Domain Requirements and Supported Topologies

Microsoft Active Directory Tools

Before you install Unified ICM in a new or existing AD environment, ensure that the environment is stable. As a rule, for all domain controllers in a forest, monitor replication, server, and AD health daily using the Microsoft System Center Operations Manager or an equivalent monitoring application. For information about using Operations Manager to monitor AD, see the *Operations Manager Monitoring Scenarios* for the current version of Operations Manager on the Microsoft TechNet website.

Microsoft provides several tools that you can use to ensure AD health and connectivity and that your environment is ready for Unified ICM. Some of the tools which you can use to check the health are as follows:

- dcdiag
- repadmin

Table 1: Microsoft AD Tools

Tool	Purpose	Command Line
dcdiag.exe	• Generates a report on AD health. • Verifies connectivity, replication, topology integrity, inter-site health, and trust verification. • Checks Network Card (NC) head security descriptors, net logon rights, and roles. • Locates or gets the domain controller.	`dcdiag /v /e /f:dcdiag.txt` **Note** Run this tool on the enterprise domain.
repadmin.exe	• Retrieves the replication status of all domain controllers in a spreadsheet. • Verifies DNS infrastructure, Kerberos, Windows time service (W32time), remote procedure call (RPC), and network connectivity.	`repadmin /showrepl * /csv >showrepl.csv`

Note Your network administrator or a qualified AD expert (for example, Microsoft Support Services), should evaluate the reports that these tools generate.

After you install the tools, run the following setups:

- dcdiag.exe
- repadmin.exe

Run dcdiag.exe

Procedure

Step 1 Choose **Start** > **Run**.

Step 2 Type **cmd**.

Step 3 Press **Enter**.

A command console opens.

Step 4 At the prompt, enter **dcdiag.exe /e /v /f:dcdiag.txt**.

Note If you use the /e option, run dcdiag.exe at the root level. If you do not use the "/e" option, run dcdiag.exe on each individual domain controller.

The application creates the text file dcdiag.txt in the folder containing dcdiag.exe.

Step 5 Open the text file and note any items that are prefaced with "Warning" or "Error."

Step 6 Correct all the issues, then rerun dcdiag.exe to ensure that no issues remain.

Run repadmin.exe

Procedure

Step 1 Choose **Start** > **Run**.

Step 2 Type **cmd**.

Step 3 Press **Enter**.

A command console opens.

Step 4 At the prompt, enter **repadmin.exe /showrepl * /csv >showrepl.csv**.

Step 5 Open Excel and choose **File** > **Open**.

Note Depending on your version of Excel, the menu cascades may be slightly different.

Step 6 In the "Files of type" section, click **Text Files (*.prn;*.txt;*.csv)**.

Step 7 In the "Look in" section, navigate to *showrepl.csv*, then click **Open**.

Step 8 In the Excel spreadsheet, right-click the column heading for showrepl_COLUMNS (column A), then click **Hide**.

Step 9 In the Excel spreadsheet, right-click the column heading for Transport Type, then click **Hide**.

Step 10 Select the row just under the column headings, then choose **Windows** > **Freeze Pane**.

Step 11 Click the upper-left corner of the spreadsheet to highlight the entire spreadsheet. Choose **Data** > **Filter** > **AutoFilter**.

Step 12 In the heading of the Last Success column, click the **down arrow**, then click **Sort Ascending**.

Step 13 In the heading of the Source DC column, click the **down arrow**, then click **Custom**.

In the Custom AutoFilter dialog box, complete the custom filter as follows:

a. Under Source DC, click **does not contain**.

b. In the corresponding text box, enter **del** to filter deleted domain controllers from the spreadsheet.

Step 14 In the heading of the Last Failure column, click the **down arrow**, then click **Custom**.

In the Custom AutoFilter dialog box, complete the custom filter as follows:

a. Under Last Failure, click **does not equal**.

b. In the corresponding text box, enter **0** to filter for only domain controllers that are experiencing failures.

For every domain controller in the forest, the spreadsheet shows the following:

- Source replication partner
- The time that replication last occurred
- The time that the last replication failure occurred for each naming context (directory partition)

Step 15 Use Autofilter in Excel to view the replication health for the following:

- Working domain controllers only
- Failing domain controllers only
- Domain controllers that are the least, or most recent

You can observe the replication partners that replicate successfully.

Step 16 Locate and resolve all errors.

Step 17 Rerun repadmin.exe to ensure that no issues remain.

Domain Requirements

Warning The Domain Controller and DNS servers can not be co-located on any Unified ICM component and must be installed on a separate server.

Unified ICM Requirements for AD:

- Authenticated users require credentials of a domain account with write privileges to the ICM OU.
- Microsoft AD tools or Domain Manager are the only supported tools for provisioning AD.

Note Permissions are needed during setup for creation of Service Logon accounts.

- You cannot create Unified ICM servers in the Unified ICM OU hierarchy.
- You can only apply the Unified ICM group policy template to OUs containing the Unified ICM servers.
- Single-label DNS domain names (such as “ICM”) are not supported when you use them with Unified ICM/CCE. Multi-part names such as ICM.org, ICM.net, ICM.com, or sales.ICM.org are acceptable.

