Symantec System Recovery 2011: Protecting Active Directory Domain Controllers

Symantec™ System Recovery 2011

To sustain your operations, your business, and even your brand, you need to recover from a system failure as quickly as possible. However, manual system recovery processes prolong system downtime – and potential losses.

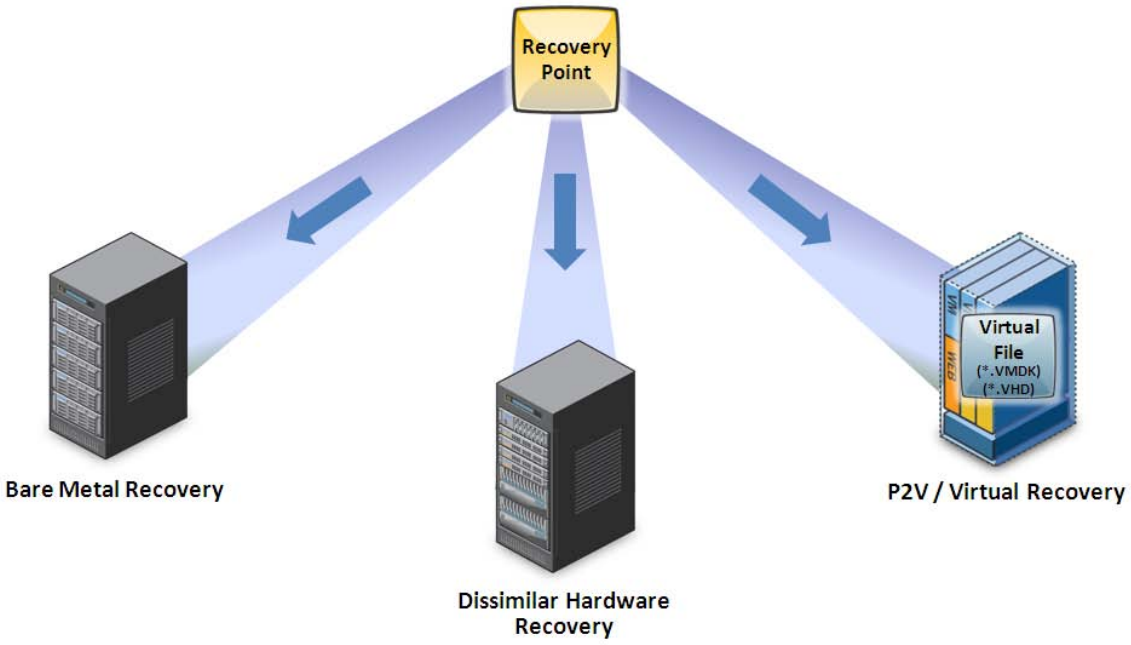
Symantec System Recovery 2011 offers a superior solution by delivering fast and reliable system recovery that helps minimize downtime and meet recovery time objectives with confidence. In just four simple steps, quickly restore physical and virtual systems to bare metal in minutes, even to dissimilar hardware, virtual environments, or remote locations with Symantec's patented Restore Anyware technology.

Built on 10 years of research and development and with more than 787,000 protected systems, Symantec System Recovery (formerly Backup Exec System Recovery) is one of the most proven, trusted, and reliable system recovery solutions.

Protecting Windows Domain Controllers

Symantec System Recovery 2011 fully supports the backup and recovery of Windows Server 2003 and Windows Server 2008 Active Directory Domain Controllers in either standalone or domain forest environments. Backups created by Symantec System Recovery 2011 are referred to as recovery points. Key supported recovery operations for Active Directory Domain Controllers include the following:

- Bare metal recovery of domain controllers back to their original hardware configuration
- Recovery of domain controllers to hardware configurations that differ from the original server's hardware
- Conversion of domain controller recovery points to both VMware and Microsoft Hyper-V virtual format



Note: For detailed information on the specific Microsoft server platforms supported by Symantec System Recovery, please consult the Symantec System Recovery Software Compatibility List (SCL) available for download here: http://entsupport.symantec.com/umi/V-306-38.

