten Microsoft-Betriebssystemen installiert werden kann, kann er Systeme verwalten, auf denen unterstützte Microsoft-, SUSE® Linux Enterprise Server- und Red Hat Enterprise Linux-Betriebssysteme ausgeführt werden. In diesem Abschnitt wird die Konfiguration von SNMP auf diesen verwalteten Systemen beschrieben.

Jedem verwalteten System, auf dem das SNMP-Protokoll zur Kommunikation mit IT Assistant verwendet wird, müssen Lesen/Schreiben- sowie schreibgeschützte Community-Namen zugewiesen sein. Wenn der IT Assistant Traps von diesen verwalteten Systemen empfangen soll, muss ebenfalls ein SNMP-Trap-Ziel konfiguriert werden, das entweder durch einen Host-Namen oder eine IP-Adresse definiert ist.

### SNMP-Community-Namen im IT Assistant und Server Administrator

Damit der IT Assistant erfolgreich Informationen lesen, Informationen ändern und Maßnahmen auf einem System durchführen kann, auf dem Dell OpenManage Server Administrator (der von Dell empfohlene Server Agent) und/oder andere unterstützte Agenten ausgeführt werden, müssen die vom IT Assistant verwendeten Community-Namen mit den entsprechenden Nur-Lesen- (Get) und Lesen/Schreiben- (Set) Community-Namen auf dem verwalteten System übereinstimmen. Damit der IT Assistant also Traps (asynchrone Ereignisbenachrichtigungen) von einem System empfangen kann, auf dem Server Administrator ausgeführt wird, muss das System für das Senden von Traps zu dem System, auf dem IT Assistant ausgeführt wird, konfiguriert sein. Weitere Informationen finden Sie unter ["SNMP für Systemverwaltungsfunktionen konfigurieren"](#).

### Community-Namen müssen sicher sein

Das Betriebssystem enthält Standardnamen für die Get und Set Community-Namen. Aus Sicherheitsgründen sollten diese Namen geändert werden. Beachten Sie bei der Auswahl der Community-Namen für das Netzwerk die folgenden Richtlinien:

- 1 Ändern Sie sowohl den Get als auch den Set Namen in schwer zu erratende Kennwörter.
- 1 Vermeiden Sie bestimmte Zeichenketten, wie z. B. Name oder Telefonnummer des Unternehmens oder bekannte persönliche Informationen.
- 1 Verwenden Sie eine alphanumerische Zeichenkette mit Buchstaben und Ziffern und vermischen Sie Groß- und Kleinschreibung; bei Community-Namen muss Groß- und Kleinschreibung beachtet werden.

1. Verwenden Sie mindestens sechs Zeichen lange Zeichenketten.

## SNMP-Dienst auf einem System konfigurieren, auf dem ein unterstütztes Windows-Betriebssystem ausgeführt wird

### IT Assistant ausführen

IT Assistant kann auf einem System installiert werden, auf dem eines der folgenden Betriebssysteme ausgeführt wird: Windows 2000, Windows XP Professional oder Windows Server® 2003. Aktuelle Informationen über unterstützte Betriebssysteme und Hardwarekonfigurationen finden Sie in der Infodatei.


Um SNMP auf dem IT Assistant-System zu installieren, führen Sie folgende Schritte durch:


1. Klicken Sie auf die Schaltfläche **Start**, zeigen Sie auf **Einstellungen** und wählen Sie **Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Software**.
3. Klicken Sie im Fenster auf der linken Seite auf **Windows-Komponenten hinzufügen/entfernen**.
4. Wählen Sie **Verwaltungs- und Überwachungshilfsprogramme** aus, klicken Sie auf **Details**, wählen Sie **Einfaches Netzwerkverwaltungsprotokoll** und klicken Sie auf **OK**.
5. Klicken Sie auf **Weiter**.

Der **optionale Windows Netzwerkkomponenten-Assistent** installiert SNMP.

## SNMP-Dienst auf einem mit IT Assistant verwalteten System konfigurieren, auf dem ein unterstütztes Windows-Betriebssystem ausgeführt wird

Server Administrator und bestimmte verwaltete Systemagenten, wie z. B. Dell PowerConnect™-Schalter, verwenden das SNMP-Protokoll zur Kommunikation mit dem IT Assistant. Zur Aktivierung dieser Kommunikation muss der Windows SNMP-Dienst richtig konfiguriert werden, um **Get und Set Vorgänge** zu aktivieren und um Traps an ein Dienstesystem zu senden.

 **ANMERKUNG:** Weitere Einzelheiten zur SNMP-Konfiguration finden Sie in der Dokumentation des Betriebssystems.

 **ANMERKUNG:** Um Systeme zu ermitteln, auf denen Windows Server 2003 ausgeführt wird, erfordert die SNMP-Standardkonfiguration von Microsoft auf Windows Server 2003, dass SNMP zur Annahme von Paketen vom IT Assistant-Host konfiguriert ist.

### SNMP-Community-Namen ändern

Durch die Konfiguration der SNMP-Community-Namen wird festgelegt, welche Systeme das System über SNMP verwalten können.

1. Falls Windows Server 2003 auf dem System ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**. Falls Windows 2000 auf dem System ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**.

Das Fenster **Computerverwaltung** wird eingeblendet.

2. Erweitern Sie im Fenster das Symbol **Computerverwaltung**, falls erforderlich.
3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. Führen Sie einen Bildlauf durch die Liste der Dienste durch, bis Sie **SNMP-Dienst** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und klicken Sie dann auf **Eigenschaften**.

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

5. Klicken Sie auf das Register **Sicherheit**, um einen Community-Namen hinzuzufügen oder zu bearbeiten.
  - a. Um einen Community-Namen hinzuzufügen, klicken Sie unterhalb der Liste **Zugelassene Community-Namen** auf **Hinzufügen**.

Das Fenster **Konfiguration SNMP-Dienst** wird eingeblendet.

- b. Geben Sie im Textfeld **Community-Name** den Community-Namen eines Systems ein, das in der Lage ist, das System zu verwalten (die Standardeinstellung lautet `public`) und klicken Sie auf **Hinzufügen**.

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

- c. Wählen Sie zum Ändern eines Community-Namens einen entsprechenden Community-Namen aus der Liste **Zugelassene Community-Namen** aus und klicken Sie auf **Bearbeiten**.

Das Fenster **Konfiguration SNMP-Dienst** wird eingeblendet.

- d. Nehmen Sie im Textfeld **Community-Name** alle erforderlichen Änderungen am Community-Namen des Systems vor, das in der Lage ist, das System zu verwalten, und klicken Sie auf **OK**.

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

## SNMP-Set-Vorgänge aktivieren

SNMP Set Vorgänge müssen auf dem verwalteten System aktiviert werden, um Server Administrator-Attribute mithilfe des IT Assistant zu ändern.

1. Falls Windows Server 2003 auf dem System ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**. Falls Windows 2000 auf dem System ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**.

Das Fenster **Computerverwaltung** wird eingeblendet.

2. Erweitern Sie im Fenster das Symbol **Computerverwaltung**, falls erforderlich.
3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. Führen Sie einen Bildlauf durch die Liste der Dienste durch, bis Sie **SNMP-Dienst** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und klicken Sie dann auf **Eigenschaften**.

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

5. Klicken Sie auf das Register **Sicherheit**, um die Zugriffsrechte für eine Community zu ändern.
6. Wählen Sie einen Community-Namen aus der Liste **Zugelassene Community-Namen** und klicken Sie dann auf **Bearbeiten**.

Das Fenster **Konfiguration SNMP-Dienst** wird eingeblendet.

7. Ändern Sie die **Community-Rechte** zu **LESEN SCHREIBEN** oder **LESEN ERSTELLEN** und klicken Sie auf **OK**.

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

## Das System zum Senden von SNMP-Traps konfigurieren

Verwaltete Systemagenten, wie z. B. der Server Administrator, erzeugen auf verwalteten Systemen SNMP-Traps bei Statusänderungen der Sensoren und anderer auf einem verwalteten System überwachter Parameter. Um diese Traps an ein IT Assistant-System zu senden, müssen ein oder mehrere Trap-Ziele auf dem verwalteten System konfiguriert werden.

1. Falls Windows Server 2003 auf dem System ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**. Falls Windows 2000 auf dem System ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**.

Das Fenster **Computerverwaltung** wird eingeblendet.

2. Erweitern Sie im Fenster das Symbol **Computerverwaltung**, falls erforderlich.

3. Erweitern Sie das Symbol **Dienste und Anwendungen** und klicken Sie auf **Dienste**.
4. **Führen Sie einen Bildlauf durch die Liste der Dienste durch, bis Sie **SNMP-Dienst** finden, klicken Sie mit der rechten Maustaste auf **SNMP-Dienst** und klicken Sie dann auf **Eigenschaften**.**

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

5. Klicken Sie auf das Register **Traps**, um eine Community für Traps hinzuzufügen oder um ein Trap-Ziel für eine Trap-Community hinzuzufügen.
6. **Um eine Community für Traps hinzuzufügen, geben Sie den Community-Namen im Feld **Community-Name** ein und klicken Sie auf **Hinzufügen**.**
7. **Um ein Trap-Ziel für eine Trap-Community hinzuzufügen, wählen Sie den Community-Namen im Dropdown-Menü **Community-Name** aus und klicken Sie auf **Hinzufügen**.**

Das Fenster **Konfiguration SNMP-Dienst** wird eingeblendet.

8. Geben Sie das Trap-Ziel ein und klicken Sie auf **Hinzufügen**.

Das Fenster **Eigenschaften SNMP-Dienst** wird eingeblendet.

9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

---

## SNMP-Agent auf Systemen konfigurieren, auf denen unterstützte Linux-Betriebssysteme ausgeführt werden

In diesem Abschnitt wird die Konfiguration von SNMP-Agenten auf Systemen beschrieben, auf denen die Betriebssysteme Red Hat Enterprise Linux und SUSE Linux Enterprise Server ausgeführt werden.

Verwaltete Systemagenten, wie z. B. der Server Administrator, verwenden die SNMP-Dienste des ucd-snmp oder net-snmp SNMP-Agenten. Der SNMP-Agent kann so konfiguriert werden, dass er **Community-Namen ändert, Set-Vorgänge aktiviert und Traps an ein IT Assistant-System sendet**. Führen Sie die in den folgenden Abschnitten beschriebenen Verfahren zur Konfiguration des SNMP-Agenten für die **sachgemäße Kommunikation mit dem IT Assistant aus**.



**ANMERKUNG:** Weitere Einzelheiten zur SNMP-Konfiguration finden Sie in der Dokumentation des Betriebssystems.

### SNMP-Community-Namen ändern

Durch die richtige Konfiguration der SNMP-Community-Namen wird festgelegt, welche IT Assistant-Dienstesysteme mit verwalteten Systemen im Netzwerk kommunizieren können. Der vom IT Assistant verwendete SNMP-Community-Name muss mit einem auf einem verwalteten System konfigurierten SNMP-Community-Namen übereinstimmen, so dass der IT Assistant von bzw. auf den verwalteten Systemen im Netzwerk **lesen, schreiben und Maßnahmen durchführen** kann.

Um den SNMP-Community-Namen zu ändern, bearbeiten Sie die Konfigurationsdatei `/etc/snmp/snmpd.conf` des SNMP-Agenten, indem Sie folgende Schritte durchführen:

1. Suchen Sie die folgende Zeile:

```
com2sec publicsec default public
```

oder

```
com2sec notConfigUser default public
```

2. Bearbeiten Sie diese Zeile, indem Sie `public` durch den neuen SNMP-Community-Namen ersetzen. Die bearbeitete Zeile sollte wie folgt lauten:

```
com2sec publicsec default Community-Name
```



oder

```
com2sec notConfigUser default Community-Name
```

Um den SNMP-Community-Namen in SUSE Linux Enterprise Server zu ändern, bearbeiten Sie die Konfigurationsdatei `/etc/snmpd.conf` des SNMP-Agenten, indem Sie folgende Schritte ausführen:

1. Suchen Sie die folgende Zeile:

```
rocommunity public 127.0.0.1
```

2. Bearbeiten Sie diese Zeile, indem Sie `rocommunity` durch den neuen SNMP-Community-Namen ersetzen. Die bearbeitete Zeile sollte wie folgt lauten:

```
rwcommunity public <IP-Adresse des ITA-Systems>
```

## SNMP-Set-Vorgänge aktivieren

SNMP Set-Vorgänge müssen auf dem System aktiviert werden, auf dem Server Administrator ausgeführt wird, um Server Administrator-Attribute mithilfe des IT Assistant zu ändern. Um SNMP-Set-Vorgänge auf dem System zu aktivieren, auf dem Server Administrator ausgeführt wird, bearbeiten Sie die Konfigurationsdatei des SNMP-Agenten, `/etc/snmp/snmpd.conf` (`/etc/snmpd.conf` bei SUSE Linux Enterprise Server), und führen folgende Schritte aus:

1. Suchen Sie die folgende Zeile:

```
access publicgroup "" any noauth exact all none none
```

oder

```
access notConfigGroup "" any noauth exact all none none
```

2. Bearbeiten Sie diese Zeile und ersetzen Sie das erste `none` durch `all`. Die bearbeitete Zeile sollte wie folgt lauten:

```
access publicgroup "" any noauth exact all all none
```

oder

```
access notConfigGroup "" any noauth exact all all none
```

Für die Betriebssysteme Red Hat Enterprise Linux (Version 7.3 oder höher) und Red Hat Enterprise Linux AS (Version 2.1 oder höher) wurde der standardmäßige SNMP-Zugriff für die Variablen `sysLocation` und `sysContact` zum Nur-Lese-Zugriff geändert. IT Assistant verwendet die Zugriffsrechte dieser Variablen, um zu bestimmen, ob bestimmte Maßnahmen von SNMP durchgeführt werden können oder nicht. Diese Variablen müssen mit Lese-Schreib-Zugriff konfiguriert sein, um "Sets" oder Systemkonfigurations-Einstellungsänderungen in IT Assistant zu aktivieren. Um die Variablen zu konfigurieren, wird empfohlen, dass Sie die Werte `sysContact` und `sysLocation` in der SNMP-Konfigurationsdatei von Red Hat Enterprise Linux and SUSE Linux Enterprise Server auskommentieren.

1. Suchen Sie die Zeile, die mit `sysContact` beginnt.
2. Ändern Sie die Zeile zu `#sysContact`.
3. Suchen Sie die Zeile, die mit `sysLocation` beginnt.
4. Ändern Sie die Zeile zu `#sysLocation`.

## Verwaltete Systeme zum Senden von Traps an den IT Assistant konfigurieren

Verwaltete Systemagenten, wie z. B. der Server Administrator, erzeugen auf verwalteten Systemen SNMP-Traps bei Statusänderungen der Sensoren und

anderer auf einem verwalteten System überwachter Parameter. Damit IT Assistant diese Traps empfangen kann, müssen ein oder mehrere Trap-Ziele auf dem verwalteten System konfiguriert werden.

Um Ihr System, auf dem Server Administrator ausgeführt wird, zum Senden von Traps an ein Dienstesystem zu konfigurieren, bearbeiten Sie die Konfigurationsdatei des SNMP-Agenten, `/etc/snmp/snmpd.conf` (`/etc/snmpd.conf` bei SUSE Linux Enterprise Server), indem Sie folgende Schritte ausführen:

1. Fügen Sie folgende Zeile zur Datei hinzu:

```
trapsink IP-Adresse Community-Name
```

wobei *IP-Adresse* die IP-Adresse des Dienstesystems und *Community-Name* den SNMP-Community-Namen darstellt.

2. Speichern Sie die Datei `snmpd.conf` und starten Sie den `snmpd`-Dienst neu.

---

## CIM einrichten


CIM steht nur auf unterstützten Microsoft Windows-Betriebssystemen zur Verfügung.


## CIM auf verwalteten Systemen einrichten

Dieser Unterabschnitt enthält Schritte zur Einrichtung von CIM auf verwalteten Systemen, auf denen unterstützte Windows-Betriebssysteme ausgeführt werden. Weitere Informationen finden Sie unter "[CIM für Verwaltungsfunktionen konfigurieren](#)".


## Empfehlung für die Erstellung eines Domänen-Administrators

Obwohl im folgenden Verfahren beschrieben wird, wie ein lokaler Administrator zu einem unterstützten Windows-Betriebssystem hinzugefügt wird, empfiehlt Dell, einen Domänenadministrator statt eines Benutzers auf jedem vom IT Assistant verwalteten System zu erstellen. Das Erstellen eines Domänenbenutzerkontos verhindert auch ein Sperren von Konten aufgrund von fehlgeschlagenen IT Assistant-Anmeldungen an Systeme, die im eingegebenen Ermittlungsbereich liegen. Der Ermittlungsbereich `192.168.0.*` würde z. B. zu dem Versuch führen, eine Anmeldung an allen 253 Systemen durchzuführen. Falls die an eines dieser verwalteten Systeme weitergeleiteten Informationen nicht authentifiziert werden könnten, würde das Konto gesperrt. Die höhere Sicherheit unter Windows XP bedeutet außerdem, dass sich der Client in derselben Domäne wie das IT Assistant-System befindet. Windows XP erfordert außerdem einen Benutzernamen und ein Kennwort (das Feld darf nicht leer sein). Weitere Informationen über das Erstellen eines Windows Domänenbenutzerkontos finden Sie in der Microsoft Dokumentation.

 **ANMERKUNG:** IT Assistant erfordert den CIM-Benutzernamen und das Kennwort mit Administratorrechten, der/das auf den verwalteten Systemen eingerichtet wurde. Stellen Sie bei der Verwendung eines Domänenbenutzers sicher, dass im Feld Benutzername die richtige Domäne angegeben wird. Ein Benutzername muss immer mit einer Domäne gekennzeichnet sein, oder mit `lokaler Host`, wenn keine Domäne vorhanden ist. Das Format ist entweder `Domäne\Benutzer` oder `lokaler Host\Benutzer`.

 **ANMERKUNG:** Zur CIM-Ermittlung sind korrekte Benutzer-ID und Kennwort erforderlich. Bei falscher Angabe dieser Informationen auf einem zur CIM-Ermittlung konfigurierten Subnetz könnte das Konto ausgeschlossen werden.

## Für verwaltete Systeme unter Windows 2000

 **ANMERKUNG:** Der WMI-Kern wird standardmäßig mit Windows 2000 installiert.

1. Klicken Sie auf **Start** → **Einstellungen** → **Systemsteuerung** → **Verwaltung** → **Computerverwaltung**.
2. Erweitern Sie in der Struktur **Computerverwaltung (lokal)** die Verzweigung **Lokale Benutzer und Gruppen** und klicken Sie auf den Ordner **Benutzer**.
3. Klicken Sie in der Menüleiste auf **Verfahren** und dann auf **Neuer Benutzer**.
  - a. Tragen Sie im Dialogfeld **Neuer Benutzer** den Benutzernamen und das Kennwort, z. B. `CIMUser` und `DELL`, in die erforderlichen Informationsfelder ein. (Diese Beispiele dienen nur zur Illustration; Sie sollten Benutzernamen und Kennwörter wählen, die angemessen für Ihr Unternehmen sind).
  - b. Stellen Sie sicher, dass das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** nicht ausgewählt ist.
  - c. Klicken Sie auf **Erstellen**.
4. Doppelklicken Sie in der rechten Hälfte des Dialogfelds **Computerverwaltung** auf `CIMUser`.

Die Liste muss eventuell durchlaufen werden, um **CIMUser** anzuzeigen.

5. Klicken Sie im Dialogfeld **Eigenschaften von CIMUser** auf das Register **Mitglied von**.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Administratoren**, auf **Hinzufügen** und dann auf **OK**.
8. Klicken Sie erneut auf **OK** und schließen Sie das Dialogfeld **Computerverwaltung**.
9. Installieren Sie Client Instrumentation 7.x oder Server Administrator, abhängig davon, ob es sich bei dem System um einen Client oder einen Server handelt.
10. Starten Sie das System neu.

## Für verwaltete Systeme unter Windows XP Professional


Die zuvor erwähnte höhere Sicherheit unter Windows XP bedeutet, dass sich der Client in derselben Domäne wie das IT Assistant-System befindet. Bei der Implementierung eines eigenen Benutzernamens und Kennworts sollte kein leerer Eintrag für das Kennwort erfolgen.

Um einen neuen lokalen Benutzer zu erstellen, führen Sie folgende Schritte durch: Dell empfiehlt dringend, einen Domänenbenutzer mit Administratorrechten zu erstellen, so dass ein Benutzer nicht manuell von Hand jedem Client hinzugefügt werden muss. Dadurch wird das Erstellen der Ermittlungsbereiche im IT Assistant erheblich vereinfacht.

1. Klicken Sie auf **Start**→ **Einstellungen**→ **Systemsteuerung**→ **Verwaltung**→ **Computerverwaltung**.
2. Erweitern Sie in der Struktur **Computerverwaltung (lokal)** die Verzweigung **Lokale Benutzer und Gruppen** und klicken Sie auf den Ordner **Benutzer**.
3. Klicken Sie in der Menüleiste auf **Verfahren** und dann auf **Neuer Benutzer**.
  - a. Tragen Sie im Dialogfeld **Neuer Benutzer** den Benutzernamen **CIMUser** und das Kennwort **DELL** in die erforderlichen Informationsfelder ein.
  - b. Stellen Sie sicher, dass das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** nicht ausgewählt ist.
  - c. Klicken Sie auf **Erstellen**.
4. Doppelklicken Sie in der rechten Hälfte des Dialogfelds **Computerverwaltung** auf **CIMUser**.

Die Liste muss eventuell durchlaufen werden, um **CIMUser** anzuzeigen.

5. Klicken Sie im Dialogfeld **Eigenschaften von CIMUser** auf das Register **Mitglied von**.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Administratoren**, auf **Hinzufügen** und dann auf **OK**.
8. Klicken Sie erneut auf **OK** und schließen Sie das Dialogfeld **Computerverwaltung**.

 **ANMERKUNG:** Windows XP Professional wird nur zur Verwendung auf IT Assistant-Client-Systemen unterstützt.

9. Installieren Sie Client Instrumentation 7.x oder Server Administrator, abhängig davon, ob es sich bei dem System um einen Client oder einen Server handelt.
10. Starten Sie das System neu.

## Für verwaltete Systeme unter Windows Server 2003

1. Klicken Sie auf **Start**→ **Einstellungen**→ **Systemsteuerung**→ **Verwaltung**→ **Computerverwaltung**.
2. Erweitern Sie in der Struktur **Computerverwaltung (lokal)** die Verzweigung **Lokale Benutzer und Gruppen** und klicken Sie auf den Ordner **Benutzer**.
3. Klicken Sie in der Menüleiste auf **Verfahren** und dann auf **Neuer Benutzer**.
  - a. Tragen Sie im Dialogfeld **Neuer Benutzer** den Benutzernamen **CIMUser** und das Kennwort **DELL** in die erforderlichen Informationsfelder ein.
  - b. Stellen Sie sicher, dass das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** nicht ausgewählt ist.
  - c. Klicken Sie auf **Erstellen**.
4. Doppelklicken Sie in der rechten Hälfte des Dialogfelds **Computerverwaltung** auf **CIMUser**.

Die Liste muss eventuell durchlaufen werden, um **CIMUser** anzuzeigen.

5. Klicken Sie im Dialogfeld **Eigenschaften von CIMUser** auf das Register **Mitglied von**.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **Administratoren**, auf **Hinzufügen** und dann auf **OK**.

8. Klicken Sie erneut auf **OK** und schließen Sie das Dialogfeld **Computerverwaltung**.
  9. Installieren Sie Client Instrumentation 7.x oder Server Administrator, abhängig davon, ob es sich bei dem System um einen Client oder einen Server handelt.
  10. Starten Sie das System neu.
- 

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Dienstprogramme von Dell OpenManage™ IT Assistant

### Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [IT Assistant-Knotenlistenimport-Dienstprogramm](#)
- [Datenbankverwaltungs-Dienstprogramm](#)
- [Ereignisquellen-Importdienstprogramm des einfachen Netzwerkverwaltungsprotokolls](#)

IT Assistant hat drei Dienstprogramme:

- 1 Knotenlistenimport-Dienstprogramm
- 1 Datenbankverwaltungs-Dienstprogramm
- 1 Ereignisquellen-Importdienstprogramm des einfachen Netzwerkverwaltungsprotokolls (SNMP)

---

## IT Assistant-Knotenlistenimport-Dienstprogramm

Mit dem **Knotenlistenimport**-Dienstprogramm kann eine Datei erstellt werden, in der eine Ermittlungsliste definiert wird, die aus verwalteten Geräten, IP-Adressen oder IP-Adressbereichen besteht. Dieses Dienstprogramm unterstützt jegliche Adressenart, die mit der IT Assistant-Benutzeroberfläche eingegeben werden kann. Das IT Assistant-Knotenlistenimport-Dienstprogramm verwendet die Datei, um die Liste schnell in den IT Assistant zu importieren. Die Verwendung dieses Dienstprogramms bietet:

- 1 Eine einfache Methode zum schnellen Import einer Konfiguration in den IT Assistant für die Benutzer, die ihre Netzwerkkonfiguration bereits in Dateien zugeordnet haben
- 1 Eine sehr gezielte Ermittlung, statt der Angabe eines allgemeinen Subnetzes zur Ermittlung, wie z. B. 10.34.56.\*

Um das **Knotenlistenimport**-Dienstprogramm zu verwenden, führen Sie folgende allgemeine Schritte durch:

1. Erstellen Sie eine Datei, die die Liste von Ermittlungsadressen und/oder Systemnamen enthält, die importiert werden sollen.

