Active Directory
Design Guide

Thursday, 25 February 2010
Version 2.0.0.0 Baseline

Prepared by
Microsoft

Microsoft

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The Active Directory® Design Guide will help accelerate the design and deployment of Microsoft® Windows Server® 2008 R2 Active Directory® Domain Services (AD DS) within a healthcare organisation, and bring about a reduction in diversity of its implementation.

Implementation of this guidance will:

- Provide consistent and secure Active Directory Domain Services that increase efficiency
- Provide a flexible framework for the organisation and management of resources, including the network authorisation of, users, client computers, servers, and printers

The guidance given in this document is based on existing public guidance within the *Infrastructure Planning and Design series*[1] (IPD) documents, the *Windows Server 2008 AD DS Design Guide*[2], and the *Windows Server 2008 and Windows Server 2008 R2 Technet Library*[3]. This guidance has also been overlaid with current best practice recommendations specific to the healthcare industry.

[1] Infrastructure Planning and Design **{R1}**:
http://technet.microsoft.com/en-gb/library/cc196387.aspx

[2] Windows Server 2008 AD DS Design **{R2}**:
http://technet.microsoft.com/en-us/library/cc754678(WS.10).aspx

[3] Windows Server 2008 and Windows Server 2008 R2 **{R3}**:
http://technet.microsoft.com/en-us/library/dd349801(WS.10).aspx

2 INTRODUCTION

This document is a component of the strategic Microsoft infrastructure guidance being provided to the healthcare industry. It provides current best-practice guidance, samples and specific design decisions for the full lifecycle (that is envision, plan, develop, stabilise, deploy and operate) of Microsoft Windows Server 2008 R2 AD DS and its principal network services, such as Domain Name System (DNS). The provision of a standard healthcare-centric approach to designing and deploying a directory authentication and authorisation service will reduce the time required to plan, deploy and operate the service, thereby enabling the Total Cost of Ownership (TCO) savings that can be achieved by decreasing diversity.

2.1 Value Proposition

This document provides guidance on designing and implementing a simplified, cost-effective, reliable, and robust directory service infrastructure for healthcare organisations. The offering is designed to:

- Help identify potential design and deployment risks
- Provide rapid knowledge transfer to reduce the learning curve of designing AD DS
- Establish some preliminary design decisions before moving ahead with the implementation
- Provide a consolidation of relevant publically available AD DS best practice guidance

2.2 Knowledge Prerequisites

This section outlines the required knowledge and skills, and provides suggested training and skill assessment resources to make the most of this guidance. The necessary infrastructure prerequisites are detailed in section 2.3.

To implement effectively the recommendations made throughout this document, a number of knowledge-based and environmental infrastructure prerequisites should be in place.

2.2.1 Skills and Knowledge

The technical knowledge and minimum skills required to use this guidance are:

- Microsoft Windows Server 2008 R2 AD DS
  - AD DS design, including DNS design
  - Domain Controller Capacity Planning, site design and Domain Controller Placement
  - Operations Master roles: placement of role holders, troubleshooting role holders and management
  - Organisation Unit (OU) design

- Group Policy, both Domain and Local
  - Controlling operating system configuration and security
  - Design and implementation for application deployment
  - Management using Microsoft Group Policy Management Console (GPMC): scripting, policy export and import, backup and restore
  - Implement within an Active Directory OU hierarchy, using security groups to further control scope
- Network Services
  - DNS, particularly what AD DS requires from DNS, and how it can be integrated with third-party systems
  - Dynamic Host Configuration Protocol (DHCP): creating scopes, defining scope and server properties, lease configuration, reserving addresses, trouble shooting, configuration to support Remote Installation Services (RIS), integration with AD DS if using Microsoft DHCP service on Windows Server 2008 R2 (preferred)
  - Windows Internet Name Service (WINS): service placement, integration with Microsoft DNS and AD DS, replication design, troubleshooting and integration with DNS
  - Local area networks (LAN) and networking devices such as switches, modems, and wireless access points

2.2.2 Training and Assessment

Guidelines on the basic skill sets that are required in order to make best use of this Deliverable are detailed in APPENDIX A. These represent the training courses and other resources available. All courses mentioned are optional and can be provided by a variety of certified training partners.

2.3 Infrastructure Prerequisites

The following are prerequisites for implementing Windows Server 2008 R2 AD DS in a healthcare organisation:

- A Windows® XP, Windows Vista® and/or Windows® 7 client infrastructure that requires authentication and management by AD DS
- A Windows Server® 2000 or later server infrastructure that requires authentication and management
- A Windows Server 2008 R2 server build that is detailed in the document *Automated Build Healthcare Desktop and Server Guide* **{R4}**
- An Internet Protocol (IP) addressing scheme for the network, utilising an automated system such as that provided by DHCP
- Hostname and Network Basic Input Output System (NetBIOS) name resolution systems, such as that provided by DNS and WINS

2.4 Audience

The guidance contained in this document is targeted at a variety of roles within a healthcare IT organisation. Table 1 provides a reading guide for this document, illustrating the roles and the sections of the document that are likely to be of most interest. The structure of the sections referred to are described in section 3.1.

Role	Document Usage	Executive Summary	Envision	Plan	Develop	Stabilise	Deploy	Operate
IT Manager	Review of the entire document to understand the justification and drivers, and to develop an understanding of the implementation requirements	✓	✓					
IT Architect	Review the relevant areas within the document against local architecture strategy and implementation plans	✓	✓	✓	✓			
IT Professional/ Administrator	Detailed review and implementation of the guidance to meet local requirements	✓	✓	✓	✓	✓	✓	✓

Table 1: Document Audience

2.5 Assumptions

It is anticipated that healthcare organisations will implement their own production AD DS infrastructure in order to use a Microsoft authentication service. However, if multiple healthcare organisations collaborate closely, it would be advantageous to implement an AD DS forest infrastructure across this larger cohesive unit, thus aiding the ability for users to roam using a single logon, and access services and resources within these organisations.

The guidance provided in this document assumes that healthcare organisations that want to share services and resources between sites already have suitable IP Addressing schemes in place to enable successful site-to-site communication; that is, unique IP Addressing schemes assigned to each participating organisation with no overlap. AD DS, and the underlying DNS, requires the use of unique IP Addressing schemes at adjoining sites in order for cross-site communication to function successfully. The use of Network Address Translation (NAT) within an AD DS environment is neither recommended nor supported by Microsoft.

3 USING THIS DOCUMENT

This document is intended for use by healthcare organisations and IT administrators who are responsible for designing AD DS, including deployment and operations practices. As a result, the guidance focuses on the decision-making process, rather than a detailed procedural implementation.

The design of a directory service requires a significant undertaking because it impacts many aspects of infrastructure design and deployment.

This Active Directory Design Guide aims to:

- Collate the numerous public technical resources available for designing AD DS, into a consolidated healthcare-specific document
- Provide the order for designing AD DS through a sequenced checklist of design and deployment steps
- Identify the Microsoft current recommended practices for designing AD DS, based on industry experience, to minimise design time and reduce risk
- Identify key design decisions pertinent to the healthcare industry, and provide design solutions which reduce configuration diversity across multiple implementations
- Provide a standardised design and configuration approach to reduce the administration and management overheads of the system, thereby reducing overall support costs
- Provide a consistent and reliable directory service to users as they move around their healthcare organisation, thereby increasing their utilisation and service quality perception of the infrastructure

3.1 Document Structure

This document contains six sections that deal with the project lifecycle, as illustrated in Figure 1 and in the list below:

- Envision
- Plan
- Develop
- Stabilise
- Deploy
- Operate

Each section is based on the Microsoft IT Project Lifecycle as defined in the Microsoft Solutions Framework (MSF) Process Model, and the Microsoft Operations Framework (MOF). The IT Project Lifecycle is described in more detail in the *Microsoft Solutions Framework Core White Papers*[4] and the *MOF Executive Overview*[5]. The MSF Process Model and MOF describe a high-level sequence of activities for building, deploying and managing IT solutions. Rather than prescribing a specific series of procedures, they are flexible enough to accommodate a broad range of IT projects.

[4] Microsoft Solutions Framework Core White Papers:
http://www.microsoft.com/downloads/details.aspx?FamilyID=e481cb0b-ac05-42a6-bab8-fc886956790e&DisplayLang=en

[5] MOF Executive Overview:
http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofeo.mspx

The following diagram illustrates the different sections of this guide:

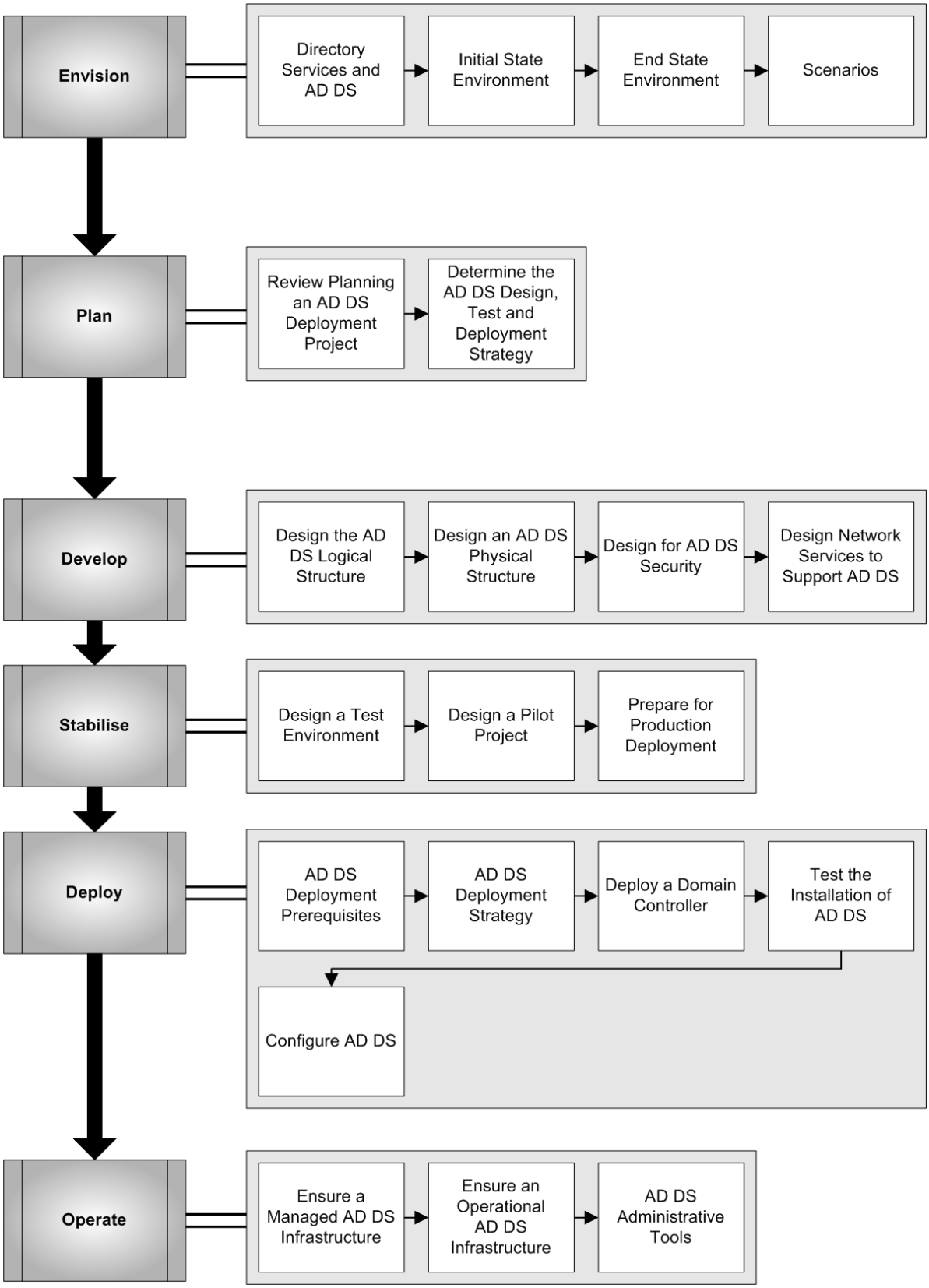


Figure 1: Microsoft Solutions Framework Process Model Phases and Document Structure

The key public documentation resources for developing an AD DS solution are listed below. Where appropriate, specific chapters or sections from these documents have been referenced throughout this guidance.

- *Infrastructure Planning and Design* **{R1}**, in the Directory Services, Directory Service Planning Guide section, for high-level architectural overview of major concepts
- *Windows Server Technologies: Networking* [6], for high-level architectural overview of major concepts
- *Active Directory Services*[7], for detailed technical review of components aimed at IT Professionals
- *Windows Server 2008 and Windows Server 2008 R2* **{R3}** for detailed technical analysis of more specialised components aimed at IT Professionals

[6] Windows Server Technologies: Networking **{R6}**: http://technet.microsoft.com/en-us/library/cc753940(WS.10).aspx

[7] Designing and Deploying Directory and Security Services **{R5}**: http://technet.microsoft.com/en-us/library/dd578336(WS.10).aspx

4 ENVISION

The Envision phase addresses one of the most fundamental requirements for success in any project unification of the project team behind a common vision. There must be a clear vision of what is to be accomplished such that it can be stated in clear terms. Envisioning, by creating a high-level view of the overall goals and constraints, will serve as an early form of planning. It sets the stage for the more formal planning process that will take place during the planning phase.

Figure 2 acts as a high-level checklist, illustrating the sequence of events that should be undertaken when envisioning a directory service within a healthcare organisation:

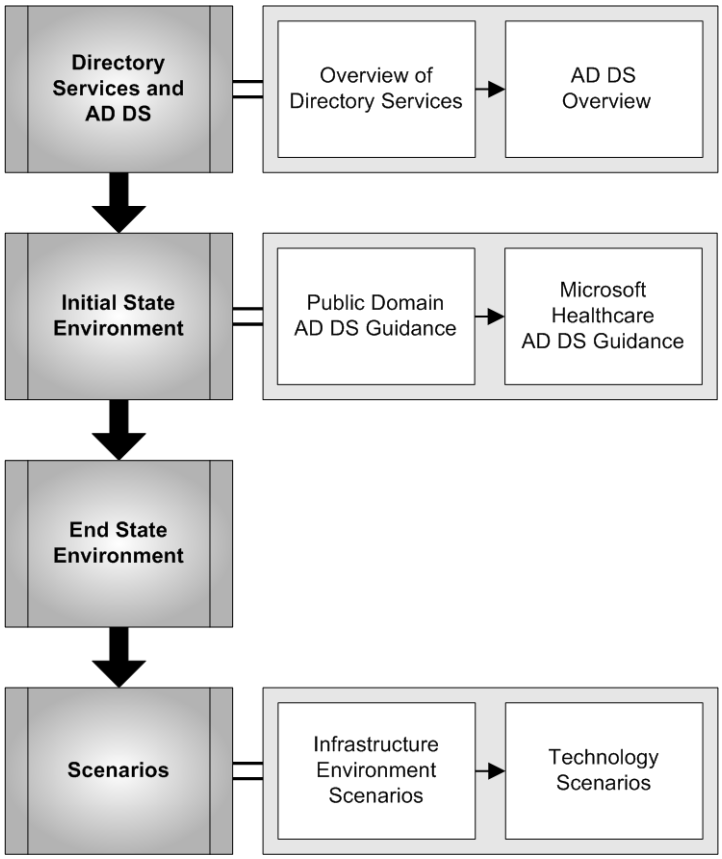


Figure 2: Sequence for Defining a Directory Service Design

4.1 Directory Services and AD DS

The persistent drive to reduce the complexity and diversity of the network infrastructure and drive down costs makes it paramount that IT delivers new value back to the business with the least amount of investment and effort. This guidance provides a rigorous process that will assist in ensuring that directory services within a healthcare organisation are designed and developed to provide maximum business value.

4.1.1 Overview of Directory Services

A directory service provides the ability to store information about networked devices and services, and the people who use them, in a central location within a distributed environment. A directory service also implements the services that make this information available to users, computers, and applications. Therefore, a directory service is both a directory (the store of this information) and a set of services that provide the means to securely add, modify, delete, and locate data in the directory store.

4.1.2 AD DS Overview

AD DS is the network focused directory service included in the Windows 2000, Windows Server 2003 and Windows Server 2008 family of operating systems. AD DS delivers an extensible and scalable service that provides network authentication, administration and management of directory services to an organisation running a Windows-based network infrastructure.

Figure 3 illustrates the benefits of AD DS and how it acts as the focal point of the Windows Server 2008 R2 network, demonstrating how it can be used to manage identities and broker relationships between distributed resources.

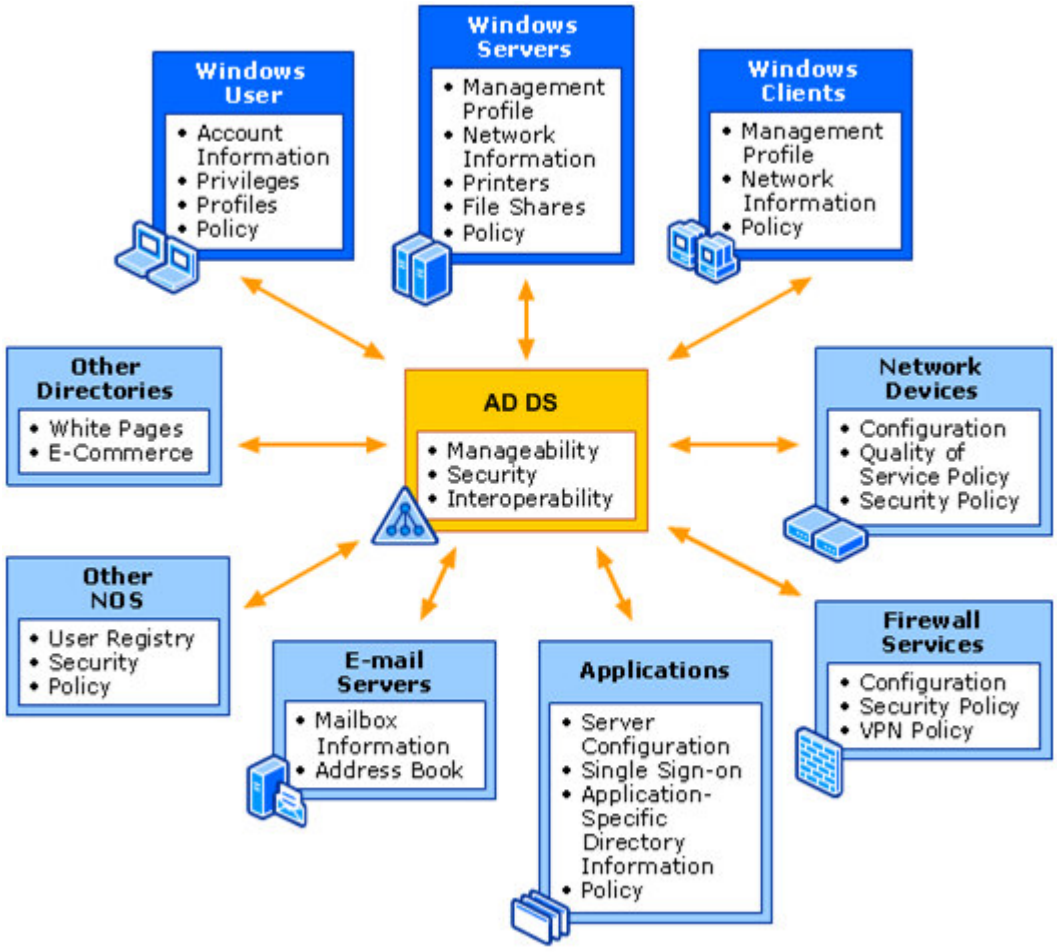


Figure 3: AD DS on a Windows Server 2008 R2 Network

AD DS provides:

- **A central location for network administration and the delegation of administrative authority**

  AD DS acts as a repository for objects representing all network users, devices, and resources, and provides the ability to group objects for ease of management and the application of security and Group Policy. Group Policy refers to applying policy (configuration settings) to groups of computers and/or users contained in AD DS.

- **Information security and single sign-on for user access to local network resources**

  Tight integration with security eliminates costly tracking of accounts for authentication and authorisation between systems. A single user name and password (or smartcard) combination can identify each network user, and this identity follows the user throughout the local network.

- **Scalability**

  AD DS can be designed and implemented in numerous configurations to achieve scalability from a single site with a small number of users, to a highly complex large-scale site to meet any current and future network authentication requirements.

- **Easy and flexible searching of the Active Directory**

  Users and administrators can use Windows XP, Windows Vista or Windows 7 desktop tools to search the entire Active Directory.

- **Storage for application data**

  AD DS provides a central location to store data that is shared between applications, and with applications that need to distribute their data across entire Windows networks.

- **Efficient synchronisation of directory updates**

  Updates are distributed throughout the network through secure and cost-efficient replication between domain controllers.

- **Remote administration**

  It is possible, providing the user has been granted appropriate permissions, to connect to any domain controller remotely from any Windows-based computer that has Windows Server administrative tools installed.

- **Single, modifiable, and extensible schema**

  The schema is the definition of the objects and their attributes that can be created in AD DS. It is possible to modify the schema to create new attributes that can be used to implement new types of objects or to extend existing objects. For example, attributes of the user object store information, such as username, password, and telephone number.

- **Integration of service names with DNS, the Internet standard name resolution service**

  AD DS relies on DNS to implement an IP-based naming system so that the Active Directory and domain controllers are locatable over standard IP, both on intranets and the Internet.

- **Lightweight Directory Access Protocol (LDAP) support**

  LDAP is the industry standard directory access protocol, making AD DS widely accessible to management and query applications. AD DS supports LDAP version 2 and version 3.

A detailed view of all the components involved in an AD DS design is illustrated in APPENDIX B.

4.2 Initial State Environment

AD DS design can be a complex undertaking and there are many different possible approaches to designing and implementing an AD DS solution. The provision of a standardised design approach, including key design recommendations, will reduce the time and effort required to design and deploy a directory service within a healthcare organisation.

Figure 4 illustrates examples of the potential diversity of a directory services design within healthcare organisations that could be derived if using purely public information sources without specific healthcare guidance.

> **Note**
>
> The following diagram provides examples, and is not intended to provide specific design recommendations.

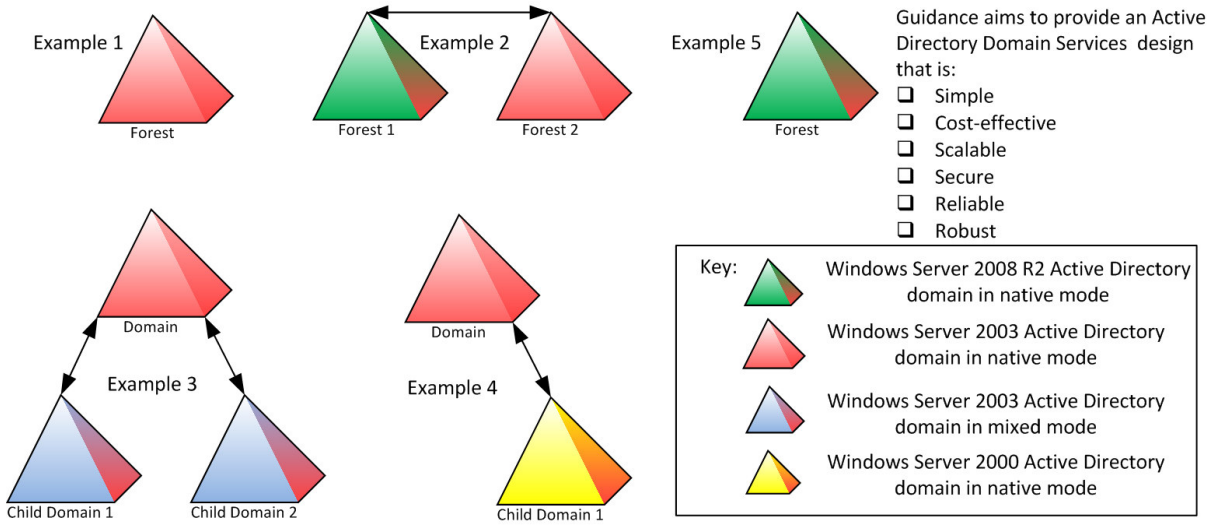


Figure 4: Potential Diversity of AD DS Designs without Guidance

4.2.1 Public Domain AD DS Guidance

The Internet hosts many web sites, documents and guidance which provide assistance in designing AD DS. This information can be hard to navigate, and often contains inaccuracies or out-of-date information. This document seeks to provide accurate and up-to-date current best practice guidance, much of which is based upon four publicly available sources of information for AD DS, which range in technical depth. These sources are:

- *Windows Server 2008 R2 Product Help* **{R7},** which provides a thorough product overview and generic deployment guidance
- *Infrastructure Planning and Design* **{R1},** which provides architectural-level design guidance for an IT infrastructure
- *Active Directory Services* **{R5},** which provides technical guidelines, tools, and the recommended process for designing and deploying Windows Server 2008 R2 Directory and Security services technologies to meet generic business needs and IT goals
- The Microsoft Technet collection of documentation: *Windows Server 2008 and Windows Server 2008 R2* **{R3}**, which contains in-depth technical guidance on specific Windows Server 2008 R2 topics, such as AD DS, Core Operating system, Networking and Windows Security

4.2.2 Microsoft Healthcare AD DS Guidance

The guidance provided within this document is predominantly based upon two Microsoft public resources, the *Infrastructure Planning and Design series* **{R1}** and the *Active Directory Services collection* **{R5}**. The specific books, chapters and sections from these resources that relate to this AD DS guidance will be identified where appropriate.

It is appreciated that healthcare organisations will each have unique requirements that cannot be met by architecture guidance alone. Sometimes, only prescriptive, step-by-step guidance will do.

The *Infrastructure Planning and Design* **{R1}** and the *Active Directory Services collection* **{R5}** have been designed and developed with the knowledge that, when adopted, organisation IT infrastructure will require further customisation to match the unique business and technology requirements of individual healthcare organisations. The referenced documentation is not intended to be a universal solution for all healthcare organisations, but rather a set of design choices and best practices that can be used to jump start the local directory services solution, understand what decisions are available, why a decision is made in a given scenario, and how to implement that decision.

This AD DS guidance endeavours not to repeat content from public documentation, but to provide a consolidated, organised and structured reference list to these documents. Where appropriate, it includes recommendations where a typical healthcare organisation should deviate from the current default installation configurations or Windows Server 2008 R2 configuration.

4.3 End State Environment

The Directory Services guidance provided within this document will help lead a healthcare organisation through the process of making inherently complex design and implementation decisions for an AD DS infrastructure.

Whilst no AD DS design guidance can be a 'one size fits all', this document enables a healthcare organisation to simplify the design process, whilst allowing them to take local requirements into account. This will result in a reduction in diversity in AD DS design across the healthcare industry, thus aiding the supportability of the directory services through the standardisation and regulation of implementations. In the future, it may be possible to further enhance these benefits through collaboration of services and service provision. Healthcare organisations will be able to establish common practice approaches to training and support of administration tasks required to maintain these directories.

It is anticipated that each healthcare organisation will implement a single domain Active Directory forest in the production environment. Additional single domain Active Directory forests will exist on isolated networks as pre-production and test environments. For more information on Active Directory forests, see section 6.1.2.

4.4 Scenarios

This section describes the following scenarios that are recommended as appropriate for the application of this guidance:

- The infrastructure environment scenarios
- The technology scenarios

4.4.1 Infrastructure Environment Scenarios

This section describes the key levels which are recommended as appropriate for the deployment of AD DS and its associated network services.

Whilst Microsoft strongly recommends starting with a simple single forest Windows Server 2008 R2 Active Directory it is not always possible due to the business requirements the directory structure needs to address.

In general, the reason why Microsoft recommends a simple single forest is to help ensure the maximum return on investment and to minimise the long term TCO of the service. In some cases where a number of individual healthcare organisations are part of a larger controlling body, there would be an advantage in implementing a single Active Directory forest for the entire body. However, while this may ultimately be the most cost and management-effective goal, it could be that the individual healthcare organisations are sufficiently autonomous that operational and political constraints render this unachievable.

The current and most appropriate level at which to deploy AD DS (which forms the most cohesive financial, administrative and security unit) is at the healthcare organisation level. A single domain Active Directory forest at the healthcare organisation level ensures that the forest acts as the local authentication and authorisation directory security boundary for that entire healthcare organisation. This infrastructure enables clinicians and administrators to move around within their organisation, utilising network resources to deliver the care required, wherever it is needed.

Healthcare organisations can range in size and functionality. For example:

- A single site with a small number of users (up to 50)
- An organisation spread over multiple locations with any number of users
- An organisation controlling between one to three hospitals, each with approximately 2000 users, potentially a total of 6000 users across a few physical sites
- An organisation controlling multiple General Practice clinics, each with, for example, 20 users at each of the multiple different physical sites, with a total of approximately 500 users across these sites
- A central organisation which provides IT services to multiple healthcare organisations, normally within a defined geographical area, including hospitals and General Practice clinics, as well as a number of administrative office locations

The IT infrastructure and IT administration for these examples could be either a centralised or distributed implementation scenario. The first, second and third examples above would be classed as centralised deployments of servers and administration. The fourth and fifth examples would be classed as a distributed deployment, potentially hosting a server locally in a General Practice clinic and delegating certain levels of administration to the local non-IT staff, whilst core control would be maintained by a central IT team.

The following points are assumed for a healthcare organisation regardless of its size:

- The organisation has the power to mandate IT solutions and the money to implement these solutions
- Each healthcare organisation has a single IT service provider who will own AD DS
- Levels of network connection can potentially be controlled, such as ensuring that there is no NAT[8] in place within the organisation (NAT may exist at the boundaries of the network, where it connects to external networks, such as the Internet)

[8] For further information regarding the use of NAT, see section 2.5.

It is acknowledged that implementing AD DS at a healthcare organisation level, rather than attempting to implement a single Active Directory forest across a number of loosely affiliated organisations, may introduce some limitations into the Directory Services design:

- There is no default Kerberos[9] authentication between forests if multiple healthcare organisations want to provide cross-organisation user roaming and resource sharing. However, this is technically achievable with additional configuration and/or Microsoft products such as Windows Server 2003 Active Directory Cross Forest Trust, and Windows Server 2003 Active Directory Federation Services (AD FS)
- A single global catalog (GC)[10] of objects (that is user accounts and their attributes, such as employee ID) would not exist within the healthcare organisation. However, this is technically achievable with additional Microsoft products, such as the Microsoft Identity and Integration Feature Pack (IIFP) and Microsoft Identity and Integration Server (MIIS)
- Healthcare organisation boundaries may change in the future, requiring further technical effort to join, consolidate or divest AD DS

With these points in mind, it is important that each healthcare organisation assesses the criteria within this guidance document during the initial AD DS design phases. It may be deemed more beneficial, from both a cost and technical perspective, to collaborate with other healthcare organisations and thereby avoid these constraints, ultimately reducing the TCO for directory services and increasing the benefits of AD DS.

Up to this point, guidance has only been provided for implementing a single domain forest within the production environment. It is expected that, in addition to the single production forest for each healthcare organisation, an additional forest is implemented as a pre-production test environment that is representative of the production implementation. Microsoft strongly recommends the use of a pre-production environment on an isolated network which mirrors the hardware and software configuration of the live environment as far as possible. This should be used for final testing of applications and patches before release to production. In addition, Microsoft recommends a 'sandbox' style test environment, either physically implemented or in a virtualised environment. This should be used to perform tasks such as basic design proving and application testing, and should be rebuilt as and when required. The remainder of this guidance focuses on the Active Directory forest requirements for the production environment.

