



The Love-Hate of AD and DNS

N3K Expert Webinar Series

Housekeeping

- Timing, Schedule, Q&A Session
- Online Etiquette (microphones, distracting activities)
- Recording and Privacy



Distinct Entities

Domain Name System (DNS)

- Hierarchical **distributed Database**
- Resolves fully-qualified Domain Names to IPs (**Internet and Intranet**)
- Based on **open Standards** (RFCs)
- Implemented by **multiple Vendors**

Active Directory (AD)

- LDAP-based **Directory Service**
- Exclusively **implemented by Microsoft** (MS)
- Not relevant on the Internet, **only Intranet**
- Serves **multiple Functions** in MS Network
- Contains Info (**Computers, Services, Users & Sites**)

Need for Integration

- Active Directory **requires DNS**
- DNS as **central Component** in Network (successor to WINS)
- DNS **Misconfigurations affect AD** Replication

Frequent Misunderstandings

- Using **same Naming Conventions** (domains like "mrddi.org")
- Each Domain in AD requires **corresponding Domain** in DNS
- **Domains are distinct** (AD Domain "mrddi.org" ≠ DNS Domain "mrddi.org")
- **Applications** built on Active Directory **impact DNS**
- Assumption that Applications would **only work with MS DNS**
- **DNS Servers are also AD Domain Controllers** in pure Windows Environments

Contact Points of AD and DNS

- DNS Resolution for all Clients in an AD Environment is expected
- Self-Registration of Windows Clients and Servers in DNS
- Announcement of Sites and Services for AD Domain Controllers via DNS
- Key Services like LDAP, Kerberos or Global Catalog
- Localization of AD Domain Controllers and their Services is main Purpose of DNS Entries
- DNS Registration via SRV Records
- Additional Information stored in AD, not in DNS (print & file services, etc.)

AD Requirements for DNS

- Microsoft DNS **Infrastructure Requirements**
 - **Service Records** required (RFC 2782)
 - **Dynamic DNS** Updates recommended (RFC 2136)
- Additional Features of **varying Importance**
 - Secure dynamic DNS (**GSS-TSIG**, RFC 3645)
 - Incremental **Zone Transfers** (RFC 1995)
 - **Notifications** (RFC 1996)
 - **Multi-Primary** DNS (not compliant with DNS RFCs)
 - **Aging & Scavenging** (not compliant with DNS RFCs)

Service Records (SRV)

- **Service-to-Host** Mapping
- Users and Applications **discover where Service is located**
- **Standardized** Service Names and Numbers¹
- **Prioritization** via Priority and Weight

```
_sip._tls.mrddi.org.      SRV 0 0 443 sip.mrddi.org.  
_xmpp-server._tcp.mrddi.org.  SRV 0 0 443 sip.mrddi.org.  
_sipfederationtls._tcp.mrddi.org. SRV 0 0 5061 sip.mrddi.org.
```

¹ <https://www.iana.org/assignments/service-names>

Example of SRV Records of a Domain Controller

```
netlogon.dns - Notepad
File Edit Format View Help
mrddi.org. 600 IN A 10.0.187.236
_ldap._tcp.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.Default-First-Site-Name._sites.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.pdc._msdcs.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.d4050841-fedb-4b15-95b9-1ad2a30dd203.domains._msdcs.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
079bf3ba-7f7e-44bb-92fa-1905839b07a1._msdcs.mrddi.org. 600 IN CNAME win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.dc._msdcs.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.gc._msdcs.mrddi.org. 600 IN SRV 0 100 3268 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.mrddi.org. 600 IN SRV 0 100 3268 win-3q2c1lv6e3e.mrddi.org.
gc._msdcs.mrddi.org. 600 IN A 10.0.187.236
_kerberos._tcp.dc._msdcs.mrddi.org. 600 IN SRV 0 100 88 win-3q2c1lv6e3e.mrddi.org.
_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs.mrddi.org. 600 IN SRV 0 100 88 win-3q2c1lv6e3e.mrddi.org.
_kerberos._tcp.mrddi.org. 600 IN SRV 0 100 88 win-3q2c1lv6e3e.mrddi.org.
_kerberos._tcp.Default-First-Site-Name._sites.mrddi.org. 600 IN SRV 0 100 88 win-3q2c1lv6e3e.mrddi.org.
_gc._tcp.mrddi.org. 600 IN SRV 0 100 3268 win-3q2c1lv6e3e.mrddi.org.
_gc._tcp.Default-First-Site-Name._sites.mrddi.org. 600 IN SRV 0 100 3268 win-3q2c1lv6e3e.mrddi.org.
_kerberos._udp.mrddi.org. 600 IN SRV 0 100 88 win-3q2c1lv6e3e.mrddi.org.
_kpasswd._tcp.mrddi.org. 600 IN SRV 0 100 464 win-3q2c1lv6e3e.mrddi.org.
_kpasswd._udp.mrddi.org. 600 IN SRV 0 100 464 win-3q2c1lv6e3e.mrddi.org.
DomainDnsZones.mrddi.org. 600 IN A 10.0.187.236
_ldap._tcp.DomainDnsZones.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
ForestDnsZones.mrddi.org. 600 IN A 10.0.187.236
_ldap._tcp.ForestDnsZones.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.mrddi.org. 600 IN SRV 0 100 389 win-3q2c1lv6e3e.mrddi.org.
mrddi.org. 600 IN AAAA 2003:c3:3f34:5d00:9e1:e02e:544b:2d2c
gc._msdcs.mrddi.org. 600 IN AAAA 2003:c3:3f34:5d00:9e1:e02e:544b:2d2c
DomainDnsZones.mrddi.org. 600 IN AAAA 2003:c3:3f34:5d00:9e1:e02e:544b:2d2c
ForestDnsZones.mrddi.org. 600 IN AAAA 2003:c3:3f34:5d00:9e1:e02e:544b:2d2c
|
Windows (CRLF) Ln 31, Col 1 100%
```

