



Dell SupportAssist

Überprüfen der Installation

Dieses Dokument enthält Informationen zu den Komponenten und Konfigurationen, die Sie überprüfen können, um sicherzustellen, dass der auf Ihrem System installierte Dell SupportAssist-Client funktioniert, wie erwartet.

Der SupportAssist-Client ist ein Plugin für Dell OpenManage Essentials. Der OpenManage Essentials Verwaltungsserver interagiert mit den unterstützten Geräten, die überwacht werden sollen und empfängt SNMP-Traps von diesen Geräten. Die SNMP-Traps werden vom SupportAssist-Client in regelmäßigen Abständen als Warnungen abgerufen. Die Warnungen werden durch die Verwendung verschiedener Richtlinien gefiltert, um genau bestimmen zu können, ob ein neuer Support-Fall erstellt oder ob ein bestehender Support-Fall aktualisiert wird. Alle entsprechend qualifizierten Warnungen werden sicher zu dem von Dell gehosteten SupportAssist-Server gesendet, um einen neuen Support-Fall zu erstellen oder einen vorhandenen Support-Fall zu aktualisieren.

Nachdem der Support-Fall erstellt oder aktualisiert wurde, führt der SupportAssist-Client die entsprechenden Diagnosehilfsprogramme auf den Geräten aus, die die Warnungen erzeugt haben und lädt die Diagnoseergebnisse zu Dell hoch. Diese Diagnoseinformationen werden vom Technischen Support von Dell verwendet, um das Problem zu beheben und eine entsprechende Lösung anzubieten.

Voraussetzungen

Die folgenden Voraussetzungen für Software und Netzwerk müssen erfüllt sein, um sicherzustellen, dass der SupportAssist-Client wie erwartet funktioniert.

Software

Die Software-Komponenten, die installiert und konfiguriert sein müssen, sind:

- OpenManage Essentials auf dem Verwaltungsserver.
- Der SupportAssist-Client muss auf dem Verwaltungsserver installiert sein. Der Verwaltungsserver muss mit dem SupportAssist-Server über das HTTPS-Protokoll kommunizieren können.

- Dell OpenManage Server Administrator (OMSA) muss auf allen Verwaltungsknoten installiert sein.



ANMERKUNG: Die Installation von OMSA auf den Verwaltungsknoten ist optional, wenn der Verwaltungsknoten ein Dell PowerEdge 12G-Server ist. Die 12G-Server können den Status, Warnungen und begrenzte Bestandsdaten über iDRAC bereitstellen, ohne den OMSA SNMP-Agenten zu verwenden.

Netzwerk

Die Anforderung an die Bandbreite für den SupportAssist-Client ist relativ gering, da dieser nur mit dem SupportAssist-Server kommuniziert, wenn ein Hardware-Problem auftritt.

Zur Sicherstellung einer erfolgreichen Kommunikation zwischen dem SupportAssist-Client und dem SupportAssist-Server:

- Der Verwaltungsserver, auf dem der SupportAssist-Client installiert ist, muss sich mit folgenden Zielorten verbinden können:
 - api.dell.com – Endpunkt für den SupportAssist-Server.
 - ddldropbox.us.dell.com/upload.ashx – Der Server zum Hochladen der Dateien, auf den die Ergebnisse des Diagnosetests hochgeladen werden.
- Port 443 muss auf dem Verwaltungsserver geöffnet sein.

Überprüfen der Konfiguration von OpenManage Essentials

Damit SupportAssist bei Auftreten eines Problems automatisch Support-Fälle erzeugen kann, ist es unerlässlich, dass OpenManage Essentials korrekt konfiguriert ist, um unterstützte Geräte ermitteln und SNMP-Traps empfangen zu können.

Folgen Sie den Anweisungen in diesem Abschnitt, um sicherzustellen, dass OpenManage Essentials die unterstützten Geräte ermitteln und SNMP-Traps empfangen kann.

Konfigurieren von SNMP auf Verwaltungsknoten

Nachdem Sie OpenManage Essentials erfolgreich installiert haben, stellen Sie sicher, dass Sie die Anweisungen zum Konfigurieren von SNMP befolgt haben. Diese sind verfügbar in OpenManage Essentials **Tutorials**→ **Erstes Setup**.

