

AppAssure Software Inc.

Written By: Kaustubh Pradhan and
Joseph Hand

[REPLAY: ENVIRONMENTAL ASSESSMENT GUIDE]

This guide will walk you through the environment before you install Replay and help you understand some of the things that will be necessary for a successful installation.

TABLE OF CONTENTS

HARDWARE REQUIREMENTS	3
Processor and Memory.....	3
Disk Subsystem.....	3
Physical Network	3
NETWORKING INFRASTRUCTURE.....	4
MICROSOFT VOLUME SHADOW SERVICE	6
Check the core services	6
COM+ Event System service is enabled.....	6
Volume Shadow Copy service is enabled	6
Check that the MS Software Shadow Copy Provider service is enabled.....	6
VSS Writers on the Agent.....	6
VSS Providers on the Agent	8
VSS Storage Space Availability	8
Enable Exchange VSS writer in Small Business Server 2003	8
SOFTWARE REQUIREMENTS.....	10
Supported Operating Systems	10
Protecting Exchange 2003 and Exchange 2007 with Replay for Exchange	10
Protecting SQL 2000, 2005 or 2008 with Replay.....	10

HARDWARE REQUIREMENTS

PROCESSOR AND MEMORY

Replay Core and Agent can run as a 32-Bit or 64-Bit application. Minimum processor requirements are 3 GHz or multi-core 2 GHz (or greater). Use Multi-core CPUs. Two CPUs will not be as fast as one CPU that is twice as fast. In addition, larger L2 processor caches will provide better performance.

Minimum memory requirements are 4 GB for 32-Bit systems and 8 GB for 64-Bit systems.

DISK SUBSYSTEM

Replay stores the recovery points of protected servers as epochs in a flat file format on a volume designated as the Replay repository. These repository volumes should preferably reside on a low latency device. Replay supports the use of block-level and CIFS or SMB devices. Devices such as internal storage, direct attached or distant devices accessed via a storage area network (SAN) are classified as Block-level devices. CIFS or SMB devices are network shares or NAS.

On the agent side, Replay can protect volumes that reside on internal drives, direct attached storage (DAS) or on Storage Area Networks (SAN). Data residing on Network Attached Storage (NAS) cannot be protected by Replay.

PHYSICAL NETWORK

Network performance is critical to Replay as it uses the network connection to transfer the snapshots from the protected server to the Replay server. Therefore, all components of the network subsystem need to perform optimally and ensure maximum performance.

Use adapters with the Gigabit bandwidth available for best performance. Note that increasing bandwidth increases the number of transmissions that are taking place and in turn makes more work for your system, including more interrupts being generated. Remove unused network adapters to reduce overhead.

Replay delivers a consistent throughput of over 5 GB/m on a 1Gbps network.

Additional factors that may benefit network performance are

1. Checksum offloading, IPSEC offloading, and large send offloading on the network card
2. Divide the network into multiple subnets or segments, attaching the server to each segment with a separate adapter. Use a subnet or segment for Replay snapshots. This reduces congestion at the server by spreading server requests.
3. Use Jumbo Frames on the backup network. Supporting larger Maximum Transmission Units (MTUs) and thus larger frame sizes, specifically Jumbo Frames, will reduce the network stack overhead incurred per byte. A 20% TCP throughput increase has been measured when the MTU was changed from 1514 to 9000. Also, a significant reduction of CPU utilization is obtained due to the fewer number of calls from the network stack to the network driver.
4. Enabling "Receive Side Scaling" allows simultaneous processing of network requests on multiple processors insure both improved performance through parallelism and CPU load distribution amongst the system processors. Receive Side Scaling, when supported by the underlying hardware, provides this capability for TCP traffic and the technology is recommended by Replay where the Replay server services requests from a large number of connections.

NETWORKING INFRASTRUCTURE

Like many IP based products, Replay relies heavily on the networking infrastructure within the environment. This covers anything from DNS and ports to firewalls and permissions. For local configurations, GigE networks are recommended. For WAN configurations when using Replay Replication, any type of link is supported, but replication performance is highly dependent on the quality of the link and the amount of data being transferred. To prepare for a smooth installation, Replay requires the following:

1. Service Account
 - a. That has local full administrative rights.
 - b. The right to Log in as a Service
 - c. Can be a local account*
 - d. If you are protecting Exchange workloads, the Replay Agent service must run under an Exchange administrator account, which must also have local administrative privileges on the Exchange server.
2. Working DNS
 - a. You should be able to ping each server by NETBIOS name and the Fully Qualified Domain Name (FQDN).
 - b. Hosts files can be leveraged where DNS cannot.

