Volume Shadow Copy Service

Helps Build an Integrated Backup System

The Microsoft® Windows Server™ 2003 operating system and its enhanced storage management features—particularly the Volume Shadow Copy Service (VSS)—can provide the framework for an integrated backup system based on industry-standard components such as Dell™ PowerEdge™ servers, Dell/EMC® storage arrays, Dell PowerVault™ tape libraries, and VERITAS Backup Exec™ software. This article explores how VSS can enable these components to interoperate, helping to reduce the time and complexity of online backups.

To be competitive in the ever-changing global economy, many enterprises must provide uninterrupted access to key services such as customer databases, e-commerce applications, and corporate messaging systems. Taking systems offline to back up data is no longer a viable option—but creating reliable backup and recovery services for enterprise systems that must remain available 24/7 can be a challenge for IT administrators. This article presents an example scenario explaining how IT administrators can integrate the backup process for a high-availability Microsoft® Exchange Server 2003 messaging system using standards-based enterprise components and the Volume Shadow Copy Service (VSS), a new file-system feature included in the Microsoft Windows Server™ 2003 operating system.

When a key business service such as Microsoft Exchange Server 2003 is online, several files are either open or undergoing changes. The large volume and dynamic nature of the data make an accurate and reliable backup difficult to perform. Creating point-in-time copies of storage volumes, such as the snapshots taken by EMC® SnapView™ software, is one way administrators can reduce the time required to back up data. However, because the underlying data is constantly changing, I/O operations to a storage volume must be paused to ensure that the data is consistent before a reliable snapshot can be taken. The challenge for system administrators is finding a way to integrate and automate the processes of pausing I/O, creating snapshots, resuming I/O, and performing back-ups from the snapshot data while the original data and service are restored to operation.

VSS provides a framework and an application programming interface (API) that enables administrators to automate several processes related to creating snapshots and performing backups. Because it allows third-party storage hardware, backup software, and application software to interoperate within the VSS framework, VSS can enable administrators to streamline the storage management process—helping to reduce the time, complexity, and cost of online backups considerably.

VSS on Windows Server 2003: Shadow copies

VSS allows system administrators to create software-driven snapshots, or shadow copies, of a volume that can be shared as a network resource. The shadow copy can be created on a reserved area that resides in the same volume...
as the data, or it can be created on a reserved area that resides in a
different volume. This native shadow copy functionality uses a copy-
on-first-write method, which makes a duplicate of any block that
has been changed since the last shadow copy was created. Only
changed file blocks are copied to the snapshot just before the change,
not the entire volume.

After a snapshot is created, VSS oversees all activities on the
source volume, including writes and reads:

- **Writes:** When an application or a user modifies a file or
  sector on the source volume, VSS identifies which blocks
  have been affected. If a shadow copy exists and the block
  has not been modified since the most recent shadow copy
  was created, VSS first saves the original data in the shadow
  copy volume and then writes the change to the source
  volume. If the block has been modified previously, VSS
  writes the change directly to the source volume.

- **Reads:** When an application or a user reads a file or sector
  from the source volume, VSS typically serves that request
  from the source volume. However, if a read requests a
  previous version of the data, VSS maps that request to the
  appropriate block(s) and the data sent back will generally
  include blocks from both the source volume and the shadow
  copy volume.

Figure 1 shows where the VSS volume snapshot driver resides
in the Windows Server 2003 layered driver model. For more infor-
mation, consult the Windows Server 2003 online help that is avail-
able from the operating system’s graphical user interface (GUI) or the

VSS also enables components associated with a backup system—
such as business application software, storage management software,
and storage hardware—to be used in an end-to-end process that helps
ensure maximum backup efficiency. In this integrated approach, a
writer (the business application software), a requester (the storage
management software), and a provider (the storage hardware driver)
interoperate with VSS to provide a consistent, reliable backup snap-
shot of the application data. In the Figure 2 scenario, the writer is
Exchange Server 2003, the requester is VERITAS Backup Exec™
storage management software, and the provider controls a Dell/EMC
storage area network (SAN).

