Troubleshooting Active Directory Replication Errors

Analysis and Troubleshooting

Microsoft Windows Server 2012 R2 Datacenter

Hands-on lab

This lab walks you through the troubleshooting, analysis and resolution phases of commonly encountered Active Directory replication errors. You will use ADREPLSTATUS, repadmin.exe and other tools to troubleshoot a five DC, three-domain environment.

TechEd

Europe 2014

Acknowledgments	
Author	Justin Turner
Bio	Justin is a Support Topic Lead and Senior Support Escalation Engineer with the Identity (Directory Services) team based in Irving, Texas, USA. He has created or contributed to many training courses, knowledge base and TechNet articles for Microsoft over the past 14 years. He teaches Microsoft employees and customers new product architecture, is a charter Microsoft Certified Master (MCM), Microsoft Certified Trainer (MCT) and holds an M.S. degree in Computer Education and Cognitive Systems (Instructional Systems Design).
Research	This lab includes research by the following: ***Ken Brumfield, Arren Conner, David Everett, John Kuehler, Glenn LeCheminant, Herbert Mauerer, Joey Seifert, Chris Simpkiss*** *and* ***Justin Turner***
Reviewers	Many thanks to the following individuals that spent their own time reviewing and providing feedback: *Chad Duffey, Ken Brumfield, Wayne McIntyre, Rob Lane, John Wu, Jack Poehlman, Bryan Debnam, Bryan Zink, Mike Yock, Richard Leung, Milan Tresnak and Ashley McGlone*

Introduction

Estimated time to complete this lab

75 minutes

Objectives

After completing this lab, you will be able to:

- Troubleshoot and resolve five of the most common Active Directory (AD) replication errors.
- Analyze replication metadata using ADREPLSTATUS, repadmin and configuration settings in order to diagnose replication failures.
- Use troubleshooting tools to identify configuration problems or failures in AD Replication dependencies: DNS, RPC, LDAP & Kerberos.

Prerequisites

Before working on this lab, you must have an understanding of the following:

- Active Directory logical model
- Active Directory replication model
    - Active Directory replication concepts
    - Active Directory replication topology
- Basic DNS concepts
- Basic Kerberos concepts

However, detailed step-by-step instructions are included, so those new to Active Directory replication troubleshooting will be able to follow along.

More:

The appendix contains a lot more detail, background information, sample log output, references and information on how to reproduce the issues in a lab. Ensure you save off the document for later reference.

Overview of the lab

This lab will walk learners through the troubleshooting, analysis and resolution phases of commonly encountered Active Directory replication errors. Learners will use ADREPLSTATUS, repadmin.exe and PowerShell to troubleshoot a five DC, three-domain environment.

Scenario

Active Directory replication problems are one of the top support call generators for Microsoft. AD replication failures cause innumerous problems in other applications and services that rely on the consistency of the data stored in Active Directory. This lab presents five of the most commonly encountered AD replication problems.

Computers in this lab

This lab uses computers as described in the following table.

Virtual Machine	Role	IP Address	DNS Client settings
DC1.root.contoso.com	Domain controller in the forest root domain, DNS, GC, All FSMO roles	192.168.10.1	192.168.10.2; 127.0.0.1
DC2.root.contoso.com	Domain controller in the forest root domain, DNS, GC	192.168.10.2	192.168.10.1; 127.0.0.1
ChildDC1.child.root.contoso.com	Domain controller in a child domain in the forest, DNS, GC, Domain-wide FSMO roles	192.168.10.11	192.168.10.1; 127.0.0.1
ChildDC2.child.root.contoso.com	Read-only domain controller (RODC) in the child domain in the forest, DNS, GC, MinShell	192.168.10.12	192.168.10.11; 127.0.0.1
TRDC1.treeroot.fabrikam.com	Domain controller in a tree-root domain in the forest, DNS, GC, Domain-wide FSMO roles	192.168.10.21	127.0.0.1; 192.168.10.1
WIN8Client.root.contoso.com	Windows 8.1 administration workstation in the forest root domain	192.168.10.5	192.168.10.1; 192.168.10.2

All user accounts in this lab use the password adrepl123!

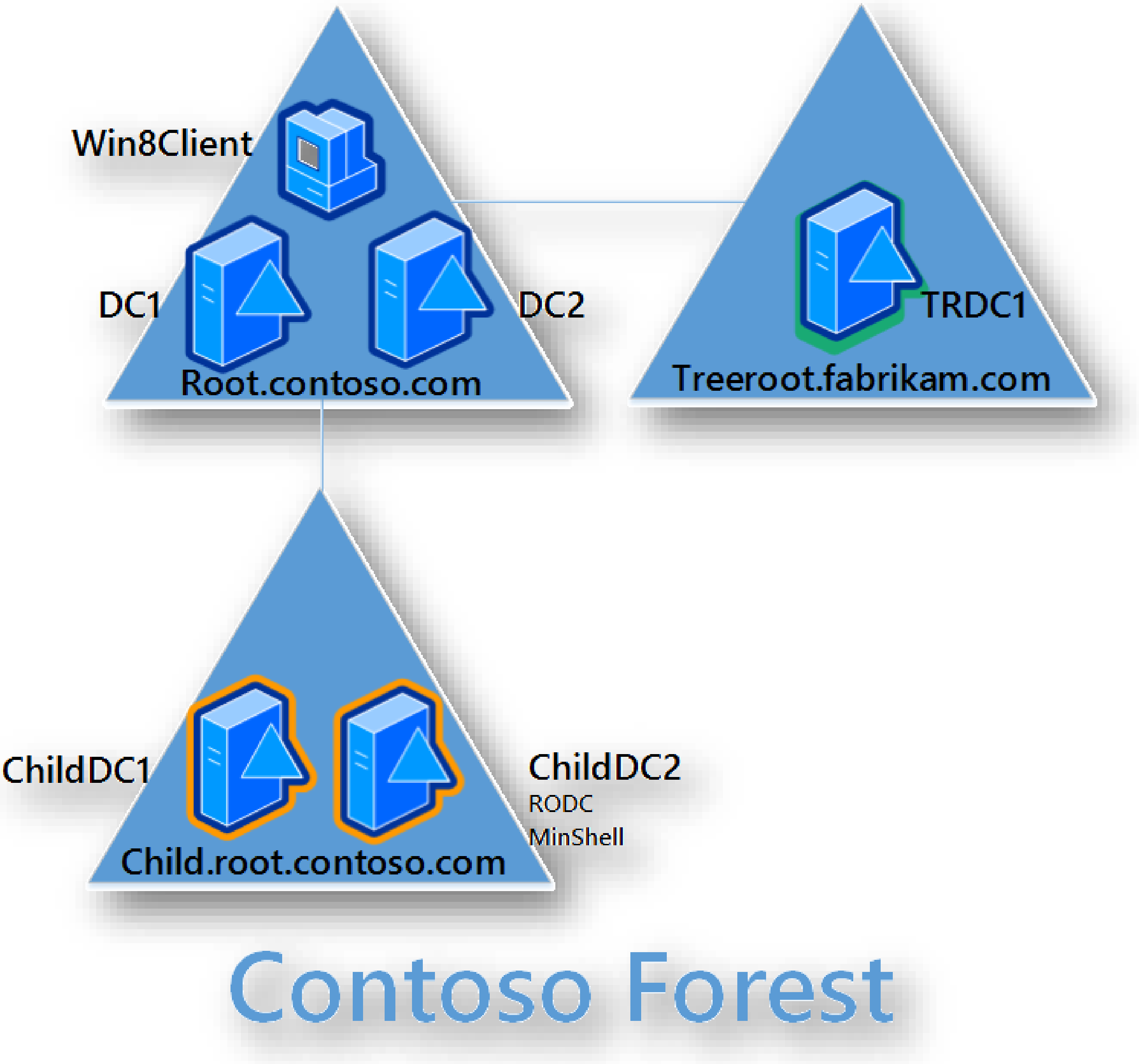


Figure 1 Lab environment

Exercise 1: AD replication symptom identification

In this exercise, you will use repadmin.exe, the AD Replication Status tool (adreplstatus.exe) and Windows PowerShell to display the Active Directory replication status for the Contoso forest. Each task presents a different method to accomplish the same thing.

Exercise setup:

Manually initiate replication on DC1 from all replica DCs using one of the following methods.

- Repadmin /syncall DC1 /Aed
- Using DSSITE.msc

  On a per-partition, per source DC basis
- Repadmin /replicate DC1 DC2 "dc=root,dc=contoso,dc=com"

Task 1 - Use the AD Replication Status tool to view forest-wide AD replication health

In this task, you will use the **AD replication Status Tool** to view the current state of AD replication in the Contoso environment.

More:

AD Replication Status Tool is publicly downloadable from Microsoft.com
Prerequisites

- .NET Framework 4.0
- Network connectivity to all DCs from any supported version of Windows client or Windows Server (not core) that is domain joined
- Domain user account

You will use **Win8Client** in this task.

1. Connect to **Win8Client** for this task.
   - The ROOT\Administrator account is already logged on to this machine.
   - Note: Domain admin privileges are not needed for this task, but these privileges are required in later exercises.
2. Open an elevated command prompt and use repadmin to verify that Win8Client can connect to DC1.

```
Repadmin /bind dc1
```

Important:

If the above command returned data proceed to step 3. If it fails with an LDAP error 82, do the following:

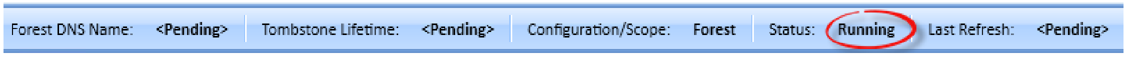
- Switch to **DC2** and pause the virtual machine by selecting **Pause** from the holSystems Launchpad
- Switch to **Win8Client** and attempt to bind to DC1 again:

```
Repadmin /bind dc1
```

- When this completes and returns data, switch back to **DC2** and click **Resume**

The above steps may be necessary if Win8Client uses DC2 for KDC operations. For this task, we need the client to use DC1 as a KDC since DC2 has been intentionally broken for a later exercise. The issue with DC2 is resolved in exercise 2.

3. On **Win8Client**, double click the **AD Replication Status Tool 1.0** shortcut on the desktop.
4. Within the AD Replication Status Tool, click **Refresh Replication Status**.
   - The tool will take one to two minutes to check the AD replication status.
   - You will know data collection is complete when the **Status:** prompt changes from **Running** to **Ready** and the focus is switched to the **Replication Status Viewer** tab.

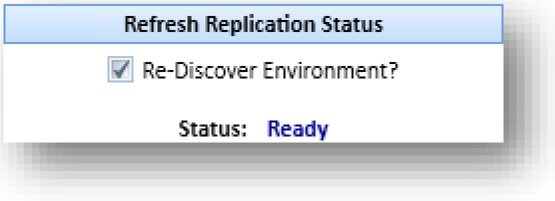


Forest DNS Name: <Pending> Tombstone Lifetime: <Pending> Configuration/Scope: Forest Status: Running Last Refresh: <Pending>

   - Note that replication status is reported for three DCs, but there are actually five DCs in the forest. You will see why replication status is missing from two DCs in the next step.
5. The **Configuration/Scope Settings** tab displays the results of the data collection.
   - Click the **Configuration/Scope Settings** tab.
   - The **Replication Status Collection Details** pane lists all DCs in which the tool was able to collect data.
     - Review the **Environment Discovery** tab for any errors.
     - Take note there is an error for child.root.contoso.com.
     - The **Discovery Missing Domain Controllers** tab notes that NTDS Settings objects exist but since discovery failed for the child domain, the tool was unable to collect data from these DCs: ChildDC1 and ChildDC2. This issue is resolved in Exercise 3.

Important:

When refreshing replication status on future runs of the tool, ensure you select the **Re-Discover Environment** option so it will attempt to collect data from the child domain DCs.



☑ Re-Discover Environment?

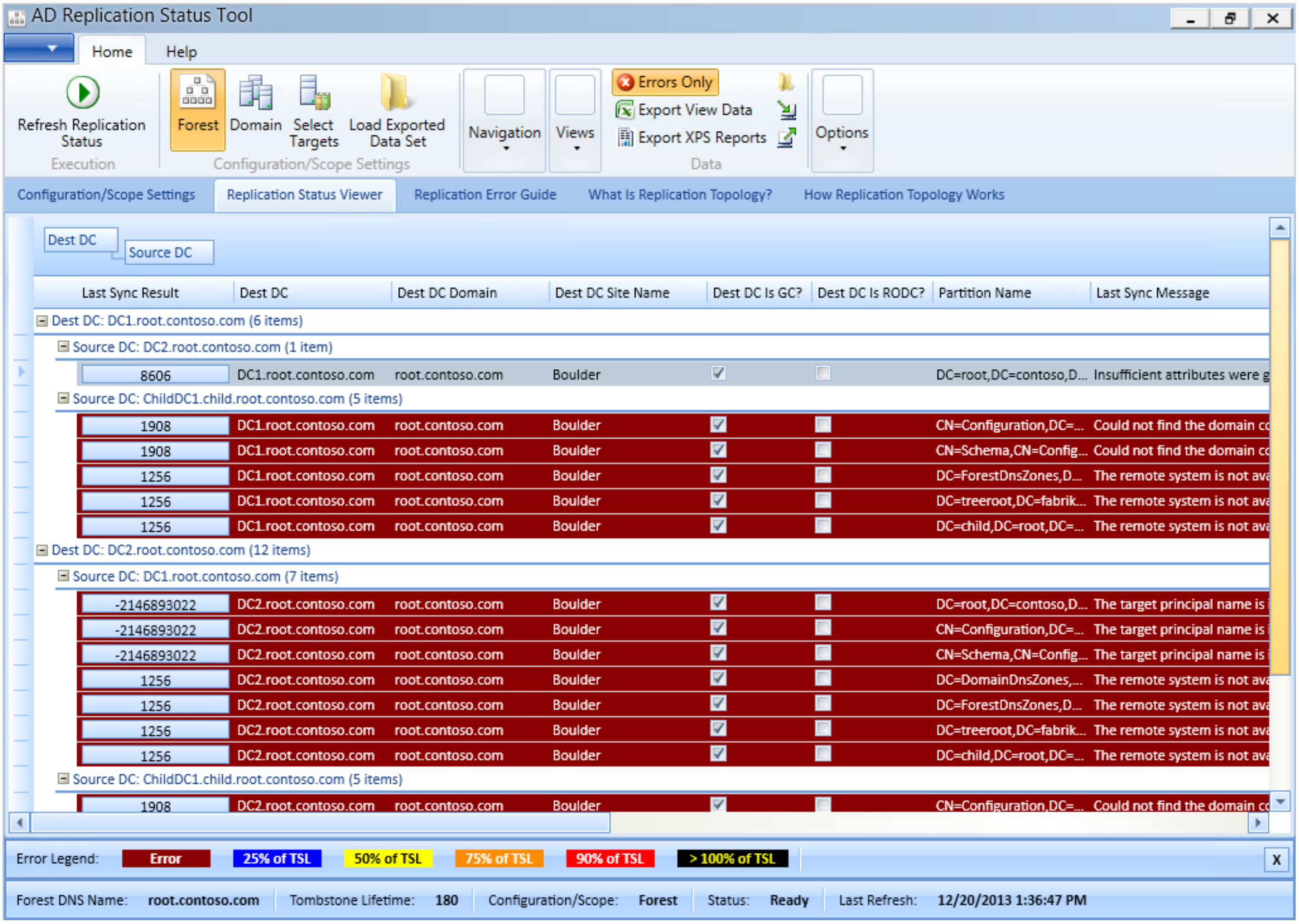
Status: Ready

6. Click the **Replication Status Viewer** tab, and then select **Errors Only**.

   Errors currently reported in the environment: -2146893022, 1908, 1256 and 8606

Note:

If error 8614 is observed, you will need to perform the steps in Exercise 6 at some point in the lab.


AD Replication Status Tool
Home
Help
Refresh Replication Status
Execution
Forest
Domain
Select Targets
Load Exported Data Set
Configuration/Scope Settings
Navigation
Views
Errors Only
Export View Data
Export XPS Reports
Data
Options
Configuration/Scope Settings
Replication Status Viewer
Replication Error Guide
What Is Replication Topology?
How Replication Topology Works
Dest DC
Source DC

Last Sync Result	Dest DC	Dest DC Domain	Dest DC Site Name	Dest DC Is GC?	Dest DC Is RODC?	Partition Name	Last Sync Message
⊟ Dest DC: DC1.root.contoso.com (6 items)							
⊟ Source DC: DC2.root.contoso.com (1 item)							
8606	DC1.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=root,DC=contoso,D...	Insufficient attributes were g
⊟ Source DC: ChildDC1.child.root.contoso.com (5 items)							
1908	DC1.root.contoso.com	root.contoso.com	Boulder	☑	☐	CN=Configuration,DC=...	Could not find the domain c
1908	DC1.root.contoso.com	root.contoso.com	Boulder	☑	☐	CN=Schema,CN=Config...	Could not find the domain c
1256	DC1.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=ForestDnsZones,D...	The remote system is not ava
1256	DC1.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=treeroot,DC=fabrik...	The remote system is not ava
1256	DC1.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=child,DC=root,DC=...	The remote system is not ava
⊟ Dest DC: DC2.root.contoso.com (12 items)							
⊟ Source DC: DC1.root.contoso.com (7 items)							
-2146893022	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=root,DC=contoso,D...	The target principal name is
-2146893022	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	CN=Configuration,DC=...	The target principal name is
-2146893022	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	CN=Schema,CN=Config...	The target principal name is
1256	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=DomainDnsZones,...	The remote system is not ava
1256	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=ForestDnsZones,D...	The remote system is not ava
1256	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=treeroot,DC=fabrik...	The remote system is not ava
1256	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	DC=child,DC=root,DC=...	The remote system is not ava
⊟ Source DC: ChildDC1.child.root.contoso.com (5 items)							
1908	DC2.root.contoso.com	root.contoso.com	Boulder	☑	☐	CN=Configuration,DC=...	Could not find the domain c

Error Legend: Error | 25% of TSL | 50% of TSL | 75% of TSL | 90% of TSL | > 100% of TSL

Forest DNS Name: **root.contoso.com** | Tombstone Lifetime: **180** | Configuration/Scope: **Forest** | Status: **Ready** | Last Refresh: **12/20/2013 1:36:47 PM**

7. Click the **Replication Error Guide** tab.
8. Click on the message text for any error. A list of DCs with that replication status is displayed in the bottom pane.
9. Click on any error code. Our recommended troubleshooting content on TechNet is displayed (if the machine has Internet access). Click the **Detected Errors Summary** tab to see the previous results.

