LDAP Sequence Diagram (Session with Kerberos Tickets and Security)					
LDAP Client			LDAP Server		**EventStudio System Designer 6**
LDAP Application	LDAP Client :3116	LDAP Client :3118	LDAP Server :88	LDAP Server :389	17-Apr-14 16:59 (Page 1)

This sequence diagram describes authenticated LDAP directory lookup. The steps covered are:

(1) TCP connection establishment with the LDAP server

(2) Initial interaction to list the available services.

(3) Authenticate with the Kerberos server and obtain a ticket to proceed with the authentication with the LDAP server.

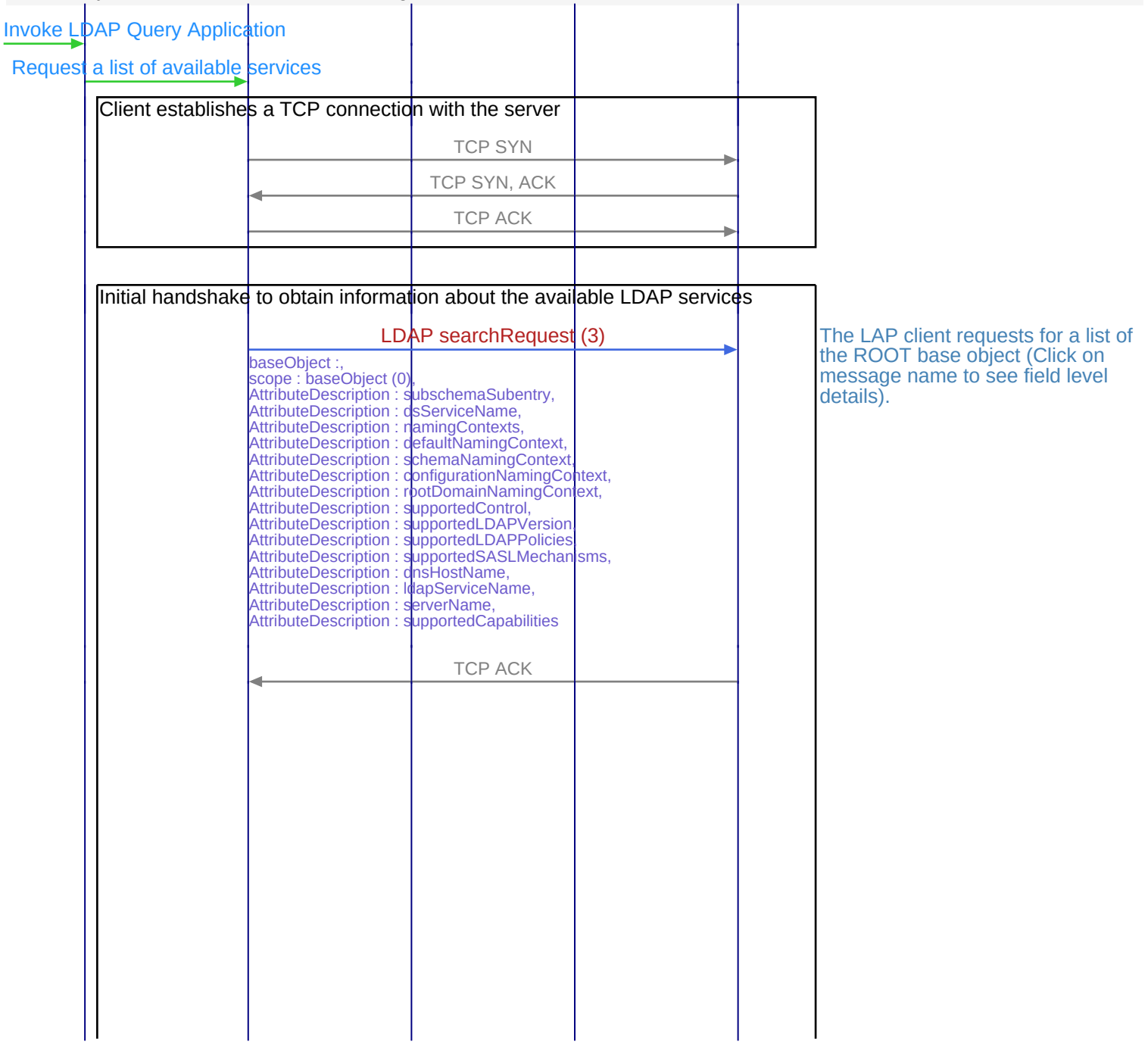
(4) Armed with the Kerberos ticket, the LDAP client uses bind to authenticate and initiate a secure connection.

(5) Encrypted LDAP communication follows

This call flow has been generated with from a Wireshark PCAP file using VisualEther (http://www.eventhelix.com/VisualEther/).

The generated call flow was later modified with EventStudio (http://www.eventhelix.com/EventStudio/) to add comments explaining the feature.

Note that you can click on the LDAP message names to full field level details.



