# Lab: Troubleshooting Replication Failures

This page left blank intentionally

### Overview

#### What You Will Learn

After completing this lab, you will be able to:

* Track update sequence numbers (USN) numbers during replication.
* Use Replmon to observe replication of objects and attributes.
* Troubleshoot a replication failure.

### Exercise 1

#### Introduction

At this stage of the class, you have two domain controllers and two servers that are members of that domain. In this exercise, you will promote one of your member servers to a domain controller in a new domain in the existing classroom forest. Once that is complete, you will promote the second server as a replica domain controller.

cx.contoso.com

m

Contoso.com

cz.contoso.com

### 

BOX1and BOX2 are currently domain controllers for c*x*.contoso.com and will remain so.

BOX3 and BOX4 are currently member servers for c*x*.contoso.com and will be promoted to domain controllers for a new domain c*z*.contoso.com where *z* is a number assigned to you by the instructor.

#### Procedure

1. Run DCPROMO on BOX3 to create a new child domain in an existing domain tree. Give the domain the DNS name of c*z*.contoso.com and the NetBIOS name of R*z* where *z* is a number assigned to you. Use the following credentials :
   1. Account: **Childadmin**
   2. Password: **Password1**
   3. Domain: **contoso.com**

Place the SYSVOL on drive D: (which should be NTFS). Leave the directory services restore password blank. Select permissions compatible with pre-Microsoft® Windows® 2000 server operating systems.

1. After BOX3 restarts, log on and verify that NETLOGON and SYSVOL are shared (run **Net Share** at the command prompt).
2. Run DCPROMO on BOX4 to create a replica domain controller of BOX3. Place the SYSVOL on drive D:. Leave the directory services restore password blank. Select permissions compatible with pre-Windows 2000 server operating systems.

### Exercise 2

#### Introduction

In this exercise you will use Active Directory Users and Computers on your group’s BOX1 and BOX3 to view the update sequence numbers for new Active Directory user objects. You will also view them after they have been replicated to BOX2 and BOX4.

#### Procedure

1. Log on to your group’s BOX1 and BOX3 as an administrative account.
2. Create a new user using Active Directory Users and Computers.
3. On the **View** menu, ensure that **Advanced Features** are enabled.
4. Open the **Properties** for the user you have just created and select the **Object** tab.

Note the following information for the user you have just created.

Answers

Yes. This is because the object is created in one transaction, and the attributes are populated in subsequent transactions. However, the time may be the same depending on the speed of the computer and the load on the computer. It may be that both of these were committed in the same second.

**Object Class:**

**Created: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Modified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Current USN:**

**Original USN:**

Are the time created and time modified different? If so, why?

1. Open Active Directory® Sites and Services on BOX1 and BOX3, and navigate to the NTDS Settings for your partner’s BOX (expand the tree in the left pane).
2. In the right pane, right-click the connection object for your BOX and select **Replicate now**.
3. On BOX2 and BOX4 in Active Directory Users and Computers, open the **Properties** for the user you have just received from your partner, and select the **Object** tab.

Note the following information for the user your partner just created.

Answers

The object was created using a single database transaction, thus creating a single USN.

**NOTE:** The USN values will be different in this step if students clicked any other property page or changed any other property value.

**Object Class:**

**Created: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Modified: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Current USN:**

**Original USN:**

Are the time created and time modified different? If so, why?

### Exercise 3

#### Introduction

In this exercise you will view replication between domain controllers in a domain using Active Directory Replication Monitor.

#### Procedure

1. Start REPLMON on your domain controllers.
2. On the **View** menu, click **Options.**

The **Active Directory Replication Monitor Options** page appears.

1. Click the **Status Logging** tab, select **Display Changed Attributes when Replication Occurs,** and then click **OK.**
2. Right-click **Monitored Servers**, and then click **Add Monitored Server**. The Add Monitored Server Wizard appears.
3. Select **Add the server explicitly by name,** and then click **Next**.
4. In the **Enter the name of the server to monitory explicitly** box, type the *servername,* of your BOX, and then click **Finish.** Your server’s naming contexts and replication partners are displayed in the console tree.
5. Add your partners BOX as a monitored server so that its naming contexts and replication partners are also displayed in the console tree.
6. Right-click the *servername* for your BOX.
7. Click **Show Attribute Meta-Data for Active Directory Object.**
8. Select **Use Credentials Already Supplied for Server**, and then click **OK**.

Answers

Because this user was created locally, all attributes were last modified locally.

1. In the text box for **View Meta-Data for Object,** type the distinguished name of the user you created in exercise 2.
2. The **Display Property Meta-Data for Object** dialog box appears.

Are the values in the **Local USN** column and the **USN on Orig Server** columnthe same for each attribute? Why or why not?

