Virtualized Domain Controller Troubleshooting

Article • 08/31/2016

In this article

Applies To: Windows Server 2012, Windows 8

This topic provides detailed methodology on troubleshooting the virtualized domain controller feature.

- Troubleshooting virtualized domain controller cloning
- Troubleshooting virtualized domain controller safe restore

Introduction

The most important way to improve your troubleshooting skills is build a test lab and rigorously examine normal, working scenarios. If you encounter errors, they are more obvious and easy to understand, since you then have a solid foundation of how domain controller promotion works. This also allows you to build your analysis and network analysis skills. This goes for all distributed systems technologies, not just virtualized domain controller deployment.

The critical elements to advanced troubleshooting of domain controller configuration are:

1. Linear analysis combined with focus and attention to detail.
2. Understanding network capture analysis
3. Understanding the built-in logs

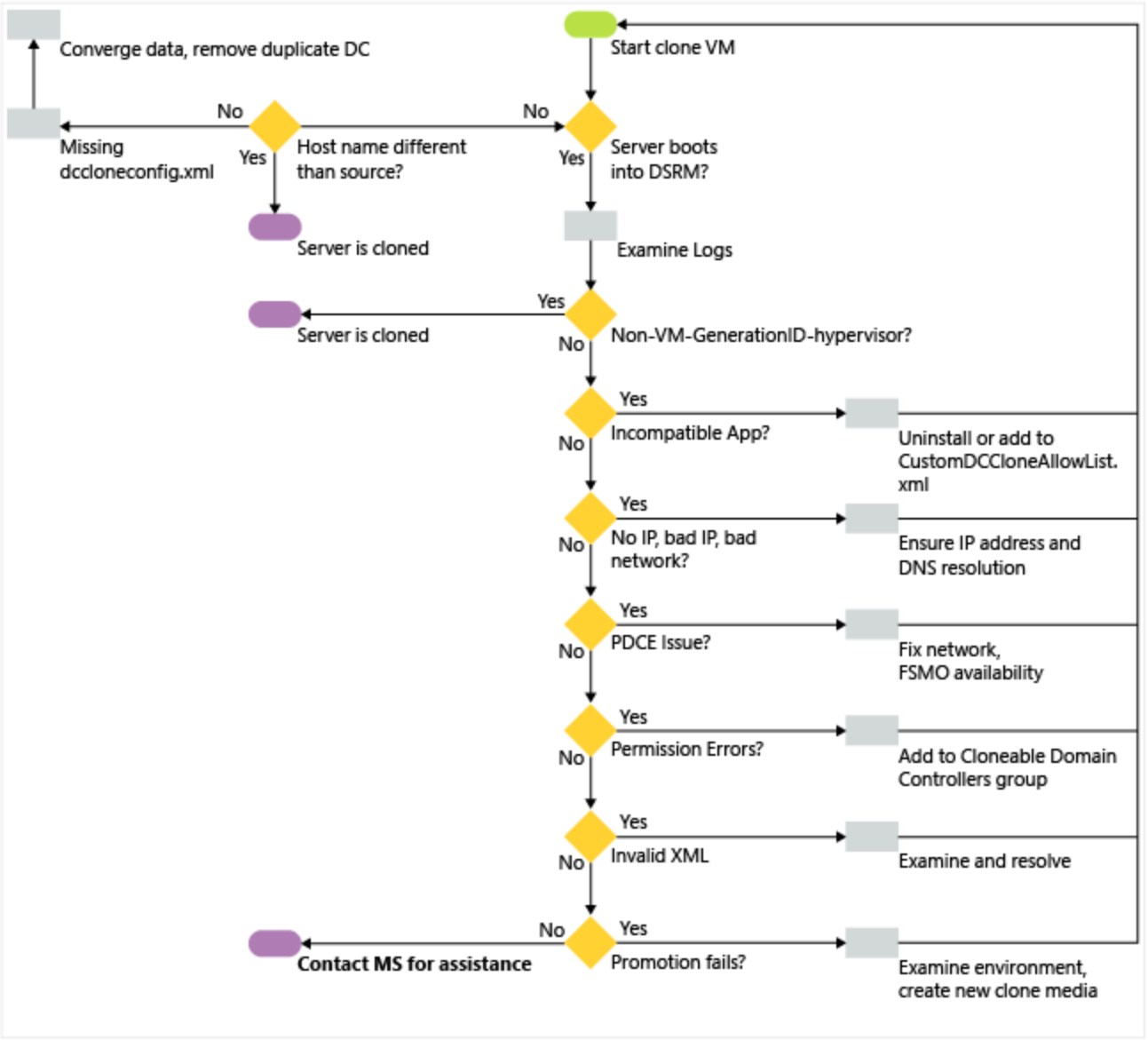
The first and second are beyond the scope of this topic, but the third can be explained in some detail. Virtualized domain controller troubleshooting requires a logical and linear method. The key is to approach the issue using the data provided and only resort to complex tools and analysis when you have exhausted the provided output and logging.

Troubleshooting virtualized domain controller cloning

This sections covers:

- Tools for Troubleshooting
- Logging Options
- General Methodology for Troubleshooting Domain Controller Cloning
- Server Core and the Event Log
- Troubleshooting Specific Problems

The troubleshooting strategy for virtualized domain controller cloning follows this general format:



Tools for Troubleshooting

Logging Options

The built-in logs are the most important tool for troubleshooting issues with domain controller cloning. All of these logs are enabled and configured for maximum verbosity, by default.

Expand table

Operation	Log
Cloning	• Event viewer\Windows logs\System • Event viewer\Applications and services logs\Directory Service • %systemroot%\debug\dcpromo.log
Promotion	• %systemroot%\debug\dcpromo.log • Event viewer\Applications and services logs\Directory Service

- Event viewer\Windows logs\System
- Event viewer\Applications and services logs\File Replication Service
- Event viewer\Applications and services logs\DFS Replication

Tools and Commands for Troubleshooting Domain Controller Configuration

To troubleshoot issues not explained by the logs, use the following tools as a starting point:

- Dcdiag.exe
- Repadmin.exe
- Network Monitor 3.4

General Methodology for Troubleshooting Domain Controller Cloning

1. Is the VM booting into DS Repair Mode (DSRM)? This indicates troubleshooting is necessary. To log on in DSRM, use **.\Administrator** account and specify the DSRM password.

    a. Examine the Dcpromo.log.

        i. Did initial cloning steps succeed but domain controller promotion fail?

        ii. Do errors indicate issues with the local domain controller or with the AD DS environment, such as errors returned from the PDC emulator?

    b. Examine the System and Directory Services event logs and the dccloneconfig.xml and CustomDCCloneAllowList.xml

        i. Does an incompatible application need to be in the CustomDCCloneAllowList.xml allow list?

        ii. Is the IP address or computer name either duplicated or invalid in the dccloneconfig.xml?

        iii. Is the Active Directory site invalid in the dccloneconfig.xml?

        iv. Is the IP address not set in the dccloningconfig.xml and there is no DHCP server available?

        v. Is the PDC emulator online and available through the RPC protocol?

        vi. Is the domain controller a member of the Cloneable Domain Controllers group? Is the permission **Allow a DC to create a clone of itself** set on the domain root for that group?

        vii. Does the Dccloneconfig.xml file contain syntax errors that prevent correct parsing?

        viii. Is the hypervisor supported?

        ix. Did domain controller promotion fail after cloning began successfully?

        x. Was the maximum number of auto-generated domain controller names (9999) exceeded?

        xi. Is the MAC address duplicated?

2. Is host name of the clone the same as the source DC?

    a. Is there a Dccloneconfig.xml file in one of the allowed locations?

3. Is the VM booting into normal mode and cloning completed, but the domain controller is not functioning correctly?

   a. First check if the host name is changed on the clone. If the host name is different, cloning has at least partially completed.

   b. Does the domain controller have a duplicate IP address of the source domain controller from the dccloneconfig.xml, but the source domain controller was offline during cloning?

   c. If the domain controller is advertising, treat the issue as any normal post-promotion issue you would have without cloning.

   d. If the domain controller is not advertising, examine the Directory Service, System, Application, File Replication and DFS Replication event logs for post-promotion errors.

Disabling DSRM Boot

Once booted into DSRM due to any error, diagnose the cause for failure and if the dcpromo.log does not indicate that cloning cannot be retried, fix the cause for failure and reset the DSRM flag. A failed clone does not return to normal mode on its own on the next reboot; you must remove the DS Restore Mode boot flag in order to try cloning again. All of these steps require running as an elevated administrator.

Removing DSRM with Msconfig.exe

To turn DSRM boot off using a GUI, use the System Configuration tool:

1. Run msconfig.exe
2. On the **Boot** tab, under **Boot Options**, de-select **Safe boot** (it is already selected with the option **Active Directory repair** enabled)
3. Click OK and restart when prompted

Removing DSRM with Bcdedit.exe

To turn DSRM boot off from the command-line, use the Boot Configuration Data Store Editor:

1. Open a CMD prompt and run:

```
Bcdedit.exe /deletevalue safeboot
```

2. Restart the computer with:

```
Shutdown.exe /t /0 /r
```

> ⓘ **Note**
>
> Bcdedit.exe also works in a Windows PowerShell console. The commands there are: Bcdedit.exe /deletevalue safeboot Restart-computer

Server Core and the Event Log

The event logs contain much of the useful information about virtualized domain controller cloning operations. By default, a Windows Server 2012 computer installation is a Server Core installation, which means there is no graphical interface and therefore, no way to run the local Event Viewer snap-in.

To review the event logs on a server running a Server Core installation:

- Run the Wevtutil.exe tool locally
- Run PowerShell cmdlet Get-WinEvent locally
- If you have enabled the Windows Advanced Firewall rules for the "Remote Event Log Management" groups (or equivalent ports) to allow inbound communication, you can manage the event log remotely using Eventvwr.exe, wevtutil.exe, or Get-Winevent. This can be done on Server Core installation using NETSH.exe, Group Policy, or the new Set-NetFirewallRule cmdlet in Windows PowerShell 3.0.

> ⚠ **Warning**
>
> Do not attempt to add the graphical shell back to the computer while it is in DSRM. Windows servicing stack (CBS) cannot operate correctly while in Safe Mode or DSRM. Attempts to add features or roles while in DSRM will not complete and leave the computer in an unstable state until it is booted normally. Since a virtualized domain controller clone in DSRM cannot boot normally, and should not be booted normally under most circumstances, it is impossible to safely add the graphical shell. Doing so is unsupported and may leave you with an unusable server.

Troubleshooting Specific Problems

Events

All virtualized domain controller cloning events write to the Directory Services event log of the clone domain controller VM. The Application, File Replication Service, and DFS Replication event logs may also contain useful troubleshooting information for failed cloning. Failures during the RPC call to the PDC emulator may be available in the event log on the PDC emulator.

Below are the Windows Server 2012 cloning-specific events in the Directory Services event log, with notes and suggested resolutions for errors.

Directory Services Event Log

Expand table

Event ID	**2160**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	The local <*COMPUTERNAME*> has found a virtual domain controller cloning configuration file. The virtual domain controller cloning configuration file is found at: %1 The existence of the virtual domain controller cloning configuration file indicates that the local virtual domain controller is a clone of another virtual domain controller. The <*COMPUTERNAME*> will start to clone itself.
Notes and resolution	This is a success event and only an issue if unexpected. Examine the DSA Working Directory, %systemroot%\ntds, and root of any local or removable disks for the

	dcclconeconfig.xml file.

Expand table

Event ID	**2161**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	The local <*COMPUTERNAME*> did not find the virtual domain controller cloning configuration file. The local machine is not a cloned DC.
Notes and resolution	This is a success event and only an issue if unexpected. Examine the DSA Working Directory, %systemroot%\ntds, and root of any local or removable disks for the dcclconeconfig.xml file.

Expand table

Event ID	**2162**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Virtual domain controller cloning failed. Please check events logged in System event logs and %systemroot%\debug\dcpromo.log for more information on errors that correspond to the virtual domain controller cloning attempt. Error code: %1
Notes and resolution	Follow message instructions, this error is a catchall.

Expand table

Event ID	**2163**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	DsRoleSvc service was started to clone the local virtual domain controller.
Notes and resolution	This is a success event and only an issue if unexpected. Examine the DSA Working Directory, %systemroot%\ntds, and root of any local or removable disks for the dcclconeconfig.xml file.

Expand table

Event ID	**2164**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to start the DsRoleSvc service to clone the local virtual domain controller.
Notes and resolution	Examine the service settings for the DS Role Server service (DsRoleSvc) and ensure its start type is set to manual. Validate that no third party program is preventing the start of this service.

Expand table

Event ID	**2165**

Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	*<COMPUTERNAME>* failed to start a thread during the cloning of the local virtual domain controller. Error code:%1 Error message:%2 Thread name:%3
Notes and resolution	Contact Microsoft Product Support

Expand table

Event ID	**2166**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	*<COMPUTERNAME>* needs RPCSS service to initiate rebooting into DSRM. Waiting for RPCSS to initialize into a running state failed. Error code:%1
Notes and resolution	Examine the System event log and service settings for the RPC Server service (Rpcss)

Expand table

Event ID	**2167**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	*<COMPUTERNAME>* could not initialize virtual domain controller knowledge. See previous event log entry for details. Additional Data Failure code:%1
Notes and resolution	Follow message instructions, this error is a catchall.

Expand table

Event ID	**2168**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Microsoft-Windows-ActiveDirectory_DomainService The DC is running on a supported hypervisor. VM Generation ID is detected. Current value of VM Generation ID: %1
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	**2169**
Source	Microsoft-Windows-ActiveDirectory_DomainService

Severity	Informational
Message	There is no VM Generation ID detected. The DC is hosted on a physical machine, a down-level version of Hyper-V, or a hypervisor that does not support the VM Generation ID. Additional Data Failure code returned when checking VM Generation ID:%1
Notes and resolution	This is a success event if not intending to clone. Otherwise, examine the System event log and review hypervisor product support documentation.

