

Benefits of Using NDS for NT

NDS for NT provides the following benefits:

- A single namebase from which to administer all components of a network such as users, workstations and servers.
- NDS as the central point of administration for NDS and domain resources.
- The robustness of NDS applied to Windows NT Servers.
- NDS support and administration for Microsoft BackOffice and other applications that use domains.
- Single login to both Windows NT Server and IntranetWare
- User access to multiple domains without complicated domain trust configurations.

A Central Point of Administration

The NDS for NT makes it possible to manage the domain name base from within NDS. When the domain name base is redirected to NDS, all NT domain objects in the database are represented by NDS objects. This means the domain objects can be managed from the NW Admin utility. When NDS for NT is installed, the NDS schema is extended so that objects migrated from NT domains can be managed in NW Admin like domain objects are managed with Microsoft User Manager and Server Manager.

Once the information is migrated to NDS, NW Admin provides a single point of administration. This means that network supervisors no longer need to use separate utilities to manage NDS users and NT domains. Furthermore, it means that IntranetWare shops that want to use an application that requires a domain on an NT Advanced Server can now be managed from an NDS environment. These advantages reduce the amount of time that a network supervisor needs to spend managing two platforms.

This functionality can save time and effort for anybody who manages a network containing both IntranetWare and Windows NT servers.

Store All Objects in a Single Namebase

For example, assume that a single person needs access to both an NT domain and an IntranetWare server. If NDS for NT is not installed, the network supervisor must create and maintain two accounts for that user, one on each platform. If several hundred users need accounts in a domain and on NDS, the amount of work required to maintain those accounts can be prohibitive. However, if NDS for NT is installed, the domain object and NDS object are easily and safely combined into a single NT Domain object in NDS that controls access to both the domain and NDS, cutting the network supervisor's work in half without affecting the way users access services and information on the network.

NDS for NT moves the information from a primary domain controller to NDS. The NDS objects are not synchronized objects as they are if you use Novell Administrator for Windows NT; they are real NDS objects that exist only in NDS. When an object is migrated to NDS, it no longer exists in the NT domain. The workstation is not changed, so users continue to log in to their workstations as they always have, even if they log in from workstations using an operating system other than Windows NT.

Access to Multiple Domains without Complicated Trust Relationships

In the Windows NT domain model, for a user to exist in multiple domains and be able to access all of those domains, separate user objects must be set up in each domain and trust relationships must be established between the domains.

Because NDS for NT migrates domain objects to NDS, a single User object can be associated with as many NT Domain objects as necessary. This gives the user a single login for all NT Domain objects and gives the administrator a single object to administer.

The Robustness of NDS on an NT Server

If an administrator needs to add a new user with access to a Windows NT server using NDS for Windows NT, the administrator could use NWAdmin and the provided snap-ins to add the user in NDS and grant them rights to the Windows NT Server. Alternatively, the administrator could use Microsoft User Manager to create the user. User Manager would send requests to the NT Server to create the user in the domain and NDS for Windows NT would redirect those requests to the NDS database. The user would be created in NDS with the same properties and access restrictions that would have been available from the domain itself. Any subsequent modifications made to that user with User Manager or any other domain administration utility would be serviced in the same way.

Note: Although Microsoft User Manager can be used to create and modify users in NDS, NW Admin and the provided snap-ins offer all the same administration features, as well as significantly more configuration options.

Support for Applications that Use NT Domains

NDS for Windows NT has been designed so that any application requiring domain information will receive that information from NDS.

NDS for NT

Novell NDS for NT enables Windows NT administrators to move objects from NT domains to NDS. The objects that were once in the NT domains become true NDS objects that can be managed with the Novell NW Admin utility.

NDS for NT moves the information from the Security Accounts Manager (SAM) on a Windows NT primary domain controller to NDS. The workstation is not changed, so users continue to log in to their workstations as they always have.

