VMS Software

VSI OpenVMS

VSI Availability Manager Data Server Guide for Microsoft Windows

Document Number: DO–AMDSCG–01A

Publication Date: May 2024

Operating System and Version: Microsoft Windows 10

Software Version: VSI Availability Manager Version 3.2-1

VMS Software, Inc. (VSI)
Boston, Massachusetts, USA

VSI Availability Manager Data Server Guide for Microsoft Windows

Legal Notice

Preface

1. About VSI

VMS Software, Inc. (VSI) is an independent software company licensed by Hewlett Packard Enterprise to develop and support the OpenVMS operating system.

2. Intended Audience

This guide is intended for system managers who install and use the VSI Availability Manager software. It is assumed that the system managers who use this product are familiar with Microsoft Windows[1] terms and functions.

3. Document Structure

This guide is organized as follows:

- Chapter 1 provides an introduction to this guide.
- Chapter 2 provides a configuration example for the Data Server running on Windows 10 and explains how to configure network adapters for this system.

4. Related Documents

The following manuals provide additional information:

- *VSI Availability Manager Version 3.2-1 Installation Instructions* contain information about installing the VSI Availability Manager on OpenVMS and Windows systems.
- *VSI Availability Manager User's Guide* explains how to use the VSI Availability Manager software to detect and correct system availability problems.

For additional information about VSI OpenVMS products and services, please visit the VSI OpenVMS website at or contact us at <info@vmssoftware.com>.

5. VSI Encourages Your Comments

You may send comments or suggestions regarding this manual or any VSI document by sending electronic mail to the following Internet address: <docinfo@vmssoftware.com>. Users who have VSI OpenVMS support contracts through VSI can contact <support@vmssoftware.com> for help with this product.

[1]The term **Windows**, as it is used in this manual, refers to Windows 10.

Chapter 1. Introduction

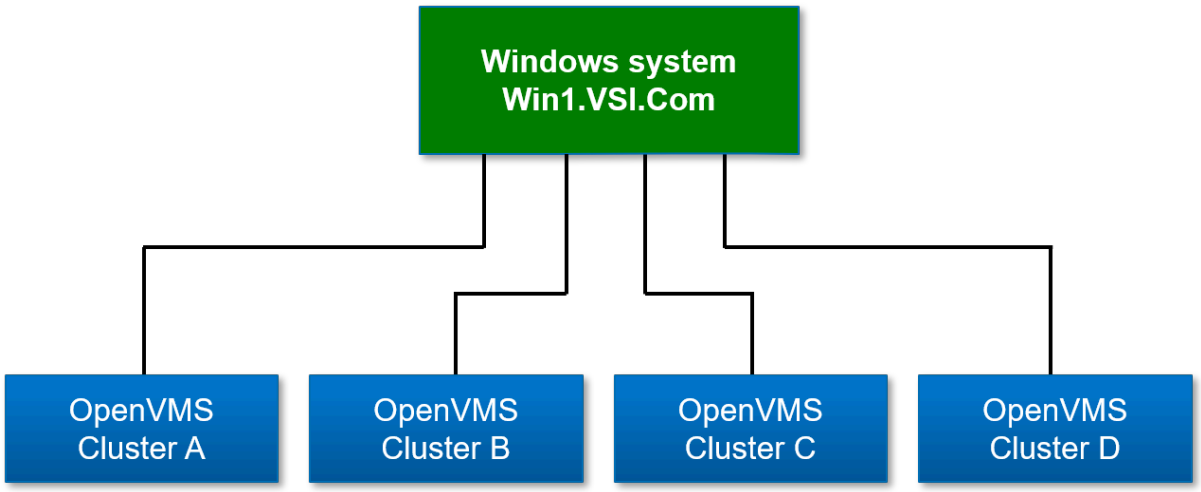
This document provides instructions on how to configure use of the network adapters for a system running Microsoft Windows by the Availability Manager Data Server. This Guide applies to Windows installations of the VSI Availability Manager kit for Windows. The equivalent configuration for the Data Server running on OpenVMS is covered in Chapter 2 of the *VSI Availability Manager User's Guide*.

As documented in the *VSI Availability Manager User's Guide*, Section 1.2.2, a system running the Data Server must have a network adapter connected to the local LAN for each OpenVMS cluster or system monitored by one or more Data Analyzers. This guide shows how to assign a port number to each network adapter on a Microsoft Windows system.

Chapter 2. Configuration Example Used by This Guide

This guide is using a Microsoft Windows system with four network adapters as an example configuration. Each adapter is connected to the local LAN of a cluster of OpenVMS systems (see Figure 2.1).

Figure 2.1. The Data Server Configuration Example on Windows



2.1. Steps to Setup the Configuration Example

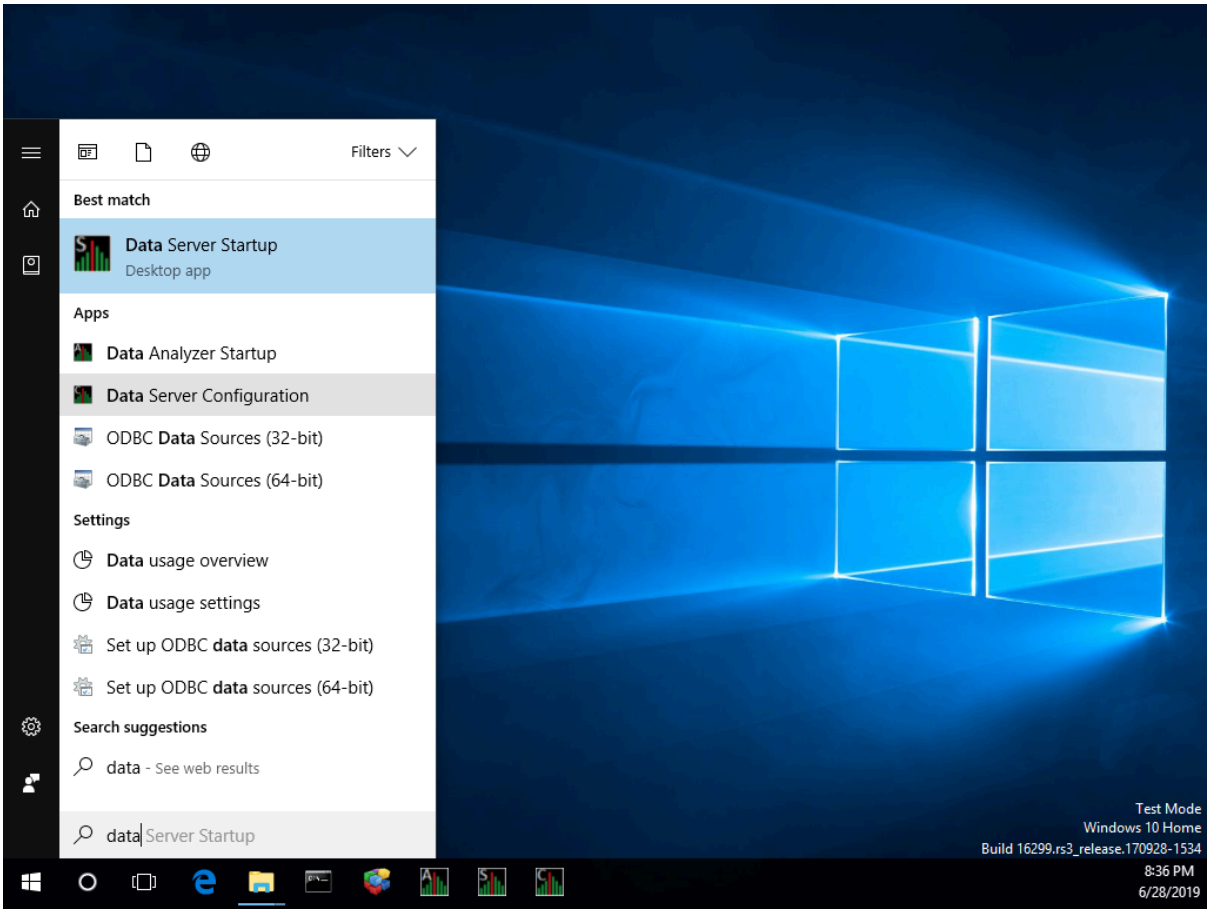
The Data Server Configuration utility assigns a TCP/IP port number to a network adapter. For this example, network adapter #1 is connected to OpenVMS cluster A, #2 to OpenVMS cluster B, #3 to OpenVMS cluster C, and #4 to OpenVMS cluster D. The port numbers assigned to the network adapters are 9810 through 9813 respectively.

