



Active Directory Domain Controller Location Service

Anthony Liguori

aliguor@us.ibm.com

IBM Linux Technology Center



Overview



Overview

◆ History

- Acronyms Galore!
- The 80 node network

◆ MS-CLDAP and Domain Location

- LDAP Explained
- The magic structure

◆ Future

- Fooling clients
- Load Balancing
- Implementing a MS-CLDAP daemon





History

- ◆ **The 80 Node Network**
- ◆ **Systems Network Architecture (SNA)**
- ◆ **NetBIOS**
 - Naming limitations
 - NetBIOS Name Service
- ◆ **SNA vs. OSI**
 - NetBIOS Naming vs. DNS
- ◆ **Mailslots**





NetBIOS Name Server

- ◆ **WINS**
 - Problems
 - Configuration
- ◆ **NetBIOS over different transports**
 - TCP/IP
 - DECnet
 - NetWare
 - SNA
- ◆ **We just couldn't hold on to it forever...**





DNS

- ◆ **Conceived in 1981 by Dr. David Mills**
- ◆ **"My interests [in creating Internet Name Domains] were more focused on the mechanics of doing this and on mail forwarding principles for the Internet," Mills recently said. "Not the least of my concerns were the mechanisms for handing off mail between forwarders and handling errors as they might develop." [1]**
- ◆ ***Hierarchical namespace***
- ◆ **Scales much nicer than NetBIOS naming**
- ◆ **In some ways though less flexible**



Connectionless LDAP

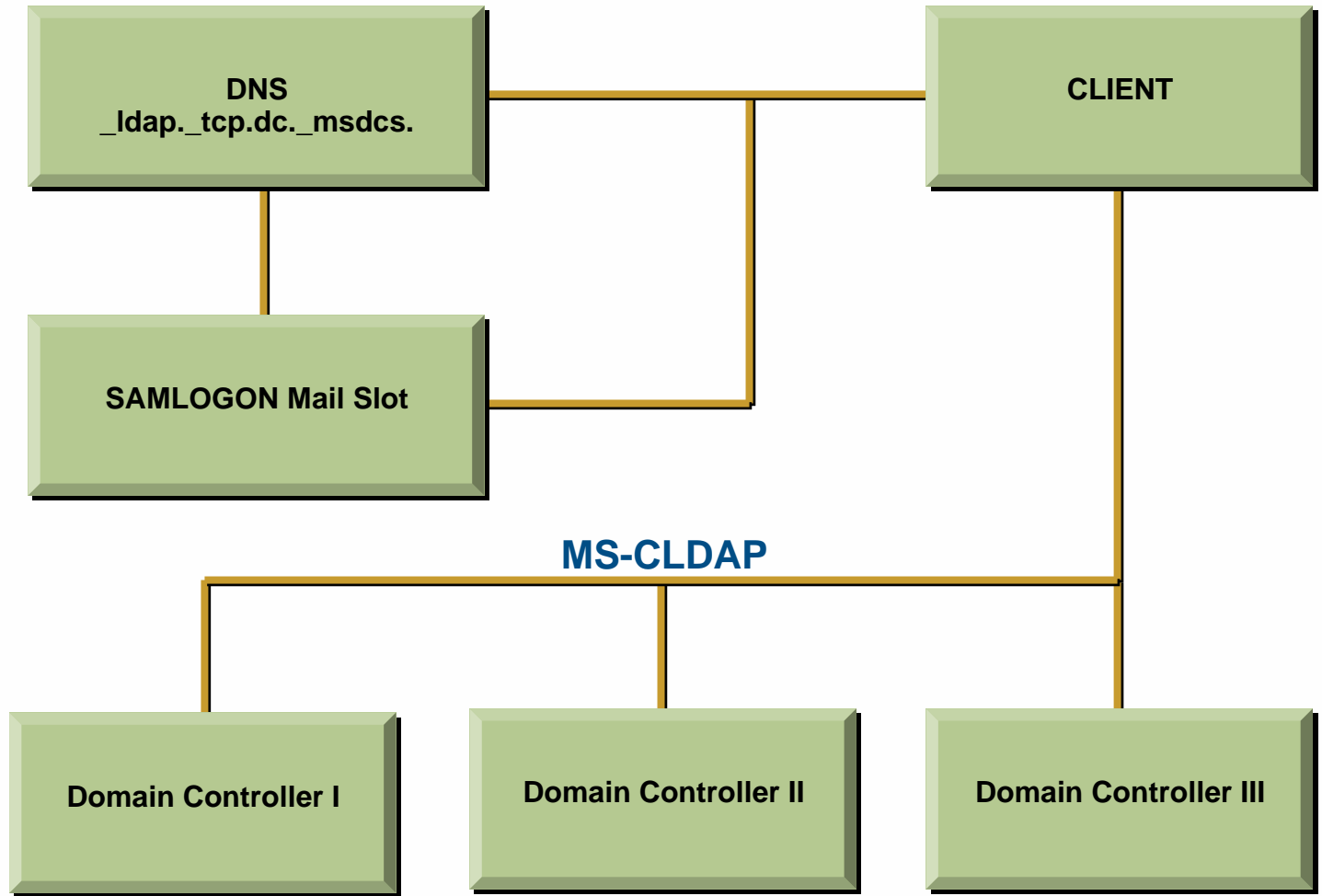
- ◆ **LDAP**
 - Lightweight Directory Access Protocol
 - Excels at frequent reads
 - Not so hot with frequent writes
- ◆ **The mysterious traffic on UDP 389**
- ◆ **RFC-1798**
 - LDAPv2
 - Now historical via RFC-3377 (March 2003)
 - “In particular, it is aimed at avoiding the elapsed time that is associated with connection-oriented communication and it facilitates use of the Directory in a manner analagous to the DNS.” [2]