Answers

Yes, the highest and lowest USN values will match if the object has not been modified since it was created. However, if you switched to other user property pages, these numbers will not match because some property values are not committed to Active Directory until they are first viewed on the screen.

1. Note the following information for the user object.

Lowest USN on any attribute:

Highest USN on any attribute:

1. Do the lowest USN and highest USN values match the USN created and USN modified values recorded for this object earlier?
2. View the metadata for the same object on your partner’s BOX.
3. Are the values in the Local USN column and the USN on Orig Server column the same for each attribute? Why or why not?

Answers

16. No. Most attributes were last modified on your partner’s server. Since the USN on Orig Server reflects the USN for the server where the attribute was last modified, most attributes have a different local USN.

17. cn

1. Which attribute was last modified locally?
2. Edit the properties of the user you have just created, for example, enter an Office number.
3. Note the following information for your user.

Current USN: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Original USN: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Replicate the change to your partner.
2. User REPLMON to observe the USNs of the attribute.
3. Modify the attribute on your partner’s computer.
4. Replicate the changes.
5. Use REPLMON to observer the USNs of the attribute on both computers.

### Exercise 4

#### Introduction

In this exercise you will create Active Directory application partitions.

#### Procedure

Creating and Managing Application Partitions with NTDSUTIL

The following section outlines how to create and view application directory partitions.

1. Logon to BOX1 and BOX3 using Enterprise Admin credentials from the contoso.com domain
2. Open a command prompt and type **ntdsutil**
3. At the ntdsutil command prompt type **domain management**
4. At the domain management command prompt, type: **connection**
5. At the connection command prompt, type: **connect to server *ServerName***.  
     
   ServerName: The DNS name of the domain controller on which to create or delete the application directory partition.
6. At the connection command prompt, type: **quit**
7. At the domain management command prompt: type:   
   **create nc <*ApplicationPartition> <DomainController>***ApplicationDirectoryPartition  
   The distinguished name of the application directory partition that you want to create or delete. For example, the distinguished name of the application directory partition AppPart*X*.C*X*.contoso.com is dc=AppPart*X*,dc=c*X*,dc=contoso,dc=com  
     
   DomainController  
   The DNS name of the domain controller on which to create or delete the application directory partition. Or, type NULL to create the application directory partition on the domain controller to which you are currently connected.  
   The value for the DomainController parameter of the create nc command must either be the DNS name of a domain controller or, if you are creating the application directory partition on the domain controller to which you are currently connected, use the NULL variable.
8. To verify the application partition was created.  
   At the domain management command prompt type: **list**
9. Verify the crossRef object for your new app partition is enabled.  
     
   Use ADSIEdit to check the status of the **Enabled** attribute of your app partitions crossRef object. Make sure the value is set to **True**.
10. To add an application directory partition replica:  
      
    At the domain management command prompt type:  
      
    **add nc replica <*ApplicationDirectoryPartition> <DomainController>***DomainController  
    The DNS name of the domain controller on which to add or remove the replica of the application directory partition.  
      
    ApplicationDirectoryPartition   
    The distinguished name for the application directory partition of which you want to add or remove a replica. For example, the distinguished name of the application directory partition AppPart*X*.c*X*.contoso.com is dc=AppPart*X*,dc=c*X*,dc=contoso,dc=com   
    The value NULL can be used for the DomainController parameter of the add nc replica and remove nc replica commands if you are adding or removing the application directory partition replica on the domain controller to which you are currently connected.
11. Once a domain controller is added as a replica of the partition, the Microsoft® Active Directory® Knowledge Consistency Checker (KCC) builds the replica links and connection objects (if necessary). After the links are added to both members, the replication of the partition will commence.   
    Use **“Repadmin /kcc”** to immediately initiate a review of the topology and generate connection objects and replication links.   
    Use **“repadmin /showrepl”** to view the status of links.
12. Viewing Application Partitions  
      
    Just like any other partitions, application partitions can be viewed from LDP.EXE or ADSI Edit. Connect to any root domain controller and set the base distinguished name (DN) to view the forest root domain. All the partitions that are hosted under the forest root are visible and can be expanded to the containers and zone data.
13. Use ADSIEdit to connect directly to the application partition you created earlier and test the app partitions functionality
    1. Right-click on **ADSI Edit** and select **Connect to**
    2. Under **Connection Point** select the option:  
       **Select or type Distinguished Name or Naming Context**
    3. Enter the DN of your application partition
14. Attempt to create a container object in the new application partition.  
    Did this succeed?
15. Use ADSIEDIT to verify that replication is occurring across all replica servers.
16. Attempt to create a new user object in the application partition.  
    What was the result and why?