Für jeden Eintrag in der Datei müssen die Protokolleinstellungen angegeben werden (wie z. B. der Community-Name des SNMP-Protokolls). Um diese Informationen dem IT Assistant zur Verfügung zu stellen, muss eine Vorlage verwendet werden. Mit einer Vorlage können jedem Eintrag in der Datei Protokolleinstellungen zugewiesen werden.

2. Definieren Sie eine Vorlage, die auf einen oder mehrere Ermittlungsbereiche angewendet wird. Eine Vorlage wird definiert, indem ein Ermittlungsbereich mit dem Host-Namen `Standard_Vorlage` eingegeben wird. Das Knotenlistenimport-Dienstprogramm wendet die in dieser Vorlage definierten Protokolleinstellungen auf jedes Ermittlungselement in dieser Datei an.
3. Führen Sie das Dienstprogramm von der Befehlszeile aus. (Das Knotenlistenimport-Dienstprogramm befindet sich im IT Assistant-Verzeichnis `/bin`.) Geben Sie den Dateinamen der von Ihnen erstellten Datei und wahlweise auch den Vorlagennamen an. Der Vorlagename kann auch in der Datei angegeben werden. Beispiel:

```
importnodelist Knotenliste.txt
```

Es stehen die folgenden Optionen zur Verfügung, die in jeglicher Reihenfolge nach dem Dateinamen angegeben werden können:

**-delete** - Mit dieser Option wird/werden die verwendete(n) Vorlage(n) automatisch gelöscht, nachdem das Dienstprogramm die Knotenliste erfolgreich importiert hat.

**-default <Vorlagename>** - Lässt die Verwendung eines anderen Standard-Vorlagennamens zu. Der Standardname ist **Standard\_Vorlage**.

Weitere Informationen finden Sie in den Beispielsbefehlen.

4. IT Assistant-Dienste neu starten.

Zum Importieren einer Ermittlungsliste in den IT Assistant kann eine Standardvorlage verwendet werden. Um eine Knotenliste zu importieren, führen Sie folgende Schritte aus:

1. Erstellen Sie eine Datei im folgenden Format (ohne die Angaben <begin\_file> oder <end\_file>):

```
<begin_file>
```

```
#This is a comment (a "#" sign at the beginning of the line means to #ignore the line).  
(Dies ist eine Anmerkung [das Symbol "#" am Anfang einer Zeile bedeutet, dass die Zeile #ignoriert werden soll]).
```

```
23.45.65.34
```

```
23.45.65.35
```

```
hostname1
```

```
hostname2
```

```
23.34.55.*
```

```
12.34.56.20-30
```

```
<end_file>
```

Die letzte Zeile in der Datei muss einen Zeilenvorschub enthalten. Es kann auch jegliche Kombination von Subnetzformaten verwendet werden, die von der IT Assistant-Benutzeroberfläche unterstützt werden. Es muss darauf geachtet werden, dass jeder Eintrag ein korrektes Format besitzt, da das Knotenlistenimport-Dienstprogramm das Format für Sie nicht überprüft oder validiert.

2. Speichern Sie die Datei und geben Sie einen Dateinamen an, wie z. B. **Knotenliste.txt**.

## Beispielsbefehle des Knotenlistenimport-Dienstprogramms

Importieren der Knoten aus der Datei **Knotenliste.txt**:

```
importnodelist Knotenliste.txt
```

Die Vorlagen nach einem erfolgreichen Importieren löschen:

```
importnodelist -delete
```

Die Knoten aus der Datei **Knotenliste.txt** importieren, die verwendeten Vorlagen nach dem erfolgreichen Importieren löschen und "meine\_Vorlage" als Standard-Vorlagenamen verwenden:

```
importnodelist Knotenliste.txt -delete -default meine_Vorlage
```

## Vorlagen erstellen

Folgen Sie diesen allgemeinen Schritten, um für das Knotenlistenimport-Dienstprogramms eine Vorlage zu erstellen:

1. Unter **Ermittlung und Überwachung** wählen Sie **Bereiche**.
2. Klicken Sie mit der rechten Maustaste in der Struktur **Ermittlungsbereiche** auf **Einschlussbereiche**, und wählen Sie **Neuer Einschlussbereich...**
3. Wählen Sie unter **Assistent zur Neuermittlung, Schritte 1 bis 6** **Host-Name** aus.
4. Geben Sie unter **Host-Name** den Vorlagennamen ein (z. B. Vorlage\_1).
5. Schließen Sie den Assistenten ab, indem Sie die erforderlichen Protokollkonfigurationen eingeben.

Vorlage\_1 kann im Knotenlistenimport-Dienstprogramm verwendet werden.

## Verwendung von mehreren Vorlagen

Das Knotenlistenimport-Dienstprogramm unterstützt die Verwendung von mehreren Vorlagen, wobei jeder einzelne Eintrag in der Datei verschiedene Protokolleinstellungen verwenden kann und unterschiedliche Vorlagen erfordert. Die folgende Importdatei stellt ein Beispiel der Verwendung von mehreren Vorlagen dar:

```
<begin_file>
```

```
#This is a comment (a "#" sign at the beginning of the line means to ignore #the line).  
(Dies ist eine Anmerkung [das Symbol "#" am Anfang einer Zeile bedeutet, dass die Zeile #ignoriert werden soll]).
```

```
23.45.65.34,template1
```

```
23.45.65.35,template1
```

```
hostname1
```

```
hostname2,template2
```

```
23.34.55.*,template2
```

```
12.34.56.20-30
```

```
<end_file>
```

In diesem Beispiel verwenden die ersten zwei Einträge eine Vorlage mit dem Namen **Vorlage1** und Einträge vier und fünf eine Vorlage mit dem Namen **Vorlage2**. Alle anderen Einträge verwenden die Standardvorlage. In diesem Beispiel müssen die Ermittlungs-Konfigurationsbereiche von "Standard\_Vorlage", "Vorlage1" und "Vorlage2" eingegeben (in der IT Assistant-Benutzeroberfläche) und deren Protokolleinstellungen ordnungsgemäß konfiguriert werden (sie besitzen eventuell verschiedene SNMP-Community-Namen). Beachten Sie, dass jeglicher Name als Vorlagenname verwendet werden kann, sogar eine IP-Adresse oder ein Subnetzbereich. Dell empfiehlt jedoch die Verwendung von Namen, die das Identifizieren einer Vorlage erleichtern.

## Vorlagen speichern

Falls mehrere Vorlagen zur richtigen Konfiguration einer Datei mit Knoteneinträgen erforderlich sind, ist es möglich, die Vorlagen in IT Assistant einzurichten und dann die Einstellungen für den Backup oder zu einem anderen Zweck zu exportieren. Das Datenbankverwaltungs-Dienstprogramm, **dcdbmng.exe**, befindet sich im IT Assistant-Verzeichnis **/bin**. Mit diesem Dienstprogramm können IT Assistant-Datenbanktabellen importiert, exportiert und geleert werden. Um Vorlagen zu exportieren, führen Sie folgende Schritte aus:

1. Konfigurieren Sie alle erforderlichen Vorlagen im IT Assistant.
2. Exportieren Sie die Tabelle, die alle eingegebenen Vorlagen enthält. Navigieren Sie zum IT Assistant-Verzeichnis **/bin**, und doppelklicken Sie auf **dcdbmng.exe**. Die Datenbankverwaltungs-Dienstprogrammoberfläche wird gestartet. Navigieren Sie in der linken Struktur zur Ermittlungskonfigurations-Tabelle. Klicken Sie mit der rechten Maustaste auf diesen Strukturknoten und wählen Sie **Tabelle exportieren** aus. Geben Sie einen Namen für die Datei ein, in die exportiert werden soll.

Die Datei mit den enthaltenen Vorlagen kann jetzt in eine andere IT Assistant-Installation importiert werden. Die Datei kann auch in einer neuen IT Assistant-Installation wiederhergestellt werden, indem die Option Tabelle importieren verwendet wird (klicken Sie mit der rechten Maustaste auf den Tabellennamen im Datenbankverwaltungs-Dienstprogramm). Nachdem die Vorlagen importiert wurden, kann das Knotenlistenimport-Dienstprogramm mit der beigefügten Knoteneintragdatei ausgeführt werden.


## Vorlagen im IT Assistant beibehalten


Falls es sich bei den Vorlagennamen um Adressen handelt, die nicht ermittelbar sind, (z. B. ist es unwahrscheinlich, dass ein Host-Name mit dem Namen "Standard\_Vorlage" existiert), können die Vorlagen im IT Assistant verbleiben. IT Assistant versucht das Element zu ermitteln, aber die versuchte Ermittlung bleibt ohne Erfolg. Wenn viele Vorlagen verwendet werden, ist es empfehlenswert, die Vorlagen zu löschen, um zu vermeiden, dass IT Assistant-Ermittlungszyklen für nicht ermittelbare Adressen verschwendet werden.

---

## Datenbankverwaltungs-Dienstprogramm

Das Dell OpenManage IT Assistant-Datenbankverwaltungs-Dienstprogramm hat zwei Ausführungen: eine graphische Benutzeroberfläche (GUI) und eine Befehlszeilenoberfläche. Mit beiden Versionen des Dienstprogramms können Benutzer Vorgänge mit Datenbanken und Tabellen ausführen, die sich im IT Assistant-Daten-Repository befinden.

 **ANMERKUNG:** Das IT Assistant 6.x-Datenbankschema ist nicht direkt mit dem IT Assistant 7.x-Datenbankschema kompatibel. Nur bestimmte Tabellen im Datenbank-Schema von IT Assistant 6.x werden migriert. Hierzu gehören z. B. Ermittlungskonfigurations-, globale Konfigurations- und Warnungsmaßnahmenstabellen. Das Datenbankschema kann nur während einer IT Assistant-Erweiterung migriert werden.

 **ANMERKUNG:** IT Assistant unterstützt ein direktes Upgrade von Version 6.x zu Version 8.0 nicht. Es ist erforderlich, zuerst IT Assistant Version 6.x zu 7.0 zu erweitern und dann zu IT Assistant Version 8.0.

Die GUI-Version des Datenbankverwaltungs-Dienstprogramms muss separat vom IT Assistant gestartet werden. Wenn das Dienstprogramm gestartet wird, öffnet sich ein Fenster, das Datenbank- und Tabellenverwaltungsfunktionen enthält. Die Befehlszeilenanwendung führt die Funktionen des GUI-Dienstprogramms und einige andere durch.

## Verwendung des Befehlszeilen-Datenbankverwaltungs-Dienstprogramms

Navigieren Sie bei einer Befehlszeileneingabe zum Verzeichnis `\Programme\Dell\SysMgt\IT Assistant\bin`.

Geben Sie `dcdbmng` ein, gefolgt von einem Schalter, der den von Ihnen gewünschten Befehl angibt. Um eine Liste der gültigen Schalter anzuzeigen, geben Sie Folgendes ein:


```
dcdbmng /h
```

ODER

```
dcdbmng /h
```

ODER

```
dcdbmng /?
```


 **ANMERKUNG:** Geben Sie zwischen dem Befehl `dcdbmng` und dem / (Schrägstrich) eine Leerstelle ein.

Mit diesem Befehl wird ein Dialogfeld angezeigt, das Befehle auflistet, die zum Folgenden verwendet werden können:

- 1 Die entsprechende Datenbank-Engine (Microsoft® Data Engine (MSDE) für IT Assistant Version 7.x und früher oder SQL Server 2005 Express für IT Assistant Version 8.0) installieren.



- 1 Die Datenbank-Engine starten und stoppen.
- 1 Hinzufügen und Trennen von Datenbankdateien zu und von der Database Engine.
- 1 Importieren und Exportieren von Tabellen und Datenbanken.

 **ANMERKUNG:** Aufgrund von Unterschieden in der Art und Weise, in der Microsoft Daten in verschiedenen Betriebssystemversionen verschlüsselt, wird das Exportieren von IT Assistant-Datenbanktabellen mit verschlüsselten Kennwörtern von einer Version eines Microsoft-Betriebssystems (z. B. Windows 2000) und das Importieren in eine andere Version (z. B. Windows 2003) nicht unterstützt.

- 1 Tabellen leeren.
- 1 Daten für die globale IT Assistant-Konfiguration oder nur für die Ereignisverwaltungs-Systemkonfiguration wieder herstellen.

## Hilfe

- 1 Befehl: **dcdbmng /h** oder **dcdbmng /H** oder **dcdbmng /?**
- 1 Beschreibung: Zeigt die Befehlszeilenoptionen an.

## Datenbank anhängen


- 1 Befehl: **dcdbmng /A Pfad** oder **dcdbmng /a Pfad**
- 1 Beschreibung: Verbindet die einzelne Datenbankdatei festgelegt nach *Pfad* mit SQL Server 2005 Express oder Microsoft SQL 2005 Server.

## Tabelle leeren

- 1 Befehl: **dcdbmng /Z Tabellename** oder **dcdbmng /z Tabellename**
- 1 Beschreibung: Entfernt alle Reihen aus der angegebenen Tabelle, löscht aber nicht die Tabelle.

## Datenbank abtrennen

- 1 Befehl: **dcdbmng /R** oder **dcdbmng /r**
- 1 Beschreibung: Trennt die verbundene Datenbankdatei von SQL Server 2005 Express oder SQL 2005 Server ab.

 **ANMERKUNG:** Die abgetrennte Datenbankdatei verbleibt an dem Speicherort, von dem aus sie mit SQL Server 2005 Express oder SQL 2005 Server verbunden wurde.

## Tabelle exportieren

- 1 Befehl: **dcdbmng /E Tabellename Dateiname** oder **dcdbmng /e Tabellename Dateiname**
- 1 Beschreibung: Exportiert die Daten in der mit *Tabellename* angegebenen Tabelle in eine Flat-Textdatei, die mit *Dateiname* angegeben wurde. Falls keine Flat-Textdatei existiert, wird sie vom Dienstprogramm erstellt. Falls der *Dateiname* keine Pfadinformationen enthält, erstellt das Dienstprogramm die Datei im lokalen Verzeichnis.

## Datenbank exportieren

Befehl: **dcdbmng /X Pfad** oder **dcdbmng /x Pfad**

Beschreibung: Exportiert die Daten aus allen Tabellen der Datenbank in Flat-Textdateien in der vom Pfad angegebenen Speicherstelle.

 **ANMERKUNG:** Das Dienstprogramm erstellt die Dateien im Format **tablename.txt** am vom Pfad angegebenen Speicherplatz.

## Tabelle importieren


- 1 Befehl: **dcdbmng /I Tabellename Pfad [migrieren]** oder **dcdbmng /i Tabellename Pfad [migrieren]**
- 1 Beschreibung: Importiert Daten in eine mit *Tabellename* angegebene Tabelle von einer Flat-Textdatei, die mit dem *Pfad* angegeben wurde.

## Datenbank importieren

- 1 Befehl: **dcdbmng /M Pfad** oder **dcdbmng /m Pfad**
- 1 Beschreibung: Importiert Daten in alle Tabellen in der Datenbank von Flat-Textdateien, die sich in der vom *Pfad* angegebenen Speicherstelle befinden.

## MSDE installieren

- 1 Befehl: **dcdbmng /N** oder **dcdbmng /n**
- 1 Beschreibung: Installiert MSDE ohne Warnungen.

 **ANMERKUNG:** Die Dateien **MSDEx85.exe** und **iss** müssen sich am korrekten Speicherplatz befinden.

## Server starten

- 1 Befehl: **dcdbmng /T** oder **dcdbmng /t**
- 1 Beschreibung: Startet den **MSSQLServer**-Dienst.


## Server stoppen

- 1 Befehl: **dcdbmng /P** oder **dcdbmng /p**
- 1 Beschreibung: Stoppt den **MSSQLServer**-Dienst.

## Meldungen ausblenden

Wenn das Datenbankverwaltungs-Dienstprogramm als Befehlszeilenanwendung ausgeführt wird, werden Meldungen zur erfolgreichen bzw. fehlerhaften Durchführung eines Befehls angezeigt. Der Befehl zur Ausblendung der Meldungen stoppt diese Benachrichtigungen.

- 1 Befehl: **dcdbmng /S**
- 1 Beschreibung: Ausführung ohne Anzeige von jeglichen Meldungen (ob die Maßnahme erfolgreich oder fehlerhaft war). Dieser Befehl ist bei der Ausführung des Dienstprogramms von einer Stapeldatei aus von Nutzen.

 **ANMERKUNG:** Bei der Verwendung von **/S** ohne andere Option wird der Befehl ignoriert.

---

## Ereignisquellen-Importdienstprogramm des einfachen Netzwerkverwaltungsprotokolls

Sie können mehrere Ereignisquellen, die nicht systemeigen in IT Assistant unterstützt werden, in die IT Assistant-Datenbank importieren.

Erstellen Sie eine Textdatei, die die entsprechenden Ereignisquelleninformationen enthält. Nach der Erstellung wird diese Textdatei nicht zur Freigabe an verschiedene Benutzer des Produktes verfügbar sein.

Führen Sie ein Befehlszeilenschnittstellen-Dienstprogramm (CLI) aus (Sie können dieses Dienstprogramm unter *<Installationsordner von IT Assistant>/bin* finden), um die Textdateidaten in die IT Assistant-Datenbank zu importieren.

Stellen Sie sicher, dass das Textdateiformat die folgenden Formatierungsregeln erfüllt:


1. Das Format zum Verwenden des Dienstprogramms muss Folgendes sein:


```
ImportEventSources.exe <vollqualifizierter Pfad\Dateiname>
```


2. Alle Werte einer bestimmten Ereignisquelle müssen nach Leiste getrennt sein.
3. Jede Ereignisquelle muss sich in einer separaten Zeile befinden.
4. Das Format der Einträge für alle Ereignisquellen muss folgendes sein:

<EventCategoryName>|<EventSourceName>|<Severity>|<Format String>|<SNMPEnterpriseOID>|<SNMPGenericTrapID>|<SNMPSpecificTrapID>  
|<EventPackageName>

5. Das Format für Schweregrad-Zeichenketten nach Wert muss folgendes sein: <ObjectId>,<ObjectValue>,<Severity>;<ObjectId1>,<ObjectValue1>,<Severity1>
6. Der Ereignisquellenname darf nicht NULL oder eine leere Zeichenkette sein.

 **ANMERKUNG:** Wenn der EventCategoryName eine leere Zeichenkette ist, wird die Kategorie standardmäßig auf **Other** umgestellt. Wenn der Kategorienname mit keinem der vordefinierten Kategorietypen in IT Assistant übereinstimmt, wird anhand des von Ihnen eingegebenen Kategorienamens eine neue Ereigniskategorie erstellt.

 **ANMERKUNG:** Stimmt die Schweregrad-Zeichenkette, die in der Eingabedatei eingegeben wurde, nicht mit den vordefinierten Schweregrad-Zeichenketten überein, wird eine entsprechende Fehlermeldung eingeblendet.

 **ANMERKUNG:** Eine Kombination von EnterpriseOID, Generic TrapID und sSpecificTrapID für jedes Ereignis sollte eindeutig sein. Die Kombination von EventSourceName und EventPackageName wird außerdem validiert, damit nachgeprüft werden kann, ob die Eingabe eindeutig ist.

 **ANMERKUNG:** Geben Sie zwei aufeinander folgende Balkenzeichen (" || ") ein, die NULL oder leere Zeichenketten darstellen sollen.

Der folgende Eintrag ist ein Beispiel-MIB-Eintrag.

```
-- Lower Critical threshold crossed
```

```
asfTrapFanSpeedProblem TRAP-TYPE
```

```
ENTERPRISE asfPetEvts
```

```
DESCRIPTION
```

```
"Generic Critical Fan Failure"
```

```
--#SUMMARY "Generic Critical Fan Failure"
```


```
--#ARGUMENTS {}
```

```
--#SEVERITY CRITICAL
```

```
::= 262402
```


Der Umsetzungsprozess ist wie folgt:

```
EventCategory : Environmental
```

 **ANMERKUNG:** IT Assistant hat eine Reihe vordefinierter Kategorien (Environmental [Umgebungsbedingungen], General Redundancy [Allgemeine Redundanz], Keyboard-Video-Mouse (KVM) [Tastatur-Video-Maus (KVM)], Memory [Speicher], Physical Disk [Physische Festplatte], Power [Strom], Printers [Drucker], Processor [Prozessor], Security [Sicherheit], Storage Enclosure [Speichergehäuse], Storage Peripheral [Speicherperipheriegeräte], Storage Software [Speichersoftware], System Events [Systemereignisse], Tape [Band], Virtual Disk [Virtuelle Festplatte] und Other [Anderes]). Das Ereignis kann unter jede dieser Kategorien fallen. Es kann jedoch auch eine neue Kategorie erstellt werden.

```
EventSourceName : asfTrapFanSpeedProblem
```

```
Severity : Critical [--#SEVERITY]
```

 **ANMERKUNG:** IT Assistant kategorisiert Ereignisse unter die folgenden Kategorien: (Ok [OK], Warning [Warnung], Critical [Kritisch], Information [Informationen], und Unknown [Unbekannt]).

Format String : Generic Critical Fan Failure [--#SUMMARY]

EnterpriseOID : .1.3.6.1.4.1.3183.1.1 (Um die Enterprise-OID zu erhalten, kompilieren Sie die MIB - in diesem Falle "DcAsfSrv.mib" - in MG-Soft oder einem beliebigen anderen MIB-Browser).

GenericTrapId : 6

SpecificTrapId : 262402 [::=]

EventPackageName : ASF (Sie können diese Informationen über die MIB beziehen). Öffnen Sie die MIB. Der EventPackageName wird innerhalb von [--Begin Definition] angezeigt ).

Wenn kein Paket vorhanden ist, unter das die EventSource fällt, können Sie einen neuen Kategorienamen angeben.

Der letzte Eintrag in der Textdatei wird folgendem ähnlich sein:

Environmental|asfTrapFanSpeedProblem|Critical|Generic Critical Fan Failure|.1.3.6.1.4.1.3183.1.1|6|262402|ASF

 **ANMERKUNG:** Im Falle, dass die Importdatei eine nicht vorhandene Kategorie enthält, wird die Kategorie erstellt.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Leistungsüberwachung

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

Leistungsüberwachung hilft Ihnen, die Leistung einer Gerätegruppe unterstützter Microsoft® Windows®- oder Linux-Betriebssysteme über einen bestimmten Zeitraum hinweg zu überwachen. Leistung wird mithilfe einer Reihe von Leistungsindikatoren überwacht, die für jede Komponente zur Verfügung stehen. Sie können diese Leistungsindikatoren auswählen und überwachen. Sie können für jeden Leistungsindikator Schwellenwerte konfigurieren und auch Warnungen konfigurieren, die dann gesendet werden, wenn die Schwellenwerte überschritten werden.


Anhand der Leistungsüberwachungsfunktion können Sie die Leistung der Geräte anzeigen, die in der **Geräte**struktur aufgezeigt werden. Die Gesamtleistung eines Geräts wird als der ungünstigste Status individueller Leistungsindikator-Attribute berechnet, die für das Gerät überwacht werden. Wenn z. B. der Status des CPU-Verwendungsindikators kritisch und der Status des Speicher-Paging-Indikators Warnung anzeigt, wird der Gesamtleistungsstatus des Geräts als kritisch angezeigt. Von der **Geräte**struktur aus können Sie sich nach unten zu den Leistungsindikatoren vorarbeiten und entsprechende Maßnahmen ergreifen.

Um Details zur Leistung der einzelnen Leistungsindikatoren auf einem Dell™ PowerEdge™-System anzuzeigen, gehen Sie folgendermaßen vor:

1. Von der **Geräte**struktur aus erweitern Sie die Server-Kategorie.
2. Wählen Sie das PowerEdge-System aus, über das Sie Informationen beziehen möchten.
3. Wählen Sie im Fenster auf der rechten Seite das Register **Leistung** aus.

Dieses Register zeigt die Leistungsindikator-Informationen zum ausgewählten Gerät an.