Falls Sie SNMP noch nicht konfiguriert haben, führen Sie Folgendes durch:

- 1 Klicken Sie auf **Start**→ **Ausführen**.
Das Dialogfeld **Ausführen** wird angezeigt.
- 2 Geben Sie im Feld **Öffnen services.msc** ein und klicken Sie auf **OK**.
Das Fenster **Dienste** wird angezeigt.
- 3 Durchsuchen Sie die Liste der Dienste und stellen Sie sicher, dass der Status des **SNMP-Dienstes** als **Started** (Gestartet) angezeigt wird.
- 4 Klicken Sie mit der rechten Maustaste auf **SNMP-Dienst**→ **Eigenschaften**.
Das Dialogfeld **SNMP-Dienst Eigenschaften** wird angezeigt.
- 5 Klicken Sie auf die Registerkarte **Sicherheit** und führen Sie Folgendes durch:
 - a Deaktivieren Sie die Trap-Option **Authentifizierung senden**.
 - b Klicken Sie unter **Akzeptierte Community-Namen** auf **Hinzufügen**.
Das Dialogfeld **SNMP-Dienst Konfiguration** wird angezeigt.
 - c Wählen Sie im Kästchen **Community-Rechte** die Option **NUR LESEN**.
 - d Geben Sie im Feld **Community-Name** den Community-Namen ein und klicken Sie auf **Hinzufügen**.
 - e Wählen Sie die Option **SNMP-Pakete von diesen Hosts akzeptieren** und klicken Sie auf **Hinzufügen**.
Das Dialogfeld **SNMP-Dienst Konfiguration** wird angezeigt.
 - f Geben Sie im Feld **Host-Name, IP- oder IPX-Adresse** den OpenManage Essentials-Servernamen oder die -adresse ein und klicken Sie auf **Hinzufügen**.
- 6 Klicken Sie auf die Registerkarte **Traps** und führen Sie Folgendes durch:
 - a Geben Sie im Kontrollkästchen **Community-Name** den Community-Namen ein und klicken Sie **Zur Liste hinzufügen**.
 - b Klicken Sie unter **Trap-Zielorte** auf **Hinzufügen**.
Das Dialogfeld **SNMP-Dienst Konfiguration** wird angezeigt.
 - c Geben Sie im Feld **Host-Name, IP- oder IPX-Adresse** den OpenManage Essentials-Servernamen oder die -adresse ein und klicken Sie auf **Hinzufügen**.



ANMERKUNG: Der Standard-Port zum Senden von SNMP-Traps ist 162. Lesen Sie den Abschnitt „Ändern des Standard-SNMP-Ports“ im *Dell OpenManage Essentials Benutzerhandbuch*, verfügbar unter support.dell.com/manuals, um einen Verwaltungsknoten so zu konfigurieren, dass er einen Nicht-Standard-Port verwendet.

Installation von OMSA auf allen Verwaltungsknoten



ANMERKUNG: Die Installation von OMSA auf den Verwaltungsknoten ist optional, wenn der Verwaltungsknoten ein Dell PowerEdge 12G-Server ist. Die 12G-Server können den Status, Warnungen und begrenzte Bestandsdaten über iDRAC bereitstellen, ohne den OMSA SNMP-Agenten zu verwenden.

OMSA ist der bandinterne Verwaltungsagent, der die Schnittstelle zum Verwalten des Zustands und der Bestandsdaten enthält und der außerdem dazugehörige SNMP-Traps auf Dell Servern erzeugt.

Wenn OMSA noch nicht auf den Verwaltungsknoten installiert ist, installieren Sie OMSA von:

- dem OpenManage-Datenträger, der mit Ihrem Dell Server geliefert wurde oder unter.
- support.dell.com.

Aktivieren der Netzwerkermittlung (nur Windows Server 2008)

Wenn OpenManage Essentials auf einem System installiert ist, das Microsoft Windows Server 2008 ausführt, aktivieren Sie die Option „Netzwerkermittlung“:

- 1 Klicken Sie auf **Start**→ **Systemsteuerung**→ **Netzwerk und Internet**→ **Netzwerk- und Freigabecenter**→ **Erweiterte Freigabeeinstellungen ändern**.
- 2 Klicken Sie auf den Drop-Down-Pfeil für das zutreffende Netzwerkprofil (**Privat oder Arbeitsplatz oder Öffentlich**).
- 3 Wählen Sie unter **Netzwerkermittlung** die Option **Netzwerkermittlung einschalten**.
- 4 Klicken Sie auf **Änderungen speichern**.