4.4.2 Technology Scenarios

The core technology required by this guidance is Windows Server 2008 R2. Many of the features discussed in this guidance were also available in Windows Server 2008 which itself extended the technology provided by Windows Server 2003. Where appropriate, Windows Server 2008 R2 components will be discussed.

Additional components included as part of the Windows Server 2008 R2 installation DVD that are required include:

- DNS service
- WINS
- Remote Server Administrative Tools (RSAT)
- Security Configuration Wizard

[9] Kerberos – a security system that authenticates users. Kerberos does not provide authorisation to services or databases; it establishes identity at logon, which is used throughout the session. The Kerberos protocol is the primary authentication mechanism in the Windows 2000 and above operating systems.

[10] The global catalog contains a partial replica of every Windows Server 2003 domain in the Active Directory. This lets users and applications find objects in an Active Directory domain tree, given one or more attributes of the target object without knowing which domain holds them, and without requiring a contiguous extended namespace in the environment.

In the past it was recommended to install the Windows Server support tools and Resource kit tools but a strategic change incorporated into Windows Server 2008 was to eliminate these resources and to include all of the tools as part of the Operating system itself. Additional Microsoft software that is required and available for free download from the Internet includes:

- Active Directory Management Pack[11], if using Microsoft System Center Operations Manager

The hardware requirements are stated in the *Windows Server 2008 R2 Build* **{R4}**.

> **Note**
>
> Services mentioned within this section will not be available between parts of a healthcare organisation that have identical IP Address schemes. The use of NAT as a workaround between such parts of the organisation within an AD DS environment is neither recommended nor supported by Microsoft.
>
> For further information please read the Assumptions statement in section 2.5, and the Microsoft whitepaper *Active Directory in Networks Segmented by Firewalls*[12].

[11] Active Directory Management Pack for Operations Manager 2007 **{R8}**: http://www.microsoft.com/downloads/details.aspx?FamilyId=008F58A6-DC67-4E59-95C6-D7C7C34A1447&displaylang=en&displaylang=en

[12] Active Directory in Networks Segmented by Firewalls **{R10}**: http://www.microsoft.com/downloads/details.aspx?FamilyID=c2ef3846-43f0-4caf-9767-a9166368434e&DisplayLang=en

5 PLAN

The Plan phase is where the bulk of the implementation planning is completed. During this phase, the areas for further analysis are identified and a design process commences.

Figure 5 acts as a high-level checklist, illustrating the sequence of events that the IT Manager and IT Architect need to perform when planning for deployment of AD DS within a healthcare organisation:

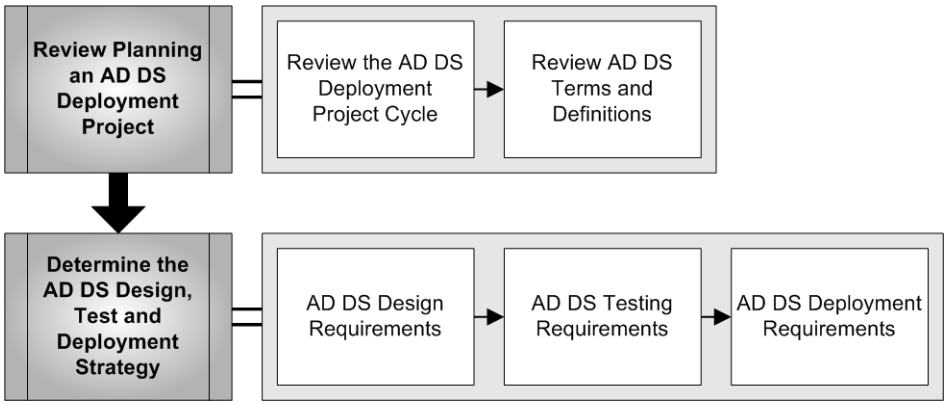


Figure 5: Sequence for Planning an AD DS Design

It is vital that, before embarking on the Windows Server 2008 R2 AD DS design, all IT Professionals involved have a thorough understanding, at architectural level, of how AD DS can be used to provide a directory services solution specifically for their healthcare organisation.

In addition to the AD DS guidance in this document, it is important to frequently visit the Microsoft web site for up to date product information, guidance on best practices and architectural information. It should be noted that, where features and technology have not changed since the Windows Server 2003 release, the documentation has not been updated.

- *Active Directory Best practices*[13] (Windows Server 2003)
- *DNS best practices*[14] (Windows Server 2003)
- *WINS Best Practices*[15]

5.1 Review Planning an AD DS Deployment Project

Before beginning to plan the Windows Server 2008 R2 AD DS, it is important to become familiar with the AD DS deployment project cycle, as well as AD DS related terms that are required during the project process.

[13] Active Directory Best practices **{R11}**:
http://technet2.microsoft.com/WindowsServer/en/library/5712b108-176a-4592-bcde-a61e733579301033.mspx?mfr=true

[14] DNS best practices **{R12}**:
http://technet2.microsoft.com/windowsserver/en/library/59d7a747-48dc-42cc-8986-c73db47398a21033.mspx

[15] WINS Best Practices **{R13}**:
http://technet2.microsoft.com/windowsserver/en/library/ed9beba0-f998-47d2-8137-a2fc52886ed71033.mspx

5.1.1 Review the AD DS Deployment Project Cycle

An AD DS deployment project involves six key phases. Figure 6 shows the relationship between the phases of the project cycle, relative to the lifetime of the deployment project.

During the Planning phase, it is important to understand the interaction between the subsequent phases for project planning purposes. In the Developing phase, a design for Active Directory that best meets the needs of the healthcare organisation that will be using the directory service should be created. After the design is approved, the design should be stabilised by testing it in a lab environment and then implementing the final design in the production environment.

As testing is typically performed by those that would deploy the Active Directory, and it could potentially affect the designing phase, it is an interim activity that overlaps both design and deployment. When the deployment is complete, the Active Directory service becomes the responsibility of those that will carry out the day-to-day activities of maintaining it. Lab testing and the implementation of a pilot program should continue throughout the lifetime of the deployment.

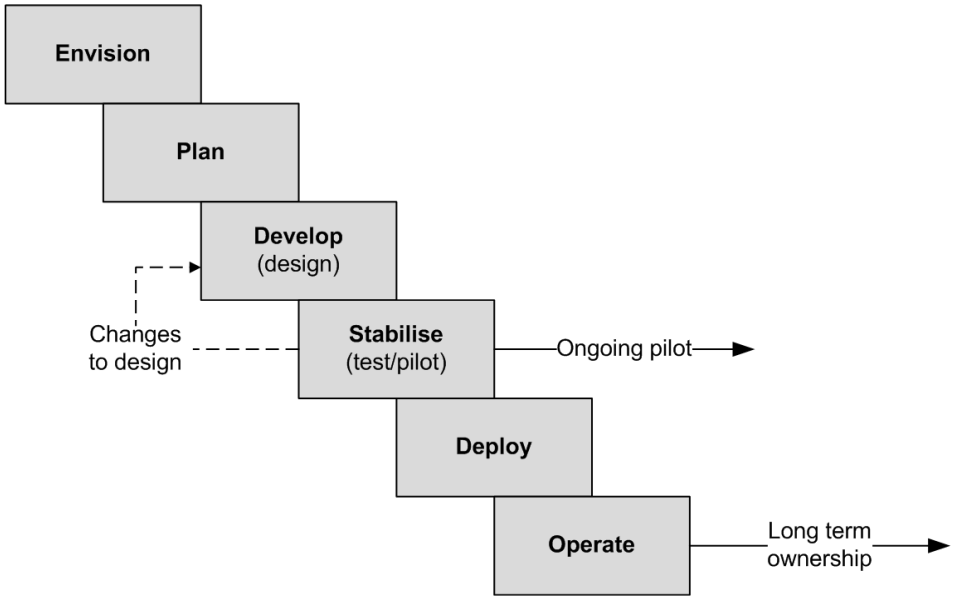


Figure 6: AD DS Deployment Project Phases

5.1.2 Review AD DS Terms and Definitions

It is important to ensure that certain terms and definitions referred to in this guidance are understood when designing an AD DS deployment process. Table 2 details the most important of these.

Term	Definition
AD DS domain(Active Directory domain)	An administrative unit in a computer network which groups capabilities together for management convenience, such as network-wide user identity, authentication, trust relationships, policy administration and replication.
AD DS forest (Active Directory forest)	A collection of one or more Active Directory domains that share the same directory schema and a common logical configuration structure. It also includes automatic transitive trust relationships between domains in the forest so that any object in one domain can be granted access to resources in any domain in the forest. The forest is also the security boundary for an AD DS instance.
AD DS functional level (Active Directory functional level)	An advanced domain-wide or forest-wide AD DS feature which can be enabled through a setting in Windows Server 2008 R2 AD DS. Typically the functional levels enable specific features that rely on all domain controllers being at a minimum operating system version.
Migration	The process of moving an object from a source domain to a target domain. This process involves either preserving or modifying properties of the object to ensure it is accessible in the target domain.
Domain restructure	A migration process that involves changing the domain structure of a forest.
Domain consolidation	A restructuring process which involves merging the contents of one domain with another domain in order to reduce the overall number of domains in use.
Domain upgrade	The process of upgrading the directory service of a domain to a later version.
In-place domain upgrade	This process involves an upgrade of the operating system on all domain controllers while all domain objects remain in place.
Regional domain	A child domain that is created based on a geographic region in order to optimise replication traffic.

Table 2: Windows Server 2008 R2 AD DS Important Terms and Definitions

5.2 Determine the AD DS Design, Test and Deployment Strategy

The level of AD DS strategy required will vary according to the healthcare organisation's existing network configuration. The guidance presented within this document is focused on the components required for a new AD DS, rather than looking at upgrading or restructuring an existing implementation. However some of these concepts overlap.

> **Note**
>
> Microsoft has produced the *Active Directory Migration Guide* Deliverable which provides guidance on the migration to Windows Server 2003 Active Directory. This guidance can be used in conjunction with this document to aid a healthcare organisation investigating the restructuring of an existing implementation.

The AD DS design and testing requirements are expanded further in sections 6 and 7 detailed technical references and relevant healthcare organisation design decisions where appropriate.

5.2.1 AD DS Design Requirements

Table 3 identifies the most important aspects which require understanding and planning when designing AD DS for a healthcare organisation. See section 6 for a more detailed breakdown of these components.

AD DS Design Component	Section Number for Further Detail
Designing an AD DS Logical Structure	6.1
Identify the Deployment Project Participants	6.1.1
Create a Forest Design	6.1.2
Create a Domain Design for Each Forest	6.1.3
Design the OU Structure for Each Domain	6.1.4
Prepare to Enable Advanced Features via Functional Levels	6.1.5
Active Directory Trust Design	6.1.6
AD DS Naming Standards	6.1.7
Design an AD DS Physical Structure	6.2
Collect Network Information	6.2.1
Domain Controller Placement	6.2.2
Operations Master Role Placement	6.2.3
Create a Site Design	6.2.4
Create a Site Link Design	6.2.5
Create a Site Link Bridge Design	6.2.6
Domain Controller Hardware Availability and Scalability Requirements	6.2.7
Designing for AD DS Security	6.3
Plan a Secure AD DS Environment	6.3.1
Design an Authentication Strategy	6.3.2
Design a Resource Authorisation Strategy	6.3.3
Design a Public Key Infrastructure (PKI)	6.3.4
Designing Network Services to Support AD DS	6.4
DNS Infrastructure to Support AD DS	6.4.1
WINS Infrastructure to Support AD DS	6.4.2
Additional Network Services	6.4.3

Table 3: AD DS Design Components

It is important that the AD DS design components are planned for whilst scoping the project, such that they are included in the Build phase. Thoroughly planning the AD DS design is essential to ensure a secure, stable and cost-effective deployment.

5.2.2 AD DS Testing Requirements

Table 4 identifies the most important aspects that require understanding and planning when testing and verifying AD DS for a healthcare organisation. See section 7 for a more detailed breakdown of these components.

AD DS Testing Component	Section Number for Further Detail
Design a Test Environment	7.1
Create a Test Plan	7.1.2
Develop the Test Lab	7.1.5
Design the Test Cases	7.1.6
Conduct the Tests	7.1.7
Design a Pilot Environment	7.2
Create a Pilot Plan	7.2.2
Deploy and Test the Pilot	7.2.4
Evaluate the Pilot	7.2.5
Prepare for Production Deployment	7.3

Table 4: AD DS Testing Components

5.2.3 AD DS Deployment Requirements

Table 5 identifies the most important aspects which require understanding and planning when deploying AD DS for a healthcare organisation. See section 8 for a more detailed breakdown of these components.

AD DS Deployment Component	Section Number for Further Detail
AD DS Deployment Prerequisites	8.1
AD DS Deployment Strategy	8.2
Active Directory Forest Root Domain Deployment	8.2.1
Raise the Functional Level	8.2.2
Deploy a Domain Controller	8.3
Test the Installation of AD DS	8.4
Configure AD DS	8.5

Table 5: AD DS Deployment Components

6 DEVELOP

During the Develop phase the solution components are built based on the planning and designs completed during the earlier phases. Further refinement of these components will continue into the stabilisation phase.

The Develop phase has been structured into four major components, for which design decisions are required for an Active Directory service.

Figure 7 acts as a high-level checklist, illustrating the sequence of these components that the IT Manager and IT Architect need to determine when planning for AD DS deployment within a healthcare organisation:

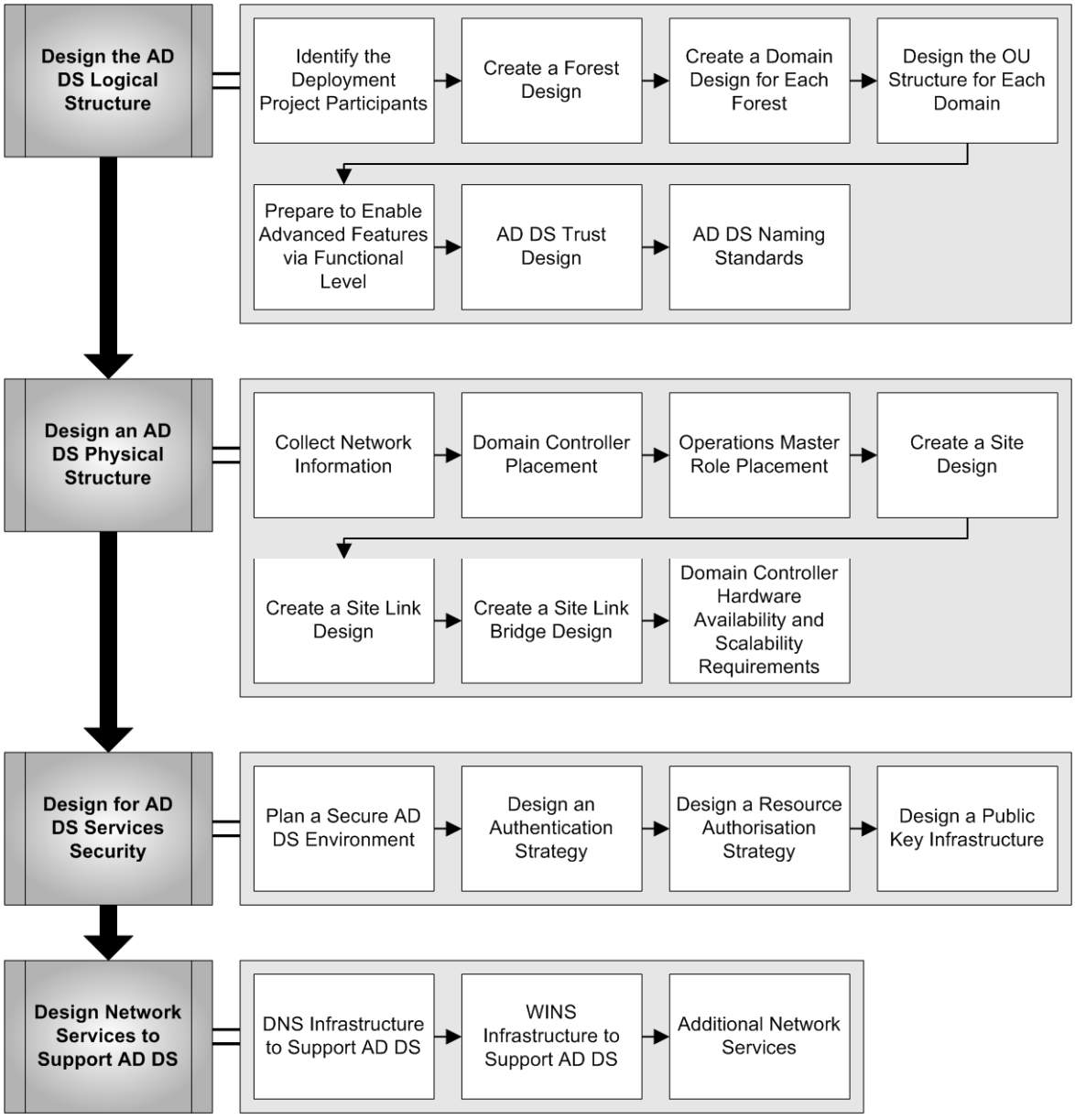


Figure 7: Sequence for Building an Active Directory Design

The aim of the Develop phase is to provide a structured synopsis of these major components, with each component being broken down into why it is important, determine what its critical aspects are, and also identify for these what key design decisions are required for the healthcare organisation.

For many of the major AD DS components, job aids are available in the Windows Server 2003 Deployment Kit, comprising of worksheets that can help an IT professional document design decisions and create subsequent deployment plans. There are currently no such similar job aids for Windows Server 2008 R2 although the Windows Server 2003 Deployment kit aids could be used in conjunction with the documented Windows Server 2008 AD DS Deployment Guide {**R33**}. The specific job aid filenames have been referenced in the relevant sections of this guidance and can be downloaded from the Microsoft Download Center[16].

> **Information**
>
> In section 4.4.1, various implementation scenarios and infrastructure environments were identified. Where possible, throughout this section, the recommended design decisions will be identified, allowing healthcare organisations to map these to their environment, and therefore reduce the amount of time required to produce the AD DS design. It is recommended that these are used in conjunction with the Windows Server 2003 Deployment Kit job aids.

6.1 Design the AD DS Logical Structure

Designing an AD DS logical structure involves defining the structure of, and relationships between, the forests, domains, and OUs that require deployment.

Careful designing of the AD DS logical structure provides the following benefits:

- Ensures that the time and effort required to implement AD DS in the live environment is minimised
- Allows an efficient structure to be designed that best meets the health organisation's administrative requirements
  - Simplifies the management of the Windows networks that may contain large numbers of objects, such as users, computers and groups
  - Consolidates the domain structure and reduces administration costs
  - Provides the ability to delegate administrative control over resources, as appropriate
- Reduces impact on network bandwidth
- Simplifies resource sharing
- Optimises search performance
- Lowers TCO

A well-designed AD DS logical structure facilitates the efficient integration of features such as Group Policy, enabling desktop lockdown, software distribution, and the administration of users, groups, workstations, and servers, into the infrastructure environment. In addition, a carefully designed logical structure facilitates the integration of other services, such as PKI for added security, and domain-based Distributed File System (DFS) for file collaboration.

[16] Job Aids for Windows Server 2003 Deployment Kit **{R14}**: http://www.microsoft.com/downloads/details.aspx?FamilyID=edabb894-4290-406c-87d1-607a58fc81f0&DisplayLang=en

6.1.1 Identify the Deployment Project Participants

6.1.1.1 Determine Project Specific Roles

Specific roles during an AD DS design should be identified. The key roles[17] include Executive Sponsor, IT Architect, IT Manager and IT Professionals.

Depending upon the size of the healthcare organisation, the number of individuals that need to take part in the project will vary; large healthcare organisations may require several individuals to get involved, whilst smaller healthcare organisations may only require a couple of resources with multiple project roles, such as the IT Architect and the IT Manager. The roles of the IT Professionals design team and the deployment team may also overlap depending upon the size of the organisation and number of resources available.

The established design team that is required to begin the forest planning and deployment process should include IT professionals who are familiar with the existing network, the potential forest owners, the individuals who manage the corporate namespace, and the owners and administrators who will be responsible for AD DS after the deployment project is complete.

6.1.1.2 Establish Owners and Administrators

Ensure that service owners and administrators **{R15}** are established for the following roles in AD DS:

- **Service and Data owners for AD DS**

  The service owners are those who are responsible for planning and managing AD DS, defining the forest structure and ensuring the service availability. The data owners are those who are responsible for the data stored in AD DS. For example, IT Manager roles which include the forest owner, the AD DS DNS owner, the site topology owner, and the OU owner.

- **Service and Data Administrators for AD DS**

  The service administrators are those who have been delegated the privilege to implement decisions or design changes defined by the service owners and who are trusted to manage AD DS on a day-to-day basis. Data administrators are those who have been delegated the permissions to update, create or delete specific data stored within AD DS such as modifying the properties of user objects. For example, IT Administrators responsible for retaining service control of AD DS, and IT Professionals responsible for the data administration of AD DS objects such as users and groups.

As with the project specific roles, the owners and administrators in larger healthcare organisations may be different individuals, whereas in smaller organisations, individuals may be responsible for multiple roles.

6.1.1.3 Document the Project Teams

Once the participants of the project have been defined, the names and roles should be documented. It is advised that this is done using the *Design and Deployment Team Information* job aid document, named *DSSLOGI_1.doc* **{R14}**.

[17] Identifying the deployment Project Participants **{R15}**: http://technet.microsoft.com/en-us/library/cc732532(WS.10).aspx

> **Recommendation**
>
> The use of the job aids available in the Windows Server 2003 Deployment Kit **{R14}** is highly recommended as they can aid a healthcare organisation in quickly documenting the design decisions made throughout the AD DS design, particularly if the IT professionals involved are not experienced in creating complex detailed design documents.

6.1.2 Create a Forest Design

Creating a forest design involves identifying the groups within the healthcare organisation that have the resources available to host an Active Directory forest, defining the forest design requirements, and then determining the number of forests required in order to meet these requirements.

6.1.2.1 Identify Groups able to Host an Active Directory Forest

Prior to understanding whether a multiple forest design within a single organisation is required, it must be first ascertained whether the various groups within the organisation that will host and administer an Active Directory forest have the financial and human resources available to do so. If a group does not have these resources available, it will not be possible to implement a multiple forest design.

6.1.2.2 Identify the Forest Design Requirements

Whilst Microsoft strongly recommends in public documentation to start with a simple single forest Windows Server 2008 R2 AD DS, there are situations where multiple forest designs within a single organisation will be required. This section highlights some of these key factors and the resultant recommendations for a healthcare organisation.

> **Recommendation**
>
> It is recommended that where possible a single Active Directory forest is implemented at the healthcare organisation level for the production environment, therefore following the organisational forest model[18].

Identifying the business requirements that the directory structure needs to accommodate involves determining how much autonomy the groups in the healthcare organisation need to manage their network resources, and whether each group needs to isolate their resources on the network from other groups.

The three critical types of business requirements that need thoroughly investigating to help identify the Active Directory forest design requirements are:

- Organisational structure requirements
- Operational requirements
- Legal requirements

Part of identifying the forest design requirements[19] involves identifying the degree to which groups in the healthcare organisation can trust the potential forest owners and their service administrators, and identifying the autonomy and isolation requirements for each group in the healthcare organisation.

[18] Forest Design Models **{R16}**:
http://technet.microsoft.com/en-us/library/cc770439(WS.10).aspx

[19] Identifying Forest Design Requirements **{R17}**:
http://technet.microsoft.com/en-us/library/cc730924(WS.10).aspx

During the forest design process, it is important to identify who are the AD DS administrators[20] and what their scope of authority will be, as this will help determine forest security boundaries.

> **Recommendations**
>
> - There should be a strict division of service and data administration within AD DS
> - There should be as few 'service' administrators as possible, all of whom are highly trusted
> - All other AD DS tasks should be related to 'data' based administration, and delegated out appropriately on the principle of 'Least Privilege', thus helping to maximise security
> - Additional forests should only be considered if there is a requirement to isolate or provide complete autonomy for the service owners or system administrators of a particular section in a directory service

Once the forest design requirements regarding data, service, autonomy and isolation considerations have been defined, they should be documented. It is advised that this is done using the *Forest Design Requirements* job aid document, named *DSSLOGI_2.doc* **{R14}**.

> **Note**
>
> If no groups within the organisation have identified additional requirements, a simple single forest design will be suitable for the healthcare organisation.

6.1.2.3 Determine the Number of Forests

If a simple single forest design is not suitable due to the identification of additional requirements, it is necessary to determine the forest design model and the number of forests needed. Current best practice forest design models[21] that can be identified include:

- **Organisational forest model**

  User accounts and resources are contained in the forest and managed independently.

- **Resource forest model**

  A separate forest is used to manage resources.

- **Restricted access forest model**

  A separate forest is created to contain user accounts and data that must be isolated from the rest of the healthcare organisation.

- **Impending divestiture**

  A separate forest is recommended to accommodate users and services for the elements of a healthcare organisation that will be separated out into a separate organisation in the near future. Although this creates extra work it makes the separation much easier as the forest can be separated and there is no need to perform a migration of the affected users and applications out of the health organisation's AD DS.

Once the number of forests has been defined, it should be documented. It is advised that this is done using the *Forest Design* job aid document, named *DSSLOGI_3.doc* **{R14}**. Table 6 provides an example of a simple record of the design decisions made, taking into account the recommendation of a single forest for a healthcare organisation.

---

[20] Service Administrator Scope of Authority **{R18}**: http://technet.microsoft.com/en-us/library/cc772268(WS.10).aspx

[21] Forest Design Models **{R19}**: http://technet.microsoft.com/en-us/library/cc770439(WS.10).aspx

Group Name	Contact	Forest Type	Requirements
Health Organisation Group IT	IT Architect Name Email Phone	Organisational	A single forest created for the entire organisation. All groups within the organisation will use this forest.

Table 6: Example Completed Job Aid for Forest Design

6.1.3 Create a Domain Design for Each Forest

The forest owner is responsible for creating a domain design for the forest. Creating a domain design involves examining the replication requirements and the existing capacity of the network infrastructure, and then building a domain structure that enables AD DS to function in the most efficient way.

6.1.3.1 Review the Domain Models

It is advised that any AD DS design should start with a single domain and forest design in the production environment to maintain management simplicity and ensure lowest possible TCO. In a single domain design, all information is replicated to all of the domain controllers. The release of Windows Server 2008 R2 has further reduced the reasons for needing separate domains in a forest leaving a small set of specific reasons for multiple domains.

There are justifiable reasons for having multiple domain model designs within a forest. The following factors will impact this decision:

- The amount of available bandwidth capacity on the network that is able to be allocated to AD DS
- The number of users in the healthcare organisation
- The number of domain controllers that would be needed to support the healthcare organisation

6.1.3.2 Determine the Number of Domains Required

It is best to minimise the number of domains that are deployed in the forest as this reduces the overall complexity of the deployment and, as a result, further reduces TCO.

> **Recommendations**
>
> A single domain forest should be implemented at the healthcare organisation level, forming the simplest possible domain design within this cohesive unit. This enables reduced administrative complexity by providing the following advantages:
>
> - Any domain controller can authenticate any user in the forest
> - All domain controllers can be GC servers
> - A reduced number of domain controllers

The following information can be used in circumstances where a single domain forest is not suitable for the healthcare organisation.

Taking into account the factors listed in section 6.1.3.1, the following table shows the recommended maximum number of users in a single domain in conjunction with the slowest link available and the percentage of bandwidth available to AD DS replication. Table 7 can aid in determining the number of domains required in this situation.

Slowest Link Connecting a Domain Controller (Kbps)	Maximum Number of Users if 1% Bandwidth Available	Maximum Number of Users if 5% Bandwidth Available	Maximum Number of Users if 10% Bandwidth Available
28.8	10,000	25,000	40,000
32	10,000	25,000	50,000
56	10,000	50,000	100,000
64	10,000	50,000	100,000
128	25,000	100,000	100,000
256	50,000	100,000	100,000
512	80,000	100,000	100,000
1500	100,000	100,000	100,000

Table 7: Recommended Maximum Number of Users in a Single Domain

> **Note**
>
> The figures quoted in Table 7 are based upon the following environment conditions:
>
> - 20 percent new user accounts created per year
> - 15 percent user accounts removed per year
> - Each user account is a member of five global groups and five universal groups
> - For every one user there is one computer
> - The DNS solution in use is AD DS Integrated DNS
> - DNS scavenging is enabled

On this basis, if a healthcare organisation has only one percent of bandwidth available to AD DS replication, using a 28.8 Kbps link between locations where domain controllers reside, it can still support up to 10,000 users in a single domain.

It is recommended that, once the number of domains has been defined, it should be documented using the *Indentifying Regions* job aid document, named *DSSLOGI_4.doc* **{R14}**.Table 8 provides an example of a simple record of the design decisions made, taking into account the recommendation of a single domain forest for a healthcare organisation.

Name of Region	Slow Link	# of Users	Comment
Healthcare Organisation	56 Kbps	5,000	A single forest with a single domain and 5% bandwidth allocation for AD DS

Table 8: Example Completed Job Aid for the Number of Domains

6.1.3.3 Determine Whether to Upgrade Existing or Deploy New Domains

This AD DS guidance is focused on providing guidance for new installations. Specific guidance on upgrading Windows NT 4.0 and Windows 2000 domains, as well as migrating from Novell NetWare, is provided in the *Active Directory Migration Guide,* and includes the following scenarios:

- Migrating from Windows NT 4.0 domains
- Migrating from Windows 2000 domains
- Migrating from Novell NetWare

6.1.3.4 Assign Domain Names

DNS and NetBIOS names for each domain must be determined and assigned. It is recommended that this is done using the *Domain Planning* job aid, named *DSSLOGI_5.doc* **{R14}**.

> **Recommendations**
>
> The recommended naming standards guidance shown in section 6.1.7 should be followed when determining any domain names.
>
> It is advised that the Active Directory domain name follows the naming convention of the healthcare organisation scale for which it is being deployed and is prefixed with the letters 'AD' to easily identify the name as being associated with the AD DS implementation.

6.1.3.5 Select the Forest Root Domain

Once the domain model has been determined, it is necessary to select the domain which will act as the forest root domain. This involves determining whether one of the AD DS domains in the domain design can function as the forest root domain, or whether it is necessary to deploy a dedicated forest root domain.

> **Recommendation**
>
> A single domain forest for the production environment should be implemented at the healthcare organisation level, forming the simplest design, whereby the single domain acts as the forest root domain.

The forest root domain name is also the name of the forest. The forest root name is a DNS name that consists of a prefix and a suffix, in the form of *prefix.suffix*. Creating a new namespace for AD DS ensures that any existing DNS infrastructure does not need to be modified to accommodate AD DS.

> **Recommendation**
>
> The recommended naming standards guidance given in section 6.1.7 should be followed when determining any domain names.

6.1.4 Design the OU Structure for Each Domain

Forest owners are responsible for creating OU designs for each domain. Creating an OU design involves designing the OU structure, assigning the OU owner role, and creating account and resource OUs. For further information on the best practice methods around OU design, refer to the guidance document, *Group Policy for Healthcare Desktop Management* **{R20}**.

