

# Re: Global Catalogue

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-01/msg00834](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg00834)

---

- *From:* "Joe Richards [MVP]" <[humorexpress@xxxxxxxxxxxxx](mailto:humorexpress@xxxxxxxxxxxxx)>
  - *Date:* Fri, 12 Jan 2007 21:00:37 -0500
- 

- > If this is the case, why does it seem that Microsoft
- > does not recommend
- > installing the GC on more than one DC?

What makes you think they don't? Recommendation is at least one GC per site. If you have a single domain in your forest the recommendation is to make every DC in the domain a GC. If you have multiple domains and you have the available bandwidth to replicate all of the GC info everywhere the recommendation is to make every DC in the forest a GC.

—

Joe Richards Microsoft MVP Windows Server Directory Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

buddd wrote:

Hello,

I was wondering if someone might be able to assist me in a better understanding of the role of the Global Catalogue.

It seems if one has an active directory network configured, one requires a Global Catalogue (GC) to operate correctly. My understanding is that if the Domain Controller (DC) that has the GC is lost or fails, there will be serious issues.

If this is the case, why does it seem that Microsoft does not recommend installing the GC on more than one DC?

## Re: Global Catalogue

My environment is quite straight forward: Windows 2003 Active Directory network with 2 DC's. One of the DC's has the GC and all 5 FSMO roles. The second DC has no FSMO roles nor GC. There network has 100 users.

Below is Microsoft's definition of GC.

Can someone explain this better to me? Why does Microsoft say it is not good practise to designate both DC's as a GC and replicate between the two DC's?

Thanks,

Mark  
budman@xxxxxxxxxxxxxxxx

---

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

In addition to configuration and schema directory partition replicas, every domain controller in a Windows 2000 Server or Windows Server 2003 forest stores a full, writable replica of a single domain directory partition. Therefore, a domain controller can locate only the objects in its domain. Locating an object in a different domain would require the user or application to provide the domain of the requested object.

The global catalog provides the ability to locate objects from any domain without having to know the domain name. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the forest. The additional domain directory partitions are partial because only a limited set of attributes is included for each object. By including only the attributes that are most used for searching, every object in every domain in even the largest forest can be represented in the database of a single global catalog server.

Note

- A global catalog server can also store a full, writable replica of an application directory partition, but objects in application directory partitions are not replicated to the global catalog as partial, read-only directory partitions.

## Re: Global Catalogue

The global catalog is built and updated automatically by the Active Directory replication system. The attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS) and are defined by Microsoft. However, to optimize searching, you can edit the schema by adding or removing attributes that are stored in the global catalog.

In Windows 2000 Server environments, any change to the PAS results in full synchronization (update of all attributes) of the global catalog. Windows Server 2003 reduces the impact of updating the global catalog by replicating only the attributes that change.

In a single-domain forest, a global catalog server stores a full, writable replica of the domain and does not store any partial replica. A global catalog server in a single-domain forest functions in the same manner as a non-global-catalog server except for the processing of forestwide searches.

### Common Global Catalog Scenarios

The following events require a global catalog server:

- Forestwide searches. The global catalog provides a resource for searching an Active Directory forest. Forestwide searches are identified by the LDAP port that they use. If the search query uses port 3268, the query is sent to a global catalog server.
- User logon. In a forest that has more than one domain, two conditions require the global catalog during user authentication:
  - In a Windows 2000 native mode domain or a Windows Server 2003 domain at either the Windows 2000 native or Windows Server 2003 domain functional level, domain controllers must request universal group membership enumeration from a global catalog server.
  - When a user principal name (UPN) is used at logon and the forest has more than one domain, a global catalog server is required to resolve the name.
- Universal Group Membership Caching: In a forest that has more than one domain, in sites that have domain users but no global catalog server, Universal Group Membership Caching can be used to enable caching of logon credentials so that the global catalog does not have to be contacted for subsequent user logons. This feature eliminates the need to retrieve universal group memberships across a WAN link from a global catalog server in a different site.

### Note:

Universal groups are available only in a Windows 2000 Server native mode domain or a Windows Server 2003 domain at either the Windows 2000

## Re: Global Catalogue

native or Windows Server 2003 domain functional level.

