

AppAssure Software Inc.

Written By: Kaustubh Pradhan &
Joseph Hand

[REPLAY: TROUBLESHOOTING GUIDE]

This guide describes the considerations you should take into account when troubleshooting issues with Replay technology.

TABLE OF CONTENTS

TABLE OF CONTENTS _____ 3

REPLAY _____ 5

 PRODUCT ARCHITECTURE _____ 5

 REPLAY UNIQUE FEATURES _____ 5

TROUBLESHOOTING REFERENCE _____ 7

COLLECTING LOG FILES FOR SUPPORT _____ 8

 Collecting Log from the Replay Core _____ 8

 Collecting Logs from the Replay Agents _____ 8

REPLAY SERVICE MANAGEMENT _____ 9

 Using Services _____ 9

 Using the command line _____ 9

NETWORK CONNECTIVITY _____ 10

 Validate Network Connectivity _____ 10

 Multi-Homed Hosts _____ 10

 Name Resolution _____ 10

 Firewall and Port Availability _____ 10

PERMISSION ISSUES _____ 12

 Service Account _____ 12

 Local Group Membership _____ 12

 Local Server Rights _____ 12

 Exchange 2003 Administrator Role _____ 13

 Permissions to the MDBDATA folder in Exchange 2003 _____ 14

 Exchange 2007 Administrator Role _____ 14

 Permissions to the MDBDATA folder in Exchange 2007 _____ 15

AUTHENTICATION _____ 16

REPLICATION _____ 17

 Validate Network Connectivity _____ 17

 Port Availability _____ 17

 Authentication _____ 18

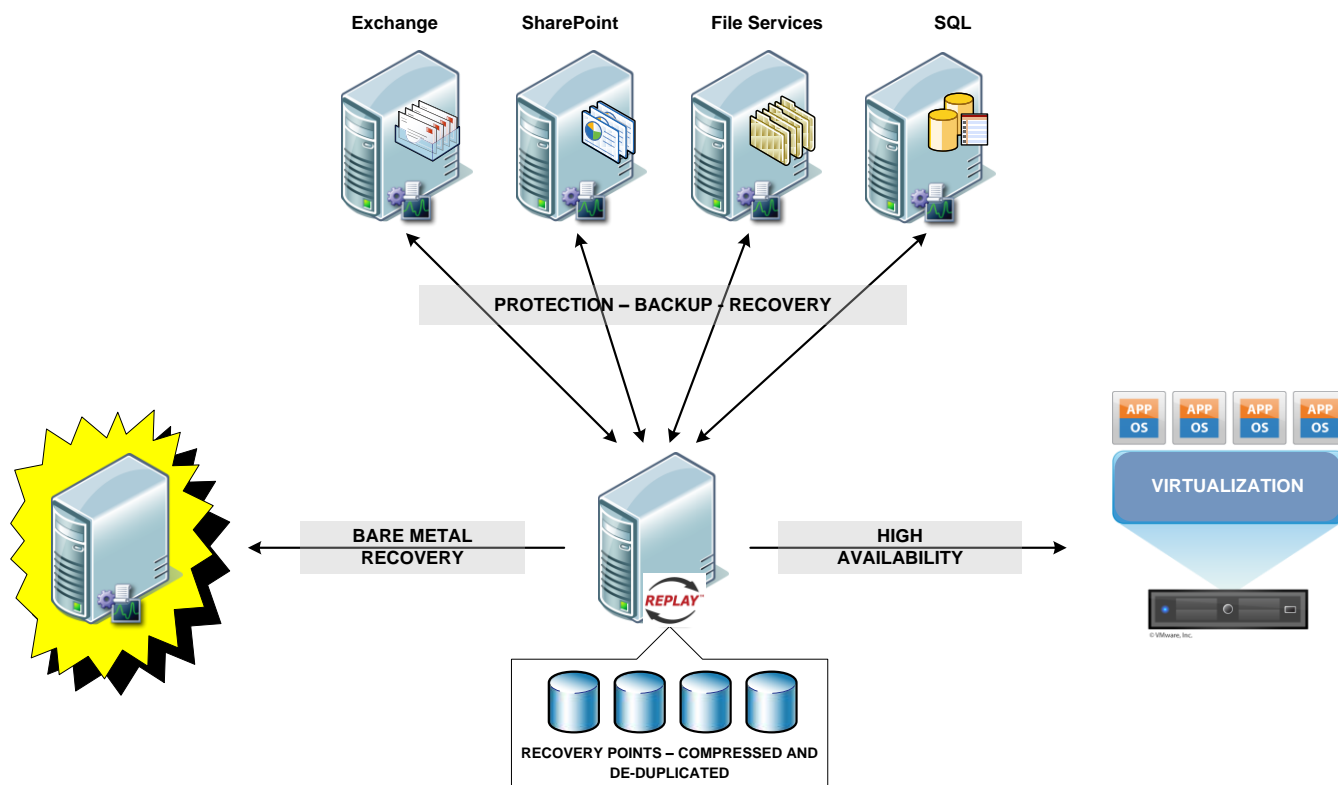
 User Access Control (UAC) _____ 18

MICROSOFT VOLUME SHADOW COPY SERVICE _____	19
Check The Core Services _____	19
VSS Writers on the Agent _____	19
VSS Providers on the Agent _____	21
VSS Storage Space Availability _____	21
Enable Exchange VSS writer in Small Business Server 2003 _____	22
VSS Troubleshooting _____	22
Volume Shadow Copy Time-Out Error _____	24

REPLAY

PRODUCT ARCHITECTURE

Replay can be deployed as a single-server or a multi-server architecture. Single-server architecture consists of Replay Server and Agent running on the same server typically seen in small environments where as a multi-server architecture consists of a dedicated Replay server protecting one or multiple agents running different application workloads.



REPLAY UNIQUE FEATURES

CORRUPTION DETECTION

It is known that 20% of all outages in Exchange are due to data corruption.