Task 2 - Use repadmin to view forest-wide AD replication health

In this task, you will use repadmin.exe to display the AD replication results for the Contoso environment, and output it to a CSV file for later analysis.

Use **Win8Client** to perform the following task.

Note:

Repadmin /?:showrepl
"Displays the replication status when specified domain controller last attempted to inbound replicate Active Directory partitions.

Status is reported for each source DC that the destination has an inbound connection object from, grouped by partition. SHOWREPL helps administrators understand the replication topology and replication failures.

The REPADMIN console must have RPC network connectivity to all DC's targeted by the DCLIST parameter."

Use the Repadmin /showrepl command to display replication status for one or more DCs specified with the DSA_LIST parameter. Use **Repadmin /listhelp** from a command prompt, or see this section in the appendix for details about DSA_LIST options.

Repadmin /showrepl usage examples:

- Return replication status for DC1:
  Repadmin /showrepl DC1
- Return replication status for all DCs that reside in the Boulder site:
  Repadmin /showrepl site:Boulder
- Return replication status for all DCs in the forest and output to a CSV format into a file called showrepl.csv:
  Repadmin /showrepl * /csv >showrepl.csv

1. Open a command prompt and type the following command, and then press ENTER:

```
repadmin /showrepl * /csv >showrepl.csv
```

2. Take note of any errors reported on-screen. You will typically see an **LDAP error 81** for any DC the tool is unable to collect replication results. Since two LDAP errors are displayed on screen, we failed to collect data from two DCs. (this is due to an issue you will resolve in Exercise 3)
3. At the command prompt, type **showrepl.csv** to open the showrepl.csv file in Microsoft Excel
4. Within Microsoft Excel: from the **Home** menu, click **Format as Table** in the Styles section and click any of the table designs.
5. Hide column **A** and column **G**, by right clicking the column headers and select **Hide**

6. Reduce the width of other columns so that column K, **Last Failure Status** is visible.
7. In the **Last Failure Time** column, click the down arrow and deselect **0**

   This filters the spreadsheet so just the replication errors are displayed.

More: Repldiag.exe (available from CodePlex) can also be used to create an Excel importable XML file with this information.

What replication errors are present?

(Use column K)

When was replication last successful?

(Use column J)

Task 3 - Use repadmin and PowerShell to view forest-wide AD replication health

In this task, you will get replication status with repadmin and display it using PowerShell. This eliminates the need to use Microsoft Excel to display and filter the results.

Use **DC1** to perform the following task.

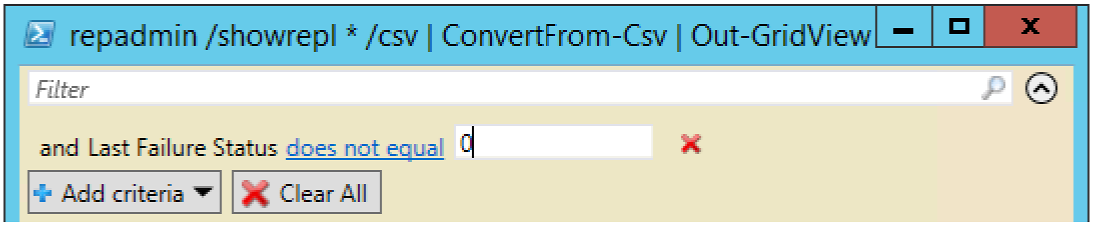
1. Open a PowerShell prompt and type the following commands, and then press ENTER:

PowerShell:

```
Repadmin /showrepl * /csv | convertfrom-csv | out-gridview
```

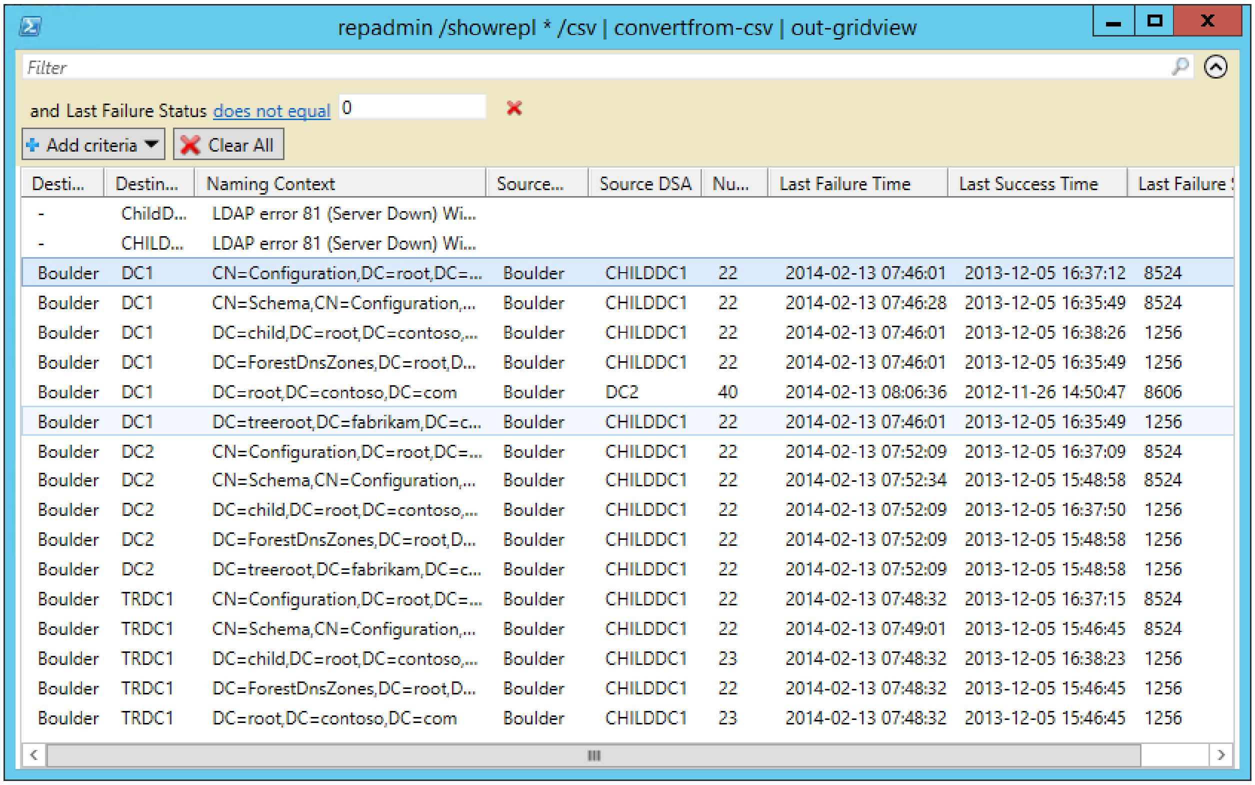
It is a good idea to view an unfiltered report initially to see both what is working and not working. To filter the output to just replication errors:

2. Select **Add criteria** and check **Last Failure Status**. Select **Add**.
3. From the "and Last Failure Status contains" filter criteria, select the blue-underlined word "**contains**" and select **does not equal**. Type **0** in the text box.



repadmin /showrepl * /csv | ConvertFrom-Csv | Out-GridView

and Last Failure Status does not equal 0



and Last Failure Status does not equal 0

Desti...	Destin...	Naming Context	Source...	Source DSA	Nu...	Last Failure Time	Last Success Time	Last Failure S
-	ChildD...	LDAP error 81 (Server Down) Wi...						
-	CHILD...	LDAP error 81 (Server Down) Wi...						
Boulder	DC1	CN=Configuration,DC=root,DC=...	Boulder	CHILDDC1	22	2014-02-13 07:46:01	2013-12-05 16:37:12	8524
Boulder	DC1	CN=Schema,CN=Configuration,...	Boulder	CHILDDC1	22	2014-02-13 07:46:28	2013-12-05 16:35:49	8524
Boulder	DC1	DC=child,DC=root,DC=contoso,...	Boulder	CHILDDC1	22	2014-02-13 07:46:01	2013-12-05 16:38:26	1256
Boulder	DC1	DC=ForestDnsZones,DC=root,D...	Boulder	CHILDDC1	22	2014-02-13 07:46:01	2013-12-05 16:35:49	1256
Boulder	DC1	DC=root,DC=contoso,DC=com	Boulder	DC2	40	2014-02-13 08:06:36	2012-11-26 14:50:47	8606
Boulder	DC1	DC=treeroot,DC=fabrikam,DC=c...	Boulder	CHILDDC1	22	2014-02-13 07:46:01	2013-12-05 16:35:49	1256
Boulder	DC2	CN=Configuration,DC=root,DC=...	Boulder	CHILDDC1	22	2014-02-13 07:52:09	2013-12-05 16:37:09	8524
Boulder	DC2	CN=Schema,CN=Configuration,...	Boulder	CHILDDC1	22	2014-02-13 07:52:34	2013-12-05 15:48:58	8524
Boulder	DC2	DC=child,DC=root,DC=contoso,...	Boulder	CHILDDC1	22	2014-02-13 07:52:09	2013-12-05 16:37:50	1256
Boulder	DC2	DC=ForestDnsZones,DC=root,D...	Boulder	CHILDDC1	22	2014-02-13 07:52:09	2013-12-05 15:48:58	1256
Boulder	DC2	DC=treeroot,DC=fabrikam,DC=c...	Boulder	CHILDDC1	22	2014-02-13 07:52:09	2013-12-05 15:48:58	1256
Boulder	TRDC1	CN=Configuration,DC=root,DC=...	Boulder	CHILDDC1	22	2014-02-13 07:48:32	2013-12-05 16:37:15	8524
Boulder	TRDC1	CN=Schema,CN=Configuration,...	Boulder	CHILDDC1	22	2014-02-13 07:49:01	2013-12-05 15:46:45	8524
Boulder	TRDC1	DC=child,DC=root,DC=contoso,...	Boulder	CHILDDC1	23	2014-02-13 07:48:32	2013-12-05 16:38:23	1256
Boulder	TRDC1	DC=ForestDnsZones,DC=root,D...	Boulder	CHILDDC1	22	2014-02-13 07:48:32	2013-12-05 15:46:45	1256
Boulder	TRDC1	DC=root,DC=contoso,DC=com	Boulder	CHILDDC1	23	2014-02-13 07:48:32	2013-12-05 15:46:45	1256

When did DC1 last successfully replicate the ROOT partition from DC2?

DC1 holds all FSMO roles and has recently restarted.

What impact do the current AD replication failures on DC1 have on the environment?

<Answers to questions are provided in the relevant section in the Appendix>

Exercise 2: Troubleshoot and resolve AD replication error -2146893022

-2146893022 | The target principal name is incorrect.

In this exercise, you will use repadmin.exe and nltest.exe to resolve AD replication error -2146893022.

Trends:

Why is time important to Active Directory? It's not just about Kerberos and authentication.

AD replication errors -2146893022, 8614 and 8606 routinely go hand in hand. When all are seen together (or at least the first two), it is a good indicator that the domain controller's time changed by greater than tombstone lifetime.

Consider:

- Machine account passwords change every 30 days by default
- Tombstone Lifetime is usually 60 or 180 days

Pay attention to:

- DCs without time safeguards in place
- Virtualized DC guests configured to sync time with their hosts

For more info: see "Fixing When Your Domain Traveled Back In Time, the Great System Time Rollback to the Year 2000" article linked to in the **References** section.

Scenario

- DC2 is failing to replicate from DC1 with error -2146893022, "the target principal name is incorrect".

You will use **DC1** and **DC2** in this exercise.

Task 1 - Use repadmin and the system event log to see the symptoms of this problem

1. Use one of the methods from exercise 1 to review the replication status for DC1. Verify the last replication status result from DC2 lists error -2146893022 / the target principal name is incorrect.

   Output from repadmin /showrepl DC2:

```
DC=root,DC=contoso,DC=com

  Boulder\DC1 via RPC
    DSA object GUID: 70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e
    Last attempt @ 2013-12-09 12:53:48 failed, result -2146893022 (0x80090322):
      The target principal name is incorrect.
    17 consecutive failure(s).
    Last success @ 2012-11-26 14:50:47.
```

2. Test basic LDAP connectivity from **DC2**

   a. From **DC2**, attempt to use repadmin to bind to DC1:

```
Repadmin /bind DC1
```

   What error is displayed?

```
"LDAP Error 82(0x52): Local Error…"
```

3. Attempt to initiate AD replication from DC1 to DC2 using repadmin:

```
Repadmin /replicate dc2 dc1 "dc=root,dc=contoso,dc=com"
```

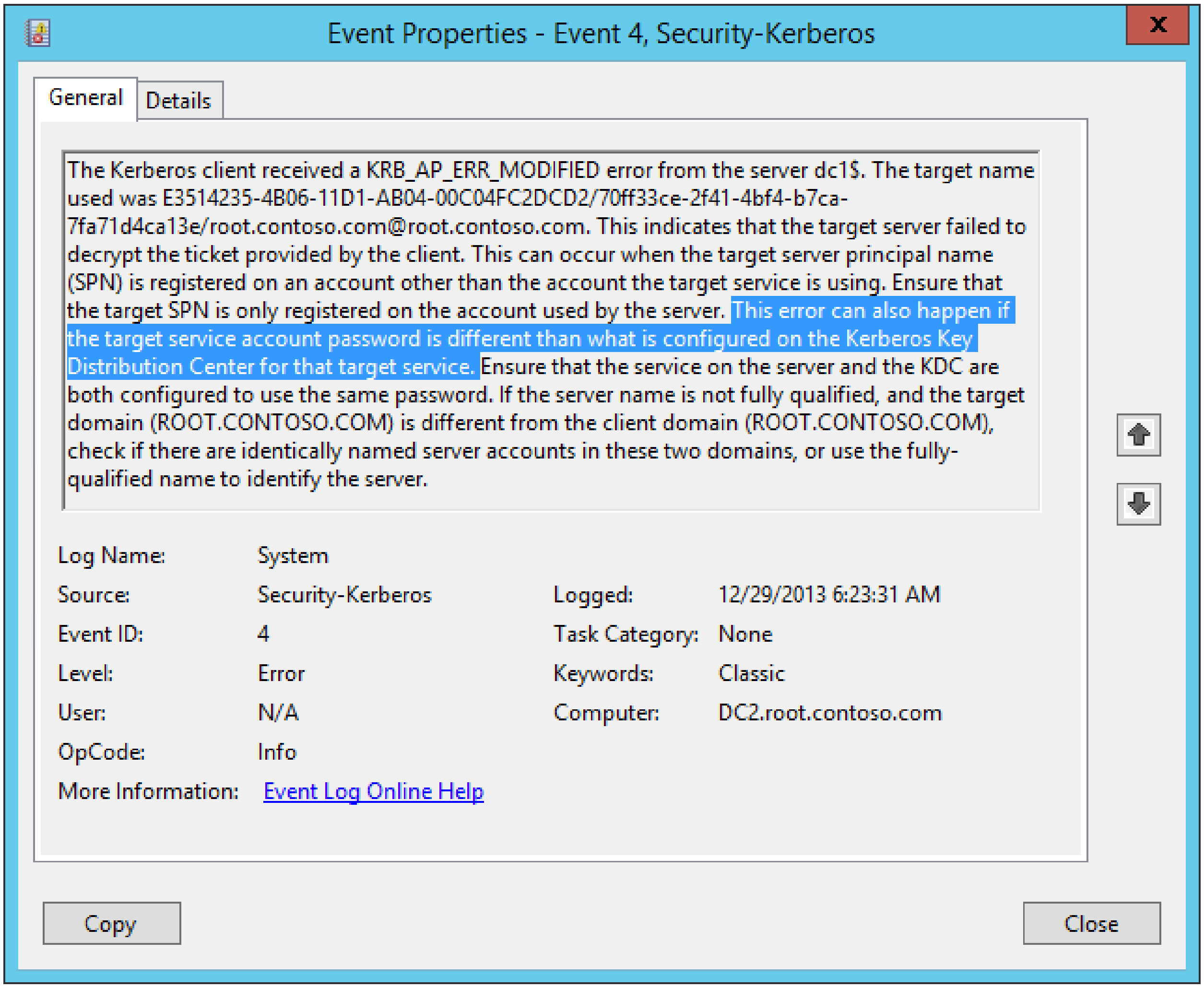
Note:

Repadmin /replicate syntax:

/replicate <Dest_DCs> <Source DC> <Naming Context> [/force] [/async] [/full] [/addref] [/readonly]

```
DsReplicaSync() failed with status -2146893022 (0x80090322):
    The target principal name is incorrect
```

4. On **DC2**, open up the event viewer (eventvwr.msc), and review the **system** event log for event ID **4**. You can also see this event via Server Manager's **Local Server** node, **EVENTS** pane on **DC2**.



The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server dc1$. The target name used was E3514235-4B06-11D1-AB04-00C04FC2DCD2/70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e/root.contoso.com@root.contoso.com. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Ensure that the target SPN is only registered on the account used by the server. This error can also happen if the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and the KDC are both configured to use the same password. If the server name is not fully qualified, and the target domain (ROOT.CONTOSO.COM) is different from the client domain (ROOT.CONTOSO.COM), check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.

Log Name:	System		
Source:	Security-Kerberos	Logged:	12/29/2013 6:23:31 AM
Event ID:	4	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	DC2.root.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		

Among other things, the text of event ID 4 indicates the problem can be caused by, "the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service".

For this scenario, that means:

- DC1s computer account password is different than the password stored in AD for DC1 on the KDC (DC2)

Task 2 - Determine cause of the AD replication failure

In this task, you will use repadmin /showobjmeta to determine if DC1's computer account password matches what is stored on DC2.

Tip:

How you can quickly identify if attributes on a given object are the same on a given set of DCs: **repadmin /showobjmeta**

The /showobjmeta parameter is used to display the replication metadata for a given object. If the attribute values of a given object are in-sync amongst DCs, the version information reported in the output will be the same when compared with the replication metadata from other DCs.

Perform this task on **DC1**.

1. Open a command prompt on **DC1**
2. Obtain replication metadata of the source DCs computer object from both DCs

```
Repadmin /showobjmeta dc1 "cn=dc1,ou=domain controllers,dc=root,dc=contoso,dc=com"
>dc1objmeta.txt

Repadmin /showobjmeta dc2 "cn=dc1,ou=domain controllers,dc=root,dc=contoso,dc=com"
>>dc1objmeta.txt
```

3. Open up the **dc1objmeta.txt** file with Notepad.exe and observe the version number differences for the password related attributes: (dBCSPwd, UnicodePWD, NtPwdHistory, PwdLastSet and lmPwdHistory). The version number is the second to last column with the heading of "Ver".