LDAP searchResDone (5)

CN =Aggregate,CN =Schema,CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
CN =NTDS Settings,CN =W2K3 -101,CN =Servers,CN =Standardname -des -ersten -Standorts,CN =Sites,CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
DC =w2k3,DC =vmnet1,DC =vm,DC =base,
CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
CN =Schema,CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
DC =DomainDnsZones,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
DC =ForestDnsZones,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
DC =w2k3,DC =vmnet1,DC =vm,DC =base,
CN =Schema,CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
DC =w2k3,DC =vmnet1,DC =vm,DC =base,
GSSAPI,
GSS -SPNEGO,
EXTERNAL,
DIGEST -MD5,
w2k3 -101.w2k3.vmnet1.vm.base,
w2k3.vmnet1.vm.base :w2k3 -101 $@W2K3.VMNET1.VM.BASE,
CN =W2K3 -101,CN =Servers,CN =Standardname -des -ersten -Standorts,CN =Sites,CN =Configuration,DC =w2k3,DC =vmnet1,DC =vm,DC =base,
resultCode : success (0)

The LDAP server replies back with available binding strings. This initial handshake is used by the LDAP client to display LDAP directories available to the end user. When the end user initiates a query, it will issue a new search request with LDAP searchRequest that includes the binding string for the object being searched.

LDAP Binding Strings

Binding string is a text string that uniquely identifies the LDAP objects. They may be of the form:

"LDAP://cn=John Smith,ou=West Coast,dc=EventHelix,dc=com"

This means access the object with a common name (cn) "John Smith", organization unit (ou) "West Coast" at the domain specified with the domain components (dc) "EventHelix.com".

List of available services

Display available services to user

TCP ACK

Obtain Kerberos Ticket

Obtain Kerberos ticket and authentication information

Kerberos TGS-REQ

Type : PA -TGS -REQ (1),
Tkt -vno : 5,
Realm : SUB1.W2K3.VMNET1.VM.BASE,
Name -type : Service and Instance (2),
Encryption type : rc4 -hmac (23),
Encryption type : rc4 -hmac (23),
KDC _REQ _BODY,
Realm : W2K3.VMNET1.VM.BASE,
Name -type : Service and Instance (2),
Encryption type : rc4 -hmac (23),
Encryption type : des -cbc -md5 (3),
Encryption type : des -cbc -crc (1),
Encryption type : rc4 -hmac -exp (24),
Encryption type : rc4 -hmac -old -exp (-135)

The client asks the Kerberos Ticket Granting Server for a ticket to the LDAP server.

Kerberos TGS-REP

Name -type : Principal (1),
Tkt -vno : 5,
Realm :
W2K3.VMNET1.VM.BASE,
Name -type : Service and
Instance (2),
Encryption type : rc4 -hmac (23),
Encryption type : rc4 -hmac (23)

The Kerberos server grants the ticket.

Kereberos Ticket

Initiate Authentication

Authenticate with LDAP using the Kerberos Authenticator and Ticket

LDAP bindRequest (0)

Kerberos Authenticator,
Kerberos Ticket

The client uses the Kerberos authenticator and ticket to authenticate with the LDAP server.

LDAP bindResponse (1)

resultCode : success (0)

The LDAP server successfully autheticates the user.

Authentication Complete

Display that the LDAP communication is now secure

Secure LDAP communication using the GSS-API

User initiates a directory query

Initiate the query using LDAP

GSS-API Generic Security Service Application Program Interface

SASL Buffer Length : 98,
krb5 _sgn _alg : HMAC (0x0011),
krb5 _seal _alg : RC4 (0x0010),
krb5 _snd _seq : 75b15340fbb34295

Encrypted LDAP search request (Click on message name to see field level details).

TCP ACK

GSS-API Generic Security Service Application Program Interface

SASL Buffer Length : 2525,
krb5 _sgn _alg : HMAC (0x0011),
krb5 _seal _alg : RC4 (0x0010),
krb5 _snd _seq : 1509749e1afd7c6f

Encrypted LDAP search response (Click on message name to see field level details).

Format the received directory query response

Display directory query response

TCP ACK

GSS-API Generic Security Service Application Program Interface

SASL Buffer Length : 143,
krb5 _sgn _alg : HMAC (0x0011),
krb5 _seal _alg : RC4 (0x0010),
krb5 _snd _seq : 539ac890319eae11

Encrypted LDAP message.

GSS-API Generic Security Service Application Program Interface

SASL Buffer Length : 174,
krb5 _sgn _alg : HMAC (0x0011),
krb5 _seal _alg : RC4 (0x0010),
krb5 _snd _seq : 46c59088626b557f

Encrypted LDAP message.

This call flow has been generated with from a Wireshark PCAP file using VisualEther (http://www.eventhelix.com/VisualEther/).

The generated call flow was later modified with EventStudio (http://www.eventhelix.com/EventStudio/) to add comments explaining the feature.

Explore more TCP/IP networking sequence diagrams at: http://www.eventhelix.com/RealtimeMantra/Networking/