Konfigurieren der Firewall

Wenn eine Firewall auf dem OpenManage Essentials Server oder auf dem Verwaltungsknoten aktiviert ist, stellen Sie sicher, dass folgende Ports konfiguriert sind wie folgt:

- Öffnen Sie den Port **162** für SNMP auf dem OpenManage Essentials Server.
- Öffnen Sie Port **161** für SNMP und Port **1311** für OMSA auf den Verwaltungsknoten.

Sobald OpenManage Essentials korrekt konfiguriert ist, muss es SNMP-Traps von den unterstützten Geräten ermitteln und empfangen können.

Überprüfen der Konfiguration von Dell SupportAssist

Der SupportAssist-Client interagiert mit den OpenManage Essentials Servern in Ihrer Umgebung und kommuniziert mit dem von Dell gehosteten SupportAssist-Server.

Sie können die Kommunikation zwischen dem SupportAssist-Client und dem SupportAssist-Server überprüfen, indem Sie den E-Mail-Konnektivitätstest durchführen.

E-Mail-Konnektivitätstest

So führen Sie den E-Mail-Konnektivitätstest durch:



ANMERKUNG: Stellen Sie sicher, dass Sie als Mitglied der OpenManage Essentials Administratoren (**OmeAdministrators**) oder der Hauptbenutzergruppe (**OmePowerUsers**) eingeloggt sind. Der Link **Konnektivitätstest** ist deaktiviert, wenn Sie nicht als ein Mitglied der OpenManage Essentials Administratoren oder der Hauptbenutzergruppe eingeloggt sind.

- 1 Starten Sie Dell SupportAssist.
- 2 Klicken Sie auf den Link **Konnektivitätstest**, der in der oberen rechten Ecke des Dashboards angezeigt wird.
Die Seite **Konnektivitätstest** wird angezeigt.
- 3 Klicken Sie auf **Senden**.
Der SupportAssist-Server empfängt den Konnektivitätstest und sendet eine Probe- E-Mail mit Konnektivitätsstatus an den primären und sekundären (optional) Kontakt.

Wenn die Probe-E-Mail vom primären oder sekundären (optional) Kontakt nicht empfangen wird, zeigt dies an, dass die Kommunikation des SupportAssist-Clients mit dem SupportAssist-Server fehlgeschlagen ist.

Der E-Mail-Konnektivitätstest kann fehlschlagen aufgrund von:

- Proxy-Einstellungen – Wenn Ihr Netzwerk erfordert, dass der Datenverkehr des Internet-Browsers über einen Proxy-Server läuft, stellen Sie sicher, dass der Proxy aktiviert ist und im SupportAssist-Client konfiguriert ist. Um Probleme bezüglich Proxy-Einstellungen zu lösen, lesen Sie den entsprechenden Abschnitt unter Probleme der Proxy-Einstellungen lösen.

- SSL-Verbindungsfehler – Wenn die Proxy-Einstellungen ordnungsgemäß konfiguriert sind, aber der E-Mail-Konnektivitätstest fehlschlägt, könnte ein SSL-Verbindungsfehler vorliegen. Um Probleme der SSL-Verbindung zu lösen, lesen Sie den Abschnitt unter Beseitigen von SSL-Verbindungsfehlern.

Probleme der Proxy-Einstellungen lösen

So lösen Sie Probleme mit Proxy-Einstellungen:

- 1 Konfigurieren Sie Ihre Proxy-Server-Einstellungen im SupportAssist-Client. Siehe Konfigurieren der Proxy-Server-Einstellungen (Dell SupportAssist Version 1.1 und höher).
- 2 Führen Sie den E-Mail-Konnektivitätstest durch. Siehe E-Mail-Konnektivitätstest.

Konfigurieren der Proxy-Server-Einstellungen (Dell SupportAssist Version 1.1 und höher)

So konfigurieren Sie Ihre Proxy-Server-Einstellungen:



ANMERKUNG: Stellen Sie sicher, dass Sie als Mitglied der OpenManage Essentials Administratoren (**OmeAdministrators**) oder der Hauptbenutzergruppe (**OmePowerUsers**) eingeloggt sind. Der Link **Profil** ist deaktiviert, wenn Sie nicht als ein Mitglied der OpenManage Essentials Administratoren oder der Hauptbenutzergruppe eingeloggt sind.