Table 1: dc1objmeta.txt -partial repadmin /showobjmeta output of DC1's computer object

DC1 object replication metadata according to:	Ver	Attribute
DC1	19	dBCSPwd
DC2	11	dBCSPwd

The replication metadata reveals that DC2 has old password information for DC1. The Kerberos operation failed because DC1 was unable to decrypt the Service Ticket presented by DC2. Review the **Kerberos details** section for Exercise 2 in the appendix for more information.

PowerShell:

There is a PowerShell script in the appendix that will help if this issue is encountered in a larger environment.

Task 3 - Resolve the AD replication failure

The KDC running on DC2 cannot be used for Kerberos operations with DC1 since DC2 has old password information for DC1. In this task, you will force DC2 to use the KDC on DC1 so that the replication operation will complete.

Perform this task on **DC2**.

1. From **DC2** stop the Kerberos Key Distribution Center service:

```
Net stop kdc
```

2. Initiate replication of the Root partition using repadmin

```
Repadmin /replicate dc2 dc1 "dc=root,dc=contoso,dc=com"
```

If replication still fails, clear any cached Kerberos tickets for the Local System account on DC2 using the klist.exe utility from a command prompt: Klist.exe -li 0x3e7 purge

(The logon ID for Local System is 0x3e7)

If replication of the root partition was successful, DC2 now has the updated password information for DC1, so DC2 can now be used for KDC operations. You can confirm this if you like by running the two repadmin /showobjmeta commands from task 2.

3. Start the Kerberos Key Distribution Center service on **DC2**.

```
Net start kdc
```

An alternative method to resolve this issue:

In this exercise, we simply stop the KDC to force DC2 to use DC1 as the KDC. We know this will work because DC1 has the updated password. This is a small environment, so doing the same thing in a larger environment may not be an option since we cannot control what new KDC will be contacted. If all other KDCs are up to date, this will work. Another method to resolve this is to reset DC1's computer account password manually and specify DC2 as the DC to update with the information. The following command will cause DC1 to reset its computer account password and update DC2 with this information:

On **DC1** open a command prompt and enter the following command:

```
Netdom resetpwd /server:192.168.10.2 /userd:root\administrator /passwordd:adrepl123!
```

The command instructs DC1 to change its password and tell the DC specified with the /server parameter the new password.

Exercise 3: Troubleshoot and resolve AD replication error 1908

1908 | Could not find the domain controller for this domain.

In this exercise, you will review the netlogon.log to determine the cause of AD replication error 1908. Nltest.exe will be used to enable verbose Netlogon logging as well as exercising the DC locator function of Netlogon. You will then use dcdiag.exe and the DNS management snap-in to further diagnose and resolve the problem.

Scenario

- DC1, DC2 and TRDC1 are failing to replicate from ChildDC1 with error 1908 "Could not find the domain controller for this domain".
  - This error is returned when there is a failure by Netlogon to locate a DC that is advertising the KDC flag.

Perform the following steps from **DC1**.

Task 1 - Determine the cause of the AD replication failure

Perform this task on **DC1**.

1. Enable verbose logging for Netlogon by executing the following command on DC1:

```
Nltest /dbflag:2080ffff
```

This enables additional detail to be logged to the Netlogon.log file located in the C:\Windows\Debug directory.

2. On DC1, initiate replication from ChildDC1

```
repadmin /replicate dc1 childdc1 dc=child,dc=root,dc=contoso,dc=com
```

```
DSReplicaSync() failed with status 1908 (0x774):
    Could not find the domain controller for this domain.
```

3. From DC1, test Netlogon's ability to locate a KDC in the **child.root.contoso.com** domain

```
Nltest /dsgetdc:child /kdc
```

```
Getting DC name failed: Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN
```

4. Execute the same command without the /KDC option to see if Netlogon can find any DC in the **child** domain

```
Nltest /dsgetdc:child
"Getting DC name failed: Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN"
```

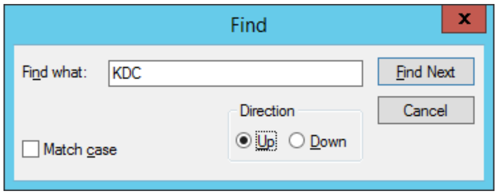
5. You will now review the netlogon.log file to see what was logged upon the execution of the first nltest command.

   a. Open up the Netlogon.log file in (C:\Windows\Debug\Netlogon.log), and go to the bottom of the file to see the most recent entries.

   b. Look for the entry that begins with **DSGetDcName function called**.

   There will be multiple similar entries. Find the entry in the log that has the same parameters you specified in the first nltest command. (Dom:**child** and Flags: **KDC**)

   If you have trouble locating the call, place your cursor on the last line of text and search up for **KDC.**



Find what: KDC

Direction: ● Up ○ Down

□ Match case

The entry will look similar to the following:

```
DsGetDcName function called: client PID=2176, Dom:child Acct:(null) Flags: KDC
```

View the results of the operation (everything with the same thread ID) that follows. The last entry will begin with **DsGetDcName function returns**.

Date	Time	Category	ThreadID	Message Text
date	12:21:42	MISC	3372	ROOT: **DsGetDcName function called**: client PID=2176, Dom:**child** Acct:(null) Flags: **KDC**
date	12:21:42	MISC	3372	NetpDcInitializeContext: DSGETDC_VALID_FLAGS is c07ffff1
date	12:21:42	MAILSLOT	3372	Received ping from DC1(DC1.root.contoso.com) child.root.contoso.com (null) on <Local>
date	12:21:42	CRITICAL	3372	Ping from DC1 for domain child.root.contoso.com child for (null) on <Local> is invalid since we don't host the named domain.
date	12:21:50	CRITICAL	3372	NetpDcGetDcNext: _kerberos._tcp.Boulder._sites.dc._msdcs.child.root.contoso.com.: Cannot Query DNS. 9002 0x232a
date	12:21:50	CRITICAL	3372	NetpDcGetNameIp: child.root.contoso.com: **No data returned from DnsQuery**.
date	12:21:50	MISC	3372	NetpDcGetName: NetpDcGetNameIp for child.root.contoso.com returned 1355

date	12:21:50	CRITICAL	3372	NetpDcGetName: child.root.contoso.com: IP and Netbios are both done.
date	12:21:50	MISC	3372	ROOT: DsGetDcName function returns 1355 (client PID=2176): Dom:child Acct:(null) Flags: KDC

In the Netlogon log output, you can see a DNS lookup failure for a KDC SRV record in the Child domain.

How do the domain controllers in root.contoso.com resolve names for the Child domain? (Open up the DNS management snap-in in order to determine the answer)

Can you ping child.root.contoso.com?

6. Test the DNS delegation settings with Dcdiag.exe

```
dcdiag /test:dns /dnsdelegation >dnstest.txt
```

7. Open up **dnstest.txt** to see the results of the DNS delegation test.

Are there any failures reported for the DNS delegation test?

What is the cause of the failure to locate a KDC in the child domain?

Task 2 - Resolve the AD replication failure

In this task, you will fix the broken DNS delegation for the child domain.

Perform this task on **DC1**.

1. Open up the DNS management snap-in (dnsmgmt.msc)
2. Expand **Forward Lookup Zones**, expand **root.contoso.com** and select **child**
3. Open up the properties of the **(same as parent folder)** NS record
4. Select the entry for **lamedc1.child.contoso.com** and then select **Remove**
5. Add a valid child domain DNS server to the delegation settings
    a. Select **Add**

   b. In the Server fully qualified domain name (FQDN) text box, type: **childdc1.child.root.contoso.com**

   c. In the IP Addresses of this NS record section, type the IP address of ChildDC1: **192.168.10.11**

   d. Select **OK** and then select **OK** again.

   e. Select **Yes** to the dialogue window that opens up asking if you want to delete the glue record lamedc1.child.contoso.com [192.168.10.1]

6. Now use nltest to verify we are able to locate a KDC in the child domain.

```
Nltest /dsgetdc:child /kdc /force
```

   The /force option is used to ensure the Netlogon cache is not used.

7. Test AD replication (replicate from childdc1 to dc1 and dc2) now that you have corrected the DNS delegation.

   Initiate replication using repadmin.exe OR via AD Sites and Services

   Initiate replication using repadmin:

```
Repadmin /replicate dc1 childdc1 "dc=child,dc=root,dc=contoso,dc=com"
```

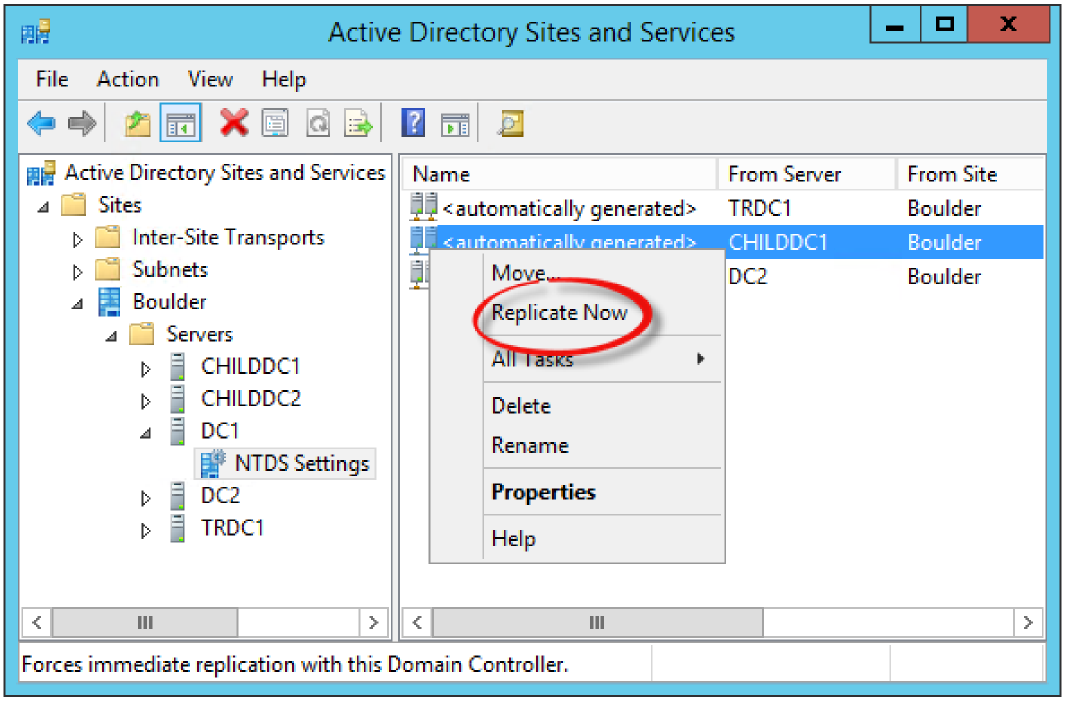
   Initiate replication on DC1 from CHILDDC1 using Active Directory Sites and Services:

   a. Open up Active Directory Sites and Services (dssite.msc)

   b. Expand Sites, Boulder, Servers and DC1

   c. Select DC1's **NTDS Settings** object

   d. Right click the **<automatically generated>** connection object from server CHILDDC1 and choose **Replicate Now**



Name	From Server	From Site
<automatically generated>	TRDC1	Boulder
<automatically generated>	CHILDDC1	Boulder
	DC2	Boulder

Forces immediate replication with this Domain Controller.

a. Expand DC2's server object and initiate replication from CHILDDC1

b. Expand TRDC1's server object and initiate replication on TRDC1 from CHILDDC1

Tip:

Use **repadmin /syncall** to quickly initiate AD replication in this lab environment:

```
Synchronizes a specified domain controller with all replication partners.
 By default, if no directory partition is provided in the naming context
 parameter, the command performs its operations on the configuration
 directory partition.
        [SYNTAX]
        /syncall <DSA> [<Naming Context>] [<flags>]

        The following flags are supported
        /a Abort if any server is unavailable.
        /A Sync all naming contexts which are held on the home server.
        /d Identify servers by distinguished name in messages.
        /e Enterprise, cross sites.
        /h Print this help screen.
        /i Iterate indefinitely.
        /I Perform showreps on each server pair in path instead of syncing.
        /j Synchronize adjacent servers only.
        /p Pause for possible user abort after every message.
        /P Push changes outward from home server.
        /q Run in quiet mode, suppress call back messages.
```

```
            /Q Run in very quiet mode, report fatal errors only.
            /s Do not synchronize.
            /S Skip initial server response check.

            By default /syncall does not cross site boundaries
```

Lab specific examples

Synchronizes the target dc with all its partners, all partitions including ones cross-site, displaying the partners by DN rather than GUID.

```
repadmin /syncall DC1 /Aed
repadmin /syncall DC2 /Aed
repadmin /syncall ChildDC1 /Aed
repadmin /syncall ChildDC2 /Aed
repadmin /syncall TRDC1 /Aed
```

8. Refresh the forest-wide replication status using adreplstatus or repadmin.

If using adreplstatus, ensure you click the **Configuration/Scope Settings** tab and then check **Re-Discover Environment** before refreshing the replication status. This is required, because the broken DNS delegation caused an error in the tool's initial discovery of the Child domain.

9. Observe that you now have replication status from the child domain DCs. At this point, the only replication error displayed is error 8606.

Tip:

If errors other than 8606 or 8614 are displayed:

Ensure you have initiated AD replication from DCs where it was failing before, and then run repadmin /showrepl or adreplstatus again

Note:

Note that error 1256 is no longer displayed. This was cleared up by resolving the first set of errors. Error 1256 is logged when the replication task is cancelled after a failure to replicate the Schema, configuration, or domain partitions for other replication errors. For this reason, you should always troubleshoot the error that led to the replication task being cancelled (do not bother troubleshooting 1256).

Exercise 4: Troubleshoot and resolve AD replication error 8606

8606 | Insufficient attributes were given to create an object

In this exercise, you will use repadmin.exe to identify lingering objects. You will then use repadmin or repldiag.exe to remove lingering objects from the Contoso forest and resolve AD replication error 8606 in the process. This replication status is an indication that one or more lingering objects exist on the source DC.

Tip:

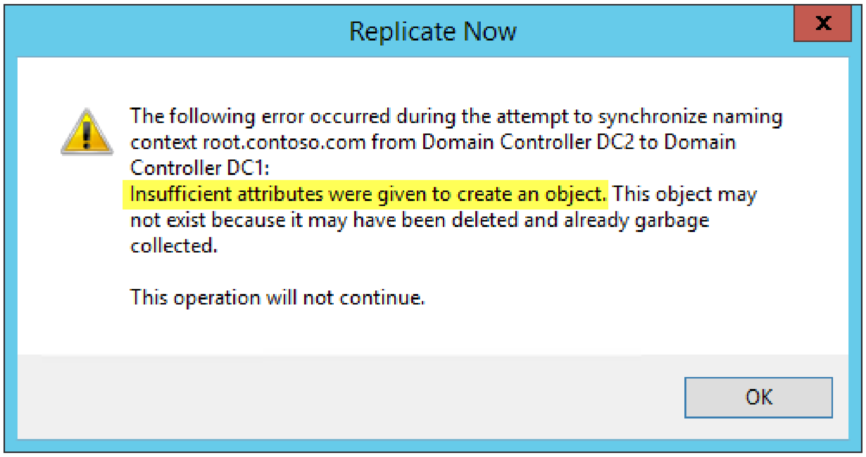
This section is jargon intense, a **Lingering Object Glossary** is provided in the Appendix for your reference.

More:

Lingering object: An object that is present on one DC, but has been deleted and garbage collected on one or more DCs. Error 8606 is logged when the source DC sends an update of one or more attributes for an object that does not exist on the destination DC.

Scenario

- AD replication of the Root partition from DC2 to DC1 fails with error, "Insufficient attributes were given to create an object".
- AD replication of the Root partition from TRDC1 to other GCs hosting a read-only copy of the partition fail with the same error.



The following error occurred during the attempt to synchronize naming context root.contoso.com from Domain Controller DC2 to Domain Controller DC1:
Insufficient attributes were given to create an object. This object may not exist because it may have been deleted and already garbage collected.

This operation will not continue.

- DC2 and TRDC1 are DCs that have at least one lingering object in the root.contoso.com partition
- DC1 reports error 8606 replicating from DC2

More:

There are many methods to remove lingering objects. This exercise presents the two most common:

- Repldiag /removelingeringobjects
- Repadmin /removelingeringobjects

Other methods are listed in the appendix.

Task 1 - Lingering object symptoms and identification

AD replication status 8606 and event ID 1988 are good indicators of lingering objects (when the DCs are configured for Strict Replication Consistency). It is important to note, however, that AD replication may complete successfully (and not log an error) from a DC containing lingering objects since replication is based on changes. If there are no changes to any of the lingering objects, there is no reason to replicate them and they will continue to exist. For this reason, when cleaning up lingering objects, do not just clean up the DCs logging the errors; instead, assume that all DCs may contain them, and clean them up as well.

Perform this task on **DC1**.