After assigning port numbers to network adapters in the Data Server Configuration utility, the ports need to be opened for incoming traffic in the Microsoft Windows Firewall.

2.1.1. Data Server Steps

Open the Data Server Configuration utility. One way to do this is to click on the Windows **Start** button and type "Data" to display the three components of the Availability Manager on Windows.

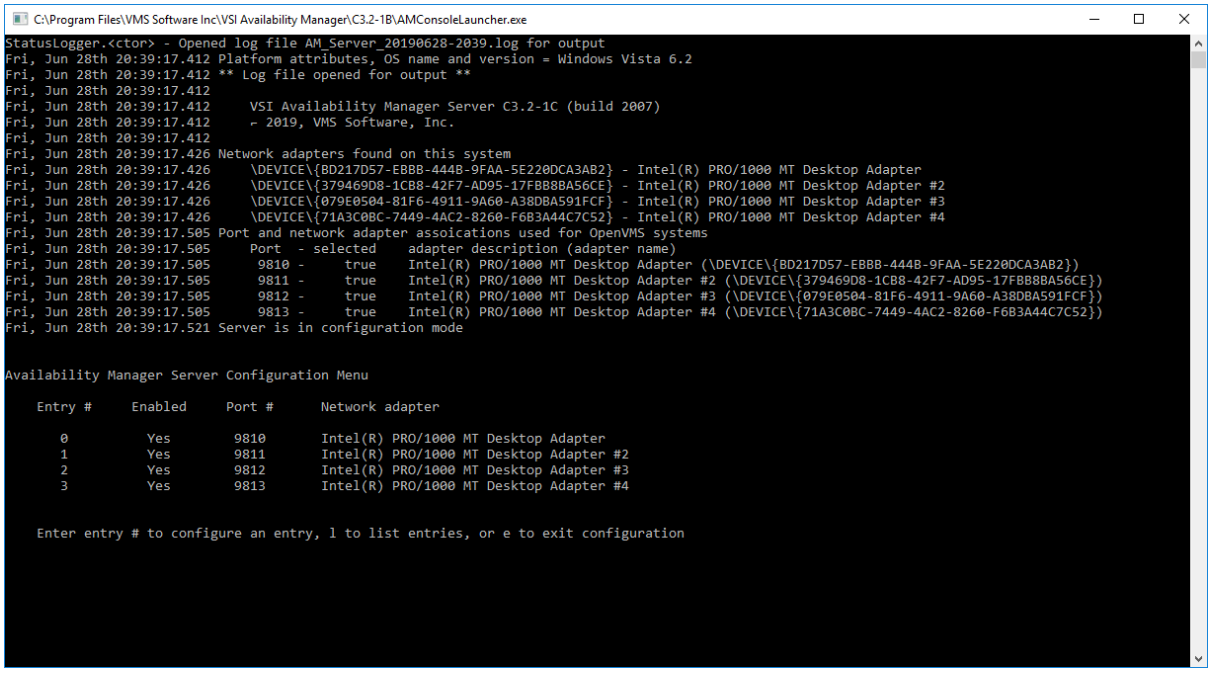
Figure 2.2. Starting the Data Server Configuration Utility



Right-click the Data Server Configuration entry and select **Run as administrator** from the menu to start the utility along with the Availability Manager protocol driver, which scans the system for available network adapters.

The Data Server Configuration utility utilizes a Windows Command Prompt to display the network adapters and assigned port numbers. Figure 2.3 shows the default configuration from the first time that the Data Server Configuration utility is run on the system.

Figure 2.3. The Default Configuration of Network Adapters and Ports



There are some things to note from the screen shown in Figure 2.3.

- Network adapter #1 is listed as "Intel(R) PRO/1000 MT Desktop Adapter".
- The first time the Data Server Configuration utility is run, it configures the network adapters as selected and assigns port numbers to each one starting with the first available port of 9810.

This is the desired configuration for the setup in Figure 2.1. Entering "e" to exit saves this configuration and then exits the utility.

Figures 2.4 and 2.5 show how to disable a network adapter so it is not used by the Data Server, and how to change the port number for an adapter. Note that disabling a network adapter stops the Data Server from using the adapter to communicate with OpenVMS systems on its local LAN. The adapter is still available for Windows and other programs.

