Setting Up Secure Server Connections

The Availability Manager uses Transport Layer Security (TLS) Version 1 for secure communication between the Data Analyzer and the Data Server. (TLS is an extension of Secure Sockets Layer (SSL) Version 3.0, which is the most widely-used protocol for security on the Web.)

TSL uses **public key cryptography** (also called asymmetric cryptography) to guarantee secure communication over a network. This type of cryptography uses an encryption algorithm that produces a pair of keys:

- A public key, which is made public, provides authentication
- A private key, which is kept private, works with digital certificates to provide privacy and data integrity

These two keys work together: what one key encrypts, only the other key can decrypt.

Key Pairs and Key Stores

> Notes: **Data Server** refers to the Availability Manager Data Server software;
> **server system** refers to the hardware that runs the Data Server software.
> Also, the term **Combined kit** refers to the Data Analyzer/Data Server kit.

Before you can use the Data Server, you need to create an asymmetric **key pair** for the Data Server to use. The Data Server keys are stored in a **Key Store**. The Data Server Key Store, named AM$KeyStore.jks, is in the AMDS$AM_CONFIG: directory on OpenVMS systems; for Windows systems, the Key Store is in the installation folder. Currently, HP supports configurations in which the Data Server has only one key pair in a Key Store.

You create the initial Key Store after installing either the Combined kit for OpenVMS, or the Availability Manager kit for Windows. The numbered tasks in the following sections explain how to do this.

Trusted Certificates and Trust Stores

After you create a Data Server key pair, you can create a **trusted certificate** to contain the public key for the Data Server. The Data Analyzer uses a trusted certificate to establish a secure connection to the Data Server. The trusted certificate is *exported* from the Data Server Key Store and then *imported* into the Data Analyzer **Trust Store**. The Data Analyzer Trust Store, named AM$TrustStore.jks, is in the AMDS$AM_CONFIG: directory for OpenVMS systems or in the installation folder for Windows systems.

The Key Store and Trust Store have essentially the same format; each store can contain both private keys and trusted certificates. However, to avoid complication, HP recommends that you set up the following:

- For each Data Server, a Key Store with a single entry.
- For each Data Analyzer, a Trust Store that contains a trusted certificate for each server you want to connect to.

