20

Active Directory Troubleshooting

Like any other IT engineer, I remember spending long and sleepless nights fixing systems. I remember working on weekends to fix critical issues. Even though we do not like it, as engineers, we spend most of our time *fixing* something.

In order to troubleshoot an issue and find a solution, we first need to have relevant knowledge about the application or the service. You do not need to be a master of everything but you should at least have enough knowledge to begin the troubleshooting process. Then, we need to collect the relevant telemetry data that could help us to understand the situation. This can be in the form of logs, events, screenshots, or discussions. The next stage is to analyze the collected data and try to find a solution.

I have been involved in many interviews over the past few years. As a part of interviews, I usually ask the candidate a few scenario-based questions. After I explain the scenario, I always say that I do not need an exact answer. All I care about is the approach they would take to find a solution. To become a good troubleshooter, the starting point of the troubleshooting process is crucial. When we are troubleshooting a problem, we may have a lot of information from logs, users, and monitoring systems to process. Also, based on the impact, we will have pressure from the business end too. So, engineers have to deal with all this and still choose the correct approach. Knowledge and experience can be gained, but knowing the basics will help engineers to come up with the correct approach to solve the issue.

In this chapter, we are going to look at the most common errors that can occur in an on-prem **Active Directory** (**AD**) environment and what steps we can take to troubleshoot/fix them. The issues will be categorized under the following topics:

- Troubleshooting **Active Directory Domain Services** (**AD DS**) replication issues
- Troubleshooting Group Policy issues
- Troubleshooting replication issues
- Troubleshooting Azure AD Connect issues
- **Distributed File System** (**DFS**) replication issues
- Troubleshooting AD DS database issues

Healthy replication is a primary requirement of an Active Directory environment. So, let's go ahead and start this chapter by looking into common replication issues.

Troubleshooting AD DS replication issues

An Active Directory environment with replication issues is a disaster; it can cause all sorts of problems. Active Directory uses a multi-master database. A change made on one domain controller should be advertised to other domain controllers to maintain consistency. The two types of replication in an Active Directory environment are as follows:

- **Intra-site replication**: Replication between domain controllers in the same Active Directory site
- **Inter-site replication**: Replication between domain controllers in different Active Directory sites

In *Chapter 11*, *Active Directory Services*, we looked at exactly how both types of replication work. I encourage you to refer to it for more details.

There is no smoke without fire. When there are replication issues, we can see the following symptoms in the infrastructure:

- New user accounts experience authentication issues with their systems and applications.
- Once a password is updated, user accounts get locked out frequently.
- After a password is reset, AD-integrated applications fail to authenticate users.
- When an object attribute value is modified, not every domain controller can see it.
- When a new Group Policy is created, it only applies to some of the target objects.
- When there is a Group Policy change, it doesn't apply to the target object group, or it only applies to a part of the group.
- When an AD object is removed using one domain controller, it still appears on other domain controllers.
- DNS name resolution issues.

The above list contains the most common replication issues, but that's not all. Depending on the complexity of the environment, you may notice more complicated issues.

Identifying replication issues

When we have a fever, it could be just a cold or a symptom of a different health issue. If it does not go away with paracetamol, then we need to go for a diagnosis to find the problem. When you walk into a GP's, they collect some reports and evidence before they come to a conclusion. Likewise, once we see the aforementioned symptoms, we need to collect data and evidence, which can help us to find the root cause. There are a few tools and methods we can use for that.

Event Viewer

Event Viewer is the most commonly used tool to gather information about any application or service-related issue. Active Directory replication issues will also log certain events in Event Viewer.

Some of them will help us to identify the root cause directly and some will only provide insights that we will need to follow with additional troubleshooting steps:

Event ID	Event description	Possible issues
`2087, 2088`	AD could not resolve the following DNS hostname of the source domain controller to an IP address. This error prevents additions, deletions, and changes in AD DS from replicating between one or more domain controllers in the forest. Security groups, Group Policy, users, computers, and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting login authentication and access to network resources.	• The source domain controller is in shutdown status or non-responsive status. • There is a network-layer communication issue between the source and destination domain controllers. • Due to a hardware or software failure, the source domain controller cannot be brought online. In such a situation, a metadata cleanup is required and we need to remove the relevant entries forcibly from Active Directory. • There are DNS-related issues preventing name resolution.
`1844`	The local domain controller could not connect with the following domain controller, which is hosting the following directory partition to resolve distinguished names.	• The source domain controller is in shutdown status or non-responsive status. • There is a network-layer communication issue between the source and destination domain controllers. • Domain controller **service resource records** (**SRV**) are not registered with the DNS server. • It's recommended to test the DNS name resolution and see whether the domain controller name can be resolved properly. • It's recommended to try forcible replication of the directory partition using `repadmin /replicate` to confirm whether it's a temporary issue or not.

`4013`	The DNS server is waiting for AD DS to signal that the initial synchronization of the directory has been completed. The DNS 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, then consider adding the IP address of another DNS server for this domain to the DNS server list in the **Internet Protocol** (**IP**) properties of this computer. This event will be logged every two minutes until AD DS has signaled that the initial synchronization has successfully completed.	• The domain controller is using the wrong IP range or VLAN, which prevents communication with the replication partner. • A network-layer communication issue between hosts. • DNS name resolution issues.
`1925`	The attempt to establish a replication link for the following writable directory partition failed.	• A network-layer communication issue between hosts. • DNS name resolution issues. • The source domain controller is in shutdown status or non-responsive status. • Check the maximum TCP packet size (you can use the `ping` command with the `-f -l` parameters) and verify compatibility with devices and network configuration.

`1311`	The **Knowledge Consistency Checker** (**KCC**) has detected problems with the following directory partition. **Directory partition**: %1. There is insufficient site connectivity information for the KCC to create a spanning tree replication topology. Or, one or more directory servers with this directory partition are unable to replicate the directory partition information. This is probably due to inaccessible directory servers.	• There are network communication issues between AD sites. • Verify that the domain controllers that host the identified directory partition are accessible using `dcdiag /test:connectivity`.
`8524`	The DSA operation is unable to proceed because of a DNS lookup failure.	• Due to hardware or software failure, the source domain controller cannot be brought online. In such a situation, a metadata cleanup is required. • DNS name resolution issues. • Verify that the A and CNAME records exist for the source domain controller.
`8456, 8457`	The operation failed because AD could not transfer the remaining data in the directory partition (`<directory partition DN path>`) to the domain controller (`<destination DC>`). The source server is currently rejecting replication requests.	• The **Directory System Agent** (**DSA**) is not writable. Check the relevant registry keys at `KLM\System\CurrentControlSet\Services\NTDS\Parameters`. • Insufficient disk space. • The Netlogon service has crashed or is in a paused status in the source.

`8453`	Replication access was denied.	• The `UserAccountControl` attribute on the destination domain controller computer account is missing. It is either the `SERVER_TRUST_ACCOUNT` or the `TRUSTED_FOR_DELEGATION` flag. • The default permissions of Active Directory partitions have been altered. • The destination domain controller is a **Read-Only Domain Controller** (**RODC**) and ADPREP/RODCPREP wasn't executed. Or, the enterprise RODC group does not have directory change replication permissions for the partition that is failing to replicate. • Trust relationships are no longer valid. • There is a time difference between the domain controllers that exceeds the maximum time skew allowed.
`1722`	The RPC server is unavailable.	• System resource limitation. • IP stack issue. • DNS service issues. • Network routing issues. • Relevant TCP ports are blocked by a firewall or application.
`1127`	AD could not replicate the directory partition (`<DN path of failing partition>`) from the remote domain controller (`<fully qualified computer name of helper DC>`). While accessing the hard disk, a disk operation failed, even after retries.	• An application or corrupted system component is preventing AD from writing data to a hard disk. • Hard disk faults. • Firmware issues related to disk controllers.

`1645`	`AD_TERM` did not perform an authenticated **Remote Procedure Call** (**RPC**) to another directory server because the desired **Service Principal Name** (**SPN**) for the destination directory server is not registered on the **Key Distribution Center** (**KDC**) domain controller that resolves the SPN. Destination directory server: %1 SPN: %2	This can be due to a recent change to the domain controller, such as domain promotion or demotion. Force replication using `repadmin /syncall` and check the registered SPN values.

System Center Operations Manager (SCOM)

SCOM can be used to proactively and reactively monitor the health of AD DS and related components. We need the relevant management packs to do it. The latest management packs for AD DS are available at `https://bit.ly/3qZN4OS`. If you're running SCOM 2016/2019, then you do not need to install this manually. Once domain controllers are added to the monitoring, the system will scan and recommend which management packs to install. Once the relevant management packs are in place, they can identify issues related to the following:

- Replication
- **Lightweight Directory Access Protocol** (**LDAP**)
- The domain controller locator
- Trusts
- The Netlogon service
- **File Replication Service** (**FRS**)
- DFS Replication
- The Intersite Messaging service
- The Windows Time service
- **Active Directory Web Services** (**AD WS**)
- **Active Directory Management Gateway Service** (**AD MGS**)
- The KDC

Also, SCOM can monitor service availability, collect key performance data, and provide reports.

The findings from management packs will be notified in the form of alerts.

We can also automate some of the recovery tasks by binding alerts to runbooks via System Center Orchestrator.

Troubleshooting replication issues

There are certain Windows cmdlets and utilities that we can use for replication issue troubleshooting purposes. Among these, `Repadmin.exe` is the most commonly used Microsoft utility to troubleshoot Active Directory replication issues. It is available in servers that have the AD DS or AD LDS role installed. It is also part of the **Remote Server Administration Tools** (**RSAT**). It is recommended to run this utility as a Domain Admin or Enterprise Admin. However, it is also possible to delegate permissions to only review and manage replication.

> Microsoft also has a great little utility called **Active Directory Replication Status Tool** (**ADREPLSTATUS**), which allows us to review the replication status of an AD environment. We can download it via `https://bit.ly/3HP0pzu`.

The following list contains the commands supported by `repadmin`:

Command	**Description**
`repadmin /kcc`	Forces the KCC on targeted domain controllers to immediately recalculate the inbound replication topology.
`repadmin /prp`	Allows an administrator to view or modify the password replication policy for RODCs.
`repadmin /queue`	Displays inbound replication requests that the domain controller must issue in order to become consistent with its source replication partners.
`repadmin /replicate`	Triggers the immediate replication of the specified directory partition to a domain controller.
`repadmin /replsingleobj`	Replicates a single object between any two domain controllers that have common directory partitions.
`repadmin /replsummary`	Quickly and concisely summarizes the replication state and relative health of a forest.
`repadmin /rodcpwdrepl`	Triggers the replication of passwords for specific users from the source domain controller to one or more RODC.

`repadmin /showattr`	Displays the attributes of an object.
`repadmin /showobjmeta`	Displays the replication metadata for a specified object stored in AD, such as attribute ID, version number, originating and local **Update Sequence Numbers** (**USNs**), and the originating server's **Globally Unique Identifier** (**GUID**), datestamp, and timestamp.
`repadmin /showrepl`	Displays the replication status of the last attempted inbound replication on AD partitions.
`repadmin /showutdvec`	Displays the highest committed USN that the targeted domain controller shows as committed for itself and its transitive partners.
`repadmin /syncall`	Synchronizes a specified domain controller with all replication partners.

Let's see some of these commands in action.

As listed in the preceding table, we can use `repadmin/replsummary` to summarize the following command of the replication status for all domain controllers based on the replication destination:

```
repadmin /replsummary /bydest
```

The following command summarizes the replication status for all domain controllers based on the replication source:

```
repadmin /replsummary /bysrc
```

The following command shows the replication partners for `REBEL-SRV01.therebeladmin.com` and the status of the last sync attempt:

```
repadmin /showrepl REBEL-SRV01.therebeladmin.com
```

The following command lists the replication partners that have replication errors (the last sync attempt failed):

```
repadmin /showrepl /errorsonly
```

We also can view the results in CSV format:

```
repadmin /showrepl /csv
```

The following command initiates domain directory partition synchronization with all replication partners of `REBEL-SRV01`:

```
repadmin /syncall REBEL-SRV01 dc=therebeladmin,dc=com
```

It also reports whether there were any issues during synchronization.

The following command shows whether there are any unprocessed inbound replication requests. If the system keeps sending queue requests, then it can be due to a high number of Active Directory changes, system resource issues, or too many replication partners:

```
repadmin /queue
```

The following command lists the changes that are not replicated between the REBELNET-PDC01 and REBEL-SRV01 servers:

```
repadmin /showchanges REBELNET-PDC01 d3f89917-5fff-40a8-scc2-b148b60d9309
dc=therebeladmin,dc=com
```

Here, REBEL-SRV01 is the source server and it is listed with the object's GUID.

The following command initiates immediate directory partition replication from REBELNET-PDC01 to REBEL-SRV01:

```
repadmin /replicate REBEL-SRV01 REBELNET-PDC01 dc=therebeladmin,dc=com
```

Apart from repadmin, there are certain PowerShell cmdlets that we can use to troubleshoot replication issues. The Get-ADReplicationFailure cmdlet is one that can collect information about replication failures.

The following command collects information about replication failures associated with REBEL-SRV01:

```
Get-ADReplicationFailure -Target REBEL-SRV01
```

This can also be done with multiple servers:

```
Get-ADReplicationFailure -Target REBEL-SRV01,REBELNET-PDC01
```

Furthermore, we can target all the domain controllers in the domain:

```
Get-ADReplicationFailure -Target "therebeladmin.com" -Scope Domain
```

Or we can target all the domain controllers in the entire forest:

```
Get-ADReplicationFailure -Target " therebeladmin.com" -Scope Forest
```

The Get-ADReplicationConnection cmdlet can list replication partner details for the given domain controller:

```
Get-ADReplicationConnection -Filter *
```

The preceding command lists all replication connections for the domain controller you logged in to.

