



*Operating System*

## Chapter 6

# Planning for Building and Deploying Branch Office Domain Controllers

### Planning Guide

---

#### **Abstract**

This chapter presents the best practices, planning, and monitoring involved in the building of the domain controllers for the remote branches. Most importantly, this is where we provide warnings about steps that should not be performed and what the consequences would be. Quality assurance steps are provided to ensure a smooth deployment, including the necessity of having good documentation for future administration and maintenance.

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

*1200*

---

## CONTENTS

INTRODUCTION .....	1
Resource Requirements	1
What You Will Need	1
What You Should Know	1
PROCESS FLOWCHART .....	2
DESIGN CONSIDERATIONS .....	3
Severe Problems	3
Domain Controller Disconnected for Longer Than Tombstone Lifetime	3
ISTG turned Off, no inter-Site Connection Objects Created	3
Moderate	3
Domain Controller Disconnected for More Than Two Times Domain Controller Password Change Policy	4
Old Connection Objects Created for Staging Site Are Not Cleaned Up	4
Basic Steps for Domain Controller Pre-Staging	4
INSTALLING SOFTWARE .....	5
Installation Planning	5
Verification (QA1)	5
PROMOTING THE SERVER TO DOMAIN CONTROLLER.....	6
Verification of Promotion (QA2)	6
Domain Controller Continues Running	7
PREPARING THE COMPUTER FOR TRANSPORT.....	8
Verify Preparation (QA3)	8
Ship the Computer to the Destination	8
ALTERNATIVE CONFIGURATION .....	10
DOCUMENTATION .....	11
POST-DEPLOYMENT .....	12
GENERAL ACTIVE DIRECTORY DEPLOYMENT GUIDELINES..	13
Ensure that Your Hub is a Robust Data Center	13
Do Not Deploy All Branch Office Domain Controllers Simultaneously	13
Balance Replication Load Between Bridgehead Servers	13
Keep Track of Hardware and Software Inventory and Versions	14
Allow Enough Time for the Branch Office Deployment	14
Include Operations in Your Planning Process	14
Monitoring Plans and Procedures	14
Disaster Recovery and Troubleshooting Strategy	15
Personnel Assignment and Training	15

---

SUMMARY .....17

## INTRODUCTION

In this chapter, you will plan the process for staging your domain controllers.

### Resource Requirements

Before you begin this portion of your branch office deployment, you will need the following personnel, programs, and other resources.

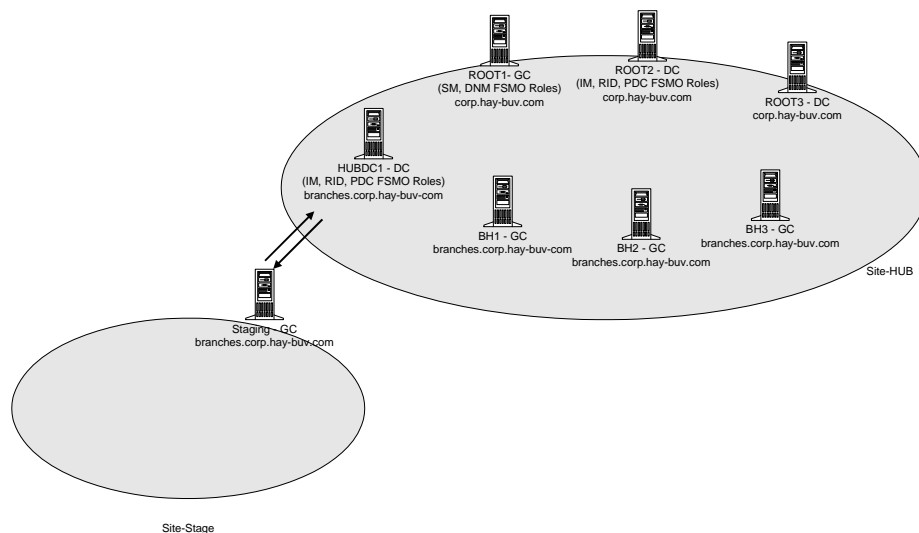
#### What You Will Need

You will need to have completed the planning as laid out in the previous chapters. The personnel for this phase of the planning process should include personnel from the following areas:

- Microsoft® Windows® 2000 Active Directory™ service architecture
- Windows 2000 Active Directory administration
- Infrastructure administration
- Network administration
- The out-sourcing company representative responsible for your staging process

