Lab 3: Perform LDAP Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after SNMP enumeration is to perform LDAP enumeration to access directory listings within Active Directory or other directory services. Directory services provide hierarchically and logically structured information about the components of a network, from lists of printers to corporate email directories. In this sense, they are similar to a company's org chart.

LDAP enumeration allows you to gather information about usernames, addresses, departmental details, server names, etc.

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

Overview of LDAP Enumeration

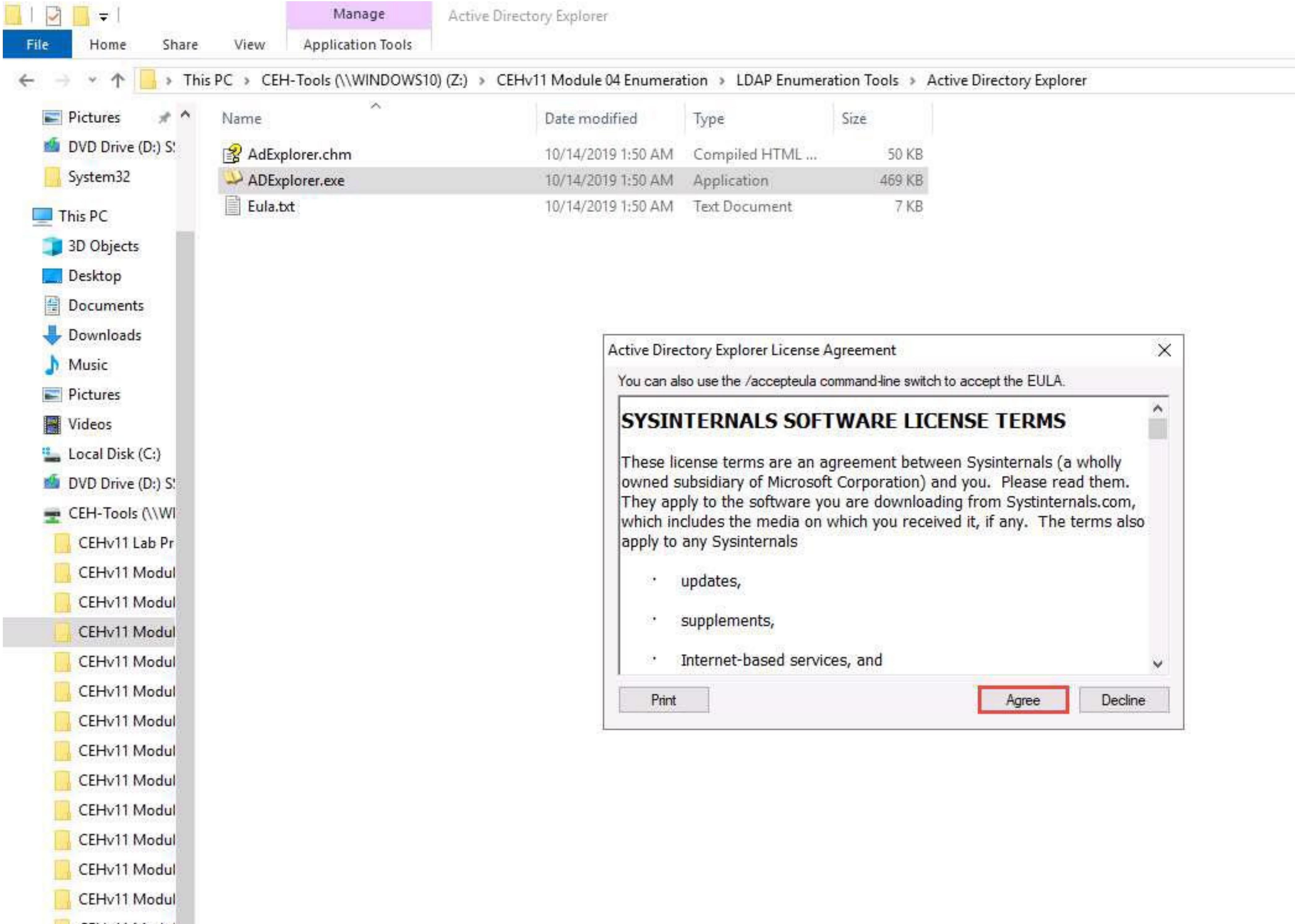
LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.

Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

1. □ In the **Windows Server 2019** machine, navigate to **Z:\CEHv11 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.
2. □ The **Active Directory Explorer License Agreement** window appears; click **Agree**.



