



Operating System

Chapter 11

Troubleshooting Guidelines for Branch Office Environments

Deployment and Operations Guide

Abstract

This chapter outlines the steps necessary to diagnose, understand, and resolve issues that may arise in large Active Directory™ directory service branch office deployments.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries/regions.

CONTENTS

INTRODUCTION	1
Resource Requirements	1
What You Will Need	1
What You Should Know	1
INTRODUCTION	2
TCP/IP AND DNS CONFIGURATION	3
ACTIVE DIRECTORY REPLICATION TROUBLESHOOTING	4
Checking Replication Partners	4
Checking Replication Failures	5
No Inbound Neighbors	5
Replication Status Error	5
TROUBLESHOOTING "NO INBOUND NEIGHBORS"	7
TROUBLESHOOTING REPLICATION ERRORS	9
Access Denied	9
Resolution Options for Replication Failure	10
Replication Failure Resolution Option One	10
Replication Failure Resolution Option Two	12
Verification of Success	13
Authentication Service Is Unknown	13
The Domain Controller Fails to Establish a Replication Link	14
Replication Link Already Exists	14
Target Account Name Is Incorrect	15
RPC Server Not Available	17
DNS Lookup Failure	18
Directory Service Too busy – Duplicate Connection Object	20
Time Difference / LDAP Error 82	22
The replication system encountered an internal error	22
No More End-Point	23
LDAP Error 49	24
Unable to Run Administration Tools	24
Non-Error Status	25
FALLBACK PLANS	27
Fallback Plan prior to running the Active Directory Installation Wizard	27
Fallback Plan After running the Active Directory Installation Wizard	27
Failure During the Active Directory Installation Wizard	27
Option One: Remove the NTDS Settings Object	27
Option Two: Remove the Server Object from Active Directory	29
TROUBLESHOOTING FRS	31

NON-AUTHORITATIVE FRS RESTORE	35
Restoring Hub Domain Controllers	35
Restoring Branch Office Domain Controllers	36
SUMMARY	37
More Information	37

INTRODUCTION

This chapter provides information to enable you to resolve any issues that may arise in your Active Directory™ directory service environment. The information contained in this chapter is not specific to branch office environments, but can be used to troubleshoot Active Directory issues in any type of Active Directory deployment.

Resource Requirements

Individuals from the following teams will be required to perform the troubleshooting tasks in this chapter:

- Microsoft® Windows® 2000 Active Directory Administration
- Infrastructure Administration
- Network Administration

What You Will Need

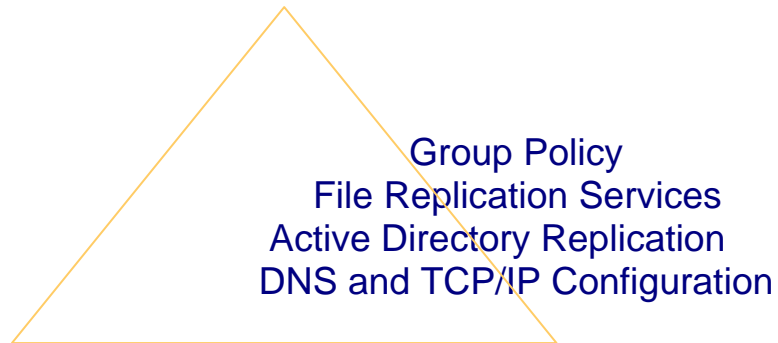
You will need copies of the complete Branch Deployment Planning Guide and previous chapters of the Branch Deployment and Operations Guide, in addition to the plan and final configuration deployed for your organization. In addition, it is recommended that you have a copy of the Microsoft Windows 2000 Resource Kit and, in particular, the TCP/IP Core Networking Guide.

What You Should Know

You must know the basics of network troubleshooting, including the usage of tools such as **ipconfig**, **ping**, **arp**, and **nslookup**, and Event Viewer.

INTRODUCTION

The first task in troubleshooting any network problem requires correctly identifying the problem. In a large branch office deployment of Active Directory, the distributed and layered nature of the technologies can make problem diagnosis challenging. To assist with the troubleshooting process, you must understand where the various technologies exist in the layered hierarchy as illustrated in the diagram below:



Instability or improper configuration can lead to problems with some of the layers in the illustration above. To successfully troubleshoot any of these areas, you must start your analysis with the bottom layer and progress up through each layer until all issues have been resolved.

TCP/IP AND DNS CONFIGURATION

Active Directory requires that Transmission Control Protocol/Internet Protocol (TCP/IP) and associated services, such as Domain Name System (DNS), run correctly. This assumes that the Internet Protocol (IP) and DNS are configured correctly for Active Directory to be able to run properly and, specifically, that the following parameters are configured correctly:

- IP address and subnet mask
- Default gateway
- IP address for preferred and alternate DNS server
- DNS forwarders

The availability of DNS directly impacts the availability of Active Directory. DNS provides the namespace and name resolution mechanisms that Active Directory uses. It is therefore essential that each computer have the correct IP address of the appropriate DNS servers.

The local DNS server must also be configured correctly. It should be authoritative for the DNS namespace its clients are in, and the DNS Server service itself should be configured correctly and functioning normally.

The tools required to troubleshoot TCP/IP and DNS include:

- ipconfig
- ping
- arp
- nslookup

This paper assumes that you have a familiarity with these tools. For more information about using these tools, see Chapter 3, "Troubleshooting," in the TCP/IP Core Networking Guide of the Microsoft Windows 2000 Resource Kit.

After TCP/IP and DNS configuration have been checked successfully, you must check that Active Directory is working. Only after you are sure Active Directory is working can you begin troubleshooting the File Replication service (FRS) and Group Policy. The main tool to use for checking the status of the Active Directory replication between two replication partners is the Replica Administration tool, or Repadmin.

Repadmin is included in the Support Tools that are shipped with Windows 2000. It has a number of switches that allow administrators to check the replication partners used by a given domain controller and to display and amend replication configuration. A number of these switches should be used during your troubleshooting of replication. Common replication error events, and how Repadmin can be used to analyze and correct these errors, will be presented.

Checking Replication Partners

When troubleshooting replication errors, it is helpful to know who the replication partners of a specific domain controller are and the status of replication with each of those partners. This can be done by using the command **repadmin /showreps**. The resulting output shows the replication partners in the “inbound neighbors” section and the replication state of each of the three naming contexts (Domain, Schema, and Configuration).

Scenario information

In the examples used in this document, the branch office domain name is *branches.corp.hay-buv.com*. The root domain name is *corp.hay-buv.com*. The branch office domain controller is *BODC1.branches.corp.hay-buv.com*. It is located on a site called *BOSite1*. Its replication partner is *BH1.branches.corp.hay-buv.com* located in a site *HubSite*. The PDC Emulator of *branches.corp.hay-buv.com* is *Hubdc1.branches.corp.hay-buv.com*

Repadmin Tool

When replication is running properly, the output for the **repadmin /showreps** command can be seen in the example below. (Note that commentary has been added at the right, which tells you what information is being provided in the output at that point, which in some cases wraps to the beginning of the next line.)

```
repadmin /showreps
BOSite1\BODC1                               ← Site name and computer
DSA Options : (none)
objectGuid : c8ffb9f6-94b4-428f-bbf2-749f583737c2 ← Globally unique identifier (GUID)
of the NTDS Settings object of the local computer
invocationID: 9578742f-ac12-4802-b8fb-ef073d41f370

==== INBOUND NEIGHBORS =====
DC=branches,DC=corp,DC=hay-buv,DC=com       ← Replication link for the domain naming context
HubSite\BH1 via RPC                          ← Replication status with the replication partner
objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51 ← GUID of the NTDS Settings
object of replication partner
Last attempt @ 2000-10-15 20:09.57 was successful. ← Status of last replication

CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com ← Replication link for
the schema naming context
HubSite\BH1 via RPC                               ← Replication status with the replication
partner
```

```

        objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51 ← GUID of the NTDS Settings
object of replication partner
        Last attempt @ 2000-10-15 19:54.18 was successful. ← Status of last replication

CN=Configuration,DC=corp,DC=hay-buv,DC=com ← Replication link for
the configuration naming context
        HubSite\BHL via RPC ← Replication status with the replication
partner
        objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51 ← GUID of the NTDS Settings
object of replication partner
        Last attempt @ 2000-10-15 19:54.10 was successful. ← Status of last replication

==== OUTBOUND NEIGHBORS FOR CHANGE NOTIFICATIONS =====
DC=branches,DC=corp,DC=hay-buv,DC=com
        HubSite\BHL via RPC
        objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51

CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com
        HubSite\BHL via RPC
        objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51

CN=Configuration,DC=corp,DC=hay-buv,DC=com
        HubSite\BHL via RPC
        objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51