6.1.5 Prepare to Enable Advanced Features via Functional Level

In order to utilise the advanced features in Windows Server 2008 R2, the domain and/or forest must be raised to the appropriate functional level. This not only enables new features to be used, but also limits the versions of Windows that can be run on domain controllers in the environment. The following are references for the advanced features available:

- Table 23 (APPENDIX C) summarises the AD DS features that are available by default on any domain controller running Windows Server 2008 R2
- Table 24 (APPENDIX C) lists the Windows Server 2008 R2 domain functional levels, the operating systems that they support, and the Windows Server 2008 R2 features that are available at each domain functional level
- Table 25 (APPENDIX C) lists the Windows Server 2008 R2 forest functional levels, the operating systems that they support, and the Windows Server 2008 R2 features that are available at each forest functional level

6.1.5.1 Prepare to Enable Functional Levels

In order to determine what preparation is required to enable domain and/or forest functional level changes, the following should be identified:

- Assess the current environment requirements. It is recommended that this is done using the *Domain Controller Assessment* job aid document, named *DSSPFL_1.doc* **{R14}**
- Identify the functional level scenario, for example, a Windows NT 4.0 environment, a Windows 2000 mixed-mode environment, a Windows 2000 native-mode environment, a Windows Server 2003 environment or a new Windows Server 2008 R2 forest
- Identify any applications that cannot support the desired functional level and assess which is the maximum functional level they can support. This is typically a scenario around the release of a new version of the operating system which offers new functional levels in AD DS. For the majority of applications it is not necessarily the functional level that is unsupported but rather what it means in terms of domain controllers. Some applications in the past have failed to work in an environment where all domain controllers are running the latest Windows Server operating system version

Once the current environment has been assessed and the functional level requirements are gathered, the appropriate domain and/or forest functional level can be enabled during the deployment phase.

> **Recommendation**
>
> In order for healthcare organisations to be able to utilise advanced features, the forest functional level should be raised to Windows Server 2008 R2 native-mode as soon as possible after forest creation. Raising the forest functional level automatically raises the domain functional level.
>
> **Information**
>
> - It is not possible to lower the functional level of a domain or forest after it has been raised without a full domain or forest restore
> - Only members of the Domain Admins group can raise the domain functional level
> - Only members of the Enterprise Admins group can raise the forest functional level
> - The Primary Domain Controller (PDC) emulator operations master is the domain controller that should be used to raise the domain functional level
> - The schema operations master is the domain controller that should be used to raise the forest functional level

6.1.6 AD DS Trust Design

By default, all users in a specific Active Directory domain can be authenticated and authorised for resources contained within that domain. In this way, users can be provided with secured access to all resources in that domain. To expand that access to include resources beyond the boundaries of a single domain, trust relationships are required. Trust relationships provide a mechanism for one domain to allow access to resources, from user accounts that have been authenticated in another domain.

Transitive trust relationships allow full forest wide authentication and resource access within an Active Directory forest. However, in order for controlled users to have authentication and resource access, it is necessary to manually design for, and deploy, trusts to external domains and forests.

The trust technologies[22] in Windows Server 2008 R2 can provide a starting point to help healthcare organisations address these business requirements, and enhance their ability to offer and maintain Single Sign-On (SSO) and Reduced Sign-On (RSO).

Applications integrated with Windows Server 2008 R2 and AD DS use the built-in features of the operating system to establish and maintain trust for a wide variety of business requirements and scenarios, including domain trusts, cross-forest trusts and external trusts.

Windows Server 2008 R2 fully audits trust configuration at a detailed level. Auditable events include the creation, deletion and modification of trusts.

> **Recommendations**
>
> A single domain forest should be implemented at healthcare organisation level, therefore no additional internal trusts will be required in the forest unless:
>
> - It is necessary to have an external trust relationship with another healthcare organisation Active Directory forest in order to allow roaming users and the collaboration of resources
> - Cater for third-party IT service provision requirements
>
> Ideally, in a design requiring collaboration between multiple forests, each forest should be, at a minimum, configured with Windows Server 2003 forest functional level and cross forest trusts should be implemented, ensuring that Kerberos is used between forests, and allowing for a greater degree of configuration with regards to security.

Should additional trusts be required, the Multiple Forest Considerations in Windows 2000 and Windows Server 2003[23] whitepaper should be reviewed in conjunction with this section. However, if it is determined that no additional trusts are required, section 6.1.6.1 can be skipped.

[22] Trust Technologies **{R21}**:
http://technet2.microsoft.com/windowsserver/en/library/9d688a18-15c7-4d4e-9d34-7a763baa50a11033.mspx and
http://technet.microsoft.com/en-us/library/cc770299.aspx

[23] Multiple Forest Considerations in Windows 2000 and Windows Server 2003 **{R22}**:
http://technet2.microsoft.com/windowsserver/en/library/bda0d769-a663-42f4-879f-f548b19a8c7e1033.mspx

6.1.6.1 Identify and Design for Trust Model Required

Once the AD DS trust requirements have been determined, if required, the trust model relationships should be designed and documented.

Administrators can use a number of methods[24] to configure and manage trust relationships in AD DS environments, including the following:

- Trust tools built into the Windows Server Operating system
- Trust Windows Management Instrumentation (WMI) classes
- Script based solution using classes and APIs provided in the operating system

Configuring Trust relationships also requires cooperation with the network security team to ensure that the required network ports are configured to support the trust and its associated traffic.

Before designing and deploying trust relationships between two forests (also known as interforest trusts, including both external and forest trusts), ensure that all possible security threat scenarios are reviewed[25].

6.1.7 Active Directory Naming Standards

Every object in AD DS is an instance of a class defined in the schema. Each class has attributes that ensure:

- Unique identification of each object (instance of a class) in a directory data store
- Backward compatibility with Security Identifiers (SIDs) used in Windows NT 4.0 and earlier for security principals
- Compatibility with LDAP standards for directory object names

Each object in AD DS can be referenced by several different names. AD DS creates a relative distinguished name (RDN), and a canonical name (CN), for each object based upon information that was provided when the object was created or modified. Each object can also be referenced by its distinguished name (DN), which is derived from the relative distinguished name of the object and all of its parent container objects.

> **Recommendation**
>
> Windows Server 2008 R2 does not provide any software based policy for enforcing a naming standard. Therefore, a healthcare organisation naming policy should be established and communicated to all employees who have been delegated the right to create objects in AD DS.

The following sections contain the guidelines and guidance for the naming standards of the most common Active Directory objects.

6.1.7.1 AD DS Forest and Domain Naming Requirements

AD DS domain names are usually the full DNS name of the domain. However, for backward compatibility, each domain also has a pre-Windows 2000 name for use by computers running pre-Windows 2000 operating systems.

---

[24] Domain and Forest Trust Tools and Settings **{R23}**: http://technet2.microsoft.com/windowsserver/en/library/108124dd-31b1-4c2c-9421-6adbc1ebceca1033.mspx. Windows Server 2008 R2 specific content is embedded within the individual chapters documented in the Active Directory Domains and Trusts section http://technet.microsoft.com/en-us/library/cc770299.aspx

[25] Security Considerations for Trusts **{R24}**: http://technet2.microsoft.com/windowsserver/en/library/1f33e9a1-c3c5-431c-a5cc-c3c2bd579ff11033.mspx and specific Windows Server 2008 R2 content related to the separate Trust types is contained in the Active Directory Domains and Trusts section http://technet.microsoft.com/en-us/library/cc770299.aspx

The pre-Windows 2000 domain name can be used to log on to a Windows Server 2008 R2 domain from computers running pre-Windows 2000, Windows 2000, Windows XP, or servers running Windows Server 2003 using the *DomainName\UserName* format. Users can also log on to computers running any Windows operating system from Windows 2000 onwards using the User Principal Name (UPN) associated with their user account.

Recommendations

The following recommended naming standards should be adhered to when determining any DNS or pre-Windows 2000 (NetBIOS) domain names:

- Use a prefix that is not likely to become outdated
- Use a prefix that includes Internet standard characters only, which include A-Z, a-z, 0-9 and (-), but are not entirely numeric
- Ensure that DNS naming policy is identifiable with, and relevant to, the healthcare organisation that AD DS is representing
- Ensure that it is clear and meaningful
- Keep DNS naming intuitive, using 15 characters or fewer in the prefix, and as such allowing the NetBIOS name to be the same as the prefix
- The chosen name should avoid generic words such as AD, Corp and root. Any name that looks as though it could easily clash with another organisation should be avoided, something quite likely with generic words
- Domain and forest names cannot be comprised solely of numbers. Neither the domain name nor the forest name can commence with a period (.)or a hyphen (-)
- Avoid the use of any of the words listed in the table of reserved words documented in Microsoft Knowledge Base article 909264[26]
- The Active Directory DNS domain name should be the healthcare organisation's name preceded by the letters 'AD'; for example, ADHealthOrg. See section 6.1.7.2 for more information
- The Active Directory NetBIOS domain name should be an abridged version of the organisation's name preceded by the letters 'AD' so that it is not longer than 15 characters in total
- UPNs should be used for user account log on. See section 6.1.7.3 for more information on AD DS Security Principal Object Naming Requirements

6.1.7.2 DNS Naming Requirements

The DNS and NetBIOS names for each domain will be determined in section 6.1.3, based on the guidelines in section 6.1.7.1. It is recommended that this is documented using the *Domain Planning* job aid, named *DSSLOGI_5.doc* **{R14}**. Table 9 provides an example of a simple record of the design decisions made, taking into account the recommendations made for DNS and NetBIOS names.

Region	Origin	DNS Prefix	NetBIOS Name	Justification / Notes
Health Organisation	☑ New domain ☐ Upgrade From: Owner: *IT Administrator*	ADHealthOrg.healthorg.com	ADHealthOrg	The ADHealthOrg domain is a sub-domain of the organisation's externally registered domain, this is also the Forest Root Domain

Table 9: Example Completed Job Aid for DNS and NetBIOS Names

[26] Naming conventions in Active Directory for computers, domains, sites, and OUs: **{R25}** http://support.microsoft.com/kb/909264

The DNS and NetBIOS names should be incorporated into the DNS infrastructure, and a forest DNS name identified.

> **Recommendations**
>
> The DNS namespace should not be a single label DNS name, as detailed in Microsoft Knowledge Base article 300684: *Information about configuring Windows for domains with single-label DNS* names **{R26}**.
>
> The DNS name should be registered as a sub-domain of the organisation's external DNS registration, and should follow their suffix standards, for example, *healthorg.org.com.* This reduces administration, whilst maintaining simplicity and flexibility in working towards an integrated collaborative infrastructure for the healthcare organisation.
>
> The DNS name should be as short as possible while still remaining meaningful and unique. This reduces the risk of any file system issues with very long domain names.

Table 10 lists the character sets that are supported by DNS and NetBIOS.

Character Restriction	Standard Domain Name System (Including Windows NT4.0)	Microsoft Domain Name System (Windows 2000, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2)	NetBIOS
Characters permitted	Supports Request for Comments (RFC) 1123, which permits: A to Z, a to z, 0 to 9, and the hyphen (-).	Supports RFC 1123 and Universal Transformation Format-8 (UTF-8). Windows 2000 Server onwards DNS server can be configured to allow or disallow the use of UTF-8 characters.	Not allowed: Unicode characters, numbers, white space, and the symbols: / \ [ ] : | < > + = ; , ? and *).
Maximum host name and Fully Qualified Domain Name (FQDN) length.	63 bytes for each name and 255 bytes for the complete FQDN (254 bytes for the FQDN plus one byte for the terminating dot).	The same as standard DNS with the addition of UTF-8 support. Some UTF-8 characters exceed one byte in length.	15 bytes in length.

Table 10: Domain Name System and NetBIOS Naming Character Set Restrictions

6.1.7.3 AD DS Security Principal Object Naming Requirements

Security principal objects are AD DS objects that are assigned SIDs, and can be used to log on to the network, as well as being granted access to domain resources. An administrator needs to provide names for security principal objects (user accounts, computer accounts, and groups) that are unique within a domain.

Establishing an organisation-wide naming convention for AD DS objects helps to ensure that secure access control within any Active Directory forest is not compromised. Without a universal naming convention, the potential for user error when adding, modifying or removing AD DS security principal objects increases substantially, especially if IT Administrators move around the infrastructure.

> **Recommendation**
>
> When establishing an AD DS object naming convention for the healthcare organisation, ensure that it provides for the inclusion of information about the object's scope and purpose in its name, and also its owner in its description. This helps to differentiate each object from similar objects.

The names of security principal objects can contain all Unicode characters except the special LDAP characters defined in RFC 2253. This list of special characters includes: a leading space, a trailing space and any of the following characters: # , + " \ < > and ;

Table 11 displays the security principal object names and the guidelines that they must conform to:

Type of Account Name	Maximum Size	Special Limitations
User account	Computers running Windows Server 2003 and Windows 2000 can use a UPN for a user account. Computers running Windows NT 4.0 and earlier are limited to 20 characters or 20 bytes, depending upon the character set. Individual characters may require more than one byte.	A user account cannot consist solely of periods (.) or spaces, or end in a period. Any leading periods or spaces are cropped. Use of the @ symbol is not supported with the logon format for Windows NT 4.0 and earlier, which is *DomainName**UserName*. Windows 2000 logon names are unique to the domain and Windows Server 2003 logon names are unique within the forest.
Computer account	NetBIOS = 15 characters or 15 bytes, depending upon the character set. Individual characters may require more than one byte. DNS = 63 characters or 63 bytes, depending upon the character set, and 255 characters for a FQDN. Individual characters may require more than one byte.	A computer account cannot consist solely of numbers, periods (.), or spaces. Any leading periods or spaces are cropped.
Group account	63 characters or 63 bytes, depending upon the character set. Individual characters may require more than one byte.	A group account cannot consist solely of numbers, periods (.), or spaces. Any leading periods or spaces are cropped.

Table 11: Guidelines for Security Principal Names

> **Note**
>
> If the administrator changes the default security settings, then it is possible to use computer names containing more than 15 characters.

6.1.7.3.1 User Account Names

In AD DS, each user account has:

- A user logon name
- A pre-Windows 2000 user logon name (Security Account Manager (SAM) account name)
- A UPN suffix

The administrator enters the user logon name and selects the UPN suffix when creating the user account. AD DS suggests a pre-Windows 2000 user logon name using the first 20 bytes of the user logon name. Administrators can change the pre-Windows 2000 logon name at any time.

In AD DS, each user account has a UPN based on Internet Engineering Task Force (IETF) RFC 822: *Standard for the Format of ARPA Internet Text Messages*[27]. The UPN is composed of the user logon name and the UPN suffix joined by the @ sign.

> **Important**
>
> Do not add the @ sign to the user logon name or the UPN suffix as AD DS automatically adds it when it creates the UPN. A UPN that contains more than one @ sign is invalid.
>
> Windows NT4.0 and earlier domains allowed the use of a period (.) at the end of a user logon name as long as the user logon name did not consist solely of period characters. Windows Server 2008 R2 domains do NOT allow the use of a period or multiple periods at the end of a user logon name.

[27] Standard for the Format of ARPA Internet Text Messages **{R27}**: http://www.ietf.org/rfc/rfc2822.txt

The second part of the UPN, the UPN suffix, identifies the domain in which the user account is located. This UPN suffix can be the DNS domain name, the DNS name of any domain in the forest, or it can be an alternative name created by an administrator and used just for log on purposes. This alternative UPN suffix does not need to be a valid DNS name.

In AD DS, the default UPN suffix is the DNS name of the domain in which the user account was created. In most cases, this is the domain name registered as the enterprise domain on the Internet. Using alternative domain names as the UPN suffix can provide additional logon security and simplify the names used to log on to another domain in the forest.

Recommendations

- User account names should follow the format of *firstname.lastname*
- Duplicate names should be handled by including the middle initials in the user name such as *firstname.initial.lastname*
- UPN suffixes should be used for user log on. For more information see the Microsoft Knowledge Base article: *Users Can Log On Using User Name or User Principal Name*[28]
- Whilst users log on to the AD DS using UPN names, the common name (CN) displayed within the Active Directory Users and Computers Microsoft Management Console (MMC) should be named such that different user accounts are easily identified, for example administrator account names are preceded with 'adm_', service accounts preceded with 'svc_' and temporary staff account names could be preceded with 'tmp_'
- Staff with administrative responsibilities should have at least two accounts: A regular user account with which they perform their normal, day to day activities such as email and document creation and a separate account used purely for administrative tasks. The administrative account should not have access to email and should be named the same as the regular user account but with a prefix of 'adm_'. This allows administrative actions to be audited and a clear association between the administrative activities and the user

For enhanced security, the local Administrator user account should be renamed from *Administrator* to make it harder to guess and attack[29].

Recommendation

- It is recommended that the built in Administrator user account is renamed to blend in with the chosen naming scheme, as well as delete the default comment on this account, and therefore aid security
- A dummy user account should be created with the name 'Administrator' to act as a decoy account, this account should then be disabled

6.1.7.3.2 Group Account Names

It is possible to apply any group naming strategy that works for the organisation, as long as group names provide enough information to distinguish them from other groups. A common approach is to create a security group naming standard that organises groups according to business structure. In this way, group names are composed of labels that represent the organisational structure, such as department, team, and task.

Without descriptive labels, it is possible to create confusing group names. Adding more descriptive labels takes time and planning, but user group searches and rights assignments are more accurate as a result.

An organised system for naming groups makes it easy to locate the correct security group, and helps protect against duplicate naming.

---

[28] User Can Log on Using User Name or User Principal Name **{R28}**: http://support.microsoft.com/kb/243280

[29] The Administrator Accounts Security Planning Guide **{R29}**: http://www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.mspx

In addition, following should be considered when creating group names and descriptions:

- Both the name and description of an object can include up to 256 characters
- The naming standard should be able to distinguish between security and distribution groups as well as group scope and purpose. For example security groups could be prefixed with SEC and distribution groups prefixed with a DIST. The scope of the group could be identified with the use of GLO (for Global security groups), DLG (for Domain Local Groups) and UNI (Universal Security Groups). A typical naming scheme for group names is <type>-<scope>-<description> for example, SEC-GLO-InternetAccessAllowed
- The first 20 characters of the name are usually visible in a list without resizing columns and scrolling. When viewing the Properties dialog box of the object, about 50 characters of the name are viewable. It is current best practice to abbreviate any organisational labels used in the object name to ensure that the distinguishing portion of the object name can be viewed in these environments

6.1.7.3.3 Workstation Computer Account Names

Each computer account created in AD DS has the following names:

- A relative distinguished name
- A pre-Windows 2000 computer name (Security Account Manager (SAM) account name)
- A primary DNS suffix
- A DNS host name
- A Service Principal Name (SPN)

The administrator enters the computer name when creating the computer account. This computer name is used as the LDAP relative distinguished name.

AD DS suggests the pre-Windows 2000 name is used, including the first 15 bytes of the relative distinguished name. The administrator can change the pre-Windows 2000 name at any time.

The DNS name for a host, also the full computer name, is a DNS fully qualified domain name (FQDN). The full computer name is a concatenation of the computer name (the first 15 bytes of the SAM account name of the computer account without the "$" character) and the primary DNS suffix (the DNS domain name of the domain in which the computer account exists). It is listed on the **Computer Name** tab in System Properties in the Control Panel.

When creating a workstation build, it is important to have a consistent workstation naming convention to ease support and to avoid duplicate network names, see the *Automated Build Healthcare Desktop and Server Guide* **{R4}** guidance document for more information.

> **Recommendations**
>
> An organisation-wide computer naming standard should be implemented that allows for, and conforms to, the following criteria:
>
> - Workstation names should be easy for users to remember
> - Workstation names identify the location of the workstation
> - Select names that describe the type of workstation
> - Use unique names for all computers in the organisation. Do not assign the same computer name to different computers in different DNS domains
> - Do not use the character case to convey the owner or purpose of a computer, because DNS is not case-sensitive

An example of a workstation naming standard could be of the form illustrated in Table 12, where the workstation name is **DTRHW00001**:

Computer Type	Location	Machine Number or Asset Number
DT	RHW	00001 OR A567B

Table 12: Example Workstation Naming Standard

Where the following is the case:

Component	Example Use	
Computer Type		
A two character code indicating the machine type	Laptop	LT
	Desktop	DT
	Tablet	TP
	Pocket PC	PP
Location		
A three character site code	**RHW** (ROYAL BERKSHIRE NHS FOUNDATION TRUST)	
Machine Number or **Asset Number**	Machine number could be a sequential number, such as **00001**, whereas Asset Number is the official Asset Tag, such as **A567B**	

Table 13: Recommended Workstation Naming Convention

> **Recommendation**
>
> It is recommended that the healthcare organisation use an asset number and machine type scheme, as detailed in Table 13.

6.1.7.3.4 Server Computer Account Names

The naming convention for servers should follow a similar standard to that of the workstations. The difference would be that the two-character code would indicate the server role rather than the machine type.

Table 14 provides examples of server roles and two-character codes that could be used to identify them. Only the most common server roles have been given, therefore the table is not exhaustive.

Server Role	Two-Character Codes
Domain Controller	DC
File Server	FS
Print Server	PR
SQL Server	SQ
WSUS Server	WU
Anti-Virus Server	AV
Web Server	WW
Application Server (not fitting into another named role)	AP
Multi-role server (for example, File/Print/WSUS/Custom Application)	MR
Proxy Server	PX

Table 14: Example Server Role Naming Standards

6.1.7.3.5 Organisational Unit Names

The AD DS OU structure is not intended to be visible to end users. The OU structure is an administrative tool for Service and Data Administrators.

> **Recommendation**
>
> The names used to represent the OU object within AD DS should reflect the objects contained within the organisation and the administrative and policy-based structure for the OUs. For detailed information on the best practice recommendations for the OU structure, see the *Group Policy for Healthcare Desktop Management* **{R20}** guidance document.

6.1.7.3.6 Site and Site Link Names

Sites and subnets are represented in AD DS by site and subnet objects. The replication path between sites is designated to AD DS by use of site link objects.

> **Important**
>
> It is recommended to use legal DNS names when creating new site names, otherwise the site will only be accessible where a Microsoft DNS server is used. The primary reason for this is that site names are published in DNS and must therefore adhere to DNS naming rules. It is also advisable that site names should not consist entirely of numbers.

Sites should have easily identifiable and standardised national codes associated with them to aid administrators with locating sites and site links.

> **Recommendation**
>
> The name for the site object that will be created in AD DS should only use Internet standard characters and should contain the name of the organisation, as well as the Site code for the location of the site to aid IT Administration, such that, the format will be, *<Healthcare Organisation code>< Site Code><number>*.

For example, a North London Hospital in a healthcare organisation called Contoso would have the site name **CONNLH3901**. Table 15 provides a breakdown of the meaning of the site object name for this example:

Characters	Identifier	Value	Example
1-3	Healthcare Organisation Code	3 character combination of letters or letters and numbers	CON
4-8	Site Code	5 character combination of letters or letters and numbers	NLH39
9-10	Sequential number	01-99	01

Table 15: Site Object Naming Convention

Site link objects require a straightforward naming structure that easily identifies both ends of the link for ease of administration.

> **Recommendation**
>
> Site Link object names can be generated from two sites which are interconnected, separated by a hyphen (-). For example, linking the North London Hospital in Contoso with the Manchester Hospital in the Contoso would give a site link object name of:
>
> CONNLH3901-CONMAH0101

6.2 Design an AD DS Physical Structure

The AD DS physical structure incorporates the following components of AD DS:

- Site topology
- Domain controller placement
- Operations Master role placement
- Hardware availability and scalability requirements

The site topology is a logical representation of the physical network. Designing an AD DS site topology involves planning for domain controller placement and designing sites, subnets, site links and site link bridges, to ensure efficient routing of authentication, query and replication traffic.

Planning domain controller placement and capacity helps determine the appropriate number of domain controllers to place in each domain that is represented in a site. Capacity planning also assists in estimating the hardware requirements for each domain controller so that cost can be minimised and an effective service level is maintained for the users.

Before beginning to design the site topology, it is important that the following components of AD DS have been designed and reviewed:

- AD DS logical structure, including the administrative hierarchy, forest plan, and domain plan for each forest (see section 6.1)
- DNS infrastructure design for AD DS (see section 6.4.1)

6.2.1 Collect Network Information

Before beginning to design the AD DS physical components, it is important to understand the existing physical network structure and devices. The following components should be identified and documented:

- A location map that represents the physical network infrastructure of the healthcare organisation
- List communication links and available bandwidth. It is advised that this is documented using the *Geographic Locations and Communication Links* job aid, named *DSSTOPO_1.doc* **{R14}**
- List IP subnets within each location. It is advised that this is documented using the *Locations and Subnets* job aid, named *DSSTOPO_1.doc* **{R14}**
- List domains and number of users for each location. It is advised that this is documented using the *Domains and Users in Each Location* job aid, named *DSSTOPO_1.doc* **{R14}**

6.2.2 Domain Controller Placement

After gathering all of the network information that will be used to design the site topology, planning where to place domain controllers including regional and forest root domain controllers should take place.

> **Note**
>
> This process does not include the identification of the proper number of domain controllers and the domain controller hardware requirements for each domain represented in each site. This is covered in section 6.2.7.

6.2.2.1 Plan Forest Root Domain Controller Placement

Forest root domain controllers are needed to establish the forest, create AD DS trust paths for clients that need to access resources in domains other than their own, and for hosting the Operations Master Roles. These are covered in section 6.2.3.

> **Recommendations**
>
> - As a single domain forest is being recommended, this production domain is also the forest root domain
> - For both centralised and distributed implementation scenarios, there should be at least two domain controllers deployed to assume forest root functions and provide a basic level of resilience for the AD DS authentication service
> - The domain controllers covering forest root functions should, where possible, be hosted within a centralised hub or data centre location. If there is only a single central data centre, the two forest root domain controllers should be located in different physical locations to provide a degree of resilience.

It is recommended that the forest root domain controller placement design decisions are documented using the *Domain Controller Placement* job aid, named *DSSTOPO_4.doc* **{R14}**.

6.2.2.2 Plan Additional Domain Controller Placement

For cost efficiency, plan to place as few regional domain controllers as possible outside of the centralised hub or data centre. Evaluate whether a regional domain controller is required locally, based on centralised hub and distributed satellite locations within the healthcare organisation.

When planning domain controller placement, regardless of which domain it is for, it is critical to consider the following points:

- Domain controller physical security
- Remote management strategy
- WAN link availability
- Authentication availability
- Logon performance over WAN link
- Remote applications and services that depend on directory services

To help determine whether to place a domain controller at a satellite location, see the decision tree in Figure 8:

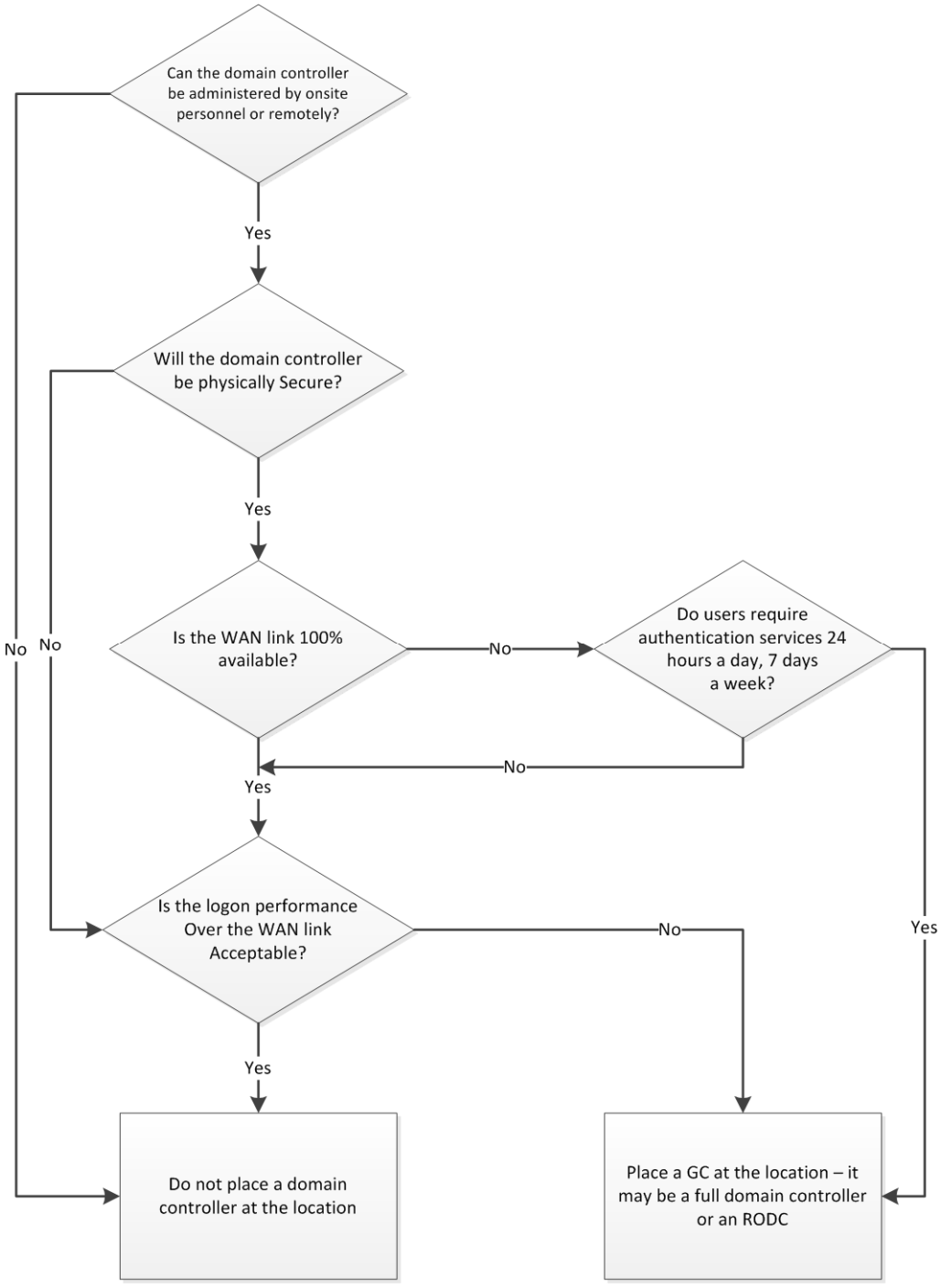


Figure 8: Determining Whether to Place Domain Controllers at Satellite Locations

Recommendations

It is possible, in small sites, to have multiple services running on a single domain controller.

Typically, these services include: AD DS-integrated DNS, WINS and DHCP. However, it is not current best practice for full read / write domain controllers to provide additional services to the network due to potential security risks. It is therefore current best practice to minimise the number of service administrators, applications and services that are installed on read / write domain controllers to help minimise these risks.

