26. DECUS Symposium in Bonn

DNS in a Windows 2003 Server World

Thomas Strasser, Technischer Projektleiter
HPS C&I
Thomas.Strasser@hp.com

Bonn, 9.04.2003

Agenda

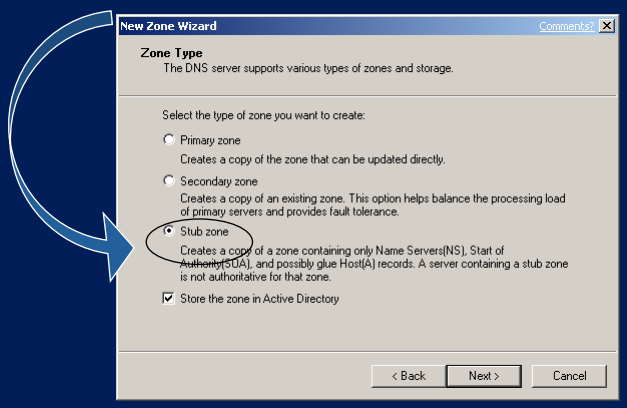
- Updates to DNS in Windows 2003
  - DNS Stub Zones
  - Conditional forwarding
  - Security extensions
  - Managing DNS Client with GP
  - DNS Islands
- DNS and Application Partitions
  - What are Application Partitions
  - How was DNS handled in Windows 2000?
  - How does DNS fit into Application Partitions?

DNS Stub Zones

- So what's the problem?
  - Delegations are static
  - Once assigned they need to be manually updated
  - Can easily become stale
- What's a stub zone?
  - Basically it is like a dynamic delegation
  - Periodically the stub zone server will query the target zone Name Server's
  - Stub zone gets updated
  - "Load balancing" between target Name Server's

Configuring Stub Zones

- New installation option
  - New Stub Zone



Conditional Forwarding (I)

- What is forwarding?
  - Long established mechanism for controlling how DNS servers respond to requests they can't answer authoritatively.
  - If the DNS server cannot authoritatively answer the query they will use their forwarders.

Conditional Forwarding (II)

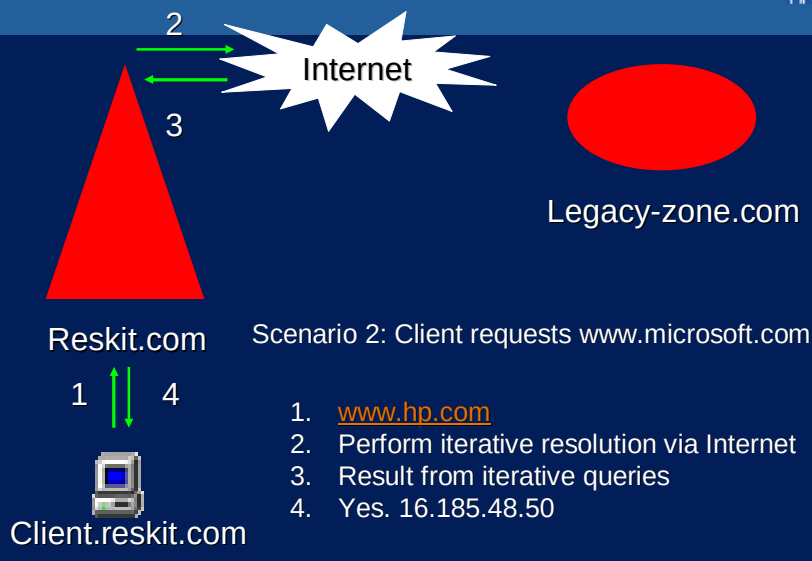
- So what is conditional forwarding?
  - Allows more selective forwarding
  - Configure multiple forwarding options depending upon the query
  - More flexible

Conditional Forwarding (III)

