

# 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

---

# VSI Availability Manager Data Server Guide for Microsoft Windows



VMS Software

---

Copyright © 2024 VMS Software, Inc. (VSI), Boston, Massachusetts, USA

## Legal Notice

Confidential computer software. Valid license from VSI required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for VSI products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. VSI shall not be liable for technical or editorial errors or omissions contained herein.

HPE, HPE Integrity, HPE Alpha, and HPE Proliant are trademarks or registered trademarks of Hewlett Packard Enterprise.

Microsoft, Windows, Windows-NT and Microsoft XP are U.S. registered trademarks of Microsoft Corporation. Microsoft Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

<b>Preface .....</b>	<b>v</b>
1. About VSI .....	v
2. Intended Audience .....	v
3. Document Structure .....	v
4. Related Documents .....	v
5. VSI Encourages Your Comments .....	v
<b>Chapter 1. Introduction .....</b>	<b>1</b>
<b>Chapter 2. Configuration Example Used by This Guide .....</b>	<b>3</b>
2.1. Steps to Setup the Configuration Example .....	3
2.1.1. Data Server Steps .....	3
2.1.2. Windows Firewall Steps .....	7
2.1.3. Data Analyzer Steps .....	14



# 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<sup>1</sup> 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 [www.vsi.com](http://www.vsi.com) or contact us at [info@vmssoftware.com](mailto: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](mailto:docinfo@vmssoftware.com). Users who have VSI OpenVMS support contracts through VSI can contact [support@vmssoftware.com](mailto:support@vmssoftware.com) for help with this product.

---

<sup>1</sup>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.

