Veritas Enterprise Vault™ Technical Note

Configuring a Windows Server's Firewall for File System Archiving

8.0 to 12 original release

VERITAS™

Veritas Enterprise Vault: Configuring a Windows Server's Firewall for File System Archiving

Last updated: 2017-08-04.

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

http://www.veritas.com/docs/000095758

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

http://www.veritas.com/docs/000001907

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community

Configuring a Windows server's firewall for File System Archiving

This document includes the following topics:

About access through a Windows server's firewall for File System Archiving

This technical note describes the access that Enterprise Vault File System Archiving (FSA) requires through a Windows server's firewall.

FSA requires access through the file server's firewall to do any of the following:

- Install the FSA Agent from a remote Enterprise Vault Administration Console.
- Archive files from the server.
- Create placeholder shortcuts on the server.
- Perform File Blocking on the server, or use the server as a File Blocking agent server for a NetApp filer.
- Perform FSA Reporting on the server, or use the server as an FSA Reporting proxy server for non-Windows file servers.

If a target server's firewall is enabled and you do not configure the firewall to allow the required access, the following problems occur:

- Installation of the FSA Agent from the Administration Console fails.
- The File System Archiving task fails. You may receive error messages such as the following from DTrace, or in the File System Archiving task report:
  - The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)
  - Error making file a placeholder file. Catastrophic failure (Exception from HRESULT: 0x8000FFFF)

Firewall access required for archiving without the FSA Agent

You can configure a Windows file server target without installing the FSA Agent, if you do not require placeholder shortcuts, File Blocking, or FSA Reporting.

Table 1-1 lists the access that FSA requires through a Windows server's firewall, for archiving without the FSA Agent.

The table lists the inbound port requirements, and the associated programs and services. From Windows Server 2008 onwards, you can use Windows Firewall rules to open selected ports for specified programs and their services, for enhanced security.

Table 1-1 Windows server firewall ports required for archiving without the FSA Agent

Inbound port	Protocol	Program	Service	Required for	Notes
445	TCP	System	(none)	CIFS share (SMB file sharing)	On Windows Server 2003 this port is included in the supplied Windows Firewall exception **File and Printer Sharing**. On Windows Server 2008 R2 this configuration is provided for example by the supplied inbound rule **File and Printer Sharing (SMB-In)**.

Table 1-1 Windows server firewall ports required for archiving without the FSA Agent *(continued)*

Inbound port	Protocol	Program	Service	Required for	Notes
135	TCP	svchost.exe	RpcSs	RPC (DCOM) Endpoint Mapper	On Windows Server 2008 R2 this configuration is provided for example by the supplied inbound rule **Com+ Network Access (DCOM-In)**.
RPC Dynamic Ports (Randomly allocated high TCP port)	TCP	svchost.exe	Winmgmt	RPC (DCOM) connection ports for Windows Management Instrumentation (WMI)	On Windows Server 2008 R2 this configuration is provided for example by the supplied inbound rule **DFS Management (WMI-In)**.

Firewall access required for installing and using the FSA Agent

To enable the installation of the FSA Agent from a remote Administration Console, Enterprise Vault requires the same access as for archiving without the FSA Agent.

See Table 1-1.

For File System Archiving with the FSA Agent, the FSA Agent programs also require access through the server's firewall.

Enterprise Vault installs the FSA Agent programs on the file server in the Enterprise Vault program folder, typically `C:\Program Files (x86)\Enterprise Vault`.

Table 1-2 lists the FSA Agent programs and the ports and protocols to associate with them. You must configure the server's firewall to allow access for the programs whose functions you require.

Table 1-2 Windows server firewall access required for the FSA Agent programs

Inbound port	Protocol	Program	Service	Required for	Notes
RPC Dynamic Ports	TCP	EvPlaceholderService.exe	(none)	Placeholder shortcuts	Required if you configure placeholder shortcuts for the server.
RPC Dynamic Ports	TCP	FileScreenService.exe	(none)	File Blocking	Required if you configure File Blocking for the server. If you configure File Blocking Notifications such as Windows Messenger Service, SMTP, and event logging, additional access is required. Refer to your Microsoft documentation for information on the ports that are required for these services.
RPC Dynamic Ports	TCP	FSAReportingService.exe	(none)	FSA Reporting	Required if you configure FSA Reporting for the server.

Where to find more about Windows Firewall ports and port configuration

For general information on configuring Windows Firewall's ports and DCOM access, see the Microsoft documentation for your target server's operating system.

- For an overview of Windows network ports and RPC, see the following Microsoft article, and the articles in its Reference section under “Remote Procedure Calls and DCOM”:
  http://support.microsoft.com/kb/832017
- For information for Windows Server 2003 on creating rules to allow the inbound traffic that uses dynamic RPC, see the following Microsoft article:
  https://msdn.microsoft.com/library/aa389286.aspx
- For information for Windows Server 2008 and later on creating rules to allow the inbound traffic that uses dynamic RPC, see the following Microsoft article:

http://technet.microsoft.com/library/cc732839.aspx

- For guidelines on how to configure dynamic port ranges for TCP/IP on Windows Server 2008 and later, see the following Microsoft knowledge base article: http://support.microsoft.com/kb/929851
- For more information about the ports that Enterprise Vault uses, see the appendix “Ports used by Enterprise Vault” in the *Administrator's Guide*.