Dell OpenManage™ IT Assistant Version 7.2: 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.

Dezember 2005

Zurück zum Inhaltsverzeichnis

Protokolle für das Senden von Informationen zum IT Assistant konfigurieren

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

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 der IT Assistant den Status von Dell™ 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
Novell® NetWare®-Betriebssystem	Immer installiert.	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 der IT Assistant nur auf unterstützten Microsoft-Betriebssystemen installiert werden kann, kann der IT Assistant Systeme verwalten, auf denen unterstützte Microsoft-, Novell NetWare- und Red Hat 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 Verbindung mit dem IT Assistant verwendet wird, müssen Lesen/Schreiben- und Nur-Lesen-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.

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:

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

- 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.

Den SNMP-Agenten auf Systemen konfigurieren, auf denen unterstützte Red Hat Linux-Betriebssysteme 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
```

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** und führen Sie folgende Schritte durch:

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. Zur Konfiguration der Variablen müssen Sie die `sysContact`- und `sysLocation`-Werte in der SNMP-Konfigurationsdatei von Red Hat Enterprise Linux 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 das System, auf dem Server Administrator ausgeführt wird, für das Senden von Traps an ein Dienstesystem zu konfigurieren, bearbeiten Sie die Konfigurationsdatei des SNMP-Agenten **/etc/snmp/snmpd.conf**, indem Sie folgende Schritte durchführen:

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.

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

Verwaltete Systemagenten, wie z. B. der Server Administrator, verwenden die SNMP-Dienste des NetWare SNMP-Agenten. Der SNMP-Agent kann konfiguriert werden, um den Community-Namen zu ändern, Set-Vorgänge zu aktivieren und Traps an ein Dienstesystem zu senden. Führen Sie zur Konfiguration des SNMP-Agenten für die korrekte Kommunikation mit dem IT Assistant die in den folgenden Abschnitten beschriebenen Verfahren aus.

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

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

SNMP-Community-Namen ändern

Der vom IT Assistant verwendete SNMP-Community-Name muss mit dem auf allen verwalteten Systemen konfigurierten SNMP-Community-Namen übereinstimmen. Diese Übereinstimmung ist erforderlich, damit der IT Assistant Verwaltungsinformationen vom Server Administrator und allen anderen unterstützten Agenten erhalten kann.

Um den SNMP-Community-Namen auf einem verwalteten System zu ändern, führen Sie folgende Schritte durch:

1. Geben Sie an der NetWare-Befehlszeilenkonsole `inetcfg` ein und drücken Sie <Eingabe>.

   Das Menü **Netzwerkkonfiguration** wird eingeblendet.

   ANMERKUNG: Wenn Sie den Befehl `inetcfg` das erste Mal verwenden, werden Sie eventuell gefragt: `Do you want to transfer LAN drivers, protocol, and remote access commands? (Wollen Sie die LAN-Treiber-, Protokoll- und Remote-Zugriff-Befehle übertragen?)` Dell empfiehlt, diese Frage mit **Ja** zu beantworten. Weitere Informationen über diese Eingabeaufforderung finden Sie auf der Novell Website. Wenn Sie **Ja** wählen, wird das System neu gestartet. Kehren Sie nach dem Neustart zur Konsole zurück und geben Sie den Befehl `inetcfg` erneut ein. Eine Bildschirmmeldung mit folgender Aufforderung wird eingeblendet: `Do you want to use the fast setup method or the standard method? (Wollen Sie die schnelle Setup-Methode oder die Standardmethode verwenden?)` Dell empfiehlt, die Standardmethode für das SNMP-Setup auszuwählen. Fahren Sie nach Auswahl der Standardmethode mit dem nächsten Schritt fort.

2. Wählen Sie **Konfiguration verwalten**.

   Das Menü **Konfiguration verwalten** wird eingeblendet.

3. Wählen Sie **SNMP-Parameter konfigurieren**.

   Das Menü **SNMP-Parameter** wird eingeblendet.

4. Wählen Sie **Status überwachen**, um den Lesen (bzw. Get) Community-Namen zu konfigurieren.

   Das Menü **Community-Bearbeitung überwachen** wird zusammen mit den folgenden Optionen eingeblendet:

   - Jede Community darf lesen
   - Als Standardeinstellung belassen
   - Keine Community darf lesen
   - Angegebene Community darf lesen

   ANMERKUNG: Drücken Sie die Taste <F1>, um weitere Informationen über die Funktion **Status überwachen** zu erhalten. Drücken Sie <Esc>, um das Hilfefenster zu schließen.

5. Wählen Sie **Angegebene Community darf lesen**.
6. Geben Sie unter **Community überwachen** den Lesen Community-Namen ein.
7. Wählen Sie **Status steuern**, um den Schreiben (bzw. Set) Community-Namen zu konfigurieren.

   Das Menü **Community-Bearbeitung steuern** wird zusammen mit den folgenden Optionen eingeblendet:

   - Jede Community darf schreiben

- Als Standardeinstellung belassen
- Keine Community darf schreiben
- Angegebene Community darf schreiben

ANMERKUNG: Drücken Sie die Taste <F1>, um weitere Informationen über die Funktion **Status steuern** zu erhalten. Drücken Sie <Esc>, um das Hilfefenster zu schließen.

8. Wählen Sie **Angegebene Community darf schreiben**.
9. Geben Sie unter **Community steuern** den Schreiben Community-Namen ein.
10. Wählen Sie **Trap-Status**, um die Trap-Community-Bearbeitung zu konfigurieren.

Das Menü **Trap-Bearbeitung** wird zusammen mit den folgenden Optionen eingeblendet:

- Keine Traps senden
- Als Standardeinstellung belassen
- Traps mit angegebener Community senden

11. Wählen Sie **Traps mit angegebener Community senden**.
12. Geben Sie unter **Trap-Community** den Community-Namen ein, an den die Traps gesendet werden sollen.

ANMERKUNG: Drücken Sie die Taste <F1>, um weitere Informationen über die Funktion **Trap-Status** zu erhalten. Drücken Sie <Esc>, um das Hilfefenster zu schließen.

13. Drücken Sie <Esc>, um das Menü **SNMP-Parameter** zu schließen.

Ein Dialogfeld mit der Aufforderung zum Speichern der Änderungen wird eingeblendet.

14. Wählen Sie **Ja**.

Das Menü **Konfiguration verwalten** wird eingeblendet.

15. Drücken Sie <Esc>, um das Menü **Konfiguration verwalten** zu schließen.

Das Menü **Netzwerkkonfiguration** wird eingeblendet.

16. Wählen Sie **Protokolle**.

Das Menü **Protokollkonfiguration** wird eingeblendet.

17. Wählen Sie **TCP/IP**.

Das Menü **Konfiguration TCP/IP-Protokoll** wird eingeblendet.

18. Wählen Sie **SNMP-Managertabelle**.

Das Menü **SNMP Managertabelle** wird zusammen mit den folgenden Optionen eingeblendet:

- Drücken Sie <Einfg>, um SNMP-Trap-Ziele hinzuzufügen.
- Drücken Sie <Eingabe>, um SNMP-Trap-Ziele zu bearbeiten.
- Drücken Sie <Entf>, um SNMP-Trap-Ziele zu löschen.

ANMERKUNG: Drücken Sie die Taste <F1>, um weitere Informationen über die Funktion **SNMP-Managertabelle** zu erhalten. Drücken Sie <Esc>, um das Hilfefenster zu schließen.

19. Wählen Sie unter **SNMP-Managertabelle** eine der Menüoptionen aus.
20. Drücken Sie <Esc>, um das Menü **SNMP-Managertabelle** zu schließen.

Ein Dialogfeld mit der Aufforderung zum Aktualisieren der Datenbank wird eingeblendet.

21. Wählen Sie **Ja**.

    Das Menü **Konfiguration TCP/IP-Protokoll** wird eingeblendet.

22. Drücken Sie zweimal die Taste <Esc>, um das Menü **Konfiguration TCP/IP-Protokoll** zu schließen.

    Das Menü **Netzwerkkonfiguration** wird eingeblendet.

23. Starten Sie das System neu, um die Änderungen an der Konfiguration zu aktivieren.

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.

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 verhütet 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 **localhost (lokaler Host)**, wenn keine Domäne vorhanden ist. Das Format ist entweder **domain\user (Domäne\Benutzer)** oder **localhost\user (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

Einführung in IT Assistant

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

Dell OpenManage™ IT Assistant bietet einen zentralen Zugriffspunkt, um Systeme in einem lokalen Netzwerk (LAN) oder einem übergreifenden Netzwerk (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:

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

Systemgruppen zur Remote-Verwaltung identifizieren

IT Assistant führt eine grundlegende Ermittlung und eine Statusabfrage aus, 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 Verwaltungskonsole angezeigt und in der IT Assistant-Datenbank eingetragen. Als Standard-Datenbank dient Microsoft® Database Engine (MSDE) 2000. Benutzer, die eine leistungsfähigere Datenbank benötigen, können Microsoft SQL Server einsetzen.

Anzeige aller Systeme konsolidieren

Mit dem IT Assistant können Systemadministratoren von der Verwaltungskonsole aus Maßnahmen auf verwalteten Systemen durchführen. Mit dem IT Assistant können Sie Tasks erstellen, die auf ein einzelnes System oder jedes System in der Gruppe angewendet werden. Sie können dynamische Gruppen von Systemen erstellen, um die Verwaltung zu erleichtern und eine Bestandsaufnahme auf jedem System durchzuführen. Außerdem bietet IT Assistant einen konsolidierten Startpunkt für die folgenden Dell™ Systems Management-Anwendungen und -Geräte: Dell OpenManage Server Administrator, Dell OpenManage Array Manager, Remote Access-Konsole, Dell PowerConnect™ und Digitaltastatur/-video/-maus (KVM).

Warnungsfilter und -maßnahmen erstellen

Sie können IT Assistant verwenden, um Warnungs*filter* zu erstellen, um Warnungen zu isolieren, die für einen Systemadministrator am wichtigsten sind. System-Administratoren können dann entsprechende Warnungs*maßnahmen* 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 Reporte für alle Geräte und Gruppen im ganzen Unternehmen erstellen. Diese

Reporte können Gerätebestandsaufnahme-Informationen enthalten, die auf einer umfassenden Auswahl an Attributen basieren. Zum Beispiel können Sie einen Report erstellen, der Details für jede Gerätekarte in allen Servern in einer Gruppe aufführt, darunter die Bustaktrate und -breite, Hersteller sowie Steckplatzlänge und/oder -nummer. IT Assistant bietet auch eine Sammlung vorformatierter Reporte, 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 durchführen, oder Befehlszeilen-Tasks auf jedem System der verwalteten Gruppe ausführen. IT Assistant ermöglicht Ihnen, Dell Update Packages und System Update Sets in ein Zentral-Repository zu laden und dann deren Übereinstimmung mit Servern im Unternehmen zu überprüfen. Der Systemadministrator kann dann IT Assistant beauftragen, die Aktualisierungen sofort oder nach einem festgelegten Plan auszuführen.