Figure 2.4. Disabling a Network Adapter

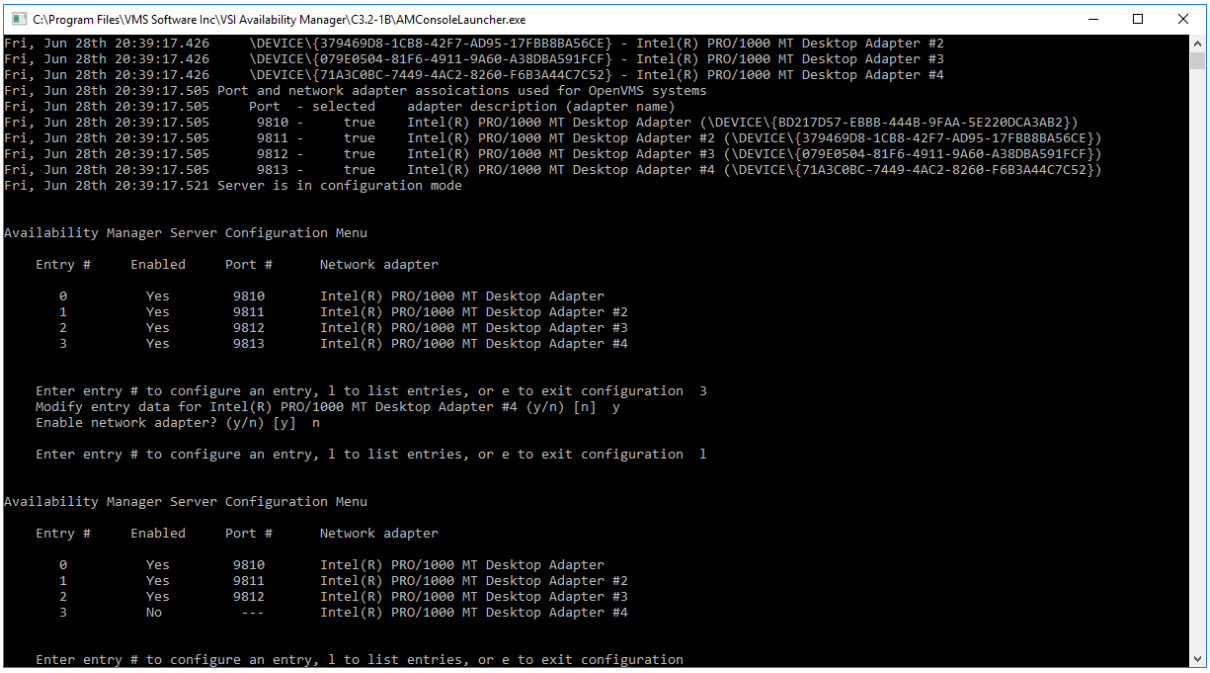


Figure 2.4 shows how to disable a network adapter. Adapter #3 is selected, and disabled. Then, the list of adapters and their current setup is displayed.

Figure 2.5. Enabling a Network Adapter

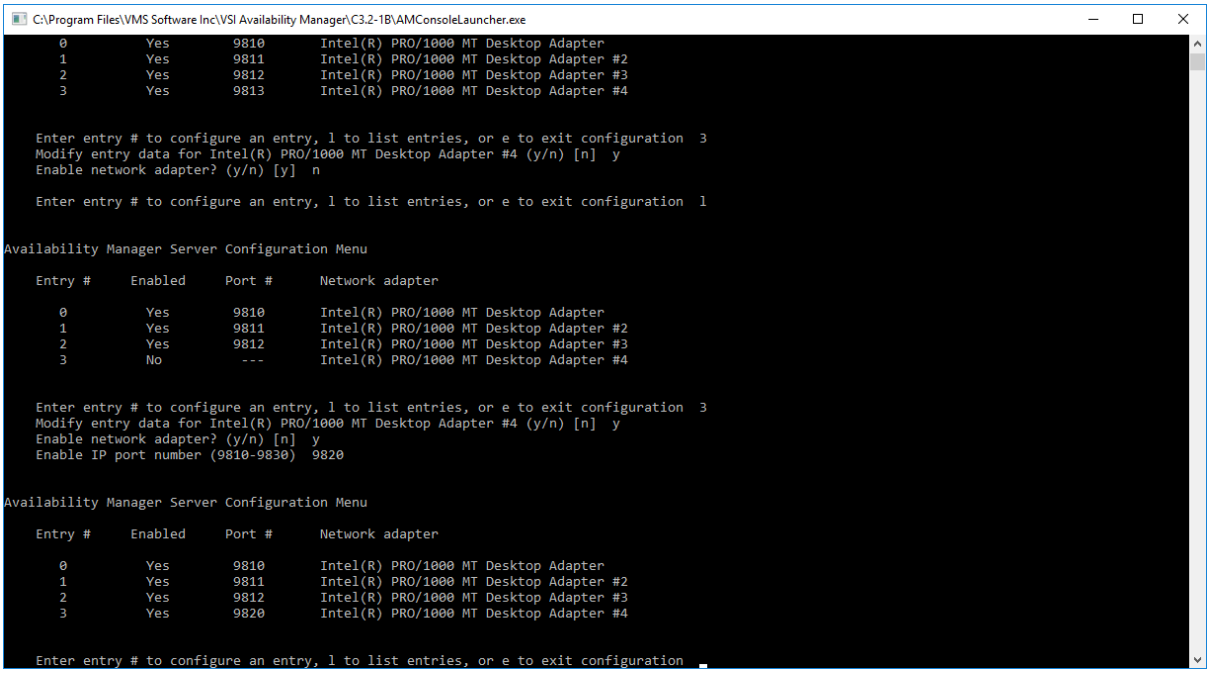


Figure 2.5 displays the steps to enable a network adapter. Adapter #3 is selected, and enabled. The list of adapters is displayed after this change. Note the range of port numbers to use in the "Enable IP port number" prompt. These port numbers are used by the Data Server when it is started.