```

Checking Replication Failures

By using the Repadmin tool, replication failures can be detected when repadmin /showreps shows one of the following outputs:

- No inbound neighbors
- Replication status error

Each of these errors and its meaning is discussed below:

No Inbound Neighbors

When this error appears, the following output can be seen from the Repadmin tool:

```

BOSitel\BODC1
DSA Options : (none)
objectGuid : c8ffb9f6-94b4-428f-bbf2-749f583737c2
invocationID: 9578742f-ac12-4802-b8fb-ef073d41f370

==== INBOUND NEIGHBORS =====
==== OUTBOUND NEIGHBORS FOR CHANGE NOTIFICATIONS =====

```

This error indicates one of the following:

- No connection object exists to indicate from which domain controller(s) this domain controller should replicate.
- One or more connection objects exist, but the domain controller is unable to contact the source domain controller to create the replication links.

Replication Status Error

This error message tells you the replication has failed with the replication partner for the specific naming context shown. For example:

```

DC=branches,DC=corp,DC=hay-buv,DC=com
        HubSite\BHL via RPC
        objectGuid: 62d85225-76bf-4b46-b929-25a1bb295f51
        Last attempt @ 2000-10-16 14:50.05 failed, result 8442:
        The replication system encountered an internal error.

```

Last success @ (never).

The following sections will discuss the steps you should take to analyze and fix these two errors.

TROUBLESHOOTING "NO INBOUND NEIGHBORS"

When you receive the "No inbound neighbors" output, you first must start Active Directory Sites and Services to see that a connection object has been created between the domain controller and its replication partner. You connect to the destination domain controller by right-clicking on Active Directory Sites and Services, selecting Connect to Domain Controller, and then selecting *Sites* (where *Sites* is the name of the site), *Servers* (where *Servers* is the name of the server), and NTDS Settings. For effective troubleshooting, follow the process outlined below.

If no connection object exists, it must be created. This can be done in one of the following ways:

- Manually by using Active Directory Sites and Services to create the connection object.
- Automatically if the Inter-Site Topology Generator (ISTG) function of the Knowledge Consistency Checker (KCC) is enabled.
- By using the `Mkdsx` script. This is the best way to proceed for creating connection objects between domain controllers located in different sites in a branch office environment. For more information about `Mkdsx`, see Chapter 3, "Planning Replication for Branch Office Environments" of the Active Directory Branch Office Planning Guide, Chapter 4, "Pre-Staging Configuration at the Hub," of the Active Directory Branch Office Deployment and Operations Guide, and Chapter 7, "Pre-shipment Configuration of the Branch Office Domain Controller," of the Active Directory Branch Office Deployment and Operations Guide.

After the connection objects have been created, or if they already exist, run **repadmin /kcc**. The domain controller will then contact its replication partners and authenticate itself against them. This is necessary to create the replication links.

After the replication procedure has been performed, look for the following events in the directory services event log of Event Viewer:

Event ID 1264:

A replication link for the partition CN=Configuration,DC=corp,DC=hay-buv,DC=com from server CN=NTDS Settings,CN=BH1,CN=Servers,CN=HubSite,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com has been added.

This event is logged by the KCC after it has properly created the replication link. As long as this event is logged, replication should occur automatically at the next scheduled time. This process can be initiated manually for each of the three naming contexts on the local domain controller by using the following commands:

```
repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

```
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com  
%computername% <rep_partner_GUID>
```

If event identification (ID) 1264 is not logged in Event Viewer, the replication link failed to be established. The directory services event log will then log event ID 1265 describing the reason for the failure. In this case, use the same resolution process as that used in dealing with errors generated when running the **repadmin /showreps** command.

There are a variety of errors that may be displayed when running **repadmin /showreps**. These errors and their corresponding resolution mechanisms are discussed in the remainder of this chapter.

TROUBLESHOOTING REPLICATION ERRORS

Replication errors are shown by the output of **repadmin /showreps**. The output from this command shows the status of the last replication for each naming context over an existing replication link. These replication failures are usually not recorded in the Directory Service event log.

As explained in the previous section, replication errors can occur when the KCC fails to establish a replication link with a given replication partner. When this happens, **repadmin /showreps** displays no information. You must go to the Directory Service event log in Event Viewer and note the error explanation in event ID 1265.

A list of errors produced by event ID 1265 and a corresponding list of resolution methods are discussed below.

Access Denied

This error occurs if the local domain controller fails to authenticate with a replication partner when creating the replication link or when trying to replicate over an existing link. This typically happens when a domain controller has been disconnected from the rest of the network for an extended period of time. In this scenario, the computer account password may differ from the corresponding value stored in Active Directory of its replication partner. Each of these situations and their corresponding outputs are shown below.

Failure to Establish a Replication Link

In this case, **repadmin /showreps** will show no inbound neighbors. As a result, no error is displayed. Go to the Directory Service event log in Event Viewer where you will see the following event:

Event ID 1265

The attempt to establish a replication link with parameters

Partition: DC=branches,DC=corp,DC=hay-buv,DC=com

Source DSA DN: CN=NTDS

Settings, CN=HubDC1, CN=Servers, CN=HubSite, CN=Sites, CN=Configuration, DC=corp, DC=hay-buv, DC=com

Source DSA Address: 62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com

Inter-site Transport (if any): CN=IP, CN=Inter-Site

Transports, CN=Sites, CN=Configuration, DC=corp, DC=hay-buv, DC=com

failed with the following status:

Access is denied.

The record data is the status code. This operation will be retried.

Replication Fails and Displays an Error

When a replication link exists between the two domain controllers, but replication cannot be properly performed, **repadmin /showreps** shows a failed status for the previous replication of one or more of the listed naming contexts. The information is

provided in the format: "Last attempt at <date - time> failed" with the "Access denied" error. Unlike the failure to establish a replication link, in which the cause was indicated in the error message in the error log in Event Viewer, no event will be logged in the event log.

Resolution Options for Replication Failure

A number of resolution methods are possible, depending on the nature of the given problem. Each of these methods is outlined below.

Replication Failure Resolution Option One

This set of procedures should be attempted first. You will stop the Key Distribution Center (KDC) service, remove the Kerberos tickets, and then reset the computer password. Then, you will synchronize the domain naming context and determine that replication is working properly. Finally, you will synchronize each of the naming contexts.

On the local domain controller, stop the KDC service by typing "net stop KDC" at a command prompt. If the KDC service will not stop, set its startup state to "disable" and then restart.

Reset the computer account's password on the domain PDC Emulator by opening a command prompt and then typing:

```
netdom resetpwd /server:<PDC Emulator name>
/userd:<domain>\administrator /passwordd:*
```

You should now see the following output:

```
The machine account password for the local computer has been
successfully reset. The command completed successfully.
```

If the command fails with a "Logon failure, the target account name is incorrect" error, the domain controller is probably not in the Domain Controllers organizational unit.

Synchronize and Check Replication

Synchronize the domain naming context of the replication partner with the HUBDC1 PDC Emulator by typing at a command prompt:

```
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com
<hub_server> <GUID of the Hubdc1 PDC Emulator>
```

This forces the replication of the computer account.

The GUID of the HUBDC1 PDC Emulator NTDS Settings object can be found in the output (as ObjectGUID) by using the following command:

```
repadmin /showreps <name of the Hubdc1 PDC emulator>
```

If the replication partner of the local domain controller is not itself a replication partner of the HUBDC1 PDC Emulator, this command will fail. In this case, a replication link can be created manually between the replication partner and the HUBDC1 PDC Emulator by using the following command at a command prompt:

```
repadmin /add <Domain NC> <Replication partner FQDN> <Hubdc1 PDC Emulator FQDN> /u:<domain>\administrator /pw:*
```

The creation of this replication link will trigger automatically the replication of the domain naming context between the HUBDC1 PDC Emulator and the replication partner. After the procedures above have been performed, the computer account of the local domain controller should be synchronized with its replication partner. Replication between the two domain controllers should now function correctly.

To check that replication is operating properly, type the following command in the command prompt:

```
Repadmin /showreps
```

If the replication partner connection is shown in the result, everything is functioning correctly. If the output of this command is blank, in a command prompt, type **repadmin /kcc**. The domain controller then contacts its corresponding replication partners and authenticates itself against them to create the replication links. Then look for the following events in the Directory Services event log :

Event ID 1264 :

```
A replication link for the partition CN=Configuration,DC=corp,DC=hay-buv,DC=com from server CN=NTDS Settings,CN=BH1,CN=Servers,CN=HubSite,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com has been added.
```

This event is logged by the KCC after it has properly created the replication link. Provided that this event is logged, replication should occur automatically the next time it is scheduled. If this event is not logged, review the error message, and see the relevant section of this chapter.

Synchronize Each Naming Context

After the replication links are in place successfully, synchronize each of the naming contexts by using the relevant commands below.

The Schema naming context is used first because it is the smallest. This will lead to confirmation of success in the quickest time possible. Synchronize the schema naming context on the local domain controller by typing the following command in a command prompt:

```
repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

Replication of the configuration and domain naming contexts can also be triggered by typing the following commands in a command prompt:

```
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

```
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

If the **repadmin /sync** command fails with a new error, see the relevant section of this chapter to solve the newly identified problem.

If **repadmin /sync** command is successful, **repadmin /showreps** should not show

any errors. Restart the KDC service on the local domain controller. This can be done by typing the following command at the command prompt:

```
net start kdc
```

Replication Failure Resolution Option Two

In this option, you create a temporary link between the local domain controller and its replication partner for the naming contexts. You will do this if a new event ID 1265 is logged relating to a new access denied when running **repadmin /kcc** or if **repadmin /sync** fails with another "Access denied" error. To create this link, perform the following steps.

1. For the configuration naming context, at a command prompt, type the following:
`repadmin /add <Configuration NC> <Local DC FQDN> <Replication partner FQDN> /u:<domain>\administrator /pw:*`

For example, on BODC1 you would enter:

```
repadmin /add CN=Configuration,DC=corp,DC=hay-buv,DC=com  
%computername%.branches.corp.hay-buv.com HubDC1.branches.corp.hay-  
buv.com /u:branches\administrator /pw:*
```

2. For the schema naming context, at a command prompt, type the following:
`repadmin /add <Schema NC> <Local DC FQDN> <Replication partner FQDN> /u:<domain>\administrator /pw:*`

For example, on BODC1 you would enter:

```
repadmin /add CN=Schema,CN=Configuration,DC=corp,DC=hay-  
buv,DC=com %computername%.branches.corp.hay-buv.com  
HubDC1.branches.corp.hay-buv.com /u:branches\administrator /pw:*
```

3. For the domain naming context, at a command prompt, type the following:
`repadmin /add <Domain NC> <Local DC FQDN> <Replication partner FQDN> /u:<domain>\administrator /pw:*`

For example, on BODC1 you would enter:

```
repadmin /add DC=branches,DC=corp,DC=hay-buv,DC=com  
%computername%.branches.corp.hay-buv.com HubDC1.branches.corp.hay-  
buv.com /u:branches\administrator /pw:*
```

If successful, all of these commands should return the following result:

```
One-way replication from source:HubDC1.branches.corp.hay-buv.com to  
dest:BODC1.branches.corp.hay-buv.com established.
```

Note: This command can fail if the KCC starts during this process and no corresponding connection object exists. If this occurs, the KCC will delete any replication links for which no corresponding connection object exists. So you should make sure there is a connection object first.

Note: These commands can take a very long time to complete because they trigger the replication of the corresponding naming context. All naming contexts must be replicated properly. If a replication gets pre-empted, rerun the command until it completes successfully. Otherwise the "Access denied" error might appear again.

Verification of Success

Success can be checked in the same way as before. Run **repadmin /showreps** at the command prompt. If the output of this command shows no corresponding replication partner, run **repadmin /kcc** at the command prompt, and then look for event ID 1264 in the Directory Services event log in Event Viewer.

Then trigger the replication of the schema naming context using **repadmin /showreps**. Restart the KDC on the local DC by typing the following command at the command prompt:

```
net start kdc
```

If the methods used above are successful, replication will occur properly for the three naming contexts at the next scheduled interval. After each naming context has been replicated, **repadmin /showreps** on the local domain controller will show a successful status.

Authentication Service Is Unknown

An authentication service is unknown error can occur when a replication link exists between the two domain controllers but replication cannot be properly performed. In this scenario, as described in the first section, **repadmin /showreps** shows inbound neighbors, but the status of the last replication for one or more naming contexts returns "Last attempt at <date - time> failed" with the "Authentication service is unknown" error. Then no event is logged in the event log.

This error can occur in one of the following situations:

The local domain controller tries to establish a replication link with its replication partner and it fails. In this scenario, **repadmin /showreps** shows no inbound neighbors, so it does not include an error description. To see the error, go to the Directory Service event log in which the following event is logged:

```
Event ID 1265
Partition: DC=branches,DC=corp,DC=hay-buv,DC=com
Source DSA DN: CN=NTDS
Settings,CN=BH1,CN=Servers,CN=HubSite,CN=Sites,CN=Configurati
on,DC=corp,DC=hay-buv,DC=com
Source DSA Address: 62d85225-76bf-4b46-b929-
25a1bb295f51._msdcs.corp.hay-buv.com
Inter-site Transport (if any): CN=IP,CN=Inter-Site
Transports,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com
failed with the following status:
The authentication service is unknown.
The record data is the status code. This operation will be retried.
```

These two types of errors are generally related to the local KDC service. This will happen because of one of the following reasons:

- The domain controller fails to establish a replication link.
- A replication link already exists between the two domain controllers.

To correct this, follow the appropriate procedure below.

The Domain Controller Fails to Establish a Replication Link

In this scenario, you will stop the KDC service, purge the ticket cache, and then create the replication link.

To correct the domain controller fails to establish a replication link:

1. Stop the KDC service by typing the following command at the command prompt :
`net stop KDC`

It may be impossible to stop the service. In this scenario, set the KDC service startup state to "disable" and reboot.

2. Set the KDC service startup state to "disable" by using the Computer Management Microsoft Management Console (MMC) tool, and then reboot the domain controller.
3. On the domain controller, run `repadmin /kcc` at a command prompt. The domain controller then contacts its replication partners and authenticates itself against them to create the replication links.
4. Look for the following events in the Directory Services event log in Event Viewer:

Event ID 1264 :

A replication link for the partition CN=Configuration,DC=corp,DC=hay-buv,DC=com from server CN=NTDS Settings,CN=HubDC1,CN=Servers,CN=HubSite,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com has been added.

