The following paper was originally published in the
Digest of the Large Scale System Administration of Windows NT Workshop
Seattle, Washington, August 1997

Domain Engineering for Mission Critical Environments

Chris Rouland
Lehman Brothers

Abstract

Windows NT has grown quickly as an integrated solution for file and print services in Microsoft environments. Engineering NT solutions beyond the workgroup to integrate into heterogeneous environments is a task that in the past has required a large amount of trial and error. This paper addresses some real world issues that affect global NT deployments. The structure of the NT domains and their relationships is built upon organizational and performance requirements. The logical domain architecture affects the NT deployment from day one. Name services under NT are critical to day to day operations and must be engineered to incorporate fault tolerance while avoiding shortcomings in product. Authentication under NT must be molded to fit security and organizational requirements, while keeping cross platform and performance issues in mind.

Domain Structure

There are several logical models for NT domain architecture, the most feasible for large organizations are the Master or Multiple-Master domain models. Since NT only provides a two dimensional namespace, security and organizational relationships must be built into the domain architecture. NT provides an object based security model, however due to practical limitations in current product, architecture must take some numbers into consideration. To work around product limitations (performance and memory consumption), large organizations today must use the multiple master domain model. In this multiple master domain model ìMasterî domains provide authentication to users and services, and ìResourceî domains contain filesystem, printer, or other ìResourceî objects. By dividing username and resource utilization across Domains, product limitations are averted. Cross-Master resource access is provided by ìtrust-relationshipsî. Resource domains must also ìtrustî master domains when appropriate; to allow for administration of distributed resources by the master domains administration staff. Master domain models inherently offer fault tolerance through an architecture which provides for multiple domain controllers (DCís). DCís offer highly available authentication services for both machine and user accounts when properly distributed through the enterprise. A fault tolerant DC architecture will consist of authentication services aligned to both logical and physical network requirements. When properly configured a distributed DC architecture allows for timely synchronization of security data while providing low cost authentication. System requirements can be determined for DCís based on the following; number of global groups, number of machine accounts and the number of user accounts to be administered in the domain. Additional security services which rely on Windows NT domain authentication (i.e.: Microsoft Exchange) should be considered in planning for domain authentication throughput requirements. NT domain growth must be closely monitored and new domains properly managed. In the case of a domain which loses all DCís, all user, machine, and inter-domain security databases will be lost. NT Domains rely heavily upon a stable NT namespace (WINS). DCís manage their inter and intra-domain relationships based on functional name resolution. When namespace problems arise, inter-domain authentication can become dysfunctional through the loss of secure channels, or by establishing secure channel relationships across the WAN. Namespace dependant DC problems can be monitored with tools such as DOMMON and NLTEST in the server resource kit.

Name Service

NT name resolution is provided by four services:

WINS (Windows Internet Name Service)
LMHOSTS (static hosts file)
DNS (Domain Name Service)
Lanman Browsing

Although Windows NT supports multiple network protocols, the only protocol suitable for large NT infrastructures is TCP-IP. In the enterprise, a combination of the above name service providers will be found. WINS is the most scalable nameservice solution for NT environments today. WINS is a dynamic name service; machines are registered in the nameserver as the client network protocol stack is initialized. In addition to providing host information, WINS provides the following basic resource record types:

Software services (i.e.: RAS, NetDDE, NetMon)
Currently logged on user
Domain controllers
Domain master browser

These NetBios resource records are required for NT to authenticate and provide services across the WAN. Without a distributed namespace such as WINS, NetBios broadcasts would have to be routed to provide nameservice. WINS itself has limitations which if not adhered to can cause wide scale outages or corruption.
To propagate WINS updates across multiple servers, WINS provides replication services among servers. In many enterprises it appears at first logical to provide in a parallel infrastructure to the DNS space, aligning servers to subnets or as locally as possible to clients. Unlike DNS, whose zone transfers propagate in a tree fashion to ASCII flat file databases, WINS propagates in any configured topology, to a JET database back-end. The WINS JET database itself is not programmatically accessible and can only be maintained by a few primitive tools. In a large WINS infrastructure, a common mistake is to configure replication back upon the ìownerî of a resource record, or circular replication. In a case of circular replication, resource records in the JET database become corrupt and must be removed. A few tools, such as WINSCL.EXE and the WINS scavenging function can help in removing such records, but in the case of widespread corruption databases must be re-initialized or restored from tape (to a known good condition prior to the circular reference). A more manageable solution for WINS is to minimize the number of WINS servers and absorb the network costs.

DNS is a stable and scalable namespace found in most TCP-IP environments today. DNS can be used as a hybrid namespace for NT by providing access to core file and print resources while relying on an NT namespace solution to provide access to domain authentication resources. Solutions including a combination of LMHOSTS and DNS or static WINS entries for DCís and DNS can provide a stable and managed NT namespace. NT Server 4.0 can be configured as a DNS server, and also provides a DNS to WINS proxy service to allow for name resolution of WINS resources by DNS clients. Since most large enterprises deploying NT have a Unix based DNS infrastructure in production, NT DNS has been slow to gain adoption as a core primary DNS infrastructure.

At the lowest common denominator, NT supports two static namespace configuration files; LMHOSTS and HOSTS. Both configuration files are found under \WINNT\SYSTEM32\DRIVERS\ETC. The HOSTS file provides based name to IP address translation vis a vis the Unix /etc/hosts file. The LMHOSTS file contains static LAN Manager resource records in addition to IP addresses. LMHOSTS provides DC resource records, and supports limited centralization through client side #INCLUDEís. Although static hosts files provide reliable local name resolution, in a distributed NT environment, delivery and maintenance of these files can be difficult to administer.

Highly Available Servers

Several solutions exist today from third parties to provide fault tolerance in both software and hardware. One concern in implementing third party solutions in the NT DC and nameservice space is time to market for third party products as aligned to NT service packs. In an NT domain infrastructure is it critical to keep DCís and nameservice at the same software revision. Software enhancements (such as strong SAM, and SMB signing) as well as bug fixes, usually revision dependant for clients, servers and domain controllers. In a mixed revision DC infrastructure, DCís usually need to be brought to the same revision to be supported. Historically, the WINS services have been updated in every service pack of NT, and servers should be upgraded in unison. Due to the strong requirements of the NT DCís and namespace to be a ìcleanî environment, it is difficult to identify products that can meet all these needs. Most HA products for NT today provide well for file and print services.

The most supportable solution today for a highly available namespace, from the server side, is to provide hardware fault tolerance. Mission critical servers in the namespace should implement disk fault tolerance and verify nightly backups. Additional fault tolerance such as fail-over network interfaces, processors and error correcting memory add to availability as well. Due to namespace problems, in some cases, multi-homing servers can actually become destabilizing to the infrastructure.

Summary

Windows NT can be built to meet the needs of mission critical applications today by providing a stable namespace and authentication architecture. As NT drops legacy support of older protocols we will see a much more supportable and integrated NT namespace. By adhering to upcoming protocols such as dynamic DNS, and existing ones such as Kerberos, the difficult issues in managing a closed namespace and authentication architecture will open up.