ANMERKUNG: Um eine Software-Aktualisierung auszuführen, muss die entsprechende Agent-Software auf dem Zielgerät installiert sein. Weitere Informationen zu Agenten finden Sie unter "Agenten auf den zu überwachenden Systemen".

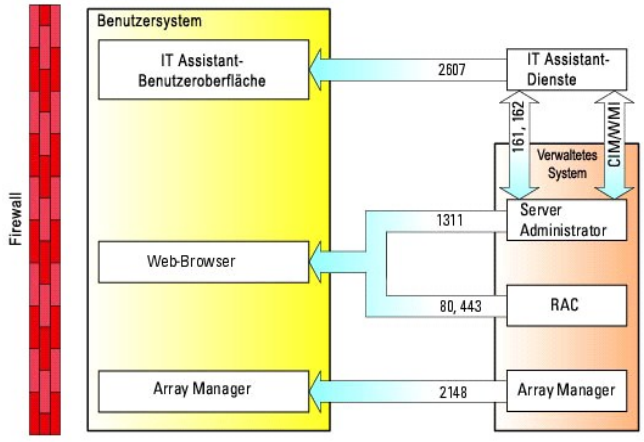
Funktionen der IT Assistant-Komponenten verstehen

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

- IT Assistant-UI
- IT Assistant-Dienstestufe (Netzwerküberwachungsdienst, Verbindungsdienst und Datenbank)
- Verwaltetes System

Die IT Assistant-UI bietet eine graphische Benutzeransicht der durch die IT Assistant-Dienstestufe 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.

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 Warnungsfiltern und -maßnahmen sowie das Aus- und Einschalten von Systemen.

Die IT Assistant-Benutzeroberfläche basiert auf Sun Java-Technologie. Remote-Zugriff erfolgt entweder durch einen Webbrowser (Internet Explorer auf

Microsoft Windows®- und Mozilla oder Firefox auf Red Hat® Enterprise Linux-Systemen) oder eine Terminaldienstesitzung.

IT Assistant-Dienste

Die IT Assistant-Dienstestufe ist Teil der Standardinstallation. Rein technisch besteht die Dienstestufe aus dem Netzwerküberwachungsdienst, dem Verbindungsdienst und der Datenbank. Bei im hohen Grade benutzerspezifischen Installationen können Benutzer eine eigene Datenbank auf einem separaten System installieren. Bei der Konfiguration des SNMP-Agenten auf einem verwalteten System müssen die Trap-Ziele für den SNMP-Dienst auf den Host-Namen oder die IP-Adresse, wo der IT-Assistant installiert ist, zeigen.

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.

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 des IT Assistant umfasst assistentenbasierte Dialoge zur Ausführung zahlreicher Standard-Tasks. Die Optionen der IT Assistant-Menüleiste haben sich geändert, weshalb erfahrene Benutzer etwas Zeit investieren sollten, um sich an das neue Layout zu gewöhnen.

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 Javatechnologie von Sun Microsystems und unterstützt Linux-Systeme.

DMI-Support

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

Neue 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 IT Assistant-Online-Hilfe.

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 Warnungsfilter oder einen Task erstellen bzw. bearbeiten.

Anwendungsstart

IT Assistant bietet die Möglichkeit einer gemeinsamen Start-URL für die folgenden Systems Management-Anwendungen von Dell: Server Administrator, Array Manager, Remote Access-Konsole, PowerConnect und Digital-KVM (Tastatur/Video/Maus). Weitere Informationen finden Sie unter dem Thema Anwendungsstart in der IT Assistant-Online-Hilfe.

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 individuell einstellbare Reportfunktion, die Daten von der Microsoft Data Engine (MSDE) und von der SQL-Serverdatenbank einholt. 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 :

- Details zu den Hardwaregeräten, die von IT Assistant verwaltet werden, einschließlich Systeme, Schalter und Speichergeräte
- BIOS-, Firmware- und Treiberversionen
- 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 Spreadsheet-Hilfsprogramm 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-Online-Hilfe zur Verfügung.

Software-Aktualisierungen

Mit IT Assistant können Sie Dell Aktualisierungspakete und System-Aktualisierungspakete 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, Komponentenname und Softwaretyp.

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

Tasks verwalten

Der IT Assistant bietet eine aktualisierte Task-Funktionalität, die es Ihnen ermöglicht, bestimmte Tasks im Remote-Zugriff auf allen Systemen des Unternehmens einzurichten und auszuführen, einschließlich Gerätesteuerung (Herunterfahren und Hochfahren), Softwareaktualisierung und Befehlszeilenausführung.

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

Fehlerbehebungshilfsprogramm

Unter **Hilfsprogramme→ Fehlerbehebungshilfsprogramm** steht ein graphisches Fehlerbehebungshilfsprogramm zur Verfügung, mit dem Ermittlungs- und Konfigurationsprobleme, u. a. Probleme mit dem einfachen Netzwerkverwaltungsprotokoll (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-Online-Hilfe.

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 Active Directory-Schema und wie man es für die Verwendung mit IT Assistant konfigurieren kann (einschließlich der Konfiguration 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 Bestandsaufnahmeeinstellungen 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 Einmalige Anmeldung können Sie die Anmeldungsseite umgehen, und durch Klicken auf das **IT Assistant**-Symbol auf dem Desktop 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 einmalige 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.

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 auf der Dell Support-Website unter **support.dell.com** oder auf der Dokumentations-CD zur Verfügung:

- 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.
- Das *Dell OpenManage Server Administrator SNMP-Referenzhandbuch* dokumentiert die SNMP-Verwaltungsinformationsbasis (MIB). Die SNMP-MIB definiert Variablen, die über die Standard-MIB hinausgehen, um die Fähigkeiten von Systemverwaltungsagenten abzudecken.
- Das *Dell OpenManage Server Administrator CIM-Referenzhandbuch* beschreibt den CIM-Anbieter, einer Erweiterung der Standard-MOF-Datei

(Verwaltungsobjektformat). Die von den MOF-Dokumenten des CIM-Anbieters unterstützten Klassen von Verwaltungsobjekten.

- 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-Online-Hilfe zugreifen: entweder indem Sie auf den **Hilfe**-Link an der oberen rechten Seite des Browser-Fensters klicken, oder indem Sie auf die Schaltfläche **Hilfe** innerhalb des Dialogs oder Assistenten, den Sie verwenden, klicken.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

IT Assistant-Installation planen

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

Es ist wichtig, einen Plan vor der Installation von Dell OpenManage™ IT Assistant zu machen. 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. Auf der anderen Seite wollen Sie eventuell dass IT Assistant nur Warnungen über Probleme auf spezifischen verwalteten Systemen erhält und an Support-Mitarbeiter weitergibt. 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:

- Ereignisfilter und Benachrichtigungsstrategie
- Datenbank zur Speicherung von IT Assistant-Daten
- Hardwarekonfiguration
- Betriebssystem
- Systemverwaltungsprotokolle
- 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 Aktualisierungsverfahren finden Sie unter "IT Assistant installieren, deinstallieren und aktualisieren".

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 zur Durchführung der Installation Tabelle 2-4 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 (MSDE) verwenden oder die Microsoft® SQL Server-Datenbank installieren?
    - Wie viele Systeme sollen ermittelt oder verwaltet werden?
    - Wie dicht wird der Ereignisverkehr im Netzwerk voraussichtlich sein?
5. Welche Systemverwaltungsprotokolle sollten installiert oder aktiviert werden?
    - Welche Systemtypen sollen verwaltet werden?
    - Welche Agenten und Instrumentationen sind derzeitig in den verwalteten Systemen installiert?
    - Welche Agenten sollen eventuell auf dem verwalteten System ausgeführt werden?
    - 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

Der IT Assistant kann auf jedem System installiert werden, auf dem eines der Betriebssysteme in Tabelle 2-1 ausgeführt wird.

Tabelle 2-1. 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	Windows 2000 mit SP4

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™ Servern installiert werden, die Red Hat® Enterprise Linux-Betriebssysteme ausführen. Diese Server können IT Assistant jedoch durch unterstützte Browser (Mozilla Version 1.7.3 und höher sowie Firefox Version 1.0.1 oder höher) starten.

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:

- Viel Warnungsverkehr für verwaltete Systeme erwartet wird
- Komplexe Warnungsfilter mit konfigurierten Warnungsmaßnahmen eingesetzt werden
- Häufig Ermittlungs-, Bestandsaufnahmen-, und Statusabfragen durchgeführt werden
- Microsoft SQL Server mit maximaler Leistung ausgeführt wird.

Die empfohlene minimale Hardwarekonfiguration für den IT Assistant wird in Tabelle 2-2 gezeigt.

Tabelle 2-2. 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	bis zu 5 GB

ANMERKUNG: Die benötigte Menge an Festplattenspeicherplatz kann zunehmen, wenn Sie zahlreiche Aktualisierungspakete importieren.

MSDE-Standarddatenbank oder SQL 2000 Server auswählen

Allgemein wird die mit dem IT Assistant eingesetzte Datenbank durch die Anzahl der Systeme zur Verwaltung sowie der Anzahl der Warnungen der verwalteten Systeme festgelegt. Wenn weniger als 500 Systeme verwaltet werden, ist die SQL-serverkonforme Standarddatenbank (Microsoft Data Engine [MSDE] 2000), die mit dem IT Assistant versandt wird, wahrscheinlich 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. Wenn zusätzlich Ermittlungen oder Statusabfragen häufig durchgeführt werden, könnten Sie von der höheren Leistung, die SQL Server 2000 gegenüber MSDE 2000 bietet, profitieren.

ANMERKUNG: IT Assistant Version 6.3 und höher kann so konfiguriert werden, dass Microsoft SQL Server auf einem dedizierten Remote-Server anstatt auf einem der IT Assistant-Systeme ausgeführt wird. Lesen Sie dazu das entsprechende Whitepaper von Dell mit dem Titel "Remote Microsoft SQL

Server Use with IT Assistant Step-by-Step" (Remote-Verwendung des Microsoft SQL Server mit IT Assistant - schrittweise erklärt) unter **www.dell.com/openmanage**.

E-Mail-Benachrichtigungsfunktion

E-Mail-Warnungsmaßnahmen sind in Umgebungen hilfreich, in denen ein Systemadministrator den Status von verwalteten Systemen nicht visuell über die IT Assistant-Benutzeroberfläche (UI) überwachen will. 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 durch IT Assistant nicht mehr erforderlich, da eine E-Mail-Benachrichtigung ausgegeben wird, sobald eine Ereignisbedingung erfüllt wird.

