ntdsutil

- Table of Contents

Open all sections | Close all sections

- Tool Overview

Category

Information Collection

Description

Used to maintain Active Directory databases.

Example of Presumed Tool Use During an Attack

This tool is used to extract NTDS.DIT (a database for NTDS) and another tool is used to analyze passwords.

- Tool Operation Overview

Item	Description
OS	Windows Server
Belonging to Domain	Required
Rights	Administrator
Service	Active Directory Domain Services

- Information Acquired from Log

Standard Settings

- Domain Controller
  - Start of service, history of driver installation to storage devices (system event log)
  - History of shadow copy creation (security event log)

Additional Settings

- Domain Controller
  - Execution history (audit policy, Sysmon)

- Evidence That Can Be Confirmed When Execution is Successful

- ntdsutil.exe was executed, and the Event ID: 8222 is recorded in the event log "Security".
- A request for a handle for object "[System Drive]\SNAP_[Date and Time]_VOLUME[Drive Letter]$" was successful.

- Main Information Recorded at Execution

- Domain Controller

Event log

#	Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **CommandLine**: Command line of the execution command (ntdsutil) • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\ntdsutil.exe) • **User**: Execute as user
2	Application	2006	ShadowCopy	The lsass ([Process ID]) shadow copy instance [Instance] completed successfully.
3	System	7036	Service Control Manager	The [Service Name] service entered the [Status] state. • **Status**: State after the transition (Running) • **Service Name**: Target service name (Volume Shadow Copy, Microsoft Software Shadow Copy Provider)
4	Security	8222	VSSAudit	Shadow copy has been created. • **Shadow Device Name**: Created name of the shadow device • **User SID**: Created SID of the user • **Process ID**: Created ID of the process • **User Name**: Created name of the user • **Source Computer**: Name of partition in the creation source host (\\?\Volume{[GUID]}\) • **Provider ID**: Created host • **Shadow Set ID/Shadow ID**: Created ID of the shadow • **Process Image Name**: Created GUID of the process • **Source Volume**: Volume served as the creation source (\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[Number])
5	Microsoft-Windows-Kernel-PnPConfig/Configuration	4	Kernel-PnPConfig	A new device interface of the interface class {[Interface Class]} '\\?\STORAGE#VolumeSnapshot#HarddiskVolumeSnapshot[Number]#{[Interface Class]}' has been registered.
6	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\VSSVC.exe) • **Object > Object Name**: Target file name (C:\$SNAP_[Date and Time]_VOLUMEC$)

Registry entry

#	Path	Value
1	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?	STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]

	#STORAGE#VolumeSnapshot#HarddiskVolumeSnapshot[Number]#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\DeviceInstance	
2	HKEY_USERS\[User SID]\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{[GUID]}	(Key)

- Details: Domain Controller

- Event Log

#	Event Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **LogonGuid/LogonId**: ID of the logon session • **ParentProcessGuid/ParentProcessId**: Process ID of the parent process • **ParentImage**: Executable file of the parent process (C:\Windows\System32\cmd.exe) • **CurrentDirectory**: Work directory • **CommandLine**: Command line of the execution command (ntdsutil) • **IntegrityLevel**: Privilege level (High) • **ParentCommandLine**: Command line of the parent process ("C:\Windowssystem32\cmd.exe") • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user • **Hashes**: Hash value of the executable file • **Image**: Path to the executable file (C:\Windows\System32\ntdsutil.exe)
	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Source Process Name**: Path to parent process that created the new process • **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (C:\Windows\System32\ntdsutil.exe) • **Process Information > Token Escalation Type**: Presence of privilege escalation • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process
2	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\system32\ntdsutil.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher)
3	Security	4624	Logon	An account was successfully logged on. • **Process Information > Process ID**: Process ID (hexadecimal) • **Network Information > Source Port**: Source port number • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Advapi)