- 1 Klicken Sie auf den Link **Profil**, der in der oberen rechten Ecke des SupportAssist-Dashboards angezeigt wird. Die Seite **Kontaktinformationen** wird angezeigt.
- 2 Klicken Sie auf die Registerkarte **Proxy-Einstellungen**. Daraufhin wird die Seite **Proxy-Einstellungen** angezeigt.
- 3 Wählen Sie **Proxy-Einstellungen verwenden** aus.



ANMERKUNG: SupportAssist bietet nur Unterstützung für Windows NT LAN Manager (NTLM) Authentifizierungsprotokoll.

- 4 Geben Sie **Proxy-Server-Adresse oder Name** und die **Proxy-Port-Nummer** in die entsprechenden Felder ein.



ANMERKUNG: Wenn die Proxy-Anmeldeinformationen nicht bereitgestellt werden, verbindet sich SupportAssist mit dem Proxy-Server als anonymer Benutzer.

- 5 Wenn der Proxy-Server eine Authentifizierung erfordert, dann wählen Sie **Proxy erfordert Authentifizierung** und stellen Sie die folgenden Informationen in den entsprechenden Feldern bereit:
 - **Benutzername** – Der Benutzername muss mindestens ein druckfähiges Zeichen enthalten und darf aus maximal 104 Zeichen bestehen.
 - **Kennwort** – Das Benutzerkennwort muss mindestens ein druckfähiges Zeichen enthalten und darf aus maximal 127 Zeichen bestehen.
 - **Kennwort bestätigen** – Wiederholen Sie das Benutzerkennwort. Das Kennwort sollte mit dem übereinstimmen, das Sie im Feld „Kennwort“ angegeben haben.
- 6 Klicken Sie auf **Anwenden**.
SupportAssist testet die Proxy-Server-Einstellungen. Das Testergebnis wird in einem Dialogfeld angezeigt.

Beseitigen von SSL-Verbindungsfehlern

SSL-Verbindungsfehler können auftreten, wenn Ihr System kein von der Stammzertifizierungsstelle **GTE CyberTrust Global Root** ausgegebenes Zertifikat aufweist. Alle Zertifikate von Dell werden von dieser Zertifizierungsstelle ausgegeben.

So überprüfen sie, ob das Zertifikat im Internet Explorer installiert ist:

- 1 Klicken Sie im Fenster des Internet-Browsers auf **Extras**→ **Internetoptionen**.
Das Dialogfeld **Internetoptionen** wird angezeigt.
- 2 Klicken Sie auf die Registerkarte **Inhalt** und anschließend auf **Zertifikate**.
Das Dialogfeld **Zertifikate** wird angezeigt.
- 3 Klicken Sie auf die Registerkarte **Vertrauenswürdige Stammzertifizierungsstellen**.
- 4 Scrollen Sie zum Überprüfen, ob **GTE CyberTrust Global Root** aufgelistet ist in den **Ausgegeben an** und **Ausgegeben von** Spalten.

Wenn **GTE CyberTrust Global Root** nicht aufgelistet ist, nehmen Sie Kontakt zum Technischen Support von Dell auf. Dort bekommen Sie Unterstützung beim Installieren des Zertifikats.

© 2012 Dell Inc. Alle Rechte vorbehalten.

In diesem Text verwendete Warenzeichen: Dell™, das Dell-Logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10 und Vostro™ sind Warenzeichen von Dell Inc. Intel®, Pentium®, Xeon®, Core® und Celeron® sind eingetragene Warenzeichen von Intel Corporation in den USA und anderen Ländern. AMD® ist eine eingetragene Marke und AMD Opteron™, AMD Phenom™ und AMD Sempron™ sind Marken von Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® und Active Directory® sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern. Red Hat® und Red Hat® Enterprise Linux® sind eingetragene Marken von Red Hat, Inc. in den USA und/oder anderen Ländern. Novell® and SUSE® sind eingetragene Marken von Novell Inc. in den USA und anderen Ländern. Oracle® ist eine eingetragene Marke der Oracle Corporation und/oder von ihren Tochterunternehmen. Citrix®, Xen®, XenServer® und XenMotion® sind eingetragene Marken oder Marken von Citrix Systems, Inc. in den USA und/oder anderen Ländern. VMware®, Virtual SMP®, vMotion®, vCenter® und vSphere® sind eingetragene Marken oder Marken von VMWare, Inc. in den USA oder anderen Ländern. IBM® ist eine eingetragene Marke der International Business Machines Corporation.