

How to Troubleshoot the Remote Backup Client log Error Message:

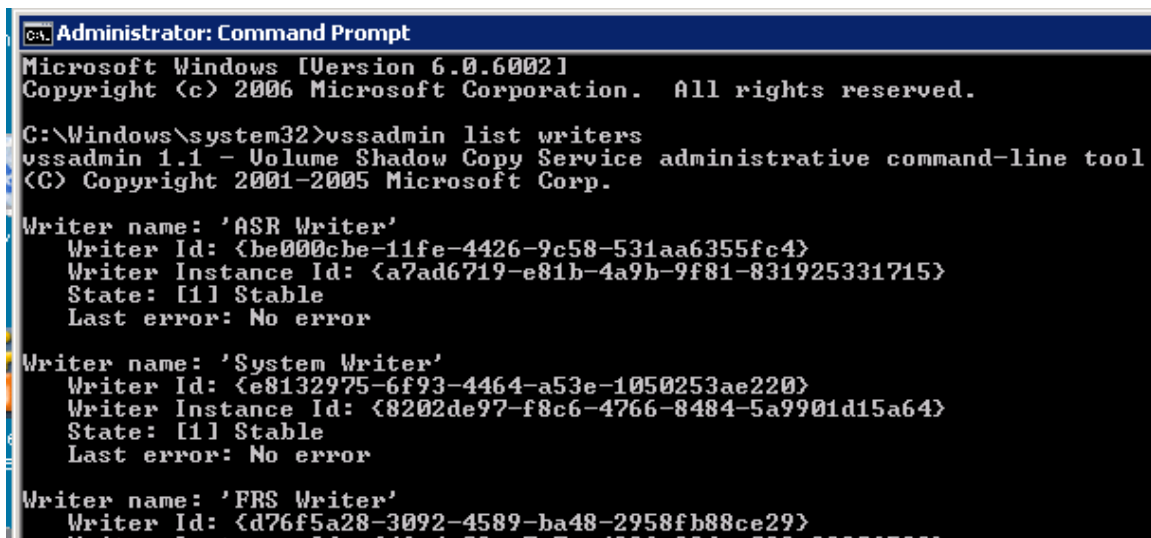
VSS open files Backup failed. Error: Connection is not established with the VSS Requestor, restart the client and try again later. In BCVssOpenFilesProcess

When this error message appears in the Remote Backup client log, it means that an attempt to snapshot an open/in-use file on a Windows 64-bit machine has failed. On 64-bit machines, a special “helper” service exists to facilitate interactions with Windows Volume Shadow Service – the operating system software component that helps make the snapshot copy.

Clearing up this situation is essential to enabling the Remote Backup client software to perform future snapshots of open/in-use files – which are necessary in some backup configurations/customer situations.

The following steps should be taken, in progressive order, when troubleshooting this problem to resolution. These diagnostics are valid **ONLY** for the error message shown above.

1. **Do basic VSS testing** – If VSS is not properly operating on the machine, then the remote backup client will not be able to make snapshot copies of open/in-use files. From an administrator account, use the command: `VSSAdmin List Writers`. If basic VSS operations are functional, then you will see a status display of all known VSS “writers” displayed on the screen (See below). If the command fails to display this status, then repair of VSS is required prior to proceeding. (Use of a separate VSS Test utility is also recommended here on general principles.)