When Microsoft Exchange 2003 and 2007 mailbox servers are protected with Replay, it performs a mountability check on all exchange databases after every incremental snapshot. This corruption detection feature delivers the ability to alert administrators before failure and provides a path for immediate recovery in the case of a failure. Replay also performs an off-host nightly attach to all the databases being protected on a SQL server

OFF-HOST PROCESSING

Backup applications consume memory and processor cycles application servers, therefore they have traditionally been run during off-hours. Also, as the data size continues to grow backup windows continue to shrink. Lastly, traditional backup applications are not equipped deliver effective post data processing such as compression and data de-duplication.

Replay allows ridding backup windows and alleviating server load caused by processor and memory hog backup programs by offloading all tasks to the Replay server. Also by performing continuous incremental snapshots, Replay eliminates backup windows and its optimized architecture allows effective compression and de-duplication of data helps you save costs associated with long term storage. Lastly, using a single pass approach Replay also delivers the ability to perform transaction log management on Exchange servers.

REPLAY LIVE

Replay enables you to bring your application service online even before the data restore is complete.

Replay Live enables data to be instantly available during recovery – As matter of fact the data is available for use before it is recovered. We also perform Bare Metal Recovery to similar, dissimilar and virtual infrastructure that most competitors do not. Replay Live used with Bare Metal Recovery (both to similar and dissimilar hardware) can be coupled to recover application servers that face total outage

CONTINUOUS HIGH-AVAILABILITY

Native high-availability solutions are expensive, needy and localized. Customers looking at keeping the Recovery Point and Recovery Time to a minimum find management of these solutions to be very overwhelming.

The Standby features of Replay deliver continuous high availability to physical or virtual infrastructure using incremental approach – allows you to keep the Recovery Point and Recovery Time to a minimum. Replay Standby allows you to leverage physical or virtual infrastructure to keep the Recovery Point and Recovery Time to a minimum. Replay standby solutions do not require the acquisition of additional Licenses needed for OS or Application Servers.