Note For additional information, see Information about configuring Windows for domains with single-label DNS names.

- Requires no AD schema changes. Authenticated users require read access to the contents of AD.

Requirements for Group Policy in AD

Group Policy plays a pivotal role in AD management. Group Policy directly affects the function of distributed applications like Unified ICM. This section explains Group Policy and defines requirements to ensure proper functioning of your Cisco applications related to Unified ICM servers.

Group Policy Overview

Administrators can manage computers centrally through AD and Group Policy. Using Group Policy to deliver managed computing environments allows administrators to work more efficiently because of the centralized, 'one-to-many management' it enables. Group Policy defines the settings and allows actions for users and computers. It can create desktops that are tailored to user job responsibilities and level of experience with computers. Unified ICM uses this centralized, organized structure to help ease the administrative burden and create an easily identifiable structure for troubleshooting. However, some settings can adversely affect Unified ICM and the Unified ICM servers ability to function. Therefore, you must control the OU structure for Unified ICM components and ensure adherence to a standard.

Group Policy Settings

Administrators use Group Policy to define specific configurations for groups of users and computers by creating Group Policy settings. These settings are specified through the Group Policy Object Editor tool (known as GPedit.msc) and are present in a Group Policy Object (GPO), which is in turn linked to AD containers (such as sites, domains, or OUs). In this way, Group Policy settings are applied to the users and computers in the AD containers. For more information on Group Policy management, see *Group Policy Management Console* at https://technet.microsoft.com/en-us/library/cc753298(v=ws.11).aspx.

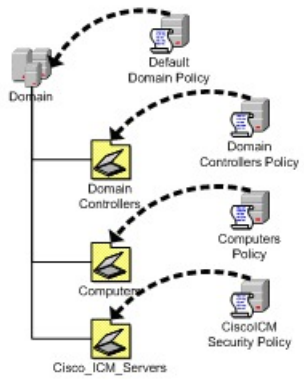
Caution Do not perform group policy updates during production hours as it may impact CVP/UCCE services.

Unified ICM Server Domain Requirements

You can move all Unified ICM servers into a separate OU to ensure proper functioning of the Unified ICM application and to improve security. You must clearly identify the OU as Cisco_ICM_Servers (or a similar clearly identifiable name) and documented in accordance with your corporate policy.

Note Create this OU either at the same level as the computer or at the Cisco ICM Root OU. If you are unfamiliar with AD, engage your Domain Administrator to assist you with Group Policy deployments.

Figure 1: Group Policy Deployments



After you apply the Group Policy to the OU, you must prevent propagation of default or custom Group Policies to this OU. You can use block inheritance to prevent this propagation. For details, see Block Policy Inheritance, on page 6.

Verify that a global Enforced policy is not applied in the domain. For details, see Prevent Use of Improper Policies, on page 6.

You cannot block enforced GPO links from the parent container.

Block Policy Inheritance

You can block inheritance for a domain or organizational unit. Blocking inheritance prevents Group Policy objects (GPOs) that are linked to higher sites, domains, or organizational units from being automatically inherited by the child-level. If a domain or OU is set to block inheritance, it appears with a blue exclamation mark in the console tree.

Procedure

Step 1 In the Group Policy Management Console (GPMC) console tree, double-click the forest containing the domain or organizational unit (OU) for which you want to block inheritance for GPO links.

Step 2 To block inheritance for an OU, double-click **Domains**, double-click the domain containing the OU, and then right-click the OU.

Step 3 Choose **Block Inheritance**.

Prevent Use of Improper Policies

You must prevent improper policies from being propagated. If the Enforced option is selected in a Group Policy Object being applied to a Cisco OU, a parent object enabled the option, which takes precedence over block policy inheritance. You must uncheck the Enforced option on all parent OUs or Group Policy Objects.

Procedure

Step 1 Select a parent OU or Group Policy Object from the Group Policy Management console tree.

The Default Domain Policy opens in the right pane.

Step 2 In the **Links** section, locate the domain, and note whether the **Enforced** option is enabled (**Yes** if enabled, **No** if not).

Step 3 If the option is enabled, right-click on **Yes** and deselect the **Enforced** option.

Install the Administration Client on a Different Domain in a Single Forest

You can install the Administration client on a different domain other than the Central Controller domain within a single forest.

Before you begin:

- A transitive trust must exist between the Administration client domain and Central Controller domain.
- An ICM domain user from the Central Controller domain must be granted local administrator privilege on the Administration client machine.

Note The following steps are only required when the AdminClientInstaller is in a different domain than the Central Controller.

Procedure

Step 1 Log in to the Administration client machine using the credentials from the Central Controller domain user, which is a part of local administrators group.

Step 2 Find the fully qualified domain name of the Central Controller domain.

Step 3 Install the Administration client.

Step 4 Launch the Administration client setup.
The Log in page appears.

