Active Directory Domain Services in the Perimeter Network (Windows Server 2008)

Microsoft Corporation

Published: April 2009

Author: Davanand Bahall

Editor: Jim Becker

Technical Contributors: Raul Gonzalez Rodriguez, Rob Lane, Nathan Muggli, and Siddharth Bhai

Abstract

This guide contains direction for determining whether Active Directory Domain Services (AD DS) is appropriate for your perimeter network (also known as the DMZs or extranets), the various models for deploying AD DS in perimeter networks, and planning and deployment information for Read Only Domain Controllers (RODCs) in the perimeter network.

Because RODCs provide new capabilities for perimeter networks, most of the content in this guide describes how to plan for and deploy this new Windows Server 2008 feature. However, the other Active Directory models introduced in this guide are also viable solutions for your perimeter network.

Microsoft

Contents

Active Directory Domain Services in the Perimeter Network (Windows Server 2008) 5
Planning your perimeter network 5
Corporate and remote access to perimeter network resources 6
Centrally managed perimeter network resources 7

Planning Deployment of AD DS in the Perimeter Network 7
AD DS models for the perimeter network 7
No AD DS 8
Isolated forest model 8
Extended corporate forest model 9
Forest trust model 10
Choosing the proper deployment scenario in the perimeter network 11
Planning for RODCs in the perimeter network 15
Application compatibility 16
Applications that require AD DS 17
Replacing a writeable domain controller with an RODC 17
Client computer updates 19
Impact of data that is stored on RODCs in a perimeter network 19

Designing RODCs in the Perimeter Network 21
Promoting the RODC 21
Recommendations 21
Configuring DNS for name resolution and registration 22
Considerations 22
Approaches and configuration options 23
No DNS 23
Manual administration of host (A) resource records 23
Open DNS communication with writeable domain controllers 23
Using DHCP server to perform name registration for clients 24
Administrative Role Separation 25
Recommendation 25
Configuring the RODC Password Replication Policy 25
Choosing which accounts should be cached 25
User accounts 25
Computer accounts 26
Further considerations 26
Administering the PRP 26
Monitoring PRP compliance 26
Active Directory replication 27
Considerations 27

Approaches and recommendations 27
Securing RODC communication 28
Writeable domain controller vs. RODC 28
RODC improvements 28
Considerations 28
Security 28
Performance 28
Reliability 29
Approaches 29
Technologies options 29
IPsec 29
Client firewall 30
Design options 31
Communication from client computers that belong to the perimeter network 31
Communication from the RODC to a writeable domain controller 31
Communication from the perimeter network to a writeable domain controller 31
Tools 32
Required communication ports 32
Domain join using RODC 34
RODC vs. writeable domain controller 34
RODC improvements 34
Considerations 34
Approaches 34
Allow a join with a writeable domain controller 34
Join through the RODC 35
Tools 35

Deploying RODCs in the Perimeter Network 35
Deploying an RODC in the perimeter network 35
Prepare the intranet forest and domain for the RODC 35
Prepare the server that is to be promoted to be the RODC 37
Prepare firewall rules for communication from the RODC to the writeable domain controller 37
Promote the RODC server 39
Configure DHCP on the RODC 40
Add computers to the perimeter network site 40
Assumptions 40
Performing a domain join through an RODC 41
Precreate the computer account 41
Set a nondefault password for the computer account 41
Make the account cacheable at the RODC 42
Replicate the secrets of the computer account to the RODC 43
Run the join script on the client computer 43
Sample script for RODC domain join 43

Active Directory Domain Services in the Perimeter Network (Windows Server 2008)

Perimeter networks (also known as DMZs or extranets) can be a challenging environment for an information technology (IT) department. Security mandates, such as auditing and protecting assets, often contrast with the constantly changing connectivity requirements of mobile and remote users and applications that are deployed in a perimeter network.

This guide contains information about the following:

- Determining whether Active Directory® Domain Services (AD DS) is appropriate for your perimeter network
- The various models for deploying AD DS in perimeter networks
- Planning and deploying read-only domain controllers (RODCs) in perimeter networks

Because RODCs provide new capabilities for perimeter networks, most of the content in this guide describes how to plan for and deploy this new Windows Server 2008 feature. However, the other Active Directory models introduced later in this guide are also viable. Choose an appropriate model in accordance with the business needs of your organization.

In this guide

Planning Deployment of AD DS in the Perimeter Network

Designing RODCs in the Perimeter Network

Deploying RODCs in the Perimeter Network

Planning your perimeter network

Applications that provide services to customers, partners, and corporate users drive the security and connectivity requirements of a perimeter network. These applications greatly influence the design of the network topology and the infrastructure services that are provided.

As shown in the Figure 1, a typical perimeter network design can require constraints on communication between the internal network and the perimeter network. The constraints can be modeled either at the physical network layer (routers and firewalls) or at a logical layer (Internet Protocol security (IPsec), Secure Sockets Layer (SSL), and so on.

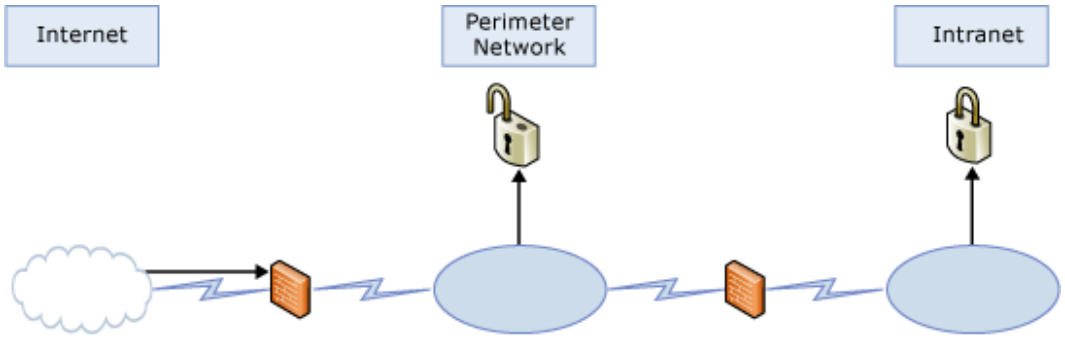

Figure 1 Perimeter networks

Corporate and remote access to perimeter network resources

Many organizations provide resources in their perimeter networks that customers, partners, and corporate users need to access. Typical resources include Microsoft® Office SharePoint® Server 2007 for collaborating on documents, SQL Server databases, or tools such as remote connection software. Planning for and deploying identity infrastructure for partner or customer resource access is beyond the scope of this document. However, this document describes the following scenarios:

1. Intranet identities access resources that are also accessible to partners.
2. Intranet identities access resources that are dedicated to those identities (such as e-mail).

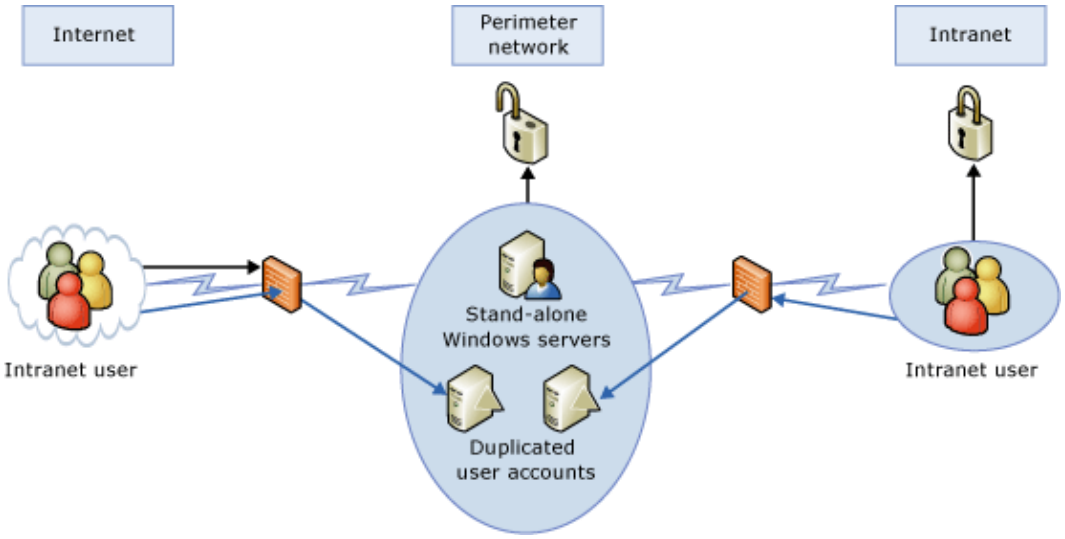

Figure 2 Using perimeter networks to manage identities that access resources

As shown in Figure 2, placing Active Directory servers in the perimeter network is a strong consideration for organizations that have intranet-owned identities that are needed for authentication or authorization. AD DS in the perimeter network also enables scalability and is a cost-effective way to manage the users and computers.

Centrally managed perimeter network resources

As shown in Figure 3, many solutions for AD DS in perimeter networks require a large number of servers as a result of different layers of design or the number of front-line servers that are required for workload balance.

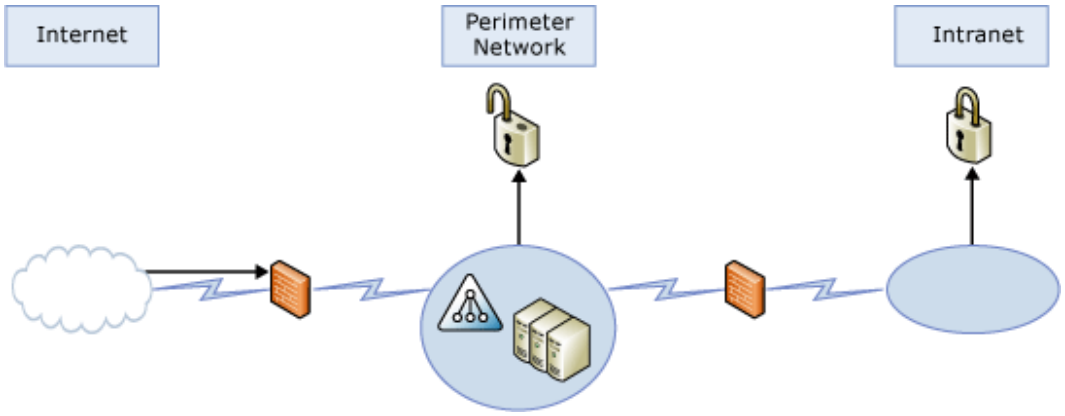

Figure 3 Perimeter solutions often require a large number of servers

The central or delegated administration, management, and configuration that AD DS provides can be a key consideration in your decision to place domain controllers in your perimeter network. Placing servers that belong to the perimeter network solution in a domain or organizational unit (OU) makes it possible to take advantage of the management technologies, tools, and procedures that are common to all Windows-domain-based systems.

Planning Deployment of AD DS in the Perimeter Network

This topic provides details to consider when you plan the deployment of Active Directory Domain Services (AD DS) in a perimeter network. These details include planning concerns and costs, different deployment models, and considerations for choosing an appropriate Active Directory deployment model.

AD DS models for the perimeter network

After you evaluate the considerations for deploying AD DS in your perimeter network, you can choose one or more of the following AD DS models.

After you read this guide, you may find that there is no benefit in including AD DS in your perimeter network or that other software or tools can provide all the benefits. If this is the case, it is possible that the best option is to not include AD DS in your perimeter network.