TROUBLESHOOTING REFERENCE

Port Number	Purpose
Contact AppAssure Support	Telephone : (703) 547-9696 Email : support@appassure.com
Collecting and sending log files	1. Collecting Log files for support
Cannot Add Server for Protection	2. Check Network 3. Check if Core and/or Agent Services are running 4. Check VSS
In case of inadequate Permissions Issues	1. Check Permissions Granted to the Service Account
In case of authentication Errors	1. Authentication Errors
Replication Issues	1. Check Network 2. Check Permissions 3. Check authentication with Replication 4. Check Replication
VSS Issues	1. Diagnose VSS Issues

COLLECTING LOG FILES FOR SUPPORT

The Replay Core and Agent perform comprehensive logging. These logs are stored in the Replay.Log file that is created at the root of C:\.

COLLECTING LOG FROM THE REPLAY CORE

1. Stop the “Replay Core” Service
2. Copy the Replay.Log to a temp location as CASE#_CORE_MACHINENAME_DATE.log
3. Use Zip or Rar to compress the file as CASE#_CORE_MACHINENAME_DATE.zip or CASE#_CORE_MACHINENAME_DATE.rar and send file to support
4. Start the “Replay Core” Service

COLLECTING LOGS FROM THE REPLAY AGENTS

Since a Replay Core can protect one or more agents make sure to collect logs from all agents.

1. Stop the “Replay Agent” Service
2. Copy the Replay.Log to a temp location as CASE#_CORE_MACHINENAME_DATE.log
3. Use Zip or Rar to compress the file as CASE#_CORE_MACHINENAME_DATE.zip or CASE#_CORE_MACHINENAME_DATE.rar and send file to support
4. Start the “Replay Agent” Service

The log files can be uploaded to the AppAssure FTP site (coordinates available from support) or emailed to AppAssure support.

REPLAY SERVICE MANAGEMENT

To start, stop, pause, resume, or restart the “Replay Core” or “Replay Agent” service

USING SERVICES

1. Open Services. To open Services, click Start, click Control Panel, double-click Administrative Tools, and then double-click Services.
2. In the details panel, do one of the following:
 - Click the “Replay Core” or “Replay Agent” service, and then, on the Action menu, click Start, Stop, Pause, Resume, or Restart.
 - Right-click the service, and then click Start, Stop, Pause, Resume, or Restart.

USING THE COMMAND LINE

1. Open Command Prompt.
2. Type one of the following:
 - To start a service, type: *net start “Replay Core”* or *net start “Replay Agent”*
 - To stop a service, type: *net stop “Replay Core”* or *net stop “Replay Agent”*
 - To pause a service, type: *net pause “Replay Core”* or *net pause “Replay Agent”*
 - To resume a service, type: *net continue “Replay Core”* or *net continue “Replay Agent”*

NETWORK CONNECTIVITY

VALIDATE NETWORK CONNECTIVITY

The first step is to validate the network connectivity between the Replay core and the agent or two Replay cores. Perform a ping test to the other Replay core using the

- Hostname
- IP Address
- Fully Qualified Domain Name (FQDN)

Perform this test from and on both the cores and the agents and you should be able to successfully ping the other replay core

MULTI-HOMED HOSTS

Communication with a multihomed Replay Core or Agent domain controllers may fail intermittently. This issue occurs if one of the network adapters is attached to separate networks. In this scenario, network adapters on the Replay Core or the Agent are registering both (or all) IP addresses with the DNS server. DNS name resolution lookup requests return records in a "round robin" fashion, alternating the different IP addresses. Thus when the Core or the Agents lookup DNS to communicate with each half of the DNS lookup requests return an IP address that cannot be contacted, and the operation fails. To fix this

- Disable registration on the outside network adapter on the multihomed Replay Core or Agent.
- Disable the round robin functionality on the DNS server.
- Remove the existing entries in DNS and re-register interface with DNS.

NAME RESOLUTION

Check the DNS and Host files to make sure that the server names are resolved correctly. If Host files are used to resolve server names, then make sure to check the hosts file on the Replay Core as well as the Protected Servers. Both methods of name resolution should point to the preferred NIC on the servers.