1. Manually initiate replication between **DC1** and **DC2** (have DC1 pull from DC2):

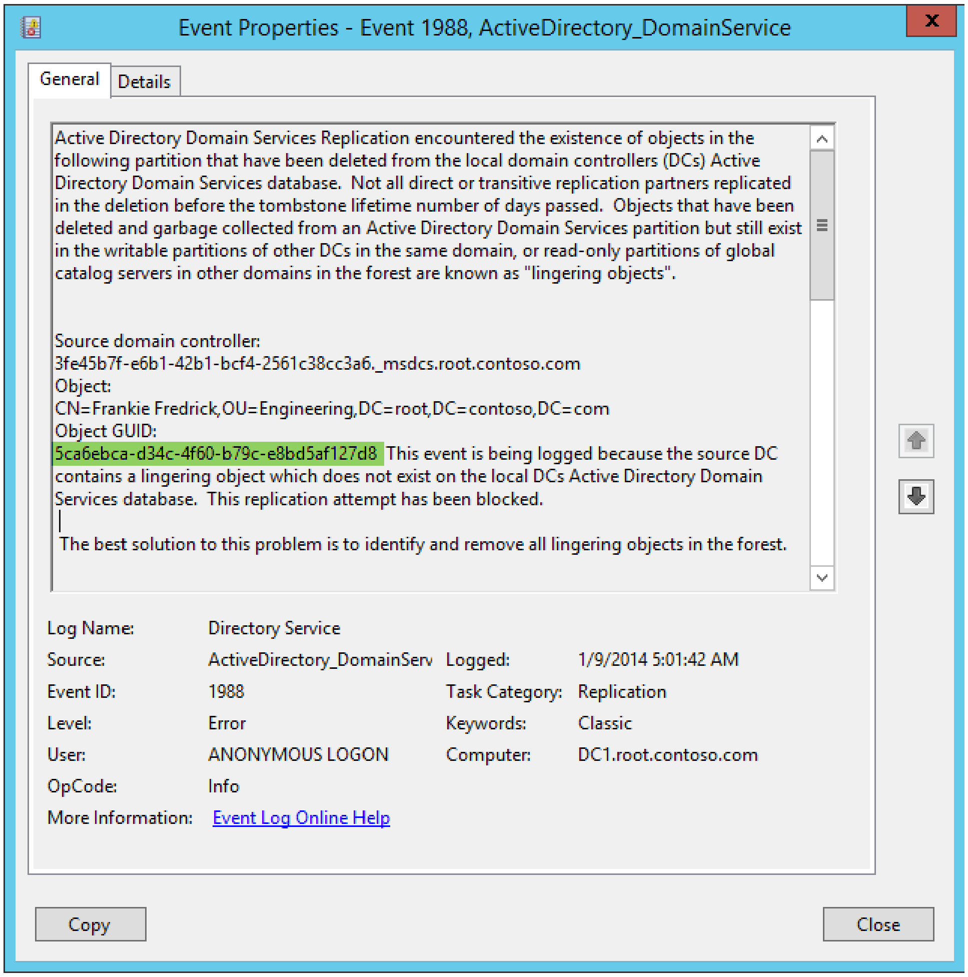
```
Repadmin /replicate dc1 dc2 "dc=root,dc=contoso,dc=com"
```

Replication fails with the following error:

```
DsReplicaSync() failed with status 8606 (0x219e):
Insufficient attributes were given to create an object. This object may not exist because it may
have been deleted and already garbage collected.
```

Event 1988 is logged in the Directory Service event log.

2. Review the Directory Services event log on DC1 for event 1988 using event viewer (eventvwr.msc) or PowerShell


Event Properties - Event 1988, ActiveDirectory_DomainService
General
Details
Copy
Close

Active Directory Domain Services Replication encountered the existence of objects in the following partition that have been deleted from the local domain controllers (DCs) Active Directory Domain Services database. Not all direct or transitive replication partners replicated in the deletion before the tombstone lifetime number of days passed. Objects that have been deleted and garbage collected from an Active Directory Domain Services partition but still exist in the writable partitions of other DCs in the same domain, or read-only partitions of global catalog servers in other domains in the forest are known as "lingering objects".

Source domain controller:
3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6._msdcs.root.contoso.com
Object:
CN=Frankie Fredrick,OU=Engineering,DC=root,DC=contoso,DC=com
Object GUID:
5ca6ebca-d34c-4f60-b79c-e8bd5af127d8 This event is being logged because the source DC contains a lingering object which does not exist on the local DCs Active Directory Domain Services database. This replication attempt has been blocked.

The best solution to this problem is to identify and remove all lingering objects in the forest.

Log Name:	Directory Service		
Source:	ActiveDirectory_DomainServ	Logged:	1/9/2014 5:01:42 AM
Event ID:	1988	Task Category:	Replication
Level:	Error	Keywords:	Classic
User:	ANONYMOUS LOGON	Computer:	DC1.root.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 2 Event 1988

```
Get-WinEvent -LogName "Directory Service" -MaxEvents 5 | fl
```

Note: Event 1988 only reports the first lingering object encountered during the replication attempt. There are usually many more lingering objects present on the source DC. Use repadmin /removelingeringobjects with the **/advisory_mode** switch to have all lingering objects reported.

3. Identify the following from event 1988 (they are needed later in the exercise):

   - Object GUID
   - Source DC
   - Partition DN

   How can you translate the DNS alias provided in the event to the host name of the DC?

Task 2 - Lingering object analysis

In this task, you will use repadmin to return replication metadata for the lingering object identified in event ID 1988. The repadmin output will allow you to identify DCs containing the lingering object reported in the event.

Perform this task on **DC1** and **DC2**.

1. Obtain the ObjectGUID reported in the event on **DC1**. (see Figure 2 for location of ObjectGUID)
2. Identify all DCs that have a copy of this object using repadmin /showobjmeta

```
Repadmin /showobjmeta * "<GUID=5ca6ebca-d34c-4f60-b79c-e8bd5af127d8>" >obj.txt
```

3. Open **obj.txt**. Any DC that returns replication metadata for this object are DCs containing one or more lingering objects. DCs that do not have a copy of the object report status 8439, "The distinguished name specified for this replication operation is invalid".

   Which DCs return replication metadata for the object?

Important: This is a good method to conduct a quick spot check of DCs containing the lingering object reported in the event. It is NOT a good method to discover all lingering objects. For more information, see the **Lingering Object discovery** section of the appendix.

4. Obtain DC1's DSA ObjectGUID and use repadmin /removelingeringobjects with the /advisory_mode parameter to identify all lingering objects in the ROOT partition on **DC2**.

Note: In order to use the /removelingeringobjects command you need to know three things:
1. You need to know which DCs contain lingering objects
2. Which partition the lingering object resides in
3. The DSA Object GUID of a good reference DC that hosts that partition that does not contain lingering objects

a. Obtain the DSA object GUID on DC1

```
Repadmin /showrepl DC1 >showrepl.txt
```

The DSA object GUID is at the top of the output and will look like this:

```
DSA object GUID: 70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e
```

b. In the following command, you will verify the existence of lingering objects on DC2 by comparing its copy of the ROOT partition with DC1.

Run the following repadmin command (ensure you use the /advisory_mode parameter)

```
Repadmin /removelingeringobjects DC2 70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e
"dc=root,dc=contoso,dc=com" /Advisory_Mode
```

```
RemoveLingeringObjects successful on dc2.
```

c. Review the Directory Service event log on DC2. If there are any lingering objects present, each one will be reported in its own event ID 1946. The total count of lingering objects for the partition checked is reported in event 1942.

Task 3 - Remove lingering objects

In this task, you will remove the lingering objects using either repldiag or repadmin.

Tip:

- There is a new GUI-based Lingering object removal tool that was developed after this lab was created. This tool is featured in a new lab titled "Troubleshooting Active Directory Lingering Objects".

Note:

- Repldiag requires a well-connected topology. It will fail to run in environments that suffer from poor network connectivity *.
- Always check for the latest version on CodePlex: *http://activedirectoryutils.codeplex.com/*

  * There is a hidden parameter that allows the tool to continue in spite of topology issues, but do not use it without recognizing the ramifications: Use of the /BypassStabilityCheck parameter will likely result in a failure to fully clean up the environment.

You will run commands to remove lingering objects from all partitions even though only one lingering object was discovered in the prior task.

Important: When lingering objects are discovered, assume they are present on all DCs in all partitions. Do not just clean up the DCs reporting the errors. Repldiag automates the majority of the cleanup work. See the **Lingering Object discovery and cleanup** section in the appendix for more information.

Perform this task on **Win8Client** and **ChildDC2**.

Repldiag (preferred method)

The following command will check for and remove lingering objects from all DCs for all partitions (except Schema)

1. From **Win8Client**, run the following from an elevated command prompt

```
Repldiag /removelingeringobjects
```

2. Verify that AD replication completes successfully. (error 8606 is no longer logged)

```
repadmin /replicate dc1 dc2 "dc=root,dc=contoso,dc=com"
```

3. Rerun the repadmin /showobjmeta command executed in Task 2 to see if the object was removed from all DCs

```
Repadmin /showobjmeta * "<GUID=5ca6ebca-d34c-4f60-b79c-e8bd5af127d8>" >obj.txt
```

Notice the RODC in the child domain still contains the object.

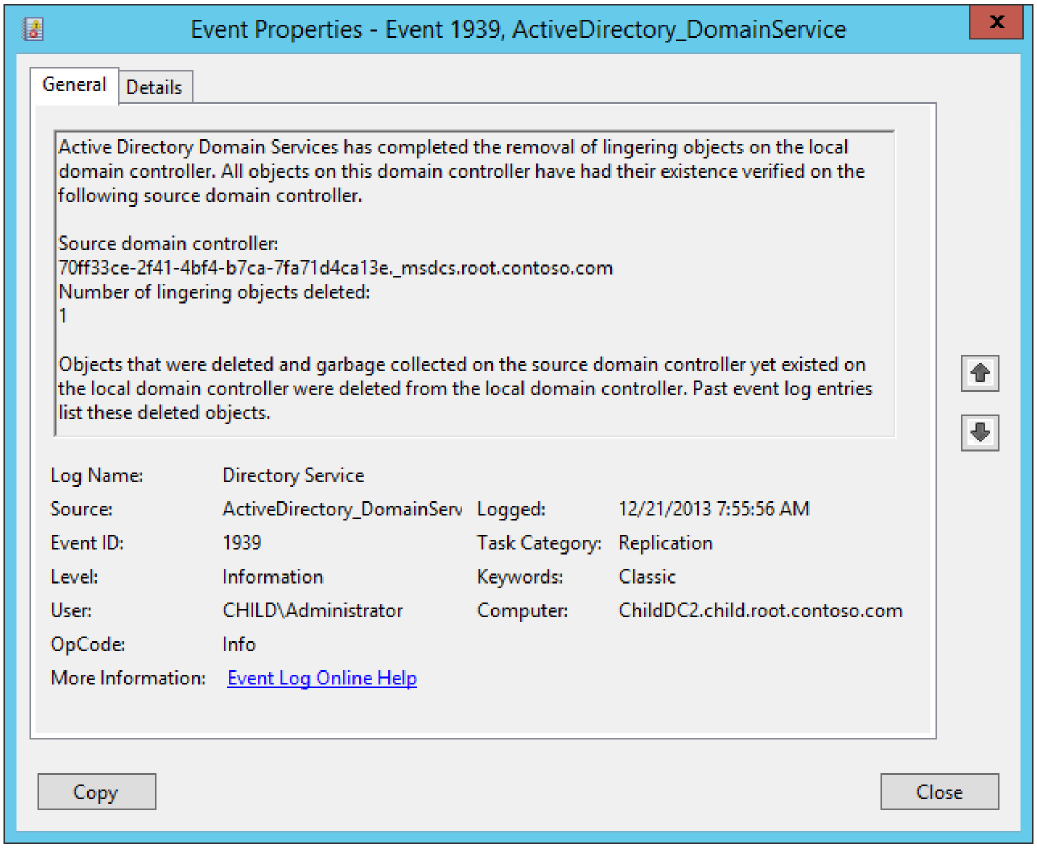
Note: At the time of this writing, Replidag (v 2.0.4947.18978) does not remove lingering objects from RODCs. (It was developed prior to the existence of RODCs.) This functionality has been requested.

4. Run the following command to clean up the RODC (childdc2).

```
Repadmin /removelingeringobjects childdc2.child.root.contoso.com 70ff33ce-2f41-4bf4-
b7ca-7fa71d4ca13e "dc=root,dc=contoso,dc=com"
```

5. Review the Directory Service event log on **ChildDC2** for the results of the lingering object removal request. Since this server runs a minimal server interface, you will need to open Event Viewer from the command prompt by typing **eventvwr.msc**.

   - Review the details of event ID 1939, which reports the status of the lingering object removal process.


Event Properties - Event 1939, ActiveDirectory_DomainService
General
Details
Copy
Close

Active Directory Domain Services has completed the removal of lingering objects on the local domain controller. All objects on this domain controller have had their existence verified on the following source domain controller.

Source domain controller:
70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e._msdcs.root.contoso.com
Number of lingering objects deleted:
1

Objects that were deleted and garbage collected on the source domain controller yet existed on the local domain controller were deleted from the local domain controller. Past event log entries list these deleted objects.

Log Name: Directory Service
Source: ActiveDirectory_DomainServ Logged: 12/21/2013 7:55:56 AM
Event ID: 1939 Task Category: Replication
Level: Information Keywords: Classic
User: CHILD\Administrator Computer: ChildDC2.child.root.contoso.com
OpCode: Info
More Information: Event Log Online Help

Note: If this were a production environment, you would also run the repadmin /removelingeringobjects command for the remaining partitions on the RODC(s).

If you used repldiag to remove the lingering objects, you are done with this task, and do not need to perform the alternate task steps.

Alternate task steps

Repadmin (method)

Use these steps if you prefer to remove the lingering objects using repadmin.

1. Clean up the reference DCs first

Configuration partition

```
Repadmin /removelingeringobjects childdc1.child.root.contoso.com 70ff33ce-2f41-4bf4-
b7ca-7fa71d4ca13e "cn=configuration,dc=root,dc=contoso,dc=com"
```

```
Repadmin /removelingeringobjects childdc1.child.root.contoso.com 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6 "cn=configuration,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc1.child.root.contoso.com 0b457f73-96a4-429b-ba81-1a3e0f51c848 "cn=configuration,dc=root,dc=contoso,dc=com"
```

ForestDNSZones partition

```
Repadmin /removelingeringobjects childdc1.child.root.contoso.com 70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e "dc=forestdnszones,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc1.child.root.contoso.com 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6 "dc=forestdnszones,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc1.child.root.contoso.com 0b457f73-96a4-429b-ba81-1a3e0f51c848 "dc=forestdnszones,dc=root,dc=contoso,dc=com"
```

Root domain partition

```
repadmin /removelingeringobjects dc1.root.contoso.com 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6 "dc=root,dc=contoso,dc=com"
```

DomainDNSZones application partition for the **root** domain

```
repadmin /removelingeringobjects dc1.root.contoso.com 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6 "dc=domaindnszones,dc=root,dc=contoso,dc=com"
```

Note:

You do not need to clean up reference DCs for the **Child**, **TreeRoot** or their **DomainDNSZones** partitions. This is because there is only one DC in each domain that hosts a writable copy of the partition. The schema partition is not checked or cleaned up because you cannot delete objects from the schema.

2. Now that the reference DCs are cleaned up. Clean up all remaining DCs against the reference DCs

Configuration

```
Repadmin /removelingeringobjects dc1.root.contoso.com 0c559ee4-0adc-42a7-8668-e34480f9e604 "cn=configuration,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects dc2.root.contoso.com 0c559ee4-0adc-42a7-8668-e34480f9e604 "cn=configuration,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc2.child.root.contoso.com 0c559ee4-0adc-42a7-8668-e34480f9e604 "cn=configuration,dc=root,dc=contoso,dc=com"


Repadmin /removelingeringobjects trdc1.treeroot.fabrikam.com 0c559ee4-0adc-42a7-8668-e34480f9e604 "cn=configuration,dc=root,dc=contoso,dc=com"
```

ForestDNSZones

```
Repadmin /removelingeringobjects dc1.root.contoso.com 0c559ee4-0adc-42a7-8668-
e34480f9e604 "dc=forestdnszones,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects dc2.root.contoso.com 0c559ee4-0adc-42a7-8668-
e34480f9e604 "dc=forestdnszones,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc2.child.root.contoso.com 0c559ee4-0adc-42a7-
8668-e34480f9e604 "dc=forestdnszones,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects trdc1.treeroot.fabrikam.com 0c559ee4-0adc-42a7-8668-
e34480f9e604 "dc=forestdnszones,dc=root,dc=contoso,dc=com"
```

Root domain partition

```
Repadmin /removelingeringobjects childdc1.child.root.contoso.com 70ff33ce-2f41-4bf4-
b7ca-7fa71d4ca13e "dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc2.child.root.contoso.com 70ff33ce-2f41-4bf4-
b7ca-7fa71d4ca13e "dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects dc2.root.contoso.com 70ff33ce-2f41-4bf4-b7ca-
7fa71d4ca13e "dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects trdc1.treeroot.fabrikam.com 70ff33ce-2f41-4bf4-b7ca-
7fa71d4ca13e "dc=root,dc=contoso,dc=com"
```

DomainDNSZones - Root

```
Repadmin /removelingeringobjects dc2.root.contoso.com 70ff33ce-2f41-4bf4-b7ca-
7fa71d4ca13e "dc=domaindnszones,dc=root,dc=contoso,dc=com"
```

Child domain partition

```
Repadmin /removelingeringobjects dc1.root.contoso.com 0c559ee4-0adc-42a7-8668-
e34480f9e604 "dc=child,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects dc2.root.contoso.com 0c559ee4-0adc-42a7-8668-
e34480f9e604 "dc=child,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects childdc2.child.root.contoso.com 0c559ee4-0adc-42a7-
8668-e34480f9e604 "dc=child,dc=root,dc=contoso,dc=com"

Repadmin /removelingeringobjects trdc1.treeroot.fabrikam.com 0c559ee4-0adc-42a7-8668-
e34480f9e604 "dc=child,dc=root,dc=contoso,dc=com"
```

DomainDNSZones - Child

```
Repadmin /removelingeringobjects childdc2.child.root.contoso.com 0c559ee4-0adc-42a7-
8668-e34480f9e604 "dc=domaindnszones,dc=child,dc=root,dc=contoso,dc=com"
```

TreeRoot domain partition

```
Repadmin /removelingeringobjects childdc1.child.root.contoso.com 0b457f73-96a4-429b-
ba81-1a3e0f51c848 "dc=treeroot,dc=fabrikam,dc=com"

Repadmin /removelingeringobjects childdc2.child.root.contoso.com 0b457f73-96a4-429b-
ba81-1a3e0f51c848 "dc=treeroot,dc=fabrikam,dc=com"
```

```
Repadmin /removelingeringobjects dc1.root.contoso.com 0b457f73-96a4-429b-ba81-
1a3e0f51c848 "dc=treeroot,dc=fabrikam,dc=com"

Repadmin /removelingeringobjects dc2.root.contoso.com 0b457f73-96a4-429b-ba81-
1a3e0f51c848 "dc=treeroot,dc=fabrikam,dc=com"
```

Exercise 5: Troubleshoot and resolve AD replication error 8453

8453 | "Replication access was denied"

In this exercise, you will use repadmin and the Directory Service event log to see the symptoms of AD replication error 8453. A special DCDIAG test is used to identify the cause of the failure. You will then use ADSIEdit.msc to resolve the problem.

Scenario

- There is an RODC in the Child domain **ChildDC2** that is not advertising as a global catalog server.

