CONFIDENTIAL

From: Gary Hein
Date: Sat, May 30, 1998 3:34 PM
Subject: Fwd: NDS for NT / LDS Church

Don't know if you guys have seen this document yet, but it's just another example of lies propagated by MS. There are some very disturbing remarks, including:

Although it is possible to establish bi-directional trust, the trust connection can not be used for administering remote, unmigrated domains. This means that centralizing management with NDS for NT requires a wholesale conversion of the entire enterprise

GH: False

Note that NT servers would need to run IPX/SPX to support NDS for NT as well as TCP/IP to access other network resources and to comply with current standards.

GH: False - NDS for NT works over IP - no need to add IPX. This is a scare tactic.

Service Pack updates are questionable at best. MCS has not yet released Service Pack 4.0, however we suspect it will replace the existing samsvr.dll. To protect against NT Service Packs replacing samsrv.dll, NDS for NT checks at shutdown time and replaces samsrv.dll with the Novell version. MCS believes potential for failure is very high, as soon as any dll starts depending on new exports from samsrv.dll. Replacing this one critical dll could case the system to fail to boot and recovery could be very difficult.

GH: Perhaps advance knowledge of SP4?

Microsoft has repeatedly stated that it will support their NT customers and NT's basic functionality, but in areas that NDS touches, namely security and authentication, Microsoft will refer customers to Novell. This has the potential of creating some confusion in the resolution of issues revolving around security and authentication.

GH: Scare tactic

Also, comments from PeopleSoft should be solicited to see if PeopleSoft and Tuxedo are supported in environments where NDS for NT is in use as well as the IntranetWare client.

GH: Is it possible that MS is telling NT developer that they should not support their products with NDS for NT?

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who wanted enhanced security requested the ability to optionally restrict this functionality. Windows NT 4.0 Service Pack 3 and a hotfix for Windows NT 3.51 provide a mechanism for administrators to restrict the ability for anonymous logon users from obtaining system information. These anonymous connections are also known as NULL session connections. During the installation of Novell's NDS for NT, the samsrv.dll is replaced. Novell NDS for NT currently does not include support for restricting anonymous connections. MCS see this deficiency as a security weakness.

GH: This is the Red Button attack, which MS 'claims' is fixed with SP3, but really isn't. Again, this is completely incorrect - using NDS for NT will not impact the security flaw mentioned in this document.

Anyhow - I don't know if this is of any use to you but I thought I'd forward it over anyway.

Thanks,

Gary

CONFIDENTIAL

From: Loren Bishop <BishopLK@chq.byu.edu>
To: HUB-OREM1.SLC(BRICHAN)
Date: Wed, May 27, 1998 7:52 AM
Subject: Fwd: NDS for NT

Here is the document from Microsoft Consulting Services. We need a similar document from Novell. Please keep this confidential. I don't know that Microsoft would appreciate me sharing it with you.

CONFIDENTIAL

From: Eugene Morgan <emorgan@microsoft.com>
To: "Kenji Suzuki (E-mail)" <ksuzuki@chq.byu.edu>, "'b...
Date: Thu, May 21, 1998 4:43 PM
Subject: NDS for NT

Attach is the final version of the document that addresses NDS for NT. If you have any questions please call me.

<<NDSForNTConcerns.wpd>>

Eugene Morgan
Microsoft Consulting Services
Rocky Mountain District
(801) 540-4907

CONFIDENTIAL

The Church of Jesus Christ of Latter-day Saints

NDS for NT:

Microsoft's Consulting Services Concerns

Prepared By:
Eugene Morgan
Microsoft Consulting Services
May 1998
Document Version 1.2

Table of Contents

NDS for NT - Microsoft Consulting Services Concerns

1.1 Introduction

As the Church contemplates the deployment of NDS for NT there are some things to consider. There has been some questions about NDS for NT directed to Microsoft Consulting Services regarding NDS for NT from Novell. This document will hopefully articulate our concerns with regard to this product.