We also can filter replication connections based on attributes. The following command lists replication connections with the REBEL-SRV01 destination server:

```
Get-ADReplicationConnection -Filter {ReplicateToDirectoryServer -eq "REBEL-SRV01"}
```

We also can force objects to sync between domain controllers. The following command will sync the adam user object from REBEL-SRV01 to REBELNET-PDC01:

```
Sync-ADObject -object "adam" -source REBEL-SRV01 -destination REBELNET-PDC01
```

In *Chapter 16*, *Advanced AD Management with PowerShell*, I shared some scripts we can use with Active Directory replication troubleshooting. In the same chapter, I also explained some other PowerShell cmdlets that we can use for troubleshooting and information gathering.

Lingering objects

Let's assume a domain controller has been disconnected from the Active Directory environment and stayed offline for more than the value specified as the tombstone lifetime attribute. Then, after some time, the server is turned on again. In such a situation, the objects which were deleted from Active Directory during the time it was offline will remain as lingering objects.

When an object was deleted using one domain controller, it is replicated to other domain controllers as a tombstone object. It contains a few attribute values but it cannot be used for active operations. It remains in the domain controllers until it reaches the time specified by the tombstone lifetime value. Then, the tombstone object will be permanently deleted from the directory. The tombstone time value is a forest-wide setting and depends on the OS that is running. For OSes after Windows Server 2003, the default tombstone value is 180 days.

A problem occurs when a domain controller with a lingering object is involved with outbound replication. In such a situation, one of the following can happen:

- If the destination domain controller has **strict replication consistency** enabled, then it will halt the inbound replication from that particular domain controller.
- If the destination domain controller has **strict replication consistency** disabled, then it will request a full replica and will reintroduce it to the directory.

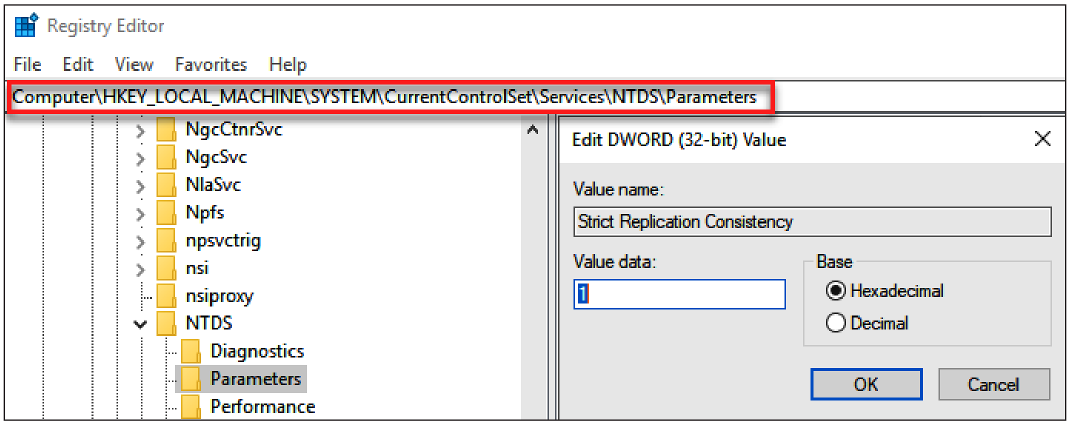
Events `1388`, `1988`, and `2042` suggest lingering objects in the AD infrastructure:

Event ID	Event description
`1388`	Another domain controller has attempted to replicate an object that is not present in the local AD DS database in this domain controller. The object may have been deleted and already garbage collected (a tombstone lifetime or more has passed since the object was deleted) on this domain controller. The attribute set included in the update request is not sufficient to create the object. The object will be re-requested with a full attribute set and re-created on this domain controller. The source domain controller (transport-specific network address) is `xxxxxxxxxxxxxxxxx._msdcs.contoso.com Object: CN=xxxx,CN=xxx,DC=xxxx,DC=xxx Object GUID: xxxxxxxxxxxxx Directory partition: DC=xxxx,DC=xx Destination highest property USN: xxxxxx`.
`1988`	AD DS replication encountered the existence of objects in the following partition that have been deleted from the local domain controller's AD DS database. Not all direct or transitive replication partners are replicated in the deletion before the number of days in the tombstone lifetime have passed. Objects that have been deleted and garbage collected from an AD DS partition, but still exist in the writable partitions of other domain controllers in the same domain or read-only partitions of global catalog servers in other domains in the forest, are known as lingering objects. This event is logged because the source domain controller contains a lingering object that does not exist in the local domain controller's AD DS database. This replication attempt has been blocked. The best solution to this problem is to identify and remove all lingering objects in the forest. The source domain controller (transport-specific network address) is `xxxxxxxxxxxxxx._msdcs.contoso.com Object: CN=xxxxxx,CN=xxxxx,DC=xxxxxx,DC=xxx Object GUID: xxxxxxxxxxxx`.
`2042`	It has been too long since this machine last replicated with the named source machine. The time between replications with this source has exceeded the tombstone lifetime. Replication has been stopped with this source. The reason why replication is not allowed to continue is that the two machine's views of deleted objects may now be different. The source machine may still have copies of objects that have been deleted (and garbage collected) on this machine. If they were allowed to replicate, then the source machines might return objects that have already been deleted. Time of last successful replication: `<date> <time>`. Invocation ID of source: `<Invocation ID>`. Name of source: `<GUID>._msdcs.<domain>`. Tombstone lifetime (days): `<TSL number in days>`. The replication operation has failed.

As mentioned before, the strict replication consistency setting is important to prevent lingering object replication. In the next section, let's go ahead and see how we can enable this setting.

Strict replication consistency

This setting is controlled by a registry key. After Windows Server 2003, by default, this setting is enabled. The key can be found under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`:



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

Edit DWORD (32-bit) Value

Value name: Strict Replication Consistency

Value data: 1

Base: ● Hexadecimal ○ Decimal

Figure 20.1: Strict replication consistency registry settings

This feature prevents destination domain controllers from replicating lingering objects. It is important to make sure this is enabled in all the domain controllers.

Removing lingering objects

Lingering objects can be removed using the following command:

```
repadmin /removelingeringobjects <faulty DC name> <reference DC GUID>
<directory partition>
```

In the preceding command, `faulty DC name` represents the domain controller that contains lingering objects, `reference DC GUID` is the GUID of a domain controller that contains an up-to-date database that can be used as a reference, and `directory partition` is the directory partition where lingering objects are contained.

Issues involving DFS Replication

After Windows Server 2003, FRS is no longer used for SYSVOL replication. It has been replaced by DFS. But, if you are upgrading AD DS from an older version, then the older version will still be in use and migration from FRS to DFS is required. If it is Windows Server 2022, first we need to migrate SYSVOL replication from FRS to DFS before proceeding with the AD DS upgrade.

The `SYSVOL` folder in a domain controller includes the domain's public files, such as Group Policy files, batch files, and login scripts. Healthy replication of SYSVOL is required to maintain a functional Active Directory environment. When there are SYSVOL replication issues, you may experience issues such as the following:

- New/updated group policies are applied partially or not applied at all
- Group policies are applied to part of the target object group
- Login scripts are not running

The following events in Event Viewer, under the `DFS Replication log` and `System log` files, help us to recognize DFS Replication issues:

Event ID	**Event description**
`4612`	The DFS Replication service initialized SYSVOL at the `C:\Windows\SYSVOL\domain` local path and is waiting to perform the initial replication. The replicated folder will remain in the initial synchronization state until it has replicated with its partner, `<FQDN>`. If the server was in the process of being promoted to a domain controller, then 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 sync partner. If this event occurred during the migration of SYSVOL from FRS to DFS Replication, then 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.
`2213`	The DFS Replication service stopped replication on volume `C:`. This occurs when a **DFS Replication** (**DFSR**) JET database is not shut down cleanly and Auto Recovery is disabled. To resolve this issue, back up the files in the affected replicated folders, and then use the `ResumeReplication` WMI method to resume replication. The recovery steps are as follows: Back up the files in all replicated folders on the volume. Failure to do so may result in data loss due to unexpected conflict resolution during the recovery of the replicated folders. To resume the replication for this volume, use the `ResumeReplication` WMI method of the `DfsrVolumeConfig` class. For example, from an elevated Command Prompt, type the following command: `wmic /namespace:\\root\microsoftdfs path dfsrVolumeConfig where volumeGuid="xxxxxxxx” call ResumeReplication`.
`5002`	The DFS Replication service encountered an error communicating with the `<FQDN>` partner for the Domain System Volume replication group.

5008	The DFS Replication service failed to communicate with the <FQDN> partner for the Home-Replication replication group. This error can occur if the host is unreachable, or if the DFS Replication service is not running on the server.
5014	The DFS Replication service is stopping communication with the <FQDN> partner for the Domain System Volume replication group due to an error. The service will retry the connection periodically.
1096	The processing of a Group Policy failed. Windows could not apply the registry-based policy settings for the <Object GUID> Group Policy object. Group Policy settings will not be resolved until this event is resolved. View the event details for more information on the filename and path that caused the failure.
4012	The DFS Replication service stopped replication on the replicated folder at the `c:\xxx` local path. It has been disconnected from other partners for 70 days, which is longer than the `MaxOfflineTimeInDays` parameter. Because of this, DFS replication considers this data to be stale and will replace it with data from other members of the replication group during the next replication. DFS Replication will move the stale files to the local `Conflict` folder. No user action is required.

When there is a SYSVOL replication issue, we can carry out the following troubleshooting steps to rectify the issue.

Verifying the connection

Check whether the problematic SYSVOL folder can reach other domain controllers. A simple ping can verify the connectivity between nodes. Also, try to access the replication partner shares using `\\domaincontroller` (network path). Verify that replication partners are also in a healthy state. DFS Replication requires specific TCP and UDP ports. Make sure the following TCP and UDP ports are allowed via hardware/software firewalls:

Service name	**TCP**	**UDP**
NetBIOS name service	137	137
NetBIOS datagram service	-	138
NetBIOS session service	139	-
RPC	135	-
Server Message Block Protocol (**SMB protocol**)	445	445
Lightweight Directory Access Protocol (**LDAP**)	389	389

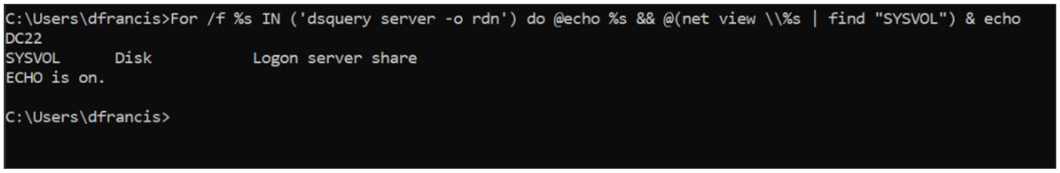
In some organizations, engineers use antivirus and malware protection on domain controllers with settings made for desktop computers. On many occasions, I have seen that the DFS process has been blocked by endpoint protection solutions. Therefore, if such a solution is in place, then make sure you follow the guidelines provided by Microsoft and exclude the relevant files and processes. These guidelines can be found at `https://bit.ly/3FHQPwn`.

SYSVOL share status

We need to verify whether the SYSVOL share exists on the domain controllers. This is one of the basic troubleshooting steps. This can be done by running the following command on a domain controller:

```
For /f %s IN ('dsquery server -o rdn') do @echo %s && @(net view \\%s |
find "SYSVOL") & echo
```

This will list down the servers and the SYSVOL shares that are available:



```
C:\Users\dfrancis>For /f %s IN ('dsquery server -o rdn') do @echo %s && @(net view \\%s | find "SYSVOL") & echo
DC22
SYSVOL      Disk           Logon server share
ECHO is on.

C:\Users\dfrancis>
```

Figure 20.2: List of servers and SYSVOL shares

As part of the troubleshooting process, we need to verify the DFS replication status. In the next section, we are going to look into DFS troubleshooting.

DFS replication status

The status of the DFS replication can be determined based on the status code.

Status codes for DFS are as follows:

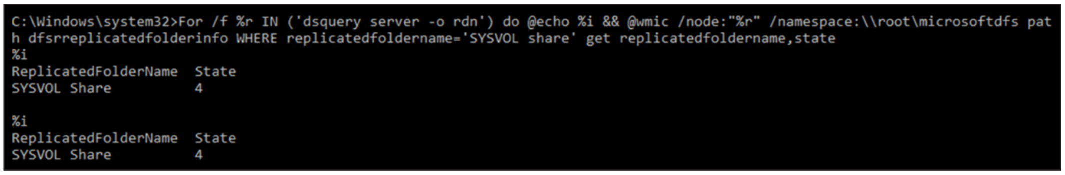
- `0`: Uninitialized
- `1`: Initialized
- `2`: Initial synchronization
- `3`: Auto Recovery
- `4`: Normal
- `5`: In error state

- 6: Disabled
- 7: Unknown

In order to review the status, we can use the following command:

```
For /f %r IN ('dsquery server -o rdn') do @echo %i && @wmic /node:"%r"
/namespace:\\root\microsoftdfs path dfsrreplicatedfolderinfo WHERE
replicatedfoldername='SYSVOL share' get replicatedfoldername,state
```

Once we run the preceding command, the output is as follows:



```
C:\Windows\system32>For /f %r IN ('dsquery server -o rdn') do @echo %i && @wmic /node:"%r" /namespace:\\root\microsoftdfs pat
h dfsrreplicatedfolderinfo WHERE replicatedfoldername='SYSVOL share' get replicatedfoldername,state
%i
ReplicatedFolderName  State
SYSVOL Share          4

%i
ReplicatedFolderName  State
SYSVOL Share          4
```

Figure 20.3: DFS status

Next, we are going to look into the most common DFS issues and steps we can take to fix those.

DFSR crash due to the dirty shutdown of the domain controller (event ID 2213)

This is one of the most common DFSR errors; it happens when a domain controller crashes. This can be fixed by using the existing command listed for event ID 2213. It will resume replication in the volume.

