Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Considerations for Dynamic DNS Implementation in a Windows2000 Environment

Windows2000 name resolution is based on Dynamic DNS. Microsoft's implementation of Dynamic DNS is based on RFC 2136. This correlates to BIND v8 and v9. BIND v9 is covered in the 4th Edition of "DNS and BIND" by Paul Albitz & Cricket Liu, published by O'Reilly. In Windows2000, Dynamic DNS is integrated with and related to DHCP, WINS, and Active Directory. There are 3 ways to implement DNS in a Windows2000 domain: Active Directory Integrated, Active Directory primary with non-Active Directory secondary(s), or non-Active ...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Considerations for Dynamic DNS Implementation in a Windows2000 Environment

Deborah Wade

Security Essentials v1.2e

Windows2000 name resolution is based on Dynamic DNS. Microsoft's implementation of Dynamic DNS is based on RFC 2136. This correlates to BIND v8 and v9. BIND v9 is covered in the 4th Edition of "DNS and BIND" by Paul Albitz & Cricket Liu, published by O'Reilly.

In Windows2000, Dynamic DNS is integrated with and related to DHCP, WINS, and Active Directory. There are 3 ways to implement DNS in a Windows2000 domain: Active Directory Integrated, Active Directory primary with non-Active Directory secondary(s), or non-Active Directory primary and non-Active Directory secondary(s). When DNS is fully integrated into Active Directory, we can then utilize three important security benefits in a Windows2000 network: Secure dynamic updates, Secure zone transfers, and Access Control Lists for zones and resource records.

1.0 SECURE DYNAMIC UPDATES

One of the most important security features of Dynamic DNS (DDNS) is the secure update feature. A major consideration in implementing the secure update feature is ownership of the records that comprise a DNS entry. Ownership is determined by a combination of how DHCP is configured and which clients need to be supported.

Two DNS resource records are associated with each client: the A record and the PTR record. The A record resolves the name to address, while the PTR record resolves address to name. The address refers to the IP address of the client. The name refers to the Fully Qualified Domain Name of the client machine. This would be the computer name appended to the Domain Name of the network.

In a Windows2000 environment, client DNS records are registered when the client is requesting an IP address via DHCP. Depending upon setup, the client, the DHCP server, or a combination of these two can update the A and the PTR records associated with the client. Ownership of these records depends upon who registered the record.

Here are the options for defining ownership of the A and PTR records for clients in a Windows2000 network.

1.1 Windows2000 Native Mode

In a Windows2000 environment, both DHCP servers and DHCP clients can register records with DNS. A Windows2000 environment is defined as "Native Mode" when the network consists solely of Windows2000 servers and clients.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

When the client is a Windows2000 client, then the default configuration is for the client to dynamically update its own A record during registration on the network. During this same time, the DHCP server updates the client's PTR record. So, ownership of the A record resides with the client and ownership of the PTR record resides with the DHCP server.

A second possible configuration is for the DHCP server to always update the forward and reverse lookups. In this case, the DHCP server owns both the A and PTR records, respectively.

The third possible configuration is for the DHCP server to be configured to NOT perform dynamic updates. In this case, the client will update both the A and PTR records and therefore own both of these records.

1.2 Windows2000 Mixed Mode

In a mixed environment, DHCP clients cannot register with DNS. A mixed environment is defined as "Mixed mode" when the network consists of Windows2000 servers, with clients consisting of Windows NT 4.0 or Windows98, in addition to Windows2000.

Legacy clients, such as Windows NT 4.0 and Windows 9x, cannot register directly with DNS. Since only DHCP servers can register records with DNS, the only option in a mixed environment is to have the DHCP server register both the A and PTR records. In this case, the server owns both the forward and reverse lookup records.

1.3 Secure dynamic updates

Secure dynamic update in a Windows2000 network is only available via Active Directory integrated DNS zones. So what does secure dynamic updates mean? In Windows2000 it means utilizing the Active Directory ACLs to specify users' and groups' authority to modify the DNS zone &/or its resource records. In addition to utilizing ACLs, secure updates also utilizes secure channels and authentication in order to allow updates of the DNS zones &/or its resource records.

