

Tru64 UNIX

Integrating Windows 2000 DNS Clients with Tru64 UNIX DNS Servers

October 2000

This Best Practice describes how to integrate Windows 2000 Domain Name System (DNS) clients in an environment that uses Tru64 UNIX systems as primary DNS servers.

Contents

Integrating Windows 2000 DNS Clients with Tru64 UNIX DNS Servers

Is This Best Practice Right for You?	1
Before You Begin	2
A Sample Integration Scenario	2
Applying the Best Practice	3
Configuring the Tru64 UNIX DNS Master Server	3
Configuring the Windows 2000 Systems	5
Verifying Success	5
Troubleshooting	6
Alternative Practices	6
Comments and Questions	6
Legal Notice	6

Integrating Windows 2000 DNS Clients with Tru64 UNIX DNS Servers

Windows 2000 uses the Domain Name System (DNS) as its Windows Service Locator. The domain controller inserts service locator (SRV) records dynamically into a DNS zone. Windows 2000 clients then use these records to locate services on the domain controller.

Windows 2000 also relies on dynamic updates with the option of having secure dynamic updates. However, the Windows 2000 secure dynamic update is proprietary as it was finished before the secure dynamic update standard (RFC 2137) was approved. As a result, Windows 2000 secure dynamic updates cannot be interpreted by non-Microsoft DNS servers, including Tru64 UNIX DNS servers.

For those organizations with an existing DNS infrastructure using Tru64 UNIX DNS servers, there is a solution that enables you to use the latest security features of Windows 2000 while providing interoperability between the domain controller and the DNS primary server for the zone.

See the Tru64 UNIX Best Practices Web page for more information about Best Practices documentation:

http://www.tru64unix.compaq.com/docs/best_practices/

Is This Best Practice Right for You?

Not all Best Practices apply to all configurations, so you must be sure that it is appropriate for your system and circumstances. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 5.1
System Configuration	DNS primary server (BIND Version 8.2.2 P5)

Requirement	Description
Impact on Availability	None
Skills	Knowledge of DNS and Windows 2000 environments

If you do not meet the previous requirements, see *Alternative Practices* for information.

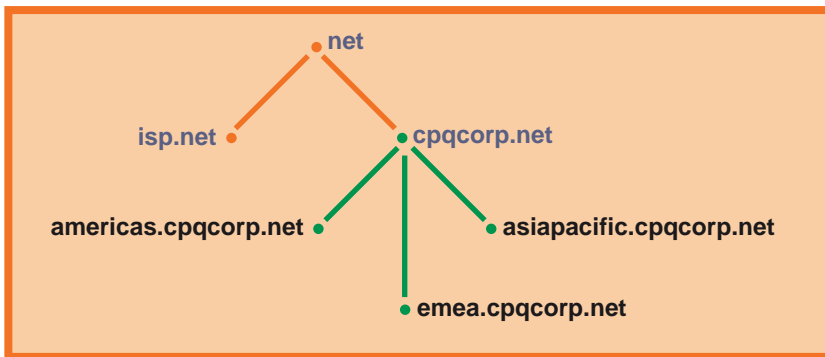
Before You Begin

Before you apply the Best Practice for integrating Windows 2000 DNS clients with Tru64 UNIX DNS servers, you must understand some background information and perform some preliminary tasks.

- Understand Windows 2000 DNS operation
You must have a thorough knowledge of Windows 2000 system administration, specifically DNS configuration and operation. You should also know what an Active Directory server is and how it operates. See the Windows 2000 documentation.
- Understand Tru64 UNIX DNS Operation
You must know how to configure a Tru64 UNIX DNS server. See the *Network Administration* manual for more information.
- Understand Windows 2000 DNS integration issues. See *Overview of DNS for Windows 2000* in Compaq's ActiveAnswers web site and the Microsoft Product Support Services web site.

A Sample Integration Scenario

One way to integrate Windows 2000 clients with your Tru64 UNIX DNS servers is shown in the following illustration of a representative enterprise DNS hierarchical map. However, companies can add their Windows 2000 DNS zone at any point in the hierarchy, from the root zone on down. However, the namespace must be contiguous.



In this scenario, Compaq added three Windows 2000 DNS zones to its `cpqcorp.net` zone (the parent zone). The `cpqcorp.net` zone might have as its primary DNS server the system `server1.cpqcorp.net` (`server1`). The `server1` system has primary authority for the `cpqcorp.net` zone.

There are three Windows 2000 zones: `americas.cpqcorp.net`, `emea.cpqcorp.net`, and `asiapacific.cpqcorp.net`. The DNS server for the `americas.cpqcorp.net` zone might be `dc1.americas.cpqcorp.net` (`dc1`), which also has the IP address `10.1.0.1`.

This integration scenario enables you to take full advantage of the DNS features of Windows 2000, particularly Active Directory and secure dynamic updates, and your existing DNS infrastructure. In addition, you can designate an entire subnet as being safe for updates, and thereby reduce the size and complexity of the access control lists for the primary DNS server.