DNS name resolution can be tested using the command "nslookup"

The Hosts file resides in the `%systemroot%\system32\drivers\etc` directory on 32 bit versions and If you are using 64 bit version of Windows, `%systemroot%\SysWOW64\drivers\etc`.

FIREWALL AND PORT AVAILABILITY

If the ping test is successful, perform the port scan test. Replay uses port 8080 for replication. A port scan test can be performed using Microsoft's PortQryUI tool. To download PortQryUI click [here](#)

To perform the test, simply enter the IP Address, hostname or the FQDN of the target Replay core and the desired port. PortQryUI tool will indicate if the port on the target Replay Core is

- Listening (open),
- Not Listening (Closed) or

- Filtered (Not Blocked but No response from the target)

Replay uses the following ports between the Replay Core and the Agents

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 by Replay server to communicate with a peer Replay Core for Replication.

Make sure that the firewalls are configured to allow the aforementioned ports or disabled altogether.

PERMISSION ISSUES

SERVICE ACCOUNT

To create a new service user account for Replay, follow these steps on Active Directory Domain Controller:

1. Click Start, point to Administrative Tools, and then click Active Directory Users and Computers to start the Active Directory Users and Computers console.
2. Click the domain name that you created, and then expand the contents.
3. Right-click Users, point to New, and then click User.
4. Type the first name - Replay, last name - Service, and user logon name - ReplayAdmin, and then click Next.
5. Type a new password, confirm the password, and then click to select Password never expire and then click Next.
6. Review the information that you provided, and if everything is correct, click Finish.

LOCAL GROUP MEMBERSHIP

Perform this step on the Replay and the protected server

1. In Administrative Tools, click Computer Management.
2. In the console tree, expand Local Users and Groups, and then click Groups.
3. Right-click the Administrators group, and then click Add to Group. Click Add.
4. Click Look in to display a list of domains from which users and groups can be added to the group.
5. In Location, click the domain containing the users and computers you want to add, and then click OK.
6. In Enter the object names to select, type the name of the user ReplayAdmin, and then click OK.
7. If you want to validate the user or group names that you are adding, click Check Names.

LOCAL SERVER RIGHTS

On each computer that you want to install the Replay Recovery Server component, you must configure the permissions of the Replay service account that you plan to use when installing Replay.

1. Click Start, point to Administrative Tools, and then click Local Security Policy to start the Local Security Policy console.
2. Enable the following rights for the user
 - a. log on locally with local permissions (if not assigned by default)
 - b. log on locally with local permissions
 - c. log on as a service

EXCHANGE 2003 ADMINISTRATOR ROLE

Use the Exchange Administration Delegation Wizard to grant administrative permissions to the Replay Service account.

1. Click Start, point to Programs, point to Microsoft Exchange, and then click System Manager.
2. Right-click the organization or the administrative group where you want to delegate administrative permissions, and then click Delegate control. Exchange Administration Delegation Wizard starts. Click Next.
3. On the Users or Groups page, click Add.
4. In the Delegate Control dialog box, click Browse.
5. In the Select Users, Computers, or Group dialog box, click the appropriate location in the Look in box, click the name ReplayAdmin, and then click OK.
6. Under Role in the Delegate Control dialog box, click Exchange Administrator permissions to assign to the ReplayAdmin account, and then click OK. The user or the group that you added appears in the Users and groups list.
7. Click Next, and then click Finish.
8. Grant "Send As," "Receive As," and "Administer Information Store" permissions at the server level for each Exchange Server. To do this, follow these steps:
 - a. In Exchange System Manager, right-click the first Exchange Server administrative group name, and then expand the Servers group.
 - b. Right-click an Exchange Server server, click Properties, and then click Security.
 - c. In the top pane, select the Replay service account. In the bottom pane, make sure that the "Send As," "Receive As," and "Administer Information Store" permissions are set to Allow.
 - d. Repeat steps 8b and 8c for each Exchange Server.
9. Grant "Send As," "Receive As," and "Administer Information Store" permissions to the mailbox store. To do this, follow these steps:
 - a. In Exchange System Manager, right-click the first Exchange administrative group name, and then expand the Servers group.
 - b. Expand the first mailbox store group, right-click each mailbox store, click Properties, and then click Security.
 - c. In the top pane, select the Replay service account. In the bottom pane, make sure that the "Send As," "Receive As," and "Administer Information Store" permissions are set to Allow.
10. Repeat steps 8b and 8c for each mailbox store on each Exchange Server.