Volume Shadow Copy Service (VSS) Integration

Symantec System Recovery 2011 (SSR) works in accordance with Microsoft best practices to protect Windows 2003/R2 and Windows 2008/R2 servers, including Active Directory Domain Controllers. Through integration with the Microsoft Volume Shadow Copy Service (VSS), SSR ensures that Active Directory Domain Controller databases are correctly prepared for backup, ensuring that the server can be recovered properly.

There are three communicators in the VSS framework:

- Requestor
- Writer
- VSS Service

Within the VSS framework, Symantec System Recovery 2011 (SSR) acts as a requestor. When preparing to capture a snapshot of a volume, SSR sends a message to the VSS writers to prepare the volume and associated VSS-aware processes for backup. This momentarily halts operations and the volume and associated processes enter a 'silent' or consistent state that is optimal for backups. Symantec System Recovery 2011 then executes a snapshot of the volume it's protecting and captures backup data from those snapshots.

Upon completion of the snapshot capture process—only the momentary snapshot process, not the entire backup operation—SSR sends a message to the VSS writer that the snapshot is complete. The writer then notifies the volume and associated VSS-aware processes, and normal operations continue. SSR then proceeds to create recovery points of the protected volumes from the snapshots that have been captured.

The process whereby Symantec System Recovery 2011 (SSR) works with VSS to prepare server volumes and associated VSS-aware processes for backup is fully automated and is invisible to the user.

Note: If the 'Perform full VSS backup' advanced option is selected in the Symantec System Recovery backup job wizard, a request will also be sent to the VSS writer to truncate transaction logs (if needed). Using this option is highly recommended.

Resetting Domain Controller Invocation IDs and Preventing USN Rollbacks

An important element of properly backing up a domain controller is ensuring the backup process deals with the resetting of the domain controller's Invocation ID. Each domain controller in a forest has a different Invocation ID, allowing each domain controller to be properly identified in the forest and allowing replication processes to proceed correctly. If a domain controller is recovered in a forest environment and its Invocation ID has not been reset, a USN rollback can occur causing replication problems and allowing old data to return to the domain environment.

Symantec System Recovery 2011 integrates with the Microsoft Volume Shadow Copy Service (VSS) to properly prepare domain controllers for backup. During a backup operation, the VSS writer ensures that the backup being created of the domain controller is flagged as a backup copy. If a domain controller is recovered from that backup (either to original hardware, dissimilar hardware, or to a virtual environment via P2V) it will request a new Invocation ID allowing it to rejoin the domain properly and avoiding replication problems such as USN rollbacks. This process is fully automated and requires no user intervention.

Best Practices When Protecting Active Directory Domain Controllers

Please consider the following recommendations and best practices when protecting Active Directory Domain Controllers with Symantec System Recovery 2011:

- **Tombstone Lifetime** - Recovery points captured from domain controllers should not be older than the Tombstone Lifetime for the Active Directory Domain. Restoring a recovery point older than the Tombstone Lifetime could result in previously purged Active Directory objects being reintroduced into the domain environment.

  Note: The Tombstone Lifetime is the number of days before a deleted object is permanently purged from the directory services database. For Windows Server 2003 and Windows Server2008/R2, the default Tombstone Lifetime is 60 days.

- **Computer Account Password Age** - A recovery point of a domain controller should not be older than two times the maximum computer account password age. A maximum password age determines the number of days a password can be used before the system requires it to be changed. By default, this setting is defined in the Default Domain Group Policy Object (GPO) and in the local security policy of workstations and servers with a value of 30.

- **Recently Recovered Domain Controllers** - Newly-promoted or recovered domain controllers use a default computer account for the first few hours while they establish a valid and unique computer account**.** After performing a recover of an Active Directory Domain Controller, allow the domain controller to run for at least 24 hours before you create the first recovery point. This ensures that the domain controller has obtained a valid and unique computer account.

- **Check for Consistency** - Check a newly promoted or a restored Active Directory Domain Controller for consistency before creating the first recovery point.

- **Point In Time Consistency for Multi-volume Backups** - A recovery point of all the active disk volumes on a domain controller must be created and restored at the same time to preserve the synchronization of the domain controller's data. To do so, select all the domain controller's volumes when you create the schedule of the backup job. When multiple server volumes are included in the same backup job, snapshots for all included volumes are captured at the same point in time.

