applications (their problems)
backup (to support the apps)
…
restore (just a click)
recovery (the real job)

Ondřej Ševeček |
ondrej@sevecek.com |
www.sevecek.com

26. – 28. september 2022

#ntk22

Backup types

- VSS backup from inside an OS
  - block copy-on-write backup
  - application signal
- VSS backup from outside VM in its hosting hypervisor
  - block copy-on-write backup in host
  - application signal into guest
- standard VM checkpoint (snapshot)
  - block incremental backup in host
- production VM checkpoint (snapshot)
  - block incremental backup in host
  - application signal into guest
- Hyper-V replica
  - block incremental backup in host
  - application signal into guest sometimes

Volume Shadow Copy

The application problems solved by VSS

- killed applications with in-memory cached data
  - fail, freeze, power failure, accidental kill, ...
- exclusively locked database files
- inconsistent data files when "tearing" the drive between two sector writes
  - dirty shutdowns and recovery

VSS useful commands

```
diskshadow /l c:\temp\diskshadow.txt

# no writers called here
(gwmi -list Win32_ShadowCopy).Create('C:\', 'ClientAccessible')

gwmi Win32_ShadowCopy

# mind the terminating backslash
mklink /J c:\backup \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\
```

VSS useful commands

```
gwmi Win32_ShadowStorage | select @{ N = 'Disk'; E = { gwmi Win32_Volume | ? DeviceId -eq
$PSItem.Volume.Split('=')[1].Trim('"').Replace('\\', '\') | select -Expand Name } }, MaxSpace, UsedSpace

# for Hyper-V guests to get notified, you must let the writers be called and include all volumes
diskshadow
        set context persistent
        begin backup
        add volume d:
        add volume e:
        create
        end backup

diskshadow
        list shadows all
        delete shadows all
```

VSS writers - registry

diskshadow.txt - Notepad

File Edit Format View Help

```
* WRITER "Registry Writer"
        - Writer ID   = {afbab4a2-367d-4d15-a586-71dbb18f8485}
        - Writer instance ID = {6d60a336-5270-45ff-bb7a-d19f95a419f1}
        - Supports restore events = FALSE
        - Writer restore conditions = VSS_WRE_NEVER
        - Restore method = VSS_RME_RESTORE_AT_REBOOT_IF_CANNOT_REPLACE
        - Requires reboot after restore = TRUE
        - Excluded files:
        + Component "Registry Writer:\Registry"
                - Name: Registry
                - Logical path:
                - Full path: \Registry
                - Caption: Registry
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: TRUE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - C:\Windows\System32\SMI\Store\Machine
                        - C:\Windows\system32\config
                - Volumes affected by this component:
                      - \\?\Volume{6de0fe21-a857-4147-8298-3d4be655b84f}\ [C:\]
                - Component Dependencies:
```

VSS writers - Active Directory (NTDS)

diskshadow.txt - Notepad

File Edit Format View Help

```
* WRITER "NTDS"
        - Writer ID   = {b2014c9e-8711-4c5c-a5a9-3cf384484757}
        - Writer instance ID = {f3ef6337-13d5-4dde-b8fd-0bfa2cfbe141}
        - Supports restore events = FALSE
        - Writer restore conditions = VSS_WRE_NEVER
        - Restore method = VSS_RME_RESTORE_IF_CAN_REPLACE
        - Requires reboot after restore = TRUE
        - Excluded files:
        + Component "NTDS:\C:_Windows_NTDS\ntds"
                - Name: ntds
                - Logical path: C:_Windows_NTDS
                - Full path: \C:_Windows_NTDS\ntds
                - Caption:
                - Type: VSS_CT_DATABASE [1]
                - Is selectable: FALSE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - C:\Windows\NTDS
                - Volumes affected by this component:
                      - \\?\Volume{6de0fe21-a857-4147-8298-3d4be655b84f}\ [C:\]
                - Component Dependencies:
```

VSS writers - DFSR

diskshadow.txt - Notepad

File Edit Format View Help

```
* WRITER "DFS Replication service writer"
        - Writer ID   = {2707761b-2324-473d-88eb-eb007a359533}
        - Writer instance ID = {a212513a-2194-46a6-9dcd-226fa96730a3}
        - Supports restore events = TRUE
        - Writer restore conditions = VSS_WRE_ALWAYS
        - Restore method = VSS_RME_RESTORE_IF_CAN_REPLACE
        - Requires reboot after restore = FALSE
        - Excluded files:
                - Exclude: Path = C:\Windows\SYSVOL\domain\DfsrPrivate, Filespec =
                - Exclude: Path = C:\Windows\SYSVOL\staging areas\gopas.virtual, Fi
                - Exclude: Path = C:\Windows\SYSVOL\domain\DfsrPrivate\ConflictAndD
       + Component "DFS Replication service writer:\SYSVOL\4D13DCC3-E7AF-40FF-8000
                - Name: 4D13DCC3-E7AF-40FF-8000-898F94E07FBE-EEAEE362-3B7D-4084-86E
                - Logical path: SYSVOL
                - Full path: \SYSVOL\4D13DCC3-E7AF-40FF-8000-898F94E07FBE-EEAEE362-
                - Caption: SYSVOL Share
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: TRUE
                - Is top level: TRUE
                - Notify on backup complete: TRUE
                - Paths affected by this component:
                        - C:\Windows\SYSVOL
                - Volumes affected by this component:
                        - \\?\Volume{6de0fe21-a857-4147-8298-3d4be655b84f}\ [C:\]
                - Component Dependencies:
```

VSS writers - NPS server

diskshadow.txt - Notepad

File Edit Format View Help

```
* WRITER "NPS VSS Writer"
        - Writer ID   = {35e81631-13e1-48db-97fc-d5bc721bb18a}
        - Writer instance ID = {5decb375-d4be-4102-bbad-27e45f737292}
        - Supports restore events = FALSE
        - Writer restore conditions = VSS_WRE_NEVER
        - Restore method = VSS_RME_RESTORE_AT_REBOOT
        - Requires reboot after restore = TRUE
        - Excluded files:
        + Component "NPS VSS Writer:\NPS Database"
                - Name: NPS Database
                - Logical path:
                - Full path: \NPS Database
                - Caption: NPS Database
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: FALSE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - C:\Windows\system32\ias
                - Volumes affected by this component:
                      - \\?\Volume{6de0fe21-a857-4147-8298-3d4be655b84f}\ [C:\]
                - Component Dependencies:
```

VSS writers - DHCP server

diskshadow.txt - Notepad

File Edit Format View Help

```
* WRITER "Dhcp Jet Writer"
        - Writer ID   = {be9ac81e-3619-421f-920f-4c6fea9e93ad}
        - Writer instance ID = {89774d31-045e-4316-bbd3-140e5aac702f}
        - Supports restore events = TRUE
        - Writer restore conditions = VSS_WRE_IF_REPLACE_FAILS
        - Restore method = VSS_RME_RESTORE_AT_REBOOT
        - Requires reboot after restore = TRUE
        - Excluded files:
        + Component "Dhcp Jet Writer:\C:_Windows_system32_dhcp\dhcp"
                - Name: dhcp
                - Logical path: C:_Windows_system32_dhcp
                - Full path: \C:_Windows_system32_dhcp\dhcp
                - Caption:
                - Type: VSS_CT_DATABASE [1]
                - Is selectable: FALSE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - C:\Windows\system32\dhcp
                - Volumes affected by this component:
                      - \\?\Volume{6de0fe21-a857-4147-8298-3d4be655b84f}\ [C:\]
                - Component Dependencies:
```

VSS writers - SQL server

diskshadow.txt - Notepad

File Edit Format View Help

```
* WRITER "SqlServerWriter"
        - Writer ID   = {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
        - Writer instance ID = {51541a18-eadb-40f9-a6da-6be94eab11d4}
        - Supports restore events = TRUE
        - Writer restore conditions = VSS_WRE_ALWAYS
        - Restore method = VSS_RME_RESTORE_IF_CAN_REPLACE
        - Requires reboot after restore = FALSE
        - Excluded files:
        + Component "SqlServerWriter:\DATA1\SPINTRANET\master"
                - Name: master
                - Logical path: DATA1\SPINTRANET
                - Full path: \DATA1\SPINTRANET\master
                - Notify on backup complete: TRUE
                - Paths affected by this component:
                        - F:\SQL-SPIntranet\MSSQL11.SPINTRANET\MSSQL\DATA
                - Volumes affected by this component:
                      - \\?\Volume{22a69c25-1a77-4a8f-a051-668c2c5c23c4}\ [F:\]
        + Component "SqlServerWriter:\DATA1\SPINTRANET\AdventureWorks"
                - Name: AdventureWorks
                - Logical path: DATA1\SPINTRANET
                - Full path: \DATA1\SPINTRANET\AdventureWorks
                - Notify on backup complete: TRUE
                - Paths affected by this component:
                        - F:\SQL-SPIntranet\MSSQL11.SPINTRANET\MSSQL\Data
                - Volumes affected by this component:
                      - \\?\Volume{22a69c25-1a77-4a8f-a051-668c2c5c23c4}\ [F:\]
```

VSS writers - IIS

writers.txt - Notepad

File Edit Format View Help

```
* WRITER "IIS Config Writer"
        - Writer ID   = {2a40fd15-dfca-4aa8-a654-1f8c654603f6}
        - Writer instance ID = {a7f169fe-0b15-4e99-8845-9603c21e8dc5}
        - Supports restore events = FALSE
        - Writer restore conditions = VSS_WRE_NEVER
        - Restore method = VSS_RME_RESTORE_AT_REBOOT_IF_CANNOT_REPLACE
        - Requires reboot after restore = FALSE
        - Excluded files:
        + Component "IIS Config Writer:\IISCONFIG"
                - Name: IISCONFIG
                - Logical path:
                - Full path: \IISCONFIG
                - Caption:
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: FALSE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - C:\Windows\system32\inetsrv\config
                - Volumes affected by this component:
                      - \\?\Volume{b7f9a468-3e6f-11ed-80bf-806e6f6e6963}\ [C:\]
                - Component Dependencies:
```

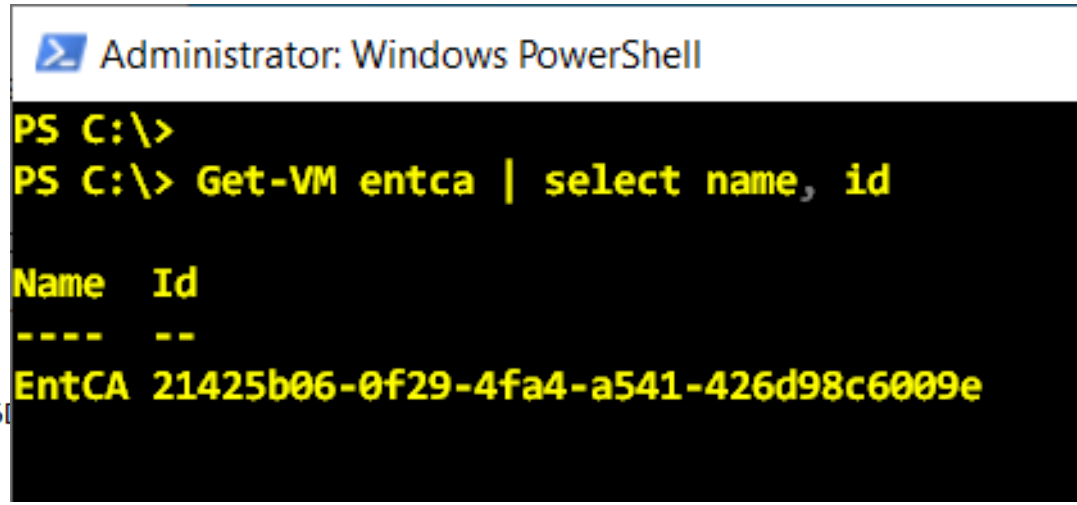
VSS writers - ADFS with dependency

```
* WRITER "ADFS VSS Writer"
        - Writer ID    = {772c45f8-ae01-4f94-940c-94961864acad}
        - Writer instance ID = {b71a9b91-e89a-49ce-81d9-d2366e5cf054}
        - Supports restore events = FALSE
        - Writer restore conditions = VSS_WRE_NEVER
        - Restore method = VSS_RME_STOP_RESTORE_START
        - Requires reboot after restore = FALSE
        - Excluded files:
        + Component "ADFS VSS Writer:\ADFS"
                - Name: ADFS
                - Logical path:
                - Full path: \ADFS
                - Caption: ADFS files
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: TRUE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - C:\Windows\ADFS
                - Volumes affected by this component:
                      - \\?\Volume{3ac60c6d-d332-40fa-9564-4efda269b0eb}\ [C:\]
                - Component Dependencies:
        + Component "ADFS VSS Writer:\ADFSDatabase"
                - Name: ADFSDatabase
                - Logical path:
                - Full path: \ADFSDatabase
                - Caption: ADFS Database files
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: TRUE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                - Volumes affected by this component:
                - Component Dependencies:
                        - Dependency to "{8d5194e1-e455-434a-b2e5-51296cce67df}:\AUTH\MICROSOFT##WID\AdfsConfigu

                        - Dependency to "{8d5194e1-e455-434a-b2e5-51296cce67df}:\AUTH\MICROSOFT##WID\AdfsArtifac
```

VSS writers - Hyper-V

```
* WRITER "Microsoft Hyper-V VSS Writer"
        - Writer ID   = {66841cd4-6ded-4f4b-8f17-fd23f8ddc3de}
        - Writer instance ID = {f0f3f007-6372-431a-9c56-ef9c6e52d56e}
        - Supports restore events = TRUE
        - Writer restore conditions = VSS_WRE_ALWAYS
        - Restore method = VSS_RME_RESTORE_IF_CAN_REPLACE
        - Requires reboot after restore = FALSE
        - Excluded files:
        + Component "Microsoft Hyper-V VSS Writer:\21425B06-0F29-4FA4-A541-426D
                - Name: 21425B06-0F29-4FA4-A541-426D98C6009E
                - Logical path:
                - Full path: \21425B06-0F29-4FA4-A541-426D98C6009E
                - Caption: Online\EntCA
                - Type: VSS_CT_FILEGROUP [2]
                - Is selectable: TRUE
                - Is top level: TRUE
                - Notify on backup complete: FALSE
                - Paths affected by this component:
                        - D:\MACHINES-goc173\EntCA
                        - D:\MACHINES-goc173\EntCA\
                        - D:\MACHINES-goc173\EntCA\Snapshots
                        - D:\MACHINES-goc173\EntCA\Snapshots\
                        - D:\MACHINES-goc173\EntCA\Snapshots\5245D1D8-17FE-408A-9F
                        - D:\MACHINES-goc173\EntCA\Virtual Machines\
                        - E:\BUILDER\!Base\
                - Volumes affected by this component:
                      - \\?\Volume{084da6ea-0000-0000-0000-a01e06000000}\ [D:\]
                      - \\?\Volume{06fcd6c9-0000-0000-0000-100000000000}\ [E:\]
```