PERMISSIONS TO THE MBDATA FOLDER IN EXCHANGE 2003

If you are using Exchange 2003, to resolve this issue you need to grant the default permissions to the Mdbdata folder and to the root of the drive that contains the Mdbdata folder. To grant the default permissions to the Mdbdata folder, do the following:

1. Start Windows Explorer, and then expand the Exchsrvr folder.
2. Right-click the Mdbdata folder, and then click Properties.
3. Click the Security tab, and then grant the following default permissions:

<i>Account</i>	<i>Permissions</i>
<i>Administrators</i>	<i>Full Control</i>
<i>Authenticated Users</i>	<i>Read and Execute, List Folder Contents, Read</i>
<i>Creator Owner</i>	<i>None</i>
<i>Server Operators</i>	<i>Modify, Read and Execute, List Folder Contents, Read, Write</i>
<i>System</i>	<i>Full Control</i>

To grant the default permissions to the drive that contains the Mdbdata folder, follow these steps:

4. Start Windows Explorer.
5. Right-click the Local Disk object that contains the Mdbdata folder, and then click Properties.
6. Click the Security tab, and then grant the following default permissions, according to the operating system:

<i>Account</i>	<i>Permissions</i>
<i>Administrators</i>	<i>Full Control</i>
<i>Creator Owner</i>	<i>None</i>
<i>Everyone</i>	<i>None</i>
<i>System</i>	<i>Full Control</i>
<i>Users</i>	<i>Read and Execute, List Folder Contents, Read</i>

To mount the affected mailbox or public store, start Exchange System Manager, right-click the mailbox or the public store, and then click Mount Store

EXCHANGE 2007 ADMINISTRATOR ROLE

1. To set Send As, Receive As, and Administer Information Store permissions:
 - a. Open Windows PowerShell, and then open a command prompt window.
 - b. At the command prompt window, type the following line, and then press ENTER:
 - c. `get-mailboxserver Exchange2007ServerName | add-adpermission -user <ReplayAdmin> -accessrights GenericRead, GenericWrite -extendedrights Send-As, Receive-As, ms-Exch-Store-Admin`

where: Exchange2007ServerName is the name of the Microsoft Exchange 2007 Server and <ReplayAdmin> is the name of the BlackBerry Enterprise Server service account

2. To check the Send As, Receive As, and Administer Information Store permissions:
 - a. Open Windows PowerShell, and then open a command prompt window.
 - b. At a command prompt, type the following line, and then press ENTER:
get-mailboxserver Exchange2007 | get-ADpermission -user ReplayAdmin | Format-List

PERMISSIONS TO THE MDBDATA FOLDER IN EXCHANGE 2007

If you are using Exchange 2007 to resolve this issue, you will need to grant the default permissions to the folder that contains the Exchange databases and to the drive on which this folder resides. To grant the default permissions to the folder that contains the Exchange databases, do the following:

1. Start Windows Explorer, and then move to the folder that contains the Exchange databases.
2. Right-click the folder, and then click **Properties**.
3. Click the **Security** tab, and then grant the following default permissions.