Name	Date modified	Type	Size
AdExplorer.chm	10/14/2019 1:50 AM	Compiled HTML ...	50 KB
ADExplorer.exe	10/14/2019 1:50 AM	Application	469 KB
Eula.txt	10/14/2019 1:50 AM	Text Document	7 KB

Active Directory Explorer License Agreement

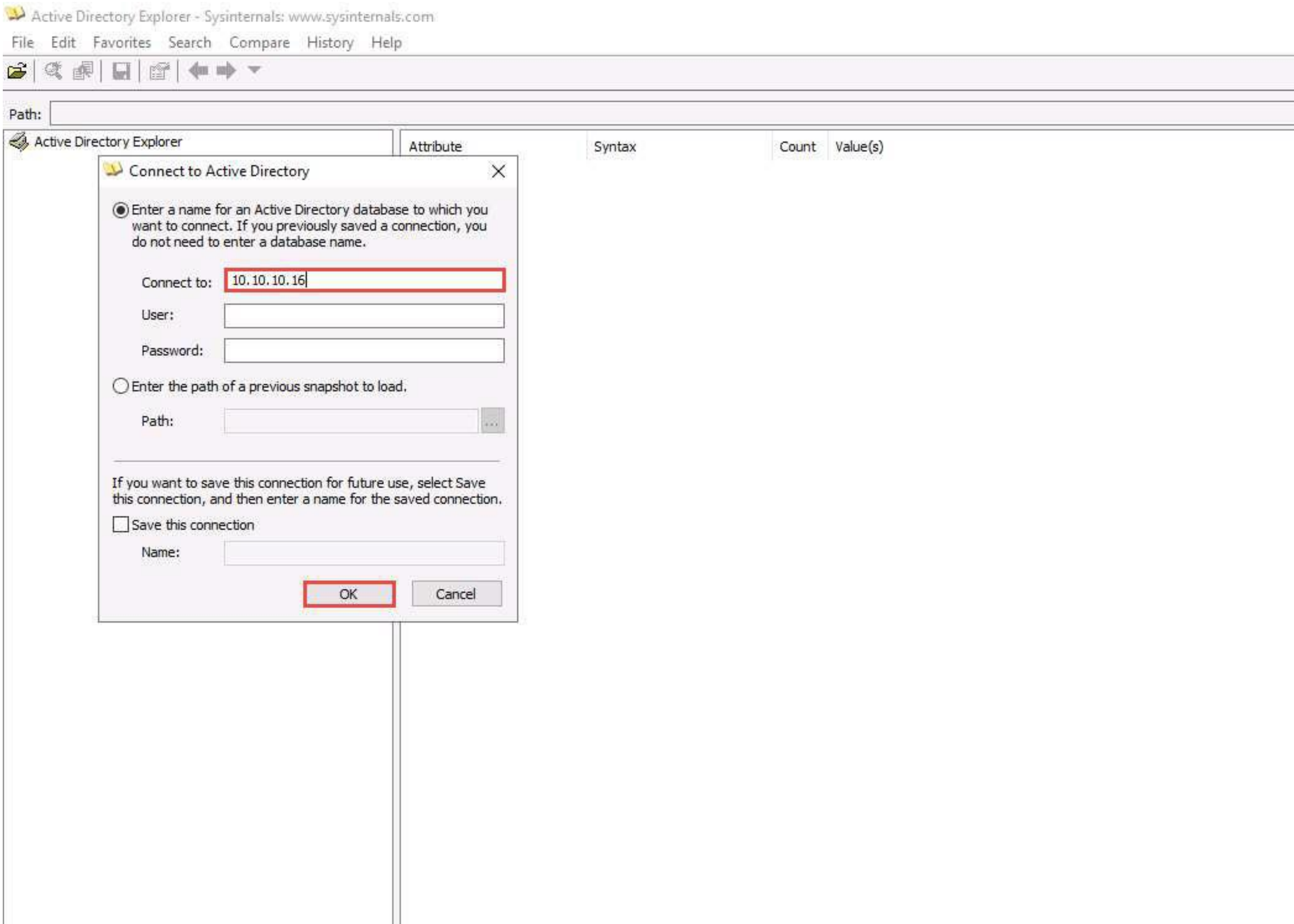
You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

3. □ The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (in this example, we are targeting the **Windows Server 2016** machine: **10.10.10.16**) and click **OK**.


Active Directory Explorer - Sysinternals: www.sysinternals.com
File
Edit
Favorites
Search
Compare
History
Help
Path:
Active Directory Explorer
Attribute
Syntax
Count
Value(s)
Connect to Active Directory
OK
Cancel

● Enter a name for an Active Directory database to which you want to connect. If you previously saved a connection, you do not need to enter a database name.

Connect to: 10.10.10.16

User:

Password:

○ Enter the path of a previous snapshot to load.