Task 1 - Symptoms of error 8453

Perform the following task on **ChildDC2**.

1. From any machine, run:

```
Repadmin /showrepl childdc2 >repl.txt
```

2. Review the repl.txt file to see the symptoms of this issue.

   a. Notice at the top of the output that this DC is failing to advertise as GC.

```
Boulder\CHILDDC2

DSA Options: IS_GC DISABLE_OUTBOUND_REPL IS_RODC

  WARNING:  Not advertising as a global catalog.
```

   b. The **DC=treeroot,DC=fabrikam,DC=com** partition is missing from the inbound neighbors section (as it is not replicated from any DC).

   c. The bottom of the output reveals that it is unable add a replication link for the **TreeRoot** partition with error 8453, "Replication access was denied."

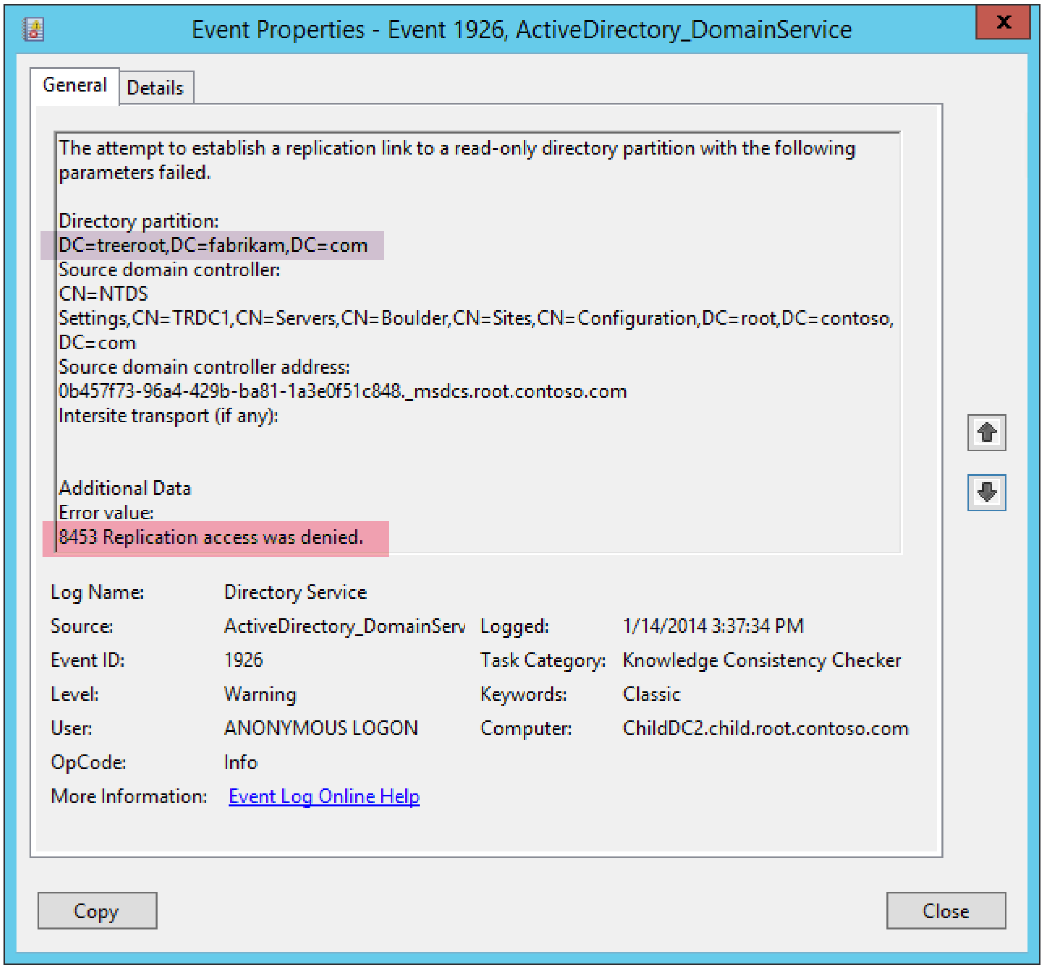
```
Source: Boulder\TRDC1

******* 1 CONSECUTIVE FAILURES since 2014-01-14 15:37:34

Last error: 8453 (0x2105):
        Replication access was denied.
```

```
Naming Context: DC=treeroot,DC=fabrikam,DC=com
```

3. Review the Directory Service event log on **ChildDC2** for event 1926. It shows the partition we failed to establish a replication link with and the error in the Additional Data section.


Event Properties - Event 1926, ActiveDirectory_DomainService
General
Details
Copy
Close

The attempt to establish a replication link to a read-only directory partition with the following parameters failed.

Directory partition:
DC=treeroot,DC=fabrikam,DC=com
Source domain controller:
CN=NTDS Settings,CN=TRDC1,CN=Servers,CN=Boulder,CN=Sites,CN=Configuration,DC=root,DC=contoso,DC=com
Source domain controller address:
0b457f73-96a4-429b-ba81-1a3e0f51c848._msdcs.root.contoso.com
Intersite transport (if any):

Additional Data
Error value:
8453 Replication access was denied.

Log Name: Directory Service
Source: ActiveDirectory_DomainServ
Logged: 1/14/2014 3:37:34 PM
Event ID: 1926
Task Category: Knowledge Consistency Checker
Level: Warning
Keywords: Classic
User: ANONYMOUS LOGON
Computer: ChildDC2.child.root.contoso.com
OpCode: Info
More Information: Event Log Online Help

4. From C**hildDC2** run the DCDIAG test that checks for security related problems:

```
Dcdiag /test:checksecurityerror
```

```
Doing primary tests

 Testing server: Boulder\CHILDDC2
   Starting test: CheckSecurityError
     Source DC CHILDDC1 has possible security error (8453).  Diagnosing...
         Error ROOT\Enterprise Read-only Domain Controllers doesn't have
```

```
        Replicating Directory Changes
      access rights for the naming context:
      DC=treeroot,DC=fabrikam,DC=com
Source DC TRDC1 has possible security error (8453).  Diagnosing...
      Error ROOT\Enterprise Read-only Domain Controllers doesn't have
        Replicating Directory Changes
      access rights for the naming context:
      DC=treeroot,DC=fabrikam,DC=com
......................... CHILDDC2 failed test CheckSecurityError
```

As reported in the output, error 8453 is because the **Enterprise Read-only Domain Controllers** security group does not have the "Replicating Directory Changes" permission.

More:

This access control entry is added during the RODCPREP process. Sometimes the infrastructure master for a given domain is not available when the command executes, and the entry is never added. RODCs must have this permission in order to replicate the partition.

Another common scenario where you encounter this error:

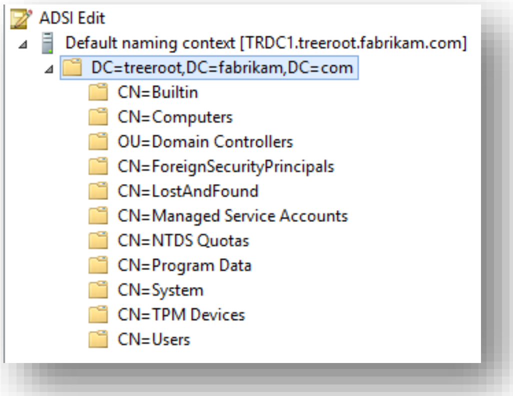
An administrator manually initiates AD replication: Error 8453 is displayed when attempting to initiate replication from a DC in another domain for which we do not have the "replicating directory changes" control access right. This is not actually an AD replication failure; it is just a failure on the Admin initiated operation. The Enterprise Administrators group has this right by default, and will not see this error.

Task 2 - Resolve error 8453

In this task, you will add the missing access control entry to the TreeRoot partition.

Perform the following task on **TRDC1.**

1. On **TRDC1**, Open up ADSIEDIT (ADSIEdit.msc).

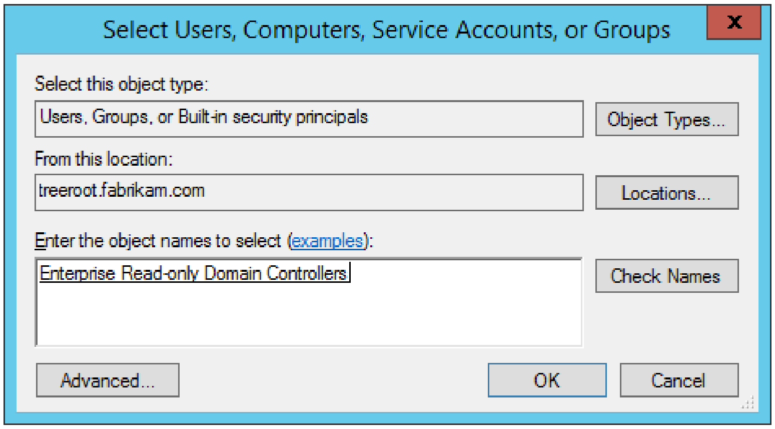


ADSI Edit
- Default naming context [TRDC1.treeroot.fabrikam.com]
  - DC=treeroot,DC=fabrikam,DC=com
    - CN=Builtin
    - CN=Computers
    - OU=Domain Controllers
    - CN=ForeignSecurityPrincipals
    - CN=LostAndFound
    - CN=Managed Service Accounts
    - CN=NTDS Quotas
    - CN=Program Data
    - CN=System
    - CN=TPM Devices
    - CN=Users

2. Right-click *DC=treeroot,DC=fabrikam,DC=com*, and then click **Properties**.
3. Select the **Security** tab.
4. Review the permissions on this partition. Notice there are no entries for the *Enterprise Read-Only Domain Controllers* group.
5. Click **Add**.
6. In the *Enter the object names to select* box, type:

   ROOT\Enterprise Read-only Domain Controllers

7. Click the **Check Names** button and then choose **OK** if the object picker resolves the name.



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

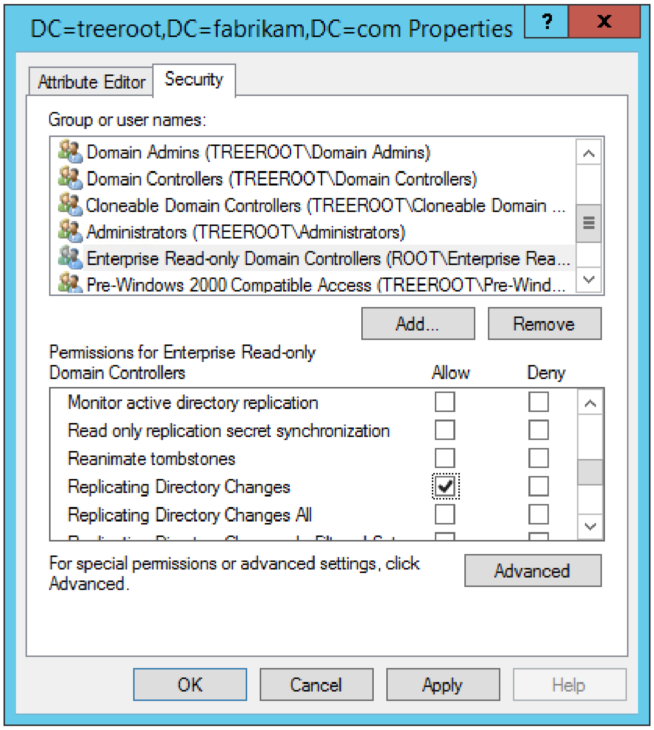
From this location:
treeroot.fabrikam.com

Enter the object names to select (examples):
Enterprise Read-only Domain Controllers

8. In the **Permissions for Enterprise Read-only Domain Controllers** dialog box, clear the **Allow** boxes that are automatically checked:

- Read
- Read domain password & lockout policies
- Read Other domain parameters

9. Select the **Allow** box next to "Replicating Directory Changes" and then click **OK**.



Group or user names:

- Domain Admins (TREEROOT\Domain Admins)
- Domain Controllers (TREEROOT\Domain Controllers)
- Cloneable Domain Controllers (TREEROOT\Cloneable Domain ...
- Administrators (TREEROOT\Administrators)
- Enterprise Read-only Domain Controllers (ROOT\Enterprise Rea...
- Pre-Windows 2000 Compatible Access (TREEROOT\Pre-Wind...

Permissions for Enterprise Read-only Domain Controllers	Allow	Deny
Monitor active directory replication	□	□
Read only replication secret synchronization	□	□
Reanimate tombstones	□	□
Replicating Directory Changes	☑	□
Replicating Directory Changes All	□	□

For special permissions or advanced settings, click Advanced.

10. Manually initiate the KCC to immediately recalculate the inbound replication topology on ChildDC2 (this will force it to attempt to add the TreeRoot partition again).

```
Repadmin /kcc childdc2
```

11. Verify ChildDC2 is able to replicate the TreeRoot partition.

More:

The next exercise is optional and the lab environment likely does not have the issue.

Please click the "**Exit Lab Environment**" button once you have completed all exercises to your liking. Ensure you **save a copy of the manual** for later reference and please **take the the survey** as it won't be available at a later time, and we really value your feedback.

Exercise 6: Troubleshoot and resolve AD replication error 8614

8614 | The directory service cannot replicate with this server because the time since the last replication with this server has exceeded the tombstone lifetime.

Important: This exercise is needed only if error 8614 is logged in showrepl or adreplstatus output.

Error 8614 is logged when a destination DC has not replicated with a source DC over an existing replication connection for longer than tombstone lifetime.

Warning:

- This quarantine is put in place on a per-replica, per-partition basis so that replication with an out of date DC does not introduce lingering objects into the environment.
- If this issue occurs in a production environment, careful consideration should be made prior to removing the replication safeguard.
- In some cases, forceful demotion of the source DC makes more sense. See the content linked in the appendix for more information.
- Large jumps in system time (forward or backward) are common causes of this issue

In this exercise, you will use repadmin to resolve AD replication error 8614 in a supported manner.

Perform this exercise from **Win8Client**.

1. Run the AD Replication Status tool or repadmin /showrepl * /csv. Review the output. **If AD replication error 8614 is not present, then do not do this exercise.**

2. Ensure Strict Replication consistency is set on all DCs

   ```
   Repadmin /regkey * +strict
   ```

   In the output of the above command, verify status for all DCs: registry key set

   ```
   "Strict Replication Consistency" REG_DWORD 0x0000001 (1)
   ```

3. Remove lingering objects if present using repldiag (skip if already performed in exercise 4).

```
Repldiag /removelingeringobjects
```

4. Run the following command on destination DCs that fail to replicate from source DCs with error 8614: (replace *DestinationDCName* with the actual DC name)

Do Not:

Do not run the following command without first verifying that Strict replication consistency is enabled.

```
Repadmin /regkey DestinationDCName +AllowDivergent
```

In this lab environment, it is safe to just temporarily set the registry value on all DCs

```
Repadmin /regkey * +AllowDivergent
```

Verify status from all DCs:

```
"Allow Replication With Divergent and Corrupt Partner" REG_DWORD 0x0000001 (1)
```

5. Initiate replication to all destination DCs from all source DCs where replication failed with status 8614

6. Use repadmin /showrepl * /csv or the AD Replication Status tool to verify error 8614 is no longer logged in the environment

7. Delete the registry value so that the replication quarantine safeguards are back in place

```
Repadmin /regkey * -AllowDivergent
```

Appendix

Exercise 1: AD replication symptom identification

Answers

When did DC1 last successfully replicate the ROOT partition from DC2?

Use

DC1 holds all FSMO roles and has recently restarted.

What impact do the current AD replication failures on DC1 have on the environment?

Table 2: FSMO role and initial synchronization

Role	Partition that must replicate for role to become active	Impact
Schema Master	Schema	No impact as this partition replicates successfully
Domain Naming Master	Configuration	No impact as this partition replicates successfully
PDC emulator	Domain	
RID Master	Domain	The ROOT partition fails to replicate to DC1 and any RID pool allocations will fail as a result. Since both DC1 and DC2 were recently imported into a new Hyper-V host, their local RID pool was discarded, and therefor operations that require a RID will fail (such as user, computer account or security group creation)
Infrastructure	Domain (and potentially application partitions)	

Repadmin /listhelp

```
DSA_LIST = { <DSA_NAME> | * | <part_server_name>* | site:<SITE_NAME>
          | gc: | nc: | pnc: | mnc: | fsmo_<FSMO_TYPE>:<FSMO_DN> }

Examples:
"*" = All DSAs in the enterprise/forest/configuration set.
"part_server_name*" = would pick "part_server_name_dc_01" and "part_server_name_dc_02" but
not server "part_server_diff_name".
"site:east_site1" = All DSAs in site "east_site1".
"gc:" = All GCs in the enterprise.
"nc:DC=fabrikam,..." = All DSAs hosting DC=fabrikam,...
"pnc:DC=fabrikam,..." = All DSAs hosting a partial copy of DC=fabrikam,...
"mnc:DC=fabrikam,..." = All DSAs hosting a master copy of DC=fabrikam,...
"fsmo_pdc:DC=my-corp-dom,DC=com" - repadmin runs against the PDC in the NC  "DC=my-corp-
dom,DC=com"
"fsmo_istg:east_site1" would pick the ISTG for the east_site1 site.

Additional option for DSA_LIST:  /homeserver:[dns name]
   The initial DS server that facilitates DSA_LIST expansion is called the homeserver. If the
DSA_LIST argument is a resolvable server name (such as a DNS or WINS name) this will be used
as the homeserver.  If a non-resolvable parameter is used for the DSA_LIST, repadmin will use
the locator to find a server to be used as the homeserver.  If the locator does not find a server,
repadmin will try the local box (port 389).  The /homeserver:[dns name] option is available to
explicitly control home server selection. This is especially useful when there are more than one
forest or configuration set possible.  For example, the DSA_LIST command "fsmo_istg:site1"
would target the locally joined domain's directory, so to target an AD/LDS instance,
/homeserver:adldsinstance:50000 could be used to resolve the fsmo_istg to site1 defined in the
ADAM configuration set on adldsinstance:50000 instead of the fsmo_istg to site1 defined in the
locally joined domain.


FSMO_TYPE = dnm | schema | pdc | rid | im | istg
NOTE: different types of FSMOs require different base DNs/RDNs.
"fsmo_dnm:" - is an enterprise wide FSMO, and doesn't take any DN.
"fsmo_schema:" - is an enterprise wide FSMO, and doesn't take any DN.
"fsmo_pdc:" - is a domain specific FSMO, and takes the DN of the domain the   user wants.
"fsmo_rid:" - is a domain specific FSMO, and takes the DN of the domain the user wants.
"fsmo_im:" - is a partition/NC specific FSMO, and takes the DN of the NC the user wants.
"fsmo_istg:" - is a site specific quasi-FSMO, and takes the RDN of the site.


DSA_NAME = { . | <server_dns> | <dsa_guid> | <server_obj_rdn> | <dsa_dn> }
. = Tells repadmin to try to pick one for you.
adlds_dns:ldap_port = specifies a specific AD LDS instance.
server_dns = specifies a specific server by DNS.
dsa_guid = specifies a specific server by its DSA GUID.
server_obj_rdn$service_short_name = specifies a specific AD LDS instance by its full server object
rdn.
```

```
server_obj_rdn = specifies a server by its server object rdn (usually the same as its NetBios
name)
The "$service_short_name" is not necessarily needed, but the DSA will only find a server, if the
portion of the server_obj_rdn specified in unambiguous.
dsa_dn = specifies a server by the DN of its DSA object.


OBJ_LIST = { ncobj:<NC_NAME> | dsaobj: }
"ncobj:" = means use the DN of NC Head specified in NC_NAME.
"dsaobj:" = means use the DN of the DSA we're connected to.

NC_NAME = { config: | schema: | domain: }
"config:" = Configuration Directory Partition.
"schema:" = Schema Directory Partition.
"domain:" = Domain Directory Partition for the Domain of the DC repadmin is running against.

OBJ_LIST OPTIONS = { /onelevel | /subtree} /filter:<Ldap_Filter>
With these options, the showattr and viewlist commands can be used to cover a list of objects,
instead of just a single object.

NOTES:
 o The * in wildcards are evaluated by LDAP.
 o Some options are not valid in AD LDS such as "gc:", "fsmo_pdc:", "fsmo_rid", "domain:", etc
```

Exercise 2: The Target Principal Name is Incorrect -2146893022

The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server dc1$. The target name used was E3514235-4B06-11D1-AB04-00C04FC2DCD2/70ff33ce-2f41-4bf4-b7ca-7fa71d4ca13e/root.contoso.com@root.contoso.com. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Ensure that the target SPN is only registered on the account used by the server. This error can also happen if the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and the KDC are both configured to use the same password. If the server name is not fully qualified, and the target domain (ROOT.CONTOSO.COM) is different from the client domain (ROOT.CONTOSO.COM), check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.