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

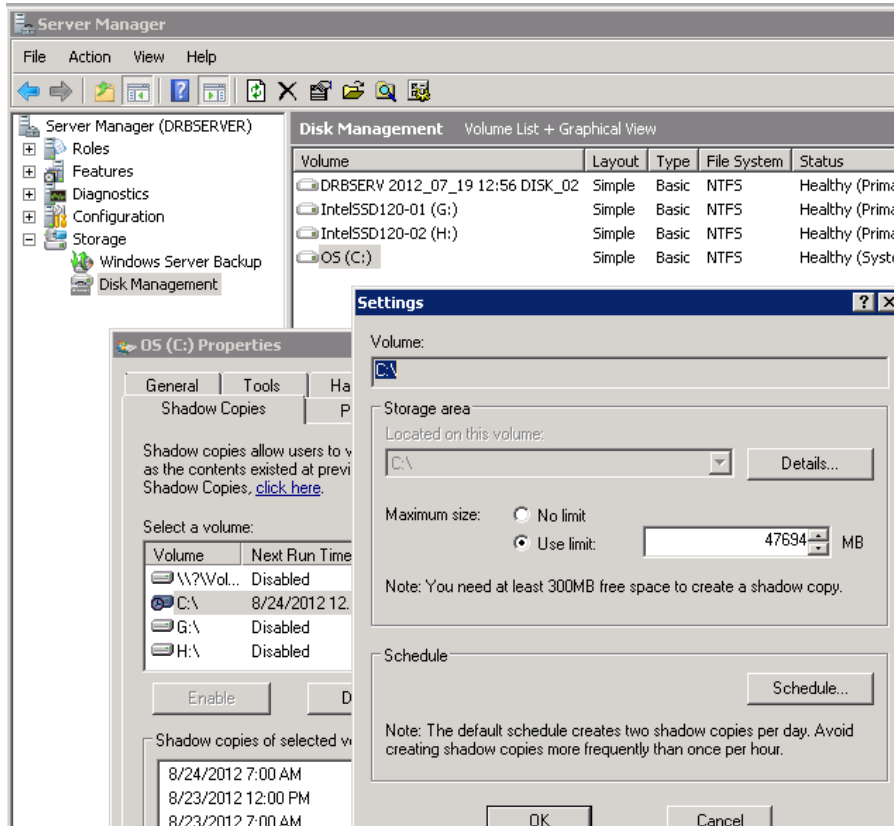
Writer name: 'ASR Writer'
  Writer Id: {be000cbe-11fe-4426-9c58-531aa6355fc4}
  Writer Instance Id: {a7ad6719-e81b-4a9b-9f81-831925331715}
  State: [1] Stable
  Last error: No error

Writer name: 'System Writer'
  Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
  Writer Instance Id: {8202de97-f8c6-4766-8484-5a9901d15a64}
  State: [1] Stable
  Last error: No error

Writer name: 'FRS Writer'
  Writer Id: {d76f5a28-3092-4589-ba48-2958fb88ce29}
  Writer Instance Id: {46e4e82c-7e7e-4886-801e-802e88206520}
```

2. **Make sure VSS Storage Space is available** – Shadow storage space must be made available on each partition where open file snapshots are required. On

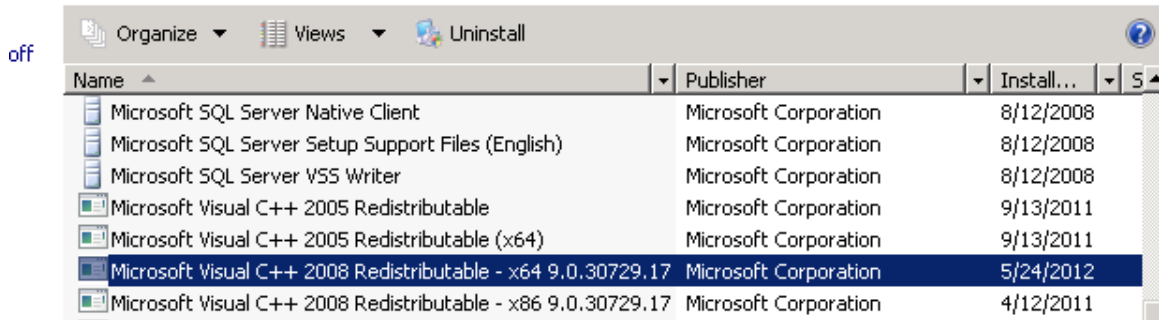
Windows XP, Vista and Windows 7, shadow storage space is (usually) automatically managed on behalf of the user. On Windows server platforms, this disk storage used for snapshots must be manually established. Do this by right clicking on My Computer and selecting Manage option. Expand the Storage icon to reveal Disk Management as shown below. Examine the Shadow Copies property of each partition and make sure that the Maximum size value is set to at least 10% of the size of the volume. You do not need to Enable shadow copies, you just need to set the Maximum size value.



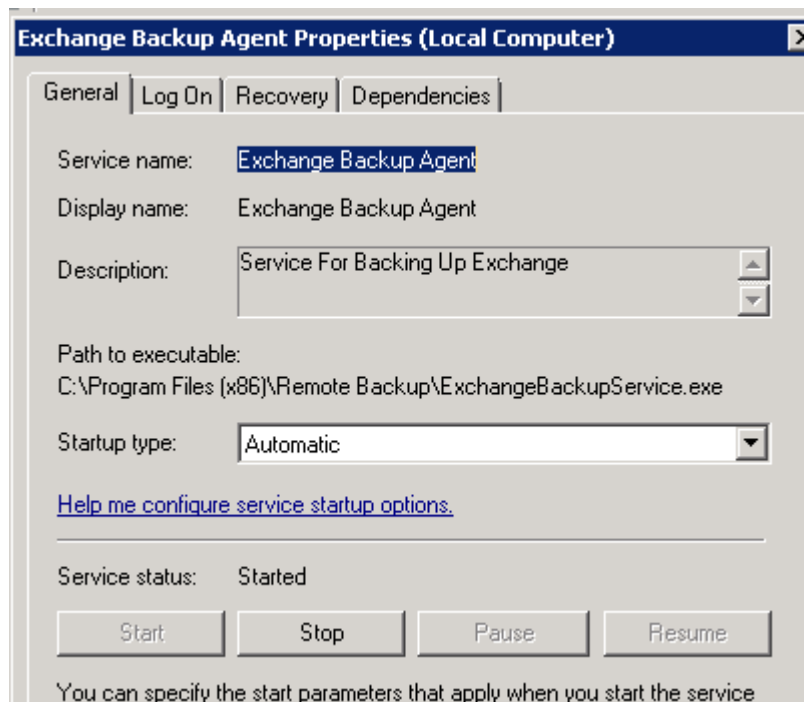
3. Make sure that the required runtime libraries are installed - In order to snapshot an open file, the remote backup VSS Requestor service (named Exchange Backup Agent) must have access to the 64-bit re-distributable version of Microsoft Visual C++ 2008 (runtime libraries) or later. Verify this in the Programs and Features applet of the control panel or Add/Remove Programs on earlier server versions. (See below.)

Uninstall or change a program

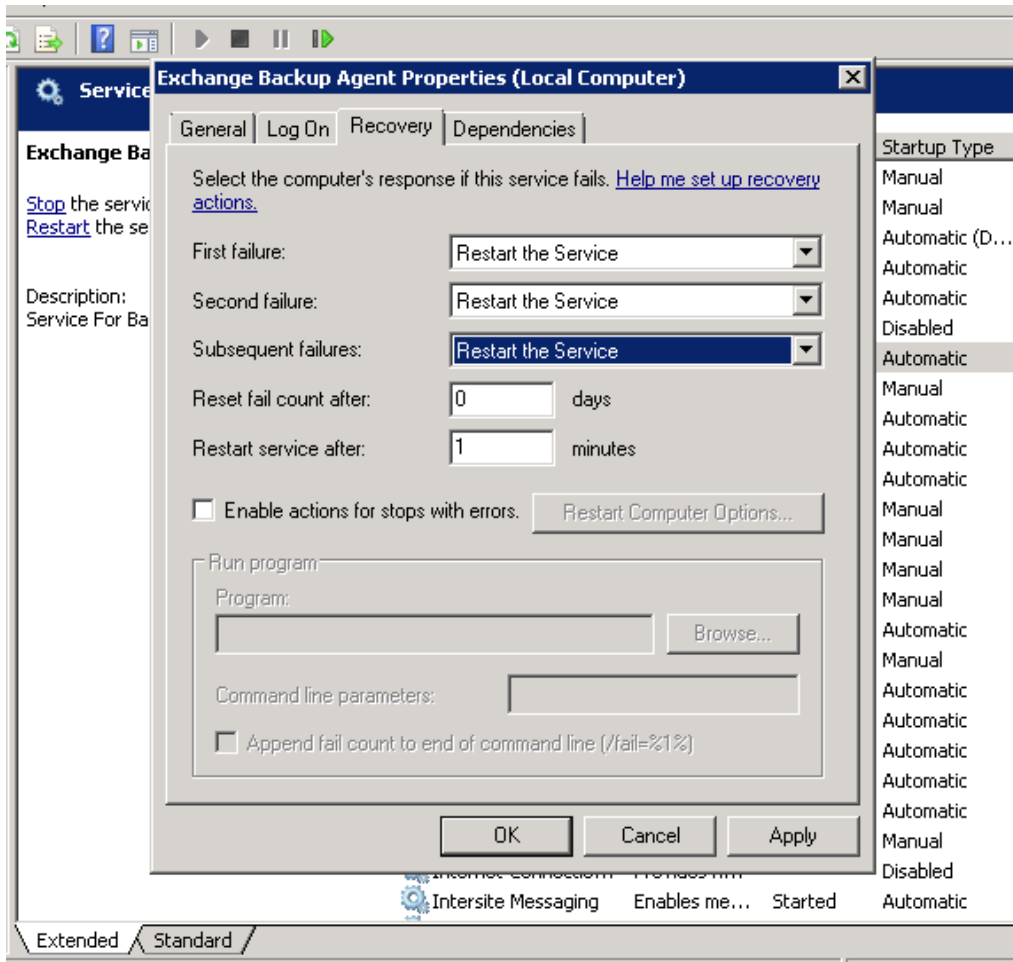
To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".



4. **Make sure that the “Exchange Backup Agent” service is started** - The remote backup client software uses this service as a general purpose 64-bit VSS Requestor agent. Various components of the backup program use this service to facilitate creation of a VSS snapshot. It must be started at all times.



5. **Set the service to Auto-restart** - If the Exchange Backup Agent service start type is Automatic (or Automatic with delay), and you find that the service is stopped, then a first step is to use the Recovery tab in the service definition to attempt to have Windows restart this service if for any unknown reason it stops. The restart options are set on the Recovery tab in the picture below.



6. Extend the time for a Windows Service to Start - If after performing all the changes above, you attempt to start the service and get an error 1053 (timeout starting service or non-responsive), the next step is to increase the time Windows permits to start an actual service. By default, all services must acknowledge their startup to the service control manager within 30 seconds (30000 milliseconds). This timeframe can be extended to a maximum of 120 seconds (120000 milliseconds) by changing the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServicesPipeTimeout

If key is not present, you will need to create it as a DWORD with a value of decimal 120000. A system reboot is required for this change to take effect.

7. Adjust the CRL timeout parameters – If you have extended the permitted service startup time to 120000 milliseconds via a registry change, and after 120 seconds you (still) get the 1053 timeout message, then two additional registry changes may help.

The Exchange Backup Agent service is implemented in a Windows .NET program assembly located by default in C:\Program Files (x86)\Remote

Backup\ExchangeBackupService.exe. This image is “signed” with an authenticode digital signature issued to the manufacturer of the software.

On image activation, Windows automatically attempts to pull the Certificate Revocation List (CRL) from Verisign (issuer of digital signature authority.) If the process of verifying the digital signature (isn’t revoked) takes too long – due to slow internet, firewall blockage, etc. – the startup process is delayed until certain programmed timeouts expire.

Unfortunately, these timeouts may in some instances, on machines very busy disk drives, exceed 120 seconds, thereby preventing the startup of the Exchange Backup Agent service.

To ensure this doesn’t happen on very sluggish systems, Microsoft recommends that the timeout periods be shorted for the CRL checks. This is done by carefully creating two new keys in the registry as follows:

Name: ChainUrlRetrievalTimeoutMilliseconds
Location: HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType
0\CertDllCreateCertificateChainEngine\Config
Type: REG_DWORD
The value is defined in milliseconds.

This registry setting defines the default timeout for a single CRL retrieval. If this value is set to 0 or if this value is undefined, the default value that is used is 15,000 milliseconds.
SET THIS TO 200 (ms)

Name: ChainRevAccumulativeUrlRetrievalTimeoutMilliseconds
Location: HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType
0\CertDllCreateCertificateChainEngine\Config
Type: REG_DWORD
The value is defined in milliseconds.

This registry setting defines the cumulative timeout for all CRL retrievals. If this value is set to 0 or if this value is undefined, the default value that is used is 20,000 milliseconds.
SET THIS TO 500 (ms)

PLEASE BE VERY CAREFUL IN DEFINING THESE REGISTRY KEYS. THEY ARE LONG AND COMPLEX TO TYPE AND MUST MATCH EXACTLY.

A reboot is required after creating these keys to make them active. Please note that if the services timeout message 1053 is displayed prior to 120 seconds, you must go back and change the value of the ServicesPipetimeout key.