Step 5 Log in with your Active Directory user name and password.
The log in fails because you are attempting to log in from a non-UCCE domain.

Step 6 Log in again with your Active Directory user name and password and the fully qualified UCCE domain name that you obtained in step 2.
You will now be able to log in to the Administration client.

DNS Requirements

The following are DNS requirements:

- AD Integrated Zone for both forward and reverse lookup zones.
- Enterprise level Standard Secondary Zone for the Unified ICM/Unified CCH Child Domain model or the Unified ICMH/Unified CCH Domain model.
- Manually add all additional addresses (high, privates, private highs, and so forth) to the forward lookup zone in DNS along with associated PTR records.
- Corporate DNS servers have forwarding enabled to the AD servers (if using Corporate DNS servers as opposed to the Domain Controllers for name resolution).

Global Catalog Requirements

In a multi-domain forest, a Global Catalog is required at each AD site. The Global Catalog is a central repository of domain information in an AD forest. A significant performance degradations and failure happen without

the local or Global Catalog. It is important for every AD query to search each domain in the forest. The multi-site deployments are required to query across WAN links.

Contact center enterprise solutions use the Global Catalog for Active Directory. All domains in the AD Forest in which the Unified CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookup, and group lookup.

Note This does not imply cross-forest operation. Cross-forest operation is not supported.

Supported Topologies

Unified ICME/Unified CCH systems support the following AD topologies:

- Single Domain
  - Unified ICM/Unified CCH in the Corporate domain
  - Unified ICM/Unified CCH in a child domain of the Corporate domain
  - Unified ICM/Unified CCH as a standalone domain
  - Unified ICM/Unified CCH as a tree root

A forest is a collection of AD domains that provide a namespace and control boundary within AD.

/Unified CCH systems support the following AD topologies:

- Single Domain
  - Customer HDSs in a single domain
- Single Forest, Single Tree
  - You can have an Administration client in a different domain from the Unified ICM/CCE instance in the same tree.
- Single Forest, Multiple Tree

Note You can have an Administration client in a different domain from the Unified ICM/CCE instance in the same tree.

Use the following example to determine how your domain structure looks before installing the Domain Controller.

This information is intended for the individuals responsible for:

- Configuring the AD Domain and Forest Topologies
- Staging new deployments of /Unified CCH on Microsoft Windows Server

You must train the administrators of your /Unified CCH system on the use and functions of:

- /Unified CCH
- Microsoft Windows Server
- AD
- DNS

This section does not provide detailed Unified ICME or Microsoft Windows Server specific information. You can find this information elsewhere in Cisco and Microsoft documentation. Individuals using this document must have at least intermediate knowledge and experience with AD.

The ability to integrate Unified ICM into existing infrastructures is one of the premises of Unified ICM. You can mitigate the impact that the unique environments in these existing infrastructures have on Unified ICM with minor adjustments to the support schema.

For more information, see the chapter Organizational Units.

Multiple Forests Not Supported

"Multiple forests" means two or more forests in a given environment that share resources through manually created trust relationships. All Unified CCE nodes, services, and users must reside in the same AD forest.

For additional information, see Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Use Microsoft Services or third-party Microsoft partner professional services to mitigate any Microsoft specific issues that might arise, as domain topologies vary.

Single Forest, Single Tree, and Single Domain Benefits and Usage Scenarios

The following are the benefits of using Single Forest, Single Tree, and Single Domain:

- Benefits
  - Simple setup
  - High stability
  - Smallest AD footprint
  - Least deployment-to-complexity ratio
  - Easiest support profile
- Sample usage scenarios
  - Enterprise Deployment

Single Domain Model

This type of domain structure has one major advantage over the other models: simplicity. A single security boundary defines the borders of the domain and all objects are located within that boundary. You do not need

to establish trust relationships between other domains. Group Policy execution is easier due to this simple structure.

When designing the new Active Directory structure from a multiple domain NT style structure, it was generally believed you could not consolidate on a single domain model. AD changes this. The capacity to span multiple domains in a single forest is improved and simplified.

Advantages of Single Domain Model

The single domain model is ideal for many Unified ICM deployments. The first advantage of a single domain structure is simplicity. When you add unnecessary complexity to a system architecture you introduce potential risk, and make it difficult to troubleshoot. A simpler, single AD domain structure reduces the administration costs and minimizes setbacks.

Another advantage is centralized administration. Organizations with a strong central IT structure want the capability to consolidate their control over their entire IT and user structure. Because NT domains were not able to scale to these levels, the central control that organizations wanted was not available. Now, AD and the single domain model allow for a high level of administrative control, including the capability to delegate tasks to lower sets of administrators.

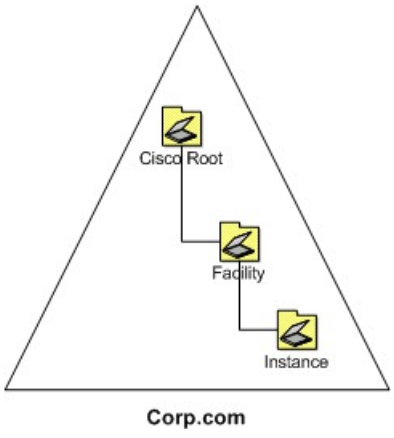
Unified ICM benefits from this design because AD traversal queries are limited to the single domain. As a result, request processing time is reduced. AD controls access and provides security which dramatically improves the overall performance of Unified ICM.