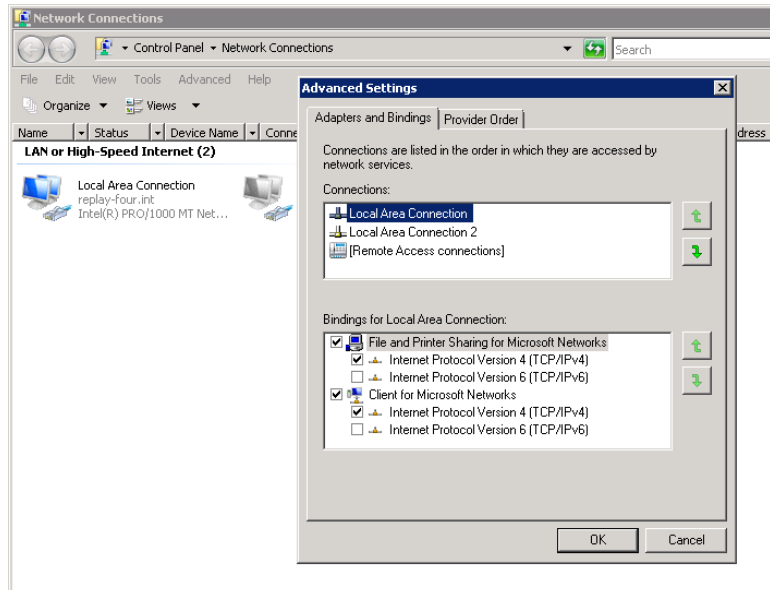
3. Firewalls

- a. The following ports should be allowed or the firewall should be disabled:

Port	Port Number	Purpose
TCP	8001/TCP	Used by Replay for transfers from the protected server to the Replay server
TCP	8002/TCP	Used by Replay for mounting existing recovery points by Replay DSM or rollback
TCP	8003/TCP	Used by Replay administrative console to communicate with the MMC
TCP	8004/TCP	Used by Replay server to communicate with the agent on the protected server.
TCP	8005/TCP	Used as the default port for WAN based replication.

4. Connections Order

- a. Under Advanced Settings in the Network Connections window, on the Adapters and Bindings tab, make sure that the connection listed on the top is the network connection you will be using for backup communications.



5. Private Backup Networks

- a. For performance reasons, you may decide to use a dedicated backup network. This is done by using separate NICs with a separate subnet and hosts files to sort out the naming issues. By utilizing a backup network, you are moving any traffic associated with backup off the production network.

***NOTE:** Replay can take full advantage of “Passthrough”. This is the ability to use the same username and password, but from either different domains or non-domain machines. For example, you may have a server, which is part of the domain ACMECORP, running the Replay Agent Service by logging on with an ACMECORP domain account called REPLAYSVC with a password of “widget01” that has been granted local admin rights on the server to be backed up. The Core server is not a part of the ACMECORP domain, but a standalone system called REPLAYCORE. You can create a service account on REPLAYCORE called REPLAYSVC with a password of “widget01”. To Replay, the two accounts ACMECORP\REPLAYSVC and REPLAYCORE\REPLAYSVC are the same account as long as the passwords match.

MICROSOFT VOLUME SHADOW SERVICE

Replay uses the Volume Shadow Copy Service (VSS) that is included in the Microsoft Windows Server 2003, 2008 and Windows XP, Windows Vista and Windows 7 operating systems to take volume shadow copies. VSS is a mechanism for creating consistent point-in-time copies of data known as shadow copies. VSS produces consistent shadow copies by coordinating Replay with business applications (Exchange, SQL etc), file-system services.

Before installing Replay Agents on the application servers, it is necessary to verify that you have installed the latest Windows service packs and the latest VSS updates.

Here are some simple steps to check the VSS subsystem. Check the following to ensure that the VSS subsystem on the protected server is in a healthy state

CHECK THE CORE SERVICES

COM+ Event System service is enabled

The Volume Shadow Copy Service (VSS) relies on COM+ to deliver events to VSS components and applications. If the COM+ Event System service is unavailable, VSS cannot function properly.

1. To check that the COM+ Event System service is enabled:
2. Click Start, click Administrative Tools, and then click Services.
3. In the results pane, double-click COM+ Event System.
4. Ensure that Startup type is set to Automatic.
5. Click OK.

Volume Shadow Copy service is enabled

To check that the Volume Shadow Copy service is enabled:

1. Click Start, click Administrative Tools, and then click Services.
2. In the results pane, double-click Volume Shadow Copy.
3. Ensure that Startup type is set to Manual.
4. Click OK.