First consider the problem we are trying to solve, mainly, "the administration of user accounts within the Utility." As the Intranet has begun to be an important resource it has become necessary to use NT Domains in order to control access to this and other NT resources. Additionally, WinFrame administration has also been an issue. Simply stated, managing NT domains effectively is becoming more and more a necessity within the Church. This necessity has come about because of the recognized value of NT to address important business functions within the Church. It's interesting to consider that NT's success has also brought about the need to possibly alter NT in a manner that Microsoft feels would be contrary to NT's design.

From an MCS perspective there are two ways to ease management concerns: minimize the number of directory services the Utility supports or find a tool that will allow the administration of multiple directory services from one console. Let's examine the pros and cons of both approaches.

1.2 Minimizing the Number of Directory Services

The major advantage of minimizing the number of directory services the Utility supports is that administration can be accomplished for from one point, but can it really? Can the Church standardize on one directory service? The answer is, not really. The use of the many operating systems within the Church Utility, MVS, VMS, OS/2, NDS, and NT make it a formidable task to do so.

The other problem with this approach is that the current user account management process does not support this approach. Currently, the NetWare team handles account administration of NDS; the VMS and MVS team handles account administration of their respective environments, and the Security Administration Team handles NT account administration.

The security team would like to take ownership of user account administration and currently does some account administration on practically all platforms. However, they are currently not in a position to offer the 7x24 hour support that is necessary to support the Church's operational environment.

It should also be pointed out that the Help Desk also does some account administration on practically all platforms, but only under break/fix conditions. Also, their administrative privileges are severely restricted to the basic rights necessary to provide basic account administration as dictated by the limitations of the respective operating system.

1.3 Global Administration Through One Administrative Console

The next approach would be to utilize tools and technologies that allow for the administration of all directory services through the use of one console or a minimum number of consoles. This can be accomplished to some degree by adopting an enterprise management approach. Adopting this approach would require both changes in the process model for account administration and a deployment of enterprise management solution rather than point solutions that are currently in place or are being deployed.

1.4 Concerns With NDS for NT

Microsoft has published a number of documents on NDS for NT, unfortunately

most are internal and not available to the public. In addition, there has been a considerable amount of discussion on the various e-mail aliases within Microsoft. The following represents a distillation of the various documents and discussions and enumerated what MCS feels are areas of concern.

1.4.1 Administration

Multiple tools for administration due to missing functionality. Novell's NWAdmin does not give access to the full set of Windows NT security capabilities; in particular, there is no way to manage trust links with external (unmigrated) domains, and no way to manage local policies. The administrator uses NWAdmin for most tasks, but must use User Manager and Server manager for trust and local policy management

Although it is possible to establish bi-directional trust, the trust connection can not be used for administering remote, unmigrated domains. This means that centralizing management with NDS for NT requires a wholesale conversion of the entire enterprise.

Password synchronization: Since NDS for NT must support all Windows NT clients, not just Windows NT clients with the IntranetWare client installed, Novell must maintain two passwords for every user: a Windows NT password and an NDS password. From Novell's own announcement documents it is clear that this is a compromise solution that is far from transparent to the user. It important to point out that it is possible for the passwords to get out of sync. This could cause additional problems for uses as well as the Help Desk and other operational teams supporting the Utility.

ACL (Access Control List) confusion: In the case of a single NDS user being granted access to multiple domains, the same user, "BobSmith" would appear in the context of each "trusted domain" selected. A Windows NT ACL could have entries for Domain1\BobSmith, Domain2\BobSmith, and Domain3\BobSmith. All three are in fact the same user, but with different SIDs (NT Security ID's).

Also, in NDS for NT it is possible to create case-sensitive account names, for example "bsmith" and "BSmith". Because NT is not case sensitive for user names only one of the accounts would be accessible even though both would exist within NDS for NT. This could be a security issue and would also be confusing to administrators and others managing user accounts and of course customers.

Multiple group paradigms: Windows NT Groups are not NDS groups. To make a group visible in Windows NT the administrator must create an IWSam group as a child of a domain object. Only users can be added to IWSam groups.