Systems Management-Protokolle festlegen

Eine der wichtigsten Entscheidungen im Verlauf der Planung der IT Assistant-Installation ist die Festlegung der Protokolle, die mit dem 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 wollen, Agenten haben, die das einfache Netzwerkverwaltungsprotokoll (SNMP) oder Protokolle des allgemeinen Informationsmodells (CIM) verwenden, müssen diese auch im IT Assistant konfiguriert werden.

Unterstützte Protokolle

IT Assistant unterstützt zwei Systemverwaltungsprotokolle: SNMP, und CIM. 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 Serververwaltung wird nachhaltig empfohlen, dass Sie beide Protokolle 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.

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.

Faktoren, die die Wahl des Protokolls beeinflussen

Die Wahl des Protokolls wird durch zwei Faktoren beeinflusst:

- Durch die zu überwachenden Systeme
- Agenten auf den zu überwachenden Systemen

Zu überwachenden Systeme

Das Netzwerk besteht aus einer Kombination von Client- und Server-Systemen, einschließlich portablen Computern, Desktops, Workstations und Standalone-Servern, wie z. B. Drucker- und Dateiserver, Servermodule (oder Blades), Cluster-Server oder hunderte von Servern in dicht bestückten Racks. 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 2-3 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. In Folge dessen können Systeme, auf denen DMI mit Dell OpenManage Server Agent 4.5.1 (und darunter) und OMCI 6.0 (und darunter) ausgeführt wird, von IT Assistant nicht ermittelt werden.

Tabelle 2-3. Von IT Assistant unterstützte Agenten

Gerät	Unterstützte Version(en)	Automatisch ermittelbar	Alarmierung
Dell PowerEdge™-Agenten*			
Server Administrator	1.0-2.2	Ja	Ja
Server Agent	4.2-4.5	Ja	Ja
Array Manager	2.5-3.7	Ja	Ja
DRAC 4	1.0-1.30	Ja	Ja
DRAC III, DRAC III/XT	1.0-3.50	Ja	Ja
ERA, ERA/O	1.0-3.50	Ja	Ja
ERA/MC	1.0-3.50	Ja	Ja
Integrierter PowerEdge 1655MC/1855MC-Schalter	-	Ja	Ja
* IT Assistant erfordert Server Administrator 2.0 oder höher für Remote-Softwareaktualisierungen.			
Dell PowerVault™-Agenten			
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
Adaptec CIO	4.02	Nein	Ja
Von IT Assistant unterstützte Dell PowerConnect™-Agenten und PowerConnect-Firmware-Versionen			
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 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*	Ja	Ja
PowerConnect 5316M	1.0.0.*x*	Ja	Ja
PowerConnect 5324	1.0.1.*x*	Ja	Ja
PowerConnect 6024	1.0.2.*x*	Ja	Ja
PowerConnect 6024F	1.0.2.*x*	Ja	Ja
Digital-KVM-Agenten			
2161 DS	-	Ja	Ja
Netzwerkadapteragenten			
Intel® PRO	-	Nein	Ja
Broadcom	-	Nein	Ja

ASF	1	Nein	Ja
Client-Agenten			
Dell OpenManage Client Instrumentation	7.*x*	Ja	Ja

Zusammenfassung der Entscheidungen vor der Installation

In diesem Abschnitt werden die vor der Installation und Verwendung des IT Assistant zur Systemverwaltung im Netzwerk zu beachtenden Hauptfaktoren aufgeführt. In Tabelle 2-4 werden die in den vorhergehenden Abschnitten aufgekommenen Fragen, die verfügbaren Optionen und Maßnahmen sowie der Abschnitt in diesem Handbuch, in dem das entsprechende Verfahren zur Durchführung dieser Maßnahmen zu finden ist, aufgeführt.

Tabelle 2-4. 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 installierte IT Assistant-Komponente unterstützt wird.	Installieren Sie die IT Assistant-Dienste bei einem großen Netzwerk auf einem serverbasierten Betriebssystem.	Lesen Sie dazu die neueste Infodatei **readme.txt** des IT Assistant, die entweder auf der Dell Support-Website unter **support.dell.com** oder auf der CD *Dell Systems Management Consoles* zu finden ist.
Muss ich eine bestimmte Hardwarekonfiguration für die IT Assistant-Installation wählen?	Stellen Sie sicher, dass die Hardwarekonfiguration die empfohlenen Anforderungen an die IT Assistant-Komponenten, die auf dem System installiert werden, erfüllt oder übertrifft.		
Soll ich die installierte Standarddatenbank (MSDE) verwenden oder die Microsoft SQL Server-Datenbank installieren?	Normalerweise ist MSDE zur Verwaltung von weniger als 500 Systemen ausreichend. Bei starkem Ereignisverkehr oder anderen Anforderungen an die Leistung kann SQL Server gewählt werden.	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 "IT Assistant installieren, deinstallieren und erweitern" und "IT Assistant zur Überwachung der Systeme konfigurieren".
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 "Sichere Dell OpenManage IT Assistant-Installation gewährleisten"

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

IT Assistant installieren, deinstallieren und aktualisieren

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

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 der Dell™ Support-Website unter **support.dell.com** gelesen werden. In dieser Datei werden die derzeit unterstützten Betriebssysteme und Hardware-Anforderungen 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 erhalten Sie unter "IT Assistant-Installation planen".

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. Um zusätzlich sicherzustellen, dass Systeme von den IT Assistant-Ermittlungs- und Bestandsaufnahmefunktionen wahrgenommen werden, vergewissern Sie sich, dass Agenten und Instrumentation auf verwalteten Systemen durch das CIM-Protokoll (allgemeines Informationsmodell) zugänglich sind.

ANMERKUNG: CIM ist unter 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**.

   Das Fenster **Software** wird 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 Überwachungsprogramme**, klicken Sie auf **Details**, wählen und markieren Sie **Einfaches Netzwerk-Verwaltungsprotokoll** 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.

Der 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 Novell® NetWare® ausgeführt werden, finden Sie unter "Protokolle für das Senden von Informationen zum 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 für das Senden von Informationen zum IT Assistant konfigurieren".

RBAC-Benutzerinformationen einrichten

IT Assistant unterstützt funktionsbasierte Access Control (RBAC), um die spezifischen Vorgänge zu definieren, die jeder Benutzer durchführen kann. Das IT Assistant-Installationsverfahren erfordert jedoch nicht, dass diese Benutzerfunktionen vor der Installation eingerichtet sind. Um RBAC-Benutzer entweder vor oder nach der Installation des 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** 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 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 Abhängigkeit gefunden wird, sehen Sie ein Informationsfenster und werden eventuell dazu aufgefordert, das erforderliche Paket zu installieren.

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

   Der Installations-Assistent 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 **Schnelle** oder **Benutzerdefinierte** Installation im Fenster **Setup-Typ**.

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

5. Stellen Sie sicher, dass **IT Assistant** in der Liste installierbarer Komponenten markiert 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 **Schnell** ausgewählt haben erscheint dieser Dialog 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.

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 allen Abhängigkeiten (z. B., ob Sie SNMP installiert haben oder ob Sie eine unterstützte Datenbankanwendung haben). Wenn eine Abhängigkeit gefunden wird, sehen Sie ein Informationsfenster und werden eventuell dazu aufgefordert, die erforderlichen Pakete zu installieren.

   ANMERKUNG: Wenn Sie IT Assistant Version 6.*x* haben, installieren Sie IT Assistant 7.0, bevor Sie Version 7.1 oder eine neuere Version installieren. Das IT Assistant 7.0-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 7.0 oder eine neuere Version haben, installiert das Installationsprogramm IT Assistant 7.2 als Service Pack.
3. Wenn keine Abhängigkeiten gefunden werden, klicken Sie auf **Management Station installieren, modifizieren, reparieren oder entfernen**.

   Der Installations-Assistent 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 **Schnelle** oder **Benutzerdefinierte** Installation im Fenster **Setup-Typ**.

   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 **Schnell** installiert alle Dell OpenManage-Anwendungen (einschließlich IT Assistant) mit vorausgewählten Standardeinstellungen für den Standort und die Schnittstelle.
6. Stellen Sie sicher, dass **IT Assistant** in der Liste installierbarer Komponenten markiert 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 **Schnell** ausgewählt haben erscheint dieser Dialog nicht.
8. Standardmäßig ist **IT Assistant-Datenbankeinstellungen migrieren** ausgewählt. Bei Auswahl dieser Option, werden die folgenden Datenbankeinstellungen der vorhandenen IT Assistant-Installation in der neuen Installation erhalten:
   - Globale Konfiguration
   - Nach Ereignissen gespeicherte Maßnahmen
   - Ermittlungskonfiguration
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.

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 **Management Station** von der Liste der zurzeit installierten Programme 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 unempfänglich 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 Sie dann auf **Weiter**.
6. Stellen Sie im Zusammenfassungsbildschirm sicher, dass IT Assistant in die Liste der zu entfernenden Anwendungen aufgenommen ist. Klicken Sie auf **Installieren**.
7. Klicken Sie nach Abschluss der Deinstallation auf **Fertig stellen**.
8. Starten Sie das System neu.

Microsoft SQL Server und IT Assistant im Fernzugriff

Im Whitepaper "Remote Microsoft SQL Server Use With IT Assistant Step-by-Step" (Remote-Verwendung des Microsoft SQL Server mit IT Assistant - schrittweise erklärt) unter **www.dell.com/openmanage** wird beschrieben, wie IT Assistant Version 6.3 oder eine neuere Version zur Verwendung von Microsoft SQL Server als IT Assistant-Datenbank auf einem Remote-Server konfiguriert wird.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

IT Assistant zur Überwachung von Systemen konfigurieren

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

Dell OpenManage™ IT Assistant kann Ermittlung, Bestandsaufnahme und eine Reihe von Änderungsverwaltungs-Tasks für jedes System in Ihrem Unternehmen ausführen. Verwaltete Systeme können eine Mischung von Client-Systemen (Desktops, Portables und Workstations), Servern, Systemen mit Remote-Zugriffskarten, Dell™ PowerConnect™-Schaltern und Digitaltastatur/video-/maus (KVMs) -schaltern, die bei Systemen mit dicht gefüllten Racks verwendet werden, umfassen.

IT Assistant in authentischen Benutzerszenarios

In diesem Abschnitt wird beschrieben, wie IT Assistant in zwei verschiedenen Kundenszenarios eingesetzt werden kann.

- Eine kleine bis mittelgroße Firma
- Eine Umgebung in größeren Unternehmen

Obwohl es sich bei den beiden in diesem Abschnitt präsentierten Szenarios 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-Online-Hilfe.