### Exercise 5

#### Introduction

In this exercise you will observe what happens to an object when it is moved under a deleted parent.

#### Procedure

1. Create an organizational Units OU1 and OU2 and a user inside each one on BOX1 and BOX3.
2. Replicate those additions to your partner.
3. On BOX 1 and 3 delete the OU1. On your other domain controllers move the user account you created in step 1 from OU2 to OU1
4. Replicate those changes.
5. What has happened to the user accounts?

Answers

5. They have been moved into the LostAndFound container.

**For the next exercise you will need to supply the instructor with details of the objectGUID for BOX1 and BOX3. To do this, run**

**repadmin /showreps**

**Stop before continuing and wait for other teams to finish the labs to this point and the instructor to complete the classroom setup changes.**

### Exercise 6

#### Introduction

Do not begin this exercise until the instructor advises you to begin.

BOX2 and BOX4 do not seem to be receiving changes made on their partners.

Instructor Note

This is the domain name service (DNS) portion of this lab. Before starting this lab, remove the following record for BOX1 out of each group of two:

<GUID>.\_msdcs.contoso.com

(where <GUID> is the objectGUID of the server with the data portion of the record being the FQDN of the machine – e.g. STUDENTx.*childDomain*.contoso.com)

Important: Disable Dynamic Update on the zone file or the pre-staged problem will heal itself when the Netlogon service attempts to re-register.

#### Procedure

1. Restart the Netlogon service on BOX2 and BOX4.
2. Increase the logging for Replication events on BOX2 and BOX4 to a value of 3*.*
3. What events are recorded in the Directory Service event log? What is the error? (You may need to reboot your domain controller) Note the globally unique identifier (GUID) that is referred to in the recorded events. Also note the fully qualified domain name (FQDN) referred to in the events (e.g. 00000000-0000-0000-0000-000000000000.\_msdcs.contoso.com). This is the GUID of the domain controller that the local computer is attempting to replicate FROM.

1. Can you ping your partner’s server by its IP address?

Answers

4. Yes, however, that is not what the domain server uses to replicate with partners. It must resolve the CNAME record used by the partner (objectGUID) and resolve that to a host name, which in turn is resolved to an IP address.

5. No. Ping should return “unknown host.”

1. Can you ping the FQDN that resolves the GUID of the server to the domain controller (from step 3)?
2. Before you resolve the problem, you will use REPADMIN and REPLMON to view the same error displayed by both of these tools.
   1. From a command prompt, enter the command **repadmin /showreps**. For each naming context or directory partition replicated on the local computer, the direct replication partners for each are displayed along with the replication status for the last successful and last attempted replication. Note the objectGUID. This maps to the “NTDS Settings” object in the Active Directory Configuration container that is used to resolve the replication partner and should also be the same GUID (in our example) identified in the event logs.
   2. REPLMON displays the same information, in GUI and report form, in a very similar manner, but can also be used to determine the GUID for a server without having event log errors, etc.
      1. Start Replmon.
      2. From the **Edit** menu, click **Add Monitored Server**, select **Add the server explicitly by name**, and then click **Next**.
      3. In the “Enter the name of the server to monitor explicitly” field, enter the name of your server, and then click **Finish**.
      4. After the naming contexts and the replication partners have been enumerated, you can tell at a glance which ones are failing by the icons associated with each (red x on an icon that depicts two servers on a network). More information is available in the detail log report in the right pane.
      5. Right-click the monitored server (the child object that represents the server you are monitoring directly beneath the site node) and select **Generate Status Report**.
      6. Enter a filename to store the output results and click **Save**.
      7. Keep the defaults for the Report Options and click **OK**.
      8. After the report is generated, select **Open Log** from the **File** menu and load the file you just created.
      9. In the “Enterprise Data” section of the report (located near the bottom of the report), each server in each site is listed along with associated information about the server. Included in this information is the Server GUID (used for DNS). This GUID is what should be registered in DNS (should be the same GUID displayed in the event logs and from REPADMIN) so that other domain controllers can resolve a server from its GUID and in turn resolve an IP address from the host name.

Answers

Restarting the NETLOGON service should re-register these records. The student can also look in the NETLOGON.DNS file that gets created during the startup of the NETLOGON service. Note: If the lab goes on for too long, NETLOGON will re-register this record automatically, and it will appear that the problem is no longer present, which it isn’t.