No immediately obvious scripting support: ADSI supports NDS, but ADSI does not expose the SID, password residue, and other items required to migrate a Windows NT domain to NDS. This means the migration process is via the user interface, and the current user interface makes this quite laborious.

1.4.2 Disaster Recover

MCS is concerned with the effects NDS for NT has on recoverability in the case of a system failure. Because NDS for NT moves all of the directory information from the registry to the NetWare Directory, if the NT Primary Domain Controller fails, the following steps would be necessary to recover.

Do a reverse migrate to all the BDCs in the Domain.
Promote one of the BDCs to a PDC.
Reinstall and restore the original PDC as a BDC and restore files and applications.
Promote the restored BDC back to a PDC.
Reinstall NDS for NT on the PDC and each BDC in the domain.

This process seems rather involved and would cause a severe interruption of services and applications hosted on NT. It's important to point out that some of these applications are mission critical, PeopleSoft for example. Furthermore, if any NT backup domain controllers are located remotely to facilitate faster WAN login and lower WAN traffic, as in the case of England and Australia, this becomes an even more complex process. (Note: Novell has said that they will have a fix for this at some point.)

MCS offers the following disaster recovery advice; prior to implementing NDS for NT thoroughly test the above scenario and update the disaster recovery plan on how to recover in the advent of a failure.

1.4.3 Scalability

MCS has not heard of any large implementations of NDS for NT. Considering what it takes to architect a large NDS implementation, MCS questions what effects NDS for NT will have on the existing NDS infrastructure. MCS would suggest interviewing early adopters of NDS for NT prior to implementing NDS for NT. Furthermore, it would be important to

understand the impact of NDS on NT would have on the existing NDS servers and supporting network infrastructure. Note that NT servers would need to run IPX/SPX to support NDS for NT as well as TCP/IP to access other network resources and to comply with current standards.

NDS has partitioning requirements to keep from overloading its database as well as replication limitations. The NDS data is threaded through several files, remarkably similar to the file structure used by Microsoft directory service prior to moving NT's directory to utilize the JET database engine in 1991. Our concern is that the duplication of objects in the NDS directory will impact performance significantly for all NDS authenticated users.

It's also our understanding that in NDS for NT there is a limited one to one relationship between an NDS container and a Domain. Therefore if an enterprise has users spread across multiple NDS containers it may be necessary to implement separate NT domains that are related to the respective NDS containers.

With NDS for NT, NT domains become NDS groups. It is MCS's understanding, based on Novell recommendation that NDS groups should not have more than 2000 members. This does raise the question about the scalability of NDS for NT. Will this group limitation be an issue for the Church?

Given that NDS for NT converts NT domains to NDS groups, it is recommended that interdependence between these NDS groups be tested in order to ascertain that the necessary relationships exists between these NDS created groups.

As the Church begins to develop large applications, the Church my find it reasonable or necessary to deploy NT on Alpha systems in a effort to scale an application to meet demand. There is no support for NDS for NT on Alpha NT servers. Novell has indicated this is, "a hard problem" and has offered no guarantees and little hope that it will be addressed in the future.

1.4.4 Upgrade and Update Capability

"NDS for NT: Making Windows NT Work for You", Brain Share, 1998, Salt Lake City, Utah.

Service Pack updates are questionable at best. MCS has not yet released Service Pack 4.0, however we suspect it will replace the existing samsvr dll To protect against NT Service Packs replacing samsrv dll, NDS for NT checks at shutdown time and replaces samsrv dll with the Novell version MCS believes potential for failure is very high, as soon as any dll starts depending on new exports from samsrv dll Replacing this one critical dll could case the system to fail to boot and recovery could be very difficult.

Also, if for what ever reason the new samsrv dll is left in place after a service pack install on a PDC or a BDC the potential of causing login and security problems is high. If the upgraded server is a primary domain controller there would be the possibility that no one, including the NT administrators, would not be able to log onto the system, potentially a very disastrous situation. We realize this sounds like a lot of FUD but the weakness created in the system by the replacement of this critical dll should be clearly understood and MCS would be remiss in its responsibilities to our customers if this fact was not pointed out.