> Where this is not appropriate or is cost-prohibitive, additional measures (such as running each application in its own virtual instance on the server) should be taken in configuring the co-hosted application and operating system security policies, to mitigate the associated risk. Windows Server 2008 R2 also offers the option of deploying a Read Only Domain Controller (RODC) to further enhance the security of the domain information making the decision to host domain controller functionality on a shared physical server with other services such as DHCP and DNS. To ensure the security database integrity, Active Directory domain controllers should be located in a physically secure server room with audited access control, and kept in a locked cabinet with access restricted to the IT Administrators.
>
> Large or distributed Healthcare organisation infrastructure environments may consider the implementation of additional domain controllers after careful review of the performance requirements within the network. For example:
>
> - The user population exceeds 50 in a remote location and where they are authenticating over a low bandwidth WAN link to the hub site
> - If the users are performing network intensive transactions across a WAN link
> - Running applications that require frequent access to a domain controller or a GC

Windows Server 2008 introduces a new option to consider when planning domain controller placement, namely Read Only Domain Controllers (RODCs). The advantage of an RODC is that it performs the major functions of a domain controller by authenticating users. However, it also addresses many of the security concerns of businesses when placing domain controllers in remote locations through some specific capabilities and restrictions:

- **Read Only**: As the name suggests these are domain controllers that only provide read access to AD DS. This means that it is not possible to make changes to AD DS on a RODC and have them replicate around the rest of the domain or forest
- **Unidirectional replication**: Because RODCs will not be used to initiate any changes to AD DS, there is no need to support replication *from* an RODC. Therefore RODCs will only replicate in one direction, from a read / write domain controller. This not only applies to AD DS itself but also to the supporting services such as SYSVOL and DNS. This also helps to reduce the replication load on Bridgehead servers in the data centre as they can support more outbound replication partners or reduce the amount of time spent replicating (outbound replication is a parallel activity for a domain controller whereas inbound replication is serial)
- **Filtered Attribute Set**: Although an RODC is a fully functional domain controller it does not automatically replicate all information. To enhance the security advantages of an RODC there is a set of attributes and objects that are not replicated to an RODC. These rules are managed via the Filtered Attribute Set property of an RODC. Examples of information that is not replicated includes PKI Account credentials, BitLocker recovery information and the passwords of the built in privileged accounts such as Administrator. The RODC will cache user credentials as and when they authenticate against it thus reducing the number of users who will be at risk should an RODC be stolen or compromised. It is possible to pre-load the RODC cache to improve performance

- **Administrative Role Separation:** The design of a RODC allows for separation of administrative roles by using a separate Kerberos Key Distribution Centre (KDC) account to the one used by the read / write domain controllers. This also makes it possible to support delegating administrative privileges to non-domain administrators for the management and maintenance of the RODC without compromising the security of the domain. This makes it easier to support multiple applications and services running on a domain controller as there is no longer the same security risk
- **Security:** This is addressed in a number of ways by RODCs. Firstly they do not cache or replicate privileged account information or significant 'secrets' maintained in the domain. Secondly they will only cache a subset of users – by default only the users that authenticate against the RODC. Thirdly, in the event that an RODC is stolen or compromised there is an option to reset the password of all the user accounts whose credentials have been cached by the RODC

The capabilities introduced by RODCs add another option for AD DS administrators to provide authentication services locally to users while ensuring the security of the directory. Because RODCs provide the separation of administration capabilities, it re-opens the possibility of hosting multiple services on a single server.

It is recommended that the additional domain controller placement design decisions are documented using the *Domain Controller Placement* job aid, named *DSSTOPO_4.doc* **{R14}**.

6.2.2.3 Branch Office Infrastructure Solution

The Branch Office Infrastructure Solution (BOIS) version 3 for Microsoft Windows Server 2008 is a set of publicly available guidance, providing further design information for situations where the consideration of satellite locations needs to be taken into account. The aim of BOIS is to help in the following areas:

- More efficient use of hardware and software
- More efficient systems administration and management
- Faster and more complete recovery of data in the event of a disaster
- Higher degree of standardisation

A healthcare organisation could benefit from using the BOIS guides, in conjunction with this guidance document, to help plan for remote satellite locations which require multiple server roles to service users. BOIS can be viewed online at the Branch Office TechCenter[30] or can be downloaded from the Microsoft Download Center[31].

6.2.3 Operations Master Role Placement

Using the gathered network information used to design the site topology, plan where to locate the domain controllers that will host the operations master roles and GCs.

6.2.3.1 Determine Global Catalog Placement

Assuming the healthcare organisation follow the recommended guidance of having a single domain forest, all domain controllers can (and should) act as GCs.

[30] Branch Office TechCenter **{R32}**:
http://technet.microsoft.com/en-us/branchoffice/default.aspx

[31] Branch Office Infrastructure Solution for Windows Server 2008
http://www.microsoft.com/downloads/details.aspx?familyid=02057405-49AF-4867-BF1D-E0232B5C59E3&displaylang=en

> **Recommendation**
>
> For a single domain forest, configure all domain controllers as GC servers. In a single domain forest, the database content of a domain controller and a GC server are the same. Therefore, to load-balance client lookups across GC servers within the single domain forest, ensure that all domain controllers are configured as GCs.

If the AD DS design should vary from the single domain forest, it is necessary to determine GC placement based on the following points:

- GC-aware application presence
- The number of users at the location
- Whether the WAN link is 100 percent available
- Whether roaming users work at the location

Figure 9 displays a decision tree that may be used to determine the placement of the GC servers:

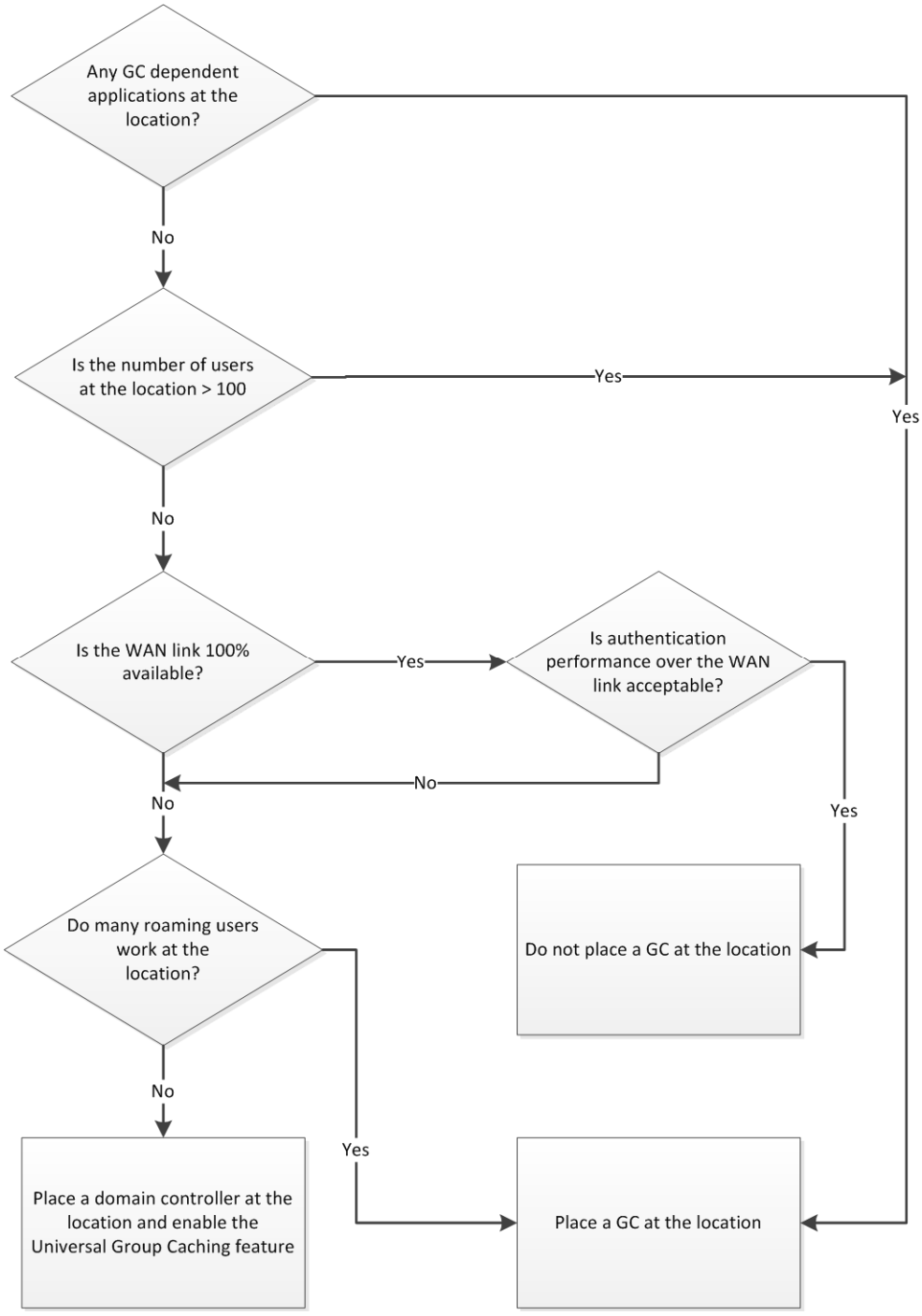


Figure 9: Determining the Placement of Global Catalog Servers

> **Recommendation**
>
> If a multiple domain forest has been deployed, the provision of GC should be further investigated[32] based on the information provided in Figure 9 to determine the requirements.

[32] Windows Server 2008 R2 AD DS Deployment Guide Web page **{R33}**: http://technet.microsoft.com/en-us/library/cc732877(WS.10).aspx

For all of the scenarios that dictate placing a GC at a location there is the further question of whether to place a full read / write domain controller or an RODC. For any situations where there is any doubt about the physical security of the domain controller or whether there is a need to provide local administration access to the server, a RODC should be considered instead of a full read / write domain controller.

It is recommended that the GC server placement design decisions are documented using the *Domain Controller Placement* job aid, named *DSSTOPO_4.doc* **{R14}**.

6.2.3.2 Determine Placement of the Operations Master Role Holders

There are five Operations Master roles within a forest. Table 16 provides details on their roles.

Operations Master Role	Role Type	Description
PDC Emulator	Domain level role	Performs a number of tasks including processing all replication requests from Microsoft Windows NT 4.0 Backup Domain Controllers (BDCs) and processing all password updates for clients that are not running AD DS client software
RID Master	Domain level role	Allocates relative identifiers (RID) to all domain controllers to ensure that all security principals have a unique identifier
Infrastructure Master	Domain level role	Maintains a list of the security principals from other domains that are members of groups within its domain
Schema Master	Forest level role	Governs changes to the schema
Domain Naming Master	Forest level role	Adds and removes Naming Contexts (such as domains), to and from the forest

Table 16: Operations Master Roles

> **Recommendations**
>
> For a single domain forest covering a healthcare organisation, it is recommended that the Operations Master roles are left on the first domain controller commissioned.
>
> If the load on an Operations Master role holder domain controller is high and causing any performance problems, then it may be necessary to relocate individual roles to separate domain controllers as per the guidance in the Microsoft Knowledge Base article 223346: *FSMO (Flexible Single Master Operations) placement and optimization on Active Directory domain controllers*[33].

[33] FSMO placement and optimization on Active Directory domain controllers **{R34}**: http://support.microsoft.com/kb/223346

Should a single domain forest implementation not be suitable, it is necessary to carefully plan the placement of the Operations Master role holders[34]. The Operations Master role loads can be determined by the identification of the following components and their effect on an Operations Master:

- Legacy clients, such as Windows NT® 4.0
- Password change forwarding and logon forwarding requests with mismatched passwords for users, computers, and service accounts
- RID and PDC emulator load/communication
- Group Policy updates
- The initial update of DFS

It is recommended that the design decisions for the Operations Master role placement are documented using the *Domain Controller Placement* job aid, named *DSSTOPO_4.doc* **{R14}**.

6.2.4 Create a Site Design

Creating a site design involves deciding which locations will become sites, creating site objects, creating subnet objects, and associating the subnets with sites.

Designing a site topology helps efficiently route client queries and AD DS replication traffic. A well-designed site topology will help the healthcare organisation achieve the following benefits:

- Minimise the cost of replicating AD DS data, for example, bandwidth, time, and effort
- Minimise administrative efforts that are required to maintain the site topology
- Schedule replication that enables locations with slow or dial-up network links to replicate AD DS data during off-peak hours
- Optimise the ability of client computers to locate the nearest resources, such as domain controllers and DFS servers, reducing network traffic over slow WAN links, improving logon and logoff processes, and speeding up file download operations

For the purposes of the site topology design within a healthcare organisation, the following guidelines should be adhered to:

- Small infrastructure environments should typically have fewer than 75 seats on a single IP Subnet on a single LAN (being determined as a network having high speed interconnects of greater than 10Mb/s) with little or no server infrastructure
- Distributed infrastructure environments should have any number of seats being spread over multiple IP Subnets or being on separate LANs interconnected by fully routed WAN connections, with or without server infrastructure

[34] Operations Master Role Placement **{R35}**: http://technet.microsoft.com/en-us/library/cc754889(WS.10).aspx

6.2.4.1 Decide Which Locations Will Become Sites

Determine the healthcare organisation's geographic locations and communication links, in particular identify the following components:

- Healthcare organisation hub location, for example, a centralised data centre
- Healthcare organisation satellite locations, for example, a distributed office location such as a General Practice clinic
- Connection type
- Available bandwidth between locations

An AD DS site design should be created based on the gathered information of the existing physical infrastructure. This requires the identification of the healthcare organisation locations that will become sites.

Figure 10 displays a decision tree that will act as an aid when deciding which locations should become sites.

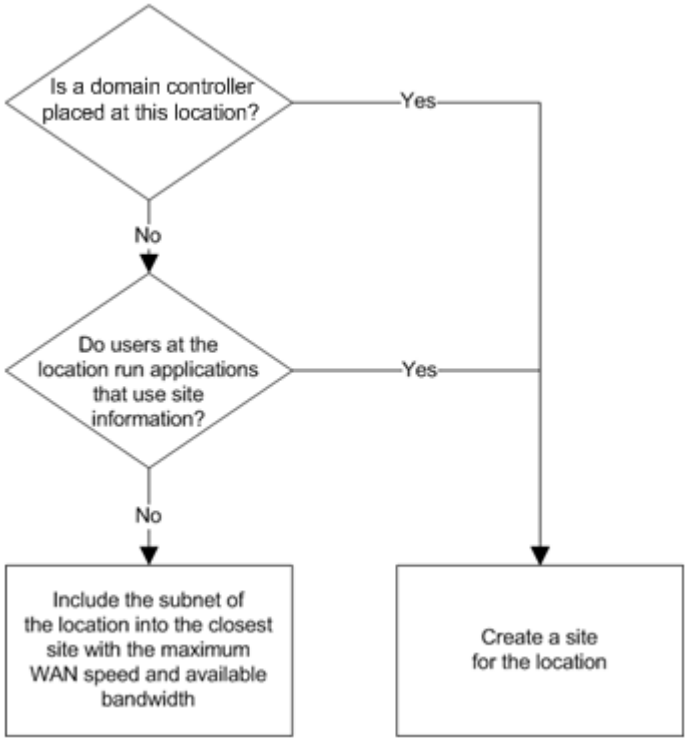


Figure 10: Deciding Which Locations Will Become Sites

Recommendations

- Create sites for all locations in which it is planned to place domain controllers
- Create sites for those locations that include servers, which are running applications that require a site to be created, for example DFS
- If a site is not required for a location, add the subnet of the location to a site for which the location has the maximum WAN speed and available bandwidth

It is recommended that site locations, including their network addresses and subnet masks, are documented using the *Associating Subnets with Sites* job aid, named *DSSTOPO_4.doc* **{R14}**.

6.2.4.2 Create a Site Object Design

It is recommended that each location where a site is to be created is documented using the *Associating Subnets with Sites* job aid, named *DSSTOPO_4.doc* **{R14}**. This job aid can then be used to create the site objects.

6.2.4.3 Create a Subnet Object Design

It is recommended that the IP subnets and subnet masks associated with each location are documented using the *Associating Subnets with Sites* job aid, named *DSSTOPO_4.doc* **{R14}**. This job aid can then be used to create the subnet objects. All subnets that are in use within the healthcare organisation should be documented and created in AD DS.

6.2.4.4 Associate Subnets With Sites

Each subnet object should be associated with a site object. It is recommended that these are documented using the *Associating Subnets with Sites* job aid, named *DSSTOPO_4.doc* **{R14}**. Subnets that are not defined within AD DS will result in event log messages on domain controllers when users authenticate at a location where the computer has an unrecognised IP address. This is unnecessary noise in the event logs that is easy to eliminate.

> **Recommendations**
>
> - For a healthcare organisation with a small centralised infrastructure environment, it is appropriate to implement a single Active Directory site
> - For a healthcare organisation whose infrastructure is physically distributed, Active Directory sites should ideally be implemented per IP subnet, where the IP subnets are configured to segregate client from server traffic on a network within a LAN environment, or where there is a network distinction of clients based on functional or geographic information that aids management of the client estate
> - It is important to ensure that all defined subnets are associated with a site. Subnets that are not directly associated with a physical location should be linked to the central hub site.

6.2.5 Create a Site Link Design

Site links reflect the intersite connectivity and method used to transfer replication traffic. It is important to connect sites with site links so that domain controllers at each site can replicate AD DS changes. Site links are used by AD DS administrators to define the preferred replication topology and the specific relationship between the individual sites.

6.2.5.1 Connect Sites With Site Links

To connect sites with site links, the sites to connect with the site link should be identified, a site link object in the respective 'Inter-Site Transports' container should be created, and the site link named. The healthcare organisation sites and associated site links should be determined and, in particular, the following components should be identified.

- Healthcare organisation site names, following the guidance given in section 6.2.4.1
- Name of site link, following the guidance given in section 6.1.7.3.6, and as documented in the *Associating Subnets with Sites* job aid, named *DSSTOPO_4.doc* **{R14}**
- Site link type. When creating the site link object, it is created in either the IP container (which associates the site link with the Remote Call Procedure (RPC) over IP transport) or the Simple Mail Transfer Protocol (SMTP) container (which associates the site link with the SMTP transport)

It is recommended that site names and associated site link names are documented using the *Site and Associated Site Links* job aid, named *DSSTOPO_5.doc* **{R14}**.

Recommendation

Site Link objects should be created in the IP container. As it is recommended that a healthcare organisation implements a single domain forest, then RPC over IP is the only site link type available at this scale.

A site link should only contain two sites: the two sites for which the explicit relationship is being defined. Although it is possible to have more than two sites in a site link, AD DS will treat all of the sites in the site link as being equally connected and will generate replication connection objects between domain controllers in each of the member sites. For the majority of AD DS installations this results in an inappropriate replication topology where domain controllers in remote sites could be attempting to replicate with each other.

6.2.5.2 Set Site Link Properties

Intersite replication occurs according to the properties of the connection objects. When the Knowledge Consistency Checker (KCC) creates connection objects, it derives the replication schedule from properties of the site link objects. Each site link object represents the WAN connection between two or more sites.

Setting the site link object properties[35] includes the following steps:

- Determining the cost that is associated with that replication path. The KCC uses cost to determine the least expensive route for replication between two sites that replicate the same directory partition
- Determining the schedule that defines the times during which intersite replication can occur
- Determining the replication interval that defines how frequently replication should occur during the times when replication is allowed, as defined in the schedule

Recommendations

- When determining the site link cost, the cost should be calculated based on the available bandwidth and not the link bandwidth of the inter-network link
- The KCC should be left on, which is the default setting. Windows Server 2008 R2 is scalable to over three thousand sites before further design consideration is required regarding switching off the KCC and manually configuring a replication topology

6.2.6 Create a Site Link Bridge Design

A site link bridge connects two or more site links. For most AD DS implementations there is no need for a site link bridge especially if they are single domain forests. In cases where there are multiple domains in a forest distributed across multiple physical locations where some of those physical locations have only a single domain controller, it may be necessary to implement site link bridges to ensure that full replication can be achieved.

Recommendation

By default, all site links are transitive and it is recommended this is left enabled. However, occasionally it may be necessary to disable 'Bridge all site links' for replication and complete a site link bridge design if either of the following applies:

- The IP network is not fully routed
- It is necessary to control the replication flow of the changes made in AD DS, such as controlling replication failover, or Active Directory replication through a firewall

[35] Site Link Properties **{R36}**:
http://technet.microsoft.com/en-us/library/cc753700(WS.10).aspx

Currently the DFS topology generation and 'next closest site' features require that the Bridge all Site Links option remains enabled. A new switch has been introduced to repadmin.exe to allow the DFS topology generation to continue while disabling the Active Directory replication site link bridging topology. If the circumstances require the DFS topology generation but not the Active Directory site link bridging feature, the site link bridging option should be left enabled and the following command run for each site that is affected:

```
C:\Windows> repadmin /siteoptions <domain controller> /site:<site name>
+W2K3_BRIDGES_REQUIRED
```

If required, the site link bridge requirements should be determined, based on network connectivity and the site link bridge design. For instance, the requirements would need to be identified for the following scenarios[36]:

- Disjointed networks
- Control of the AD DS replication flow

6.2.7 Domain Controller Hardware Availability and Scalability Requirements

Planning domain controller capacity helps determine the appropriate number of domain controllers to place in each domain that is represented in a site. Capacity planning also assists in estimating the hardware requirements for each domain controller, enabling the cost to be minimised and an effective service level to be maintained for the healthcare organisation users. When planning the domain controller hardware it is worth noting that Windows Server 2008 R2 is only available as a 64 bit operating system. Depending upon the domain controller requirements it may be possible to reduce the overall number of domain controllers required as the capacity and performance of 64 bit servers exceeds those of 32 bit servers.

6.2.7.1 Determine Domain Controller Capacity

Before planning domain controller capacity, the Active Directory site topology design must be complete. Part of designing site topology involves deciding which locations require domain controllers and what type of domain controllers are required in each location. After designing the site topology, planning the domain controller capacity will help to determine the number of domain controllers that are needed in each domain for each site, and the hardware that is required for each domain controller. Various elements can affect the performance of a domain controller and, in turn, influence the domain controller capacity[37].

[36] Creating a Site Link Bridge Design **{R37}**:
http://technet.microsoft.com/en-us/library/cc753638(WS.10).aspx

[37] Background Information for Planning Domain Controller Capacity **{R38}**:
http://technet2.microsoft.com/windowsserver/en/library/52bf61a8-9845-4878-8fa4-a85c57fe25e51033.mspx

6.2.7.2 Determine Minimum Number of Domain Controllers Required

To maintain an effective service level, a sufficient number of domain controllers should be placed in each domain in a site, thus allowing the number of users that are also within each domain in that site to be supported. The identification of inbound and outbound replication requirements should be understood, adding domain controllers to support replication between sites if required[38].

As each healthcare organisation is different, it is not possible to place actual recommendations for the number of domain controllers that will be required. However, the following guidance may help a healthcare organisation to understand the hardware which may be required to support a certain number of users within a site:

- The Domain Controller Capacity Test Configurations information, as provided in the Windows Server 2003 Deployment Guide article: *Determining the Minimum Number of Domain Controllers Required*[39]

> **Important**
>
> Following the guidance in this section will allow a healthcare organisation to estimate the number of domain controllers required with a given configuration, but this should only be used as a guideline. Any design decisions regarding the hardware chosen should be tested thoroughly in an isolated environment which, as much as possible, matches the live environment where AD DS will be implemented.

6.2.7.3 Determine Disk Space and Memory Requirements

Underestimating hardware requirements can cause poor performance and application response time, and can prevent users from quickly logging on to the network to access resources.

The required disk space and memory requirements for each domain controller should be determined, taking into account that this may vary according to the following:

- GC distribution
- AD DS application partition requirements
- Memory and large memory support requirements

The number of users per domain in a site should be used to determine the minimum memory requirements for each domain controller in that domain. Table 17 provides details of the minimum memory requirements per domain controller.

Users per Domain in a Site	Minimum Memory per Domain Controller
1 – 499	512 MB
500 – 999	1 GB
1000 – > 10000	2 GB

Table 17: Minimum Memory Requirements per Domain Controller

Domain controllers require at least enough disk space for the AD DS database, AD DS log files, the SYSVOL shared folder, and the operating system.

[38] Adding Domain Controllers to Support Replication Between Sites **{R39}**: http://technet2.microsoft.com/windowsserver/en/library/4a59cc62-9425-463f-89b6-95347e2ea91e1033.mspx

[39] Determining the Minimum Number of Domain Controllers Required **{R40}**: http://technet2.microsoft.com/windowsserver/en/library/2619a7f0-c6ab-435a-83db-34f1425107e71033.mspx.

Recommendations

- On the drive that will contain the AD DS database, NTDS.dit, 0.4 GB of storage for each 1,000 users should be made available
- On the drive that will contain the AD DS transaction log files, at least 500 MB of space should be made available
- On the drive that will contain the SYSVOL shared folder, at least 500 MB of space should be made available
- On the drive that will contain the Windows Server 2008 R2 operating system files, at least 20 GB of space should be made available
- When selecting suitable hardware for providing the AD DS, consideration should be given to ensuring resiliency within the server components, including network interfaces, power supply units, processors, memory, hard drives, and the provision of out-of-band management
- Sufficient air conditioning, power and network (where possible resilient in-band connections and out-of-band management network) provisioning should be planned and implemented as part of a capacity management process

When configuring the hard disk space on a domain controller, the data types should be segregated by operating system, security database and SYSVOL, and logs, and allocated to separate volumes for storage.

Recommendations

- To prevent single disk failures, a Redundant Array of Independent Disks (RAID) should be used
- For domain controllers that are accessed by fewer than 1,000 users, all four components may be located on a single RAID 1 array
- For domain controllers that are accessed by more than 1,000 users, the log files should be placed on one RAID array and the SYSVOL shared folder and the database should be kept together on a separate RAID array, as specified in Table 27

It is recommended that the hardware requirements are documented using the *Hardware Assessment* job aid, named *DSSTOPO_5.doc* **{R14}**.

6.3 Design for AD DS Security

To plan a secure environment, it is vital to have a clear and consistent strategy for addressing the many aspects of the Microsoft Windows Server 2008 R2 operating system, including security-related issues and features. Firstly, the user-related requirements that impact security should be identified, together with the other aspects of the network that comprise a secure common infrastructure.

6.3.1 Plan a Secure AD DS Environment

The Windows Server 2008 R2 AD DS security planning process is based on a high-level view of the security configuration options and capabilities. The security planning process is based on two organising principles:

- **Users need access to resources** – This access can be very basic, including only desktop logon and the availability of Access Control Lists (ACLs) on resources. It may also include optional services, such as remote network logons, wireless network access, and access for external users, such as business partners or customers
- **The network requires a secure shared IT infrastructure** – This infrastructure includes security boundaries, secure servers and services, secure networking, and an effective plan for delegating administration

Used together, the two principles of network operating system security can provide the trust and integrity needed to help secure complex operating environments. By using a security planning process to analyse the security requirements of a healthcare organisation deploying AD DS, it is possible to establish a high-level security framework for the Windows Server 2008 R2 deployment.

> **Important**
>
> This security planning process is not intended to replace a detailed assessment of existing security systems, gaps, and solutions.

A breach in AD DS security may result in the loss of access to network resources by legitimate clients, or the inappropriate disclosure of potentially sensitive information.

The Best Practice Guide for Securing Active Directory Installations[40] whitepaper provides detailed technical information covering the following components of AD DS security:

- Planning in-depth AD DS security
- Establishing secure AD DS boundaries
- Deploying secure domain controllers
- Securing DNS
- Strengthening domain and domain controller policy settings
- Establish secure administrative practices

> **Recommendation**
>
> Ideally, there should be very few service administrators who use highly privileged accounts. All other AD DS tasks should be related to data-based administration, and delegated out appropriately on the principle of 'least privilege'. This model of AD DS administration helps maximise security. For more information see the whitepaper: *Best Practices for Delegating Active Directory Administration*[41] and the notes on user accounts earlier in this document {6.1.7.3.1}.

6.3.1.1 Address User-Related Requirements

User-related requirements are essential considerations in network design. There are security requirements associated with almost every user-related design decision that needs to be made.

The following items are key security-related user requirements that each healthcare organisation must address:

- Keyboard logons which require an authentication strategy design (see section 6.3.2)
- Access to resources which require a resource authorisation strategy design (see section 6.3.3)

It may be necessary for Healthcare organisations to implement other security-related requirements that are not as universally applicable[42], for example:

- Remote network access
- Wireless network access

---

[40] Deployment Whitepaper: Best Practice Guide for Securing Active Directory Installations **{R41}**: http://technet2.microsoft.com/windowsserver/en/library/edc08cf1-d4ba-4235-9696-c93b0313ad6e1033.mspx?mfr=true

[41] Best Practices for Delegating Active Directory Administration **{R42}**: http://go.microsoft.com/fwlink/?LinkID=22708

[42] Addressing User-Related Requirements **{R43}**: http://technet2.microsoft.com/windowsserver/en/library/a35e88e7-2504-4a60-ba78-7c9efa05d3fa1033.mspx

- Standard Client configurations (see the *Automated Build Healthcare Desktop and Server Guide* **{R30}** and the *Group Policy for Healthcare Desktop Management* **{R20}**)
- Encrypting File System (EFS) (see the *Healthcare EFS Tool Administration Guide* **{R44}**)
- Extranet access

6.3.1.2 Establish a Secure Shared IT Infrastructure

Not all security-related features apply directly to users. Many basic network services and configuration decisions involve creating and defining explicit boundaries, securing network traffic, and securing the servers.

It is very important to prevent unauthorised users from viewing data, even if they gain physical access to the server. It is advised that the following points are identified and planned for:

- Securing domain controllers against physical access
- Preventing domain controllers from booting into alternate operating systems
- Protecting domain controllers on restart by using syskey
- Securing backup media against physical access
- Enhancing the security of the network infrastructure
- Securing the remote restart of domain controllers
- Securing service administrator accounts
- Securing the workstations belonging to service administrators
- Avoiding the delegation of security-sensitive operations

> **Recommendations**
>
> Active Directory domain controllers maintain sensitive security information for all users within the forest and, therefore, should be housed in a physically secure environment.
>
> AD DS is backed up as part of System State, which includes the database, log files, registry, system boot files, COM+ Registration Database, and System Volume (Sysvol). Therefore, it is critical that these volumes be backed up and restored as a set. Backup and restore plans help to ensure service continuity in the event of a directory issue. These backups should be stored in a physically secure location, both onsite and offsite.

6.3.2 Design an Authentication Strategy

Most healthcare organisations need to support seamless access to the network for multiple types of users. At the same time, the healthcare organisation needs to protect the network resources from potential intruders. A well-designed authentication strategy can help achieve this complex balance between providing reliable access for users and strong network security.

Designing an authentication strategy involves:

- Evaluating the existing infrastructure and account creation process
- Establishing a means of securing the authentication process
- Establishing standards for network authentication and time synchronisation

6.3.2.1 Create a Foundation for Authentication

When designing an AD DS solution, it is necessary to create a foundation for secure authentication of users, computers, and services which require authorisation to access resources within the appropriate healthcare organisation level. As such, the following must be included in the design process[43]:

- Evaluation of the current environment
- Creation of user accounts
- Creation of a user account management plan, including creating, disabling and resetting user accounts
- Creation of a computer account management plan, including creating, deleting and resetting computer account passwords
- Creation and security of service accounts, including the local service and network service built in accounts
- Application of authentication policies to groups

It is recommended that the design decisions are documented using the *Authentication Strategy Planning* job aid, named *DSSAUT_1.doc* **{R14}**.

6.3.2.2 Secure the Authentication Process

It is important to secure the authentication process to protect the system against various security threats, such as password cracking tools, brute force or dictionary attacks, abuse of system access rights, impersonation of authenticated users, and replay attacks. The following areas of an authentication process should be considered:

- Assign logon hours
- Create a ticket expiration policy
- Establish network authentication standards
- Set clock synchronisation tolerance to prevent replay attacks
- Review the Default Domain Policy GPO:
  - Create a strong password policy for the domain
  - Establish an account lockout policy for the domain
  - Create a Kerberos ticket expiration policy
- Review the Default Domain Controllers Policy GPO:
  - Review domain controller audit policy settings
  - Strengthen domain controller user rights assignment policy settings
  - Strengthen domain controller security options policy settings
  - Strengthen domain controller event log policy settings

[43] Creating a Foundation for Authentication **{R45}**: http://technet2.microsoft.com/windowsserver/en/library/2df33645-5e3e-4b79-9733-ffa2a3cf60c41033.mspx

> **Recommendation**
>
> The points above are the only settings that should be altered within the Default Domain Policy (DDP) and Default Domain Controller Policy (DDCP), all other settings to be applied at these levels should be contained within new GPOs. For further detailed information, see the *Group Policy for Healthcare Desktop Management* **{R26}** guidance document.

The design decisions can be documented using the *Authentication Security* job aid, named *DSSAUT_2.doc* **{R14}**.

It is also critical to strengthen DC policy settings. This can be achieved by utilising The Microsoft Security Configuration Wizard (SCW).

> **Recommendations**
>
> The SCW, supplied as part of the Windows Server 2008 R2 operating system, can be used to help configure the appropriate settings[44].
>
> For baseline security policies refer to the Microsoft Security Reference Framework Toolkit which provides guidance on establishing a secure baseline for users, workstations and servers based on Microsoft recommended practices.

The SCW reduces the attack surface for computers running Windows Server 2008 R2 or later. It determines the minimum functionality required for a server's role or roles, and disables functionality that is not required. Specifically, the SCW assists in authoring a security policy that:

- Disables unneeded services
- Blocks unused ports
- Allows additional address or security restrictions for ports that are left open
- Reduces protocol exposure to Server Message Block (SMB), LAN Manager, and Lightweight Directory Access Protocol (LDAP)
- Defines a high signal-to-noise audit policy[45]
- Guides through the process of creating, editing, applying, or rolling back a security policy based on the selected roles of the server

The deployed group policy settings can be documented using the HTML reports available within the GPMC.

It is also possible to create a GPO from the SCW settings that can be linked to the domain or an OU to provide a centrally managed and administered way for applying the configuration settings. It should be noted that the default settings for Windows Server 2008 R2 are very secure. Installation of additional services or applications that are part of the operating system is through the Server Manager application. These new services and applications are referred to as Roles and Role Services in Windows Server 2008 and Windows Server 2008 R2. Part of the installation of a Role or role service includes adding any new firewall port rules to the server on which the Roles or Role Services are installed. If a role or role service is removed these required firewall port rules are removed.

[44] Deployment Guide for the Security Configuration Wizard **{R46}**: http://technet2.microsoft.com/windowsserver/en/library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and http://technet.microsoft.com/en-us/library/cc731515(WS.10).aspx

[45] A high signal-to-noise audit policy is one that provides useful audit information whilst minimising the information commonly retrieved with it which is not regarded as useful.

6.3.2.3 Extend the Authentication Framework

If more than one Active Directory forest is deployed and it is determined that resource access is required between forests, then it is necessary to extend the authentication framework[46]. This can be accomplished by creating trust relationships and additional accounts, as appropriate, covering the following requirements:

- Establish inter-forest authentication
- Enable interoperability with Kerberos clients and servers running other operating systems

It is recommended that the design requirements are documented using the *Extended Authentication Framework* job aid, named *DSSAUT_3.doc* **{R14}**.

6.3.2.4 Educate Users about the Authentication Process

It is important that, once the authentication process has been designed, it is communicated to users, such that they can be educated as to their own role in the authentication process. Ensuring that users are aware of the guidelines in creating passwords and the reasons behind the process being implemented, can reduce the chances of users sharing their credentials or leaving them written down where others have access to it.

6.3.3 Design a Resource Authorisation Strategy

Logging on does not automatically give users access to the resources they require. Users must be authorised to access specific resources, but only at the level of access they need. Moreover, many users have identical needs for access to a network resource. For example, all users in the clerical administration department of a hospital might need access to a specific colour printer, so it is possible to easily manage access by putting every member of the clerical administration department into a security group that is authorised to access that printer.

Because security groups are so critical for controlling access, they form the main component of the authorisation strategy. Consequently, it is important to know what security group types are available and how they should be used.

By applying this information appropriately, a healthcare organisation can design a resource authorisation strategy that is scalable, easy to maintain, and cost effective.

6.3.3.1 Establish a Resource Authorisation Method

Depending on the resource and the needs of the healthcare organisation, access to shared resources should be setup by applying any or all of the following authorisation methods:

- **Account Group/ACL (AG/ACL) method** – Security groups, rather than individual user accounts, are added to the resource ACL, and the group is given a set of access permissions
- **Account Group/Resource Group (AG/RG) method** – Users with similar access requirements are grouped into account groups. The account groups are then added to a resource group that has been granted specific resource access permissions
- **Role-based authorisation** – Often uses scripts, called authorisation rules, or third-party tools to enable users with similar roles to be authorised to perform predefined sets of tasks in specific applications

[46] Extending Your authentication Framework **{R47}**: http://technet2.microsoft.com/windowsserver/en/library/1d90e7c1-37e3-4efe-bf64-1b9ffa93b1a71033.mspx and supplementary information for Windows Server 2008 and Windows Server 2008 R2 http://technet.microsoft.com/en-us/library/dd548350(WS.10).aspx

Recommendations

For small, centrally managed healthcare organisations it is most appropriate to use the AG/RG resource authorisation model. In which case, the local groups or domain local groups should be selected as the resource groups.

For larger, distributed healthcare organisations, it is more appropriate to use the role-based authorisation method using the Authorization Manager **{R7}**.

6.3.3.2 Define Policies for Security Group Management

Policies for security group management are a significant part of the resource authorisation strategy. It is important to establish a policy defining who can create security groups and when they should be created. It is also important to define the following policies[47]:

- Security group creation policy, including which members are allowed to create new security groups, and the process used to create them
- Security group naming policy, using the information provided in section 6.1.7.3.2
- Security group retirement policy, including when security groups become obsolete as these should be identified and retired (deleted) to minimise security risks
- Security group nesting policy. Security group nesting occurs when one security group is made a member of another security group, and the nested group inherits all of the privileges and permissions that are granted to the parent

Important

Unrestrained group nesting can result in access token size problems as the token contains the SIDs for each group of which the user is a member, either directly or indirectly. The default group membership limitation is 120 groups[48]. This can also be impacted in cases where users have been migrated into the new forest and maintained SID History. The SIDs that are migrated over as part of SID History will also be included in the access token further increasing the size.

6.3.3.3 Delegate Policies for Security Group Management

In large AD DS deployments, it is appropriate to delegate the ability to perform routine membership maintenance on groups, and the ability to administer the ACLs and resource groups for resources. Policies for security group management should be defined, considering the following points:

- Identify individuals to maintain security groups
- Delegate account group maintenance
- Delegate resource group maintenance

6.3.4 Design a Public Key Infrastructure

Microsoft Windows Server 2008 R2 enables a variety of secure applications and business scenarios based on the use of digital certificates. Before it is possible to use digital certificates, it is necessary to design a PKI, which involves planning configuration options for one or more certification authorities, preparing certificates to meet the needs of the healthcare organisation, and creating a PKI management plan.

[47] Defining Policies for Security Group Management **{R48}**: http://technet2.microsoft.com/windowsserver/en/library/033a0042-ff57-4657-8350-c7a6ebe3b8991033.mspx

[48] Selecting Local Groups or Domain Local Groups as Resource Groups **{R49}**: http://technet2.microsoft.com/windowsserver/en/library/1b3070ce-c6b1-4849-ae47-ce17bbec17ee1033.mspx

A PKI based on Microsoft Windows Server 2008 R2 Certificate Services provides a means to perform tasks such as:

- Digitally signing files, including documents and applications
- Securing e-mail from unintended viewers
- Enabling secure connections between computers, even if they are connected over the public Internet or through a wireless network
- Enhancing user authentication through the use of smart cards

It is out of the scope of this document to detail the information required to fully understand PKI, and therefore provide recommendations. However, a high-level review of the interdependent processes required to create a PKI is listed below:

- Defining certificate requirements. It is recommended that these are documented using the *Summary of User Certificate Requirements* and *Certificate Practice Statement Outline* job aids named DSSPKI_1.doc and DSSPKI_2.doc respectively **{R14}**
- Designing the Certificate Authority (CA) infrastructure
- Extending the CA infrastructure
- Defining certificate configuration options and documenting the certificate lifecycle plan using the *Windows Server 2003 Certificate Lifecycle Plan* job aid DSSPKI_3.doc **{R14}**
- Creating a certificate management plan
- Deploying the PKI

6.4 Design Network Services to Support AD DS

In an IT environment, users need to make use of resources such as file and print services, authentication services, email and messaging services, and access to enterprise applications. In addition, for the resources of one computer or device to access another, they need to be able to identify and reference each other. There are two primary name resolution services used on Windows networks: DNS and WINS. DNS is essential for AD DS as all resources are registered with DNS and it provides the naming standards for the directory. DNS is a host name resolution service that is the standard service used across private TCP/IP networks and public networks such as the Internet. Without DNS AD DS will not function. Since Windows 2000 when Active Directory was first introduced, Windows clients and servers have used DNS as the primary name resolution service.

WINS (Windows Internet Name Service) is the Microsoft implementation of a NetBIOS name resolution service. Historically Windows based networking used NetBIOS as the foundation for service location and network access. WINS provides a distributed NetBIOS name resolution service to support applications and services that rely on NetBIOS name resolution. On the whole, Windows-based networks no longer require NetBIOS name resolution services as the dependencies on the underlying technology have been gradually removed. However, in a mixed infrastructure where there are still Windows NT-based machines, legacy applications or down level, external trusts it is likely that there will be a requirement for a WINS infrastructure. Because the reliance on WINS has diminished significantly the WINS infrastructure will almost certainly be small, possibly consisting of a single, centralised implementation. Because there may be some legacy clients and applications still in the environment, WINS is discussed in section 6.4.2.

All other network services that are not specifically related to the requirements of AD DS are considered out of scope for this guidance.

6.4.1 DNS Infrastructure to Support AD DS

After creating the Active Directory forest and domain designs, it is necessary to design a DNS infrastructure to support the AD DS logical structure. DNS provides a mapping of computer names to IP addresses in a distributed network environment, allowing connectivity between computers and other resources using names on IP networks.

Windows Server 2008 R2 uses DNS for name resolution, instead of the WINS NetBIOS name resolution method used in Windows NT 4.0-based networks. A WINS infrastructure is still required to support NetBIOS based applications, but AD DS specifically requires DNS.

The process for designing DNS to support AD DS within a healthcare organisation will vary according to whether or not there is an existing DNS infrastructure. This section focuses on implementing a DNS service to support AD DS, and provides guidance around integrating this with an existing DNS infrastructure.

The DNS solution for a healthcare organisation will depend very much on the requirements and the existing infrastructure. If there is no existing DNS solution then the recommendation is to use the DNS service that comes as part of the Windows Server 2008 R2 Operating system. This has all the features that AD DS needs and can make use of all the benefits that the Windows-based service offers such as AD DS integration and secure dynamic updates. For healthcare organisations that already have a DNS solution there are several options:

- **Use the existing DNS solution to manage DNS for AD DS**: If the existing DNS solution is robust, reliable and well configured it can be used to support AD DS provided it supports Service Location Records (SRV). It is even better if it supports dynamic updates as this makes the maintenance of the DNS information easier. If the DNS solution does not support dynamic updates it is essential that the AD DS related DNS entries are regularly and accurately maintained. Each domain controller writes to a local file all of the DNS entries that it expects to see in DNS. The file is netlogon.dns and is located in the Windows\System32\Config folder
- **Use the existing solution as it is but use Windows DNS for AD DS**: As the existing DNS solution is already configured for the environment and is working it can be left as it is and a delegation to the Active Directory namespace created. This would then allow the healthcare organisation to use the Windows DNS service to manage AD DS and to make use of all the Windows DNS features without impacting the existing DNS solution. The Active Directory namespace can then forward to the existing, internal DNS infrastructure
- **Use the Windows DNS service for everything**: The existing DNS solution may be old or expensive to maintain. In these cases the whole DNS infrastructure can be moved over to the Windows DNS service. The existing zones and host records can be imported into the Windows DNS service and it can be used for all name resolution throughout the healthcare organisation

> **Recommendation**
>
> Active Directory namespace planning and DNS planning should be approached separately, as there may be separate requirements for each. Before finalising any DNS design however, it is important to reconcile the approaches.
>
> Where possible use the Windows DNS service to support AD DS for the best levels of integration and reporting on the state of the service as well as making the most of the Windows DNS service features and capabilities.

6.4.1.1 Review Domain Name System Concepts

DNS is a critical service for the successful implementation of AD DS, and requires careful design and deployment. It is recommended that core DNS concepts, such as delegation and recursive name resolution, are reviewed[49].

6.4.1.2 Review Domain Name System and Active Directory

Review DNS specifically, as it relates to AD DS, focusing particularly on the following design considerations:

- Domain controller location
- DNS name server location
- AD DS integrated zones
- Computer naming

> **Recommendations**
>
> - For smaller to mid size environments consider installing the DNS service on every domain controller in the forest
> - Larger environments will need to consider only deploying the Windows DNS service on a carefully chosen subset of domain controllers to maintain the efficiency and performance of the DNS service
> - Use AD DS integrated DNS zones
> - Configure all DNS zones to allow dynamic updates, preferably secure dynamic updates
> - Ensure that domain names are registered with the proper Internet authorities (see the current best practice naming standards guidance in section 6.1.7 for more information)

These recommendations provide the following benefits:

- Enabling of fault tolerance across a uniform domain controller configuration, with a centrally managed, yet distributed, name resolution service that will be available alongside local authentication services
- Integrating DNS with AD DS enables DNS servers to take advantage of the security, performance, and fault tolerance capabilities of AD DS
- Microsoft DNS provides efficient name resolution and interoperability designed to fully support all AD DS DNS requirements. It is also based on recognised industry standards-based technologies

The AD DS DNS owner is responsible for the AD DS DNS design and responsible for overseeing the deployment of AD DS DNS for the forest

> **Recommendations**
>
> - Ensure that an AD DS DNS Owner role is identified and someone is assigned to it
> - Ensure that DNS management permissions are delegated appropriately, and that DNS management processes are understood, documented and followed

> **Note**
>
> Any DNS server that supports AD DS can be implemented as long as it supports Service (SRV) records[50]. It is also strongly recommended that the DNS server supports secure Dynamic Updates[51], which requires Berkeley Internet Name Domain (BIND) version 8.2.2, patch 7 or later[52].

[49] DNS Concepts **{R51}**:
http://technet.microsoft.com/en-us/library/dd197461(WS.10).aspx

6.4.1.3 Identify the Domain Name System Infrastructure Requirements

DNS forwarding and conditional forwarding pointers should be configured appropriately. This allows for the required communication internally between healthcare organisations and for directing appropriate external traffic. Conditional forwarding can also be used which enables a DNS server to forward DNS queries based on the DNS domain name in the query.

> **Recommendations**
>
> - All domain controllers should be configured to forward to the existing DNS infrastructure if one exists.
> - Where possible domain controllers should not be configured to resolve names that are external to the healthcare organisation
> - The DNS root zone should be removed from the DNS hierarchy if it has been installed. This is typically a feature that occurred in Windows 2000 Server. This zone indicates that the server is acting as a root Internet server, and therefore the DNS server does not use forwarders or root hints in the name-resolution process. To ensure that an internal DNS server forwards queries appropriately within the infrastructure and to internal Internet facing DNS servers, it is important to delete the root '.' (also known as 'dot') zone. This also allows for future integration of healthcare organisations.

AD DS integrated DNS should utilise the appropriate DNS application directory partitions. These enable setting of the appropriate replication scope for AD DS integrated DNS data. By limiting the scope of replication traffic to a subset of the servers running AD DS in the forest, it is possible to reduce replication traffic and also help to keep the Global Catalog size down in cases where there are multiple domains in a forest.

> **Recommendation**
>
> Ensure that the DNS application partitions are used for controlling the replication scope.

If the Healthcare organisation's Active Directory forest is configured with more than one domain, then careful planning of the _msdcs zone is required.

> **Recommendation**
>
> The _msdcs zone should be hosted in the forest-wide DNS application directory partition, thereby replicating to every DNS server in the forest and enabling clients to find GC servers and all other forest-wide resources. This configuration provides replication and security benefits. However if a Microsoft DNS or BIND infrastructure has already been deployed to support an existing AD DS, then the _msdcs zone must be appropriately delegated to allow resolution throughout the forest.

Ensure that the Active Directory namespace is securely configured such that it is not externally visible.

[50] RFC 2782 – A DNS RR for specifying the location of services (DNS SRV) **{R52}**

[51] RFC 2136 – Dynamic Updates in the Domain Name System (DNS UPDATE) **{R53}**

[52] Configuring BIND to work with Microsoft Active Directory **{R54}**: http://www.microsoft.com/technet/archive/interopmigration/linux/mvc/cfgbind.mspx

Recommendation

The Active Directory namespace should only be visible on the internal network with no external presence. Without proper name resolution, users may not be able to locate resources on the network. It is critical that the organisation's Internet facing DNS namespace does not conflict with their internal Active Directory namespace.

Where possible split brain DNS installations should be avoided. This is where the same domain name is shared between different DNS servers. It occurs where an organisation gives its AD DS the same name as its external DNS name, for example the external DNS name of a healthcare organisation is *exampleHealthOrg.org.com* and the Active Directory forest name is *exampleHealthOrg.org.com*. This situation provides extra administration work and can be easily avoided by ensuring the Active Directory name is unique such as a delegated name from the public namespace, for example, *HealthOrgAD.exampleHealthOrg.org.com*.

The Secure Dynamic Updates setting allows only the computers and users specified in an ACL to modify objects within a DNS zone. This enhances the consistency and security of the DNS infrastructure, whilst maintaining the flexibility offered by dynamic update.

Recommendation

Secure dynamic updates should be enabled[53] on DNS zones. By default, this allows members of the Active Directory forest and domain to register and update DNS records in the zone, but can be extended if required.

DNS Ageing and Scavenging can be configured to allow automatic clean-up and removal of stale resource records (RRs), which can accumulate in zone data over time. To ensure that the scavenging is most effective this should be enabled on the zone before any host records are added to it. To configure scavenging ensure:

- The zone is configured to scavenge stale records
- The specific domain controllers that will perform the scavenging are configured

Recommendation

Ageing and Scavenging for DNS should be enabled on two domain controllers (running the DNS Server service) per domain. Although it is only necessary to enable it on a single domain controller, by selecting two the solution is providing for fail-over of the scavenging activity.

A DNS client configuration for both the DNS servers and all of their clients should be created. It is recommended that this is documented using the *DNS Inventory* job aid, named DSSLOGI_8.doc **{R14}**.

Recommendations

The DNS client configuration for each domain controller should be configured to use itself as the primary DNS server, and an alternative DNS server in the same site or hub site should be configured as the secondary DNS server.

All other network devices, for example member servers, and Windows XP, Windows Vista or Windows 7 clients, use a local domain controller as their primary DNS server, and their secondary DNS server is configured as a domain controller in another AD DS site preferably the nearest data centre.

DNS and NetBIOS names for each domain have been determined during section 6.1.3 and documented using the *Domain Planning* job aid, named DSSLOGI_5.doc **{R14}**. See section 6.1.7 for specific guidance on DNS naming standards.

[53] Microsoft Knowledge Base article 816592 – *How to configure DNS dynamic updates in Windows Server 2003* **{R55}:** http://support.microsoft.com/kb/816592

6.4.1.4 Integrate AD DS into an Existing Domain Name System Infrastructure

There are three likely scenarios for DNS configuration within a healthcare organisation. Table 18 provides recommendations for how to deal with these scenarios.

DNS Scenario	Recommendation
No existing DNS	▪ Host all Healthcare organisation's local DNS requirements on the AD DS integrated DNS ▪ Forward any unresolved queries to the Local Service Provider's (LSP's) DNS infrastructure ▪ Create a stub zone or delegation in the LSP DNS infrastructure for the Healthcare organisation's AD DS DNS zone
Existing Windows based DNS (NT4.0, 2000 or 2003)	▪ Host only Active Directory DNS requirements on the AD DS integrated DNS ▪ Consider consolidating all DNS services to AD DS integrated DNS on the DCs ▪ Configure Active Directory DNS to forward all unresolved queries to either the local Healthcare organisation DNS service if not consolidated, or the LSP DNS service if the DNS infrastructure has been consolidated ▪ Create a stub zone or delegation in the LSP DNS infrastructure for the Healthcare organisation's AD DS DNS zone
Existing Unix based DNS	▪ Host only Active Directory DNS requirements on the AD DS integrated DNS ▪ Configure AD DS DNS to forward all unresolved queries to the Unix based DNS in the Healthcare organisation ▪ Create a stub zone or domain delegation in the Unix DNS for the Healthcare organisation's AD DS DNS zone

Table 18: Existing Domain Name System Scenarios and Subsequent Recommendations

6.4.2 WINS Infrastructure to Support AD DS

WINS servers map IP addresses to NetBIOS computer names and NetBIOS computer names back to IP addresses.

6.4.2.1 WINS and Windows Server 2008 R2 AD DS

WINS[54] and NetBIOS are not required in an environment where computers run only Windows Server 2008, Windows Server 2003 or Windows 2000, but WINS is required for interoperability between Windows 2000-based domain controllers, computers that are running earlier versions of Windows, and applications that depend on the NetBIOS namespace. For example, applications that call NetServerEnum, and other 'Net*' Application Programming Interfaces (APIs), that depend on NetBIOS.

[54] Deploying WINS **{R56}**: http://technet2.microsoft.com/windowsserver/en/library/a5e0f87f-9b40-47ed-b613-3b4963bd91e61033.mspx and http://technet.microsoft.com/en-us/library/cc771750(WS.10).aspx

Recommendation

The use of WINS in the infrastructure should be assessed and minimised where possible, as products exist that still require NetBIOS name resolution in order to function correctly. It is advised that, during upgrade phases, healthcare organisations remove older applications and operating systems that require NetBIOS functionality from the environment. In the meantime, it may be necessary to provide WINS as a method for NetBIOS name resolution so that clients can locate older services through a server's NetBIOS name.

If a WINS infrastructure is needed, it should be kept as simple and efficient as possible. It may be possible that just two WINS servers in the data centre that are configured as push / pull replication partners proves to be enough to support the entire NetBIOS name resolution requirements for the Healthcare organisation.

6.4.3 Additional Network Services

In provisioning an infrastructure environment, an appreciation of the following network services is required:

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Dynamic Host Configuration Protocol (DHCP)
- Internet Protocol Security (IPSec)
- Dial-up and Virtual Private Network (VPN)
- Wireless LAN

Guidance on these technologies can be obtained from:

- Windows Server 2003 Product Documentation **{R7}**
- Windows Server Systems Reference Architecture **{R1}**
- Windows Server 2003 Deployment guide **{R2}**
- TechNet Technology Collections **{R3}**

Note

Services mentioned within this section will not be available between healthcare organisations that have identical IP Address schemes. The use of NAT as a workaround between such healthcare organisations within an AD DS Environment is neither recommended nor supported by Microsoft.

For further information please read the Assumptions statement in section 2.5, and the Microsoft whitepaper: *Active Directory in Networks Segmented by Firewalls*[55].

[55] Active Directory in Networks Segmented by Firewalls **{R57}**: http://www.microsoft.com/downloads/details.aspx?FamilyID=c2ef3846-43f0-4caf-9767-a9166368434e&DisplayLang=en

7 STABILISE

The Stabilise phase involves testing the solution components whose features are complete, resolving and prioritising any issues that are found. Testing during this phase emphasises usage and operation of the solution components under realistic environmental conditions.

During this phase, testing and acceptance of the Active Directory service and its associated network components will take place. The aim is to minimise the impact on normal business operations by testing the design assumptions and verifying the deployment process in a pilot program. It is important that this phase of testing and verifying should begin during the Design phase and continue through the Deployment and Operations phase.

Figure 11 acts as a high-level checklist, illustrating the critical components that an IT Professional responsible for testing and validating the design of AD DS needs to determine:

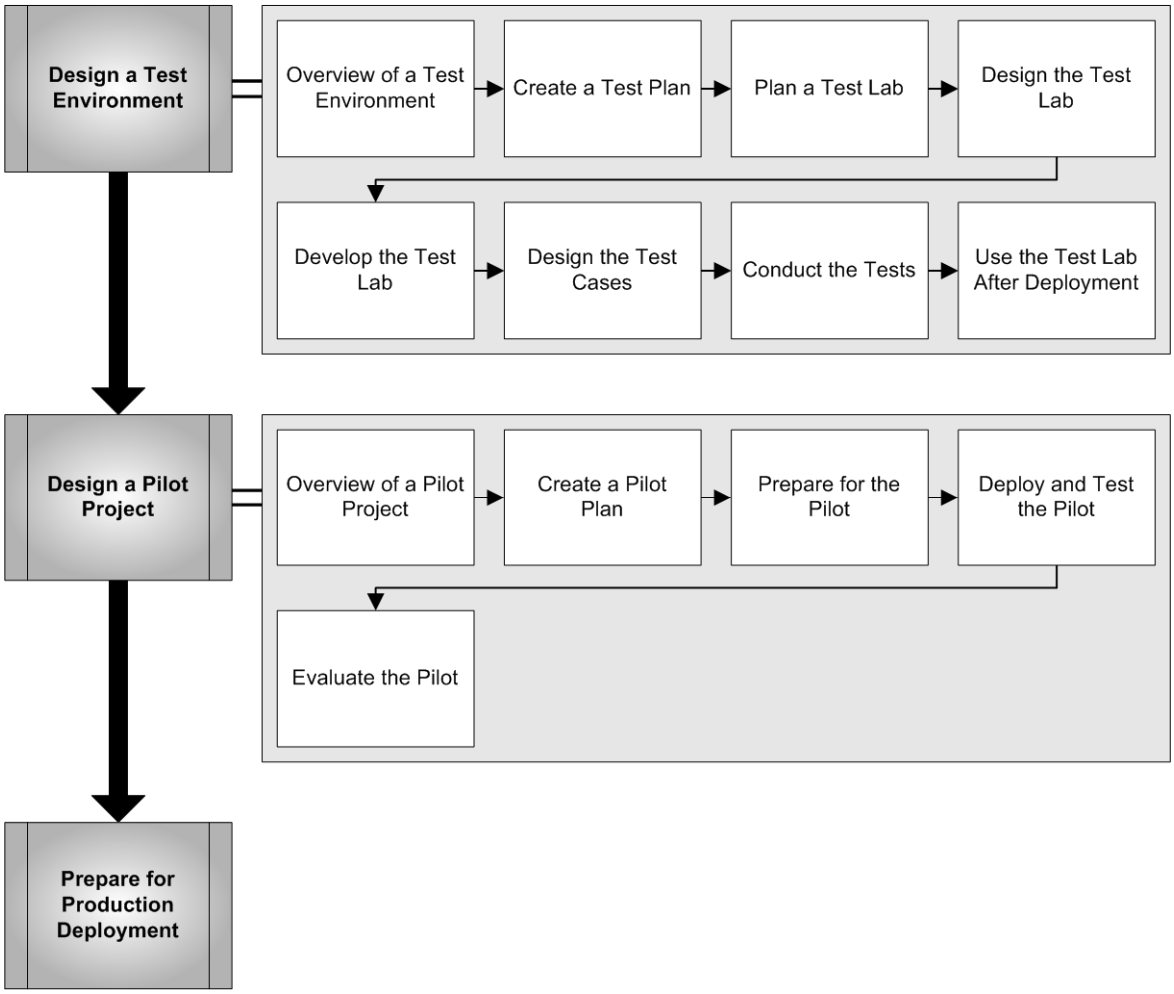


Figure 11: Sequence for Stabilising the AD DS Design

7.1 Design a Test Environment

7.1.1 Overview of a Test Environment

Before deploying AD DS, even during a pilot, it is vital to test the proposed design in an environment that simulates and protects the existing production environment. In this test environment, it will be possible to test hardware, operating systems, or applications designed to run together, before introducing them into the production environment. A test environment consists of a lab, detailed plans of what will be tested, and test cases that describe how each component of the

design and deployment will be tested. This means that, as a minimum, there will be a second Active Directory forest for each healthcare organisation, one in the production environment and one in the dedicated test environment.

By using server virtualisation (there is specific documented guidance around Microsoft® Hyper-V[56]), it is possible to install and configure multiple virtual domain controllers on a single physical server. This platform is well suited for test environments enabling a rapid reinstall back to a baseline configuration to repeat new tests.

7.1.2 Create a Test Plan

It is critical to the success of the testing, that a test plan be created. This should define the following components:

- The testing scope and objectives of the testing effort
- The testing methodology that the IT test team will use to conduct the tests
- The required resources, such as hardware, software and tools required for testing
- The features and functions that will be tested
- The risk factors that may jeopardise testing
- A testing schedule

> **Recommendations**
>
> It is important to include tests that verify or address the following:
>
> - The functionality of a feature is being used as the design intended
> - Interoperability with existing components and systems in the production environment
> - Hardware, driver, software and application compatibility testing for the domain controllers
> - Baselines and stress tests for capacity planning
> - Procedures for deployment and back-out plans, should any issues occur during deployment
> - Tests for the required tools and utilities

7.1.3 Plan a Test Lab

A test lab is a network that is designed for testing, and is isolated from the production network. The test lab is used to verify that components and features work correctly together in an integrated environment that simulates the target production environment.

When establishing a test lab, it is necessary to decide how it will be set up[57]. This could include the following options:

- Upgrade an existing test lab versus building a new test lab
- Create an ad hoc test lab versus a permanent test lab
- Have the test lab centralised versus distributed

[56] Running Domain Controllers in Hyper-V **{R58}**:
http://technet.microsoft.com/en-us/library/dd363553(WS.10).aspx

[57] Planning the Test Plan **{R60}**:
http://technet2.microsoft.com/windowsserver/en/library/05f4d318-f2b4-4544-b50a-6aef2174532a1033.mspx

7.1.4 Design the Test Lab

The lab planning process includes documenting the proposed test lab configuration. To design a lab that mimics the future production environment, it will also need to simulate the proposed server and client environments as closely as possible that will utilise AD DS.

Designing the test lab will involve:

- Gathering information about the current and proposed environments
- Documenting the test lab configuration so that it can be rebuilt as and when required
- Simulating the proposed server environment
- Simulating the proposed client computer environment
- Designing domains for testing

The documentation of the test lab should form two documents, one which details the components required, such as servers, switches/hubs, UPS, workstations, and another document that details both the logical and physical diagrams of the test lab[58].

7.1.5 Develop the Test Lab

Once the test lab planning process is finalised and has received management approval, it is necessary to build the lab. The following steps should be performed to ensure smooth operation of the lab:

- Assign a test lab manager
- Build the test lab
- Develop test lab guidelines and procedures

> **Recommendations**
>
> - It is recommended that, when building the test lab, every change made to server and client computers is documented in chronological order. This documentation can help resolve problems that might arise later and help explain why a specific computer behaves as it does over time
> - Ensure that an escalation plan is created which describes what the test team needs to do when problems arise during testing
> - Ensure that an incident-tracking system[59] is used for recording and reporting bugs and other testing problems, recording how they are resolved and the test results
>
> **Note**
>
> While this document outlines the ideal approach based on the experiences of Microsoft Services with large scale infrastructure deployment projects it is understood that many healthcare organisations simply do not have the staff resources to be appointing Network Managers and Test Lab managers. It is likely to be the same person in many cases. The primary principle here is that there is some accountability and an agreement from management that the lab facilities are properly considered and implemented to allow proper testing of the solution before they are rolled out into production.

[58] Documenting the Test Lab Configuration **{R61}**: http://technet2.microsoft.com/windowsserver/en/library/232b6b08-d5b7-4437-bddf-a142636091741033.mspx

[59] Developing an Incident-Tracking System **{R62}**: http://technet2.microsoft.com/windowsserver/en/library/e213d6a5-7d4e-48cf-87b8-00eb52aae61f1033.mspx

7.1.6 Design the Test Cases

A test case is a detailed procedure that fully tests a feature, or an aspect of a feature. Whereas the test plan describes what to test, a test case describes how to perform a particular test. A test case needs developing for each test listed in the test plan.

A test case includes:

- The purpose of the test
- Special hardware requirements, such as a modem
- Special software requirements, such as a utility or tool
- Specific setup or configuration requirements
- A description of how to perform the test
- The expected results or success criteria for the test

Full test case instructions for testing AD DS are provided in the Appendices of the document *The Windows Server System Reference Architecture*, (which is no longer publicly available) but for convenience the test descriptions are listed within APPENDIX E of this document.

7.1.7 Conduct the Tests

When conducting tests, the tester must perform each test as described in the test case, evaluate the test results, escalate problems that arise until they are resolved, and document the test results. Figure 12 illustrates the testing process:

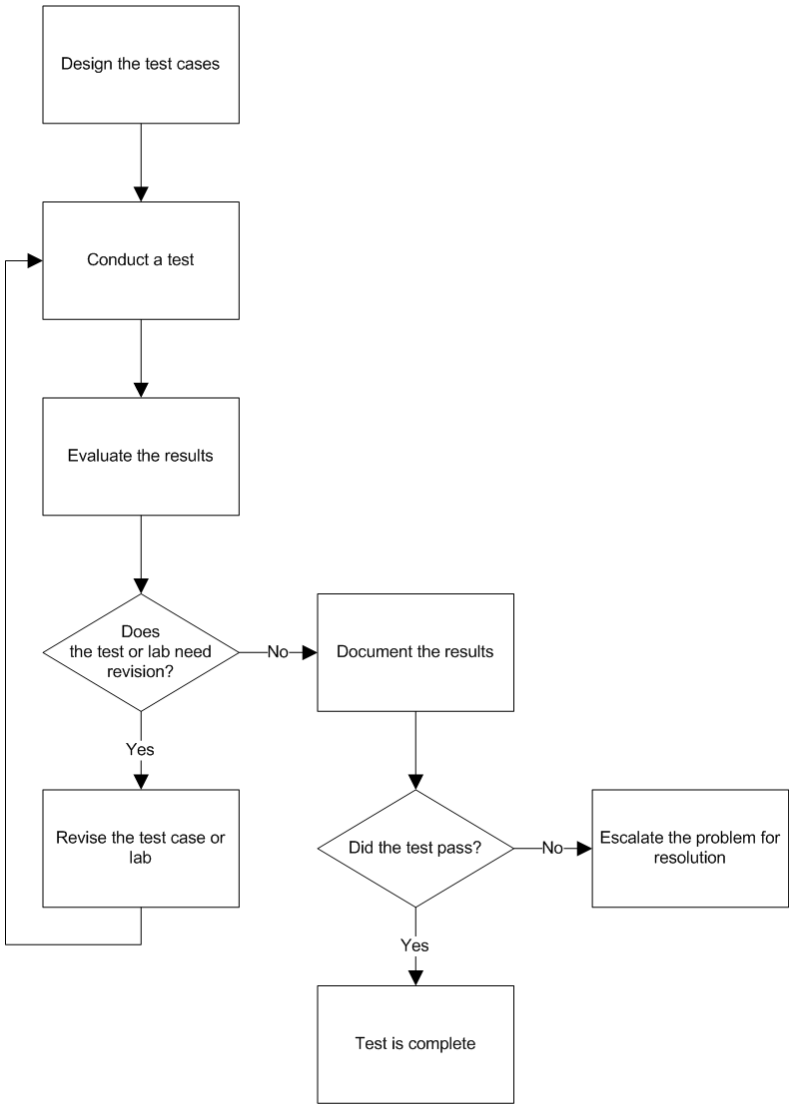


Figure 12: The Testing Process

> **Recommendation**
>
> It is highly likely that the lab will change frequently as tests are run and new tests are begun. It is recommended that backups of baseline configurations are made so that testers can quickly restore a computer to its prior state. The restore process should be tested and backup files should be documented and stored in a safe, accessible place. With the snapshot technology in place and the ability to save Virtual Server images it should be possible to create a solution where changes can be rolled back to a consistent state if the testing results in a negative result. Great care still needs to be taken to avoid issues such as Update Sequence Number (USN) Rollback and selectively restoring previous images of some servers and not others.

7.1.8 Use the Test Lab After Deployment

The importance of testing changes to the IT environment after deploying Windows Server 2008 R2, and the latest Windows clients cannot be overemphasised. Due to the potential effect that changes can have in the production environment, it is important to test every update and Service Pack until the anticipated results are achieved, before they are piloted or rolled out to the production environment.

> **Recommendation**
>
> As far as possible, the test lab should remain in place after deployment. This will enable continued testing of the infrastructure, as and when new design decisions are made, avoiding adverse affects occurring within the production environment.

7.2 Design a Pilot Project

Conducting the pilot is the last major step before deployment of the Windows Server 2008 R2 AD DS. The pilot should include the creation of a plan, deployment of a test environment and testing by designated users. The results are then evaluated to ensure the pilot was successful.

7.2.1 Overview of a Pilot Project

During the pilot, tests of the design take place in a controlled environment in which users perform their normal business tasks using the new features. This demonstrates that the design works in the production environment as expected, and that it meets the Healthcare organisation's business requirements. Any encountered problems can immediately be fed back into testing and redesigned as required, therefore minimising the risk to the business of issues during deployment. Figure 13 illustrates the process of planning and conducting a pilot project:

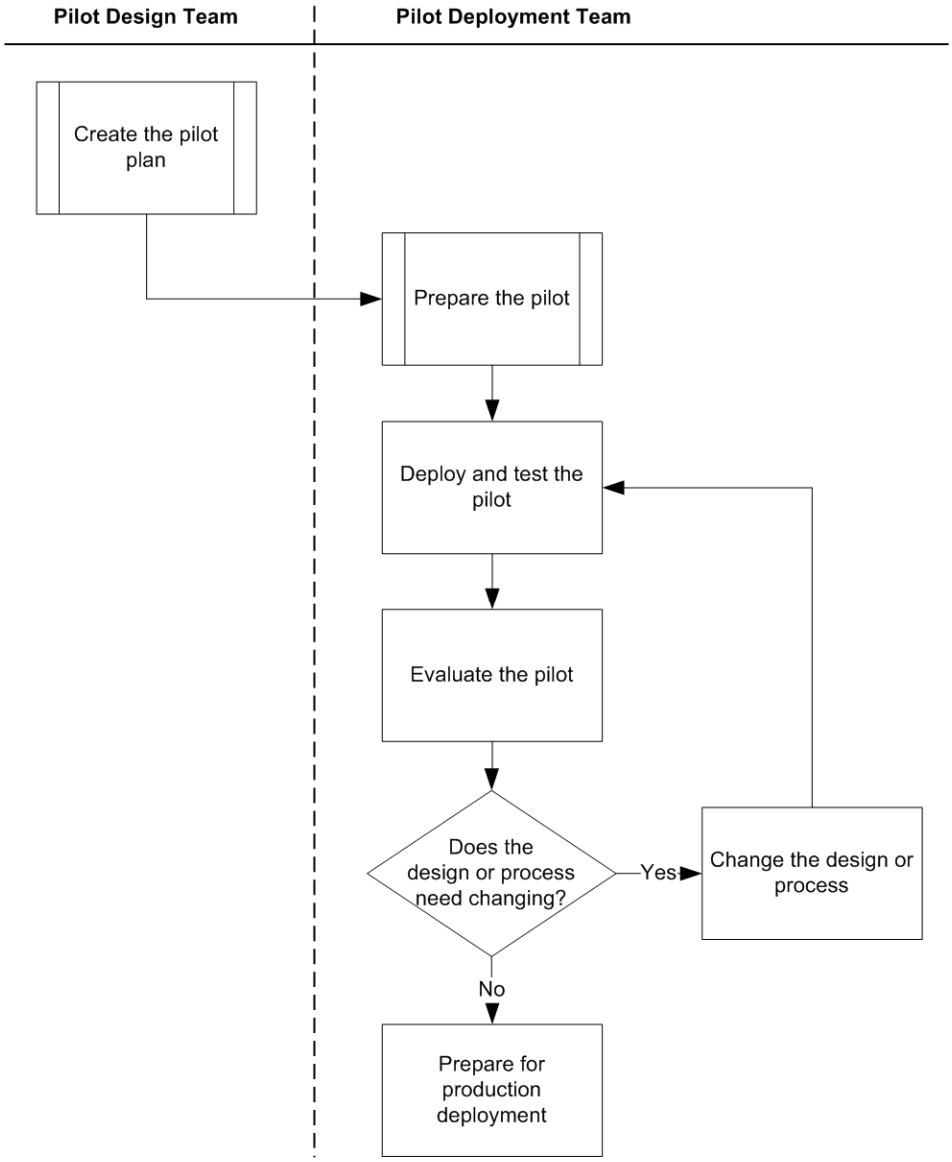


Figure 13: Designing a Pilot Project

Although the pilot is conducted during the Test and Validate phase of the project cycle, planning for the pilot occurs during the Define and Plan phases of the deployment project, and preparing for the pilot occurs during development. Figure 14 illustrates the tasks involved in planning for and conducting a pilot, and shows the appropriate phase during which each of these activities might occur. The timeframes are generic estimations that will obviously vary from deployment to deployment.

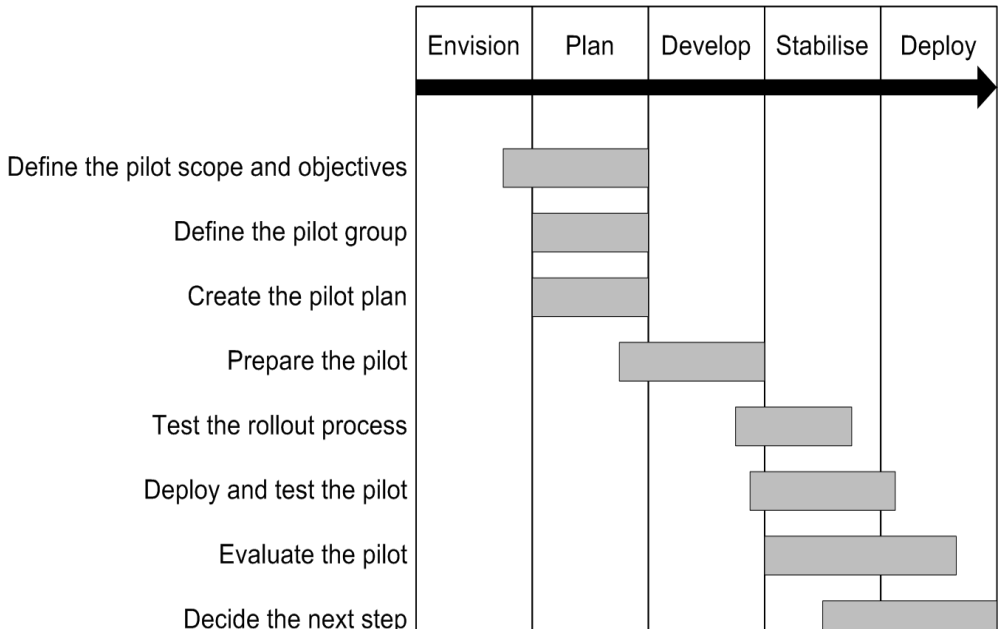


Figure 14: Role of the Pilot in the Project Lifecycle

7.2.2 Create a Pilot Plan

The pilot plan[60] should define:

- The scope and objectives of the pilot
- Pilot participants and where the pilot will be conducted
- A schedule for deploying and conducting the pilot
- Plans for training and communicating with pilot participants
- Evaluation of the pilot
- Risks and contingencies

7.2.3 Prepare for the Pilot

Preparation for the pilot[61] deployment begins with development, during the Build phase of the project, and should consider:

- Preparation of the pilot sites
- Preparation of the pilot participants
- Testing of the rollout process

[60] Creating a Pilot Plan **{R63}**:
http://technet2.microsoft.com/windowsserver/en/library/99f07a8e-503b-4751-b108-c85e188ada951033.mspx

[61] Preparing for the Pilot **{R64}**:
http://technet2.microsoft.com/windowsserver/en/library/0a5f853e-28d2-4afe-a9db-92761a8d3ed61033.mspx

7.2.4 Deploy and Test the Pilot

When deploying the pilot, the Windows Server 2008 R2 AD DS implementation is being tested under live conditions. The pilot deployment process should be started with a trial run of the pilot to identify problems with the deployment and the pilot plan. Then, when the full pilot begins, keep track of which deployment tasks have been completed so that it is possible to monitor the progress of the pilot.

As participants use the system, it is advised that the pilot team track the progress of the pilot and identify areas of concern. All participants should be encouraged to use the incident-tracking system to report problems and to use the escalation plan when immediate problem resolution is not possible.

7.2.5 Evaluate the Pilot

When the pilot is complete, feedback should be obtained from a variety of sources, including participants, pilot management and support teams, and other observers, to evaluate the success of the pilot.

Once enough pilot data has been collected, and participant feedback has been evaluated, the team must decide how to proceed. Depending on how well the pilot meets the success criteria, there are a number of strategies that can be employed at this point in the pilot deployment:

- Overlap the stages of the pilot when moving forward
- Roll back the pilot
- Suspend the pilot
- Update the pilot and continue
- Proceed to the production deployment phase

The pilot is not complete until the team ensures that the proposed solution is viable in the production environment and that every component of the solution is ready for deployment.

7.3 Prepare for Production Deployment

Once the team has agreed that the pilot has been successfully completed and has obtained management approval for proceeding, the next step is to fully deploy the system to the appropriate Healthcare organisation level. During this phase, the release team should deploy the core technology and site components, stabilise the deployment, transition the management of the project to the operations and support teams, and obtains final management approval of the project.

8 DEPLOY

The Deploy phase is used to manage the deployment of core solution components for widespread adoption in a controlled environment. During the managed deployment, the solution is tested and validated through ongoing monitoring and evaluation. A well-planned deployment of solution components as an end-to-end system will enable the delivery of a quality service that meets or exceeds customer expectations.

This section describes the build process for the Windows Server 2008 R2 AD DS forest and provides additional configuration information required for the supporting network services, such as DNS. Once installed and configured, it is vital to test and validate the functionality of AD DS before using this mission critical system. This section provides AD DS deployment information that is not specific to each of the healthcare scenarios mentioned in section 4.4.1 and, as such, can be used in a multitude of different scenarios.

Successful completion of the guidance given in this section requires that the IT Professionals concerned have a certain level of technical knowledge and deployment experience.

The designated forest owner is responsible for deploying the forest root domain. After the forest root domain deployment is complete, the remainder of the Active Directory forest should be deployed as specified by the AD DS design (see section 6 for further details).

Figure 15 acts as a high-level checklist, illustrating the critical components that an IT Professional responsible for deploying AD DS needs to determine:

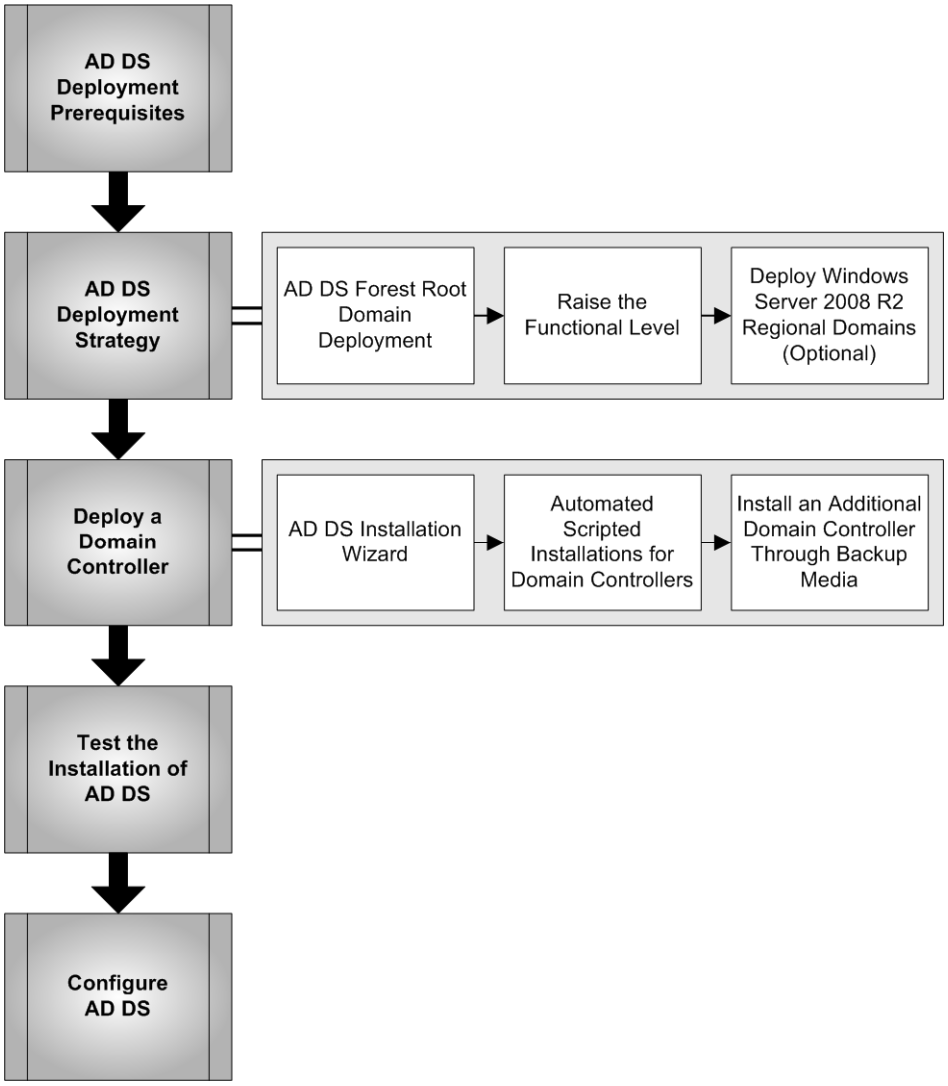


Figure 15: Sequence for Deploying AD DS

8.1 AD DS Deployment Prerequisites

Before beginning the AD DS deployment (by promoting a server to be the first domain controller and therefore creating the forest), it is important to ensure the following prerequisites have been completed:

- Review of the AD DS forest (logical, physical and security) and network services design, utilising the job aids that have been completed during the Build phase
- The Network is operational and configured as required
- Windows Server 2008 R2 operating system base build is complete, as per the requirements of the *Windows Server 2008 R2 Build* **{R4}**
- The domain controller drives have been configured as stated in the design
- The chosen Active Directory forest DNS name has been registered

- Any existing DNS service in the healthcare organisation has been configured with a delegation (optional, depending on the environment). The DNS administrator of the existing healthcare organisation DNS service must delegate the zone that matches the name of the forest root domain to the DNS servers (DCs) that will be installed in the forest root domain
- The DNS service has been installed on the server which will become a domain controller. The domain controller promotion process can configure DNS automatically if the installation defaults match those that the Healthcare organisation wishes to use. If the Healthcare organisation has separate configuration requirements these must be configured (as much as they can be) prior to promoting the server[62]
- Configure the Time Service on the server that is to be configured as the Active Directory forest PDC emulator role holder, to synchronise from a valid Network Time Protocol (NTP) source. By default this will be the first domain controller installed in each domain
- All necessary operations and support staff are in place to take ownership of the AD DS

> **Recommendation**
>
> It is recommended that a hardware based clock for time synchronisation is installed, such as a radio or a GPS device, and that this is used as the source for the Windows Time Service on the PDC emulator. If this is not possible, then an external time server should be used such as time.windows.com.

8.2 AD DS Deployment Strategy

The first domain that is created in the Active Directory forest is automatically designated as the forest root domain. The forest root domain provides the foundation for the Active Directory forest infrastructure.

It is possible to save time during the deployment process by automating installations and by using the AD DS Installation Wizard, rather than installing via a purely manual configuration. This is discussed further in section 8.3.1.

8.2.1 AD DS Forest Root Domain Deployment

The first step in creating the forest root domain is deploying the first forest root domain controller. The forest owner is responsible for deploying the forest root domain. This is followed by the deployment of the second domain controller, DNS reconfiguration, site topology configuration and operations master role placement.

8.2.1.1 Deploy the First Root Domain Controller

To deploy the first domain controller in the forest root domain, complete the following tasks:

- Install Windows Server 2008 R2 including any available service packs and patches, based on the *Windows Server 2008 R2 Build* **{R4}**
- Install AD DS, using either a scripted install or DCPromo to start the AD DS Installation Wizard. (See section 8.3 for more information on this step.)
- Verify the AD DS installation. (See section 8.4 for more information.)
- Verify DNS server recursive name resolution[63]

[62] Configuring DNS for the Forest Root Domain **{R65}**: http://technet.microsoft.com/en-us/library/cc771849(WS.10).aspx

[63] Verify DNS Server Recursive Name Resolution on the First Forest Root Domain Controller **{R66}**: http://technet.microsoft.com/en-us/library/cc754529(WS.10).aspx

8.2.1.2 Deploy the Second Domain Controller in the Same Site

After deploying the first forest root domain controller, deploy the second forest root domain controller in the same site, according to the design. To deploy the second forest root domain controller, complete the following tasks:

- Install Windows Server 2008 R2 including any available service packs and updates, based on the *Windows Server 2008 R2 Build* **{R4}**
- Install AD DS, using either a scripted install or Dcpromo to start the AD DS Installation Wizard (see section 8.3 for more information on this step)
- Install DNS Server service after AD DS installation has finished and the computer has restarted
- Verify the AD DS installation (see section 8.4 for more information)

8.2.1.3 Reconfigure the Domain Name System Service

Reconfigure the DNS service to account for the addition of the second domain controller in the forest root domain. It is also possible to use these procedures as additional domain controllers are deployed, which are running the DNS service.

To reconfigure the DNS service:

- Enable Ageing and Scavenging for DNS on two DCs running the DNS Server service per domain, to allow automatic cleanup and removal of stale RRs, which can accumulate in zone data over time
- Configure the DNS client settings of the first and subsequent domain controllers
- Update the DNS delegation

For more detailed steps, see the TechNet Web page 'Reconfigure the DNS Service'[64].

8.2.1.4 Configure the Site Topology

The site topology owner configures the site topology for the forest. Configuring the site topology for the forest involves the following tasks:

- Delegating AD DS site administration. The forest owner should delegate this task to a designated site topology owner
- Creating required AD DS sites using the AD DS Sites and Services MMC
- Creating and assigning AD DS subnets using the AD DS Sites and Services MMC
- Creating AD DS site links using the AD DS Sites and Services MMC

8.2.1.5 Deploy Additional Domain Controllers in Other Sites (Optional)

If the design specifies deployment of additional forest root domain controllers in other sites, they should be deployed using the procedures listed in section 8.2.1.2.

[64] Reconfigure the DNS service **{R67}**: http://technet.microsoft.com/en-us/library/cc732922(WS.10).aspx

8.2.1.6 Configure Operations Master Roles

The forest-level and domain-level operations master roles for the forest root domain should be configured as per the design. By default, the first domain controller installed in the forest root domain is assigned all operations master roles. These can be further configured[65] to meet the requirements of the organisation if it is necessary or can be transferred to alternative domain controllers to balance the performance load[66].

8.2.2 Raise the Functional Level

When deploying the first domain controller in the forest root domain, the forest operates by default at the Windows 2000 forest functional level, and the domain operates by default at the Windows 2000 mixed functional level.

> **Recommendations**
>
> - Raise the forest functional level to Windows Server 2003 native mode. Provided there are no application issues, raise the forest functional level to Windows Server 2008 R2
> - Use AD DS Domains and Trusts to enable the Windows Server forest functional levels

8.2.3 Deploy Windows Server 2003 Regional Domains (Optional)

Deploying Windows Server 2008 R2 regional domains involves creating new geographically based child domains under the forest root domain. This is only necessary if the Build phase has designed a multiple domain Active Directory forest.

Windows Server 2008 R2 in any regional domains should be deployed following the sequence outlined in section 8.2.2 for a forest root domain. The high-level steps required are listed below:

- Reviewing the regional domain design
- Delegating the DNS domain for the new regional domain
- Deploying the first domain controller in a new regional domain
- Deploying additional domain controllers in a new regional domain
- Reconfiguring the DNS service
- Configuring operations master roles

> **Recommendation**
>
> No additional information is provided on this process as a single domain forest is recommended for each Healthcare organisation.

8.3 Deploy a Domain Controller

The *Windows Server 2008 R2 Build* **{R4}** requires reconfiguring into the domain controller role to host AD DS. This is performed by running the inbuilt DCPromo.exe tool to start the AD DS Installation Wizard. The AD DS Installation Wizard can be used for the following three methods:

---

[65] Configure the Operations Master roles {**R104**}:
http://technet.microsoft.com/en-us/library/cc732963(WS.10).aspx

[66] Transfer operations master roles **{R70}**:
http://technet2.microsoft.com/windowsserver/en/library/5da4f9f2-7f90-417a-9d11-5ee1db75bfb61033.mspx and:
http://technet.microsoft.com/en-us/library/cc816946(WS.10).aspx

- AD DS Installation Wizard from running DCPromo from the command line, or by selecting the 'Configure Your Server Wizard' menu option
- Automated install using an unattended setup script called an answer file
- Installing from media for additional domain controllers

> **Recommendation**
>
> It is recommended that the use of the unattended answer file is used to deploy a domain controller. This is primarily for two reasons:
>
> 1. The answer files can become part of the design documentation which can be referenced in the future.
> 2. Automating the install removes the element of human error when completing the AD DS Installation Wizard manually.

8.3.1 AD DS Installation Wizard

To configure a server as a domain controller, install AD DS on the server by running DCPromo.exe either from a command line or by selecting 'Configure your server wizard' from the menu option.

It is possible to create two types of domain controllers by using the AD DS Installation Wizard:

- Domain controller for a new domain
- Additional domain controller for an existing domain

When creating a domain controller for a new domain, the domain can be one of the following types:

- Domain in a new forest – Select this domain type if creating the first domain in the organisation, or if wanting the new domain to be independent of any existing forests. This first domain is the forest root domain
- Child domain in an existing domain tree – Select this domain type if wanting the new domain to be a child of an existing domain
- Additional domain tree in an existing forest – Select this domain type if wanting to create a domain tree that is separate from any existing domain trees

8.3.2 Automated Scripted Installations for Domain Controllers

It is possible to run the AD DS Installation Wizard without having to be present to answer the questions by using an 'answer file'. An answer file is a text file that can be populated with the parameters that the wizard needs to install AD DS.

An answer file can be used to install Windows Server 2008 R2, and can also include the options necessary to subsequently install AD DS. Alternatively, it is possible to create an answer file that contains only the options necessary for installing AD DS. These parameters[67] include the domain controller type (additional domain controller for an existing domain or a new domain controller for a new domain), the configuration of the domain that is being created (new forest, new tree root, or new child) and AD DS forest and domain functional levels. Additional switches have been added through Windows Server 2008 and Windows Server 2008 R2 to support the unattended installation of the newer services and features[68].

Once the answer file has been created, the file name can be appended to the */answer* switch when running the DCPromo command from the command line. For example:

---

[67] How to use unattended mode to install and remove Active Directory Domain Services on Windows Server 2008-based domain controllers **{R68}**:
http://support.microsoft.com/kb/947034

[68] Appendix of Unattended Installation Parameters {**R105**}:
http://technet.microsoft.com/en-us/library/cc732086(WS.10).aspx

```
C:\Windows> dcpromo /answer:dcinstall.txt
```

The following is an example content of an unattended answer file for automating the installation of AD DS. The answers provided in this example would install a domain controller in a new domain in a new forest. The contents of this file would need to change appropriately for subsequent installations of domain controllers, such as specifying Join for the CreateOrJoin and Replica for the ReplicaOrNewDomain parameter.

```
[DCInstall]
AutoConfigDNS = No
CreateOrJoin = Create
CriticalReplilcationOnly = No
DatabasePath = %SYSTEMROOT%\NTDS
DisableCancelForDnsInstall = Yes
DNSOnNetwork = Yes
DomainNetBiosName = HEALTHORG
LogPath = %SYSTEMROOT%\NTDS
NewDomain = Forest
NewDomainDNSName = healthorg.org.com
Password = Qw3ertyu!0P
RebootOnSuccess = Yes
ReplicaOrNewDomain = Domain
SafeModeAdminPassword = P0!uytr3wQ
SetForestVersion = Yes
SysVolPath = %SYSTEMROOT%\SYSVOL
TreeOrChild = Tree
UserDomain = HEALTHORGDEMODC1
UserName = Administrator
```

> **Note**
>
> The example answer file above has been given purely for demonstration purposes and is not a recommendation of the options that should be implemented. However, the example may act as an aid when structuring an answer file that will fit the requirements and design decisions of the Healthcare organisation. Also, the example password given in the example is purely for demonstration purposes of how a complex password should be used, a similarly complex password should be chosen.

> **Important**
>
> Once the answer file has been used by the DCPromo tool, any passwords contained within the file are removed. Therefore, during testing of the answer file, if it is necessary to run the DCPromo tool multiple times with the same answer file, the password must be entered before it can be run, otherwise the AD DS Installation Wizard will prompt for this information.

8.3.3 Install an Additional Domain Controller Through Backup Media

With the Windows Server 2008 R2 family, it is possible to install AD DS on member servers using a restored backup of system state data taken from an existing domain controller running Windows Server 2008 R2 – a feature known as Install From Media (IFM). This backup can be stored on any backup media (for example, tape, CD, or DVD) or a shared network resource. By using restored backup files to create an additional domain controller, it is possible to greatly reduce the network bandwidth used when installing AD DS over a shared network resource. Network connectivity is still needed to replicate all new objects and recent changes for existing objects to the new domain controller. This option is suitable for either of the following situations:

- Where there is a poor WAN link between the site where the domain controller is being installed and the nearest site that hosts a domain controller which will be used for performing the initial replication of the directory
- Where the AD DS is so large that the time taken to promote the new domain controller will be excessive. Typically this would be a case where the existing AD DS store exceeds 24GB

It is unlikely that any healthcare organisation will use this method for installing AD DS but it is documented here for completeness.