<i>Account</i>	<i>Permissions</i>
<i>Administrators</i>	<i>Full Control</i>
<i>System</i>	<i>Full Control</i>

To grant the default permissions to the drive that contains the Exchange database folder, follow these steps:

4. Start Windows Explorer.
5. Right-click the Local Disk object that contains the Mdbdata folder, and then click **Properties**.
6. Click the **Security** tab, and then grant the following default permissions, according to the operating system:

<i>Account</i>	<i>Permissions</i>
<i>Administrators</i>	<i>Full Control</i>
<i>Creator Owner</i>	<i>None</i>
<i>Everyone</i>	<i>None</i>
<i>System</i>	<i>Full Control</i>
<i>Users</i>	<i>Read and Execute, List Folder Contents, Read</i>

AUTHENTICATION

If the REPLAY Core is unable to connect to the REPLAY Agent, please verify the following requirements:

1. The account used to install and execute the REPLAY Core service can be a local administrator account or a domain account that has administrator privileges on the server. If you are protecting servers across domains, you have 2 options.
 - Use an account that belongs to the same domain as the server or another domain with a trust relationship between domains.
 - Use pass-through authentication.
2. The REPLAY Core service does **not** require domain administrator privileges, only a domain user account with local administrator privileges.
3. 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.

It is recommended that the service account is not a domain administrator account or administrator account. The account should be an Exchange administrator for the REPLAY Agent and should have local administrative privileges for both the Replay Agent service and Replay Core service.

If the credentials are invalid, the Replay Agent and Replay Core services will not be able to authenticate.

4. For proper e-mail restore operation (e-mail restore using MailRetriever), the account used to launch MailRetriever must have full control permission granted on the database you will be performing restores to, including “send as” and “receive as” permissions.

Note: You can install Replay using a local administrator account. However, when protecting application servers, many tasks require domain user privileges. In this case, we recommend installing Replay using a domain account that is a member of the domain administrators group.

For more detailed information, please see the AppAssure Knowledge Base at <http://kb.AppAssure.com>.

REPLICATION

VALIDATE NETWORK CONNECTIVITY

The first step is to validate the network connectivity between the Replay core and the agent or two Replay cores. Perform a ping test to the other Replay Core using

- Hostname
- IP Address
- Fully Qualified Domain Name (FQDN)

Perform this test from and on both the cores and the agents and you should be able to successfully ping the other replay core

PORT AVAILABILITY

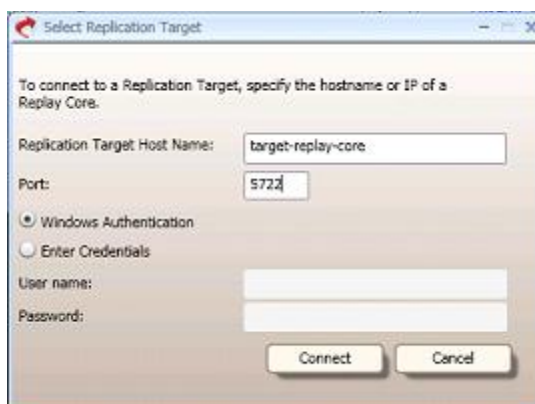
If the ping test is successful, perform the port scan test. Replay uses port 8080 for replication. A port scan test can be performed using Microsoft's PortQryUI tool. To download PortQryUI click [here](#)

To perform the test, simply enter the IP Address, hostname or the FQDN of the target Replay core and the desired port. PortQryUI tool will indicate if the port on the target Replay Core is

- Listening (open),
- Not Listening (Closed) or
- Filtered

If the default port 8080 is already in use by another application. Follow the steps to reassign the replication port on the target

1. Stop the Replay Core service
2. Open Regedit and Navigate to HKLM \SOFTWARE\AppAssure\ReplayMirror\SecondaryGlobalSetting
3. Create a string value (REG_SZ) ReplicationServiceUri
4. Enter the value http://localhost:PORT_NUMBER (Where PORT_NUMBER reflects the port you would like to use. For e.g 5722)



