What Is a Global Catalog Server?

blog.netwrix.com/2021/11/30/what-is-a-global-catalog-server

The global catalog is a feature of Active Directory (AD) that allows a domain controller (DC) to provide information on any object in the forest, regardless of whether the object is a member of its domain. Domain controllers with the global catalog feature enabled are referred to as **global catalog servers**.

Handpicked related content:

[Free eBook] What is AD? An introduction to Active Directory

Core Functionality

Global catalog servers perform several functions, which are especially important in a multi-domain forest environment:

Authentication. During an interactive domain logon, a DC will process the authentication request and provide authorization information regarding all of the groups the user account is a member of, which will be included in the generated user access token. The DC must access a global catalog server to obtain the following:

- **User principal name resolution.** Logon requests made using a user principal name (e.g., "username@domain.com") require a search of the global catalog to identify the distinguished name of the associated user object.
- **Universal group membership.** Logon requests made in multi-domain environments require the use of a global catalog that can check for the existence of any universal groups and determine if the user logging on is a member of any of those groups. Because the global catalog is the only source of universal group membership information, access to a global catalog server is a requirement for authentication in a multi-domain forest.

Handpicked related content:

[Free Guide] Active Directory Group Management Best Practices

Object Search. The global catalog makes the directory structure within a forest transparent to users who perform a search. For example, any global catalog server in a forest is capable of identifying a user object given only the object's *samAccountName*. Without a global catalog server, identifying a user object given only its *samAccountName* could require separate searches of every domain in the forest.

How a Global Catalog Works

Active Directory Partitions

To understand how the global catalog works, it is important to first understand a little bit about how the Active Directory database is structured. Domain controllers store the Active Directory database in a single file, NTDS.dit. To simplify administration and facilitate efficient replication, the database is logically separated into partitions.

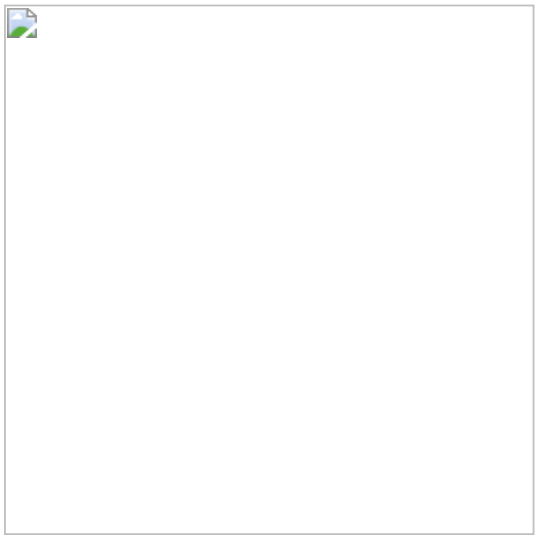
Every domain controller maintains at least three partitions:

- The **domain partition** contains information about a domain's objects and their attributes. Every DC contains a complete writable replica of its local domain partition.
- The **configuration partition** contains information about the forest's topology, including domain controllers and site links. Every DC in a forest maintains a complete writable replica of the configuration partition.
- The **schema partition** is a logical extension of the configuration partition; it contains definitions of every object class in the forest and the rules that control the creation and manipulation of those objects. Every DC in a forest maintains a complete replica of the schema partition. The schema partition is read-only on every DC except the DC that owns the Schema Master operations role for the forest.

Domain controllers may also maintain **application partitions.** These partitions contain information relating to AD-integrated applications and can contain any type of object except for security principals. Application partitions have no specific replication requirements; they are not required to replicate to other domain controllers but can be configured to replicate to any DC in a forest.