**Exchange Server 2003: The writer**
Exchange Server 2003 supports the Windows Server 2003 VSS fea-
ture, which helps reduce backup time and simplify backup man-
tagement for Exchange data. The VSS writer service helps backup
software obtain consistent, point-in-time shadow copies of data on
a live Exchange server. When VSS receives a shadow copy request
from backup software, VSS communicates with the running Exchange
application (the writer) to pause new transactions, finish current trans-
actions, and flush all the cached data to disk. VSS then communi-
cates with the appropriate storage provider (in this scenario, the
Dell/EMC storage array) to initiate the shadow copy process for the
disk volumes that contain Exchange Server 2003 data. Once a shadow
copy has been created, the backup software (in this scenario,
VERITAS Backup Exec) then can copy data from the shadow copy
to a tape without involving the Exchange application, thus reduc-
ing the impact of backup operations on Exchange Server 2003
performance and availability.

After the shadow copy has been created, VSS communicates
with the Exchange writer service to signal that Exchange Server 2003
can resume writing to disk. The shadow copy process typically
takes less than a minute. Clients using the Microsoft Outlook® 2003
messaging and collaboration client in cached mode most likely will
not notice a disruption. Clients using earlier versions of Outlook may
experience a delay of several minutes during the shadow copy
process. Retaining the snapshot of an Exchange Server 2003

Figure 2 shows the VSS volume snapshot driver resides
in the Windows Server 2003 layered driver model. For more infor-
mation, consult the Windows Server 2003 online help that is avail-
able from the operating system’s graphical user interface (GUI) or the

VSS also enables components associated with a backup system—
such as business application software, storage management software,
and storage hardware—to be used in an end-to-end process that helps
ensure maximum backup efficiency. In this integrated approach, a
writer (the business application software), a requester (the storage
management software), and a provider (the storage hardware driver)
interoperate with VSS to provide a consistent, reliable backup snap-
shot of the application data. In the Figure 2 scenario, the writer is
Exchange Server 2003, the requester is VERITAS Backup Exec™
storage management software, and the provider controls a Dell/EMC
storage area network (SAN).

**Exchange Server 2003: The writer**
Exchange Server 2003 supports the Windows Server 2003 VSS fea-
ture, which helps reduce backup time and simplify backup man-
tagement for Exchange data. The VSS writer service helps backup
software obtain consistent, point-in-time shadow copies of data on
a live Exchange server. When VSS receives a shadow copy request
from backup software, VSS communicates with the running Exchange
application (the writer) to pause new transactions, finish current trans-
actions, and flush all the cached data to disk. VSS then communi-
cates with the appropriate storage provider (in this scenario, the
Dell/EMC storage array) to initiate the shadow copy process for the
disk volumes that contain Exchange Server 2003 data. Once a shadow
copy has been created, the backup software (in this scenario,
VERITAS Backup Exec) then can copy data from the shadow copy
to a tape without involving the Exchange application, thus reduc-
ing the impact of backup operations on Exchange Server 2003
performance and availability.

After the shadow copy has been created, VSS communicates
with the Exchange writer service to signal that Exchange Server 2003
can resume writing to disk. The shadow copy process typically
takes less than a minute. Clients using the Microsoft Outlook® 2003
messaging and collaboration client in cached mode most likely will
not notice a disruption. Clients using earlier versions of Outlook may
experience a delay of several minutes during the shadow copy
process. Retaining the snapshot of an Exchange Server 2003

Figure 2 shows the VSS volume snapshot driver resides
in the Windows Server 2003 layered driver model. For more infor-
mation, consult the Windows Server 2003 online help that is avail-
able from the operating system’s graphical user interface (GUI) or the

VSS also enables components associated with a backup system—
such as business application software, storage management software,
and storage hardware—to be used in an end-to-end process that helps
ensure maximum backup efficiency. In this integrated approach, a
writer (the business application software), a requester (the storage
management software), and a provider (the storage hardware driver)
interoperate with VSS to provide a consistent, reliable backup snap-
shot of the application data. In the Figure 2 scenario, the writer is
Exchange Server 2003, the requester is VERITAS Backup Exec™
storage management software, and the provider controls a Dell/EMC
storage area network (SAN).