Check that the MS Software Shadow Copy Provider service is enabled

To check that the MS Software Shadow Copy Provider service is enabled:

1. Click Start, click Administrative Tools, and then click Services.
2. In the results pane, double-click MS Software Shadow Copy Provider.
3. Ensure that Startup type is set to Manual.
4. Click OK.

VSS WRITERS ON THE AGENT

To test the status of the VSS writers on the Agent, perform the following steps

1. Open an elevated Command Prompt.
2. Click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.
3. Type `vssadmin list writers`, and then press Enter.
4. The output should appear as follows:

```

C:\>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Writer name: 'System Writer'
  Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
  Writer Instance Id: {d3b95161-b724-450a-9d40-b914ecf5ef8e}
  State: [1] Stable
  Last error: No error

Writer name: 'ASR Writer'
  Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
  Writer Instance Id: {48ed2aa7-4972-466f-ba3c-e7e0665ba06d}
  State: [1] Stable
  Last error: No error

Writer name: 'IIS Config Writer'
  Writer Id: {2a40fd15-dfca-4aa8-a654-1f8c654603f6}
  Writer Instance Id: {abbaaf35-e158-47db-b4b4-9abe2e3975b6}
  State: [1] Stable
  Last error: No error

Writer name: 'IIS Metabase Writer'
  Writer Id: {59b1f0cf-90ef-465f-9609-6ca8b2938366}
  Writer Instance Id: {e5bf750f-975d-4dc5-8eed-3943f8af9dc1}
  State: [1] Stable
  Last error: No error

Writer name: 'COM+ REGDB Writer'
  Writer Id: {542da469-d3e1-473c-9f4f-7847f01fc64f}
  Writer Instance Id: {85f1feb4-3fe6-4621-b2e8-e1673b397b67}
  State: [1] Stable
  Last error: No error

Writer name: 'Shadow Copy Optimization Writer'
  Writer Id: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
  Writer Instance Id: {a6f3127c-5013-4819-bda7-5922a7242c70}
  State: [1] Stable
  Last error: No error

Writer name: 'Registry Writer'
  Writer Id: {afbab4a2-367d-4d15-a586-71dbb18f8485}
  Writer Instance Id: {480efb0e-32da-49da-843d-25d139bb9ce2}
  State: [1] Stable
  Last error: No error

Writer name: 'Microsoft Exchange Writer'
  Writer Id: {76fe1ac4-15f7-4bcd-987e-8e1acb462fb7}
  Writer Instance Id: {058ab8cc-a186-44b4-9ee7-ba90c46252ad}
  State: [1] Stable
  Last error: No error

Writer name: 'WMI Writer'
  Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
  Writer Instance Id: {5b433de4-ec2-4140-8bda-13cf72343cf0}
  State: [1] Stable
  Last error: No error

Writer name: 'BITS Writer'
  Writer Id: {4969d978-be47-48b0-b100-f328f07ac1e0}
  Writer Instance Id: {03140b75-22b0-4d97-bdc3-de7ddc7281b3}
  State: [1] Stable
  Last error: No error

C:\>

```

The output of this command should provide all writers registered with VSS. Check the State of the Writers. If the state is anything other than Stable, it might be a cause of concern; however, it does not necessarily have to be a cause of backup failure. If the Exchange writer is not in stable state (in "Retryable error" state as shown below) then we have to restart the information store service on the exchange server to get the exchange server in stable state.

```

Writer name: 'Microsoft Exchange Writer'
  Writer Id: {76fe1ac4-15f7-4bcd-987e-8e1acb462fb7}
  Writer Instance Id: {5f6c3fb9-f287-48eb-aa62-ac493514a00e}
  State: [14] Failed
  Last error: Retryable error

```

Upon restarting the information store service, you should see "No error" as shown below.

```
Writer name: 'Microsoft Exchange Writer'  
Writer Id: <76fe1ac4-15f7-4bcd-987e-8e1acb462fb7>  
Writer Instance Id: <050f1ad1-9890-4c72-8bb9-ea45b1410a40>  
State: [1] Stable  
Last error: No error
```

Refer to MS KB 838133 (<http://support.microsoft.com/kb/838183>) How to turn on the Exchange writer for the Volume Shadow Copy service in Windows Small Business Server 2003

VSS PROVIDERS ON THE AGENT

To test the status of the VSS writers on the Agent, perform the following steps

1. Open an elevated Command Prompt.
2. Click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.
3. Type `vssadmin list providers`, and then press Enter.
4. The output should appear as follows:

```
C:\>vssadmin list providers  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
<C> Copyright 2001-2005 Microsoft Corp.  
  
Provider name: 'Microsoft Software Shadow Copy provider 1.0'  
Provider type: System  
Provider Id: <b5946137-7b9f-4925-af80-51abd60b20d5>  
Version: 1.0.0.7  
  
C:\>_
```

The output of the command must list the provider name "Microsoft Software Shadow Copy Provider 1.0". If any other compatible hardware VSS providers are installed on the agent, they will be listed here.