Von dieser Ansicht aus können Sie verschiedene Tasks erstellen, um verschiedene Geräte zu überwachen und diese Tasks zu verwalten, sowie Ergebnisse und Protokolle dieser Tasks anzuzeigen.

 **ANMERKUNG:** Leistungsüberwachung ermöglicht Ihnen, den Gebrauch Ihrer Systeme im Gegensatz zum Funktionszustand der Systeme zu überwachen.

---

## Leistungsüberwachung in Christians Geschäft (Unternehmensgröße)

Christian möchte von dieser Funktion Gebrauch machen, um zu überwachen, wie die PowerEdge x9xx-Systeme in seinem Netzwerk verwendet werden.

Seine hauptsächlichsten Erwägungen bzgl. des Verwendens dieser Funktion sind folgende:

1. Ist der Gebrauch der Systeme in meinem Netzwerk zu niedrig oder zu hoch?
1. Muss ich meine Hardware (z. B. CPU) oder Anwendungen auf ein anderes System verschieben?
1. Welche Leistung erbringen meine Systeme während Spitzenzeiten und Nichtspitzenzeiten?
1. Müsste ich die Last unter meinen Systemen ausgleichen?

Um diese Fragen beantworten zu können, müsste Christian Folgendes ausführen:

1. Leistungsüberwachungs-Task erstellen
1. Systeme über einen gewissen Zeitraum hinweg überwachen
1. Daten auf der IT Assistant-Konsole anzeigen
1. Daten in kommagetrennte Werte exportieren und zum späteren Gebrauch speichern

## Leistungsüberwachungs-Task erstellen

Um einen Leistungsüberwachungs-Task zu erstellen, führt Christian folgende Schritte aus:

1. Christian wählt **Verwalten** → **Leistungsüberwachung** aus der Menüleiste aus.

- Christian klickt mit der rechten Maustaste auf **Leistungsüberwachungs-Task** und wählt **Neuer Task...** aus.


Der **Assistent für neuen Task** wird eingeblendet.

- Christian gibt einen beschreibenden Namen für den Task ein. Zum Beispiel *Alle x9xx-Systeme*.

Christian klickt auf **Weiter**.

- Unter **Zeitplan auswählen** wählt Christian ein Startdatum und ein optionales Enddatum aus, um das Leistungsattribut zu messen. Er wählt einen 24-Stunden-Zeitplan aus, um seine Systeme während Spitzen- und Nichtspitzenzeiten zu überwachen.

Basierend darauf, wie oft er Systemproben entnehmen will, stellt Christian auch das Sampling-Intervall ein.

 **ANMERKUNG:** Christian sollte die Netzwerkkapazität in Betracht ziehen. Ein größeres Sampling-Intervall würde kein genaues Bild vermitteln, und ein kleineres Intervall könnte das Netzwerk und die überwachten Systeme belasten.


- Unter **Attribute auswählen** wählt Christian die CPU und die Speicherattribute aus und stellt die Schwellenwerte Warnung und Kritisch für sie ein. Er stellt z. B. den Warnungsschwellenwert für Folgendes ein:

- 1 %Kernel-Gebrauchszeit als > 70 % für 10 Proben
- 1 %Prozessor-Gebrauchszeit als > 70 % für 10 Proben

Und den kritischen Schwellenwert für:

- 1 %Kernel-Gebrauchszeit als > 90 % für 15 Proben
- 1 %Prozessor-Gebrauchszeit als > 90 % für 15 Proben

Christian kann **Warnung aussenden** oder **Kritische Warnung aussenden** auswählen, um Warnungen oder kritische Warnungen zu erhalten.

 **ANMERKUNG:** Wenn Christian ein kleineres Sampling-Intervall festlegt, jedoch eine große Anzahl von Indikatoren und Geräten auswählt, wird eventuell eine Warnungsmeldung angezeigt, die auf eine zu hohe Ressourcennutzung hinweist. Christian sollte ein höheres Sampling-Intervall festlegen oder die Anzahl der Indikatoren und Geräte reduzieren, um diese Situation zu vermeiden.

- Unter **Geräteauswahl** wählt Christian die Gruppen aus der Struktur aus, die seine x9xx-Systeme beinhalten, oder er gibt eine Abfrage aus.
- Unter **Anmeldeinformationen eingeben** gibt Christian die **Benutzer-ID** und das **Kennwort** des Betriebssystems ein, was für alle ausgewählten Geräte gültig ist.
- Christian prüft seine Auswahl im Bildschirm **Zusammenfassung** und klickt auf **Fertig stellen**.

Der Task *Alle x9xx-Systeme* erscheint in der Struktur unter dem Parent-Knoten **Leistungsüberwachungs-Tasks**.

## Systemgebrauch im Netzwerk überwachen

Um den Gebrauch aller PowerEdge x9xx-Systeme im Netzwerk zu überwachen, führt Christian folgende Schritte aus:

- Christian klickt unter dem Parent-Knoten **Leistungsüberwachungs-Tasks** auf den Task *Alle x9xx-Systeme*.
- Die Zusammenfassung des Tasks wird unter dem Register **Zusammenfassung** auf der rechten Seite des Bildschirms angezeigt.
- Um die Überwachung in detaillierterer Form anzuzeigen, wählt Christian das Register **Ausführungsergebnisse** aus.

Dieses Register zeigt die Indikatoren an, die Christian in [Schritt 5](#) unter "[Leistungsüberwachungs-Task erstellen](#)" ausgewählt hat.

Die Indikatoren verfolgen, wie ein System eingesetzt wird.

Christian kann die Indikatoren so einstellen, dass er anzeigen kann, wie eine bestimmte Komponente für jedes System (z. B. die %Kernel-Gebrauchszeit) eingesetzt wird.

Wenn die Indikatoren entsprechend eingestellt wurden, würden die Farben des Indikators recht gut anzeigen, in welchem Ausmaß die Systeme eingesetzt werden. Ziehen Sie den Mausfeil über den Indikatoren, um eine Vorstellung von der Leistung der Systemkomponente zu erhalten.

Beispiel:

Wenn der Indikator für die meiste Zeit grün ist, könnte dies anzeigen, dass sich der Indikator gut innerhalb der festgelegten Grenzen befindet, und dass der Gebrauch der Systemkomponente zu niedrig ist oder nur teilweise stattfindet.

Wenn der Indikator für einen kurzen Zeitraum rot ist, könnte dies anzeigen, dass der Gebrauch der Systemkomponente nur teilweise stattfindet.

Wenn der Indikator für die meisten Proben rot ist, könnte dies anzeigen, dass der Gebrauch der Systemkomponente zu hoch ist.

[Tabelle 7-1](#) zeigt ein Beispiel dessen, wie Systeme in Christians Netzwerk gebraucht werden können.

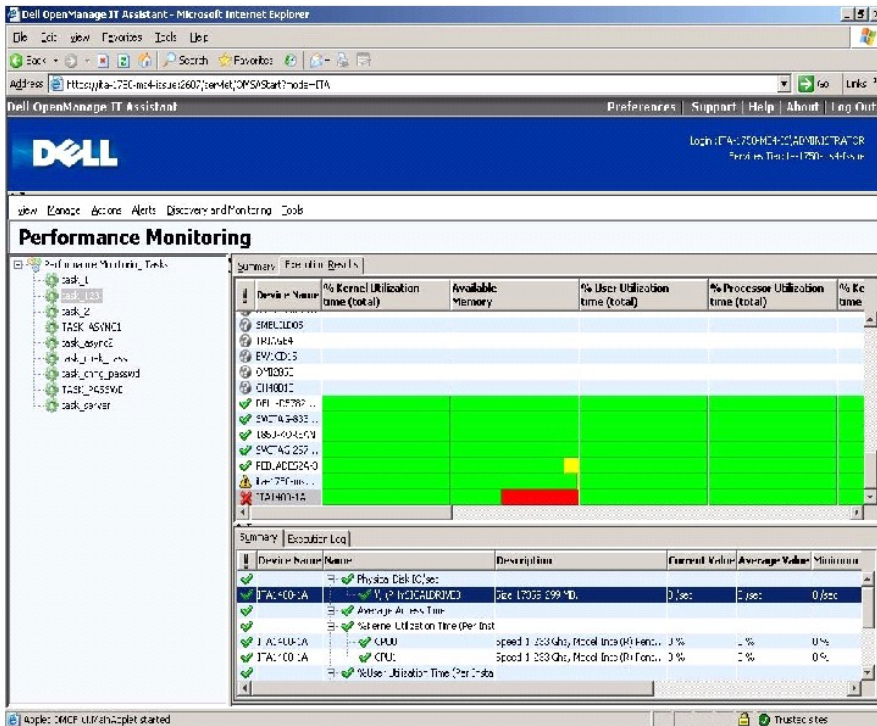
**Tabelle 7-1. Beispiel des Gebrauchs von Christians Netzwerk**

	CPU-Gebrauch	Speichergebrauch	Netzwerkgebrauch
System 1	Hoch	Niedrig	Mittelmäßig
System 2	Niedrig	Hoch	Mittelmäßig

Wenn %CPU-Gebrauchszeit für die meisten eingeholten Proben rot ist (hoher Gebrauch), könnte dies bedeuten, dass der CPU-Gebrauch durch eine Anwendung zu hoch ist. Christian könnte in Erwägung ziehen, diese Anwendung auf ein System zu verschieben, bei dem die %CPU-Gebrauchszeit für die meisten Proben grün ist. In diesem Falle von System 1 auf System 2. Christian könnte auch ein Speichermodul von System 1 auf System 2 verschieben, um die Last auszugleichen, oder er könnte in Erwägung ziehen, die Hardware zu erweitern oder neue Speichermodule zu erwerben.

Wenn Christian seine Systeme am *Wochenende* überwacht und feststellt, dass die Netzwerk- und CPU-Gebrauchsindikatoren bei 70 % der Proben grün sind (innerhalb des festgelegten Bereichs), bei 20 % der Proben gelb (Nicht-kritisch) und bei 10 % der eingeholten Proben rot (kritisch), könnte dies bedeuten, dass die Netzwerk- und CPU-Gebrauchsindikatoren während *Werktagen* bei den meisten Proben eventuell rot wären. Die Systeme wären überladen, und Christian könnte sich entscheiden, seinem Netzwerk weitere Systeme hinzuzufügen oder eine andere Art des Lastenausgleichs zu finden.

**Abbildung 7-1. Bildschirm Proben-Leistungsüberwachung**



4. Im Register **Ausführungsergebnisse** kann Christian mit der rechten Maustaste auf einen Indikator klicken und einen der folgenden Vorgänge ausführen:
  - **Exportieren** auswählen. Hierdurch werden die Details in eine CSV-Datei (kommagetrennte Werte) exportiert. Christian kann dann andere Hilfsprogramme wie Microsoft® Excel verwenden, um bessere Reporte zu erstellen.
  - Auf **Schaubild anzeigen** klicken, um die graphische Darstellung der Leistungsdaten des Geräts anzuzeigen. Christian kann einen zeitlichen Bereich angeben und den Systemgebrauch graphisch anzeigen.

**ANMERKUNG:** Christian kann auch die Diagramme anzeigen und sie im unteren Fenster vom Register **Zusammenfassung** aus exportieren.

  - Auf **Ausführungsergebnisse löschen** klicken.
  - Mit der rechten Maustaste auf eine Spaltenüberschrift klicken und **Ansicht an die eigenen Bedürfnisse anpassen** auswählen. Diese Anzeige passt die Geräteanzeige den speziellen Kundenbedürfnissen an.
1. Im Register **Ausführungsprotokoll** kann Christian die Ausführungszusammenfassungen für jede Ausführung des Tasks anzeigen. Er kann auch die Zeitauswahl-Felder verwenden, um die **Von**-Zeit auszuwählen, von der an er die Protokolle anzeigen möchte.
 

**ANMERKUNG:** Die Ausführungsprotokoll-Einträge werden geleert, wenn die Ausführungsprotokoll-Einträge älter als 14 Tage sind.
6. Im Register **Leistung** in der **Gerätestruktur** kann Christian die Informationen der Leistungsindikatoren für das ausgewählte Gerät anzeigen.

## Vorgeschlagene Schwellenwertkonfiguration für die Leistungsüberwachung

Tabella 7-2 zeigt die Proben-Schwellenwerteneinstellungen für jeden Leistungsindikator an.

Tabella 7-2. Proben-Schwellenwerteneinstellungen für Leistungsindikatoren

Ressource	Leistungsindikator-Attribut	Vorgeschlagener Schwellenwert	Anmerkungen
CPU	%Prozessor-Gebrauchszeit	Niedriger als 85 %	Gesamt-Prozessorgebrauch sollte unter 85 % bleiben, wobei gelegentliche kurzzeitige Spitzen über 85 % akzeptabel sind.
System	Kontextwechsel/Sekunde	Hängt von der Systemaktivität ab	Fortlaufende Spitzen über längere Zeiträume können eine Erhöhung der Systembelastung mit sich ziehen.
System	Länge der Prozessorwarteschlange	2	Hängt von der Anzahl von Prozessoren im System ab. Hierbei handelt es sich um eine unmittelbare Anzahl. Beobachtung über mehrere Zyklen ist erforderlich.




Speicher	Verfügbare Speicher	Weniger als 10-20 % installierten RAMs Weniger als 4 MB bei Systemen mit großem Speicher	Wenn der verfügbare Speicher über einen längeren Zeitraum unter 10 % - 20 % des installierten RAM beträgt, könnte zusätzlicher Speicher notwendig werden.
Speicher	Seiten/Sekunde	Weniger als 20	Sollte unter 20 verbleiben (mit Ausnahme kurzzeitiger Spitzen).
Speicher	%Auslagerungsdateieinutzung	95 %	Überprüfen Sie diesen Wert in Verbindung mit Verfügbarem Speicher und Seiten/Sekunde.
Netzwerk	EmpfangeneBytes/Sekunde EmpfangenePakete/Sekunde GesendeteBytes/Sekunde GesendetePakete/Sekunde	Beträchtliche Abweichung von durchschnittlichen Werten über einen längeren Zeitraum. Hängt vom Netzwerktyp ab	Eine beträchtliche Zunahme oder Abnahme über normalen Stufen weist stark auf Netzwerkprobleme hin.
Physische Festplatte	E/A der physischen Festplatte pro Sekunde	Hängt von den Herstellerangaben ab	Überprüfen Sie die festgelegte Transferrate für Ihre Festplatten, um sicherzustellen, dass diese Rate die Angaben nicht überschreitet. Im Allgemeinen können Ultra Wide-SCSI-Festplatten 50 bis 70 E/A-Vorgänge pro Sekunde bewältigen.
Logische Festplatte	Freier Speicherplatz	Weniger als 15 %	Der Schwellenwert ist hinsichtlich der Gesamtsumme des Festplattenspeicherplatzes und der durchschnittlichen E/A-Aktivität auf dem System relativ.

## Ressourcengebrauch durch SQL Server und IT Assistant

[Tabelle 7-3](#) zeigt die empfohlene Hardwarekonfiguration, die für die Leistungsüberwachung erforderlich ist.

**Tabelle 7-3. Empfohlene Hardwarekonfiguration bei IT Assistant für die Leistungsüberwachung**

Minimale Anzahl von CPUs	Minimaler erforderlicher Speicher	Datenbank	Maximale Anzahl von Benutzersitzungen pro Benutzer	Maximale Anzahl von Leistungsindikatoren	Minimale unterstützte Probenfrequenz	Maximale Anzahl von Geräten
Einzelne CPU 2,0 GHz	512 MB	MSDE/SQL Express 2005	1	10	2 Minuten	15
Einzelne CPU 2,0 GHz	512 MB	MSDE/SQL Express 2005	1	18	2 Minuten	8
Einzelne CPU 2,0 GHz	1 GB	SQL 2000/ SQL 2005 Server	2	10	2 Minuten	30
Einzelne CPU 2,0 GHz	1 GB	SQL 2000/ SQL 2005 Server	2	18	2 Minuten	20
Dual-CPU 2,0 GHz	1 GB	SQL 2000/ SQL 2005 Server	2	10	3 Minuten	100
Dual-CPU 2,0 GHz	1 GB	SQL 2000/ SQL 2005 Server Enterprise Edition	5	10	5 Minuten	200

 **ANMERKUNG:** Die in dieser Tabelle aufgeführte Hardwarekonfiguration bezieht sich auf die unterstützte Mindestkonfiguration. Die neuste Aktualisierung dieser Voraussetzungen finden Sie in der IT Assistant-Infodatei auf Dells Support-Website unter [support.dell.com](http://support.dell.com).

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

# Installationsplan für Dell OpenManage™ IT Assistant

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Entscheidungen vor der Installation](#)
- [Primäre Fragen zur Planung](#)
- [Betriebssystem auswählen](#)
- [Hardwarekonfiguration auswählen](#)
- [SQL Server 2005 Express-Standarddatenbank oder SQL 2005 Server auswählen](#)
- [E-Mail-Benachrichtigungsfunktionen](#)
- [Systems Management-Protokolle festlegen](#)
- [Zusammenfassung der Entscheidungen vor der Installation](#)


Es ist wichtig, vor der Installation von Dell OpenManage IT Assistant einen Plan zu erstellen. Je nach dem, welche Netzwerkverwaltungsziele Ihr Unternehmen hat, wollen Sie eventuell den IT Assistant in erster Linie als ein Ermittlungs- und Statusabfrage-Hilfsprogramm verwenden, das schnell das Netzwerk scannt, um Informationen zu verwalteten Systemen abzurufen. Andererseits möchten Sie eventuell, dass IT Assistant auch Warnungen über Probleme auf spezifischen verwalteten Systemen erhält und an Support-Mitarbeiter weiterleitet. Oder vielleicht wollen Sie eine Kombination von beiden.

---

## Entscheidungen vor der Installation

Nach der Bestimmung der Netzwerkgröße und der Anforderungen an die Netzwerkverwaltung muss eine Konfiguration gesucht werden, mit der die angestrebten Ziele der Netzwerkverwaltung erreicht werden können. Wenn das Netzwerk über eine umfangreiche Ausstattung verfügt und bereits ein gut durchdachter IT Assistant-Verwaltungsplan vorliegt, wurden viele dieser Entscheidungen vielleicht bereits getroffen. Bei der Planung vor der Installation müssen folgende Optionen gewählt werden:

- 1 Ereignisfilter und Benachrichtigungsstrategie
- 1 Datenbank zur Speicherung von IT Assistant-Daten
- 1 Hardwarekonfiguration
- 1 Betriebssystem
- 1 Systemverwaltungsprotokolle
- 1 Agenten für die verwalteten Systeme

 **ANMERKUNG:** In diesem Dokument wird vorausgesetzt, dass die Systeme über ein TCP/IP-Netzwerk verbunden sind, und es werden keine Annahmen bezüglich der Komplexität des Netzwerks gemacht oder ob bereits Systems Management-Anwendungen eingesetzt werden. Außerdem werden keine Annahmen bezüglich der im Netzwerk vorhandenen System- und Gerätetypen gemacht. Informationen zu allen Installations-, Deinstallations- und Upgrade-Verfahren finden Sie unter "[Dell OpenManage™ IT Assistant installieren, deinstallieren und erweitern](#)".

---

## Primäre Fragen zur Planung

Die Systemtypen und Anforderungen an die Netzwerkverwaltung unterscheiden sich einem Unternehmen zum anderen. Die Beantwortung der folgenden Fragen kann Ihnen dabei helfen, eine IT Assistant-Installation vorzubereiten, mit der die Ziele des Unternehmens zur Netzwerkverwaltung erreicht werden. Lesen Sie diesen Abschnitt, und sehen Sie sich dann vor der Ausführung der Installation [Tabelle 4-4](#) an.

1. Wie lauten die Grundanforderungen an Hardware und Betriebssystem zur Installation des IT Assistant? Erfüllt mein Unternehmen diese?
2. Muss ich ein bestimmtes unterstütztes Betriebssystem für die IT Assistant-Installation wählen?
3. Muss ich eine bestimmte Hardwarekonfiguration für die IT Assistant-Installation wählen?
4. Soll ich die installierte Standard-Datenbank (Microsoft® SQL Server 2005 Express) verwenden oder die Microsoft SQL Serverdatenbank installieren?
  - 1 Wie viele Systeme sollen ermittelt oder verwaltet werden?
  - 1 Wie dicht wird der Ereignisverkehr im Netzwerk voraussichtlich sein?
5. Welche Systemverwaltungsprotokolle sollten installiert oder aktiviert werden?
  - 1 Welche Systemtypen sollen verwaltet werden?
  - 1 Welche Agenten und Instrumentationen sind derzeit in den verwalteten Systemen installiert?
  - 1 Welche Agenten sollen eventuell auf dem verwalteten System ausgeführt werden?
  - 1 Welche Protokolle werden von diesen Agenten benötigt oder unterstützt?
6. Wie soll ich die IP-Adressen der verwalteten Systeme organisieren, wenn mehr als ein Systemverwaltungsprotokoll in einem Subnetz verwendet wird?





---

## Betriebssystem auswählen

IT Assistant kann auf allen Systemen installiert werden, auf denen eines der Betriebssysteme in [Tabelle 4-1](#) ausgeführt wird.

**Tabelle 4-1. Minimale Anforderungen an unterstützte Betriebssysteme für IT Assistant**

Klein (bis zu 500 verwaltete Systeme)	Groß (500 und mehr verwaltete Systeme)
Microsoft Windows® XP Professional mit SP2	Windows Server 2003 mit SP1
Windows 2000 mit SP4	Windows 2000 mit SP4
Windows Server® 2003 mit SP1	

-  **ANMERKUNG:** IT Assistant wird nicht auf Microsoft Windows Small Business Server 2003 unterstützt.
-  **ANMERKUNG:** Lesen Sie bei die Installation und Konfiguration der Terminaldienste oder des Remote-Desktop die Dokumentation des Microsoft Betriebssystems.
-  **ANMERKUNG:** IT Assistant kann nicht auf Dell-Systemen installiert werden, auf denen die Betriebssysteme Red Hat® Enterprise Linux oder SUSE® Linux Enterprise Server ausgeführt werden. Diese Systeme können IT Assistant jedoch durch unterstützte Browser starten (Mozilla Version 1.7.3 und höher sowie Firefox Version 1.0.1 oder höher).
-  **ANMERKUNG:** Wenn Sie die Leistungsüberwachungsfunktion verwenden, erhalten Sie in [Tabelle 7-3](#) Informationen zu Hardware- und Betriebssystemanforderungen.

---

## Hardwarekonfiguration auswählen



Bei der gewählten Hardwarekonfiguration muss die empfohlene Konfiguration für IT Assistant erfüllt oder übertroffen werden. Abhängig von der jeweiligen Bereitstellung des IT Assistant und der Netzwerkumgebung ist es eventuell ratsam, über die empfohlenen Konfigurationen für Prozessorgeschwindigkeit, Speichergröße und Festplattenspeicher hinaus zu gehen. Vielleicht möchten Sie z. B. die höchste empfohlene Konfiguration erfüllen oder übertreffen, wenn:

- 1 Viel Warnungsverkehr für verwaltete Systeme erwartet wird
- 1 Komplexe Warnungsfiler mit konfigurierten Warnungsmaßnahmen eingesetzt werden
- 1 Häufig Ermittlung, Bestandsaufnahme, Statusabfragen oder Leistungsüberwachung durchgeführt wird
- 1 Microsoft SQL Server mit maximaler Leistung ausgeführt wird.

Die empfohlene minimale Hardwarekonfiguration für IT Assistant wird in [Tabelle 4-2](#) gezeigt.

**Tabelle 4-2. Empfohlene minimale Hardwarekonfiguration für IT Assistant (aufgeführt nach Unternehmensgröße)**

Komponente	Klein (bis zu 500 verwaltete Systeme)	Groß (500 und mehr verwaltete Systeme)
Prozessor	1 Prozessor (1,8-GHz Minimum)	2 bis 4 Prozessoren (800-MHz Minimum)
Speicher	512 MB	1-2 GB
Festplattenspeicherplatz	mindestens 1 GB	mindestens 5 GB


-  **ANMERKUNG:** Die Größe des erforderlichen Speicherplatzes kann zunehmen, wenn Sie zahlreiche Dell Update Packages (DUPs) und MSI-Dateien für Softwareaktualisierung und -bereitstellung importieren.
-  **ANMERKUNG:** Wenn Sie die Leistungsüberwachungsfunktion verwenden, erhalten Sie in [Tabelle 7-3](#) Informationen zu Hardware- und Betriebssystemanforderungen.