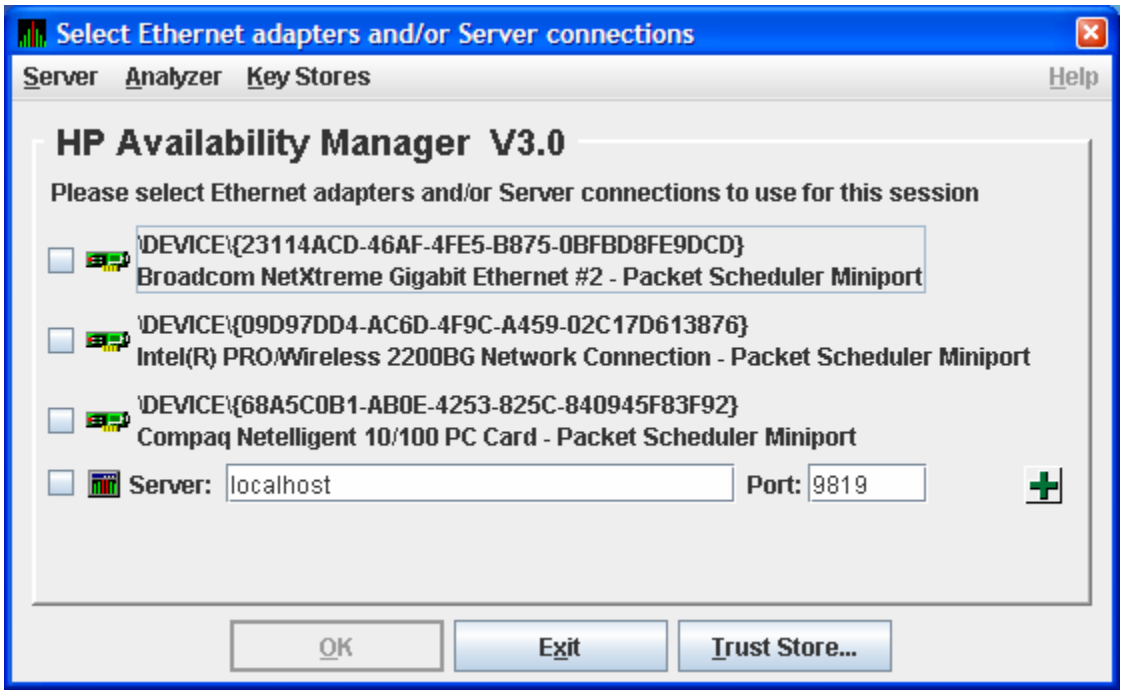
Getting Started

Step 1 – Create a new private key for the Data Server

The Data Server must have a private key in its Key Store before it starts. Start the Availability Manager Data Analyzer, either on the system that you plan to use as the Availability Manager server system (that is, the hardware) or, if you prefer, on another system.

When you start the Data Analyzer, it displays the Connections Dialog box, shown in Figure 1.