> **Recommendation**
>
> Should a healthcare organisation wish to use backup media to install additional domain controllers, it is recommended that the unattended answer file is still used and that the `ReplicateFromMedia` and `ReplicationSourcePath` parameters are specified.

Full details on this option are available within the Microsoft Knowledge Base article: *How to use the Install from Media feature to promote Windows Server 2003-based domain controllers*[69] which can be used to supplement the Windows Server 2008 documentation for installing domain controllers via IFM[70] and RODCs with IFM[71].

8.4 Test the Installation of AD DS

As a minimum, the following tests should be conducted to verify the AD DS installation on the first root domain controller:

- Review the Windows Server 2008 R2 event log and resolve any errors
- At the command line, run Dcdiag.exe and Netdiag.exe, and resolve any errors that are reported
- Run Task Manager and verify that the processor and memory system resources are within acceptable limits

[69] How to use the Install from Media feature to promote Windows Server 2003-based domain controllers **{R69}**: http://support.microsoft.com/kb/311078.

[70] Installing an Additional Domain Controller by Using IFM **{R106}:** http://technet.microsoft.com/en-us/library/cc816722(WS.10).aspx

[71] Installing AD DS from Media **{R107}:** http://technet.microsoft.com/en-us/library/cc770654(WS.10).aspx

- Open the DNS snap-in, navigate to Forward Lookup Zones, and verify that the zones _msdcs.*forest_root_domain_name* and *forest_root_domain_name* were created. Expand the *forest_root_domain_name* node and verify that DomainDnsZones and ForestDnsZones were created, where *forest_root_domain_name* is the name of the forest root
- Consideration should also be given to running the Active Directory Best Practice Analyzer once the forest has been configured to verify that there are no minor configuration settings that have either not been set or have been set sub optimally

On the second domain controller installed in the forest root domain perform the following additional validation check:

- Use the same tests as shown in the procedure for the first domain controller, but instead of verifying that DomainDnsZones and ForestDnsZones were created, use the `repadmin /showreps` command to verify that the ForestDnsZones and DomainDnsZones application directory partitions have been replicated successfully. Use `dnscmd` to verify that the domain controller has been enlisted in the replication scope of the DNS Application Partitions. Use the DNS snap-in to verify that DNS server recursive name resolution is configured according to the method used by the Healthcare organisation.

8.5 Configure AD DS

Once the AD DS service has been installed and verified, it is necessary to review the AD DS design and configure any outstanding settings. This should include:

- Configuring domain controllers as GC Servers
- Creating the OU structure
- Creating any remaining sites, associating sites to subnets and assigning sites to site links
- Applying security policies, such as the additional configuration required in the DDP and DDCP
- Creating and deploying any new GPOs that supplement the default GPOs and are required
- Creating service and data administrative accounts
- Delegating the appropriate administration rights to the new administrative accounts
- Applying the delegation of the administration model to the OU structure
- Creating user accounts
- Creating group accounts
- Nesting groups appropriately
- Assigning resource access permissions to groups
- Establish any required Active Directory trusts to external domains or forests

9 OPERATE

During the Operate phase, solution components are proactively managed as an end-to-end IT Service to ensure the service provides the required levels of solution functionality, reliability, availability, supportability and manageability. Successfully bringing a well-designed service into a production environment takes efficient planning to balance speed, cost and safety, while ensuring minimum disruption to operations and supporting the 'business as usual' delivery of the organisation's IT requirements.

This section is the starting point for the operations of the Windows Server 2008 R2 AD DS. It is designed to provide a significant head start in formulating the necessary and appropriate product operations materials for the creation of healthcare-specific solution operations guidance. The operational infrastructure to support AD DS will depend on the scale of the implementation within each Healthcare organisation. Small infrastructures will benefit from the reduction of administration through the use of the built in tools, scripting repetitive tasks and the implementation of services, such as Group Policy and RIS. Medium and large healthcare organisations will also benefit from these services, as well as receiving benefit from the implementation of enterprise software distribution solutions, and will need to be more aware of capacity management and operations management.

Through a combination of these technologies, public best practices guidance, and training opportunities, the healthcare organisations can improve service, reliability, availability, and security while lowering the TCO.

Figure 16 acts as a high-level checklist, illustrating the critical components for which an IT Professional is responsible for ensuring in a managed and operational AD DS infrastructure:

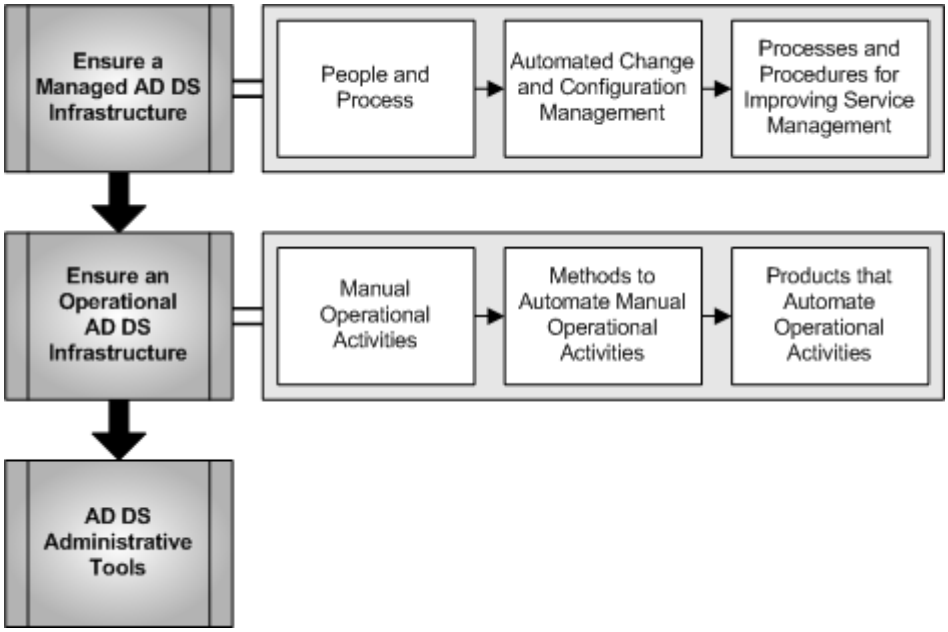


Figure 16: Sequence for Operating AD DS

9.1 Ensure a Managed AD DS Infrastructure

Being more proactive with the administration and management of the network circumvents potential security risks and network failure problems that impact employee productivity and potential data loss. Windows Server 2008 R2 and AD DS provide distributed and delegated levels of administration and management, through the use of the Delegation of Control (DoC) wizard[72], so that a healthcare organisation can assign common tasks to department managers or other personnel for functions like password resets, assigning department level security, reset print queues, or scan for security vulnerabilities.

By distributing administration tasks on an 'as needed' basis, the medium and large healthcare organisations can be more proactive to potential problems, and can quickly respond to system problems, whilst achieving a lower TCO.

> **Recommendations**
>
> Where a healthcare organisation has enough staff to support it, routine administrative tasks such as password resets, should be delegated to ease the burden on IT support staff, so that they are more often available for proactive system monitoring.
>
> All staff should be suitably trained in the use of the core support and administration tools to allow them to effectively and competently manage AD DS.

9.1.1 People and Process

Public guidelines are available to help effectively design, develop, deploy, operate, and support solutions built on Microsoft technologies. These guidelines are organised into two integrated frameworks, the Microsoft Operations Framework (MOF)[73] and Microsoft Solutions Framework (MSF)[74], which include white papers, operations guides, assessment tools, best practices, case studies, templates, support tools and services.

MOF provides the regime that addresses the people, process, technology, and management issues pertaining to operating complex, distributed, heterogeneous IT environments.

> **Recommendation**
>
> It is vital to ensure that appropriate processes are in place to help manage the IT environment within the Healthcare organisation.

9.1.2 Automated Change and Configuration Management

For medium to large healthcare organisations, looking to incorporate Microsoft System Center Configuration Manager into the environment, it is important to consider the following points with regard to an AD DS design:

- The requirements for software distribution in AD DS site design should be considered when deciding to allocate subnets to sites
- The design of Active Directory OUs, distribution lists, and security groups need consideration when integrated with Configuration Manager software distribution

---

[72] *Active Directory delegation tools (Windows Server 2003)* **{R71}**: http://technet.microsoft.com/en-us/library/cc756087(WS.10).aspx and for Windows Server 2008 http://technet.microsoft.com/en-us/library/dd145344.aspx

[73] Microsoft Operations Framework 4.0 **{R72}**: http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofeo.mspx

[74] Microsoft Solutions Framework Core Whitepapers **{R73}**: http://www.microsoft.com/downloads/details.aspx?FamilyID=e481cb0b-ac05-42a6-bab8-fc886956790e&DisplayLang=en

For smaller scale deployments, where System Center Configuration Manager (SCCM) is not appropriate, it is still paramount that the Healthcare organisation ensures the manageability of system patches and security updates. In preparing for simple automated patch management services, Windows Server Update Services (WSUS)[75] in conjunction with Group Policy can be used to help implement a more secure, robust infrastructure. The patch management process should be structured to ensure regular review of vulnerability assessment across the infrastructure, thus reducing the exposure of unpatched systems.

The Microsoft Baseline Security Analyser (MBSA)[76] is a free tool from Microsoft that can be used to detect common security misconfigurations and missing security updates on computer systems in small and medium sized environments. It is designed to determine the security state of computers in accordance with Microsoft security recommendations and offers specific remediation guidance.

> **Recommendation**
>
> Each Healthcare organisation should have the ability to centrally deploy and manage the operating system, security and application patches and updates. Ideally an audit trail of what patches are deployed to what machines should be maintained.

9.1.3 Processes and Procedures for Improving Service Management

Microsoft has published product operations guides, available on the Internet, that describe the processes and procedures required for improving the management of many of its core products. The following list highlights the essential guidance for an AD DS infrastructure:

- Active Directory Product Operations Guide[77]
- DNS Service Product Operations Guide[78]
- WINS Service Product Operations Guide[79]

These guides contain tables that provide a quick reference for those product maintenance processes that need to be performed on a regular basis. These tables represent a summary of the processes, and their subordinate tasks and procedures, described in more detail in subsequent chapters of the guides. They are limited to those processes required for maintaining the product.

[75] Microsoft Windows Server Update Services **{R74}**:
http://www.microsoft.com/windowsserversystem/updateservices/default.mspx

[76] Microsoft Baseline Security Analyser **{R75}**:
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

[77] Active Directory Product Operations Guide TechNet article **{R76}**:
http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/adpog/adpog1.mspx

[78] DNS Product Operations Guide TechNet article **{R77}**:
http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/dnspog/dnspog1.mspx

[79] WINS Service Product Operations Guide TechNet article **{R78}**:
http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/winspog/winspog1.mspx

9.2 Ensure an Operational AD DS Infrastructure

The ability to monitor the health of AD DS is a key aspect of the operational manageability of each Healthcare organisation. Proactively monitoring the distributed AD DS and the services that it depends on is critical to maintain consistent directory data and a consistent level of IT service throughout the forest[80]. Monitoring AD DS assures administrators that:

- All necessary services that support AD DS are running on each domain controller
- Data is consistent across all domain controller s and end-to-end replication completes in accordance with Service Level Agreements (SLAs)
- There are no domain controllers that are consistently failing to replicate and thus in danger of becoming orphaned
- Lightweight Directory Access Protocol (LDAP) queries respond quickly
- Domain controllers do not experience high Central Processing Unit (CPU) usage

9.2.1 Manual Operational Activities

Healthcare organisations that have deployed AD DS with few domains and domain controller s, or healthcare organisations that do not require a critical level of service, might only check the performance of a single domain controller periodically by using the built-in tools that are provided with Windows Server 2008 R2, such as Performance and Reliability Monitor[81].

Microsoft has published product operations guides, available on the Internet, that provide appropriate administration and troubleshooting information for the following products:

- Windows Server 2008 Active Directory Operations Guide[82]
- Windows Server 2008 DNS Server Operations Guide[83]
- Windows Server 2008 Group Policy Planning and Deployment Guide[84]

Most of the individual routine AD DS operations tasks are well documented on the Microsoft Web site, including:

- Routine AD DS tasks detailed for Windows Server 2003 in the section *Common Administrative Tasks*[85]. These have not been updated for Windows Server 2008 or Windows Server 2008 R2. Some of the tasks listed for Server 2003 will transfer over to Windows Server 2008 R2. For changes or alternative methods review the Windows Server 2008 R2 product documentation and the Technet documentation.
- A list of step-by-step guides[86]

---

[80] Monitoring Domain Controller Performance **{R79}**:
http://technet2.microsoft.com/windowsserver/en/library/c5d72b6f-5974-4263-b29f-2eece0ab44371033.mspx

[81] Performance and Reliability Monitor overview **{R80}**:
http://technet.microsoft.com/en-us/library/cc771692(WS.10).aspx

[82] Active Directory Operations Guide **{R81}**:
http://technet.microsoft.com/en-us/library/cc816807(WS.10).aspx

[83] DNS Server Operations Guide **{R82}**:
http://technet.microsoft.com/en-us/library/cc816603(WS.10).aspx

[84] Group Policy Planning and Deployment Guide **{R83}**:
http://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx

[85] Common Administrative Tasks **{R84}**:
http://technet2.microsoft.com/windowsserver/en/library/f2d54234-6d65-439b-9d3b-ac1c4b2a3f991033.mspx

[86] Active Directory Step-by-step Guides **{R85}**:
http://technet.microsoft.com/en-gb/windowsserver/2008/default.aspx

- Performance tuning for AD DS, detailed in the paper *Performance Tuning Guidelines for Windows Server 2008 R2*[87] with a comprehensive reference list of the relevant *performance counters for* AD DS available in the paper *Windows Server 2003 Performance Counters Reference*[88].This reference has not been updated yet for Windows Server 2008 or Windows Server 2008 R2.

> **Important**
>
> The most critical daily operational task to perform on the AD DS is to perform a backup of the service. AD DS is backed up as part of System State, (which includes the database, log files, registry, system boot files, and COM+ registration database), and SYSVOL[89].
>
> Therefore, it is critical that these volumes be backed up and restored as a set. Backup and restore plans help to ensure service continuity in the event of a directory issue, and provide the facility to recover objects that may have been accidentally deleted. This is less of an issue in Windows Server 2008 R2 with the AD DS Recycle Bin feature but still does not undermine the importance of regular and consistent backups.

To help minimise the impact of a disaster, and ensure service continuity, it is important that the AD DS backup is periodically restored into a test environment. This should be performed in conjunction with applying the appropriate procedures for AD DS recovery. The following document provides useful guidance on these procedures:

- Microsoft whitepaper *Windows Server 2008: Planning for Active Directory Forest Recovery*[90]

9.2.2 Methods to Automate Manual Operational Activities

It is possible to script and automate many AD DS administrative tasks in order to reduce pressure on AD DS and reduce the TCO of the service. Scripting AD DS tasks also reduces the risk of administrative error that can be introduced, such as typing errors. The scripts themselves should be thoroughly tested and verified before being applied to the production environment.

The following is a list of reusable AD DS script resources, technologies and references for example scripts:

- Microsoft Script Center[91]
- Sample scripts for Active Directory[92]
- Scripts for DNS[93]

---

[87] Performance Tuning Guidelines for Windows Server 2008 R2 **{R86}**:
http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv-R2.mspx

[88] Windows Server 2003 Performance Counters Reference **{R87}**:
http://technet2.microsoft.com/WindowsServer/en/Library/3fb01419-b1ab-4f52-a9f8-09d5ebeb9ef21033.mspx

[89] Active Directory Product Operations Guide, Chapter 3 **{R88}**:
http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/adpog/adpog3.mspx

[90] Best Practices: Active Directory Forest Recovery whitepaper **{R89}**:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=326c8a7a-dcad-4333-9050-a6303ff3155c

[91] Microsoft Script Center **{R90}**:
http://www.microsoft.com/technet/scriptcenter/default.mspx

[92] Script Repository: Active Directory **{R91}**:
http://gallery.technet.microsoft.com/ScriptCenter/en-us/site/search?f%5B0%5D.Type=RootCategory&f%5B0%5D.Value=activedirectory&f%5B0%5D.Text=Active%20Directory

[93] Script Repository: DNS Server **{R92}**:
http://www.microsoft.com/technet/scriptcenter/scripts/network/dns/default.mspx

The *Active Directory Domain Services*[94] Web page details how to programmatically achieve many of the routine AD DS tasks, such as managing users, groups, backing up and restoring AD DS.

One of the most significant additions to Windows Server 2008 R2 is the inclusion of support for Powershell v2.0 for AD DS administration. Powershell is the powerful new scripting and administration framework for Windows Server and Microsoft Server products going forward[95]. Windows Server 2008 R2 includes over 80 Powershell cmdlets dedicated to automating and administering AD DS[96].

For batch administration of AD DS, using both the LDAP Data Interchange Format (LDIF) utility (ldifde.exe) and several sample programs written using the Microsoft Visual Basic Scripting Edition (VBScript) development system, see the *Step-by-step guide to Active Directory bulk import and export*[97]. Note that this document was released for Windows 2000 Server and has not been updated. As such it may contain some outdated material, but it remains a useful resource to a Windows Server 2008 R2 user.

9.2.3 Products that Automate Operational Activities

Larger deployments of AD DS within healthcare organisations that have many domain controllers and sites, or that provide a critical service and cannot afford the cost of lost productivity because of a service outage, should use an enterprise-level monitoring solution.

> **Recommendation**
>
> The monitoring solution that best meets the organisation's requirements should be used, but the important indicators should be monitored to ensure that all aspects of AD DS are functioning correctly. The chosen monitoring solution should be implemented and fully proven in a lab before deploying it in the production environment.

9.3 AD DS Administrative Tools

Administrators can use a number of methods to configure and manage AD DS domain and forest environments. Windows Server 2008 R2 contains a rich set of tools and features that can be used to manage the Windows environment, including AD DS and its associated network services. Microsoft no longer provides separate tools through mechanisms such as the Windows Server Resource Kit or Support Tools as the most relevant and practical tools have been incorporated into the Windows Server Operating system.

[94] Using Active Directory Domain Services **{R93}**:
http://msdn2.microsoft.com/en-gb/library/aa746434.aspx

[95] Microsoft Powershell {**R108**}:
http://technet.microsoft.com/en-us/library/bb978526.aspx

[96] Active Directory Module for Windows Powershell {**R109**}:
http://technet.microsoft.com/en-us/library/dd378783(WS.10).aspx

[97] Step-by-Step Guide to Active Directory Bulk Import and Export **{R94}**:
http://technet.microsoft.com/en-us/library/bb727091.aspx

A number of sections in the Windows Server 2008 R2 product Help include discussions on appropriate AD DS graphical user interface (GUI) based tools, command line tools, and scripts. Table 19 below provides references to useful information for those administering AD DS. Unfortunately there is no corresponding information for Windows Server 2008 R2.

Administration Area	Internet Reference
Information about the technologies, issues, and methods to consider when deciding which tools to use to perform management tasks.	Windows Server commands, references and tools[98]
Background information on the tools that can be installed remotely to administer Windows Server 2008 R2.	Windows Server 2008 Remote Server Administration Tools (RSAT)[99]
For an overview of the key Windows Server 2008 R2 administration interface , providing more technical details on how it supports and manages the various Windows Server 2008 R2 roles and role	TechNet Library: Server Manager[100]
Information and a detailed reference about administering Active Directory with Windows Powershell	Active Directory Administration with Windows Powershell[101]
A technical reference that details how to use and configure Windows Performance Monitor	Windows Performance Monitor[102]
A detailed reference of the areas covered and reported on by the Best Practices Analyzer for Active Directory Domain Services.	Best Practice Analyzer for Active Directory Domain Services[103]

Table 19: Active Directory Administrative Tools Internet References

[98] Windows Server Commands, References and Tools **{R95}**:
http://technet.microsoft.com/en-us/library/dd560674(WS.10).aspx

[99] Remote Server Administration Tools **{R96}**:
http://technet.microsoft.com/en-us/library/cc731209.aspx

[100] Windows Server 2008 and Windows Server 2008 R2 Server Manager **{R98}**:
http://technet.microsoft.com/en-us/library/cc770629(WS.10).aspx

[101] Administration with Windows Powershell **{R99}**:
http://technet.microsoft.com/en-us/library/dd378937(WS.10).aspx

[102] Windows Performance Monitor **{R100}**:
http://technet.microsoft.com/en-us/library/cc749249.aspx

[103] Best Practice Analyzer for Active Directory Domain Services **{R101}**:
http://technet.microsoft.com/en-us/library/dd391875(WS.10).aspx

APPENDIX A SKILLS AND TRAINING RESOURCES

The tables in this Appendix provide details of the suggested training and skill assessment resources available. This list is not exhaustive; there are many third-party providers of such skills. The resources listed are those provided by Microsoft.

PART I MICROSOFT ACTIVE DIRECTORY

For further information on Active Directory, see http://www.microsoft.com/activedirectory

Skill or Technology Area	Resource Location	Description
Active Directory Design, including DNS design	http://technet.microsoft.com/en-us/library/cc732058(WS.10).aspx	Links to sections on designing AD DS components
DC capacity planning, site design and DC placement	As above	As above
Operations Master roles: placement of role holders, troubleshooting role holders and management	As above	As above
OU design	As above	As above

Table 20: Microsoft Active Directory 2008 R2 Training and Skill Assessment Resources

PART II GROUP POLICY, BOTH DOMAIN AND LOCAL

For an overview of Group Policies, see http://www.microsoft.com/grouppolicy.

Skill or Technology Area	Resource Location	Description
Controlling operating system configuration and security	http://www.microsoft.com/grouppolicy	Follow links on the page to resources
Design and implementation for application deployment	As above	As above
Management using GPMC: scripting, policy export and import, backup and restore	As above	As above
Implementation within an Active Directory OU hierarchy, and using security groups to control scope	As above	As above

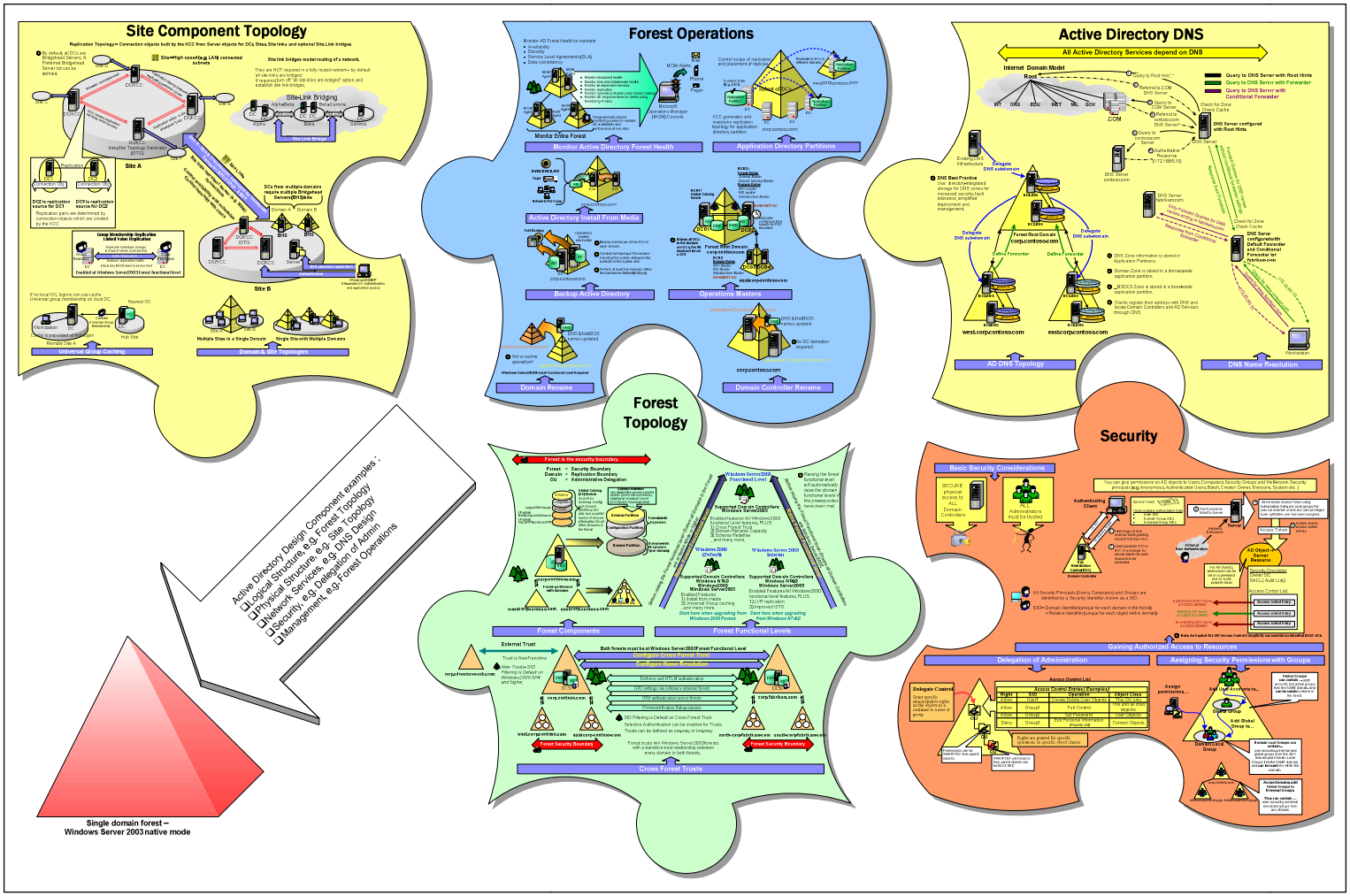
Table 21: Local and Domain Group Policy Training and Skill Assessment Resources

PART III NETWORK SERVICES

Skill or Technology Area	Resource Location	Description
DNS	http://technet.microsoft.com/en-us/library/cc732997(WS.10).aspx	The Windows Server 2008 DNS Website
	http://www.microsoft.com/dns	The Windows Server DNS technology Website
DHCP	http://technet.microsoft.com/en-us/library/cc896553(WS.10).aspx	The Windows Server 2008 DHCP Technology Website
WINS	http://technet.microsoft.com/en-us/library/cc771750(WS.10).aspx	The Windows Server 2008 WINS technology Website
Network Policy and Access Technologies	http://technet.microsoft.com/en-us/library/cc754521(WS.10).aspx	The Windows Server 2008 and Windows Server 2008 R2 Network Policy and Access technologies such as Network Access Protection
DirectAccess	http://technet.microsoft.com/en-us/library/dd630627(WS.10).aspx	The Windows Server 2008 R2 DirectAccess technology Website

Table 22: Network Services Training and Skill Assessment Resources

APPENDIX B WINDOWS SERVER 2003 ACTIVE DIRECTORY DESIGN COMPLEXITY



This diagram is included for reference. It has not been updated for Windows Server 2008 or Windows Server 2008 R2 but still provides a useful pictorial overview of the key AD DS components.

APPENDIX C AD DS FUNCTIONALITY FEATURES

Feature	Functionality
Multiple selection of user objects	Allows modification of common attributes of multiple user objects at one time.
Drag and drop functionality	Allows moving of Active Directory objects from container to container by dragging one or more objects to a location in the domain hierarchy. It is also possible to add objects to group membership lists by dragging one or more objects (including other group objects) to the target group.
Efficient search capabilities	Search functionality is object-oriented, and provides an efficient search that minimises network traffic associated with browsing objects.
Saved queries	Allows saving of commonly used search parameters for reuse in Active Directory Users and Computers.
Active Directory command-line tools	Allows running of new directory service commands for administration scenarios.
InetOrgPerson class	The inetOrgPerson class has been added to the base schema as a security principal and can be used in the same manner as the user class.
Application directory partitions	Allows configuring of the replication scope for application-specific data among domain controllers. For example, control the replication scope of DNS zone data stored in AD DS so that only specific domain controllers in the forest participate in DNS zone replication.
Ability to add additional domain controllers by using backup media	Reduces the time it takes to add an additional domain controller in an existing domain by using backup media.
Universal group membership caching	Prevents the need to locate a GC across a WAN when logging on by storing universal group membership information on an authenticating domain controller.
Secure LDAP traffic	AD DS administrative tools sign and encrypt all LDAP traffic by default. Signing LDAP traffic guarantees that the packaged data comes from a known source and that it has not been tampered with.
Partial synchronisation of the GC	Provides improved replication of the GC when schema changes add attributes to the GC partial attribute set. Only the new attributes are replicated, not the entire GC.
Active Directory quotas	Quotas can be specified in AD DS to control the number of objects a user, group, or computer can own in a given directory partition. Members of the Domain Administrators and Enterprise Administrators groups are exempt from quotas.
Active Directory Recycle Bin	Deleted objects have their attributes retained so that Administrators can restore accidentally deleted objects without having to resort to the most recent AD DS backup.
Active Directory Best Practice Analyzer	Provides a summary view of where the current AD DS configuration deviates from the recognised recommended practices for configuring and deploying AD DS.
Fine Grained Password Policies	A mechanism that allows administrators to configure different password policies for distinct and separate groups of users.
Read Only Domain Controllers	Domain controllers that will not allow changes to be made locally to AD DS and will only replicate changes in from a Read Write domain controller. Supports separation of administration as well as providing a way of deploying domain controllers to remote locations without the risks of compromising the AD DS.
Restartable Active Directory Domain Services	The capability to pause and stop AD DS on a domain controller to carry out updates or repairs without having to stop or restart the whole server.
Directory Service Auditing	The whole auditing subsystem has been revamped to allow a more granular and targeted approach to auditing. Introduction of audit subcategories allows for individual elements of auditing to be enabled or disabled allowing a measured and precise approach to auditing AD DS activities.

Table 23: Windows Server 2008 R2 AD DS Features

Windows Server Domain Functional Level	Supported Domain Controller Operating Systems	Advanced Features Available at Each Domain Functional Level`
Windows 2000 native	Windows 2000 Windows Server 2003	All default AD DS features, all features from the Windows 2000 mixed domain functional level and: ■ Universal Groups are enabled for both distribution and security groups ■ Group conversion is enabled, allowing conversion between security and distribution groups ■ Group nesting is available, allowing nesting of groups within other groups ■ Security identifier (SID) history is available, allowing the migration of security principals from one domain to another
Windows Server 2003	Windows Server 2003 Windows Server 2003 R2 Windows Server 2008 Windows Server 2008 R2	All default AD DS features, all features from the Windows 2000 native domain functional level and: ■ Supports new functionality of the netdom.exe tool to prepare domain controllers for rename. It is recommended to rename a domain controller by using netdom.exe to ensure that all appropriate steps are taken ■ Enables updates to the logon timestamp attribute. The *lastLogonTimestamp* attribute is updated with the last logon time of the user or computer. This attribute is replicated within the domain ■ Provides the ability to set the *userPassword* attribute as the effective password on inetOrgPerson and user objects ■ Provides the ability to redirect the Users and Computers containers in order to define a new well-known location for user and computer accounts ■ Allows for authorisation manager to store its authorisation policies in AD DS ■ Includes constrained delegation, which allows applications to take advantage of the secure delegation of user credentials by means of the Kerberos authentication protocol. Delegation can be configured to be allowed only to specific destination services ■ Supports selective authentication, by which it is possible to specify the users and groups from a trusted forest who are allowed to authenticate to resource servers in a trusting forest
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2	All of the default AD DS features, all of the features from the Windows Server 2003 domain functional level, and the following features are available: ■ Distributed File System (DFS) replication support for the Windows Server 2003 System Volume (SYSVOL) ■ DFS replication support provides more robust and detailed replication of SYSVOL contents ■ Advanced Encryption Standard (AES 128 and AES 256) support for the Kerberos protocol ■ Last Interactive Logon Information: Last Interactive Logon Information displays the following information: The time of the last successful interactive logon for a user The name of the workstation from which the used logged on ■ Fine-grained password policies: Fine-grained password policies make it possible for you to specify password and account lockout policies for users and global security groups in a domain

Windows Server Domain Functional Level	Supported Domain Controller Operating Systems	Advanced Features Available at Each Domain Functional Level`
Windows Server 2008 R2	Windows Server 2008 R2	All default AD DS features, all features from the Windows Server 2008 domain functional level, plus the following features: ▪ Authentication mechanism assurance, which packages information about the type of logon method (smart card or user name/password) that is used to authenticate domain users inside each user's Kerberos token. When this feature is enabled in a network environment that has deployed a federated identity management infrastructure, such as Active Directory Federation Services (AD FS), the information in the token can then be extracted whenever a user attempts to access any claims-aware application that has been developed to determine authorization based on a user's logon method.