Novell claims that customers will be able to upgrade to NT 5.0 from NDS for NT without any consequences. This is true if the customers migrate or imports a domain into NT 5's Active Directory, but that simply brings the same directory objects over to the Active Directory Domain. The upgrade from Windows NT Server 4.0 to Windows NT Server 5.0 converts the SAM by reading it directly, not by calling SAM APIs. The users and groups created in NDS will not be picked up in the upgrade (assuming the upgrade can even begin with the modified SAMSRV.DLL installed, which is unlikely). NDS for NT users will be faced with a second migration after installing Windows NT Server 5.0, to bring the NDS users into Active Directory. Furthermore, there are multiple paths into the authorization and authentication system in Windows NT Server 5.0, there is no single place to trap and redirect these operations. A Windows NT Server 5.0 version of NDS for NT will require a total rewrite, and there is little motivation for this since Windows NT Server 5.0 comes with its own very robust directory service, Active Directory.

It should be noted that there are issues with supportability of an NT environment that has been implemented utilizing NDS for NT. Microsoft has repeatedly stated that it will support their NT customers and NT's basic functionality, but in areas that NDS touches, namely security and authentication, Microsoft will refer customers to Novell. This has the potential of creating some confusion in the resolution of issues revolving around security and authentication.

1.4.5 Speed

Because all security calls are redirected from the PDC and BDC, to NetWare, users may experience additional delays in any operation that requires any type of NT authentication.

At a recent Novell event, Brain Share1, a demonstration of NDS for NT was given. It was observed that at that demonstration it took 35 seconds for a user to log on against a (presumably) unloaded server in a tree with under ten users. This, naturally, raises concerns about speed and response time, not only for user authentication but also for any application that requires NT authentication.

1.4.6 Reliability

In order to install NDS for NT it is necessary to install the IntranetWare Client. Based on past performance, Microsoft does not recommend the IntranetWare Client for installation on servers, especially servers that also host mission critical applications. MCS feels this is a high risk and should be

considered carefully. It's also important to know that there are issues with using TCP/IP with Novell's current IntranetWare client. This is one of the main reasons the Church has had to maintain its dependence on IPX/SPX.

It will also be necessary to retest any NT server based applications that runs on NT for reliability. COH will need to be tested; DHCP, WINS, and DNS services will all need to be tested.

Also, comments from PeopleSoft should be solicited to see if PeopleSoft and Tuxedo are supported in environments where NDS for NT is in use as well as the IntranetWare client.

1.4.7 Security

What are the implications of calls that used to go between the samsvr.dll and the registry now being redirected across the network? Do the passwords retain their encrypted state that they were originally transmitted in? If they are encrypted, is that encryption secure?

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who wanted enhanced security requested the ability to optionally restrict this functionality. Windows NT 4.0 Service Pack 3 and a hotfix for Windows NT 3.51 provide a mechanism for administrators to restrict the ability for anonymous logon users from obtaining system information. These anonymous connections are also known as NULL session connections. During the installation of Novell's NDS for NT, the samsrv.dll is replaced. Novell NDS for NT currently does not include support for restricting anonymous connections. MCS see this deficiency as a security weakness.

1.5 Conclusion

To summerize the major points:

- NDS for NT is a poor technical solution that fundamentally alters NT Server by replacing its security and authentication mechanism.
- NDS for NT make the migration from NT 4 to NT 5 more difficult.
- NDS for NT is not an interoperability solution but a point solution.
- NDS for NT may have an adverse impact on network response time.

Microsoft. "Restricting Information Available to Anonymous Logon Users - Q143474." TechNet CD, January (1998): Microsoft May 1998.

- NDS for NT does not simplify the administrative process but further complicates it.

It is the feeling of MCS, as well as many others in the computer industry, that NDS for NT is not a mainstream product. It is a point solution that is designed to appeal to NetWare customers with an expanding base of Windows NT servers and applications in a NetWare legacy environment. While NDS for NT appeals to some of these customers as a stopgap measure to provide more centralized administration of Windows NT domains, the substantial expense, questionable stability, and dead-end nature of the implementation all argue against it.