Figure 2.6. Exiting the Data Server Configuration Utility

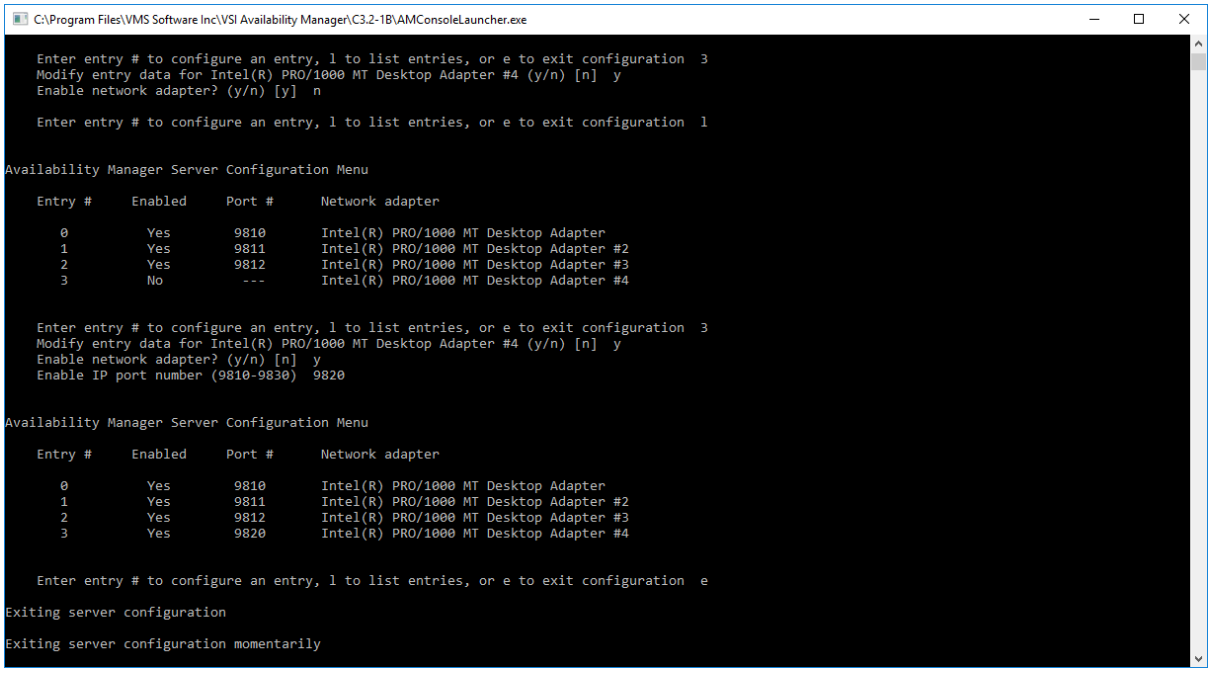


Figure 2.6 displays the text when the utility is directed to exit. This screen is displayed for a short time while the utility saves the configuration, and then Windows Command Prompt closes.

2.1.2. Windows Firewall Steps

After configuring the network adapters, the ports need to be opened for incoming traffic in the Windows Firewall, as incoming traffic to them is blocked by default.

Start the Windows Firewall application by clicking on the Windows **Start** button. Type "Firewall", and select the Windows Firewall entry.

Figure 2.7. Windows Defender Firewall with Advanced Security

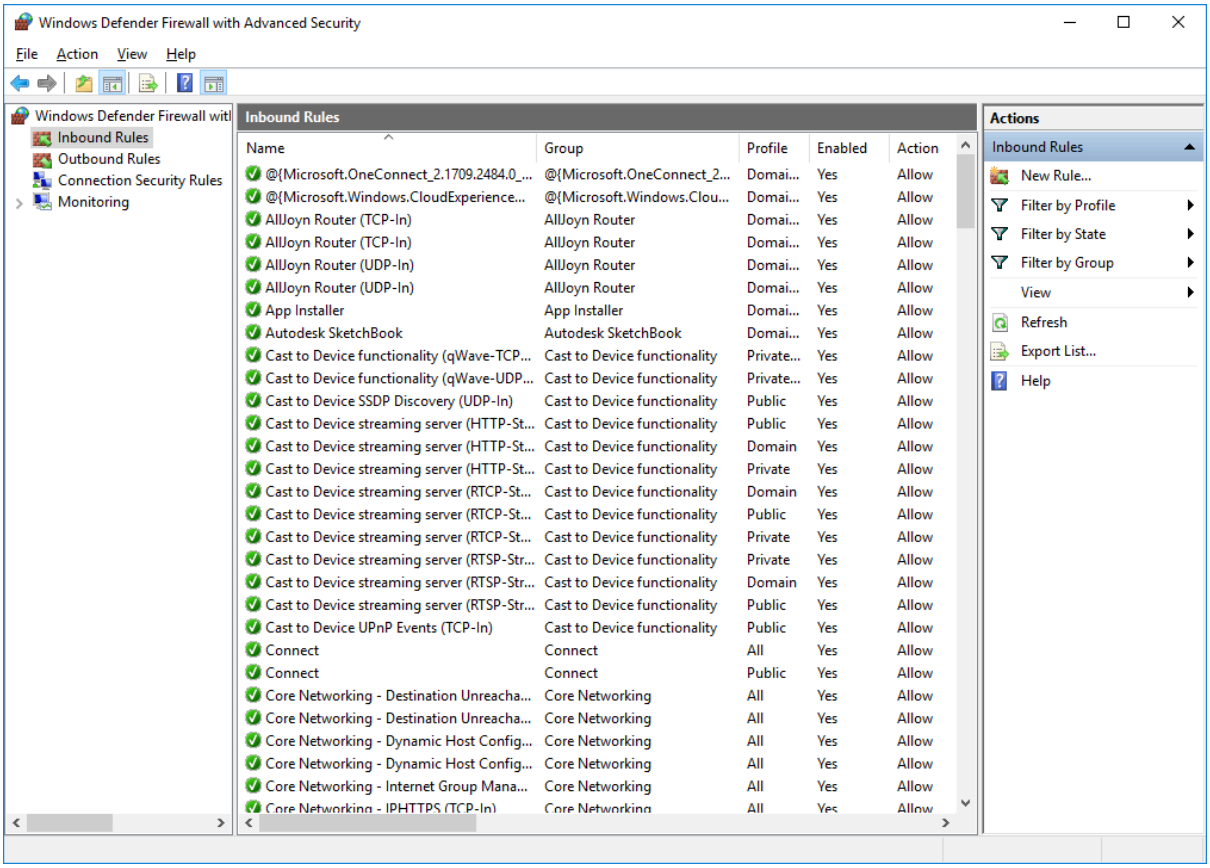


Figure 2.7 shows the Windows Firewall application after clicking on the **Inbound Rules** menu item in the upper left-hand corner. Click on **New Rule...** in the upper right-hand corner to display the New Inbound Rule Wizard.