Expand table

Event ID	**2170**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Warning
Message	A Generation ID change has been detected. Generation ID cached in DS (old value):%1 Generation ID currently in VM (new value):%2 The Generation ID change occurs after the application of a virtual machine snapshot, after a virtual machine import operation or after a live migration operation. <*COMPUTERNAME*> will create a new invocation ID to recover the domain controller. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services aware backup application.
Notes and resolution	This is a success event if intending to clone. Otherwise, examine the System event log.

Expand table

Event ID	**2171**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	No Generation ID change has been detected. Generation ID cached in DS (old value):%1 Generation ID currently in VM (new value):%2
Notes and resolution	This is a success event if not intending to clone, and should be seen at every reboot of a virtualized DC. Otherwise, examine the System event log.

Expand table

Event ID	**2172**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Read the msDS-GenerationId attribute of the Domain Controller's computer object. msDS-GenerationId attribute value:%1
Notes and resolution	This is a success event if intending to clone. Otherwise, examine the System event log.

Expand table

Event ID	**2173**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Failed to read the msDS-GenerationId attribute of the Domain Controller's computer object. This may be caused by database transaction failure, or the generation id does not exist in the local database. The msDS-GenerationId does not exist during the first reboot after dcpromo or the DC is not a virtual domain controller. Additional Data Failure code:%1
Notes and resolution	This is a success event if intending to clone and it is the first VM reboot after cloning has completed. It can also be ignored on non-virtual Domain controllers. Otherwise, examine the System event log.

Expand table

Event ID	**2174**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	The DC is neither a virtual domain controller clone nor a restored virtual domain controller snapshot.
Notes and resolution	This is a success event if not intending to clone. Otherwise, examine the System event log.

Expand table

Event ID	**2175**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Virtual domain controller clone configuration file exists on an unsupported platform.
Notes and resolution	This occurs when a dccloneconfig.xml is found but a VM Generation-ID could not be found, such as when a dccloneconfig.xml file is found on a physical computer or on a hypervisor that does not support VM Generation-ID.

Expand table

Event ID	**2176**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Renamed virtual domain controller clone configuration file. Additional Data Old file name:%1 New file name:%2
Notes and resolution	Rename expected when booting a source VM back up, because the VM Generation ID has not changed. This prevents the source domain controller from trying to clone.

Expand table

Event ID	**2177**

Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Renaming virtual domain controller clone configuration file failed. Additional Data File name:%1 Failure code:%2 %3
Notes and resolution	Rename attempt expected when booting a source VM back up, because the VM Generation ID has not changed. This prevents the source domain controller from trying to clone. Manually rename the file and investigate installed third party products that may be preventing the file rename.

Expand table

Event ID	**2178**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Detected virtual domain controller clone configuration file, but VM Generation ID has not been changed. The local DC is the clone source DC. Rename the clone configuration file.
Notes and resolution	Expected when booting a source VM back up, because the VM Generation ID has not changed. This prevents the source domain controller from trying to clone.

Expand table

Event ID	**2179**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	The msDS-GenerationId attribute of the Domain Controller's computer object has been set to the following parameter: GenerationID attribute:%1
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	**2180**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Warning
Message	Failed to set the msDS-GenerationId attribute of the Domain Controller's computer object. Additional Data Failure code:%1
Notes and resolution	Examine the System event log and Dcpromo.log. Lookup the specific error in MS TechNet, MS Knowledgebase, and MS blogs to determine its usual meaning, and then troubleshoot based on those results.

Expand table

Event ID	**2182**

Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Internal event: The Directory Service has been asked to clone a remote DSA:
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	**2183**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Internal event: <*COMPUTERNAME*> completed the request to clone the remote Directory System Agent. Original DC name:%3 Request clone DC name:%4 Request clone DC site:%5 Additional Data Error value:%1 %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	**2184**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to create a domain controller account for the cloned DC. Original DC name:%1 Allowed number of cloned DC:%2 The limit on the number of domain controller accounts that can be generated by cloning <*COMPUTERNAME*>was exceeded.
Notes and resolution	A single source domain controller name can only automatically generate 9999 times if domain controllers are not demoted, based on the naming convention. Use the <computername> element in the XML to generate a new unique name or clone from a differently named DC.

Expand table

Event ID	**2191**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> set the following registry value to disable DNS updates. Registry Key:%1 Registry Value: %2 Registry Value data: %3 During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled

	during this period so clients cannot send requests to the local machine undergoing cloning. The cloning process will enable DNS updates again after cloning is completed.
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	**2192**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to set the following registry value to disable DNS updates. Registry Key:%1 Registry Value: %2 Registry Value data: %3 Error code:%4 Error message:%5 During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled during this period so clients cannot send requests to the local machine undergoing cloning.
Notes and resolution	Examine Application and System event logs. Investigate third party application that may be blocking registry updates.

Expand table

Event ID	**2193**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> set the following registry value to enable DNS updates. Registry Key:%1 Registry Value: %2 Registry Value data: %3 During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled during this period so clients cannot send requests to the local machine undergoing cloning.
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	**2194**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to set the following registry value to enable DNS updates. Registry Key:%1 Registry Value: %2 Registry Value data: %3

	Error code:%4 Error message:%5 During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled during this period so clients cannot send requests to the local machine undergoing cloning.
Notes and resolution	Examine Application and System event logs. Investigate third party application that may be blocking registry updates.

Expand table

Event ID	**2195**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Failed to set DSRM boot. Error code:%1 Error message:%2 When virtual domain controller cloning failed or virtual domain controller clone configuration file appears on a non-supported hypervisor, the local machine will reboot into DSRM for troubleshooting. Setting DSRM boot failed.
Notes and resolution	Examine Application and System event logs. Investigate third party application that may be blocking registry updates.

Expand table

Event ID	**2196**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Failed to enable shutdown privilege. Error code:%1 Error message:%2 When virtual domain controller cloning failed or virtual domain controller clone configuration file appears on a non-supported hypervisor, the local machine will reboot into DSRM for troubleshooting. Enabling shutdown privilege failed.
Notes and resolution	Examine Application and System event logs. Investigate third party application that may be blocking privilege usage.

Expand table

Event ID	**2197**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Failed to initiate system shutdown. Error code:%1 Error message:%2 When virtual domain controller cloning failed or virtual domain controller clone configuration file appears on a non-supported hypervisor, the local machine will reboot into DSRM for troubleshooting. Initiating system shutdown failed.

Notes and resolution	Examine Application and System event logs. Investigate third party application that may be blocking privilege usage.

Expand table

Event ID	**2198**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	*<COMPUTERNAME>* failed to create or modify the following cloned DC object. Additional data: Object: %1 Error value: %2 %3
Notes and resolution	Lookup the specific error in MS TechNet, MS Knowledgebase, and MS blogs to determine its usual meaning, and then troubleshoot based on those results.

Expand table

Event ID	**2199**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	*<COMPUTERNAME>* failed to create the following cloned DC object because the object already exists. Additional data: Source DC: %1 Object: %2
Notes and resolution	Validate the dccloneconfig.xml did not specify an existing domain controller or that copies of the dccloneconfig.xml have been used on multiple clones without editing the name. If the collision is still unexpected, determine which administrator promoted it; contact them to discuss if the existing domain controller should be demoted, the existing domain controller metadata cleaned, or if the clone should use a different name.

Expand table

Event ID	**2203**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Last virtual domain controller cloning failed. This is the first reboot since then so this should be a re-try of the cloning. However, neither virtual domain controller clone configuration file exists nor virtual machine generation ID change is detected. Boot into DSRM. Last virtual domain controller cloning failed:%1 Virtual domain controller clone configuration file exists:%2 Virtual machine generation ID change is detected:%3

Notes and resolution	Expected if cloning failed previously, due to missing or invalid dccloneconfig.xml

Expand table

Event ID	2210
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<COMPUTERNAME> failed to create objects for clone domain controller. Additional data: Clone Id: %6 Clone domain controller name: %1 Retry loop: %2 Exception value: %3 Error value: %4 DSID: %5
Notes and resolution	Review the System and Directory Services event logs and the dcpromo.log for further details on why cloning failed.

Expand table

Event ID	2211
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> has created objects for clone domain controller. Additional data: Clone Id: %3 Clone domain controller name: %1 Retry loop: %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2212
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> started to create objects for the clone domain controller. Additional data: Clone Id: %1 Clone name: %2 Clone site: %3 Clone RODC: %4
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2213
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> created a new KrbTgt object for Read-Only domain controller cloning. Additional data: Clone Id: %1 New KrbTgt Object Guid: %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2214
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> will create a computer object for the clone domain controller. Additional data: Clone Id: %1 Original domain controller: %2 Clone domain controller: %3
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2215
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> will add the clone domain controller in the following site. Additional data: Clone Id: %1 Site: %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2216
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> will create a servers container for the clone domain controller. Additional data:

	Clone Id: %1 Servers Container: %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2217
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> will create a server object for the clone domain controller. Additional data: Clone Id: %1 Server Object: %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2218
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> will create a NTDS Settings object for the clone domain controller. Additional data: Clone Id: %1 Object: %2
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2219
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> will create connection objects for the clone Read-Only domain controller. Additional data: Clone Id: %1
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2220
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational

Message	<COMPUTERNAME> will create SYSVOL objects for the clone Read-Only domain controller. Additional data: Clone Id: %1
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2221
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<COMPUTERNAME> failed to generate a random password for the cloned domain controller. Additional data: Clone Id: %1 Clone domain controller name: %2 Error: %3 %4
Notes and resolution	Examine the system event log for further details on why the machine account password could not be created.

Expand table

Event ID	2222
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<COMPUTERNAME> failed to set password for the cloned domain controller. Additional data: Clone Id: %1 Clone domain controller name: %2 Error: %3 %4
Notes and resolution	Examine the system event log for further details on why the machine account password could not be set.

Expand table

Event ID	2223
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<COMPUTERNAME> successfully set machine account password for the cloned domain controller. Additional data: Clone Id: %1 Clone domain controller name: %2 Total retry times: %3

Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2224
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Virtual domain controller cloning failed. The following %1 Managed Service Account(s) exist on the cloned machine: %2 For cloning to succeed, all Managed Service Accounts must be removed. This can be done using the Remove-ADComputerServiceAccount PowerShell cmdlet.
Notes and resolution	Expected when using standalone MSAs (not group MSA). Do *not* follow the event advice to remove the account - it is incorrectly written. Use Uninstall-AdServiceAccount - https://technet.microsoft.com/library/hh852310. Standalone MSAs - first released in Windows Server 2008 R2 - were replaced in Windows Server 2012 with group MSAs (gMSA). GMSAs support cloning.

Expand table

Event ID	2225
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	The cached secrets of the following security principal have been successfully removed from local domain controller: %1 After cloning a read-only domain controller, secrets which were previously cached on the cloning source read-only domain controller will be removed on the cloned domain controller.
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	2226
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Failed to remove cached secrets of the following security principal from local domain controller: %1 Error: %2 (%3) After cloning a read-only domain controller, secrets which were previously cached on the cloning source read-only domain controller need to be removed on the clone in order to decrease the risk that an attacker can obtain those credentials from stolen or compromised clone. If the security principal is a highly privileged account and should be protected against this, please use rootDSE operation rODCPurgeAccount to manually clear its secrets on local domain controller.
Notes and resolution	Examine the System and Directory Services event logs for further information.

Expand table

Event ID	2227
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Exception is raised while trying to remove cached secrets from local domain controller. Additional data: Exception value: %1 Error value: %2 DSID: %3 After cloning a read-only domain controller, secrets which were previously cached on the cloning source read-only domain controller need to be removed on the clone in order to decrease the risk that an attacker can obtain those credentials from stolen or compromised clone. If any of these security principals is a highly privileged account and should be protected against this, please use rootDSE operation rODCPurgeAccount to manually clear its secrets on local domain controller.
Notes and resolution	Examine the System and Directory Services event logs for further information.

Expand table

Event ID	2228
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	The Virtual machine generation ID in the Active Directory database of this domain controller is different from the current value of this virtual machine. However, a virtual domain controller clone configuration file (DCCloneConfig.xml) could not be located so domain controller cloning was not attempted. If a domain controller cloning operation was intended, please ensure that a DCCloneConfig.xml is provided in any one of the supported locations. In addition, the IP address of this domain controller conflicts with another domain controller's IP address. To ensure no disruptions in service occur, the domain controller has been configured to boot into DSRM. Additional data: The duplicate IP address: %1
Notes and resolution	This protection mechanism stops duplicate domain controllers when possible (it will not when using DHCP, for example). Add a valid DcCloneConfig.xml file, remove the DSRM flag, and re-attempt cloning

Expand table

Event ID	29218
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed. The cloning operation could not be completed and the cloned domain controller was rebooted into Directory Services Restore Mode (DSRM). Please check previously logged events and %systemroot%\debug\dcpromo.log for more information on errors that correspond to the virtual domain controller cloning attempt and whether or not this clone image can be reused. If one or more log entries indicate that the cloning process cannot be retried, the image must be securely destroyed. Otherwise you may fix the errors, clear the DSRM boot flag, and reboot normally; upon reboot, the cloning operation will be retried.

Notes and resolution	Review the System and Directory Services event logs and the dcpromo.log for further details on why cloning failed.

Expand table

Event ID	29219
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Informational
Message	Virtual domain controller cloning succeeded.
Notes and resolution	This is a success event and only an issue if unexpected.