---


## SQL Server 2005 Express-Standarddatenbank oder SQL 2005 Server auswählen

Im Allgemeinen bestimmen die Anzahl der zu verwaltenden Systeme sowie die Anzahl der Warnungen, die Sie von den verwalteten Systemen erwarten, welche Datenbank mit IT Assistant verwendet wird. Wenn weniger als 500 Systeme verwaltet werden, ist die mit IT Assistant gelieferte SQL Server-konforme Standarddatenbank, SQL Server 2005 Express, höchstwahrscheinlich ein geeignetes Daten-Repository. Wenn jedoch 500 oder mehr Systeme verwaltet

werden sollen und/oder mehrere Warnungen pro Sekunde empfangen werden, sollte Microsoft SQL Server 2000 oder höher als Datenbank eingesetzt werden. Es wird auch notwendig sein, die Auswirkung der Leistungsüberwachungsfunktion auf Ihrer Auswahl der Datenbank in Erwägung zu ziehen. Weitere Informationen finden Sie unter "[Leistungsüberwachung](#)". Wenn außerdem häufig Ermittlungen oder Statusabfragen durchgeführt werden, könnten Sie von der höheren Leistung profitieren, die SQL 2005 Server gegenüber SQL Server 2005 Express bietet.

 **ANMERKUNG:** IT Assistant Version 6.3 und höher kann so konfiguriert werden, dass Microsoft SQL Server auf einem dedizierten Remote-Server ausgeführt wird, statt auf dem IT Assistant-System konfiguriert zu werden. Weitere Informationen finden Sie unter "[Remote Microsoft SQL Server und IT Assistant](#)".

 **ANMERKUNG:** IT Assistant Version 8.0 ist mit der SQL Server-konformen Standarddatenbank rückwärtskompatibel, die mit IT Assistant 7.x geliefert wird.

 **ANMERKUNG:** SQL Server 2005 Express und SQL 2005 Server nur auf Windows 2000 mit SP4, Windows Server 2003 SP1 oder Windows XP mit SP2 ausgeführt.

---

## E-Mail-Benachrichtigungsfunktionen

E-Mail-Warnungsmaßnahmen sind in Umgebungen hilfreich, in denen ein Systemadministrator den Status verwalteter Systeme nicht visuell über die IT Assistant-Benutzeroberfläche (UI) überwachen möchte. Durch Kombinieren von E-Mail-Warnungsmaßnahmen mit Warnungsmaßnahmenfiltern kann ein Administrator eine Person angeben, die elektronisch benachrichtigt wird, wenn ein bestimmtes System Warnungen an die IT Assistant-Netzwerkverwaltungsstation sendet. Diese Person kann dann entsprechende Korrekturmaßnahmen für das System einleiten. Durch die Konfiguration von Warnungsfiltern mit entsprechenden Warnungsmaßnahmen ist eine konstante Überwachung des Systemstatus in der IT Assistant-Benutzeroberfläche nicht mehr erforderlich, da eine E-Mail-Benachrichtigung ausgegeben wird, sobald ein Ereigniskriterium erfüllt wurde.


---


## Systems Management-Protokolle festlegen

Eine der wichtigsten Entscheidungen im Verlauf der Planung der IT Assistant-Installation ist die Festlegung der Protokolle, die mit IT Assistant verwendet werden sollen. Die Auswahl der Protokolle wird im Allgemeinen durch die zu überwachenden Systeme sowie durch die jeweiligen unterstützten Agentenprotokolle bestimmt. Wenn die Systeme, die Sie überwachen möchten, Agenten besitzen, die das einfache Netzwerk-Verwaltungsprotokoll (SNMP) bzw. die Protokolle für das allgemeine Informationsmodell (CIM) oder die intelligente Plattform-Verwaltungsschnittstelle (IPMI) verwenden, müssen diese Protokolle auch in IT Assistant konfiguriert sein.

### Unterstützte Protokolle

IT Assistant unterstützt drei Systemverwaltungsprotokolle: SNMP, CIM und IPMI. Diese Protokolle ermöglichen die Kommunikation zwischen der IT Assistant-Netzwerkverwaltungsstation und den verwalteten Systemen im Netzwerk. Für eine erfolgreiche Kommunikation zwischen dem IT Assistant und jedem verwalteten System müssen auf jedem der zu verwaltenden Systeme Agenten (Instrumentationen) installiert werden. Für die Systemverwaltung wird nachhaltig empfohlen, alle Protokolle zu aktivieren und konfigurieren.

 **ANMERKUNG:** Wenn das entsprechende Protokoll nicht richtig auf den verwalteten Systemen konfiguriert ist, kann IT Assistant die Systeme nicht richtig klassifizieren. Dadurch ist eventuell die Verwaltbarkeit jener Systeme eingeschränkt.

 **ANMERKUNG:** Die Dell|EMC-Speicher-Arrays verwendet sowohl SNMP- als auch NaviCLI-Protokolle.

### SNMP

Um eine IT Assistant-Installation erfolgreich auszuführen, müssen Sie den SNMP-Dienst des Betriebssystems installieren und aktivieren.

### CIM


CIM wird zur Verwaltung von Client- und Server-Systemen verwendet. Es kann auch zur Überwachung von Server Instrumentation in einem Netzwerk verwendet werden, das SNMP-Verwaltung nicht erlaubt.

### IPMI

Die intelligente Plattform-Verwaltungsschnittstelle (IPMI) wird unabhängig vom Betriebssystem betrieben und ermöglicht Administratoren, ein System im

Remote-Zugriff sogar dann zu verwalten, wenn kein Betriebssystem bzw. keine Systems Management-Software vorhanden ist, oder wenn das überwachte System nicht eingeschaltet ist. IPMI kann auch funktionieren, wenn das Betriebssystem gestartet wurde und bietet erweiterte Funktionen, wenn sie mit der Systems Management-Software verwendet wird.

Damit ein System erfolgreich über IPMI ermittelt werden kann, muss sich auf Ihrem System ein Baseboard-Verwaltungs-Contoller (BMC) befinden, auf dem IPMI Version 1.5 oder höher ausgeführt wird.

 **ANMERKUNG:** Der BMC überwacht nicht das Speicher-Subsystem auf Ihrem Netzwerk. Damit diese Geräte überwacht werden können, muss Server Administrator auf Ihren verwalteten Systemen installiert sein.

## Faktoren, die die Wahl des Protokolls beeinflussen

Die Wahl des Protokolls wird durch zwei Faktoren beeinflusst:

- 1 Durch die zu überwachenden Systeme
- 1 Agenten auf den zu überwachenden Systemen


## Zu überwachenden Systeme

Ihr Netzwerk kann aus einer Kombination von Client- und Server-Systemen, Dell|EMC-Speicher-Arrays, Druckern und Bandbibliotheken bestehen. Bei der Planung der IT Assistant-Installation werden Sie diese sowie all die Systeme prüfen, die zum Netzwerk hinzugefügt werden sollen, und Sie werden festlegen, welche dieser Systeme überwacht werden sollen. Während dieser Beurteilung werden Sie nicht nur auf die Anzahl der Client- und Server-Systeme achten, sondern auch auf alle Systemverwaltungsagenten und Betriebssysteme, die auf diesen Systemen installiert sind. Im folgenden Abschnitt werden die Agenten und entsprechenden Protokolle beschrieben, die möglicherweise im IT Assistant konfiguriert werden müssen. Zur erfolgreichen Verwaltung des Netzwerks ist die richtige Konfiguration dieser Protokolle innerhalb des IT Assistant erforderlich.

## Agenten auf den zu überwachenden Systemen

Die auf den verwalteten Systemen ausgeführten Agenten unterstützen ein bestimmtes Systemverwaltungsprotokoll. Um die bereits auf diesen Systemen installierten Agenten beizubehalten, müssen diese weiterhin mit den entsprechenden Protokollen verwaltet werden. Wenn es sich bei dem von bestimmten Agenten verwendeten Protokoll um ältere Protokolle handelt, können diese Agenten in den meisten Fällen durch Agenten ersetzt oder aktualisiert werden, die neuere Protokolle unterstützen. In [Tabelle 4-3](#) werden eine Reihe von Agenten und Instrumentationen aufgeführt, die eventuell auf Dell Clients und Servern installiert sind. Solange das entsprechende Protokoll im IT Assistant aktiviert ist, können diese Systeme im Netzwerk ermittelt und verwaltet werden.

*Agent* ist ein allgemeiner Begriff, der auf Softwarekomponenten der Systems Management-Instrumentation angewendet wird. Die folgende Tabelle zeigt die durch den IT Assistant unterstützten Verwaltungs- und Warnungsagenten. Der Grad der Unterstützung variiert von Agent zu Agent. IT Assistant z. B. bietet automatische Ermittlung, Anzeige und automatischen Empfang von Warnungen von den vom Dell OpenManage Server Administrator verwalteten Systemen. IT Assistant kann Maßnahmen auf diesen Systemen ausführen, aber Warnungen nur von bestimmten Speichergeräteagenten empfangen.

 **ANMERKUNG:** IT Assistant unterstützt das DMI-Protokoll (Desktop-Verwaltungsschnittstelle) nicht mehr. Infolgedessen können Systeme, auf denen DMI unter Verwendung von Dell OpenManage Server Agent 4.5.1 (und früher) und Dell OpenManage Client Instrumentation 6.0 (und früher) ausgeführt wird, von IT Assistant nicht ermittelt werden.

**Tabelle 4-3. Von IT Assistant unterstützte Agenten**

Gerät	Unterstützte Version(en)	Automatisch ermittelbar	Alarmierung
<b>Dell PowerEdge-Agenten</b>			
Server Administrator	1.5 und später	Ja	Ja
Firmware des Baseboard-Verwaltungs-Controllers	1.0 und später Unterstützt nur die Systeme Dell PowerEdge™ x8xx und x9xx	Ja	Ja
Array Manager	3.7	Ja	Ja
DRAC 5	1.0 und später	Ja	Ja
DRAC 4	1.0 und später	Ja	Ja
DRAC III, DRAC III/XT	1.0 und später	Ja	Ja
ERA, ERA/O	1.0 und später	Ja	Ja
DRAC/MC	Unterstützt nur die Systeme PowerEdge 1855 und 1955	Ja	Ja
ERA/MC	Unterstützt nur das System PowerEdge 1655	Ja	Ja
PowerEdge 1655MC Integrierter Schalter	-	Ja	Ja
<b>Dell PowerVault™-Agenten</b>			
PowerVault 701N	-	Ja	Ja

PowerVault 705N	-	Ja	Ja
PowerVault 735N	-	Ja	Ja
PowerVault 750N	-	Ja	Ja
PowerVault 755N	-	Ja	Ja
PowerVault 715N	-	Ja	Ja
PowerVault 725N	-	Ja	Ja
PowerVault 770N	-	Ja	Ja
PowerVault 775N	-	Ja	Ja
PowerVault 745	-	Ja	Ja
PowerVault Adaptec CIO	4.02	Nein	Ja
<b>Von IT Assistent unterstützte Dell PowerConnect™-Agenten und PowerConnect-Firmware-Versionen</b>			
PowerConnect 3024	5.2.5.x, 6.0.4.x, 6.1.2.x	Ja	Ja
PowerConnect 3048	5.2.5.x, 6.0.4.x, 6.1.2.x	Ja	Ja
PowerConnect 3248	1.0.1.x, 2.0.0.x, 2.1.0.x	Ja	Ja
PowerConnect 3324	1.0.0.x, 1.1.0.x, 1.2.0.x	Ja	Ja
PowerConnect 3348	1.0.0.x, 1.1.0.x, 1.2.0.x	Ja	Ja
PowerConnect 3424	1.0.0.x	Ja	Ja
PowerConnect 3424P	1.0.0.x	Ja	Ja
PowerConnect 3448	1.0.0.x	Ja	Ja
PowerConnect 5012	5.2.5.x, 6.0.4.x, 6.1.2.x	Ja	Ja
PowerConnect 5212	1.0.0.x, 3.1.0.x	Ja	Ja
PowerConnect 5224	1.0.1.x, 2.0.0.x, 2.1.0.x, 3.1.0.x	Ja	Ja
PowerConnect 5316M	1.0.0.x	Ja	Ja
PowerConnect 5324	1.0.0.x	Ja	Ja
PowerConnect 6024	1.0.2.x, 2.0.0.x	Ja	Ja
PowerConnect 6024F	1.0.2.x, 2.0.0.x	Ja	Ja
Cisco-Schalter (nur in Modular Chassis)	-	Ja	Ja
<b>Digital-KVM-Agenten</b>			
2161 DS	-	Ja	Ja
4161 DS	-	Ja	Ja
<b>Netzwerkadapteragenten</b>			
Intel® PRO	-	Nein	Ja
Broadcom	-	Nein	Ja
ASF	1	Nein	Ja
<b>Client-Agenten</b>			
Dell OpenManage Client Instrumentation	7.0 und später	Ja	Ja
<b>Dell EMC</b>			
CX300	-	Ja	Ja
CX500	-	Ja	Ja
CX700	-	Ja	Ja
AX100	-	Ja	Ja
AX100i	-	Ja	Ja
CX3-20	-	Ja	Ja
CX3-40	-	Ja	Ja
CX3-80	-	Ja	Ja
AX150	-	Ja	Ja
<b>Drucker</b>			
5210n	-	Ja	Ja
5310n	-	Ja	Ja
3110cn	-	Ja	Ja
3115cn	-	Ja	Ja
1700n	-	Ja	Ja
W5300cn	-	Ja	Ja
M5200cn	-	Ja	Ja
5310	-	Ja	Ja
5210	-	Ja	Ja
1710	-	Ja	Ja
5100cn	-	Ja	Ja
5100cn w HD	-	Ja	Ja

5100cn w MPC	-	Ja	Ja
5100cn w HD & MPC	-	Ja	Ja
3100cn	-	Ja	Ja
3000cn	-	Ja	Ja
1710n	-	Ja	Ja
1600n	-	Ja	Ja
<b>Bandautomation</b>			
PowerVault 132T	-	Ja	Ja
PowerVault 136T	-	Ja	Ja
ML6000	-	Ja	Ja
<b>ANMERKUNG:</b> SNMP kann nur über das Bedienfeld am Gerät konfiguriert werden.			
<b>ANMERKUNG:</b> Die Standard-Community-Zeichenkette ist publicCmtyStr.			

## Zusammenfassung der Entscheidungen vor der Installation

In diesem Abschnitt werden die Hauptfaktoren aufgeführt, die vor der Installation und Verwendung von IT Assistant zur Systemverwaltung im Netzwerk zu beachten sind. In [Tabelle 4-4](#) werden die in den vorhergehenden Abschnitten gestellten Fragen, die verfügbaren Optionen und Maßnahmen sowie der Abschnitt in diesem Handbuch zusammengefasst, in dem das entsprechende Verfahren zur Ausführung dieser Maßnahmen zu finden ist.

**Tabelle 4-4. Fragen zur Vorinstallation, Optionen und Maßnahmen**

Frage	Option/Maßnahme	Option/Maßnahme	Nächster Schritt
Muss ich ein bestimmtes unterstütztes Betriebssystem für die IT Assistant-Installation wählen?	Stellen Sie sicher, dass das Betriebssystem für die zu installierenden Komponenten unterstützt ist.	Installieren Sie IT Assistant bei einem großen Netzwerk auf einem Server-Betriebssystem.	Lesen Sie dazu die neueste Infodatei <a href="#">readme.txt</a> des IT Assistant, die entweder auf der Dell Support-Website unter <a href="#">support.dell.com</a> oder auf der CD <i>Dell Systems Management Consoles</i> zu finden ist.
Muss ich eine bestimmte Hardwarekonfiguration für die IT Assistant-Installation wählen?	Stellen Sie sicher, dass die Hardwarekonfiguration die empfohlenen Anforderungen erfüllt oder übertrifft, die an die auf dem System zu installierenden Komponenten gestellt werden.		
Soll ich die installierte Standard-Datenbank (SQL Server 2005 Express) verwenden oder die Microsoft SQL 2005-Server-Datenbank installieren?	Im Allgemeinen ist SQL Server 2005 Express ausreichend, wenn Sie weniger als 500 Systeme verwalten. Hoher Ereignis-Datenverkehr oder der Gebrauch des Leistungsüberwachungs-Subsystems könnte Sie jedoch dazu bewegen, SQL 2005 Server auszuwählen.	Bei Auswahl der SQL-Datenbank und bei starkem Ereignisverkehr sind z. B. höhere Prozessorgeschwindigkeiten und/oder zusätzliche Prozessoren, mehr Arbeitsspeicher und größere Festplattenspeicher erforderlich, um die Leistung des IT Assistant zu gewährleisten.	
Welche Systemverwaltungsprotokolle sollten installiert oder aktiviert werden?	Untersuchen Sie die Agenten, die auf den verwalteten Systemen ausgeführt werden sollen, und legen Sie fest, welche Protokolle unterstützt werden; prüfen Sie den zu verwaltenden Systemtyp.		Siehe " <a href="#">Dell OpenManage™ IT Assistant installieren, deinstallieren und erweitern</a> " und " <a href="#">Dell OpenManage™ IT Assistant zur Überwachung von Systemen konfigurieren</a> ".
Wie soll ich die IP-Adressen der verwalteten Systeme organisieren, wenn mehr als ein Systemverwaltungsprotokoll in einem Subnetz verwendet wird?	Falls möglich, gruppieren Sie Systeme, die das gleiche Systemverwaltungsprotokoll verwenden, in aufeinanderfolgenden Subnetzen. Diese Strategie erhöht die Handhabbarkeit während der Erstellung von IT Assistant-Ermittlungsbereichen.		
Werde ich funktionsbasierten Zugriff verwenden, um Benutzerebenen im IT Assistant zuzuweisen?	IT Assistant unterstützt normale funktionsbasierte Zugriffsebenen. Die drei unterstützten Ebenen sind: Benutzer, Hauptbenutzer und Administrator.	Die Verwendung dieser Zugriffsfunktionen in Ihrem Unternehmen kann eine zusätzliche Sicherheitsstufe bieten.	Siehe " <a href="#">Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten</a> ".

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Berichterstattung und Task-Verwaltung

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Benutzerdefinierte Berichterstattung](#)
- [IT Assistant-Datenbankschemainformationen](#)
- [Tasks verwalten](#)

Dell OpenManage™ IT Assistant hat die Befähigung:

- 1 Benutzerspezifische Report für alle Systeme in Ihrem Unternehmen zu erstellen
- 1 Befehlszeilenanleitungen auf verwalteten Geräten von einer zentralen Konsole aus durchführen, einschließlich Herunterfahren und Hochfahren
- 1 Software-Übereinstimmungsprüfungen und -Aktualisierungen auf einem einzelnen verwalteten System durchzuführen

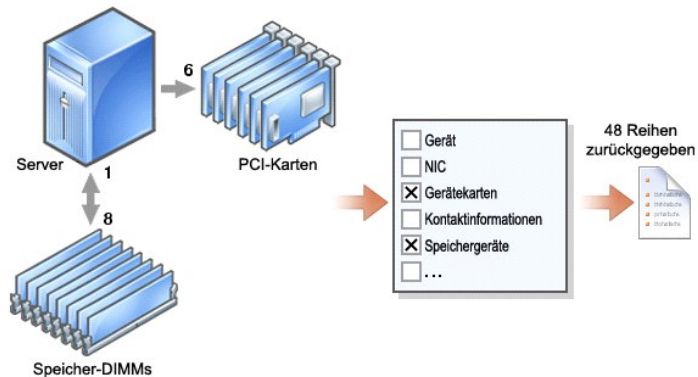
Die Grundlagen dieser Fähigkeiten sind hier mithilfe der gleichen Benutzerszenarien angezeigt, welche in "[Dell OpenManage™ IT Assistant zur Überwachung von Systemen konfigurieren](#)" dargestellt sind. Detailliertere Informationen zu diesen Themen finden Sie in der [Dell OpenManage IT Assistant-Onlinehilfe](#).

## Benutzerdefinierte Berichterstattung

IT Assistant verwendet Daten der Microsoft® SQL Serverdatenbank, um an die Bedürfnisse des Kunden angepasste Reporte zu erstellen. Diese Reporte basieren auf Daten, die während der Ermittlungs- und Bestandsaufnahmezyklen gesammelt wurden.

Die Geräte oder Gruppen die Sie zur Aufnahme in den Report auswählen, entsprechen Feldern in der IT Assistant-Datenbank. Wenn Sie einen Report ausführen, wird eine Datenbankabfrage erstellt. Die folgende Abbildung zeigt ein Beispiel.

Abbildung 9-1. Benutzerdefinierte Berichterstattung im IT Assistant



Zum Beispiel können Sie einen Report zusammenstellen, der folgendes enthält:

- 1 Details zu den Hardwaregeräten, die von IT Assistant verwaltet werden, einschließlich Servern, Schaltern und Speichergeräten
- 1 BIOS-, Firmware- und Treiber-Versionen, die auf bestimmten Geräten enthalten sind
- 1 Andere Details zum Bestand oder den Betriebskosten

Sie können für jeden Report verschiedene Ausgabeformate, wie HTML, XML oder CSV (von Komma getrennte Werte) angeben. Alle von Ihnen erstellten benutzerspezifischen Reportvorlagen können gespeichert und später verwendet werden.



## Neuen Report erstellen

Um die Reportfähigkeiten von IT Assistant zu illustrieren, werden wir uns noch einmal das Unternehmen von Sabine ansehen:

In ihrer Gruppe verwalteter Systeme hat sie 50 Dell™ PowerEdge™-Server. Sie ist sich jedoch nicht ganz sicher, welcher Netzwerkschnittstellenkartentyp auf welchen Servern installiert ist. Sie kann diese Frage mithilfe des Reporthilfsprogramms von IT Assistant schnell beantworten:

Von IT Assistant aus wird Sabine wie folgt vorgehen:

1. Sie wählt **Ansicht** → **Reporte** aus und klickt dann mit der rechten Maustaste auf **Alle Reporte** im linken Navigationsfenster.
2. Sie wählt **Neuer Report**.


Der Report hinzufügen-Assistent startet.

Sie gibt dann folgendes an:

- 1. Einen **Namen** für ihren Report, der nicht länger als 64 Zeichen sein darf
- 1. Eine optionale **Beschreibung**

Klicken Sie auf **Weiter**.

3. Im Dialogfeld **Geräte auswählen** wählt Sabine **Geräte/Gruppen aus der unten stehenden Struktur auswählen** aus und dann **Server** aus der Liste der verfügbaren Geräte.

 **ANMERKUNG:** Die Auswahl des Attributs der höchsten Ebene in der Geräteliste bedeutet die automatische Auswahl aller Attribute darunter. Die Erweiterung der Attribute in der Struktur ermöglicht Ihnen, die spezifischen Attribute auszuwählen, die Sie einschließen wollen. Ein Häkchen mit grauem Hintergrund für die Gruppenauswahl zeigt an, dass Sie innerhalb der Gruppe individuelle Auswahlen getroffen haben. Ein Häkchen mit weißem Hintergrund zeigt an, dass Sie die komplette Gruppe ausgewählt haben. Folglich ist die Auswahl bei einer Änderung der Gruppenmitgliedschaft auf die modifizierten Gruppenmitglieder anwendbar.

Klicken Sie auf **Weiter**.

4. Unter **Attribut auswählen** sucht sie **NIC** aus.
5. Als Nächstes legt sie eine bevorzugte **Sortieren nach**-Reihenfolge fest und klickt auf **Weiter**.
6. Auf der Seite **Zusammenfassung** akzeptiert sie entweder ihre Auswahl oder wechselt zurück und ändert sie. Hierdurch wird ein neuer Report erstellt mit dem Namen, den Sabine in [Schritt 2](#) festgelegt hat.

Wenn Sabine ihre Konfiguration bestätigt hat, wechselt sie zum Fenster **Reporte** in IT Assistant, klickt mit der rechten Maustaste auf den Reportnamen, den sie erstellt hat, und wählt **Ausführen** → **HTML-Reporte** aus.

Ein auf HTML-Format basierender Report mit NIC-Geräteinformationen wird zu allen 50 PowerEdge-Servern des Unternehmens angezeigt.