5. Start the Replay Core service

6. Configure Replication to the target Replay Core by using the aforementioned port number

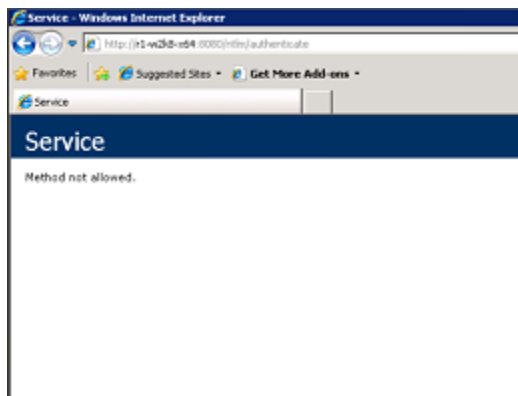
AUTHENTICATION

If the target Replay core is in the same domain as the source Replay core, select windows authentication in the “Select Replication Target” dialog box or select “Enter Credentials” and explicitly enter the username and password of the Replay Core service account

If the target Replay core is in a different domain as the source Replay core, select “Enter Credentials” and explicitly enter the username and password of the Replay Core service account windows authentication in the “Select Replication Target” dialog box.

To test authentication on the target Replay Core,

1. Connect to `http://target-replay-core:8080/ntlm/authenticate`
2. Enter the credentials
3. If the credentials are accepted then you will see the following message



USER ACCESS CONTROL (UAC)

For computers running the target Core on Windows 2008, Windows Vista, or Windows 7, and the administrator credentials being used are those of a local (that is, not domain) administrator user. Due to the design of Windows UAC, local administrators authenticated remotely are never elevated, thus do not have the permissions necessary to establish replication on that Core.

To work around this problem, either use a domain account with local admin rights on the target Core, or disable UAC for administrators in Admin Approval mode using the `secpol.msc` tool as described on <http://www.howtogeek.com/>

MICROSOFT VOLUME SHADOW COPY SERVICE

Replay uses the Volume Shadow Copy Service (VSS) that is included in the Microsoft Windows Server 2003, 2008 and Windows XP, Vista and 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-b724-458a-9d40-b914ecf5ef8e}
  State: [1] Stable
  Last error: No error

Writer name: 'ASR Writer'
  Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
  Writer Instance Id: {c1d52bf1-dca4-47af-b991-2d0517a05d49}
  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: 'BITS Writer'
  Writer Id: {4969d978-be47-48b0-b100-f328f07ac1e0}
  Writer Instance Id: {03140b75-22b0-4d97-bdc3-de7ddc7281b3}
  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: 'Registry Writer'
  Writer Id: {afbab4a2-367d-4d15-a586-71dbb18f8485}
  Writer Instance Id: {097700a4-0940-4ec4-ae04-fd861688f605}
  State: [1] Stable
  Last error: No error

Writer name: 'Shadow Copy Optimization Writer'
  Writer Id: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
  Writer Instance Id: {2736f6b7-a432-4128-872a-72da67e78f29}
  State: [1] Stable
  Last error: No error

Writer name: 'COM+ REGDB Writer'
  Writer Id: {542da469-d3e1-473c-9f4f-7847f01fc64f}
  Writer Instance Id: {4276ecbf-abb9-41d7-8a9c-344a45423471}
  State: [1] Stable
  Last error: No error