Kerberos details

Operation	AD replication attempt from DC1 to DC2 fails with -2146893022
Kerberos client	DC2
Kerberos target	DC1
KDC	DC2

- This replication error occurs because the source DC (DC1 - Kerberos target) failed to verify the AP request that DC2 sent. Specifically, the source DC (DC1) attempted to decrypt the service ticket in the AP request and failed.
- The Service Ticket was encrypted by the KDC (DC2) with the password hash of the DC1s computer account stored in AD (the KDCs version of the password).
- The Service Ticket decryption takes place on the Kerberos target (DC1). It attempts to decrypt the ticket with its actual password (which differs from what is stored in AD on the KDC).
- Since the Service Ticket was encrypted with the wrong computer account password, the operation fails.

More:

For more information, see:

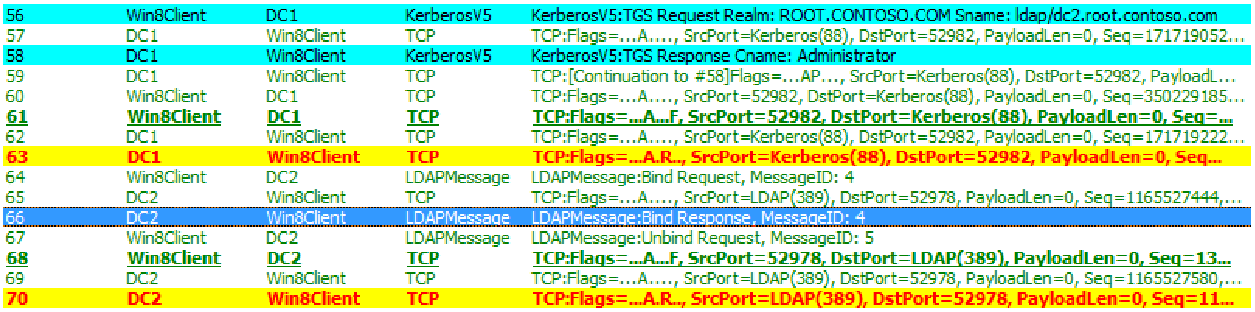
Troubleshooting AD Replication error -2146893022: The target principal name is incorrect.
http://support.microsoft.com/kb/2090913

AND
Kerberos for the busy admin
http://blogs.technet.com/b/askds/archive/2008/03/06/kerberos-for-the-busy-admin.aspx

Repadmin /bind failure log details

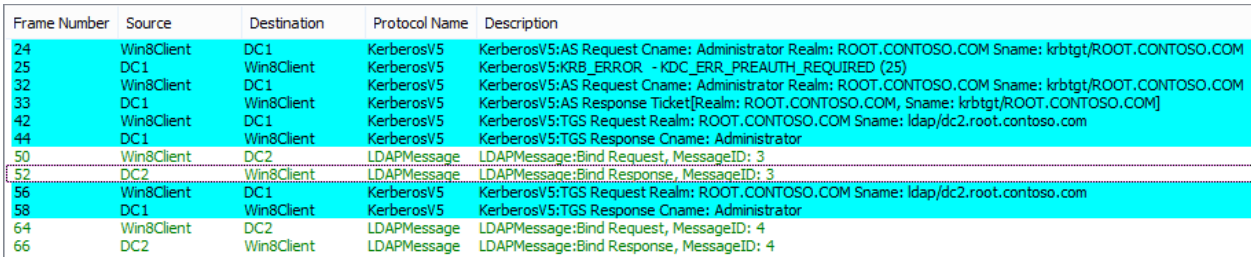
Troubleshooting Operation	Repadmin /bind dc2
Kerberos client	Win8Client
Kerberos target	DC2
KDC	DC1

Network trace of the LDAP bind failure



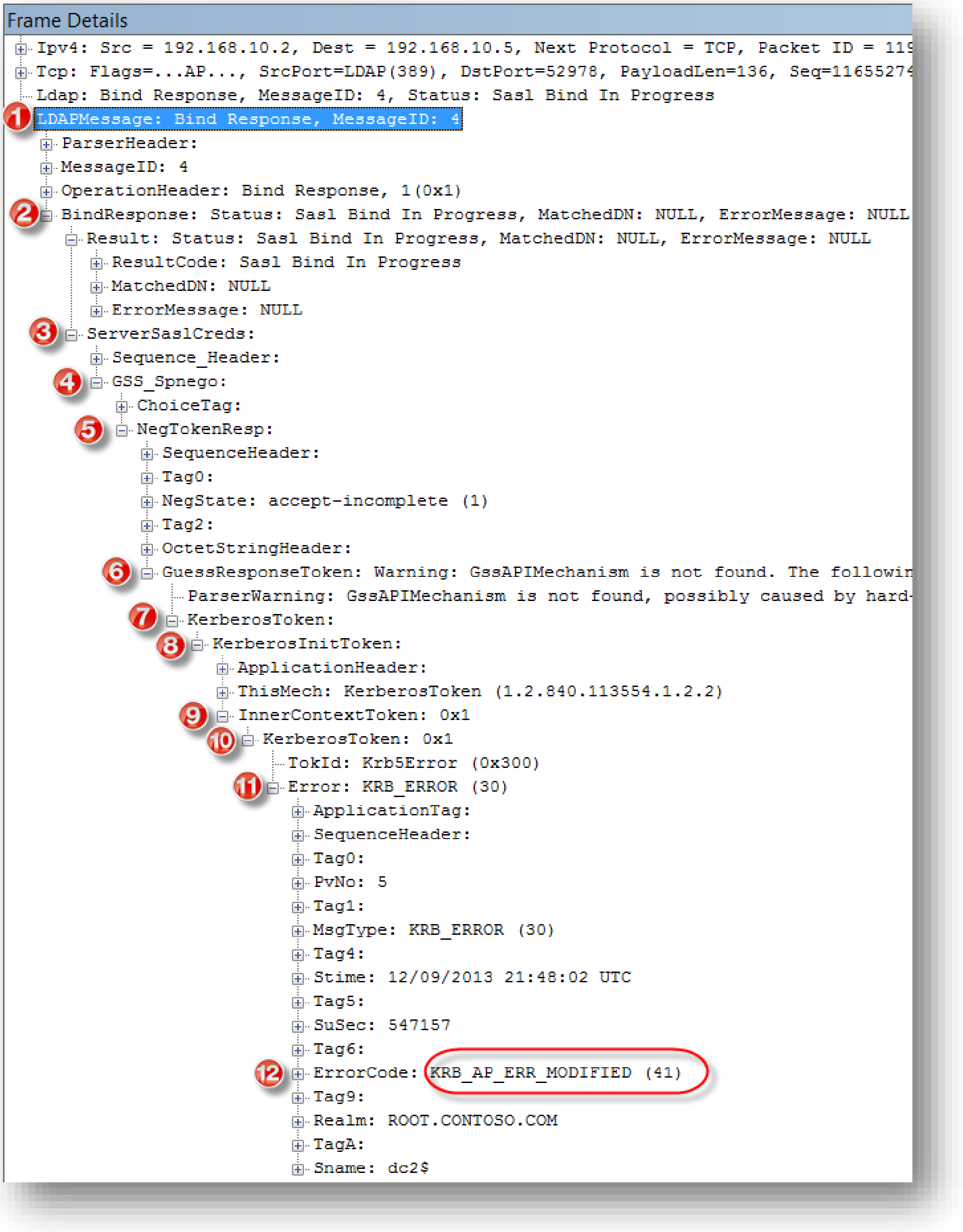
56	Win8Client	DC1	KerberosV5	KerberosV5:TGS Request Realm: ROOT.CONTOSO.COM Sname: ldap/dc2.root.contoso.com
57	DC1	Win8Client	TCP	TCP:Flags=...A...., SrcPort=Kerberos(88), DstPort=52982, PayloadLen=0, Seq=171719052...
58	DC1	Win8Client	KerberosV5	KerberosV5:TGS Response Cname: Administrator
59	DC1	Win8Client	TCP	TCP:[Continuation to #58]Flags=...AP..., SrcPort=Kerberos(88), DstPort=52982, PayloadL...
60	Win8Client	DC1	TCP	TCP:Flags=...A...., SrcPort=52982, DstPort=Kerberos(88), PayloadLen=0, Seq=350229185...
61	**Win8Client**	**DC1**	**TCP**	**TCP:Flags=...A...F, SrcPort=52982, DstPort=Kerberos(88), PayloadLen=0, Seq=...**
62	DC1	Win8Client	TCP	TCP:Flags=...A...., SrcPort=Kerberos(88), DstPort=52982, PayloadLen=0, Seq=171719222...
63	**DC1**	**Win8Client**	**TCP**	**TCP:Flags=...A.R.., SrcPort=Kerberos(88), DstPort=52982, PayloadLen=0, Seq...**
64	Win8Client	DC2	LDAPMessage	LDAPMessage:Bind Request, MessageID: 4
65	DC2	Win8Client	TCP	TCP:Flags=...A...., SrcPort=LDAP(389), DstPort=52978, PayloadLen=0, Seq=1165527444,...
66	DC2	Win8Client	LDAPMessage	LDAPMessage:Bind Response, MessageID: 4
67	Win8Client	DC2	LDAPMessage	LDAPMessage:Unbind Request, MessageID: 5
68	**Win8Client**	**DC2**	**TCP**	**TCP:Flags=...A...F, SrcPort=52978, DstPort=LDAP(389), PayloadLen=0, Seq=13...**
69	DC2	Win8Client	TCP	TCP:Flags=...A...., SrcPort=LDAP(389), DstPort=52978, PayloadLen=0, Seq=1165527580,...
70	**DC2**	**Win8Client**	**TCP**	**TCP:Flags=...A.R.., SrcPort=LDAP(389), DstPort=52978, PayloadLen=0, Seq=11...**

Figure 3 Network trace of LDAP bind failure



Frame Number	Source	Destination	Protocol Name	Description
24	Win8Client	DC1	KerberosV5	KerberosV5:AS Request Cname: Administrator Realm: ROOT.CONTOSO.COM Sname: krbtgt/ROOT.CONTOSO.COM
25	DC1	Win8Client	KerberosV5	KerberosV5:KRB_ERROR - KDC_ERR_PREAUTH_REQUIRED (25)
32	Win8Client	DC1	KerberosV5	KerberosV5:AS Request Cname: Administrator Realm: ROOT.CONTOSO.COM Sname: krbtgt/ROOT.CONTOSO.COM
33	DC1	Win8Client	KerberosV5	KerberosV5:AS Response Ticket[Realm: ROOT.CONTOSO.COM, Sname: krbtgt/ROOT.CONTOSO.COM]
42	Win8Client	DC1	KerberosV5	KerberosV5:TGS Request Realm: ROOT.CONTOSO.COM Sname: ldap/dc2.root.contoso.com
44	DC1	Win8Client	KerberosV5	KerberosV5:TGS Response Cname: Administrator
50	Win8Client	DC2	LDAPMessage	LDAPMessage:Bind Request, MessageID: 3
52	DC2	Win8Client	LDAPMessage	LDAPMessage:Bind Response, MessageID: 3
56	Win8Client	DC1	KerberosV5	KerberosV5:TGS Request Realm: ROOT.CONTOSO.COM Sname: ldap/dc2.root.contoso.com
58	DC1	Win8Client	KerberosV5	KerberosV5:TGS Response Cname: Administrator
64	Win8Client	DC2	LDAPMessage	LDAPMessage:Bind Request, MessageID: 4
66	DC2	Win8Client	LDAPMessage	LDAPMessage:Bind Response, MessageID: 4

Figure 4 Network trace with Netmon 3.4 Authentication traffic filter applied



```
Ipv4: Src = 192.168.10.2, Dest = 192.168.10.5, Next Protocol = TCP, Packet ID = 119
Tcp: Flags=...AP..., SrcPort=LDAP(389), DstPort=52978, PayloadLen=136, Seq=11655274
Ldap: Bind Response, MessageID: 4, Status: Sasl Bind In Progress
LDAPMessage: Bind Response, MessageID: 4
  ParserHeader:
  MessageID: 4
  OperationHeader: Bind Response, 1(0x1)
  BindResponse: Status: Sasl Bind In Progress, MatchedDN: NULL, ErrorMessage: NULL
    Result: Status: Sasl Bind In Progress, MatchedDN: NULL, ErrorMessage: NULL
      ResultCode: Sasl Bind In Progress
      MatchedDN: NULL
      ErrorMessage: NULL
    ServerSaslCreds:
      Sequence_Header:
      GSS_Spnego:
        ChoiceTag:
        NegTokenResp:
          SequenceHeader:
          Tag0:
          NegState: accept-incomplete (1)
          Tag2:
          OctetStringHeader:
          GuessResponseToken: Warning: GssAPIMechanism is not found. The followin
            ParserWarning: GssAPIMechanism is not found, possibly caused by hard-
            KerberosToken:
              KerberosInitToken:
                ApplicationHeader:
                ThisMech: KerberosToken (1.2.840.113554.1.2.2)
                InnerContextToken: 0x1
                  KerberosToken: 0x1
                    TokId: Krb5Error (0x300)
                    Error: KRB_ERROR (30)
                      ApplicationTag:
                      SequenceHeader:
                      Tag0:
                      PvNo: 5
                      Tag1:
                      MsgType: KRB_ERROR (30)
                      Tag4:
                      Stime: 12/09/2013 21:48:02 UTC
                      Tag5:
                      SuSec: 547157
                      Tag6:
                      ErrorCode: KRB_AP_ERR_MODIFIED (41)
                      Tag9:
                      Realm: ROOT.CONTOSO.COM
                      TagA:
                      Sname: dc2$
```

Figure 5 Kerberos error in LDAP bind response

System event log

```
Log Name:     System
Source:       Microsoft-Windows-Security-Kerberos
Event ID:     4
Level:        Error
Computer:     win8client.root.contoso.com
Description:
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server dc2$. The target name used was
LDAP/DC2.root.contoso.com/root.contoso.com@ROOT.CONTOSO.COM. This indicates that the target server failed to
decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on
an account other than the account the target service is using. Ensure that the target SPN is only registered on the
account used by the server. This error can also happen if the target service account password is different than what is
configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and
the KDC are both configured to use the same password. If the server name is not fully qualified, and the target
domain (ROOT.CONTOSO.COM) is different from the client domain (ROOT.CONTOSO.COM), check if there are
identically named server accounts in these two domains, or use the fully-qualified name to identify the server.
```

Ashley McGlone's PowerShell script to dump pwd version from DCs

This can be leveraged in a larger environment where you want to see which KDCs have an old computer account password for a given DC.

The PowerShell scriptlet does the following:

1. Query DCs in the domain
2. Outputs a list of DCs and asks you to select the one you want to obtain replication metadata for
3. Returns the version number of the dBCSPwd attribute from all DCs in that domain

```
$report = @()

$DCs = Get-ADDomainController -Filter *

$DCQuery = $DCs | Select-Object HostName, IPv4Address, Site, OperatingSystem,
OperationMasterRoles, ComputerObjectDN | Out-Gridview -Title "Select the DCs to query"
-PassThru | Select-Object -ExpandProperty ComputerObjectDN

ForEach ($DC in $DCs) {$report += Get-ADReplicationAttributeMetadata -Object $DCQuery -
Server $DC.HostName | Where-Object {$_.AttributeName -eq 'dBCSPwd'}}

$report | ogv
```

Exercise 3: Could not find the domain controller for this domain 1908

More:

For more information, see:

Troubleshooting AD Replication error 1908: Could not find the domain controller for this domain.
http://support.microsoft.com/kb/2712026

Answers

How do the domain controllers in root.contoso.com resolve names for the child domain?

Via DNS delegation - the Child domain zone is delegated to a different DNS server

Are there any failures reported for the DCDIAG DNS delegation test?

Yes:

```
DC1
TEST: Delegations (Del)
                  Error: DNS server: lamedc1.child.contoso.com.
IP:192.168.10.1
                  [Broken delegated domain child.root.contoso.com.]
```

Does a server named lamedc1.child.contoso.com server exists that hosts the child.root.contoso.com DNS zone?

No. Also, the IP address 192.168.10.1 belongs to DC1.