## Einen abfragebasierten Report wählen:


Sabine könnte auch einen abfragebasierten Report wählen. Statt **Geräte/Gruppen aus der Struktur unten auswählen** im Report-Assistenten auszusuchen, könnte Sie sich für **Abfrage auswählen** entscheiden. Dann kann sie entweder eine zuvor erstellte Abfrage auswählen oder, durch Klicken auf die Schaltfläche **Neu**, eine neue Abfrage erstellen. Sie kann die Parameter für einen Abfrage-Report wie in der folgenden Tabelle gezeigt, angeben:

Tabelle 9-1. Abfragereportparameter

<b>Name der Abfrage</b>	Gibt den Namen der Abfrage an.
<b>Abfragekriterien</b>	Gibt die Abfragekriterien an. Um z. B. eine neue Abfrage mit den Abfragekriterien für alle Geräte zu erstellen, die sich auf ein Subnetz beziehen, geben Sie folgendes an:  Where: IP Address Starts With 143.166.155

	<p>(Wo: die IP-Adresse beginnt mit 143.166.155)</p> <p>Die Abfrage-Operatoren sind:</p> <ul style="list-style-type: none"> <li>1 Enthält - legt fest, dass die Abfragekriterien-Zeichenkette einen bestimmten Satz von Zeichen enthält.</li> <li>1 Endet mit - legt fest, dass die Abfragekriterien mit einem bestimmten Satz von Zeichen enden.</li> <li>1 Ist - legt fest, dass die Abfragekriterien-Zeichenkette mit diesen Zeichen genau übereinstimmt.</li> <li>1 Beginnt mit - legt fest, dass die Abfragekriterien-Zeichenkette mit diesen Zeichen beginnt.</li> </ul> <p>Sie können die Abfrage mit bis zu 10 Unterabfragen erweitern, die zusammen die gesamte Abfrage ausmachen. Sie verbinden die Unterabfragen anhand von UND/ODER-Operatoren.</p> <p><b>ANMERKUNG:</b> Wenn Sie irgendwelche Änderungen vornehmen während Sie eine bestehende Abfrage bearbeiten und diese Abfrage speichern, wird die ursprüngliche Abfrage ersetzt.</p>
<b>Abfrage ausführen</b>	Führt die Abfrage aus und zeigt die Ergebnisse.
<b>Abfrage speichern</b>	Speichert die Abfrage.
<b>Abbrechen</b>	Schließt das Fenster <b>Abfragebearbeiter</b> ohne die Eingaben zu speichern.

 **ANMERKUNG:** Sie können auf **Abfrage ausführen** klicken, um eine Abfrage vor dem Speichern zu testen.

 **ANMERKUNG:** Wenn Sie Reporte zu RAC-Geräten ausführen möchten und **RAC-Typ** als eines der im Report aufzuführenden Attribute wählen, wird der erstellte Report eventuell die Wert 2, 8 oder 16 für die Spalte RAC-Typ aufführen. Diese Wert sind wie folgt zugeordnet:

- 2 = DRAC II
- 8 = DRAC III/DRAC 4/DRAC 5
- 16 = Baseboard-Verwaltungs-Controller (BMC)

## Bearbeiten, Löschen oder Reporte ausführen

Ganz gleich, welche Art von Report Sabine erstellt, sie kann ihn jederzeit bearbeiten, löschen, umbenennen oder ausführen, indem sie mit der rechten Maustaste auf den Reportnamen im Fenster **Reporte** klickt.

## Vordefinierte Reporte

IT Assistant bietet mehrere vordefinierte Reporte, die Sie sofort verwenden können. Diese Reporte werden im linken Teil des Fensters **Reporte** angezeigt. Klicken Sie auf den Reportnamen, um eine Zusammenfassung der Informationen zu sehen, die der Report sammeln soll.

## IT Assistant-Datenbank-Schemainformationen

IT Assistant sammelt Daten, die in zugeordneten Tabellen gespeichert und durch die **DeviceID**, eine interne Kennzeichnung, verknüpft sind. Die zugeordneten Daten sind in den folgenden Tabellen gespeichert.


 **ANMERKUNG:** Die Hauptschlüssel der Tabelle sind mit einem Sternchen (\*) markiert.

Tabelle 9-2. IT Assistant-Datenbank-Schemainformationen

Spaltenname	Datentyp	Datengröße	Nullen zugelassen	Beschreibung
<b>Tabelle der Geräteoptionen</b>				
DeviceId*	int	4	Nein	Interne Geräteidentifikation, die in allen zugehörigen Tabellen als fremder Schlüssel verwendet wird.
DeviceName	nvarchar	256	Ja	Der von IT Assistant zur Kennzeichnung des Geräts verwendete Name, welcher in der <b>Gerätestruktur</b> der Benutzeroberfläche (UI) angezeigt wird.
DeviceInstrumentationName	nvarchar	256	Ja	Der Name des Geräts, der von MIB II SysName oder von CIM abgerufen wird.
DeviceDNSName	nvarchar	256	Ja	Vollständig qualifizierter Name, wie durch DNS-Server zurückgegeben
DeviceType	int	4	Ja	Der Gerätetyp. Workstations = 3 Server = 4 Desktops = 5 Portables = 6 Netzwerkschalter = 8

				RACs = 9 KVMs = 10 Unbekannt = 2 oder ein nicht aufgeführter Wert
DeviceInventoryTime	datetime	8	Ja	Der Zeitpunkt, zu dem IT Assistant zum letzten Mal Bestandsaufnahmedaten vom Gerät eingesammelt hat.
DeviceStatusedTime	datetime	8	Ja	Der Zeitpunkt, zu dem IT Assistant zum letzten Mal globale Funktionszustandsdaten vom Gerät eingesammelt hat
DeviceDiscoveredTime	datetime	8	Ja	Der Zeitpunkt, zu dem IT Assistant zum letzten Mal das System befragt hat, um festzustellen, welche Agenten vorhanden sind.
DeviceProtocols	int	4	Ja	Bitmaske, die anzeigt, welche Protokolle das Gerät unterstützt. Bit 1 = SNMP Bit 4 = CIM Bit 8 = IPMI
DevicePreferredProtocol	int	4	Ja	Das vom Remote-Gerät für seine Verwaltung bevorzugte Protokoll. 1 = SNMP 2 = CIM
DeviceAssetTag	nvarchar	64	Ja	Dieses Attribut definiert die Systemkennnummer des Geräts.
DeviceServiceTag	nvarchar	64	Ja	Dieses Attribut definiert die Service-Tag-Nummer des Geräts.
DeviceSystemId	int	4	Ja	Die Hersteller-ID des Systemmodells.
DeviceSystemModelType	nvarchar	64	Ja	Der Modellname des Herstellers.
DeviceLocation	nvarchar	256	Ja	Der vom Remote-Agenten abgerufene Gerätestandort.
DellSystem	int	4	Ja	Die boolesche Flagge, die anzeigt, ob ein Gerät einen von Dell aktivierten Agenten besitzt.
SubnetLastDiscoveredOn	nvarchar	256	Ja	Der Ermittlungsbereich, der zur letzten Ermittlung des Geräts verwendet wurde.
<b>Tabelle der Agentenoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel (FK) zur Gerätetabelle.
AgentName*	nvarchar	256	Nein	Der Name des Agenten.
AgentVersion	nvarchar	64	Ja	Die Version des Agenten.
AgentManufacturer	nvarchar	64	Ja	Der Hersteller des Agenten.
AgentDescription	nvarchar	256	Ja	Eine kurze Beschreibung dessen, was der Agent verwaltet.
AgentGlobalStatus	int	4	Ja	Der globale Status des Agenten. Nicht bekannt = 0 Unbekannt = 1 Normal = 4 Warnung = 8 Kritisch = 16
AgentInstallTime	datetime	8	Ja	Zeitpunkt, zu dem der Agent installiert wurde (falls verfügbar).
AgentId	int	4	Ja	Interne ID, die zur Unterscheidung zwischen Agenten verwendet wird. Bandexterner RAC-Agent = 1 Server Administrator = 2 Microsoft@ WMI = 3 OMCI = 4 Physischer Verwalter = 6 Speicherverwalter = 7 Dell™ PowerEdge™1655MC-Schalter = 8 Dell PowerConnect™ 3248 = 9 PowerConnect 5224 = 10 PowerConnect 3024 = 11 PowerConnect 5012 = 12 PowerConnect 3048 = 13 PowerConnect 3000MIB = 14 KVM = 15 Bestandsaufnahme-Agent = 16 Bandinterner RAC-Agent = 17
AgentURL	nvarchar	256	Ja	Die Internetadresse der Verwaltungsanwendung (wenn der Agent webbasierten Zugriff unterstützt).
AgentData	ntext	16	Ja	Erweiterte Agentendaten; nur zum internen Gebrauch.
<b>Tabelle der Array-Festplatte</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ArrayDiskNumber*	int	4	Nein	Die Instanznummer dieses Array-Festplatteneintrags.
ArrayDiskName	nvarchar	256	Ja	Der Name der Array-Festplatte, wie er in Storage Management dargestellt wird.
ArrayDiskVendorName	nvarchar	64	Ja	Der Name des Array-Festplatten-Verkäufers bzw. Wiederverkäufers.
ArrayDiskModelNumber	nvarchar	64	Ja	Die Modellnummer der Array-Festplatte.
ArrayDiskSerialNumber	nvarchar	64	Ja	Die eindeutige Herstelleridentifikationsnummer der Array-Festplatte.
ArrayDiskPartNumber	nvarchar	64	Ja	Die Teilenummer der Array-Festplatte.
ArrayDiskRevision	nvarchar	64	Ja	Die Firmware-Version der Array-Festplatte.
ArrayDiskEnclosureId	nvarchar	64	Ja	Die SCSI-ID des Gehäuseprozessors, dem diese Array-Festplatte zugeordnet ist.
ArrayDiskChannel	int	4	Ja	Der Bus, an dem diese Array-Festplatte angeschlossen ist.
ArrayDiskLength	int	4	Ja	Die Größe der Array-Festplatte in Gigabyte. Bei einer Größe von 0 ist sie kleiner als ein Gigabyte.

ArrayDiskBusType	nvarchar	64	Ja	Der Bustyp der Array-Festplatte. Mögliche Werte: SCSI, IDE, Fibre Channel, SSA, USB und SATA.
ArrayDiskTargetId	int	4	Ja	Die SCSI-Ziel-ID, die dieser Array-Festplatte zugewiesen wurde.
ArrayDiskLUNId	int	4	Ja	Die permanente eindeutige ID dieser Array-Festplatte.
<b>Tabelle der Controller-Optionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ControllerNumber*	int	4	Nein	Die Instanznummer dieses Controller-Eintrags.
ControllerName	nvarchar	64	Ja	Der Name des Controllers in diesem Subsystem, wie er in Storage Management dargestellt ist. Umfasst Controller-Typ und -Instanz, z. B.: PERC 3/QC 1.
ControllerVendor	nvarchar	64	Ja	Der Name des Händlers des Controllers.
ControllerType	nvarchar	64	Ja	Der Controller-Typ.
ControllerState	nvarchar	64	Ja	Der aktuelle Zustand des Controller-Subsystems.
ControllerStatus	int	4	Ja	Der Controller-Status
ControllerFWVersion	nvarchar	64	Ja	Die aktuelle Firmware-Version des Controllers.
ControllerCacheSize	int	4	Ja	Die aktuelle Cache-Speichermenge des Controllers.
ControllerPhysicalDeviceCount	int	4	Ja	Die Anzahl der physikalischen Geräte auf dem Controller-Kanal, einschließlich Festplatten und Controller.
ControllerLogicalDeviceCount	int	4	Ja	Die Anzahl der virtuellen Laufwerke auf dem Controller.
ControllerPartnerStatus	nvarchar	64	Ja	Weist auf die Verfügbarkeit des redundanten Controllers in einer redundanten Konfiguration hin.
ControllerMemorySize	int	4	Ja	Die Speichergröße des Controllers.
ControllerDriveChannelCount	int	4	Ja	Die Anzahl von redundanten Controller-Laufwerkkanälen.
ControllerChargeCount	int	4	Ja	Zeigt wie oft die Batterie dieses Controllers aufgeladen wurde.
ControllerDriverVersion	nvarchar	64	Ja	Die zurzeit installierte Treiberversion dieses Controllers.
ControllerSPAReadCacheSize	int		Ja	Lese-Cache-Größe auf Controller A.
ControllerSPAWriteCacheSize	int		Ja	Die Schreib-Cache-Größe auf Controller A.
ControllerSPBReadCacheSize	int		Ja	Die Lese-Cache-Größe auf Controller B.
ControllerSPBWriteCacheSize	int		Ja	Die Schreib-Cache-Größe auf Controller B.
ControllerCachePageSize	int		Ja	Die Page-Cache-Größe für den Controller.
ControllerSPAReadCachePolicy	nvarchar	64	Ja	Die Lese-Cache-Regel auf Controller A.
ControllerSPAWriteCachePolicy	nvarchar	64	Ja	Die Schreib-Cache-Regel auf Controller A.
ControllerSPBReadCachePolicy	nvarchar	64	Ja	Die Lese-Cache-Regel auf Controller B.
ControllerSPBWriteCachePolicy	nvarchar	64	Ja	Die Schreib-Cache-Regel auf Controller B.
<b>Tabelle der Gehäuseoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
EnclosureNumber*	int	4	Nein	Die Instanznummer dieses Gehäuseeintrags.
EnclosurePartNumber	nvarchar	64	Ja	Die Teilenummer des Gehäuseeintrags.
EnclosureSerialNumber	nvarchar	64	Ja	Die Seriennummer des Gehäuseeintrags.
EnclosureName	nvarchar	256	Ja	Der Gehäusename.
EnclosureVendor	nvarchar	256	Ja	Der Name des Händlers des Gehäuses.
EnclosureId	int	4	Ja	Die SCSI-Adresse des Prozessors.
EnclosureLocationofManufacture	nvarchar	256	Ja	Der Herstellungsort des Gehäuses.
EnclosureServiceTag	nvarchar	64	Ja	Die Gehäuse-Identifikation, die bei Anfragen an den Kunden-Support benötigt wird.
EnclosureAssetTag	nvarchar	64	Ja	Vom Benutzer definierbare Systemkennnummer des Gehäuses.
EnclosureAssetName	nvarchar	64	Ja	Vom Benutzer definierbarer Bestandsname des Gehäuses.
EnclosureProductId	nvarchar	64	Ja	Die Produkt-Identifikation des Gehäuses, die auch dem Gehäusotyp entspricht.
EnclosureType	nvarchar	64	Ja	Der Gehäusotyp.
EnclosureChannelNumber	int	4	Ja	Die Kanalnummer, oder der Bus, an dem das Gehäuse angeschlossen ist.
EnclosureBackplanePartNum	nvarchar	64	Ja	Die Teilenummer der Gehäuse-Rückwandplatine.
EnclosureSCSIId	int	4	Ja	Die SCSI-ID des Controllers, an den dieses Gehäuse angeschlossen ist.
<b>Tabelle der Gehäusemanagementmodul-Optionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
EMMNumber*	int	4	Nein	Die Instanznummer des Gehäusemanagementmoduls.
EMMName	nvarchar	256	Ja	Der Name des Gehäuses.
EMMVendor	nvarchar	256	Ja	Der Name des Händlers des Managementmoduls.
EMMPartNumber	nvarchar	64	Ja	Die Teilenummer des Gehäusespeichermoduls.
EMMFWVersion	nvarchar	64	Ja	Die Firmware-Version des Gehäusespeichermoduls.
<b>Tabelle der virtuellen Laufwerkoptionen</b>				

DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
VirtualDiskNumber*	int	4	Nein	Die Instanznummer dieses virtuellen Laufwerkeintrags.
VirtualDiskName	nvarchar	256	Ja	Die vom Storage Management erstellte oder vom Benutzer eingegebene Bezeichnung des virtuellen Laufwerks.
VirtualDiskDeviceName	nvarchar	256	Ja	Gerätename, der von den Mitgliedsfestplatten dieses virtuellen Laufwerks verwendet wird.
VirtualDiskLength	int	4	Ja	Die Größe dieser virtuellen Festplatte in Gigabyte.
VirtualDiskWritePolicy	nvarchar	64	Ja	Zeigt an, ob der Schreib-Cache des Controllers beim Schreiben an ein virtuelles Laufwerk verwendet wird.
VirtualDiskReadPolicy	nvarchar	64	Ja	Zeigt an, ob der Lese-Cache des Controllers beim Lesen von einem virtuellen Laufwerk verwendet wird.
VirtualDiskCachePolicy	nvarchar	64	Ja	Zeigt an, ob der Cache des Controllers zum Lesen von bzw. Schreiben zu einem virtuellen Laufwerk verwendet wird.
VirtualDiskLayout	nvarchar	64	Ja	Der RAID-Typ des virtuellen Laufwerks.
VirtualDiskStripeSize	int	4	Ja	Die Stripe-Größe dieses virtuellen Laufwerks in Bytes.
VirtualDiskStripeElementSize	int	4	Ja	Die Größe der Stripe-Elemente dieser virtuellen Festplatte in Blöcken.
VirtualDiskTargetId	int	4	Ja	Die eindeutige ID des virtuellen Laufwerks.
VirtualDiskLUNId	nvarchar	64	Ja	Die permanente eindeutige LUN-ID dieser virtuellen Festplatte.
<b>Tabelle der Datenträgeroptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
VolumeNumber*	int	4	Ja	Instanznummer des Datenträger-Eintrags.
VolumeDriveLetter	nvarchar	64	Ja	Der Pfad (oder Laufwerkbuchstabe) des Datenträgers gemäß dem Betriebssystem.
VolumeLabel	nvarchar	256	Ja	Die vom Benutzer definierbare Bezeichnung dieses Datenträgers.
VolumeSize	int	4	Ja	Die Größe des Datenträgers in Megabytes.
<b>Tabelle der Firmware-Optionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
FirmwareChassisIndex*	int	4	Nein	Der Firmware-Gehäuseindex (nullbasiert).
FirmwareIndex*	int	4	Nein	Der Firmware-Index (nullbasiert).
FirmwareType	nvarchar	64	Ja	Der Firmware-Typ.
FirmwareName	nvarchar	64	Ja	Der Name der Firmware.
FirmwareVersion	nvarchar	64	Ja	Die Firmware-Version
<b>Tabelle der Speichergeräteoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
MemoryDeviceChassisIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des zugeordneten Gehäuses.
MemoryDeviceIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des Speichergeräts.
MemoryDeviceName	nvarchar	256	Ja	Dieses Attribut definiert den Standort des Speichergeräts.
MemoryDeviceBankName	nvarchar	256	Ja	Dieses Attribut definiert den Standort der Bank des Speichergeräts.
MemoryDeviceType	nvarchar	256	Ja	Dieses Attribut definiert den Typ des Speichergeräts.
MemoryDeviceFormFactor	nvarchar	256	Ja	Dieses Attribut definiert den Formfaktor des Speichergeräts.
MemoryDeviceSize	int	4	Ja	Dieses Attribut definiert die Größe des Speichergeräts.
MemoryDeviceFailureMode	nvarchar	256	Ja	Dieses Attribut definiert den Fehlermodus des Speichergeräts.
<b>Tabelle der NIC-Optionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
NICId*	int	4	Nein	Die eindeutige Instanz-ID dieses NIC.
NICIPAddress	nvarchar	40	Ja	Die dem NIC zugewiesene IP-Adresse.
NICNetmask	nvarchar	40	Ja	Die dem NIC zugewiesene Subnetzmaske.
NICMACAddress	nvarchar	24	Ja	Die MAC-Adresse des NIC.
NICManufacturer	nvarchar	256	Ja	Der Händler des NIC.
NICPingable	int	4	Ja	Eine Flag, die anzeigt, dass IT Assistant mit dem Gerät mithilfe der IP-Adresse kommuniziert.
<b>Tabelle der Betriebssystemoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
OSId*	int	4	Nein	Die Instanz-ID für das Betriebssystem.
OSName	nvarchar	64	Ja	Der Name des Betriebssystems.
OSRevision	nvarchar	64	Ja	Die Revision des Betriebssystems (z. B. der Microsoft Windows®-Service Pack oder die Linux-Kernel-Version)
OSTotalPhysicalMemory	int	4	Ja	Die Gesamtmenge an physikalischem Speicher, die vom Betriebssystem in Megabytes gemeldet wird.
OSLocale	nvarchar	64	Ja	Das Gebietsschema für das Betriebssystem.

OSType	int	4	Ja	Der Typ des Betriebssystems.
<b>Tabelle der Netzteiloptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
PowerSupplyChassisIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des Gehäuses.
PowerSupplyIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des Netzteils.
PowerSupplyType	nvarchar	256	Ja	Dieses Attribut definiert den Typ des Netzteils.
PowerSupplyLocation	nvarchar	256	Ja	Dieses Attribut definiert den Standort des Netzteils.
PowerSupplyOutputWatts	int	4	Ja	Dieses Attribut definiert die maximale, anhaltende Ausgangswattleistung des Netzteils, in Zehntel-Watt.
<b>Tabelle der Prozessoroptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ProcessorChassisIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des Gehäuses.
ProcessorIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des Prozessors.
ProcessorFamily	nvarchar	256	Ja	Dieses Attribut definiert die Familie des Prozessorgeräts.
ProcessorCurrentSpeed	int	4	Ja	Dieses Attribut definiert die aktuelle Taktrate des Prozessorgeräts in MHz. Null zeigt an, dass die aktuelle Taktrate unbekannt ist.
ProcessorSlotNumber	int	4	Ja	Dieses Attribut definiert den Steckplatz, den der Prozessor belegt.
<b>Tabelle der SMBIOS-Optionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ParallelPortConfiguration	nvarchar	64	Ja	Definiert die Konfiguration der parallelen Schnittstelle.
ParallelPortMode	nvarchar	64	Ja	Der Modus der parallelen Schnittstelle.
SerialPortYesConfiguration	nvarchar	64	Ja	Definiert die Konfiguration der seriellen Schnittstelle 1.
SerialPort2Configuration	nvarchar	64	Ja	Definiert die Konfiguration der seriellen Schnittstelle 2.
IDEController	nvarchar	64	Ja	Legt fest, ob der IDE-Controller aktiviert oder deaktiviert ist.
BuiltInNIC	nvarchar	64	Ja	Legt fest, ob der integrierte NIC aktiviert oder deaktiviert ist.
BuiltInFloppy	nvarchar	64	Ja	Legt fest, ob der integrierte Disketten-Controller auf aktiviert, automatisch oder schreibgeschützt eingestellt ist.
BuiltInPointingDevice	nvarchar	64	Ja	Legt fest, ob die Schnittstelle des integrierten Zeigergeräts (die Maus) aktiviert oder deaktiviert ist.
WakeUpOnLAN	nvarchar	64	Ja	Definiert, ob Wake-on-LAN deaktiviert, nur für integrierte NIC aktiviert oder nur für Add-In-NIC aktiviert ist. Bei Auswahl der Option <b>Aktiviert mit Start zum NIC</b> , startet das System nach einer Remote-Aktivierung von der NIC-Start-ROM.
WakeUpOnLANMethod	nvarchar	64	Ja	Definiert die vom System unterstützte Wake-on-LAN-Methode.
AutoOn	nvarchar	64	Ja	Definiert die automatische Konfiguration: deaktiviert, jeden Tag oder Wochentags (Montag bis Freitag).
AutoOnHour	nvarchar	64	Ja	Definiert zu welcher Stunde das System eingeschaltet wird (0-23).
AutoOnMinute	nvarchar	64	Ja	Definiert die Minuten, während denen das System eingeschaltet ist (0-59).
BootSequence	nvarchar	64	Ja	Definiert die Startsequenz für den nächsten Systemstart.
ChassisIntrusionStatus	nvarchar	64	Ja	Meldet den Status des Systems in Bezug zum <b>Gehäuseeingriff (Ermittelt oder Nicht ermittelt)</b> . Der Wert <b>Unbekannt</b> bedeutet, dass entweder der Gehäuseeingriff von diesem System nicht unterstützt wird oder dass die Meldung von Gehäuseeingriff-Ereignissen vom Benutzer deaktiviert wurde. Wenn der Wert <b>Ermittelt ist</b> , können Sie ihn auf <b>Nicht ermittelt</b> setzen, um dem System den Empfang des nächsten Ereignisses zu ermöglichen und das Erstellen von Ereignissen zu diesem Zeitpunkt zu stoppen.
IntegratedAudio	nvarchar	64	Ja	Der Status des integrierten Audiogeräts des Systems.
PCISlots	nvarchar	64	Ja	Der Status der Add-On-PCI-Steckplätze des Systems (aktiviert/deaktiviert).
USBPorts	nvarchar	64	Ja	Der Status der USB-Schnittstellen (ein/aus).
<b>Tabelle der Software-Bestandsaufnahmeoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ComponentId	nvarchar	64	Ja	Der Komponentenkennzeichner für die Software.
InstanceId*	nvarchar	32	Nein	Der Instanz-Kennzeichner für die Hardware.
HWDeviceId	nvarchar	16	Ja	Der Hardware-Gerätekenzeichner der PCI-ID.
HWVendorId	nvarchar	16	Ja	Der Hardware-Herstellerkenzeichner der PCI-ID.
HWSubDeviceId	nvarchar	16	Ja	Der Hardware-Untergerätekenzeichner der PCI-ID.
HWSubVendorId	nvarchar	16	Ja	Der Hardware-Unterherstellerekenzeichner der PCI-ID.
SubComponentId	nvarchar	64	Ja	Der Unterkomponentenkennzeichner für die Hardware.
HWDescription	nvarchar	128	Ja	Die Beschreibung der Hardware.
SoftwareType	nvarchar	64	Ja	Der Softwaretyp, z. B. Treiber (DRVR), Firmware (FRMW) usw.
SoftwareVersion	nvarchar	64	Ja	Die Nummer der Softwareversion.
SoftwareDescription	nvarchar	128	Ja	Die Beschreibung der Software.
<b>Tabelle der Software-Bestandsaufnahme-Betriebssystemoptionen</b>				

DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
OSVendor	nvarchar	64	Ja	Der Name des Betriebssystemherstellers.
OSMajorVersion	nvarchar	16	Ja	Die Hauptversion des Betriebssystems.
OSMinorVersion	nvarchar	16	Ja	Die Nebenversion des Betriebssystems.
OSSPMajorVersion	nvarchar	16	Ja	Die Hauptversion des Service Pack.
OSSPMinorVersion	nvarchar	16	Ja	Die Nebenversion des Service Pack.
<b>Tabelle der Schaltergeräteoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
SwitchIndex*	int	4	Nein	Der Index des Schalters.
SwitchAssetTag	nvarchar	255	Ja	Die Systemkennnummer des Schalters.
SwitchServiceTag	nvarchar	255	Ja	Die Service-Tag-Nummer des Schalters.
SwitchSerialNumber	nvarchar	255	Ja	Die Seriennummer des Schalters.
<b>Tabelle der Betriebskostenoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
CooIndex*	int	4	Nein	Der Index der Betriebskosten.
PurchaseCost	nvarchar	64	Ja	Die ursprünglichen Erwerbskosten des Systems.
WayBillNumber	nvarchar	64	Ja	Die Frachtbriefnummer.
InstallationDate	nvarchar	64	Ja	Das Datum, an dem das System installiert wurde.
PurchaseOrderNumber	nvarchar	64	Ja	Die Kaufauftragsnummer.
PurchaseDate	nvarchar	64	Ja	Das Datum, an dem das System erworben wurde.
SigningAuthorityName	nvarchar	64	Ja	Die Signaturstellenreferenz.
OriginalMachineConfigurationExpensed	nvarchar	64	Ja	Die ursprüngliche Systemkonfiguration, deren Kosten verrechnet wurden.
OriginalMachineConfigurationVendorName	nvarchar	64	Ja	Der Name des Herstellers der ursprünglichen Systemkonfiguration.
CostCenterInformationVendorName	nvarchar	64	Ja	Der Herstellername in den Kostenstelleninformationen
UserInformationUserName	nvarchar	64	Ja	Der Name des Benutzers.
ExtendedWarrantyStartDate	nvarchar	64	Ja	Das Startdatum der erweiterten Garantie.
ExtendedWarrantyEndDate	nvarchar	64	Ja	Das Enddatum der erweiterten Garantie.
ExtendedWarrantyCost	nvarchar	64	Ja	Die Kosten der erweiterten Garantie.
ExtendedWarrantyProviderName	nvarchar	64	Ja	Der Name des Anbieters der erweiterten Garantie.
OwnershipCode	nvarchar	64	Ja	Der Besitzcode.
CorporateOwnerName	nvarchar	64	Ja	Der Name des Besitzers.
HazardousWasteCodeName	nvarchar	64	Ja	Der Sondermüll-Code-Name.
DeploymentDateLength	nvarchar	64	Ja	Die Länge des Bereitstellungszeitraums.
DeploymentDurationUnitType	nvarchar	64	Ja	Art der Einheit - Bereitstellungsdauer.
TrainingName	nvarchar	64	Ja	Der Trainingsname.
OutsourcingProblemDescription	nvarchar	64	Ja	Die Beschreibung des Problems der Auslagerung von Tätigkeiten.
OutsourcingServiceFee	nvarchar	64	Ja	Die Servicegebühr für die Auslagerung von Tätigkeiten.
OutsourcingSigningAuthority	nvarchar	64	Ja	Die Signaturstelle für die Auslagerung von Tätigkeiten.
OutsourcingProviderFee	nvarchar	64	Ja	Die Anbietergebühr für die Auslagerung von Tätigkeiten.
OutsourcingProviderServiceLevel	nvarchar	64	Ja	Die Anbieter-Dienstebene für die Auslagerung von Tätigkeiten.
InsuranceCompanyName	nvarchar	64	Ja	Der Name der Versicherungsgesellschaft.
BoxAssetTagName	nvarchar	64	Ja	Die Systemkennnummer des Geräts.
BoxSystemName	nvarchar	64	Ja	Der Host-Name des Geräts.
BoxCPUSerialNumberName	nvarchar	64	Ja	Die CPU-Seriennummer des Geräts.
DepreciationDuration	nvarchar	64	Ja	Die Abschreibungsdauer.
DepreciationDurationUnitType	nvarchar	64	Ja	Die Einheiten für die Abschreibungsdauer.
DepreciationPercentage	nvarchar	64	Ja	Der Abschreibungsprozentsatz.
DepreciationMethod	nvarchar	64	Ja	Die Abschreibungsmethode.
RegistrationIsRegistered	nvarchar	64	Ja	Die Registrierung ist registriert.
<b>Tabelle der Kontaktinformationsoptionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ContactName*	nvarchar	64	Nein	Der Kontaktname.
ContactInformation	nvarchar	64	Ja	Die Informationen zu diesem Kontakt.
ContactDescription	nvarchar	64	Ja	Die Beschreibung dieses Kontakts.
<b>Tabelle der Cluster-Optionen</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ClusterIndex*	int	4	Nein	Der Cluster-Index.
ClusterType	int	4	Ja	Der Cluster-Typ.

ClusterTypeName	nvarchar	64	Ja	Der Name des Cluster-Typs.
ClusterName	nvarchar	255	Ja	Der Cluster-Name.
ClusterDescription	nvarchar	255	Ja	Die Beschreibung des Clusters.
<b>Tabelle zu FRU-Informationen</b>				
DeviceId*	int	4	Nein	Die Geräte-ID.
FRUChassisIndex*	int	4	Nein	Der Gehäuseindex der austauschbaren Funktionseinheit (FRU).
FRUIndex*	int	4	Nein	Der FRU-Index.
FRUDeviceName	nvarchar	255	Ja	Der FRU-Gerätename.
FRUManufacturer	nvarchar	255	Ja	Der Name des FRU-Herstellers.
FRUSerialNumber	nvarchar	255	Ja	Die FRU-Seriennummer.
FRUPartNumber	nvarchar	255	Ja	Die FRU-Teilenummer.
FRURevision	nvarchar	255	Ja	Die FRU-Revisionsnummer.
FRUManufacturingDate	Datum	8	Ja	Das FRU-Herstelldatum.
<b>Tabelle des Druckerverbrauchsmaterials</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
PrinterSupplyIndex*	int	4	Nein	Der Druckerverbrauchsmaterialindex.
PrinterSupplyDescription	nvarchar	64	Ja	Die Verbrauchsmaterialbeschreibung des Druckers.
PrinterSupplyLevel	nvarchar	16	Ja	Die Druckerverbrauchsmaterialstufe.
PrinterSupplyMaxLevel	int	4	Ja	Die maximale Druckerverbrauchsmaterialstufe.
PrinterSupplyType	nvarchar	64	Ja	Der Druckerverbrauchsmaterialtyp.
<b>Tabelle zum Druckereingabefach</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
PrinterInputTrayIndex*	int	4	Nein	Der Index des Druckereingabefachs.
PrinterInputName	nvarchar	64	Ja	Der Name der Druckereingabe.
PrinterInputVendorName	nvarchar	64	Ja	Name des Drucker-Verkäufers bzw. -Wiederverkäufers.
PrinterInputModel	nvarchar	64	Ja	Name des Eingabefachmodells.
PrinterInputDescription	nvarchar	64	Ja	Die Eingabebeschreibung des Druckers.
PrinterInputMaxCapacity	nvarchar	64	Ja	Die maximale Kapazität des Druckereingabemoduls.
PrinterInputCurrentCapacity	nvarchar	64	Ja	Die aktuelle Kapazität des Druckereingabemoduls.
PrinterInputMediaType	nvarchar	64	Ja	Der Datenträgertyp.
<b>Tabelle zum Druckerausgabefach</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
PrinterOutputIndex*	int	4	Nein	Der Ausgabeindex des Druckers.
PrinterOutputName	nvarchar	64	Ja	Name der Ausgabeeinheit.
PrinterOutputVendorName	nvarchar	64	Ja	Name des Drucker-Verkäufers bzw. -Wiederverkäufers.
PrinterOutputModel	nvarchar	64	Ja	Name des Ausgabefachmodells.
PrinterOutputDescription	nvarchar	64	Ja	Die Ausgabebeschreibung des Druckers.
PrinterOutputMaxCapacity	nvarchar	64	Ja	Die maximale Ausgabekapazität des Druckers.
<b>Tabelle zur Druckerabdeckung</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
PrinterCoverIndex*	int	4	Nein	Der Index zur Druckerabdeckung.
PrinterCoverDescription	nvarchar	64	Ja	Die Beschreibung der Druckerabdeckung.
PrinterCoverStatus	nvarchar	64	Ja	Der Status der Druckerabdeckung.
<b>Tabelle zum Bandlaufwerk</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
TapeDriveIndex*	int	4	Nein	Der Index zum Bandlaufwerk.
TapeDriveVendor	nvarchar	64	Ja	Name des Bandlaufwerkherstellers.
TapeDriveModel	nvarchar	64	Ja	Name des Bandlaufwerkmodells.
TapeDriveType	nvarchar	64	Ja	Der Bandlaufwerktyp.
TapeDriveFirmwareVersion	nvarchar	32	Ja	Firmware-Version des Bandlaufwerks.
TapeDriveSerialNumber	nvarchar	32	Ja	Seriennummer des Bandlaufwerks.
TapeDriveWMN	nvarchar	32	Ja	WMN des Bandlaufwerks.
TapeDriveCleaningRequired	nvarchar	32	Ja	Gibt an, ob das Bandlaufwerk gereinigt werden muss.
TapeLibraryScsiId	int			Gibt die SCSI-ID der Bandbibliothek an
<b>Tabelle zur Bandbibliothek</b>				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
TapeLibraryIndex*	int	4	Nein	Der Index zur Bandbibliothek.
TapeLibraryVendor	nvarchar	64	Ja	Name des Bandbibliothekherstellers.
TapeLibraryModel	nvarchar	64	Ja	Name des Bandbibliotheksmodells.



TapeLibraryFirmwareVersion	nvarchar	32	Ja	Firmware-Version der Bandbibliothek.
TapeLibraryDriveCount	int	4	Ja	Die Laufwerkanzahl.
TapeLibrarySlotCount	int	4	Ja	Die Anzahl der Steckplätze.
TapeLibrarySerialNumber	nvarchar	32	Ja	Seriennummer der Bandbibliothek.

## Tasks verwalten

IT Assistant ermöglicht Ihnen auch, bestimmte Tasks auf verwalteten Systemen im gesamten Unternehmen im Remote-Zugriff auszuführen. Diese Tasks umfassen:

- 1 Allgemeine Befehlszeilenausführung (die Fähigkeit, die Dell OpenManage Server Administrator-Befehlszeilenoberfläche im Remote-Zugriff aufzurufen, wird auch unterstützt, wenn Dell OpenManage 4.3 (oder höher) -Instrumentation aktiviert ist)
- 1 Gerätesteuerung, einschließlich Herunterfahren und Hochfahren
- 1 Geplante Software-Aktualisierungen
- 1 Die Fähigkeit, Intelligente Plattformverwaltungsschnittstelle (IPMI) -Befehle im Remote-Zugriff auszuführen
- 1 Die Fähigkeit, Remote-Client-Instrumentationsbefehle im Remote-Zugriff auszuführen
- 1 Fähigkeit, den Dell-Agenten (Server Administrator) auf Systemen bereitzustellen

 **ANMERKUNG:** Die Befehlszeilenooptionen IPMI und Remote-Client-Instrumentation sind eventuell nicht verfügbar, wenn IT Assistant die Installation der notwendigen Komponenten in der IT Assistant-Dienststufe nicht ermittelt.

Diese Tasks können so konfiguriert werden, dass sie nach einem festgelegten Plan oder sofort ausgeführt werden. Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.


## Gerätesteuerungs-Task erstellen

Sabine möchte z. B. die Stromsteuerung eines Systems über IT Assistant vornehmen. Um diese Tasks in IT Assistant auszuführen, würde sie folgendermaßen vorgehen:

1. Sie wählt **Verwalten** → **Tasks** aus und klickt im linken Navigationsfenster mit der rechten Maustaste auf **Gerätesteuerung**.
2. Wählen Sie **Neuer Task**.

Der Task-Erstellungsassistent wird eingeblendet.

3. Sabine gibt einen **Task-Namen** ein, wählt **Gerät herunterfahren** aus dem Pulldown-Menü **Task-Typ** aus und klickt dann auf **Weiter**.
4. Im Fenster **Art des Herunterfahrens auswählen** wählt sie Folgendes:
  - a. **Neustart**, um einen problematischen Server neu zu starten, der mehrere E-Mail-Warnungen ausgegeben hat
  - b. **Aus- und einschalten (falls unterstützt)**. Über diese Option lässt sich ein Aus- und Einschalten durchführen, wenn IT Assistant über die Dell-Instrumentation anhand von SNMP mit dem System kommuniziert. Der Strom zum Gerät wird aus- und wieder eingeschaltet. Wenn die Stromzufuhr wieder hergestellt ist, wird das Gerät neu gestartet.
  - c. **Netzstrom ein**, um ein ASF-aktiviertes Gerät einzuschalten.
  - d. **Ausschalten**, um das System herunterzufahren.
  - e. **Betriebssystem zuerst herunterfahren**. Über diese Option wird ein ordentliches Herunterfahren des Betriebssystems ausgeführt, bevor die ausgewählte Maßnahme zum Herunterfahren ausgeführt wird.

 **ANMERKUNG:** Betriebssystem zuerst herunterfahren wird für ASF-aktivierte Geräte nicht angezeigt.

5. Im Fenster **Geräte auswählen** erweitert sie die **Servergeräteleiste** und wählt nur den Server aus, den sie neu starten will.
6. In **Zeitplan auswählen** wählt sie **Jetzt ausführen**.
7. Wenn sie ein SNMP-aktiviertes System neu startet, muss sie Instrumentationsbenutzernamen und -kennwort im Fenster **Anmeldeinformationen eingeben** eingeben. Wenn ihr System CIM-aktiviert ist, muss sie den voll gekennzeichneten Domänenbenutzernamen bzw. das -kennwort eingeben.
8. Im Fenster **Zusammenfassung** bestätigt sie entweder ihre Auswahl oder wählt **Zurück**, um Änderungen vorzunehmen.

Der von ihr bestimmte Server beginnt mit dem Neustart, sobald sie **Fertig stellen** ausgewählt hat.

Sabine könnte andererseits beschließen, ein Gerät in ihrer Gruppe einzuschalten, indem Sie **Gerät hochfahren** als **Task-Typ** im Assistent **Task-Erstellung** wählt. Sie könnte den Task auch so planen, dass er zu einer festgelegten Zeit und nicht sofort ausgeführt wird.

## Andere im IT Assistent verfügbare Tasks

Andere im IT Assistent verfügbare Task-Typen umfassen:

### Allgemeine Befehlszeile

Die Auswahl von **Allgemeine Befehlszeile** im Pull-Down-Menü ermöglicht Ihnen, Befehle innerhalb des Netzwerks auszuführen. **Remote-Server Administrator-Befehlszeile** - Ermöglicht die Ausführung von Befehlszeilenoberflächen (CLI) -Befehlen des Server Administrator im Remote-Zugriff.

Eine vollständige Liste der von IT Assistent akzeptierten Argumente finden Sie in der Online-Hilfe.

### Softwareaktualisierung

Die Auswahl von **Serversoftware-Upgrade** ermöglicht Ihnen, das Software-Upgrade-Verfahren auf Ihren verwalteten Systemen, einschließlich der Festlegung getrennter Zeitpläne für jede Komponente des Upgrade, ganz an die eigenen Bedürfnisse anzupassen.

Eine vollständige Erklärung aller Tasks und ihrer Funktionen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.

### IPMI -Befehlszeile

Die Auswahl von **IPMI -Befehlszeile** aus dem Pulldown-Menü ermöglicht Ihnen, IPMI-Befehle auszuführen.

Zusätzliche Informationen finden Sie in der Online-Hilfe.

### Befehlszeile für Remote-Client-Instrumentation

Die Auswahl von **Remote-Instrumentationsbefehlszeile** ermöglicht Ihnen Client-Instrumentationsbefehle im Remote-Zugriff auszuführen.

Zusätzliche Informationen finden Sie in der Online-Hilfe.


### Server Administrator-Softwarebereitstellung


Die Auswahl von **Softwarebereitstellung** unter dem Parent-Knoten **Task** ermöglicht Ihnen, den Dell-Agenten auf verschiedenen Systemen bereitzustellen.

Zusätzliche Informationen finden Sie unter "[Server-Softwarebereitstellung verwenden](#)".

### Gerät herunterfahren (bandintern)

Die Auswahl von **Gerät herunterfahren (bandintern)** ermöglicht Ihnen, den Herunterfahrensvorgang zu bestimmen, den Sie ausführen möchten.

 **ANMERKUNG:** Dieser Task erfordert, dass CIM- oder SNMP-Ermittlung aktiviert oder Server Administrator auf dem verwalteten Knoten installiert ist.

 **ANMERKUNG:** Der Task zum Herunterfahren wird nicht für Geräte unterstützt, die ausschließlich anhand von IPMI ermittelt wurden.

## Gerät aktivieren (über WakeOnLAN)


Die Auswahl von **Gerät aktivieren (über WakeOnLAN)** ermöglicht Ihnen, die Schnittstellenummer des Geräts festzulegen, das Sie aktivieren möchten. IT Assistant verwendet die MAC-Adressen und Subnetzmasken, die für das Gerät ermittelt wurden, zur Aktivierung dieses Geräts. Wenn das Gerät für NIC-Teaming konfiguriert wurde, wird nur ein MAC vom Betriebssystem angekündigt. Wake-on-LAN (WOL) funktioniert nur, wenn es für alle NICs in diesem Team aktiviert wurde. Damit ein WOL-Paket sein beabsichtigtes Ziel erreicht, muss auf den Zwischen-Routern Directed Broadcasting (auch als Subnetz-Broadcasting bezeichnet) aktiviert sein. Directed Broadcasting ist meistens auf den Routern deaktiviert. Deshalb ist es notwendig, diese Funktion auf dem Router zur Aktivierung zu konfigurieren.

**ANMERKUNG:** Aktivieren Sie in den NIC-Einstellungen und dem System-BIOS die WOL-Eigenschaft.


## Stromsteuerungsgerät (über ASF)


Die Wahl von **Stromsteuerungsgerät (über ASF)** ermöglicht Ihnen, auf den Geräten, die mit dem Warnstandardformat (ASF) 2.0 konform sind, Remote-Stromsteuerungsvorgänge auszuführen.

**ANMERKUNG:** Anleitungen zu ASF-Konfiguration und Setup finden Sie in der Systemdokumentation.

 **ANMERKUNG:** IT Assistant verwendet den bandinternen Broadcom-Windows Management Instrumentation-Anbieter (WMI), um zu überprüfen, ob ein Gerät ASF-Fähigkeiten aufweist.


IT Assistant verwendet den bandinternen Broadcom-WMI-Anbieter auch, um festzustellen, ob ein Gerät für systementfernte sichere RMCP-Vorgänge (Remote Management Control Pakets) aktiviert ist, und ob die Administratorfunktion über ausreichende Berechtigungen verfügen, um Stromsteuerungsvorgänge auszuführen.

 **ANMERKUNG:** Sie können die Stromsteuerungsvorgänge über das Broadcom-ASF-Konfigurationsdienstprogramm konfigurieren.

 **ANMERKUNG:** Stellen Sie sicher, dass die Optionen **ASF aktiviert**, **Remote-Verwaltung** und **Sichere Verwaltung (ASF 2.0)** im Broadcom-ASF-Konfigurationsdienstprogramm aktiviert sind. Stellen Sie außerdem sicher, dass der Authentifizierungsschlüssel und der KG-Schlüssel im korrekten Format (Hex oder ASCII) eingegeben werden.

Der WMI-Anbieter ist als Teil der Broadcom-ASF-Verwaltungssuite verfügbar (auf Dells Support-Website unter [support.dell.com](http://support.dell.com)) verfügbar und muss auf dem Remote-Client-Gerät installiert werden.

Sie können die Geräte, die als aktiviert erkannt werden, im Geräteauswahl-Fenster des ASF-Stromsteuerungs-Assistenten auswählen. Wenn der WMI-Anbieter nicht auf dem Remote-Gerät installiert oder nicht für sichere Remote-RMCP-Vorgänge aktiviert ist, oder wenn die Administratorrechte nicht korrekt für die Stromsteuerungsvorgänge konfiguriert wurden, erscheint das Gerät in IT Assistant als deaktiviert.

 **ANMERKUNG:** Sie können die deaktivierten Geräte auswählen, wenn Sie die Option **Alle aktivieren** auswählen.

Wenn die Einstellungen verändert werden, ermitteln Sie das Gerät neu, um IT Assistant zu ermöglichen, die aktualisierte Konfiguration zum Aktivieren/Deaktivieren der Client-Geräte im Assistenten zu verwenden.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Sichere Dell OpenManage™ IT Assistant-Installation gewährleisten

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [TCP/IP-Paket-Anschlussicherheit](#)
- [Verwaltete Desktops, Laptops und Workstations sichern](#)
- [Verwaltete Serversysteme sichern](#)
- [IT Assistant hinter einer Firewall ausführen](#)
- [Erweiterte Sicherheit für IT Assistant-Zugriff einrichten](#)
- [Anschlüsse für IT Assistant und andere unterstützte Dell OpenManage-Anwendungen sichern](#)
- [Einmalige Anmeldung](#)
- [Funktionsbasierter Zugriff - Sicherheitsverwaltung](#)
- [Benutzerberechtigungen zuweisen](#)
- [Gastkonten und anonyme Konten deaktivieren](#)


Dieser Abschnitt bespricht mehrere spezifische Themen, die zur Umsetzung einer sichereren Dell OpenManage IT Assistant-Installation nützlich sind. IT Assistant setzt HTTPS für sichere Kommunikationen ein und das Active Directory® von Microsoft® für den funktionsbasierten Zugriff.

Ausführliche Informationen zur Sicherheit in der gesamten Dell OpenManage-Plattform, einschließlich IT Assistant, finden Sie im *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

---

### TCP/IP-Paket-Anschlussicherheit

Ein TCP/IP-Paket sendet eine Anfrage an ein Zielsystem. Eine Schnittstellennummer, die mit einer bestimmten Anwendung verbunden ist, ist innerhalb dieses Pakets verschlüsselt. Der Zugriff auf IT Assistant erfolgt durch Angabe von `https://<Host-Name>:<Schnittstellennummer>`. Die Verwendung von https erfordert, dass die eingesetzte Anwendung die Daten gemäß der SSL-Spezifikation (Sichere Sockelschicht) verschlüsseln, sodass vertrauliche Informationen wie Kennwörter nicht von jemandem anders, der Pakete im Netzwerk beobachtet, empfangen und gelesen werden können. Benutzer werden dann über die IT Assistant-Anmeldeseite authentifiziert, und ihre Anmeldeinformationen werden anhand der im Active Directory oder dem lokalen Betriebssystem zugewiesenen Funktion überprüft. Informationen zu den drei von IT Assistant unterstützten Funktionen finden Sie unter "[Funktionsbasierter Zugriff - Sicherheitsverwaltung](#)".

 **ANMERKUNG:** Die IT Assistant-Benutzeroberfläche kommuniziert mit der IT-Dienststufe über Schnittstelle 2607.

---


### Verwaltete Desktops, Laptops und Workstations sichern

#### Betriebssystem des verwalteten Systems sichern

Der erste Schritt bei der Einrichtung einer sicheren Netzwerkumgebung besteht darin, sicherzustellen, dass das aktuellste Service-Pack und/oder alle weiteren sicherheitsrelevanten Sicherheitsaktualisierungen für alle Betriebssysteme der verwalteten Systeme installiert sind. Zur Vereinfachung dieses Verfahrens hat Microsoft Softwareaktualisierungsdienste eingeführt. Weitere Details finden Sie auf der [Microsoft-Website](#). Führen Sie ähnliche Aktualisierungen auch für andere Betriebssysteme der verwalteten Systeme aus.

#### Sitzungszeitlimit

Eine IT Assistant-UI-Sitzung kann so konfiguriert werden, dass das Zeitlimit nach einer festgelegten Periode der Untätigkeit erreicht wird. Um das Sitzungszeitlimitintervall zu konfigurieren, klicken Sie auf der oberen IT Assistant-Navigationsleiste auf **Einstellungen** und wählen **Web Server-Eigenschaften**. Sie können das Sitzungszeitlimit entweder ganz deaktivieren oder bis zu 30 Minuten Untätigkeit zulassen.