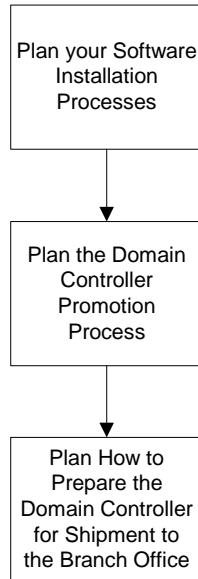
#### What You Should Know

You will need to know whether your organization is planning to use a third-party, or is planning to build its own staging site, and the connectivity that has been specified between the staging site and the hub. For the sample scenario, this would appear as follows:



---

## PROCESS FLOWCHART



---

## DESIGN CONSIDERATIONS

On first glance, building a new server, promoting it to a domain controller and shipping it to its final destination would seem to be a fairly straightforward task. In fact it is, if it is carefully planned and executed. There are a number of things that can be done wrong when domain controllers are built in a location that is different from the one where they will eventually be deployed. Some mistakes are harmless and are corrected by the system automatically, some are annoying and produce unwelcome additional network traffic, and some may severely impact the domain controller or affect the entire deployment.

This section highlights the risks, categorizes them by severity, and suggests how to avoid them. With these issues in mind, the guide then presents what the pre-staging process should be.

### Severe Problems

The following conditions can cause severe problems.

**Domain Controller Disconnected for Longer Than Tombstone Lifetime**  
Replication uses a tombstone on an object to indicate an object deletion to other domain controllers. If the time that a domain controller is disconnected exceeds the tombstone lifetime from the deployment, other domain controllers will not learn that some objects have been deleted. This might re-introduce objects to the directory that had been deleted before.

**Solution:** Never disconnect domain controllers from the network for longer than the tombstone lifetime. If this happens, the domain controller must be reinstalled.

### ISTG turned Off, no inter-Site Connection Objects Created

If the Inter-Site Topology Generator (ISTG) is turned off, and the connection objects created for the staging site are cleaned up, but the creation of connection objects either from or to a hub bridgehead server fail, the computer will become abandoned. If connection objects on both the bridgehead server and the branch domain controller are missing, the computer is also abandoned. No changes will ever replicate to or from that domain controller. If this lasts for longer than the tombstone lifetime, the computer will have to be reinstalled. If only one connection object is missing, one-way replication will work for a while, until password mismatches occur. This can take from four to eight weeks, at which point replication will not occur in either direction.

**Solution:** Regularly monitor replication. Make sure that changes flow in both directions. If a new connection object must be created, always create it on the domain controller directly. Do not rely on automatic replication to replicate a new connection object to a domain controller if a connection object is missing.

### Moderate

The following conditions are usually not severe, and only somewhat damaging.

---

### Domain Controller Disconnected for More Than Two Times Domain Controller Password Change Policy

If a domain controller has been disconnected for more than twice the length of the password change policy, the domain controller has no means to verify the passwords of replication partners. Therefore, replication will be broken until the problem is resolved.

**Solution:** Domain controllers should not be disconnected for a long time. To solve this problem, the computer passwords need to be synchronized manually.

**Old Connection Objects Created for Staging Site Are Not Cleaned Up**  
Since the ISTG is turned off, old connection objects to a domain controller in a different site are not automatically deleted after the domain controller is moved, for example from the staging site to the branch site. Therefore, the domain controller may still try to replicate from the staging site domain controller. This does not cause any problems in itself, even if the staging site is reachable, but may create additional network traffic.

**Solution:** Before the domain controller is moved from the staging site to the branch, the old connection objects on the staging domain controller must be deleted.

### Basic Steps for Domain Controller Pre-Staging

The basic steps in pre-staging a domain controller are:

- Install the operating system on a server, including Service Packs, Quick Fix Engineering (QFE) solutions, troubleshooting tools, monitoring tools, and in-house developed scripts
- Verify the installation (QA1)
- Promote the server to a domain controller
- Verify the promotion (QA2)
- Leave computer up and running in the staging site
- Prepare computer for transport
- Verify preparation (QA3)
- Ship the computer to the destination

---

## INSTALLING SOFTWARE

### Installation Planning

Ideally, all new servers and domain controllers are installed from a new image. Use *sysprep* and third-party cloning software for the installation. This process is fast and ensures that you always load the right release versions of the operating system (including Service Packs and QFEs) as well as all necessary tools on the servers. As mentioned earlier, the tools installed should include the Support Tools, the Resource Kit tools, and additional scripts developed in-house. If a third-party management tool is used, such as NetIQ's Operations Manager, the agents should be installed as part of the image.

For remote management, it is absolutely necessary to install command line tools such as the Remote Command Service and Windows Terminal Services in Remote Administration mode.