Contents

[Understanding NDS for NT](#)

[Planning for NDS for NT](#)

[Setting up NDS for NT](#)

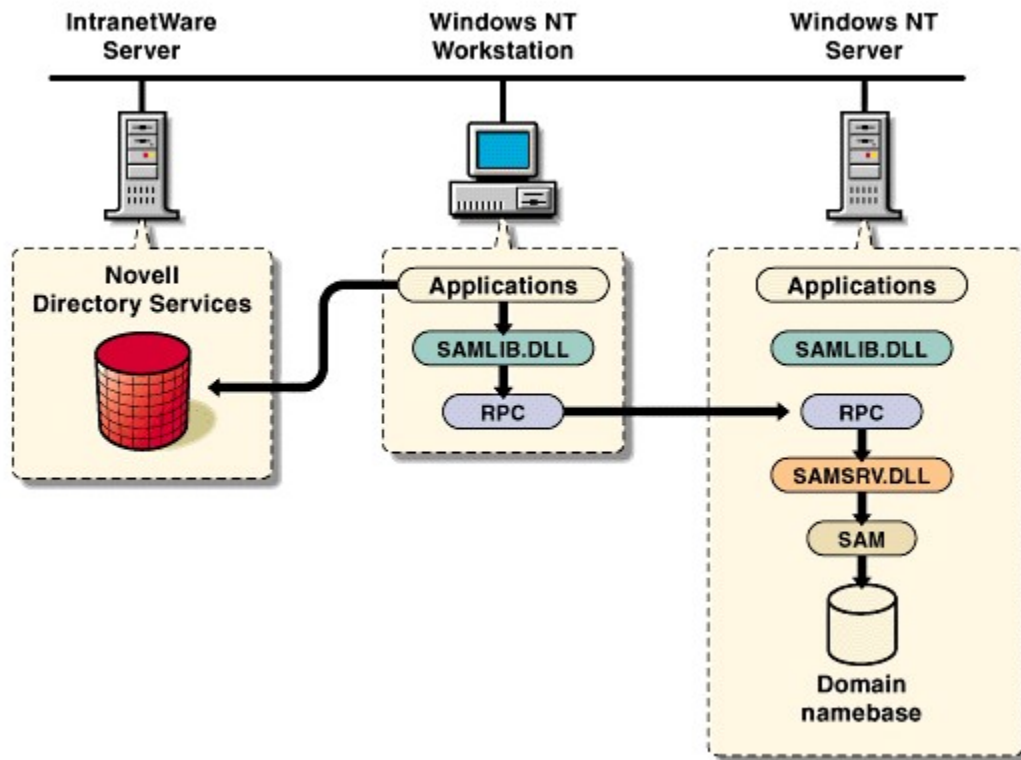
[Using NDS for NT](#)

[Troubleshooting NDS for NT](#)