Sicherstellen, dass Agenten und Instrumentation installiert sind und ausgeführt werden

Ganz gleich, ob es sich um große oder kleine Netzwerke handelt, alle von IT Assistant verwalteten Netzwerke haben eine grundlegende Anforderung gemeinsam: Dell Systems Management-Agenten (Instrumentation) müssen auf allen verwalteten Systeme im Netzwerk installiert sein und ausgeführt werden. Für verwaltete Systeme notwendige Dell Agenten sind im Dell OpenManage Server Administrator enthalten; Für Client-Systeme notwendige Dell Agenten (Workstations, Desktops und Portables) sind in Dell OpenManage Client Instrumentation (OMCI) enthalten.

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

Wenn diese zwei Agenten nicht installiert sind, 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 beide installiert sind und ordnungsgemäß ausgeführt werden, starten Sie IT Assistant und lesen Sie weiter.

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 Active Directory-Plug-in konfiguriert haben. Die Berechtigungen, die Sie im IT Assistant haben, hängen von den definierten Benutzereinstellungen ab.

   ANMERKUNG: Weitere Informationen zum Einstellen von rollenbasiertem Zugriff 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>:<Schnittstellennummer>` eingeben. Die Standardschnittstellennummer 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 Authorisierungszertifikat 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 an, 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

Genaue Informationen zur SNMP-Konfiguration für das IT Assistant-System und für alle unterstützten Betriebssysteme der verwalteten Systeme finden Sie unter "Protokolle für das Senden von Informationen zum 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:

- Verwendung eines Host-Namens oder einer statischen IP-Adresse für das IT Assistant-System.
- 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 DNS im Netzwerk richtig konfiguriert sein.
- Stellen Sie sicher, dass sich die **Get** und **Set** Community-Namen für SNMP unterscheiden.
- 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

Stellen Sie für jedes über das SNMP-Protokoll zu ermittelnde und zu verwaltende System sicher, dass:

- SNMP installiert ist.
- Die Liste mit dem Namen bzw. der IP-Adresse für das IT Assistant-System finden Sie hier: Fenster SNMP-Dienst-Eigenschaften → Register Sicherheit → Optionsschaltfläche **SNMP-Pakete von diesen Hosts annehmen**. Dieser Wert muss auf dem verwalteten System konfiguriert werden.
- Falls verwaltete Systeme Traps an IT Assistant senden, muss der Host-Name bzw. die IP-Adresse des IT Assistant im Register **Traps** des Fensters **Eigenschaften SNMP-Dienst** als **Trap-Ziel** aufgeführt werden.
- In den Registern **Traps** und **Sicherheit** des Fensters **SNMP-Dienst-Eigenschaften** müssen gültige Community-Namen entsprechend zugewiesen werden.

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.

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 verwaltete Systeme umfasst, die ein Microsoft® Windows®-Betriebssystem ausführen.

CIM im Betriebssystem konfigurieren

IT Assistant verwendet zur Herstellung von CIM-Verbindungen den WIM (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 für das Senden von Informationen zum 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 **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.

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 4-1. 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

---

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:

- 50 Dell PowerEdge™-Systemen
- 200 Dell OptiPlex™-Desktops
- 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:

- Systemverwaltungsprotokolle, die zur Verwaltung der Systeme und Geräte in ihrem Netzwerk erforderlich sind
- Community-Namen und Trap-Ziele für Systeme, die durch SNMP verwaltet werden sollen
- SNMP-Anforderungen für PowerConnect-Schalter
- CIM-Anmeldeinformationen zur Authentifizierung
- 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:

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

Protokollanforderungen finden Sie unter "Protokolle für das Senden von Informationen zum 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 den Servern finden Sie unter "Protokolle für das Senden von Informationen zum IT Assistant konfigurieren".

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:

- Community-Namen
- Trap-Ziele
- 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:

- Kommunikationsprotokolle auf den verwalteten Systemen konfigurieren.
- Einstellungen für die Ermittlung konfigurieren.
- 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: Bestandsaufnahmekonfiguration - kontrolliert, wie oft IT Assistant eine ausführliche Bestandsaufnahme aller ermittelten Systeme abruft

Schritt 3: Statusabfrage - kontrolliert, wie oft IT Assistant den Funktionszustand und den Netzwerkkonnektivitätsstatus von ermittelten Systemen abruft

Schritt 4: Bereiche - identifiziert spezifische Bereiche für den 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 zur Definition 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.

So werden Ermittlungseinstellungen in IT Assistant konfiguriert:

1. Wählen Sie **Ermittlung und Überwachung**→ **Ermittlungskonfiguration** von der IT Assistant-Menüleiste aus.

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

2. Im Dialogfeld unter **Geräteermittlung einleiten** wählen Sie aus, wann IT Assistant die Ermittlung ausführen soll.

   Sabine wählt 6:00:00 Uhr an allen sieben Tagen der Woche, da sie die Daten aller Tage benötigt und die Netzwerkbelastung gering sein soll.

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

3. Bestimmen Sie über den Schieberegler unter **Ermittlungsgeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die für die Ermittlung zur Verfügung gestellt werden sollen.

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

4. Unter **Ermitteln**, wählen Sie aus, ob **Alle Geräte** oder **Nur instrumentierte Geräte** ermittelt werden sollen.

   Sabine wählt **Nur instrumentierte Geräte**, da sie will, dass IT Assistant nur Geräte mit SNMP- oder CIM-Instrumentation entdeckt. 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 Domänennamesystem (DNS) im Netzwerk konfiguriert ist.

5. Unter **Namensauflösung** wählen Sie **DNS-Namensauflösung** oder **Instrumentationsnamensauflösung**.

   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. Klicken Sie auf **OK**.

Bestandsaufnahmeeinstellungen konfigurieren

Als nächstes muss Sabine sie Bestandsaufnahmeneinstellungen eingeben. IT Assistant sammelt Bestandsaufnahmeninformationen 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 Reporte verwendet werden.

So werden Bestandsaufnahmeeinstellungen eingestellt:

1. Wählen Sie **Ermittlung und Überwachung**→ **Bestandsaufnahmekonfiguration** aus der Menüleiste aus.

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

2. Unter **Bestandsaufnahme einleiten**, wählen Sie aus, wann IT Assistant die Bestandsaufnahme ausführen soll.

Sabine wählt jeden Tag der Woche um 06:00:00, da dies keine Spitzenzeit für den Netzwerkverkehr ist.

3. Bestimmen Sie über den Schieberegler unter **Bestandsaufnahmegeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die für die Bestandsaufnahme zur Verfügung gestellt werden sollen.

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

4. Klicken Sie auf **OK**.

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.

So werden Statusabfrageeinstellungen eingestellt:

1. Wählen Sie **Ermittlung und Überwachung**→ **Statusabfragekonfiguration** aus der Menüleiste aus.

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

2. Unter **Bestandsaufnahme der Statusabfrage**, wählen Sie aus, welches Intervall IT Assistant zur Ausführung der Statusabfrage verwenden soll.
3. Bestimmen Sie über den Schieberegler unter **Statusabfragegeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die für die Statusabfrage zur Verfügung gestellt werden sollen.

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

4. Klicken Sie 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.

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

So legen Sie einen *Einschluss*bereich fest:

1. Wählen Sie **Ermittlung und Überwachung**→ **Bereiche** aus der Menüleiste aus.

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

2. Erweitern Sie **Ermittlungsbereiche**, klicken Sie mit der rechten Maustaste auf **Einschlussbereiche** und wählen Sie **Neuer Einschlussbereich**.

   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 geben Sie eine IP-Adresse (bzw. einen Bereich) oder einen Host-Namen ein und klicken Sie 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-Online-Hilfe. Die Datei **importnodelist.exe** befindet sich im Verzeichnis **/bin**.

4. In Schritt 2 des Assistenten verwenden Sie die Standardwerte für die Internetsteuerungs-Meldungsprotokoll (ICMP)-Zeitüberschreitung und versuchen den Bereich erneut. Verwenden Sie das Fehlerbehebungs-Hilfsprogramm, um diese Werte zu bestimmen.
5. In Schritt 3 des Assistenten, konfigurieren Sie die SNMP-Parameter, die während der Ermittlung verwendet werden sollen:
   - Stellen Sie sicher, dass die Option **SNMP-Ermittlung aktivieren** ausgewählt ist.
   - Geben Sie 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-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, kann sie im Feld **Get-Community**-Name mehrere durch Kommas getrennte Community-Namen eingeben.

   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.

   - Geben Sie 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, 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.

   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.

   - Zeitüberschreitungs- und Wiederholungswert für den SNMP-Ermittlungsbereich eingeben. Für Sabines Netzwerktyp sind die Standardwerte gewöhnlich eine gute Wahl.
6. In Schritt 4 des Assistenten, konfigurieren Sie 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.

   - Stellen Sie sicher, dass **CIM-Ermittlung aktivieren** ausgewählt ist.
   - In **Domäne\Benutzername**, geben Sie denselben Namen ein, den Sie zur CIM-Konfiguration auf dem verwalteten System verwendet haben.
   - Geben Sie dasselbe **Kennwort** ein, das Sie als CIM Kennwort auf dem verwalteten System verwendet haben.
7. In Schritt 5 des Assistenten, wählen Sie, welche Maßnahme IT Assistant nach Beendigung des Assistenten ausführen wird.
8. In Schritt 6 des Assistenten, sehen Sie sich Ihre Auswahl noch einmal an und wählen **Fertig stellen**, um den Assistenten abzuschließen oder **Zurück**, um die Auswahl zu ändern.

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

ändern

Sie können jederzeit zur Bearbeitung der eingegebenen Einstellung 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 im Stande sein, eine Warnungsmaßnahme zu erstellen, die ihr automatisch eine E-Mail-Benachrichtigung sendet, wenn die Server- und Schalterkomponenten einen dieser 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 Maßnahmenwarnungsfilter**.

   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 **Warnungskategoriekonfiguration** markieren Sie entweder **Alle auswählen** oder wählen die Ereigniskategorien, die in den Warnungsfiltern enthalten sein sollen.

   Sabine markiert **Alle auswählen**, da sie von jedem Warnungs- oder kritischen Ereignis benachrichtigt werden möchte, das ihre Netzwerkschalter oder Server beeinflusst.

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

   Sabine markiert **Server und Netzwerkgeräte**.

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.

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.

9. Die **Zusammenfassung für Neuer Filter** zeigt Ihre Auswahl. Klicken Sie auf **Fertig stellen**, um anzunehmen oder auf **Zurück**, um Änderungen vorzunehmen.

10. 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:

1. Wählen Sie **Warnungen**→ **Maßnahmen** aus der Menüleiste aus.
2. Klicken Sie mit der rechten Maustaste auf **Warnungsmaßnahmen** in der Navigationsleiste und wählen Sie **Neue Warnungsmaßnahme**.