				• **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on • **Logon Type**: Logon path, method, etc. (5=Service) • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\services.exe) • **Detailed Authentication Information > Authentication Package**: Authentication package used (Negotiate) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication (SYSTEM)
	Security	4672	Special Logon	Privileges assigned to a new logon. • **Privileges**: Assigned privileges (SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool (SYSTEM/SYSTEM/NT AUTHORITY) • **Subject > Logon ID**: Session ID of the user who executed the process
	Security	4670	Authorization Policy Change	Permissions on an object were changed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (change successful) • **Object > Object Name**: Target file name • **Subject > Account Name**: Name of the account that executed the tool • **Subject > Account Domain**: Domain to which the account belongs • **Change permissions > New security descriptor**: Security descriptor after the change (D:(A;;GA;;;SY)(A;;RC;;;OW)(A;;GA;;;[SID])) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\services.exe) • **Change permissions > Original security descriptor**: Security descriptor before the change (D:(A;;GA;;;SY)(A;;RCGXGR;;;BA)) • **Subject > Security ID**: SID of the user who executed the tool (SYSTEM) • **Object > Object Type**: Target category (Token) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
4	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **LogonGuid/LogonId**: ID of the logon session • **ParentProcessGuid/ParentProcessId**: Process ID of the parent process • **ParentImage**: Executable file of the parent process (C:\Windows\System32\services.exe) • **CurrentDirectory**: Work directory (C:\Windows\system32\) • **CommandLine**: Command line of the execution command (C:\Windows\system32\vssvc.exe) • **IntegrityLevel**: Privilege level (System) • **ParentCommandLine**: Command line of the parent process (C:\Windows\system32\services.exe) • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user (NT AUTHORITY\SYSTEM) • **Hashes**: Hash value of the executable file • **Image**: Path to the executable file (C:\Windows\System32\VSSVC.exe)
	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Source Process Name**: Path to parent process that created the new process

				• **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (C:\Windows\System32\VSSVC.exe) • **Process Information > Token Escalation Type**: Presence of privilege escalation • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process
5	Microsoft-Windows-Sysmon/Operational	12/13	Registry object added or deleted / Registry value set (rule: RegistryEvent)	Registry object added or deleted. / Registry value set. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\system32\vssvc.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Registry value at the write destination (multiple entries under \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag)
6	Security	4661	SAM	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target object name • **Access Request Information > Access**: Requested privilege • **Object > Object Server**: SecurityAccount Manager (Security Account Manager) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\lsass.exe) • **Object > Object Type**: Target category (SAM_DOMAIN) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4661	SAM	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target object name • **Access Request Information > Access**: Requested privilege • **Object > Object Server**: SecurityAccount Manager (Security Account Manager) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\lsass.exe) • **Object > Object Type**: Target category (SAM_ALIAS) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the objec (C:\Windows\System32\lsass.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)

	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\VSSVC.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
7	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (C:\Windows\system32\vssvc.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\System Volume Information\RemoteVss) • **CreationUtcTime**: File creation date and time (UTC)
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including SYNCHRONIZE and WriteAttributes) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\System Volume Information\RemoteVss) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\VSSVC.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteAttributes) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\System Volume Information\RemoteVss) • **Access Request Information > Access**: Requested privilege • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\VSSVC.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\VSSVC.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
8	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (C:\Windows\system32\vssvc.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\System Volume Information\RemoteVss\{[GUID]}-{[GUID]}.PMS) • **CreationUtcTime**: File creation date and time (UTC)