Single Domain Topology Design

Design is the most important aspect of any AD deployment. Follow Microsoft planning and design technical documentation to ensure a smooth transition.

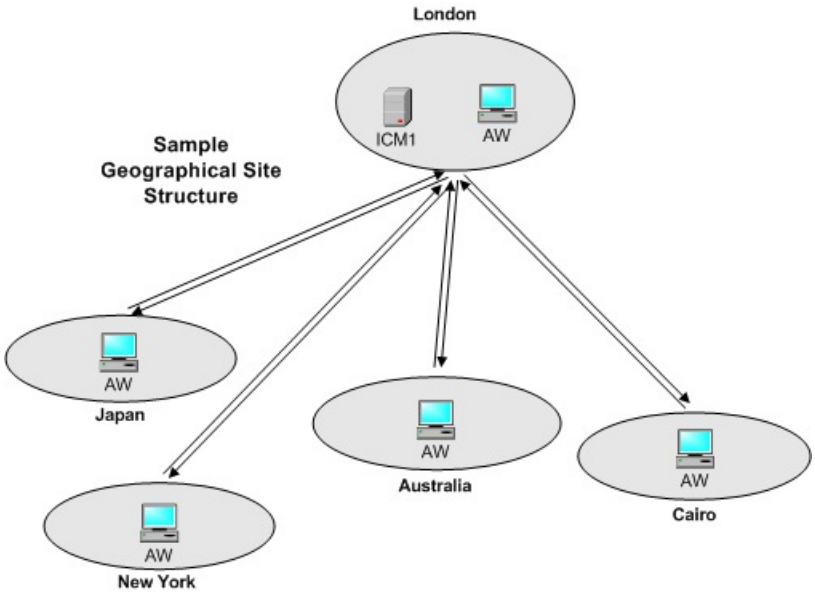
Delegation of password-change control and other local administrative functions can be granted to individuals in each specific geographical OU. The delegation of administrative functions provides administrators with permissions specific to the resources within their own group while maintaining central administrative control in the root OU.

Figure 2: Sample Single Domain Layout



You can create several AD sites to control the frequency of replication. Position a site to correspond with a separate geographical area, creating a site structure similar to the one shown in the following figure.

Figure 3: Site Organization by Geographical Location

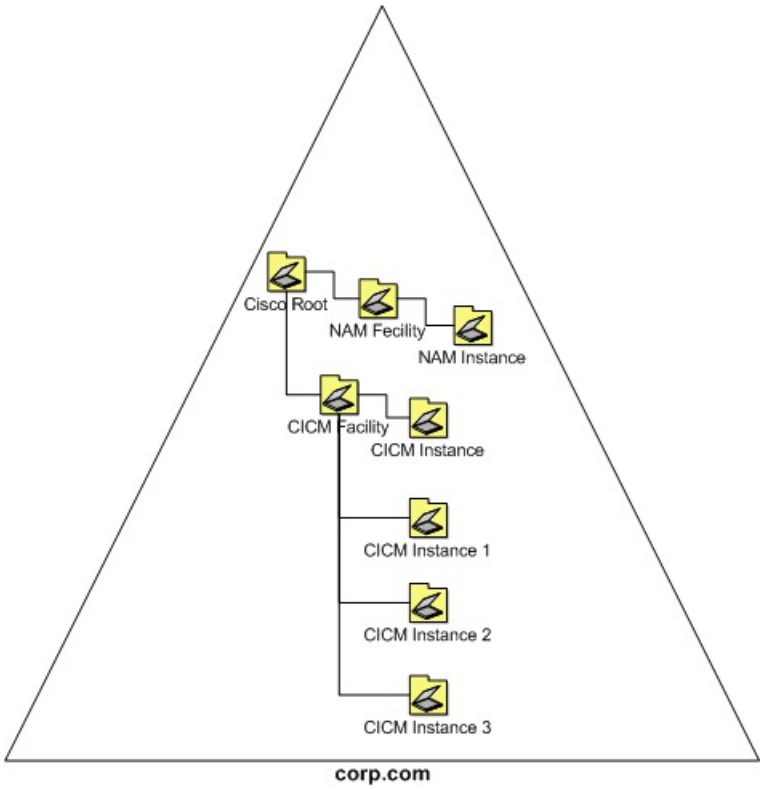


Create separate sites to help throttle replication traffic and reduce the load placed on the WAN links between the sites. For more details about site links and replication, see How Active Director Replication Topology Works.

This type of single domain design is ideal for both large and small organizations. Multiple domain use is reduced as delegation of administration is now accomplished by using OUs and Group Policy objects, and the throttling of replication is accomplished through AD sites.