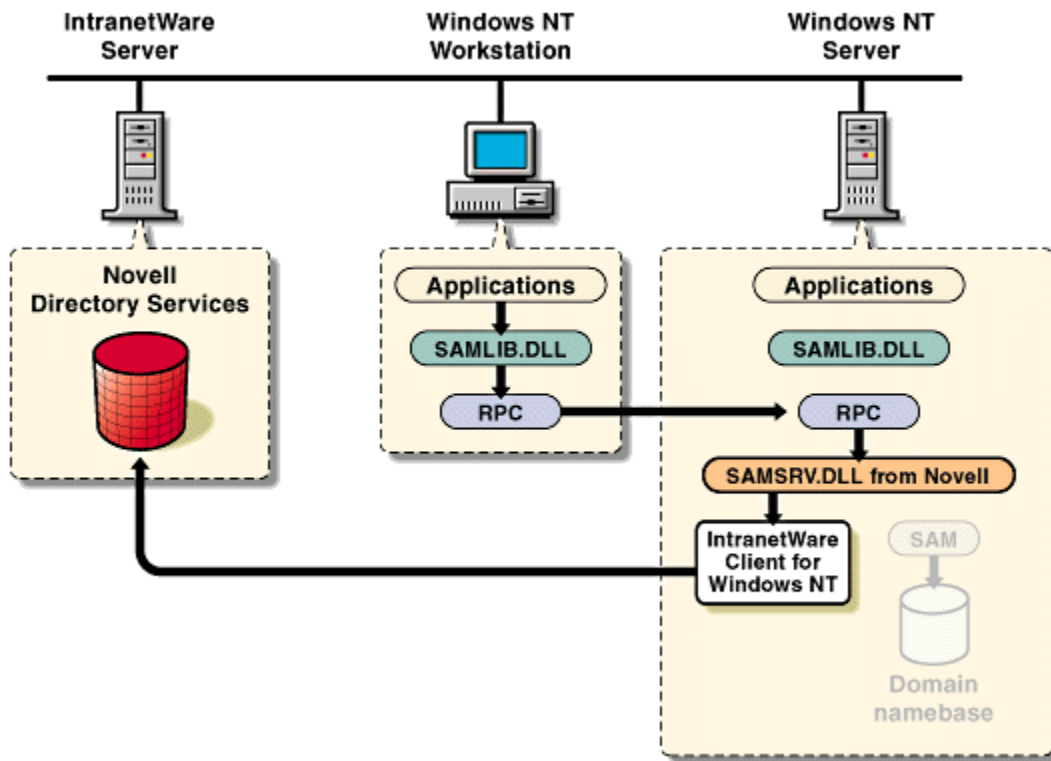
How NDS for NT Works

Applications that need information from the NT domain make requests to SAMLIB.DLL. This includes applications run on the NT server or an NT workstation. Some of the applications that require information from the domain are NT User Manager, NT Server Manager, and Microsoft Exchange.

SAMLIB.DLL communicates to SAMSRV.DLL using Remote Procedure Calls (RPC). For applications being run on the server this is all done internally. For requests originating from a workstation the RPC requests are received at the server via the network. Once the request is received by the server RPC, the request is extracted and passed to SAMSRV.DLL. SAMSRV.DLL then accesses the Windows NT Security Accounts Manager (SAM) where the domain namebase is stored and performs the requested operation.



NDS for Windows NT integrates Windows NT domains into NDS by enhancing the NT SAMSRV.DLL to redirect domain access calls to NDS. The only difference is that the new SAMSRV.DLL redirects all requests from the domain to NDS through the Novell Client for Windows NT. NDS can then be populated with user, computer and group objects that take the place of the objects previously used from the domain.



Planning for NDS for NT

Before installing NDS for NT, you should plan your migration from NT domains to NDS. A little bit of thinking ahead can prevent problems later on. Some of the questions you might ask yourself include:

Which objects in the domain do you want to migrate?

How will objects be organized?

Do the users and other objects already exist in NDS?

Do the objects in NT domains have the same names as existing NDS objects?

Relative Identifier

Windows NT domains do not allow a user to be a member of more than one domain. In NT, the RID is stored as part of the user object. NT uses the RID in the User object, which is only valid on a single domain. To move a User object to a different domain, the object must first be deleted from the previous domain, then created in the new domain. This affects the user's access to the first domain. If the User object is then created again in the first domain, another new RID is created.

NDS for NT, on the other hand, stores each user's RID in the NT Domain object in NDS. Because the RID is not stored as part of the User object, that one NDS User object can be associated with more than one NT Domain object. That makes it so a single user can access the resources that used to be available in multiple domains. Under NDS, an NT Domain object functions like a group. As you'd expect from a group, users can be members of more than one group.

Security Identifier

A Security Identifier (SID) uniquely identifies an NT domain across a network. When the Windows NT operating system is installed, a SID is created to identify the computer.

When a User object is moved from the domain to NDS, the global SID from the NT domain is moved to NDS. This SID is associated with the User object for as long as the User object exists as a member of that domain.

Objects within the domain, such as users and groups, are identified by combining the domain SID and a unique relative identifier (RID) value. The RID value is assigned to an object within a domain only once. RID values are never reused within a domain. The combination of the domain SID and the unique RID comprise the user or group SID, and is used throughout the system to identify the object and its access to system resources.

Setting up NDS for NT

To install NDS for NT, run the Setup program. The Setup program includes context-sensitive help to guide you through the installation process.

Technical Information about NDS for NT Passwords

Understanding NDS for NT

Novell NDS for NT enables Windows NT administrators to move objects from NT domains to NDS. The objects that were once in the NT domains become NDS objects that can be managed with the Novell NW Admin utility.

NDS for NT moves the information from the Security Accounts Manager (SAM) on a Windows NT primary domain controller to NDS. The workstation is not changed, so users continue to log in to their workstations as they always have.

By migrating objects from Windows NT domains to NDS, network supervisors can use NW Admin to manage all objects that were migrated from the NT domain. Having a single point of administration can greatly reduce the amount of work a network administrator has to do.

See Also

[How NDS for NT Works](#)

[Benefits of Using NDS for NT](#)

[Understanding Passwords in NDS for NT](#)

Understanding Passwords in NDS for NT

Default NDS Password

If migrating an NT domain user to NDS creates a new NDS User object (that is, if the User object did not previously exist in NDS), that object is created without a password. New NDS users should always set a new password.