In the following command, the `volumeGuid` value needs to be replaced with the relevant value from your environment:

```
wmic /namespace:\\root\microsoftdfs path dfsrVolumeConfig where
volumeGuid="xxxxxxxx" call ResumeReplication
```

The relevant `volumeGuid` value can be found under the event ID 2213 description.

If this doesn't solve the issue, then we will have to do an authoritative or non-authoritative restore, which will be explained later, in the *Authoritative DFS Replication* and *Non-Authoritative DFS Replication* sections of this chapter.

Content Freshness

With Windows Server 2008, Microsoft introduced a setting called **Content Freshness protection** to protect DFS shares from stale data. Azure DFS also uses a multi-master database similar to AD. It also has a tombstone time limit similar to AD: 60 days by default. So, if there is no replication beyond that time and replication is reenabled in a DFS member, it can create stale data. This is similar to lingering objects in AD. To prevent this, we can define a value for `MaxOfflineTimeInDays`. If the number of days since the last successful DFS replication is more than the `MaxOfflineTimeInDays` value, then it will prevent replication. In such a situation, you will see event `4012`. After Windows Server 2012, this feature is enabled by default and the initial value is set to 60 days.

We can check this value using the following:

```
For /f %m IN ('dsquery server -o rdn') do @echo %m && @wmic /
node:"%m" /namespace:\\root\microsoftdfs path DfsrMachineConfig get
MaxOfflineTimeInDays
```

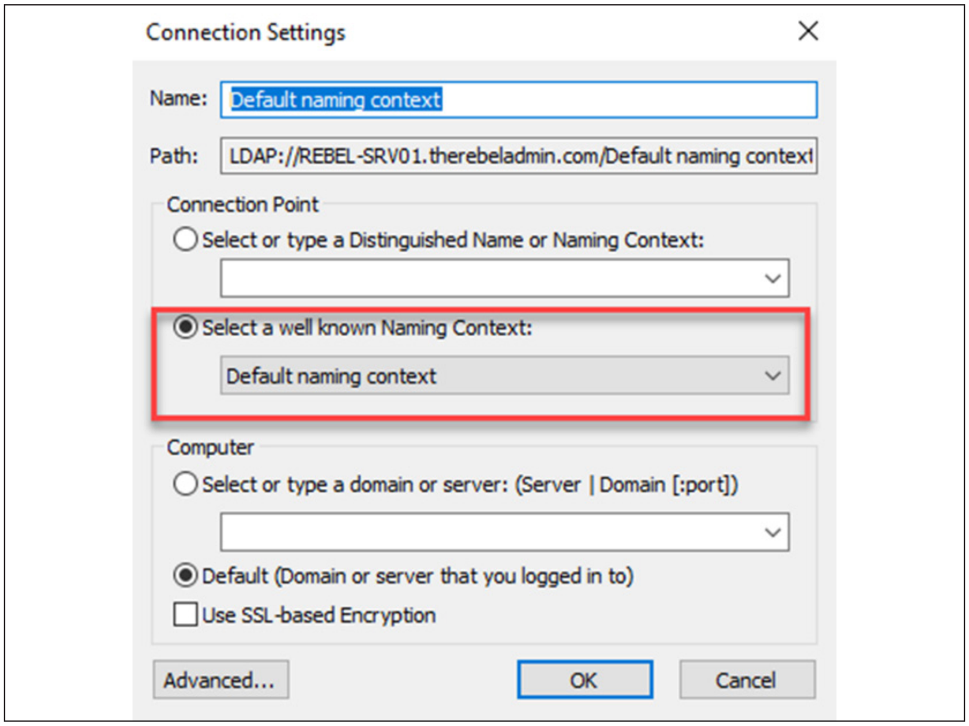
The only way to recover from this is to use non-authoritative or authoritative recovery for DFS.

Non-authoritative DFS Replication

In most situations, only one or a few domain controllers (less than 50%) have replication issues at a given time. In such situations, we can issue a non-authoritative replication request so the system will replicate the SYSVOL from the **Primary Domain Controller** (**PDC**). In order to perform non-authoritative replication, follow these steps:

1. First, we need to back up the existing SYSVOL. This can be done by copying the `SYSVOL` folder from the domain controller that has DFS Replication issues to a secure location.
2. Log in to the domain controller as Domain Admin/Enterprise Admin.

3. Launch the `ADSIEDIT.MSC` tool and connect to `Default naming context`:



Connection Settings

Name: Default naming context

Path: LDAP://REBEL-SRV01.therebeladmin.com/Default naming context

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context:

Default naming context

Computer

○ Select or type a domain or server: (Server | Domain [:port])

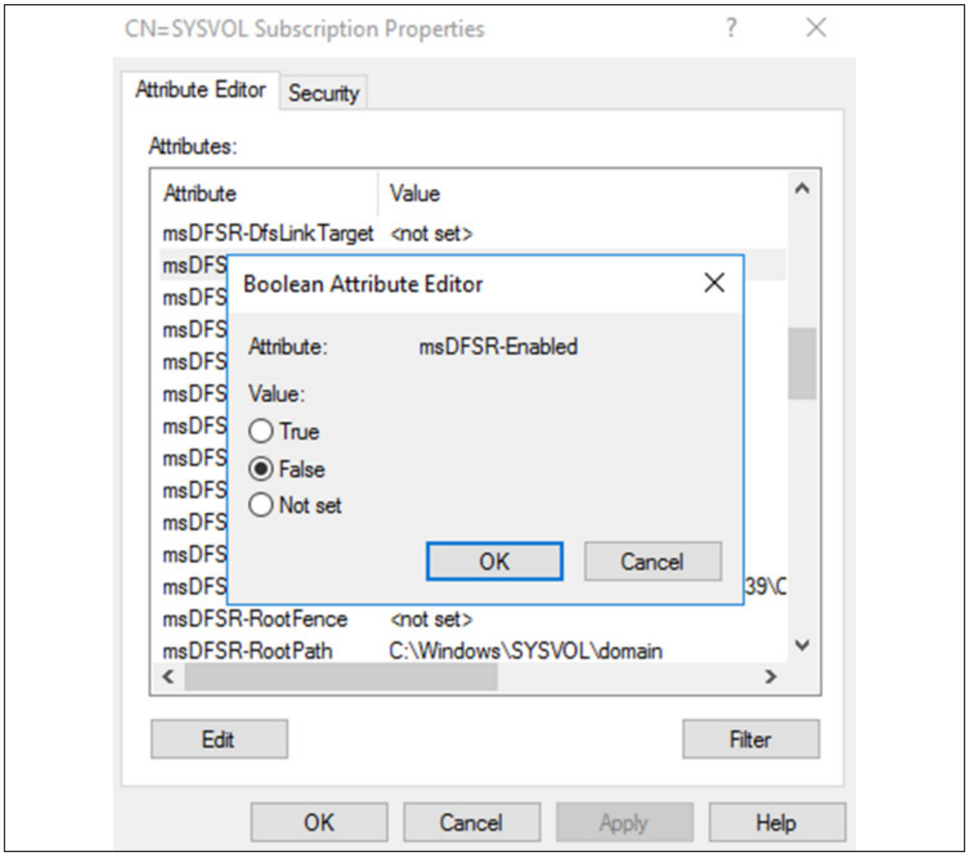
● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

Figure 20.4: ADSIEdit Connection Settings

4. Browse to `DC=domain,DC=local | OU=Domain Controllers | CN=(DC NAME) | CN=DFSR-LocalSettings | Domain System Volume | SYSVOL Subscription`.

5. Change the value of the `msDFSR-Enabled` attribute to `False`:



CN=SYSVOL Subscription Properties

Attributes:

Attribute	Value
msDFSR-DfsLinkTarget	<not set>
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	
msDFS	39\C
msDFSR-RootFence	<not set>
msDFSR-RootPath	C:\Windows\SYSVOL\domain

Boolean Attribute Editor

Attribute: msDFSR-Enabled

Value:

○ True
● False
○ Not set

Figure 20.5: msDFSR-Enabled attribute

6. Force AD replication using the following command:

   ```
   repadmin /syncall /AdP
   ```

7. Run the following command to install the DFS management tools (unless they are already installed):

   ```
   Add-WindowsFeature RSAT-DFS-Mgmt-Con
   ```

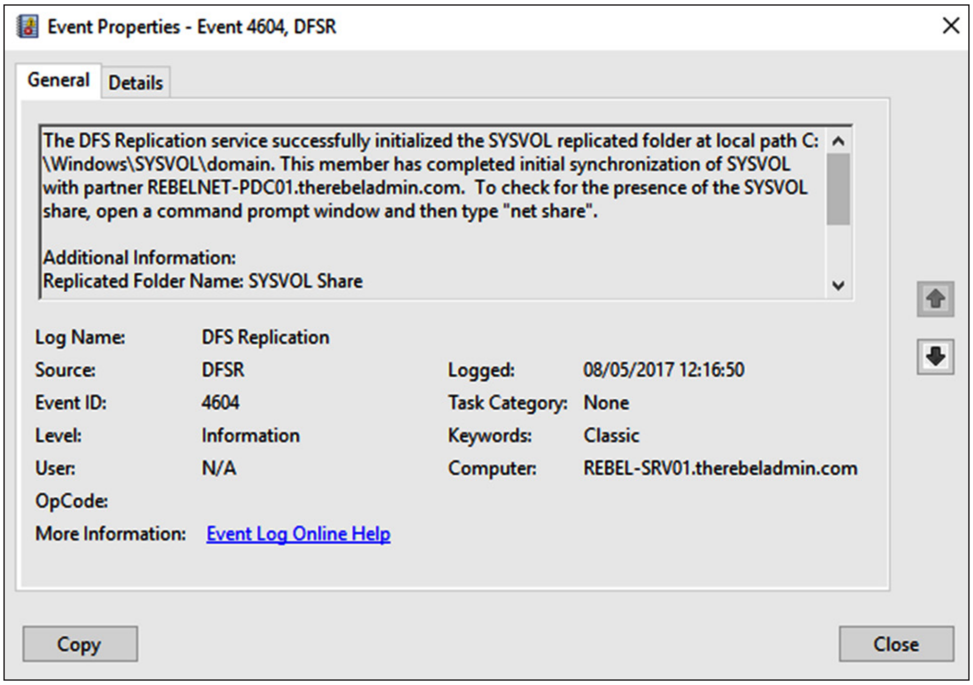
8. Run the following command to update the DFRS global state:

   ```
   dfsrdiag PollAD
   ```

9. Search for event 4114 to confirm that SYSVOL replication is disabled:

   ```
   Get-EventLog -Log "DFS Replication" | where {$_.eventID -eq 4114} |
   fl
   ```

10. Change the attribute value of `msDFSR-Enabled` back to `True` (*step 5*).
11. Force AD replication, as in *step 6*.
12. Update the DFRS global state by running the command in *step 8*.
13. Search for events `4614` and `4604` to confirm successful non-authoritative synchronization:



Event Properties - Event 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 REBELNET-PDC01.therebeladmin.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

Log Name: DFS Replication
Source: DFSR
Logged: 08/05/2017 12:16:50
Event ID: 4604
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: REBEL-SRV01.therebeladmin.com
OpCode:
More Information: Event Log Online Help

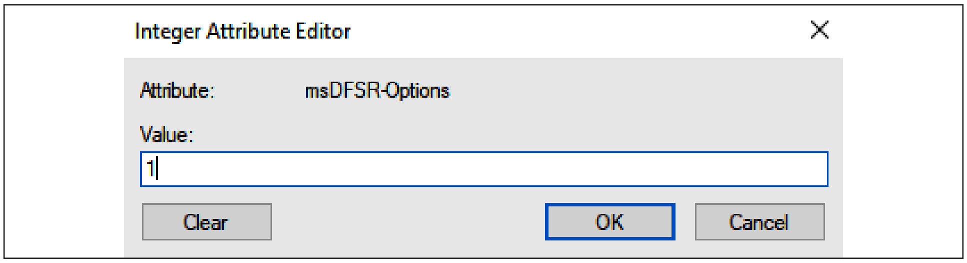
Figure 20.6: Event 4604

All the commands should be run from the domain controllers that are set as non-authoritative. It's only recommended that you use this in cases where less than 50% of domain controllers have DFS Replication issues.

Authoritative DFS Replication

In the previous section, only a selected number of domain controllers were involved with forceful replication from the PDC. But there are situations where we need to recover SYSVOL from a backup and then forcefully replicate it to all other domain controllers. This is also the recommended recovery option when more than 50% of domain controllers are experiencing DFS Replication issues. In order to initiate authoritative DFS Replication, follow these steps:

1. Log in to the PDC FSMO role holder as Domain Administrator or Enterprise Administrator.
2. Stop the DFS Replication service (this is recommended on all the domain controllers).
3. Launch the `ADSIEDIT.MSC` tool and connect to `Default naming context`.
4. Browse to `DC=domain,DC=local | OU=Domain Controllers | CN=(DC NAME) | CN=DFSR-LocalSettings | Domain System Volume | SYSVOL Subscription`.
5. Update the given attributes' values as follows:
   - `msDFSR-Enabled` as `False`
   - `msDFSR-Options` as `1`



Integer Attribute Editor

Attribute: msDFSR-Options

Value: 1

Figure 20.7: msDFSR-Options

6. Modify the `msDFSR-Enabled` attribute to `False` on all other domain controllers.
7. Force AD replication using the following:

```
repadmin /syncall /AdP
```

8. Start the DFS Replication service on the PDC.
9. Search for event `4114` to verify that SYSVOL replication is disabled.