	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\System Volume Information\RemoteVss\{[GUID]}-{[GUID]}.PMS) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\VSSVC.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile, AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\System Volume Information\RemoteVss\{[GUID]}-{[GUID]}.PMS) • **Access Request Information > Access**: Requested privilege • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\VSSVC.exe) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\VSSVC.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
9	Security	4624	Logon	An account was successfully logged on. • **Process Information > Process ID**: Process ID (hexadecimal) • **Network Information > Source Port**: Source port number • **New Logon > Logon ID/Logon GUID**: Session ID of the user who was logged on • **Detailed Authentication Information > Package Name (NTLM only)**: NTLM version • **Detailed Authentication Information > Logon Process**: Process used for logon (Advapi) • **New Logon > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who was logged on (SYSTEM/SYSTEM/NT AUTHORITY) • **Logon Type**: Logon path, method, etc. (5) • **Network Information > Workstation Name**: Name of the host that requested the logon • **Detailed Authentication Information > Key Length**: Length of the key used for the authentication (0) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\services.exe) • **Detailed Authentication Information > Authentication Package**: Authentication package used (Negotiate) • **Network Information > Source Network Address**: IP address that requested the logon • **Subject > Logon ID**: Session ID of the user who executed the authentication (SYSTEM)
	Security	4672	Special Logon	Privileges assigned to a new logon.

				• **Privileges**: Assigned privileges (SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool (SYSTEM/SYSTEM/NT AUTHORITY) • **Subject > Logon ID**: Session ID of the user who executed the process
	Security	4670	Authorization Policy Change	Permissions on an object were changed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (change successful) • **Object > Object Name**: Target file name • **Subject > Account Name**: Name of the account that executed the tool • **Subject > Account Domain**: Domain to which the account belongs • **Change permissions > New security descriptor**: Security descriptor after the change (D:(A;;GA;;;SY)(A;;RC;;;OW)(A;;GA;;;[SID])) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\services.exe) • **Change permissions > Original security descriptor**: Security descriptor before the change (D:(A;;GA;;;SY)(A;;RCGXGR;;;BA)) • **Subject > Security ID**: SID of the user who executed the tool (SYSTEM) • **Object > Object Type**: Target category (Token) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
10	System	7036	Service Control Manager	The [Service Name] service entered the [Status] state. • **Status**: State after the transition (Running) • **Service Name**: Target service name (Volume Shadow Copy)
	System	7036	Service Control Manager	The [Service Name] service entered the [Status] state. • **Status**: State after the transition (Running) • **Service Name**: Target service name (Microsoft Software Shadow Copy Provider)
11	Security	4661	SAM	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target object name • **Access Request Information > Access**: Requested privilege • **Object > Object Server**: SecurityAccount Manager (Security Account Manager) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\lsass.exe) • **Object > Object Type**: Target category (SAM_DOMAIN) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4661	SAM	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target object name • **Access Request Information > Access**: Requested privilege • **Object > Object Server**: SecurityAccount Manager (Security Account Manager) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\lsass.exe) • **Object > Object Type**: Target category (SAM_ALIAS) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle

	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the objec (C:\Windows\System32\lsass.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the objec (C:\Windows\System32\lsass.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
12	System	7036	Service Control Manager	The [Service Name] service entered the [Status] state. • **Status**: State after the transition (Running) • **Service Name**: Target service name (Device Setup Manager)
	Application	2005	ShadowCopy	The lsass ([Process ID]) shadow copy instance [Instance] starting. This will be a full shadow copy.
	Application	2001	ShadowCopy	The lsass ([Process ID]) shadow copy instance [Instance] freeze started.
	Application	2003	ShadowCopy	The lsass ([Process ID]) shadow copy instance [Instance] freeze ended.
	Application	2006	ShadowCopy	The lsass ([Process ID]) shadow copy instance [Instance] completed successfully.
	Microsoft-Windows-Kernel-PnP/Configuration	400	Kernel-PnP	Device STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number] was configured. • **Driver Name**: Name of the driver (volsnap.inf) • **Class GUID**: Device class ({533c5b84-ec70-11d2-9505-00c04f79deaf}) • **Driver Date**: Date of the driver • **Driver Version**: Version of the driver • **Matching Device ID**: Device ID (STORAGE\VolumeSnapshot) • **Driver Provider**: Provider of the driver (Microsoft) • **Driver Rank**: Rank of the driver (0xFF0000) • **Driver Section**: Section of the driver (volume_snapshot_install.NTamd64)
	Microsoft-Windows-Kernel-PnP/Configuration	410	Kernel-PnP	Device STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number] was started. • **Driver Name**: Name of the driver (volsnap.inf) • **Class GUID**: Device class ({533c5b84-ec70-11d2-9505-00c04f79deaf})
	Microsoft-Windows-Kernel-PnPConfig/Configuration	1	Kernel-PnPConfig	The configuration of device container {[Container Number]} was canceled.
	Microsoft-Windows-Kernel-PnPConfig/Configuration	4	Kernel-PnPConfig	A new device interface of the interface class {[Interface Class]} '\\?\STORAGE#VolumeSnapshot#HarddiskVolumeSnapshot[Number]#{[Interface Class]}' has been registered.
14	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (System) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\System Volume Information\{[GUID]}{[GUID]}) • **CreationUtcTime**: File creation date and time (UTC)
	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (System) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\System Volume Information\{[GUID]})