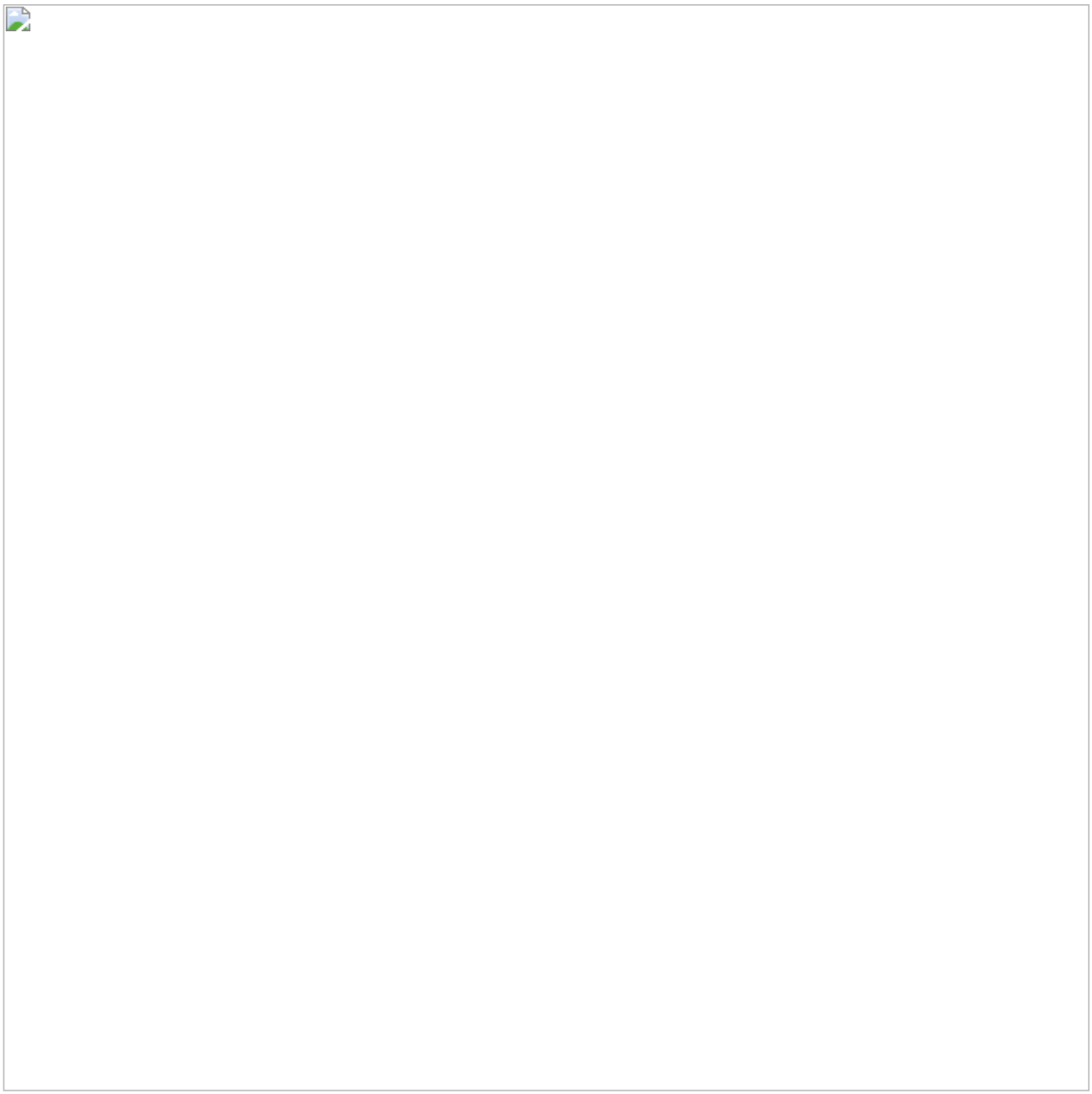
You can identify the partitions present on a DC using the following PowerShell cmdlet:

```
Get-ADDomainController -Server <SERVER> | Select-Object -ExpandProperty Partitions
```



Global Catalog Partitions

Consider a forest that consists of three domains, each with one global catalog server, as depicted below:

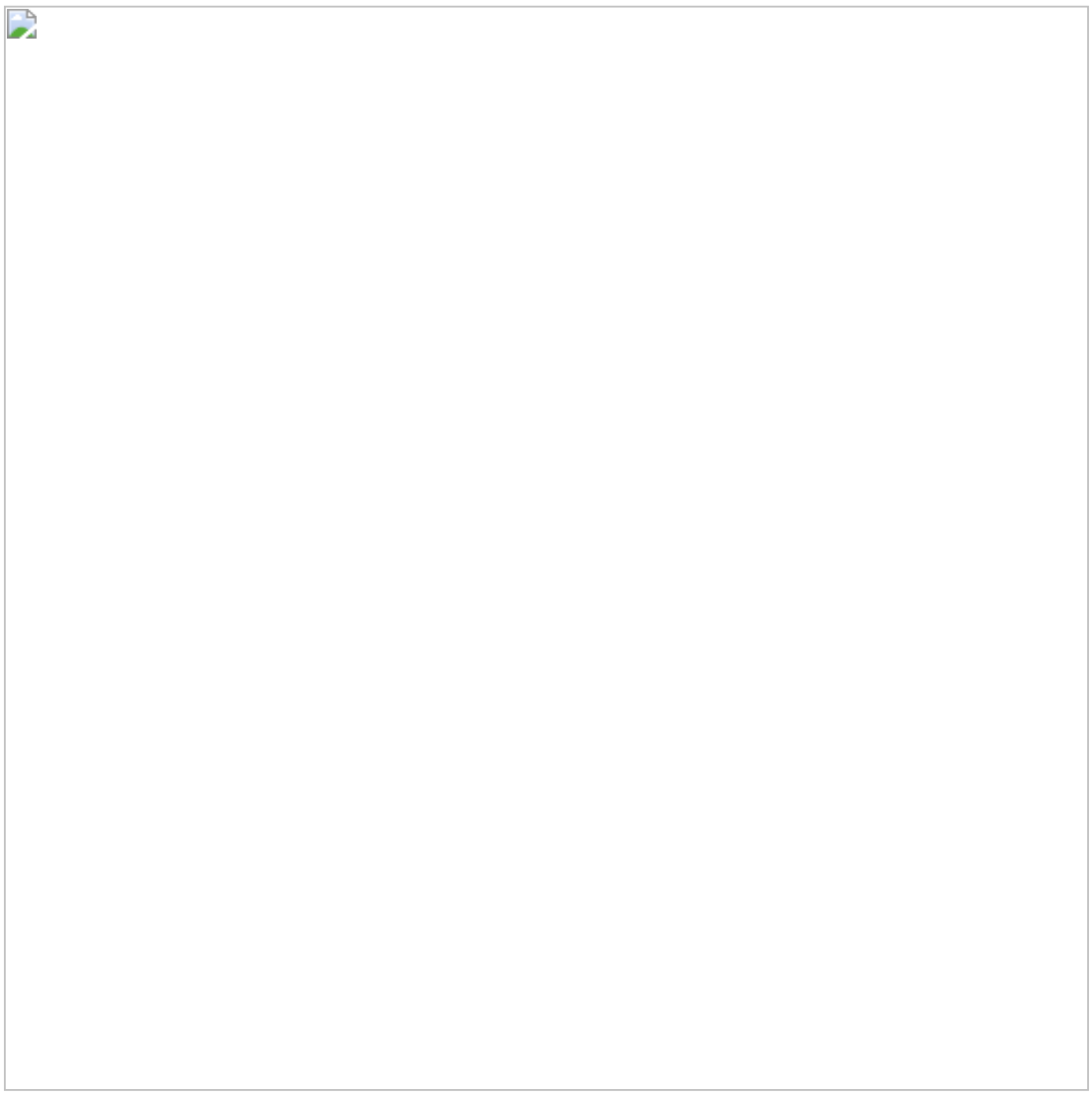


As explained earlier, every DC maintains a replica of its local domain partition, the configuration partition and the schema partition. In a multi-domain forest like this one, global catalog servers also host an additional set of read-only partitions, each of which contains a partial, read-only replica of the domain partition from one of the other domains in the forest. It is the information in these partial, read-only partitions that allow global catalog servers to process authentication and forest-wide search requests in a multi-domain forest.

The subset of object attributes that are replicated to global catalog servers is called the **Partial Attribute Set** (PAS). The members of the Partial Attribute Set in a domain can be listed using this PowerShell cmdlet:

```
Get-ADObject -SearchBase (Get-ADRootDSE).SchemaNamingContext -LDAPFilter "
(isMemberOfPartialAttributeSet=TRUE)" -Properties lDAPDisplayName | Select lDAPDisplayName
```

In a single-domain forest, all DCs host the only domain partition in the forest; therefore, each one contains a record of all of the objects in the forest and can process authentication and domain service requests.



Active Directory takes advantage of this by allowing any domain controller in a single-domain forest to function as a *virtual* global catalog server, regardless of whether it has been configured as a global catalog server. The only limitation is that only DCs configured as global catalog servers can respond to queries directed specifically to a global catalog.

Deploying Global Catalog Servers

When a new domain is created, the first DC will be made a global catalog server. To configure additional DCs as global catalog servers, either enable the Global Catalog checkbox in the server's NTDS Settings properties in the Active Directory Sites and Services management console, or use the following PowerShell cmdlet:

```
Set-ADObject -Identity (Get-ADDomainController -Server <SERVER>).NTDSSettingsObjectDN -
Replace @{options='1'}
```

Each site in the forest should contain at least one global catalog server to eliminate the need for an authenticating DC to communicate across the network to retrieve global catalog information. In situations where it is not feasible to deploy a global catalog server in a site (such as a small remote branch office), Universal Group Membership Caching can reduce authentication-related network traffic and allow the remote site's DC to process local site login requests using cached universal group membership information. This feature requires the remote DC to communicate with a global catalog server to process initial logons and perform search requests.

It is recommended that all DCs be configured as global catalog servers unless there is a specific reason to avoid doing so.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.