It is important to document what software releases were installed on the new server. Resist the temptation to use post-install scripts to add new QFEs or scripts. If the set of software to install changes, a new image should be created. By documenting the image, you can recover from the loss of documentation for one particular server, as long as you know when the computer was built.

It is important to correctly configure the computer after the first boot to ensure that the following are correct:

- Computer name
- IP configuration (needs valid IP address for the staging site)
- DNS configuration (finds the correct DNS server)

### Verification (QA1)

The quality assurance after the initial install is relatively simple. The person who installed the computer needs to double-check that the computer name is correct, and that the IP configuration is correct. Simple tools like *ping* and *nslookup* can be used for the IP configuration. Also check that the server registers its A record in the DNS server.

---

## PROMOTING THE SERVER TO DOMAIN CONTROLLER

Now the server is ready to be promoted to a domain controller. As mentioned above, an Active Directory Installation Wizard answer file should be used to run the promotion in unattended mode. This has the following advantages:

- You can specify the domain controller used as the source for the initial replication.
- Answer files can be re-used. All information in the answer file is not domain controller specific, but domain or site specific. This eliminates errors during the promotion.
- The new domain controllers should always be installed into the staging site. This automatically configures the new domain controller, so that the Knowledge Consistency Checker (KCC) is used for neither inter-site nor intra-site replication.

After the domain controller restarts, the appropriate connection objects have to be verified, or created if missing:

- The incoming connection object from the staging site domain controller to the new domain controller has to be created on the new domain controller.
- The incoming connection object from the new domain controller to the staging site domain controller has to be created on the staging site domain controller.

If a script is used to create the connection objects, make sure that the script binds to the right domain controller and always creates the incoming connection objects locally on the domain controller.

### Verification of Promotion (QA2)

This verification is critical. It is very important to make sure that the new domain controller now replicates with the rest of the environment. As mentioned above, this is crucial, so that all other domain controllers are informed of the new domain controller and do not abandon the computer from the rest of the environment.

Verification steps are as follows:

- Verify that the two necessary connection objects exist on both the new and the staging site domain controller.
- On the new domain controller, verify that incoming replication from the staging site domain controller works (use *Repadmin* or *replmon*).
- On the staging domain controller, verify that replication from the new domain controller works.
- Verify that the new domain controller registered its SRV records and A records in DNS.
- Verify that the new domain controller registered its CNAME record (holding the GUID used for replication) on a DNS server authoritative for the `_msdcs.<forest-root-domain>` DNS domain.
- Verify that NTFRS replication succeeded.
- Verify that sysvol is shared.

- 
- Verify that computer received a RID pool from the RID pool FSMO role owner.

#### Domain Controller Continues Running

After the quality assurance, it is important that the domain controller stays connected to the rest of the network. Domain controllers need to update information, such as password changes, frequently. For risks involved in leaving the computer disconnected, refer to the Design Considerations section earlier in this chapter.

---

## PREPARING THE COMPUTER FOR TRANSPORT

Before the computer is packed and shipped to its final destination, it needs to be configured correctly for the new branch office site. All data necessary (IP subnet of the branch, site, and site links) should already have been created in the Active Directory, and therefore replicated as part of the promotion process.

Necessary changes on branch office domain controller are:

- IP address and subnet mask have to be changed to a valid address for the branch office, where the domain controller is shipped.
- DNS configuration must be changed, so that the domain controller points to itself as its primary DNS server and to a hub site DNS server as its alternate DNS server. This will allow it to register its records correctly.
- Server object in the configuration container needs to be moved to the new site (the branch office site).
- Incoming connection object from the staging site domain controller has to be deleted.
- New incoming connection object from the bridgehead server must be created. This new connection object will be used later as replication partner when the computer has arrived in the branch.

On the staging site domain controller, the incoming connection object from the new domain controller must be deleted.

On the bridgehead server or servers to be used later, an incoming connection object from the new domain controller has to be created.

### Verify Preparation (QA3)

After making the changes in the configuration, they should be thoroughly verified. Note that this is the last time the computer can be touched by an administrator. After these last configuration changes, the computer should not respond on the staging site network. The IP address should not work in the staging site, and the routers will not be set up in such a way that they let the traffic to and from the new domain controller through, once the IP address was switched to the new address.

### Ship the Computer to the Destination

Immediately after the configuration changes, the computer should be shipped to the branch office and promptly turned on again. A QA script should be run that ensures that replication and DNS registration works properly. Make sure that the script reports results to a central location. If the results do not show up within a few days, the administrator should be notified and determine what has happened.