**Exchange Server 2003: The writer**
Exchange Server 2003 supports the Windows Server 2003 VSS fea-
ture, which helps reduce backup time and simplify backup man-
tagement for Exchange data. The VSS writer service helps backup
software obtain consistent, point-in-time shadow copies of data on
a live Exchange server. When VSS receives a shadow copy request
from backup software, VSS communicates with the running Exchange
application (the writer) to pause new transactions, finish current trans-
actions, and flush all the cached data to disk. VSS then communi-
cates with the appropriate storage provider (in this scenario, the
Dell/EMC storage array) to initiate the shadow copy process for the
disk volumes that contain Exchange Server 2003 data. Once a shadow
copy has been created, the backup software (in this scenario,
VERITAS Backup Exec) then can copy data from the shadow copy
to a tape without involving the Exchange application, thus reduc-
ing the impact of backup operations on Exchange Server 2003
performance and availability.

After the shadow copy has been created, VSS communicates
with the Exchange writer service to signal that Exchange Server 2003
can resume writing to disk. The shadow copy process typically
takes less than a minute. Clients using the Microsoft Outlook® 2003
messaging and collaboration client in cached mode most likely will
not notice a disruption. Clients using earlier versions of Outlook may
experience a delay of several minutes during the shadow copy
process. Retaining the snapshot of an Exchange Server 2003
A database on disk enables a faster restore operation, thereby helping to reduce the interruption to the Exchange service.1

**VERITAS Backup Exec: The requester**

VERITAS Backup Exec for Windows Servers is designed to be a comprehensive backup tool for Microsoft Windows-based server environments. Backup Exec 9.1 supports VSS-enabled backups, minimizing disruption of applications and services while data is being backed up. This enables Backup Exec to perform a nonintrusive backup by obtaining a consistent copy of data from VSS, which is done by temporarily stopping I/O to the data through the writer (Exchange, in this scenario) when a backup is initiated. Administrators can select the appropriate VSS writers from a list of supported shadow copy components during Backup Exec backup and restore operations. Backup Exec supports the following types of VSS writers:

- **Service state:** Critical operating system and application service data such as event logs, Windows Management Instrumentation (WMI), and Removable Storage Manager (RSM)
- **System state:** Critical operating system data such as Windows system files, Component Object Model+ (COM+) Class Registration database, registry, and Microsoft Active Directory directory service
- **User data:** Microsoft SQL Server, Exchange Server, Active Directory Application Mode (ADAM), third-party application and user data, and so on

Service state, system state, and user data compose the Backup Exec shadow copy components file system. Backup Exec supports only full backups of storage groups using the Exchange writer. To back up Exchange data, system administrators select the Exchange writer during the backup operation—the Backup Exec interface lists the available Exchange servers and information stores available for backup. In addition, administrators can use the Backup Exec Advanced Open File Option by selecting VSS as the service for open file operations.2

<table>
<thead>
<tr>
<th>SnapView snapshot</th>
<th>SnapView clone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Logical point-in-time copy using copy-on-first-write method</td>
</tr>
<tr>
<td><strong>Storage requirement</strong></td>
<td>One or more SnapView cache LUNs must be available; cache space is consumed when either the source LUN or the snapshot is modified</td>
</tr>
<tr>
<td><strong>Persistence</strong></td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Required array software</strong></td>
<td>EMC SnapView</td>
</tr>
</tbody>
</table>

**Dell/EMC storage array: The provider**

EMC SnapView software and the SnapView clones provider are optional components available for Dell/EMC CX300, CX400, CX500, CX600, and CX700 storage arrays. SnapView snapshots are logical point-in-time copies of a logical storage unit (LUN), and SnapView clones are block-level duplicates of a LUN. Figure 3 compares SnapView snapshots and clones.

Administrators can create and manage snapshots and clones using the Dell/EMC storage array. The Dell/EMC VSS hardware provider—installed on a Dell™ PowerEdge™ server running Windows Server 2003—enables VSS to use EMC SnapView and the SnapView clones provider to create hardware-resident shadow copies on a Dell/EMC CX300, CX400, CX500, CX600, or CX700 array attached to the server. Figure 4 shows the hardware configuration for the Exchange backup scenario described in this article, including key software components that must be installed on both the PowerEdge server and the Dell/EMC storage array.

