Active Directory Quotas

9 out of 10 rated this helpful - Rate this topic

Updated: April 30, 2010
Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2, Windows Server 2008

You can use Active Directory and Active Directory Domain Services (AD DS) to implement limitations on the number of objects that a security principal (a user, computer, and group) can create in a directory node. You can define these limitations through Active Directory quotas.

What are Active Directory quotas?

Active Directory quotas are limits on the number of objects that a security principal (that has been delegated the Create Child Objects or Delete Child Objects permission) can own and create. You can use quotas to mitigate the risk of a denial-of-service attack against a directory service. For example, you can restrict the owner of the Accounting organizational unit (OU) in your organization to creating no more than 100 new user accounts.

If a security principal that has been delegated the permission to create objects in the directory is compromised and there are no quota limitations in place, a rogue attack on the directory service can create objects until the disk that houses the NTDIS.dit file on the domain controller runs out of space. By implementing quotas, you can limit the number of objects that a security principal can create in the directory, which helps insulate the directory from a denial-of-service attack through the creation of a very large number of objects.

Where to apply quotas

You can specify quotas for security principals on each directory partition. These partitions include application partitions, domain partitions, and configuration partitions.

Quota exemptions

Schema partitions are exempt from quota restrictions. Modifications to the schema are highly restricted operations that only members of the Schema Admins group can perform. In addition, members of the Domain Admins and Enterprise Admins groups are also exempt from quota limitations.

Quota container

Quota objects are stored in the NTDS Quotas container under the domain, application, and configuration naming contexts. To view the NTDS Quotas container in the Active Directory Users and Computers snap-in, you must enable **Advanced Features** on the **View** menu. The NTDS Quotas container is of the object class **msDS-QuotaContainer**. There are two special attributes that you can set on the NTDS Quotas container:

- **msDS-DefaultQuota**
- **msDS-TombstoneQuotaFactor**

Values that you can assign to these attributes are described in the following sections: Default quotas and Tombstone objects.

Default quotas

You can set a default quota for every security principal in a given partition. To set a default quota for all security principals in a partition, you must modify the **msDS-DefaultQuota** attribute of the NTDS Quotas container.
By default, the **msDS-DefaultQuota** is not set. If there is no value for this attribute or if the attribute has a value of -1, security principals in the given partition (that have been delegated the Create and Delete Child permissions) can create and delete an unlimited amount of objects in the partition for which they have these permissions.

Tombstone objects

Tombstone objects, which are created when you delete an object from a partition, count toward a security principal's quota limit. You can define the percentage by which tombstone objects count against a security principal's quota limit by modifying the NTDS Quotas container's **msDS-TombstoneQuotaFactor** attribute.
The **msDS-TombstoneQuotaFactor** attribute is the percentage factor (a value between 1 and 100) by which tombstone objects count against a security principal's quota limit. By default, the value is set to 100. For example, if you leave the default value unchanged and a security principal has a quota limit of two, the user can create one object and delete another object, which creates a tombstone object. If the user creates an object and then deletes the same object, the quota limit is only reduced by one. By contrast, if you set the value of this attribute to 50, the user can create one new object and delete two objects, because creating a tombstone object only counts as half the value of creating one "live" object.

Access control for specifying quotas

By default, only members of the Domain Admins group can administer quotas. If you want a security principal outside the Domain Admins group to administer quotas, that security principal must have the following permissions:

- Write permissions to modify the attributes on the NTDS Quotas container
- Create Child permissions on the NTDS Quotas container
- Write Property permissions on any quota objects in the NTDS Quotas container
- Delete Child permissions on the NTDS Quotas container

Creating quotas

To assign a quota to a security principal, you must use the directory services tools. The command and required parameters for assigning a quota to a security principal are as follows:

```
dsadd quota –part <partition distinguished name> –qlimit <quotalimit> –acct
<security prinicipal>
```

Example

To set a quota limit of 10 on the security principal user object bsmith in the HelpDesk OU of the fabrikam.com directory partition, use the following command:

```
dsadd quota -part dc=fabrikam,dc=com -qlimit 10 -acct
cn=bsmith,ou=HelpDesk,dc=fabrikam,dc=com
```

At the completion of this command, the user bsmith is limited to creating 10 objects in the fabrikam.com directory partition.

To ensure that the quota was created successfully, open Active Directory Users and Computers and navigate to the **NTDS Quotas** container. That container should now have an object titled **FABRIKAM_bsmith**, which represents the NETBIOS name of the directory partition and the account name of the security principal. You can control the name of the object that appears in the **NTDS Quotas** container by passing arguments into the **-rdn** parameter of the **dsadd quota** command. For a full list of switches that you can use with the **dsadd quota** command, type **dsadd quota /?** at a command prompt.

Quota enforcement

Quota enforcement occurs during the following actions on the directory partition:

- Add Object. When an object is created in a directory partition, it is subject to all applicable quota limits. Adding an object causes the quota tracking system to decrement by one from the quota of the security principal that is stamped as the owner of the object. If this operation causes the object owner to exceed the allocated quota, the add operation will fail.