   Der **Assistent Warnungsmaßnahme hinzufügen** wird eingeblendet.

3. Geben Sie der Maßnahme einen logischen Gerätenamen im Feld **Name**.
4. Wählen Sie **E-Mail** im Pull-Down-Menü **Typ**.

   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 und 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 EnterpriseOID, Allgemeine TrapId bzw. Spezifische Trap-ID des Original-Trap haben. Diese Werte werden in der Beschreibung des weitergeleiteten Traps erscheinen.

5. Im **E-Mail-Konfigurations**dialog, geben Sie eine gültige E-Mail-Adresse (innerhalb der SMTP-Servergruppe Ihres Unternehmens) an, 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 Onlinehilfe von IT Assistant.

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

   Sabine wählt *Sabines Netzwerk - Warnung und Kritisch*, der Name, den sie dem zuvor eingerichteten Warnungsmaßnahmenfilter gegeben hat.

7. Ein Zusammenfassungsdialog zeigt Ihre Auswahl. Klicken Sie auf **Fertig stellen**, um anzunehmen oder auf **Zurück**, um Änderungen vorzunehmen.

   Überprüfen Sie, ob der Name der Warnungsmaßnahme, den Sie in Schritt 3 zugewiesen haben, im Fenster **Zusammenfassung der Warnungsmaßnahmen** erscheint.

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 eine Warnung 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. Aus- und Einschalten bzw. Herunterfahren der Systeme 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:

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

Ermittlungszyklus 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 des Ermittlungszyklus für seine Server muss er die folgenden Aufgaben durchführen:

- Subnetzbereiche, IP-Adressen und/oder Host-Namen für die zu überwachenden Server festlegen.
- Die Subnetzbereiche, Host-Namen oder IP-Adressen festlegen, die nicht überwacht werden sollen.
- Öffentliche (Get) und private (Set) Community-Namen für SNMP festlegen, die für das Netzwerk verwendet werden sollen.
- SNMP-Agenten und SNMP-Dienst des Betriebssystems auf jedem zu überwachenden System installieren und konfigurieren.
- 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 4-2 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 öffentliche und private 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 private Community-Namen für bestimmte Datenzentrum einrichten möchte.

ANMERKUNG: IT Assistant bietet ein Fehlerbehebungs-Hilfsprogramm 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 Fehlerbehebungs-Hilfsprogramm 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 Serververwaltbarkeit konfigurieren (beide Szenarien)".

Tabelle 4-2 enthält Informationen zu den von Christian überwachten Remote-Systemen.

Tabelle 4-2. Beispiele für Subnetzbereiche, IP-Adressen oder Host-Namen sowie entsprechende Informationen zu Datenzentrums- und Remote-Servern

Systemgruppenname	Subnetzbereich einschließen	Hosts oder Subnetzbereich ausschließen	Öffentliche/private Community-Namen	Anzahl der Server im Subnetz	Längste ermittelte Ping-Antwortzeit in einem Subnetz
Datenzentrum-Server 1	192.166.153.*	192.166.153.2	dcp123/dcsecure01	100	64
Datenzentrum-Server 2	192.166.154.*	examplehost	dcp123/dcsecure02	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

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: Bestandsaufnahmenkonfiguration

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 zur Definition von Ermittlungsbereichen.

Ermittlungseinstellungen 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 werden auf die entsprechenden Ermittlungsbereiche angewendet, die er später im Verfahren erstellt. Er kann diese Werte jedoch jederzeit mit diesem Dialogfeld ändern.

So werden Ermittlungseinstellungen für große Unternehmen in IT Assistant konfiguriert:

1. Wählen Sie **Ermittlung und Überwachung**→ **Ermittlungskonfiguration** aus der IT Assistant-Menüleiste aus.

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

2. Unter **Geräteermittlung einleiten**, wählen Sie 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. Der Netzwerkverkehr ist zu dieser Zeit am geringsten.

3. Bestimmen Sie über den Schieberegler unter **Ermittlungsgeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die für die Ermittlung zur Verfügung gestellt werden sollen.

   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 Systemleistung drastisch beeinflusst, während er versucht, andere Tasks auf dem System auszuführen, kann er die **Ermittlungsgeschwindigkeit** für nachfolgende Ermittlungen so ändern, dass weniger Netzwerkressourcen verbraucht werden.

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

   DNS (Domänennamesystem) -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. Klicken Sie auf **OK**.

Bestandsaufnahmeeinstellungen konfigurieren

Als nächstes gibt Christian die Einstellungen der Bestandsaufnahme ein. IT Assistant sammelt Bestandsaufnahmeninformationen 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 Reporte verwendet werden.

So werden Bestandsaufnahmeeinstellungen eingestellt:

1. Wählen Sie **Ermittlung und Überwachung**→ **Bestandsaufnahmekonfiguration** aus der Menüleiste aus.

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

2. Im Dialogfeld unter **Bestandsaufnahme einleiten** wählen Sie 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. Bestimmen Sie über den Schieberegler unter **Bestandsaufnahmegeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die für die Bestandsaufnahme zur Verfügung gestellt werden sollen.

   ANMERKUNG: Je höher Sie die Bestandsaufnahmegeschwindigkeit einstellen, desto mehr Netzwerk-Ressourcen wird die Ermittlung verbrauchen. Höhere Bestandsaufnahmegeschwindigkeiten können die Netzwerkleistung negativ beeinflussen.

4. Klicken Sie auf **OK**.

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.

So werden Statusabfrageeinstellungen eingestellt:

1. Wählen Sie **Ermittlung und Überwachung**→ **Statusabfragekonfiguration** aus der Menüleiste aus.

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

2. Unter **Bestandsaufnahme der Statusabfrage**, wählen Sie aus, welches Intervall IT Assistant zur Ausführung der Statusabfrage verwenden soll.
3. Bestimmen Sie über den Schieberegler unter **Statusabfragegeschwindigkeit** die Netzwerkbandbreite sowie die Systemressourcen, die für die Statusabfrage zur Verfügung gestellt werden sollen.

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

4. Klicken Sie 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 verwendet die IP-Subnetzbereiche, die er für seine Server notiert hat (siehe Tabelle 4-2).

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.

So legen Sie einen *Einschluss*bereich fest:

1. Wählen Sie **Ermittlung und Überwachung**→ **Bereiche** aus der Menüleiste aus.

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

2. Erweitern Sie **Ermittlungsbereiche**, klicken Sie mit der rechten Maustaste auf **Einschlussbereiche** und wählen Sie **Neuer Einschlussbereich**.

   Der **Assistent Neue Ermittlung** startet.

3. In Schritt 1 des Assistenten geben Sie eine IP-Adresse (bzw. einen Bereich) oder einen Host-Namen ein und klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

   Basierend auf den Informationen zu Christians Systemen in Tabelle 4-2 muss er diesen Assistenten zweimal abschließen, um alle Systeme einzuschließen. Das erste Mal gibt er folgendes ein:

   192.166.153-161.*

   Das zweite Mal gibt er folgendes ein:

   10.9.72-73.*

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-Online-Hilfe. Die Datei **importnodelist.exe** befindet sich im Verzeichnis **/bin**.

4. In Schritt 2 des Assistenten, geben Sie die Internetsteuerungs-Meldungsprotokoll (ICMP) -Zeitüberschreitung ein und versuchen den Bereich erneut.
5. In Schritt 3 des Assistenten, konfigurieren Sie die SNMP-Parameter, die während der Ermittlung verwendet werden sollen:
   - Stellen Sie sicher, dass die Option **SNMP-Ermittlung aktivieren** ausgewählt ist.
   - Geben Sie 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 Assistant 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 Assistant zugewiesen wurden.

   - Geben Sie 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.

   - Zeitüberschreitungs- und Wiederholungswert für den SNMP-Ermittlungsbereich eingeben. Für Christians Netzwerktyp sind die Standardwerte gewöhnlich eine gute Wahl.
6. In Schritt 4 des Assistenten, konfigurieren Sie die CIM-Parameter, die während der Ermittlung verwendet werden sollen.

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

   - Stellen Sie sicher, dass **CIM-Ermittlung aktivieren** ausgewählt ist.
   - In **Domäne\Benutzername**, geben Sie denselben Namen ein, den Sie zur CIM-Konfiguration auf dem verwalteten System verwendet haben.
   - Geben Sie dasselbe **Kennwort** ein, das Sie als CIM Kennwort auf dem verwalteten System verwendet haben.
7. In Schritt 5 des Assistenten, wählen Sie, welche Maßnahme IT Assistant nach Beendigung des Assistenten ausführen wird.
8. In Schritt 6 des Assistenten, sehen Sie sich Ihre Auswahl noch einmal an und wählen **Fertig stellen**, um den Assistenten abzuschließen oder **Zurück**, um die Auswahl zu ändern.

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.

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

   Das Dialogfeld **Neuer Ausschlussbereich** wird eingeblendet.

3. Er 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 ausführen.

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:

1. Eine benutzerdefinierte Gruppe für die Datenzentrumsserver sowie eine benutzerdefinierte Gruppe für die Remote-Server zu erstellen.
2. Einen Warnungsmaßnahmenfilter für jeden der vier Administratoren, die Christian bei den Remote- und Datenzentrumsservern an verschiedenen Tagen und in verschiedenen Schichten unterstützen, zu erstellen.
3. 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)
- Bettina hat an Wochenenden von Freitags 19 Uhr bis Montags 7 Uhr Bereitschaft

Deshalb will Christian IT Assistant so konfigurieren, dass:

- Thomas, Sven und er selbst jedes Mal durch E-Mail benachrichtigt werden, wenn Warnungs- oder kritische Ereignisse bei Datenzentrumsservern eintreten
- 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 Techniker, die bei kritischen und Warnungsereignissen seiner 1,000 Server Maßnahmen ergreifen. Bei den benutzerdefinierten Gruppen handelt es sich um Remote-Server und Datenzentrumsserver.

1. Wählen Sie **Ansicht**→ **Geräte** aus der Menüleiste des IT Assistant aus.
2. Klicken Sie mit der rechten Maustaste den Stamm der obersten Ebene in der IT Assistant-Navigationsstruktur und wählen Sie **Neue Gruppe**.

   Der **Assistent Gruppe hinzufügen** wird eingeblendet.
3. Geben Sie in einen Namen und eine Beschreibung für die Gruppe ein, die Sie hinzufügen wollen.

   Christian nennt seine Gruppe **Datenzentrumsserver**.
4. Im Dialog **Gruppenmitgliedschaft** wählen Sie entweder die Geräte aus, die in der neuen Gruppe eingeschlossen sein sollen, oder, wenn es sich um eine abfragebasierte Gruppe handelt, wählen Sie die Abfrage aus dem Pull-Down-Menü aus.