Scenario 1: Client requests www.reskit.com

1. www.reskit.com
2. Yes. 192.168.10.200

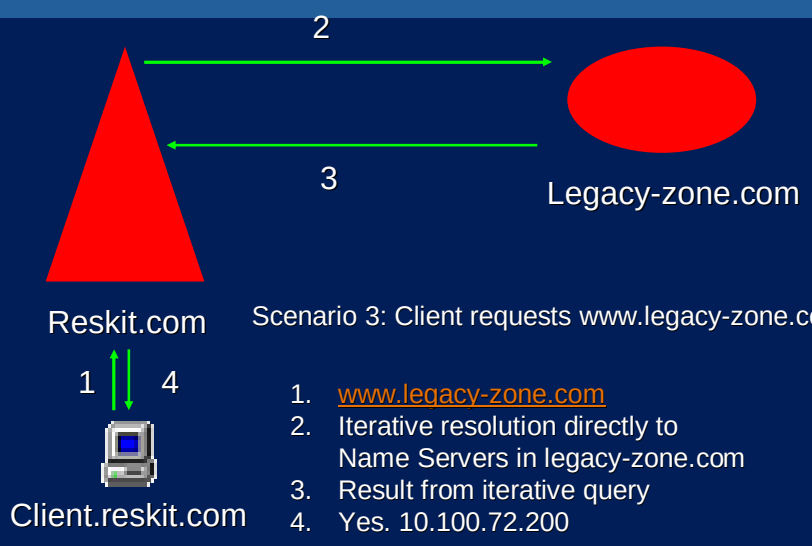
Conditional Forwarding (III)



Scenario 2: Client requests www.microsoft.com

1. www.hp.com
2. Perform iterative resolution via Internet
3. Result from iterative queries
4. Yes. 16.185.48.50

Conditional Forwarding (III)



Scenario 3: Client requests www.legacy-zone.com

1. www.legacy-zone.com
2. Iterative resolution directly to Name Servers in legacy-zone.com
3. Result from iterative query
4. Yes. 10.100.72.200

Security Extensions

- Support for storing:
  - KEY
  - SIG
  - NXT
- However full use of these is not supported by the Windows 2003 DNS Server i.e. it does not perform the cryptographic functions outlined for these record types.

Managing DNS Client with GP

- New GP configuration settings:

DNS Islands

- What are DNS Islands?
  - A rare possibility in Windows 2000 Forest root Domains
  - See q275278
- So how did we fix it?
  - Windows 2003 server DNS service will now register SRV records with partner DNS servers as well as locally.

DNS and Application Partitions

- What did we have in Windows 2000?
  - Standard DNS
  - AD integrated
- Advantages of AD integrated:
  - Multi-master registration and replication
  - Fault-tolerance
  - Single replication topology for AD and DNS
- Disadvantages of AD integrated:
  - Unnecessary Replication to non DNS DC's
  - Replication to GC
  - Limited to Domain Scope

DNS and Application Partitions

- What do we have now in Windows 2003?
  - Standard DNS
    - As we have always had
  - AD Integrated
    - As we had in Windows 2000 but with some additions
  - Application Partitions
    - All new feature

AD Integrated DNS

- Now support 3 types of Active Directory integrated zone:
  - Primary
  - Secondary
  - Stub Zone
- Stored in Domain Naming Context: *Domain*\System\Microsoft DNS
  - As is the case today in Windows 2000
  - Replicated to GC

Application Partitions (I)

- Designed for a number of scenarios:
  - Dynamic data
  - Application data
  - Give control to scope of replication and placement of replicas
- They have Forest-wide scope
- Also referred to as ‘Non-Domain Naming Contexts’

Application Partitions (II)

- Leverage existing infrastructure
  - Use same Site definitions and parameters
  - Use same replication model
- Same security and access control model
  - Access to objects is controlled by ACL's
- Application Partitions are created in the same way as Domain partitions:
  - A crossRef object is created in cn=partitions,cn=configuration,dc=*forestRootDomain*
  - It is of type DomainDNS
  - However there is no NetBIOS name association

Creating Application Partitions

- Application Partitions are created by:
  - Ntdsutil
  - Dcpromo
  - Dnscmd
  - LDAP / ADSI API's
- Requires:
  - Enterprise Admin credentials
  - Access to the Domain Naming Master
- Default Application Partitions:
  - DNS – ForestDNSZones and DomainDNSZones

Benefits of Application Partitions

- Custom replication topology
- Advantages :
  - Reduces unnecessary replication
  - Security
  - Spans domains
  - Not replicated to the GC

Locating Partitions

- Application partitions located using DNS
  - Registers two SRV records per partition:
    - _ldap._tcp.*AppPartName*
    - _ldap._tcp.*SiteName*._sites.*AppPartName*

Interoperability

- Windows 2000 domain controllers do not support Application Partitions
  - However, Application Partitions can still be used in mixed environments
  - Note that Windows 2000 DC's will not participate in the replication of Application Partitions

