

David Thomsen
SYS-265

```
mgmt01-SYS265-01-david.thomsen

Recycle Bin

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\david-thomsen-adm> Get-ADComputer -Filter *

DistinguishedName : CN=AD01-DAVID,OU=Domain Controllers,DC=david,DC=local
DNSHostName       : ad01-david.david.local
Enabled           : True
Name              : AD01-DAVID
ObjectClass       : computer
ObjectGUID        : d5f7ba12-0a02-49fa-995e-901ac828ffe7
SamAccountName    : AD01-DAVID$
SID               : S-1-5-21-3364371340-3348759129-4140418422-1000
UserPrincipalName :

DistinguishedName : CN=MGMT01-DAVID,CN=Computers,DC=david,DC=local
DNSHostName       : mgmt01-david.david.local
Enabled           : True
Name              : MGMT01-DAVID
ObjectClass       : computer
ObjectGUID        : 857488d0-b469-40f2-9763-44c1f6b8f60b
SamAccountName    : MGMT01-DAVID$
SID               : S-1-5-21-3364371340-3348759129-4140418422-1103
UserPrincipalName :

DistinguishedName : CN=WKS01-DAVID,CN=Computers,DC=david,DC=local
DNSHostName       : wks01-david.david.local
Enabled           : True
Name              : WKS01-DAVID
ObjectClass       : computer
ObjectGUID        : b6e8a316-8884-4c22-a652-ce392ad9ddd0
SamAccountName    : WKS01-DAVID$
SID               : S-1-5-21-3364371340-3348759129-4140418422-1104
UserPrincipalName :

PS C:\Users\david-thomsen-adm>

PS C:\Users\david-thomsen-adm> Get-ADUser -filter 'Name -like "david*"' -Properties MemberOf

DistinguishedName : CN=david thomsen,CN=Users,DC=david,DC=local
Enabled           : True
GivenName         : david
MemberOf          : {}
Name              : david thomsen
ObjectClass       : user
ObjectGUID        : c6294390-08a8-4c28-b629-e8967984f19b
SamAccountName    : david-thomsen
SID               : S-1-5-21-3364371340-3348759129-4140418422-1105
Surname           : thomsen
UserPrincipalName : david-thomsen@david.local

DistinguishedName : CN=david thomsen adm,CN=Users,DC=david,DC=local
Enabled           : True
GivenName         : david
MemberOf          : {CN=Domain Admins,CN=Users,DC=david,DC=local}
Name              : david thomsen adm
ObjectClass       : user
ObjectGUID        : 0fb11f58-be13-42d4-bee9-15305789763c
SamAccountName    : david-thomsen-adm
SID               : S-1-5-21-3364371340-3348759129-4140418422-1106
Surname           : thomsen
UserPrincipalName : david-thomsen-adm@david.local
```

```
PS C:\Users\david-thomsen-adm> Get-DnsClientServerAddress
```

InterfaceAlias	Interface Index	Address Family	ServerAddresses
Ethernet0	5	IPv4	{10.0.5.5}
Ethernet0	5	IPv6	{}
Loopback Pseudo-Interface 1	1	IPv4	{}
Loopback Pseudo-Interface 1	1	IPv6	{fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}

```
PS C:\Users\david-thomsen-adm> Get-DnsServerResourceRecord -ZoneName david.local -ComputerName ad01-david -RRType A
```

HostName	RecordType	Type	Timestamp	TimeToLive	RecordData
@	A	1	1/23/2022 12:00:0...	00:10:00	10.0.5.5
ad01-david	A	1	0	01:00:00	10.0.5.5
DomainDnsZones	A	1	1/23/2022 1:00:00 PM	00:10:00	10.0.5.5
ForestDnsZones	A	1	1/23/2022 1:00:00 PM	00:10:00	10.0.5.5
fw01-david	A	1	0	01:00:00	10.0.5.2
mgmt01-david	A	1	0	01:00:00	10.0.5.10
wks01-david	A	1	1/23/2022 1:00:00 PM	00:20:00	10.0.5.100

```
PS C:\Users\david-thomsen-adm> Test-NetConnection champlain.edu -TraceRoute -Hops 3
```

```
WARNING: Trace route to destination 208.115.107.132 did not complete. Trace terminated :: 192.168.4.251
```

```
ComputerName      : champlain.edu
RemoteAddress     : 208.115.107.132
InterfaceAlias    : Ethernet0
SourceAddress     : 10.0.5.10
PingSucceeded     : True
PingReplyDetails (RTT) : 79 ms
TraceRoute        : 10.0.5.2
                  : 10.0.17.2
                  : 192.168.4.251
```

```
PS C:\Users\david-thomsen-adm> tracert -h 3 champlain.edu
```

```
Tracing route to champlain.edu [208.115.107.132]
over a maximum of 3 hops:
```

1	<1 ms	<1 ms	<1 ms	fw01-david.david.local [10.0.5.2]
2	<1 ms	<1 ms	<1 ms	10.0.17.2
3	1 ms	1 ms	1 ms	192.168.4.251

```
Trace complete.
```

```
PS C:\Users\david-thomsen-adm>
```

```
PS C:\Users\david-thomsen-adm> Get-DnsServerResourceRecord -ZoneName david.local -ComputerName ad01-david -RRType PTR
```

The screenshot shows the DNS Manager console. The left pane displays the hierarchy: DNS > ad01-david.david.local > Forward Lookup Zones > david.local. The right pane shows a list of records for the david.local zone.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[7], ad01-david.david.local...	static
(same as parent folder)	Name Server (NS)	ad01-david.david.local.	static
10.0.5.10	Pointer (PTR)	mgmt01-david.david.local.	static
10.0.5.100	Pointer (PTR)	wks01-david.david.local.	static
10.0.5.2	Pointer (PTR)	fw01-david.david.local.	static

I was unable to get the command to show the PTR Records however, they are all shown in the Server Manager. Most likely the command is wrong but I was unable to find one that worked.

Git: <https://github.com/dthomsen116/SYS-265/wiki/TJ1:-Lab00>