VSS STORAGE SPACE AVAILABILITY

The Volume Shadow Copy Service (VSS) requires sufficient storage space to create the shadow copies. The volume shadow copy storage area must be on an NTFS file system volume. To successfully create a shadow copy for volumes less than 500 megabytes, the minimum is 50 megabytes of free space. For volumes more than 500 megabytes, the minimum is 320 megabytes of free space. Lastly, maintain at least 1 gigabyte of free disk space on each volume if volume size is more than 1 gigabyte.

Do not store the volume shadow copy storage area on a storage device that can be easily removed from the computer for e.g. a USB disk. Do not store the volume shadow copy storage area on a storage device that may not be available to Windows until late in the system startup sequence. For example, a logical unit number (LUN) created on an Internet SCSI (iSCSI) storage subsystem might not appear until a software initiator has started. Lastly, also make sure that Disk Management displays an online status for fixed disks and a Healthy status for volumes.

ENABLE EXCHANGE VSS WRITER IN SMALL BUSINESS SERVER 2003

By default, the Setup program for Microsoft Windows Small Business Server 2003 disables the Microsoft Exchange Server 2003 writer for the Volume Shadow Copy service. The Exchange 2003 writer may cause conflicts with the Backup utility (NTBackup.exe). However, you can manually turn on the Exchange writer for use with Replay.

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and then double-click the following registry subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
3. Double-click the Disable Exchange Writer value.
4. In the Value data text box, change the value from 1 to 0, and then click OK.
5. Quit Registry Editor.
6. Click Start, point to Administrative Tools, and then click Services.
7. Stop and then restart the Microsoft Exchange Information Store service.

SOFTWARE REQUIREMENTS

SUPPORTED OPERATING SYSTEMS

Operating System	Platform Architecture
Windows® Server 2008 R2	64-bit
Windows® Server 2008	64-bit
Windows® Server 2003 R2	32-bit or 64-bit
Windows® Server 2003	32-bit or 64-bit
Windows® Small Business Server 2008	64-bit
Windows® Small Business Server 2003	32-bit
Windows® Vista	32-bit or 64-bit
Windows® 7	32-bit or 64-bit
Windows® XP	32-bit or 64-bit

PROTECTING EXCHANGE 2003 AND EXCHANGE 2007 WITH REPLAY FOR EXCHANGE

Replay for Exchange support includes the ability to perform periodic mountability checks on all databases, nightly or weekly page-by-page integrity checksum checks on all databases and finally the ability to truncate storage group logs on the exchange server. These features are only exposed if ..

		and Replay Core runs on			
Protected Application and Platform		Windows Server 2003 32-Bit	Windows Server 2003 64-Bit	Windows Server 2008 32-Bit	Windows Server 2008 64-Bit
If Replay Agent is installed on	Exchange Server 2003 on Windows Server (x86)	Yes	Yes	No	No
	On Exchange Server 2007 on Windows 2003 (x64)	No	Yes	No	Yes
	On Exchange Server 2007 on Windows 2008 (x64)	No	Yes	No	Yes

PROTECTING SQL 2000, 2005 OR 2008 WITH REPLAY

Replay for SQL support includes the ability to perform an instance aware nightly attachability checks on all databases using a locally installed instance of SQL on the Replay Core. These features are only exposed if ..

		And Replay Core runs on			
Protected Application and Platform		Windows Server 2003 32-Bit*	Windows Server 2003 64-Bit*	Windows Server 2008 32-Bit*	Windows Server 2008 64-Bit*
If Replay Agent is installed on	SQL 2000 on Windows 2003 (x86)	Yes	Yes	Yes	Yes
	On SQL 2005 on Windows 2003 (x86)	Yes	Yes	Yes	Yes
	On SQL 2005 on Windows 2003 (x64)	Yes	Yes	Yes	Yes
	On SQL 2008 on Windows 2008 (x86)	Yes	Yes	Yes	Yes

		And Replay Core runs on			
Protected Application and Platform		Windows Server 2003 32-Bit*	Windows Server 2003 64-Bit*	Windows Server 2008 32-Bit*	Windows Server 2008 64-Bit*
	On SQL 2008 on Windows 2008 (x64)	Yes	Yes	Yes	Yes

Replay Attachability test requires that equal or a newer version of SQL server be installed on the Replay Core