Using Application Partitions

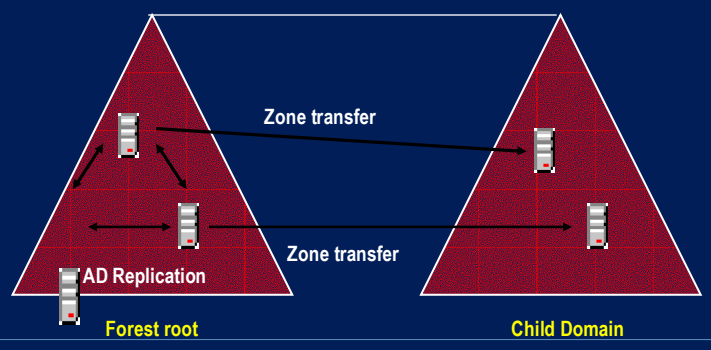
- Two default DNS application partitions:
  - DC=domaindnszones, DC=*forest_root_domain_name*
    - Targeted at DNS servers in the same Domain
  - DC=forestdnszones, DC=*forest_root_domain_name*
    - Targeted at DNS servers in the forest

Using Application Partitions

- The importance of the _msdcs zone:
  - Forest resources such as GC
  - Replication DSA GUID's
  - These resources are required Forest wide
  - Any failure to locate these resources will affect the Forest

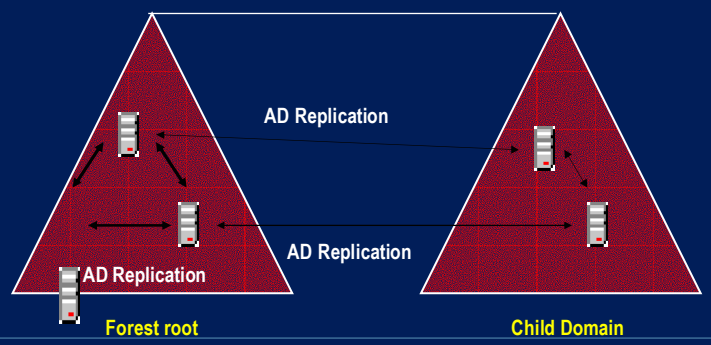
Using Application Partitions

- Common scenario in Windows 2000:
  - _msdcs zone configured in Forest Root
  - Secondary zones created in child domains



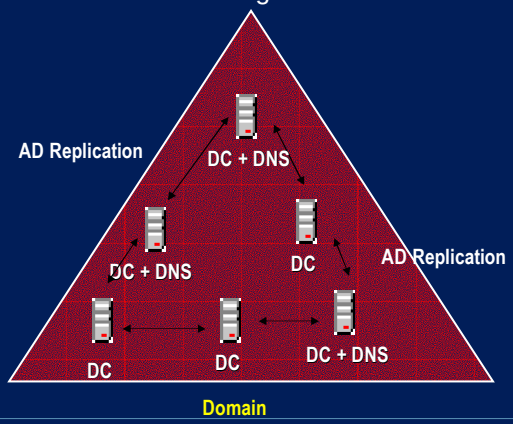
Using Application Partitions

- With Windows 2003 Server now:
  - Default application partition DC=forestdnszones
  - Replicated to all DC's running DNS in the forest



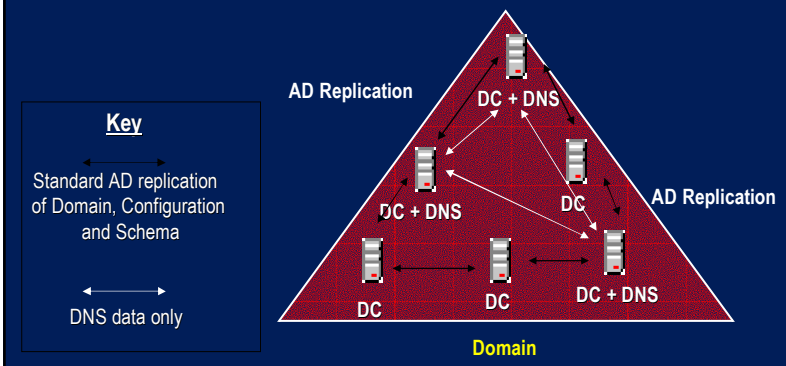
Using Application Partitions

- With Windows 2000:
  - AD integrated DNS data was replicated to all DC's
  - Even if the DC was not running DNS



Using Application Partitions

- With Windows 2003 Server now:
  - Default Domain Application Partition domaindnszones
  - Domain DNS data is ONLY replicated to DNS servers



Fragen ?

invent