 **ANMERKUNG:** Wenn der Datenübertragungskanal zwischen der IT Assistant-Benutzeroberfläche und dem Web-Server aktiv ist aufgrund asynchroner Aktualisierungen wie z. B. Leistungsüberwachungs-Tasks, Geräteermittlung, Statusabfragen usw., wird für die Benutzersitzung selbst dann keine Zeitüberschreitung eintreten, wenn Sitzungszeitlimit aktiviert ist.

#### Die Protokolle ASF und SNMP

Eine abschließende Sicherheitserwägung, eingeführt mit den Dell™ OptiPlex™ GX260-Systemen, ist die Unterstützung des Warnstandardformats (ASF) für integrierte Netzwerkschnittstellen-Controller (NIC). ASF gibt Plattformereignis-Traps (PET) dem Funktionszustand und den Sicherheitsrisiken eines Systems gemäß aus. Da diese Traps vom SNMP-Protokoll unterstützt werden, muss der NIC des verwalteten Systems mit einer IP-Adresse und einer Community-

Zeichenkette der Verwaltungsstation, auf der IT Assistant ausgeführt wird, konfiguriert werden.

Zusammenfassend sollten Systemadministratoren die folgenden empfohlenen Verfahren genau befolgen, um Desktops, Laptops und Workstations mithilfe der zuvor beschriebenen Sicherheitsmaßnahmen erfolgreich und sicher zu verwalten:

- 1 Stellen Sie sicher, dass das Betriebssystem mit den neuesten Sicherheitspatches aktualisiert wurde.
- 1 Deaktivieren Sie bei ASF-fähigen Desktops entweder ASF oder implementieren Sie schwer zu erratende SNMP-Community-Namen.

---

## Verwaltete Serversysteme sichern

### Betriebssystem des verwalteten Systems sichern


Wie bei Desktops und Workstations besteht der erste Schritt bei der Sicherung eines Servers darin, dass die neuesten Service-Packs sowie die entsprechend wichtigen Hotfixes installiert wurden. Die im vorhergehenden Abschnitt beschriebenen Softwareaktualisierungsdienste von Microsoft können auch für Microsoft Windows® 2000- und Windows Server® 2003-Server eingesetzt werden. Ähnliche Dienste sollten auch für Red Hat® Linux und SUSE® Linux Enterprise Server in Betracht gezogen werden.


### Das sicherste Protokoll für verwaltete Systemserver auswählen

Dell OpenManage Server Administrator, die aktuelle Dell Server-Instrumentationssoftware, verwendet die SNMP- und CIM-Protokolle, die während der benutzerdefinierten Installation konfiguriert werden können.

### CIM-Überwachung, DCOM- und Windows-Authentifizierung

Das CIM-Protokoll, das die DCOM-Sicherheit einsetzt, wendet die Windows Challenge/Response-Authentifizierung (Benutzername/Kennwort) an. Des Weiteren wird die Kommunikation mit dem verwalteten System über Domäne/Benutzername/Kennwort-Konten hergestellt, die in allen konfigurierten IT Assistant-Ermittlungsbereichen angegeben werden. Das Format für diese Konten ist **<Domänenname>\<Benutzername>** oder **lokaler Host\<Benutzername>**.


 **ANMERKUNG:** Die WMI-Sicherheit kann mithilfe von Dienstprogrammen wie z. B. **dcomcnfg.exe**, **wmimgmt.msc** und **wbemctl** geändert werden. Auf Grund möglicher unerwünschter Nebenwirkungen werden Änderungen mithilfe dieser Methoden nicht empfohlen. Weitere Informationen finden Sie auf der Microsoft Website.

 **ANMERKUNG:** Selbst in Umgebungen, in denen zur Überwachung ausschließlich CIM verwendet wird, ist SNMP normalerweise aktiviert, da der Server Administrator Fehlerbenachrichtigungen nur über SNMP-Traps sendet.

### Sicherheit und das SNMP-Protokoll

Über das SNMP-Protokoll stehen verschiedene Maßnahmen zur Erhöhung der Sicherheitsumgebung zur Verfügung. Obwohl sich die folgenden Beispiele auf Microsoft Windows-Betriebssysteme beziehen, können für die Betriebssysteme Red Hat Enterprise Linux und SUSE Linux Enterprise Server ähnliche Schritte ausgeführt werden. Bei installiertem SNMP ist der Community-Name standardmäßig auf **public** eingestellt. Diese Zeichenkette sollte wie ein Kennwort behandelt werden und unterliegt ähnlichen Regeln, die bei der Wahl der Zeichenkette berücksichtigt werden sollten - eine Zeichenkette geeigneter Länge, schwer zu erraten und möglichst aus Buchstaben und Ziffern bestehend. Bei Windows Betriebssystemen kann der SNMP-Community-Name im Dialogfeld **Eigenschaft** des SNMP-Dienstes über das Register **Sicherheit** konfiguriert werden.

Als weitere Vorsichtsmaßnahme sollte SNMP auch auf **Nur-Lesen** eingestellt werden, um unbefugte Konfiguration und Steuermaßnahmen zu vermeiden. Diese Einstellung kann über den Eintrag **snmpsets=no option** während der Installation des Server Administrators ausgeführt werden. Es wäre weiterhin möglich, diese Änderungen über die Benutzeroberfläche oder die Befehlszeilenschnittstelle (CLI) des Server Administrators vorzunehmen. Der SNMP-Dienst kann ebenso konfiguriert werden, dass Anfragen nur von einem bestimmten Server (in diesem Fall vom System, auf dem IT Assistant ausgeführt wird) bearbeitet werden. Diese Einstellung kann ebenfalls im zuvor erwähnten Windows-Register **Sicherheit** konfiguriert werden, indem Sie die Optionsschaltfläche mit der Bezeichnung **SNMP-Pakete von diesen Hosts annehmen** auswählen und dann auf **Hinzufügen** klicken, um die IP-Adresse bzw. den Namen des Systems einzugeben, auf dem IT Assistant ausgeführt wird. Weitere Details finden Sie in Ihrer Dokumentation zum Betriebssystem.

 **ANMERKUNG:** Um die die sachgemäße Konfiguration aller Systeme sicherzustellen, wird empfohlen, Hilfsprogramme wie z. B. Group Policies in Active Directory zu verwenden, um diese SNMP-Einstellungen durchzusetzen.

Als abschließender Schritt zur Sicherheit ist der Server Administrator so zu konfigurieren, dass der Zugriff auf Benutzer- und möglicherweise auch Power-Benutzerkonten verweigert wird und somit der Zugriff nur auf die Administratorkonten beschränkt wird. Diese Konfiguration kann über die obere Navigationsleiste im Server Administrator erfolgen, indem Sie **Einstellung** auswählen und die Auswahl der **Benutzerzugriffsfelder** aufheben.

**ANMERKUNG:** Der Benutzerzugriff kann auch über den CLI-Befehl `omconfig preferences useraccess enable= admin` des Server Administrator eingeschränkt werden.

Weitere Informationen finden Sie im *Benutzerhandbuch zur Dell OpenManage Server Administrator-Befehlszeilenoberfläche* auf Dells Support-Website unter [support.dell.com](http://support.dell.com) oder auf der Dokumentations-CD.

Zusammenfassend sollten Systemadministratoren die folgenden empfohlenen Verfahren genau befolgen, um Server mithilfe der zuvor beschriebenen Sicherheitsmaßnahmen erfolgreich und sicher zu verwalten:

- 1 Stellen Sie sicher, dass das Betriebssystem mit den neuesten Sicherheitspatches aktualisiert wurde.
- 1 Führen Sie schwer zu erratende SNMP-Community-Namen ein.
- 1 Konfigurieren Sie SNMP für den **Nur-Lese**-Zugriff, um nur den Server Administrator Konfigurationen, Aktualisierungen und Steuerung des Netzstroms durchführen zu lassen.
- 1 Konfigurieren Sie SNMP so, dass Anfragen nur von der IP-Adresse des Systems angenommen werden, auf dem IT Assistant ausgeführt wird.
- 1 Verwenden Sie Hilfsprogramme wie z. B. Group Policies in Active Directory, um die SNMP-Einstellungen für alle zu verwaltenden Server zu erzwingen.
- 1 Konfigurieren Sie Server Administrator so, dass der Zugriff auf Benutzerebene verweigert wird.

## Datenbanksicherheit bei Einsatz des IT Assistant sicherstellen

Wenn bei der Installation von IT Assistant keine Microsoft SQL Serverdatenbank ermittelt wurde, wird eine Kopie von SQL Server 2005 Express installiert, das auf den Authentifizierungsmodus Vertrauenswürdig oder Nur Windows eingestellt wird. Andere Anwendungen, die zu einem früheren Zeitpunkt eventuell MSDE oder SQL-Server installiert haben, einschließlich älterer Versionen des IT Assistant, wählen häufig entweder den Authentifizierungsmodus bzw. SQL oder eine Mischung aus beiden, wodurch SQL-Server seine eigenen Benutzer-IDs und Kennwörter verwalten kann. Falls frühere Versionen von IT Assistant installiert sind, wurde das Supervisor-Kontokennwort entweder auf `nu11` oder `de11` gesetzt. Verringern Sie auf jeden Fall das Risiko eines Netzwerkeinbruchs, indem Sie mindestens diese Kennwörter nach den zuvor empfohlenen Verfahren in Zeichenketten ändern. Eine bessere Lösung wäre es, den Datenbank-Authentifizierungsmodus zu Vertrauenswürdig oder Nur Windows zu ändern.

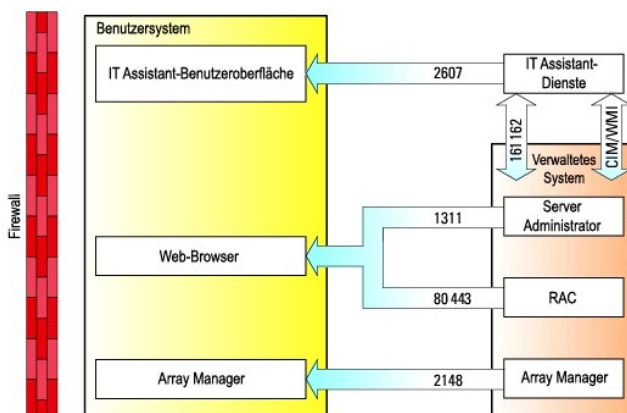
## IT Assistant hinter einer Firewall ausführen

[Abbildung 10-1](#) zeigt eine typische Installation, bei der sich sowohl IT Assistant als auch die verwalteten Systeme hinter einer Firewall befinden. Auf bestimmten Schnittstellen blockiert die Firewall den Durchgang von Verkehr zwischen dem geschützten Netzwerk und der Außenwelt. Gleichzeitig erlaubt sie trotzdem einem Administrator sowohl mit dem IT Assistant als auch mit dem verwalteten System frei zu kommunizieren.

Zu den typischen Sicherheitseinrichtungen für das System, auf dem IT Assistant in einer Umgebung hinter einer Firewall ausgeführt wird, zählen u. A.:

- 1 Verwendung vertrauenswürdiger Konten anstelle von benannten oder gemischten Konten für die Datenbank.
- 1 Begrenzung von Benutzeroberflächenverbindungen zu einem bekannten System.

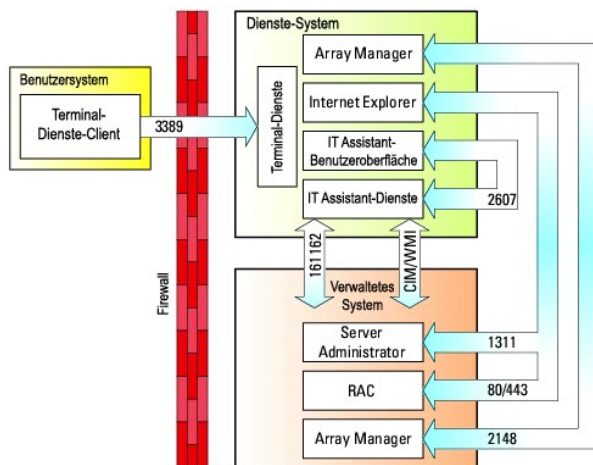
Abbildung 10-1. Typische Installation hinter einer Firewall



## Erweiterte Sicherheit für IT Assistant-Zugriff einrichten

Bisher wurde das Thema Sicherheit in diesem Abschnitt hinsichtlich der vorhandenen TCP/IP-Verbindung zwischen IT Assistant und dem verwalteten System behandelt. Zusätzlich zu diesen Sicherheitsvorsichtsmaßnahmen können die Microsoft-Terminaldienste, die nicht aufgezeichnete Remote-Verbindungen nur durch Benutzer mit Administratorkonten (Administrationsmodus) zulassen, auch zum Einschränken von Benutzeroberflächen-Verbindungen zu einem System verwendet werden, auf dem die IT Assistant-Benutzeroberfläche und -Dienste ausgeführt werden. Ein Beispiel eines Netzwerks, das die Terminaldienste nutzt, ist in [Abbildung 10-2](#) dargestellt.

Abbildung 10-2. Verwendung von Terminaldiensten für zusätzliche Sicherheit



In [Abbildung 10-2](#) kann ein Benutzer eine Verbindung zur IT Assistant-Verwaltungsstation über einen lokal installierten Terminaldienste-Client oder über eine Windows XP-Remote-Desktopverbindung herstellen. Für diese Verbindung ist gültige Domäne/Benutzer-ID/Kennwort erforderlich. Weitere Informationen finden Sie auf der Website von Microsoft.

Die zusätzliche Sicherheitsstufe wird erlangt, indem auf allen verwalteten Systemen Einschränkungen so eingerichtet werden, dass SNMP-Datenverkehr nur von der IP-Adresse des Systems aus akzeptiert wird, das die IT Assistant-Benutzeroberfläche ([UI], die Netzwerkverwaltungsstation) ausführt. Terminaldienste und Remote-Desktop-Sitzungen emulieren Verkehr, der direkt von der Netzwerkverwaltungsstation kommt, daher wird der Zugriff auf den IT Assistant nur für Terminaldienste-Clients oder für einen lokalen Benutzer der Netzwerkverwaltungsstation erlaubt. Jede andere Verbindung, wie z. B. eine andere Remote-Installation der IT Assistant-Benutzeroberfläche, könnte keine effektive Verbindung mit korrekt konfigurierten verwalteten Systemen im Netzwerk herstellen, da Verkehr abgelehnt würde, der von einem anderen System als der Netzwerkverwaltungsstation stammt.

- ANMERKUNG:** Terminaldienste sind optionale Komponenten von Microsoft Windows 2000 und Microsoft Windows Server 2003, die entweder im Admin-Modus oder Anwendungsmodus installiert werden können.
- ANMERKUNG:** Wenn die Terminaldienste im administrativen Modus installiert werden, können sich bis zu zwei Benutzer anmelden, vorausgesetzt sie sind Mitglieder der Administratorengruppe. Wenn die Terminaldienste im Anwendungsmodus installiert werden, können sich Nicht-Administratorengruppen anmelden und es werden mehr als zwei Sitzungen unterstützt. Die Installation im Anwendungsmodus enthält jedoch zusätzliche Lizenzierungsanforderungen. Wenn IT Assistant auf einem System installiert wird, auf dem die Terminaldienste im Anwendungsmodus ausgeführt werden, muss die Installation lokal erfolgen und nicht über eine Terminalsitzung.

## Anschlüsse für IT Assistant und andere unterstützte Dell OpenManage-Anwendungen sichern

Die Sicherung von Schnittstelle 2607 der IT Assistant-Dienststufe sowie der Schnittstellen 1311, 623, 161 und 162 des verwalteten Systems kann über IP-Sicherheit (IPSec) erfolgen. Die derzeit auf dem Server ausgeführten Anschlüsse können über den Befehl `netstat -an` von einer Befehlsaufforderung aus aufgelistet werden, um den Status aller Anschlüsse im System anzuzeigen. Die Ergebnisse dieses Befehls sollten zeigen, dass die IT Assistant-Verwaltungsstation nur eine Verbindung über Anschluss 2607 von dem Server akzeptiert, auf dem sich die IT Assistant-UI befindet (eine über Terminaldienste hergestellte Verbindung). In gleicher Weise sollten die verwalteten Systeme so konfiguriert sein, dass sie Verbindungen von der verwalteten Station über die Anschlüsse 1311, 161 und 162 zuzulassen.

## Einmalige Anmeldung

Die Option Einmalige Anmeldung bei Windows-Systemen ermöglicht es allen angemeldeten Benutzern die Anmeldeseite zu umgehen und durch Klicken auf das **IT Assistant**-Symbol auf dem Desktop direkt auf IT Assistant zuzugreifen. Das Desktop-Symbol erfragt bei der Registrierung, ob die Option Automatische Anmeldung mit aktuellem Benutzernamen und aktuellem Kennwort in Internet Explorer aktiviert ist. Wenn diese Option aktiviert ist, wird die einfache Anmeldung ausgeführt; andernfalls wird die normale Anmeldeseite angezeigt. Die NTLM (NT-LAN-Manager) -Authentifizierung im Windows-Netzwerk darf nicht deaktiviert werden.

Zur Aktivierung der automatischen Anmeldung mit aktuellem Benutzernamen und aktuellem Kennwort führen Sie folgende Schritte in Internet Explorer aus.

1. Klicken Sie auf **Internetoptionen** im Menü **Extras**.
2. Klicken Sie auf das Register **Sicherheit**.
3. Wählen Sie die Sicherheitszone aus, die auf das IT Assistant-System zutrifft, d. h. die **Vertrauenswürdige Site**, und klicken Sie auf **Benutzerdefinierte Stufe**.
4. Wählen Sie im Dialogfeld **Sicherheitseinstellung** unter **Benutzerauthentifizierung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und aktuellem Kennwort**.
5. Klicken Sie zweimal auf **OK** und starten Sie Internet Explorer neu.

Zum Zugriff auf ein lokales System müssen Sie ein Konto bei diesem System haben und die korrekten Berechtigungen (Benutzer, Hauptbenutzer oder Administrator). Andere Benutzer werden durch Abgleichen mit dem Microsoft-Active Directory authentifiziert.

Damit der IT Assistant mit der einmaligen Anmeldeauthentifizierung über das Microsoft-Active Directory gestartet werden kann, müssen die folgenden Parameter eingestellt werden:

```
authType=ntlm&application=[ita]
```

Beispiel:

```
https://localhost:2607/?authType=ntlm&application=ita
```

Damit der IT Assistant mit der einmaligen Anmeldeauthentifizierung über die lokalen Systembenutzerkonten gestartet werden kann, müssen die folgenden Parameter eingestellt werden:

```
authType=ntlm&application=[ita]&locallogin=true
```

Beispiel:

```
https://localhost:2607/?authType=ntlm&application=ita&locallogin=true
```

---

## Funktionsbasierter Zugriff - Sicherheitsverwaltung

IT Assistant bietet Sicherheit durch funktionsbasierte Access Control (RBAC), Authentifizierung und Verschlüsselung.

### Funktionsbasierte Access Control

RBAC erreicht Sicherheit durch Festlegung der Vorgänge, die von Personen in besonderen Funktionen ausgeführt werden können. Jedem Benutzer werden eine oder mehrere Funktionen zugeteilt, und jeder Funktion sind eine oder mehrere Benutzerberechtigungen zugewiesen, die für Benutzer in dieser Funktion zugelassen sind. Mit RBAC entspricht Sicherheitsverwaltung genau der Organisationsstruktur.

### Benutzerberechtigungen



IT Assistant gewährt unterschiedliche Zugriffsberechtigungen, die auf den zugewiesenen Gruppenberechtigungen des Benutzers basieren. Die drei Benutzerebenen sind: Benutzer, Hauptbenutzer und Administrator.

Benutzer haben Nur-Lesen-Zugang zu allen IT Assistant-Informationen.

Hauptbenutzer können Tasks zur unmittelbaren Ausführung erstellen. Sie können keine Ermittlungskonfigurationseinstellungen modifizieren, Warnungsverwaltungseinstellungen modifizieren oder Tasks planen bzw. löschen.

Administratoren können alle IT Assistant-Tasks und Funktionen ausführen.

## Microsoft Windows-Authentifizierung

Für unterstützte Windows-Betriebssysteme basiert die IT Assistant-Authentifizierung auf dem Benutzerauthentifizierungssystem des Betriebssystems unter Verwendung von Windows NT® LAN-Manager (NTLM) -Modulen zur Authentifizierung. Dieses grundlegende Authentifizierungssystem ermöglicht die Integration der IT Assistant-Sicherheit in ein Gesamtsicherheitsschema für Ihr Netzwerk.

---


## Benutzerberechtigungen zuweisen

Es ist nicht notwendig, IT Assistant-Benutzern vor der Installation des IT Assistant Benutzerberechtigungen zuzuweisen.


Die folgenden Verfahren bieten schrittweise Anleitungen zur Erstellung von IT Assistant-Benutzern und zur Zuweisung von Benutzerberechtigungen für Windows-Betriebssysteme:

 **HINWEIS:** Gastkonten sollten für unterstützte Microsoft Windows-Betriebssysteme deaktiviert sein, um Ihre kritischen Systemkomponenten vor Zugriff zu schützen. Anleitungen hierzu erhalten Sie unter "[Gastkonten und anonyme Konten deaktivieren](#)".

## IT Assistant-Benutzer für unterstützte Windows-Betriebssysteme erstellen


 **ANMERKUNG:** Sie müssen mit Admin-Berechtigungen angemeldet sein, um diese Verfahren auszuführen.

### Benutzer erstellen und Benutzerberechtigungen für unterstützte Windows 2000- und Windows Server® 2003-Betriebssysteme zuweisen

 **ANMERKUNG:** Bei Fragen zur Erstellung von Benutzern und zur Zuweisung von Benutzergruppenberechtigungen oder um ausführlichere Anleitungen zu erhalten, lesen Sie die Dokumentation zum Betriebssystem.

1. Klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und zeigen Sie auf **Verwalten**.
2. In der Konsolenstruktur erweitern Sie **Lokale Benutzer und Gruppen** und klicken Sie dann auf **Benutzer**.
3. Klicken Sie auf **Maßnahme** und dann auf **Neuer Benutzer**.
4. Geben Sie die zutreffenden Informationen im Dialogfeld ein, markieren Sie die entsprechenden Kontrollkästchen oder heben Sie die Markierungen auf und klicken Sie dann auf **Erstellen**.

Sie müssen jedem Benutzerkonto, das auf IT Assistant zugreifen kann, ein Kennwort zuweisen, um den Zugriff auf Ihre kritischen Systemkomponenten zu schützen. Außerdem können sich Benutzer, die kein zugewiesenes Kennwort besitzen, nicht bei IT Assistant auf einem System anmelden, auf dem Windows Server 2003 ausgeführt wird. Der Grund hierfür sind Einschränkungen des Betriebssystems.


 **ANMERKUNG:** Verwenden Sie in Kennwörtern keine doppelten oder einzelnen Anführungszeichen.


5. Klicken Sie in der Konsolenstruktur unter **Lokale Benutzer und Gruppen** auf **Gruppen**.
6. Klicken Sie auf die Gruppe, zu der Sie den neuen Benutzer hinzufügen wollen: **Benutzer**, **Hauptbenutzer** oder **Administratoren**.
7. Klicken Sie auf **Maßnahme** und dann auf **Eigenschaften**.
8. Klicken Sie auf **Hinzufügen**.

9. Geben Sie den Benutzernamen, den Sie hinzufügen, ein und klicken Sie zur Bestätigung auf **Namen überprüfen**.
10. Klicken Sie auf **OK**.

Neue Benutzer können sich bei IT Assistant mit den Benutzerberechtigungen ihrer zugewiesenen Gruppe anmelden.


## Benutzer zu einer Domäne hinzufügen

 **ANMERKUNG:** Bei Fragen zur Erstellung von Benutzern und zur Zuweisung von Benutzergruppenberechtigungen oder um ausführlichere Anleitungen zu erhalten, lesen Sie die Dokumentation zum Betriebssystem.

 **ANMERKUNG:** Active Directory muss auf Ihrem System installiert sein, damit die folgenden Verfahren ausgeführt werden können.

1. Klicken Sie auf die Schaltfläche **Start** und zeigen Sie dann auf **Systemsteuerung**→ **Verwaltung**→ **Active Directory-Benutzer und -Computer**.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Benutzer** oder klicken Sie mit der rechten Maustaste auf den Container, zu dem Sie den neuen Benutzer hinzufügen wollen, und zeigen Sie dann auf **Neu**→ **Benutzer**.
3. Geben Sie die entsprechenden Informationen zum Benutzernamen im Dialogfeld ein und klicken Sie dann auf **Weiter**.

Es ist erforderlich, jedem Benutzerkonto, das auf IT Assistant zugreifen kann, ein Kennwort zuzuweisen, um den Zugriff auf Ihre kritischen Systemkomponenten zu schützen. Zusätzlich können Benutzer, die kein zugewiesenes Kennwort haben, sich nicht beim IT Assistant anmelden, wenn dieser auf einem System mit Windows Server 2003 ausgeführt wird (aufgrund von Betriebssystemeinschränkungen).