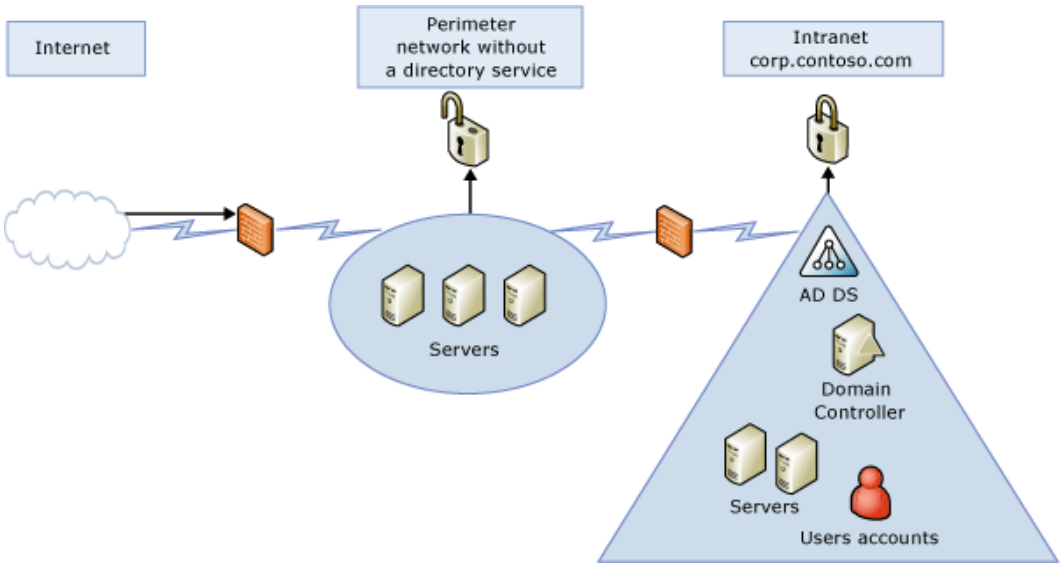

Figure 1 Perimeter model with no AD DS

No AD DS

One solution that you can implement in the perimeter network does not use AD DS. It uses the local server's Security Accounts Manager (SAM) database to authenticate corporate-network-owned identities. This solution, as shown in Figure 1, has the disadvantage of becoming very difficult to manage—even when there is a low number of users that are granted access to the server's resources—because you must manage the appropriate identities on several local SAMs. Another disadvantage is that more modern authentication methods, such as the Kerberos protocol or certificates, are not available for local SAM authentication.

In addition, this solution has the limitation of not being able to share identities between the servers. It also has a limitation on the number of users that can be stored locally. Duplication of identities across different databases increases the solution's total cost of ownership (TCO) and decreases the customer experience as a result of a lack of single-sign-on (SSO) functionality.

Isolated forest model

The isolated forest model provides the perimeter network with a dedicated deployment of AD DS. In this model, the forest in the perimeter network does not formally communicate with any forests in the internal network. The identities that are stored in this forest have meaning only inside the perimeter network solution, as shown in Figure 2.

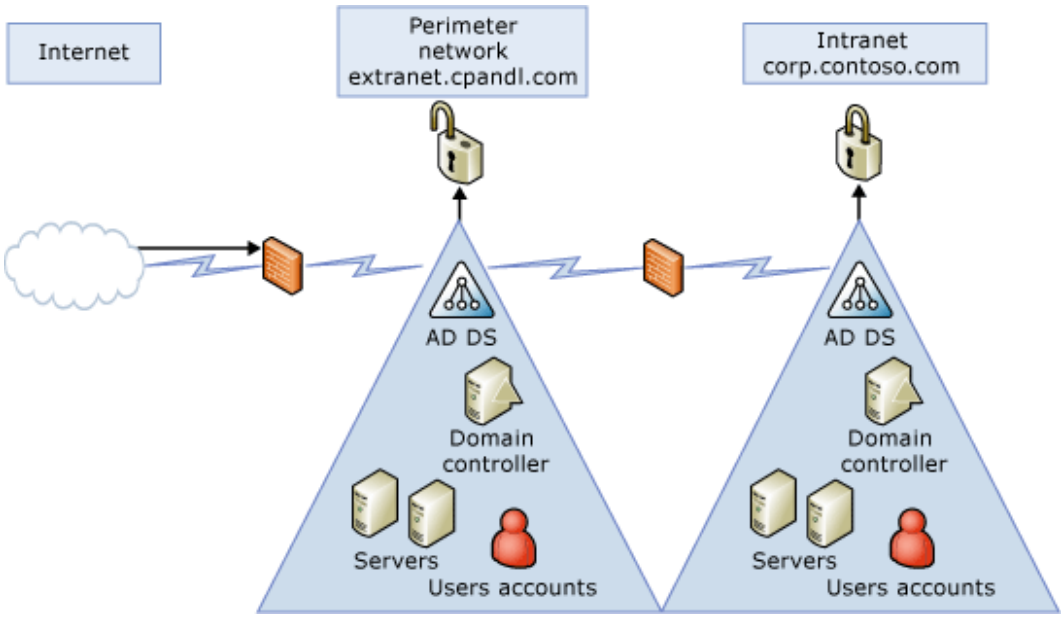

Figure 2 Isolated forest model

Consider this solution if your organization wants the manageability and security benefits that AD DS provides, but autonomy and isolation from any internal forests are also required. The Windows Server 2008 forest planning documentation explains the benefits of isolated forests. For more information, see Creating a Forest Design (http://go.microsoft.com/fwlink/?LinkId=135966).

Consider the use of an isolated forest in the perimeter in the following scenarios:

- A perimeter network in which SSO through Windows Integrated authentication between intranet-owned identities and extranet resources is not required. However, because of the number of computers in the perimeter network, the centralized management capabilities that AD DS provides are desired.
- An application that provides services in the perimeter network requires AD DS. Microsoft Exchange Server is an example of an application that requires AD DS to function, regardless of whether the forest has trust relationships with other domains or forests.

Extended corporate forest model

The solution that has an extended corporate forest in the perimeter places domain controllers—ideally, read-only domain controllers (RODCs)—that belong to the corporate forest in the perimeter network. As shown in Figure 3, this model takes advantage of the benefits of a single forest while enabling the use of corporate identities in the perimeter network.

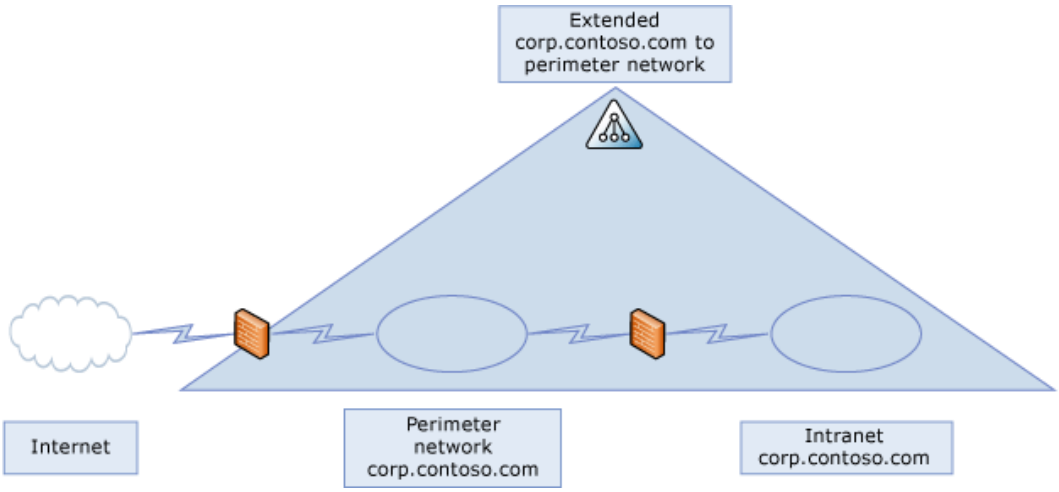

Figure 3 Extended corporate forest model

This model allows corporate identities to access resources in the perimeter network from both the Internet and the corporate network—if there is connectivity between the two networks—without requiring multiple identity stores (duplicating identities) or having to set up trust relationships between internal forest and perimeter forest for authentication.

Most of the directory information that is stored in the corporate Active Directory infrastructure is accessible to domain-joined computers or domain users in the perimeter network, as if they were accessing the directory on the internal network. This depends on the users being given appropriate permissions through access control lists (ACLs).

There are two variations of this model: One is to deploy writeable domain controllers from the corporate forest into the perimeter network. The second is to use RODCs. Because of the security and manageability benefits that are available with the RODC solution, this is the recommended model. However, if your current integrated application writes information to the directory, you might be blocked from using the new RODC role in the perimeter network. RODCs might also have application compatibility issues that require more planning and changes to your perimeter. More information about RODCs in the perimeter is provided later in this guide.

Forest trust model

The forest trust model is based on a forest that is deployed in the perimeter, like the isolated forest model. However, the forest trust model establishes Active Directory trusts with one or more forests in the internal network. In this design, a forest trust is established between the two forests to enable SSO scenarios for resource access and administration.

Figure 4 illustrates two forests—one forest in the internal network and the other forest in the perimeter network—with a trust between the two forests.

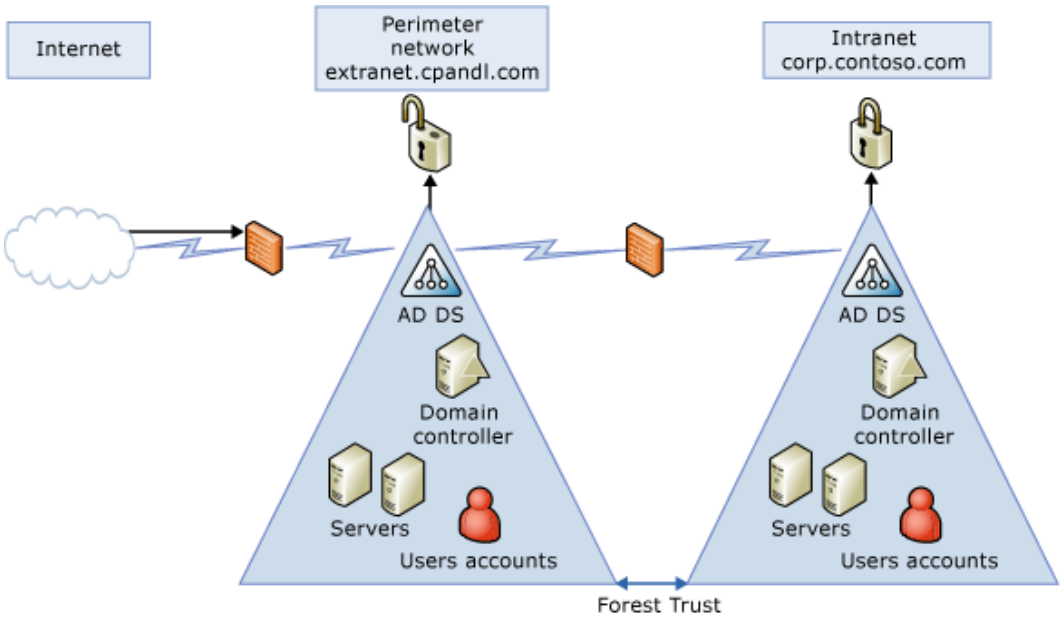

Figure 4 Forest trust model

This model helps reduce the exposure of corporate information in the perimeter network because directory information that is stored in one forest does not physically reside in the other forest. In addition, forest trusts can be unidirectional so that the perimeter network forest trusts the internal forest but not the other way around.

