Dell SupportAssist

Verifying The Installation

This document provides information about the components and configurations that you can verify to ensure that the Dell SupportAssist client installed on your system works as expected.

The SupportAssist client is a plugin for Dell OpenManage Essentials. The OpenManage Essentials management server, interacts with the supported devices that are to be monitored and receives SNMP traps from these devices. The SNMP traps are periodically retrieved as alerts by the SupportAssist client. The alerts are filtered using various policies to decide if the alerts qualify for creating a new support case or updating an existing support case. All qualifying alerts are securely sent to the SupportAssist server hosted by Dell, for a creating a new support case or updating an existing support case.

After the support case is created or updated, the SupportAssist client, runs the appropriate diagnostic tools on the devices that generated the alerts, and uploads the diagnostic results to Dell. This diagnostic information is used by Dell technical support to troubleshoot the issue and provide an appropriate solution.

Prerequisites

The following are the software and network prerequisites to ensure that the SupportAssist client works as expected.

Software

The software components that must be installed and configured are:

- OpenManage Essentials on the management server.
- The SupportAssist client must be installed on the management server. The management server must be able to communicate with the SupportAssist server over the HTTPS protocol.
- Dell OpenManage Server Administrator (OMSA) must be installed on all managed nodes.

  NOTE: Installing OMSA on the managed nodes is optional if the managed node is a Dell PowerEdge 12G server. The 12G servers are capable of providing status, alerts, and limited inventory data through iDRAC without using the OMSA SNMP agent.

Network

The bandwidth requirement for the SupportAssist client is relatively low as it communicates with the SupportAssist server only when there is a hardware issue.

To ensure successful communication between the SupportAssist client and the SupportAssist server:

- The management server on which the SupportAssist client is installed must be able to connect to the following destinations:
  - **api.dell.com** — end point for the SupportAssist server.
  - **ddldropbox.us.dell.com/upload.ashx** — the file upload server where the diagnostic test results are uploaded.
- Port 443 must be open on the management server.

Verifying The OpenManage Essentials Configuration

For SupportAssist to automatically generate support cases if there is a problem, it is essential that OpenManage Essentials is configured correctly to discover supported devices and receive SNMP traps.

Follow the instructions in this section to ensure that OpenManage Essentials is able to discover the supported devices and receive SNMP traps.

Configuring SNMP On Managed Nodes

After successful installation of OpenManage Essentials, ensure that you have followed the instructions for configuring SNMP available in the OpenManage Essentials **Tutorials→ First Time Setup**. If you have not already configured SNMP, perform the following:

1. Click **Start→ Run.**
   The **Run** dialog box is displayed.
2. In the **Open** box, type `services.msc`, and click **OK**.
   The **Services** window is displayed.
3. Browse the list of services, and ensure that the status of the **SNMP Service** is displayed as `Started`.
4. Right-click the **SNMP Service→ Properties.**
   The **SNMP Service Properties** dialog box is displayed.

5 Click the **Security** tab, and perform the following:

   a Clear the **Send authentication** trap option.

   b Under **Accepted community names**, click **Add**.
   The **SNMP Service Configuration** dialog box is displayed.

   c In the **Community rights** box, select **READ ONLY**.

   d In the **Community Name** field, type the community name, and click **Add**.

   e Select **Accept SNMP packets from these hosts** option, and click **Add**.
   The **SNMP Service Configuration** dialog box is displayed.

   f In the **Host name, IP or IPX address** field, type the OpenManage Essentials server name or address, and click **Add**.

6 Click the **Traps** tab and perform the following:

   a In the **Community name** box, type the community name, and click **Add to list**.

   b Under **Trap destinations**, click **Add**.
   The **SNMP Service Configuration** dialog box is displayed.

   c In the **Host name, IP or IPX address** field, type the OpenManage Essentials server name or address, and click **Add**.

NOTE: The default port for sending SNMP traps is 162. To configure the managed node to use a non-default port, see the "Changing the Default SNMP Port" section in the *Dell OpenManage Essentials User's Guide* available at **support.dell.com/manuals**.

Installing OMSA On All Managed Nodes

NOTE: Installing OMSA on the managed nodes is optional if the managed node is a Dell PowerEdge 12G server. The 12G servers are capable of providing status, alerts, and limited inventory data through iDRAC without using the OMSA SNMP agent.

OMSA is the in-band management agent which provides the interface to manage the health and inventory data and also generates related SNMP traps on Dell servers.

If OMSA is not already installed on the managed nodes, install OMSA from:

- The OpenManage media that was provided with your Dell server.
- **support.dell.com**.