Figure 2.8. Creating an Inbound Port Rule

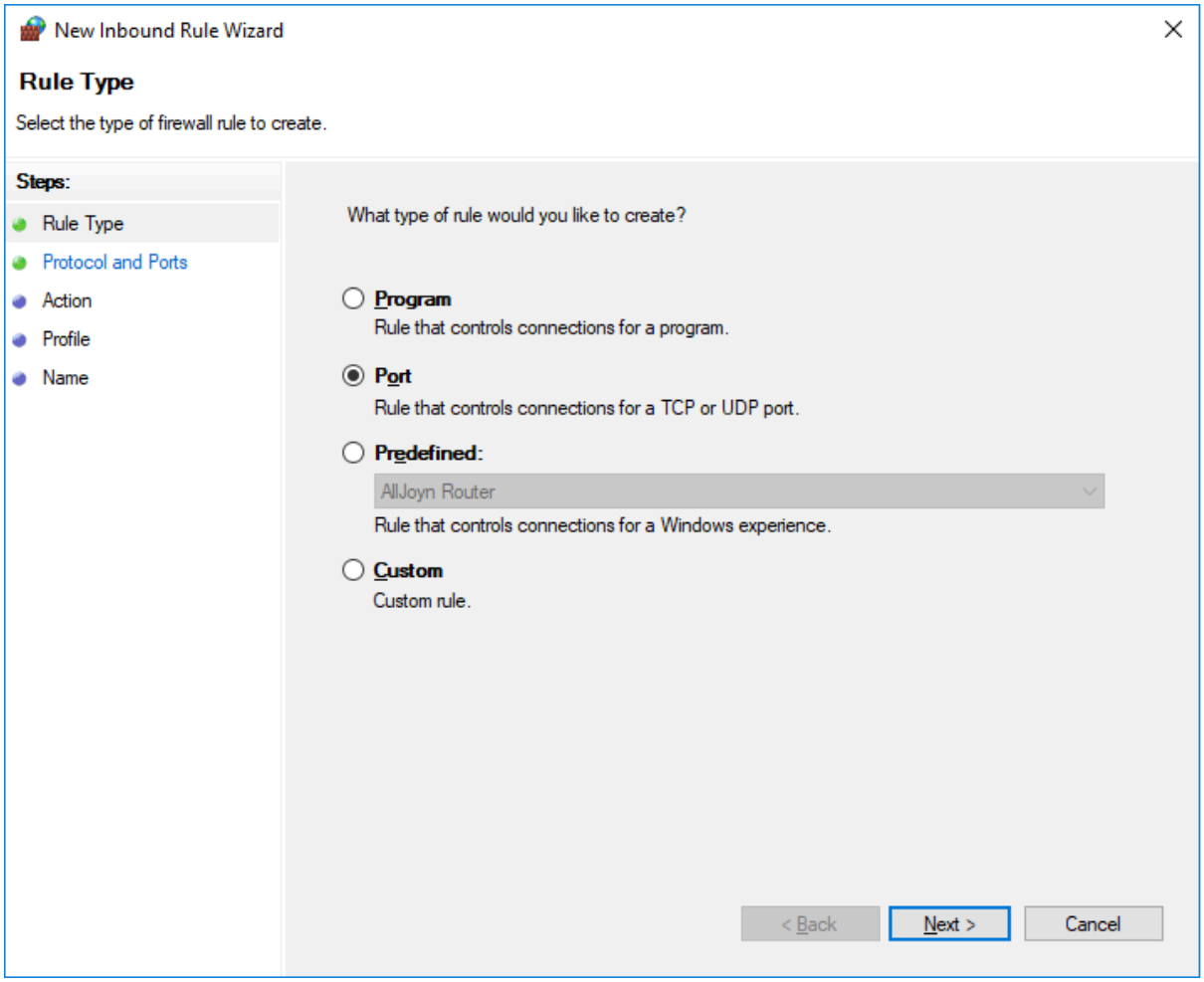
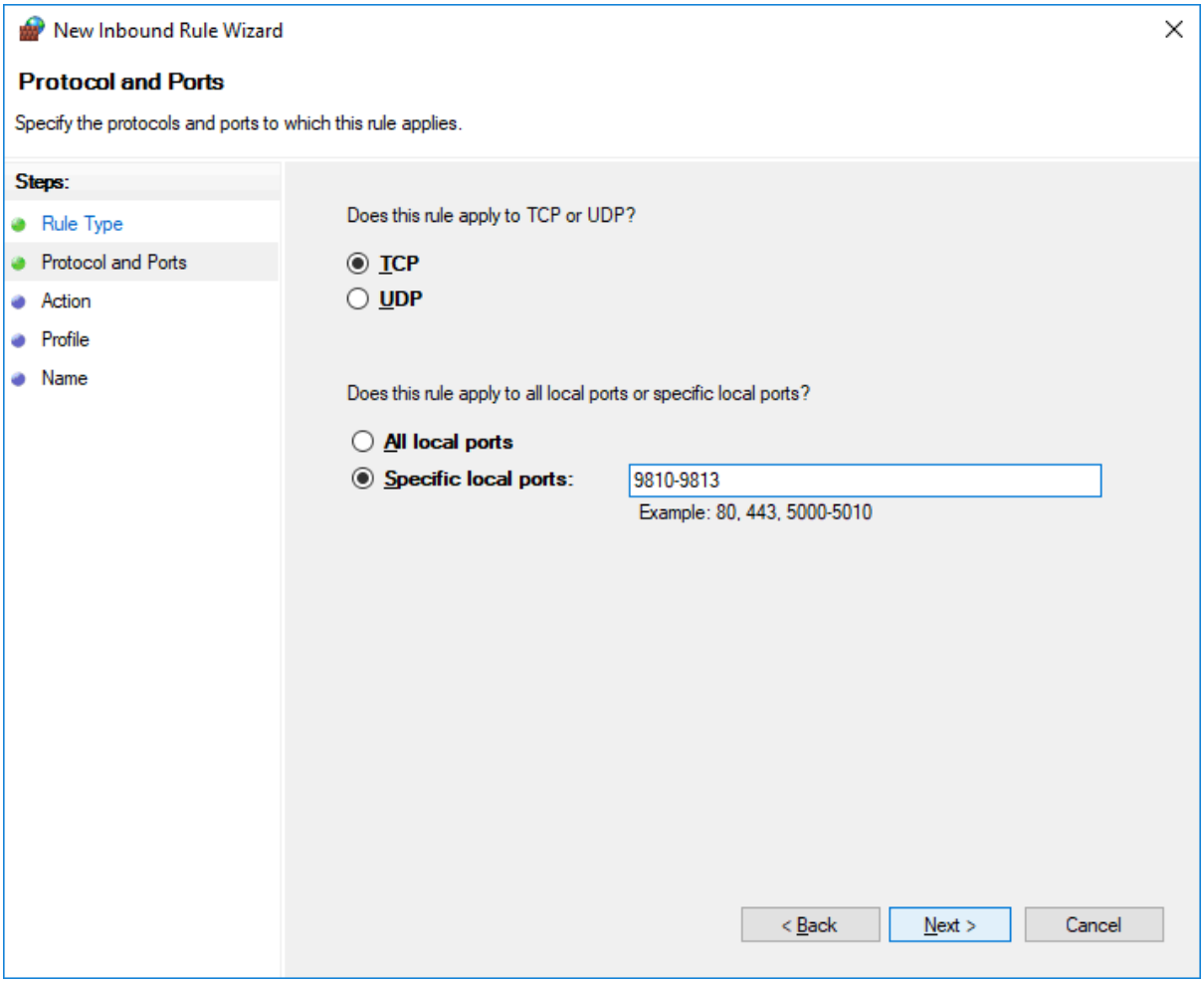