Figure 1 – Connections Dialog Box

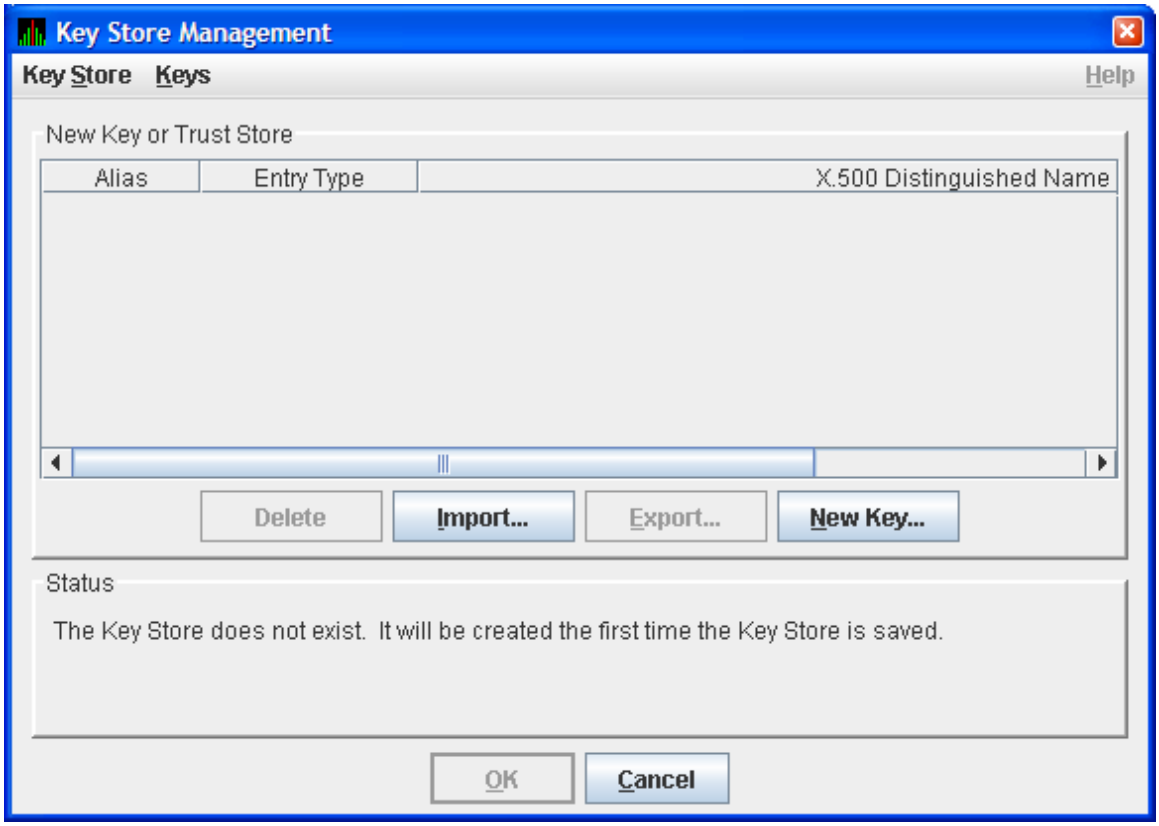


If this system is to be the Availability Manager server system, select the "Server" menu item to open the default Key Store for this system. If another system is to be the

Availability Manager server system, select the "Key Stores" menu and then select "New Trust or Key Store."

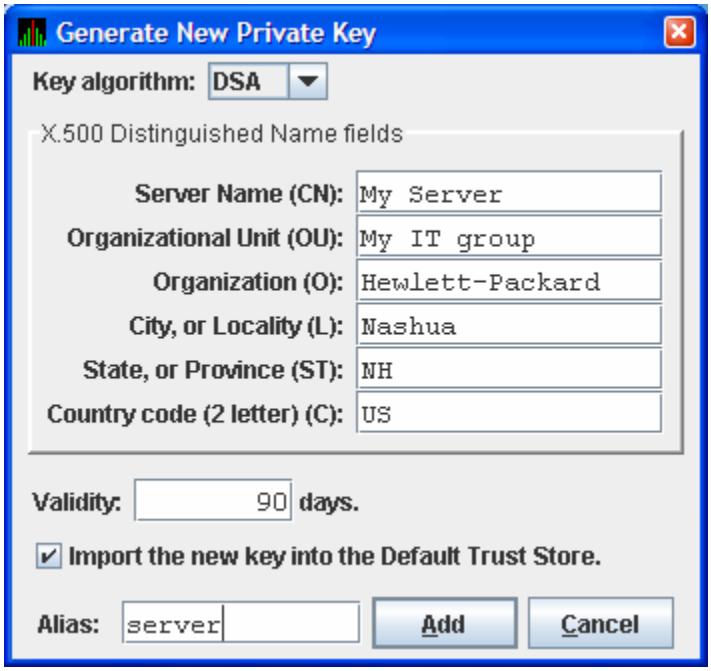
The Availability Manager next displays the Key Store Dialog box, shown in Figure 2.

Figure 2 – Key Store Dialog Box



In the Key Store Dialog box, press "New Key..." to display the “Generate New Private Key” Dialog box (see Figure 3), and fill in the fields to create a new private key.

Figure 3 – New Private Key Dialog Box



The information you enter in the New Private Key Dialog box includes fields that apply to an "X.500 Distinguished Name." HP recommends that you use the name of the server system as the first field (CN) and also as the alias for the key. ("Alias" is simply a name that is used to track items in the Key Store and is not part of the generated key.)

Currently, the Availability Manager does not check to see if a key has expired; therefore, the “Validity” field is not used. However, for the field to work in future versions, HP recommends that you enter a large value if you are creating a key that will be valid for a long time.

If you want to connect this system to the server, leave the “Default Trust Store” check box checked; this action allows you to bypass step 3 in this set of instructions for this system.

When you finish entering information to create a new private key, press “Add.” (It might take a few seconds to create the key.) If you checked the “Default Trust Store” check box, a Trust Store for this key pair is created.

You now have one key in the table in the Key Store Dialog box (see Figure 4). Note that the Key Store is not saved until you press “OK” in the Key Store Management Dialog box. If you run the Data Analyzer on this system, press “OK” to create the Key Store and go to step 4.

If you want Data Analyzers on other systems to access the Data Server in this system, export the server public key as a trusted certificate in step 2. Then press "OK" to save the Key Store.