10. Modify the `msDFSR-Enabled` value to `True`, which was set in *step 5*.
11. Force AD replication using the following:

    ```
    repadmin /syncall /AdP
    ```

12. Run the following command to update the DFRS global state:

    ```
    dfsrdiag PollAD
    ```

13. Search for event `4602` and verify successful SYSVOL replication.
14. Start the DFS service on all other domain controllers.
15. Search for event `4114` to verify that SYSVOL replication is disabled.
16. Modify the `msDFSR-Enabled` value to `True`, which was set in *step 6*. This needs to be done on all domain controllers.
17. Run the following command to update the DFRS global state:

    ```
    dfsrdiag PollAD
    ```

18. Search for events `4614` and `4604` to confirm successful authoritative synchronization.

This completes the authoritative synchronization process. During this process, no one can use SYSVOL. But in a non-authoritative process, only domain controllers with DFS issues will be affected.

How to troubleshoot Group Policy issues

Group Policy troubleshooting is one of the most painful and time-consuming tasks for most IT engineers. There are so many things that can go wrong with group policies. I have listed some of the most common reasons for Group Policy issues:

Reason	**Description**
Replication issues	Active Directory and SYSVOL replication-related errors are the most common reason for Group Policy issues. In the *Identifying replication issues* section of this chapter, we looked into possible replication issues that can occur in an Active Directory environment and how we can recover from them.
Poor design	Using group policies in the infrastructure is like eating curd with a two-edged sword. By design, it should be spot on, but continuous reviewing is also required to maintain it. In *Chapter 10*, *Managing Group Policies*, we learned about how we can design a Group Policy infrastructure properly.

Connectivity issues	If users/devices do not have a stable connection with domain controllers, then this also creates Group Policy-related issues. This is mostly not a problem for periodic disconnection as Group Policy refreshes every 90 minutes.
Loopback processing	Loopback processing settings can create a lot of hassle if you do not use the modes properly. My recommendation is to use the *replace* mode whenever possible.
Group Policy permissions	If a user is having issues with applying certain group policies, then you should always check whether the user has **Read** and **Apply Group Policy** permissions under Group Policy delegation.
Security filtering	Group policies can target individual users, groups, or devices using security filtering. If a particular user or group is having issues with applying specific group policies, then it's better to check whether the particular user or groups are being targeted.
WMI filters	WMI filters are also used by group policies for granular targeting. These filters use system-specific settings such as OS version and architecture. If WMI filtering is in place, then make sure the rules are updated according to target changes.
Inheritance	Group policies, by default, allow inheritance, and it is important to control them wherever necessary. Block inheritance action prevents us from applying unnecessary Group Policy settings, which can result in a longer Group Policy processing time and operation-related issues. We can review inheritance using the **Group Policy Inheritance** tab. The applied order system will also decide which one is the winning Group Policy (if the same setting is used by multiple group policies).

Apart from issue-specific troubleshooting steps, there are some common tools and methods we can use to troubleshoot Group Policy-related issues. In this section, we will look at some of them.

Forcing Group Policy processing

This is the most common starting point for any Group Policy-related troubleshooting. Once we log in to a system, it refreshes group policies every 90 minutes. But if required, we can forcefully process the group policies using the following command:

```
gpupdate /force
```

If a Group Policy change is related to a user setting, then we need to log off and log back in. If it's a computer setting, then the system needs to reboot after running the command.

Resultant Set of Policy (RSoP)

In a system, RSoP can be used to extract details about the group policies that are already applied, and also the policy settings that are planned. RSoP also helps us determine which policy is the winning policy and in which order the policies have been applied.

RSoP has two modes. In planning mode, we can simulate the effect of policy settings that we would like to apply to a computer and user. In logging mode, it reports existing policy settings for a computer and the user that is currently logged on.

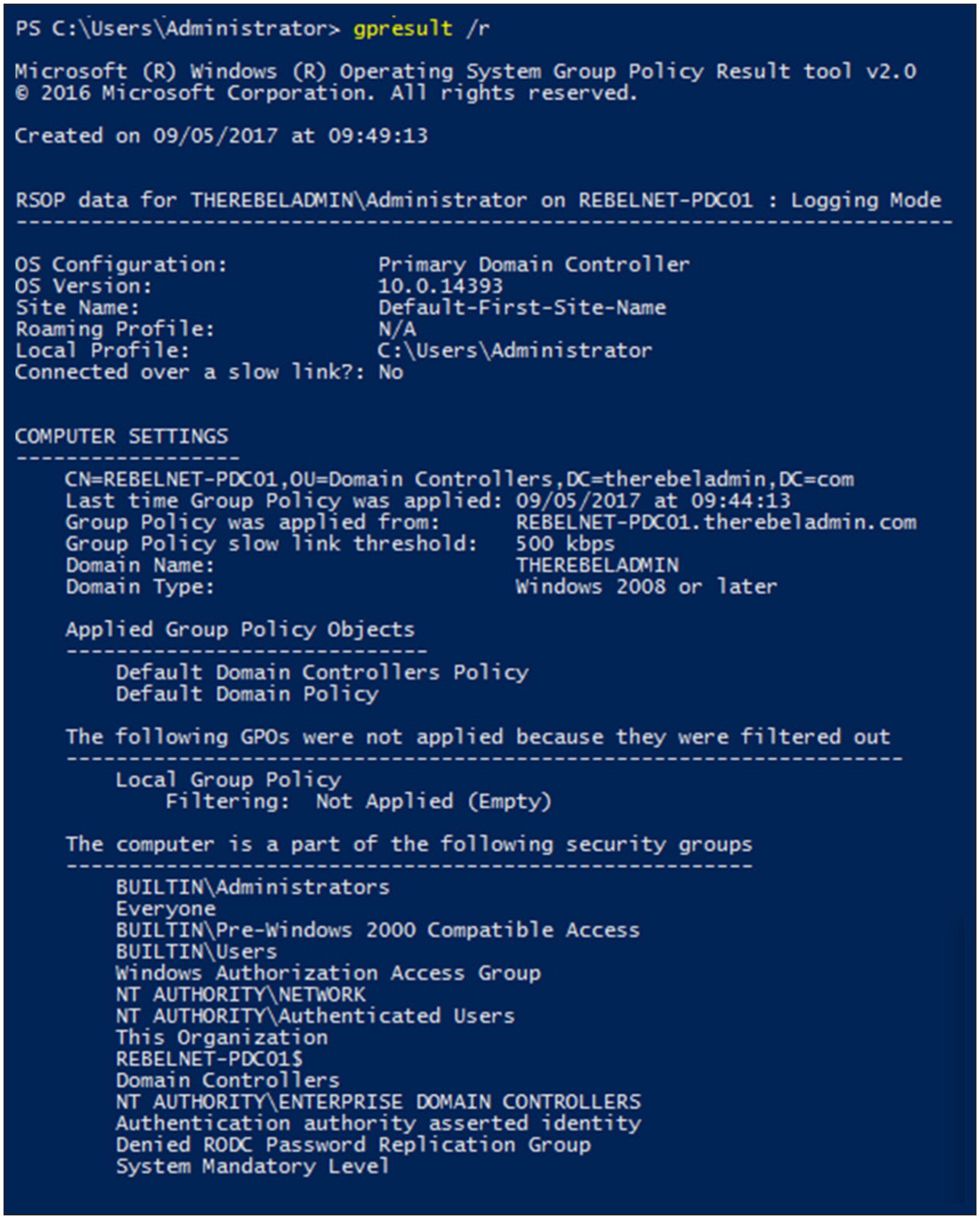
RSoP and the command-line-based tool, `GPRESULT`, both do the same work. However, after Vista, Microsoft recommended using `GPRESULT` instead of `RSoP.msc` as `GPRESULT` doesn't show all the Group Policy settings. For example, Group Policy preferences are not shown.

GPRESULT

This is a command-line utility that can be used to display RSoP information for users and computers. It can be used either locally or remotely.

The following command provides RSoP summary data for the currently logged-in user. This is similar to the `RSOP.msc` default run in logging mode:

```
Gpresult /r
```



```
PS C:\Users\Administrator> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2016 Microsoft Corporation. All rights reserved.

Created on 09/05/2017 at 09:49:13


RSOP data for THEREBELADMIN\Administrator on REBELNET-PDC01 : Logging Mode
---------------------------------------------------------------------------

OS Configuration:            Primary Domain Controller
OS Version:                  10.0.14393
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=REBELNET-PDC01,OU=Domain Controllers,DC=therebeladmin,DC=com
    Last time Group Policy was applied: 09/05/2017 at 09:44:13
    Group Policy was applied from:      REBELNET-PDC01.therebeladmin.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        THEREBELADMIN
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Default Domain Controllers Policy
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The computer is a part of the following security groups
    -------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Pre-Windows 2000 Compatible Access
        BUILTIN\Users
        Windows Authorization Access Group
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        This Organization
        REBELNET-PDC01$
        Domain Controllers
        NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
        Authentication authority asserted identity
        Denied RODC Password Replication Group
        System Mandatory Level
```

Figure 20.8: gpresult /r output

The preceding command lists the summary data for the user and computer configurations. We also can scope it out to user configurations using the following command:

```
gpresult /r /scope:user
```

We can also scope `gpresult` output to computer configurations using the following command:

```
gpresult /r /scope:computer
```

We can also run `gpresult` by targeting a remote system:

```
gpresult /s REBEL-SRV01 /r
```

In the preceding command, `/s` specifies the remote computer name. The preceding command uses the same account details as the user who is running the command.

We can also run it by specifying user account details:

```
gpresult /s REBEL-SRV01 /u therebeladmin\R540328 /p 1Qaz2Wsx /r
```

The preceding command uses the `therebeladmin\R540328` user account with its password specified with the `/p` parameter.

We also can export the result as an HTML report. This is really useful for troubleshooting:

```
gpresult /h r01.html
```

The preceding command runs RSoP summary data for the currently logged-in system and saves it as an HTML report.

The Group Policy Results Wizard

This tool does the same thing as `GPRESULT`, but, instead of the command line, it uses a GUI. This allows us to access the results via the same console that is used to manage group policies. It is useful for troubleshooting as you do not need to move between different interfaces.

In order to access this, follow these steps:

1. Launch Group Policy Management (you can use the domain controller or any other system that has relevant management tools installed).
2. Right-click on the **Group Policy Results** container in the left-hand panel. Then, click on **Group Policy Results Wizard...** from the list, as shown in the following screenshot:

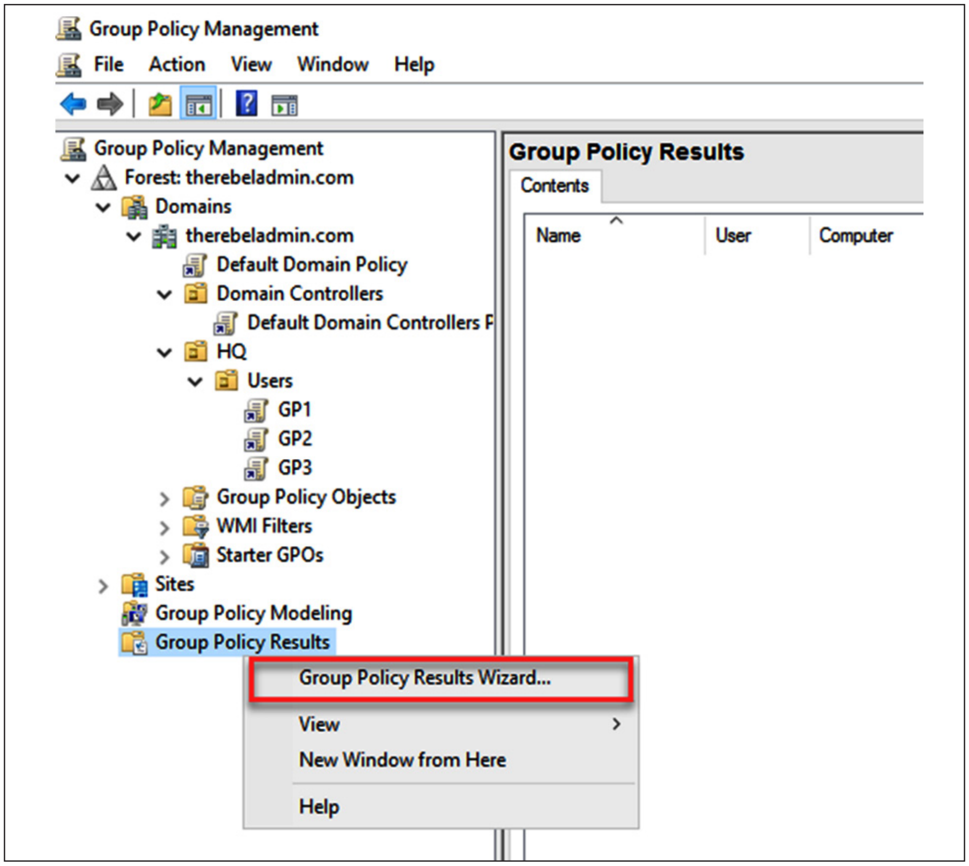
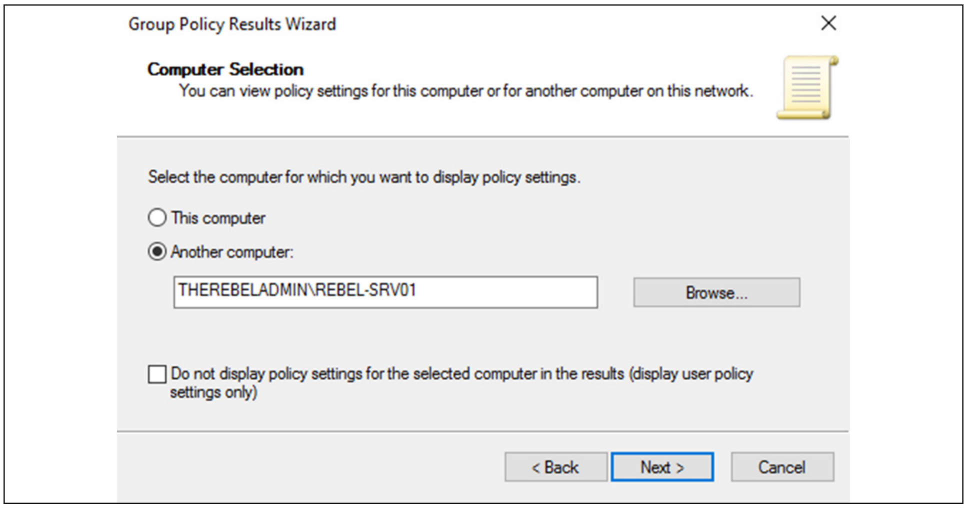


Figure 20.9: Open Group Policy Results Wizard

3. This opens up a new wizard. Click on **Next** to continue.

4. Then, the wizard asks us to specify which system it should use as the target. It can be a local system or any remote system. Once you have made your selection, click on **Next** to proceed:



Group Policy Results Wizard

Computer Selection

You can view policy settings for this computer or for another computer on this network.