5. Sehen Sie sich im Zusammenfassungsbildschirm Ihre Auswahl noch einmal an und wählen Sie **Fertig stellen**, um den Assistenten abzuschließen oder **Zurück**, um die Auswahl zu ändern.
6. Wiederholen Sie 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.

So wird ein Warnungsmaßnahmenfilter erstellt:

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

   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 Maßnahmenwarnungsfilter**.

   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:

- Datenzentrum erste Schicht (M-F, 7-19 Uhr)
- Datenzentrum zweite Schicht (M-F, 19-7 Uhr)
- Wochenend-Administrator (Samstag und Sonntag, 24 Stunden)

3. Geben Sie 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. Wählen Sie unter **Schweregrad** den Schweregrad der Ereignisse aus, für die Warnungen und Protokolle empfangen werden sollen.

   Für den Filter DZ 1. Schicht wählt Christian **Warnung** und **Kritisch**.

   Klicken Sie auf **Weiter**.

5. Unter **Warnungskategoriekonfiguration** markieren Sie entweder **Alle auswählen** oder wählen Sie die Ereigniskategorien, die in den Warnungsfiltern enthalten sein sollen.

   Christian markiert **Alle auswählen**, weil er alle Server in seinem Unternehmen überwachen will.

6. Unter **Geräte-/Gruppenkonfiguration** wählen Sie den Namen des Geräts oder der Gruppe aus, das/die dem neuen Maßnahmenwarnungsfilter zugeordnet werden sollen.

   Christian wählt **Datenzentrumsserver**, der Name einer der benutzerdefinierten Gruppen die er zuvor erstellt hat.

7. Unter **Datum/Uhrzeit-Bereichskonfiguration** geben Sie die Werte für einzelne oder alle optionalen 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 Dienstanbieter 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 aktiviert Christian den Zeitbereich 00:00:00 Uhr bis 12:00:00 Uhr sowie die Tage Samstag und Sonntag.

8. Unter **Warnungsmaßnahmenverbindung** wählen Sie, ob das durch den Filter erfasste Ereignis eine Warnung auslösen oder ob es 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.

9. Die **Zusammenfassung für Neuer Filter** zeigt Ihre Auswahl. Klicken Sie auf **Fertig stellen**, um anzunehmen oder auf **Zurück**, um Änderungen vorzunehmen.
10. Überprüfen Sie, ob der Name des Filters, den Sie in Schritt 3 zugewiesen haben, im Fenster **Zusammenfassung der Warnungsmaßnahmenfilter** erscheint.

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:

- 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
- 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 erstens 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 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**.

Warnungsmaßnahme erstellen

So wird eine Warnungsmaßnahme erstellt:

1. Wählen Sie **Warnungen→ Maßnahmen** aus der Menüleiste aus.
2. Klicken Sie mit der rechten Maustaste auf **Warnungsmaßnahmen** in der Navigationsleiste und wählen Sie **Neue Warnungsmaßnahme**.

   Der **Assistent Warnungsmaßnahme hinzufügen** wird eingeblendet.
3. Geben Sie der Maßnahme einen logischen Gerätenamen 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**:

   - Christian ADMIN MGR E-Mail
   - DZ 1. Schicht Thomas E-Mail
   - DZ 2. Schicht Sven E-Mail
   - Wochenende Admin Bettina E-Mail
4. Wählen Sie **E-Mail** im Pull-Down-Menü **Typ**.
5. Im **E-Mail-Konfigurations**dialog, geben Sie eine gültige E-Mail-Adresse (innerhalb der SMTP-Servergruppe Ihres Unternehmens) an, 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.
6. In **Warnungsfilterverbindung** legen Sie den Warnungsmaßnahmenfilter fest, der diese E-Mail auslösen wird.

   Christian gibt die Namen der Warnungsfilter, die er im vorherigen Verfahren eingerichtet hat - entweder **DZ 1. Schicht**, **DZ 2. Schicht** oder **Wochenende Admin** - dabei führt er jedes Mal diesen Schritt aus.
7. Ein Zusammenfassungsdialog zeigt Ihre Auswahl. Klicken Sie auf **Fertig stellen**, um anzunehmen oder auf **Zurück**, um Änderungen vorzunehmen.

   Überprüfen Sie, ob der Name der Warnungsmaßnahme, die Sie in Schritt 3 definiert haben, im Fenster **Zusammenfassung der Warnungsmaßnahmen** erscheint.

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

- IT Assistant wird unaufhörlich alle Server auf Christians Netzwerk überwachen.
- 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.
- 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.

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

Zurück zum Inhaltsverzeichnis

Berichterstattung und Task-Verwaltung

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

Dell OpenManage™ IT Assistant hat die Befähigung:

- Benutzerspezifische Report für alle Systeme in Ihrem Unternehmen zu erstellen
- Befehlszeilenausführung auf verwalteten Geräten von einer zentralen Konsole aus durchzuführen, einschließlich Herunterfahren und Hochfahren
- Software-Übereinstimmungsprüfungen und -Aktualisierungen auf einem einzelnen verwalteten System durchzuführen

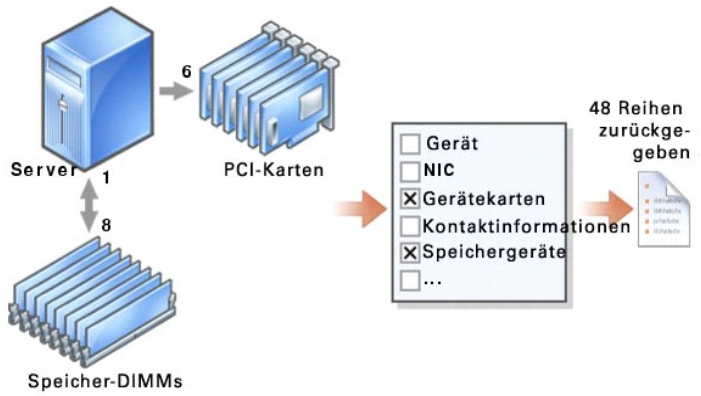
Die Grundlagen dieser Fähigkeiten sind hier mithilfe der gleichen Benutzerszenarien angezeigt, welche in "IT Assistant zur Überwachung Ihrer Systeme konfigurieren" dargestellt sind. Detailliertere Informationen zu diesen Themen finden Sie in der IT Assistant-Online-Hilfe.

Benutzerdefinierte Berichterstattung

IT Assistant verwendet Daten der Microsoft® Data Engine (MSDE) oder der SQL-Server-Datenbank, um benutzerdefinierte 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 5-1. Benutzerdefinierte Berichterstattung im IT Assistant



Zum Beispiel können Sie einen Report zusammenstellen, der folgendes enthält:

- Details zu den Hardwaregeräten, die von IT Assistant verwaltet werden, einschließlich Servern, Schalter und Speichergeräte
- BIOS-, Firmware- und Treiber-Versionen, die auf bestimmten Geräten enthalten sind
- 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** 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 :

   - Einen **Namen** für ihren Report, der nicht länger als 64 Zeichen sein darf
   - Eine optionale **Beschreibung**
3. In diesem Fall wird sie **Geräte/Gruppen aus der Struktur unten auswählen** aussuchen und dann **Server** aus der Liste verfügbarer Geräte.

ANMERKUNG: Die Auswahl des Attributs der höchsten Ebene in der Geräteliste bedeutet die automatisch 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 gilt die Auswahl für die modifizierten Gruppenmitglieder, wenn sich die Gruppenmitgliedschaft ändert.

4. Unter **Attribut auswählen** sucht sie **NIC** aus.
5. Dann gibt sie in **Sortieren nach** an, welche Reihenfolge sie in der Sortierung bevorzugt.
6. Unter **Zusammenfassung** akzeptiert sie entweder ihre Auswahl oder sie geht zurück und ändert sie.
7. Wenn sie ihre Konfiguration bestätigt hat, wechselt sie zum Fenster Reporte im IT Assistant, klickt mit der rechten Maustaste auf den Reportnamen, den sie erstellt hat, und wählt **Ausführen**→ **HTML-Reporte**.

   Ein auf HTML basierter Report mit NIC-Geräteinformationen zu jedem der 50 PowerEdge-Server des Unternehmens wird angezeigt.

Einen abfragebasierten Report wählen:

Sabine konnte 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 5-1. Abfragereportparameter

Name der Abfrage	Gibt den Namen der Abfrage an.
Abfragekriterien	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 (Wo: die IP-Adresse beginnt mit 143.166.155)` Die Abfrage-Operatoren sind: - Enthält - legt fest, dass die Abfragekriterien-Zeichenkette einen bestimmten Satz von Zeichen enthält. - Endet mit - legt fest, dass die Abfragekriterien mit einem bestimmten Satz von Zeichen enden. - Ist - legt fest, dass die Abfragekriterien-Zeichenkette mit diesen Zeichen genau übereinstimmt. - Beginnt mit - legt fest, dass die Abfragekriterien-Zeichenkette mit diesen Zeichen beginnt. Sie können die Abfrage mit bis zu 10 Unterabfragen erweitern, die zusammen die gesamte Abfrage ausmachen. Sie verbinden die Unterabfragen mit UND/ODER-Operatoren.

	ANMERKUNG: Wenn Sie irgendwelche Änderungen vornehmen während Sie eine bestehende Abfrage bearbeiten und diese Abfrage speichern, wird die ursprüngliche Abfrage ersetzt.
Abfrage ausführen	Führt die Abfrage aus und zeigt die Ergebnisse.
Abfrage speichern	Speichert die Abfrage.
Abbrechen	Schließt das Fenster **Abfragebearbeiter** 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
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

Die Reihen in der Tabelle der Geräteoptionen stehen für die Geräte im Netzwerk. 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 5-2. IT Assistant-Datenbank-Schemainformationen

Spaltenname	Datentyp	Datengröße	Nullen zugelassen	Beschreibung
Tabelle der Geräteoptionen				
DeviceId*	int	4	Nein	Interne Geräteidentifikation, die in allen zugehörigen Tabellen verwendet wird.
DeviceName	nvarchar	256	Ja	Der von IT Assistant zur Kennzeichnung der Geräte verwendete Name, welcher in der **Gerätestruktur** der Benutzeroberfläche (UI) gezeigt wird.
DeviceInstrumentationName	nvarchar	256	Ja	Der Name des Geräts, der von MIB II SysName oder von CIM abgerufen wird.
DeviceDNSName	nvarchar	256	Ja	Name des Computersystems
DeviceType	int	4	Ja	Der Gerätetyp. Workstation = 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
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 Boolean-Flag, die anzeigt, ob ein Gerät ein von Dell aktivierter Agent ist.
SubnetLastDiscoveredOn	nvarchar	256	Ja	Der Ermittlungsbereich, der zur letzten Ermittlung des Geräts verwendet wurde.