Documentation that was begun at the staging site (when the computer was reconfigured in the staging site, and left the staging site) should be continued and include when it was turned on at the branch office site, and its first successful replication cycle. If for any reason, a domain controller reconnection is delayed, the documentation will give you all the data necessary to decide whether the domain controller can still be turned on in the branch, it has to be re-installed, or a

---

replacement has to be shipped to the branch.

---

## ALTERNATIVE CONFIGURATION

An alternative to the configuration process described is to install a new domain controller, with its destination branch IP address and site information, during the initial installation process. This can be achieved by configuring the staging site router to let branch office site traffic pass, and supplying the correct site information in the unattended Active Directory Installation Wizard file.

The advantage of this solution is that the computer has to be configured only once, so there are fewer QA steps.

The disadvantage of this solution is that if more than one domain controller is planned for the branch office, the new domain controller will start intra-site replication with the already existing domain controllers in that site, not knowing that they are far away. This will cause more network traffic.

The configuration of the router is complicated and error-prone. Errors can lead to all routers forwarding all traffic for an existing branch to the staging site, which is very undesirable.

Therefore, while it is possible to use the eventual configuration of the branch domain controller in the staging site, the preferred solution is to use staging site IP addresses and connection objects, and to reconfigure the domain controller just prior to shipment.

---

## DOCUMENTATION

The documentation of the whole installation process, including the configuration, and the result of the QA testing, is an important deliverable of the team that performs the pre-staging. If the pre-staging is out-sourced, this deliverable has to be part of the contract with the out-sourcing partner. If this documentation is not available, a high risk exists that decisions cannot be made correctly concerning the following:

- Re-connecting domain controllers
- Deploying Service Packs
- Deploying QFEs
- Configuring domain controllers

In addition, it is absolutely mandatory that the data center administrators have an exact list of domain controllers that are deployed, and what the names, locations, and IP addresses of these computers are. Without this information, troubleshooting of missing services is very hard, if not impossible.

---

## POST-DEPLOYMENT

Assuming that the configuration of the branch office domain controller was performed correctly in the staging site, this is the easiest part of the deployment. Some considerations are:

- The domain controller should be turned on immediately after arrival in the branch office.
- The QA script should run automatically. Results must be reported to a central location.
- Replication success of the computer must be monitored very closely.

Assuming that the deployment was successful, the maintenance and ongoing monitoring of your Active Directory branch office environment begins.

---

## GENERAL ACTIVE DIRECTORY DEPLOYMENT GUIDELINES

Windows 2000 and Active Directory are enterprise-ready products. Because of the impact on your business operations, deployment of Windows 2000 and Active Directory requires extra care and diligence in both the planning and deployment stages.

This section provides you with a summarized set of general guidelines on deploying Active Directory in a large branch office environment with slow links.

### Ensure that Your Hub is a Robust Data Center

It is very important to ensure that your data center is ready to support your enterprise before you deploy the first domain controller to either the staging site or a branch office. Make sure that hardware is deployed in a robust and fault-tolerant fashion. Servers should be in racks and connected to a universal power supply (UPS). All servers should be reachable through Windows Terminal Services so that you can perform remote administration and troubleshooting. Also make sure that troubleshooting checklists and spare hardware are available where they may be needed. Standardizing on one type of server hardware can reduce troubleshooting costs and thereby reduce your overall deployment costs.

### Do Not Deploy All Branch Office Domain Controllers Simultaneously

Rather than building and deploying all domain controllers at once, we recommend that you deploy your branch office domain controllers in smaller batches, such as 50 or fewer at a time. After each batch is rolled out, verify and monitor the environment closely (For more information, refer to Chapter 9, "Post Deployment Monitoring of Domain Controllers," of the Active Directory Branch Office Deployment and Operations Guide). The following questions need to be addressed before the next batch is deployed:

- Is the current load on the bridgehead servers still within the planned range?
- Did the newly deployed domain controllers register in DNS and in Active Directory? Do they show up as domain controllers in Active Directory Sites and Services on bridgehead servers and are they in the correct sites?
- Do the newly deployed domain controllers receive changes from the bridgehead servers?
- Do the bridgehead servers receive changes from the new domain controllers?

To answer some of these quality assurance issues, a quality assurance script is included with the Active Directory Branch Office Deployment and Operations Guide. If the load on the bridgehead servers is higher than expected, add bridgehead servers or upgrade the hardware on your current bridgehead servers.

### Balance Replication Load Between Bridgehead Servers

Determining the right number of required bridgehead servers is an important exercise, but it is also important to balance replication load equally across

---

bridgehead servers. If connection objects are created using the Mkdsx scripts included with this guide, it will balance connection objects for you. If not, the administrator will be responsible for creating connection objects in a way that they balance the load across the bridgehead servers equally and monitoring the balance.