Applying the Best Practice

Before you integrate Windows 2000 DNS clients with Tru64 UNIX DNS servers, be sure to follow the recommendations in *Before You Begin*.

Configuring the Tru64 UNIX DNS Master Server

For this scenario, do the following on the DNS master server:

1. Delegate the Windows 2000 zones (forward and maybe reverse) from an existing DNS zone (parent). In the example, the child

americas.cpqcorp.net zone is delegated from the parent cpqcorp.net zone. You might also delegate the reverse (in-addr.arpa) zone at the same time, depending on your organization's reverse zone delegation policies.

To delegate new zones, add an NS record and an A record for the DNS server (may also be a domain controller) in the Windows 2000 domain to the domain database file. In the example, add the following records to the hosts.db file for the cpqcorp.net zone:

```
w2k-americas                IN    NS    dcl.americas.cpqcorp.net.
dcl.americas.cpqcorp.net    IN    A     10.1.0.1
```

If you are delegating reverse records, add an NS record in the parent reverse zone for the in-addr.arpa zone. In the example, if you were delegating a class C address block, you would add the following record to the parent reverse zone:

```
0.1.10.in-addr.arpa        IN    NS    dcl.americas.cpqcorp.net.
```

If and how you do this depends on the type of network you have and its network mask. If you use Classless Inter-Domain Routing (CIDR) address delegation, see RFC 2317 for more information.

2. If the Windows 2000 DNS server is to be a slave server for the parent zone and is not listed in the Start of Authority (SOA) record of the parent zone, add the also-notify option and the IP address of the domain controller to the named.conf file. In the example, the zone statement with this option is as follows:

```
zone "cpqcorp.com" {
    type master;
    file "hosts.db";
    also-notify {10.1.0.1};
};
```

Be aware that the allow-transfer option may be specified in the configuration file to restrict zone transfers. If you use this option, you need to add the IP address of any slave servers, including Windows 2000 DNS servers, to the address list.

3. Send a SIGHUP signal to the named daemon master server to force it to reread its configuration files, as follows:

```
# /sbin/init.d/named restart
```

Configuring the Windows 2000 Systems

For the sample scenario, follow these steps:

1. Determine the roles of the DNS server.

In this scenario, the DNS server will be primary for its own domain. The server can also be any of the following:

- A slave server for the parent zone (`cpqcorp.net` in the sample configuration). You might choose this option if the DNS server has sufficient storage for the parent zone information and needs access to the information locally. Having this information resident on the server might result in faster name resolution.
 - A system that uses a forwarder. You might choose this option if the DNS server does not have enough storage or if your recursion policy directs forward lookups through a forwarder hierarchy. Any queries for which the server is not authoritative are forwarded to a DNS server.
2. Determine if you want the Windows 2000 domain to be an Active Directory Integrated zone.
 3. Determine if you want to enable secure dynamic updates.
 4. Set the Windows 2000 DNS server (`dc1`) as the primary for the delegated zone by configuring a forward lookup zone using the Microsoft Management Console (MMC) DNS snapin. See your Windows 2000 documentation for information. See your Windows 2000 documentation for information.
 5. Configure the other Windows 2000 clients and servers. See your Windows 2000 documentation for information.

Verifying Success

After you apply the Best Practice for integrating Windows 2000 DNS clients with Tru64 UNIX DNS systems, you can verify whether it was successful by doing the following:

1. Use the `nslookup` command from any DNS client outside of the Windows 2000 domain and obtain the IP address for a system in the Windows 2000 domain.
2. Use the `nslookup` command from any Windows 2000 client and obtain the IP address for a system outside the Windows 2000 domain.

See `nslookup(8)` for more information.

If the Best Practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

Troubleshooting

If you determine that the Best Practice was not successful, as described in *Verifying Success*, use the extensive problem solving information and DNS server testing information contained in the *Network Administration* manual.

Alternative Practices

Although this Best Practice is the recommended method for integrating Windows 2000 DNS clients with Tru64 UNIX DNS systems, if your system does not meet the requirements described in *Is This Best Practice Right for You?*, you can use one of the following alternative methods:

- Convert your existing DNS domain to run on a Windows 2000 DNS server through conventional zone transfers. See your Windows 2000 documentation for information.
- Disable secure dynamic updates on the Windows 2000 systems (see your Windows 2000 documentation for information). Then, enable the Tru64 UNIX DNS server to manage the Windows 2000 dynamic zones by allowing dynamic updates (with the `allow-update` statement) and restricting the updates to certain DNS and DHCP servers (with the `acl` statement). See the *BIND Configuration File Guide* for information on the `allow-update` and `acl` statements.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

`best_practices@zk3.dec.com`

Legal Notice

Compaq, the Compaq logo, and Tru64 are trademarks of Compaq Information Technologies Group, L.P. in the U.S. and/or other countries. UNIX is a trademark of The Open Group in the United States and/or other countries. Active Directory and Windows are trademarks of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.