Tabelle der Agentenoptionen				
DeviceId*	int	4	Nein	Fremdschlüssel zur Tabelle der Geräteoptionen.
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. Band-externer RAC-Agent = 1 Server Administrator = 2 Microsoft WMI =3 OMCI = 4 DRAC II = 5 Array Manager = 6 Storage Manager = 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 Band-interner RAC-Agent = 17
AgentURL	nvarchar	256	Ja	Die Webadresse zur Verwaltungsanwendung (wenn der Agent eine Webadresse unterstützt).
AgentData	ntext	16	Ja	Erweiterte Agentendaten; nur zum internen Gebrauch.
Tabelle der Array-Festplattenoptionen				
DeviceId*	int	4	Nein	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 Händlers der Array-Festplatte.
ArrayDiskModelNumber	nvarchar	64	Ja	Die Modellnummer der Array-Festplatte.
ArrayDiskSerialNumber	nvarchar	64	Ja	Die eindeutige Herstelleridentifikationsnummer 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 Megabytes. Bei einer Größe von 0 ist sie kleiner als ein Megabyte.
ArrayDiskBusType	nvarchar	64	Ja	Der Bustyp der Array-Festplatte. Mögliche Werte: SCSI, IDE, Fibre Channel, SSA, USB, 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.
Tabelle der Controller-Optionen				
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.
Tabelle der Gehäuseoptionen				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
EnclosureNumber*	int	4	Nein	Die Instanznummer dieses 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.
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 Gehäusetyp entspricht.
EnclosureType	nvarchar	64	Ja	Der Gehäusetyp.
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.
Tabelle der Gehäusemanagementmodul-Optionen				
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.
Tabelle der virtuellen Laufwerkoptionen				
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 dieses virtuellen Laufwerks in Megabytes.
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.
VirtualDiskTargetId	int	4	Ja	Die eindeutige ID des virtuellen Laufwerks.
Tabelle der Datenträgeroptionen				
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.
Tabelle der Firmware-Optionen				
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
Tabelle der Speichergeräteoptionen				
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.
Tabelle der NIC-Optionen				
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.
Tabelle der Betriebssystemoptionen				
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.
Tabelle der Netzteiloptionen				
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.
Tabelle der Prozessoroptionen				
DeviceId*	int	4	Nein	Der Fremdschlüssel zur Tabelle der Geräteoptionen.
ProcessorChassisIndex*	int	4	Nein	Dieses Attribut definiert den Index (einsbasiert) des Gehäuses.
ProcessorCores	int	4	Ja	Dieses Attribut definiert die Anzahl der ermittelten Prozessorkerne für das Prozessorgerät.
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.
Tabelle der SMBIOS-Optionen				
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 Nur-Lesen eingestellt ist.
BuiltinPointingDevice	nvarchar	64	Ja	Legt fest, ob die Schnittstelle des integrierten Zeigegeräts (die Maus) aktiviert oder deaktiviert ist.
WakeupOnLAN	nvarchar	64	Ja	Definiert, ob Wake Up On LAN deaktiviert ist, bzw. ob es nur für integrierte NIC oder nur für Add-in-NIC aktiviert ist. Bei Auswahl der Option **Aktiviert mit Start zum NIC**, startet das System nach einer Remote-Aktivierung von der NIC-Start-ROM.
WakeupOnLANMethod	nvarchar	64	Ja	Definiert die vom System unterstützte Wake Up 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 zu welcher Minute das System eingeschaltet wird (0-23).
BootSequence	nvarchar	64	Ja	Definiert die Startsequenz für den nächsten Systemstart.
ChassisIntrusionStatus	nvarchar	64	Ja	Meldet den Status des Systems in Bezug zum **Gehäuseeingriff** (**Ermittelt** oder **Nicht ermittelt**). Der Wert **Unbekannt** 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 **Ermittelt** ist, können Sie ihn auf **Nicht ermittelt** 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-In-PCI-Steckplätze des Systems (aktiviert/deaktiviert).
USBPorts	nvarchar	64	Ja	Der Status der USB-Schnittstellen (ein/aus).
Tabelle der Software-Bestandsaufnahmeoptionen				
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-Gerätekennzeichner der PCI-ID.
HWVendorId	nvarchar	16	Ja	Der Hardware-Herstellerkennzeichner der PCI-ID.
HWSubDeviceId	nvarchar	16	Ja	Der Hardware-Untergerätekennzeichner der PCI-ID.
HWSubVendorId	nvarchar	16	Ja	Der Hardware-Unterherstellerkennzeichner 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.
Tabelle der Software-Bestandsaufnahme-Betriebssystemoptionen				
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.
Tabelle der Schaltergeräteoptionen				
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.
Tabelle der Betriebskostenoptionen				
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 Betriebssystemname 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.
Tabelle der Kontaktinformationsoptionen				
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.
Tabelle der Cluster-Optionen				
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.

Software-Aktualisierungen

IT Assistant bietet eine zentralisierte Software-Aktualisierungsfähigkeit. Sie können Dell Update Packages und System Update Sets in ein zentrales Repository laden und dann prüfen, ob alle Systeme im Unternehmen mit den Aktualisierungspaketen übereinstimmen. Ein System Update Set ist ein logischer Satz von Dell Update Packages, die so konstruiert sind, dass sie Paketablaufsteuerung aktivieren und Systemneustarts minimieren. Dell Update Packages sind auf der Dell Support-Website unter **support.dell.com** oder auf der CD *Dell PowerEdge Updates* verfügbar. Diese CD ist über den Abonnement-Dienst von Dell OpenManage erhältlich oder als kann als ein ISO-Image von **support.dell.com** heruntergeladen werden. Der OpenManage Subscription Service kann von **www.dell.com** heruntergeladen werden.

Die CD *Dell PowerEdge Updates* CD enthält vierteljährliche Aktualisierung für die Dell Update Packages und System Update Sets (zertifizierte Paketsätze für spezifische PowerEdge-Plattformen).

Zur Verwendung der Dell Update Packages im IT Assistant, führen Sie folgende Schritte durch:

1. Navigieren Sie zu **Verwalten→ Softwareaktualisierungen**.
2. Klicken Sie mit der rechten Maustaste auf den Stammknoten (**Softwareaktualisierungs-Repositorys**) und wählen Sie **Repository öffnen (Aktualisierungs-CD)...**".
3. Legen Sie die CD *Dell PowerEdge Updates* in das CD-Laufwerk ein.
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 Updates* ist innerhalb des IT Assistant verfügbar. Sie können Vorgänge wie den Import von Paketen sowie die Ausführung von Übereinstimmungsprüfungen und Softwareaktualisierungen durchführen.

Softwareaktualisierungen im IT Assistant verwenden

Lassen Sie uns ansehen, wie Sabine diese Funktion in ihrem Unternehmen verwenden könnte.

Sabine hat ein Aktualisierungspaket von der Dell Support-Website unter **support.dell.com** heruntergeladen. Sie weiß, dass einige ihrer Systeme die Firmware-Aktualisierung benötigen, die darin enthalten ist, aber sie möchte gerne feststellen welche dies sind, ohne jeden der 50 Server manuell zu überprüfen. Sie kann IT Assistant verwenden, um dies schnell herauszufinden.

So würde sie vorgehen:

1. Sie wählt **Verwalten** → **Softwareaktualisierungen**.
2. Sie klickt mit der rechten Maustaste auf **IT Assistant-Repository** im linken Navigationsfenster und wählt **Hinzufügen**.

   Sabine navigiert zu dem Standort auf ihrem System, wo sie das Aktualisierungspaket gespeichert hat. Das Paket kann eine **catalog.xml**-Datei oder ein anderer Dateiname auf einer CD sein. Wenn sie den Dateinamen markiert und auf **Öffnen** klickt, fügt der IT Assistant es zum Fenster hinzu.
3. Durch Klicken des Aktualisierungspaketnamens 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 Aktualisierungspakets gewählt hat.

   IT Assistant führt einen Vergleich durch und erstellt einen Übereinstimmungsreport, der die gefundenen Unterschiede durch Symbole darstellt, vollständige Versionsinformationen zu den ausgesuchten Geräten gibt, sowie andere Informationen, die bei der Identifizierung von nicht übereinstimmenden Systemen oder Geräten helfen.
6. Wenn IT Assistant Server oder Geräte findet, die aktualisiert werden müssen, wählt Sabine aus, welche sie aktualisieren möchte, und klickt dann 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.

Tasks verwalten

IT Assistant ermöglicht Ihnen auch, bestimmte Tasks auf verwalteten Systemen im gesamten Unternehmen im Remote-Zugriff auszuführen. Diese Tasks umfassen:

- 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)
- Gerätesteuerung, einschließlich Herunterfahren und Hochfahren
- Geplante Software-Aktualisierungen
- Die Fähigkeit, Intelligente Plattformverwaltungsschnittstelle (IPMI) -Befehle im Remote-Zugriff auszuführen
- Die Fähigkeit, Remote-Client-Instrumentationsbefehle im Remote-Zugriff auszuführen

ANMERKUNG: Die Befehlszeilenoptionen IPMI und Remote-Client-Instrumentation sind eventuell nicht verfügbar, wenn IT Assistant die Installation der notwendigen Komponenten in der IT Assistant-Dienstestufe nicht ermittelt.

Diese Tasks können so konfiguriert werden, dass sie nach einem festgelegten Plan oder sofort ausgeführt werden. Weitere Informationen finden Sie in der IT Assistant-Online-Hilfe.

Gerätesteuerungs-Task erstellen

Sabine will z. B. einen problematischen Server neu starten, der mehrere E-Mail-Warnungen durch T Assistant ausgegeben hat. Um diesen Task im IT Assistant auszuführen, würde sie wie folgt vorgehen:

1. Sie wählt **Verwalten** → **Tasks** und klickt im linken Navigationsfenster mit der rechten Maustaste auf **Gerätesteuerung**.
2. Wählen Sie **Neuer Task**.

   Der Task-Erstellungsassistent startet.
3. Sabine gibt einen **Task-Namen** ein und wählt dann **Gerät herunterfahren** aus dem Pull-Down-Menü **Task-Typ**.
4. Sie wählt **Neustarten** im Fenster **Art des Herunterfahrens auswählen**.
5. Im Fenster **Geräte auswählen** erweitert sie die **Server**geräteliste 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 ihre Auswahl oder wählt **Zurück**, um Änderungen vorzunehmen.

   Der von ihr bestimmte Server beginn 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 Assistant verfügbare Tasks

Andere im IT Assistant 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 Assistant akzeptierten Argumente finden Sie in der Online-Hilfe.

Software-Aktualisierung

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 IT Assistant-Online-Hilfe.

IPMI-Befehlszeile

Die Auswahl von **IPMI-Befehlszeile** aus dem Pull-Down-Menü ermöglicht Ihnen, IPM-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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sichere Dell OpenManage IT Assistant Installation sicherstellen

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

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 und das Active Directory von Microsoft® für den funktionsbasierten Zugriff ein.