If you opened the Key Store using the "New Trust or Key Store" menu item, you are prompted to enter file-saving information. If you do not want this system to be the Availability Manager server, move the new Key Store to the server system using one of the following names:

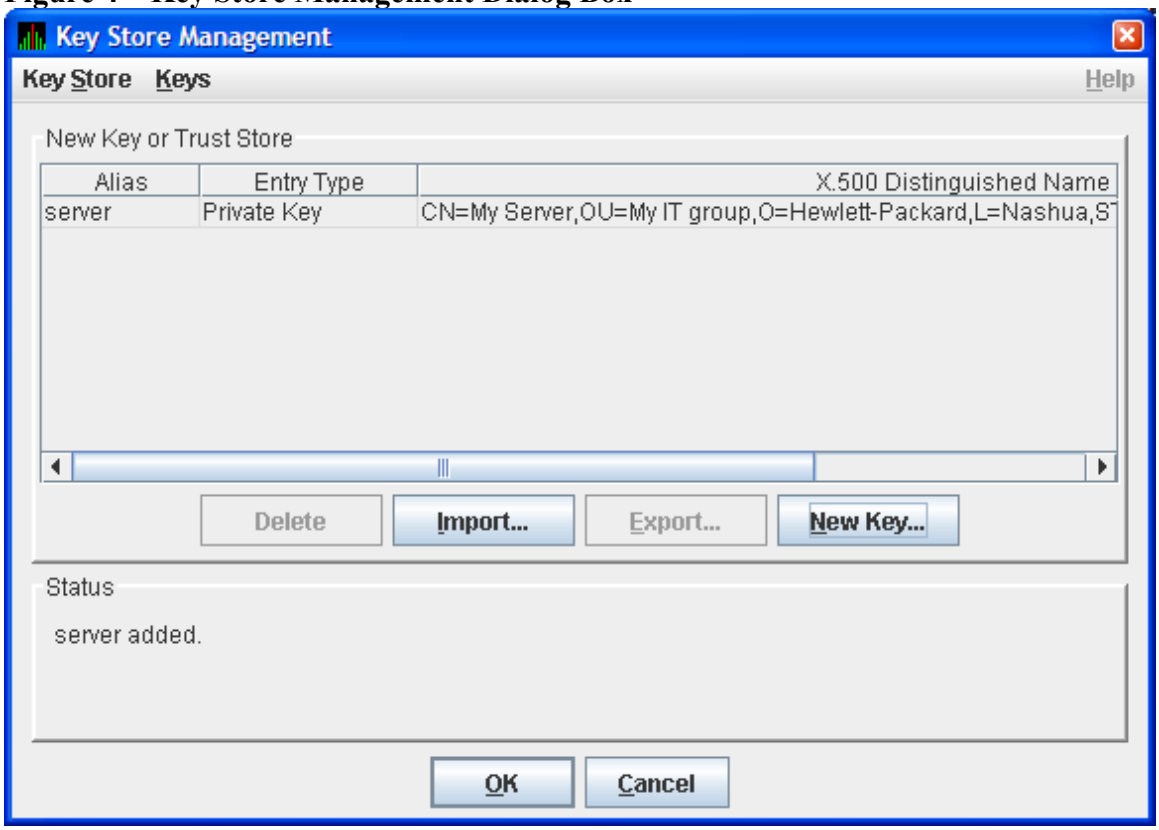
- `AMDS$AM_CONFIG:AM$KEYSTORE.JKS` for VMS systems
- `AM$KeyStore.jks` in the AM installation folder for Windows systems.

If you use FTP to move the Key Store, use binary mode.

Step 2 - Export the key for other Data Analyzers to use

If other systems are to be used as Data Analyzers connecting to the Data Server referred to in step 1, you need to export the public key as a trusted certificate and import it into the Trust Store on each Data Analyzer system. With the Key Store open, select the key so that it is highlighted, as shown in Figure 4. Then press "Export."