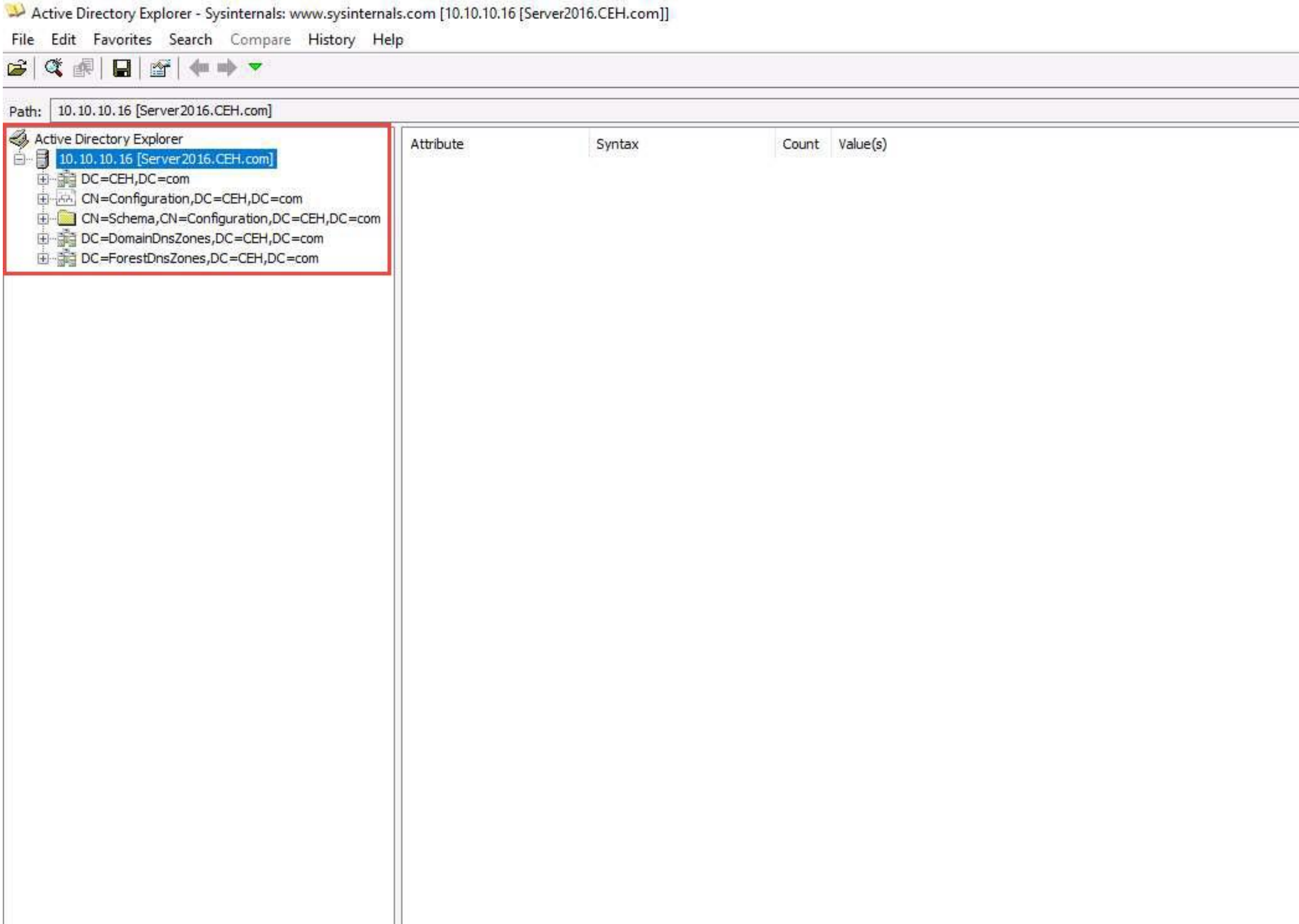
Path:

If you want to save this connection for future use, select Save this connection, and then enter a name for the saved connection.

□ Save this connection

Name:

4. □ The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.