Ausführliche Informationen zur Sicherheit in der gesamten Dell OpenManage-Plattform, einschließlich IT Assistant, finden Sie im *Dell OpenManage Installations- und Sicherheitsbenutzerhandbuch*.

TCP/IP-Paket-Anschlusssicherheit

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 Standardschnittstellennummer ist 2607. 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 durch die IT Assistant-Anmeldungsseite authentifiziert und ihre Anmeldeinformationen anhand der im Active Directory oder dem lokalen Betriebssystem zugeordneten Funktion überprüft. Informationen zu den drei von IT Assistant unterstützten Funktionen finden Sie unter "Rollenbasierter Zugriff - Sicherheitsverwaltung".

ANMERKUNG: Die IT Assistant-Benutzeroberfläche kommuniziert mit der IT-Dienstestufe 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. Siehe die **Microsoft Website**. Führen Sie diese Aktualisierungen auch für andere Betriebssysteme der verwalteten Systeme durch.

Sitzungszeitlimit

Eine IT Assistant-UI-Sitzung kann so konfiguriert werden, dass das Zeitlimit nach einer festgelegten Periode der Untätigkeit erreicht wird. Um das Sitzungszeitüberschreitungsintervall zu konfigurieren, klicken Sie auf **Einstellungen** auf der oberen IT Assistant-Navigationsleiste und wählen **Web Servereigenschaften**. Sie können die Sitzungszeitüberschreitung entweder ganz deaktivieren oder bis zu 30 Minuten Untätigkeit zulassen.

Die Protokolle ASF und SNMP

Eine abschließende Sicherheitsmaßnahme, eingeführt mit den Dell™ OptiPlex™ GX260-Systemen, ist der integrierte NIC (Network Interface Controller [Netzwerkschnittstellen-Controller]), der Unterstützung für ASF (Alert Standard Format [Warnungsstandardformat]) enthält. 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:

- Stellen Sie sicher, dass das Betriebssystem mit den neuesten Sicherheitspatches aktualisiert wurde.
- 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. Für die Betriebssysteme Red Hat® Linux und Novell® NetWare® sollte überprüft werden, ob ähnliche Dienste verfügbar sind.

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 (Benutzer-ID/Kennwort) an. Des weiteren wird die Verbindung zum verwalteten System über Domäne/Benutzer-ID/Kennwort-Konten hergestellt, die in jedem der konfigurierten IT Assistant-Ermittlungsbereiche angegeben werden. Das Format für diese Konten ist **<Domänenname>\<Benutzername>** oder **localhost (lokaler Host) \<Benutzername>**.

ANMERKUNG: Die WMI-Sicherheit kann mithilfe von Dienstprogrammen wie z. B. **dcomcnfg.exe**, **wmimgmt.msc** und **wbemcntl** 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 die folgenden Beispiele auf Microsoft Windows Betriebssysteme ausgerichtet sind, sind für die Betriebssysteme Red Hat Linux und Novell NetWare ähnliche Schritte erforderlich. 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 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 dieser Hosts annehmen** auswählen und dann auf **Hinzufügen** klicken, um die Adresse bzw. den Namen des Systems einzugeben, auf dem IT Assistant ausgeführt wird.

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 **Benutzerzugriffs**felder aufheben. Der Benutzerzugriff kann auch über den CLI-Befehl des Server Administrators **omconfig preferences useraccess enable= admin** eingeschränkt werden. Weitere Informationen finden Sie im *Server Administrator-Befehlszeilenschnittstelle: Benutzerhandbuch* unter **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:

- Stellen Sie sicher, dass das Betriebssystem mit den neuesten Sicherheitspatches aktualisiert wurde.
- Verwenden Sie das SNMP- und CIM- (Server Administrator) Protokoll.
- Führen Sie schwer zu erratende SNMP-Community-Namen ein.
- Konfigurieren Sie SNMP für den **Nur-Lese**-Zugriff, um nur den Server Administrator Konfigurationen, Aktualisierungen und Steuerung des Netzstroms durchführen zu lassen.
- Konfigurieren Sie SNMP so, dass Anfragen nur von der IP-Adresse des Systems angenommen werden, auf dem IT Assistant ausgeführt wird.
- Verwenden Sie Hilfsprogramme wie z. B. Group Policies in Active Directory, um die SNMP-Einstellungen für alle zu verwaltenden Server zu erzwingen.
- Konfigurieren Sie Server Administrator so, dass der Zugriff auf Benutzerebene verweigert wird.

Datenbanksicherheit bei Einsatz des IT Assistant sicherstellen

Wenn bei der Installation des IT Assistant keine SQL-Server-Datenbank ermittelt wurde, wird eine Kopie von MSDE 2000 installiert, das auf den Authentifizierungsmodus Vertraut 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 des IT Assistant installiert sind, wurde das Supervisor- bzw. das Konto-Kennwort entweder auf `null` oder `dell` 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 Vertraut oder Nur Windows zu ändern.

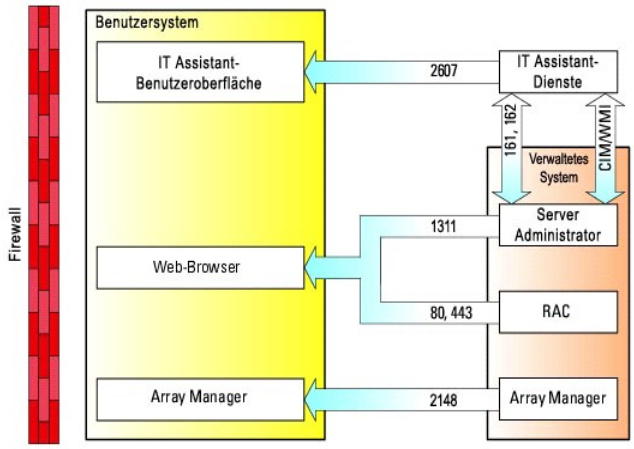
IT Assistant hinter einer Firewall ausführen

Abbildung 6-1 zeigt eine typische Installation, bei der sowohl der IT Assistant als auch die zu verwaltenden Systeme hinter einer Firewall liegen. 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.:

- Verwendung vertrauter Konten anstelle von benannten oder gemischten Konten für die Datenbank.
- Begrenzung von Benutzeroberflächenverbindungen zu einem bekannten System.

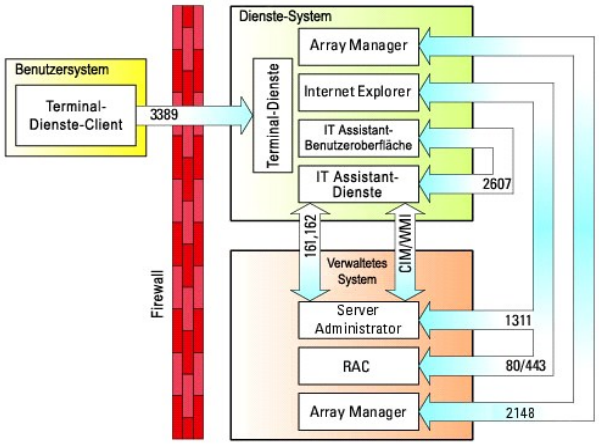
Abbildung 6-1. Typische Installation hinter einer Firewall



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 Sicherheitsmaßnahmen stehen die Microsoft Terminaldienste zur Verfügung, mit denen unangemeldete Remote-Verbindungen nur von Benutzern mit Administratorkonten (administrativer Modus) hergestellt werden können, und die ebenfalls zur Begrenzung der Verbindungen über eine Benutzeroberfläche zu einem System verwendet werden, auf dem die IT Assistant-Benutzeroberfläche und die Dienste ausgeführt werden. Das Beispiel eines Netzwerks, das die Terminaldienste nutzt, wird in Abbildung 6-2 dargestellt.

Abbildung 6-2. Verwendung von Terminaldiensten für zusätzliche Sicherheit



In Abbildung 6-2 könnte ein Benutzer die Verbindung zur IT Assistant-Verwaltungsstation über einen lokal installierten Terminaldienste-Client oder über eine Windows XP-Remote-Desktop-Verbindung herstellen. Für diese Verbindung ist gültige Domäne/Benutzer-ID/Kennwort erforderlich. Weitere Informationen finden Sie auf der Website von Microsoft.

Die zusätzliche Sicherheitsstufe wird erreicht, indem auf allen verwalteten Systemen Beschränkungen eingerichtet werden, damit ausschließlich SNMP-Verkehr von der IP-Adresse des Systems, auf dem die IT Assistant-Benutzeroberfläche ([UI] die Netzwerkverwaltungsstation) ausgeführt wird, zugelassen ist. 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-Administratorgruppen anmelden und es werden mehr als zwei Sitzungen unterstützt. Die Installation im Anwendungsmodus enthält jedoch zusätzliche Lizensierungsanforderungen. 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 Anschluss 2607 der IT Assistant-Dienstestufe sowie der Anschlüsse 1311, 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 zulassen.

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 einmalige 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 **Extras** im Menü **Hilfsprogramme**.
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 authentisiert.

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 "Gast- 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 zuweisen für unterstützte Windows Server 2003-Betriebssysteme

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**.

HINWEIS: Sie müssen jedem Benutzerkonto, das auf IT Assistant zugreifen kann, ein Kennwort zuteilen, um Ihre kritischen Systemkomponenten vor Zugriff 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).

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 beim IT Assistant mit den Benutzerberechtigungen der ihnen zugewiesenen Gruppe anmelden.

Benutzer erstellen und Benutzerberechtigungen zuweisen für unterstützte Windows 2000-Betriebssysteme

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 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**.

HINWEIS: Sie müssen jedem Benutzerkonto, das auf IT Assistant zugreifen kann, ein Kennwort zuteilen, um Ihre kritischen Systemkomponenten vor Zugriff 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).

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. Klicken Sie auf den Namen des Benutzers, den Sie hinzufügen wollen, und dann auf **Hinzufügen**.
10. Klicken Sie auf **Namen überprüfen**, um den Benutzernamen, den Sie hinzufügen, zu bestätigen.
11. Klicken Sie auf **OK**.

Neue Benutzer können sich beim IT Assistant mit den Benutzerberechtigungen der ihnen 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**.

HINWEIS: Sie müssen jedem Benutzerkonto, das auf IT Assistant zugreifen kann, ein Kennwort zuteilen, um Ihre kritischen Systemkomponenten vor Zugriff 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).

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 beim IT Assistant mit den Benutzerberechtigungen der ihnen 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 das Benutzerkonto **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

Dell OpenManage™ IT Assistant Version 7.2: Benutzerhandbuch

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.

Dezember 2005

Zurück zum Inhaltsverzeichnis