Figure 4 – Key Store Management Dialog Box

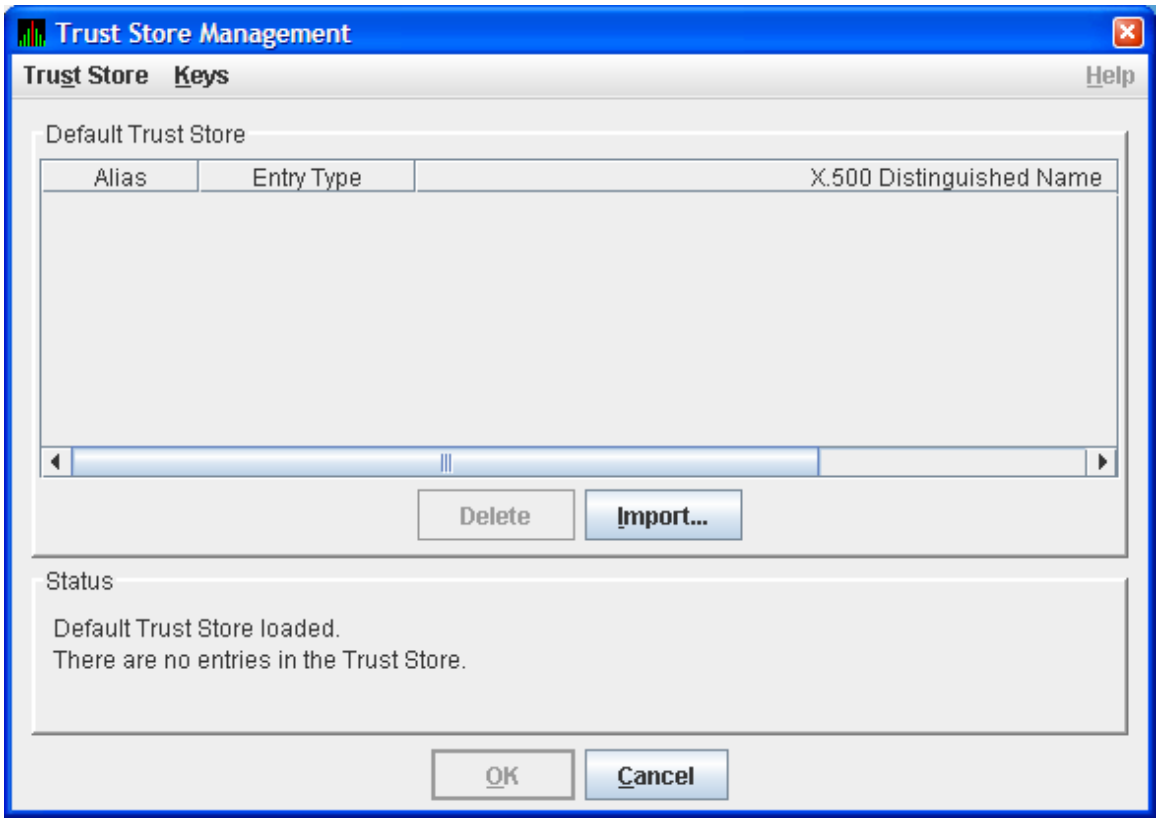


The Availability Manager prompts you to save the certificate as a file; for example, `server.cer`. Copy the certificate to systems that are to run the Data Analyzer using a Windows share, FTP, or DECnet file copy. (FTP users, use binary mode.)
Press “OK” to save and close the Key Store.

Step 3 - Import certificates for the Data Analyzer to use

Before a Data Analyzer can connect to a Data Server, you must import a trusted certificate for that server into its Trust Store. Start the Data Analyzer, and, in the Connections dialog box (Figure 1), press "Trust Store" to open the default Trust Store Management Dialog box for this system, which is shown in Figure 5.