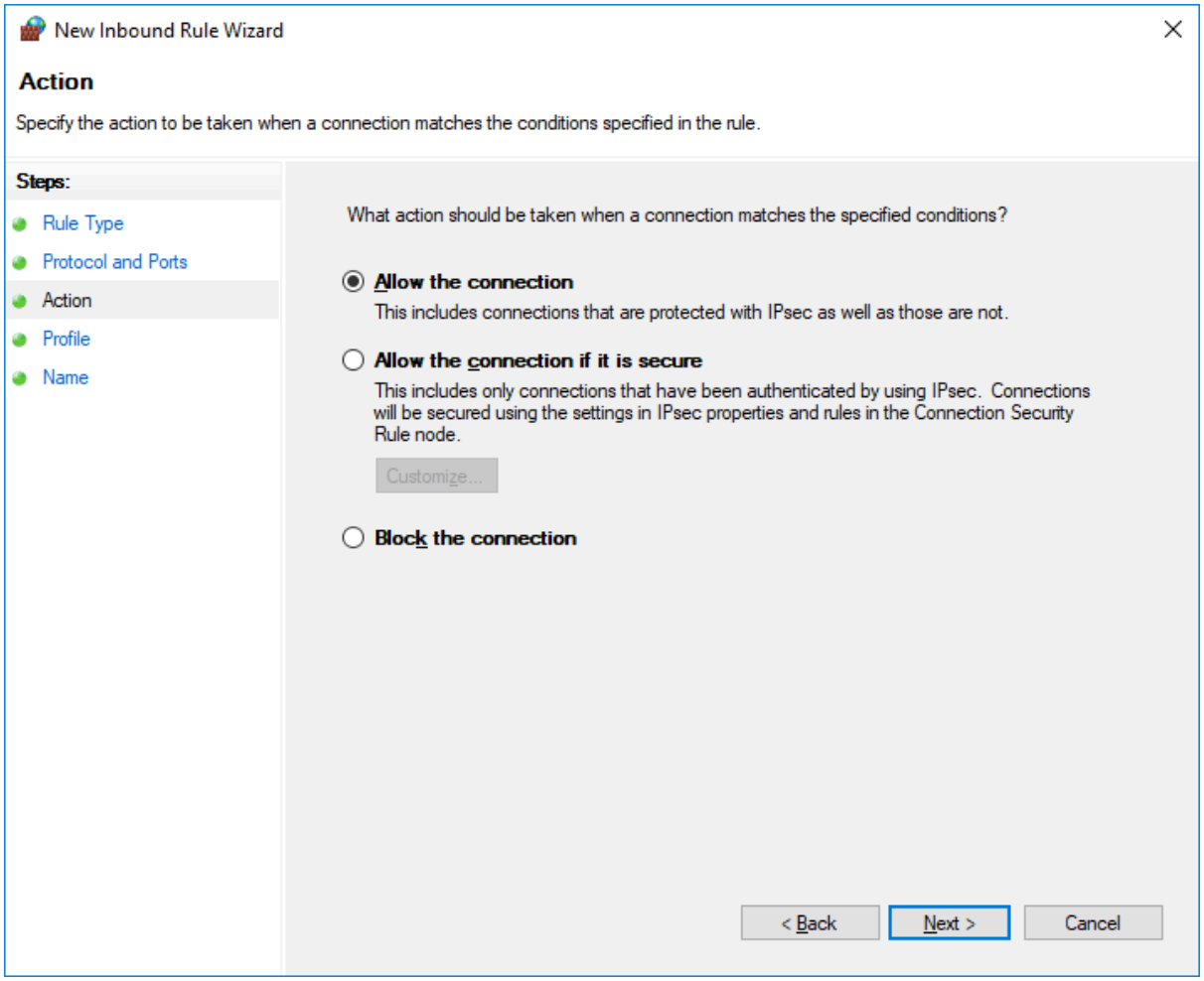
Figure 2.8 shows the first wizard step of the **New Rule...** menu entry. Select **Port** and then click on **Next**.

Figure 2.9. Specifying Port Numbers



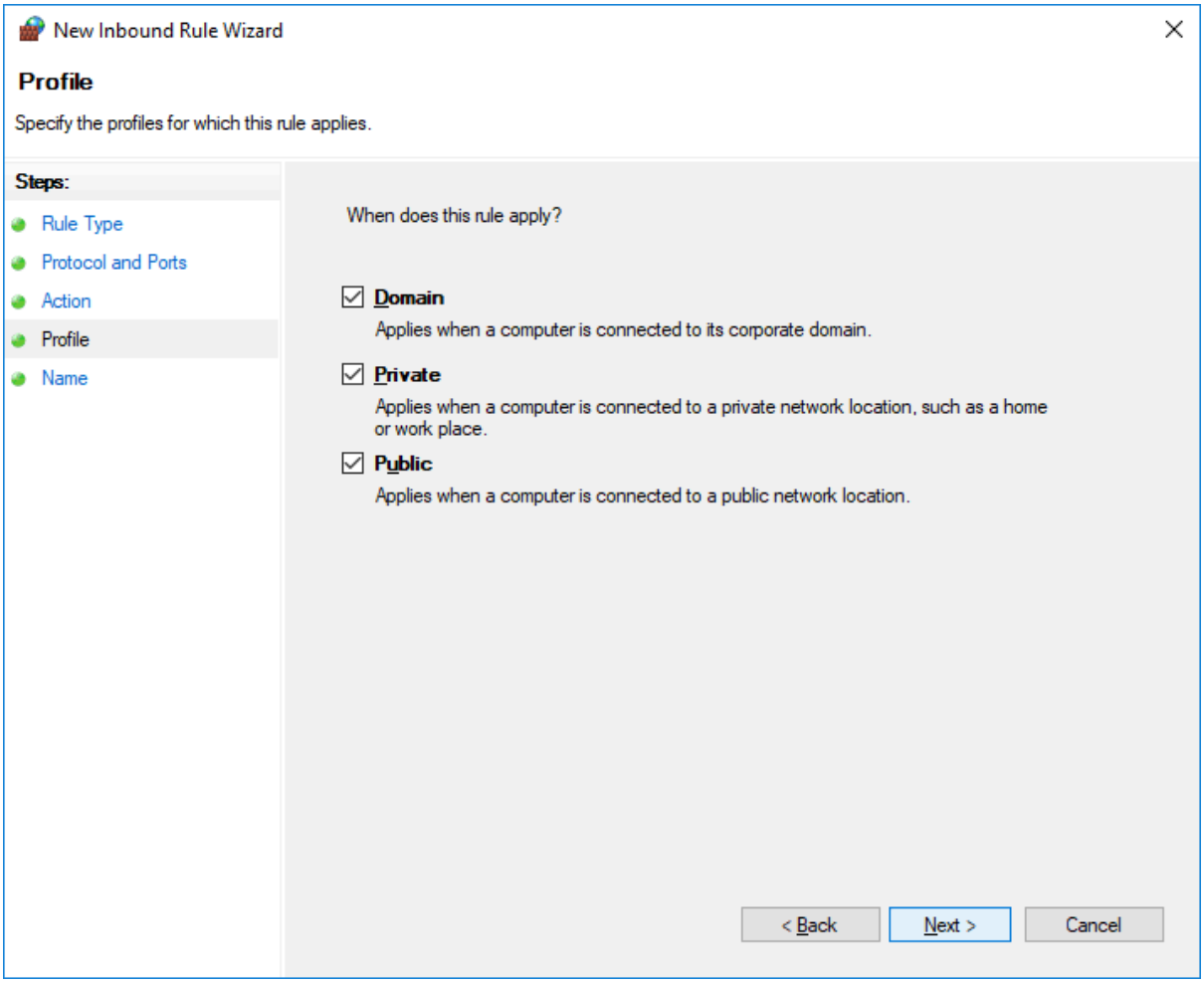
In this wizard step, enter the port numbers selected while running the Data Server Configuration utility. For this setup, ports 9810 through 9813 were selected. Enter these ports here and click on **Next**.