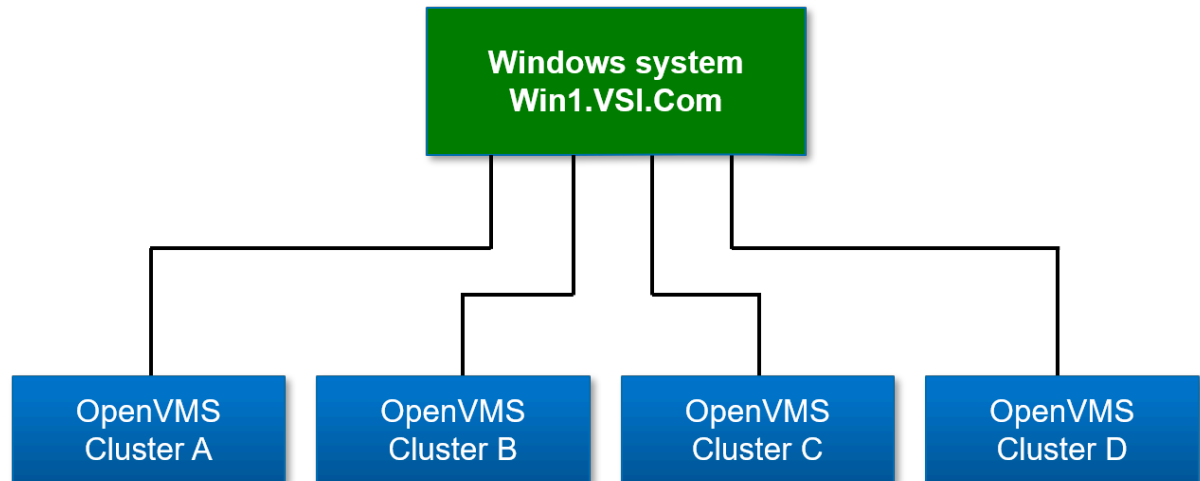




# Chapter 2. Configuration Example Used by This Guide

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**



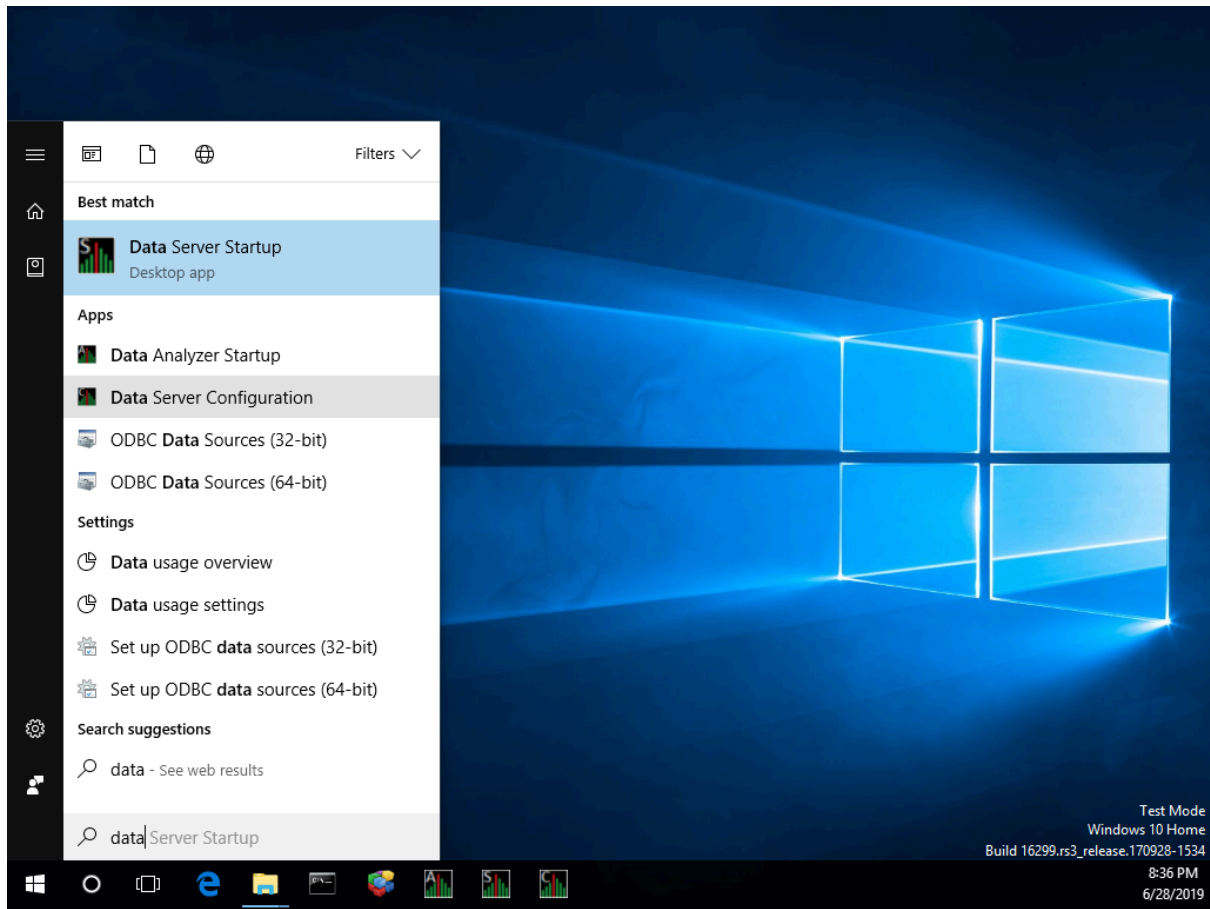
## 2.1. Steps to Setup the Configuration Example