Figure 5 – Trust Store Management Dialog Box



Press "Import" to import the certificate created in step 2. If this is the same system that was used in step 1, and the check box in the New Key Dialog box (Figure 3) was checked, this step has already been completed for you.

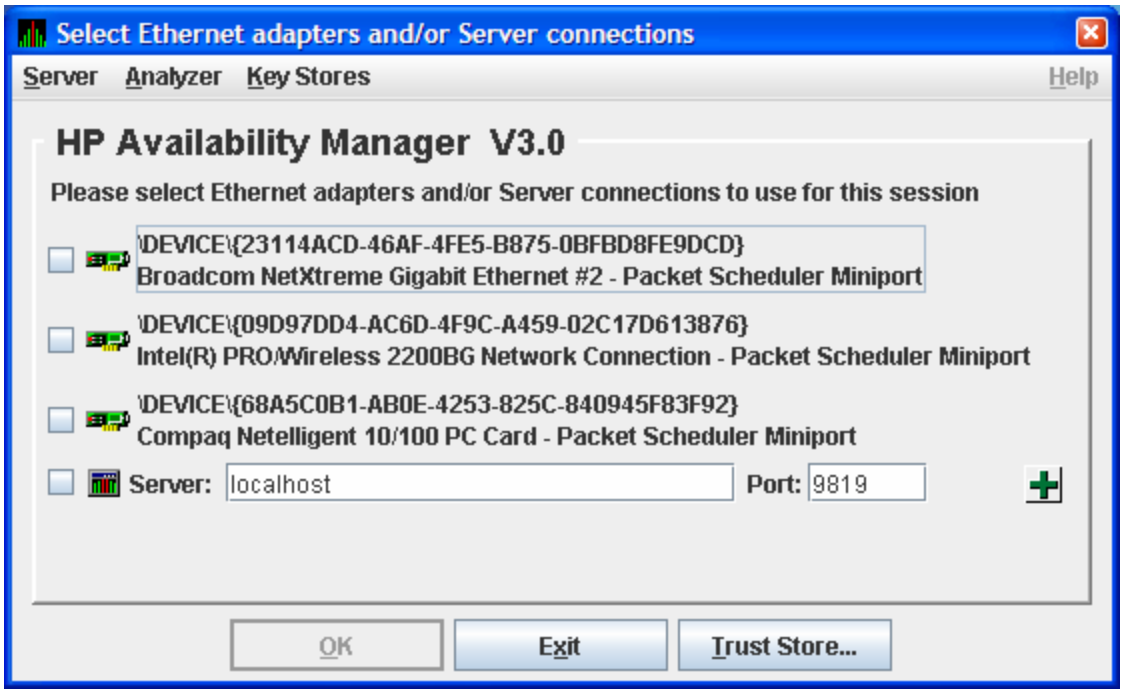
For each certificate that you import, information about the certificate is displayed, and you are prompted to assign an alias for this certificate.

If needed, repeat these steps to import certificates for more Data Servers. Press “OK” to save the Trust Store and return to the Connection Dialog box (see Figure 1).

Step 4 - Run the Availability Manager

Once the Key Store and Trust Store are in place, you can then connect the Data Analyzer to the Data Server. This is done through the Connections Dialog box in Figure 6.