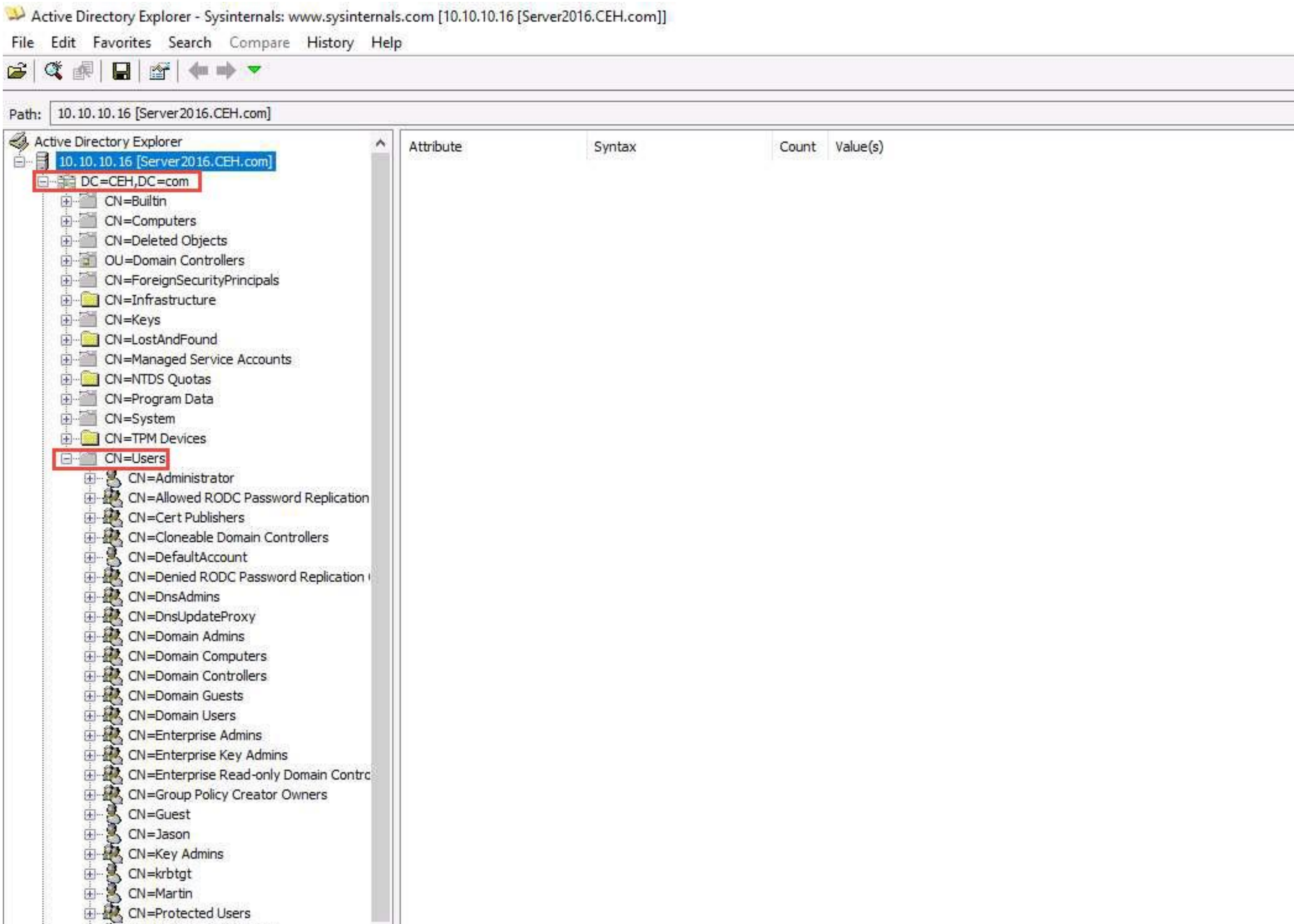
Active Directory Explorer - Sysinternals: www.sysinternals.com [10.10.10.16 [Server2016.CEH.com]]

Path: 10. 10. 10. 16 [Server2016.CEH.com]

```
Active Directory Explorer
  10. 10. 10. 16 [Server2016.CEH.com]
    DC=CEH,DC=com
    CN=Configuration,DC=CEH,DC=com
    CN=Schema,CN=Configuration,DC=CEH,DC=com
    DC=DomainDnsZones,DC=CEH,DC=com
    DC=ForestDnsZones,DC=CEH,DC=com
```

Attribute	Syntax	Count	Value(s)