Hosted scenarios have many instances deployed in various ways (such as geographically, client size, or however this model fulfills your needs). The following figure shows an example domain layout.

Figure 4: Hosted OU Structure for Single Domains



A single-domain design enables AD to manage access to the domain using Group Policies, Kerberos, and ACLs. This greatly simplifies administrative overhead and provides an increased return on investment for the entire organization.

For more information, see the chapter Organizational Units.

Single Tree Multiple Child Domains

Some deployments of /Unified CCH systems require Unified ICM to be installed in more than one domain. Sometimes the addition of one or more child domains into the forest is necessary. Keep in mind that a Unified ICM/Unified CCH system must be in a single domain, even when you install ICM in more than one domain. When adding a domain to the forest, consider the particular characteristics of multiple domain models.

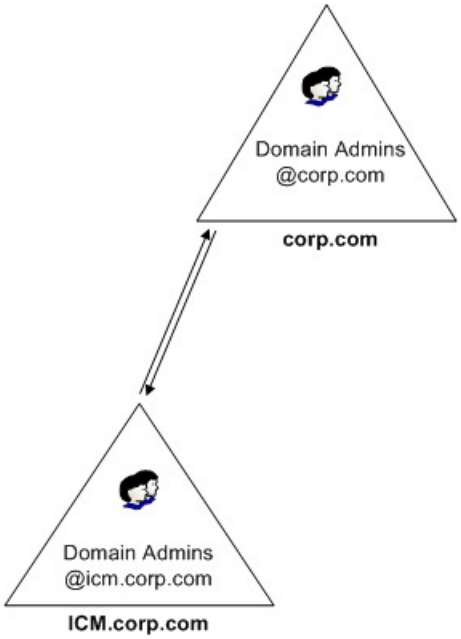
By default, two-way transitive trusts exist between the child domain and the parent domain in AD. However, this two-way transitive trust does not mean that resource access is automatically granted to members of other domains. For example, a user in the child domain is not automatically granted any rights in the parent domain. Explicitly define all rights by using groups. Understanding this concept helps to determine the requirements of domain addition.

When to Add Additional Domains

Begin design with a single domain and only add domains when necessary. If your infrastructure needs decentralized administration, you may need to add child domains to your existing domain structure. Multiple interconnected domains may be useful if your organization requires its own IT structure to manage Unified ICM, and there are no plans to consolidate the domains into a centralized model. A domain acts as a security

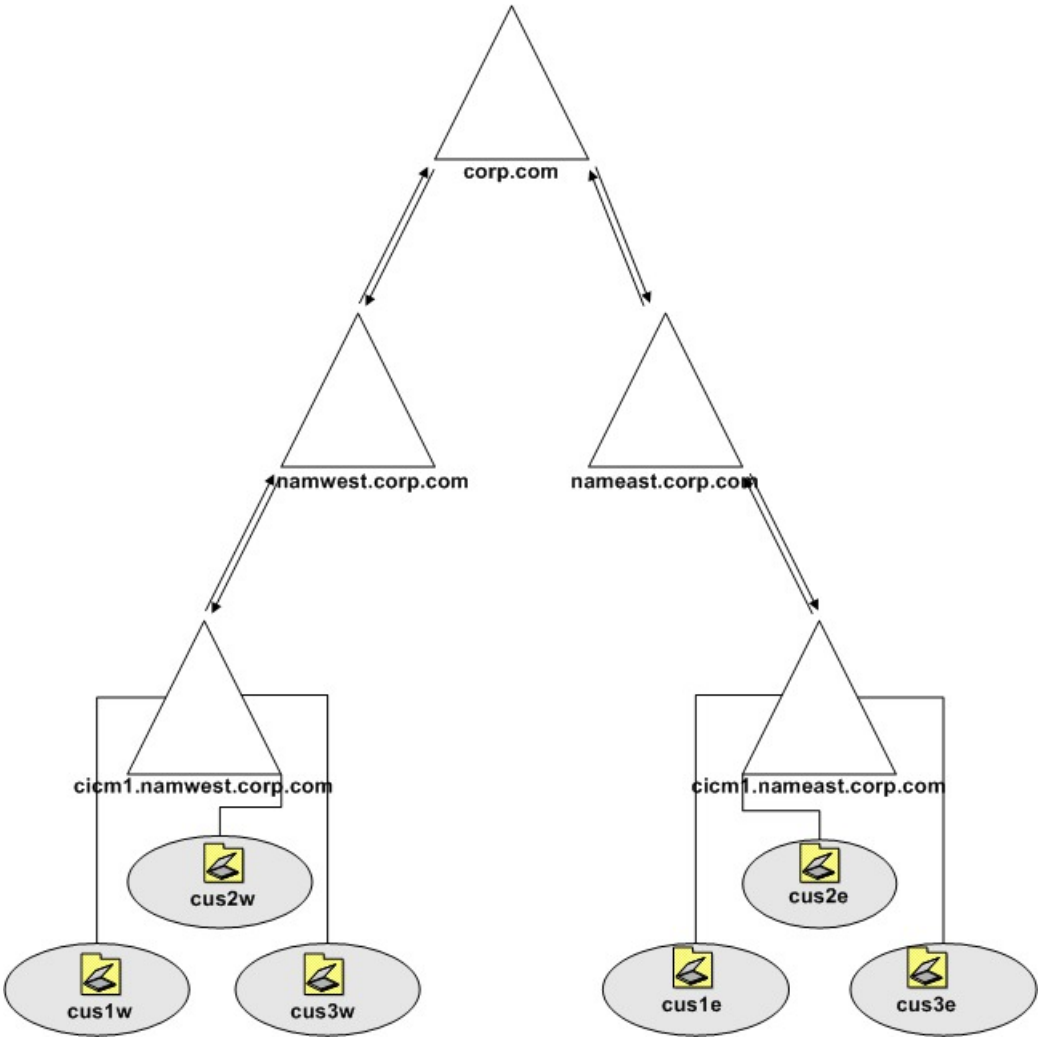
boundary for most types of activities and blocks administration from escaping the boundaries of the domain. NT domains inherit many of their associated limitations. This design approach operates in much the same way. Try to centralize administration before you deploy AD because you gain more AD advantages. AD advantages include centralized management, a simpler deployment model, simplified user and group management, and enhanced operability. The following figure demonstrates the default boundary in this topology. Assign the rights to give the user access to resources in the parent domain.