- Exchange Address Book lookups. Servers running Microsoft Exchange 2000 Server and Exchange Server 2003 rely on access to the global catalog for address information. Users use global catalog servers to access the global address list (GAL).
- In a Windows 2000 native mode domain or a Windows Server 2003 domain at either the Windows 2000 native or Windows Server 2003 domain functional level, domain controllers must request universal group membership enumeration from a global catalog server.
- When a user principal name (UPN) is used at logon and the forest has more than one domain, a global catalog server is required to resolve the name.

### Search Requests

Because a domain controller that acts as a global catalog server stores objects for all domains in the forest, users and applications can use the global catalog to locate objects in any domain within a multidomain Active Directory forest without a referral to a different server.

When a forest consists of a single domain, every domain controller has a full, writable copy of every object in the domain and forest. However, it is important to retain the global catalog on at least one domain controller because many applications use port 3268 for searching. For example, if you do not have any global catalog servers, the Search command on the Start menu of Windows 2000 Professional, Windows 2000 Server, Windows XP Professional, and Windows Server 2003 cannot locate objects in Active Directory.

The replicas that are replicated to the global catalog also include the access permissions for each object and attribute. If you are searching for an object that you do not have permission to access, you do not see the object in the list of search results. Users can find only objects to which they are allowed access.

### User Logon Support

In addition to its role as a search provider, in a forest that has more than one domain, the global catalog has a role as an identity source during the user logon process. Universal groups can provide access to resources outside of the users domain. User principal names (UPNs) can specify a domain other than the domain of the user. By making universal group membership and UPN domain–user mapping information available on all global catalog servers, the global catalog provides the definitive source for groups that are capable of providing access in more than one domain and names that do not unequivocally identify the domain of the user.

## Re: Global Catalogue

### Universal Group Membership

During the domain logon process, the user must be authenticated. During the authentication process, the user is validated (the domain controller verifies the identity of the user) and the user receives authorization data for access to resources. To provide authorization data of a user, the authenticating domain controller retrieves the security identifiers (SIDs) for all security groups of which the user is a member and adds these SIDs to the user's access token. In a forest that has more than one domain, the global catalog is the only location where memberships of all universal groups in that forest can be ascertained. For this reason, access to a global catalog server is required for successful Active Directory authentication in a domain that can have universal groups.

### Note

- Universal groups are available only in a Windows 2000 Server native mode domain or a Windows Server 2003 domain at either the Windows 2000 native or Windows Server 2003 domain functional level.

The global catalog stores the membership (the member attribute) of only universal groups. The membership of other groups can be ascertained at the domain level.

Because a universal group can have members from domains other than the domain where the group object is stored and can be used to provide access to resources in any domain, only a global catalog server is guaranteed to have all universal group memberships that are required for authentication.

For example, a user might be a member of a universal group that has its group object stored in a different domain but provides access to resources in the user's domain. To ensure that the user can be authorized to access resources appropriately in this domain, the domain controller must have access to the membership of all universal groups in the forest.

If a global catalog server is not available, the user logon fails.

### User Principal Name

A user principal name (UPN) is a logon name that takes the form of an e-mail address. A UPN specifies the user ID followed by a DNS domain name, separated by an "@" character (for example, jsmith@xxxxxxxxxx). UPNs allow administrative management of the UPN suffix to provide logon names that:

- Match the user's e-mail name.
- Do not reveal the domain structure of the forest.

## Re: Global Catalogue

When a user account is created, the UPN suffix is generated by default as `userName@DnsDomainName`, but it can be changed administratively. For example, in a forest that has four domains, the UPN suffix might be configured to map to the external DNS name for the organization. The `userPrincipalName` attribute of the user account identifies the UPN and is replicated to the global catalog.

When you use a UPN to log on to a domain, your workstation contacts a global catalog server to resolve the name because the UPN suffix is not necessarily the domain for which the contacted domain controller is authoritative. If the DNS domain name in the UPN suffix is not a valid DNS domain, the logon fails. Assuming the UPN suffix is a valid DNS name, the global catalog server returns the name of the Active Directory domain name to your workstation, which then queries DNS for a domain controller in that domain.

If a company has more than one forest and uses trust relationships between the domains in the different forests, a UPN cannot be used to log on to a domain that is outside the user's forest because the UPN is resolved in the global catalog of the user's forest.

### Universal Group Membership Caching

Universal Group Membership Caching is a new feature in Windows Server 2003 that eliminates the need for a domain controller in a multidomain forest to contact a global catalog server during the logon process in domains where universal groups are available. Caching group membership reduces WAN traffic, which helps in sites where updating the cached group membership of security principals, including user and computer accounts, generates less traffic than replicating the global catalog to the site.