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**

```

C:\Program Files\VMS Software Inc\VSI Availability Manager\C3.2-1B\AMConsoleLauncher.exe
StatusLogger.<ctor> - Opened log file AM_Server_20190628-2039.log for output
Fri, Jun 28th 20:39:17.412 Platform attributes, OS name and version = Windows Vista 6.2
Fri, Jun 28th 20:39:17.412 ** Log file opened for output **
Fri, Jun 28th 20:39:17.412
Fri, Jun 28th 20:39:17.412 VSI Availability Manager Server C3.2-1C (build 2007)
Fri, Jun 28th 20:39:17.412 - 2019, VMS Software, Inc.
Fri, Jun 28th 20:39:17.412
Fri, Jun 28th 20:39:17.426 Network adapters found on this system
Fri, Jun 28th 20:39:17.426 \DEVICE\{BD217D57-EBBB-444B-9FAA-5E220DCA3AB2} - Intel(R) PRO/1000 MT Desktop Adapter
Fri, Jun 28th 20:39:17.426 \DEVICE\{379469D8-1CB8-42F7-AD95-17F8B8BA56CE} - Intel(R) PRO/1000 MT Desktop Adapter #2
Fri, Jun 28th 20:39:17.426 \DEVICE\{079E0504-81F6-4911-9A60-A38DBA591FCF} - Intel(R) PRO/1000 MT Desktop Adapter #3
Fri, Jun 28th 20:39:17.426 \DEVICE\{71A3C08C-7449-4AC2-8260-F6B3A44C7C52} - Intel(R) PRO/1000 MT Desktop Adapter #4
Fri, Jun 28th 20:39:17.505 Port and network adapter associations used for OpenVMS systems
Fri, Jun 28th 20:39:17.505 Port - selected adapter description (adapter name)
Fri, Jun 28th 20:39:17.505 9810 - true Intel(R) PRO/1000 MT Desktop Adapter (\DEVICE\{BD217D57-EBBB-444B-9FAA-5E220DCA3AB2})
Fri, Jun 28th 20:39:17.505 9811 - true Intel(R) PRO/1000 MT Desktop Adapter #2 (\DEVICE\{379469D8-1CB8-42F7-AD95-17F8B8BA56CE})
Fri, Jun 28th 20:39:17.505 9812 - true Intel(R) PRO/1000 MT Desktop Adapter #3 (\DEVICE\{079E0504-81F6-4911-9A60-A38DBA591FCF})
Fri, Jun 28th 20:39:17.505 9813 - true Intel(R) PRO/1000 MT Desktop Adapter #4 (\DEVICE\{71A3C08C-7449-4AC2-8260-F6B3A44C7C52})
Fri, Jun 28th 20:39:17.521 Server is in configuration mode

Availability Manager Server Configuration Menu

Entry #    Enabled    Port #    Network adapter
-----
0          Yes       9810      Intel(R) PRO/1000 MT Desktop Adapter
1          Yes       9811      Intel(R) PRO/1000 MT Desktop Adapter #2
2          Yes       9812      Intel(R) PRO/1000 MT Desktop Adapter #3
3          Yes       9813      Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, l to list entries, or e to exit configuration

```

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**

```

C:\Program Files\WMS Software Inc\WSI Availability Manager\C3.2-1B\AMConsoleLauncher.exe
Fri, Jun 28th 20:39:17.426 \DEVICE\{379469D8-1CB8-42F7-AD95-17F8B8BA56CE} - Intel(R) PRO/1000 MT Desktop Adapter #2
Fri, Jun 28th 20:39:17.426 \DEVICE\{079E0504-81F6-4911-9A60-A38DBA591FCF} - Intel(R) PRO/1000 MT Desktop Adapter #3
Fri, Jun 28th 20:39:17.426 \DEVICE\{71A3C0BC-7449-4AC2-8260-F6B3A44C7C52} - Intel(R) PRO/1000 MT Desktop Adapter #4
Fri, Jun 28th 20:39:17.505 Port and network adapter associations used for OpenVMS systems
Fri, Jun 28th 20:39:17.505 Port - selected adapter description (adapter name)
Fri, Jun 28th 20:39:17.505 9810 - true Intel(R) PRO/1000 MT Desktop Adapter (\DEVICE\{BD217D57-E8BB-444B-9FAA-5E220DCA3AB2})
Fri, Jun 28th 20:39:17.505 9811 - true Intel(R) PRO/1000 MT Desktop Adapter #2 (\DEVICE\{379469D8-1CB8-42F7-AD95-17F8B8BA56CE})
Fri, Jun 28th 20:39:17.505 9812 - true Intel(R) PRO/1000 MT Desktop Adapter #3 (\DEVICE\{079E0504-81F6-4911-9A60-A38DBA591FCF})
Fri, Jun 28th 20:39:17.505 9813 - true Intel(R) PRO/1000 MT Desktop Adapter #4 (\DEVICE\{71A3C0BC-7449-4AC2-8260-F6B3A44C7C52})
Fri, Jun 28th 20:39:17.521 Server is in configuration mode

Availability Manager Server Configuration Menu

Entry #   Enabled   Port #   Network adapter
-----
0         Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1         Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2         Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3         Yes      9813     Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 3
Modify entry data for Intel(R) PRO/1000 MT Desktop Adapter #4 (y/n) [n] y
Enable network adapter? (y/n) [y] n

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 1

Availability Manager Server Configuration Menu

Entry #   Enabled   Port #   Network adapter
-----
0         Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1         Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2         Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3         No       ---      Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration

```

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**

```

C:\Program Files\WMS Software Inc\WSI Availability Manager\C3.2-1B\AMConsoleLauncher.exe
0         Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1         Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2         Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3         Yes      9813     Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 3
Modify entry data for Intel(R) PRO/1000 MT Desktop Adapter #4 (y/n) [n] y
Enable network adapter? (y/n) [y] n

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 1

Availability Manager Server Configuration Menu

Entry #   Enabled   Port #   Network adapter
-----
0         Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1         Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2         Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3         No       ---      Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 3
Modify entry data for Intel(R) PRO/1000 MT Desktop Adapter #4 (y/n) [n] y
Enable network adapter? (y/n) [n] y
Enable IP port number (9810-9830) 9820

Availability Manager Server Configuration Menu

Entry #   Enabled   Port #   Network adapter
-----
0         Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1         Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2         Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3         Yes      9820     Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration

```

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**

```

C:\Program Files\VMS Software Inc\VSI Availability Manager\C3.2-1B\AMConsoleLauncher.exe
Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 3
Modify entry data for Intel(R) PRO/1000 MT Desktop Adapter #4 (y/n) [n] y
Enable network adapter? (y/n) [y] n

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 1

Availability Manager Server Configuration Menu

Entry #    Enabled    Port #    Network adapter
0          Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1          Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2          Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3          No       ---      Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration 3
Modify entry data for Intel(R) PRO/1000 MT Desktop Adapter #4 (y/n) [n] y
Enable network adapter? (y/n) [n] y
Enable IP port number (9810-9830) 9820

Availability Manager Server Configuration Menu

Entry #    Enabled    Port #    Network adapter
0          Yes      9810     Intel(R) PRO/1000 MT Desktop Adapter
1          Yes      9811     Intel(R) PRO/1000 MT Desktop Adapter #2
2          Yes      9812     Intel(R) PRO/1000 MT Desktop Adapter #3
3          Yes      9820     Intel(R) PRO/1000 MT Desktop Adapter #4

Enter entry # to configure an entry, 1 to list entries, or e to exit configuration e

Exiting server configuration
Exiting server configuration momentarily

```

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.

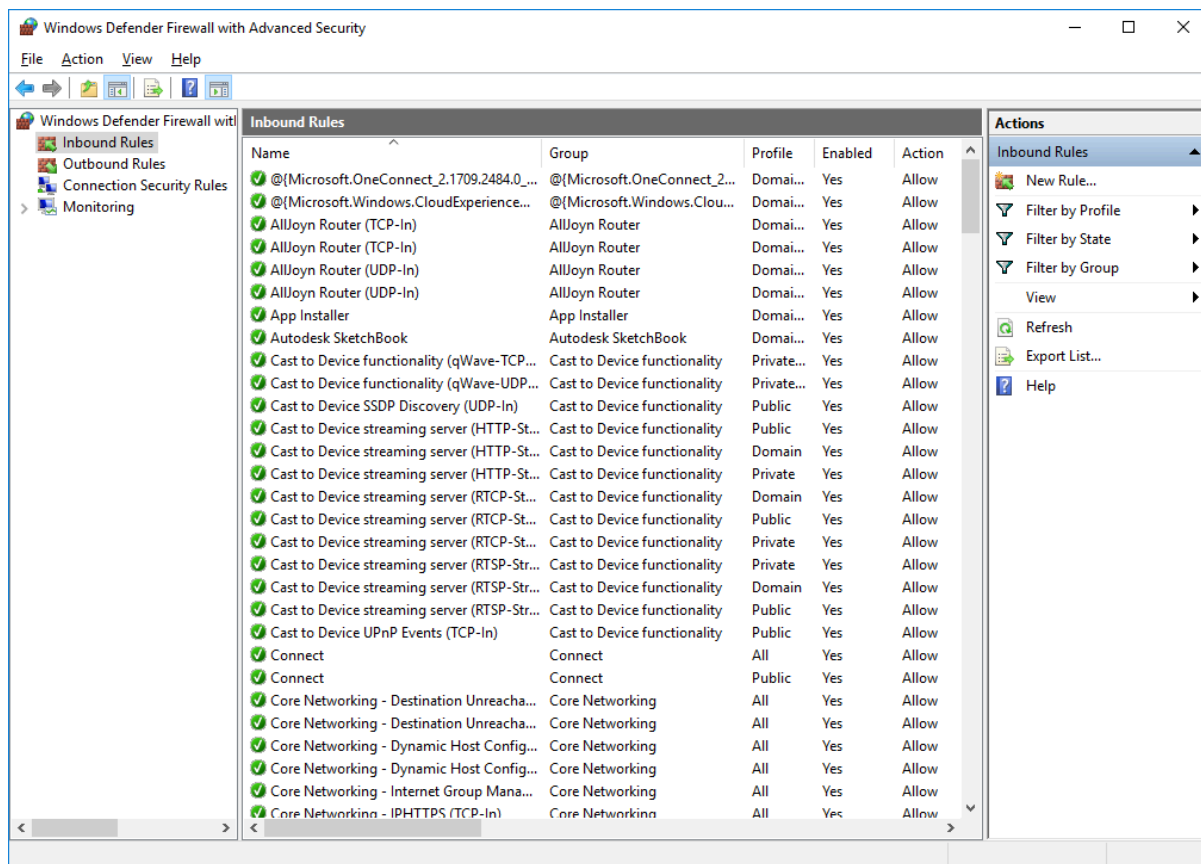
**Figure 2.7. Windows Defender Firewall with Advanced Security**

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.