Performance considerations

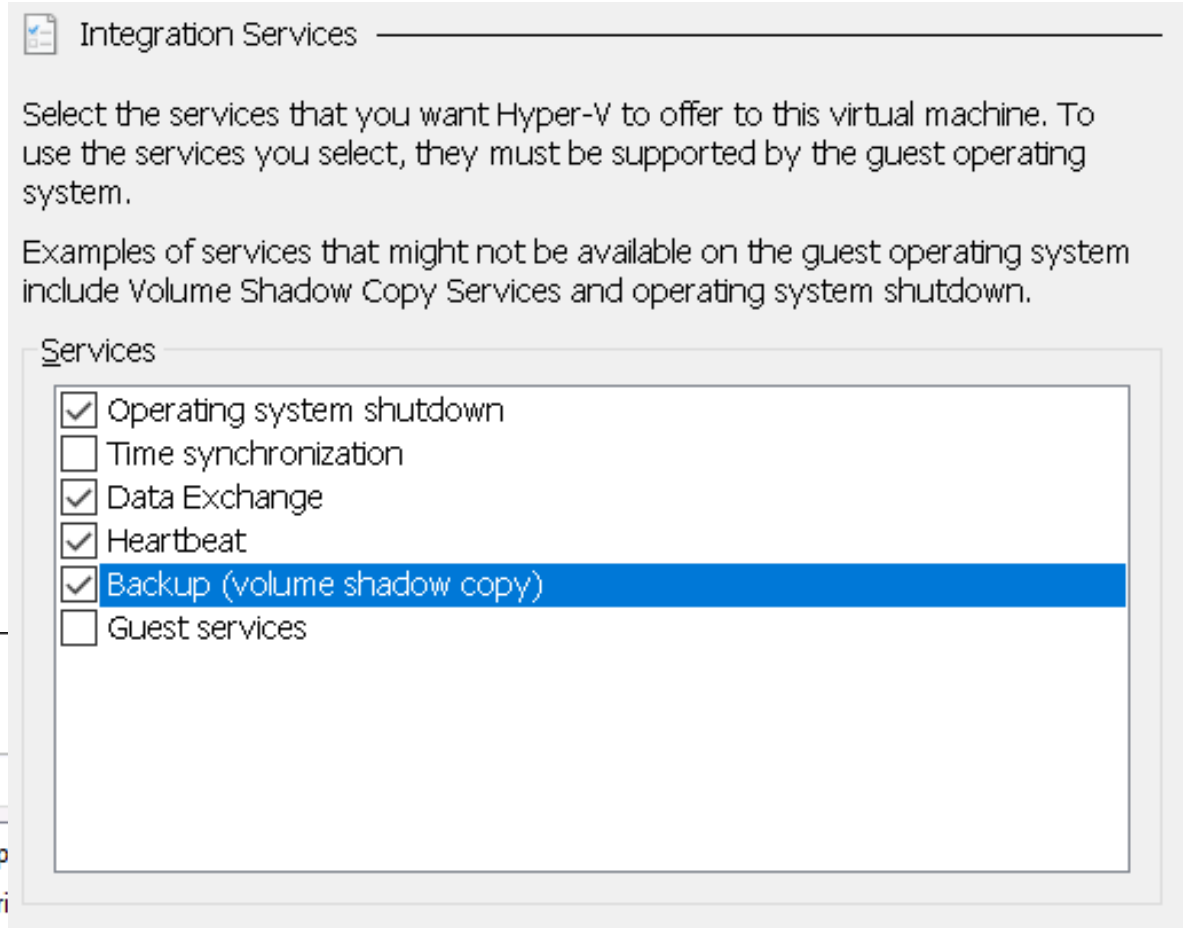
- copy-on-write (System Volume Information cache)
  - slower disk writes
- space consumption
  - per 64 kB blocks
- automatic liquidation on space overflow
  - backup failure

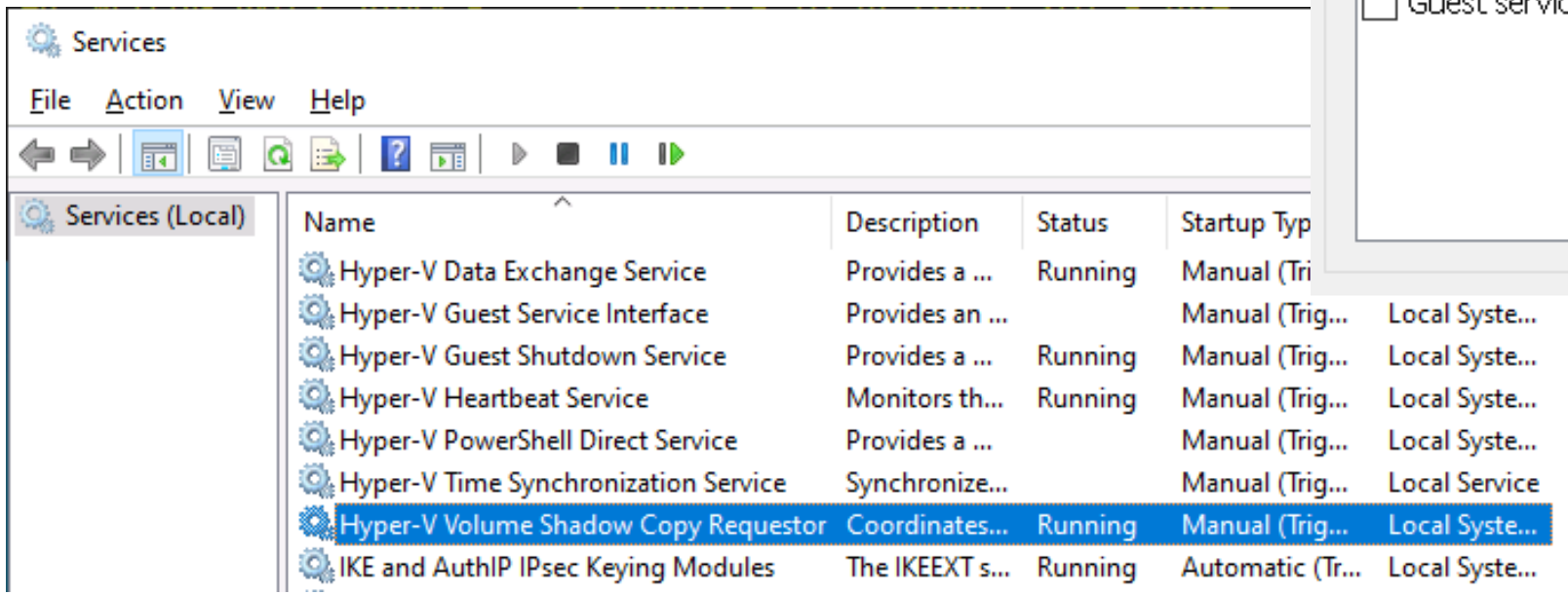
- registry exemptions
  - `HKLM\System\CurrentControlSet\Control\BackupRestore`
  - `FileNotToSnapshot = MULTI_SZ = C:\path\* /s`
  - `must use DISKSHADOW, not for ClientAccessible`

Backup from hypervisor

Backup from outside VM inside its hosting hypervizor

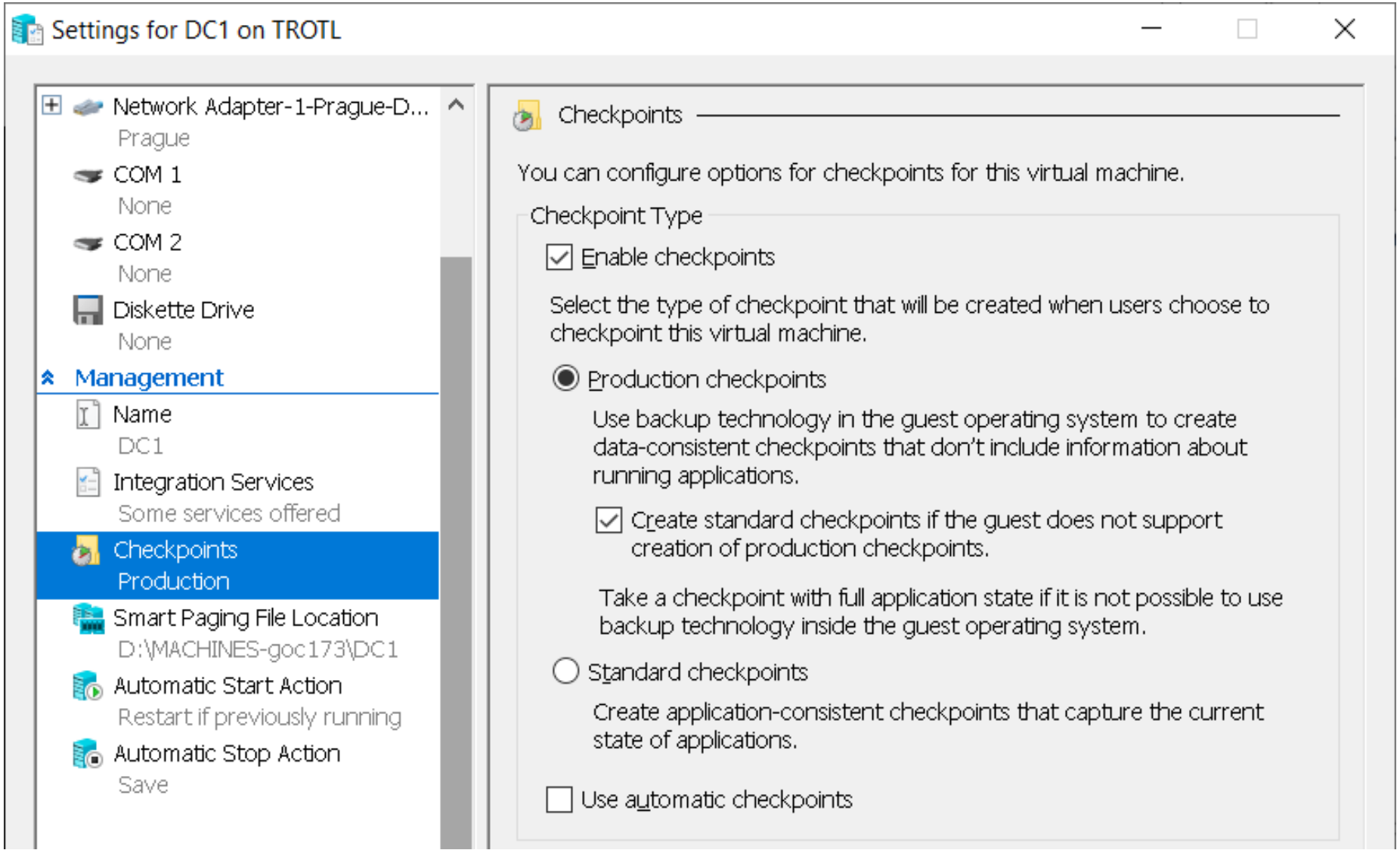
- VSS signal inside the VM
  - requires backup HVIC
  - signal only, no copy created inside





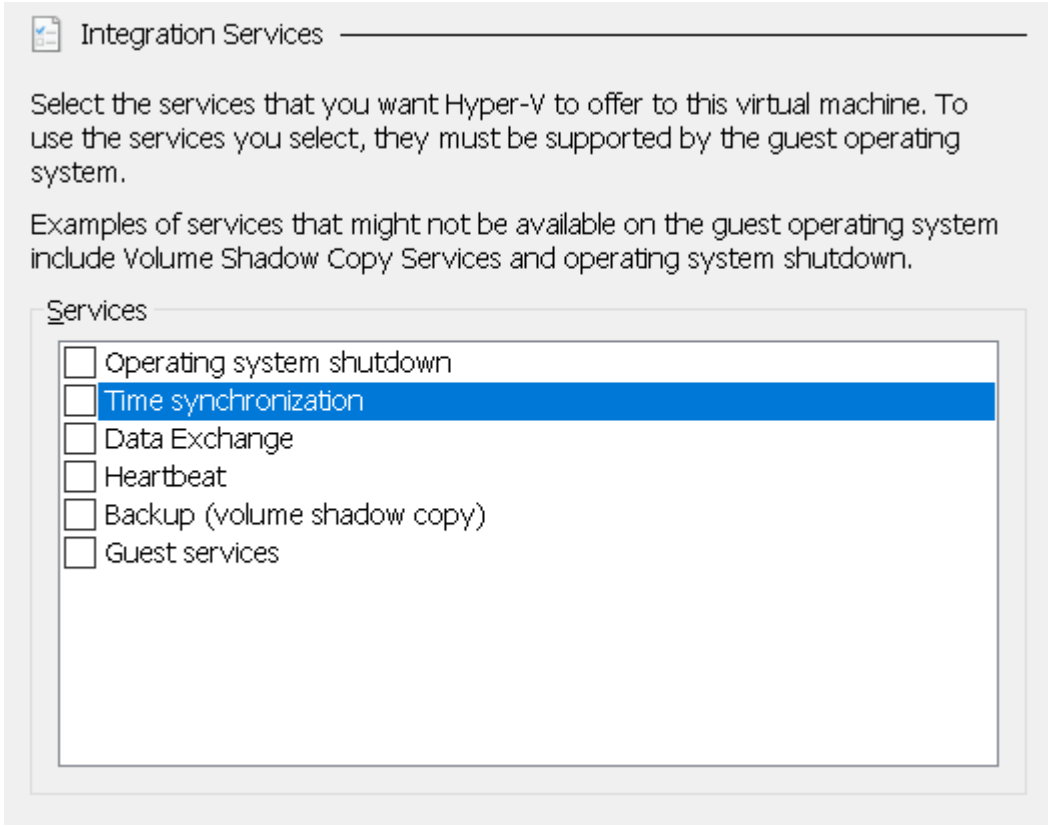
Checkpoints (snapshots)

Production vs. standard checkpoint settings



Standard checkpoints

- running with memory
- no information inside VM
- time left flowing when restored
  - without integration components (HVIC)



Standard checkpoints

Administrator: C:\Windows\system32\cmd.exe

```
12:07:48: writing bytes: block = final | bytes = 152 of 2200 | size = 2200
12:07:50: writing bytes: block =     1 | bytes = 512 of 2200 | size = 512
12:07:51: writing bytes: block =     2 | bytes = 512 of 2200 | size = 1024
12:07:52: writing bytes: block =     3 | bytes = 512 of 2200 | size = 1536
12:07:53: writing bytes: block =     4 | bytes = 512 of 2200 | size = 2048
12:07:55: writing bytes: block = final | bytes = 152 of 2200 | size = 2200
12:07:56: writing bytes: block =     1 | bytes = 512 of 2200 | size = 512
12:07:57: writing bytes: block =     2 | bytes = 512 of 2200 | size = 1024
```

Administrator: C:\Windows\system32\cmd.exe

```
12:07:55: writing bytes: block = final | bytes = 152 of 2200 | size = 2200
12:07:56: writing bytes: block =     1 | bytes = 512 of 2200 | size = 512
12:07:57: writing bytes: block =     2 | bytes = 512 of 2200 | size = 1024
12:07:58: writing bytes: block =     3 | bytes = 512 of 2200 | size = 1536
12:08:00: writing bytes: block =     4 | bytes = 512 of 2200 | size = 2048
12:08:01: writing bytes: block = final | bytes = 152 of 2200 | size = 2200
12:08:02: writing bytes: block =     1 | bytes = 512 of 2200 | size = 512
```