This event is logged by the KCC after it has properly created the replication link. Provided that this event is logged, replication should occur automatically the next time it is scheduled. To make sure it can happen correctly, it can be triggered manually for the three naming contexts by using the following commands:

```
repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

```
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

```
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

If no event ID 1264 is logged, the replication link failed to be established. The Directory Service event log in Event Viewer then logs event ID 1265 describing the reason for the failure. Look for this event and perform the relevant troubleshooting steps described in this chapter.

If this procedure worked, the replication then occurs properly for the three naming contexts at the next scheduled time. Restart the KDC service on the local domain controller by typing the following command at the command prompt:

```
net start kdc
```

Replication Link Already Exists

In this scenario, perform the following procedure.

To correct the replication link already exists:

1. Stop the KDC service by typing the following command at the command prompt:
`net stop kdc`
It may be impossible to stop the service. In this event, set the startup state of the service to "disable" by using the Computer Management MMC tool, and then reboot.
2. Set the KDC service startup state to "disable" by using the Computer Management MMC tool,
3. Restart the domain controller.
4. Synchronize the schema naming context on the local domain controller by typing the following command at a command prompt:
`repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>`
The schema naming context is used first because it is the smallest. This will lead to confirmation of success in the quickest time possible.
5. Replication of the configuration and domain naming contexts can also be triggered by typing the following commands at a command prompt:
`repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>`
`repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>`
6. If the **repadmin /sync** command fails with a new error, see the corresponding section of this document. If the **repadmin /sync** command is successful, **repadmin /showreps** should not show any more errors. Restart the KDC on the local domain controller. This can be done by typing the following command at the command prompt:
`net start kdc`

Target Account Name Is Incorrect

This error can occur either because of a failure to establish a replication link or because there is a link but the target account name is incorrect.

Failure to Create a Replication Link

The local domain controller tries to establish a replication link with its replication partner and it fails. In this event, **repadmin /showreps** shows no inbound neighbors, so it will not display a cause for the error. To see the cause, go to the Directory Service event log in Event Viewer and examine the logged event.

Event ID 1645

The Directory Service received a failure while trying to perform an authenticated RPC call to another Domain Controller. The failure is that the desired Service Principal Name (SPN) is not registered on the target server. The server being contacted is 62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com. The SPN being used is E3514235-4B06-11D1-AB04-00C04FC2DCD2/62d85225-76bf-4b46-

b929-25a1bb295f51/branches.corp.hay-buv.com@branches.corp.hay-buv.com.

Please verify that the names of the target server and domain are correct. Please also verify that the SPN is registered on the computer account object for the target server on the KDC servicing the request. If the target server has been recently promoted, it will be necessary for knowledge of this computer's identity to replicate to the KDC before this computer can be authenticated.

Replication Link Exists, but Target Name Is Incorrect

This occurs when a replication link exists between the two domain controllers, but replication does not happen correctly. In this event, as described in the first section, **repadmin /showreps** shows inbound neighbors, but the status of the last replication for one or more of the naming contexts returns "Last attempt at <date - time> failed" with the "Target account name is incorrect" error. In this case, no event is logged in the event log. This error occurs when the required set of Service Principal Names (SPN) is not found on both the local and target server when exchanging Kerberos tickets.

To recover from this error:

1. Determine the IP address of the destination domain controller by pinging the name shown in the event in Event Viewer:
ping 62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com
Pinging HubDC1.branches.corp.hay-buv.com [10.10.20.99] with 32 bytes of data:
Reply from 10.10.20.99: bytes=32 time=94ms TTL=124
...
2. Either remotely or through Terminal Services (if installed), start Adsiedit.msc directly against the domain naming context of the two replication partners.
3. On both domain controllers, locate the local domain controller computer account and obtain the properties.
4. In the list of properties, locate "servicePrincipalName." There will be a list of multi-valued entries. One of the entries has two GUIDs, for example, "E3514235-4B06-11D1-AB04-00C04FC2DCD2/62d85225-76bf-4b46-b929-25a1bb295f51/dom1.company.com"
5. Select this entry, and press the Remove button.
6. In the edit control, select all the text, copy it to the Clipboard, and press the Add button.
7. The Edit control should now be empty. Paste the Clipboard, go to and append "@dom1.company.com" so it matches the following string: "E3514235-4B06-11D1-AB04-00C04FC2DCD2/62d85225-76bf-4b46-b929-25a1bb295f51/dom1.company.com@dom1.company.com"
8. Copy the whole string to the clipboard, and then press the add button, and then click OK.
9. On the other domain controller, paste the string to the Edit control, press the Add button, and OK.
Retry the replication action.

In some cases, you may encounter the following problems :

- The replication partner has a different pair of GUIDs (the second one is different). This can happen when the domain controller has been un-promoted and then re-promoted. The solution in that case is to add both SPNs on both domain controllers.
- One of the lists is virtually empty. This can occur when two different domain controllers update the SPN value inside the same replication cycle. When replication occurs, one set of SPN values will be lost, in turn causing the replication error. In this scenario, the solution is to copy all entries that are missing from the domain controller that has the entries to the second domain controller, as above, but without modifying any entries.

RPC Server Not Available

This error can occur either because creation of the replication link failed or because of connectivity issues.

Failure to Create a Replication Link

In this scenario, **repadmin /showreps** shows no inbound neighbors, so the **repadmin** output does not indicate the type of error. To see the cause of the failure, go to the Directory Service event log in Event Viewer. The following event will be logged:

Event ID 1265

The attempt to establish a replication link with parameters

Partition: DC=branches,DC=corp,DC=hay-buv,DC=com

Source DSA DN: CN=NTDS

Settings,CN=HubDC1,CN=Servers,CN=DMZ-

Administration,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com

Source DSA Address: **62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com**

Inter-site Transport (if any): CN=IP,CN=Inter-Site

Transports,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com

failed with the following status:

The RPC server is unavailable.

The record data is the status code. This operation will be retried.

Replication Link Exists-Connectivity Issues

There may be connectivity issues when a replication link exists between the two domain controllers, but replication does not occur (as described in the first section). The output from **repadmin /showreps** shows inbound neighbors. The status of the last replication for one or more naming contexts returns "Last attempt at <date - time> failed" with the "Target account name is incorrect" error. When the output gives these details, no event is logged in the event log.

To test for connectivity problems, ping the GUID-based DNS name displayed in the content of the message. This name is composed of the GUID of the NTDS Settings object of the replication partner, followed by `_msdcs.corp.hay-buv.com`. It is shown

on the DNS server of the forest root as an alias name pointing to the domain controller name. For example, at a command prompt you would type:

```
ping 62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com
Pinging HubDC1.branches.corp.hay-buv.com [10.10.20.99] with 32 bytes
of data:
Reply from 10.10.20.99: bytes=32 time=94ms TTL=124
```

...

From the output of the **ping** command, ensure that the <GUID>_msdcs record can be properly resolved by the DNS server at the root of the forest. This is true provided that the output shows "Pinging " followed by the fully qualified domain name of the domain controller.

If a "Request timed out" error is returned, continue to look for connectivity issues. After the ping command works, replication should work properly.

DNS Lookup Failure

A DNS lookup failure can occur when there is no replication link with the partner or when, despite the existence of the replication link, DNS lookup fails.

Failure to Create a Replication Link-DNS Lookup Failure

This occurs when the local domain controller tries to establish a replication link with its replication partner and it fails. In this scenario, **repadmin /showreps** shows no inbound neighbors, so it does not return this error. To see it, go to the Directory Services event log in Event Viewer. The following event will be logged:

Event ID 1265

The attempt to establish a replication link with parameters

Partition: DC=branches,DC=corp,DC=hay-buv,DC=com

Source DSA DN: CN=NTDS

Settings,CN=HubDC1,CN=Servers,CN=DMZ-

Administration,CN=Sites,CN=Configuration,DC=corp,DC=hay-
buv,DC=com

Source DSA Address: **62d85225-76bf-4b46-b929-
25a1bb295f51._msdcs.corp.hay-buv.com**

Inter-site Transport (if any): CN=IP,CN=Inter-Site

Transports,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com

failed with the following status:

DNS Lookup Failure.

The record data is the status code. This operation will be retried.

Replication Link Exists-DNS Lookup Failure

As described in the first section, **repadmin /showreps** shows inbound neighbors, but the status of the last replication for one or several naming contexts returns "Last attempt at <date - time> failed" with the "DNS lookup failure" error. No event is logged in the event log.

This error means the local domain controller could not resolve the GUID-based

DNS name of its replication partner (this name is composed of the GUID of the NTDS Settings object of the replication partner, followed by `_msdcs.corp.hay-buv.com`). It is declared on the root DNS server of the forest as an alias name that points to the replication partner's name.

To reproduce the error, try to ping the GUID-based DNS name of its replication partner. This should normally fail. If it succeeds, replication should function correctly at the next interval without error. If replication fails at the next interval, the local DNS server can be queried by typing the following command (with no switches) at a command prompt:

```
nslookup
```

The currently used DNS server is displayed. Ensure that it is the first one declared in the IP configuration of the local domain controller. If not, the local domain controller may have sent its initial name resolution request to the preferred (first) DNS server when it triggered replication, which resulted in failed name resolution. Since then, the name resolution may have been performed by the alternate (second) DNS server, which is able to resolve it. In this scenario you must find the reason why the preferred DNS server could not resolve the request.

If the **ping** command fails, perform the following actions:

- Check that the DNS server is authoritative for the root of the forest that contains given namespace. If the name is missing, look in the replication partner's event log for failures on registering its DNS names.
- If the DNS server is not authoritative for this namespace, verify its forwarders list (go to the DNS MMC, select the properties of the DNS server, and go to the **Forwarders** tab). Verify that the DNS servers declared as forwarders are authoritative for this namespace.
- After this problem is resolved, rerun the **ping** command on the local domain controller. It should now work. Replication should occur properly the next time it is triggered or scheduled.
- If the **ping** command still fails on the local domain controller, check to see whether the name has been cached as a negative entry by typing the following command at a command prompt:

```
Ipconfig /displaydns
```

If the name has been cached as a negative entry, this means that the local domain controller has received a "Name not found" response to the name resolution request that it sent to its DNS server the last time replication was triggered.

The DNS server replies with a "Name not found" error only in two cases.

1. It is authoritative for the zone (it has a copy of the zone that should contain the name), but the name is missing.
2. It is not authoritative for the zone, it could not resolve the name recursively by using root hints, and it could not resolve the name recursively by using the defined forwarders.

In the other cases (for example, if it is not authoritative for the zone and has no root hints or forwarder declared), it will answer "Server Failure" to the query, not "Name

not found." The client does not cache the response.

If the name has been cached as a negative entry, flush the DNS cache on the local domain controller by typing the following command at a command prompt:

```
ipconfig /flushdns
```

After you have done this, try to ping the GUID-based DNS name again. If the name can now be resolved, replication should occur properly the next time it is triggered or scheduled.

To avoid this problem in the future:

- Attempt to discover the reason why the DNS server did not resolve the name when replication was last triggered.
- Check the value of the "NegativeCacheTime" entry located in **HKEY_LOCALMACHINE/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters**. It is set to 0x12C (=300 seconds =5 minutes) by default. A high value could prevent the domain controller from going to the DNS server to look up the name the next time replication is triggered and, consequently, prevent it from happening correctly, even if the name could be resolved.

If the **ping** command still does not work, stop and restart the DNS Client service by typing the following command at a command prompt:

```
Net stop dns client
```

```
Net start dns client
```

```
ping the GUID based DNS name again.
```

If this works, this means that when replication was triggered, the domain controller could not reach its "preferred" DNS server (the DNS server declared first in its IP configuration). As a result, it proceeded to fail back to another DNS server (the second or following ones declared in the list) and this DNS server could not resolve the name either. In addition, after the DNS client fails back to an alternate DNS server, it will never return to the initial one, so replication will fail with the same status each time it is triggered.

Note: Stopping and restarting the DNS Client service on the domain controller makes it revert to its preferred DNS server. If this server is now responding and is able to resolve the name, replication should work properly the next time it is triggered or scheduled.

Directory Service Too busy – Duplicate Connection Object

When this error occurs, the following event is generally logged in the Directory Service event log:

```
Event ID : 1083
Event Type:      Warning
Event Source:    NTDS Replication
Event Category:  Replication
Event ID: 1083
Date:           10/12/2000
Time:           9:56:19 AM
```

User: Everyone

Computer: BODC1

Description:

Replication warning: The directory is busy. It couldn't update object **CN=DC2,CN=Servers,CN=Bad-Site,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com** with changes made by directory **62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com**. Will try again later.

This error generally occurs when a duplicate connection object exists in Active Directory of the destination replication partner. Because this connection object is used to facilitate replication with the local domain controller, updates are impossible when replication does occur.

The description of event ID 1083 contains:

- The distinguished name of the object causing the problem.
- The GUID-based DNS name of the replication partner. This name is composed of the GUID of the NTDS Settings object of the replication partner, followed by `_msdcs.corp.hay-buv.com`.

To resolve the problem, perform the following actions:

- Ping the GUID-based DNS name to get the IP address of the replication partner.
- Run `Ldp.exe` from Windows 2000 Support Tools, and then connect to this IP address by using the connect option from the **Connection** menu. Select the **Bind** option from the **Connection** menu, and then enter the credentials of an administrator account. Select the **Search** option from the **Browse** menu. In the **Search** dialog box, select the **Subtree** option. In the **Base Dn** option, enter the following information:

The distinguished name of the domain to search for a user or a computer: **dc=branches,dc=company,dc=com** or the distinguished name of the configuration container to search for connection objects.

- Click **Run**. The right pane of the window displays the different locations in which the object was found. Select the appropriate result from the list. Delete the other returned options by using the **Delete** option of the **Browse** menu. Enter the distinguished name of the object to delete:
CN=DC2,CN=Servers,CN=Bad-Site,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com
- Ensure that the object has been properly deleted in the right pane of the `Ldp.exe` window.

If no duplicate exists, move the object to a different site or organizational unit.

Document this for future reference in case the object needs to be moved again at a later date. Synchronize the configuration and domain naming contexts by typing the following commands at the command prompt:

```
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com  
%computername% <rep_partner_GUID>
```

```
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com
%computername% <rep_partner_GUID>
```

If replication completes successfully, the event log should not show any new instances of event ID 1083.

If necessary, move the object back to its original location, and then resynchronize the configuration and domain naming contexts by using the commands above.

Time Difference / LDAP Error 82

This error generally occurs when the local domain controller fails to synchronize its time. This is typically caused by access being denied.

If there is no replication link, as discussed before, **repadmin /showreps** shows no inbound neighbors, so it does not display the cause of the error. To see the cause, go to the Directory Service event log in the Event Viewer. The following event will be logged:

Event ID 1265

The attempt to establish a replication link with parameters

Partition: DC=branches,DC=corp,DC=hay-buv,DC=com

Source DSA DN: CN=NTDS

Settings,CN=HubDC1,CN=Servers,CN=HubSite,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com

Source DSA Address: **62d85225-76bf-4b46-b929-25a1bb295f51.msdc corp.hay-buv.com**

Inter-site Transport (if any): CN=IP,CN=Inter-Site

Transports,CN=Sites,CN=Configuration,DC=corp,DC=hay-buv,DC=com

failed with the following status:

There is a time difference between the client and server.

The record data is the status code. This operation will be retried.

When there is a replication link as described in the first section, **repadmin /showreps** shows inbound neighbors, but the status of the last replication for one or more naming contexts returns "Last attempt at <date - time> failed" with the "There is a time difference between the client and the server" error. No event is logged in the event log.

In this case you must synchronize the local time on the domain controller by typing the following command at a command prompt:

```
Net time \\server /set
```

This should fail with an "Access denied" error. Continue by performing the recovery steps described in the "Access denied" section earlier in this chapter.

The replication system encountered an internal error

This error can occur for the following reasons:

- The local domain controller tries to establish a replication link with its replication

partner but fails. In this scenario, **repadmin /showreps** shows no inbound neighbors, so it does not display this error.

- A replication link exists between the two domain controllers, but replication cannot be properly performed. In this scenario, **repadmin /showreps** shows inbound neighbors, but the status of the last replication for one or several naming contexts returns "Last attempt at <date - time> failed" with the " The replication system encountered an internal error" status.

In both cases, the following event is logged in the Directory Services event log:

Event ID 1084

Replication error: The directory replication agent (DRA) couldn't update object CN="8f03823f-410c-4483-86cc-8820b4f2103f

DEL:66aab46a-2693-4825-928f-05f6cd12c4e6",CN=Deleted Objects,CN=Configuration,DC=corp,DC=hay-buv,DC=com (GUID 66aab46a-2693-4825-928f-05f6cd12c4e6) on this system with changes which have been received from source server 62d85225-76bf-4b46-b929-25a1bb295f51._msdcs.corp.hay-buv.com. An error occurred during the application of the changes to the directory database on this system.

To recover from this error, perform the following actions:

1. Locate the last event ID 1084 in the event log. Select the GUID of the failed object (in the example: 66aab46a-2693-4825-928f-05f6cd12c4e6), and select **Copy**.
2. Run **Ldp.exe** and connect to the local domain controller (for example, 10.10.20.1)
3. Bind with administrator privileges to the local directory.
4. Select **Browse**, and then select **Delete**
5. Enter <GUID=66aab46a-2693-4825-928f-05f6cd12c4e6> as the domain controller, and then delete this entry.
6. If the error occurred when the domain controller tried to create the replication link, run **repadmin /kcc** at the command prompt.

If the error occurred when replicating over existing replication links, try to synchronize the three naming contexts by typing the following commands at a command prompt:

```
repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

```
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

```
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

If the error occurs again on a new object, start over with step 1.

No More End-Point

This error, returned by the **repadmin /showreps** command, may be caused by the following:

- No more end-points are available to establish a Transmission Control Protocol (TCP) session with the replication partner. To verify the currently established sessions, use the **NETSTAT** utility at the command prompt. The only way to

eliminate this error is to release current TCP sessions.

- The replication partner is available, but its Directory Replication Service remote procedure call (RPC) interface is not registered. This is usually an indication that the domain controller's DNS name is registered with the wrong IP address.

LDAP Error 49

This error is generally related to the local KDC service. In this scenario, stop the KDC service by typing the following command at a command prompt:

```
Net Stop KDC
```

Synchronize the schema naming context on the local domain controller by typing the following command at a command prompt:

```
repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

The schema naming context is used first because it is the smallest. This will lead to confirmation of success in the quickest time possible.

Replication of the configuration and domain naming contexts can also be triggered by typing the following command at a command prompt:

```
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com  
%computername% <rep_partner_GUID>  
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com  
%computername% <rep_partner_GUID>
```

If the **repadmin /sync** command fails with a new error, see the relevant section of this chapter. If it is successful, **repadmin /showreps** should not show any more errors. Restart the KDC service on the local domain controller. This can be done by typing the following command at the command prompt:

```
net start kdc
```

If **repadmin /showreps** returns a new error, see the relevant section of this chapter.

Unable to Run Administration Tools

If Active Directory is unavailable, the Active Directory management tools will fail when launched.

For example:

- When **repadmin /showreps** is run from the command prompt, it does not complete or returns the "Cannot open LDAP connection to localhost" error.
- When Active Directory Sites and Services is started, it returns the following error:
Naming information cannot be located because:
The Network path was not found.
Contact your system administrator to verify that your domain is properly
Configured and is currently on line.

This problem can be related to incorrect TCP/IP configuration on the local domain

controller, a network connection issue, a problem on the DNS server or because the NETLOGON service is not running locally.

In any of the above scenarios:

- Ensure that that the DNS server is unavailable.
- Try to ping the destination replication partner from the local domain controller.
- Use the **Nslookup** command to ensure that the DNS server is correctly configured on the local domain controller.
- If the problem is DNS related, flush the DNS cache on the local domain controller by using the **ipconfig /flushdns** command, or stop and restart the DNS Client service. For more information about name resolution failures, see the "DNS Lookup Failure" section earlier in the chapter.
- Ensure that the NetLogon service is running properly in Administrative Tools, Services. Also check the System and Directory Service event logs in Event Viewer for events indicating errors for NetLogon.

Non-Error Status

When using the **repadmin /showreps** command, several of the outputs can indicate that the last replication did not complete successfully. These may not necessarily reveal an error. Such examples are as follows:

- **Active Directory replication has been pre-empted.** This status means that an inbound, in-progress replication occurrence was interrupted by a higher-priority replication request (all inbound replication is serialized).
- **Replication posted, waiting.** This means that the domain controller has posted a replication request and is waiting for an answer. This indicates replication is in progress from this source.
- **Last attempt @ was not successful.** This status can mean one of two things:
 1. The KCC successfully created the replication link between the local domain controller and its destination replication partner, but because of the replication schedule, replication has not occurred since then. In this scenario, make sure that the replication schedule is properly configured and meets your requirements. To ensure that replication will be successful at the next scheduled interval, trigger it manually by typing the following command at a command prompt:

```
repadmin /sync CN=Schema,CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
repadmin /sync CN=Configuration,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
repadmin /sync DC=branches,DC=corp,DC=hay-buv,DC=com %computername% <rep_partner_GUID>
```

If it succeeds, the "@never" status will be replaced by the current date.

2. There is a large backlog of inbound replication to be performed on this domain controller (all inbound replication is serialized). Use the Performance

Monitor (Perfmon.exe) counter DRA Pending Replication Synchronizations to check the number of inbound synchronizations in the queue. (A synchronization in the queue indicates replication of a given naming context from a specific source domain controller will be attempted after previously queued replication events take place.)

FALLBACK PLANS

If you encounter problems while building your domain controllers, the fallback plan is the same whether the problem occurred while building a hub domain controller or while building a branch office domain controller. However, the fallback plan will differ depending on when during the process of building a domain controller you encountered a problem.

Fallback Plan prior to running the Active Directory Installation Wizard

The fallback plan prior to running the Active Directory Installation Wizard (Dcpromo.exe) is the most simple. If you encounter problems before running The Active Directory Installation Wizard, you should:

- Verify that your hardware and your network are functioning correctly.
- Reinstall Windows 2000 and restart the process.

Fallback Plan After running the Active Directory Installation Wizard

If you encounter problems during or after the Active Directory Installation Wizard process, follow the procedures in the Failure During the Active Directory Installation Wizard section later in this chapter. After you have cleaned up all references to the problem domain controller, you should follow the fallback plan for Prior to running the Active Directory Installation Wizard.

Failure During the Active Directory Installation Wizard

In the case of a failed Active Directory Installation Wizard, there may be items in Active Directory that must be manually removed as part of the recovery. There are two options for recovering a failed Active Directory Installation Wizard process.

- **Option One:** Remove the NTDS Settings object.
This will leave the server object in Active Directory and delete all NTDS Settings objects for the server. The Active Directory Installation Wizard process can be started again after the steps in this section are completed.
- **Option Two:** Remove the server object from Active Directory.
This option removes the server object and requires a complete reinstall of Windows 2000.

It is recommended that Option Two be used for the branch office scenario in the case of a failed Active Directory Installation Wizard process. This is primarily because the option is less risky and the staging process for new domain controllers is automated.

Option One: Remove the NTDS Settings Object

Use these procedures only if you want to keep the server object in Active Directory. Otherwise, follow the steps in the next section to remove the server object from Active Directory, and then reinstall Windows 2000 on the server and attempt to run the Active Directory Installation Wizard again.

As part of the promotion process, the Active Directory Installation Wizard adds configuration data for the domain controller to Active Directory. This data takes the form of an NTDS Settings object, which exists as a child of the server object in the Active Directory Sites and Services MMC.

The attributes of the NTDS Settings object include data representing how the domain controller is identified regarding its replication partners, the naming contexts that are maintained on the computer, whether a domain controller is a Global Catalog server, and the default query policy. The NTDS Settings object is also a container that may have child objects that represent the domain controller's direct replication partners. This data is required for the domain controller to operate in the environment, but is removed during demotion.

In the event the Active Directory Installation Wizard process fails, it is possible that the NTDS Settings object can be only partially configured. In this case, the administrator must use the **Ntdsutil** utility to manually remove the NTDS Settings object. The following steps list the procedure for removing the NTDS Settings object in Active Directory for a given domain controller. For more information about the available options at each **Ntdsutil** menu, the administrator can type **help** or **?**.

Caution: The administrator should also ensure that replication has occurred since the demotion before manually removing the NTDS Settings object for any server. Using the **Ntdsutil** utility improperly can result in partial or complete loss of Active Directory functionality.

1. Open a command prompt and type **ntdsutil**
2. Type **metadata cleanup** and then press ENTER. Based on the options given, the administrator can perform the removal, but additional configuration parameters must be specified before the removal can occur.
3. Type **connections** and press ENTER. This menu is used to connect to the specific server on which the changes occur. If the currently logged on user does not have administrative permissions, alternate credentials can be supplied by specifying the credentials to use before making the connection. To do so, type **set creds <domain name> <username> <password>** and press ENTER. For a null password, type **null** for the password parameter.
4. Type **connect to server <servername>** and then press ENTER. You should receive confirmation that the connection is successfully established. If an error occurs, verify that the domain controller being used in the connection is available and the credentials you supplied have administrative permissions on the server.
5. Type **quit** and press ENTER. The **Metadata Cleanup** menu is displayed.
6. Type **select operation target** and press ENTER.
7. Type **list domains** and press ENTER. A list of domains in the forest is displayed, each with an associated number.
8. Type **select domain <number>** (where *<number>* is the number associated with the domain which includes the server you are removing) and press ENTER. The domain you select is used to determine if the server being removed is the last domain controller of that domain.
9. Type **list sites** and press ENTER. A list of sites, each with an associated

number, is displayed.

10. Type **select site <number>** (where <number> is the number associated with the site for the server you are removing) and press ENTER. You should receive a confirmation that lists the site and domain you chose.
11. Type **list servers in site** and press ENTER. A list of servers in the site, each with an associated number, is displayed.
12. Type **select server <number>** (where <number> is the number associated with the server you want to remove) and press ENTER. You receive a confirmation that lists the selected server, its Domain Name Server (DNS) host name, and the location of the server's computer account you want to remove.
13. Type **quit** and press ENTER. The **Metadata Cleanup** menu is displayed.
14. Type **remove selected server** and press ENTER. You should receive confirmation that the removal completed successfully. If you receive the following error message:
Error 8419 (0x20E3) The DSA object could not be found
the NTDS Settings object may already be removed from Active Directory as the result of another administrator removing the NTDS Settings object or replication of the successful removal of the object after running the **dcpromo** utility.
15. Type **quit** at each menu to quit the **Ntdsutil** utility. You should receive confirmation that the connection disconnected successfully.

For more information about the **Ntdsutil** utility, see the Support Tools documentation located in the Support\Reskit folder on the Windows 2000 CD-ROM or see Chapter 3 in the TCP/IP Core Networking Guide of the Microsoft Windows 2000 Resource Kit.

Option Two: Remove the Server Object from Active Directory

If the Active Directory Installation Wizard fails, there will be a server object in Active Directory that should be deleted prior to reinstalling Windows 2000 and running the Active Directory Installation Wizard again. This issue can also occur if the Active Directory Installation Wizard is used to demote the server to a member server. This occurs because the server object is a "container" in Active Directory and may hold child objects that represent configuration data for other services installed on your computer. Because of this, the Active Directory Installation Wizard utility does not automatically remove the server object.

Warning: If the server object contains any child objects named "NTDS Settings," these are objects that represent the server as a domain controller and should be automatically removed by the demotion process. If this does not work, or a demotion could not be performed (for example, on a computer with malfunctioning hardware), these objects must be removed by using the **Ntdsutil** utility before you delete the server object.

After an administrator verifies that all other services with a dependency on the server object have been removed, or if the domain controller is being rebuilt and the decommissioning of the server could not be performed gracefully, an administrator can delete the server:

1. Click **Start, Programs, Administrative Tools**, and then click **Active Directory**

Sites and Services.

2. Expand the **Sites** branch, and then expand the appropriate site's branch (the site the server resides in).
3. Expand the server's container, right-click the server object, and then click **Delete**.
4. Click **Yes** when you are prompted to confirm deleting the object.

This process may not finish successfully for either of the following reasons:

- If you receive a message that states the server is a container that contains other objects, verify that the appropriate decommissioning of services has completed before continuing.
- If you receive a message that states the DSA object cannot be deleted, you may be attempting to delete an active domain controller.

TROUBLESHOOTING FRS

FRS is a complex distributed environment, and difficulties related to configuration, service health, and determining replica member consistency are bound to arise. When FRS stops replicating content, you first must review the FRS log in Event Viewer on the problem domain controller. Event Viewer will help you determine whether the service has started and indicate whether any errors have occurred during startup. Check the details on a particular error to find additional information.

The following list of guidelines is useful when troubleshooting FRS:

- Check to make sure that the Staging Directory is not full. It is important to realize that if the FRS Staging Directory is full, replication will stop. Check for free disk space on each domain controller. On the member of the replica set that is replicating data, check the source directory, Staging Directory, and database partition. On the member of the replica set that is receiving the replicated data, check the destination partition, the pre-install partition, and the database partition. Some common errors found in Event Viewer associated with the Staging Directory are:

MessageId=13522 Severity=Warning
SymbolicName=EVENT_FRS_STAGING_AREA_FULL

The File Replication Service paused because the staging area is full. Replication will resume if staging space becomes available or if the staging space limit is increased.

The current staging space limit is 660 KB. To change the staging space limit, start a registry editor and change the value of the Staging Space Limit in KB entry located in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters subkey.

An outbound partner that has not connected for a while can cause this. Delete the connection and stop and restart FRS to force deletion of the staging files. You can also follow the procedure described in "Tuning Recommendations" earlier in this chapter to increase the size of the Staging Directory.

MessageId=13511 Severity=Error
SymbolicName=EVENT_FRS_DATABASE_SPACE

The File Replication Service is stopping on computer A because there is no free space on the volume. The available space on the volume can be found by typing "dir *volume name*".

When free space is made available on the volume, the File Replication Service can be restarted immediately by typing "net start ntfrs" at a command prompt. Otherwise, the File Replication Service will restart automatically at a later time.

For more information about managing space on a volume, type "copy /?", "rename /?", "del /?", "rmdir /?", and "dir /?" at a command prompt.

Check for files that are larger than the amount of free space on the source or destination server or larger than the size of the Staging Directory limit in the registry. Resolve the disk space problem or increase the maximum staging file

space.

- Verify that the members of your replica set are available on the network. Because FRS uses the fully qualified domain name of the replica members, a good first check is to use a **ping** command specifying the fully qualified name of the problem replicas.
- There might be a problem with the RPC service on either domain controller or with creating a secure connection between members of a replica set. If this is the case, you will see event ID 13508 in the Event Log:

MessageId=13508 Severity=Warning
SymbolicName=EVENT_FRS_LONG_JOIN

The File Replication Service is having trouble enabling replication from computer A to computer B using the DNS name <FQDN>. FRS will keep retrying.

This warning can occur for one of the following reasons:

FRS cannot correctly resolve the DNS name from this computer.

FRS is not running on computer B.

The topology information in the Active Directory for this replica has not yet replicated to all of the domain controllers.

This event log message will appear once per connection. After the problem is fixed, you will see another event log message indicating that the connection has been established.

- If FRS is in an error state and must be restored, you will see event ID 13555 in the Event Log:

MessageId=13555 Severity=Error
SymbolicName=EVENT_FRS_IN_ERROR_STATE

The File Replication Service is in an error state. Files will not replicate to or from one or all of the replica sets on this computer until the following recovery steps are performed:

Recovery Steps:

[1] The error state may clear itself if you stop and restart the FRS service.

This can be done by performing the following in a command window:

```
net stop ntfrs  
net start ntfrs
```

If this fails to clear up the problem then proceed as follows.

[2] For Active Directory Domain Controllers that DO NOT host any DFS

alternates or other replica sets with replication enabled:

If there is at least one other Domain Controller in this domain then restore the "system state" of this DC from backup (using ntbackup or other backup-restore utility) and make it non-authoritative.

If there are NO other Domain Controllers in this domain then restore the "system state" of this DC from backup (using ntbackup or other backup-restore utility) and choose the Advanced option which marks the sysvols as primary.

If there are other Domain Controllers in this domain but ALL of them have this event log message then restore one of them as primary (data files from primary will replicate everywhere) and the others as non-authoritative.

[3] For Active Directory Domain Controllers that host DFS alternates or other replica sets with replication enabled:

(3-a) If the Dfs alternates on this DC do not have any other replication partners then copy the data under that Dfs share to a safe location.

(3-b) If this server is the only Active Directory Domain Controller for this

domain then, before going to (3-c), make sure this server does not have any

inbound or outbound connections to other servers that were formerly Domain

Controllers for this domain but are now off the net (and will never be coming back online) or have been fresh installed without being demoted.

To delete connections use the Sites and Services snapin and look for Sites->NAME_OF_SITE->Servers->NAME_OF_SERVER->NTDS Settings->CONNECTIONS.

(3-c) Restore the "system state" of this DC from backup (using ntbackup or other backup-restore utility) and make it non-authoritative.

(3-d) Copy the data from step (3-a) above to the original location after the sysvol share is published.

[4] For other Windows 2000 servers:

(4-a) If any of the DFS alternates or other replica sets hosted by

this server do not have any other replication partners then copy the data under its share or replica tree root to a safe location.

(4-b) net stop ntfrs

(4-c) rd /s /q %1

(4-d) net start ntfrs

(4-e) Copy the data from step (4-a) above to the original location after the service has initialized (5 minutes is a safe waiting time).

Note: If this error message is in the eventlog of all the members of a particular replica set then perform steps (4-a) and (4-e) above on only one of the members.

- Verify the replication schedule on the connection object by using Active Directory Sites and Services.
- Check to see whether the file on the originating server is locked on either computer. If the file is locked, FRS cannot update the file and continues to retry the update until it succeeds. The retry interval is 30 to 60 seconds.
- Check to see whether the source file was excluded from replication. Confirm that the file is not encrypted using the Encrypted File System (EFS) or excluded by a file or folder filter on the originating replica member and is not an NTFS file system junction. If any of these are the case, FRS will not replicate the file or directory.

If all of the previous conditions check out, try to replicate the file again.

NON-AUTHORITATIVE FRS RESTORE

This section describes the series of steps necessary to properly restart FRS. If for some reason FRS was stopped during or after your deployment, you should follow these procedures to restart FRS. In addition, if FRS is in an error state, such as a journal wrap error state, you should follow these procedures to start FRS again.

Restoring Hub Domain Controllers

To restore your hub domain controllers:

Note: These steps are only required if FRS is in an error state on all hub domain controllers. If there is at least one hub domain controller with a healthy copy of SYSVOL, only steps 16 through 21 are required.

1. Stop the FRS service on all domain controllers in the domain, both in the hub site and in the branch office sites. Sc.exe from the Microsoft Windows 2000 Resource Kit can be used to stop the FRS service remotely by typing the following command at a command prompt:

```
sc \\<computername> stop ntfrs
```

2. Verify that Service Pack 2 or later has been installed on all hub domain controllers.
3. On the hub domain controllers, identify the most current copy of any SYSVOL content. You can use Windiff.exe from the Windows 2000 Resource Kit to identify the most current copy.
4. Select one hub domain controller for use as the source location in which you will construct the most up-to-date version of the SYSVOL files. Delete any old folders from this source domain controller. At the end of this step you should have the needed content under the Scripts and Policies folders in the SYSVOL folder on this computer.
5. Make a copy of the SYSVOL folder to another folder as a backup.
6. Increase the Lightweight Directory Access Protocol (LDAP) maximum page size parameter on each hub domain controller to greater than the maximum number of domain controllers you expect to have in the domain in the next six months.
7. Verify that all the hub domain controllers have FRS subscription and subscriber objects under their computer objects.
8. Verify that each FRS subscriber object has a valid reference to its corresponding NTFRSMember object for SYSVOL.
9. Verify that the FRS member object has a valid server reference to the NTDS settings object for this domain controller.
10. Verify that the connection topology and schedules are properly configured.
11. Run the **Regini** command only on the source hub domain controller:

```
regini primaryrestore.reg
```

Note: This is the only time you will use the Primaryrestore.reg file.

12. Restart FRS on only the source hub domain controller, for example:

```
net start ntfrs
```

FRS will restart and enumerate the SYSVOL folder tree, place object IDs on each file and folder in the SYSVOL, and initialize its database.

-
13. Wait 15 minutes before continuing.
 14. Verify that FRS is running and has not encountered any errors by running:
ntfrsutl sets on the source hub domain controller. This should show that the service state for this SYSVOL replica set member is in the ACTIVE state.
 15. Verify that SYSVOL is shared and check the FRS event log for any problems.
 16. Select one of the other hub domain controllers that has an inbound connection to source hub domain controller, and then run the following **Regini** command:
regini nonauthrestore.reg
 17. Restart FRS on this hub domain controller, for example:
net start ntfrs

Because FRS was already stopped on all domain controllers in the domain in step 1, this step tells FRS to rename the current SYSVOL content to a "pre-existing" folder, create an empty FRS database, and then synchronize with its inbound partner (source hub domain controller) to obtain all of the SYSVOL files and folders. This should take less than 30 minutes.

18. Wait 30 minutes.
19. Verify that FRS is running and has not encountered any errors by running:
ntfrsutl sets on the hub domain controller. This should show that the service state for this SYSVOL replica set member is in the ACTIVE state.
20. Verify that SYSVOL is shared and check the FRS event log for any problems.
21. Use **Windiff.exe** from the Microsoft Windows 2000 Resource Kit to verify that the SYSVOL content is exactly the same between the two domain controllers. For example:
Windiff \\<computer1>\sysvol\<domainname>\Policies
\\<computer2>\sysvol\<domainname>\Policies
22. Select another hub domain controller, and then repeat steps 16 through 21 for each domain controller.

Note: You should perform this process on one domain controller at a time.

23. After FRS is restarted on all hub domain controllers, you can create a test file and verify that the test file replicates to all hub domain controllers. You can also do this after bringing FRS back online on each hub domain controller if you wish.

Restoring Branch Office Domain Controllers

Restoring a branch office domain controller is similar to restoring the additional hub domain controllers. Repeat steps 16 through 21 for each branch office domain controller after all of the hub domain controllers have been restored.

SUMMARY

This chapter has provided you with examples of problems that might be encountered when deploying Active Directory in a large branch office environment. Each example has included the steps required to analyze the problem and the procedures to resolve it.

More Information

For further up-to-date troubleshooting information, read the Readme.txt file in the latest Service Pack and search the Microsoft Knowledge Base and TechNet by using the error message number and wording you have encountered.