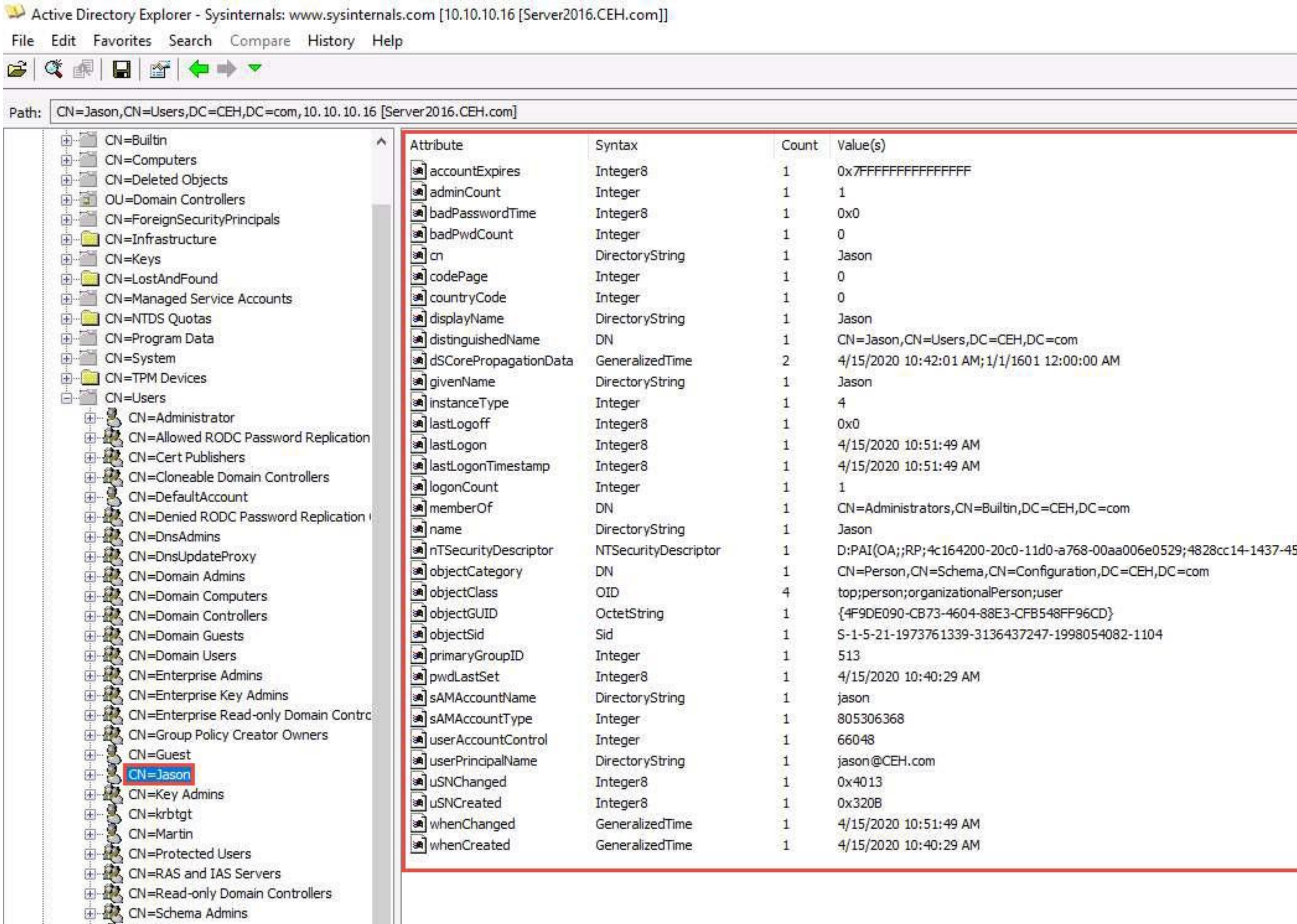
5. □ Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking “**+**” to explore domain user details.


Active Directory Explorer - Sysinternals: www.sysinternals.com [10.10.10.16 [Server2016.CEH.com]]
File
Edit
Favorites
Search
Compare
History
Help
Attribute
Syntax
Count
Value(s)

Path: 10.10.10.16 [Server2016.CEH.com]

```
Active Directory Explorer
  10.10.10.16 [Server2016.CEH.com]
    DC=CEH,DC=com
      CN=Builtin
      CN=Computers
      CN=Deleted Objects
      OU=Domain Controllers
      CN=ForeignSecurityPrincipals
      CN=Infrastructure
      CN=Keys
      CN=LostAndFound
      CN=Managed Service Accounts
      CN=NTDS Quotas
      CN=Program Data
      CN=System
      CN=TPM Devices
      CN=Users
        CN=Administrator
        CN=Allowed RODC Password Replication
        CN=Cert Publishers
        CN=Cloneable Domain Controllers
        CN=DefaultAccount
        CN=Denied RODC Password Replication
        CN=DnsAdmins
        CN=DnsUpdateProxy
        CN=Domain Admins
        CN=Domain Computers
        CN=Domain Controllers
        CN=Domain Guests
        CN=Domain Users
        CN=Enterprise Admins
        CN=Enterprise Key Admins
        CN=Enterprise Read-only Domain Contrc
        CN=Group Policy Creator Owners
        CN=Guest
        CN=Jason
        CN=Key Admins
        CN=krbtgt
        CN=Martin
        CN=Protected Users
```

6. □ Click any **username** (in the left pane) to display its properties in the right pane.