Checkpoints

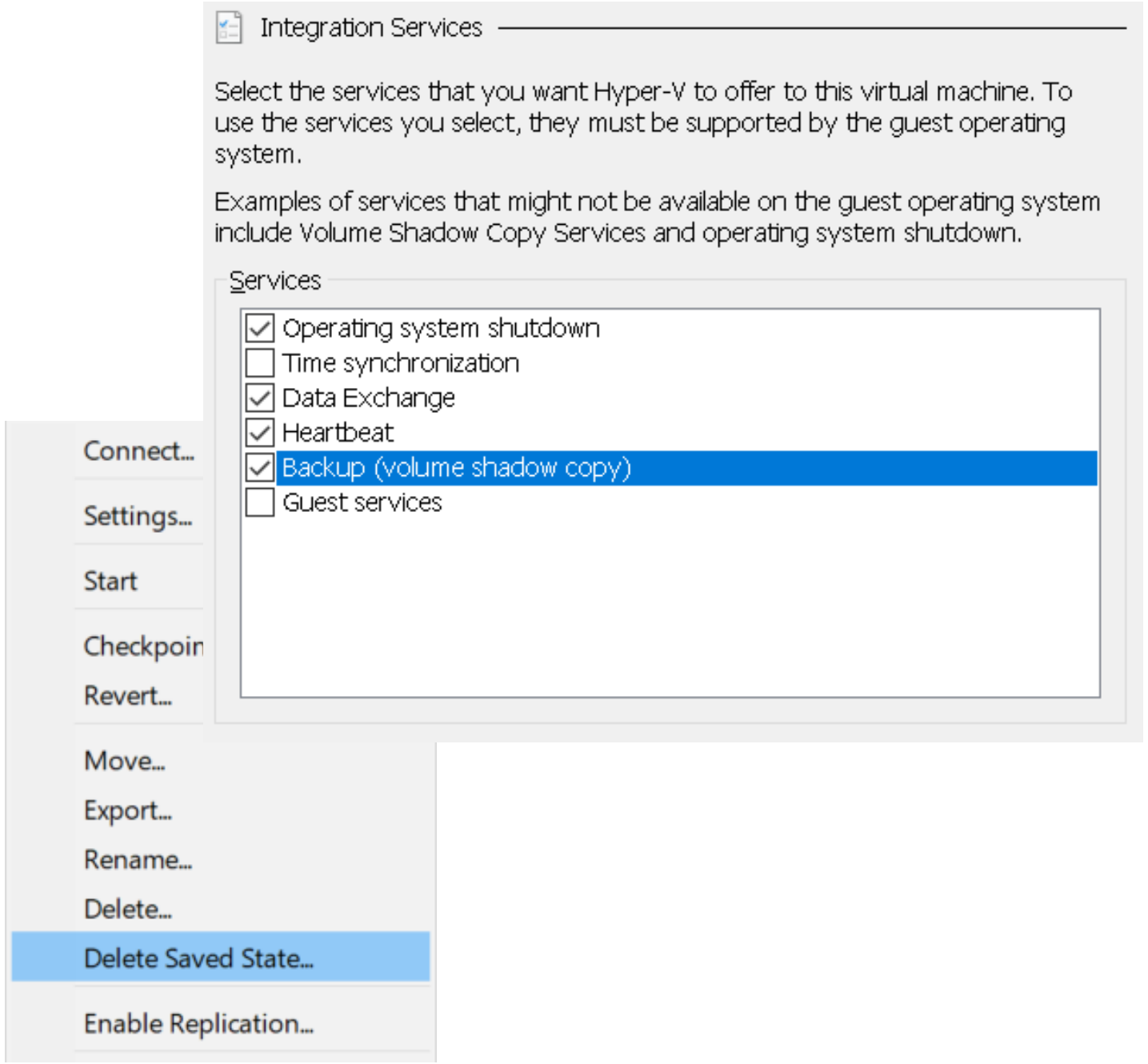
- standard checkpoint - (08.05.2022 - 12:07:58)
  - Now

standard checkpoint - (08.05.2022 - 12:07:58)

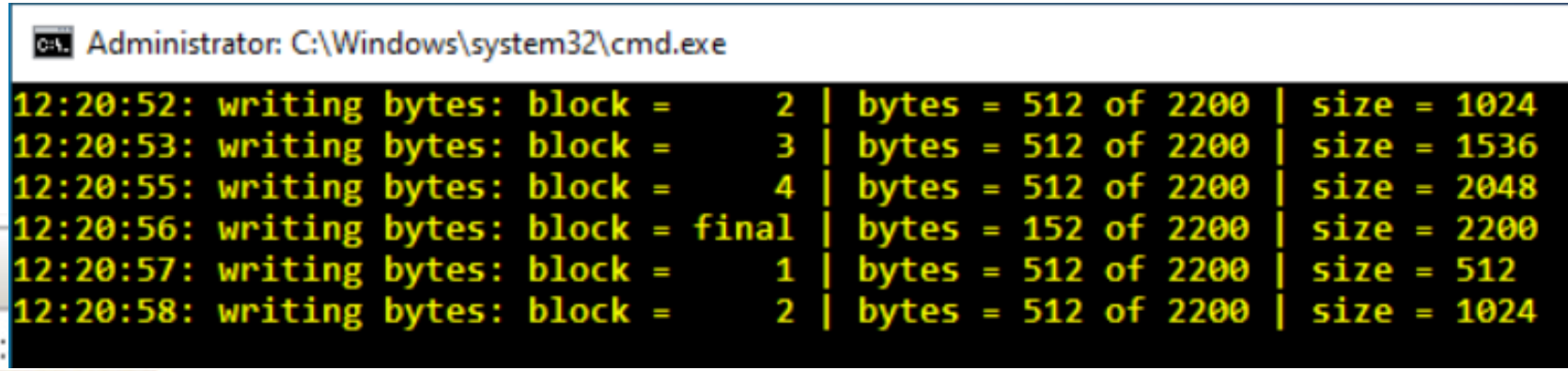
Created:	08.05.2022 12:08:00
Configuration Version:	9.0
Generation:	2
Notes:	None

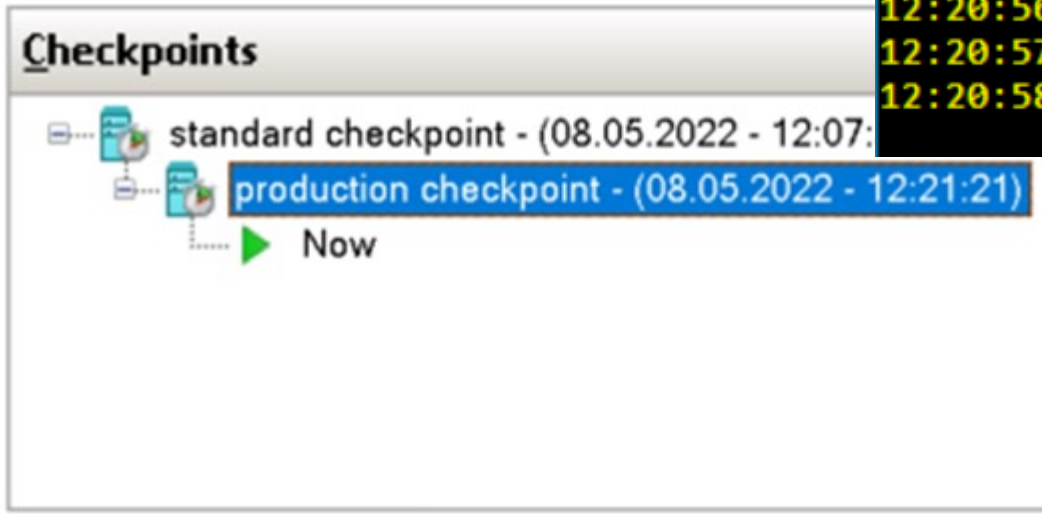
Production checkpoints

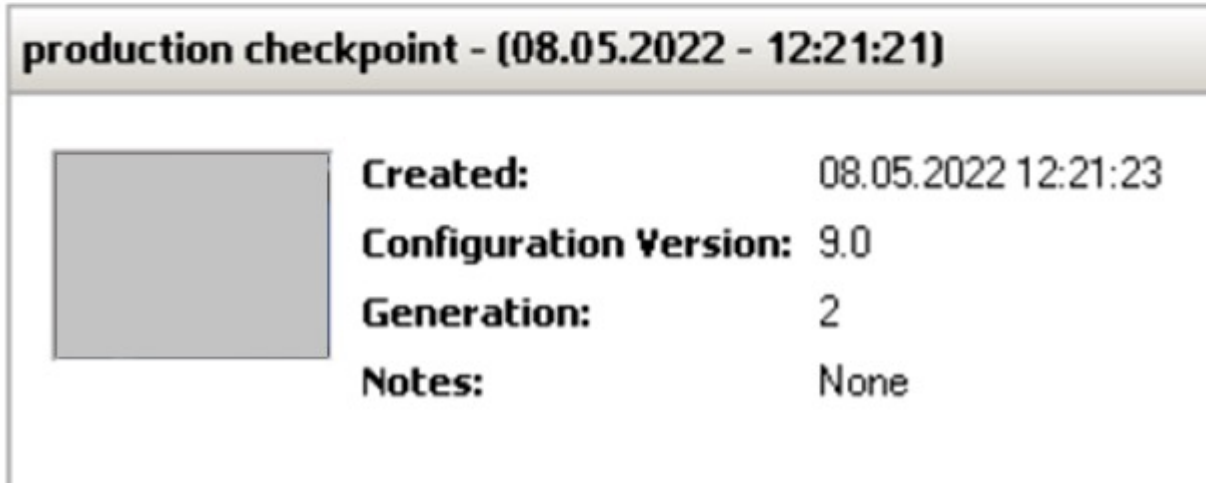
- disk only, no memory
- VSS signal inside VM
  - backup HVIC required
  - no copy created inside
- time adjusted when restored
  - even without time HVIC