- Reanimate Object. Object reanimation, such as the reanimation of tombstone objects, is subject to quota enforcement. Reanimating an object tombstone causes the quota tracking system to transfer quota usage for the object from the tombstone category to the “normal object” category. If this causes the object owner to exceed the allocated quota, the undelete operation fails.

- Owner Change. If you change the owner of an object, that ownership change causes the quota tracking system to decrement by one from the new owner’s quota and give back to the old owner’s quota. If the change in ownership causes the new owner to exceed the quota limit, the operation fails.

Determining quota limits

There may be times when you need to check a security principal’s quota limit. By checking a security principals’ quota limit, you can adjust the size of the quota limit for your organizational needs. To determine a security principal’s quota, use the following command:

```
dsget user <userDN> -part <partitionDN> -qlimit –qused
```

Example

This command displays the quota limits for the user bsmith in the HelpDesk OU of the fabrikam.com directory partition:

```
dsget user cn=bsmith,ou=HelpDesk,dc=fabrikam,dc=com –part dc=fabrikam,dc=com
–qlimit –qused
```

You can use the same parameters with the **dsget computer** and **dsget group** commands to find the quota limit for those objects.

Users who have been assigned quotas for creating objects in the directory service can query their quota limit and quota usage by examining the **msDS-QuotaEffective** and**msDS-QuotaUsed** attributes of the NTDS Quotas container. These attributes are constructed attributes that are calculated dynamically as the users' quota limits change (**msDS-QuotaEffective**) or as they add or subtract to their quota limits (**msDS-QuotaUsed**) by creating or deleting objects.

To view these attributes in Windows Server 2003, you must install the Adsiedit snap-in and select the **Show optional attributes** check box.

To view these attributes in Windows Server 2008, open Active Directory Users and Computers, click **Attribute Editor**, click **Filter**, and under **Show read-only attributes**ensure that the **Constructed** check box is selected.

Top quota usage

If you want to determine which security principals are using their quotas most often—for example, if you want to determine who is creating and deleting the most objects—you can query the **msDS-TopQuotaUsage** attribute of the NTDS Quotas container. You can also determine quota use across all partitions by querying this attribute on the RootDSE naming context. The values that are returned for this attribute are in an XML-encoded string with the following form:

```
<MS_DS_TOP_QUOTA_USAGE>
     <partitionDN>DN of directory partition</partitionDN>
     <ownerSID>SID of quota user</ownerSID>
     <quotaUsed>value rounded up of quota used (computed)</quotaUsed>
     <tobmstonedCount>number of tombstone objects</tombstonedCount>
     <liveCount>number of active objects</liveCount>
```

Multiple quotas

In certain instances, a security principal may have multiple quotas applied to it. For example, if a security principal is not covered by a quota, the effective quota for that security principal is the default value that is determined by the **msDS-DefaultQuota** attribute of the NTDS Quota container.

If a security principal is covered by a least one quota specification, that quota specification is applicable and the default quota is not applied. For example, if the default quota for a partition is 5 and user A has a quota assigned to it that specifies 10, the effective quota for user A is 10.

If a security principal is covered by more than one quota specification, the effective quota for that security principal is the maximum of the assigned quotas. For example, if a user A has two quotas assigned to it and one of the quota limits is 5 and the other limit is 10, the effective quota is the quota with the higher limit. In this example, user A's effective quota is 10.

Verifying quota integrity

If you encounter issues in which quota limitations are not being enforced or if you are receiving quota table event errors or warnings, you may need to verify the integrity of the quota table. To verify the integrity of the quota table, use the **ntdsutil** command.

To verify the integrity of the quota table in Active Directory in Windows Server 2003

1. Reboot the domain controller that hosts Active Directory in Directory Restore Services Mode (DRSM).
2. Open a command prompt as an administrator. To open a command prompt as an administrator, click **Start**. In **Start Search**, type **Command Prompt**. At the top of the **Start** menu, right-click **Command Prompt**, and then click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. Type `ntdsutil`, and then press ENTER.
4. Type `semantic database analysis`, and then press ENTER.
5. Type `check quota`, and then press ENTER.

To verify the integrity of the quota table in AD DS in Windows Server 2008

1. Open a command prompt as administrator.
2. Stop the Active Directory database process: at the command prompt, type `net stop ntds`, and then press ENTER.
3. Stop dependent services: type `y`, and then press ENTER.
4. Type `ntdsutil`, and then press ENTER.
5. Type `activate instance NTDS`, and then press ENTER.
6. Type `semantic database analysis`, and then press ENTER.
7. Type `check quota`, and then press ENTER.

Rebuilding quota tables

There are times when the quota table may become corrupt and have to be rebuilt. If you performed a quota integrity check on the quota table and corruption was detected, you can use the **ntdsutil** command to rebuild corrupt quota tables. To rebuild a corrupt a quota table, use the same procedures in the Verifying quota integrity section of this document, but instead of using the **check quota** command, use the **rebuild quota** command.

Domain controller upgrade

When you upgrade a domain controller from Windows Server 2003 functionality to Windows Server 2008 functionality or when you promote a new server to a domain controller, there is some latency time for the table to be rebuilt. This is because every object in the Active Directory database (NTDS.dit) must be read and its owner must be determined.