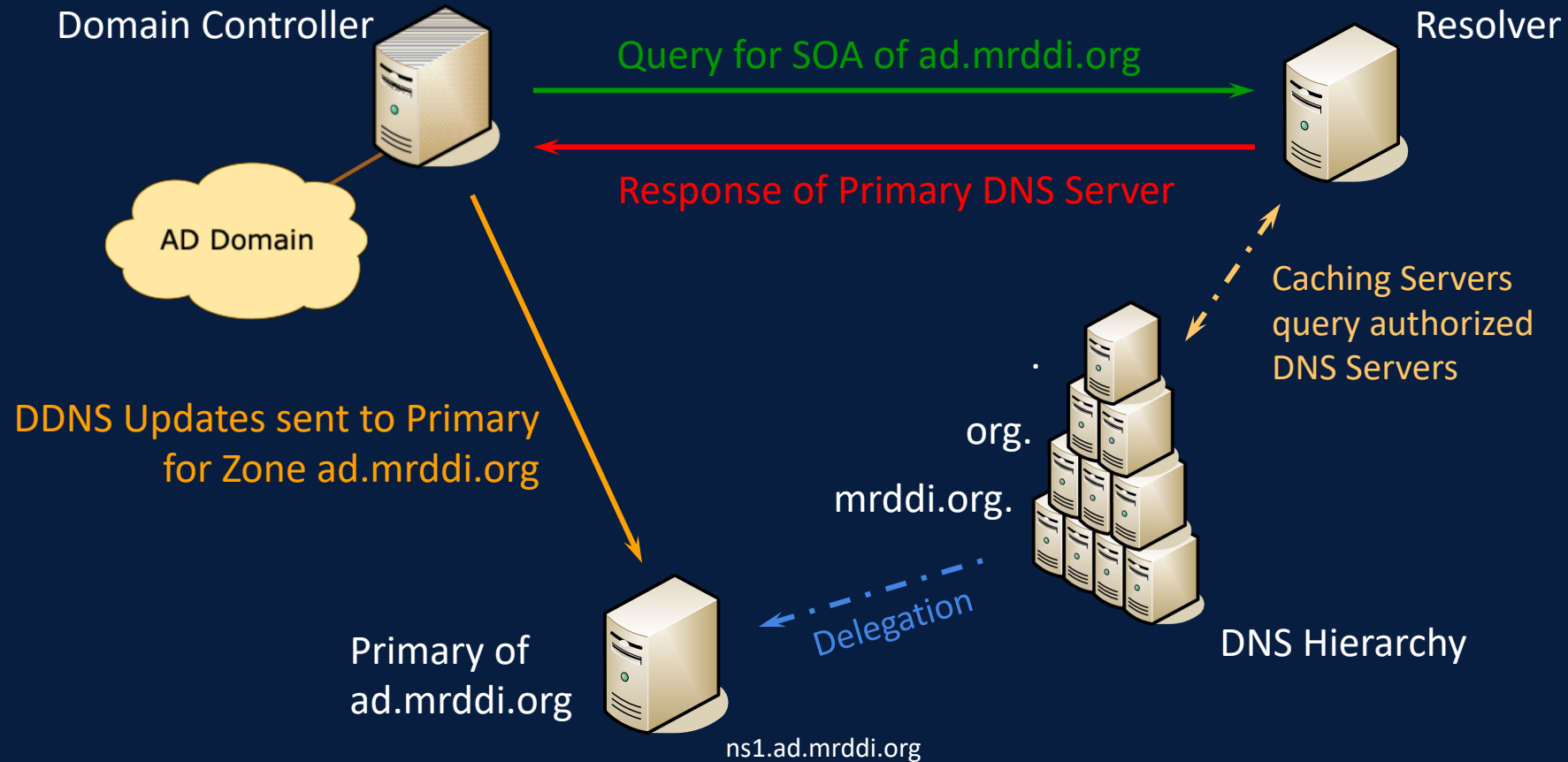
„Underscore“ Domains

- SRV Records registered in 4 “underscore” Domains
 - `_msdcs`
 - `_sites`
 - `_tcp`
 - `_udp`
 - (ForestDnsZones)
 - (DomainDnsZones)
- “Underscore” Domains **operable as individual Zones**
 - **Delegating** these Zones often advisable

Dynamic DNS Updates (DDNS)

- **Add and delete Entries in DNS** Domain via DNS Messages to authoritative DNS Server
- Sent in Active Directory by:
 - **Static MS Clients** (A/PTR Records on Boot, re-register after 24 Hours)
 - **DHCP Servers and Clients** (A/PTR records on Lease Assignment)
 - **Domain Controllers** (A/CNAME/SRV Records on Boot, Re-Registration after 60min)

DDNS Procedure



Transaction Signature (TSIG)

- **Not cached** unique DNS Resource Record
- **Signatures** for dynamic Updates & Responses
- Multiple **Authentication Methods** available
- Implementation of **MD5-based shared Secrets**
- Implemented in BIND, PowerDNS, Knot DNS, NSD, **not in MS DNS**

Generic Security Service TSIG (GSS-TSIG)

- Developed by **Lucent & Microsoft**
- Based on Generic Security Service API (**GSS-API**)
- GSS-API supports **multiple Algorithms**
- **Kerberos v5 is minimum** Requirement

Multi-Primary DNS

- Multiple Primary DNS Servers per Domain
- Unique Name in SOA Record of each Primary
- Secondary/Caching Servers deliver Data based on originating Primary
- Compatible with various Vendors (Microsoft, VitalQIP, DiamondIP, Infoblox, EfficientIP, etc.)

Without DDI

- No targeted **Permission Assignment**
- **Delays in DDNS** Update Propagation
- No **Management of Subnets** and IP Addresses
- No **integrated Management** of DNS and DHCP
- No **Auditing and Reporting**

With DDI

- **Role-based Administration** and Workflows
- **High Availability** for DNS/DHCP Servers
- **Monitoring, Reporting and Alerting**
- **Advanced Troubleshooting and Auditing**
- **DNS Security** Capabilities
- **Visibility** (Docu. = Config.)
- **Automation and Integration**

To the promised Land



Overlay


- **Non-intrusive** and easy Deployment
- Leveraging **existing Skills** and Servers
- **User Interfaces** prevents Configuration Errors
- Elimination of **duplicate Efforts** (Docu. & Config.)
- **Unified Overview** of whole DNS Infrastructure
- Fine-grained **Access Control**
- Compliance through **Logging of all Activities**

Migration


1. Clients use **AD DNS for DNS** resolution
2. **Data Migration** to IPAM System
3. MS DNS Servers set as **Forwarders** at Go-Live
4. Seamless **Transition** with no Downtime
5. **Static Systems** switched post Go-Live
6. Systems now utilize **DDI's further Benefits**

What's next?