 **ANMERKUNG:** Verwenden Sie in Kennwörtern keine doppelten oder einzelnen Anführungszeichen.

4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
5. Klicken Sie mit einem Doppelklick auf das Symbol, das den Benutzer darstellt, den Sie gerade erstellt haben.
6. Klicken Sie auf das Register **Mitglied von**.
7. Klicken Sie auf **Hinzufügen**.
8. Wählen Sie die zutreffende Gruppe und klicken Sie auf **Hinzufügen**.
9. Klicken Sie auf **OK** und dann noch einmal auf **OK**.

Neue Benutzer können sich bei IT Assistant mit den Benutzerberechtigungen ihrer zugewiesenen Gruppe und Domäne anmelden.

---

## Gastkonten und anonyme Konten deaktivieren

 **ANMERKUNG:** Sie müssen mit Administratorberechtigungen angemeldet sein, um dieses Verfahren auszuführen.

1. Falls Windows Server 2003 auf dem System ausgeführt wird, klicken Sie auf die Schaltfläche **Start**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**. Falls Windows 2000 auf dem System ausgeführt wird, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und zeigen Sie auf **Verwalten**.
2. In der Konsolenstruktur erweitern Sie **Lokale Benutzer und Gruppen** und klicken Sie dann auf **Benutzer**.
3. Klicken Sie auf das Benutzerkonto **Gast** oder **IUSR\_Systemname**.
4. Klicken Sie auf **Maßnahme** und zeigen Sie auf **Eigenschaften**.
5. Wählen Sie **Konto ist deaktiviert** und klicken Sie auf **OK**.

Ein roter Kreis mit einem X wird über dem Benutzernamen eingeblendet. Das Konto ist deaktiviert.

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)


## Softwareaktualisierungen

### Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Softwareaktualisierungen im IT Assistant verwenden](#)
- [Server-Softwarebereitstellung verwenden](#)

Die Softwareaktualisierungsfunktion von Dell OpenManage™ IT Assistant Version 8.0 umfasst:

1. **Repositories:** Ein Repository ist ein Container für Dell Update Packages und Systemaktualisierungssätze. Update Packages sind verfügbar über die CDs *Dell™ PowerEdge™ Installation and Server Management* und *Dell™ PowerEdge™ Server Update Utility* oder auf der Dell-Website unter [ftp.dell.com](http://ftp.dell.com). Die Repositories werden als hierarchische Strukturansicht angezeigt, wobei **Softwareaktualisierungs-Repository** der übergeordnete und **IT Assistant-Repository** der untergeordnete Knoten ist.
1. **Benutzerdefinierte Aktualisierungssätze:** Sie können benutzerdefinierte Systemaktualisierungssätze oder Bündel erstellen. Diese benutzerdefinierten Aktualisierungssätze können anschließend zum Erstellen von Systemkonformitätsberichten und zum Ausführen der Aktualisierungen verwendet werden.

 **ANMERKUNG:** Sie können benutzerdefinierte Bündel nur von den Systembündeln erstellen, die in das IT Assistant-Repository importiert wurden.

1. **Digitalsignatur-Überprüfung:** IT Assistant überprüft die Authentizität und Integrität der Aktualisierungspakete und MSI-Dateien anhand von Digitalsignatur-Überprüfung.

IT Assistant bietet eine zentralisierte Softwareaktualisierungsfähigkeit. Sie können Dell Update Packages und Systemaktualisierungssätze in das IT Assistant-Repository laden und dann prüfen, ob alle Systeme im Unternehmen mit den Update Packages übereinstimmen. Ein Systemaktualisierungssatz ist ein logischer Satz von Paketen, die von Dell zugelassen sind und problemlos zusammenarbeiten. Dell Update Packages stehen auf Dells Support-Website unter [support.dell.com](http://support.dell.com) oder auf der CD *Dell PowerEdge Server Update Utility* zur Verfügung. Diese CD ist über den Abonnementdienst von Dell OpenManage erhältlich oder kann als ISO-Image von Dells Support-Website unter [support.dell.com](http://support.dell.com) heruntergeladen werden. Der Dell OpenManage-Abonnement-Dienst kann von [www.dell.com](http://www.dell.com) heruntergeladen werden.

Die CD *Dell PowerEdge Server Update Utility* enthält vierteljährliche Aktualisierung für die Dell Update Packages und Systemaktualisierungssätze (zertifizierte Paketsätze für spezifische PowerEdge-Plattformen).

Zur Verwendung der Dell Update Packages im IT Assistant, führen Sie folgende Schritte durch:

1. Legen Sie die CD *Dell PowerEdge Server Update Utility* in das CD-Laufwerk ein.
2. Navigieren Sie zu **Verwalten**→ **Softwareaktualisierungen**.
3. Klicken Sie mit der rechten Maustaste auf den Stammknoten (**Softwareaktualisierungs-Repositories**) und wählen Sie **Repository öffnen (Aktualisierungs-CD)**... aus.
4. Navigieren Sie zur CD und suchen Sie das Repository-Verzeichnis.
5. Wählen Sie **catalog.xml** und klicken Sie auf **Öffnen**.  
Der Inhalt der CD *Dell PowerEdge Server Update Utility* wird auf der IT Assistant-Benutzeroberfläche angezeigt. Sie sind dann in der Lage, Pakete zu importieren, sowie Konformitätsüberprüfungen und Softwareaktualisierungen auszuführen.

---

## Softwareaktualisierungen im IT Assistant verwenden

Lassen Sie uns ansehen, wie Sabine diese Funktion in ihrem Unternehmen verwenden könnte.

Sabine hat ein Update Package von der Dell Support-Website unter [support.dell.com](http://support.dell.com) heruntergeladen. Sie weiß, dass einige ihrer Systeme das Firmware-Upgrade benötigen, das im Update Package enthalten ist, doch sie möchte feststellen, welche diese sind, ohne alle 50 Server manuell überprüfen zu müssen. Sie kann IT Assistant verwenden, um dies schnell herauszufinden.

So würde sie herausfinden, wie viele Systeme aktualisiert werden müssen:


1. Wählen Sie **Verwalten**→ **Softwareaktualisierungen** aus der Menüleiste aus.
2. Sie klickt im linken Navigationsfenster mit der rechten Maustaste auf **IT Assistant-Repository** und wählt **Hinzufügen**.

Sabine navigiert zu dem Standort auf ihrem System, wo sie das Update Package gespeichert hat. Wenn sie die Datei auswählt und auf **Öffnen** klickt, fügt IT Assistant das Update Package dem Fenster hinzu.

3. Durch Klicken des Namens des Update Packages im linken Fenster wird eine Zusammenfassung seines Inhalts im rechten Fenster gezeigt.
4. Sie klickt auf das Register **Übereinstimmung** und dann auf eine bestimmte Gerätegruppe (oder eine Abfrage), mit der das Paket abgeglichen werden soll.
5. Sie klickt auf **Vergleichen** zur Prüfung der Gerät, die sie in Abgleichung mit dem Inhalt des Update Package gewählt hat.

IT Assistant führt einen Vergleich durch und erstellt einen Übereinstimmungsreport, der eine graphische Darstellung der Unterschiede zeigt, vollständige Versionsinformationen zu den ausgewählten Geräten gibt, sowie andere Informationen, die bei der Identifizierung nicht übereinstimmender Systeme oder Geräte hilfreich sein können.


6. Wenn IT Assistant Server oder Geräte findet, die aktualisiert werden müssen, wählt Sabine aus, welche Geräte sie aktualisieren möchte, und klickt dann auf die Schaltfläche **Aktualisierung**. Diese Maßnahme startet den Task-Assistenten **Softwareaktualisierungen** automatisch.

 **ANMERKUNG:** Es ist nicht möglich, die Firmware auf dem System zu aktualisieren, auf dem IT Assistant ausgeführt wird. Um die Firmware auf diesem System zu aktualisieren, müssen die Softwareaktualisierungen von einem anderen System aus durchgeführt werden.

---

## Server-Softwarebereitstellung verwenden

IT Assistant bietet eine integrierte Methode zur Installation von Dell OpenManage Server Administrator auf unterstützten Dell-Systemen.

 **ANMERKUNG:** Auf dem System, von dem aus Sie die IT Assistant-Benutzeroberfläche ausführen, sollte die Java-Laufzeitumgebung (JRE) mindestens 256 MB freien Speicherplatzes für den JRE-Speicher (Heap-Speicher) aufweisen. Diese Speicheranforderung wird für IT Assistant empfohlen, um die MSI-Datei herunterzuladen, die den Dell-Agenten enthält. Die Größe der MSI-Datei befindet sich typischerweise im Bereich von 60 - 64 MB.

## Java-Laufzeitparameter in unterstützter Windows-Umgebung einstellen

1. Klicken Sie auf die **Start**-Schaltfläche. Zeigen Sie auf **Einstellungen** → **Systemsteuerung** → **Java**.
2. Im Register **Java** klicken Sie im Abschnitt **Einstellungen der Java Applet-Laufzeit** auf **Ansicht**.
3. Stellen Sie die Java-Laufzeitparameter auf **-Xmx256M** ein.

## Java-Laufzeitparameter in unterstützter Linux-Umgebung einstellen


1. Wechseln Sie zum Java-Basisverzeichnis. Der Standardpfad lautet `/usr/java/jre1.5.xxx/bin/`.
2. Führen Sie `./ControlPanel` aus.
3. Im Register **Java** klicken Sie im Abschnitt **Einstellungen der Java Applet-Laufzeit** auf **Ansicht**.
4. Stellen Sie die Java-Laufzeitparameter auf **-Xmx256M** ein.

## Dell-Agent auf einem verwalteten Remote-Knoten installieren

Wenn Sie mithilfe von IT Assistant ein Unternehmensnetzwerk verwalten, können Sie die neueste Version von Dell OpenManage Server Administrator auf verschiedenen Systemen in der Umgebung installieren. Es ist möglich, dass Server Administrator auf diesen Systemen zu einem früheren Zeitpunkt bereits installiert wurde.

Beschaffen Sie sich von einer der folgenden Quellen eine Server Administrator-MSI-Datei:


- 1 CD *Dell™ PowerEdge™ Installation and Server Management*

 **ANMERKUNG:** IT Assistant Version 8.0 unterstützt Server Administrator-Bereitstellung nur auf Microsoft® Windows®-Betriebssystemen.

- 1 Dells Support-Website unter [support.dell.com](http://support.dell.com) - FTP Download

Anhand der Task-Verwaltungsfunktion in IT Assistant können Sie einen Softwareagenten-Bereitstellungs-Task erstellen, um die Bereitstellung von Server Administrator auf verschiedenen Systemen im Netzwerk zu planen. Nachdem Server Administrator installiert wurde, wird ein neuer Status eingeblendet:

- 1 Nur wenn Sie unter **Erzwingung** eine Ermittlung, Bestandsaufnahme oder manuelle Statusabfrage durchführen.
- 1 Nach der nächsten geplanten Ermittlung, Bestandsaufnahme oder Statusabfrage.

-  **ANMERKUNG:** Die Protokoll-Konfigurationseinstellungen für die Bestandsaufnahme müssen während der anfänglichen Geräteerkennung für das Gerät bestimmt werden, und die entsprechenden Dienste müssen auf dem Gerät ausgeführt werden.

## Softwarebereitstellungs-Task erstellen


1. Wählen Sie **Verwalten** → **Tasks** aus der Menüleiste aus.
2. Unter dem Parent-Knoten **Task** klicken Sie mit der rechten Maustaste auf **Softwarebereitstellung** und wählen **Neuer Task...** aus.


Der **Neue Task-Assistent** wird eingeblendet.


3. Unter **Task-Erstellung** geben Sie einen beschreibenden Namen für den Task ein und wählen den Task **Server Administrator-Bereitstellung** aus.

Klicken Sie auf **Weiter**.

4. Unter **Task-Installationspezifikation** bestimmen Sie den **Installationsdateipfad**.

-  **ANMERKUNG:** Der Standardinstallationspfad auf der CD *Dell™ PowerEdge™ Installation and Server Management* ist `<CD>\srvadmin\windows\SystemManagement\SysMgmt.msi`.


-  **ANMERKUNG:** Stellen Sie sicher, dass Sie nur die **SysMgmt.msi**-Datei der Version 5.0 oder höher auswählen. Die **.msi**-Dateien früherer Versionen von Dell OpenManage werden von IT Assistant 8.0 nicht unterstützt. Sie können die Version von Server Administrator nachsehen, indem Sie mit der rechten Maustaste auf die Datei **SysMgmt.msi** klicken und **Eigenschaften** auswählen. Die Version von Server Administrator ist im Register **Zusammenfassung** angezeigt.

-  **ANMERKUNG:** Stellen Sie sicher, dass sich auf der Verwaltungsstation ausreichend freier Speicherplatz zum Erstellen des Tasks befindet (mindestens 65 MB). Dem verwalteten Knoten sollten etwa 130 MB freier Speicher in **%SYSTEMLAUFWERK%** oder auf dem Laufwerk zur Verfügung stehen, auf dem das Betriebssystem installiert ist.


-  **ANMERKUNG:** Diese Funktion unterstützt nur **ADDLOCAL**-Parameter. Weitere Informationen über diesen Parameter und die mit ihm zu verwendenden Argumente finden Sie im *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

Es wird empfohlen **Installer-Engine auf Zielknoten erweitern (falls erforderlich)** auszuwählen. Diese Option stellt sicher, dass die neueste Version von **msiexec** auf den verwalteten Systemen installiert ist.


Wenn Sie diese Option nicht auswählen und die verwalteten Systeme die erforderliche Version nicht aufweisen, wird eine Fehlermeldung eingeblendet.

-  **ANMERKUNG:** Diese Option schlägt fehl, wenn die erforderlichen Upgrade-Engine-Dateien (**.exe** und **.bat**) nicht in demselben Ordner wie das Systems Management-Installationsprogramm (**.msi**) gefunden werden. Wenn Sie diese Dateien gelöscht haben, wechseln Sie zu **ftp.dell.com** und laden sie in den **SystemsManagement**-Ordner herunter.

5. Unter **Geräteauswahl** wählen Sie die entsprechenden Systeme aus, auf denen Server Administrator bereitgestellt werden soll.

-  **ANMERKUNG:** IT Assistant führt zum Zeitpunkt der Task-Ausführung Voraussetzungsprüfungen aus. Ausführungsdetails können im Fenster **Task-Ausführungsdetails** angezeigt werden. Sollte die Task-Ausführung fehlschlagen, korrigieren Sie den Fehler (z. B. unzureichender Festplattenspeicherplatz) und führen den Task erneut aus. Weitere Informationen finden Sie in der *Dell OpenManage IT Assistant-Onlinehilfe*.

6. Unter **Zeitplan auswählen** können Sie entweder planen, den Task zu einem bestimmten Zeitpunkt oder sofort auszuführen.
7. Unter **Anmeldeinformationen eingeben** geben Sie die Anmeldeinformationen für Ihr Betriebssystem ein
8. Sie können Ihre Auswahl unter **Zusammenfassung** anzeigen und überprüfen.
9. Klicken Sie auf **Fertig stellen**, um Ihre Auswahl anzunehmen, oder auf **Zurück**, um Änderungen vorzunehmen.

-  **ANMERKUNG:** Zu diesem Zeitpunkt werden die Dateien zum IT Assistant-Repository hochgeladen. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

---



[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

**Dell OpenManage™ IT Assistant Version  
8.0: Benutzerhandbuch**

---

## Anmerkungen und Hinweise

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit deren Hilfe Sie den Computer besser einsetzen können.
-  **HINWEIS:** Ein HINWEIS warnt vor möglichen Beschädigungen der Hardware oder Datenverlust und zeigt, wie diese vermieden werden können.

---

**Irrtümer und technische Änderungen vorbehalten.  
© 2006 Dell Inc. Alle Rechte vorbehalten.**

Nachdrucke jeglicher Art ohne die vorherige schriftliche Genehmigung der Dell Inc. sind strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, das *DELL*-Logo, *OpenManage*, *OptiPlex*, *PowerEdge*, *PowerVault* und *PowerConnect* sind Marken von Dell Inc.; *Microsoft*, *Windows*, *Windows NT*, *Windows Server*, *Active Directory* und *Excel* sind eingetragene Marken der Microsoft Corporation; *Novell*, *NetWare* und *SUSE* sind eingetragene Marken von Novell, Inc. in den Vereinigten Staaten und anderen Ländern; *Red Hat* ist eine eingetragene Marke von Red Hat, Inc.; *Intel* ist eine eingetragene Marke der Intel Corporation; *EMC*, *FLARE* und *Navisphere* sind eingetragene Marken der EMC Corporation.

Alle anderen in dieser Dokumentation genannten und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. verzichtet auf alle Besitzrechte an Markenzeichen und Handelsbezeichnungen, die nicht ihr Eigentum sind.

Juni 2006

---

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

## Was ist neu in Version 8.0 des Dell OpenManage™ IT Assistant?

Dell OpenManage™ IT Assistant Version 8.0: Benutzerhandbuch

- [Leistungsüberwachung](#)
- [Ereignisquellen-Importdienstprogramm des einfachen Netzwerkverwaltungsprotokolls \(SNMP\)](#)
- [Support für IPMI-Ermittlung](#)
- [Softwarebereitstellung](#)
- [Digitalsignatur-Überprüfung](#)
- [Benutzerdefinierte Bündel](#)
- [Start der Favoriten-Anwendung](#)
- [Speicherintegration](#)
- [Druckerintegration](#)
- [Bandintegration](#)
- [FRU-Unterstützung](#)
- [Stromsteuerungs-Tasks](#)

Die folgenden Funktionen sind neu in dieser Version von IT Assistant:

---

### Leistungsüberwachung

Leistungsüberwachung hilft Ihnen, die Leistung einer Gruppe unterstützter Microsoft® Windows®- oder Linux-Systeme in Ihrer Netzwerkumgebung über einen bestimmten Zeitraum hinweg zu überwachen. Leistung wird mithilfe von Leistungsindikatoren überwacht, die für jede Komponente verfügbar sind. Sie können die Leistungsindikatoren auswählen und überwachen. Schwellenwertwarnungen können auch so konfiguriert werden, dass Sie über Systeme in Ihrem Netzwerk gewarnt und benachrichtigt werden, deren Gebrauch zu niedrig oder zu hoch ist. Weitere Informationen finden Sie unter "[Leistungsüberwachung](#)".

---

### Ereignisquellen-Importdienstprogramm des einfachen Netzwerkverwaltungsprotokolls (SNMP)

Sie können mehrere Ereignisquellen (die nicht systemeigen in IT Assistant unterstützt werden) in die IT Assistant-Datenbank importieren. Weitere Informationen finden Sie unter "[Ereignisquellen-Importdienstprogramm des einfachen Netzwerkverwaltungsprotokolls](#)".

---

### Support für IPMI-Ermittlung

IT Assistant ermittelt Systeme, die mit Baseboard-Verwaltungs-Controllern (BMC) ausgestattet sind, die die Versionen 1.5 oder höher der intelligenten Plattform-Verwaltungsschnittstelle (IPMI) unterstützen. IT Assistant kommuniziert direkt mit dem BMC oder über den Windows-IPMI-Anbieter auf einem Microsoft Windows Server® 2003 R2-System.

IT Assistant ermittelt und klassifiziert den BMC des ermittelten Systems über IPMI. Wenn jedoch der Dell-Agent auf diesem System installiert ist, korreliert IT Assistant die Informationen mit dem ermittelten System über die Service-Tag-Nummer.

---

### Softwarebereitstellung

Sie können diese Funktion verwenden, um Dell OpenManage Server Administrator auf Dell-Systemen bereitzustellen, auf denen Server Administrator nicht installiert ist. Server Administrator hilft beim Ermitteln und Klassifizieren und bei der Bestandsaufnahme und Überwachung von Systemen sowie beim Aktualisieren von Software in Ihrem Netzwerk.

Anhand dieser Funktion können Sie Server Administrator auch zu einer neueren Version aktualisieren.

---

### Digitalsignatur-Überprüfung

IT Assistant überprüft die Authentizität und Integrität der Update Packages und MSI-Dateien anhand von Digitalsignatur-Überprüfung.

Die Digitalsignatur-Überprüfung aller Dell™ Update Packages (DUP) wird ausgeführt, wenn Sie die Pakete manuell von der CD *Dell Server Update Utility* oder von einem Repository auf einer Netzwerkfreigabe importieren.

IT Assistant unterstützt auch die Signatur-Überprüfung für das Server Administrator-MSI-Paket.

---

## Benutzerdefinierte Bündel

Mithilfe von IT Assistant können Sie benutzerdefiniert einen Systemaktualisierungssatz oder ein Bündel erstellen.

Sie können benutzerdefinierte Bündel erstellen, die nur die von Ihnen gewünschten Pakete enthalten. Sie können z. B. ein benutzerdefiniertes Bündel aus einem bereits vorhandenen benutzerdefinierten Dell-Bündel erstellen, was Ihnen ermöglicht, nur die auf einem bestimmten Satz von Zielgeräten vorhandenen Gerätetreiber zu aktualisieren.

Dieses benutzerdefinierte Bündel kann anschließend zum Erstellen von Systemkonformitätsreporten und zum Ausführen benutzerdefinierter Aktualisierungen verwendet werden.

---

## Start der Favoriten-Anwendung

IT Assistant unterstützt das Starten benutzerkonfigurierter Anwendungen für verschiedene Geräte oder eine Gruppe von Geräten, wie z. B. für Drucker und Schalter. Weitere Informationen finden Sie in der *IT Assistant-Onlinehilfe*.

---

## Speicherintegration

IT Assistant ermittelt Dell|EMC-Arrays in Ihrer Speicherumgebung und zeigt sie in der Kategorie **Dell/EMC Arrays** an, die sich in der **Speichergeräte**-Gruppe befindet.

Weitere Informationen finden Sie in der *IT Assistant-Onlinehilfe*.

---

## Druckerintegration

IT Assistant Version 8.0 unterstützt die Ermittlung Dell-netzwerkaktivierter Drucker und ordnet sie unter der Kategorie **Drucker** in der **Geräte**-struktur ein.

IT Assistant verwendet SNMP zur Kommunikation mit den Druckergeräten. Dell-Drucker haben eine Standard-Drucker-MIB implementiert, wodurch standardisierter Zugriff auf wichtige Informationen möglich wird.



**ANMERKUNG:** Sie können diese Funktion von IT Assistant auch verwenden, um Nicht-Dell-Drucker in Ihrer Netzwerkumgebung zu ermitteln.

Weitere Informationen finden Sie in der *IT Assistant-Onlinehilfe*.

---

## Bandintegration



IT Assistant Version 8.0 unterstützt die Ermittlung derjenigen Dell-Bandbibliotheksgeräte, die eine bandexterne Verwaltungsschnittstelle besitzen. IT Assistant ordnet sie unter der Kategorie **Bandgeräte** in der **Speichergeräte**struktur ein. Weitere Informationen finden Sie in der *IT Assistant-Onlinehilfe*.

---

## FRU-Unterstützung


Mit IT Assistant Version 8.0 können Sie die Informationen zu den austauschbaren Funktionseinheiten (FRU) für ein verwaltetes System anzeigen. IT Assistant ruft während eines Bestandsaufnahmezyklus vom Dell OpenManage Server Administrator FRU-Informationen ab und speichert sie in der Datenbank.

Weitere Informationen finden Sie in der *IT Assistant-Onlinehilfe*.

---


## Stromsteuerungs-Tasks


Beginnend mit IT Assistant 8.0 und vor dem Versuch, SNMP-Stromsteuerungs-Tasks auszuführen, versucht IT Assistant den Befehl **omremote** auf dem verwalteten System. Dies trifft nur zu, wenn auf dem verwalteten System Dell OpenManage Version 4.3 oder höher installiert ist.

 **ANMERKUNG:** Bei Dell OpenManage-Versionen, die älter als 4.3 sind, bleiben die Stromsteuerungs-Tasks unverändert.

 **ANMERKUNG:** Der Befehl **omremote** verwendet die Anmeldeinformationen des Betriebssystems zur Authentifizierung.

IT Assistant Version 8.0 unterstützt das Ausführen von Remote-Stromsteuerungsvorgängen und Warnungsverarbeitungen auf Geräten, die mit dem Warnstandardformat (ASF) 2.0 konform sind.

 **ANMERKUNG:** In der Systemdokumentation finden Sie Informationen zum Aktivieren der Remote-Stromsteuerung durch ASF.

 **ANMERKUNG:** IT Assistant verwendet den bandinternen Broadcom-Windows Management Instrumentation-Anbieter (WMI), um zu überprüfen, ob ein Gerät ASF-Fähigkeiten aufweist.

---

[Zurück zum Inhaltsverzeichnis](#)