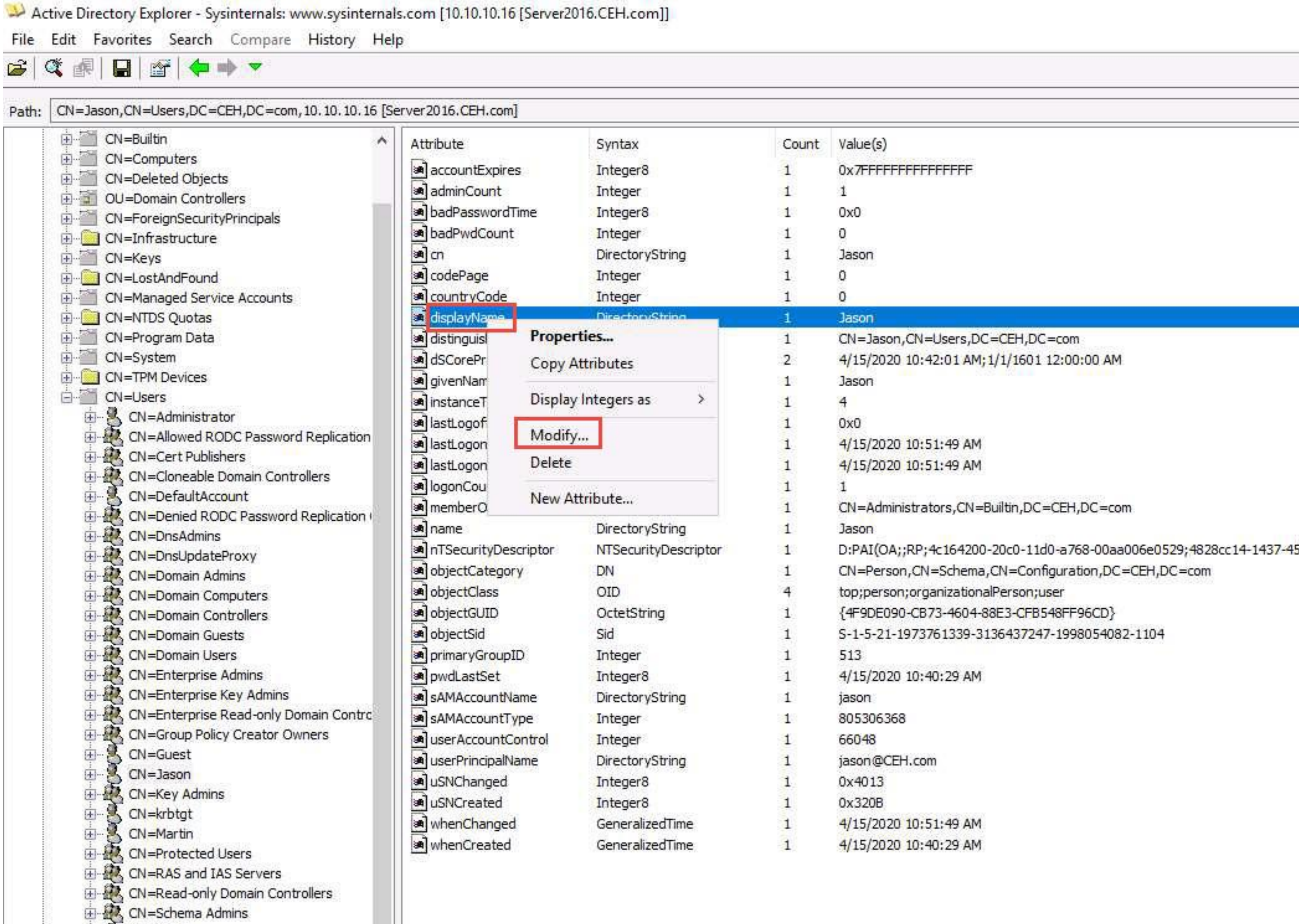
Active Directory Explorer - Sysinternals: www.sysinternals.com [10.10.10.16 [Server2016.CEH.com]]

Path: CN=Jason,CN=Users,DC=CEH,DC=com,10.10.10.16 [Server2016.CEH.com]

- CN=Builtin
- CN=Computers
- CN=Deleted Objects
- OU=Domain Controllers
- CN=ForeignSecurityPrincipals
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accounts
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
  - CN=Administrator
  - CN=Allowed RODC Password Replication
  - CN=Cert Publishers
  - CN=Cloneable Domain Controllers
  - CN=DefaultAccount
  - CN=Denied RODC Password Replication (
  - CN=DnsAdmins
  - CN=DnsUpdateProxy
  - CN=Domain Admins
  - CN=Domain Computers
  - CN=Domain Controllers
  - CN=Domain Guests
  - CN=Domain Users
  - CN=Enterprise Admins
  - CN=Enterprise Key Admins
  - CN=Enterprise Read-only Domain Contrc
  - CN=Group Policy Creator Owners
  - CN=Guest
  - CN=Jason
  - CN=Key Admins
  - CN=krbtgt
  - CN=Martin
  - CN=Protected Users
  - CN=RAS and IAS Servers
  - CN=Read-only Domain Controllers
  - CN=Schema Admins

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Jason
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	DirectoryString	1	Jason
distinguishedName	DN	1	CN=Jason,CN=Users,DC=CEH,DC=com
dSCorePropagationData	GeneralizedTime	2	4/15/2020 10:42:01 AM;1/1/1601 12:00:00 AM
givenName	DirectoryString	1	Jason
instanceType	Integer	1	4
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	4/15/2020 10:51:49 AM
lastLogonTimestamp	Integer8	1	4/15/2020 10:51:49 AM
logonCount	Integer	1	1
memberOf	DN	1	CN=Administrators,CN=Builtin,DC=CEH,DC=com
name	DirectoryString	1	Jason
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=CEH,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{4F9DE090-CB73-4604-88E3-CFB548FF96CD}
objectSid	Sid	1	S-1-5-21-1973761339-3136437247-1998054082-1104
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	4/15/2020 10:40:29 AM
sAMAccountName	DirectoryString	1	jason
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	66048
userPrincipalName	DirectoryString	1	jason@CEH.com
uSNChanged	Integer8	1	0x4013
uSNCreated	Integer8	1	0x320B
whenChanged	GeneralizedTime	1	4/15/2020 10:51:49 AM
whenCreated	GeneralizedTime	1	4/15/2020 10:40:29 AM

7. □ Right-click any attribute in the right pane (in this case, **displayName**) and click **Modify…** from the context menu to modify the user’s profile.