MS-CLDAP



MS-CLDAP Diagram





Protocol

- ◆ Protocol is LDAPv3 over TCP
- ◆ It is *not* a directory query; more akin to an RPC call (or more appropriately an ADSI call)
- ◆ The attribute requested represents the name of the function
- ◆ The filter represents the arguments being passed
- ◆ Function overloading is supported (it is possible to have the same function take different arguments)



MS-CLDAP Explained

- ◆ One of the most common types of traffic in an AD environment
- ◆ Used to locate domain controller or to find information about a particular domain
- ◆ All queries are anonymous
- ◆ Strongly connected to particular DNS entries
 - SRV `_ldap._tcp.dc._msdcs.DOMAIN`
 - Notice that the SRV record is for tcp *not* udp



Win API—DsGetDcName()

```
DWORD DsGetDcName(  
    LPCTSTR ComputerName,  
    LPCTSTR DomainName,  
    GUID* DomainGuid,  
    LPCTSTR SiteName,  
    ULONG Flags,  
    PDOMAIN_CONTROLLER_INFO*  
    DomainControllerInfo  
);
```



What goes over the wire

Query

DN: (null)

Filter: (&(DnsDomain=IBM.COM)(Host=HOST1)(NtVer=\00\00\00\06))

Attr: Netlogon

Response

Attr: Netlogon

Value: {

<i>uint32</i>	<i>type;</i>
<i>uint32</i>	<i>flags;</i>
<i>GUID</i>	<i>domain_guid;</i>
<i>string</i>	<i>forest, unknown0, domain, hostname, nb_domain, unknown1, nb_hostname, unknown2, user_name, unknown3, site_name, unknown4, client_site_name;</i>
<i>uint32</i>	<i>version;</i>
<i>uint16</i>	<i>lm_token;</i>
<i>uint16</i>	<i>nt_token;</i>

};



Caching

- ◆ **Understanding caching is very important in exploiting the benefits of MS-CLDAP**
- ◆ **Information is cached until either:**
 - **System is rebooted**
 - **Something happens that Windows doesn't like**
 - ◆ **A weaker protocol is used**
 - ◆ **A non-optimal DC is found**
- ◆ **Caching is similar to DNS caching**



Where things get messy

- ◆ **MS-CLDAP ASN.1 is a little off**
 - Length is encoded wrong
- ◆ **Response contains strings compressed with DNS compression**
- ◆ **Example:**

host.domain.com, host1.domain.com

\04host\06domain\03com\00\05host1\c005





Future



Extending Domain Controller Location Service

- ◆ **Using DCLS as a general purpose RPC mechanism**
 - Short messages that are rather simple to parse
 - Using “or” conditions to send extra information
- ◆ **Adding additional queries for non-MS specific domain controller information**
- ◆ **Support for mailslot fallback?**



Example Extension of DCLs: Avoiding Endpoint Mappers

- ◆ **An Active Directory Domain Join**
 - MS-CLDAP
 - SMB session to CreateUser2
 - LDAP w/GSS-SPNEGO to modify SPN
- ◆ **The RPCs to modify a SPN requires an End Point Mapper; Samba doesn't have an End Point Mapper**
- ◆ **Tweaking the Directory Service capability prevents the client from using these RPCs**
- ◆ **Since caching is not-persistent after reboot, DS can be re-enabled for logon**



Load Balancing

- ◆ **Early Samba DC overloading**
- ◆ **MS-CLDAP server does not have to be on the DC**
- ◆ **Can be used to redirect Windows clients to different Windows servers based on User/IP**
- ◆ **More intelligent load balancing than MS offers**





Implementing MS-CLDAP

- ◆ IBM Linux Technology Center developed a prototype MS-CLDAP daemon
- ◆ Not a good idea to add MS-CLDAP support to existing LDAP server
 - Encourages use of non-standard transport
 - May harm future connectionless LDAP standardization adoption
- ◆ LTC's implementation is quite small: < 1k LOC
- ◆ Single place to store network topology information.



References



References

- ◆ [\[1\]http://www.whmag.com/content/0601/dns/](http://www.whmag.com/content/0601/dns/)
- ◆ [\[2\]ftp://ftp.rfc-editor.org/in-notes/rfc3377.txt](ftp://ftp.rfc-editor.org/in-notes/rfc3377.txt)
- ◆ <http://ubiqx.org/cifs/NetBIOS.html>
- ◆ <ftp://ftp.rfc-editor.org/in-notes/rfc1798.txt>
- ◆ <ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt>
- ◆ <http://www.samba.org/>
- ◆ http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/dsbi/dsbi_add_vost.asp



Questions?