What is the cause of the failure to locate a KDC in the child domain?

Netlogon attempts to locate a KDC by querying a KDC SRV DNS record. Netlogon fails to get a response to this DNS query. Ultimately this is caused by a broken DNS delegation.

Log output

nltest /dsgetdc:child /kdc

Getting DC name failed: Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN

Netlogon.log

```
12/18 11:05:59 [MISC] [1856] ROOT: DsGetDcName function called: client PID=-1,
Dom:CHILD.ROOT.CONTOSO.COM Acct:(null) Flags: IP KDC
12/18 11:05:59 [MISC] [1856] NetpDcInitializeContext: DSGETDC_VALID_FLAGS is c07ffff1
12/18 11:05:59 [MAILSLOT] [1856] Received ping from DC1(DC1.root.contoso.com)
CHILD.ROOT.CONTOSO.COM (null) on <Local>
12/18 11:05:59 [CRITICAL] [1856] Ping from DC1 for domain CHILD.ROOT.CONTOSO.COM
(null) for (null) on <Local> is invalid since we don't host the named domain.
12/18 11:06:06 [MISC] [624] ROOT: DsGetDcName function called: client PID=-1,
Dom:CHILD.ROOT.CONTOSO.COM Acct:(null) Flags: IP KDC
12/18 11:06:06 [MISC] [624] NetpDcInitializeContext: DSGETDC_VALID_FLAGS is c07ffff1
12/18 11:06:06 [MAILSLOT] [624] Received ping from DC1(DC1.root.contoso.com)
CHILD.ROOT.CONTOSO.COM (null) on <Local>
12/18 11:06:06 [CRITICAL] [624] Ping from DC1 for domain CHILD.ROOT.CONTOSO.COM (null)
for (null) on <Local> is invalid since we don't host the named domain.
12/18 11:06:08 [CRITICAL] [1856] NetpDcGetDcNext:
_kerberos._tcp.Boulder._sites.dc._msdcs.CHILD.ROOT.CONTOSO.COM.: Cannot Query DNS. 9002
0x232a
12/18 11:06:08 [CRITICAL] [1856] NetpDcGetNameIp: CHILD.ROOT.CONTOSO.COM: No data
returned from DnsQuery.
12/18 11:06:08 [MISC] [1856] NetpDcGetName: NetpDcGetNameIp for
CHILD.ROOT.CONTOSO.COM returned 1355
12/18 11:06:08 [CRITICAL] [1856] NetpDcGetName: CHILD.ROOT.CONTOSO.COM: IP and
Netbios are both done.
12/18 11:06:08 [MISC] [1856] ROOT: DsGetDcName function returns 1355 (client PID=-1):
Dom:CHILD.ROOT.CONTOSO.COM Acct:(null) Flags: IP KDC
12/18 11:06:08 [CRITICAL] [624] NetpDcGetDcNext:
_kerberos._tcp.Boulder._sites.dc._msdcs.CHILD.ROOT.CONTOSO.COM.: Cannot Query DNS. 9002
0x232a
12/18 11:06:08 [CRITICAL] [624] NetpDcGetNameIp: CHILD.ROOT.CONTOSO.COM: No data
returned from DnsQuery.
12/18 11:06:08 [MISC] [624] NetpDcGetName: NetpDcGetNameIp for
CHILD.ROOT.CONTOSO.COM returned 1355
12/18 11:06:08 [CRITICAL] [624] NetpDcGetName: CHILD.ROOT.CONTOSO.COM: IP and Netbios
are both done.
12/18 11:06:08 [MISC] [624] ROOT: DsGetDcName function returns 1355 (client PID=-1):
Dom:CHILD.ROOT.CONTOSO.COM Acct:(null) Flags: IP KDC
```

Network trace

```
66   DC1   DC2   DNS:QueryId = 0x7A52, QUERY (Standard query), Query  for ChildDC1.child.root.contoso.com of type Host Addr on class Internet       ...
67   DC1   DC2   DNS:QueryId = 0x597F, QUERY (Standard query), Query  for _kerberos._tcp.Boulder._sites.dc._msdcs.CHILD.ROOT.CONTOSO.COM of type SRV
68   DC1   DC2   DNS:QueryId = 0x7A52, QUERY (Standard query), Query  for ChildDC1.child.root.contoso.com of type Host Addr on class Internet       ...
71   DC2   DC1   DNS:QueryId = 0x597F, QUERY (Standard query), Response - Server failure          {DNS:28, UDP:27, IPv4:1}
79   DC1   DC2   DNS:QueryId = 0x7A52, QUERY (Standard query), Query  for ChildDC1.child.root.contoso.com of type Host Addr on class Internet       ...
84   DC2   DC1   DNS:QueryId = 0x7A52, QUERY (Standard query), Response - Server failure          {DNS:32, UDP:31, IPv4:1}
```

Dcdiag /test:dns /dnsdelegation >dnstest.txt

```
Directory Server Diagnosis

Performing initial setup:

   Trying to find home server...
   Home Server = DC1

   * Identified AD Forest.
   Done gathering initial info.

Doing initial required tests

   Testing server: Boulder\DC1

      Starting test: Connectivity

         ......................... DC1 passed test Connectivity



Doing primary tests

   Testing server: Boulder\DC1

      Starting test: DNS


         DNS Tests are running and not hung. Please wait a few minutes...

         ......................... DC1 passed test DNS

   Running partition tests on : ForestDnsZones

   Running partition tests on : DomainDnsZones

   Running partition tests on : Schema

   Running partition tests on : Configuration

   Running partition tests on : root

   Running enterprise tests on : root.contoso.com

      Starting test: DNS

         Test results for domain controllers:

            DC: DC1.root.contoso.com
            Domain: root.contoso.com
```

```
     TEST: Delegations (Del)
       Error: DNS server: lamedc1.child.contoso.com. IP:192.168.10.1

       [Broken delegated domain child.root.contoso.com.]

Summary of test results for DNS servers used by the above domain
controllers:


   DNS server: 192.168.10.1 (lamedc1.child.contoso.com.)
     1 test failure on this DNS server

Summary of DNS test results:

                        Auth Basc Forw Del  Dyn  RReg Ext
   ____________________________________________________________
   Domain: root.contoso.com
     DC1                    PASS PASS n/a  FAIL n/a  n/a  n/a

......................... root.contoso.com failed test DNS
```

Exercise 4: Lingering Objects - Insufficient attributes were given to create an object - 8606

Table 3: Event 1988 text

Log Name	Directory Service
Source	Microsoft-Windows-ActiveDirectory_DomainService
Date	<Date> <Time>
Event ID	1988
Task Category	Replication
Computer	<computer name>
Description	
Active Directory Domain Services Replication encountered the existence of objects in the following partition that have been deleted from the local domain controllers (DCs) Active Directory Domain Services database. Not all direct or transitive replication partners replicated in the deletion before the tombstone lifetime number of days passed. Objects that have been deleted and garbage collected from an Active Directory Domain Services partition but still exist in the writable partitions of other DCs in the same domain, or read-only partitions of global catalog servers in other domains in the forest are known as "lingering objects". Source domain controller: 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6._msdcs.root.contoso.com Object:	

```
CN=Frankie Fredrick,OU=Engineering,DC=root,DC=contoso,DC=com
Object GUID:
5ca6ebca-d34c-4f60-b79c-e8bd5af127d8  This event is being logged because the source DC contains a lingering object which
does not exist on the local DCs Active Directory Domain Services database.  This replication attempt has been blocked.

 The best solution to this problem is to identify and remove all lingering objects in the forest.

User Action:
 Remove Lingering Objects:
  The action plan to recover from this error can be found at http://support.microsoft.com/?id=314282.
  If both the source and destination DCs are Windows Server 2003 DCs, then install the support tools included on the
installation CD.  To see which objects would be deleted without actually performing the deletion run "repadmin
/removelingeringobjects <Source DC> <Destination DC DSA GUID> <NC> /ADVISORY_MODE". The event logs on the source DC
will enumerate all lingering objects.  To remove lingering objects from a source domain controller run "repadmin
/removelingeringobjects <Source DC> <Destination DC DSA GUID> <NC>".
  If either source or destination DC is a Windows 2000 Server DC, then more information on how to remove lingering objects
on the source DC can be found at http://support.microsoft.com/?id=314282 or from your Microsoft support personnel.
  If you need Active Directory Domain Services replication to function immediately at all costs and don't have time to remove
lingering objects, enable loose replication consistency by unsetting the following registry key:
 Registry Key:
HKLM\System\CurrentControlSet\Services\NTDS\Parameters\Strict Replication Consistency
  Replication errors between DCs sharing a common partition can prevent user and computer accounts, trust relationships,
their passwords, security groups, security group memberships and other Active Directory Domain Services configuration data
to vary between DCs, affecting the ability to log on, find objects of interest and perform other critical operations. These
inconsistencies are resolved once replication errors are resolved.  DCs that fail to inbound replicate deleted objects within
tombstone lifetime number of days will remain inconsistent until lingering objects are manually removed by an administrator
from each local DC.
  Lingering objects may be prevented by ensuring that all domain controllers in the forest are running Active Directory Domain
Services, are connected by a spanning tree connection topology and perform inbound replication before Tombstone Live
number of days pass.
```

Answers

How can you translate the alias provided in the event to the host name of the DC?

1. Copy the alias out of the event (highlight and Ctrl + C)
2. Ping 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6._msdcs.root.contoso.com

Other options include:

- Look at the SRV record in the forest root MSDCS DNS zone (_msdcs.root.contoso.com) in the DNS Management snap-in
- Output repadmin /showrepl * to a text file and match up the GUID reported in the event to the DSA object GUID.

- Use an LDAP query tool (such as Repadmin or PowerShell) to dump the ObjectGUID of the NTDS Settings object:

Command Prompt:

```
Repadmin /showattr DC1 "<GUID=3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6>" /atts:DN
```

Return all DSA objectGUIDs

```
Repadmin /showattr DC1 NCOBJ:Config: /filter:"(Objectclass=NTDSDSA)" /atts:objectGUID
/subtree
```

PowerShell:

```
PS C:\>Get-ADObject -Identity 3fe45b7f-e6b1-42b1-bcf4-2561c38cc3a6
```

Return all DSA objectGUIDs

```
PS C:\>Get-ADObject -LDAPFilter "(Objectclass=ntdsdsa)" -SearchBase
"cn=configuration,dc=root,dc=contoso,dc=com" | Out-GridView
```

Which DCs return replication metadata for the object?

DC2, TRDC1 and ChildDC2

Lingering Object discovery and cleanup

Repadmin /removelingeringobjects /advisory_mode is a good method to conduct a spot check of lingering objects on an individual DC, per partition basis.

However, lingering objects may exist on DCs without any noticeable symptoms. For that reason, checking and cleaning up just the DCs that report errors is not a good method to ensure all lingering objects are removed from the environment.

To remove lingering objects

1. Determine the root cause of the lingering object issue and prevent it from occurring again
2. Assume all DCs contain lingering objects in all partitions and clean up everyone

Those that clean up just the source DCs reported with AD replication status 8606 usually find they have more objects to clean up later.

To accomplish the above using repadmin, you need to do the following:

1. Identify one DC per partition to use as a reference DC

2. Clean up each DC identified against all other DCs that host a writeable copy of the same partition. This DC is now considered "clean" and suitable to use as a reference DC.
3. Clean up all other DCs against the reference DCs

In the simple, five DC, three domain lab environment, this requires 30 separate executions of the repadmin command. In a real-word production environment, the count of repadmin executions is usually in the hundreds or thousands.

More:

For more information, see:

Clean that Active Directory Forest of Lingering Objects
http://blogs.technet.com/b/glennl/archive/2007/07/26/clean-that-active-directory-forest-of-lingering-objects.aspx

The good news is that repldiag /removelingeringobjects automates the above for you and requires just one execution: **Repldiag /removelingeringobjects**

To prevent their recurrence:

Important:

- Resolve replication failures within TSL
- Ensure Strict Replication Consistency is enabled
- Ensure large jumps in system time are blocked via registry key or policy
- Don't remove replication quarantine with the "allowDivergent" setting without removing LOs first
- Don't restore system backups that are near TSL number of days old
- Don't bring DCs back online that haven't replicated within TSL
- Do not allow a server to replicate that has experienced a USN rollback

Lingering Object Job Aid

Lingering Object Glossary

Table 4 Lingering Object glossary

Term	Definition

Abandoned delete	An object deleted on one DC that never was replicated to other DCs hosting a writable copy of the NC for that object. The deletion replicates to DCs/GCs hosting a read-only copy of the NC. The DC that originated the object deletion goes offline prior to replicating the change to other DCs hosting a writable copy of the partition.
Abandoned object	An object created on one DC that never got replicated to other DCs hosting a writable copy of the NC but does get replicated to DCs/GCs hosting a read-only copy of the NC. The originating DC goes offline prior to replicating the originating write to other DCs that contain a writable copy of the partition.
Lingering link	A linked attribute contains the DN of an object that no longer exists in Active Directory. These stale references are referred to as lingering links.
Lingering Object	An object that is present on one replica, but has been deleted and garbage collected on another replica.
Loose Replication Consistency	With this behavior enabled, if a destination DC receives a change to an attribute for an object that it does not have, the entire object is replicated to the target for the sake of replication consistency. This undesirable behavior causes a lingering object to be "reanimated."
Strict Replication Consistency	With this behavior enabled, if a destination DC receives a change to an attribute for an object that it does not have, replication is blocked with the source DC for the partition where the lingering object was detected
Tombstone	An object that has been deleted but not yet garbage collected
Tombstone Lifetime (TSL)	The amount of time tombstones are retained in Active Directory before being garbage collected and permanently purged from the database.

Term	Description	Notes

Deleted object	When AD recycle bin is enabled, an object that is deleted (deleted object) is recoverable with a full set of attributes using a PowerShell command (2008 R2) or via PowerShell and a GUI- based tool (ADAC) in Windows Server 2012). The object remains in this state until the **deleted object lifetime** expires and then it becomes a **recycled object**.	IsDeleted = True
		IsRecycled = <not set>
		Stored in the **Deleted Objects** container in most instances (some objects do not get moved on deletion).

Deleted object lifetime	The deleted object lifetime is determined by the value of the **msDS-deletedObjectLifetime** attribute. • By default, tombstoneLifetime is set to null. When tombstoneLifetime is set to null, the tombstone lifetime defaults to 60 days (hard-coded in the system). • By default, msDS-deletedObjectLifetime is also set to null. When msDS-deletedObjectLifetime is set to null, the deleted object lifetime is set to the value of the tombstone lifetime. • If msDS-deletedObjectLifetime is manually set, it becomes the effective lifetime of a system state backup.	CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<mydomain>,DC=<com> Attribute: **msDS-deletedObjectLifetime**
Garbage Collection	A process that permanently deletes tombstone objects or recycled objects • runs on DCs every 12 hours by default / 15 minutes after restart Can be manually initiated with LDP or other LDAP tool	`Repadmin /setattr "" "" doGarbageCollection add 1"`
Offline defrag	Invokes Esentutl.exe to compact the existing AD database and writes the compacted file to the specified directory.	Access in DS restore mode: Ntdsutil / act in ntds / files / compact to c:\temp

Term	Description	Notes
Semantic Database Analysis	Verifies the integrity of Active Directory database files with respect to Active Directory semantics	Access in DS restore mode: Ntdsutil / act in ntds / sem da an / go

Recycled object	After a deleted object lifetime expires, the logically deleted object is turned into a recycled object and most of its attributes are stripped away.	IsDeleted = True
		IsRecycled = True
		Can only be recovered if *toggle recycled objects* flag is used during the authoritative restore process.

Tombstone	Generically, this is an object that has been deleted but not garbage collected. Prior to the introduction of the AD recycle bin, this is the term for a deleted object.
	If AD recycle bin is enabled:
	An object that is deleted retains all of its attribute values and does not become a recycled object until the **deleted object lifetime** expires.
	If AD recycle bin is not enabled:
	A deleted object immediately becomes a tombstone and is stripped of most attribute values.
	To recover a tombstone with a full set of attributes, you must perform an authoritative restore.
		If AD recycle bin is not enabled:
		IsDeleted = True
		IsRecycled = True
		If AD recycle bin is enabled and the object is within the deleted object lifetime:
		IsDeleted=True
		IsRecycled=not set
		If AD recycle bin is enabled and the object is now a recycled object:
		IsDeleted=True
		IsRecycled=True

Term	Description	Notes
Tombstone Lifetime (TSL)	The number of days before tombstones or recycled objects are eligible for garbage collection. By default, tombstoneLifetime is set to null. When tombstoneLifetime is set to null, the tombstone lifetime defaults to 60 days (hard-coded in the system). This is also the effective lifetime of a system state backup. If msDS-deletedObjectLifetime is manually set, it becomes the effective lifetime of a system state backup.	CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=<mydomain>,DC=<com> Attribute: tombstoneLifetime

Replication Consistency Settings

Strict Replication Consistency

- Defines how a destination DC behaves if a source DC sends updates to an object that does not exist in the destination DC's local copy of Active Directory.
  - Destination DCs should see USN for creates before object is modified
  - Only modifies for lingering objects arrive for object not on destination DC
  - Only destination DC's enforce strict replication and log events
- Destination DCs stop replicating from source DC's partitions containing LO's
- Lingering objects are quarantined on source DCs where they can be detected
- End-to-end replication may be impacted for partitions containing lingering objects
- Administrators must remove lingering objects to restore replication

Enabling Strict Replication

Use Repadmin from Window Server 2003 SP1 or later to set strict replication via command prompt:

- For all domain controllers, type:
  ```
  repadmin /regkey * +strict
  ```
- For all global catalog servers, type:
  ```
  repadmin /regkey gc: +strict
  ```

You can also enable strict replication by manually setting the **Strict Replication Consistency** registry value to **1**.

```
Key: HKLM\System\CurrentControlSet\Services\NTDS\Parameter
Value: Strict Replication Consistency
Type: (Reg_DWORD)
Value Data: 1

1(enabled): Inbound replication of the specified directory partition from the source is
stopped on the destination.
```

Warning: Ensure you are prepared to deal with replication failures after enabling strict replication consistency due to the existence of lingering objects.

Loose Replication Consistency

If you enable Loose Replication Consistency, if a destination receives a change to an object that it does not have, the entire object is replicated to the target for the sake of replication consistency. This behavior causes a lingering object to be reapplied to all domain controllers in the replication topology.