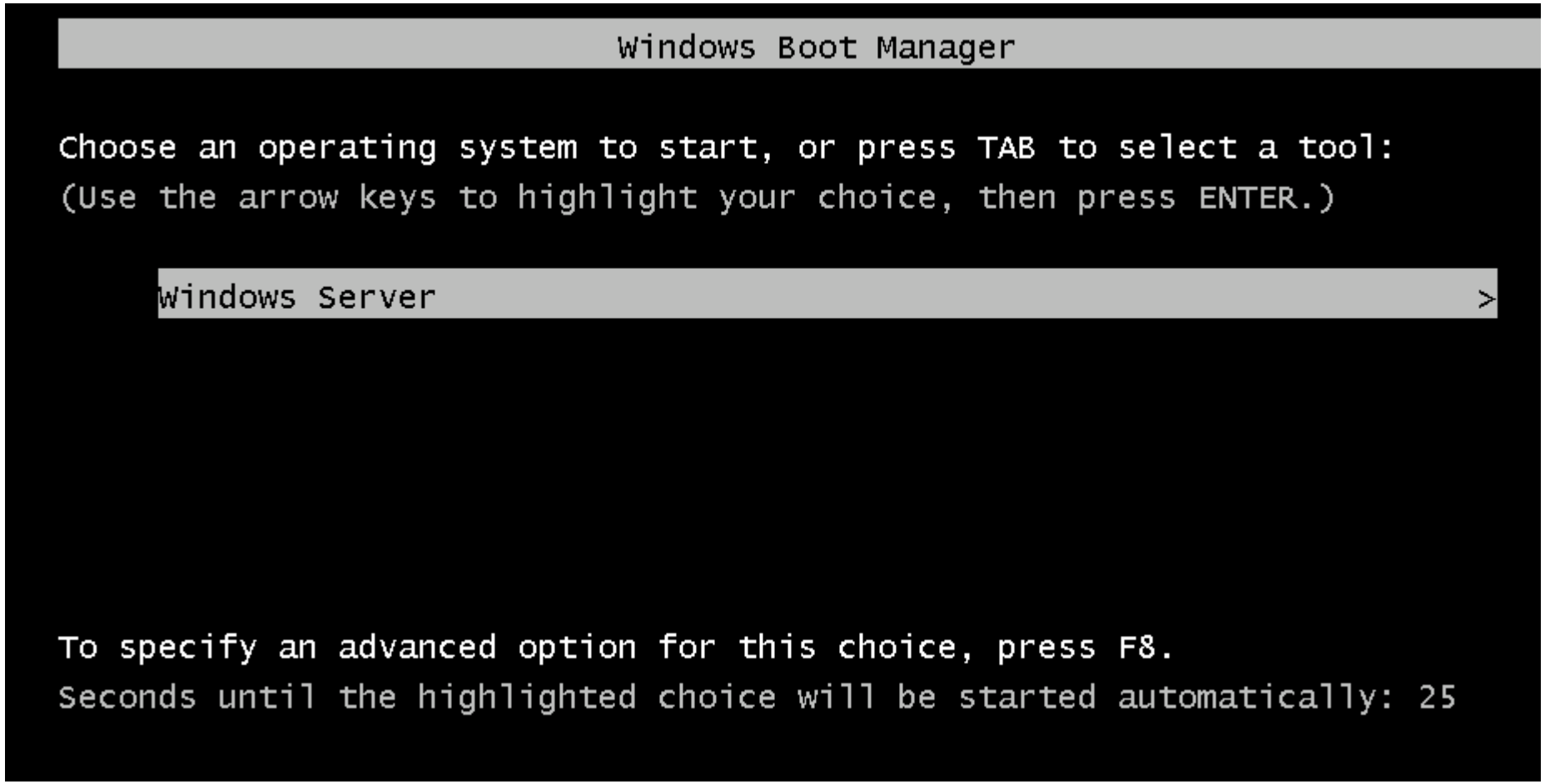
Production checkpoints



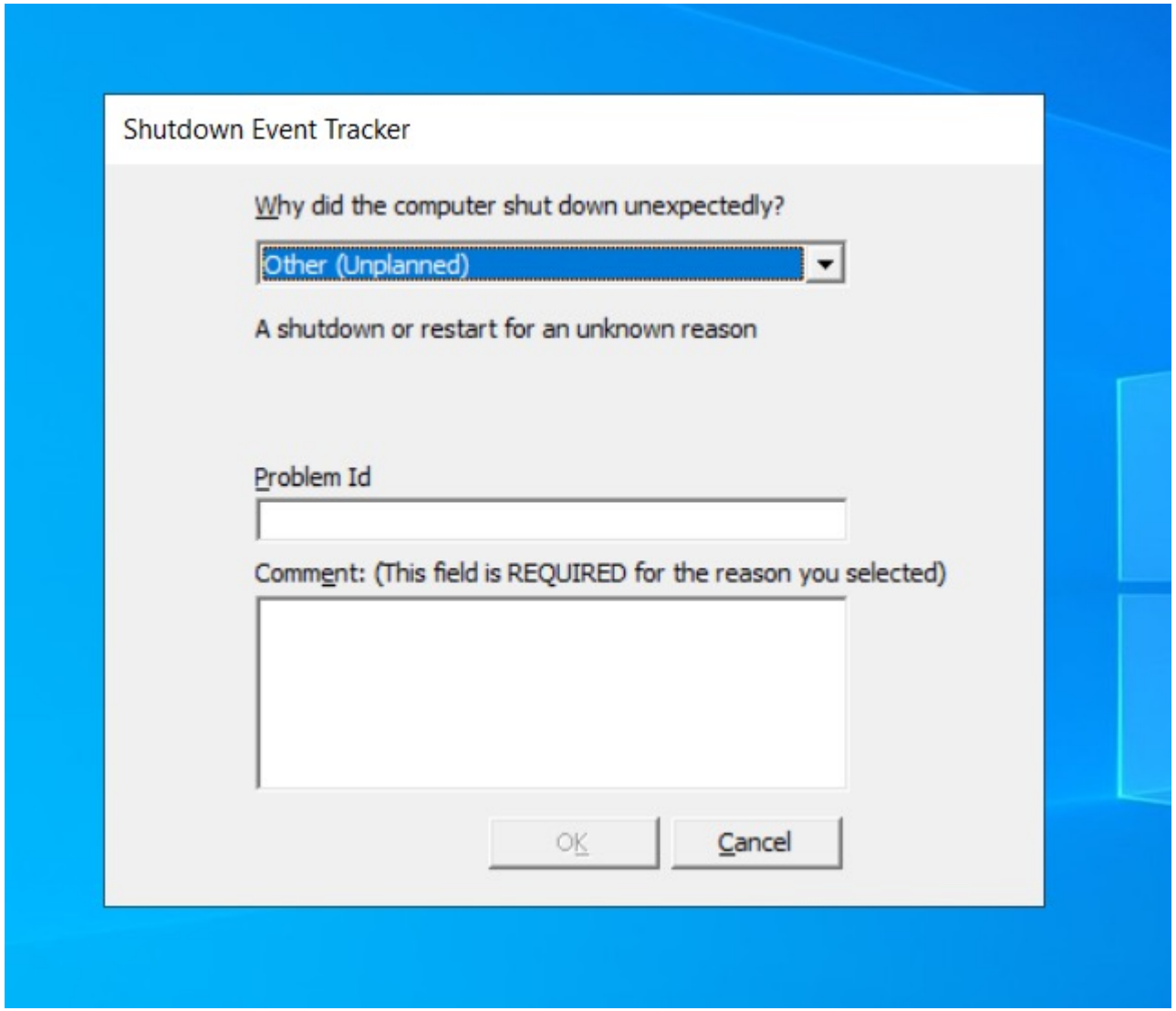




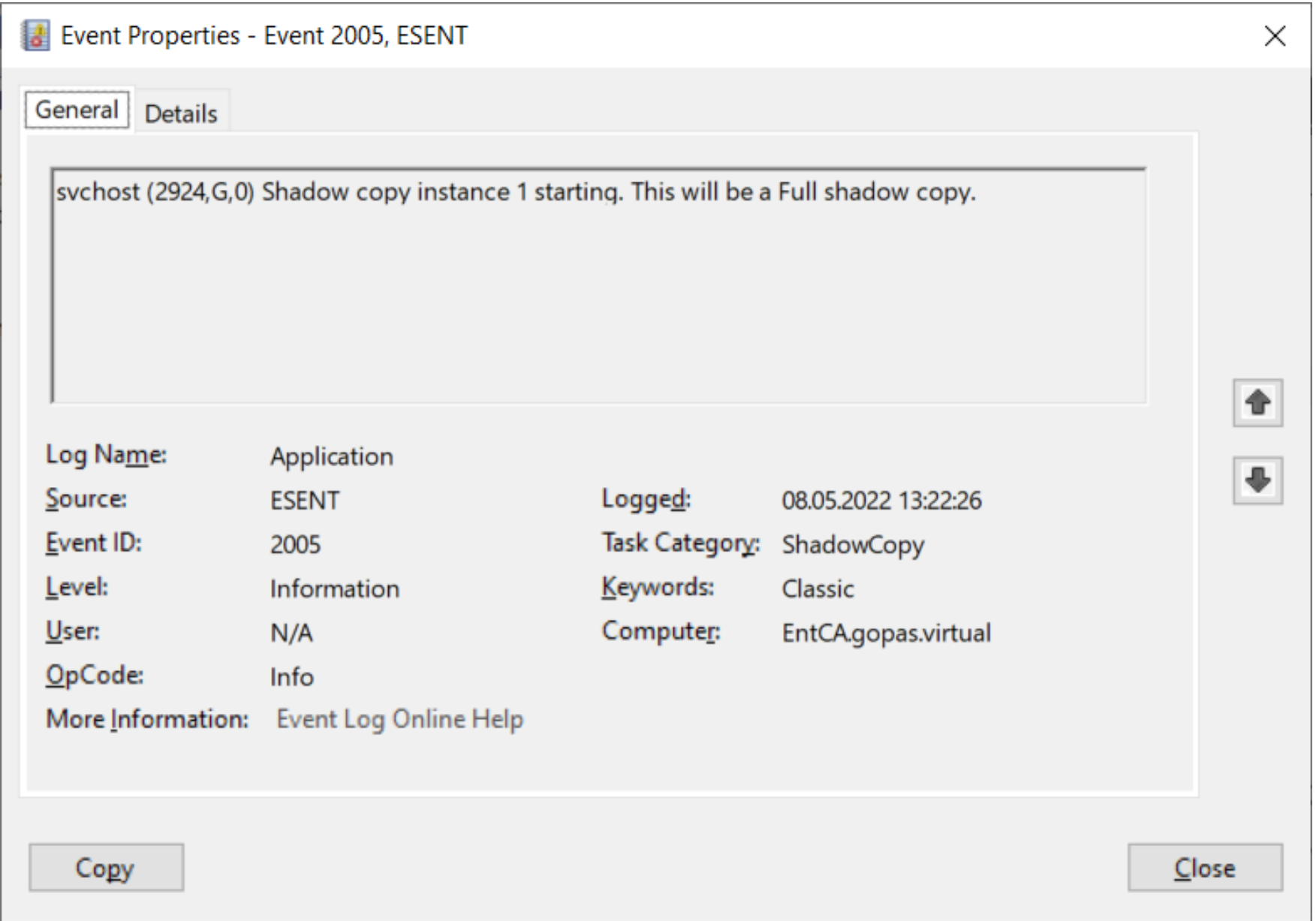
After restoring a production checkpoint



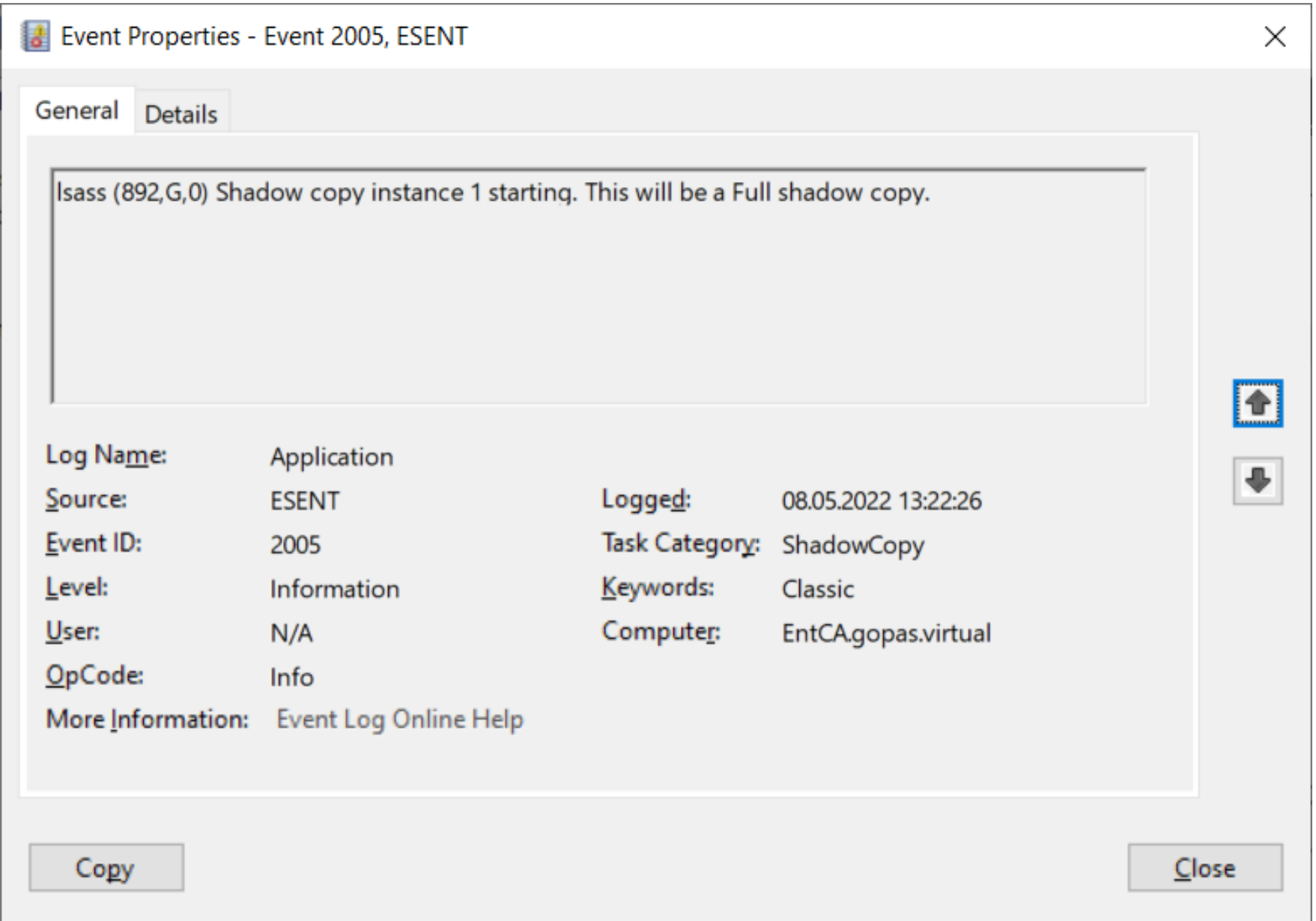
After restoring a production checkpoint



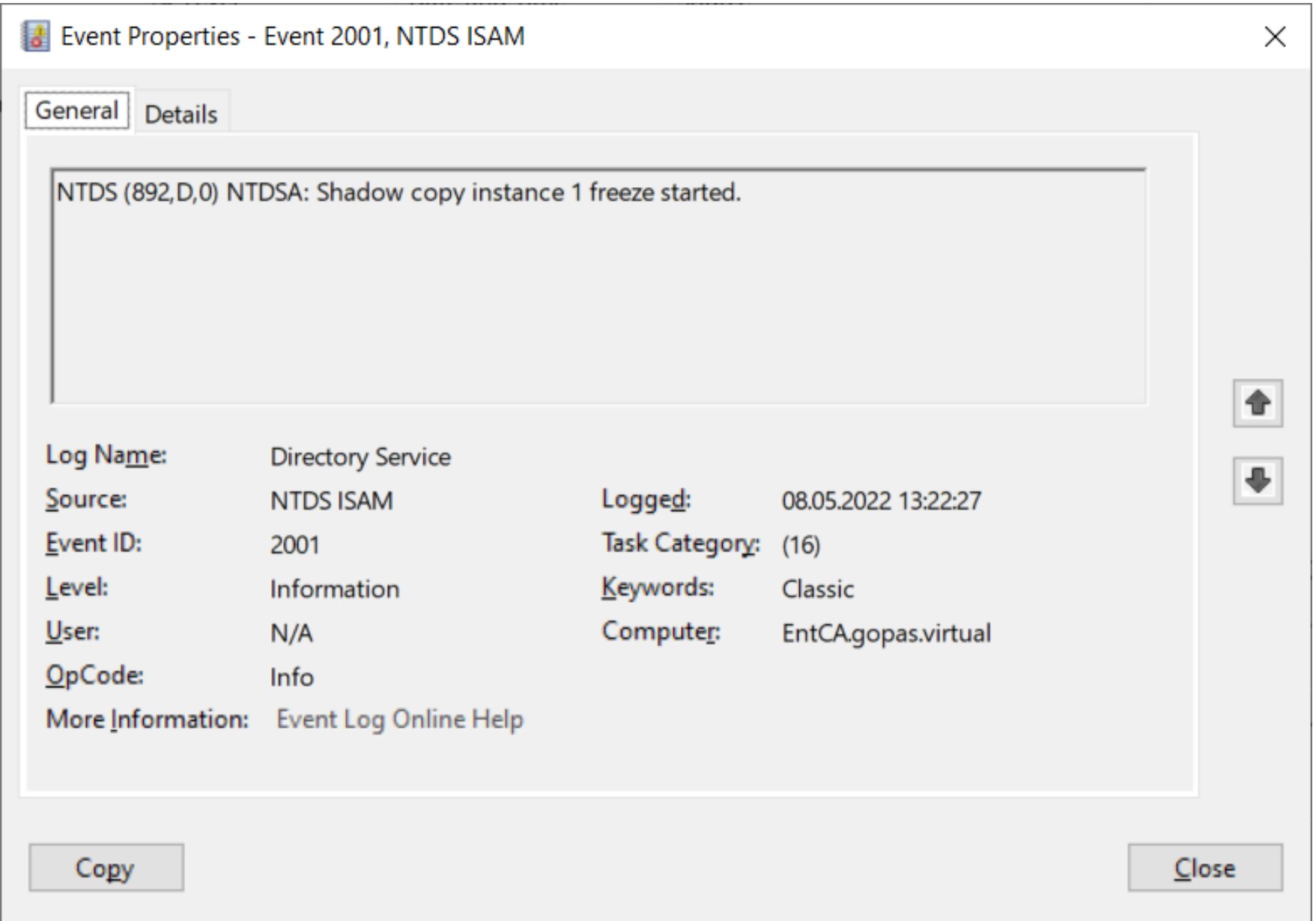
VSS event logs - DHCP server



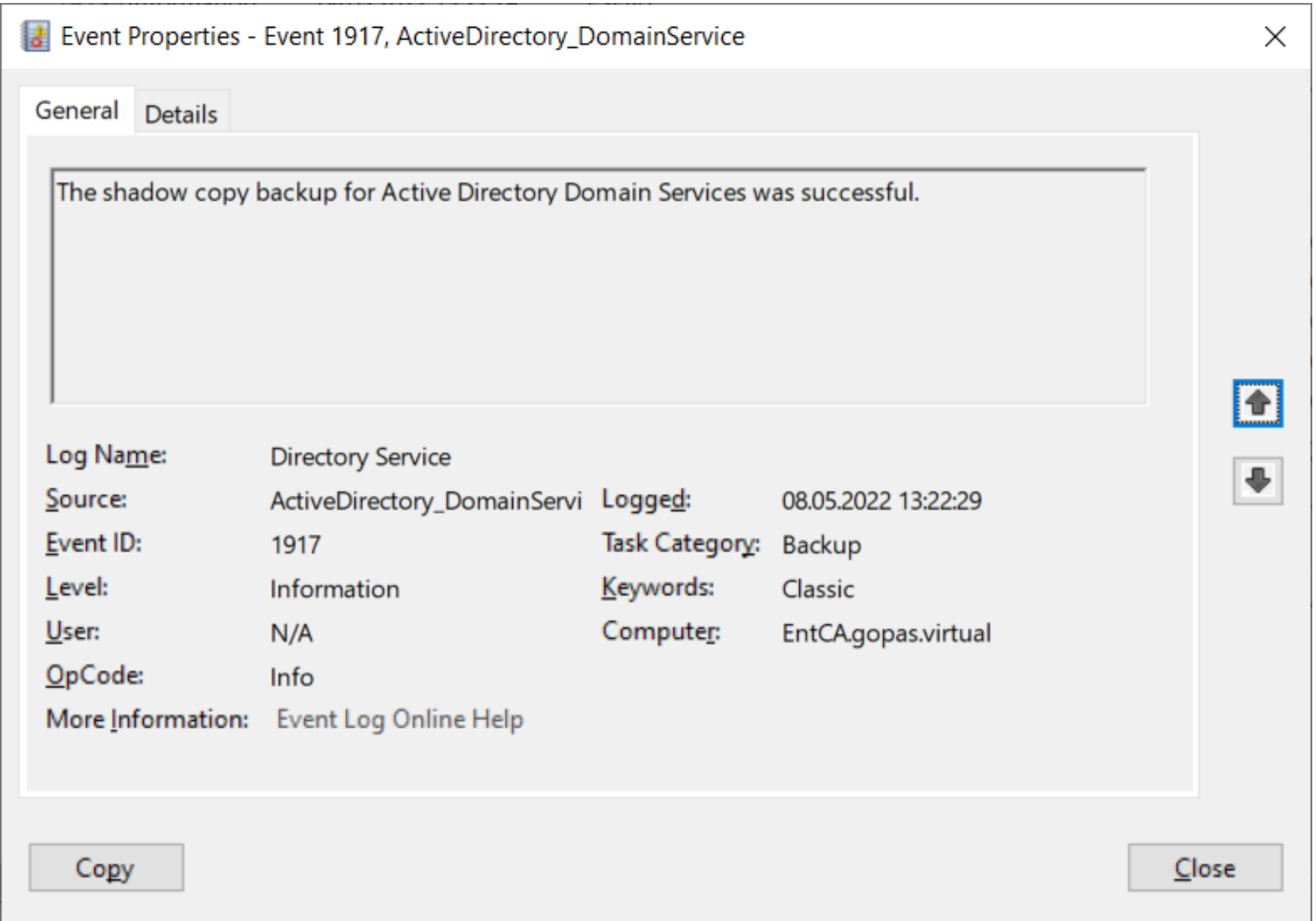
VSS event logs - AD



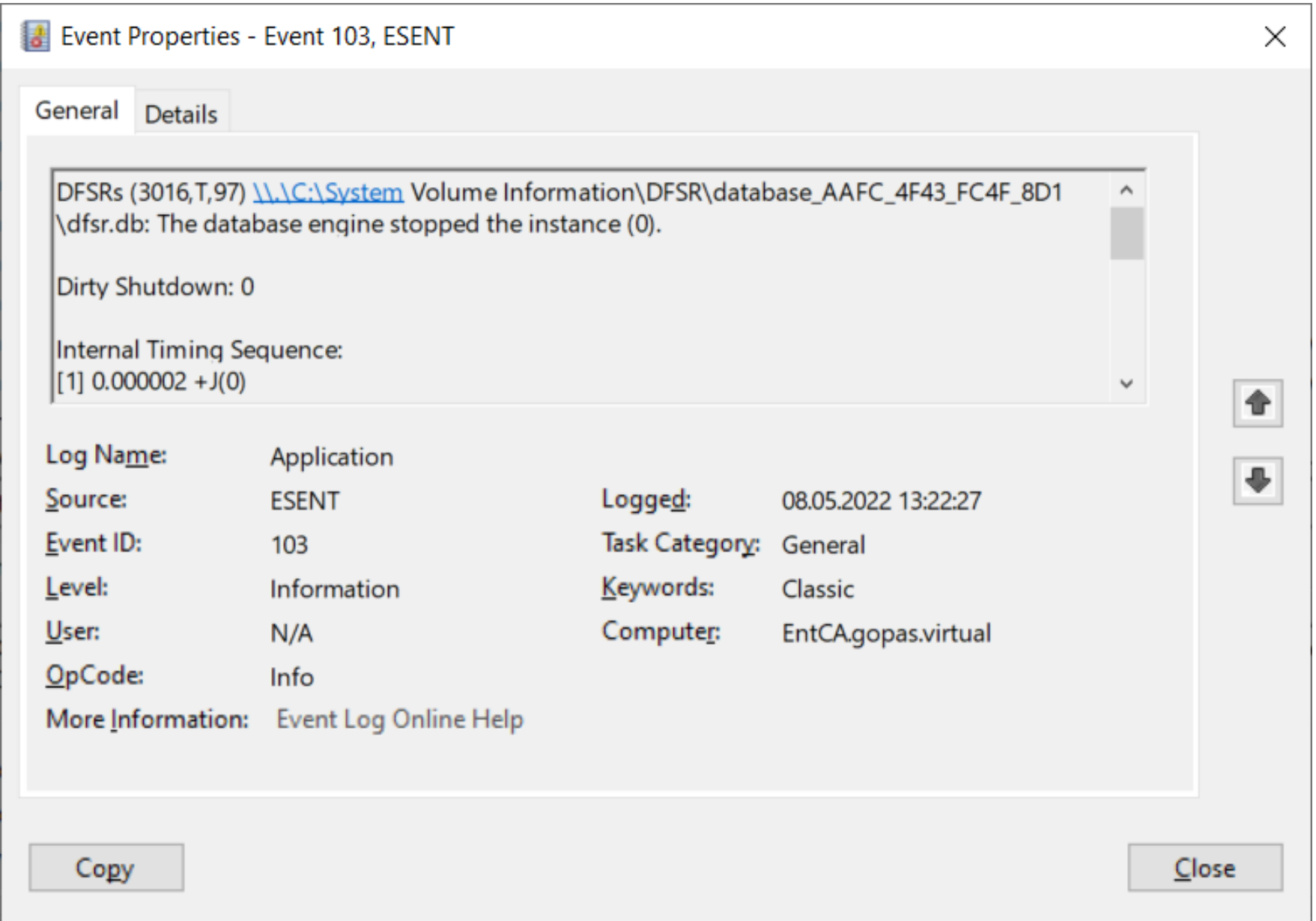
VSS event logs - AD



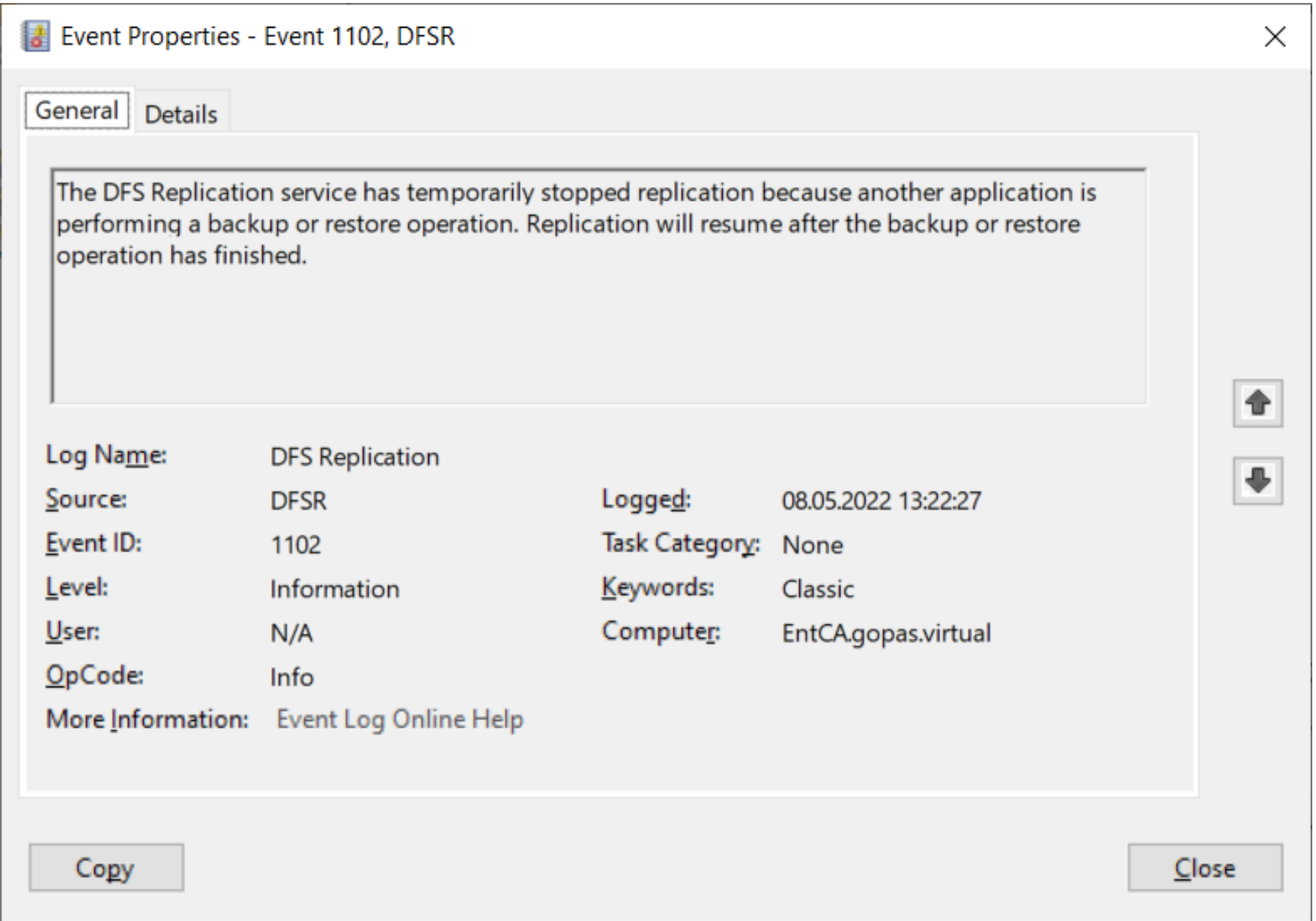
