

Novell eDirectory

Reviewing the Design of Your eDirectory Tree

Every six months, most states in the United States set their clocks ahead or back for daylight savings time. (Of course, Arizona, where I live, does not use daylight savings time. We basically confuse the rest of the country, and ourselves—but that's a subject for a different article.) Because these time adjustments happen twice a year, it's a good time to perform some periodic maintenance such as replacing batteries in smoke alarms.

Likewise, you need to remember to perform periodic maintenance on your company's network. For example, how long has it been since you checked the design of your Novell eDirectory tree? Perhaps your company has upgraded your eDirectory tree, reorganized some departments, or even merged with another company. These changes may require some changes to the design of your eDirectory tree.

Novell eDirectory has evolved over the years to become more than just a NOS directory that manages users and groups. Not only is eDirectory cross-platform, massively scalable, and extremely flexible, but it is also an e-business platform. The more your company depends on its directory for business services, the more important it is for you to review the design of your company's eDirectory tree. (Incidentally, reviewing this design is the first step to performing a comprehensive eDirectory health check.)

The design recommendations Novell has given over the past five years have held up fairly well. Some recommendations have become less relevant over time because eDirectory has evolved, especially in the area of replica scalability. For example, you no longer need to worry about limiting the number of objects in containers or the size of replicas. You now can create objects to your heart's content without any concern for the size of replicas.

Other design recommendations, such as how you organize network resources, are still valid and should be observed. Such considerations have less to do with directory performance and more to do with maintaining a flexible design that can benefit users the most. This article focuses on the following design considerations:

- Tree types and sizes
- Partitioning and replication strategies
- Multiplatform replicas

TREE TYPES AND SIZES

Most companies maintain a single eDirectory tree and install a few test trees in labs. Because you are trying to represent your company's organization in its eDirectory tree, having a single tree

still makes sense. However, the way you implement eDirectory can make a difference in how you design portions of the tree.

For example, an enterprise eDirectory tree can be defined as any tree that uses NDS 7 (or below) and eDirectory 8.5x. This tree is used primarily for file and print requests for a single organization.

The eCommerce tree serves the needs of eCommerce deployments from a single location or multiple locations. Highly scalable and cross-platform, this type of eDirectory tree is used for more than just file and print and includes secure authentication to web-based applications either inside or outside your company's firewall. In eCommerce implementations, an eDirectory tree may not be partitioned (beyond the [Root] partition and a single container) and may have only one large container with hundreds of thousands of User objects.

All eDirectory trees, regardless of their purpose, should be designed in a pyramid shape. More objects and containers should be defined at the bottom layers of the tree than at the top layers of the tree.

With eDirectory, the size of trees is theoretically unlimited. Typical User objects range in size from 3 KB to 5 KB, so you can store hundreds of thousands of objects without consuming much disk space. Populating every attribute of User objects obviously increases the amount of disk space needed.

Top Design

You should keep the [Root] container small, whether your company has an enterprise implementation of eDirectory or an eCommerce implementation. You should follow this rule no matter what platform eDirectory runs on. Having a small [Root] partition makes repairing or extending the eDirectory schema easier.

If you are designing an enterprise eDirectory tree, the top portion of the tree below the Organization container should represent WAN locations, and partitions should not span WAN connections. If you are designing an eCommerce tree, your company's eDirectory tree may have only one container below the [Root] and Organization containers.

The reason to continue this design approach is to make the best use of WAN bandwidth. Although eDirectory is massively scalable and communication between replicas is efficient, the less directory traffic that goes across WAN links, the more bandwidth that is available for other uses. For this reason, you should also use Group objects locally if possible to avoid excessive NDS traffic.

Bottom Design

Enterprise implementations of eDirectory emphasize placing containers at the lower level of the eDirectory tree. In addition, the bottom of the eDirectory tree should represent network resources such as users, servers, printers, and basically any other type of object. The best eDirectory performance is still achieved when users are grouped close to their resources.

PARTITION STRATEGIES

In earlier versions of NDS, Novell recommended partition boundaries to ensure optimal performance of the directory. Because eDirectory is so scalable and efficient, however, your partition design can now be based on what makes sense for your company.