Enable Loose Replication

Use Repadmin (from Window Server 2003 SP1 or later) to set strict replication via command prompt:

- For all domain controllers, type:
  `repadmin /regkey * -strict`
- For all global catalog servers, type:
  `repadmin /regkey gc: -strict`

You can also enable strict replication by manually setting the **Strict Replication Consistency** registry value to **0**.

```
Key: HKLM\System\CurrentControlSet\Services\NTDS\Parameters
Value: Strict Replication Consistency
Type: (Reg_DWORD)
Value Data: 0

0 (disabled): The destination requests the full object from the source domain
controller, and the lingering object is revived in the directory.
```

Critical: The Loose Replication Consistency setting will cause the undesirable behavior of reanimation of lingering objects.

Default Settings for Strict Replication Consistency

The default value for the strict replication consistency registry entry is determined by the conditions under which the domain controller was installed into the forest.

Note: Raising the domain or forest functional level does not change the replication consistency setting on any domain controller.

Upgrade Path	Default	Notes
Windows NT 4.0	Loose	
Windows 2000 RTM Root	Loose	A post-SP2 NTDSA.DLL defaulted to strict replication consistency but was quickly recalled. Windows 2000 Services 1 through 4 all default to loose replication consistency.
Windows NT 4.0 to Windows 2000 Root	Loose	
Windows 2000 to Windows Server 2003 SP1	Loose	Upgrading a Windows 2000 forest to Windows Server 2003 slipstreamed with SP1 does not enabled strict replication consistency.
Windows Server 2003 RTM Root	Strict	DCPROMO creates an operational GUID that causes Windows Server 2003 domain controllers to inherit strict replication mode but is ignored by Windows 2000 domain controllers.
Windows Server 2003 SP1 root and later: **Windows Server 2003 R2** **Windows Server 2008** **Windows Server 2008 R2**	Strict	Same as above.

Windows Server 2012 **Windows Server 2012 R2**		
Windows NT 4.0 to Windows Server 2003 root	Strict	DCPROMO creates an operational GUID that causes Windows Server 2003 domain controllers to inherit strict replication mode but is ignored by Windows 2000 domain controllers.

More Information:

For more information about this topic, see: http://blogs.technet.com/b/askds/archive/2010/02/15/strict-replication-consistency-myth-versus-reality.aspx

Repadmin RLO example usage

The command's syntax is:

repadmin /removelingeringobjects *LingeringDC ReferenceDC_DSA_GUID Partition*

Where:
LingeringDC: FQDN of DC that has the lingering objects
ReferenceDC_DSA_GUID: The DSA GUID of a domain controller that hosts a writeable copy of the partition
Partition: The distinguished name of the directory partition where the lingering objects exist

So for example:
We have a server named **DC1.contoso.com** that contains lingering objects. We know that the lingering object is in the **childdomain.contoso.com** partition. We know that **DC3.childdomain.contoso.com** hosts a writeable copy of the partition and doesn't contain any lingering objects.

We need to find the DSA GUID of DC3 is, so we run: repadmin /showrepl DC3.childdomain.contoso.com
At the top of the output, locate the DC Object GUID entry. This is the GUID you need to enter in the command for the reference DC.

The command would be

repadmin /removelingeringobjects DC1.contoso.com 5ed02b33-a6ab-4576-b109-bb688221e6e3 dc=childdomain,dc=contoso,dc=com

Repldiag quick reference

Removing lingering objects from a forest with repldiag is as simple as running repldiag /removelingeringobjects. However, it is usually best to exercise some control over the process in larger environments. The option /OverRideReferenceDC allows you to select which DC to use for cleanup. The option /outputrepadmincommandlinesyntax allows you to see what a forest-wide cleanup looks like using repadmin.

Repldiag /removelingeringobjects /outputrepadmincommandlinesyntax

This will give you output of corresponding repadmin /removelingeringobjects syntax. View the output to get an understanding of the steps repldiag uses holistically remove lingering objects

1. It first selects one DC per partition to use as a reference DC.

From the developer:

> **Reference DC selection:**
> "It is based on the DC with the highest number of link objects on a per partition basis. The assumption is that this is a hub/well connected system. This may also select a multiple "reference" DCs according to each partition." - Ken Brumfield

2. It then cleans the reference DCs up against all other DCs for the partition(s) they were selected as a reference for.
3. Finally, it cleans up all other DCs in the forest with the new "cleaned up" reference DCs as sources.

The /outputrepadmincommandlinesyntax option does not actually attempt object cleanup. You would need to leave this option off if you want to execute lingering object cleanup.

Sample Repldiag /removelingeringobjects /outputrepadmincommandlinesyntax output

```
Number Complete,Status,Server Name,Naming Context,Reference DC,Duration,Error Code,Error Message
repadmin /removelingeringobjects loncontosodc.contoso.com 9653cb84-7aa2-4a59-ab46-382e5dc1d3a8 dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com 87ccb4f8-1057-4cfa-aed6-79b5626db9fd dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com 4009aef6-b279-43d2-82f6-4298f02505e8 dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com b3ff6e2e-6025-4782-9d7b-54b0431a374a dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com 9653cb84-7aa2-4a59-ab46-382e5dc1d3a8 cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com 87ccb4f8-1057-4cfa-aed6-79b5626db9fd cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com 4009aef6-b279-43d2-82f6-4298f02505e8 cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com b3ff6e2e-6025-4782-9d7b-54b0431a374a cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com 87ccb4f8-1057-4cfa-aed6-79b5626db9fd dc=domaindnszones,dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com 4009aef6-b279-43d2-
82f6-4298f02505e8 dc=domaindnszones,dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com b3ff6e2e-6025-4782-
9d7b-54b0431a374a dc=domaindnszones,dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com 87ccb4f8-1057-4cfa-aed6-
79b5626db9fd dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com 4009aef6-b279-43d2-
82f6-4298f02505e8 dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com b3ff6e2e-6025-4782-
9d7b-54b0431a374a dc=corp,dc=contoso,dc=com
Reference NCs cleaned in 0h:0m:0s.  Cleaning everything else against reference NCs.
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com a29bbfda-8425-4cb9-
9c66-8e07d505a5c6 dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects dalcorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects nycorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects seacorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 dc=forestdnszones,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com a29bbfda-8425-4cb9-
9c66-8e07d505a5c6 cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects dalcorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects nycorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects seacorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 cn=configuration,dc=contoso,dc=com
repadmin /removelingeringobjects 5thwardcorpdc.corp.contoso.com a29bbfda-8425-4cb9-
9c66-8e07d505a5c6 dc=contoso,dc=com
repadmin /removelingeringobjects dalcorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 dc=contoso,dc=com
repadmin /removelingeringobjects nycorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 dc=contoso,dc=com
repadmin /removelingeringobjects seacorpdc.corp.contoso.com a29bbfda-8425-4cb9-9c66-
8e07d505a5c6 dc=contoso,dc=com
repadmin /removelingeringobjects dalcorpdc.corp.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=domaindnszones,dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects nycorpdc.corp.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=domaindnszones,dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects seacorpdc.corp.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=domaindnszones,dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects loncontosodc.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects dalcorpdc.corp.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects nycorpdc.corp.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=corp,dc=contoso,dc=com
repadmin /removelingeringobjects seacorpdc.corp.contoso.com 9653cb84-7aa2-4a59-ab46-
382e5dc1d3a8 dc=corp,dc=contoso,dc=com
```

```
All NCs cleaned in 0h:0m:0s.
```

This output can also be viewed in Excel: Copy commands to a text file. Modify the text file to include only the command portion of the output. Then open up the text file in Excel. (space delimited)

From the developer:

Does the /outputrepadmincommandlinesyntax exactly mirror the internal operation of repldiag when it performs the lingering object removals?

"Short answer = yes.

Long answer:

The key is that the read/write authoritative reference must be cleaned by comparing to all the other r/w references. Then everything can be done in parallel against the authoritative reference.

Repldiag is multi-threaded and runs one management thread per NC to create the clean authoritative reference, and then spawns multiple threads to clean against the authoritative reference. So different NCs may complete at different rates depending on number of r/w partitions (in addition to normal factors such as network latency and bandwidth).

As such, both they syntax and native functionality respect the need to serially clean the authoritative reference and then everything else after. In terms of actual order beyond that, there is none of significance to worry about.

In summary, yes the output order is the same as the syntax. Excluding the multi-threading considerations.

The code logic is essentially:

```
f (!isOutputSyntax)
     DsVerifyReplica(...)
Else
     Console.Write line(...)
```

W/console.write line handling the thread synchronization for the output." - Ken Brumfield

More control: /OverRideReferenceDC

This option allows you to specify a DC that you want to be used as a reference DC for the partition specified. In a large distributed environment, take careful consideration when choosing the reference DC. Things to consider when choosing a suitable reference DC:

- Well connected: Fast WAN link.
- Performance: Excellent server class hardware: Disk, RAM, CPU and NIC
- Critical Network Applications / Services do not depend on this DC: Such as an Exchange facing DC

- Other DCs don’t report replication failures with reference DC as the source: filter repadmin /showrepl * /csv ouput, or use the topology report created by repldiag /save.

```
repldiag /removelingeringobjects
/overridedefaultreferencedc:"cn=configuration,dc=contoso,dc=com":nycorpdc.corp.contoso.com
/overridedefaultreferencedc:"dc=corp,dc=contoso,dc=com":seacorpdc.corp.contoso.com
/overridedefaultreferencedc:"dc=forestdnszones,dc=contoso,dc=com":5thwardcorpdc.corp.cont
oso.com /outputrepadmincommandlinesyntax

Replication topology analyzer.  Written by kenbrumf@microsoft.com
Version:  2.0.3397.24022
Command Line Switch:  /removelingeringobjects
Command Line Switch:
/overridedefaultreferencedc:cn=configuration,dc=contoso,dc=com:nycorpdc.corp.contoso.com
Command Line Switch:
/overridedefaultreferencedc:dc=corp,dc=contoso,dc=com:seacorpdc.corp.contoso.com
Command Line Switch:
/overridedefaultreferencedc:dc=forestdnszones,dc=contoso,dc=com:5thwardcorpdc.corp.contos
o.com
Command Line Switch:  /outputrepadmincommandlinesyntax

Attempting to override NC cn=configuration,dc=contoso,dc=com with DC
nycorpdc.corp.contoso.com...       Overriden
Attempting to override NC dc=corp,dc=contoso,dc=com with DC seacorpdc.corp.contoso.com...
Overriden
Attempting to override NC dc=forestdnszones,dc=contoso,dc=com with DC
5thwardcorpdc.corp.contoso.com... Overriden
```

/UseRobustDCLocation

Query every DC for a list of DCs in the forest. This ensures replication instability does not cause any to be missed. We have had cases where we clean up lingering objects in the forest but due to an AD topology problem some DCs were not cleaned up. This option is usually recommended if you want it to do a thorough job.

References

Troubleshooting Active Directory Replication Problems - TechNet landing page for AD replication troubleshooting articles

http://technet.microsoft.com/en-us/library/cc949120(v=ws.10).aspx

Repadmin

- Troubleshooting replication with repadmin
  http://www.microsoft.com/en-us/download/details.aspx?id=9028

AD Replication Status (adreplstatus)

- Active Directory Replication Status Tool (ADREPLSTATUS) Resources Page
  http://social.technet.microsoft.com/wiki/contents/articles/12707.active-directory-replication-status-tool-adreplstatus-resources-page.aspx
- ADReplstatus introduction and screenshot walkthrough
  http://blogs.technet.com/b/askds/archive/2012/08/23/ad-replication-status-tool-is-live.aspx

-2146893022

- Troubleshooting AD Replication error -2146893022: The target principal name is incorrect.
  http://support.microsoft.com/kb/2090913
- Kerberos for the busy admin
  http://blogs.technet.com/b/askds/archive/2008/03/06/kerberos-for-the-busy-admin.aspx

1908

- Troubleshooting AD Replication error 1908: Could not find the domain controller for this domain.
  http://support.microsoft.com/kb/2712026

8606 - Lingering Objects

- Troubleshooting AD Replication error 8606: "Insufficient attributes were given to create an object"
  http://support.microsoft.com/kb/2028495
- Clean that Active Directory forest of lingering objects
  http://blogs.technet.com/b/glennl/archive/2007/07/26/clean-that-active-directory-forest-of-lingering-objects.aspx

Repldiag

- Repldiag download
  http://activedirectoryutils.codeplex.com/
- How to clean one partition at a time
  http://blogs.technet.com/b/robertbo/archive/2011/01/20/can-i-clean-one-partition-at-a-time-with-repldiag-and-other-tips-part-4-of-4.aspx

8453

- Troubleshooting AD Replication error 8453: "Replication access was denied." http://support.microsoft.com/kb/2022387

8614

- Troubleshooting AD Replication error 8614: "The Active Directory cannot replicate with this server because the time since the last replication with this server has exceeded the tombstone lifetime" http://support.microsoft.com/kb/2020053
- Fixing When Your Domain Traveled Back In Time, the Great System Time Rollback to the Year 2000 http://blogs.technet.com/b/askpfeplat/archive/2012/11/26/fixing-when-your-domain-traveled-back-in-time-the-great-system-time-rollback-to-the-year-2000.aspx

PowerShell

http://blogs.technet.com/b/ashleymcglone/

- AD PowerShell demo http://blogs.technet.com/b/ashleymcglone/archive/2013/10/26/powershell-saturday-005-atlanta-it-s-time-to-part-with-blankie-moving-from-command-line-tools-to-powershell-for-active-directory.aspx

What's new in Active Directory for Windows Server 2012 R2

- Windows Server 2012 R2 Component Updates - What's new in AD for Windows Server 2012 R2 http://technet.microsoft.com/en-us/library/dn535773.aspx

Active Directory Replication fundamentals

- **How the Active Directory Replication Model Works**

  http://technet.microsoft.com/en-us/library/cc772726(v=WS.10).aspx

- **How Active Directory Replication Topology Works**

  http://technet.microsoft.com/en-us/library/cc755994(v=WS.10).aspx

- **How DNS Support For Active Directory Works**

  http://technet.microsoft.com/en-us/library/cc759550(v=WS.10).aspx

To recreate this lab environment

Create a Windows Server 2012 R2 base image

1. Obtain a Window Server 2012 R2 ISO image and run the following command (modify the **SourcePath** parameter to point to the location of the ISO).

```
.\Convert-WindowsImage.ps1 -SourcePath
C:\isoimages\WindowsServer2012R2\en_windows_server_2012_r2_x64_dvd_2707946.iso -VHDPath
D:\Hyper-V\Disks -VHDFormat VHDX -SizeBytes 40GB -VHDType
```

2. Create a new virtualized guest and specify the VHD created in the previous step.
3. Configure the new VM guest with any applications or utilities you want on all DCs.
4. Sysprep the image and shut down
5. Delete this VM guest from Hyper-V
6. Create new differencing disks from this parent disk (one per DC required)
7. Create new VM guests each one attached to their own differencing disk
8. Configure each with a hostname and IP address information that matches this table:

Table 5 lab configuration

Virtual Machine	Role	IP Address	Subnet	DNS Client settings
DC1.root.contoso.com	Domain controller in the forest root domain, DNS, GC, All FSMO roles	192.168.10.1	255.255.255.0	192.168.10.2; 127.0.0.1
DC2.root.contoso.com	Domain controller in the forest root domain, DNS, GC	192.168.10.2	255.255.255.0	192.168.10.1; 127.0.0.1
ChildDC1.child.root.contoso.com	Domain controller in a child domain in the forest, DNS, GC, Domain-wide FSMO roles	192.168.10.11	255.255.255.0	192.168.10.1; 127.0.0.1

Virtual Machine	Role	IP Address	Subnet	DNS Client settings
ChildDC2.child.root.contoso.com	Read-only domain controller (RODC) in the child domain in the forest, DNS, GC, MinShell	192.168.10.12	255.255.255.0	192.168.10.11; 127.0.0.1
TRDC1.treeroot.fabrikam.com	Domain controller in a tree root domain in the forest, DNS, GC, Domain-wide FSMO roles	192.168.10.21	255.255.255.0	127.0.0.1; 192.168.10.1
WIN8Client.root.contoso.com	Windows 8.1 administration workstation in the forest root domain	192.168.10.5	255.255.255.0	192.168.10.1; 192.168.10.2

9. Install the AD DS role on each machine and then configure them per Table 5.

How to reproduce the issues in this lab environment

Replication Access was Denied (8453) repro

1. Remove "Replicating Directory Changes" permissions from Enterprise RODC group on TreeRoot.fabrikam.com partition
2. Promote a server as an RODC in the child.root.contoso.com domain

   Result: RODC is unable to replicate the TreeRoot partition from any DC with error 8453

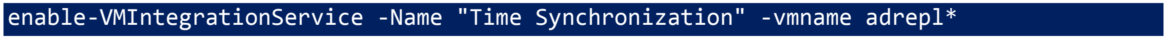
Lingering Object (8606), Tombstone lifetime (8614) and Target Principal Name is incorrect repro (-2146893022)

1. On the Hyper-v host: change system time to a time beyond TSL (in the past) ->result all Hyper-v guests configured for host time synchronization change their clock as well (this is the default configuration for hyper-v) s
   If time doesn't change immediately: stop and start the vmictimesync service to force a sync
2. Disable host time synchronization on all VMs

   ```
   Disable-VMIntegrationService -Name "Time Synchronization" -vmname adrepl*
   ```

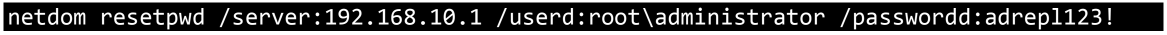
3. Fix Hyper-v Host time (all guests are still using old time)
4. Create user objects on DC1 at this time in the past
5. Move users to Engineering OU
6. Force replication out-> this replicates all new users to DCs in the forest
7. Pause all VMs other than DC1
8. On DC1, Delete one or more user objects

9. Fix time on DC1, and then force garbage collection



```
enable-VMIntegrationService -Name "Time Synchronization" -vmname adrepl*
```

11. Shutdown **DC1**, resume other DCs
12. Fix time on remaining DCs and then shutdown
13. Power on **DC1** and reset the computer account password with itself:
    netdom resetpwd /server:IP /userD root\administrator /passwordD pwd



```
netdom resetpwd /server:192.168.10.1 /userd:root\administrator /passwordd:adrepl123!
```

14. Startup the remaining DCs
15. On **DC2**: Make changes to one or more user objects (that were deleted from DC1 in step 8)