Microsoft Windows2000 supports the secure dynamic update using the algorithm defined in the IETF Internet-Draft "GSS Algorithm for TSIG (GSS-TSIG). This algorithm uses Kerberos v5 as the underlying authentication protocol. The GSS-API is specified in RFC 2078.

2.0 ZONES

2.1 Types of Zones

Windows2000 can configure DNS zones as Primary, Secondary, or Active Directory Integrated.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Primary and Secondary zones act the same as in a Unix environment and an NT 4.0 environment. Additionally, the databases remain separate from other databases such as the WINS and DHCP databases, and replication is setup separately from other replication services. Primary/Secondary zones must be utilized if any server in the network is running a BIND version below 8.1.2 because of the lack of support for Dynamic Updates in previous versions.

If Active Directory is installed, then DNS zones can become Active Directory Integrated zones. This means that the DNS zone database becomes part of the Active Directory Database. Each record becomes an Active Directory object. Each Active Directory object has its own ACL (Access Control List)

2.2 Types of Zone Transfers or Replications

Windows2000 DNS can support either AXFR or IXFR. AXFR, or all zone transfer, is the replication of the entire zone database file. IXFR, or incremental zone transfer, is a replication of the zone database changes only. These zone transfer processes are applicable if the zone type has been set to Primary/Secondary. IXFR is supported in BIND version 8.2.1 and above.

When DNS is integrated with Active Directory, all zones and resource records become Objects in the Active Directory Database. Active Directory replication is based on a multi-master model.

One of the benefits of a multi-master model is that there is no single point of failure. This is possible because the Active Directory database, of which DNS is one part, is replicated to all domain controllers.

A second benefit to the multi-master model is that only one replication topology needs to be setup. The DNS zone database becomes part of the Active Directory Database. DNS zone transfers are therefore completed as part of the Active Directory replication.

2.3 Security of Zone Transfers

If the Windows2000 network is running DNS in the Primary/Secondary zone configuration, the options for encryption and compression are not available. For BIND compatibility, Windows2000 does support AXFR sending/receiving one or multiple resource records per message. BIND versions earlier than 4.9.4 do not support multiple resource records being transferred per message. Windows2000 supports IXFR. This corresponds to BIND version 8.2.1. Windows2000 supports DNS Notify, which corresponds to BIND version 8.1.2.

When Windows2000 DNS is configured as Active Directory Integrated, then the replication process is part of the Active Directory replication and therefore will automatically utilize encryption and compression.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Encryption utilized is Microsoft Windows2000 Kerberos v5. Communication channels between domain controllers are automatically encrypted. No administrative configuration is required.

Compression is automatically utilized when Active Directory updates are being transmitted between "Bridgehead" servers. A Bridgehead server is a server that is automatically selected from among other servers within the local area network. When wide area network links need to be used for Active Directory Updates, then each local area network's bridgehead server communicates with the other Bridgehead servers. This reduces the amount of traffic across WAN links. In this instance, compression is automatically utilized in order to preserve bandwidth.

3.0 ACTIVE DIRECTORY INTEGRATION FOR DNS ZONES

Because of the integration between Active Directory and DDNS in Windows2000, a secure implementation of Active Directory is the first step toward a secure implementation of DDNS.

3.1 File System

Use NTFS. Windows2000 version is NTFS v5. This version allows for file and folder security, encrypted file system, and auditing. NTFS v5 is not compatible with previous versions of NTFS. NT4.0 can only read NTFS v5 if it has Service Pack 4 or higher installed.

NTFS permissions can be set at both the folder and file level and can be used to limit network and local access to files.

The combination of NTFS and Share permissions can be used to configure rather precise control over permissions and inheritance.

3.2 Registry

Utilize the registry editor to edit the DACLs associated with each Registry Hive. Reference SANS publication "Windows NT Security, Step-by-Step" for specifics.