A drawback of this model is the increased administration costs of maintaining an extra forest and the added complexity of managing firewall rules for domain controllers and client computers crossing trust boundaries.

As a variation of this model, you can also use Active Directory Federation Services (ADFS) to create a federation with the perimeter forest. For more information, see the ADFS Deployment Guide. (http://go.microsoft.com/fwlink/?LinkId=135967).

Choosing the proper deployment scenario in the perimeter network

This section provides information to help you choose the correct AD DS deployment model for your perimeter network. The following table is a decision matrix that summarizes the advantages and disadvantages of all the domain models to help you determine which model is best for your environment.

Consideration	No AD DS	Isolated forest perimeter network	Extended corporate forest in the perimeter network	Forest trust in the perimeter network
What are my identity management requirements?	There is no need for large-scale identity management.	Identities in the perimeter have meaning only in the perimeter network, or another identity discovery solution.	The environment requires shared identities for the corporate network and the perimeter network to provide access to resources in the perimeter network.	The environment requires shared identities for the corporate network and the perimeter network to provide access to resources in the perimeter network.
What are my centralized management needs?	No centralized management solution is needed because of the small number of computers.	The centralized management benefits of AD DS are needed in the perimeter network. The greater the number of computers in the environment, the more benefit AD DS provides for actions such	The centralized management benefits of Active Directory are needed in the perimeter network. The greater the number of computers in the environment, the more benefit AD DS provides for actions such as defining Group Policy.	The centralized management benefits of AD DS are needed in the perimeter network. The greater the number of computers in the environment, the more benefit AD DS provides for actions such

Consideration	No AD DS	Isolated forest perimeter network	Extended corporate forest in the perimeter network	Forest trust in the perimeter network
		as defining Group Policy. However, models with separate corporate and perimeter networks result in administration of two or more separate Active Directory environments.		as defining Group Policy. However, models with separate corporate and perimeter networks result in administration of two or more separate Active Directory environments.
What are my SSO requirements?	No SSO is required. Identity discovery is not needed or resides in a single computer in this model.	SSO between the corporate network and the perimeter network is not desired. However, SSO is desired in perimeter network. Windows Integrated Authentication based on security protocol	SSO between the corporate network and the perimeter network is desired. Windows Integrated Authentication based on security protocol features such as Kerberos delegation can provide SSO functionality. SSO can also maintain the levels of authentication and authorization.	SSO between the corporate network and the perimeter network is desired. Windows Integrated Authentication based on security protocol features such as Kerberos delegation can provide

Consideration	No AD DS	Isolated forest perimeter network	Extended corporate forest in the perimeter network	Forest trust in the perimeter network
		features such as Kerberos delegation can provide SSO functionality. SSO can also maintain the levels of authentication and authorization.		SSO functionality. SSO can also maintain the levels of authentication and authorization.
What type of access to and exposure control of personally identifiable information (PII) and high business impact (HBI) information do I want in my perimeter solution?	The corporate environment cannot afford any exposure of intranet data to perimeter network.	The corporate environment cannot afford any exposure of intranet data to perimeter network.	No PII or HBI is held by the corporate AD DS, or an appropriate Password Replication Policy (PRP) and filtered attribute set (FAS) to control the attributes that are replicated to the RODCs can help avoid exposure of the information. For more information about the FAS, see RODC Filtered Attribute Set, Credential Caching, and the Authentication Process with an RODC (http://go.microsoft.com/fwlink/?LinkId=133355).	The corporate environment cannot afford any exposure of intranet data to the perimeter network.
Do my perimeter applications store information	Perimeter applications do not store information	Perimeter applications store information in AD DS.	Perimeter applications store information in AD DS. Applications do not write information to the directory, without the need of opening extra ports in the firewall, and new RODC	Perimeter applications store information in AD DS.

Consideration	No AD DS	Isolated forest perimeter network	Extended corporate forest in the perimeter network	Forest trust in the perimeter network
in AD DS, and what are their compatibility requirements?	in AD DS.	Applications can write information to the directory or have compatibility issues that prevent the use of new RODC technology in the extended corporate forest model.	technology can be used.	Applications can write information to the directory or have compatibility issues that prevent the use of new RODC technology in the extended corporate forest model.

Planning for RODCs in the perimeter network

Because RODCs are a new feature in Windows Server 2008, the rest of this document describes the AD DS perimeter network models that use RODCs. To gain the full benefits of using RODCs and to mitigate any negative impacts to the perimeter network, an understanding of the features and constraints of RODCs is necessary.

From a security perspective, RODCs should be thought about as one piece of a larger IT strategy to reduce the attack surface of a perimeter network. Compared to writeable domain controllers, RODCs provide the direct security benefit of having a smaller attack surface. The specific security boundaries of RODCs are described in the Read-Only Domain Controller Planning and Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=135993).

An indirect benefit of RODCs is apparent when an IT architect or engineer examines the perimeter network as a part of the entire network. For example, consider an organization that provides a service that it sells to consumers and that it hosts in the perimeter network. This organization uses an application-specific account store and authentication mechanism (for example, Microsoft SQL Server® or Active Directory Lightweight Directory Services (AD LDS)). The organization decides to make the service available to its internal employees who register accounts with the service. The security engineer decides to audit the passwords of the employee accounts that are registered with the service and discovers that some employees used the same password for the service as they used to log on to the corporate network.

From a top-down security perspective, there is no actual trust relationship between the corporate logon accounts and the service accounts. However, in practical terms, if a sophisticated attacker takes over the service and has unfettered access to the account store that the service uses, that attacker can then use those passwords to gain access to the corporate network through remote access technologies or by gaining access to the physical corporate network. RODCs can help reduce the probability of this type of attack by ensuring that any employee that uses the service is using his or her corporate identity and authenticating through Windows Integrated Authentication. This eliminates the need to store any employee identities in the service for the purpose of authentication.

After security, the next biggest consideration for RODCs is application compatibility. An RODC is not a full, drop-in replacement for a writeable domain controller. This is for the most part intentional, to preserve the security boundaries discussed previously.

Application compatibility is a bigger consideration for an RODC in a perimeter network than for any other type of RODC deployment. This is because an RODC does not perform all the operations that a client computer or application may need from a domain controller. For example, an RODC does not process Lightweight Directory Access Protocol (LDAP) writes. Instead, it returns a referral for a writeable domain controller to the application. Depending on the network topology, the client computer may or may not be able to refer or forward the application to a writeable domain controller. Therefore, an RODC deployment in a perimeter network where client computers and applications can contact only an RODC must not be a scenario in which generic LDAP write operations are required.

IT architects and engineers must understand exactly how the client computers and applications interact with AD DS in the perimeter network. Group management and user provisioning are common scenarios that fail if they occur in the perimeter network and the application or client can contact only an RODC. RODCs can chain a limited number of scoped write operations, such as password updates, Service Principal Name (SPN) registration, and a few others. For a comprehensive list of the write operations that an RODC can perform see, the Read-Only Domain Controller Planning and Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=135993).

The following sections contain information about:

- Application compatibility
- Replacing a writeable domain controller with an RODC
- Client computer updates
- Impact of data that is stored on RODCs in a perimeter network

Application compatibility

If you want to block communication between the perimeter network and the internal corporate network, which contains writeable domain controllers, carefully consider the effect that placing RODCs in the perimeter network will have on your applications. For example, custom Active Directory Service Interfaces (ADSI) applications target writeable domain controllers by default because they pass a writeable-only flag. These applications must be modified to use a read-only flag. Otherwise, they will ignore the RODCs, which are read-only by design.

If you have an application in your perimeter network that requires LDAP writes or requests that must have communication to writeable domain controllers in the domain, in many instances the required communication ports for these applications are not opened through the firewall, and the application may fail. RODCs are best suited for an extranet environment in which Active Directory access is primarily read-only. There are some cases in which RODCs forward write requests to a writeable domain controller.

For more information about write requests that are forwarded to writeable domain controllers, see Application Compatibility with RODCs (http://go.microsoft.com/fwlink/?LinkId=135711).

Applications that require AD DS

In one possible scenario in a perimeter network, a certain product or solution requires AD DS, but because of other security constraints, extending the corporate Active Directory forest in the perimeter network is judged to be not desirable. In this scenario, you can take advantage of Windows Server 2008 technology and work around these constraints, providing an acceptable solution that places AD DS in the perimeter network. Figure 5 illustrates this scenario.

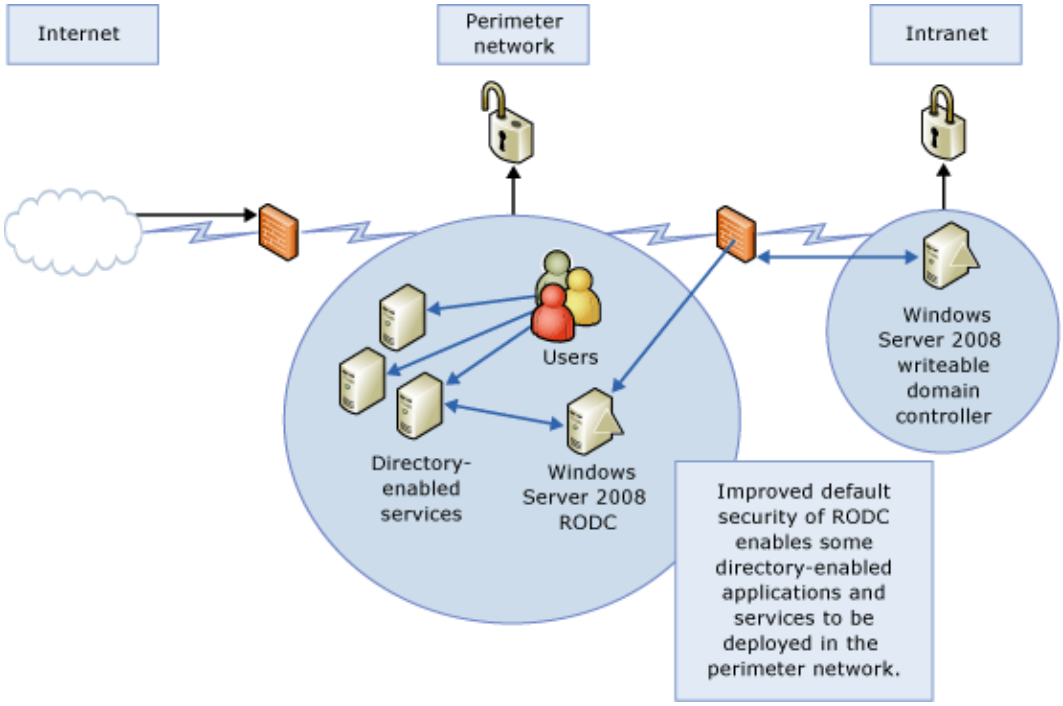

Figure 5 RODCs in perimeter deployments that require AD DS

We recommend that you check with the application vendor or independent software vendor (ISV) to determine whether the Active Directory–integrated application is compatible with RODCs.

Replacing a writeable domain controller with an RODC

The process for replacing a writeable domain controller with an RODC is the same regardless of whether or not it is deployed in a perimeter network. It is not possible to migrate a writeable

domain controller to a RODC. The best practices for replacing a writeable domain controller with an RODC are described in the Read-Only Domain Controller Planning and Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=135993).

Because deployments of AD DS in perimeter networks have existed long before RODCs, it is assumed that some organizations that are interested in deploying RODCs already have an existing AD DS deployment. For example, the organization in Figure 6 has an existing perimeter network.

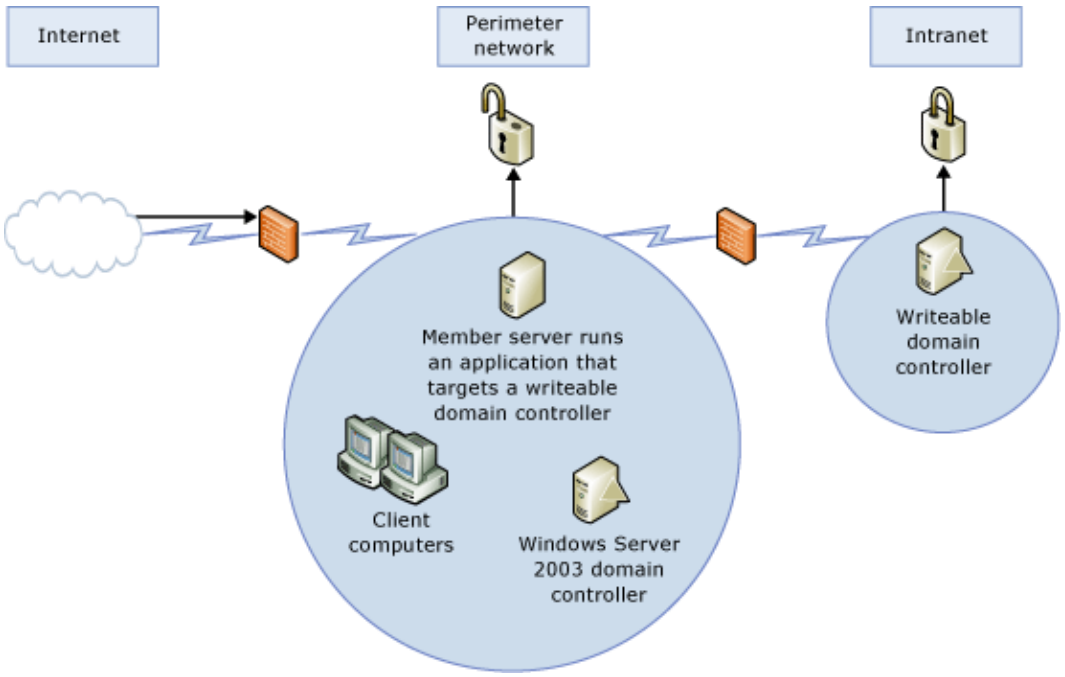

Figure 6 An organization with an existing perimeter network

The perimeter network has an application server that hosts a custom ADSI application, client computers, and a domain controller that runs Windows Server 2003. The organization is planning to replace the existing domain controller with an RODC to gain the advantages of RODCs. The new solution, after RODCs are deployed, is shown in Figure 7.

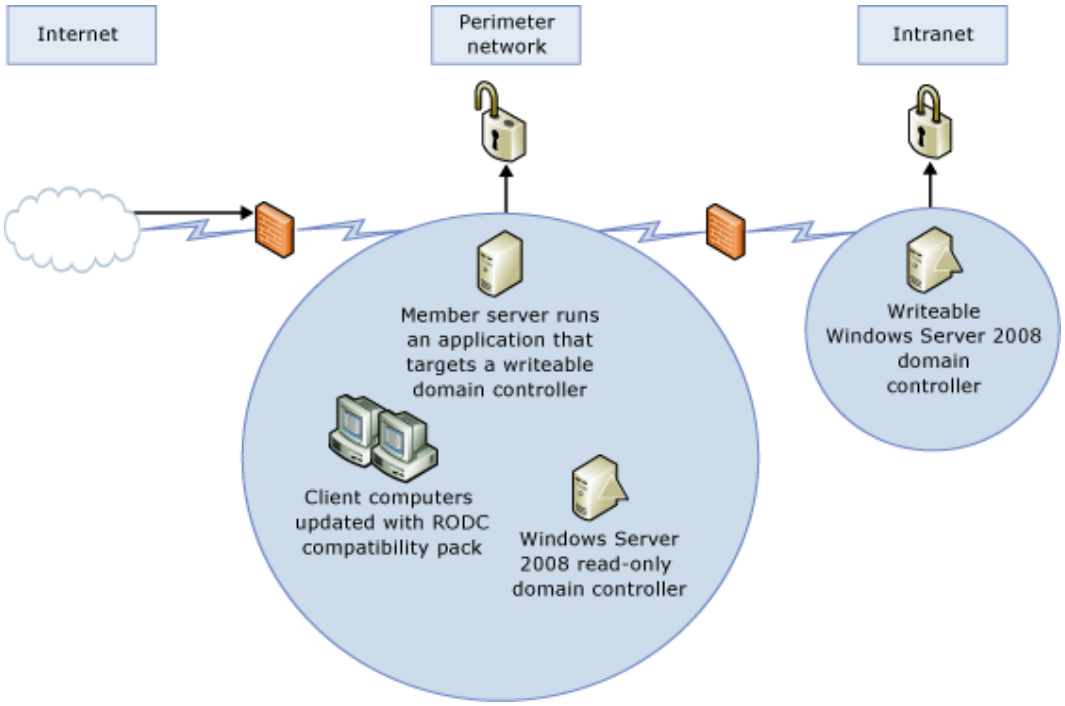

Figure 7 A writable domain controller replaced by an RODC in the perimeter network

Client computer updates

For member servers and client computers in the perimeter network that use an RODC, an update is available called the RODC compatibility pack. This update mitigates any issues that may occur when client computers interact with RODCs in their site.

For more information about client computer updates, see Known Issues for Deploying RODCs (http://go.microsoft.com/fwlink/?LinkID=135499).

For more information about the RODC compatibility, see Application Compatibility with RODCs (http://go.microsoft.com/fwlink/?LinkId=135711).To obtain the RODC compatibility pack, see article 944043 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkID=122974).

Impact of data that is stored on RODCs in a perimeter network

RODCs replicate most of the information in the directory. Therefore, organizations may be concerned about this data being replicated to the perimeter network. Figure 8 illustrates this concern.

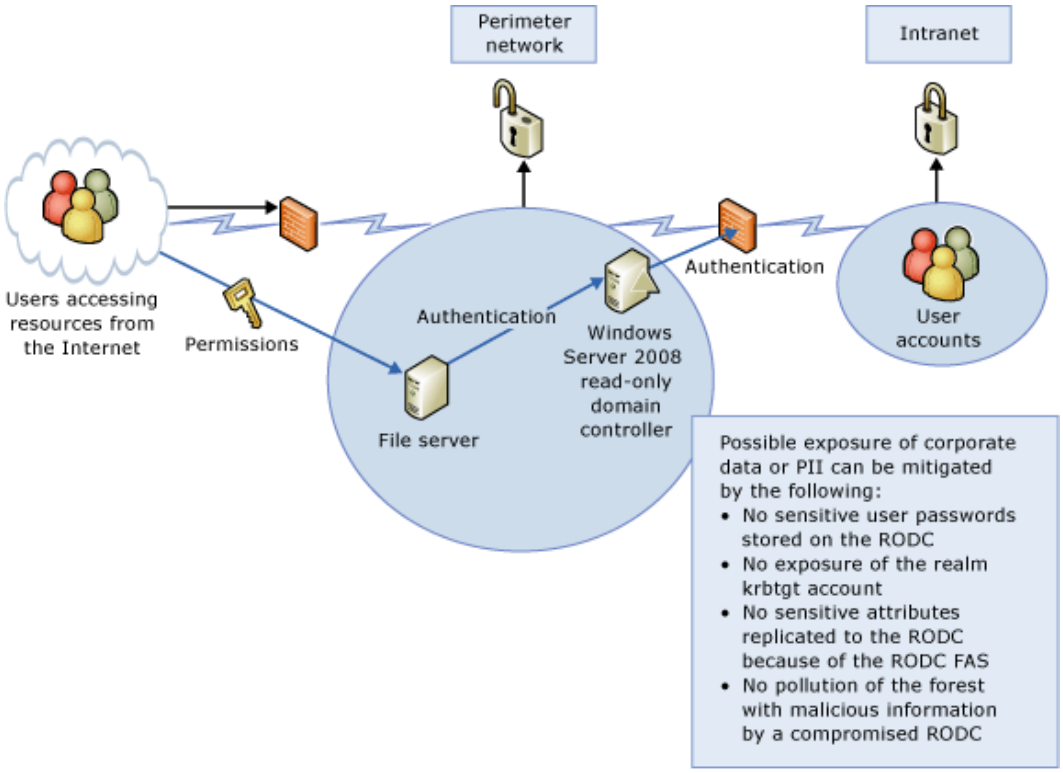

Figure 8 Data replication in an RODC

In some cases, the placement of a server in the perimeter network with information about your corporate network may not be a good idea. You have to decide how much information on a domain controller can be considered PII and HBI and how to avoid exposing this information.

There are some domain models that avoid placing sensitive information on a domain controller in the perimeter. However, Windows Server 2008 RODC technology adds extra features that reduce the exposure of sensitive information.

After taking security into account and evaluating the new features that Windows Server 2008 offers, you may come to the conclusion that placing domain controllers in the perimeter network is not your best option. Application constraints and the risk of the exposure of sensitive information not being reduced enough to meet corporate compliance standards may prevent your organization from taking advantage of the new technology. For example, if you have an application in the perimeter network that must read the Social Security number (SSN) of an employee that is stored in AD DS and exposing that identification number is too sensitive, you can add the SSN attribute to the FAS, which ensures that this attribute will not be exposed on the RODC.

Designing RODCs in the Perimeter Network

This topic describes the design of the extended corporate forest model in the perimeter network that uses a read-only domain controller (RODC):

- Promoting the RODC
- Configuring DNS for name resolution and registration
- Administrative Role Separation
- Configuring the RODC Password Replication Policy
- Active Directory replication
- Securing RODC communication
- Domain join using RODC

For more information about the extended corporate forest model, see “Extended corporate forest model” in Designing RODCs in the Perimeter Network.

Promoting the RODC

Consider the following when you promote an RODC that will be located in the perimeter network of your organization’s network infrastructure:

- Which network should the RODC be connected to during the promotion process—the internal network or the perimeter network?

  The decision about which network to promote the RODC in is important when there is a domain-based network access security policy, such as Internet Protocol Security (IPsec), in place. In this case, you must ensure that the RODC has the IPsec policy in place before it is exposed in the perimeter network.

- Should you use a two-stage promotion process?

  A new feature of Windows Server 2008 is the ability to delegate the operation of the promotion of an RODC from a security perspective. The promotion of an RODC can now be performed in two stages. The first stage requires Domain Admin privileges to create the information in Active Directory Domain Services (AD DS). The second stage involves a specific domain user or a group whose members do not have or need Domain Admin privileges. For more information about planning and deploying RODCs, see the Read-Only Domain Controller Planning and Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=135993).

Recommendations

When you promote an RODC that will be located in the perimeter network, the following actions are recommended:

- Use delegated two-stage promotion. This reduces the risk that may be associated with a Domain Admin level account interactively logging on to a server in the perimeter network.

The delegated promotion mechanism requires that the computer not be domain joined before the promotion. Therefore, a secure build of Windows Server 2008 should be used on this computer before it is placed in the perimeter network. A secure build is a build that is created with appropriate security configurations, such as appropriate firewall configurations, unnecessary services stopped, and so on.

- Install Windows Server 2008 using the Server Core installation option. This reduces the attack surface.
- If you are using IPsec, perform the promotion of the first RODC that will be placed in the perimeter network for a given domain from the internal corporate network or with full connectivity to a writeable domain controller.

This also provides an opportunity to perform important domain controller functionality tests, such as replication and authentication, before you place the domain controller in the perimeter network.

Note

Similar testing must be performed again after you move the RODC to the perimeter network.

Configuring DNS for name resolution and registration

As in all Active Directory deployments, Domain Name System (DNS) is a key part of the design. Domain controllers and client computers must be able to register, update, and resolve host names and service records. Best practices for DNS configurations on client computers and servers are still applicable for RODC deployments in perimeter networks. For more information, see the AD DS Deployment Guide (http://go.microsoft.com/fwlink/?LinkId=135996).

Considerations

The main difference in DNS configuration between a writable domain controller and an RODC is that the RODC will not be authoritative for any integrated zone; that is, it will not accept updates for any Active Directory–integrated DNS zone. Therefore, any dynamic update requests for an Active Directory–integrated zone will result in the requester being provided with the start of authority (SOA) resource record of the zone. This resource record will provide a reference to a server that is authoritative and writeable for the zone.

The read-only nature of Active Directory–integrated DNS on RODCs has the following implications in a perimeter network environment:

- It permits Active Directory–integrated zones to be available in the perimeter network without the risk of them being updated directly.
- However, it poses a problem of how secure dynamic updates can be established if they are required.

This leads to the following considerations for the design of a name resolution solution for the perimeter network:

- You must determine which namespaces must be visible.
- You must determine how those namespaces are to be updated: manually or dynamically.
- You must decide that, if dynamic updates are desired, how you can achieve this functionality within the constraints of communication inside the perimeter network and between the perimeter network and the corporate network.

The namespaces that are visible depend on whether domain controllers are deployed in the perimeter network and for which domain or forest. In some scenarios it may not be appropriate to make an entire namespace or part of a namespace visible in the perimeter network or for there to be any mechanism to allow servers or client computers to automatically update records. In other scenarios, these factors may not be a significant concern.

Approaches and configuration options

This section describes the approaches and options for configuring DNS for name resolution in the perimeter network.

No DNS

This highly restrictive approach avoids the need for hosting DNS namespaces in the perimeter network. With this approach, client computers in the perimeter network resolve names through HOST files or NetBIOS broadcasts. Any RODC in the perimeter network resolves names against a writable domain controller in the internal network and registers its DNS records against the writable domain controller through the firewall that separates the internal network from the perimeter network. This approach avoids exposure of any corporate DNS zones in the perimeter network.

Although this approach is possible, it is not practical. It does not scale well, and it incurs a high administrative cost when records must be kept up to date and consistent across more than a handful of computers.

Manual administration of host (A) resource records

With this approach, all host (A) resource records that are required in the perimeter network for name resolution are added manually, which helps avoid the need to open ports from the perimeter network to the writable domain controller. The RODC will still be able to update its records dynamically against the writable domain controller because a communication channel must be open between the RODC and writable domain controller for other domain-controller communications, such as replication. This approach works for highly controlled perimeter networks where there is little need for new registrations or updates to host (A) resource records.

Open DNS communication with writeable domain controllers

This approach is suitable for perimeter networks that must have dynamic updates enabled. With this approach there is open DNS communication from computers in the perimeter network to the writeable domain controllers. This makes it possible for computers in the perimeter network to

register their records directly against the writeable domain controllers. Even though computers in the perimeter network can communicate with a writable domain controller, having the RODC configured as a DNS server ensures that the DNS query load is handled by the RODC.

One possible issue with this configuration is that there might be a delay of up to four minutes before a new DNS resource record that is registered on the writable domain controller reaches the RODC through replication. This issue must be considered if there is a need for client computers to immediately resolve names that are registered by computers. For more information about how RODCs handle DNS updates, see Read-Only Domain Controller Planning and Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=135993).

Using DHCP server to perform name registration for clients

An alternative to allowing dynamic update registration through the firewall is to run a Dynamic Host Configuration Protocol (DHCP) server in the perimeter network and configure it to be able to perform registration of host (A) and pointer (PTR) resource records on behalf of client computers. If the DHCP role is combined with the RODC, it further reduces the number of servers that have to be allowed to pass DNS traffic through the firewall because it is assumed that the RODC is able to communicate directly with some subset of writeable domain controllers in its domain that reside in the internal network.

When you use this approach, we recommend that you:

- Configure the DHCP Server service to perform DNS updates with a specific service account. This ensures that records are registered in a manner that prevents their update in a way that is not secure.

  Note

  Do not add this service account to the DNSUpdateProxy group. For more information about the DNSUpdateProxy group, see article 816592 in the Microsoft Knowledge Base(http://go.microsoft.com/fwlink/?LinkID=133266).
- Create a scope that contains only reservations for the specific media access control (MAC) addresses of the servers in the perimeter network. This reduces the risk of an arbitrary client computer being placed on the perimeter network and registering its records in DNS.
- If the first DHCP server in the domain is to be installed on an RODC, it is important that you manually create the DHCP-Admin-related groups before this role is installed. RODCs are not allowed to create groups in their local Active Directory database. The DHCP groups that you must create in advance include the following:
  - DHCP Administrators (Domain Local)
  - DHCP Users (Domain Local)

For more information about using a DHCP server to perform name registration for client computers, see the following:

- DHCP Server Security (Part 1) (http://go.microsoft.com/fwlink/?LinkId=133263)
- DHCP Server Security (Part 2) (http://go.microsoft.com/fwlink/?LinkId=133264)

- Article 816592 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=133266)

Administrative Role Separation

The Administrative Role Separation feature that was introduced in Windows Server 2008 for RODCs makes it possible to create a delegated RODC administrator account. This account should be a regular domain user with limited rights in AD DS. For more information about Administrative Role Separation and best practices, see Read-Only Domain Controller Planning and Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=135993).

Recommendation

For RODCs that are located in a perimeter network, all local administrative server tasks (such as installing patches or modifying network settings) that must be completed with a direct logon to an RODC should be performed with a delegated RODC administrator account.

Configuring the RODC Password Replication Policy

A key RODC feature is the ability to restrict sensitive data such as passwords from being replicated to RODCs. By default, the Active Directory database of an RODC contains only the passwords for the RODC computer account and the associated Kerberos krbtgt account.

The mechanism for controlling which passwords get replicated to the RODC is known as the Password Replication Policy (PRP). The PRP offers administrators flexibility—from the extreme of the default policy, which allows only the passwords of the RODC computer account and the associated krbtgt account to be cached, to the least restrictive policy, which allows the passwords of all users except sensitive accounts, such as domain administrators, to be cached. For more information, see RODC Filtered Attribute Set, Credential Caching, and the Authentication Process with an RODC (http://go.microsoft.com/fwlink/?LinkId=133355).

When an RODC is deployed in the perimeter network and limiting the exposure of passwords is important, we recommend that you use a PRP, which is more restrictive. Typically, this means limiting the cacheable accounts to those accounts that are absolutely required inside the perimeter network.

Choosing which accounts should be cached

This section provides guidance about choosing the accounts to be cached on an RODC in your perimeter network.

User accounts

In scenarios in which corporate identities are used, it is probably desirable to allow as few accounts as possible to have their passwords replicated to the RODC. This should not affect the

user experience because the RODC is able to forward any authentication requests to a writeable domain controller.

User accounts for which it might be appropriate to allow caching include any accounts that are used for day-to-day configuration or monitoring of the RODC, such as accounts that are used for delegated administration through the Administrative Role Separation feature. The decision to allow these accounts to be cached is a tradeoff between ensuring that a user can log on locally in the absence of connectivity to a writeable domain controller and the consideration that the account password is stored in the perimeter network. Passwords for service accounts can also be included.

It should be noted that if communication to a writeable domain controller is not available, authentication fails for any accounts that do not have their passwords cached on the RODC.

Computer accounts

If there are servers in the perimeter network that are joined to the domain that the RODC is a member of, the PRP must be configured to allow the passwords for those servers to be replicated. Typically, these servers have little or no access to the corporate network. Therefore, they must build their secure channel against the RODC. This requires that the computer password be cached to allow the secure channel to be established to the RODC.

Note

If there are multiple RODCs for a given domain in the perimeter network, configure all of them with the matching PRP to avoid unexpected authentication failures if writeable domain controllers are not available.

Further considerations

To facilitate management and auditing of the PRP, we suggest that a per-domain "perimeter network RODC Allow" group be created and added to the **msdsRevealOnDemandGroup** attribute of the RODC. Any accounts that are determined to be cacheable will be added to this group. Using this type of group makes it possible for changes to be picked up by the default auditing scheme in Windows Server 2008. This results in Event ID 4756 when a security principal is added and Event ID 4757 when a security principal is removed.

Administering the PRP

For detailed information about how to administer the PRP, see Administering the Password Replication Policy (http://go.microsoft.com/fwlink/?LinkId=133488).

Monitoring PRP compliance

You may want to ensure that the principals whose passwords have been cached on the RODC match the expectation of the constraints that the PRP sets. If the PRP for the perimeter network RODC is controlled by a single group, this task involves comparing an export of the membership of the group with the constructed attribute **msDS-RevealedList** on the RODC computer account.

All the principals in the **msDS-RevealedList** output should be members of the perimeter network RODC Allow group, with the exception of the RODC account and the krbtgt account.

Active Directory replication

As a side effect of the read-only nature of the RODC, no new data originates from it. Consequently, there is no need to replicate data out of the perimeter network.

Considerations

The primary considerations for Active Directory replication in the perimeter network are domain controller placement, topology, and reliability. As with any other RODC deployment, the RODC must be able to replicate directly from a Windows Server 2008 writeable domain controller partner in the same domain. Therefore, physical connectivity to one or more writeable domain controllers is required and must be supported by a matching Active Directory site or site link configuration.

In addition, we recommend in the ”Securing RODC Communication” section, later in this topic, that the RODCs in the perimeter network be allowed to communicate only with a specific subset of the writeable domain controllers in its domain that reside in the internal network.

Approaches and recommendations

We recommend that you create a separate Active Directory site for the RODCs in the perimeter network. The writeable domain controllers that the RODCs can contact can be placed in a site of their own, with the appropriate subnet mapping and additionally consider enabling a site link between that site and the site that is specific to the RODCs in the perimeter network.

To avoid issues with a single point of failure, you may consider deploying multiple RODCs for each domain in the perimeter network.

In this case, it is important to ensure that the replication latency from the writeable domain controller to the RODC is reduced to an appropriate level.

For more information about Active Directory replication, see How Active Directory Replication Topology Works, (http://go.microsoft.com/fwlink/?LinkId=133487).

Another aspect of RODC design to consider is writeable domain controller communication with the RODC. This consideration is driven by the effort to simplify firewall configuration. We recommend that you statically assign the remote procedure call (RPC) ports that are used for replication traffic. This has the advantage of constraining, in advance, the firewall ports that must be open to enable the traffic between the domain controllers. For more information about replication traffic through a firewall, see the following:

- Article 224196 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=133489)
- Active Directory Replication over Firewalls (http://go.microsoft.com/fwlink/?LinkID=123775)

Securing RODC communication

To ensure security compliance and to reduce your organization's vulnerability to outside attack, it is critical that you secure the communication between the RODC and the internal corporate network.

Writeable domain controller vs. RODC

The main difference between a writeable domain controller and an RODC from a communication standpoint is that a writable domain controller, in a domain that operates at Windows Server 2008 domain functional level, does not create any connections for replication from an RODC. This allows for simpler planning by eliminating the need to plan for replication from the RODC to the writeable domain controller.

Note

The exception to this rule is a scenario in which SYSVOL replicates through File Replication Service (FRS), in which case the writeable domain controller must be able to open an RPC FRS connection to the RODC to allow the replication of SYSVOL content from the writeable domain controller to the RODC. This requirement does not exist when you use Distributed File System (DFS) replication for SYSVOL replication when your domain is at the Windows Server 2008 domain functional level.

RODC improvements

Reducing the inbound connections from other domain controllers to the RODC helps lower the cost of design and administration of communication policies (IPsEC and Firewall).

Considerations

Security is the most important consideration when you design your RODC communication model. Other considerations include performance, reliability, and diagnostics.

Security

As a general rule, allow only the minimum network traffic that is necessary to provide the intended service, and guarantee the correct level of reliability and supportability. To this extent you should test that the allowed traffic will permit failover and the use of diagnostic tools or troubleshooting tools. Another option is to create a recovery/troubleshooting process with a "troubleshooting communication policy" that sets up the environment for troubleshooting, when necessary, by allowing the traffic that is required for support and troubleshooting.

Performance

If you are using IPsec, the CPU load on the servers that are involved in the communication will be affected. The type of IPsec policy determines the increase in load. Authentication Header (AH) communication has less CPU usage than Encapsulating Security Payload (ESP). Firewall

configurations have an impact on performance, just as IPsec, does by blocking and permitting actions. To ensure that the impact due to IPsec is minimal, you should test solutions with different hardware and communication policies until the CPU load is deemed acceptable for your requirements.

Reliability

When you design the communication in your perimeter network solution, you should take into account the functionality that your router or firewall provides for filtering rules. RPC is one of the biggest considerations to take into account when you set firewall rules for domain members. You might find firewalls that are RPC-aware that allow the firewall to open ports based on previous communication though port TCP 135 (End Point Mapped), the appropriate port between the server and client that allows RPC dynamic port use.

This functionality allows greater flexibility when you configure RPC ports rules, although it may be too wide to open from a security point of view. You can choose an intermediate approach in which the router allows an RPC bind to a specific TCP port where a static RPC server is listening. This allows for the dynamic opening of the client RPC ports when servers reply. You can use this technology to avoid opening a wide range of ports in the router for RPC use. For more information see, Active Directory in Networks Segmented by Firewalls (http://go.microsoft.com/fwlink/?LinkID=45087).

The required RPC interfaces for using AD DS have been enabled for static assignment. As a result, you can now include design scenarios in which RPC interfaces are statically defined. Using this configuration, the routers in your environment can open RPC client ports on an RPC bind.

Approaches

You should enable traffic flow between the perimeter network and the corporate network by establishing filtering rules that you can use on the router firewall rules, the client firewall (Windows Firewall) rules, and the client IPsec policy. At the same time, you may have to enable integrity or encryption on the network traffic to increase the level of security. You can do this by using IPsec AH and IPsec ESP communication.

You can manage both client local Firewall and IPsec policy centrally from the Group Policy objects (GPOs) for the domain.

Technologies options

The two native Windows Server 2008 technologies that you can use for communication are IPsec and local Firewall.

IPsec

IPsec is a powerful filtering and communication tunneling tool that you can use to control the communication between pairs of computers or a group of computers. It offers levels of security

and encryption that can help reduce the number of “real” ports that are used, making the configuration of router firewall rules simpler. For more information about IPsec, see IPsec (http://go.microsoft.com/fwlink/?LinkID=136017).

Client firewall

You can use the client firewall (Windows Firewall) to control the traffic that is allowed in and out of the RODC or any other Windows-based computer, based on IP and originating traffic application. The following table explains the advantages and disadvantages of using these technologies.

Issue	IPsec	Windows Firewall
Router firewall ports	Allows the reduction of required ports on the firewall.	Does not reduce the required ports.
Block and permit	Allows blocking and permit rules.	Allows blocking and permit rules.
Integrity layer	Allows an Integrity check through the Authentication Headers (AH) protocol.	Does not allow an Integrity check.
Confidentiality layer	Allows a confidentiality layer if it is required by the Encapsulating Security Payload (ESP) protocol.	Does not allow a confidentiality layer.
CPU impact	Can increase CPU use in client computers and servers, depending on traffic load and the type of IPsec protocol that is used (none, AH, ESP).	No CPU impact.
Configuration	Centralized through a Group Policy object (GPO).	Centralized through a GPO.
Disable	Not easy to disable.	Easy to disable.
Policy synchronization	Requires policy synchronization between the source and destination.	No policy synchronization required.
Management cost	High management cost; you must confirm that all computers in the realm of the IPsec communication are in sync for changes to happen.	No much cost; the changed can be performed on a per-computer basis.

Issue	IPsec	Windows Firewall
Scope of the policy	Based on IP level fact as source IP, destination IP, and ports. At the same time, it can be based on Kerberos authentication if you rely on this protocol for Internet Key Exchange (IKE) key exchange.	A part of normal IP information as source/destination address and port; you can also base the configuration on the originator application.

Design options

The design options for RODC communication are split into three different segments:

- Communication from client computers that belong to the perimeter network
- Communication from the RODC to a writeable domain controller
- Communication from the perimeter network to the writeable domain controller

Communication from client computers that belong to the perimeter network

This communication depends on the solution that you implement in the perimeter network. You analyze each of the solution requirements to enable the necessary traffic into the RODC from the perimeter network.

For some examples of ports for different scenarios, see the “Required communication ports” section later in this topic.

Communication from the RODC to a writeable domain controller

To enable the RODC role on a server that is designated to be an RODC, there must be communication between that server and a writeable domain controller.

For the required the ports for each functionality, see the “Required communication ports” section later in this topic.

Communication from the perimeter network to a writeable domain controller

Based on the requirements of your RODC design, you may have to allow traffic from the perimeter network client computers and servers to a writeable domain controller that resides in the corporate network. For example, you may have to allow DNS traffic for dynamic updates, LDAP referrals, or other protocols, depending on your deployment scenario.

Tools

There are several tools that you can use to monitor the communication from the perimeter network to the internal corporate network:

- Sniffing tools, such as Microsoft Network Monitor and router filtering logging
- IPsec Mon
- Resultant Set of Policy (RSoP)
- Third-party traffic-monitoring tools

Note

Many of the traffic-monitoring solutions require traffic to reach the wire in clear format. IPsec ESP encrypts the content and prevents these tools from detecting traffic that may be coming from attacks. You can check whether your traffic-monitoring solutions are compatible with IPsec AH. This protocol does not encrypt the traffic, although it still permits IPsec security to be in place.

Required communication ports

The following table lists the ports that you must open on the firewall to allow communication from a writeable domain controller in the corporate network to the RODC in the perimeter network, along with the type of traffic that is used on these ports.

Port	Type of traffic
TCP 135	EPM
TCP Static 53248	FrsRpc
TCP 389	LDAP

Note

For more information about configuring file replication through a specific static port see the Microsoft support article, (http://go.microsoft.com/fwlink/?LinkId=149419)

The following table below lists the ports that you must open on the firewall to allow communication from the RODC in the perimeter network to a writeable domain controller in the corporate network, along with the type of traffic that is used on these ports.

Port	Type of traffic
TCP 57344	DRSUAPI, LsaRpc, NetLgonR
TCP Static 53248	FrsRpc
TCP 135	EPM
TCP 389	LDAP

Port	Type of traffic
TCP 3268	GC, LDAP
TCP 445	DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc
TCP 53	DNS
TCP 88	Kerberos
UDP 123	NTP
UDP 389	C-LDAP
UDP 53	DNS
TCP and UDP 464	Kerberos Change/Set Password

Note

For more information about configuring Active Directory replications through a specific port see the Microsoft support article, (http://go.microsoft.com/fwlink/?LinkID=133489)

The following table lists the ports that you must open on the firewall to allow communication between the member servers in the perimeter network and the RODC in the perimeter network, along with the type of traffic that is used on these ports. You must open these ports only if there is an internal firewall that separates your member servers in the perimeter network from the RODC in the perimeter network.

Port	Type of traffic
TCP 135	EPM
TCP 389	LDAP
TCP 445	DFS, LsaRpc, NbtSS, NetLogonR, SamR, SMB, SrvSvc
TCP 88	Kerberos
TCP Dynamic	DNS, DRSUAPI, NetLogonR, SamR
UDP 389	C-LDAP
UDP 53	DNS

Note

If you are using Windows Server 2003 in the perimeter network, you must also open port UDP 88 for Kerberos communication. In contrast, by default Windows Server 2008 uses only port TCP 88 for Kerberos communication.

Domain join using RODC

During deployment and management of the perimeter network, you have to join computers to the domain.

RODC vs. writeable domain controller

RODCs do not allow normal domain joins; they allow only ”read-only” domain joins. This is an unsecure join that requires no write to the database. Therefore, you must ensure that the appropriate information that is necessary for the join to succeed is in place before you proceed with the join.

RODC improvements

Because an RODC only allows ”read-only” domain joins, the security of the domain is enhanced if the RODC is compromised. To join a new member to the domain, you must perform certain actions on the writeable domain controller in advance.

Considerations

The Windows user interface (UI) does not perform a ”read-only” domain join by default. Regular UI domain-join code triggers a discovery for a writable domain controller. When that domain controller is found, a regular join is attempted. In most perimeter networks, the access to a writeable domain controller is blocked, even the discovery process fails. At the same time, the communication of a client computer using the Netlogon RPC interface that targets a writeable domain controller might be blocked also. Therefore, even if the discovery succeeds, the join fails.

To enable the domain join through an RODC, you must follow a process in which computer accounts, the PRP, and account passwords are updated on the writeable domain controller. After that you must use a specific tool (a script or executable file) that performs the RPC call with the required unsecure switch.

In addition, these new switches are not present on Windows systems that do not have the RODC compatibility pack installed. You must update these systems in advance with the RODC compatibility pack. To download the RODC compatibility pack, see article 944043 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkID=122974).

Approaches

This section describes the tasks to complete when you perform a domain join using an RODC.

Allow a join with a writeable domain controller

If you have a perimeter network solution that allows for a window of time when services are not available, you can configure connectivity rules that allow for direct communication between client computers and the domain’s writeable domain controller. You can consider the use of these windows of time to make the domain joins of the computers in the perimeter network.

Join through the RODC

Follow the steps in Deploying RODCs in the Perimeter Network section of this guide to perform a read-only domain join through the RODC.

Tools

In the Deploying RODCs in the Perimeter Network section of the guide, there is a sample script that you can use to perform a domain join with a RODC

Deploying RODCs in the Perimeter Network

This topic describes how to deploy a read only domain controller (RODC) in a perimeter network, thereby extending the corporate forest into the perimeter network.

Deploying an RODC in the perimeter network

To deploy an RODC in a perimeter network:

- Prepare the corporate forest and domain for the RODC
- Prepare the server that is to be promoted to an RODC
- Prepare firewall rules for communication from the RODC to the writeable domain controller
- Promote the RODC server
- Configure the RODC
- Add computers to the perimeter network site

Prepare the intranet forest and domain for the RODC

Complete the following procedure to prepare the corporate forest and domain for the RODC. Membership in **Enterprise Admins**, or equivalent, is the minimum required to prepare the corporate forest for an RODC. Membership in **Domain Admins**, or equivalent, is the minimum required if you are preparing a domain for a RODC. Review details about using the appropriate accounts and group memberships at http://go.microsoft.com/fwlink/?LinkId=83477.

To prepare the intranet forest and domain for the RODC

1. Ensure that you have completed the prerequisites for deployment of an RODC in domain and forests. For more information about RODC deployment, see Prerequisites for Deploying an RODC (http://go.microsoft.com/fwlink/?LinkId=133514).
2. Create an Active Directory site in the perimeter network, and call it the PerimeterNetwork site. For more information about creating a site in Active Directory Domain Services, see Adding a New Site (http://go.microsoft.com/fwlink/?LinkID=93237).
3. Create another Active Directory site in the internal corporate network. This site will be the closet intranet site to the perimeter network. It will contain the only writable domain

controllers that RODCs in the perimeter network can access. Call this site the PerimeterNetwork Support Site.

4. Create a site link between the PerimeterNetwork Site and the PerimeterNetwork Support Site with a 24x7x15 schedule and higher cost than normal. For more information about site linking, see Linking Sites for Replication (http://go.microsoft.com/fwlink/?LinkId=133515) and Changing Site Link Properties (http://go.microsoft.com/fwlink/?LinkId=133517).

   Note

   The higher cost of the site link between the site where the perimeter network's RODCs live and the intranet helps avoid the possibility of client computers in the corporate network site preferring the RODC site to another corporate site if a domain controller fails in the PerimeterNetwork Support Site.

5. Install two or more domain controllers in each domain that must validate users in the PerimeterNetwork Support Site. For information about installing an additional Windows Server 2008 domain controller, see Installing an Additional Windows Server 2008 Domain Controller (http://go.microsoft.com/fwlink/?LinkID=133258). For more information about installing a new Windows Server 2008 child domain, see Installing a New Windows Server 2008 Child Domain (http://go.microsoft.com/fwlink/?LinkId=133519).
6. Create a delegated RODC administrator account on each domain in the perimeter network. This can be a group or user account, but the best practice is for this account to be a group account. For more information about best practices for RODC administration, see "Delegating local administration of an RODC" in RODC Administration (http://go.microsoft.com/fwlink/?LinkId=133521).
7. Add the perimeter network administrator users, which can belong to PerimeterNetwork domain or UsersDomain, to the properly domain-linked, delegated RODC administrator group.
8. Create a PerimeterNetworkAllow group per domain.
9. Create a PerimeterNetworkDeny group per domain.
10. Add the delegated administrator group to the domain PerimeterNetworkAllow group for every domain.
11. If no other RODC will act as the Dynamic Host Configuration Protocol (DHCP) server in the domain, allow the DHCP role to run on the RODC. For more information about DHCP, see article 822048 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=133526). For more information about DHCP on a RODC, see Applications That Are Known to Work with RODCs (http://go.microsoft.com/fwlink/?LinkId=133779).

    Note

    If you are not using DHCP in your perimeter network, you can skip this step as DHCP is not required.

12. Create required Group Policy objects (GPOs) for the Perimeter Network domain:
    a. IPsec RODC-to-writeable domain controller communication policy
    b. Computer local firewall filter

    For more information about the IPSEC RODC-to-writeable domain controller communication policy and computer local firewall filter, see the Step-by-Step Guide to Internet Protocol Security (IPSec) (http://go.microsoft.com/fwlink/?LinkId=136018) and Checklist: Implementing a Standalone Server Isolation Policy Design (http://go.microsoft.com/fwlink/?LinkId=133780).

Prepare the server that is to be promoted to be the RODC

Complete the following procedure to prepare a server to assume the role of an RODC in the perimeter network. To complete this procedure, you need local server administrator credentials.

To prepare the server that is to be promoted to be the RODC

1. Install Windows Server 2008 in a secure configuration on the computer that will become an RODC.
2. Configure the network adapter of the server that will become an RODC with the appropriate static IP configuration.
3. Configure the IPsec Local policy definition to allow RODC-to-writeable domain controller communication based on the writeable domain controller's IPsec policy definition.

    Notes

    While it is suggested that RODC promotion be performed from the perimeter network local area network (LAN), it is not possible to promote the first RODC in the perimeter network by using IPsec as the only means of communication with writeable domain controllers. Therefore, the promotion must be performed with full communication to a writeable domain controller by placing it temporarily on an internal network. In this case, the IPsec policy that belongs to the local computer's GPO does not have to be active.

    If you install a second RODC in the perimeter network, you can use the IPsec policy to promote the server to an RODC.

Prepare firewall rules for communication from the RODC to the writeable domain controller

Complete the following procedure to prepare the firewall for RODC-to-writeable domain controller communication. To complete this procedure, you need local server administrator credentials.

Note

This procedure is only applicable is you are using IPsec. If you do not plan to use IPsec, you can skip this procedure.

To prepare the firewall rules for communication from the RODC to the writeable domain controller

1. Prepare ports for RODC-to-writeable domain controller communication.

   The choice of which ports to open depends in part on your decisions about:

   a. Which authentication method to use for IPsec communication: certificates or the Kerberos authentication protocol.

   b. Whether DNS updates are to be performed directly by client computers in the perimeter network or by a DHCP server.

2. Configure domain-based IPsec policy to enable communication between writeable domain controllers and RODCs after the RODC is placed in the perimeter network.

   You must make a choice between certificates and the Kerberos protocol. Certificates eliminate the requirement for Kerberos port 88 to be open on the firewall. For more information about certificates, see Certificates (http://go.microsoft.com/fwlink/?LinkId=136020) and Certificate stores (http://go.microsoft.com/fwlink/?LinkId=136019).

   For example, you might:

   a. Modify IPsec policy settings in Group Policy that applies to the domain controllers that must communicate with IPsec.

   b. Use the settings and methods in the following table.

Encryption	Integrity	Diffie Hellman
3DES	SHA1	2
3DES	MD5	2
DES	SHA1	1
DES	MD5	1

   IPFILTER: Ensure that the IP filter encompasses the writable domain controllers and the RODC that is being promoted.

   AUTHENTICATION: Add **Certificate** as an authentication mechanism and select the root certification authority (CA) for your enterprise. Ensure that the certificate method has priority over Kerberos authentication.

   FILTER ACTION: Set the security methods **Integrity Only** and **Integrity and Encryption**. Select the **Fall back to unsecured communication if secure not established** check box.

   When the settings are in place, mark the policy as assigned.

3. Prepare the certificate store on the RODC:

   a. Import the Root CA from the corporate CA into the Computer certificate store under **Trusted Root CAs**.

b. Import the IPsec CA from the corporate CA into the Computer certificate store under **Personal Certificates**.

4. Create a local IPsec policy on the computer to be **RODC**. The policy should include the following:
   a. An appropriate IPFILTER to specify communication between the RODC and writeable domain controllers
   b. The AUTHENTICATION method set to Certificates with the Corporate Root CA cert specified
   c. The FILTER ACTION that specifies methods and configuration that match the domain-based IPsec policy
5. Assign the local IPsec policy, and test that communication between the RODC and the writeable domain controller is successful.

Promote the RODC server

Complete the following two procedures to promote the RODC server. To complete the tasks in part 1 and part 2 of this procedure, you must have delegated RODC administrator credentials.

To promote the RODC server (part 1)

1. Precreate the RODC account.
2. Add the PerimeterNetworkAllow group to the RODC PRP Allow list.
3. Add the PerimeterNetworkDeny group to the RODC PRP Deny list.
4. Add the delegated RODC administrator group as a delegated administrator of RODC.

To promote the RODC server (part 2)

1. Install the RODC computer with a Secure Base Image.
2. Configure the RODC network adapter with the appropriate static IP configuration for the LAN where promotion will take place.
3. Import the IPsec Local policy definition to allow RODC-to-writeable domain controller communication based on the writeable domain controller IPsec policy definition. (Complete this step only if promotion is being performed from the perimeter network LAN.)
4. Run Dcpromo.exe with delegated RODC administrator account credentials using an answer file if you are using a Windows Server 2008 Core installation.

   For more information about using an answer file to run Dcpromo.exe on a server, see Installing a New Windows Server 2008 Forest by Using an Answer File (http://go.microsoft.com/fwlink/?LinkId=133800).

   The answer file should include a replication/source writeable domain controller.
5. Run a quality control test after you reboot the server.

Note

Repeat the Dcpromo operation for each RODC to be installed in the perimeter network.

Configure DHCP on the RODC

Complete the following procedure to configure DHCP on the RODC server in the perimeter network. To complete this procedure, you must have delegated RODC administrator credentials.

Note

If you do not plan to use DHCP on the RODC, you can skip this procedure.

To configure DHCP on the RODC

1. Install the DHCP Service on the RODC.
2. Add scope for the subnets in the Perimeter Network site.
3. Configure the scope options with the RODC's IP address as the DNS address. Use the RODC's IP address as the DNS setting for perimeter network clients.
4. Set the DHCP option to overwrite client requests and update DNS on behalf of client requests.
5. Configure a domain account to be used for performing DNS updates on behalf of client computers.
6. Add reservations for known client media access control (MAC) addresses in the perimeter network to associate them with IP addresses for servers in the Perimeter Network site.

Add computers to the perimeter network site

In this section, you will find instructions and a sample script that can be used to domain join a Windows Server 2008, Windows Server 2008 R2 or Windows Vista SP 1 machine to a perimeter network.

Note

For read-only domain joins on Windows Server 2003 or Windows XP client computers, install the RODC compatibility pack. For more information about the installation of the RODC compatibility pack see the Microsoft support article, http://go.microsoft.com/fwlink/?LinkID=122974.

Assumptions

The following conditions are assumed to be in place in order to complete a domain join through a read-only domain controller (RODC):

- The perimeter network and the intranet are separated by a firewall.

- The client computer can communicate with the RODC in the perimeter network but not with domain controllers in the internal network.
- The RODC can communicate with a domain controller in the internal network at the time of the domain join.
- The first four procedures have been completed before the join is attempted.
- If NETBIOS name resolution is required in the perimeter network, ensure Windows Internet Name Service (WINS) is enabled.

Performing a domain join through an RODC

Complete the following tasks to perform a domain join through an RODC. Domain Admin credentials are required to perform these tasks.

- Precreate the computer account
- Set a nondefault password for the computer account
- Make the account cacheable at the RODC
- Replicate the secrets of the computer account to the RODC
- Run the join script on the client computer

Precreate the computer account

In the following procedure, you precreate the computer account that you plan to join to the domain through an RODC.

To precreate the computer account

1. Log on to a domain controller in the internal network.
2. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog appears, confirm that the action it displays is what you want, and then click **Continue**.
4. At the elevated command prompt, type the following command, and then press ENTER:

   ```
   net computer \\comp1 /add
   ```

   Replace `comp1` with the name of the computer account that is to join the domain.

Set a nondefault password for the computer account

In the following procedure, you set a nondefault password for the computer account. In general, whenever you create a computer account, a default password is created.

To set a nondefault password for the computer account

1. Log on to a domain controller in the intranet.
2. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog appears, confirm that the action it displays is what you want, and then click **Continue**.

4. At the elevated command prompt, type the following command, and then press ENTER:

   ```
   net user comp1$ <password>
   ```

   Replace `comp1` with the name of the computer account that is to join the domain.

Make the account cacheable at the RODC

In the following procedure, you make the computer account cacheable at the RODC. There are two approaches you can take to make the computer account cacheable at the RODC. Both approaches are described here, but the second approach is the recommended approach because it is more secure.

Approach 1: To make the computer account cacheable at all the RODCs in the domain

1. Log on to a domain controller in the intranet.
2. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog appears, confirm that the action it displays is what you want, and then click **Continue**.
4. To make the computer account cacheable at all RODCs, type the following command at the elevated command prompt, and then press ENTER:

   ```
   net localgroup Allowed Password Replication Group comp1$ /add
   ```

   Replace `comp1` with the name of the computer account that is to be cacheable at all RODCs.