Select the computer for which you want to display policy settings.

○ This computer

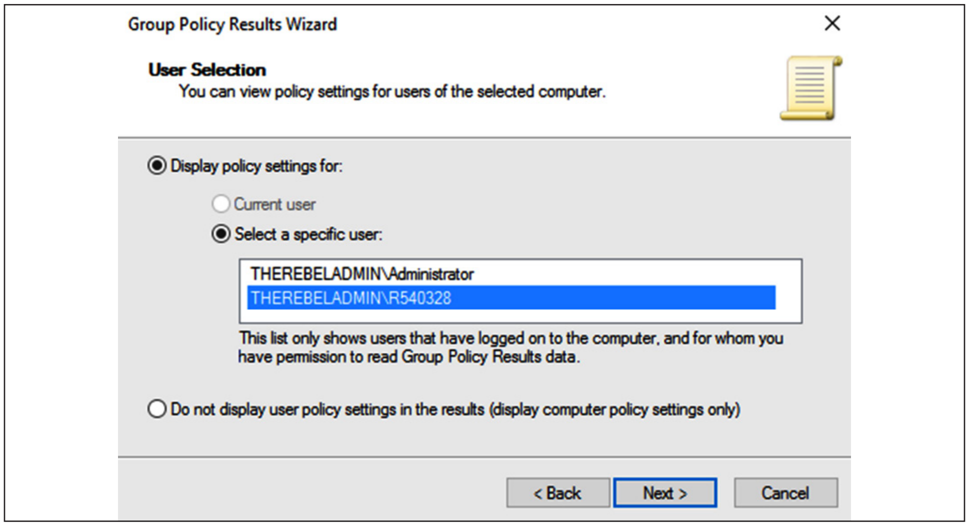
● Another computer:

THEREBELADMIN\REBEL-SRV01

□ Do not display policy settings for the selected computer in the results (display user policy settings only)

Figure 20.10: Group Policy Results Wizard – Computer Selection

5. Then, it asks us to specify the user to display policy settings. The list only shows the users who are already logged into the system and have permission to read Group Policy result data. If we only want to see the computer policy settings, then we can select the option to not display user settings. Once you have made your selection, click on **Next** to continue:



Group Policy Results Wizard

User Selection

You can view policy settings for users of the selected computer.

● Display policy settings for:

○ Current user

● Select a specific user:

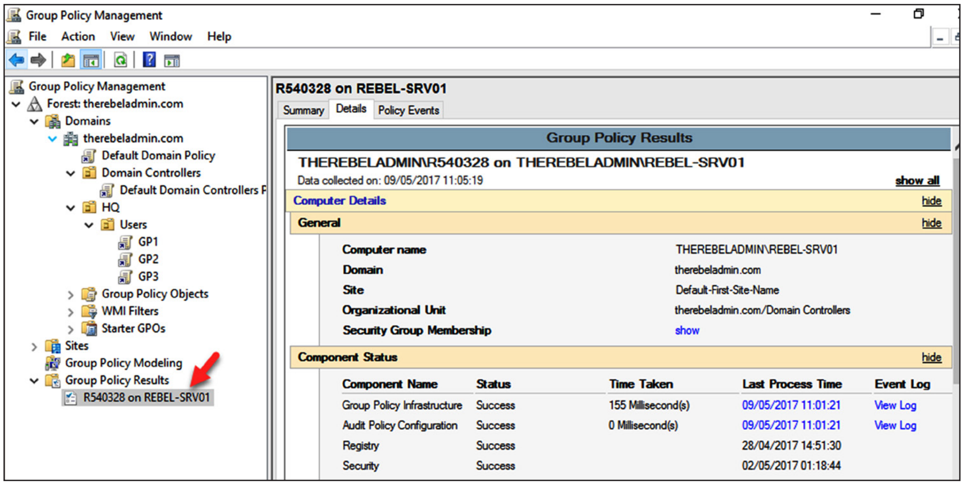
THEREBELADMIN\Administrator
THEREBELADMIN\R540328

This list only shows users that have logged on to the computer, and for whom you have permission to read Group Policy Results data.

○ Do not display user policy settings in the results (display computer policy settings only)

Figure 20.11: Group Policy Results Wizard – User Selection

6. The next window provides us with a summary of the selection. Click on **Next** to run the job.
7. Once it is completed, we can see the report in the Microsoft Management Console (MMC). If required, the same query can be run at any time:



R540328 on REBEL-SRV01

Group Policy Results

THEREBELADMIN\R540328 on THEREBELADMIN\REBEL-SRV01

Data collected on: 09/05/2017 11:05:19

Computer Details

General

Computer name	THEREBELADMIN\REBEL-SRV01
Domain	therebeladmin.com
Site	Default-First-Site-Name
Organizational Unit	therebeladmin.com/Domain Controllers
Security Group Membership	show

Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	155 Millisecond(s)	09/05/2017 11:01:21	View Log
Audit Policy Configuration	Success	0 Millisecond(s)	09/05/2017 11:01:21	View Log
Registry	Success		28/04/2017 14:51:30	
Security	Success		02/05/2017 01:18:44	

Figure 20.12 – Saved query

The Group Policy Modeling Wizard allows us to simulate RSoP and evaluate the impact. This is done on the server level and there's no need to log into target systems for testing. Let's go ahead and see how this tool works.

The Group Policy Modeling Wizard

When we looked at the *Resultant Set of Policy* (*RSoP*) section, we learned about two modes of RSoP. Planning mode allows us to simulate Group Policy processing without applying it to a target. Engineers do not have to log in to different systems to see how they process the group policies. This is not only helpful for troubleshooting; we can also use it for Group Policy design.

In order to use the Group Policy Modeling Wizard, follow these steps:

1. Launch Group Policy Management (you can use the domain controller or any other system that has the relevant management tools installed).

2. Right-click on the **Group Policy Modeling** container in the left-hand panel. Then, click on **Group Policy Modeling Wizard...** from the list:

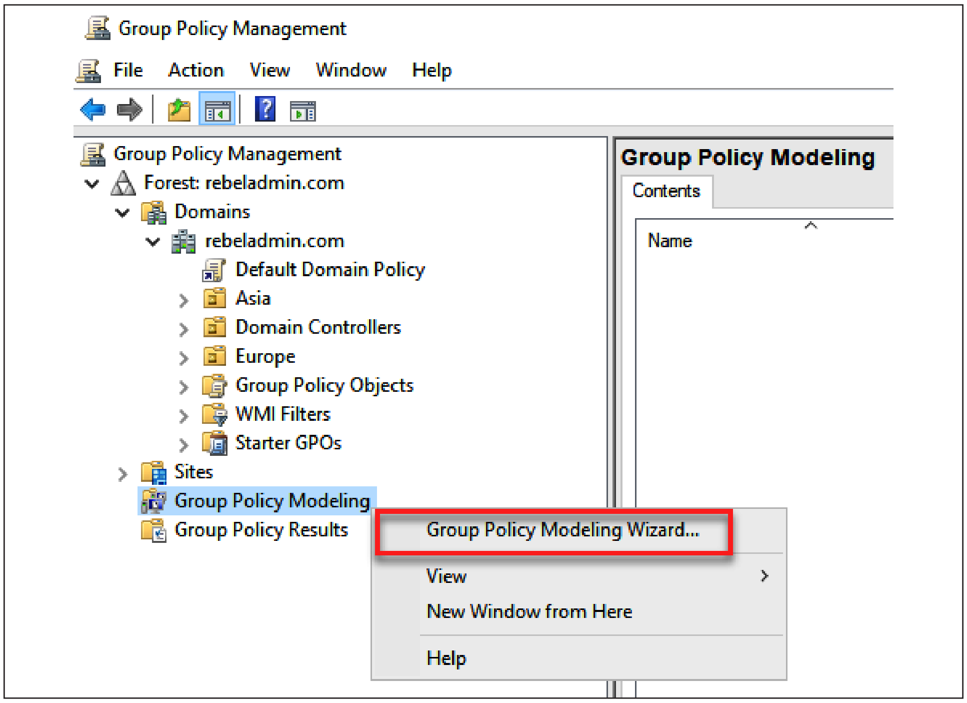
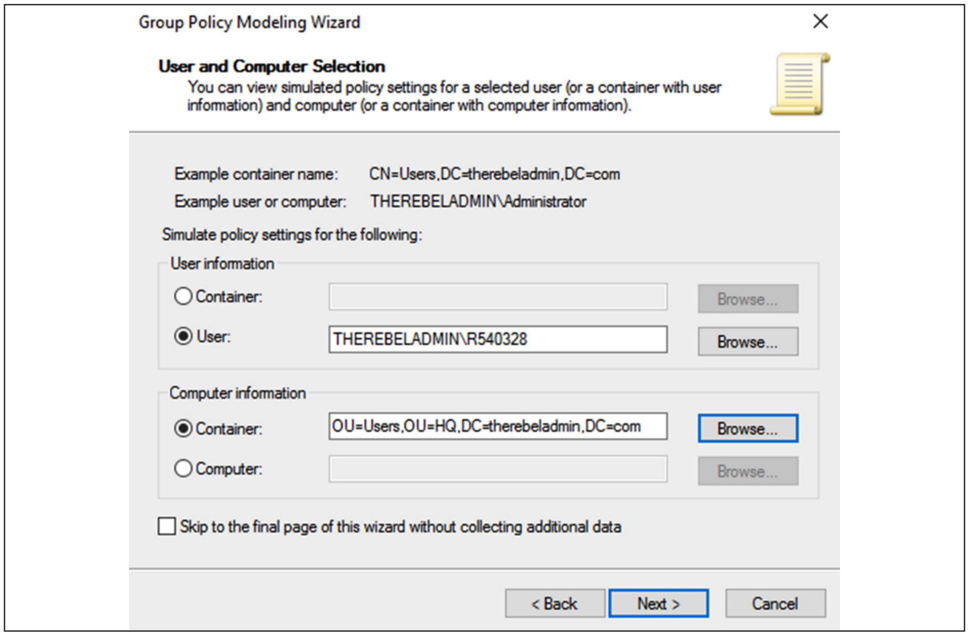


Figure 20.13: Group Policy Modeling Wizard

3. On the initial wizard page, click on **Next** to continue with the configuration.
4. In the new window, the wizard asks us to select the domain controller it should use for the simulation. It is recommended that you use a domain controller in the same Active Directory site. Once you've made your selection, click on **Next** to continue.
5. On the user and computer selection page, we can select which user and device should be used in the simulation job. It can be based on an individual entry or at the container level. Once you've made your selection, click on **Next** to proceed:



Group Policy Modeling Wizard

User and Computer Selection

You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=therebeladmin,DC=com

Example user or computer: THEREBELADMIN\Administrator

Simulate policy settings for the following:

User information

○ Container:

● User: THEREBELADMIN\R540328

Computer information

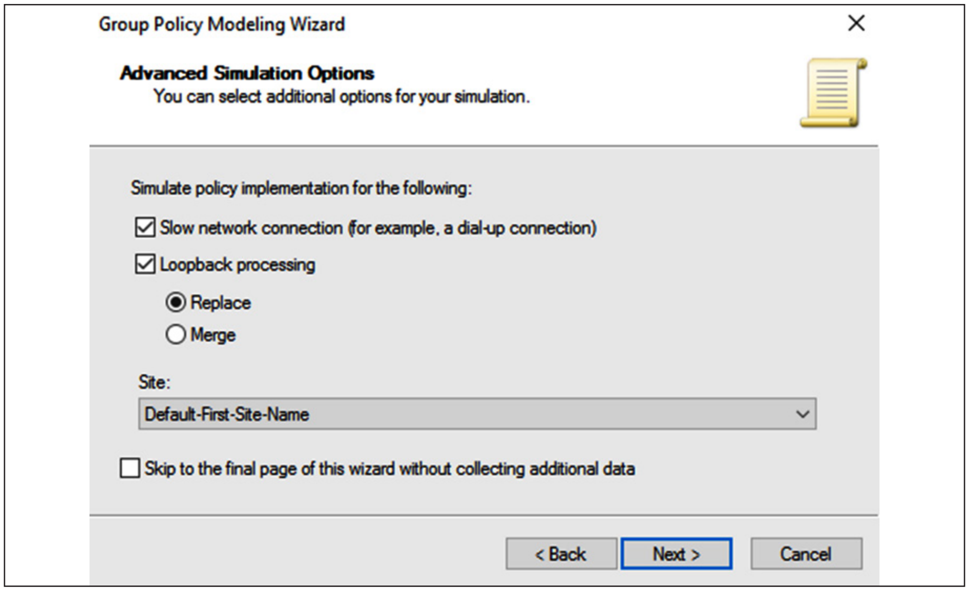
● Container: OU=Users,OU=HQ,DC=therebeladmin,DC=com

○ Computer:

□ Skip to the final page of this wizard without collecting additional data

Figure 20.14: User and Computer Selection

6. In **Advanced Simulation Options**, if required, we can select the **Slow network connection** and **Loopback processing** mode configuration options. We can also define the site that should be used for the simulation:



Group Policy Modeling Wizard

Advanced Simulation Options

You can select additional options for your simulation.