Figure 2.10. Allowing the Connection on the Specified Ports



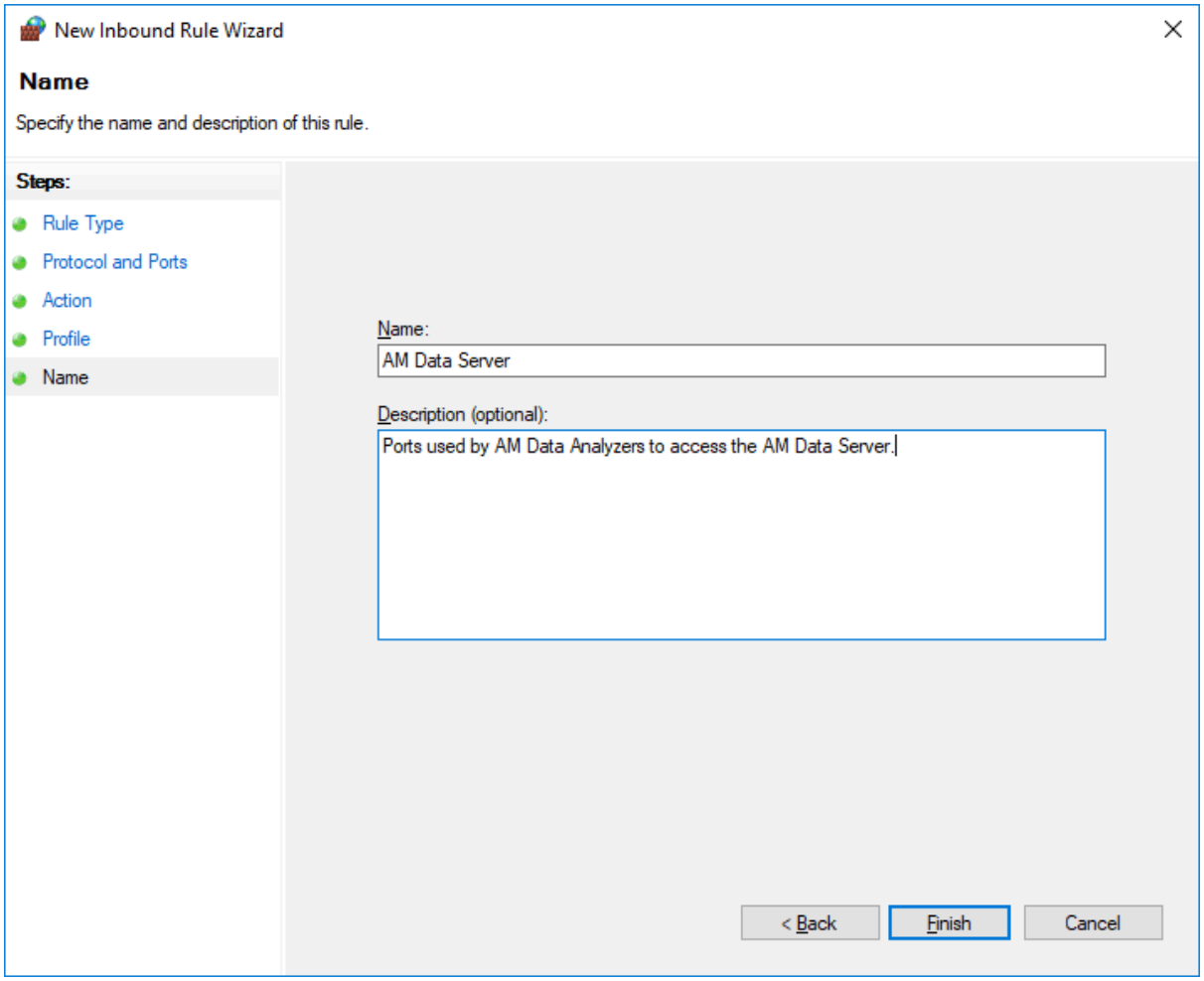
Select **Allow the connection**, then click on **Next**.

Figure 2.11. Applying Network Location Types



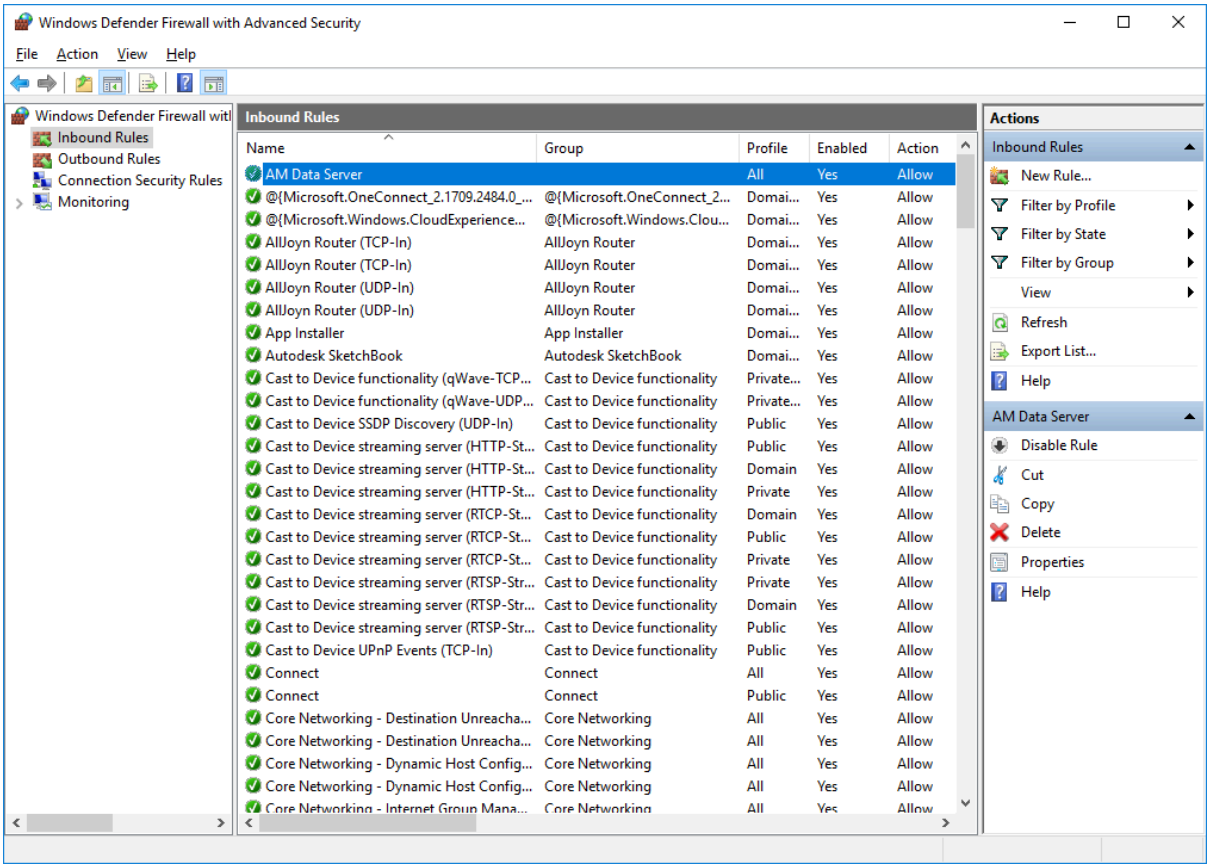
Select the checkboxes for the network profiles that apply to your site, then click on **Next**.