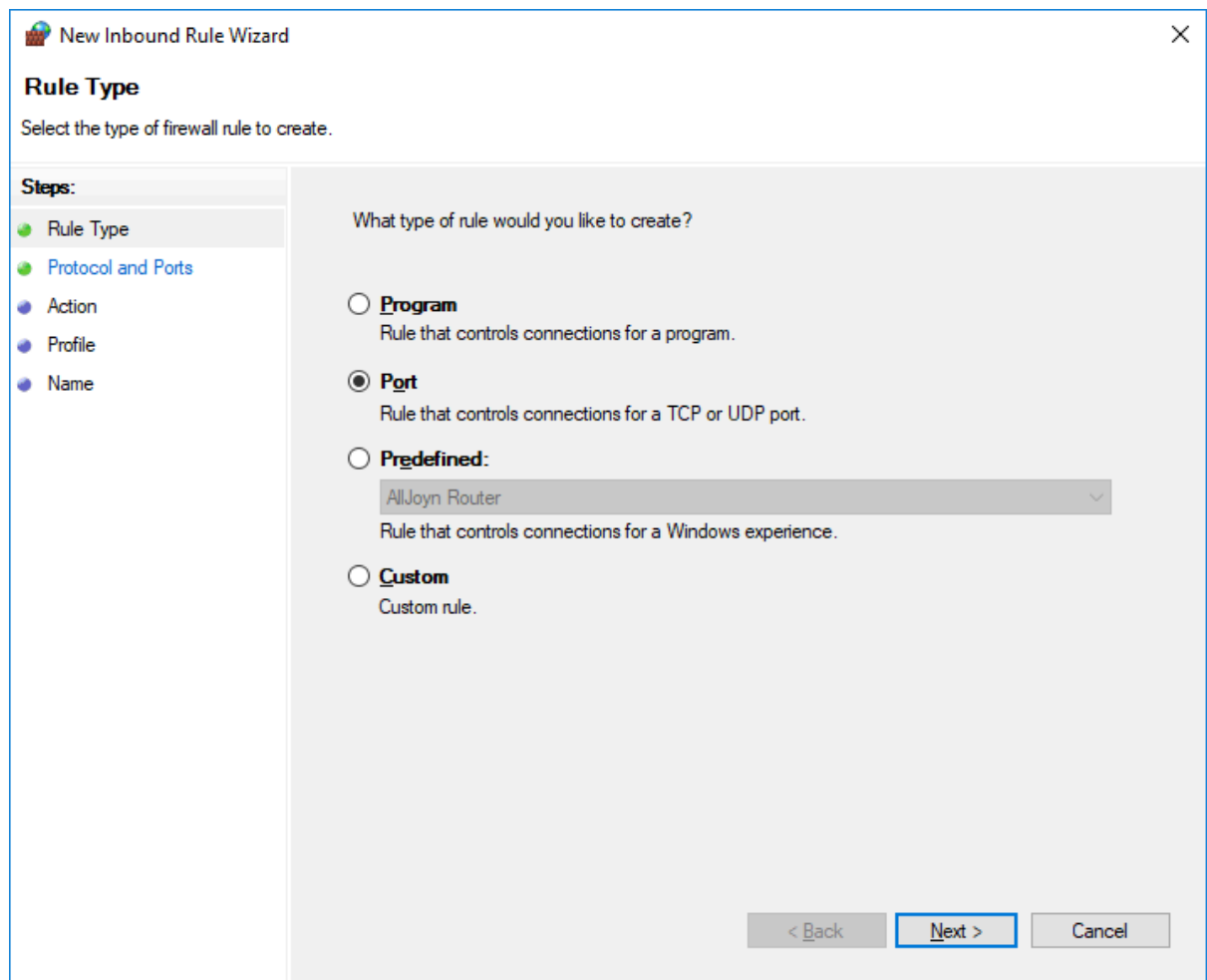
**Figure 2.8. Creating an Inbound Port Rule**

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**

The screenshot shows the 'New Inbound Rule Wizard' window with the 'Protocol and Ports' step selected in the left-hand 'Steps' pane. The main area contains two questions with radio button options. The first question, 'Does this rule apply to TCP or UDP?', has 'TCP' selected. The second question, 'Does this rule apply to all local ports or specific local ports?', has 'Specific local ports:' selected, with a text box containing '9810-9813' and an example '80, 443, 5000-5010' below it. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound Rule Wizard

**Protocol and Ports**

Specify the protocols and ports to which this rule applies.

**Steps:**

- Rule Type
- Protocol and Ports**
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ **TCP**

☐ **UDP**

Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

☒ **Specific local ports:**

Example: 80, 443, 5000-5010

< Back   Next >   Cancel

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**

The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard' with a close button (X) in the top right corner. Below the title bar, the word 'Action' is displayed in bold. A subtitle states: 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left side, there is a 'Steps:' list with five items: 'Rule Type', 'Protocol and Ports', 'Action' (which is highlighted with a grey background), 'Profile', and 'Name'. The main area of the dialog contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 1. 'Allow the connection' (selected with a filled radio button). Below it, a description reads: 'This includes connections that are protected with IPsec as well as those are not.' 2. 'Allow the connection if it is secure' (unselected). Below it, a description reads: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' Below this description is a 'Customize...' button. 3. 'Block the connection' (unselected). At the bottom right of the dialog, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

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

**Figure 2.11. Applying Network Location Types**

New Inbound Rule Wizard

**Profile**

Specify the profiles for which this rule applies.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

When does this rule apply?