If, on the other hand, the User object already exists in NDS, the NDS and domain passwords are unchanged. If these passwords are not synchronized, the user must log in with both passwords until the passwords are synchronized.

Synchronizing the Passwords

The first time you log in after installing NDS for NT and migrating NT domain objects to NDS, you log in separately to NDS and the workstation. When logging in to the workstation, check the box to synchronize the passwords. From then on, you'll only need to enter your name and password once to log in to both NDS and the workstation.

Changing the Password

In addition to the usual methods for changing passwords, you can change both the workstation and NDS passwords at the same time by using the Change Password button in NW Admin. One way that this is useful for administrators is that

See Also

[Technical Information about NDS for NT Passwords](#)

Using NDS for NT

NDS for NT includes a pair of utilities for use by network administrators.

The NDS for NT Domain Object Wizard migrates objects from the NT domain to NDS.

A snap-in for NW Admin provides the ability to manage objects migrated from the NT domain in NDS.

Each of these utilities includes context-sensitive help to assist administrators in their tasks.

What is SAM?

The Windows NT Security Accounts Manager is the database where the NT domain namebase is stored. The domain is identified by a unique number. This number, the Security Identifier or SID, uniquely identifies an NT domain across a network. Objects within the domain are also identified by a SID which is created by combining the domain SID with a Relative Identifier or RID. This object SID is used throughout the Microsoft network to identify the object and its access to system resources.

When using NDS for Windows NT each Windows NT domain is represented by a domain object in NDS. This object behaves similar to a group object in that it not only holds information about the domain and users which are a member of the domain, but it also contains member objects such as computers and groups just as an actual domain. One significant difference, however, is that NDS for Windows NT stores each user's RID in the NT Domain object and not as part of the User object. This means that one NDS User object can be a member of more than one NT Domain object. This provides a way for a single NDS user to access resources in multiple domains without having to set up complicated trusts.

Single Login to Both Windows NT Server and IntranetWare

If a user wants single sign-on to both Windows NT and IntranetWare, the passwords can be synchronized. When the user needs to access network resources from IntranetWare or Windows NT, the user only needs to enter a single username and password. Because NDS for NT places NT domain information in the NDS database, users can log in to both NDS and NT with a single login. The username and password for NT and IntranetWare are provide access to all available NDS services.

Do the Objects in NT Domains Have the Same Names as Existing NDS Objects?

If the objects in the NT domain have the same name as NDS objects that represent the same user, group, workstation, or server, there is no need to do anything special to the objects on either platform before migrating objects.

If, on the other hand, the names are different, you might want to consider changing the names so they match before migration. This ensures that everything will continue to work exactly as it did prior to migration. For example, if Exchange expects to find a user named Sam but the name has been changed to SamR, that user might not be able to use Exchange.

If objects representing two different things have the same name, one in NDS and the other in the domain, you should make the names different before migrating. Otherwise, two completely different users might become the same user.

Do the Users and Other Objects Already Exist in NDS?

If there are already NDS objects that represent the objects in the Domain (for example, if a user has objects in both NDS and the domain), you should merge those objects by migrating the domain objects to the same locations as the NDS objects. By doing this, you maximize the benefit of NDS for NT by using only one NDS object for each object that used to be located in both databases.

How Will Objects be Organized?

NDS allows great flexibility in the way objects are organized. You should think about an organization scheme that will make objects easiest to manage. You might want to place all of your NT users into a single NDS container. Or, you might want to create containers for each department. You might even want to organize the objects depending on the servers and other resources those objects need access to. You might have another organization method in mind. Whatever your plans, it's best if you think them through before migrating objects from the domain to NDS.

If the NDS containers you want to use do not already exist, you can create them before you start the migration process or you can create them from within the Migration utility.

Which Objects in the Domain Do You Want to Migrate?

You can elect to migrate all or some of the objects in your NT domain. Because NDS for NT combines the NT domain name base with the NDS name base, any objects that are not migrated will not be available. If you decide not to migrate a particular object, make sure that object is no longer needed. If you discover that you didn't migrate an object you should have, you must rename the original SAMSRV.DLL file and migrate everything again. When you migrate the objects again, everything will continue to work as it did before, as long as you migrate everything to the same container you used before.