Figure 2.12. Specifying the Rule Name and Description



In this wizard step, give the rule a name and optional description. When you are done, click on **Finish**.

Figure 2.13. The Created Inbound Port Rule



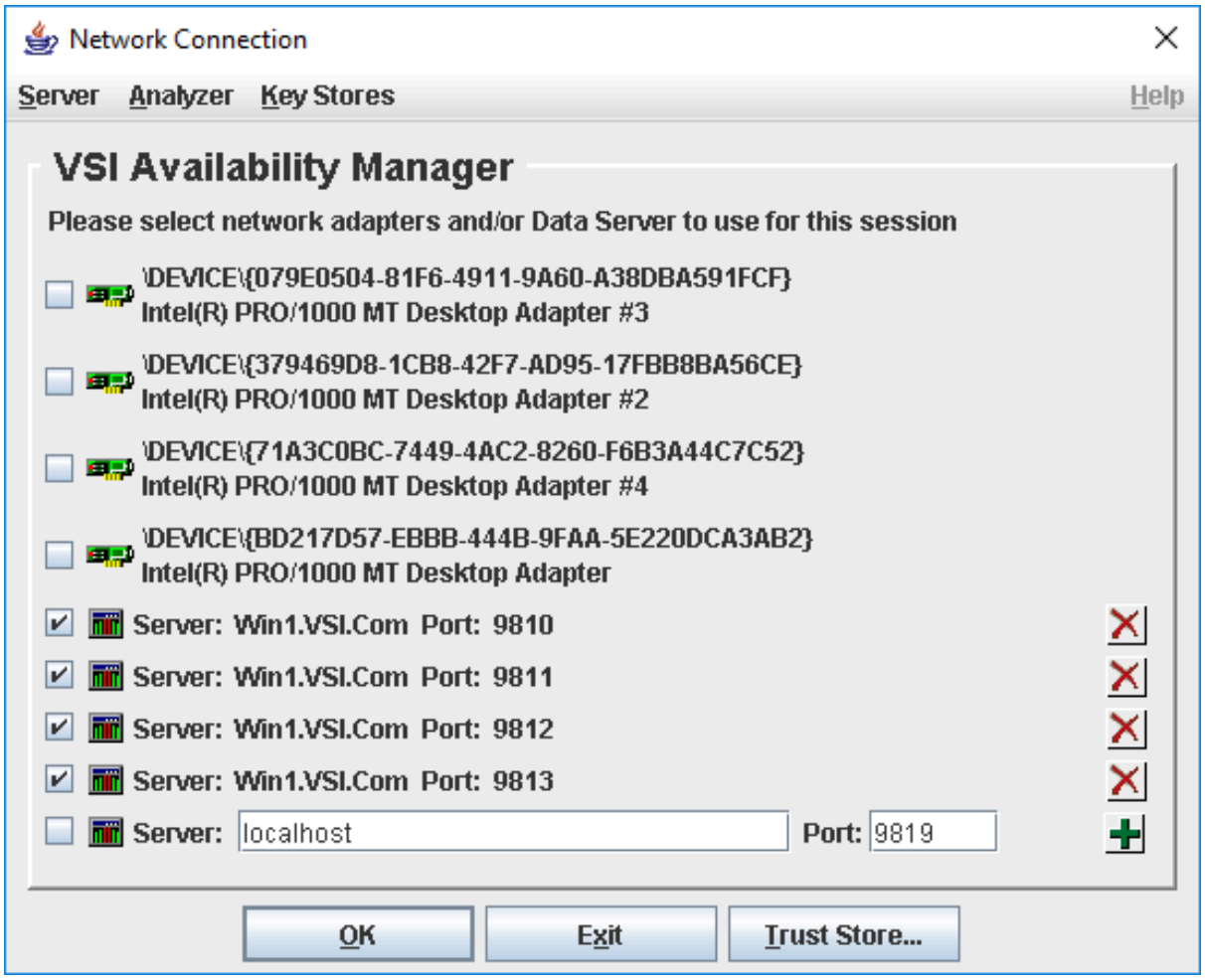
The Windows Firewall application closes the New Rule wizard window, and returns to the main window. The new rule created in the wizard steps is selected to highlight its presence.

2.1.3. Data Analyzer Steps

When you start the Data Analyzer, the Network Connections dialog appears. To monitor OpenVMS cluster D, which is accessed by port 9813, enter the IP address of the Windows system in the **Server** field, and 9813 in the **Port** field, then click on **OK**. To monitor all the OpenVMS cluster systems in the configuration example, click on the plus sign on the right and enter the Windows IP address and the other ports. Once there is an entry in the dialog for each port from 9810 through 9813, clicking on **OK** enables the Data Analyzer to monitor all four OpenVMS clusters. This setup corresponds to the setup shown in Figure 2.3.

Figure 2.14 assumes that the IP address for the Windows system is Win1.VSI.Com. All four entries use the same IP address to access the Data Server running on the Windows system. The port number indicates which network adapter the Data Analyzer uses to collect data, using the Data Server as an intermediary. In this example, port 9810 tells the Data Server to connect the Data Analyzer to the local LAN where OpenVMS cluster A resides. Since all four ports are entered and checked, the Data Analyzer displays data from all four OpenVMS clusters.

Figure 2.14. Network Connection Dialog in the Data Analyzer



Once the connections are entered into the Network Connection dialog, click on **OK** to start the Data Analyzer.