For the Dell/EMC hardware provider to register itself with VSS, the Windows Server 2003 Distributed Transaction Coordinator (DTC) service must be running when the provider is installed. After installing the provider, administrators must run `vssadmin list providers` to verify that the Dell/EMC hardware provider has been registered successfully. The hardware provider translates VSS API calls into EMC® Navisphere® command-line interface (CLI) statements that control the Dell/EMC hardware. The hardware provider can produce differential shadow copies by using `navicli.exe` to invoke

---

1 For more information, see the Exchange Server 2003 and Windows Server 2003 documentation online at http://www.microsoft.com.
2 For more information, see the help and product documentation for Backup Exec software online at http://www.veritas.com.
SnapView and create a snapshot. Similarly, the hardware provider can create plex shadow copies, which are essentially duplicates of the source LUN, by using navicli.jar to invoke the SnapView clones provider to create a clone.\(^3\)

**Integrated VSS backup: Process flow**

Figure 5 shows application and backup software used in the shadow copy–based backup scenario. In this example, a system administrator configures a backup schedule for Exchange Server 2003 through the Backup Exec software, specifying that the Exchange writer perform this service. When Backup Exec runs the scheduled job, the VSS requester informs the VSS service that Exchange Server 2003 storage groups will be affected. VSS then communicates with the Exchange writer to pause new transactions, finish current transactions, and flush all the cached data to disk.

VSS then communicates with the Dell/EMC hardware provider to create a hardware-resident shadow copy of the storage volumes containing the Exchange Server 2003 storage groups. The hardware provider invokes EMC SnapView to create a snapshot for the requested disks in the EMC storage array and returns the snapshot to VSS, which mounts the snapshot for Backup Exec. Once this step is completed, VSS instructs Exchange Server 2003 to resume normal operations. Backup Exec backs up the Exchange Server 2003 data and logs from the disk snapshots to the tape backup devices. After the backup job is completed successfully, Backup Exec instructs VSS to delete the shadow copies created for backing up the storage group volumes. Finally, VSS instructs the Dell/EMC hardware provider to delete the snapshots requested for the backup operation.

**A cost-effective, integrated approach to system backup**

IT administrators can build reliable, integrated backup systems using standards-based enterprise components such as Dell PowerEdge servers, Dell/EMC storage arrays, Dell PowerVault™ tape libraries, and VERITAS Backup Exec software. The Volume Shadow Copy Service, included in Microsoft Windows Server 2003, enables administrators to create an integrated approach to system backup and recovery that helps safeguard business-critical data without disrupting high-availability services like customer databases, e-commerce applications, and corporate messaging systems. In addition, the integrated backup approach described in this article can simplify system administration and storage management, helping to reduce total cost of ownership for today’s complex enterprise environments.

Ananda Sankaran (ananda_sankaran@dell.com) is a systems engineer in the High-Availability Cluster Development Group at Dell. His current interests related to high-availability clustering include cluster management, databases, SANs, and tape backup. Ananda has a master’s degree in Computer Science from Texas A&M University.

Kevin Guinn (kevin_guinn@dell.com) is a systems engineer in the High-Availability Cluster Development Group at Dell. His current interests include storage management and business continuity. Kevin has Microsoft Certified Systems Engineer (MCSE) and EMC Proven™ Professional certifications, and has a B.S in Mechanical Engineering from The University of Texas at Austin.

Dat Nguyen (quocdat_nguyen@dell.com) is a systems engineer in the High-Availability Cluster Development Group at Dell. His responsibilities include developing SAN-based high-availability clustering products that comprise Dell servers and Dell/EMC Fibre Channel storage systems. Dat has a B.S. in Electrical Engineering from The University of Houston.

**FOR MORE INFORMATION**


---

\(^3\)For more information, see the documentation for EMC SnapView and the Dell/EMC hardware provider online at [http://www.emc.com](http://www.emc.com).