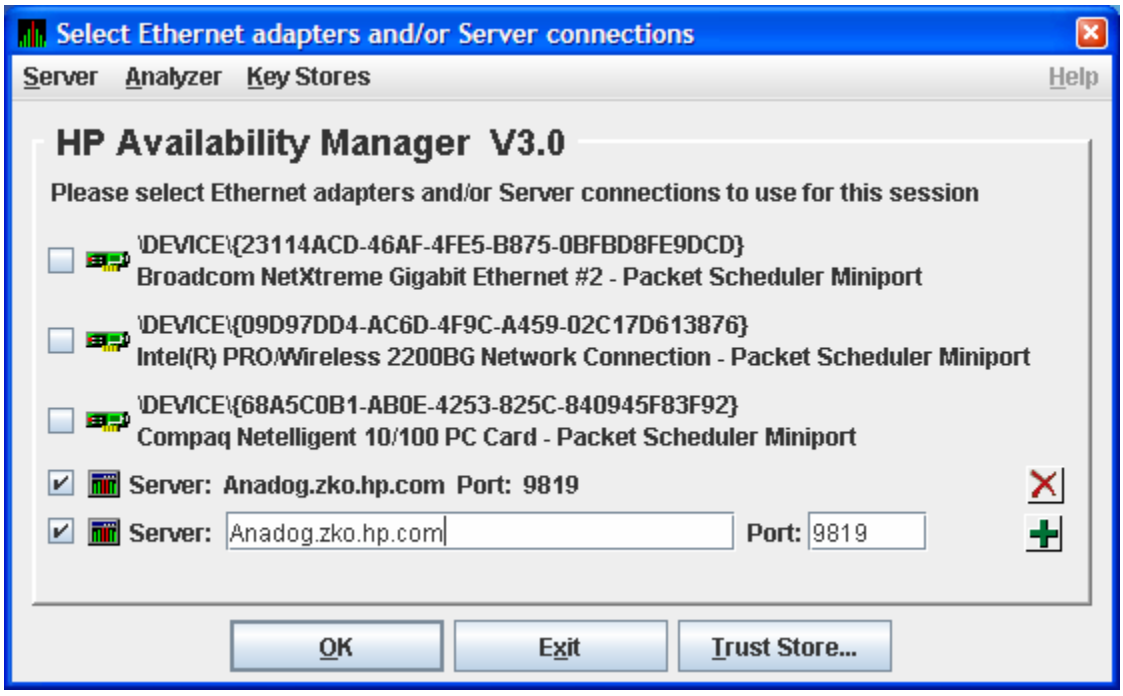
Figure 6 – Initial Connections Dialog Box



In Figure 6, there are three entries for the three network adapters on the system. The last entry is where you enter the IP address and port number of a Data Server. If you want to use one or more of these network adapters, then check the checkbox on the left of eash network adapter, and click on OK. The Data Analyzer then starts, using the network adapters you have chosen.

To use one or more Data Servers, you enter the IP address of each server, along with the IP port that the Data Server uses for communication. In this example, Anadog.zko.hp.com is entered into the Server: field, and 9819 in the Port: field, and then the green plus sign on the right is clicked with a left mouse click. The result is in Figure 7.

Figure 7 – Connections Dialog Box with one Data Server entry



To start the Data Analyzer, clear the checkbox for the last entry. The Data Analyzer then uses the Data Server running on Anadog.zko.hp.com.Figure 7.

If you want to remove a Data Server entry from the Connections Dialog Box, click on the red X on the right side of the Data Server entry.

Additional Information

Export and Import made easy:

The Availability Manager allows you to open multiple Key Stores and Trust Stores using the menus on the Connections Dialog box (Figure 1). The Key and Trust Store Dialog boxes (Figures 4 and 5) allow you to drag-and-drop items interchangeably between one dialog box and another (and also to the file system or desktop on Windows). This operation can make import and export easier if you open the Key and Trust Stores locally (or use network shares to open them).

Clarification of menu items (Connections Dialog Box menus):

Note the following:

- The "Key Store" menu item on the Server and the Key Stores menu open the default AM server key (`AM$KeyStore.jks`).

- The "Trust Store" menu item on the Analyzer and Key Stores menu and the "Trust Store" button open the default Availability Manager Data Analyzer Trust Store (`AM$TrustStore.jks`).
- The other menu items on the Key Stores menu open generic Key or Trust Stores that you are prompted to name when you open or save any of them.

Certificates:

The certificate that you create is a "self-signed" one. This means that the person who creates the certificate also signs off on its legitimacy. This type of certificate is also called a “root certificate.”