### Keep Track of Hardware and Software Inventory and Versions

Troubleshooting a distributed environment can be complex. It is even more complicated if no one knows what hardware and software has been deployed. All domain controllers that leave the staging site must be added to an inventory list and treated as running systems. If these systems do not show up during routine monitoring tests, you should determine where these domain controllers are physically located (proper documentation of hardware and location is indispensable in these situations) and why they are not responding. Remember that domain controllers may work perfectly well in a branch office (serving user logons), but replication may not be working. In such a case, the central staff may not be aware of a problem until much later when users cannot log on anymore. Documentation and knowledge of software releases is as important as hardware and location documentation. When support staff has to troubleshoot servers, they need to know what software, including release number, service packs, and QFEs, are installed on the servers. If this inventory is not available, each and every server must be tested before troubleshooting can begin, which can be a lengthy and expensive process.

### Allow Enough Time for the Branch Office Deployment

Everything goes slower and takes longer in large size deployments, so be sure your plan and schedule reflect this. Be patient. As the steps in the Active Directory Branch Office Deployment Guide indicate, there are times when you will need to wait 30 minutes while replication occurs. It takes time for all changes to reach all domain controllers. Plan for this. Chapter 3, "Planning for Replication," of this guide, outlines how to determine the time it will take for replication to occur, given the bandwidth between domain controllers.

### Include Operations in Your Planning Process

The time to start thinking about Active Directory operations, management, and maintenance is now, at the planning stage. Operations must be part of not only your deployment planning, but also your pilot testing. Important components are:

- Monitoring plans and procedures
- Disaster recovery and troubleshooting strategy
- Personnel assignment and training

#### Monitoring Plans and Procedures

The most important servers in your network are the root servers and the hub bridgehead servers. Root servers, as indicated in Chapter 2 of the Active Directory

---

Branch Office Planning Guide, perform key functions but are not usually under a heavy load. Hub bridgehead servers, on the other hand, may well become too heavily loaded. Therefore, it is especially important that you monitor your bridgehead servers closely.

Monitoring procedures—both the what and the how—are included in Chapter 9, “Post Deployment Monitoring of Domain Controllers,” of the Active Directory Branch Office Deployment and Operations Guide.

In addition to Active Directory replication, system volume (SYSVOL) replication must be monitored closely. The following guidelines are helpful:

- Monitor the files that are being replicated between your domain controllers. An easy way to do this is to place a file in SYSVOL called *<domaincontroller name and date>.txt*. The existence of this file in SYSVOL on a replication partner indicates that SYSVOL replication has occurred successfully.
- Make sure that all domain controller metadata is deleted if a domain controller is removed.
- Watch the File Replication service (FRS) staging area. Stale connections (which occur, for example, if a domain controller was removed without running the Active Directory Installation Wizard to demote it) will fill up the staging area quickly.
- If a domain controller has been disconnected for a long period of time, be careful when it is reconnected. Either make sure that the Group Policy files on that domain controller have not been modified, or perform a non-authoritative restore. A non-authoritative restore provides a clear starting point for replication from replication partners and ensures that changes that were made inadvertently on the reconnected domain controller will not be replicated out to the rest of the network.

#### Disaster Recovery and Troubleshooting Strategy

You should formulate a thorough disaster recovery plan that includes a troubleshooting strategy. Ensure that staff are properly trained in troubleshooting strategies, so that they never perform panic troubleshooting. Panic troubleshooting, such as reducing the replication interval to a very short time because a single application does not seem to work, can cause more problems than it solves, and it may not solve the problem being experienced. Panic troubleshooting often causes staff to take inappropriate actions which lead to overload situations on the bridgehead servers. These overloads then lead to new problems and mask the original, underlying issues. Documentation, again, can provide assistance. The steps taken to identify and resolve problems, if documented, can reduce downtime in similar situations. As a rule, be patient and diligent when problems arise. Correct problem identification is key.

#### Personnel Assignment and Training

Training is crucial. The deployment, operations, and support staff need to be trained on the product and on troubleshooting procedures. In addition to training, availability

---

is also important. When planning the timing of the deployment, keep in mind upcoming holidays (not only local but enterprise-wide holidays), as well as vacations. Deployment planning should include personnel contingency plans and, as with other aspects of the deployment, should be documented.

---

## SUMMARY

After you have planned your Active Directory branch office environment, as described in this and previous chapters of the Active Directory Branch Office Planning Guide, you are ready to move on to the Active Directory Branch Office Deployment and Operations Guide and begin the process of implementing your environment.