Expand table

Event ID	29248
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed to obtain Winlogon Notification. The returned error code is %1 (%2). For more information on this error, please review %systemroot%\debug\dcpromo.log for errors that correspond to the virtual domain controller cloning attempt.
Notes and resolution	Contact Microsoft Product Support

Expand table

Event ID	29249
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed to parse virtual domain controller configuration file. The returned HRESULT code is %1. The configuration file is:%2 Please fix the errors in the configuration file and retry the cloning operation. For more information about this error, please see %systemroot%\debug\dcpromo.log.
Notes and resolution	Examine the dclconeconfig.xml file for syntax errors using an XML editor and the DCCloneConfigSchema.xsd schema file.

Expand table

Event ID	29250
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed. There are software or services currently enabled on the cloned virtual domain controller that are not present in the allowed application list for virtual domain controller cloning. Following are the missing entries: %2

	%1 (if any) was used as the defined inclusion list. The cloning operation cannot be completed if there are non-cloneable applications installed. Please run Active Directory PowerShell Cmdlet Get-ADDCCloningExcludedApplicationList to check which applications are installed on the cloned machine, but not included in the allow list, and add them to the allow list if they are compatible with virtual domain controller cloning. If any of these applications are not compatible with virtual domain controller cloning, please uninstall them before re-trying the cloning operation. The virtual domain controller cloning process searches for the allowed application list file, CustomDCCloneAllowList.xml, based on the following search order; the first file found is used and all others are ignored: 1. The registry value name: HKey_Local_Machine\System\CurrentControlSet\Services\NTDS\Parameters\AllowListFolder 2. The same directory where the DSA Working Directory folder resides 3. %windir%\NTDS 4. Removable read/write media in order of drive letter at the root of the drive
Notes and resolution	Follow the message instructions

Expand table

Event ID	29251
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed to reset the IP addresses of the clone machine. The returned error code is %1 (%2). This error might be caused by misconfiguration in network configuration sections in the virtual domain controller configuration file. Please see %systemroot%\debug\dcpromo.log for more information about errors that correspond to IP addresses resetting during virtual domain controller cloning attempts. Details on resetting machine IP addresses on the cloned machine can be found at https://go.microsoft.com/fwlink/?LinkId=208030
Notes and resolution	Verify the IP information set in the dccloneconfig.xml is valid and does not duplicate the original source machine.

Expand table

Event ID	29253
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed. The clone domain controller was unable to locate the primary domain controller (PDC) operations master in the cloned computer's home domain of the cloned machine. The returned error code is %1 (%2). Please verify that the primary domain controller in the home domain of the cloned machine is assigned to a live domain controller, is online, and is operational. Verify that the cloned machine has LDAP/RPC connectivity to the primary domain controller over the required ports and protocols.

Notes and resolution	Validate the cloned domain controller IP and DNS information is set. Use Dcdiag.exe /test:locatorcheck to validate if the PDCE is online, use Nltest.exe /server:<*PDCE*> /dclist:<*domain*> to valid RPC, obtain a network capture from the PDCE while cloning fails and analyze the traffic.

Expand table

Event ID	29254
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed to bind to the primary domain controller %1. The returned error code is %2 (%3). Please verify that the primary domain controller %1 is online and is operational. Verify that the cloned machine has LDAP/RPC connectivity to the primary domain controller over the required ports and protocols.
Notes and resolution	Validate the cloned domain controller IP and DNS information is set. Use Dcdiag.exe /test:locatorcheck to validate if the PDCE is online, use Nltest.exe /server:<*PDCE*> /dclist:<*domain*> to valid RPC, obtain a network capture from the PDCE while cloning fails and analyze the traffic.

Expand table

Event ID	29255
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed. An attempt to create objects on the primary domain controller %1 required for the image being cloned returned error %2 (%3). Please verify that the cloned domain controller has privilege to clone itself. Check for related events in the Directory Service event log on primary domain controller %1.
Notes and resolution	Lookup the specific error in MS TechNet, MS Knowledgebase, and MS blogs to determine its typical meaning, and then troubleshoot based on those results.

Expand table

Event ID	29256
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	An attempt to set the Boot into Directory Services Restore Mode flag failed with error code %1. Please see %systemroot%\debug\dcpromo.log for more information about errors.
Notes and resolution	Examine the Directory Services log and dcpromo.log for details. Examine Application and System event logs. Investigate third party application that may be blocking privilege usage.

Expand table

Event ID	29257
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error

Message	Virtual domain controller cloning has done. An attempt to reboot the machine failed with error code %1. Please reboot the machine to finish the cloning operation.
Notes and resolution	Examine Application and System event logs. Investigate third party application that may be blocking privilege usage.

Expand table

Event ID	29264
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	An attempt to clear the Boot into Directory Services Restore Mode flag failed with error code %1. Please see %systemroot%\debug\dcpromo.log for more information about errors.
Notes and resolution	Examine the Directory Services log and dcpromo.log for details. Examine Application and System event logs. Investigate third party application that may be blocking privilege usage.

Expand table

Event ID	29265
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Informational
Message	Virtual domain controller cloning succeeded. The virtual domain controller cloning configuration file %1 has been renamed to %2.
Notes and resolution	N/A, this is a success event.

Expand table

Event ID	29266
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning succeeded. The attempt to rename virtual domain controller cloning configuration file %1 failed with error code %2 (%3).
Notes and resolution	Manually rename the dccloneconfig.xml file.

Expand table

Event ID	29267
Source	Microsoft-Windows-DirectoryServices-DSROLE-Server
Severity	Error
Message	Virtual domain controller cloning failed to check the virtual domain controller cloning allowed application list. The returned error code is %1 (%2). This error might be caused by a syntax error in the clone allow list file (The file currently being checked is: %3). For more information about this error, please see %systemroot%\debug\dcpromo.log.

Notes and resolution	Follow the event instructions

Error Messages

There are no direct interactive errors for failed virtualized domain controller cloning; all cloning information logs in the System and Directory Services logs and the domain controller promotion logs in dcpromo.log. However, if the server boots into DS Restore Mode, investigate immediately, as promotion or cloning failed.

The dcpromo.log is the first place to check for cloning failure. Depending on the failure listed, it may be necessary to subsequently review Directory Services and System logs for further diagnosis.

Known Issues and Support Scenarios

The following are common issues seen during the Windows Server 2012 development process. All of these issues are "by design" and have either a valid workaround or more appropriate technique to avoid them in the first place. Some may be resolved in later releases of Windows Server 2012.

Expand table

Issue	**Cloning fails, DSRM**
Symptoms	Clone boots into Directory Services Restore Mode
Resolution and Notes	Validate all steps followed from sections Deploying Virtualized Domain Controller section and General Methodology for Troubleshooting Domain Controller Cloning Described in KB 2742844.

Expand table

Issue	**Extra IP leases when using DHCP to clone**
Symptoms	After successfully cloning a DC and using DHCP, the first boot of the clone takes a DHCP lease. Then when the server is renamed and restarted as a DC, it takes a second DHCP lease. The first IP address is not released and you end up with a "phantom" lease
Resolution and Notes	Manually delete the unused address lease in DHCP or allow it to expire normally. Described in KB 2742836.

Expand table

Issue	**Cloning fails into DSRM after very long delay**
Symptoms	Cloning appears to pause at "Domain controller cloning is at X% completion" for between 8 and 15 minutes. After this, the cloning fails and boots into DSRM.
Resolution and Notes	The cloned computer cannot get a dynamic IP address from DHCP or SLAAC, or is using a duplicate IP address, or cannot find the PDC. Multiple retry attempts performed by cloning lead to the delay. Resolve the networking issue to allow cloning. Described in KB 2742844.

Expand table

Issue	**Cloning does not recreate all service principal names**
Symptoms	If a set of *three-part* service principal names (SPN) includes both a NetBIOS name with a port and an otherwise identical NetBIOS name without a port, the non-port entry is not recreated with the new computer name. For example:

	customspn/DC1:200/app1 INVALID USE OF SYMBOLS *this is recreated with the new computer name* customspn/DC1/app1 INVALID USE OF SYMBOLS *this is not recreated with the new computer name* Fully qualified names are recreated and SPNs without three parts are recreated, regardless of ports. For example, these are recreated successfully on the clone: customspn/DC1:202 INVALID USE OF SYMBOLS *this is recreated* customspn/DC1 INVALID USE OF SYMBOLS *this is recreated* customspn/DC1.corp.contoso.com:202 INVALID USE OF SYMBOLS *this is recreated name* customspn/DC1.corp.contoso.com INVALID USE OF SYMBOLS *this is recreated*
Resolution and Notes	This is a limitation of the domain controller rename process in Windows, not just in cloning. Three-part SPNS are not handled by the renaming logic in any scenario. Most included Windows services are unaffected by this, as they recreate any missing SPNs as needed. Other applications may require manually entering the SPN to resolve the issue. Described in KB 2742874.

Expand table

Issue	**Cloning fails, boots into DSRM, general networking errors**
Symptoms	Clone boots into Directory Services Repair Mode. There are general networking errors.
Resolution and Notes	Ensure that the new clone does not have a duplicate static MAC address assigned from the source domain controller; you can see if a VM uses static MAC addresses by running this command on the hypervisor host for both the source and clone virtual machines: Get-VM –VMName *test-vm* | Get-VMNetworkAdapter | fl * Change the MAC address to a unique static address or switch to using dynamic MAC addresses. Described in KB 2742844

Expand table

Issue	**Cloning fails, boots into DSRM as a duplicate of the source DC**
Symptoms	A new clone boots up without cloning. The dccloneconfig.xml is not renamed and the server starts in DS Restore Mode. The Directory Services event log shows Error 2164 <COMPUTERNAME> failed to start the DsRoleSvc service to clone the local virtual domain controller.
Resolution and Notes	Examine the service settings for the DS Role Server service (DsRoleSvc) and ensure its start type is set to Manual. Validate that no third party program is preventing the start of this service. For more information about how to reclaim this secondary DC while ensuring that updates get replicated outbound, see Microsoft KB article 2742970.

Expand table

Issue	**Cloning fails, boots into DSRM, error 8610**
Symptoms	Clone boots into Directory Services Restore Mode. Dcpromo .log shows 8610 error (which is ERROR_DS_ROLE_NOT_VERIFIED 8610 or 0x21A2)
Resolution and Notes	Will happen if the PDC can be discoverable but it has not performed sufficient replication to allow itself to assume the role. For example, if cloning is started and another administrator moves the PDCE FSMO role to a new DC. Described in KB 2742916.

Expand table

Issue	**Cloning fails, boots into DSRM, general networking errors**
Symptoms	Clone boots into Directory Services Restore Mode. There are general networking errors.
Resolution and Notes	Ensure that the new clone does not have a duplicate static MAC address assigned from the source domain controller; you can see if a VM uses static MAC addresses by running this command on the Hyper-V host for both the source and clone virtual machines: Get-VM –VMName test-vm | Get-VMNetworkAdapter | fl * Change the MAC address to a unique static address or switch to using dynamic MAC addresses. Described in KB 2742844.

Expand table

Issue	**Cloning fails, boots into DSRM**
Symptoms	Clone boots into Directory Services Repair Mode
Resolution and Notes	Ensure that the dccloneconfig.xml contains the schema definition (see sampledccloneconfig.xml, line 2): **<d3c:DCCloneConfig xmlns:d3c="uri:microsoft.com:schemas:DCCloneConfig">** Described in KB 2742844

Expand table

Issue	**No logon servers are available error logging into DSRM**
Symptoms	Clone boots into Directory Services Repair Mode. You attempt to logon and receive error: **There are currently no logon servers are available to service the logon request**
Resolution and Notes	Ensure you logon with the DSRM administrator account, and not the domain account. Use the left arrow and type a user name of: **.\administrator** Described in KB 2742908

Expand table

Issue	**Clone Source fails into DSRM, error**
Symptoms	During cloning, fails 8437 "Create clone DC objects on PDC failed" (0x20f5)
Resolution and Notes	Duplicate computer name was set in DCCloneConfig.xml as the source DC or an existing DC. The computer name also needs to be in the NetBIOS computer name format (15 characters or fewer, not an FQDN). Fix the dccloneconfig.xml file by setting a unique, valid name. Described in KB 2742959

Expand table

Issue	**New-addccloneconfigfile error "index was out of range"**
Symptoms	When running the new-addccloneconfigfile cmdlet, you receive error: Index was out of range. Must be non-negative and less than the size of the collection.
Resolution and Notes	You must run the cmdlet in an administrator-elevated Windows PowerShell console. This error is caused by lack of local administrator group membership on the

	computer. Described in KB 2742927

Expand table

Issue	**Cloning fails, duplicate DC**
Symptoms	Clone boots without cloning, duplicates existing source DC
Resolution and Notes	The computer was copied and started but does not contain a DcCloneConfig.xml file in any of the supported locations, and did not have a duplicate IP address with the source domain controller. The DC must be correctly removed in order to avoid data loss. Described in KB 2742970

Expand table

Issue	**New-ADDCCloneConfigFile fails with The server is not operational error when it checks if the source domain controller is a member of the Cloneable Domain controllers group if a GC is not available.**
Symptoms	When running New-ADDCCloneConfigFile to create a dccloneconfig.xml file, you receive error: The server is not operational
Resolution and Notes	Verify connectivity to a GC from the server where you run New-ADDCCloneConfigFile and verify that the membership of the source domain controller in the Cloneable Domain Controllers group has replicated to that GC. Run the following command as a means of flushing the DC locator cache for cases where a GC or DC may have been taken offline recently: nltest /dsgetdc: /GC /FORCE

Advanced Troubleshooting

This module seeks to teach advanced troubleshooting by using *working* logs as samples, with some explanation of what occurred. If you understand what a successful virtualized domain controller operation looks like, failures become obvious in your environment. These logs are presented by their source, with the ascending order of *expected* events (even when they are warnings and errors) related to a cloned domain controller within each log.

Cloning a Domain Controller

In this example, the clone domain controller uses DHCP to get an IP address, replicates SYSVOL using FRS or DFSR (see the appropriate log as necessary), is a global catalog, and uses a blank dccloneconfig.xml file.