VSS event logs - AD



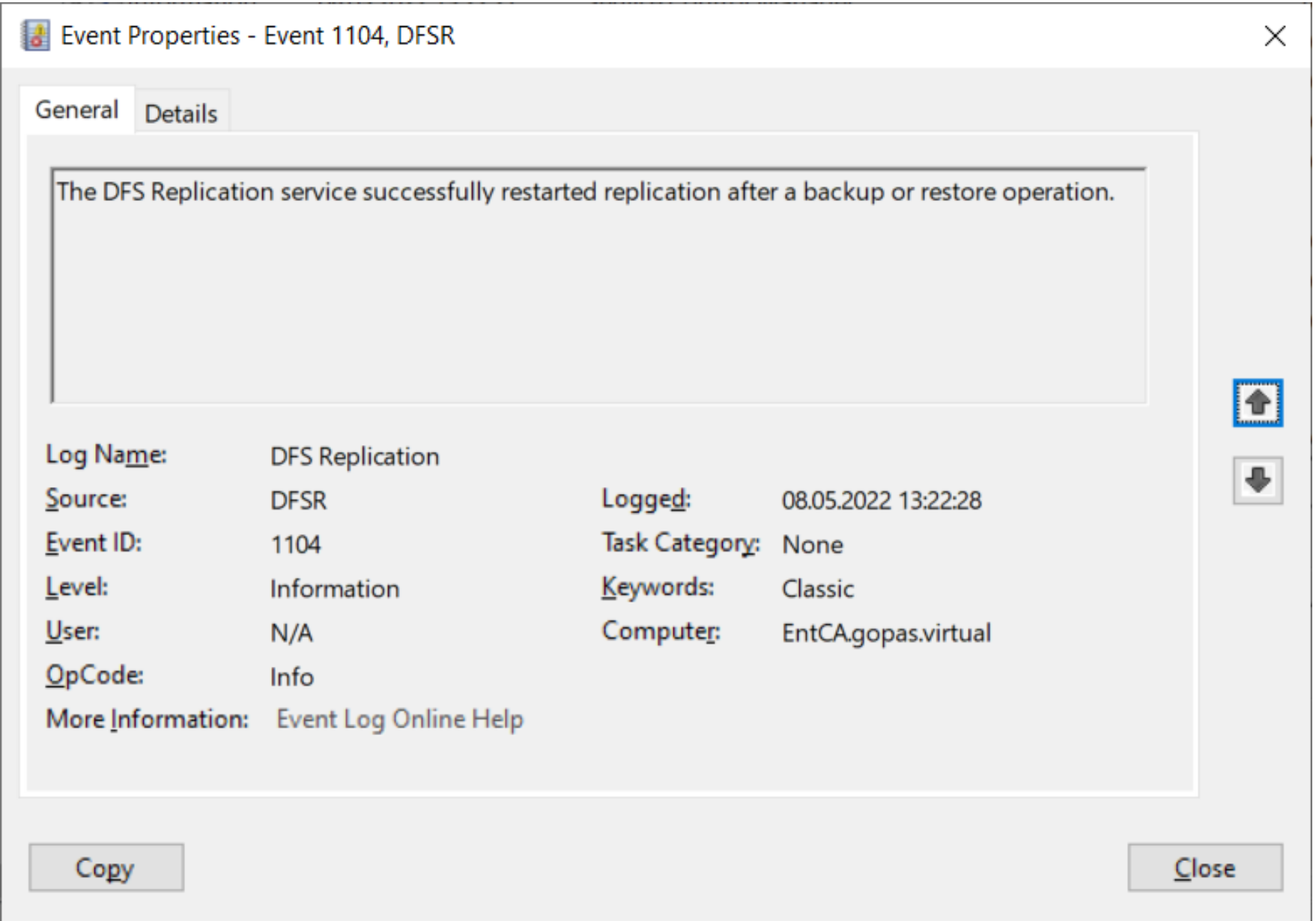
VSS event logs - DFSR



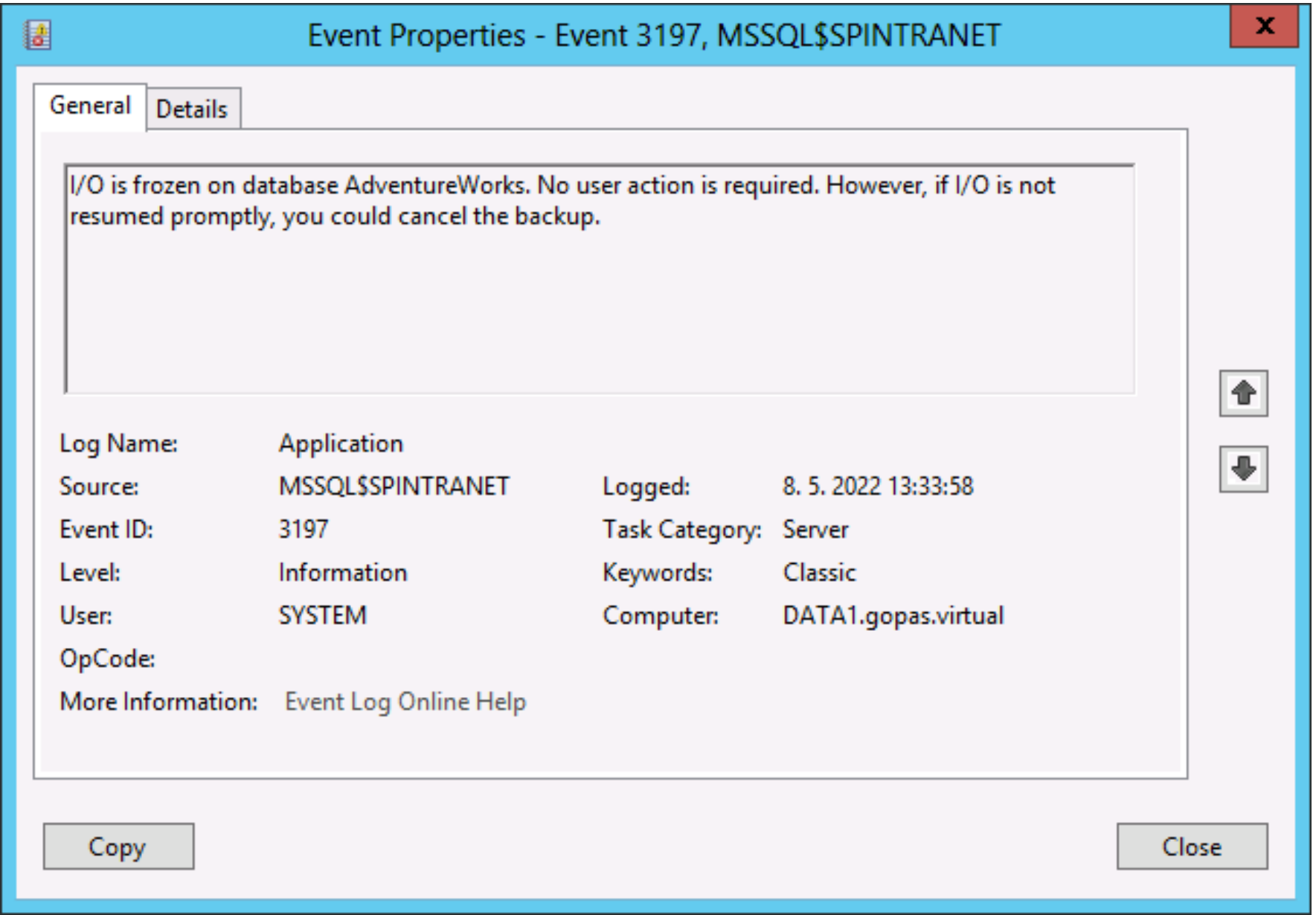
VSS event logs - DFSR



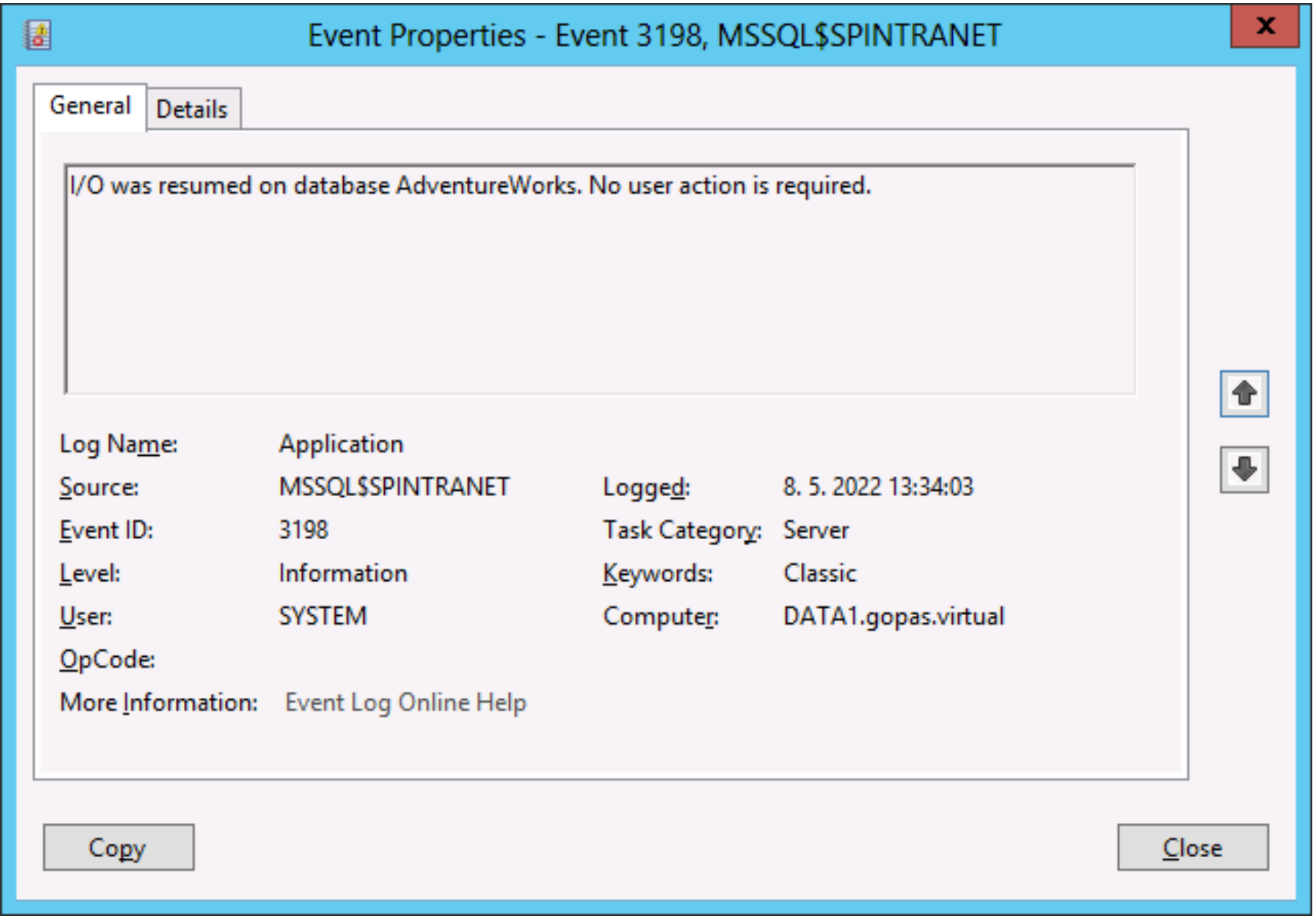
VSS event logs - DFSR



VSS event logs - SQL server



VSS event logs - SQL server



Hyper-V replica

Hyper-V replication

- 30 seconds, 5 minutes, 15 minutes
- VSS signal every several hours up to 24 latest

- planned failover
  - stop primary - start secondary - revert
- unplanned failover

Restore

Restoring images of operating systems