Simulate policy implementation for the following:

☑ Slow network connection (for example, a dial-up connection)

☑ Loopback processing

● Replace

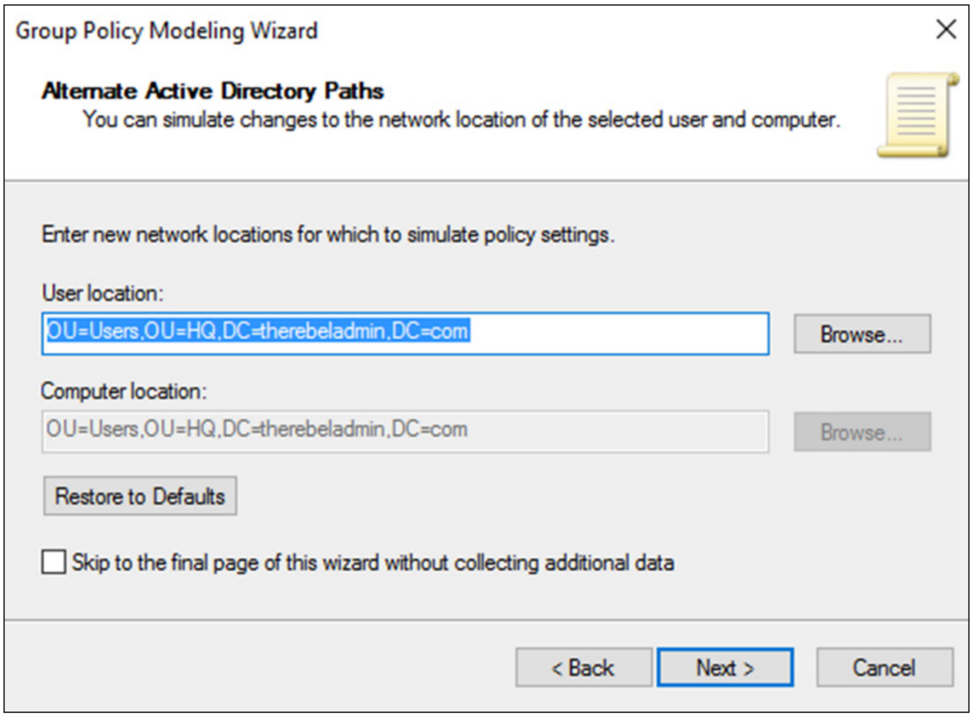
○ Merge

Site: Default-First-Site-Name

□ Skip to the final page of this wizard without collecting additional data

Figure 20.15: Advanced Simulation Options

7. In the next window, if needed, we can select an alternative Active Directory path to simulate changes to the network location of the selected user and computer. In this demo, I am using the defaults:



Group Policy Modeling Wizard

Alternate Active Directory Paths

You can simulate changes to the network location of the selected user and computer.

Enter new network locations for which to simulate policy settings.

User location: OU=Users,OU=HQ,DC=therebeladmin,DC=com

Computer location: OU=Users,OU=HQ,DC=therebeladmin,DC=com

□ Skip to the final page of this wizard without collecting additional data

Figure 20.16: Alternative Active Directory Paths

8. In the next window, if required, we can select a user security group to simulate. The default group will be **Authenticated Users**. When ready, click on **Next** to proceed.
9. Then, it asks whether we need to define the computer security group for our simulation. You can add a group here or keep the default group, which is **Authenticated Users**.
10. The next window asks whether WMI filtering for users is required. Once the necessary selections are made, click on **Next** to proceed.

11. The next window asks whether WMI filtering for computers is required. Once the necessary selections are made, click on **Next** to proceed.
12. In the end, the wizard gives us a summary window with the selected options. Click on **Next** to run the simulation job.
13. Once the process is completed, we can see the results in the console:

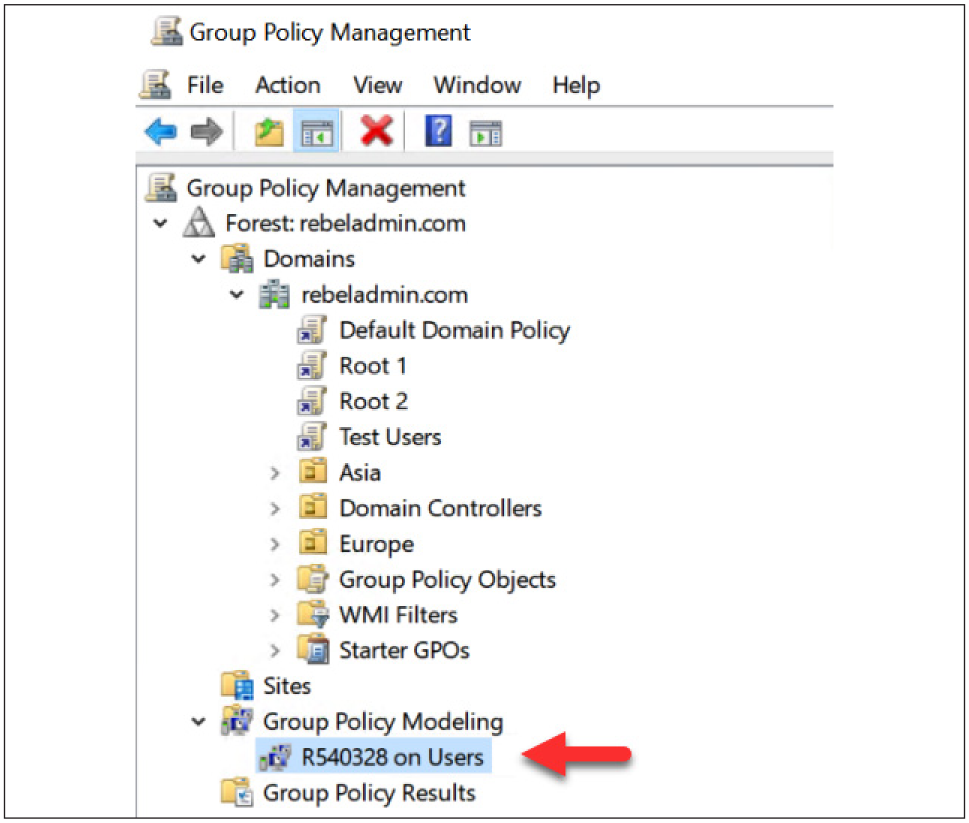


Figure 20.17: Simulation query

14. We also can rerun the simulation query at any time:

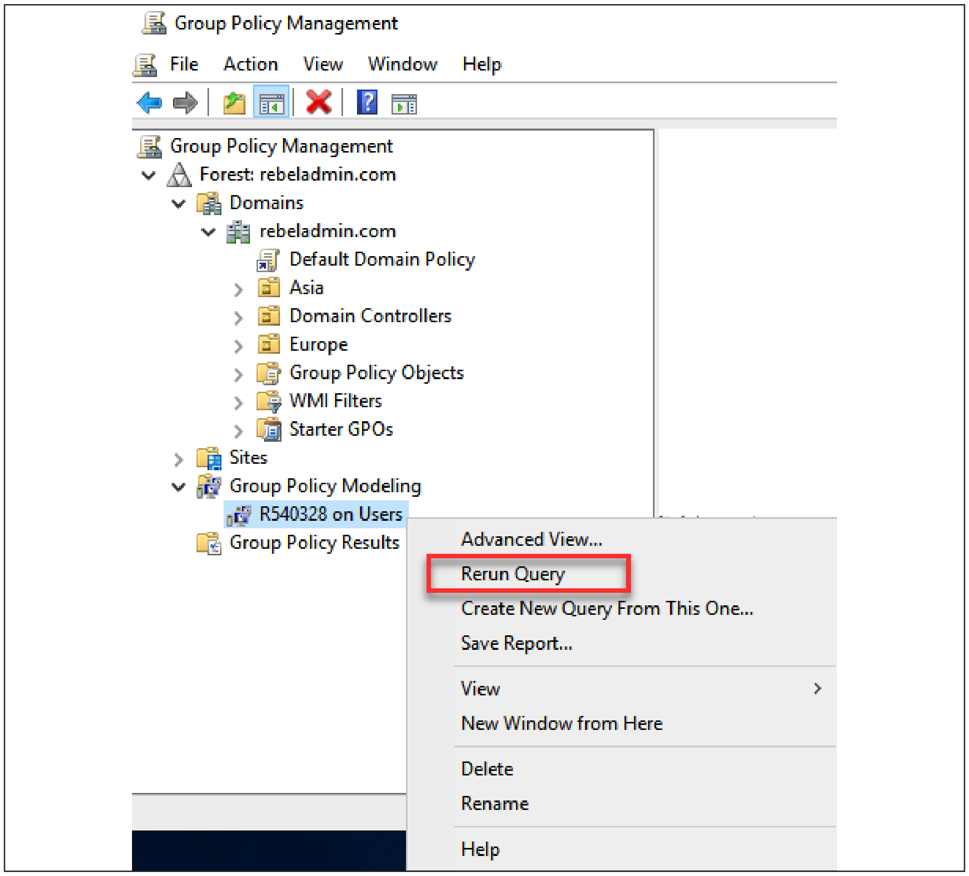


Figure 20.18: Rerun the simulation query

So far, we have only looked into issues related to on-prem Active Directory environments. If it is a hybrid environment, we have different services to maintain. In a hybrid environment, Azure AD Connect plays a major role and the health of this service is critical. Therefore, in the next section of this chapter, I am going to talk about the most common Azure AD Connect-related issues.

Common Azure AD Connect issues

When it comes to a hybrid AD setup, we have to work with different types of issues than in on-prem AD environments. Azure AD is a managed service by Microsoft, so there is nothing we can do to manage its health. Therefore, most of the hybrid AD issues are related to connectivity, directory sync, or authentication methods (password hash, pass-through authentication, federated).

The main component that connects an on-prem Active Directory environment with Azure AD is Azure AD Connect. So, most of the issues in a hybrid environment are also related to Azure AD Connect.

Connectivity issues

Azure AD Connect requires connectivity to the Azure AD service, to do the directory synchronization. The Azure AD Connect server also needs to be able to communicate with on-prem Active Directory Domain Controller. When there are directory synchronization issues, we will be able to see the following signs:

- New user accounts added in on-prem Active Directory do not appear in Azure AD or take a long time to appear (more than 30 minutes).
- After an on-premise user changes their password, they can't authenticate to Azure AD.
- If the password-writeback feature is being used, password reset in Azure AD does not work for on-premise users.
- We can see synchronization errors under Azure AD Connect Health.
- When there are directory sync issues, Azure AD will also send email notifications to directory administrators.

There can be many reasons for connectivity issues. But the most common reasons for connectivity issues are listed here:

- **Connection to the Azure AD service**: The Azure AD Connect server should have a stable connection to URLs, IP addresses, and port numbers (TCP 80 and 443) listed at `https://bit.ly/3r5GhTS`. You can simply verify the connectivity by using Telnet.
- **Connection to on-prem domain controllers**: If you have a firewall between the Azure AD Connect server and domain controllers, make sure you have the following ports open:

Protocol	**Ports**
DNS	53 (TCP/UDP)
Kerberos	88 (TCP/UDP)
MS-RPC	135 (TCP/UDP)
LDAP	389 (TCP/UDP)
SMB	445 (TCP/UDP)
LDAP/SSL	636 (TCP/UDP)
RPC	49152 – 65535 (Random high RPC port)(TCP/UDP)

- **Proxy in use**: If the organization is using a proxy for internet connectivity, make sure to update the `machin.config` file in `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config` with the proxy settings as follows:

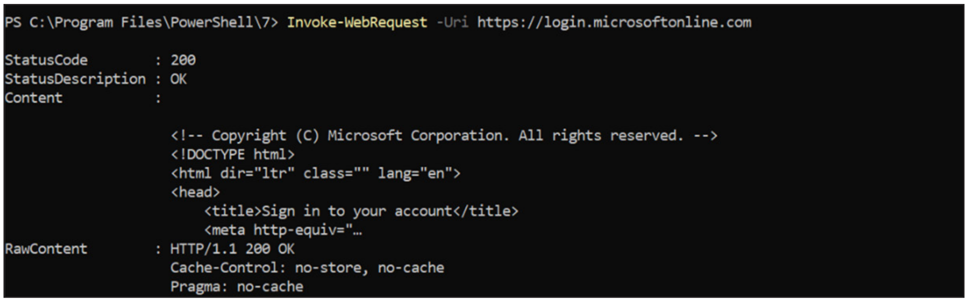
```
<system.net>
        <defaultProxy>
                        <proxy
                        usesystemdefault="true"
                               proxyaddress="http://<proxyserver
address>:<proxyport>"
                               bypassonlocal="true"
            />
        </defaultProxy>:
</system.net>
```

  This should be added to the end of the file. You also need to make sure the proxy is allowed to access Office 365 URLs and IP address ranges. I shared the relevant link earlier.

  We can verify the connectivity by using the following PowerShell command:

```
Invoke-WebRequest -Uri https://bit.ly/3l0EXxt
```

  This command verifies the connectivity to the MSOnline login page. If the connection succeeds, you should receive status code `200`.



```
PS C:\Program Files\PowerShell\7> Invoke-WebRequest -Uri https://login.microsoftonline.com

StatusCode        : 200
StatusDescription : OK
Content           :

                    <!-- Copyright (C) Microsoft Corporation. All rights reserved. -->
                    <!DOCTYPE html>
                    <html dir="ltr" class="" lang="en">
                    <head>
                        <title>Sign in to your account</title>
                        <meta http-equiv="…
RawContent        : HTTP/1.1 200 OK
                    Cache-Control: no-store, no-cache
                    Pragma: no-cache
```

Figure 20.19: Test connectivity

  If the status code is `403`, it means the proxy can't reach the URL. This is because the relevant URLs are not allowed in the proxy. If the status code is `407`, it means the proxy is expecting user authentication but none was provided. If the proxy needs authentication, the relevant settings need to be added to the `machine.config` file.