The design of your eDirectory tree can favorably or adversely affect your ability to create an effective partitioning strategy. As mentioned earlier, the enterprise eDirectory design consists of top-level Organizational Units (OUs) that represent the geographic areas in which your company operates. You can then segment the directory into partitions at the geographic level and place subsequent partitions on the appropriate local servers. Again, this design ensures that replication traffic between different sites does not consume precious WAN bandwidth.

In earlier versions of NDS, the underlying database was not practical for large partitions (such as those containing 10,000 or more objects). You had to create additional partition boundaries to limit the size of partitions. eDirectory has no such limitations because it has a highly scalable backend. Novell now recommends the following for partition sizes:

- Partition size: 500,000 objects for trees with relationships (such as group memberships); several million objects for trees that have inter-object relationships
- Total number of partitions in tree: unlimited
- Number of child partitions per parent: 150 partitions
- Number of replicas per partition: 50 replicas
- Number of replicas per replica server: 250 replicas

These rules generally apply to distributed directories for enterprises and for eProvisioning solutions. (See the related article on eProvisioning on p. 6.) When

Setting Cache for Novell eDirectory

| Platform | Location | Steps |
|----------|-----------------|--|
| NetWare | Console screen | Set DSTRACE=!MB < Amount of RAM to use in MB > |
| NT | _NDSDB.INI | Create the _NDSDB.INI file in the \NOVELL\NDS directory Enter the command CACHE= < Amount of RAM to use in MB > |
| Solaris | ndstrace screen | Launch ndstrace from the Sun Solaris server Enter Set DSTRACE=!MB < Amount of RAM to use in MB > |

designing an eDirectory tree for eCommerce solutions, however, most of these rules are not needed. Because you do not know where a particular user is coming from over the Internet, the typical eCommerce deployment of eDirectory involves storing all of the data on a single server. In most cases, eCommerce systems also have one partition. With this type of design, you have a relatively shallow and flat eDirectory structure.

REPLICA PLACEMENT

The placement of replicas on your servers is important for two reasons: accessibility and fault tolerance. For example, if your company implements an eProvisioning solution, more user identity information will be stored in your company's eDirectory tree. Data needs to be available as quickly as possible, and having the data in several places will ensure accessibility and fault tolerance. You should follow these replication rules:

- Replicate locally first. At each location, you should store at least two replicas of a local partition if you have two servers available.
- For e-business solutions, store multiple instances of data for load balancing. Your eDirectory tree will be accessed by tens of thousands of users.
- Keep the master replicas in central locations. Storing master replicas at remote sites may seem logical, but because master replicas are used for partition operations (such as creating a new partition or merging a partition), you should place master replicas where these partition operations occur.
- Use cross-platform replication when access to other platforms is required. You should place a replica on the cross-platform server for local user access. (For

more cross-platform guidelines, see Tips & Tricks at www.directorydesign.com.)

If you replicate the master replicas at a remote site or if you must store replicas over a WAN to provide accessibility or fault tolerance, you should be aware of the bandwidth that will be used for replication. You can use Novell's WAN Traffic Manager (WANMAN) utility to control the replication of eDirectory traffic over WAN links.

For example, if you have a site that has only one server, you should store a replica across your WAN link for fault tolerance. You can then use the WANMAN utility to ensure that replication traffic is controlled and limited over slow WAN links.

NDS PERFORMANCE

You can manage eDirectory performance by adjusting the eDirectory cache. You can configure the amount of RAM that will be used as the eDirectory cache. You should try to get as close to a 1:1 ratio of cache to the directory (DIB) size as possible. To set the cache level, you can use the commands shown in "Setting Cache for Novell eDirectory."

CONCLUSION

Novell continues to move forward with greater scalability and performance of its operating system and directory. This is evident with the release of eDirectory 8.5x and the soon-to-be released NetWare 6. Having a solid design along with performing a directory health check will ensure that you'll always be ready for the next wave of directory applications.

Jeff Hughes is vice president of Corporate Strategy for NetPro Computing in Scottsdale, Arizona. He is also the creator of DirectoryDesign.Com and can be reached at info@directorydesign.com. ●