Directory Services Event Log

The Directory Services log contains the majority of event-based cloning operational information. The hypervisor changes the VM-Generation ID and the NTDS service notes it, then invalidates the RID pool and changes the invocation ID. The new VM-Generation ID is set and the server replicates Active Directory data inbound. The DFSR service is stopped and its database that hosts SYSVOL is deleted, forcing a non-authoritative sync inbound. The USN high watermark is adjusted.

Expand table

Event ID	Source	Message
2160	ActiveDirectory_DomainService	The local Active Directory Domain Services has found a virtual domain controller cloning configuration file. The virtual domain controller cloning configuration file is found at: <*path*>\DCCloneConfig.xml The existence of the virtual domain controller cloning configuration file indicates that the local virtual domain controller is a clone of another virtual domain controller. The Active Directory Domain Services will start to clone itself.
2191	ActiveDirectory_DomainService	Active Directory Domain Services set the following registry value to disable DNS updates. Registry Key: SYSTEM\CurrentControlSet\Services\Netlogon\Parameters Registry Value: UseDynamicDns Registry Value data: 0 During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled during this period so clients cannot send requests to the local machine undergoing cloning. The cloning process will enable DNS updates again after cloning is completed.
2191	ActiveDirectory_DomainService	Active Directory Domain Services set the following registry value to disable DNS updates. Registry Key: SYSTEM\CurrentControlSet\Services\Dnscache\Parameters Registry Value: RegistrationEnabled Registry Value data: 0 During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled during this period so clients cannot send requests to the local machine undergoing cloning. The cloning process will enable DNS updates again after cloning is completed. “Information 2/7/2012 3:12:49 PM Microsoft-Windows-ActiveDirectory_DomainService 2191 Internal Configuration” Active Directory Domain Services set the following registry value to disable DNS updates. Registry Key: SYSTEM\CurrentControlSet\Services\Tcpip\Parameters Registry Value: DisableDynamicUpdate Registry Value data: 1

		During the cloning process, the local machine may have the same computer name as the clone source machine for a short time. DNS A and AAAA record registration are disabled during this period so clients cannot send requests to the local machine undergoing cloning. The cloning process will enable DNS updates again after cloning is completed.
2172	ActiveDirectory_DomainService	Read the msDS-GenerationId attribute of the Domain Controller's computer object. msDS-GenerationId attribute value: *<Number>*
2170	ActiveDirectory_DomainService	A Generation ID change has been detected. Generation ID cached in DS (old value): *<Number>* Generation ID currently in VM (new value): *<Number>* The Generation ID change occurs after the application of a virtual machine snapshot, after a virtual machine import operation or after a live migration operation. Active Directory Domain Services will create a new invocation ID to recover the domain controller. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services aware backup application.
1109	ActiveDirectory_DomainService	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): *<GUID>* InvocationID attribute (new value): *<GUID>* Update sequence number: *<Number>* The invocationID is changed when a directory server is restored from backup media, is configured to host a writeable application directory partition, has been resumed after a virtual machine snapshot has been applied, after a virtual machine import operation, or after a live migration operation. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services-aware backup application.
1000	ActiveDirectory_DomainService	Microsoft Active Directory Domain Services startup complete.
1394	ActiveDirectory_DomainService	All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted
2163	ActiveDirectory_DomainService	DsRoleSvc service was started to clone the local virtual domain controller.
326	NTDS ISAM	NTDS (536) NTDSA: The database engine attached a database (1, C:\Windows\NTDS\ntds.dit). (Time=0 seconds)

		Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.016, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Saved Cache: 1
103	NTDS ISAM	NTDS (536) NTDSA: The database engine stopped the instance (0). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.032, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.031, [10] 0.000, [11] 0.000, [12] 0.000, [13] 0.000, [14] 0.000, [15] 0.000.
102	NTDS ISAM	NTDS (536) NTDSA: The database engine (6.02.8225.0000) is starting a new instance (0).
105	NTDS ISAM	NTDS (536) NTDSA: The database engine started a new instance (0). (Time=0 seconds) Internal Timing Sequence: [1] 0.016, [2] 0.000, [3] 0.015, [4] 0.078, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.046, [10] 0.000, [11] 0.000.
1004	ActiveDirectory_DomainService	Active Directory Domain Services was shut down successfully.
102	NTDS ISAM	NTDS (536) NTDSA: The database engine (6.02.8225.0000) is starting a new instance (0).
326	NTDS ISAM	NTDS (536) NTDSA: The database engine attached a database (1, C:\Windows\NTDS\ntds.dit). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.015, [3] 0.016, [4] 0.000, [5] 0.031, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Saved Cache: 1
105	NTDS ISAM	NTDS (536) NTDSA: The database engine started a new instance (0). (Time=1 seconds) Internal Timing Sequence: [1] 0.031, [2] 0.000, [3] 0.000, [4] 0.391, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.031, [10] 0.000, [11] 0.000.
1109	ActiveDirectory_DomainService	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): *<GUID>* InvocationID attribute (new value): *<GUID>* Update sequence number: *<Number>* The invocationID is changed when a directory server is restored from backup media, is configured to host a writeable application directory partition, has been resumed after a virtual machine snapshot has been applied, after a virtual machine import operation, or after a live migration operation. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services-aware backup application.
1168	ActiveDirectory_DomainService	Internal error: An Active Directory Domain Services error has occurred.

		Additional Data Error value (decimal): 2 Error value (hexadecimal): 2 Internal ID: 7011658
1110	ActiveDirectory_DomainService	Promotion of this domain controller to a global catalog will be delayed for the following interval. Interval (minutes): 5 This delay is necessary so that the required directory partitions can be prepared before the global catalog is advertised. In the registry, you can specify the number of seconds that the directory system agent will wait before promoting the local domain controller to a global catalog. For more information about the Global Catalog Delay Advertisement registry value, see the Resource Kit Distributed Systems Guide
103	NTDS ISAM	NTDS (536) NTDSA: The database engine stopped the instance (0). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.047, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.016, [10] 0.000, [11] 0.000, [12] 0.000, [13] 0.000, [14] 0.000, [15] 0.000.
1004	ActiveDirectory_DomainService	Active Directory Domain Services was shut down successfully.
1539	ActiveDirectory_DomainService	Active Directory Domain Services could not disable the software-based disk write cache on the following hard disk. Hard disk: c: Data might be lost during system failures
2179	ActiveDirectory_DomainService	The msDS-GenerationId attribute of the Domain Controller's computer object has been set to the following parameter: GenerationID attribute: *<Number>*
2173	ActiveDirectory_DomainService	Failed to read the msDS-GenerationId attribute of the Domain Controller's computer object. This may be caused by database transaction failure, or the generation id does not exist in the local database. The msDS-GenerationId does not exist during the first reboot after dcpromo or the DC is not a virtual domain controller. Additional Data Failure code: 6
1000	ActiveDirectory_DomainService	Microsoft Active Directory Domain Services startup complete, version 6.2.8225.0
1394	ActiveDirectory_DomainService	All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to

		the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.
1128	ActiveDirectory_DomainService	1128 Knowledge Consistency Checker "A replication connection was created from the following source directory service to the local directory service. Source directory service: CN=NTDS Settings,<*Domain Controller DN*> Local directory service: CN=NTDS Settings, <*Domain Controller DN*> Additional Data Reason Code: 0x2 Creation Point Internal ID: f0a025d
1999	ActiveDirectory_DomainService	The source directory service has optimized the update sequence number (USN) presented by the destination directory service. The source and destination directory services have a common replication partner. The destination directory service is up to date with the common replication partner, and the source directory service was installed using a backup of this partner. Destination directory service ID: <*GUID*> *(<FQDN>)* Common directory service ID: <*GUID*> Common property USN: <*Number*> As a result, the up-to-dateness vector of the destination directory service has been configured with the following settings. Previous object USN: 0 Previous property USN: 0 Database GUID: <*GUID*> Object USN: <*Number*> Property USN: <*Number*>

System Event Log

The next indications of cloning operations are in the System Event log. As the hypervisor tells the guest computer that it was cloned or restored from a snapshot, the domain controller immediately invalidates its RID pool to avoid duplicating security principals later. As cloning

proceeds, various expected operations and messages appear, mostly around services starting and stopping and some expected errors caused by this. When completed the System event log notes overall cloning success.

Expand table

Event ID	Source	Message
16654	Directory-Services-SAM	A pool of account-identifiers (RIDs) has been invalidated. This may occur in the following expected cases: 1. A domain controller is restored from backup. 2. A domain controller running on a virtual machine is restored from snapshot. 3. An administrator has manually invalidated the pool
7036	Service Control Manager	The Active Directory Domain Services service entered the running state.
7036	Service Control Manager	The Kerberos Key Distribution Center service entered the running state.
3096	Netlogon	The primary Domain Controller for this domain could not be located.
7036	Service Control Manager	The Security Accounts Manager service entered the running state.
7036	Service Control Manager	The Server service entered the running state.
7036	Service Control Manager	The Netlogon service entered the running state.
7036	Service Control Manager	The Active Directory Web Services service entered the running state.
7036	Service Control Manager	The DFS Replication service entered the running state.
7036	Service Control Manager	The File Replication Service service entered the running state.
14533	Microsoft-Windows-DfsSvc	DFS has finished building all namespaces.
14531	Microsoft-Windows-DfsSvc	DFS server has finished initializing.
7036	Service Control Manager	The DFS Namespace service entered the running state.
7023	Service Control Manager	The Intersite Messaging service terminated with the following error: The specified server cannot perform the requested operation.
7036	Service Control Manager	The Intersite Messaging service entered the stopped state.
5806	Netlogon	Dynamic updates have been manually disabled on this domain controller. USER ACTION Reconfigure this domain controller to use dynamic updates or manually add the DNS records from the file '%SystemRoot%\System32\Config\Netlogon.dns' to the DNS database."
16651	Directory-Services-SAM	The request for a new account-identifier pool failed. The operation will be retried until the request succeeds. The error is

		The requested FSMO operation failed. The current FSMO holder could not be contacted.
7036	Service Control Manager	The DNS Server service entered the running state.
7036	Service Control Manager	The DS Role Server service entered the running state.
7036	Service Control Manager	The Netlogon service entered the stopped state.
7036	Service Control Manager	The File Replication Service service entered the stopped state.
7036	Service Control Manager	The Kerberos Key Distribution Center service entered the stopped state.
7036	Service Control Manager	The DNS Server service entered the stopped state.
7036	Service Control Manager	The Active Directory Domain Services service entered the stopped state.
7036	Service Control Manager	The Netlogon service entered the running state.
7040	Service Control Manager	The start type of the Active Directory Domain Services service was changed from auto start to disabled.
7036	Service Control Manager	The Netlogon service entered the stopped state.
7036	Service Control Manager	The File Replication Service service entered the running state.
29219	DirectoryServices-DSROLE-Server	Virtual domain controller cloning succeeded.
29223	DirectoryServices-DSROLE-Server	This server is now a Domain Controller.
29265	DirectoryServices-DSROLE-Server	Virtual domain controller cloning succeeded. The virtual domain controller cloning configuration file C:\Windows\NTDS\DCCloneConfig.xml has been renamed to C:\Windows\NTDS\DCCloneConfig.20120207-151533.xml.
1074	User32	The process C:\Windows\system32\lsass.exe (DC2) has initiated the restart of computer DC2 on behalf of user NT AUTHORITY\SYSTEM for the following reason: Operating System: Reconfiguration (Planned) Reason Code: 0x80020004 Shutdown Type: restart Comment: "

DCPROMO.LOG

The Dcpromo.log contains the actual promotion portion of cloning that the Directory Services event log does not describe. Since the log does not provide the level of explanation that the event log entries impart, this section of the module contains additional annotation.

The promotion process means that the cloning starts, the DC is scrubbed of its current configuration and re-promoted using the existing AD database (much like an IFM promotion), then the DC replicates inbound change deltas of AD and SYSVOL, and cloning is complete.

> ⓘ **Note**
>
> The log has been modified in this module for readability, by removing the date column.