Use the following criteria to determine if a site is a good candidate for Universal Group Membership Caching:

- Number of users and computers in the site: The site has less than 500 combined users and computers, including transient users who log on occasionally but not on a regular basis. The cache of a user who logs on once continues to be updated periodically for 180 days after the first logon. A general limit of 500 membership caches can be updated at a time. If greater than 500 security principals have cached group memberships, some caches might not be updated.
- Number of domain controllers: Each domain controller performs a refresh on every user in its site once every eight hours. Depending on the number of domains in the forest, 500 security principles and two domain controllers could generate more WAN traffic than placing a global catalog server in the site. Therefore, you need to rationalize the WAN costs when exceeding 500 security principals and two domain controllers.

## Re: Global Catalogue

- Tolerance for high latency in group updates. Because domain controllers in the site where Universal Group Membership Caching is enabled update the membership caches every eight hours, and because credentials are always taken from the cache, updates to group memberships are not reflected in the security principal's credentials for up to eight hours.

### Address Book Lookups

In Windows Server 2003 environments, Exchange 2000 Server and Exchange Server 2003 use the global catalog to store mail recipient data that enables clients in a forest to send and receive e-mail messages.

### Top of page

#### Global Catalog Dependencies and Interactions

Global catalog servers have the following dependencies and interactions with other Windows Server technologies:

- Active Directory installation. When Active Directory is installed on the first domain controller in a forest, the installation application creates that domain controller as a global catalog server.
- Active Directory replication. The global catalog is built and maintained by Active Directory replication:
  - Subsequent to forest creation, when a domain controller is designated as a global catalog server, Active Directory replication automatically transfers PAS replicas to the domain controller, including the partial replica of every domain in the forest other than the local domain.
  - To facilitate intersite replication of global catalog server updates, Active Directory replication selects global catalog servers as bridgehead servers whenever a global catalog server is present in a site and domains that are not present in the site exist in other sites in the forest.
- Domain Name System (DNS). Global catalog server clients depend on DNS to provide the IP address of global catalog servers. DNS is required to advertise global catalog servers for domain controller location.
- Net Logon service. Global catalog advertisement in DNS depends on the Net Logon service to perform DNS registrations. When replication of the global catalog is complete, or when a global catalog server starts, the Net Logon service publishes service (SRV) resource records in DNS that specifically advertise the domain controller as a global catalog server.
- Domain controller Locator: When a global catalog server is

## Re: Global Catalogue

requested (by a user or application that launches a search over port 3268, or by a domain controller that is authenticating a user logon), the domain controller Locator queries DNS for a global catalog server.

In the following diagram, global catalog interactions include tracking a global catalog server through the following interactions, which are indicated by boxes:

- Active Directory installation of a new forest: Global catalog creation occurs during Active Directory installation of the first domain controller in the forest.
- Net Logon registration: Resource records are registered in DNS to advertise the domain controller as a global catalog server.
- Active Directory replication:
  - When a new domain controller (DC2) is created and an administrator designates it as a global catalog server, replication of the PAS from DC1 occurs.
  - DC1 in DomainA replicates changes for DomainA to DC2, and DC2 replicates updates to data for DomainB to DC1.
- DC location: The dotted lines enclose the processes whereby two clients locate a global catalog server by querying DNS:
  - A through C: (A) ClientX sends a query to the global catalog, which prompts (B) a DNS query to locate the closest global catalog server, and then (C) the client contacts the returned global catalog server DC2 to resolve the query.
  - 1 through 5: (1) ClientY logs on to the domain, which prompts (2) a DNS query for the closest domain controllers. (3) ClientY contacts the returned domain controller DC3 for authentication. (4) DC3 queries DNS to find the closest global catalog server and then (5) contacts the returned global catalog server DC2 to retrieve the universal groups for the user.

### Interactions with Other Windows Technologies

The global catalog solves the problem of how to locate domain data that is not stored on a domain controller in the domain of the client that requires the information. By using different ports for standard LDAP queries (port 389) and global catalog queries (port 3268), Active

## Re: Global Catalogue

Directory effectively separates forestwide queries that require a global catalog server from local, domainwide queries that can be serviced by the domain controller in the user's domain