☒ **Domain**  
Applies when a computer is connected to its corporate domain.

☒ **Private**  
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**  
Applies when a computer is connected to a public network location.

< Back   Next >   Cancel

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**

New Inbound Rule Wizard

**Name**

Specify the name and description of this rule.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:

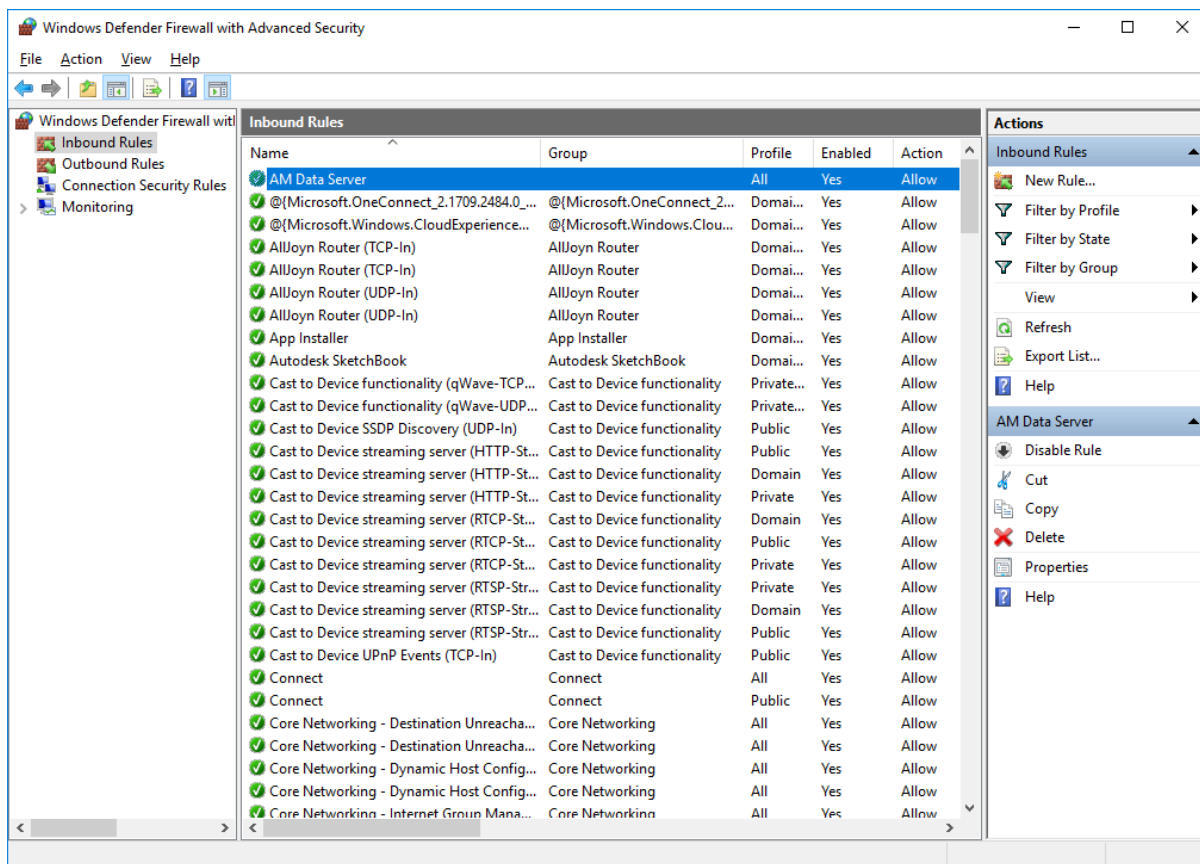
AM Data Server

Description (optional):

Ports used by AM Data Analyzers to access the AM Data Server.