> **Note**
>
> For further explanation of the dcpromo.log see the Understand and Troubleshoot AD DS Simplified Administration in Windows Server 2012.
> https://go.microsoft.com/fwlink/p/?LinkId=237244

- Start clone-based promotion
- Set the Directory Services Restore Mode flag so that the server does not boot back up normally as the original clone and cause naming or Directory Service collisions
- Update the Directory Services event log

```
15:14:01 [INFO] vDC Cloneing: Setting Boot into DSRM flag succeeded.
15:14:01 [WARNING] Cannot get user Token for Format Message: 1725l
15:14:01 [INFO] vDC Cloning: Created vDCCloningUpdate event.
15:14:01 [INFO] vDC Cloning: Created vDCCloningComplete event.
```

- Stop the NetLogon service so that the domain controller does not advertise

```
15:14:01 [INFO] Stopping service NETLOGON
15:14:01 [INFO] ControlService(STOP) on NETLOGON returned 1(gle=0)
15:14:01 [INFO] DsRolepWaitForService: waiting for NETLOGON to enter one of 7 st
15:14:01 [INFO] DsRolepWaitForService: QueryServiceStatus on NETLOGON returned 1
15:14:02 [INFO] DsRolepWaitForService: QueryServiceStatus on NETLOGON returned 1
15:14:02 [INFO] DsRolepWaitForService: exiting because NETLOGON entered STOPPED
15:14:02 [INFO] DsRolepWaitForService(for any end state) on NETLOGON service ret
15:14:02 [INFO] ControlService(STOP) on NETLOGON returned 0(gle=1062)
15:14:02 [INFO] Exiting service-stop loop after service NETLOGON entered STOPPED
15:14:02 [INFO] StopService on NETLOGON returned 0
15:14:02 [INFO] Configuring service NETLOGON to 1 returned 0
15:14:02 [INFO] Updating service status to 4
15:14:02 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Examine the dccloneconfig.xml file for administrator-specified customizations.
- In this sample case it is a blank file, so all settings are automatically generated and automatic IP addressing is required from the network

```
15:14:02 [INFO] vDC Cloning: Clone config file C:\Windows\NTDS\DCCloneConfig.xml
15:14:02 [INFO] vDC Cloning: Parsing clone config file C:\Windows\NTDS\DCCloneCo
```

- Validate that there are no services or programs installed that are not part of the DefaultDCCloneAllowList.xml or CustomDCCloneAllowList.xml

```
15:14:02 [INFO] vDC Cloning: Checking allowed list:
15:14:03 [INFO] vDC Cloning: Completed checking allowed list:
15:14:03 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Enable DHCP on the network adapters, since IP information was not specified by the administrator

```
15:14:03 [INFO] vDC Cloning: Enable DHCP:
15:14:03 [INFO] WMI Instance: Win32_NetworkAdapterConfiguration.Index=12
15:14:03 [INFO] Method: EnableDHCP
15:14:03 [INFO] HRESULT code: 0x0 (0)
```

```
15:14:03 [INFO] Return Value: 0x0 (0)
15:14:03 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:03 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Locate the PDC emulator
- Set the clone's site (automatically generated in this case)
- Set the clone's name (automatically generated in this case)

```
15:14:03 [INFO] vDC Cloning: Found PDC. Name: DC1.root.fabrikam.com
15:14:04 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:04 [INFO] vDC Cloning: Winlogon UI Notification #1: Domain Controller clor
15:14:05 [INFO] vDC Cloning: Winlogon UI Notification #2: Domain Controller clor
15:14:05 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:05 [INFO] Site of the cloned DC: Default-First-Site-Name
```

- Create the new clone computer object
- Rename the clone to match the new name

```
15:14:05 [INFO] vDC Cloning: Clone DC objects are created on PDC.
15:14:05 [INFO] Name of the cloned DC: DC2-CL0001
15:14:05 [INFO] DsRolepSetRegStringValue on System\CurrentControlSet\Services\NT
15:14:05 [INFO] vDC Cloning: Save CloneMachineName in registry: 0x0 (0)
```

- Provide the promotion settings, based on previous dccloneconfig.xml or automatic generation rules

```
15:14:05 [INFO] vDC Cloning: Promotion parameters setting:
15:14:05 [INFO] DNS Domain Name: root.fabrikam.com
15:14:05 [INFO] Replica Partner: \\DC1.root.fabrikam.com
15:14:05 [INFO] Site Name: Default-First-Site-Name
15:14:05 [INFO] DS Database Path: C:\Windows\NTDS
15:14:05 [INFO] DS Log Path: C:\Windows\NTDS
15:14:05 [INFO] SysVol Root Path: C:\Windows\SYSVOL
15:14:05 [INFO] Account: root.fabrikam.com\DC2-CL0001$
15:14:05 [INFO] Options: DSROLE_DC_CLONING (0x800400)
```

- Start promotion

```
15:14:05 [INFO] Promote DC as a clone
15:14:05 [INFO] vDC Cloning: Winlogon UI Notification #3: Domain Controller clor
15:14:05 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:05 [INFO] vDC Cloning: Winlogon UI Notification #4: Domain Controller clor
15:14:05 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:05 [INFO] Validate supplied paths
15:14:05 [INFO] Validating path C:\Windows\NTDS.
15:14:05 [INFO] Path is a directory
15:14:05 [INFO] Path is on a fixed disk drive.
15:14:05 [INFO] Validating path C:\Windows\NTDS.
15:14:05 [INFO] Path is a directory
15:14:05 [INFO] Path is on a fixed disk drive.
15:14:05 [INFO] Validating path C:\Windows\SYSVOL.
15:14:05 [INFO] Path is on a fixed disk drive.
15:14:05 [INFO] Path is on an NTFS volume
15:14:05 [INFO] vDC Cloning: Winlogon UI Notification #5: Domain Controller clor
15:14:05 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:05 [INFO] Start the worker task
15:14:05 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:14:05 [INFO] vDC Cloning: Winlogon UI Notification #6: Domain Controller clor
15:14:05 [INFO] Request for promotion returning 0
```

```
15:14:05 [INFO] vDC Cloning: Winlogon UI Notification #7: Domain Controller clor
15:14:05 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Stop and configure all of the AD DS-related services (NTDS, NTFRS/DFSR, KDC, DNS)

> **Note**
>
> The DNS service taking a long time to shutdown is expected in this scenario, as it is using AD-integrated zones that were no longer available even before the NTDS service stopped - see the DNS events described later in this section of the module.

```
15:14:15 [INFO] Stopping service NTDS
15:14:15 [INFO] Stopping service NtFrs
15:14:15 [INFO] ControlService(STOP) on NtFrs returned 1(gle=0)
15:14:15 [INFO] DsRolepWaitForService: waiting for NtFrs to enter one of 7 state
15:14:15 [INFO] DsRolepWaitForService: QueryServiceStatus on NtFrs returned 1 (g
15:14:16 [INFO] DsRolepWaitForService: QueryServiceStatus on NtFrs returned 1 (g
15:14:16 [INFO] DsRolepWaitForService: exiting because NtFrs entered STOPPED sta
15:14:16 [INFO] DsRolepWaitForService(for any end state) on NtFrs service returr
15:14:16 [INFO] ControlService(STOP) on NtFrs returned 0(gle=1062)
15:14:16 [INFO] Exiting service-stop loop after service NtFrs entered STOPPED st
15:14:16 [INFO] StopService on NtFrs returned 0
15:14:16 [INFO] Configuring service NtFrs to 1 returned 0
15:14:16 [INFO] Stopping service Kdc
15:14:16 [INFO] ControlService(STOP) on Kdc returned 1(gle=0)
15:14:16 [INFO] DsRolepWaitForService: waiting for Kdc to enter one of 7 states
15:14:16 [INFO] DsRolepWaitForService: QueryServiceStatus on Kdc returned 1 (gle
15:14:17 [INFO] DsRolepWaitForService: QueryServiceStatus on Kdc returned 1 (gle
15:14:17 [INFO] DsRolepWaitForService: exiting because Kdc entered STOPPED state
15:14:17 [INFO] DsRolepWaitForService(for any end state) on Kdc service returned
15:14:17 [INFO] ControlService(STOP) on Kdc returned 0(gle=1062)
15:14:17 [INFO] Exiting service-stop loop after service Kdc entered STOPPED stat
15:14:17 [INFO] StopService on Kdc returned 0
15:14:17 [INFO] Configuring service Kdc to 1 returned 0
15:14:17 [INFO] Stopping service DNS
15:14:17 [INFO] ControlService(STOP) on DNS returned 1(gle=0)
15:14:17 [INFO] DsRolepWaitForService: waiting for DNS to enter one of 7 states
15:14:17 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:18 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:19 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:20 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:21 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:22 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:23 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:24 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:25 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:26 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:27 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:28 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:29 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:30 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:31 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:32 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:33 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:34 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:35 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:36 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:37 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:38 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:39 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:40 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:41 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:42 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:43 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:44 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:45 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:46 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:47 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:48 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:49 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:50 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:51 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
```

```
15:14:52 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:53 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:54 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:55 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:56 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:57 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:58 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:14:59 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:15:00 [INFO] DsRolepWaitForService: QueryServiceStatus on DNS returned 1 (gle
15:15:00 [INFO] DsRolepWaitForService: exiting because DNS entered STOPPED state
15:15:00 [INFO] DsRolepWaitForService(for any end state) on DNS service returned
15:15:00 [INFO] ControlService(STOP) on DNS returned 0(gle=1062)
15:15:00 [INFO] Exiting service-stop loop after service DNS entered STOPPED stat
15:15:00 [INFO] StopService on DNS returned 0
15:15:00 [INFO] Configuring service DNS to 1 returned 0
15:15:00 [INFO] ControlService(STOP) on NTDS returned 1(gle=1062)
15:15:00 [INFO] DsRolepWaitForService: waiting for NTDS to enter one of 7 states
15:15:00 [INFO] DsRolepWaitForService: QueryServiceStatus on NTDS returned 1 (gl
15:15:01 [INFO] DsRolepWaitForService: QueryServiceStatus on NTDS returned 1 (gl
15:15:01 [INFO] DsRolepWaitForService: exiting because NTDS entered STOPPED stat
15:15:01 [INFO] DsRolepWaitForService(for any end state) on NTDS service returne
15:15:01 [INFO] ControlService(STOP) on NTDS returned 0(gle=1062)
15:15:01 [INFO] Exiting service-stop loop after service NTDS entered STOPPED sta
15:15:01 [INFO] StopService on NTDS returned 0
15:15:01 [INFO] Configuring service NTDS to 1 returned 0
15:15:01 [INFO] Configuring service NTDS
15:15:01 [INFO] Configuring service NTDS to 64 returned 0
15:15:01 [INFO] vDC Cloning: Winlogon UI Notification #8: Domain Controller clon
15:15:01 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:01 [INFO] vDC Cloning: Winlogon UI Notification #9: Domain Controller clon
15:15:01 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Force NT5DS (NTP) time synchronization with another domain controller (typically the PDCE)

```
15:15:02 [INFO] Forcing time sync
```

- Contact a domain controller that holds the source domain controller account of the clone
- Flush any existing Kerberos tickets

```
15:15:02 [INFO] Searching for a domain controller for the domain root.fabrikam.c
15:15:02 [INFO] Located domain controller DC1.root.fabrikam.com for domain root.
15:15:02 [INFO] vDC Cloning: Winlogon UI Notification #10: Domain Controller clo
15:15:02 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:02 [INFO] Directing kerberos authentication to DC1.root.fabrikam.com retur
15:15:02 [INFO] DsRolepFlushKerberosTicketCache() successfully flushed the Kerbe
15:15:02 [INFO] vDC Cloning: Winlogon UI Notification #11: Domain Controller clo
15:15:02 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:02 [INFO] Using site Default-First-Site-Name for server \\DC1.root.fabrika
15:15:02 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:02 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Stop the NetLogon service and set its start type

```
15:15:02 [INFO] Stopping service NETLOGON
15:15:02 [INFO] Stopping service NETLOGON
15:15:02 [INFO] vDC Cloning: Winlogon UI Notification #12: Domain Controller clo
15:15:02 [INFO] ControlService(STOP) on NETLOGON returned 1(gle=0)
15:15:02 [INFO] DsRolepWaitForService: waiting for NETLOGON to enter one of 7 st
15:15:02 [INFO] DsRolepWaitForService: QueryServiceStatus on NETLOGON returned 1
15:15:03 [INFO] DsRolepWaitForService: QueryServiceStatus on NETLOGON returned 1
15:15:03 [INFO] DsRolepWaitForService: exiting because NETLOGON entered STOPPED
15:15:03 [INFO] DsRolepWaitForService(for any end state) on NETLOGON service ret
15:15:03 [INFO] ControlService(STOP) on NETLOGON returned 0(gle=1062)
15:15:03 [INFO] Exiting service-stop loop after service NETLOGON entered STOPPED
15:15:03 [INFO] StopService on NETLOGON returned 0
```

```
15:15:03 [INFO] Configuring service NETLOGON to 1 returned 0
15:15:03 [INFO] Stopped NETLOGON
15:15:03 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:03 [INFO] vDC Cloning: Winlogon UI Notification #13: Domain Controller clo
```

- Configure the DFSR/NTFRS services to run automatically
- Delete their existing database files to force non-authoritative sync of SYSVOL when the service next starts

```
15:15:03 [INFO] Configuring service DFSR
15:15:03 [INFO] Configuring service DFSR to 256 returned 0
15:15:03 [INFO] Configuring service NTFRS
15:15:03 [INFO] Configuring service NTFRS to 256 returned 0
15:15:03 [INFO] Removing DFSR Database files for SysVol
15:15:03 [INFO] Removing FRS Database files in C:\Windows\ntfrs\jet
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\log\edb.log
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\log\edbres00001.jrs
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\log\edbres00002.jrs
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\log\edbtmp.log
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\ntfrs.jdb
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\sys\edb.chk
15:15:03 [INFO] Removed C:\Windows\ntfrs\jet\temp\tmp.edb
15:15:04 [INFO] Created system volume path
15:15:04 [INFO] Configuring service DFSR
15:15:04 [INFO] Configuring service DFSR to 128 returned 0
15:15:04 [INFO] Configuring service NTFRS
15:15:04 [INFO] Configuring service NTFRS to 128 returned 0
15:15:04 [INFO] vDC Cloning: Winlogon UI Notification #14: Domain Controller clo
15:15:04 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

- Start the promotion process using the existing NTDS database file
- Contact the RID Master

> **Note**
>
> The AD DS service is not actually installed here, this is legacy instrumentation in the log

```
15:15:04 [INFO] Installing the Directory Service
15:15:04 [INFO] Calling NtdsInstall for root.fabrikam.com
15:15:04 [INFO] Starting Active Directory Domain Services installation
15:15:04 [INFO] Validating user supplied options
15:15:04 [INFO] Determining a site in which to install
15:15:04 [INFO] Examining an existing forest...
15:15:04 [INFO] Starting a replication cycle between DC1.root.fabrikam.com and t
15:15:04 [INFO] Configuring the local computer to host Active Directory Domain S
15:15:04 [INFO] EVENTLOG (Warning): NTDS General / Service Control : 1539
Active Directory Domain Services could not disable the software-based disk write
Hard disk:
c:
Data might be lost during system failures.
15:15:10 [INFO] EVENTLOG (Informational): NTDS General / Internal Processing : 2
Duplicate event log entries were suppressed.
See the previous event log entry for details. An entry is considered a duplicate
the event code and all of its insertion parameters are identical. The time perio
this run of duplicates is from the time of the previous event to the time of thi
Event Code:
80000603
Number of duplicate entries:
2
15:15:10 [INFO] EVENTLOG (Informational): NTDS General / Internal Configuration
This Active Directory Domain Services server is disabling the Recycle Bin. Delet
```

- Change the existing invocation ID that existed in the source computers database
- Create a new NTDS Settings object for this clone

- Replicate in AD object delta from the partner domain controller

> **Note**
>
> Even though all objects are listed as replicated, this is just metadata needed to subsume the updates. All the unchanged objects in the cloned NTDS database already exist and do not require replication again, just like using IFM-based promotion.