- image
- Windows Server Backup .VHDX
- VM checkpoint (snapshot)
- replicated VM unplanned failover

Recovery process

- restore image/checkpoint/snapshot

- recover
  - recovery point (objective - RPO)?
  - inconsistent application data?
  - inconsistent distributed application/system states

Sample restore problems

- member of a domain
  - 30 days password change

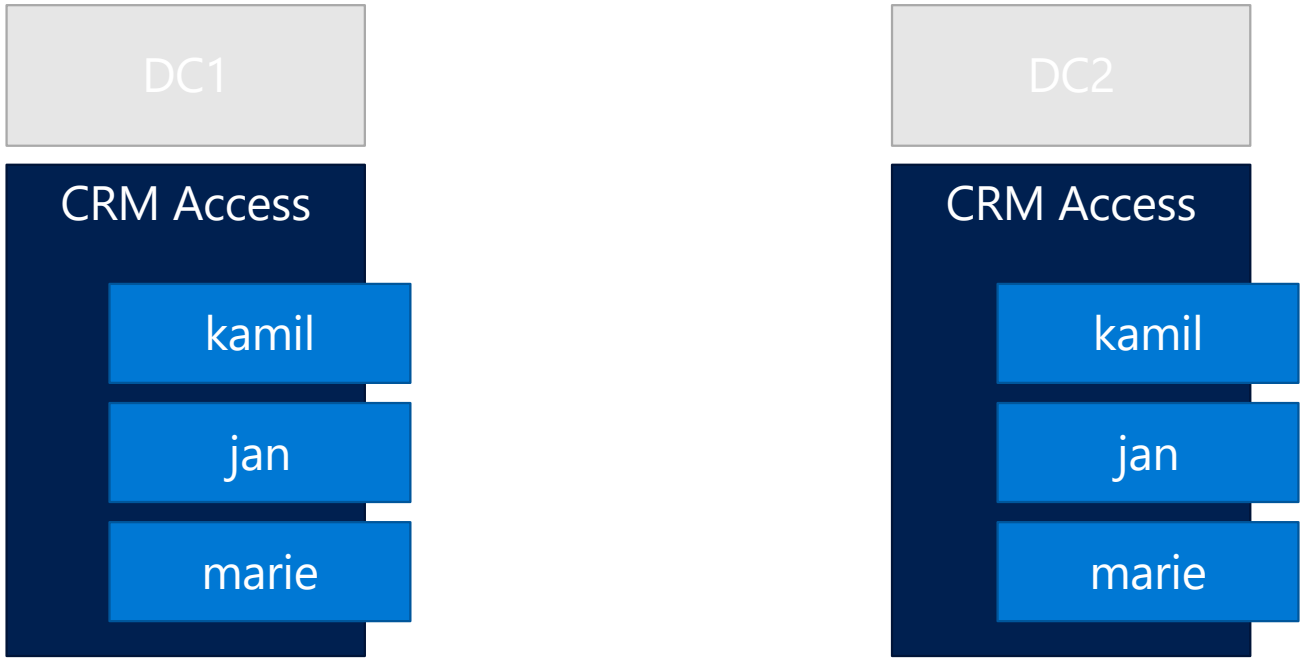
    ```
    netdom resetpwd /server:dc1 /userD:gps\domain-admin /passwordD:Pa$$w0rd
    ```