Enabling Network Discovery (Windows Server 2008 Only)

If OpenManage Essentials is installed on a system running Microsoft Windows Server 2008, enable the network discovery option:

1. Click **Start→ Control Panel→ Network and Internet→ Network and Sharing Center→ Change advanced sharing settings**.
2. Choose the drop-down arrow for the applicable network profile (**Home or Work**, or **Public**)
3. Under **Network discovery**, select **Turn on network discovery**.
4. Click **Save changes**.

Configuring The Firewall

If a firewall is enabled on the OpenManage Essentials server or on the managed node, ensure that the following ports are configured as follows:

- On the OpenMange Essentials server, open port **162** for SNMP.
- On the managed nodes, open port **161** for SNMP and port **1311** for OMSA.

Once OpenManage Essentials is configured correctly, it must be able to discover and receive SNMP traps from the supported devices.

Verifying The Dell SupportAssist Configuration

The SupportAssist client interacts with the OpenManage Essentials servers in your environment and communicates with the SupportAssist server hosted by Dell.

You can verify the communication between the SupportAssist client and the SupportAssist server by performing the e-mail connectivity test.

E-Mail Connectivity Test

To preform the e-mail connectivity test:

NOTE: Ensure that you are logged in as a member of the OpenManage Essentials admnistrators (**OmeAdministrators**) or Power Users (**OmePowerUsers**) group. The **Connectivity Test** link is disabled if you are not logged in as a member of the OpenManage Essentials Administrators or Power Users group.

1. Launch Dell SupportAssist.
2. Click the **Connectivity Test** link that is displayed at the top-right of the dashboard.
   The **Connectivity Test** page is displayed.
3. Click **Send**.
   The SupportAssist server receives the connectivity test, and sends a sample e-mail with connectivity status to the primary and secondary (optional) contact.

If the sample e-mail is not received by the primary or secondary (optional) contact, it indicates that the SupportAssist client failed to communicate with the SupportAssist server.

The e-mail connectivity test may fail due to:

- Proxy settings — If your network requires passing web browser traffic through a proxy server, ensure that the proxy is enabled and configured in the SupportAssist client. To resolve issues related to the proxy settings, see Resolving Proxy Settings Issues.
- SSL connection failure — If the proxy settings is configured properly, but the e-mail connectivity test fails, there may be a SSL connection failure. To resolve SSL connection issues, see Resolving SSL Connection Failure.

Resolving Proxy Settings Issues

To resolve issues with proxy settings:

1. Configure your proxy server settings in the SupportAssist client. See Configuring Proxy Server Settings (Dell SupportAssist Version 1.1 And Above).
2. Perform the e-mail connectivity test. See E-Mail Connectivity Test.

Configuring Proxy Server Settings (Dell SupportAssist Version 1.1 And Above)

To configure your proxy server settings:

NOTE: Ensure that you are logged in as a member of the OpenManage Essentials admnistrators (**OmeAdministrators**) or Power Users (**OmePowerUsers**) group. The **Profile** link is disabled if you are not logged in as a member of the OpenManage Essentials Administrators or Power Users group.

1. Click the **Profile** link that is displayed at the top-right corner of the SupportAssist dashboard.
   The **Contact Information** page is displayed
2. Click the **Proxy Settings** tab.
   The **Proxy Settings** page is displayed.
3. Select **Use Proxy Settings**.

   NOTE: SupportAssist provides support for Windows NT LAN Manager (NTLM) authentication protocol only.
4. Type the **Proxy Server Address or Name** and **Proxy Port Number** in the appropriate fields.

   NOTE: If the proxy credentials are not provided, SupportAssist connects to the proxy server as an anonymous user.
5. If the proxy server requires authentication, select **Proxy requires authentication**, and then provide the following information in the corresponding fields:
   - **Username** — The user name must contain one or more printable characters, and no more than 104 characters.
   - **Password** — The user password must contain one or more printable characters, and no more than 127 characters.
   - **Confirm Password** — Repeat the user password. The password should match with the one provided in the Password field.
6. Click **Apply**.
   SupportAssist tests the proxy server settings, and the result of the test is displayed in a dialog box.

Resolving SSL Connection Failure

SSL connection failure may occur if your system does not have a certificate installed from the issuing root certificate authority, **GTE CyberTrust Global Root**. All Dell certificates are issued from this certificate authority.

To verify if the certificate is installed in Internet Explorer:

1. In the web browser window, click **Tools→ Internet Options.**
   The **Internet Options** dialog box is displayed.
2. Click the **Content** tab and then click **Certificates**.
   The **Certificates** dialog box is displayed.
3. Click the **Trusted Root Certification Authorities** tab.
4. Scroll to verify if **GTE CyberTrust Global Root** is listed in the **Issued To** and **Issued By** columns.

If **GTE CyberTrust Global Root** is not listed, contact Dell technical support, for assistance in getting the certificate installed.