```
15:15:10 [INFO] EVENTLOG (Informational): NTDS Replication / Replication : 1109
The invocationID attribute for this directory server has been changed. The highe
InvocationID attribute (old value):
24e7b22f-4706-402d-9b4f-f2690f730b40
InvocationID attribute (new value):
f74cefb2-89c2-442c-b1ba-3234b0ed62f8
Update sequence number:
20520
The invocationID is changed when a directory server is restored from backup medi
15:15:10 [INFO] EVENTLOG (Error): NTDS General / Internal Processing : 1168
Internal error: An Active Directory Domain Services error has occurred.
Additional Data
Error value (decimal):
2
Error value (hexadecimal):
2
Internal ID:
7011658
15:15:11 [INFO] Creating the NTDS Settings object for this Active Directory Doma
15:15:11 [INFO] Replicating the schema directory partition
15:15:11 [INFO] Replicated the schema container.
15:15:12 [INFO] Active Directory Domain Services updated the schema cache.
15:15:12 [INFO] Replicating the configuration directory partition
15:15:12 [INFO] Replicating data CN=Configuration,DC=root,DC=fabrikam,DC=com: Re
15:15:12 [INFO] Replicated the configuration container.
15:15:13 [INFO] Replicating critical domain information...
15:15:13 [INFO] Replicating data DC=root,DC=fabrikam,DC=com: Received 109 out of
15:15:13 [INFO] Replicated the critical objects in the domain container.
```

- Populate the GC partitions as needed with any missing updates
- Complete the critical AD DS portion of the promotion

```
15:15:13 [INFO] EVENTLOG (Informational): NTDS General / Global Catalog : 1110
Promotion of this domain controller to a global catalog will be delayed for the
Interval (minutes):
5
This delay is necessary so that the required directory partitions can be prepare
15:15:14 [INFO] EVENTLOG (Informational): NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.2.8225.0
15:15:15 [INFO] Creating new domain users, groups, and computer objects
15:15:16 [INFO] Completing Active Directory Domain Services installation
15:15:16 [INFO] NtdsInstall for root.fabrikam.com returned 0
15:15:16 [INFO] DsRolepInstallDs returned 0
15:15:16 [INFO] Installed Directory Service
```

- Complete the inbound replication of SYSVOL

```
15:15:16 [INFO] vDC Cloning: Winlogon UI Notification #15: Domain Controller clo
15:15:16 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:18 [INFO] Completed system volume replication
15:15:18 [INFO] vDC Cloning: Winlogon UI Notification #16: Domain Controller clo
15:15:18 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:18 [INFO] SetProductType to 2 [LanmanNT] returned 0
15:15:18 [INFO] Set the product type
15:15:18 [INFO] vDC Cloning: Winlogon UI Notification #17: Domain Controller clo
15:15:18 [INFO] vDC Cloning: Set vDCCloningUpdate event.
```

```
15:15:18 [INFO] vDC Cloning: Winlogon UI Notification #18: Domain Controller clo
15:15:18 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:18 [INFO] Set the system volume path for NETLOGON
15:15:18 [INFO] vDC Cloning: Winlogon UI Notification #19: Domain Controller clo
15:15:18 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:18 [INFO] Replicating non critical information
15:15:18 [INFO] User specified to not replicate non-critical data
15:15:18 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:18 [INFO] vDC Cloning: Winlogon UI Notification #20: Domain Controller clo
15:15:18 [INFO] Stopped the DS
15:15:18 [INFO] vDC Cloning: Set vDCCloningUpdate event.
15:15:18 [INFO] vDC Cloning: Winlogon UI Notification #21: Domain Controller clo
15:15:18 [INFO] Configuring service NTDS
15:15:18 [INFO] Configuring service NTDS to 16 returned 0
```

- Enable client DNS registration

```
15:15:18 [INFO] vDC Cloning: Set DisableDynamicUpdate reg value to 0 to enable c
15:15:18 [INFO] vDC Cloning: Set UseDynamicDns reg value to 1 to enable dynamic
15:15:18 [INFO] vDC Cloning: Set RegistrationEnabled reg value to 1 to enable dy
```

- Run the SYSPREP modules specified by the DefaultDCCloneAllowList.xml <SysprepInformation> element.

```
15:15:18 [INFO] vDC Cloning: Running sysprep providers.
15:15:32 [INFO] vDC Cloning: Completed running sysprep providers.
```

- Cloning promotion is complete
- Remove the DSRM boot flag so the server boots normally next time
- Rename the dccloneconfig.xml so that it is not read again at next bootup
- Restart the computer