- DHCP server
  - duplicate IP address detection or BAD_ADDRESS

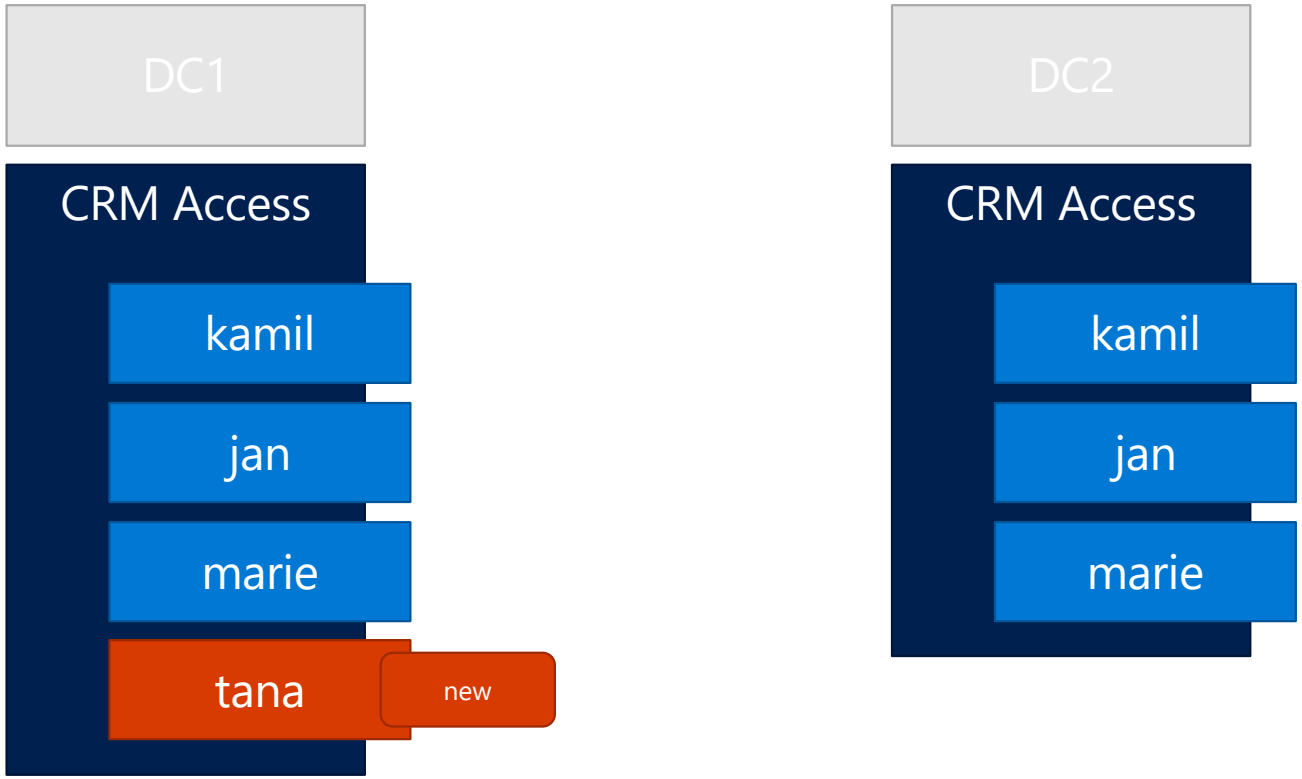
Sample restore problems

- DCs
  - USN rollback

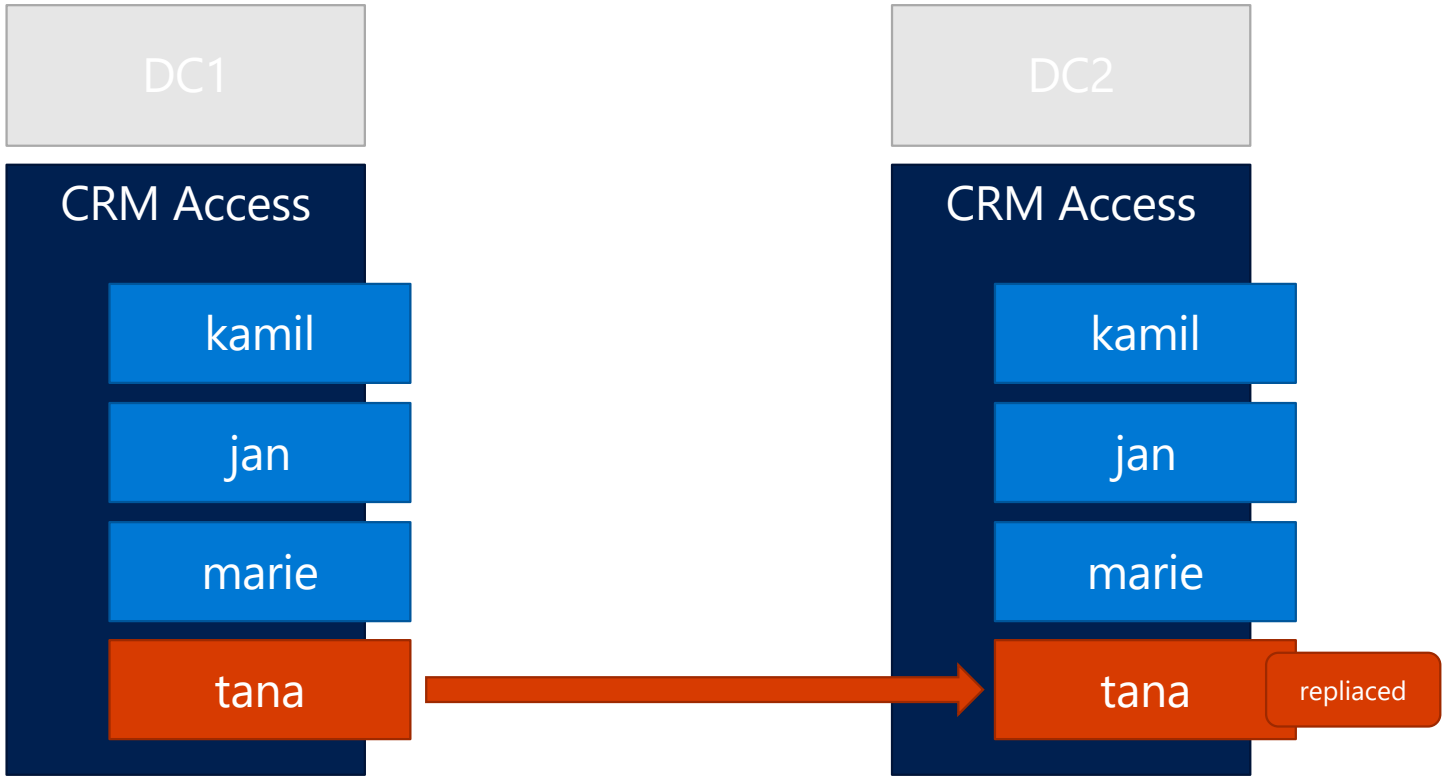
USN rollback



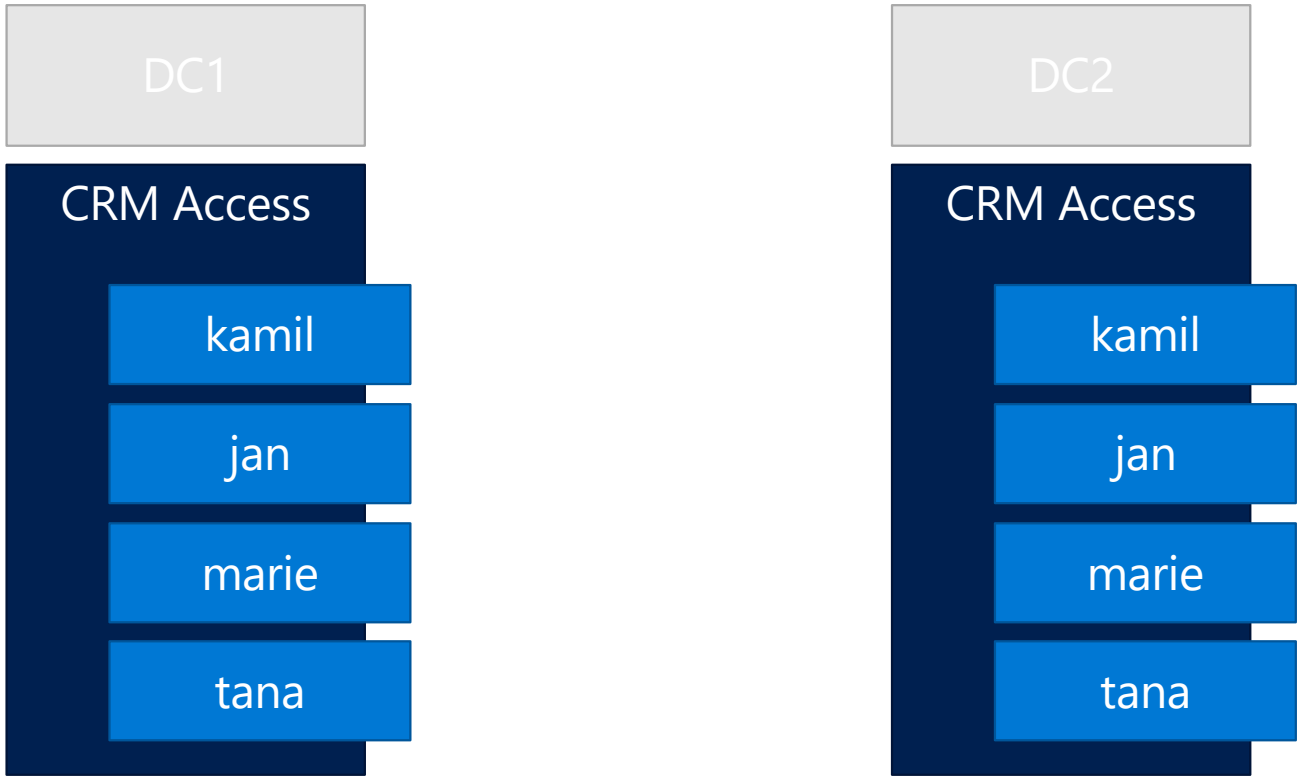
USN rollback



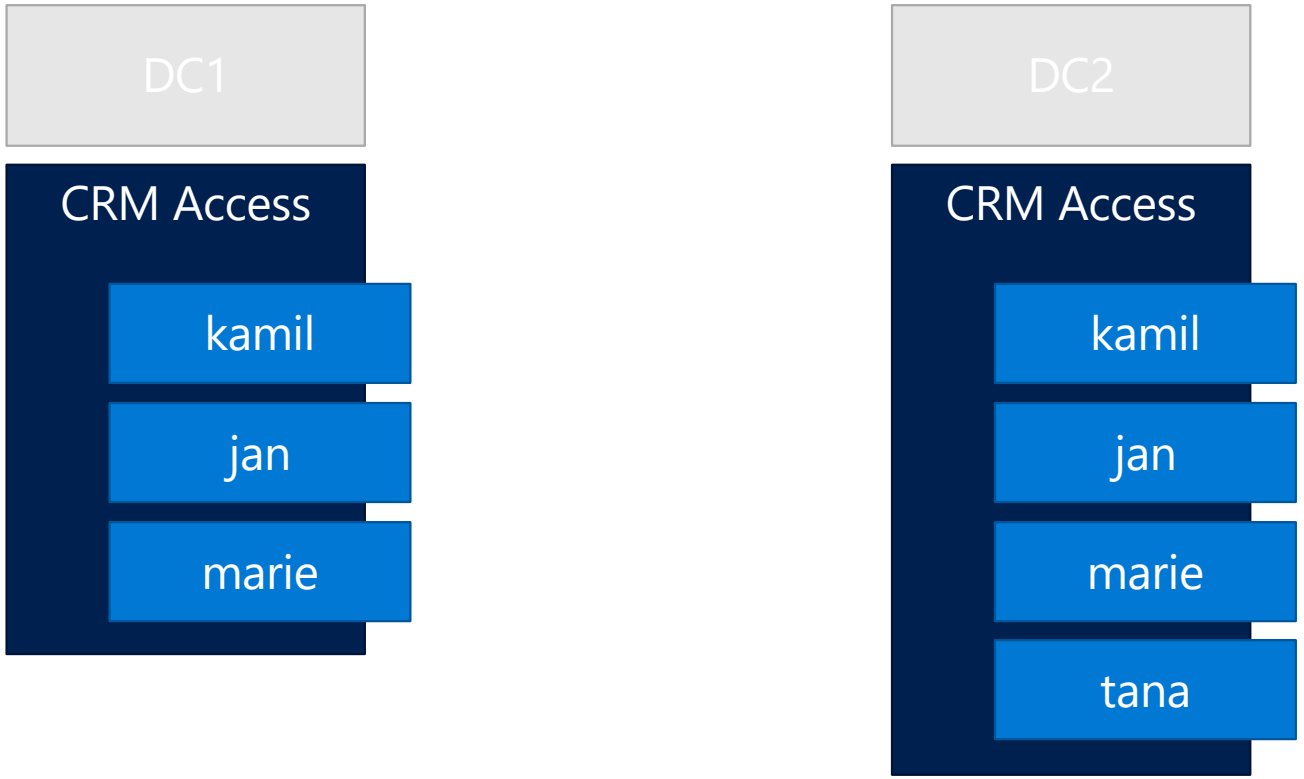
USN rollback



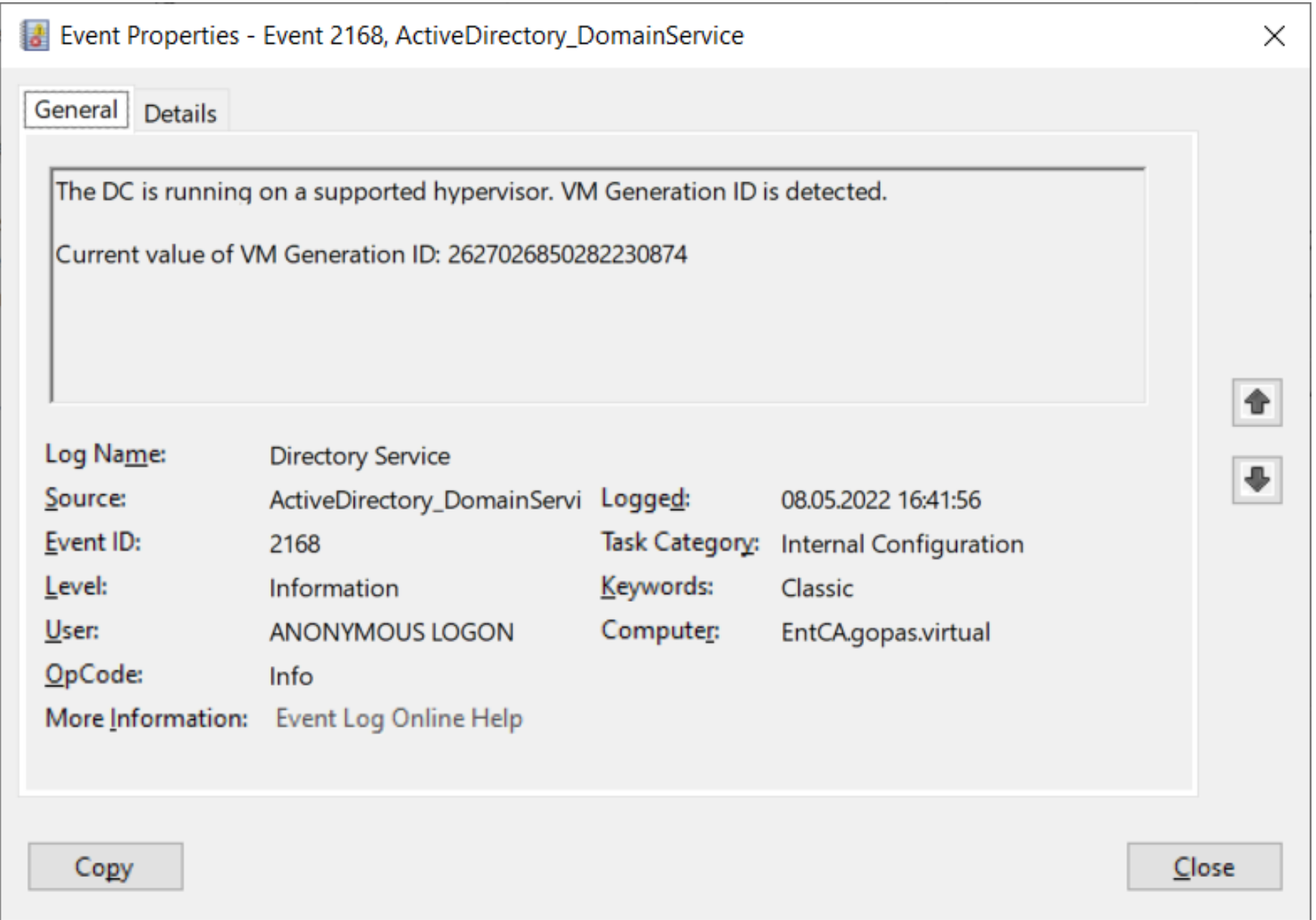
USN rollback



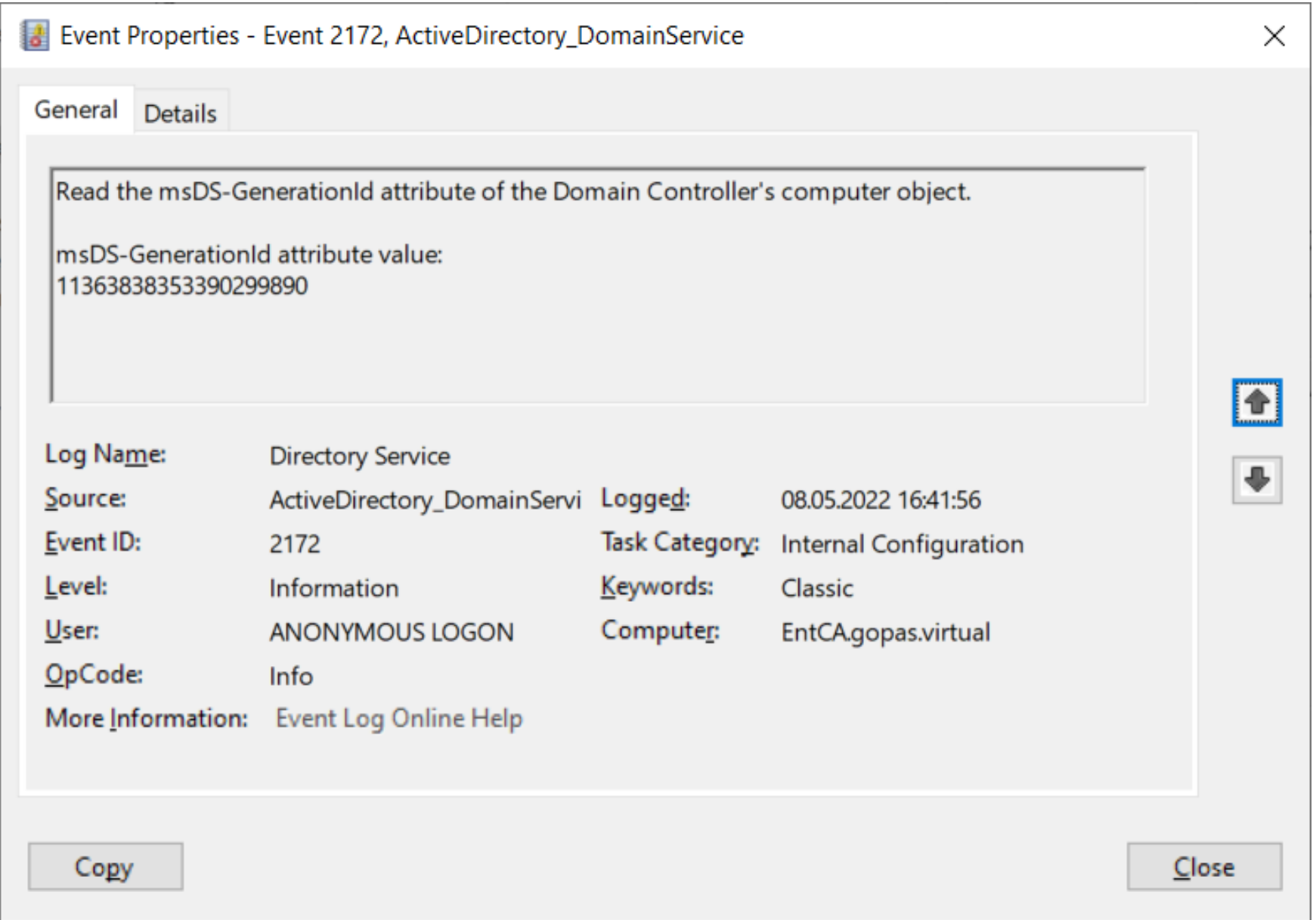
USN rollback



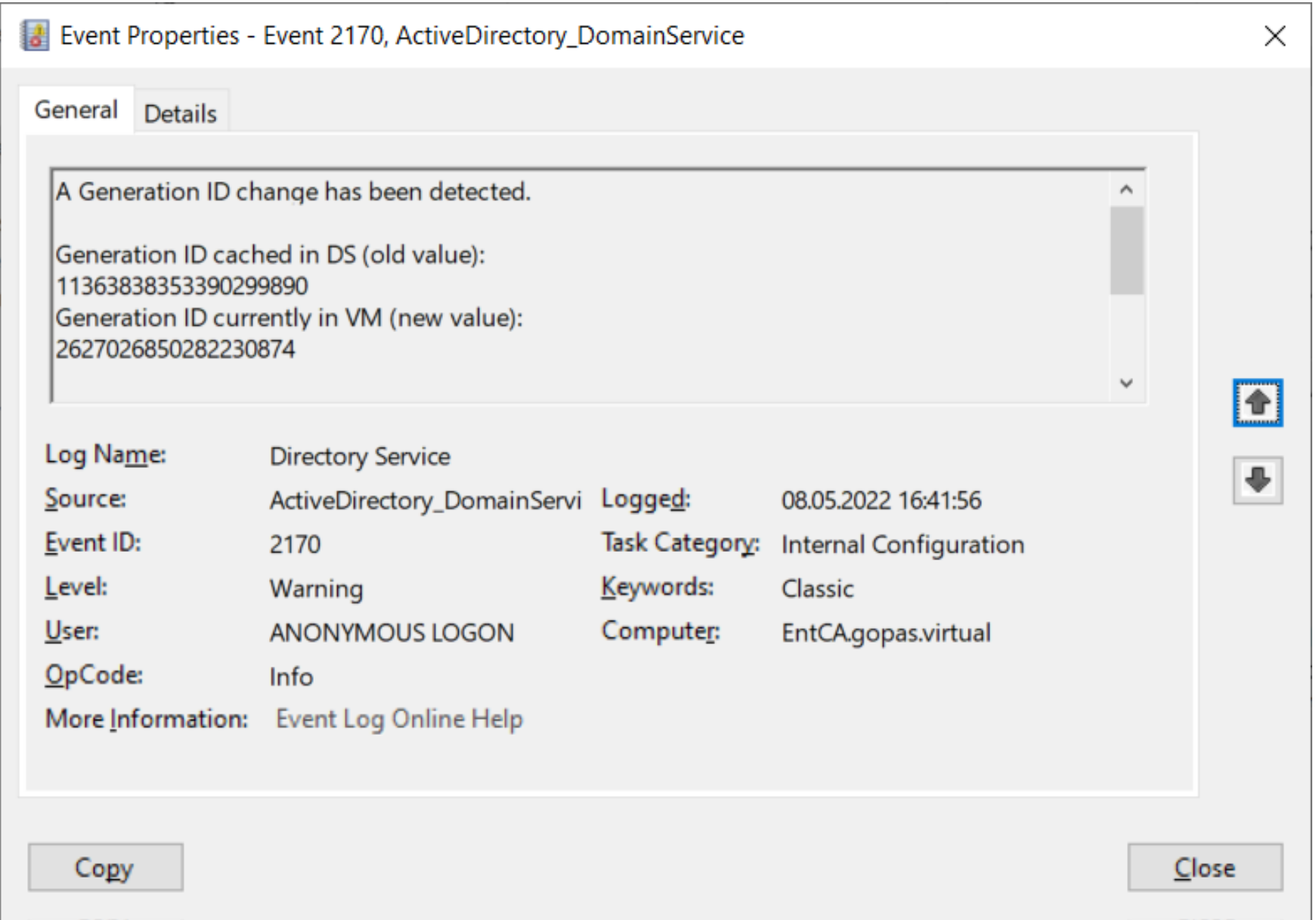
Generation ID



Generation ID



Generation ID



Generation ID

Administrator: C:\Windows\system32\cmd.exe

```
C:\>repadmin /showutdvec entca cn=configuration,dc=gopas,dc=virtual
Caching GUIDs.
..
Prague\ENTCA (retired)              @ USN     24851 @ Time 2022-05-08 16:37:48
Prague\DC1                          @ USN     62380 @ Time 2022-05-08 16:42:37
Prague\ENTCA                        @ USN     28891 @ Time 2022-05-08 16:47:57
Prague\ENTCA (retired)              @ USN     24885 @ Time 2022-05-08 16:41:55
```

Event Properties - Event 1109, ActiveDirectory_D

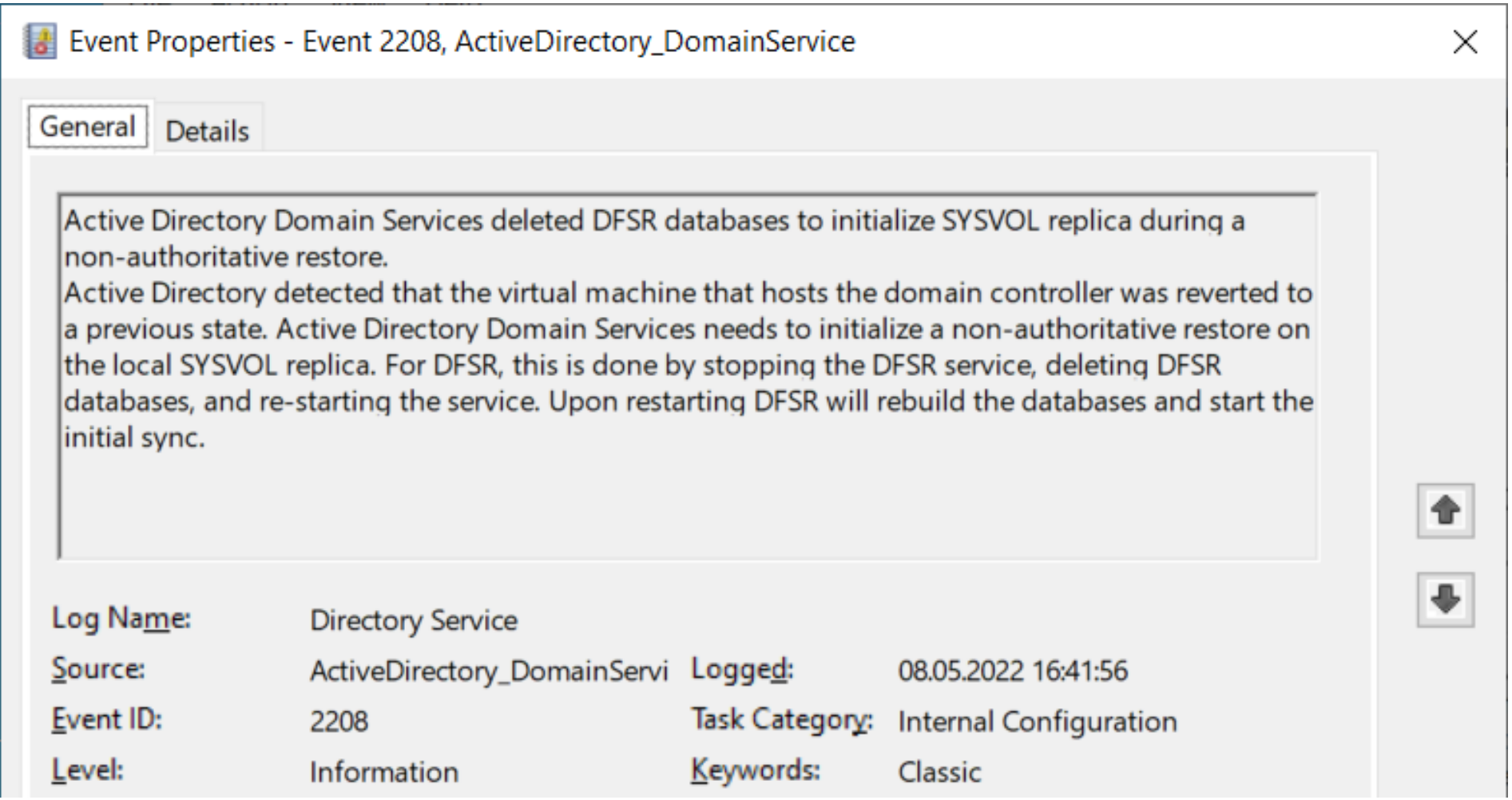
General | Details

The invocationID attribute for this directory server has been changed. The highest update sequence number at the time the backup was created is as follows:

InvocationID attribute (old value):
ebe745fc-ad72-4dad-914b-3e38f0deb6e7
InvocationID attribute (new value):
eaa2b6cd-b95e-4e7e-93b8-bbad9e350800
Update sequence number:
24885

Log Name:	Directory Service		
Source:	ActiveDirectory_DomainServi	Logged:	08.05.2022 16:41:56
Event ID:	1109	Task Category:	Replication

Generation ID



DCs even with Generation ID

- 30 days password change :-)

```
klist purge -li 3e4
klist purge -li 3e5
klist purge -li 3e7
netdom resetpwd /server:dc3 /userD:gps\domain-admin /passwordD:Pa$$w0rd
net stop kdc
```

- 30 days trust password changes

```
netdom trust gopas.virtual /domain:de.gopas.virtual /reset /userD:gps\domain-admin
/passwordD:Pa$$w0rd
```

- tombstone lifetime 180 days
- RID FSMO +500 only audit
  - audit + rIDAvailablePool + invalidateRIDPool

DCs even with Generation ID

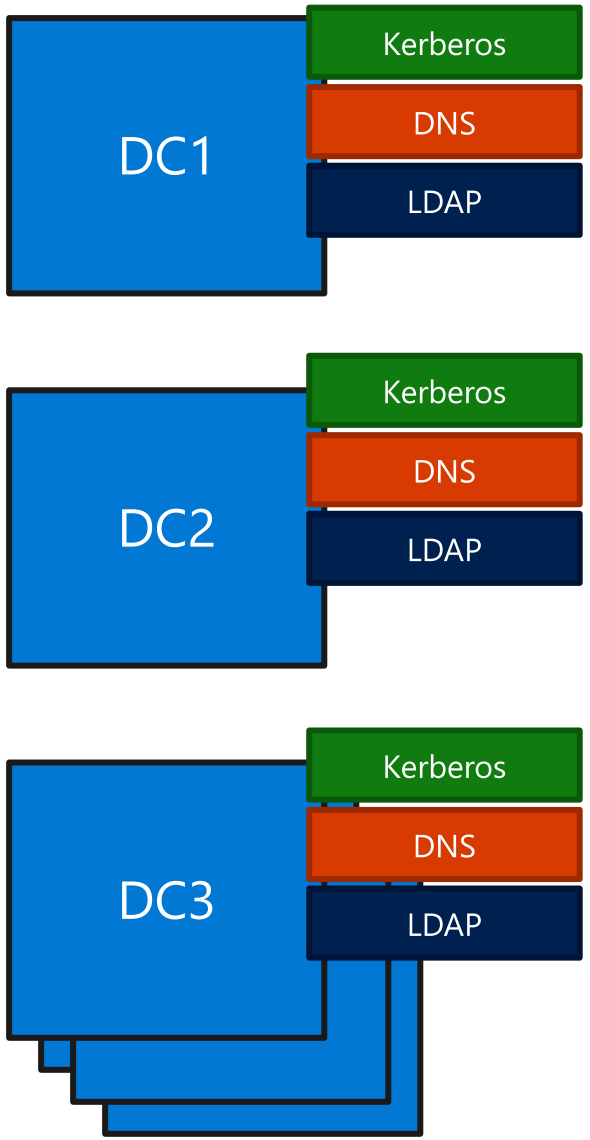
- DFSR tombstone lifetime 60 days

```
gwmi DfsrMachineConfig -Namespace root\MicrosoftDFS | select MaxOfflineTimeInDays
```

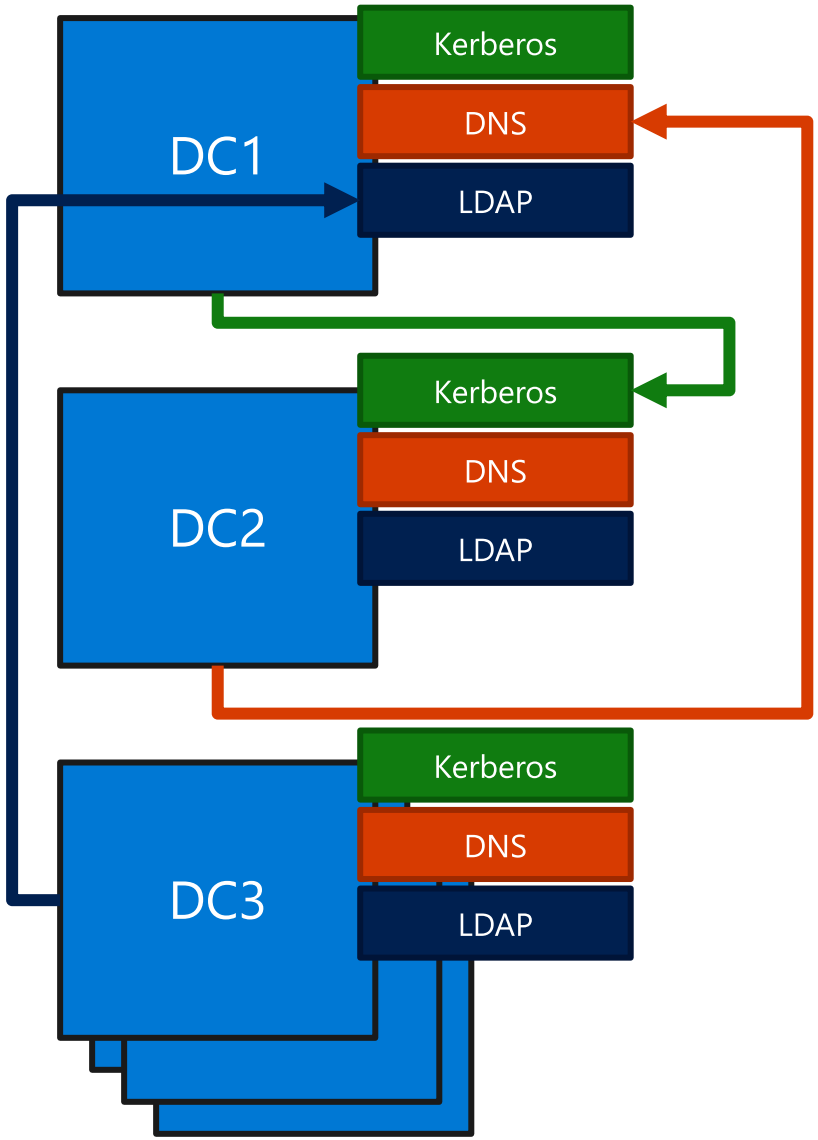
- DFSR non-authoritative restore on forest recovery (all DCs)

```
CN=DC1
  CN=DFSR-LocalSettings
    CN=Domain System Volume
      CN=SYSVOL Subscription
        msDFSR-Enabled = false # Note: this attribute does NOT exist anywhere else
        msDFSR-Options = 1 # Note: authoritative replica
        msDFSR-Options = 0 # Note: non-authoritative replica
```

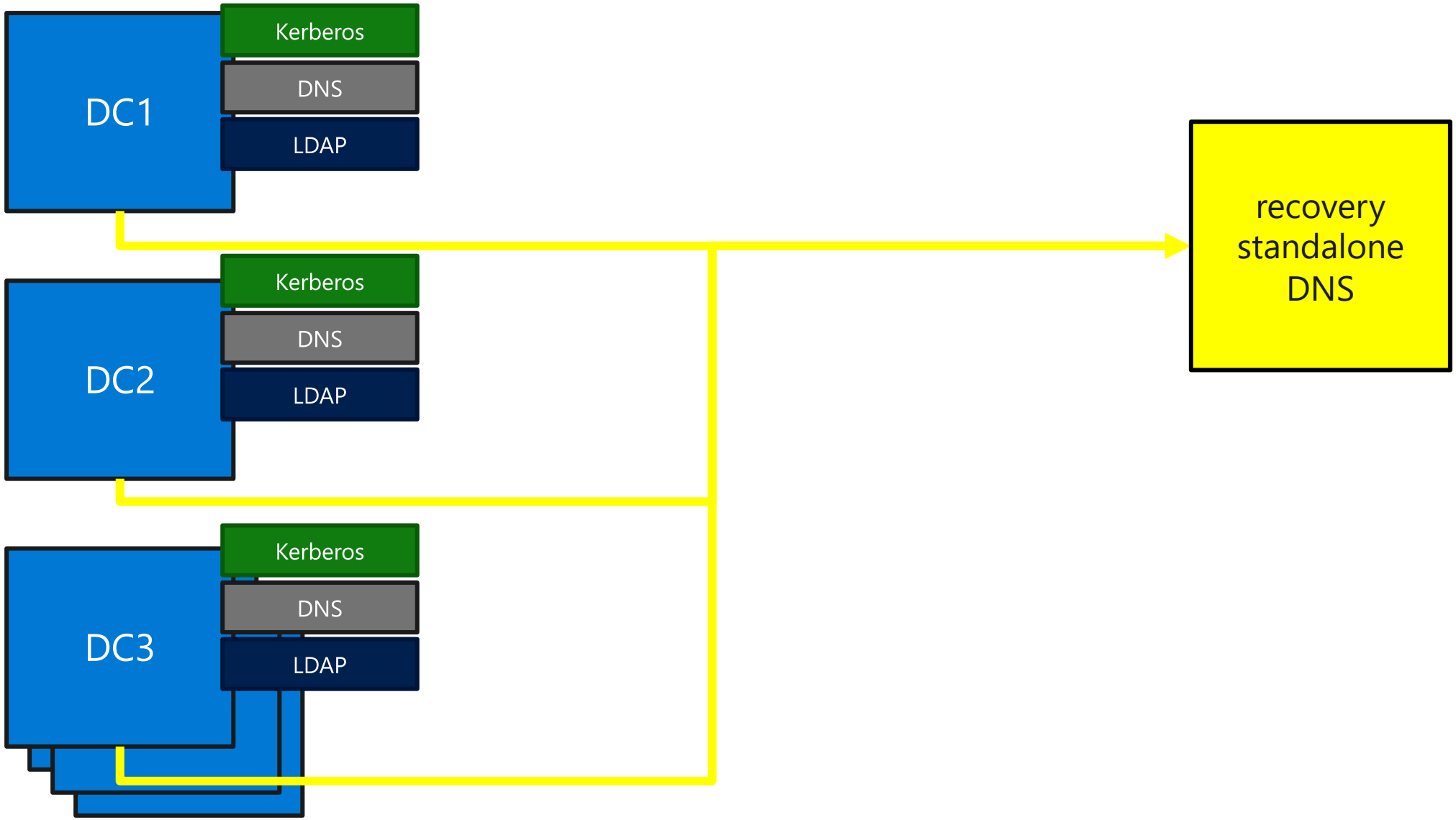
All DCs recovery in full scenario



All DCs recovery in full scenario



All DCs recovery in full scenario



All DCs recovery in full scenario