Approach 2: To make the computer account cacheable at the perimeter network RODC

1. Log on to a domain controller in the intranet.
2. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog appears, confirm that the action it displays is what you want, and then click **Continue**.
4. To make the computer account cacheable at the RODC, type the following command at the elevated command prompt, and then press ENTER:

   ```
   net localgroup <administrator created domain local group used to store user and computer accounts that are cacheable at the RODC> comp1$ /add
   ```

   Replace `comp1` with the name of the computer account that you want to be cacheable at the RODC.

   The placeholder `<administrator created domain local group used to store user and computer accounts that are cacheable at the RODC>` is a domain local group that you create to store user and computers accounts that you want to cache at the RODC.

   For example, you can create a domain local group, RODC1 Cached Accounts, and add any user or computer account to that group that you want to make cacheable at the RODC, RODC1.

Replicate the secrets of the computer account to the RODC

In the following procedure, you replicate the secrets of the computer account to the RODC.

To replicate the secrets of the computer account to the RODC

1. Log on to a domain controller in the intranet.
2. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog appears, confirm that the action it displays is what you want, and then click **Continue**.
4. At the elevated command prompt, type the following command, and then press ENTER:

   ```
   repadmin /rodcpwdrepl RODC1 DC1 CN=comp1,CN=Computers,DC=fabrikam,DC=com
   ```

   a. Replace `RODC1` with the name of the RODC computer account.

   b. Replace `DC1` with the name of the RWDC located in the intranet.

   c. Replace `CN=comp1,CN=Computer,DC=fabrikam,DC=com` with the distinguished name of the computer account that will have its secrets replicated to the RODC.

Run the join script on the client computer

In the following procedure, you run the join script on the client computer.

To run the join script on the client computer

1. Log on to the client computer that will join the domain through the RODC.
2. Create a new text file titled Join Script.
3. Copy the contents from the following section, Sample script for RODC domain join, to this text file.
4. Rename the file to Join Script.vbs, and then double-click the file to run the script.

   You can customize this script to meet the needs of your organization.

Sample script for RODC domain join

```
' JoinScript.vbs
'
'     Script to join a computer to a domain.
'
'
'


sub Usage
   wscript.echo " |-----------------------------------------------|"
```

```
   wscript.echo " |   Joins a computer to a domain or workgroup    |"
   wscript.echo " |------------------------------------------------|"
   wscript.echo ""
   wscript.echo "Usage: "
   wscript.echo " cscript JoinScript.vbs [/domain <domainname> | /workgroup
<workgroupname>]"
   wscript.echo "                        [/unjoin] [user <username>] [/password
<password>]"
   wscript.echo "                        [/machinepassword <password>] [/readonly]
[/createaccount]"
   wscript.echo "                        [/unsecure]"
   wscript.echo ""
   wscript.echo "domain           Specifies the name of a domain to join"
   wscript.echo "                 This option requires user, password"
   wscript.echo ""
   wscript.echo "workgroup        Specifies the name of a workgroup to join"
   wscript.echo ""
   wscript.echo "unjoin           Unjoin from a domain if currently joined."
   wscript.echo ""
   wscript.echo "disable          Disable the account when unjoining the domain."
   wscript.echo "                 This option requires unjoin, user, and password."
   wscript.echo ""
   wscript.echo "createaccount    Specifies to create the computer account in AD"
   wscript.echo ""
   wscript.echo "machinepassword  Specifies a password which is used to"
   wscript.echo "                 authenticate as the machine account to the DC"
   wscript.echo ""
   wscript.echo "readonly         Specifies the domain join will be read only"
   wscript.echo "                 and will not require a writable DC. This option"
   wscript.echo "                 requires machinepassword and that an Administrator"
   wscript.echo "                 has pre-created the computer account and set a"
   wscript.echo "                 password matching the machinepassword parameter."
   wscript.echo ""
   wscript.echo "DC               Specifies a DC to use during domain join."
```

```
   wscript.echo "                If readonly is specified this is mandatory, otherwise
optional."
   wscript.echo ""
   wscript.echo "OU              Specifies an OU where the machine account is created,
this is optional."
   wscript.echo ""
   wscript.echo ""
   wscript.echo "Unsecure         Specifies a an unsecure domain join."
   wscript.echo ""
   wscript.echo " |-----------------------------------------------|"
   wscript.echo " |Examples: Run 'cscript JoinScript.vbs <args>'   |"
   wscript.echo " |          <args>: Choose a scenario below       |"
   wscript.echo " | * Note lines have been wrapped for readability |"
   wscript.echo " |-----------------------------------------------|"
   wscript.echo ""
   wscript.echo "  Join domain: /domain <domainname> /user <username>"
   wscript.echo "               /password <password> /createaccount"
   wscript.echo ""
   wscript.echo "  Join domain with existing account: /domain <domainname>"
   wscript.echo "                                     /user <username>"
   wscript.echo "                                     /password <password>"
   wscript.echo ""
   wscript.echo "  Unjoin from a domain: /unjoin /user <username> /password <password>"
   wscript.echo "                        "
   wscript.echo ""
   wscript.echo "  Read Only join domain: /domain <domainname> /machinepassword
<password>"
   wscript.echo "                         /dc <rodcname> /readonly"
   wscript.echo ""
   wscript.echo "  Join workgroup: /workgroup <workgroupname>"
   wscript.echo ""
   wscript.echo ""
   wscript.quit -1
end sub
```

```
'
' Get the command line arguments
'
Set Args = Wscript.Arguments
'Set ArgCount = Args.Count

' Validation and Usage
if Args.Count = 0 then
   wscript.echo "Help Requested"
   wscript.echo ""
   Usage
end if

if Args.Count > 0 then
   if Args(0) = "/?" or Args(0) = "-?" or Args(0) = "help" then
      wscript.echo "Help Requested"
      wscript.echo ""
      Usage
   end if
   if Args.Count < 1 then
      wscript.echo "Help Requested"
      wscript.echo ""
      Usage
   end if
end if


' NetJoinDomain flags
Const NETSETUP_JOIN_DOMAIN = 1
Const NETSETUP_ACCT_CREATE = 2
Const NETSETUP_ACCT_DELETE = 4
Const NETSETUP_WIN9X_UPGRADE = 16
```

```
Const NETSETUP_DOMAIN_JOIN_IF_JOINED = 32
Const NETSETUP_JOIN_UNSECURE = 64
Const NETSETUP_MACHINE_PWD_PASSED = 128
Const NETSETUP_DEFER_SPN_SET = 256
Const NETSETUP_JOIN_READONLY = 2048
Const NETSETUP_INSTALL_INVOCATION = 262144

' Local state to track limited parameter validation
Options = 0
ReadOnly = 0
Unsecure = 0
JoinWorkgroup = 0
UnjoinDomain = 0
MachinePassword = 0

' Inputs for the join call
strDC = ""
strOU = ""
strDomainName = ""
strDomainNameAndDC = ""
strPassword = ""
strUserName = ""

' Collect parameters
ArgNum = 0

do while ArgNum < Args.Count

   if Args(ArgNum) = "/domain" or Args(ArgNum) = "/Domain" then
      strDomainName = Args(ArgNum+1)
      Options = Options + NETSETUP_JOIN_DOMAIN
      ArgNum = ArgNum + 1
   end if
```

```
if Args(ArgNum) = "/user" or Args(ArgNum) = "/User" then
   strUserName = Args(ArgNum+1)
   ArgNum = ArgNum + 1
end if

if Args(ArgNum) = "/password" or Args(ArgNum) = "/Password" then
   strPassword = Args(ArgNum+1)
   ArgNum = ArgNum + 1
end if

if Args(ArgNum) = "/machinepassword" or Args(ArgNum) = "/MachinePassword" then
   strPassword = Args(ArgNum+1)
   MachinePassword = 1
   Options = Options + NETSETUP_MACHINE_PWD_PASSED
   ArgNum = ArgNum + 1
end if

if Args(ArgNum) = "/readonly" or Args(ArgNum) = "/ReadOnly" then
   Options = Options + NETSETUP_JOIN_READONLY
   ReadOnly = 1
end if

if Args(ArgNum) = "/unsecure" or Args(ArgNum) = "/Unsecure" then
   Options = Options + NETSETUP_JOIN_UNSECURE
   Unsecure = 1
end if

if Args(ArgNum) = "/workgroup" or Args(ArgNum) = "/WorkGroup" then
   JoinWorkgroup = 1
   strDomainName = Args(ArgNum+1)
   ArgNum = ArgNum + 1
end if

if Args(ArgNum) = "/dc" or Args(ArgNum) = "/DC" then
```

```
      strDC = Args(ArgNum+1)
      ArgNum = ArgNum + 1
   end if

   if Args(ArgNum) = "/ou" or Args(ArgNum) = "/OU" then
      strOU = Args(ArgNum+1)
      ArgNum = ArgNum + 1
   end if

   if Args(ArgNum) = "/unjoin" or Args(ArgNum) = "/Unjoin" then
      UnjoinDomain = 1
      ArgNum = ArgNum + 1
   end if

   if Args(ArgNum) = "/disable" or Args(ArgNum) = "/disable" then
      Disable = 1
      Options = Options + NETSETUP_ACCT_DELETE
   end if

   if Args(ArgNum) = "/createaccount" or Args(ArgNum) = "/CreateAccount" then
      Options = Options + NETSETUP_ACCT_CREATE
   end if

   ArgNum = ArgNum + 1


loop

' Error reporting
if ReadOnly = 1 then
   if MachinePassword = 0 then
       wscript.echo "ReadOnly requires MachinePassword"
       wscript.quit(-1)
   end if
```

```
end if

if Disable = 1 and UnjoinDomain = 0 then
       wscript.echo "Disable is only valid with the unjoin option"
       wscript.quit(-1)
end if


' The username is optional and may need to be NULL when passed to the join API below
if strUserName = "" then optionAux = NULL else optionAux = strUserName

' The OU is optional and may need to be NULL when passed to the join API below
if strOU = "" then optionOU = NULL else optionOU = strOU

' Handle the case where this is a domain join and a DC was specified
if strDC = "" then strDomainNameAndDC = strDomainName else strDomainNameAndDC =
strDomainName & "\" & strDC

wscript.echo strDomainNameAndDC

Set objNetwork = CreateObject("WScript.Network")
strComputer = objNetwork.ComputerName

Set objComputer = GetObject("winmgmts:{impersonationLevel=Impersonate}!\\" & strComputer
& "\root\cimv2:Win32_ComputerSystem.Name='" & strComputer & "'")
'ReturnValue = objComputer.JoinDomainOrWorkGroup(strDomainName, strPassword,
strDomainName & "\" & strUserName, NULL, NETSETUP_JOIN_DOMAIN + NETSETUP_JOIN_READONLY +
NETSETUP_MACHINE_PWD_PASSED)

' Perform the join/unjoin operation
if UnjoinDomain = 1 then
   ReturnValue = objComputer.UnjoinDomainOrWorkGroup(strPassword, optionAux, Options)
else
   ReturnValue = objComputer.JoinDomainOrWorkGroup(strDomainNameAndDC, strPassword,
optionAux, optionOU, Options)
```

```
end if



' Report success messages
if ReturnValue = 0 then
      if JoinWorkgroup = 1 then
         wscript.echo "Welcome to the workgroup: " & strDomainName
         wscript.quit(0)
      end if

      if UnjoinDomain = 1 then
         wscript.echo "The machine was unjoined from the domain."
         wscript.quit(0)
      end if

      if JoinWorkgroup = 0 then
         wscript.echo "Welcome to the domain: " & strDomainName
         wscript.quit(0)
      end if
else
    wscript.echo "Error: " & ReturnValue
end if
```