Writer name: 'WMI Writer'
  Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}
  Writer Instance Id: {5b433de4-ecc2-4140-8bda-13cf72343cf0}
  State: [1] Stable
  Last error: No error
```

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.

VSS TROUBLESHOOTING

In case you find that the output of the vssadmin list writers command is blank, there might be registry corruption that is preventing the system from picking up and displaying the correct information. This is documented on KB940184 (<http://support.microsoft.com/kb/940184>). These steps allow you to recreate the list of VSS writers

1. Click Start, click Run, type Regedit, and then click OK.
2. Locate and then click the following registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions
3. On the Edit menu, click Delete, and then click Yes to confirm that you want to delete the subkey.
4. Exit Registry Editor.
5. Click Start, click Run, type services.msc, and then click OK.
6. Right-click the following services one at a time. For each service, click Restart:
 - COM+ Event System
 - COM+ System Application

- Microsoft Software Shadow Copy Provider
 - Volume Shadow Copy
7. Click Start, click Run, type cmd, and then click OK.
 8. At the command prompt, type `vssadmin list writers`, and then press ENTER. If the VSS writers are now listed, close the Command Prompt window. You do not have to complete the remaining steps. If the VSS writers are not listed, type the following commands at the command prompt. Press ENTER after each command.
 - `cd /d %windir%\system32`
 - `net stop vss`
 - `net stop swprv`
 - `regsvr32 ole32.dll`
 - `regsvr32 oleaut32.dll`
 - `regsvr32 /i eventcls.dll`
 - `regsvr32 vss_ps.dll`
 - `vssvc /register`
 - `regsvr32 /i swprv.dll`
 - `regsvr32 es.dll`
 - `regsvr32 stdprov.dll`
 - `regsvr32 vssui.dll`
 - `regsvr32 msxml.dll`
 - `regsvr32 msxml3.dll`
 - `regsvr32 msxml4.dll`
 9. Note The last command may not run successfully.
 10. At the command prompt, type `vssadmin list writers`, and then press ENTER.
 11. Confirm that the VSS writers are now listed.

To effectively diagnose VSS issues the following information should be gathered for Microsoft support to examine:

1. Windows application and system event log (<http://technet.microsoft.com/en-us/library/cc734545%28WS.10%29.aspx>)
2. Enable VSS trace. Examine the application and system event logs focusing on the error events created by the VolSnap and VSS sources at the time of failure. It is helpful to extract the germane events from the log to isolate the problem and have a more productive interaction with MS support.

How to perform a VSS trace:

- a. Create a file `tracefile.reg` using the contents shown below and change the `TraceFile` entry to point to a volume that is not going to be shadow copied. Note the double backslash delimiter usage—you need to enter `"\"` as the delimiter for each backslash in the path you wish to specify.
- b. Install `tracing.reg`.
- c. Reproduce the problem.

- d. Turn off tracing by deleting the key
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing"

Here are the contents of the tracefile.reg registry file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing]
"TraceFile"="c:\\trace.txt"
"TraceLevel"=dword:ffffffff
"TraceEnterExit"=dword:00000001
"TraceToFile"=dword:00000001
"TraceToDebugger"=dword:00000000
"TraceFileLineInfo"=dword:00000001
"TraceForceFlush"=dword:00000000
```

VOLUME SHADOW COPY TIME-OUT ERROR

You may experience a problem that causes certain Volume Shadow Copy service writers to time out during a lengthy shadow copy creation. This problem occurs especially on computers that have slow hard disks, low memory, or low CPU speed; or on computers that have the disk write cache disabled (for example, on a domain controller computer). You may also experience that shadow copies are lost during backup and during times when there are high levels of input/output.

This Volume shadow timeout issue is addressed in MS KB 826936. (<http://support.microsoft.com/kb/826936>)

1406 Error Message During Installation

You may receive the following error message when installing Replay Core or the Replay agent on a protected server even if you have administrative privileges on the server:

Error 1406. Setup cannot write the value to the registry key <Registry Key>. Verify that you have sufficient permissions to access the registry ...

To resolve this situation, do the following:

1. Login to the server with domain administrative privileges.
2. Create a system restore point and create a backup of the registry.
3. Go to the following link and download and install SUBINACL:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=e8ba3e56-d8fe-4a91-93cf-ed6985e3927b>
4. Stop all registry cleaner and anti-virus programs.
5. Copy the following text below into a text file named r"eset.cmd"

```
cd /d "%ProgramFiles%\Windows Resource Kits\Tools"
subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=administrators=f /grant=system=f
subinacl /subkeyreg HKEY_CURRENT_USER /grant=administrators=f /grant=system=f
subinacl /subkeyreg HKEY_CLASSES_ROOT /grant=administrators=f /grant=system=f
subinacl /subdirectories %SystemDrive% /grant=administrators=f /grant=system=f
```

```
subinacl /subdirectories %windir%*. * /grant=administrators=f/grant=system=f  
secedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose
```

6. Run reset.cmd with administrative rights (it may take a LONG time)
7. Reboot the server and re-install the Replay agent or Replay Server.