3.3 Enterprise Admins and Schema Admins groups

After the Windows2000 network is built, limit access to these two administrative groups. These groups appear at the root of the domain and have unlimited administrative capabilities. Depending upon the structure of the domain, administration can be delegated down the domain structure so that administrative capabilities are limited to individual domains.

3.4 Encrypted File Systems

Windows2000 NTFS offers the option to utilize Encrypted File Systems. EFS uses public key based technology that further inhibits unauthorized access to files.

3.5 DNS in Active Directory

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Installation of DNS will extend the Active Directory schema to include the DNSUpdateProxy group. This is a very powerful group that allows objects to be created that has no security. When this occurs, any authenticated user can take ownership of those objects created in this manner.

Client records A and PTR are updated in DNS during the DHCP process in Windows2000 as detailed above. When both clients and servers are Windows2000, then secure dynamic updates can be completed using a default installation. When other clients need to be supported, then secure dynamic updates cannot be used unless the DHCP Server is added to the DNSUpdateProxy group. This allows the DHCP server to perform dynamic updates for these legacy clients.

Special consideration must be taken if the DHCP service is running on a Domain Controller Server. In this case, addition the DHCP server to the DNSUpdateProxy group will allow any user or computer full control of the DNS records corresponding to the Domain Controller.

3.6 Ownership of Resource Records

It is important in a Windows2000 network that the DHCP server not perform a secure dynamic updates on legacy clients. If this happens, then there are instances where active records could not be updated at all. For instance, an NT4.0 client has its name registered in DNS via the DHCP server. This machine is the upgraded to a Windows2000 client. The name remains the same since the upgrade is an operating system upgrade. The DHCP server owns the resource record with this name since it originally registered the name. The Windows2000 client cannot update its own name.

3.7 WINS Lookup

As a final caveat of Windows2000, I would like to explain that WINS would most likely be a required part of all Windows2000 networks. Why? Well, NetBios resolution is still required for any client that is NOT Windows2000. Also, any programs requiring NetBios will require WINS for name resolution. WINS integrates directly into DNS by using two special resource records: WINS and WINS-R. These are the forward and reverse lookup records for WINS respectively.

4.0 CONCLUSION

In conclusion, it is important to understand the process with which Windows2000 can and does utilize DNS. These considerations were outlined in sections 1.0 Secure Dynamic Updates and 2.0 Zones in this paper. It is also important to understand some of the “gotcha’s” and “caveats” of Windows2000. Section 3.0 Active Directory Integration for DNS Zones listed some of these items.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

CITATION OF SOURCES

Albitz, Paul & Cricket Liu. DNS and BIND, 4th Edition. O'Reilly & Associates, April 2001.

Microsoft, "Windows2000 DNS White Paper"
URL:
http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/w2kdns.asp

Microsoft, "Chapter 5. Introduction to DNS" online version of Chapter 5 from "TPC/IP Core Networking Guide", part of Windows2000 Resource Kit, published by Microsoft Press.
URL:
http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cncc/cncc_dns_wgga.asp

Microsoft, "Chapter 6. Windows 2000 DNS" online version of Chapter 6 from "TPC/IP Core Networking Guide", part of Windows2000 Resource Kit, published by Microsoft Press.
URL:
http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cncf/cncf_imp_vsin.asp

Microsoft, "Designing a Secure Microsoft Windows 2000 Network" Class Pack, Material No: 2150ACP.

Microsoft, "Updating Support Skills from Microsoft Windows NT to Microsoft Windows 2000" Class Pack, Material No: 1560BCP

Microsoft, "Dynamic Host Configuration Protocol for Windows 2000 White Paper"
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/dhcpnt5.asp

SANS. "Windows NT Security, Step-by-Step" version 3.03, February 2001.

Salamon, Andras. "DNS related RFCs"
http://www.dns.net/dnsrd/rfc/

Vixie, P., Editor "RFC 2136. Dynamic Updates in the Domain Name System (DNS Update)"
URL:
http://www.faqs.org/rfcs/rfc2136.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 3rd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced