LDAP ON ASA

What is ldap?
Directory structure
Acronyms
Transaction flow
Parameters
Additional information
Troubleshooting
Documentation and links

Jatin Katyal
ASA – LDAP training

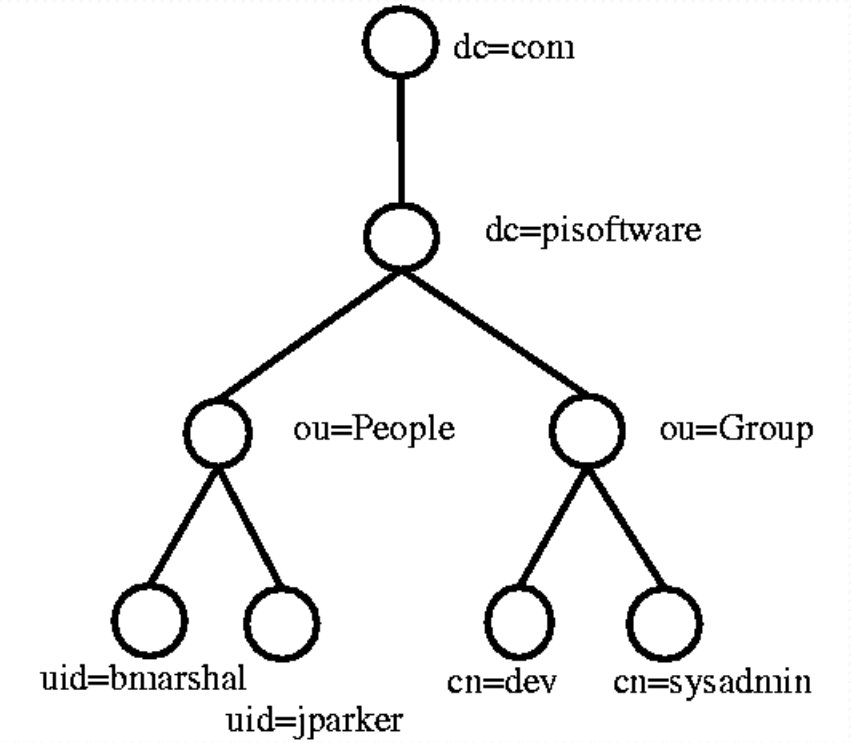
What is LDAP

- Lightweight Directory Access Protocol Based on X.500
- Directory service (RFC1777)
- Stores attribute based data
- Data generally read more than written to.
- Hierarchical data structure Entries are in a tree-like structure called Directory Information Tree (DIT)

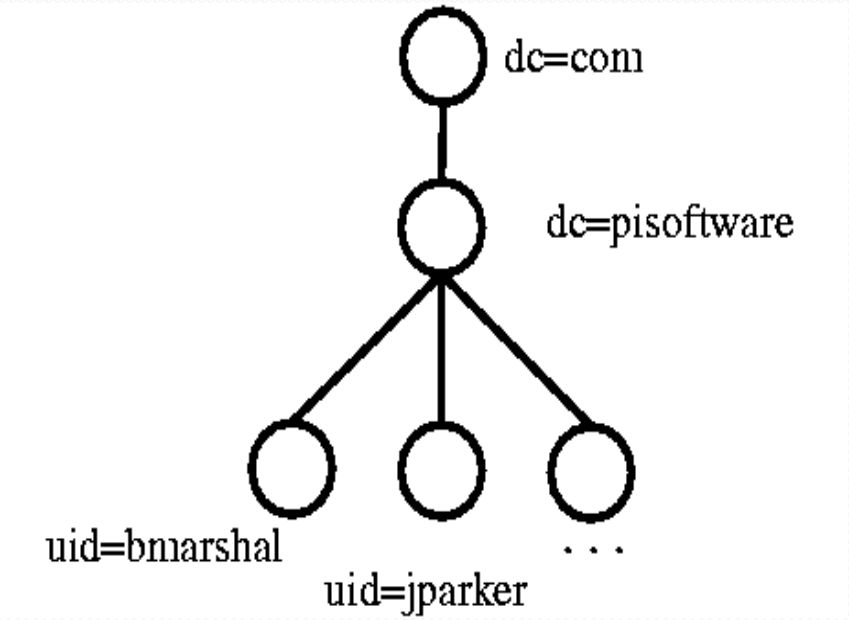
Jatin Katyal
ASA – LDAP training

Directory Structure

Hierarchical



Flat



Acroynms

LDAP: Lightweight Directory Access Protocol

DN: Distinguish Name

RDN: Relative Distinguished Name

DIT: Directory Information Tree

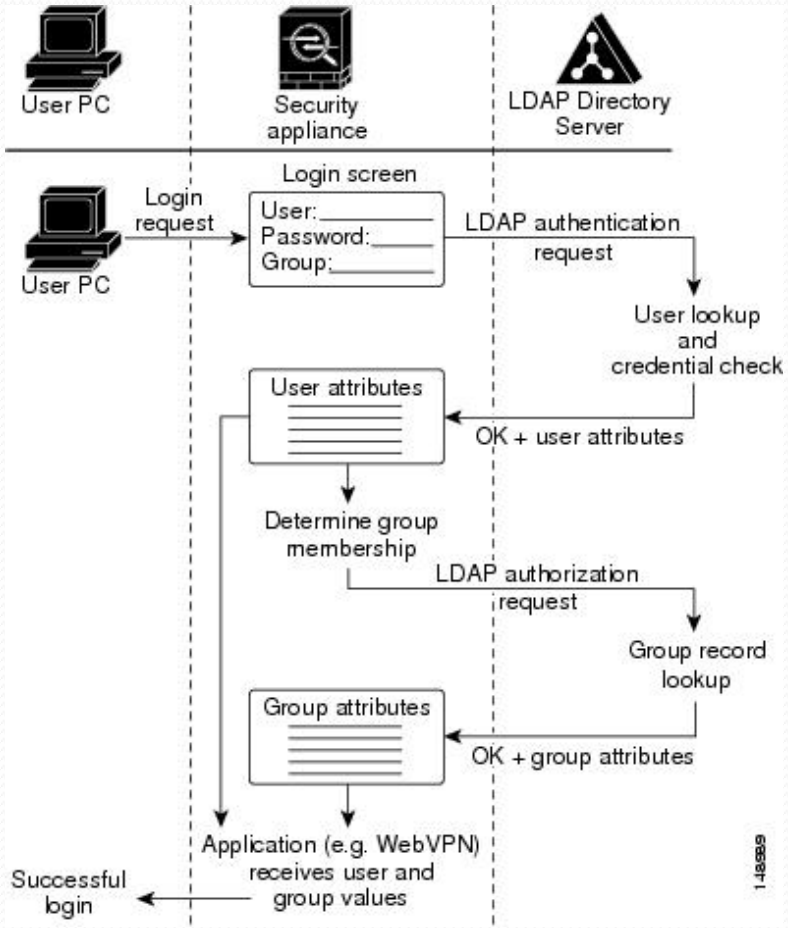
LDIF: LDAP Data Interchange Format

UID: User ID

DC: Domain Component

OU: Organizational Unit

LDAP Authentication and Authorization Transaction Flow



Parameters

ldap-base-dn <string>
To specify the location in the LDAP hierarchy where the server should begin searching when it receives a request. A case-sensitive string of up to 128 characters that specifies the location in the LDAP hierarchy .

ldap-login-dn < user dn>
To specify the name of the directory object that the system should bind.

ldap-login-password <password>
To specify the login password for the LDAP server/DN-account.

ldap-naming-attribute <attr-name>
uniquely identifies an entry on the LDAP server.

ldap-scope {onelevel | subtree}
To specify the extent of the search in the LDAP hierarchy that the server should make when it receives an request.

server-type {autp-detect| microsoft | Novell | openldap |sun}
Specifies the LDAP server vendor as either Microsoft or Sun.

server-port {389 | 636 | 3268 |3269}
Enter the server-port. This is the TCP port number by which you access the server.

ldap-over-ssl enable
To establish a secure SSL connection between the security appliance and the LDAP server

ldap-attribute-map <map-name>
To bind an existing mapping configuration to an LDAP host.

Additional Information:

SASL MD5 Authentication to use the MD5 mechanism of the SimpleAuthentication and Security Layer (SASL) to secure authentication communications between the security appliance and the LDAP server.

SASL Kerberos Authentication to use the Kerberos mechanism of the Simple Authentication and Security Layer to secure authentication communications between the security appliance and the LDAP server.

When performing a Microsoft Active Directory read-only operation (such as for authentication, authorization, or group search), the ASA can bind with a Login DN with fewer privileges. For example, the Login DN can be a user whose AD "Member Of" designation is part of Domain Users. For VPN password management write operations, the Login DN needs elevated privileges and must be part of the Account Operators AD group.

Perform Multi-domain Searches.

The ASA currently does not support the LDAP refreal mechanism for multi-domain saerches. Multi-domain searches are supported with the AD in flobal catalog server mode. In order to perform MD seraches, setup up the AD server for global catalog server mode. The key is to use an ldap-naming-attribute that must be unique across the directory tree.

Server-port 3268
ldap-scope subtree
ldap-naming-attribute userPrinicipalName

The debug ldap 255 command can help you to troubleshoot almost all cases. This command enables LDAP debugging and allows you to watch the process that the ASA uses to connect to the LDAP.

!!—Here it shows a successful authentication.
test# test aaa authen LDAP host 192.168.26.106
Username: jatin
Password: **********
INFO: Attempting Authentication test to IP address <192.168.26.106> (timeout: 12 seconds)

[-2147483639] Session Start
[-2147483639] New request Session, context 0xd8a06354, reqType = Authentication
[-2147483639] Fiber started
[-2147483639] Creating LDAP context with uri=ldap://192.168.26.106:389
[-2147483639] Connect to LDAP server: ldap://192.168.26.106:389, status = Successful.

!---The ASA connects with ASA as an admin to search user Jatin

[-2147483640] Binding as Jatin
[-2147483640] Performing Simple authentication for Jatin to 192.168.26.106
[-2147483640] LDAP Search:
Base DN = [DC=vivek2008,DC=lab]
Filter = [sAMAccountName=jatin]
Scope = [SUBTREE]
[-2147483640] User DN = [CN=Jatin,CN=Users,DC=vivek2008,DC=lab]
[-2147483640] Talking to Active Directory server 192.168.26.106
[-2147483640] Reading password policy for jatin,
dn:CN=Jatin,CN=Users,DC=vivek20
08,DC=lab

Troubleshooting

- Sh run aaa-server
- Sh run ldap
- Test aaa authentication LDAP_SRV_GRP host x.x.x.x username <user> password <pass>
- If you're unsure about the DN string, you can use the dsquery command on Windows AD from the command prompt

C:\Users\Jatin>dsquery user -samid jatin

"CN=Jatin,CN=Users,DC=vivek2008,DC=lab“

- Debug ldap 255

Documentation and Useful Links

Enforcing Microsoft Active Directory Policies Using LDAP Attribute Maps♪
http://tools.cisco.com/squish/D6b8E♪
♪
Use LDAP Authentication to Assign a Group Policy at Login♪
http://tools.cisco.com/squish/A83c9♪
♪
How to enable LDAP over SSL with a third-party certification authority♪
http://tools.cisco.com/squish/e05F♪
♪
Password management with LDAP & RADIUS♪
http://tools.cisco.com/squish/AF63a♪
♪
♪
♪
♪
♪
♪