- **Firewall Issues** – Lots of organizations use layer 7 firewalls these days instead of proxies. If the AD Connect server is behind a layer 7 firewall, make sure the relevant firewall rules are in place to allow access to Office 365 URLs and IP address ranges.
- **DNS issues** – To make a connection to Azure AD as well as on-prem domain controllers, the Azure AD Connect server should be able to resolve internal and external hostnames (FQDNs). If the firewall or proxy connectivity is not preventing communication, check if you can resolve DNS names.

Synchronization errors

Apart from connectivity issues, Active Directory object synchronization issues also have a major impact on the health of the hybrid Active Directory environment. Let's go ahead and look into some of the common synchronization issues.

Duplicate attributes

Let's assume we have two users in on-prem AD called John Smith and Jason Smith. The email address is set to `j.smith@rebeladmin.com` for both users (first name initial and last name). Since the proxy address attribute is the same for both user objects, Azure AD will give a **Duplicate Attribute** error. This can be easily fixed by removing or modifying the duplicate attribute values for the on-prem users.

Azure AD schema doesn't allow two objects to have the same value for the following attributes:

- UserPrincipalName
- ObjectId
- ProxyAddresses
- onPremisesSecurityIdentifier

Data mismatch

In an Azure AD hybrid environment, when a new object is added or an existing object is updated in on-prem Active Directory, it needs to sync back to Azure AD. This is done by Azure AD Connect. During the sync process, two attribute values are compared to check if it is a new object or an existing object for Azure AD. These two attributes are `sourceAnchor` and `immutableId`. Even though they are two attributes, they refer to the same value. When an object comes from Azure AD Connect, this particular object value is called `sourceAnchor`.

The same object value in Azure AD is called `immutableId`. The word *immutable* means cannot be changed. Similarly, once the `immutableId` value is defined in Azure AD, it cannot be changed.

When AD sync is initiated from on-prem AD, Azure AD compares the `sourceAnchor` attribute of objects with the `immutableId` attribute of objects. If they match, we can say they are a hard match. If Azure AD can't find a match, it means the object does not exist in Azure AD. In that situation, Azure AD will treat it as a new object. However, just before Azure AD creates a new object, it checks if this user object's `ProxyAddresses` and `UserPrincipalName` attributes have unique values. This is to make sure there are no duplicate objects in Azure AD. This match is called a soft match. Sometimes, in a hybrid AD environment, there can be objects that don't have a hard match but do have a soft match. This type of error is logged in Azure AD as an `InvalidSoftMatch` error. There are many reasons that can cause an `InvalidSoftMatch` error:

- Multiple objects exist in the on-prem Active Directory with the same `ProxyAddresses` or `UserPrincipalName` attributes. In such a situation, Azure AD can only create one object.
- A new object is added to on-prem Active Directory with the same `ProxyAddresses` or `UserPrincipalName` attribute but Azure AD already has an object with the same values. In such a scenario, this new object will not sync to Azure AD.
- An already synced object moved from one Active Directory forest to another. This will change the `sourceAnchor` attribute of the object.
- The Azure AD Connect server reinstalled or moved to a different server with new `sourceAnchor` attribute value.
- An Active Directory user account was deleted and recreated with the same attributes before Azure AD remove the deleted account. It will also create an `InvalidSoftMatch` error.

We can fix `InvalidSoftMatch` errors using the following methods:

- Identify the object with conflicting `ProxyAddresses` or `UserPrincipalName` attributes. If both of these objects need to sync with Azure AD, change those attributes to unique values.
- Exclude the objects with conflicting `ProxyAddresses` or `UserPrincipalName` attributes from the sync scope if not every object needs to sync with Azure AD.
- Some of the conflicting objects may not need to exist in Active Directory anymore or the conflicting value may not need to be associated with an object anymore. In such situations, we can remove the object or update the attribute value.

All of the above changes should be done in on-prem Active Directory and let Azure AD Connect sync the changes.

In some scenarios, the objects involved in a soft match are not the same object type.

As an example, there could be a user account and a contact with the same `ProxyAddresses` value. This is called an `ObjectTypeMismatch` error. These errors can also be fixed using the methods listed above.

Data validation failure

Azure AD does not accept all data coming from Azure AD Connect to be written into the directory. Azure AD is a managed service, so it has its own restrictions to maintain data integrity. As an example, for the `UserPrincipalName` attibute, Azure AD has the following restrictions:

- `userPrincipalName` must be in the email address format with the `@` sign.
- `userPrincipalName` only should have a maximum of 113 characters. Out of 113, you should only have 64 characters before the `@` sign and only 48 after the `@` sign.
- Azure AD does not accept \ % & * + / = ? { } | < > ( ) ; : , [ ] " ' for `userPrincipalName`.
- `userPrincipalName` cannot have spaces.
- `userPrincipalName` should only use routable domain names. It should not have local or internal domain names.

If the incoming object does not comply with restrictions, it will give a `Data Validation Failure` error.

Large attributes

Similar to on-prem Active Directory attributes, Azure AD also has size limits for attributes, which are defined by its schema. If an incoming object exceeds these limits, Azure AD will issue a `LargeObject` or `ExceededAllowedLength` error. This happens mainly for the following attributes:

- proxyAddresses
- userCertificate
- thumbnailPhoto
- userSMIMECertificate

As an example, the maximum number of `proxyAddresses` accepted by Azure AD is 200.

Existing admin role conflict

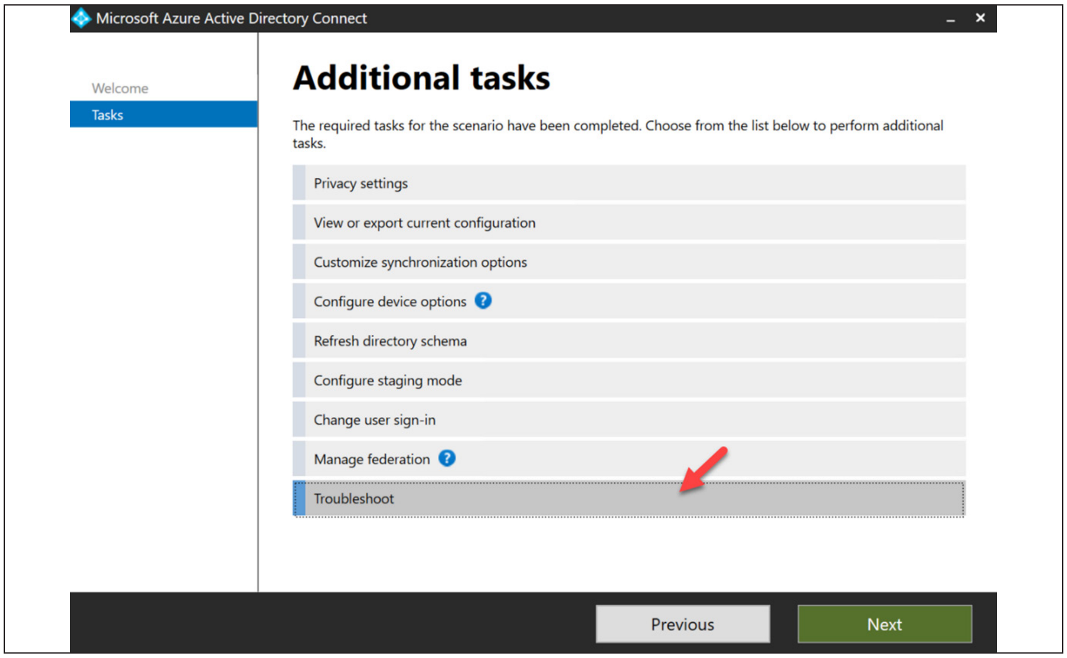
If an Azure AD administrative role holder has a **soft match** for the `userPrincipalName` attribute, Azure AD will issue an **Existing Admin Role Conflict sync error**. This error can be fixed by removing the administrative role from the conflicting object. This will resume the replication and after the sync process is completed, we can assign the administrative role to the object.

In this section, I have only listed down the most common issues related to Azure AD Connect object synchronization. Apart from those authentication issues, single-sign-on issues and design issues can also have a direct impact on the health of an Azure AD hybrid environment.

Azure AD Connect troubleshooting

Azure AD Connect Health is the best place to identify Azure AD Connect issues. I explained this tool in the previous chapter. Apart from Azure AD Connect Health, we also can use the built-in Azure AD Connect Troubleshooting Tool to troubleshoot Azure AD Connect-related issues.

To use this tool, Open Azure AD Connect and, under **Additional tasks**, select **Troubleshoot** and then click on **Next**.



Microsoft Azure Active Directory Connect

Additional tasks

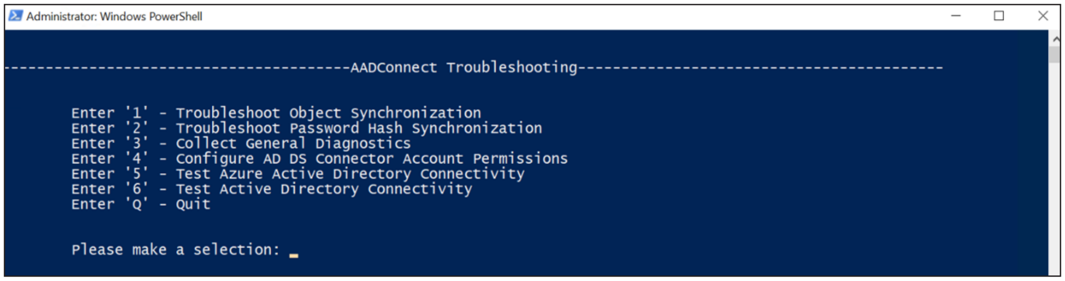
The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

Figure 20.20: Azure AD Connect Troubleshooting Tool

When we launch the tool, it will give us the following options:

- **Troubleshoot Object Synchronization**
- **Troubleshoot Password Hash Synchronization**
- **Collect General Diagnostics**
- **Configure AD DS Connector Account Permissions**
- **Test Azure Active Directory Connectivity**
- **Test Active Directory Connectivity**
- **Quit**

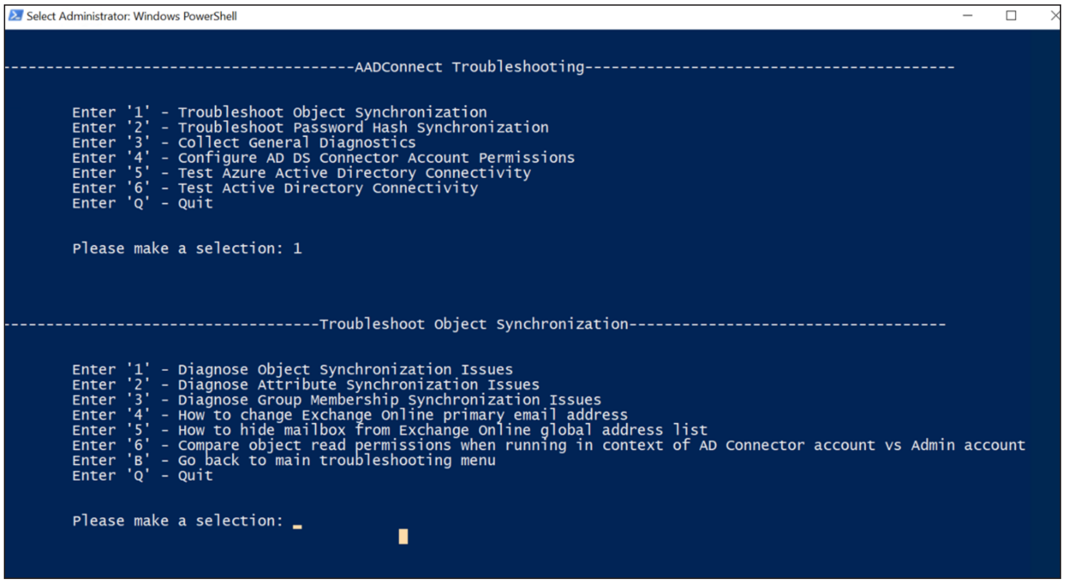
Depending on the issue, we can select the closest option to proceed with.



```
----------------------------------------AADConnect Troubleshooting------------------------------------------

        Enter '1' - Troubleshoot Object Synchronization
        Enter '2' - Troubleshoot Password Hash Synchronization
        Enter '3' - Collect General Diagnostics
        Enter '4' - Configure AD DS Connector Account Permissions
        Enter '5' - Test Azure Active Directory Connectivity
        Enter '6' - Test Active Directory Connectivity
        Enter 'Q' - Quit

        Please make a selection: _
```