Table 24: Windows Server 2008 R2 Domain Functional Levels

Windows Server 2003 Forest Functional Level	Supported Domain Controller Operating Systems	Advanced Features Available at Each Forest Functional Level
Windows 2000	Windows 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2	All default AD DS features.
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2	All Active Directory features available at the Windows Server 2000 functional level and: ■ Forest trust ■ Domain rename ■ Linked-value replication ■ Linked-value replication makes it possible for you to change group membership to store and replicate values for individual members instead of replicating the entire membership as a single unit. Storing and replicating the values of individual members uses less network bandwidth and fewer processor cycles during replication, and prevents you from losing updates when you add or remove multiple members concurrently at different domain controllers ■ The ability to deploy a read-only domain controller (RODC) ■ Improved Knowledge Consistency Checker (KCC) algorithms and scalability ■ The intersite topology generator (ISTG) uses improved algorithms that scale to support forests with a greater number of sites than AD DS can support at the Windows 2000 forest functional level. The improved ISTG election algorithm is a less-intrusive mechanism for choosing the ISTG at the Windows 2000 forest functional level ■ The ability to create instances of the dynamic auxiliary class named dynamicObject in a domain directory partition ■ The ability to convert an inetOrgPerson object instance into a User object instance, and to complete the conversion in the opposite direction ■ The ability to create instances of new group types to support role-based authorization ■ These types are called application basic groups and LDAP query groups ■ Deactivation and redefinition of attributes and classes in the schema
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2	All of the features that are available at the Windows Server 2003 forest functional level, but no additional features are available. All domains that are subsequently added to the forest, however, operate at the Windows Server 2008 domain functional level by default.
Windows Server 2008 R2	Windows Server 2008 R2	All of the features that are available at the Windows Server 2003 forest functional level, plus the following features: ■ Active Directory Recycle Bin, which provides the ability to restore deleted objects in their entirety while AD DS is running ■ All domains that are subsequently added to the forest will operate at the Windows Server 2008 R2 domain functional level by default

Table 25: Windows Server 2008 R2 Forest Functional Levels

APPENDIX D BACKGROUND INFORMATION FOR PLANNING DOMAIN CONTROLLER CAPACITY

Operation/Services	Variables Affecting Performance
PDC emulator operations master	The following operations typically have a high impact on the performance of the PDC emulator: ▪ Password change forwarding and logon forwarding requests with mismatched passwords for users, computers, and service accounts ▪ Group Policy updates ▪ The initial update of DFS ▪ Replicating directory changes to Windows NT4.0 BDCs
AD DS replication: ▪ Replication to partner Domain controllers	The impact varies depending on the number and type of replication partners. Replicating to more than fifteen intersite partners can have a high impact on performance.
Workstation logon: ▪ Startup process	The impact varies based on the number of workstations.
Application directory partition hosting	The impact varies based on the use of data that is contained in the application directory partition.
GC operations: ▪ Universal group membership lookups ▪ Forest-wide searches	If this domain controller functions as a GC server, performance varies according to the type of programs that are used. Programs that use GC searches extensively, such as Exchange 2000, have a high impact on performance.
Other operations: ▪ File and print	The impact varies based on the number of users who are using the domain controller as a file and print server.
Network Services: ▪ DNS ▪ WINS ▪ DHCP ▪ IPSec	The impact varies based on the number of services that are performed by the domain controller. For example, hosting multiple services, such as DNS, WINS, and DHCP, typically has a high impact on performance. Hosting a single service, such as DNS, typically has a low impact on performance. For IPSec, the impact on performance varies according to the number of connections.
Users logging on: ▪ User authentication ▪ Authorisation for resource access requests	The impact varies based on the number of users.
Look-up operations: ▪ LDAP searches	The impact varies based on the type of searches and the number of searches that the program performs and whether they use the newer features such as Variable List View or paged searches, whether the searches query against indexed attributes and whether the queries are scoped.
Infrastructure operations master	The validation of links to moved objects typically has a low impact on performance.
RID pool operations master	RID pool distribution typically has a low impact on performance.
Schema operations master	Modification to the schema typically has low impact on performance.
Domain naming operations master	The addition or deletion of domains typically has low impact on performance.

Table 26: Effect of Operations and Services on Domain Controller Performance

Component	Operations Performed	RAID System
Operating system files	Read and write operations	RAID 1
Active Directory log files	Mostly write operations	RAID 1
Active Directory database and SYSVOL shared folder	Mostly read operations	RAID 1 or RAID 0+1

Table 27: RAID System Requirements

> **Note**
>
> If cost is a factor in planning for disk space, then the operating system and Active Directory database should be placed on one RAID array (such as RAID 0+1), and the Active Directory log files on another RAID array (such as RAID 1). However, it is recommended that the Active Directory database and the SYSVOL shared folder are stored on the same drive.

APPENDIX E AD DS TESTS

The following list identifies some of the key tests which can be performed to prove the installation and design of AD DS:

- Verify hardware configuration of the domain controllers
- Verify system information on the domain controllers
- Verify the TCP/IP configurations and network components on the domain controllers
- Verify forward and reverse name resolution on the domain controllers
- Verify RAID and disk drive configurations on the domain controllers
- Verify the time information on the domain controllers
- Verify that Terminal Services are installed in Remote Administration mode on the domain controllers
- Verify *boot.ini* configurations on the domain controllers
- Verify connectivity for the domain controllers
- Verify shares on the domain controllers
- Verify that the event ID 13516 is logged in the event log (SYSVOL initialised)
- Verify that the *DCPromo.log*, *DCPromoui.log*, and *netsetup.log* logs are error free
- Run **nltest** to confirm domain controllers in the domain and verify that the secure channel works
- Confirm all the forests (and therefore domains) are running in native mode
- Verify that there are multiple forests, if relevant
- Verify the different domains, if relevant
- Verify that the internal OU design for the domain is correct
- Verify that the internal OU design for the service owner OUs of the domain is correct
- Verify the placement of the GC servers
- Verify the placement of the Operations Master roles
- Verify that the site design is correct
- Verify that the subnet allocation is correct
- Verify that the site links are established between the correct sites
- Verify that the site link properties are correctly configured
- Verify that the server objects are in the correct sites
- Verify that the different member servers are placed in the correct OUs
- Verify the LDAP Policy configuration
- Ensure that the Active Directory user functionality is normal
- Confirm that **dcdiag** and **netdiag** do not report any errors
- Use **replmon** to confirm error free replication between the domain controllers
- Run **repadmin** to confirm replication partners for each domain controller server
- Failover internal AD DS servers under load conditions

- Ensure that under load conditions, NIC teaming works fine on the domain controllers
- Verify that the DDP and DDCP are applied properly
- Ensure that any external or cross-forest trusts between forests are working correctly
- Verify the administrative groups in Admins OU
- Verify ports configured for the Netlogon, NTDS, and FRS services on the domain controllers
- Verify that the AD DS operation under load in an integrated environment
- Verify that only the Domain Admins have the administrative permissions on the Active Directory Users and Computers MMC
- Test that DNS is functioning as required for AD DS
- Test that WINS is functioning as required for AD DS

This is a list of tests that was originally published as part of the Windows Server System Reference Architecture (WSSRA) which has subsequently been replaced with the Infrastructure Planning and Design (IPD) series. The details of the tests were not carried forward into the IPD and so have been lost. However the tests are noted above for reference and to provide guidance on the sort of tests that are useful in verifying the successful implementation and deployment of AD DS.

APPENDIX FDOCUMENT INFORMATION

PART I TERMS AND ABBREVIATIONS

Abbreviation	Definition
ACL	Access Control List
ADFS	Active Directory Federation Service
ADSI	Active Directory Scripting Interface
AG	Account Group
API	Application Programming Interface
BIND	Berkeley Internet Name Domain
CA	Certificate Authority
CMD	Command
CN	Common Name
CPU	Central Processing Unit
CUI	Common User Interface
DC	Domain Controller
DDCP	Default Domain Controller Policy
DDP	Default Domain Policy
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
EFS	Encrypted File System
FQDN	Fully Qualified Domain Name
FSMO	Flexible Single Master Operations
GPMC	Group Policy Management Console
GPO	Group Policy Object
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
IIFP	Identity and Integration Feature Pack
IFN	Install From Media
ILM	Identity Lifecycle Manager
IIS	Internet Information Server
IM&T	Information Management and Technology
IP	Internet Protocol
IPSec	Internet Protocol Security

Abbreviation	Definition
ISA	Internet Security and Authorisation Server
IT	Information Technology
KB	Knowledge Base
KCC	Knowledge Consistency Checker
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSP	Local Service Provider
MBSA	Microsoft Baseline Security Analyser
MMC	Microsoft Management Console
MOF	Microsoft Operations Framework
MSDN	Microsoft Developer Network
MSF	Microsoft Solutions Framework
NAT	Network Address Translation
NC	Naming Context
NetBIOS	Network Basic Input Output System
NTP	Network Time Protocol
OU	Organisational Unit
PCT	Primary Care Trust
PDC	Primary Domain Controller
PKI	Public Key Infrastructure
RAID	Redundant Array of Independent Disks
RDN	Relative Distinguished Name
RFC	Request For Comments
RG	Resource Group
RID	Relative Identifier
RIS	Remote Installation Services
RPC	Remote Procedure Call
RR	Resource Record
RSO	Reduced Sign On
SAM	Security Account Manager
SCW	Security Configuration Wizard
SDK	Software Development Kit
SID	Security Identifier
SIG	Special Interest Group
SMB	Server Message Blocks
SMTP	Simple Mail Transfer Protocol

Abbreviation	Definition
SP	Service Pack
SPN	Service Principal Name
SQL	Structured Query Language
SRV	Service
SSO	Single Sign On
TCO	Total Cost of Ownership
UPN	User Principal Name
UTF-8	Universal Transformation Format-8
VPN	Virtual Private Network
WAN	Wide Area Network
WINS	Windows Internet Name Service
WMI	Windows Management Interface
WSH	Windows Scripting Host
WSSRA	Windows Server System Reference Architecture
WSUS	Windows Software Update Service

Table 28: Terms and Abbreviations

PART II REFERENCES

Reference	Document	Version
R1.	Infrastructure Planning and Design: http://technet.microsoft.com/en-gb/library/cc196387.aspx	
R2.	Microsoft TechNet: Windows Server 2008 AD DS Design: http://technet2.microsoft.com/windowsserver/en/library/c283b699-6124-4c3a-87ef-865443d7ea4b1033.mspx	
R3.	Microsoft TechNet Windows Server 2008 and Windows Server 2008 R2: http://technet.microsoft.com/en-us/library/dd349801(WS.10).aspx	
R4.	Automated Build Healthcare Desktop and Server Guide http://www.microsoft.com/industry/healthcare/technology/hpo/desktop/desktop.aspx	2.0.0.0
R5.	Microsoft TechNet: Active Directory Services: http://technet.microsoft.com/en-us/library/dd578336(WS.10).aspx	
R6.	Microsoft TechNet: Windows Server Technologies: Networking: http://technet.microsoft.com/en-us/library/cc753940(WS.10).aspx	
R7.	Microsoft TechNet: Installed help for Windows Server 2008 R2: http://technet.microsoft.com/en-us/library/dd851728.aspx	
R8.	Microsoft Download Center: Active Directory (AD) Management Pack for Operations Manager 2007: http://www.microsoft.com/downloads/details.aspx?FamilyId=008F58A6-DC67-4E59-95C6-D7C7C34A1447&displaylang=en&displaylang=en	
R9.	MSDN: Windows Script Host: http://msdn2.microsoft.com/en-us/library/9bbdkx3k	
R10.	Microsoft Download Center: Active Directory in Networks Segmented by Firewalls: http://www.microsoft.com/downloads/details.aspx?FamilyID=c2ef3846-43f0-4caf-9767-a9166368434e&DisplayLang=en	
R11.	Microsoft TechNet: Microsoft Windows Server TechCenter: Active Directory Best practices: http://technet2.microsoft.com/WindowsServer/en/library/5712b108-176a-4592-bcde-a61e733579301033.mspx?mfr=true	
R12.	Microsoft TechNet: Microsoft Windows Server TechCenter: DNS best practices: http://technet2.microsoft.com/windowsserver/en/library/59d7a747-48dc-42cc-8986-c73db47398a21033.mspx	
R13.	Microsoft TechNet: Microsoft Windows Server TechCenter: WINS Best Practices: http://technet2.microsoft.com/windowsserver/en/library/ed9beba0-f998-47d2-8137-a2fc52886ed71033.mspx	
R14.	Microsoft Download Center: Job Aids for Windows Server 2003 Deployment Kit: http://www.microsoft.com/downloads/details.aspx?FamilyID=edabb894-4290-406c-87d1-607a58fc81f0&DisplayLang=en	
R15.	Microsoft TechNet: Microsoft Windows Server TechCenter: Identifying the Deployment Project Participants: http://technet.microsoft.com/en-us/library/cc732532(WS.10).aspx	
R16.	Microsoft TechNet: Microsoft Windows Server TechCenter: Forest Design Models: http://technet.microsoft.com/en-us/library/cc770439(WS.10).aspx	
R17.	Microsoft TechNet: Microsoft Windows Server TechCenter: Identifying Forest Design Requirements: http://technet.microsoft.com/en-us/library/cc730924(WS.10).aspx	

Reference	Document	Version
R18.	Service Administrator Scope of Authority: http://technet.microsoft.com/en-us/library/cc772268(WS.10).aspx	
R19.	Forest Design Models: http://technet.microsoft.com/en-us/library/cc770439(WS.10).aspx	
R20.	Group Policy for Healthcare Desktop Management http://www.microsoft.com/industry/healthcare/technology/hpo/desktop/grouppolicy.aspx	1.0.0.0
R21.	Microsoft TechNet: Microsoft Windows Server TechCenter: Trust Technologies: http://technet2.microsoft.com/windowsserver/en/library/9d688a18-15c7-4d4e-9d34-7a763baa50a11033.mspx and http://technet.microsoft.com/en-us/library/cc770299.aspx	
R22.	Microsoft TechNet: Multiple Forest Considerations in Windows 2000 and Windows Server 2003: http://technet2.microsoft.com/windowsserver/en/library/bda0d769-a663-42f4-879f-f548b19a8c7e1033.mspx	
R23.	Microsoft TechNet: Microsoft Windows Server TechCenter: Domain and Forest Trust Tools and Settings: http://technet2.microsoft.com/windowsserver/en/library/108124dd-31b1-4c2c-9421-6adbc1ebceca1033.mspx and http://technet.microsoft.com/en-us/library/cc770299.aspx	
R24.	Microsoft TechNet: Microsoft Windows Server TechCenter: Security Considerations for Trusts http://technet2.microsoft.com/windowsserver/en/library/1f33e9a1-c3c5-431c-a5cc-c3c2bd579ff11033.mspx and http://technet.microsoft.com/en-us/library/cc770299.aspx	
R25.	Naming conventions in Active Directory for computers, domains, sites, and OUs: http://support.microsoft.com/kb/909264	
R26.	Microsoft Help and Support: Information about configuring Windows for domains with single-label DNS names: http://support.microsoft.com/kb/300684	
R27.	IETF, The Internet Engineering Task Force: Request For Comments: http://www.ietf.org/rfc/rfc2822.txt	
R28.	Microsoft Help and Support: Users Can Log On Using User Name or User Principal Name: http://support.microsoft.com/kb/243280	
R29.	The Administrator Accounts Security Planning Guide: http://www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.mspx	
R30.	Automated Build Healthcare Desktop and Server Guide http://www.microsoft.com/industry/healthcare/technology/hpo/desktop/desktop.aspx	2.0.0.0
R31.	Microsoft Technet Centre: Running Domain Controllers in Hyper-V: http://technet.microsoft.com/en-us/library/dd363553(WS.10).aspx	
R32.	Microsoft Download Center: Branch Office Infrastructure Solution for Microsoft Windows Server 2003 Release 2: http://www.microsoft.com/technet/solutionaccelerators/branch/default.mspx	
R33.	Windows Server 2008 R2 AD DS Deployment Guide Web page: http://technet.microsoft.com/en-us/library/cc732877(WS.10).aspx	
R34.	FSMO placement and optimization on Active Directory domain controllers: http://support.microsoft.com/kb/223346	
R35.	Microsoft TechNet: Microsoft Windows Server TechCenter: Planning Operations Master Role Placement: http://technet.microsoft.com/en-us/library/cc754889(WS.10).aspx	

Reference	Document	Version
R36.	Site Link Properties: http://technet.microsoft.com/en-us/library/cc753700(WS.10).aspx	
R37.	Microsoft TechNet: Microsoft Windows Server TechCenter: Creating a Site Link Bridge Design: http://technet.microsoft.com/en-us/library/cc753638(WS.10).aspx	
R38.	Microsoft TechNet: Microsoft Windows Server TechCenter: Background Information for Planning Domain Controller Capacity: http://technet2.microsoft.com/windowsserver/en/library/52bf61a8-9845-4878-8fa4-a85c57fe25e51033.mspx	
R39.	Microsoft TechNet: Microsoft Windows Server TechCenter: Adding Domain Controllers to Support Replication Between Sites: http://technet2.microsoft.com/windowsserver/en/library/4a59cc62-9425-463f-89b6-95347e2ea91e1033.mspx	
R40.	Microsoft TechNet: Microsoft Windows Server TechCenter: Determining the Minimum Number of Domain Controllers Required: http://technet2.microsoft.com/windowsserver/en/library/2619a7f0-c6ab-435a-83db-34f1425107e71033.mspx	
R41.	Windows Server 2003: Deployment Whitepaper: Best Practice Guide for Securing Active Directory Installations: http://technet2.microsoft.com/windowsserver/en/library/edc08cf1-d4ba-4235-9696-c93b0313ad6e1033.mspx?mfr=true	
R42.	Microsoft Download Center: Best Practices for Delegating Active Directory Administration: http://go.microsoft.com/fwlink/?LinkID=22708	
R43.	Microsoft TechNet: Microsoft Windows Server TechCenter: Addressing User-Related Requirements: http://technet2.microsoft.com/windowsserver/en/library/a35e88e7-2504-4a60-ba78-7c9efa05d3fa1033.mspx	
R44.	Healthcare EFS Tool Administration Guide: http://www.microsoft.com/industry/healthcare/technology/hpo/security/EFSTool.aspx	1.0.0.0
R45.	Microsoft TechNet: Microsoft Windows Server TechCenter: Creating a Foundation for Authentication: http://technet2.microsoft.com/windowsserver/en/library/2df33645-5e3e-4b79-9733-ffa2a3cf60c41033.mspx	
R46.	Microsoft TechNet: Microsoft Windows Server TechCenter: Deployment Guide for the Security Configuration Wizard: http://technet2.microsoft.com/windowsserver/en/library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and Windows Server 2008 specific content http://technet.microsoft.com/en-us/library/cc731515(WS.10).aspx	
R47.	Microsoft TechNet: Extended Your Authentication Framework: http://technet2.microsoft.com/windowsserver/en/library/1d90e7c1-37e3-4efe-bf64-1b9ffa93b1a71033.mspx with supplementary information specific to Windows Server 2008 and Windows Server 2008 R2 http://technet.microsoft.com/en-us/library/dd548350(WS.10).aspx	
R48.	Microsoft TechNet: Microsoft Windows Server TechCenter: Defining Policies for Security Group Management: http://technet2.microsoft.com/windowsserver/en/library/033a0042-ff57-4657-8350-c7a6ebe3b8991033.mspx	
R49.	Microsoft TechNet: Microsoft Windows Server TechCenter: Selecting Local Groups or Domain Local Groups as Resource Groups: http://technet2.microsoft.com/windowsserver/en/library/1b3070ce-c6b1-4849-ae47-ce17bbec17ee1033.mspx	

Reference	Document	Version
R50.	Microsoft TechNet: Microsoft Windows Server TechCenter: Planning a Smart Card Deployment: http://technet2.microsoft.com/windowsserver/en/library/5229033e-232b-4f91-9f86-0cbbd7cfc5a81033.mspx	
R51.	Microsoft TechNet: Microsoft Windows Server TechCenter: DNS Concepts: http://technet.microsoft.com/en-us/library/dd197461(WS.10).aspx	
R52.	IETF, The Internet Engineering Task Force: Request For Comments: A DNS RR for specifying the location of services (DNS SRV): http://www.ietf.org/rfc/rfc2782.txt	
R53.	IETF, The Internet Engineering Task Force: Request For Comments: Dynamic Updates in the Domain Name System (DNS UPDATE): http://www.ietf.org/rfc/rfc2136.txt	
R54.	Configuring BIND to work with Microsoft Active Directory: http://www.microsoft.com/technet/archive/interopmigration/linux/mvc/cfgbind.mspx	
R55.	Microsoft Help and Support: How to configure DNS dynamic updates in Windows Server 2003: http://support.microsoft.com/kb/816592	
R56.	Microsoft TechNet: Microsoft Windows Server TechCenter: Deploying WINS: http://technet2.microsoft.com/windowsserver/en/library/a5e0f87f-9b40-47ed-b613-3b4963bd91e61033.mspx and http://technet.microsoft.com/en-us/library/cc771750(WS.10).aspx	
R57.	Microsoft Download Center: Active Directory in Networks Segmented by Firewalls: http://www.microsoft.com/downloads/details.aspx?FamilyID=c2ef3846-43f0-4caf-9767-a9166368434e&DisplayLang=en	
R58.	Microsoft Download Center: Running Domain Controllers in Hyper-V: http://technet.microsoft.com/en-us/library/dd363553(WS.10).aspx	
R59.	Microsoft Download Center: Creating a Test Plan: http://technet2.microsoft.com/windowsserver/en/library/998c2ebb-ff0d-4bd5-82ae-d500966250121033.mspx	
R60.	Microsoft TechNet: Microsoft Windows Server TechCenter: Planning the Test Plan: http://technet2.microsoft.com/windowsserver/en/library/05f4d318-f2b4-4544-b50a-6aef2174532a1033.mspx	
R61.	Microsoft TechNet: Microsoft Windows Server TechCenter: Documenting the Test Lab Configuration: http://technet2.microsoft.com/windowsserver/en/library/232b6b08-d5b7-4437-bddf-a142636091741033.mspx	
R62.	Microsoft TechNet: Microsoft Windows Server TechCenter: Developing an Incident-Tracking System: http://technet2.microsoft.com/windowsserver/en/library/e213d6a5-7d4e-48cf-87b8-00eb52aae61f1033.mspx	
R63.	Microsoft TechNet: Microsoft Windows Server TechCenter: Creating a Pilot Plan: http://technet2.microsoft.com/windowsserver/en/library/99f07a8e-503b-4751-b108-c85e188ada951033.mspx	
R64.	Microsoft TechNet: Microsoft Windows Server TechCenter: Preparing for the Pilot http://technet2.microsoft.com/windowsserver/en/library/0a5f853e-28d2-4afe-a9db-92761a8d3ed61033.mspx	
R65.	Configuring DNS for the Forest Root Domain: http://technet.microsoft.com/en-us/library/cc771849(WS.10).aspx	
R66.	Microsoft TechNet: Microsoft Windows Server TechCenter: Verify DNS for the Forest Root Domain: http://technet.microsoft.com/en-us/library/cc754529(WS.10).aspx	
R67.	Windows Server 2008 Deployment Guide: Reconfigure the DNS service: http://technet.microsoft.com/en-us/library/cc732922(WS.10).aspx	

Reference	Document	Version
R68.	Microsoft TechNet: Microsoft Windows Server TechCenter: [DCInstall] (Unattended Installation): http://technet2.microsoft.com/WindowsServer/en/library/9639f180-c7fe-41c6-8c3d-92389023f0e71033.mspx	
R69.	Microsoft Help and Support: How to use the Install from Media feature to promote Windows Server 2003-based domain controllers: http://support.microsoft.com/kb/311078.	
R70.	Microsoft TechNet: Windows Server 2008: Transfer operations master roles: http://technet.microsoft.com/en-us/library/cc816946(WS.10).aspx	
R71.	Microsoft TechNet: Active Directory Delegation Tools: http://technet.microsoft.com/en-us/library/cc756087(WS.10).aspx and for Windows Server 2008 http://technet.microsoft.com/en-us/library/dd145344.aspx	
R72.	Microsoft TechNet: Microsoft Operations Framework 4.0: http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofeo.mspx	
R73.	Microsoft Download Center: Microsoft Solutions Framework Core White Papers: http://www.microsoft.com/downloads/details.aspx?FamilyID=e481cb0b-ac05-42a6-bab8-fc886956790e&DisplayLang=en	
R74.	WSUS: http://www.microsoft.com/windowsserversystem/updateservices/default.mspx	
R75.	Baseline Security Analyser (MSBA): http://www.microsoft.com/technet/security/tools/mbsahome.mspx	
R76.	Active Directory Product Operations Guide TechNet article: http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/adpog/adpog1.mspx	
R77.	DNS Product Operations Guide TechNet article: http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/dnspog/dnspog1.mspx	
R78.	WINS Product Operations Guide TechNet article: http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/winspog/winspog1.mspx	
R79.	Microsoft TechNet: Microsoft Windows Server TechCenter: Monitoring Domain Controller Performance: http://technet2.microsoft.com/windowsserver/en/library/c5d72b6f-5974-4263-b29f-2eece0ab44371033.mspx	
R80.	Microsoft TechNet: Microsoft Windows Server TechCenter: Performance and Reliability Monitor overview: http://technet.microsoft.com/en-us/library/cc771692(WS.10).aspx	
R81.	Microsoft TechNet: Microsoft Windows Server TechCenter: Active Directory Operations Guide: http://technet.microsoft.com/en-us/library/cc816807(WS.10).aspx	
R82.	Microsoft TechNet: Microsoft Windows Server TechCenter: DNS Server Operations Guide: http://technet.microsoft.com/en-us/library/cc816603(WS.10).aspx	
R83.	Microsoft TechNet: Microsoft Windows Server TechCenter: Group Policy Planning and Deployment Guide: http://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx	
R84.	Microsoft TechNet: Windows Server 2003 Product Help: Common Administrative Tasks: http://technet2.microsoft.com/windowsserver/en/library/f2d54234-6d65-439b-9d3b-ac1c4b2a3f991033.mspx	
R85.	Microsoft TechNet: Microsoft Windows Server TechCenter: Active Directory Step-by-step Guides: http://technet.microsoft.com/en-gb/windowsserver/2008/default.aspx	
R86.	Performance Tuning Guidelines for Windows Server 2003 whitepaper: http://go.microsoft.com/fwlink/?LinkId=24798	

Reference	Document	Version
R87.	Microsoft TechNet: Microsoft Windows Server TechCenter: Windows Server 2003 Performance Counters Reference: http://technet2.microsoft.com/WindowsServer/en/Library/3fb01419-b1ab-4f52-a9f8-09d5ebeb9ef21033.mspx	
R88.	Microsoft TechNet: Active Directory Product Operations Guide, chapter 3: http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/adpog/adpog3.mspx	
R89.	Microsoft Download Center: Active Directory Forest Recovery whitepaper: http://go.microsoft.com/fwlink/?LinkId=13079	
R90.	Microsoft TechNet: Script Center: http://www.microsoft.com/technet/scriptcenter/default.mspx	
R91.	Microsoft TechNet: Script Repository: Active Directory: http://www.microsoft.com/technet/scriptcenter/scripts/ad/default.mspx	
R92.	Microsoft TechNet: Script Repository: DNS Server: http://www.microsoft.com/technet/scriptcenter/scripts/network/dns/default.mspx	
R93.	MSDN Library: Using Active Directory Domain Services: http://msdn2.microsoft.com/en-gb/library/aa746434.aspx	
R94.	Microsoft TechNet: Microsoft Windows Server TechCenter: Step-by-Step Guide to Active Directory Bulk Import and Export: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/adbulk.mspx	
R95.	Microsoft TechNet: Windows Server Commands, References and Tools: http://technet.microsoft.com/en-us/library/dd560674(WS.10).aspx	
R96.	Microsoft TechNet: Remote Server Administration Tools: http://technet.microsoft.com/en-us/library/cc731209.aspx	
R97.	Microsoft Download Center: Windows Server 2003 Service Pack 2 32-bit Support Tools: http://www.microsoft.com/downloads/details.aspx?familyid=96A35011-FD83-419D-939B-9A772EA2DF90&displaylang=en	
R98.	Microsoft TechNet: Windows Server 2008 and Server 2008 R2 Server Manager: http://technet.microsoft.com/en-us/library/cc770629(WS.10).aspx	
R99.	Microsoft Download Center: Administration with Windows Powershell: http://technet.microsoft.com/en-us/library/dd378937(WS.10).aspx	
R100.	Microsoft TechNet: Windows Performance Monitor: http://technet.microsoft.com/en-us/library/cc749249.aspx	
R101.	Microsoft TechNet Best Practice Analyzer for Active Directory Domain Services: http://technet.microsoft.com/en-us/library/dd391875(WS.10).aspx	
R102.	Naming conventions in Active Directory for computers, domains, sites, and OUs: http://support.microsoft.com/kb/909264	
R103.	Microsoft Download Center: Branch Office Infrastructure Solution for Windows Server 2008 http://www.microsoft.com/downloads/details.aspx?familyid=02057405-49AF-4867-BF1D-E0232B5C59E3&displaylang=en	
R104.	Microsoft Technet: Configure the Operations Master roles: http://technet.microsoft.com/en-us/library/cc732963(WS.10).aspx	
R105.	Microsoft Technet: Appendix of Unattended installation parameters: http://technet.microsoft.com/en-us/library/cc732086(WS.10).aspx	
R106.	Microsoft Technet: Installing an additional domain controller by using IFM: http://technet.microsoft.com/en-us/library/cc816722(WS.10).aspx	

Reference	Document	Version
R107.	Microsoft Technet: Installing AD DS from media: http://technet.microsoft.com/en-us/library/cc770654(WS.10).aspx	
R108.	Windows Powershell: http://technet.microsoft.com/en-us/library/bb978526.aspx	
R109.	Microsoft Technet: Active Directory Module for Windows Powershell: http://technet.microsoft.com/en-us/library/dd378783(WS.10).aspx	

Table 29: References