```
15:15:32 [INFO] The attempted domain controller operation has completed
15:15:32 [INFO] Updating service status to 4
15:15:32 [INFO] DsRolepSetOperationDone returned 0
15:15:32 [INFO] vDC Cloning: Set vDCCloningComplete event.
15:15:32 [INFO] vDC Cloneing: Clearing Boot into DSRM flag succeeded.
15:15:32 [INFO] vDC Cloning: Winlogon UI Notification #22: Cloning Domain Contro
15:15:33 [INFO] vDC Cloning: Renamed vDC clone configuration file.
15:15:33 [INFO] vDC Cloning: The old name is: C:\Windows\NTDS\DCCloneConfig.xml
15:15:33 [INFO] vDC Cloning: The new name is: C:\Windows\NTDS\DCCloneConfig.2012
15:15:34 [INFO] vDC Cloning: Release Ipv4 on interface 'Wired Ethernet Connectio
15:15:34 [INFO] vDC Cloning: Release Ipv6 on interface 'Wired Ethernet Connectio
15:15:34 [INFO] Rebooting machine
```

Active Directory Web Services Event Log

While cloning is occurring, the NTDS.DIT database is often offline for extended periods. The ADWS service logs at least one event for this. After cloning is complete, the ADWS service starts, notes that there is not yet a valid computer certificate yet (there may or may not be, depending on your environment deploying a Microsoft PKI with auto-enrollment or not) and then starts the instance for the new domain controller.

Expand table

Event ID	Source	Message

1202	ADWS Instance Events	This computer is now hosting the specified directory instance, but Active Directory Web Services could not service it. Active Directory Web Services will retry this operation periodically. Directory instance: NTDS Directory instance LDAP port: 389 Directory instance SSL port: 636
1000	ADWS Instance Events	Active Directory Web Services is starting
1008	ADWS Instance Events	Active Directory Web Services has successfully reduced its security privileges
1100	ADWS Instance Events	The values specified in the <appsettings> section of the configuration file for Active Directory Web Services have been loaded without errors.
1400	ADWS Instance Events	ADWS Certificate Events"Active Directory Web Services could not find a server certificate with the specified certificate name. A certificate is required to use SSL/TLS connections. To use SSL/TLS connections, verify that a valid server authentication certificate from a trusted Certification Authority (CA) is installed on the machine. Certificate name: <*Server FQDN*>
1100	ADWS Instance Events	The values specified in the <appsettings> section of the configuration file for Active Directory Web Services have been loaded without errors.
1200	ADWS Instance Events	Active Directory Web Services is now servicing the specified directory instance. Directory instance: NTDS Directory instance LDAP port: 389 Directory instance SSL port: 636

DNS Server Event Log

The DNS service will experience brief expected outages while cloning occurs, as the DNS service is still running while the AD DS database is offline. This occurs if using Active Directory Integrated DNS, but not if using Standard Primary or Secondary DNS. These errors log multiple times. After cloning completes, DNS comes back online normally.

Expand table

Event ID	Source	Message
4013	DNS-Server-Service	The DNS server is waiting for Active Directory Domain Services (AD DS) to signal that the initial synchronization of the directory has been completed. The DNS server service cannot start until the initial synchronization is complete because critical DNS data might not yet be replicated onto this domain controller. If events in the AD DS event log indicate that there is a problem with DNS name resolution, consider adding the IP address of another DNS server for this domain to the DNS server list in the Internet Protocol properties of this computer. This event will be logged every two minutes until AD DS has signaled that the initial synchronization has successfully completed.
4015	DNS-Server-Service	The DNS server has encountered a critical error from the Active Directory. Check that the Active Directory is functioning properly. The extended error debug information (which may be empty) is """". The event data contains the error.
4000	DNS-Server-	The DNS server was unable to open Active Directory. This DNS server is configured to obtain and use information from the directory for this zone and is unable to load

	Service	the zone without it. Check that the Active Directory is functioning properly and reload the zone. The event data is the error code.
4013	DNS-Server-Service	The DNS server is waiting for Active Directory Domain Services (AD DS) to signal that the initial synchronization of the directory has been completed. The DNS server service cannot start until the initial synchronization is complete because critical DNS data might not yet be replicated onto this domain controller. If events in the AD DS event log indicate that there is a problem with DNS name resolution, consider adding the IP address of another DNS server for this domain to the DNS server list in the Internet Protocol properties of this computer. This event will be logged every two minutes until AD DS has signaled that the initial synchronization has successfully completed.
2	DNS-Server-Service	The DNS server has started.
4	DNS-Server-Service	The DNS server has finished the background loading of zones. All zones are now available for DNS updates and zone transfers, as allowed by their individual zone configuration.

File Replication Service Event Log

The File Replication Service synchronizes non-authoritatively from a partner during cloning. Cloning accomplishes this by deleting the NTFRS database files and leaving the contents of SYSVOL untouched, for use as pre-seeded data. The two attempts to synchronize are expected.

Expand table

Event ID	Source	Message
13562	NtFrs	Following is the summary of warnings and errors encountered by File Replication Service while polling the Domain Controller DC2.root.fabrikam.com for FRS replica set configuration information. Could not bind to a Domain Controller. Will try again at next polling cycle
13502	NtFrs	The File Replication Service is stopping.
13565	NtFrs	File Replication Service is initializing the system volume with data from another domain controller. Computer DC2 cannot become a domain controller until this process is complete. The system volume will then be shared as SYSVOL. To check for the SYSVOL share, at the command prompt, type: net share When File Replication Service completes the initialization process, the SYSVOL share will appear. The initialization of the system volume can take some time. The time is dependent on the amount of data in the system volume, the availability of other domain controllers, and the replication interval between domain controllers.
13501	NtFrs	The File Replication Service is starting
13502	NtFrs	The File Replication Service is stopping.
13503	NtFrs	The File Replication Service has stopped.
13565	NtFrs	File Replication Service is initializing the system volume with data from another domain controller. Computer DC2 cannot become a domain controller until this process is complete. The system volume will then be shared as SYSVOL. To check for the SYSVOL share, at the command prompt, type: net share When File Replication Service completes the initialization process, the SYSVOL share will appear.

		The initialization of the system volume can take some time. The time is dependent on the amount of data in the system volume, the availability of other domain controllers, and the replication interval between domain controllers.
13501	NtFrs	The File Replication Service is starting.
13553	NtFrs	The File Replication Service successfully added this computer to the following replica set: "DOMAIN SYSTEM VOLUME (SYSVOL SHARE)" Information related to this event is shown below: Computer DNS name is <*Domain Controller FQDN*> Replica set member name is <*Domain Controller*> Replica set root path is <*path*> Replica staging directory path is <*path*> Replica working directory path is <*path*>
13520	NtFrs	The File Replication Service moved the preexisting files in <path>to <*path*>\NtFrs_PreExisting___See_EventLog. The File Replication Service may delete the files in <*path*>\NtFrs_PreExisting___See_EventLog at any time. Files can be saved from deletion by copying them out of <*path*>\NtFrs_PreExisting___See_EventLog. Copying the files into c:\windows\sysvol\domain may lead to name conflicts if the files already exist on some other replicating partner. In some cases, the File Replication Service may copy a file from <*path*>\NtFrs_PreExisting___See_EventLog into <*path*> instead of replicating the file from some other replicating partner. Space can be recovered at any time by deleting the files in <*path*>\NtFrs_PreExisting___See_EventLog."
13508	NtFrs	he File Replication Service is having trouble enabling replication from \\<*Domain Controller FQDN*> to <*Domain Controller*> for <*path*> using the DNS name \\<*Domain Controller FQDN*>. FRS will keep retrying. Following are some of the reasons you would see this warning. [1] FRS cannot correctly resolve the DNS name \\<*Domain Controller FQDN*> from this computer. [2] FRS is not running on \\<*Domain Controller FQDN*>. [3] The topology information in the Active Directory Domain Services for this replica has not yet replicated to all the Domain Controllers. This event log message will appear once per connection, After the problem is fixed you will see another event log message indicating that the connection has been established.
13509	NtFrs	The File Replication Service has enabled replication from \\<*Domain Controller FQDN*> to <*Domain Controller*> for <*Path*> after repeated retries.
13516	NtFrs	The File Replication Service is no longer preventing the computer <*Domain Controller*> from becoming a domain controller. The system volume has been successfully initialized and the Netlogon service has been notified that the system volume is now ready to be shared as SYSVOL. Type "net share" to check for the SYSVOL share."

DFS Replication Event Log

The DFSR services synchronizes non-authoritatively from a partner during cloning. Cloning accomplishes this by deleting the DFSR database files and leaving the contents of SYSVOL untouched, for use as pre-seeded data. The two attempts to synchronize are expected.

Expand table

Event ID	Source	Message
1004	DFSR	The DFS Replication service has started.
1314	DFSR	The DFS Replication service successfully configured the debug log files. Additional Information: Debug Log File Path: C:\Windows\debug
6102	DFSR	The DFS Replication service has successfully registered the WMI provider
1206	DFSR	The DFS Replication service successfully contacted domain controller DC2.corp.contoso.com to access configuration information.
1210	DFSR	The DFS Replication service successfully set up an RPC listener for incoming replication requests. Additional Information: Port: 0"
4614	DFSR	The DFS Replication service initialized SYSVOL at local path C:\Windows\SYSVOL\domain and is waiting to perform initial replication. The replicated folder will remain in the initial synchronization state until it has replicated with its partner. If the server was in the process of being promoted to a domain controller, the domain controller will not advertise and function as a domain controller until this issue is resolved. This can occur if the specified partner is also in the initial synchronization state, or if sharing violations are encountered on this server or the synchronization partner. If this event occurred during the migration of SYSVOL from File Replication Service (FRS) to DFS Replication, changes will not replicate out until this issue is resolved. This can cause the SYSVOL folder on this server to become out of sync with other domain controllers. Additional Information: Replicated Folder Name: SYSVOL Share Replicated Folder ID: <*GUID*> Replication Group Name: Domain System Volume Replication Group ID: <*GUID*> Member ID: <*GUID*> Read-Only: 0
4604	DFSR	The DFS Replication service successfully initialized the SYSVOL replicated folder at local path C:\Windows\SYSVOL\domain. This member has completed initial synchronization of SYSVOL with partner dc1.corp.contoso.com. To check for the presence of the SYSVOL share, open a command prompt window and then type ""net share"". Additional Information: Replicated Folder Name: SYSVOL Share Replicated Folder ID: <*GUID*> Replication Group Name: Domain System Volume Replication Group ID: <*GUID*> Member ID: <*GUID*> Sync partner: <*domain controller FQDN*>

Troubleshooting virtualized domain controller safe restore

Tools for Troubleshooting

Logging Options

The built-in logs are the most important tool for troubleshooting issues with domain controller safe snapshot restore. All of these logs are enabled and configured for maximum verbosity, by default.

Expand table

Operation	Log
Snapshot creation	• Event viewer\Applications and services logs\Microsoft\Windows\Hyper-V-Worker
Snapshot restore	• Event viewer\Applications and services logs\Directory Service • Event viewer\Windows logs\System • Event viewer\Windows logs\Application • Event viewer\Applications and services logs\File Replication Service • Event viewer\Applications and services logs\DFS Replication • Event viewer\Applications and services logs\DNS • Event viewer\Applications and services logs\Microsoft\Windows\Hyper-V-Worker

Tools and Commands for Troubleshooting Domain Controller Configuration

To troubleshoot issues not explained by the logs, use the following tools as a starting point:

- Dcdiag.exe
- Repadmin.exe
- Network Monitor 3.4

General Methodology for Troubleshooting Domain Controller Safe Restore

1. Is the safe snapshot restore expected, but having issues?
    a. Examine the Directory Services event log
        i. Are there snapshot restore errors?
        ii. Are there AD replication errors?
    b. Examine the System event log
        i. Are there communication errors?
        ii. Are there AD errors?
2. Is the safe snapshot restore unexpected?
    a. Examine the hypervisor audit logs to determine who or what caused a rollback
    b. Contact all administrators of the hypervisor and interrogate them as to who rolled back the VM without notification
3. Is the server implementing USN rollback protection and not safely restoring?

a. Examine the Directory Services event log for an unsupported hypervisor or integration services

b. Examine the operating system and validate running Windows Server 2012?

Troubleshooting Specific Problems

Events

All virtualized domain controller safe snapshot restore events write to the Directory Services event log of the restored domain controller VM. The Application, System, File Replication Service, and DFS Replication event logs may also contain useful troubleshooting information for failed restores.

Below are the Windows Server 2012 safe restore-specific events in the Directory Services event log.

Expand table

Event ID	**2170**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Warning
Message	A Generation ID change has been detected. Generation ID cached in DS (old value):%1 Generation ID currently in VM (new value):%2 The Generation ID change occurs after the application of a virtual machine snapshot, after a virtual machine import operation or after a live migration operation. <*COMPUTERNAME*> will create a new invocation ID to recover the domain controller. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services aware backup application.
Notes and resolution	This is a success event if the snapshot was expected. If not, examine the Hyper-V-Worker event log or contact the hypervisor administrator.

Expand table

Event ID	**2174**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	The DC is neither a virtual domain controller clone nor a restored virtual domain controller snapshot.
Notes and resolution	Expected event when starting physical domain controllers or virtualized domain controllers not restored from snapshot

Expand table

Event ID	**2181**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational

Message	The transaction was aborted due to the virtual machine being reverted to a previous state. This occurs after the application of a virtual machine snapshot, after a virtual machine import operation, or after a live migration operation.
Notes and resolution	Expected when restoring a snapshot. Transactions track the VM Generation ID changing

Expand table

Event ID	**2185**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> stopped the FRS or DFSR service used to replicate the SYSVOL folder. Service name:%1 Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> must initialize a non-authoritative restore on the local SYSVOL replica. This is performed by stopping the FRS or DFSR service used to replicate the SYSVOL folder and starting it with the appropriate registry keys and values to trigger the restore. Event 2187 will be logged when FRS or DFSR service is restarted.
Notes and resolution	Expected when restoring a snapshot. All SYSVOL data on this domain controller is replaced with a partner DC's copy.
Event ID	2186
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to stop the FRS or DFSR service used to replicate the SYSVOL folder. Service name:%1 Error code:%2 Error message:%3 Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> must initialize a non-authoritative restore on the local SYSVOL replica. This is done by stopping the FRS or DFSR replication service used to replicate the SYSVOL folder and then starting it with the appropriate registry keys and values to trigger the restore. <*COMPUTERNAME*> failed to stop the current running service and cannot complete the non-authoritative restore. Please perform a non-authoritative restore manually.
Notes and resolution	Examine the System, FRS and DFSR event logs for further information.

Expand table

Event ID	**2187**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> started the FRS or DFSR service used to replicate the SYSVOL folder. Service name:%1 Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> needed to initialize a non-authoritative restore on the local SYSVOL replica. This was done by stopping the FRS or DFSR service

	used to replicate the SYSVOL folder and starting it with the appropriate registry keys and values to trigger the restore.
Notes and resolution	Expected when restoring a snapshot. All SYSVOL data on this domain controller is replaced with a partner DC's copy.

Expand table

Event ID	**2188**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to start the FRS or DFSR service used to replicate the SYSVOL folder. Service name:%1 Error code:%2 Error message:%3 Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> needs to initialize a non-authoritative restore on the local SYSVOL replica. This is done by stopping the FRS or DFSR service used to replicate the SYSVOL and starting it with appropriate registry keys and values to trigger the restore. <*COMPUTERNAME*> failed to start the FRS or DFSR service used to replicate the SYSVOL folder and cannot complete the non-authoritative restore. Please perform a non-authoritative restore manually and restart the service.
Notes and resolution	Examine the System, FRS and DFSR event logs for further information.

Expand table

Event ID	**2189**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> set the following registry values to initialize SYSVOL replica during a non-authoritative restore: Registry Key:%1 Registry Value: %2 Registry Value data: %3 Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> needs to initialize a non-authoritative restore on the local SYSVOL replica. This is done by stopping the FRS or DFSR service used to replicate the SYSVOL folder and starting it with the appropriate registry keys and values to trigger the restore.
Notes and resolution	Expected when restoring a snapshot. All SYSVOL data on this domain controller is replaced with a partner DC's copy.

Expand table

Event ID	**2190**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to set the following registry values to initialize the SYSVOL replica during a non-authoritative restore: Registry Key:%1

	Registry Value: %2 Registry Value data: %3 Error code:%4 Error message:%5 Active Directory detected that the virtual machine that hosts the domain controller role was reverted to a previous state. <*COMPUTERNAME*> needs to initialize a non-authoritative restore on the local SYSVOL replica. This is done by stopping the FRS or DFSR service used to replicate the SYSVOL folder and starting it with the appropriate registry keys and values to trigger the restore. <*COMPUTERNAME*> failed to set the above registry values and cannot complete the non-authoritative restore. Please perform a non-authoritative restore manually.
Notes and resolution	Examine Application and System event logs. Investigate third party applications that may be blocking registry updates.

Expand table

Event ID	**2200**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> initializes replication to bring the domain controller current. Event 2201 will be logged when the replication is finished.
Notes and resolution	Expected when restoring a snapshot. Marks the beginning of inbound AD replication.

Expand table

Event ID	**2201**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> has finished replication to bring the domain controller current.
Notes and resolution	Expected when restoring a snapshot. Marks the end of inbound AD replication.

Expand table

Event ID	**2202**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> failed replication to bring the domain controller up-to-date. The domain controller will be updated after next periodic replication.
Notes and resolution	Examine the Directory Services and System event logs. Use repadmin.exe to attempt forcing replication and note any failures.

Expand table

Event ID	**2204**
Source	Microsoft-Windows-ActiveDirectory_DomainService

Severity	Informational