Figure 5: Active Directory Boundaries



If geographic limitations (such as extremely slow or unreliable links), segment the user population into separate groups. This segmentation helps to limit replication activity between domains and makes it easier to provide support during working hours in distant time zones. AD sites throttle replication across slow links. Slow links by themselves do not mean you must create multiple domains. Administrative flexibility is the main reason to create a domain for geographical reasons. For example, if you experience a network problem in Asia, a local administrator has the power and resources to administer the Asia domain. You do not need to contact a North American administrator.

Figure 6: Regional Domains

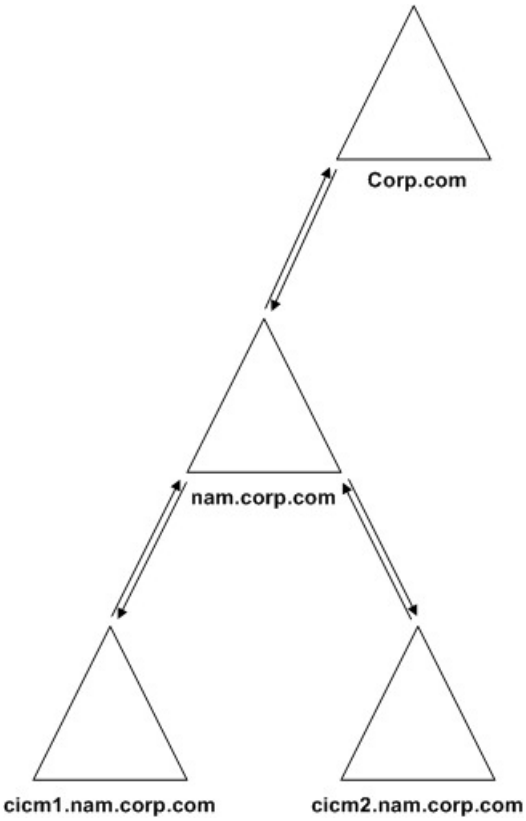


The single tree multiple child domain model allows each region to perform its own administration, creating an easily distributed and flexible topology. This domain model allows for a wide support base with immediate incident response. It also keeps the deployment clean and logical.

For Unified ICM, the addition of multiple child domains retains some of the old familiarity of NT4 topologies but gives an ease of delegation. This topology appeals to some service providers.

The single tree multiple child domain topology provides a contiguous namespace where the DNS domain names relate to the naming convention.

Figure 7: Contiguous Namespace



The flexibility in this model is apparent. However, you must be familiar with your organization requirements for a distributed, collaborative application such as Unified ICM. Use the simplest possible topology that meets your requirements.

Related Topics

Domain Name System, on page 18

Multiple-Tree Topology

A single forest with multiple trees and disjointed namespaces is a complex AD topology. This configuration can consist of one or more root domains, and one or more child domains.

Multiple Tree Forests

A forest is established when you create the first AD domain. This domain is known as the forest root. In a forest, any domains sharing a contiguous namespace form a tree. After a tree is established in a forest, any new domains added to an existing tree inherit a portion of its namespace from its parent domain.

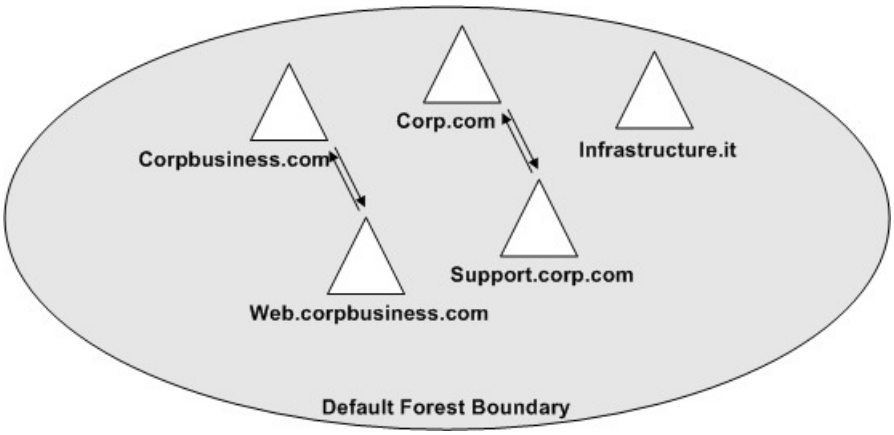
Any domain added to the forest that maintains a unique namespace form a new tree in the forest. An AD forest can consist of one or many trees in a single forest. In some instances, multiple trees are required so that a company can meet its business requirements.

Multiple Trees in a Single Forest Model

If your organization moves to an AD environment and uses an external namespace for its design, then you can integrate the external namespace into a single AD forest. Use multiple trees in a single forest to accommodate multiple DNS namespaces.

One of the most misunderstood characteristics of AD is the difference between a contiguous forest and a contiguous DNS namespace. You can integrate multiple DNS namespaces into a single AD forest as separate trees in the forest as indicated by the following figure.

Figure 8: Simple Multiple Tree Topology



Only one domain in this design is the forest root (Corp.com in the preceding figure). Only this domain controls access to the forest schema. All the other domains shown (including the subdomains of Corpbusiness.com, and the domains occupying different DNS structures) are members of the same forest. All trust relationships between the domains are transitive, and the trusts flow from one domain to another.

Business Requirements

Ensure that you plan a simple domain structure. If a business does not require multiple trees, do not increase the difficulty by creating an elaborate multiple-tree structure. However, sometimes multiple trees are required and this requirement is decided only after a thorough assessment of the business. When considering a multiple tree structure, keep the following requirements in mind:

DNS Names

If a business comprises of different subsidiaries, or has partnered with other businesses that maintain their distinct public identities as well as separate (noncontiguous) DNS names, you might have to create multiple trees in a single forest.

When to Choose a Multiple Tree Domain Model

If your organization currently operates multiple units under separate DNS namespaces, consider a multiple tree design. If you simply use multiple DNS namespaces, you are not automatically a candidate for this domain design. For example, suppose that you own five separate DNS namespaces. Then you decide to create an AD structure based on a new namespace that is contiguous throughout your organization. When you consolidate your AD under this single domain, you simplify the logical structure of your environment and keep your DNS namespaces separate from AD.

If your organization extensively uses its separate namespaces, consider the following design. Each domain tree in the forest can then maintain a certain degree of autonomy, both perceived and real. This type of design often satisfies branch office administrator needs.

The preceding domain design is logically more convoluted. Technically this domain design carries the same functionality as any other single forest design model. You set up all the domains with two-way transitive trusts to the root domain and share a common schema and global catalog. The difference is that they all use separate DNS namespaces. Reflect the separate DNS namespace use in the zones that exist on your DNS server.

Additional Considerations for Topology Design

The preceding sections provide a general overview of the considerations necessary when you choose a topology for Unified ICM in a corporate environment. Other considerations might arise, depending on a corporation's internal directives. The following topics include additional considerations for topology design.

Single Domain

In general, a Windows domain structure must be as simple as possible. The simplest approach is to create just one domain.

A single domain approach benefits:

- Most straightforward design
- Requires the least replication traffic
- Provides a minimum of administrative complexity
    - Requires the fewest domain administrators
    - Requires the fewest domain controllers
    - Allows administrative control at low levels in the domain by creating OUs and OU-level administrators—does not require a domain administrator to perform most tasks

Single Tree, Multiple Domains

A more complex structure is a root domain with domains beneath it.

Single tree, multiple domain approach provides the following benefit: the domain administrator of the root domain has complete power over the AD tree.

However, consider the following drawbacks when you use the single tree, multiple domain approach:

- More complex than a single domain
- Creates more replication traffic
- Requires more domain controllers than a single domain
- Requires more domain administrators than a single domain
- Setting tree-wide Group Policies requires using site Group Policy Objects (GPOs) or replicated domain/OU GPOs
- Tree could become complex if you create too many child domains

Single Forest, Multiple Trees

If the DNS names are contiguous for all domains in a forest, they can belong to a single domain tree. If their DNS names are not contiguous, create separate domain trees. So, if one domain tree is sufficient, there is no inherent need to create multiple trees.

Before using a single forest, multiple tree approach, consider the following drawbacks:

- Far more complex than a single domain
- Creates substantially more replication traffic
- Requires more domain controllers than a single domain
- Requires more domain administrators than a single domain
- Requires using site Group Policy Objects (GPOs) to set Group Policies

Additional Considerations

Security

Some organizations separate business units to provide security. This perception is a holdover from Windows NT4 where the domain boundary did provide the security. AD, however, provides layers of actual security. These layers are all customizable, and you can set them up in any of the supported topologies.

Corporate Directives

Many organizations have standard policies and procedures that they are accustomed to using as a Global standard. Unified ICM is a robust application and might be sensitive to some of these directives. For instance, some organizations have daily or weekly reboot policies for domain controllers. This situation requires a firm understanding of the effect AD has on the domain structure. If you turn all of the Domain Controllers off simultaneously, anything that relies on AD breaks. To avoid this problem, stagger the Domain Controller reboots so at least one domain controller per domain remains online at any given time.

Many variations and unique policies can impact Unified ICM. The procedures detailed in this guide delineate the best possible methods of deploying and maintaining Unified ICM. Review your company policies and compare them with the requirements established in this guide. If conflicts arise, correct them before deployment.

Domain Name System

AD integrates with the Domain Name System (DNS) as follows:

- AD and DNS have the same hierarchical structure.

  Although separate and executed differently for different purposes, an organization namespace for DNS and AD have an identical structure.

- You can store DNS zones in AD.

  If you use the Microsoft Windows Server DNS Server service, you can store primary zone files in AD for replication to other AD controllers.

- AD uses DNS as a locator service, resolving AD domain, site, and service names to an IP address.

To log on to an AD domain, an AD client queries their configured DNS server for the IP address of the Lightweight Directory Access Protocol (LDAP) service running on a domain controller for a specified domain.

Note You can use dcdiag.exe to troubleshoot client computers that cannot locate a domain controller. This tool can help determine both server and client DNS mis-configurations.

While AD is integrated with DNS and shares the same namespace structure, it is important to understand their differences:

- DNS is a name resolution service.

  DNS clients send DNS name queries to their configured DNS server. The DNS server receives the name query and either resolves the name query through locally stored files or consults another DNS server for resolution. DNS does not require AD to function.

- AD is a directory service.

  AD provides an information repository and services to make information available to users and applications. AD clients send queries to domain controllers using the Lightweight Directory Access Protocol (LDAP). An AD client queries DNS to locate a domain controller. AD requires DNS to function.

Follow the Microsoft method for AD to create lookup zones and to configuring DNS servers:

- Select **AD Integrated Zone** for both forward and reverse lookup zones.
- Select the **Allow Dynamic updates** and **Only Secure updates** options.
- Limit zone transfers to trusted servers in and across domains in a forest only.
- Add Unified CCE supplementary addresses manually (high, private, private high) in DNS as a Host record. Always create a PTR record for manually added hosts.
- If you use Corporate DNS servers rather than the Domain Controllers for name resolution, ensure that the Corporate DNS servers have forwarding enabled to the AD servers.

Configure Active Directory Sites

On Unified ICM Root Domain Controller:

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **AD Sites and Services**.

Step 2 Rename the default first site name as per AD Site Plan in Unified ICM System Diagram.

a) For a geographically separated DC, right-click **Sites**.
b) Select **New Site**.
c) Enter the site name of the additional domain controller based on the Unified ICM System Diagram.

Step 3 Create subnets for each DC site:

a) Right-click the Subnets folder and select **New Subnet**.
b) Enter the subnet address and mask, respective to the LAN at the Domain Controller Site.
c) Highlight the Site Name associated with that subnet.

Step 4 Expand the Servers folder from the original first site folder.

a) For each Server you need to move to a different site, right-click on server name, select **Move** and highlight the Site you want to move it to.

Step 5 Expand Inter-Site Transport under Sites.

a) Open the IP folder and select **DEFAULTIPSITELINK** from the right pane.
b) Right-click and select **Properties**. Ensure that both sites are added as entries in the Sites in this Site Link window.
c) Change the Replicate Every value to **15 minutes**.

Assign Global Catalog and Configure Time Source

To assign Global Catalogs and configure the time source per your Unified ICM System Diagram and the Unified ICM/CCE System Design Specification for your setup:

Procedure

Step 1 Open **Active Directory Sites and Services**.

Step 2 Connect to the Domain Controller designated as the Global Catalog.

Step 3 Right-click **NTDS Settings** and select **Properties**. Select **Global Catalog**.

Step 4 Move FSMO roles, as indicated in your Unified ICM System Diagram and the Unified ICM/CCE System Design Specification for your setup.

Step 5 The Forest Time Source defaults to the PDC Emulator, which is originally created on the Forest Root Domain Controller.

If the PDC Emulator moved to another Domain Controller, redefine the Time Source as either that server, or use an external Time Source.

a) On the Server currently running the PDC Emulator, run the following command: **`Net time /setsntp:<DNS Name of Time Source>`**.
b) To synchronize a Server to the Time source, see the procedure available on the Microsoft Website (http://support.microsoft.com/kb/816042).

Important Windows Server domain controllers that publish their Global Catalogs are required to be used. The preferred DNS servers must not be manually changed. It is important that all the other DNS Servers must have delegation set up with the DNS server of the forest Root Primary Domain Controller.

For detailed information on supported versions for Unified ICM, see:

Unified CCE Solution Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html