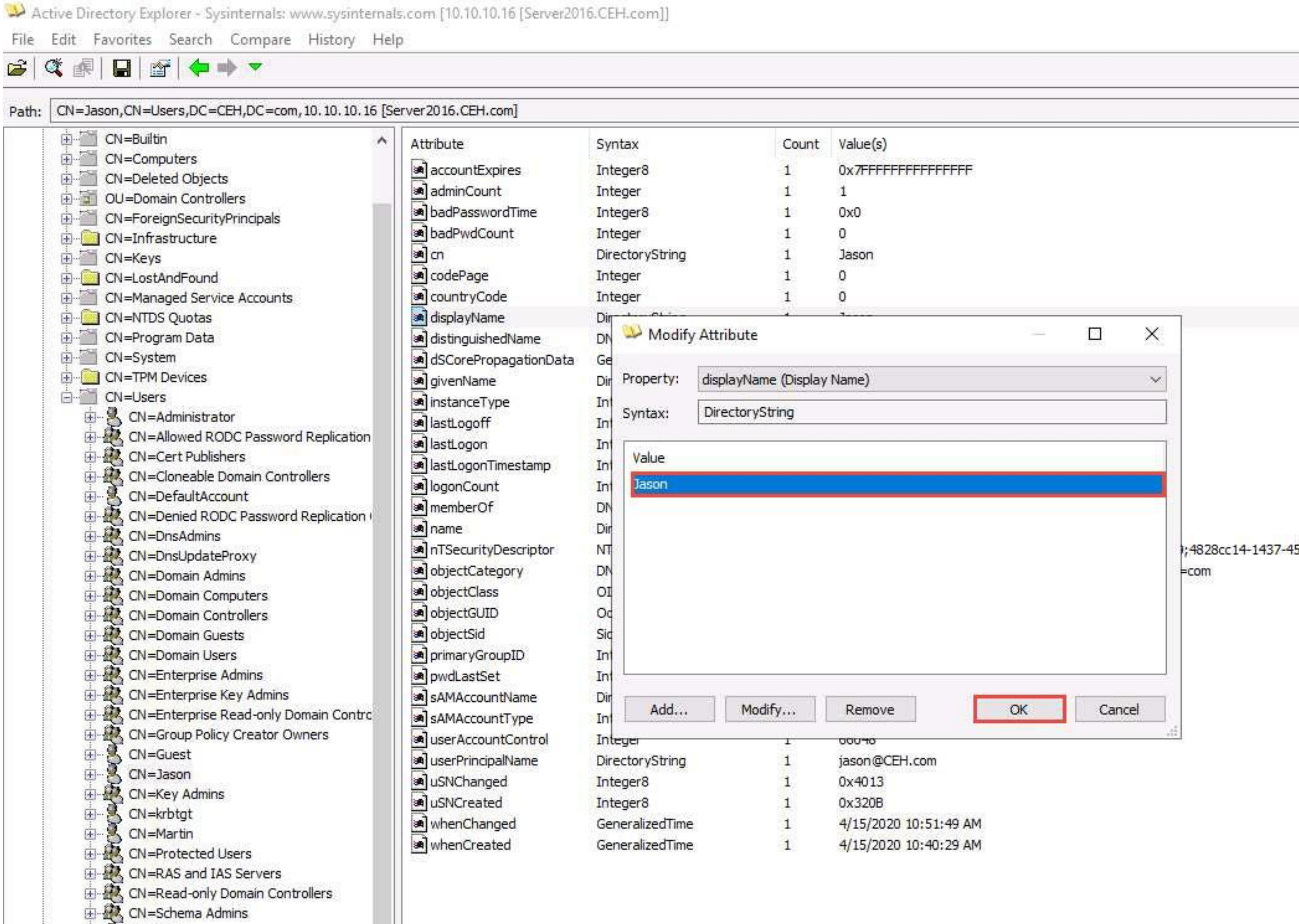


Path: CN=Jason,CN=Users,DC=CEH,DC=com,10.10.10.16 [Server2016.CEH.com]