- **Top Down Restores** - In a server forest environment, when you restore a tree or an entire forest be sure that you restore from the top down to maintain domain integrity.

Restoring an Active Directory Domain Controller to Dissimilar Hardware

Symantec System Recovery 2011 can be used to restore Windows 2003 or Windows 2008/R2 Active Directory Domain Controllers to dissimilar hardware configurations. As described above, Symantec System Recovery 2011 interacts with the VSS service to prepare the domain controller and the Active Directory database for backup. Running with VSS disabled is not supported and causes domain controller failures upon restoration.

Automatic Detection and Installation of Critical Hardware Drivers

During a dissimilar hardware recovery operation, Symantec System Recovery's Restore Anyware feature automatically detects and installs the following key driver elements of the new server hardware configuration to ensure the Active Directory Domain Controller functions properly under the new hardware configuration:

- Mass storage controller
- Hardware Abstraction Layer (HAL)
- Network interface controller (NIC)
- Operating system kernel files

Windows Mini-setup

In addition, during a dissimilar hardware restore operation, Symantec System Recovery 2011 updates the volumes it is restoring such that the Windows mini-setup process will run during the first post-restore boot event. The Windows mini-setup process detects additional hardware changes and performs similar tasks that aid in the dissimilar hardware restore process.

Converting Active Directory Domain Controller Recovery Points to Virtual Format

Symantec System Recovery 2011 can also be used to convert recovery points of Windows 2003 or Windows 2008 Active Directory Domain Controllers to virtual format, including VMware (.VMDK) and Microsoft (.VHD) virtual format. As described above, Symantec System Recovery 2011 interacts with the VSS service to prepare the domain controller and the Active Directory database for backup. Running with VSS disabled is not supported and causes domain controller failures upon restoration. This same process helps ensure that the domain controller functions properly when run as a virtual machine.

When converting recovery points to VMware format, the resulting virtual disks can be optionally uploaded directly to an available ESX/i hypervisor host available on the network, making the virtual disk available in the VMFS file system to be imported and launched within a virtual machine managed by that ESX/i host.

Automatic Detection and Installation of Virtual Hardware Drivers

During a virtual conversion operation, Symantec System Recovery's Restore Anywhere feature automatically detects and installs the required virtual driver elements of the selected virtual platform into the virtual disk file being created. This virtual driver injection process is very similar to the process used to restore recovery points to dissimilar physical hardware configurations. The process of injecting key virtual drivers for the selected virtual technology ensures the Active Directory Domain Controller will boot and function properly while running in virtual mode. The Virtual drivers added include the following:

Virtual Platform	Drivers Added During P2V
VMware vSphere	• LSI SCSI Adapter (LSI_SAS.SYS) • VMware SCSI Adapter (vmscsi.sys) • VMware VMXNET NDIS driver (vmxnet.sys)
Microsoft Hyper-V	• LSI Logic Fusion-MPT (TM) Driver • LSI Pseudo Device

Windows Mini-setup

In addition, during a virtual conversion operation, Symantec System Recovery 2011 updates the volumes it is converting such that the Windows mini-setup process will run during the first post-restore boot event. The Windows mini-setup process detects additional virtual hardware components of the virtual machine and performs other tasks that aid in the virtual conversion process.

Summary

Symantec System Recovery 2011 fully supports the backup and recovery of Windows Server 2003 and Windows Server 2008 Active Directory Domain Controllers. This includes the ability to restore a domain controller to a bare metal configuration, to recover a domain controller to a dissimilar hardware configuration, to convert a recovery point of a domain controller to virtual disk format, and even to restore granular file and folder data from a domain controller recovery point.

Through integration with the Microsoft Volume Shadow Copy Service and the inclusion of the Restore Anyware feature, Symantec System Recovery ensures that domain controller volumes are properly protected and that the servers will boot and function correctly after a recovery or conversion event.

For More Information on Symantec System Recovery 2011

Link	Description
www.symantecsystemrecovery.com	Product Website
http://www.symantec.com/business/support/index?page=home&locale=en_us	Symantec Support Portal
http://entsupport.symantec.com/umi/V-306-38	Software Compatibility List

Related Microsoft Articles

Link	Description
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/a_tombstonelifetime.asp	Tombstone Lifetime
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/501.asp also see KB 175468	Maximum Password Age