				• **CreationUtcTime**: File creation date and time (UTC)
15	Application	102	General	The lsass ([Process ID]) database engine started a new instance ([Instance]). • **Process ID**: Process ID of lsass.exe • **Instance**: Instance number of the lsass database
	Application	300	Logging/Recovery	The lsass ([Process ID]) database engine is initiating recovery steps.
	Application	216	Logging/Recovery	It was detected that the location of the lsass ([Process ID]) database had been moved from '[Move From]' to '[Move To]'. • **Process ID**: Process ID of lsass.exe • **Move From**: ntds.dit at the source location ('C:\Windows\NTDS\ntds.dit') • **Move To**: ntds.dit at the destination location ('\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[Number]\Windows\NTDS\ntds.dit')
	Application	302	Logging/Recovery	The lsass ([Process ID]) database engine completed recovery steps successfully.
	Application	105	General	The lsass ([Process ID]) database engine has started a new instance ([Instance]). (time=[Time] second) • **Process ID**: Process ID of lsass.exe • **Time**: Time required for startup • **Instance**: Instance number of the lsass database
	Application	103	General	The lsass ([Process ID]) database engine stopped an instance ([Instance]). • **Process ID**: Process ID of lsass.exe • **Instance**: Instance number of the lsass database
16	Security	4904	Audit Policy Change	An attempt was made to register a security event source. • **Event Source > Source Name**: Registered name of the event source (VSSAudit) • **Subject > Account Name**: Name of the account that executed the tool • **Event Source > Event Source ID**: Event Source ID • **Subject > Account Domain**: Domain to which the account belongs • **Process > Process ID**: ID of the process that attempted registration • **Process > Process Name**: Name of the process that attempted registration (C:\Windows\System32\VSSVC.exe) • **Subject > Security ID**: SID of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who attempted registration
	Security	8222	VSSAudit	Shadow copy has been created. • **Shadow Device Name**: Created name of the shadow device • **User SID**: Created SID of the user • **Process ID**: Created ID of the process • **User Name**: Created name of the user • **Source Computer**: Name of partition in the creation source host (\\?\Volume{[GUID]}\) • **Provider ID**: Created host • **Shadow Set ID/Shadow ID**: Created ID of the shadow • **Process Image Name**: Created GUID of the process • **Source Volume**: Volume served as the creation source (\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy[Number])

	Security	4905	Audit Policy Change	An attempt was made to unregister a security event source. • **Event Source > Source Name**: Name of the event source that was unregistered (VSSAudit) • **Subject > Account Name**: Name of the account that executed the tool • **Event Source > Event Source ID**: Event Source ID • **Subject > Account Domain**: Domain to which the account belongs • **Process > Process ID**: ID of the process that attempted unregistration • **Process > Process Name**: Name of the process that attempted unregistration (C:\Windows\System32\VSSVC.exe) • **Subject > Security ID**: SID of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who attempted unregistration
17	Security	4661	SAM	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target object name (CN=Builtin,DC=[DN]) • **Access Request Information > Access**: Requested privilege • **Object > Object Server**: SecurityAccount Manager (Security Account Manager) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\lsass.exe) • **Object > Object Type**: Target category (SAM_DOMAIN) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the objec (C:\Windows\System32\lsass.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
18	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (C:\Windows\system32\ntdsutil.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\$SNAP_[Execution Date and Time]_VOLUMEC$) • **CreationUtcTime**: File creation date and time (UTC)
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\$SNAP_[Date and Time]_VOLUMEC$) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\VSSVC.exe) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\VSSVC.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool

				• **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4673	Sensitive Privilege Use	A privileged service was called. • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process > Process ID**: Process ID of the process that used the privileges (C:\Windows\explorer.exe) • **Subject > Logon ID**: Session ID of the user who executed the process • **Service Request Information > Privilege**: Privileges used (SeTcbPrivilege) • **Process > Process Name**: Process that used the privilege
19	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	Process terminated. • **UtcTime**: Process terminated date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\ntdsutil.exe)
	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Exit Status**: Process return value (0x0) • **Log Date and Time**: Process terminated date and time (local time) • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\ntdsutil.exe) • **Subject > Logon ID**: Session ID of the user who executed the process

- Registry Entry

#	Path	Type	
1	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\DriverDesc	String	Generic vo
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\ProviderName	String	Microsoft
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\DriverDateData	String	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\DriverDate	String	[Driver Up
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\DriverVersion	String	[Version N
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\InfPath	String	volsnap.in
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\InfSection	String	volume_sn
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{533c5b84-ec70-11d2-9505-00c04f79deaf}\0000\MatchingDeviceId	String	STORAGE\
2	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#VolumeSnapshot#HarddiskVolumeSnapshot[Number]#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\DeviceInstance	String	STORAGE\
3	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\Capabilities	DWORD	0x000000
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\ConfigFlags	DWORD	0x000000
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\ContainerID	String	{0000000
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\HardwareID	String	[RANDOM
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\ClassGUID	String	{533c5b84
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\DeviceDesc	String	@volsnap. volume sh
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\Driver	String	{533c5b84
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]\Mfg	String	@volsnap.
4	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\DFS Replication service writer\IDENTIFY (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\DFS Replication service writer\IDENTIFY (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer	Key	(No value

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\FSProvider_{89300202-3cec-4981-9171-19f59559e0f2}	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelacev	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\IDENTIFY (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\PREPAREBACKUP (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\PREPAREBACKUP (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\VSS_WS_STABLE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\PREPARESNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\PREPARESNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\VSS_WS_WAITING_FOR_FREEZE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\FREEZE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\FREEZE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\VSS_WS_WAITING_FOR_THAW (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\BKGND_FREEZE_THREAD (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\THAW (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\BKGND_FREEZE_THREAD (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\THAW (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\VSS_WS_WAITING_FOR_POST_SNAPSHOT (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\POSTSNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\POSTSNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\VSS_WS_WAITING_FOR_BACKUP_COMPLETE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\GETSTATE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\GETSTATE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\BACKUPCOMPLETE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\NTDS\BACKUPCOMPLETE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}DeleteProcess (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}DeleteProcess (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}PrepareForSnapshot (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}PreExposure (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}PreExposure (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}PrepareForSnapshot (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}EndCommit (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}EndCommit (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}SetIgnorable (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}SetIgnorable (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}AdjustBitmap (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}ComputeIgnorableProduct (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}ComputeIgnorableProduct (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{[GUID]}AdjustBitmap (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher	Key	(No value
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\WMI Writer\IDENTIFY (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\WMI Writer\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer\IDENTIFY (Enter)	Binary	[Binary Val

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer\IDENTIFY (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace\OPEN_VOLUME_HANDLE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace\OPEN_VOLUME_HANDLE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace\IOCTL_FLUSH_AND_HOLD (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace\IOCTL_FLUSH_AND_HOLD (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace\IOCTL_RELEASE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace\IOCTL_RELEASE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)\OPEN_VOLUME_HANDLE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)\OPEN_VOLUME_HANDLE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)\IOCTL_FLUSH_AND_HOLD (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)\IOCTL_FLUSH_AND_HOLD (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)\IOCTL_RELEASE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(C:_)\IOCTL_RELEASE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\IDENTIFY (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\PREPAREBACKUP (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\PREPAREBACKUP (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\VSS_WS_STABLE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\PREPARESNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\PREPARESNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\VSS_WS_WAITING_FOR_FREEZE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\FREEZE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\FREEZE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\VSS_WS_WAITING_FOR_THAW (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\BKGND_FREEZE_THREAD (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\THAW (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\BKGND_FREEZE_THREAD (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\THAW (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\VSS_WS_WAITING_FOR_POST_SNAPSHOT (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\POSTSNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\POSTSNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\VSS_WS_WAITING_FOR_BACKUP_COMPLETE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\GETSTATE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\GETSTATE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\BACKUPCOMPLETE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer\BACKUPCOMPLETE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\IDENTIFY (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\PREPAREBACKUP (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\PREPAREBACKUP (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\VSS_WS_STABLE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\PREPARESNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\PREPARESNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\VSS_WS_WAITING_FOR_FREEZE (SetCurrentState)	Binary	[Binary Val

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\FREEZE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\FREEZE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\VSS_WS_WAITING_FOR_THAW (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\BKGND_FREEZE_THREAD (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\THAW (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\BKGND_FREEZE_THREAD (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\THAW (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\VSS_WS_WAITING_FOR_POST_SNAPSHOT (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\POSTSNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\POSTSNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\VSS_WS_WAITING_FOR_BACKUP_COMPLETE (SetCurrentState)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\GETSTATE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\GETSTATE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\BACKUPCOMPLETE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer\BACKUPCOMPLETE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_BEGINPREPARE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_BEGINPREPARE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_ENDPREPARE (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_ENDPREPARE (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_PRECOMMIT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_PRECOMMIT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_COMMIT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_COMMIT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_POSTCOMMIT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_POSTCOMMIT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_PREFINALCOMMIT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_PREFINALCOMMIT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_POSTFINALCOMMIT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}\PROVIDER_POSTFINALCOMMIT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\IDENTIFY (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\IDENTIFY (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\PREPAREBACKUP (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\PREPAREBACKUP (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\DOSNAPSHOT (Enter)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\DOSNAPSHOT (Leave)	Binary	[Binary Val
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\GETSTATE (Enter)	Binary	[Binary Val

	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\GETSTATE (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\BACKUPCOMPLETE (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher\BACKUPCOMPLETE (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\PREPARESNAPSHOT (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\PREPARESNAPSHOT (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_FRONT (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_FRONT (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_BACK (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_BACK (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_SYSTEM (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_SYSTEM (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_KTM (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_KTM (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_RM (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE_RM (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\FREEZE (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\THAW_KTM (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\THAW_KTM (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\THAW (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\THAW (Leave)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\POSTSNAPSHOT (Enter)	Binary	[Binary Val
	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher\POSTSNAPSHOT (Leave)	Binary	[Binary Val
5	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\DeviceContainers\{00000000-0000-0000-FFFF-FFFFFFFFFFFF}\BaseContainers\{00000000-0000-0000-FFFF-FFFFFFFFFFFF}\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Number]	Binary	(No value
6	HKEY_USERS\[User SID]\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{[GUID]}	Key	(No value
	HKEY_USERS\[User SID]\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\LocalMOF	Key	(No value