1. Before the domain controllers re-establish replication, observe the output from DCDIAG .
2. If the record is not there, how does it get re-registered? Normally, the NETLOGON service, at intervals and at service start, checks the DNS records on the server to verify they are correct. You could stop and restart the NETLOGON service to cause this process to occur. However, for this lab, you have disabled dynamic updates (something good to check for though, normally) so that the domain controllers would not heal the problem themselves. Using the Terminal Server Client, open the DNS administrative tool on the ROOTDNS server and add a CNAME record for the GUID of your server that points to the FQDN of the server. Additional note: You can also use the NETLOGON.DNS file to check the records that should be getting registered in DNS.
3. Using Active Directory Sites and Services or REPLMON, force replication FROM the failing server to its partner. Verify that replication took place.

Instructor Note

Once all students have completed this exercise, you can switch DNS dynamic updates on again.

### Exercise 7 (optional)

#### Introduction

When an Active Directory object is deleted, a small portion of the object remains for a specified period of time so that other domain controllers that are replicating changes will become aware of the deletion. In this exercise you will learn how to view the objects that have been deleted.

#### Procedure

1. Start Ldp.exe, and **Connect** and **Bind** to your domain controller using an administrative account. After the connection is established, server-specific data is displayed in the right pane.
2. On the **Browse** menu, click **Search**.
3. In the BaseDN box, type the distinguished name of the deleted objects container in your domain, for example, CN=deleted objects,DC=c1,dc=contoso,dc=com
4. Ensure that (objectclass=\*) appears in the Filter box. In the Scope section, click **Subtree**, and then click **Options**.   
     
   In the Search Options dialog box, set the Timeout (s): value to **10** and click **Extended** in the Search Call Type section.
5. Click **Controls**, and then select **Return Deleted Objects** from the Load Predefined dropdown list. Click **OK** to close the Controls dialog box.
6. In the Search Options dialog box, click **OK**. In the Search dialog box, click **Run**.

The deleted objects should be displayed in Ldp in the right pane. For example, the following sample text would be output if the administrator had deleted the "student1" user account.

ldap\_search\_ext\_s(ld, "cn=deleted objects,dc=contoso,dc=com", 2, "(objectclass=\*)", attrList, 0, svrCtrls, ClntCtrls, 0, 0 ,&msg)

Result <0>: (null)

Matched DNs:

Getting 1 entries:

>> Dn: CN={7610e92e-bc0b-49a7-a8f9-e8acbc3c7295}\|

DEL:6d7a83b8-71c4-4f6b-93f3-2bfd569424be,CN=Deleted Objects,DC=contoso,DC=com

1> canonicalName: contoso.com/Deleted Objects/{7610e92e-bc0b-49a7-a8f9-e8acbc3c7295}|

DEL:6d7a83b8-71c4-4f6b-93f3-2bfd569424be;

1> cn: {7610e92e-bc0b-49a7-a8f9-e8acbc3c7295}|

DEL:6d7a83b8-71c4-4f6b-93f3-2bfd569424be;

1> distinguishedName: CN={7610e92e-bc0b-49a7-a8f9-e8acbc3c7295}\|

DEL:6d7a83b8-71c4-4f6b-93f3-2bfd569424be,CN=Deleted Objects,DC=contoso,DC=com;

3> objectClass: top; leaf; nTDSConnection;

1> name: {7610e92e-bc0b-49a7-a8f9-e8acbc3c7295}|

DEL:6d7a83b8-71c4-4f6b-93f3-2bfd569424be;

Note that you can use the same process for looking for deleted objects in the schema and/or the Active Directory configuration partition.

A new feature in Microsoft® Windows Server™ 2003 allows you to “reanimate” objects that have been deleted. Reanimation only brings back some of the attributes. To do this, perform the following steps:

1. From the **Browse** menu, select **Modify**.
2. In the DN field, enter the current distinguished name of the deleted object you want to recover, for example, CN=Alice\0ADEL:6d7a83b8-71c4-4f6b-93f3-2bfd569424be,CN=Deleted Objects,DC=contoso,DC=com.
3. In the Attribute field, type **isDeleted**.
4. From the Operation radio buttons, select **Delete**, and click **Enter**.
5. In the Attribute field, type the attribute name **distinguishedName**.
6. In the Values field, type the new distinguished name that will represent the reanimated object. For example, CN=Alice,DC=CONTOSO,DC=COM.
7. Select the **Replace** radio button, and click **Enter**.
8. Ensure that the **Synchronous** and **Extended** check boxes are enabled (checked).
9. Click **Run**. Results will appear in the right pane indicating that the object has been modified.
10. View the object in Active Directory Users and Computers. Are there any attributes populated?

### Exercise 8 (optional)

#### Introduction

In this exercise, you will experiment with the new Windows Server 2003 feature to replicate a single object on demand.

#### Procedure

1. Create two new users.
2. Use the repadmin replsingleobj command to replicate one user. (You may need to change the default change notification period from the default of 15 seconds to a more manageable level, such as 300.)