Figure 20.21: Troubleshooting options

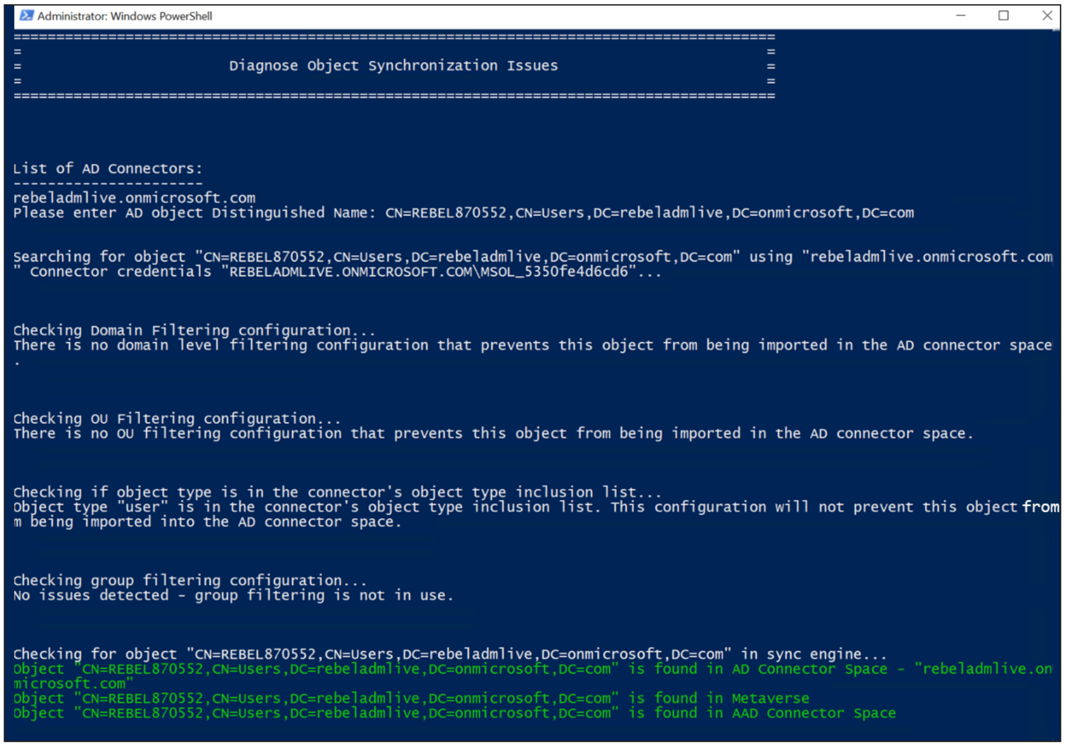
Based on the selection, the tool will provide additional options to proceed with.



```
----------------------------------------AADConnect Troubleshooting------------------------------------------

        Enter '1' - Troubleshoot Object Synchronization
        Enter '2' - Troubleshoot Password Hash Synchronization
        Enter '3' - Collect General Diagnostics
        Enter '4' - Configure AD DS Connector Account Permissions
        Enter '5' - Test Azure Active Directory Connectivity
        Enter '6' - Test Active Directory Connectivity
        Enter 'Q' - Quit

        Please make a selection: 1



------------------------------------Troubleshoot Object Synchronization------------------------------------

        Enter '1' - Diagnose Object Synchronization Issues
        Enter '2' - Diagnose Attribute Synchronization Issues
        Enter '3' - Diagnose Group Membership Synchronization Issues
        Enter '4' - How to change Exchange Online primary email address
        Enter '5' - How to hide mailbox from Exchange Online global address list
        Enter '6' - Compare object read permissions when running in context of AD Connector account vs Admin account
        Enter 'B' - Go back to main troubleshooting menu
        Enter 'Q' - Quit

        Please make a selection: _
```

Figure 20.22: Additional troubleshooting options

Once the relevant selections are made, the tool will start the troubleshooting process. At the end of the troubleshooting, the tool will provide a report with its findings.



```
=========================================================================================
=                                                                                       =
=                         Diagnose Object Synchronization Issues                        =
=                                                                                       =
=========================================================================================



List of AD Connectors:
----------------------
rebeladmlive.onmicrosoft.com
Please enter AD object Distinguished Name: CN=REBEL870552,CN=Users,DC=rebeladmlive,DC=onmicrosoft,DC=com


Searching for object "CN=REBEL870552,CN=Users,DC=rebeladmlive,DC=onmicrosoft,DC=com" using "rebeladmlive.onmicrosoft.com
" Connector credentials "REBELADMLIVE.ONMICROSOFT.COM\MSOL_5350fe4d6cd6"...



Checking Domain Filtering configuration...
There is no domain level filtering configuration that prevents this object from being imported in the AD connector space
.



Checking OU Filtering configuration...
There is no OU filtering configuration that prevents this object from being imported in the AD connector space.



Checking if object type is in the connector's object type inclusion list...
Object type "user" is in the connector's object type inclusion list. This configuration will not prevent this object from
m being imported into the AD connector space.



Checking group filtering configuration...
No issues detected - group filtering is not in use.



Checking for object "CN=REBEL870552,CN=Users,DC=rebeladmlive,DC=onmicrosoft,DC=com" in sync engine...
Object "CN=REBEL870552,CN=Users,DC=rebeladmlive,DC=onmicrosoft,DC=com" is found in AD Connector Space - "rebeladmlive.on
microsoft.com"
Object "CN=REBEL870552,CN=Users,DC=rebeladmlive,DC=onmicrosoft,DC=com" is found in Metaverse
Object "CN=REBEL870552,CN=Users,DC=rebeladmlive,DC=onmicrosoft,DC=com" is found in AAD Connector Space
```

Figure 20.23: Results of tests

If it is not possible to solve the issue using the two tools/services explained above, we can always go to Microsoft Support for further support.

How to troubleshoot AD DS database-related issues

Active Directory maintains a multi-master database. Like any other system, the Active Directory database can also have data corruption, crashes, and data loss. In my entire career, I still haven't come across a situation where a full database recovery was required in a production environment. The reason for this is that an AD DS database keeps replicating to other available domain controllers and it is very rare for all the available domain controllers to crash at the same time and lose data. Unlike other Active Directory issues, there aren't many options for AD DS database troubleshooting.

In the following table, I have listed a few reasons for AD DS database-related issues:

Issue	Description
Hardware failure	The Active Directory database is located in `C:\Windows\NTDS`. This path can be changed, but it cannot be hosted on separate systems. If there is any hardware failure, then we will lose the database along with the domain controller. If there are multiple domain controllers, then recovery is not required as we can simply introduce a new domain controller. If it's an FSMO role holder, then it is still possible to seize roles from any working domain controller and make it the new FSMO role holder.
Software failures	Active Directory runs on top of Windows. System software or any related service corruption can put the Active Directory database in an unusable status. This can also be caused by viruses or malware attacks.
Unexpected shutdown	Unexpected shutdowns can also corrupt an Active Directory database.

In order to prevent AD DS database-related issues, we can take the following precautions:

Option	Description
Back up the AD DS database	In *Chapter 11*, *Active Directory Services*, we looked at Active Directory backup options. There are many tools out there on the market that can be used to back up Active Directory. The success of a backup or disaster recovery solution depends on how quickly and easily it can bring the system back to a working state.
Maintain additional domain controllers	It is not recommended for you to have just one domain controller, even if it's covered with a disaster recovery solution. Each AD site should at least maintain two domain controllers. This is the fastest way to recover from any type of AD DS disaster. If any domain controller becomes unusable, then the other available domain controllers can continue operations with minimal interruptions.
Change the AD DS database and log path	The default location of the AD DS database file and the log files is `C:\Windows\NTDS`. It is recommended that you change the path to a different drive. It can protect database files from OS-level corruption. In *Chapter 11*, *Active Directory Services*, we learned about how we can change the default path.
Defragmentation	Like any other database system, AD DS databases can also have data de fragmentation. There are two types of data defragmentation. AD database uses online defragmentation, and it runs every 12 hours automatically. However, after a large number of object cleanups or a large configuration change, it is recommended that you initiate offline defragmentation. The complete process was explained in *Chapter 11*, *Active Directory Services*.

By running an integrity check on an Active Directory database, we can identify binary-level data corruption. Next, we are going to look into integrity checks further.

Integrity checking to detect low-level database corruption

Integrity checks come as part of the `Ntdsutil` tool, which is used for Active Directory database maintenance. This goes through every byte of the database file. The `integrity` command also checks whether the correct headers exist in the database itself and whether all the tables are functioning and consistent. This process also runs as part of **Directory Services Restore Mode** (**DSRM**).

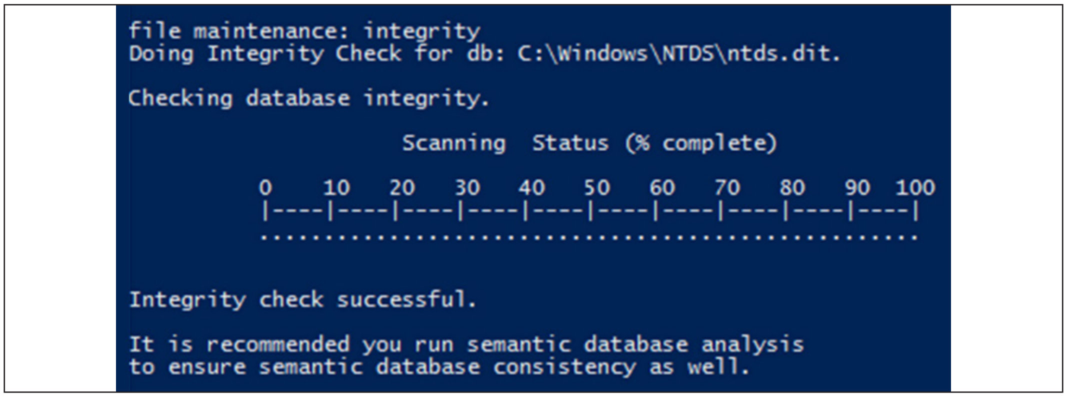
This check needs to be run with the **Windows NT Directory Services** (**NTDS**) service off.

In order to run an integrity check, take the following steps:

1. Log in to the domain controller as Domain/Enterprise Admin.
2. Open PowerShell as an administrator.
3. Stop the NTDS service using `net stop ntds`.
4. Type the following:

```
ntdsutil
activate instance ntds
files
integrity
```

The output is as follows:



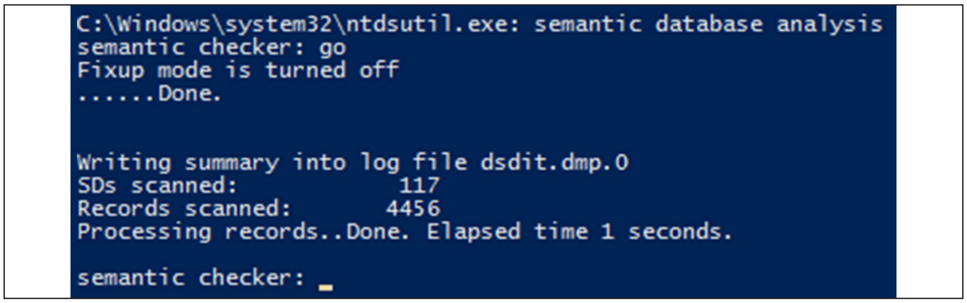
```
file maintenance: integrity
Doing Integrity Check for db: C:\Windows\NTDS\ntds.dit.

Checking database integrity.

                    Scanning  Status (% complete)

          0    10    20    30    40    50    60    70    80    90   100
          |----|----|----|----|----|----|----|----|----|----|----|
          ...................................................


Integrity check successful.

It is recommended you run semantic database analysis
to ensure semantic database consistency as well.
```

Figure 20.24: NTDS integrity check

5. To exit from the utility, type `quit`.
6. It is also recommended that you run `semantic database analysis` to confirm the consistency of the AD database contents. In order to do this, enter the following:

    ```
    ntdsutil
    activate instance ntds
    semantic database analysis
    go
    ```

    The output is as follows:

    ```
    C:\Windows\system32\ntdsutil.exe: semantic database analysis
    semantic checker: go
    Fixup mode is turned off
    ......Done.


    Writing summary into log file dsdit.dmp.0
    SDs scanned:              117
    Records scanned:         4456
    Processing records..Done. Elapsed time 1 seconds.

    semantic checker: _
    ```

    Figure 20.25: Semantic database analysis

7. If any integrity issues are detected, then you can type `go fixup` to fix the errors.
8. After the process is completed, type `net start ntds` to start the NTDS service.

If there is database corruption that cannot be soft recovered (using the preceding method and the `ntdsutil` recovery command), then you need to recover it from a backup. In order to recover an Active Directory database using a system-state-based backup, we need to use. The relevant recovery steps using DSRM were explained in *Chapter 11*, *Active Directory Services*.

As I mentioned before, Active Directory database issues are very rare in Active Directory environments. If there are any, then you can probably recover from the situation using other options, rather than restoring Active Directory from a backup. This should be the last resort in the troubleshooting process.

Summary

As with any other IT system, Active Directory components can face issues that can impact their operations. This can be due to many reasons, such as poor design, the result of a management task, hardware or software issues, and resource issues. No one is expected to know how to fix each and every Active Directory-related issue. The most important thing is the starting point of the troubleshooting process and the engineer's approach to finding the solution. This chapter showed you how to troubleshoot the most common Active Directory infrastructure issues with the correct approach.

We started the chapter with Active Directory replication issues. We looked into different scenarios that can cause replication issues and how we can recover from them. Then, we looked into Group Policy-related issues and how to troubleshoot them using Windows' built-in utilities. Azure AD Connect is the component that syncs on-prem objects and attribute values to Azure AD. Therefore, its health is crucial for a hybrid environment. In this chapter, we learned about the most common Azure AD Connect issues. Last but not least, we learned about AD DS database-related issues.

We are all living in very challenging times. The Covid-19 pandemic accelerated digital transformation and working from home become the new norm. This opened up a whole new level of challenges for IT professionals. "Identity" is definitely one of those challenges. We no longer can meet modern authentication and authorization requirements by just using on-prem Active Directory. We no longer can protect identities by using the traditional perimiter defense model. More than ever, we can clearly see why a cloud-only or hybrid identity model with Azure AD is a more appropriate way to address modern identity-related challenges. Throughout this book, I have explained the value of the hybrid identity model and the value of Azure AD, but we need to start this journey somewhere. If we do not design, manage, and secure on-prem Active Directory properly we can't experience the full potential of the hybrid identity model. The whole purpose of this book was to help IT professionals to improve their knowledge and confidence so they can help organizations to have the best of both worlds.

Thank you for purchasing this book. Your feedback would be greatly appreciated. Please feel free to send your feedback to `rebeladm@live.com`. I also encourage you to follow me on my blog, `https://bit.ly/3oPi416`, and on Twitter, `@rebeladm`, as I am constantly sharing Active Directory-related content. I wish you good health, all success, happiness, and joy in your life.