< Back Finish Cancel

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

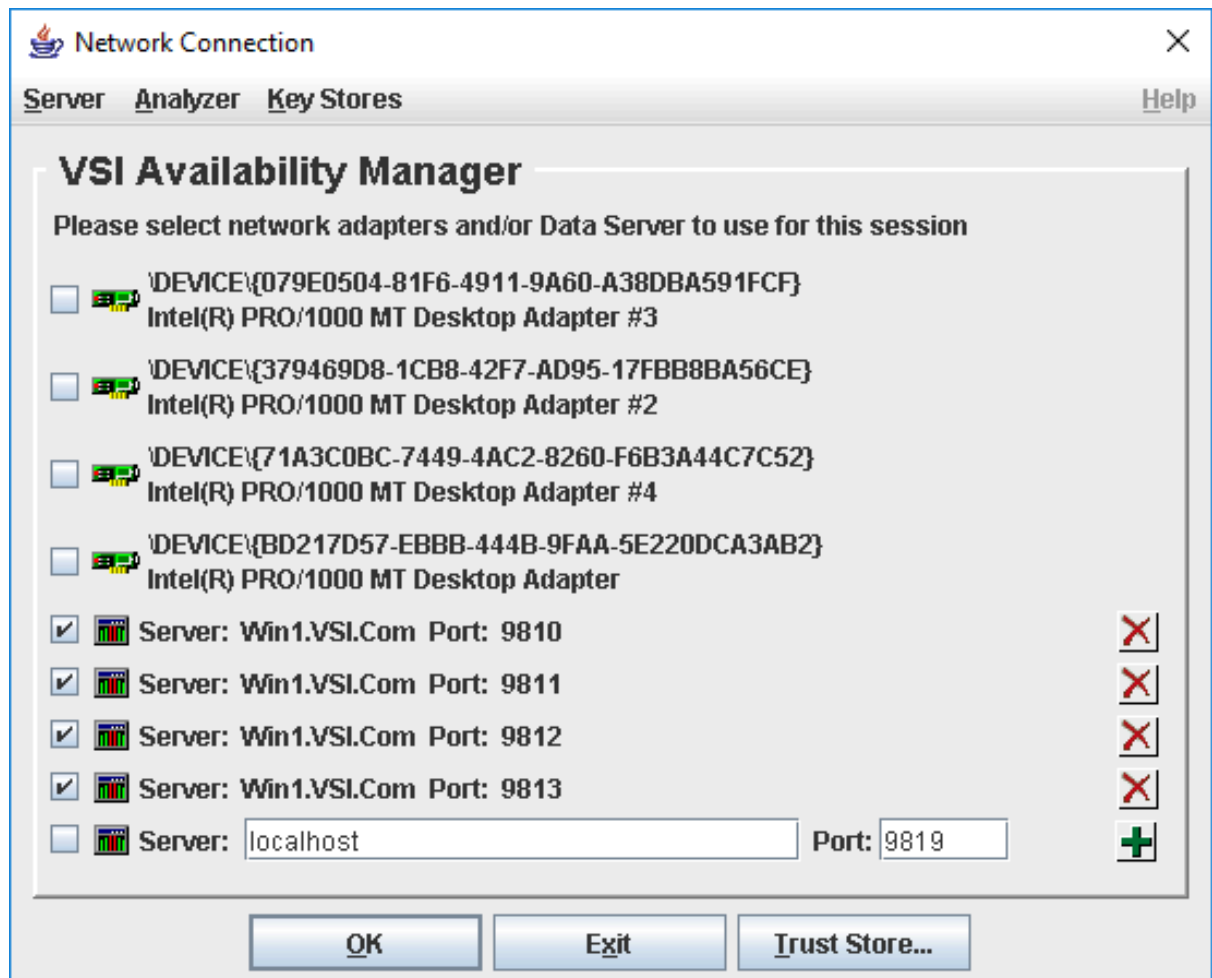
**Figure 2.13. The Created Inbound Port Rule**

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.