- CN=Builtin
- CN=Computers
- CN=Deleted Objects
- OU=Domain Controllers
- CN=ForeignSecurityPrincipals
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accounts
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
  - CN=Administrator
  - CN=Allowed RODC Password Replication
  - CN=Cert Publishers
  - CN=Cloneable Domain Controllers
  - CN=DefaultAccount
  - CN=Denied RODC Password Replication
  - CN=DnsAdmins
  - CN=DnsUpdateProxy
  - CN=Domain Admins
  - CN=Domain Computers
  - CN=Domain Controllers
  - CN=Domain Guests
  - CN=Domain Users
  - CN=Enterprise Admins
  - CN=Enterprise Key Admins
  - CN=Enterprise Read-only Domain Contro
  - CN=Group Policy Creator Owners
  - CN=Guest
  - CN=Jason
  - CN=Key Admins
  - CN=krbtgt
  - CN=Martin
  - CN=Protected Users
  - CN=RAS and IAS Servers
  - CN=Read-only Domain Controllers
  - CN=Schema Admins

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Jason
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	DirectoryString	1	Jason
distinguis		1	CN=Jason,CN=Users,DC=CEH,DC=com
dSCorePr		2	4/15/2020 10:42:01 AM;1/1/1601 12:00:00 AM
givenNam		1	Jason
instanceT		1	4
lastLogof		1	0x0
lastLogon		1	4/15/2020 10:51:49 AM
lastLogon		1	4/15/2020 10:51:49 AM
logonCou		1	1
memberO		1	CN=Administrators,CN=Builtin,DC=CEH,DC=com
name	DirectoryString	1	Jason
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=CEH,DC=com
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{4F9DE090-CB73-4604-88E3-CFB548FF96CD}
objectSid	Sid	1	S-1-5-21-1973761339-3136437247-1998054082-1104
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	4/15/2020 10:40:29 AM
sAMAccountName	DirectoryString	1	jason
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	66048
userPrincipalName	DirectoryString	1	jason@CEH.com
uSNChanged	Integer8	1	0x4013
uSNCreated	Integer8	1	0x320B
whenChanged	GeneralizedTime	1	4/15/2020 10:51:49 AM
whenCreated	GeneralizedTime	1	4/15/2020 10:40:29 AM

8. The **Modify Attribute** window appears. First, select the username under the **Value** section, and then click the **Modify...** button. The **Edit Value** pop-up appears. Rename the username in the **Value data** field and click **OK** to save the changes.



Active Directory Explorer - Sysinternals: www.sysinternals.com [10.10.10.16 [Server2016.CEH.com]]

Path: CN=Jason,CN=Users,DC=CEH,DC=com,10.10.10.16 [Server2016.CEH.com]

- CN=Builtin
- CN=Computers
- CN=Deleted Objects
- OU=Domain Controllers
- CN=ForeignSecurityPrincipals
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accounts
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
  - CN=Administrator
  - CN=Allowed RODC Password Replication
  - CN=Cert Publishers
  - CN=Cloneable Domain Controllers
  - CN=DefaultAccount
  - CN=Denied RODC Password Replication
  - CN=DnsAdmins
  - CN=DnsUpdateProxy
  - CN=Domain Admins
  - CN=Domain Computers
  - CN=Domain Controllers
  - CN=Domain Guests
  - CN=Domain Users
  - CN=Enterprise Admins
  - CN=Enterprise Key Admins
  - CN=Enterprise Read-only Domain Contro
  - CN=Group Policy Creator Owners
  - CN=Guest
  - CN=Jason
  - CN=Key Admins
  - CN=krbtgt
  - CN=Martin
  - CN=Protected Users
  - CN=RAS and IAS Servers
  - CN=Read-only Domain Controllers
  - CN=Schema Admins

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Jason
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	Di		
distinguishedName	DN		
dSCorePropagationData	Ge		
givenName	Dir		
instanceType	Int		
lastLogoff	Int		
lastLogon	Int		
lastLogonTimestamp	Int		
logonCount	Int		
memberOf	DN		
name	Dir		
nTSecurityDescriptor	NT		;4828cc14-1437-45
objectCategory	DN		=com
objectClass	OI		
objectGUID	Oc		
objectSid	Sid		
primaryGroupID	Int		
pwdLastSet	Int		
sAMAccountName	Dir		
sAMAccountType	Int		
userAccountControl	Integer	1	66048
userPrincipalName	DirectoryString	1	jason@CEH.com
uSNChanged	Integer8	1	0x4013
uSNCreated	Integer8	1	0x320B
whenChanged	GeneralizedTime	1	4/15/2020 10:51:49 AM
whenCreated	GeneralizedTime	1	4/15/2020 10:40:29 AM

Modify Attribute

Property: displayName (Display Name)

Syntax: DirectoryString

Value

Jason

9. □ You can read and modify other user profile attributes in the same way.
10. □ This concludes the demonstration of performing LDAP enumeration using AD Explorer.
11. □ You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (https://www.ldapadministrator.com), **LDAP Admin Tool** (https://www.ldapsoft.com), **LDAP Account Manager** (https://www.ldap-account-manager.org), **LDAP Search** (https://securityxploded.com), and **JXplorer** (http://www.jxplorer.org) to perform LDAP enumeration on the target.
12. □ Close all open windows and document all the acquired information.