Message	<*COMPUTERNAME*> has detected a change of virtual machine generation ID. The change means that the virtual domain controller has been reverted to a previous state. <*COMPUTERNAME*> will perform the following operations to protect the reverted domain controller against possible data divergence and to protect creation of security principals with duplicate SIDs: Create a new invocation ID Invalidate current RID pool Ownership of the FSMO roles will be validated at next inbound replication. During this window if the domain controller held a FSMO role, that role will be unavailable. Start SYSVOL replication service restore operation. Start replication to bring the reverted domain controller to the most current state. Request a new RID pool.
Notes and resolution	Expected when restoring a snapshot. This explains all the various reset operations that will occur as part of the safe restore process.

Expand table

Event ID	**2205**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> invalidated current RID pool after virtual domain controller was reverted to previous state.
Notes and resolution	Expected when restoring a snapshot. The local RID pool must be destroyed as the domain controller has time travelled and they may have already been issued.

Expand table

Event ID	**2206**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	ERROR
Message	<*COMPUTERNAME*> failed to invalidate current RID pool after virtual domain controller was reverted to previous state. Additional data: Error code: %1 Error value: %2
Notes and resolution	Examine the Directory Services and System event logs. Validate that the RID Master is online can be reached from this server using Dcdiag.exe /test:ridmanager

Expand table

Event ID	**2207**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	ERROR
Message	<*COMPUTERNAME*> failed to restore after virtual domain controller was reverted to previous state. A reboot into DSRM was requested. Please check previous events for more information.
Notes and resolution	Examine the Directory Services and System event logs.

Expand table

Event ID	**2208**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Informational
Message	<*COMPUTERNAME*> deleted DFSR databases to initialize SYSVOL replica during a non-authoritative restore.
Notes and resolution	Expected when restoring a snapshot. This guarantees DFSR non-authoritatively synchronizes SYSVOL from a partner DC. Note that any other DFSR Replicated Folders on the same volume as SYSVOL will also non-authoritatively sync (domain controllers are not recommended to host custom DFSR sets on the same volume as SYSVOL).

Expand table

Event ID	**2209**
Source	Microsoft-Windows-ActiveDirectory_DomainService
Severity	Error
Message	<*COMPUTERNAME*> failed to delete DFSR databases. Additional data: Error code: %1 Error value: %2 Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. <*COMPUTERNAME*> needs to initialize a non-authoritative restore on the local SYSVOL replica. For DFSR, this is done by stopping the DFSR service, deleting DFSR databases, and re-starting the service. Upon restarting DFSR will rebuild the databases and start the initial sync.
Notes and resolution	Examine the DFSR event log.

Error Messages

There are no direct interactive errors for failed virtualized domain controller safe snapshot restore; all cloning information logs in the Directory Services event logs. Naturally, any critical replication or server advertising errors manifest themselves as symptoms elsewhere.

Known Issues and Support Scenarios

The General Methodology for Troubleshooting Domain Controller Safe Restore section and events listed in Troubleshooting Specific Problems are usually adequate to troubleshoot most issues.

Expand table

Issue	**Cannot create new security principals on recently safe restored domain controller**
Symptoms	After restoring a snapshot, attempts to create a new security principal (user, computer, group) on that domain controller fail with: Error 0x2010 The directory service was unable to allocate a relative identifier.
Resolution and Notes	This issue is caused by the restored computer's stale knowledge of the RID Master FSMO role. If the role moved to this or another domain controller after a snapshot was taken and then later restored, the restored domain controller will not have knowledge of the RID master until initial replication has completed.

	To resolve the issue, allow AD replication to complete inbound to the restored domain controller. If still not working, validate that all domain controllers have the same correct knowledge of which DC hosts the RID Master.

Expand table

Issue	Restored domain controllers do not share SYSVOL, advertise
Symptoms	After restoring a snapshot, one or more DCs do not advertise, do not share sysvol, and do not have up to date SYSVOL contents
Resolution and Notes	The DC's upstream partners do not have a working SYSVOL replica that is correctly replicating with DFSR or FRS. This issue is unrelated to safe restore but is likely to manifest as a safe restore issue, because the customer was unaware of the other replication issue affecting un-restored DCs

Advanced Troubleshooting

This module seeks to teach advanced troubleshooting by using *working* logs as samples, with some explanation of what occurred. If you understand what a successful virtualized domain controller operation looks like, failures become obvious in your environment. These logs are presented by their source, with the ascending order of *expected* events related to a cloned domain controller within each log.

Restoring a Domain Controller that Replicates SYSVOL Using DFSR

Directory Services Event Log

The Directory Services log contains the majority of safe restore operational information. The hypervisor changes the VM-Generation ID and the NTDS service notes it, then invalidates the RID pool and changes the invocation ID. The new VM-Generation ID is set and the servers replicates AD data inbound. The DFSR service is stopped and its database that hosts SYSVOL is deleted, forcing a non-authoritative sync inbound. The USN high watermark is adjusted.

Expand table

Event ID	Source	Message
2170	ActiveDirectory_DomainService	A Generation ID change has been detected. Generation ID cached in DS (old value): <*number*> Generation ID currently in VM (new value): <*number*> The Generation ID change occurs after the application of a virtual machine snapshot, after a virtual machine import operation or after a live migration operation. Active Directory Domain Services will create a new invocation ID to recover the domain controller. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services aware backup application."
2181	ActiveDirectory_DomainService	The transaction was aborted due to the virtual machine being reverted to a previous state. This occurs after the application

		of a virtual machine snapshot, after a virtual machine import operation, or after a live migration operation.
2204	ActiveDirectory_DomainService	Active Directory Domain Services has detected a change of virtual machine generation ID. The change means that the virtual domain controller has been reverted to a previous state. Active Directory Domain Services will perform the following operations to protect the reverted domain controller against possible data divergence and to protect creation of security principals with duplicate SIDs: Create a new invocation ID Invalidate current RID pool Ownership of the FSMO roles will be validated at next inbound replication. During this window if the domain controller held a FSMO role, that role will be unavailable. Start SYSVOL replication service restore operation. Start replication to bring the reverted domain controller to the most current state. Request a new RID pool."
2181	ActiveDirectory_DomainService	The transaction was aborted due to the virtual machine being reverted to a previous state. This occurs after the application of a virtual machine snapshot, after a virtual machine import operation, or after a live migration operation.
1109	ActiveDirectory_DomainService	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): *<GUID>* InvocationID attribute (new value): *<GUID>* Update sequence number: *<number>* The invocationID is changed when a directory server is restored from backup media, is configured to host a writeable application directory partition, has been resumed after a virtual machine snapshot has been applied, after a virtual machine import operation, or after a live migration operation. Virtualized domain controllers should not be restored using virtual machine snapshots. The supported method to restore or rollback the content of an Active Directory Domain Services database is to restore a system state backup made with an Active Directory Domain Services-aware backup application."
2179	ActiveDirectory_DomainService	The msDS-GenerationId attribute of the Domain Controller's computer object has been set to the following parameter: GenerationID attribute: *<number>*
2200	ActiveDirectory_DomainService	Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. Active Directory Domain Services initializes replication to bring the domain controller current. Event 2201 will be logged when the replication is finished.
2201	ActiveDirectory_DomainService	Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. Active Directory Domain Services has finished replication to bring the domain controller current.

2185	ActiveDirectory_DomainService	Active Directory Domain Services stopped the FRS or DFSR service used to replicate the SYSVOL folder. Service name: DFSR Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. Active Directory Domain Services must initialize a non-authoritative restore on the local SYSVOL replica. This is performed by stopping the FRS or DFSR service used to replicate the SYSVOL folder and starting it with the appropriate registry keys and values to trigger the restore. Event 2187 will be logged when FRS or DFSR service is restarted."
2208	ActiveDirectory_DomainService	Active Directory Domain Services deleted DFSR databases to initialize SYSVOL replica during a non-authoritative restore. Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. Active Directory Domain Services needs to initialize a non-authoritative restore on the local SYSVOL replica. For DFSR, this is done by stopping the DFSR service, deleting DFSR databases, and re-starting the service. Upon restarting DFSR will rebuild the databases and start the initial sync. "
2187	ActiveDirectory_DomainService	Active Directory Domain Services started the FRS or DFSR service used to replicate the SYSVOL folder. Service name: DFSR Active Directory detected that the virtual machine that hosts the domain controller was reverted to a previous state. Active Directory Domain Services needed to initialize a non-authoritative restore on the local SYSVOL replica. This was done by stopping the FRS or DFSR service used to replicate the SYSVOL folder and starting it with the appropriate registry keys and values to trigger the restore. "
1587	ActiveDirectory_DomainService	This directory service has been restored or has been configured to host an application directory partition. As a result, its replication identity has changed. A partner has requested replication changes using our old identity. The starting sequence number has been adjusted. The destination directory service corresponding to the following object GUID has requested changes starting at a USN that precedes the USN at which the local directory service was restored from backup media. Object GUID: *<GUID> (<FQDN of partner domain controller>)* USN at the time of restore: *<number>* As a result, the up-to-dateness vector of the destination directory service has been configured with the following settings. Previous database GUID: *<GUID>* Previous object USN: *<number>* Previous property USN:

<*number*>

New database GUID:

<*GUID*>

New object USN:

<*number*>

New property USN:

<*number*>

System Event Log

The System event log notes that the machine time that occurs when bringing an offline virtual machine back online and synchronizing with host time. The RID pool invalidates and the DFSR or FRS services are restarted.

Expand table

Event ID	Source	Message
1	Kernel-General	The system time has changed to <*now*> from <*snapshot time/date*>. Change Reason: An application or system component changed the time.
16654	Directory-Services-SAM	A pool of account-identifiers (RIDs) has been invalidated. This may occur in the following expected cases: 1. A domain controller is restored from backup. 2. A domain controller running on a virtual machine is restored from snapshot. 3. An administrator has manually invalidated the pool. See https://go.microsoft.com/fwlink/?LinkId=226247 for more information.
7036	Service Control Manager	The DFS Replication service entered the stopped state.
7036	Service Control Manager	The DFS Replication service entered the running state.

Application Event Log

The Application event log notes the DFSR database stopping and starting.

Expand table

Event ID	Source	Message
103	ESENT	DFSRs (1360) \\.\C:\System Volume Information\DFSR\database_<*GUID*>\dfsr.db: The database engine stopped the instance (0). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.141, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.016, [12] 0.000, [13] 0.000, [14] 0.000, [15] 0.000.
102	ESENT	DFSRs (532) \\.\C:\System Volume Information\DFSR\database_<*GUID*>\dfsr.db: The database engine (6.02.8189.0000) is starting a new instance (0).

105	ESENT	DFSRs (532) \\.\C:\System Volume Information\DFSR\database_<*GUID*>\dfsr.db: The database engine started a new instance (0). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.031, [10] 0.000, [11] 0.000.
		DFSRs (532) \\.\C:\System Volume Information\DFSR\database_<*GUID*>\dfsr.db: The database engine created a new database (1, \\.\C:\System Volume Information\DFSR\database_<*GUID*>\dfsr.db). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.016, [4] 0.062, [5] 0.000, [6] 0.016, [7] 0.000, [8] 0.000, [9] 0.015, [10] 0.000, [11] 0.000.

DFS Replication Event Log

The DFSR service is stopped and the database that contains SYSVOL is deleted, forcing a non-authoritative synchronization inbound.

Expand table

Event ID	Source	Message
1006	DFSR	The DFS Replication service is stopping.
1008	DFSR	The DFS Replication service has stopped.
1002	DFSR	The DFS Replication service is starting.
1004	DFSR	The DFS Replication service has started.
1314	DFSR	The DFS Replication service successfully configured the debug log files. Additional Information: Debug Log File Path: C:\Windows\debug
6102	DFSR	The DFS Replication service has successfully registered the WMI provider.
1206	DFSR	The DFS Replication service successfully contacted domain controller <*domain controller FQDN*> to access configuration information.
1210	DFSR	The DFS Replication service successfully set up an RPC listener for incoming replication requests. Additional Information: Port: 0
4614	DFSR	The DFS Replication service initialized SYSVOL at local path C:\Windows\SYSVOL\domain and is waiting to perform initial replication. The replicated folder will remain in the initial synchronization state until it has replicated with its partner. If the server was in the process of being promoted to a domain controller, the domain controller will not advertise and function as a domain controller until this issue is resolved. This can occur if the specified partner is also in the initial synchronization state, or if sharing violations are encountered on this server or the synchronization partner. If this event occurred during the migration of SYSVOL from File Replication Service (FRS) to DFS Replication, changes will not replicate out until this issue is resolved. This can cause the SYSVOL folder on this server to become out of sync with other domain controllers. Additional Information: Replicated Folder Name: SYSVOL Share Replicated Folder ID: <*GUID*> Replication Group Name: Domain System Volume Replication Group ID: <*GUID*> Member ID: <*GUID*>

		Read-Only: 0
4604	DFSR	The DFS Replication service successfully initialized the SYSVOL replicated folder at local path C:\Windows\SYSVOL\domain. This member has completed initial synchronization of SYSVOL with partner dc1.corp.contoso.com. To check for the presence of the SYSVOL share, open a command prompt window and then type "net share". Additional Information: Replicated Folder Name: SYSVOL Share Replicated Folder ID: <*GUID*> Replication Group Name: Domain System Volume Replication Group ID: <*GUID*> Member ID: <*GUID*> Sync partner: <*partner domain controller FQDN*>

Restoring a Domain Controller that Replicates SYSVOL Using FRS

The File Replication Event log is used instead of the DFSR event log in this case. The Application event log also writes different FRS-related events. Otherwise, the Directory Services and System Event log messages are generally the same and in the same order as previously described.

File Replication Service Event Log

The FRS service is stopped and restarted with a D2 BURFLAGS value to non-authoritatively synchronize SYSVOL.

Expand table

Event ID	Source	Message
13502	NTFRS	The File Replication Service is stopping.
13503	NTFRS	The File Replication Service has stopped.
13501	NTFRS	The File Replication Service is starting
13512	NTFRS	The File Replication Service has detected an enabled disk write cache on the drive containing the directory c:\windows\ntfrs\jet on the computer DC4. The File Replication Service might not recover when power to the drive is interrupted and critical updates are lost.
13565	NTFRS	File Replication Service is initializing the system volume with data from another domain controller. Computer DC4 cannot become a domain controller until this process is complete. The system volume will then be shared as SYSVOL. To check for the SYSVOL share, at the command prompt, type: net share When File Replication Service completes the initialization process, the SYSVOL share will appear. The initialization of the system volume can take some time. The time is dependent on the amount of data in the system volume, the availability of other domain controllers, and the replication interval between domain controllers."
13520	NTFRS	The File Replication Service moved the preexisting files in <*path*> to <*path*>\NtFrs_PreExisting___See_EventLog.

		The File Replication Service may delete the files in <*path*>\NtFrs_PreExisting___See_EventLog at any time. Files can be saved from deletion by copying them out of <*path*>\NtFrs_PreExisting___See_EventLog. Copying the files into <*path*> may lead to name conflicts if the files already exist on some other replicating partner. In some cases, the File Replication Service may copy a file from <*path*>\NtFrs_PreExisting___See_EventLog into <*path*> instead of replicating the file from some other replicating partner. Space can be recovered at any time by deleting the files in <*path*>\NtFrs_PreExisting___See_EventLog.
13553	NTFRS	The File Replication Service successfully added this computer to the following replica set: "DOMAIN SYSTEM VOLUME (SYSVOL SHARE)" Information related to this event is shown below: Computer DNS name is "<*domain controller FQDN*>" Replica set member name is "<*domain controller name*>" Replica set root path is "<*path*>" Replica staging directory path is "<*path*> " Replica working directory path is "<*path*>"
13554	NTFRS	The File Replication Service successfully added the connections shown below to the replica set: "DOMAIN SYSTEM VOLUME (SYSVOL SHARE)" Inbound from "<*partner domain controller FQDN*>" Outbound to "<*partner domain controller FQDN*>" More information may appear in subsequent event log messages.
13516	NTFRS	The File Replication Service is no longer preventing the computer DC4 from becoming a domain controller. The system volume has been successfully initialized and the Netlogon service has been notified that the system volume is now ready to be shared as SYSVOL. Type "net share" to check for the SYSVOL share.

Application Event Log

The FRS database stops and starts, and is purged due to the D2 BURFLAGS operation.

Expand table

Event ID	Source	Message
327	ESENT	ntfrs (1424) The database engine detached a database (1, c:\windows\ntfrs\jet\ntfrs.jdb). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.015, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.516, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.063, [12] 0.000. Revived Cache: 0
103	ESENT	ntfrs (1424) The database engine stopped the instance (0). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.031, [10] 0.000, [11] 0.016, [12] 0.000, [13] 0.000, [14] 0.047, [15] 0.000.

102	ESENT	ntfrs (3000) The database engine (6.02.8189.0000) is starting a new instance (0).
105	ESENT	ntfrs (3000) The database engine started a new instance (0). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.062, [10] 0.000, [11] 0.141.
103	ESENT	ntfrs (3000) The database engine stopped the instance (0). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000, [13] 0.015, [14] 0.000, [15] 0.000.
102	ESENT	ntfrs (3000) The database engine (6.02.8189.0000) is starting a new instance (0).
105	ESENT	ntfrs (3000) The database engine started a new instance (0). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.078, [10] 0.000, [11] 0.109.
325	ESENT	ntfrs (3000) The database engine created a new database (1, c:\windows\ntfrs\jet\ntfrs.jdb). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.016, [4] 0.016, [5] 0.000, [6] 0.015, [7] 0.000, [8] 0.000, [9] 0.078, [10] 0.016, [11] 0.000.
103	ESENT	ntfrs (3000) The database engine stopped the instance (0). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.078, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.125, [10] 0.016, [11] 0.000, [12] 0.000, [13] 0.000, [14] 0.000, [15] 0.000.
102	ESENT	ntfrs (3000) The database engine (6.02.8189.0000) is starting a new instance (0).
105	ESENT	ntfrs (3000) The database engine started a new instance (0). (Time=0 seconds) Internal Timing Sequence: [1] 0.016, [2] 0.000, [3] 0.000, [4] 0.094, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.032, [10] 0.000, [11] 0.000.
326	ESENT	ntfrs (3000) The database engine attached a database (1, c:\windows\ntfrs\jet\ntfrs.jdb). (Time=0 seconds) Internal Timing Sequence: [1] 0.000, [2] 0.015, [3] 0.000, [4] 0.000, [5] 0.016, [6] 0.015, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000. Saved Cache: 1