The NIST Cybersecurity Framework and DDI 25% (4)



AI Possibilities for DDI 25% (4)

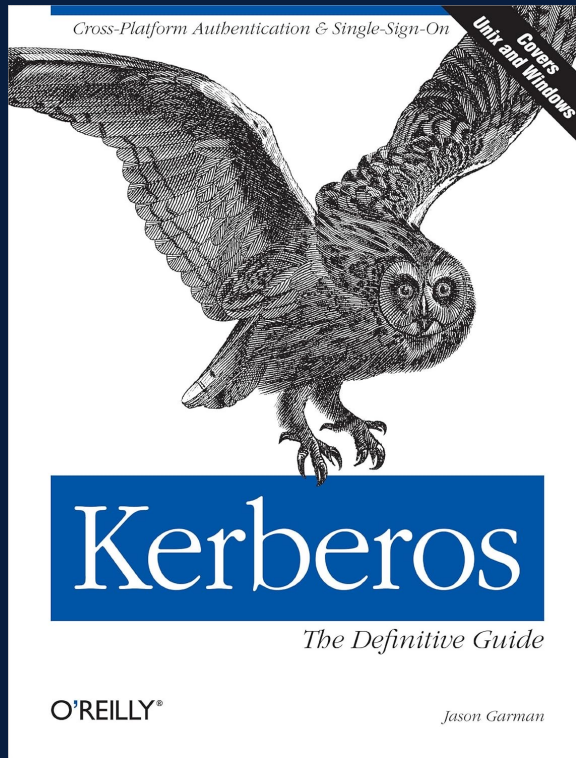


DHCP Security Considerations 50% (8)

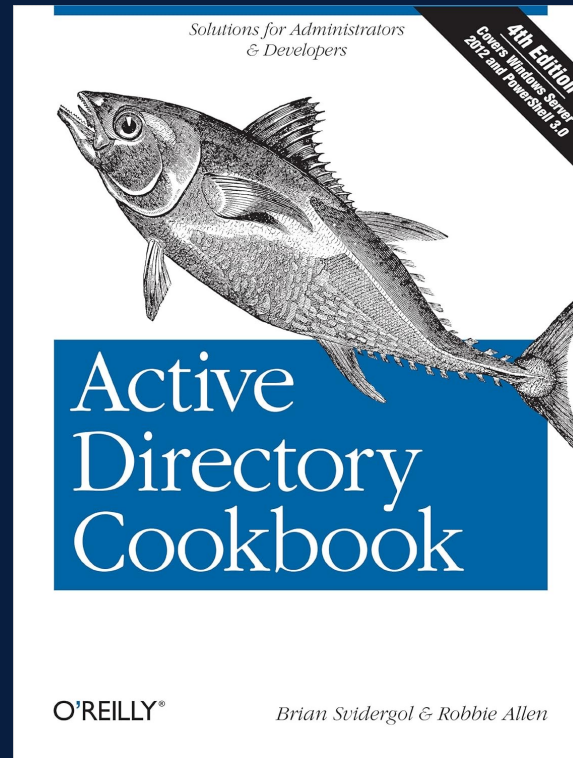


16 responses

Greedy for more?



<https://www.oreilly.com/library/view/kerberos-the-definitive/0596004036/>



<https://www.oreilly.com/library/view/active-directory-cookbook/9781449361419/>



<https://www.oreilly.com/library/view/kerberos-2nd-edition/9781098141059/>

A white sailboat with its sails up is sailing on a vast, deep blue sea under a clear, light blue sky. The horizon is visible in the distance.

Thank you for your Time.



N3K Network Systems
Ferdinand-Braun-Straße 2/1 | 74074 Heilbronn
+49 7131 594 95 0
info@n3k.de