Windows Admin Basics

Ankur Chowdhary

Agenda

Local vs Domain Accounts

Installing Win 2016 Server

Server Manager

End-to-end domain example

Basic Powershell, Processes, Services, etc.

Local vs Domain Accounts

- Workgroup-collection of computers connected using one network. No domain controller in a workgroup, authentication performed at each computer.
- A networked Windows system can have two configurations – either domain joined or workgroup. In a domain joined computer, users can access accounts using centrally managed Active Directory.
- Users can also login using local account, but local accounts will not have access to domain resources - networked printers, Web servers, e-mail servers.
- In a workgroup – local accounts managed by SAM are used.
- Security policies can be centrally managed using AD.

Server Manager

Add and Remove features

Create DC

What is Windows domain and DC?

Adding AD-DS role

-USer accounts, computers, printers, file shares, groups

AS-security authentication

Adding a Workstation or VM to domain.

Create AD

AD-> OUs-> Groups

Change Computer Name on Server -> Select Domain options

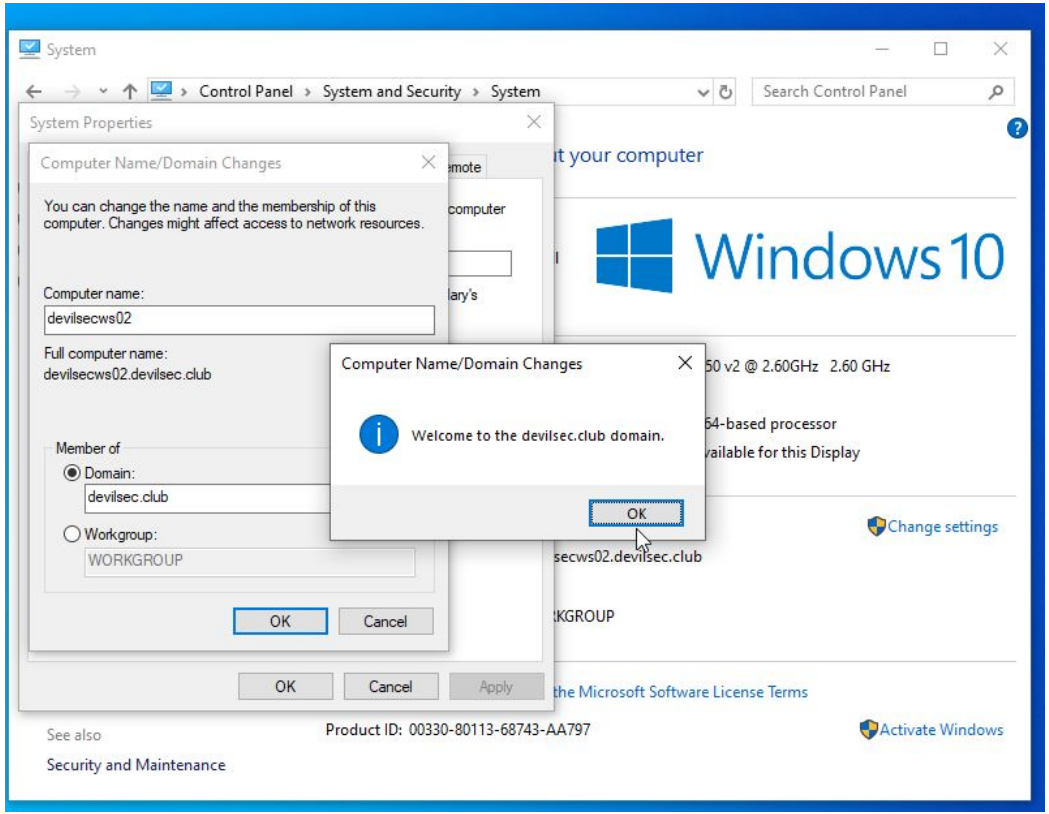
Add roles and features-> AD DS

AD USers and Computers

Netbios - DevilSec

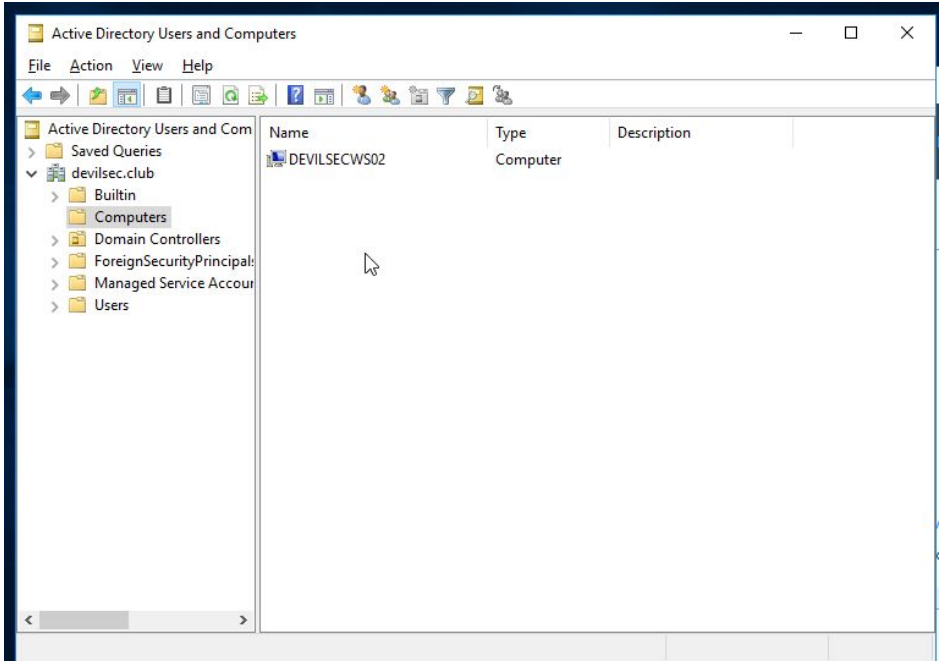
Rt-click change AD, etc

Connect Win 10 to Domain Controller



Domain Controller

Tools-AD Users and Computers, under computers



DHCP

- Static IP address vs DHCP (a network protocol, a server role).
- Ensure correct TCP/IP setting.
- DHCP allows client computers to obtain IP automatically.
- DHCP as a windows server role - allows client to obtain all TCP/IP configurations. automatically, using DHCP lease for a certain amount of time.
- On expiration lease-extension or new IP. IP exclusion, range provided by DHCP server.
- DHCP request broadcast, DHCP offer, DHCP req., ACK. (DORA) Discover, Offer, Request, Ack.
- Why use static IPs-DNS, printers, DHCP server as single point of failure, etc.

DHCP Server Role

Manage-add roles and features-next.

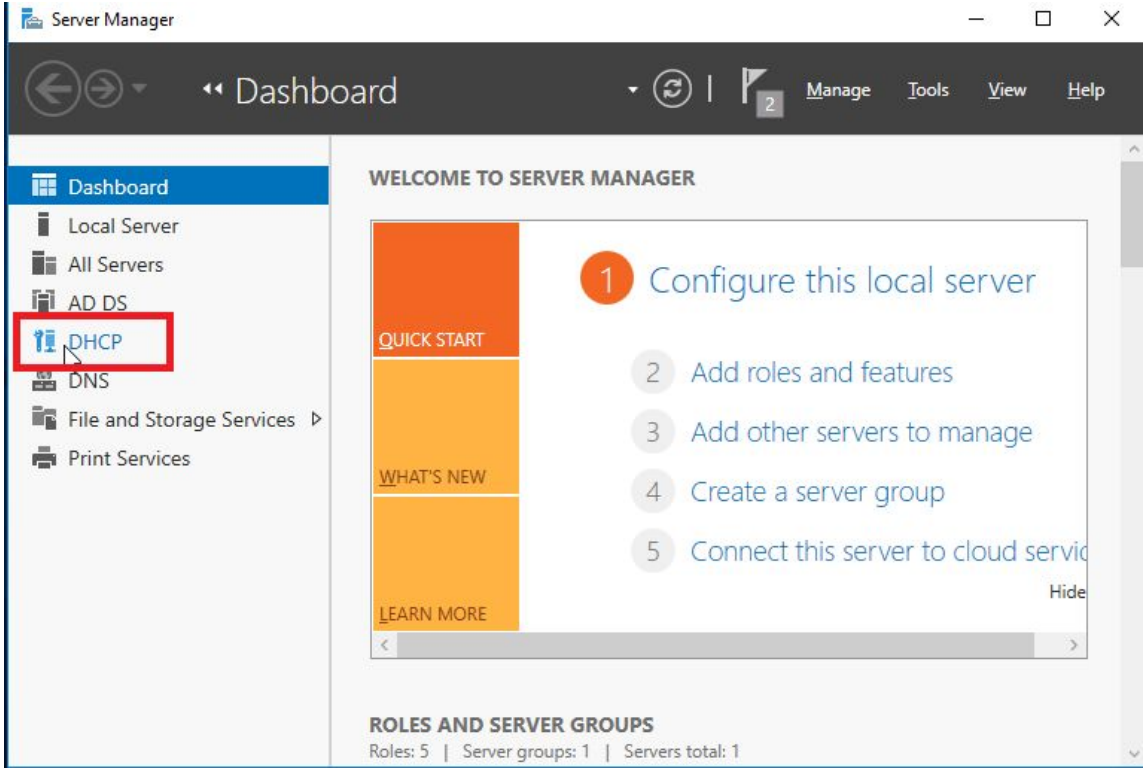
Post-install configuration - DHCP admin, users security groups need to be created, server needs to be authorized.

DevilSec\Administrator

Authorization Screen -> commit

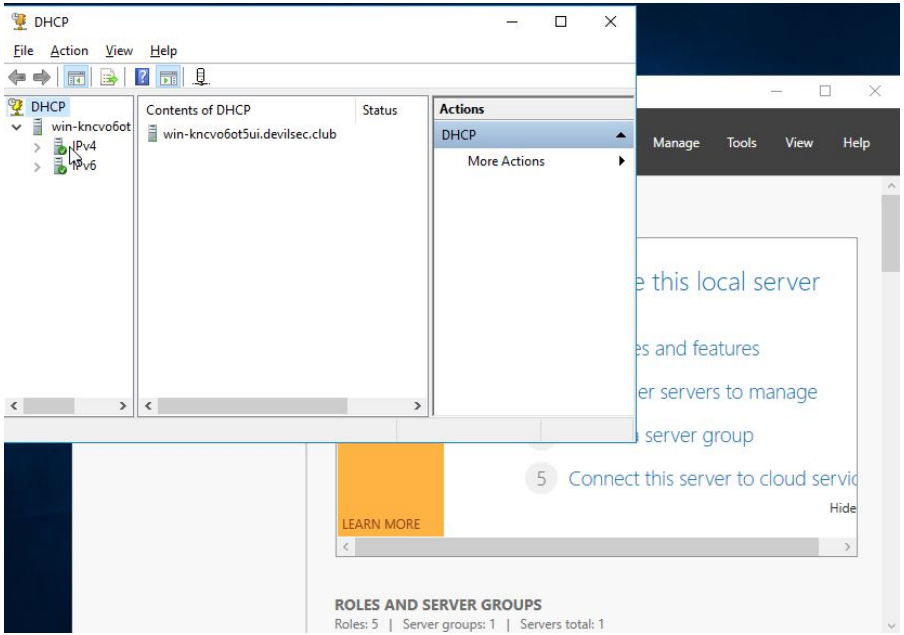
Summary screen shows completed tasks

DHCP Server Role



DHCP Management Console

Tools-> DHCP, server listed with IPv4, IPv6.



DHCP Scope

Pool of IPs on a specific subnet that can be leased by server.

Tools-DHCP-IPv4-new scope

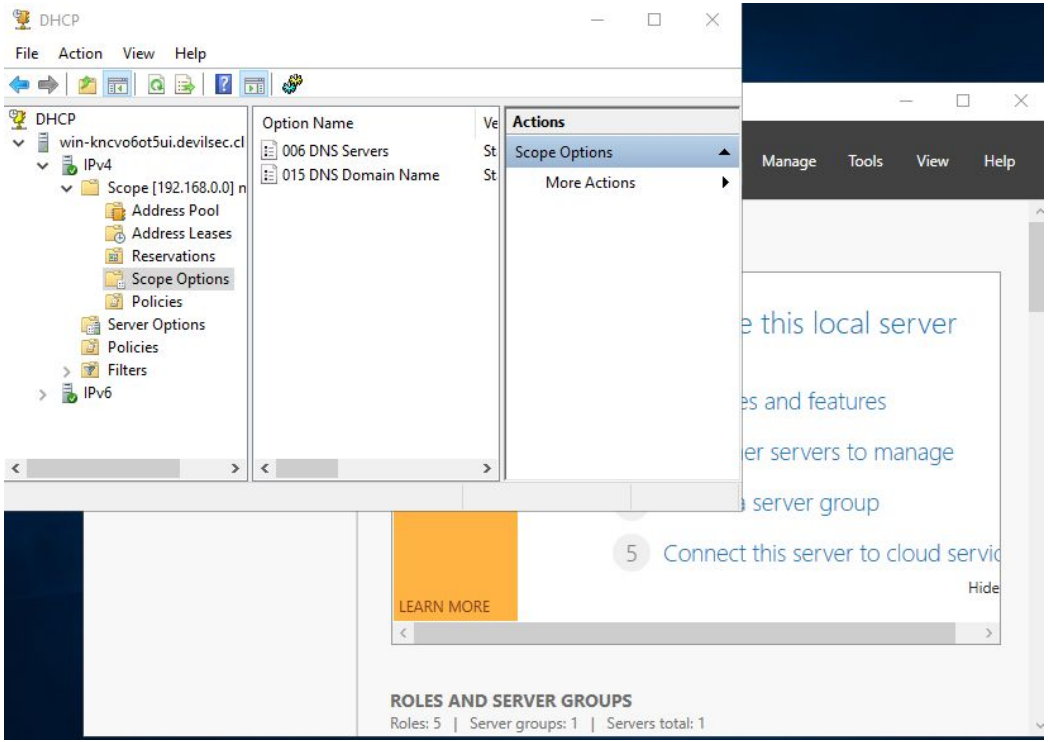
Rt. click on IPv4

Specify scope name and desc.

Add start and end IPs, info. About exclusion, lease settings, default gw, DNS, etc.

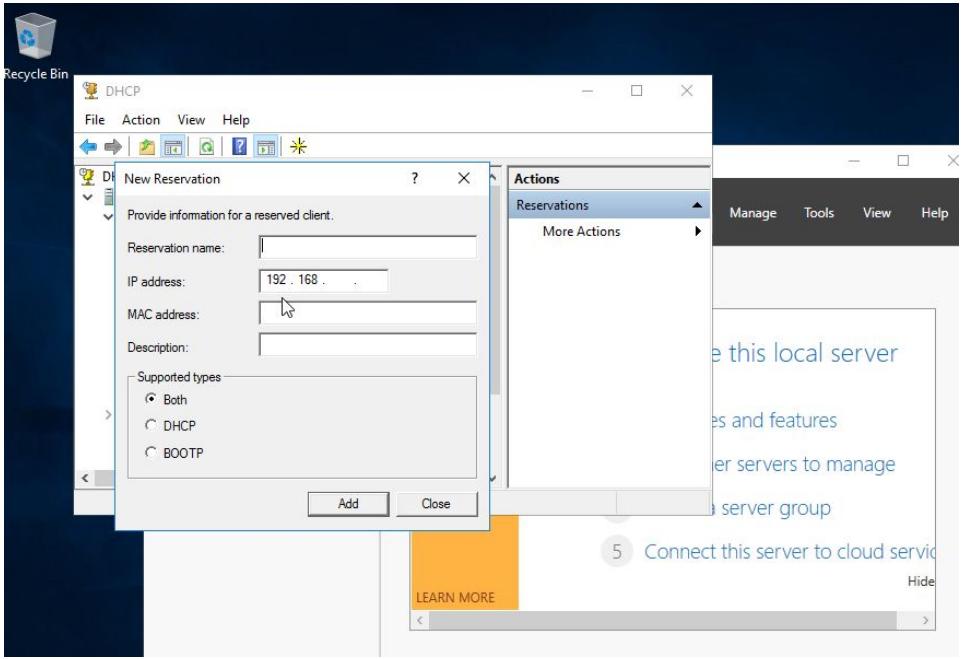
WINS server-similar to DNS server. Activate scope or later.

DHCP Scope

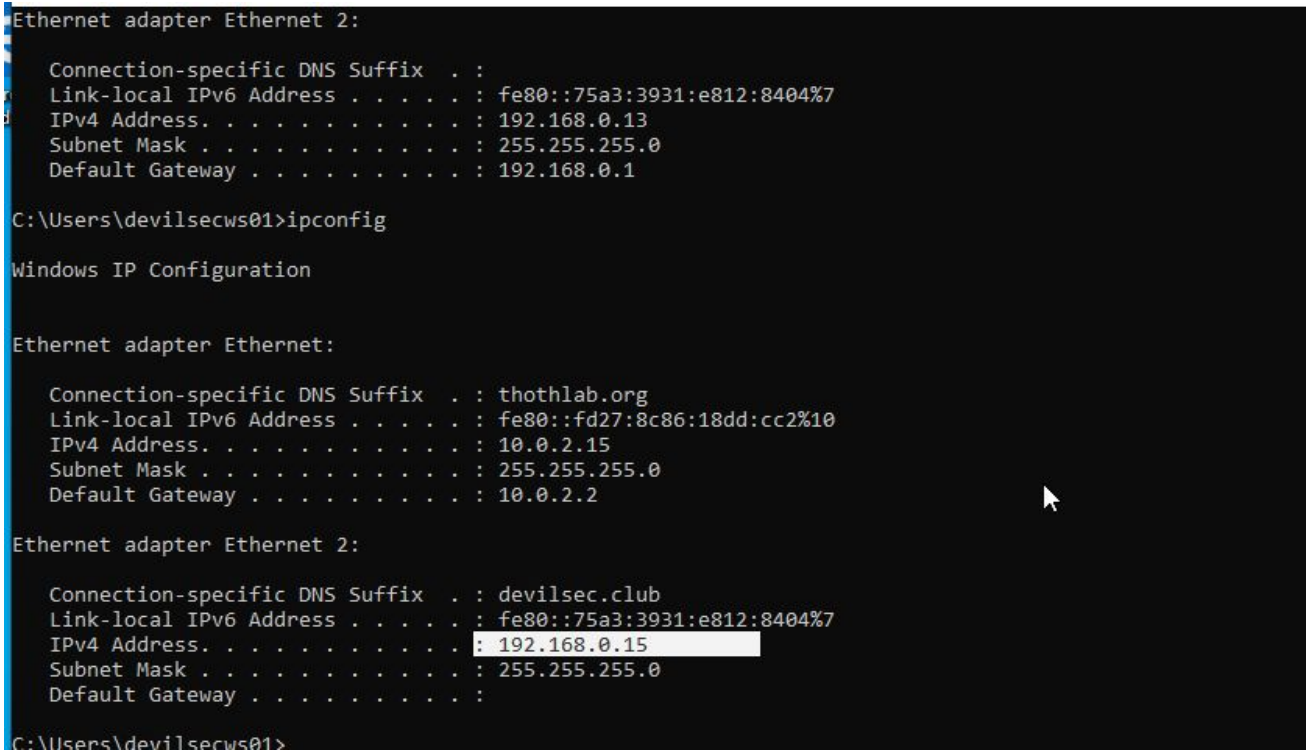

DHCP
File Action View Help
DHCP
win-kncvo6ot5ui.devilsec.cl
IPv4
Scope [192.168.0.0] n
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
IPv6
Option Name
006 DNS Servers
015 DNS Domain Name
Actions
Scope Options
More Actions
Manage Tools View Help
this local server
es and features
er servers to manage
server group
5 Connect this server to cloud servic
Hide
LEARN MORE
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1

DHCP Reservation

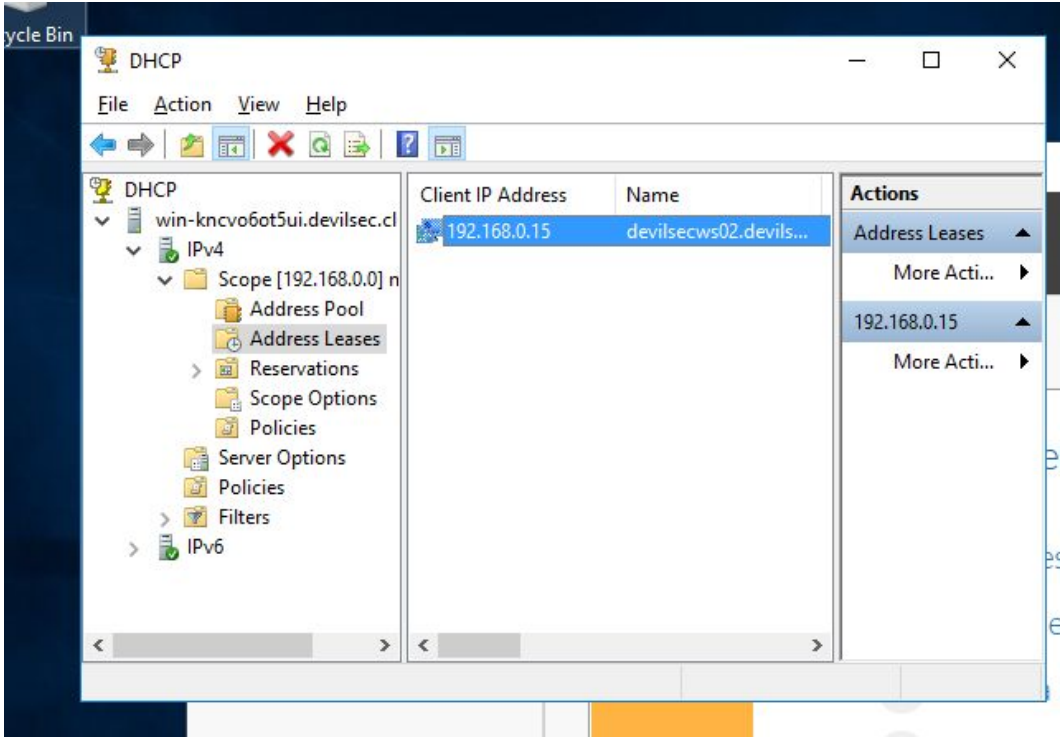
Go to Windows 10, getmac. From Server, add new reservation.



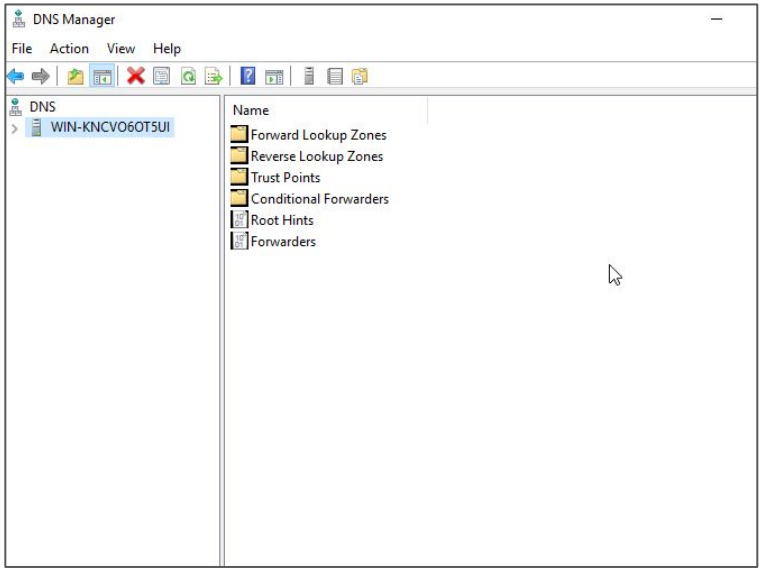
DHCP Reservation



Check Server address leases



DNS



- Associates hostname with IP address
- Devilsec.club vs 24.46.101.45
- Modem or router acts as DNS
- Tools->DNS from server manager
- Rt. click to manage remote DNS server
- Configure a DNS server
- Trust point-validate request
- Cond. forwarder - fwd req.to another dns server

Hosts file

- C:\Windows\Sys 32\drivers\etc\hosts
- Open text editor with admin rights - drag host file in text editor
- Commonly manipulated by hackers for DNS poisoning - fb.com points to some fake website.
- Try ping test.devilsec.club. Add an entry 127.0.0.1 test.devilsec.club - try ping again

DNS Zones

- Fwd lookup zone : nslookup [hostname] - gives IP address of the host
- Reverse lookup zone: nslookup [ip addr] - gives hostname info.
- Primary zone: %windir%\system32\dns. Maybe stored in AD if DNS is also writable DC. commonly due to security and ease of use.
- Secondary zone: R/O replica of primary zone. Change req. Passed to primary zone. Purpose is redundancy.
- Stub DNS zone: R/O. Information obtained from remote DNS server. Contains information about authoritative name servers. Less resource intensive.

Creating Zones, Resource Records

- Rt. click fwd lookup zone-> new zone.
- Rt. click rev lookup zone-> new zone. Network ID is first three octets of subnet with your zone.
- Resource records : SOA, NS, A, PTR, CNAME, MX, and SRV
- SOA- start of authority-info. about DNS server
- NS-zone’s auhtoritative DNS server
- A-FQDN to IP address mapping “google.com”-> 8.8.8.8
- PTR-opposite of A
- CNAME-alias for FQDN “joe.devilsec.com”-”badboy.devilsec.com”. Canonical Name
- MX-mail exchange, SRV-service record for services like webserver

DNS Resource Records

Rt. click zone you created - add other new records.

Add records for both fwd and reverse zones

CNAME for forward zone

PTR for reverse zone

End-to-end domain example

What happens when a user logs on to a Windows system – End to end domain Example

- Domain admin should add user's account information to the system before he can log on (username, account name – domain specific, and password).
- Windows creates and account in domain controller running AD. Each account has unique Security ID (SID) – unique to domain. E.g. - S-1-5-21-AAA-BBB-CCC-RRR, S-1-5-21-123625317-425641126-188346712-2895.
- If you create account "Mike", delete and re-create "Mike", they are two totally different accounts because they will have different SID.
- Once user log's in token SID is generated by OS and assigned to user.

End-to-end domain example

- Token contains user's SID, group membership information, and privileges.
- On a domain-joined computer (we'll use the 'Marketing' domain), it is possible for a user to logon to a local account by using the "." domain.
- So rather than using "Marketing\Paige" or just "Paige" Paige can use ".\Paige" assuming there is a local Paige account on the computer. The "." will substitute the machine name as the workgroup name.

Security ID

SID Identifier Authority (SECURITY_NT_AUTHORITY)

unique number representing the domain.

S-1-5-21-AAA-BBB-CCC-RRR.

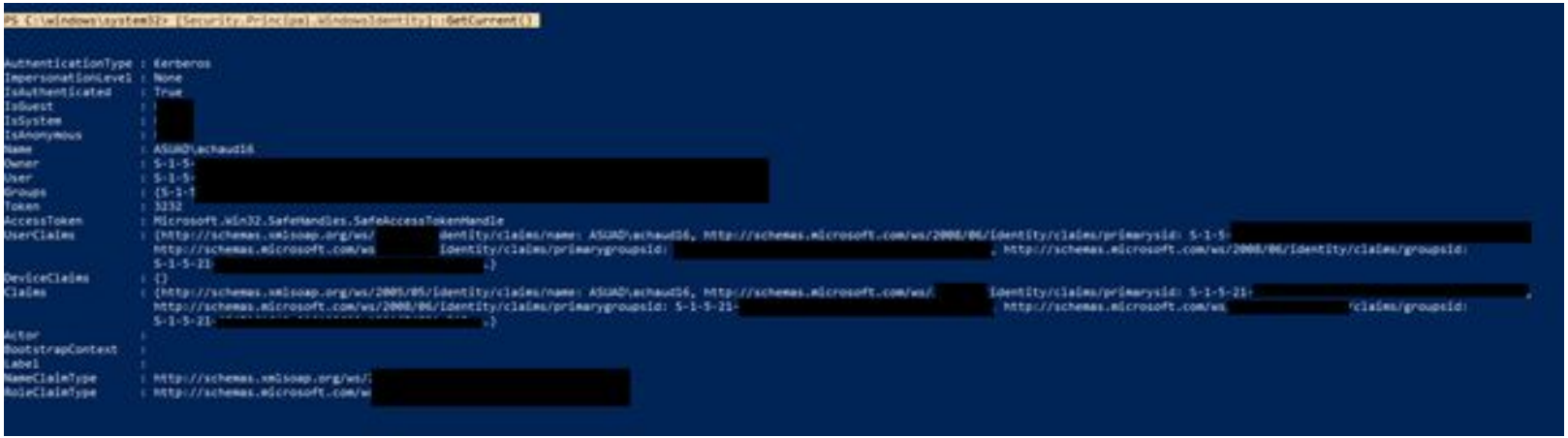
not-unique

SID version number

relative ID (RID); it's a non-repeating number that increments by 1 as each new account is created. This makes SID unique.

Security ID

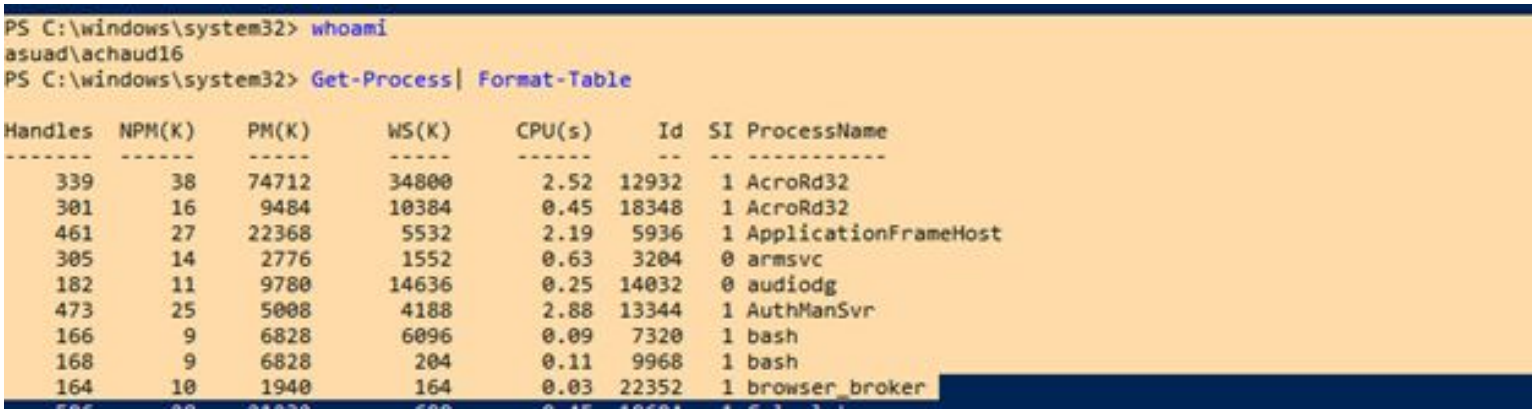
PS> [Security.Principal.WindowsIdentity]::GetCurrent()



Basic Powershell: Process Information

PS> whoami

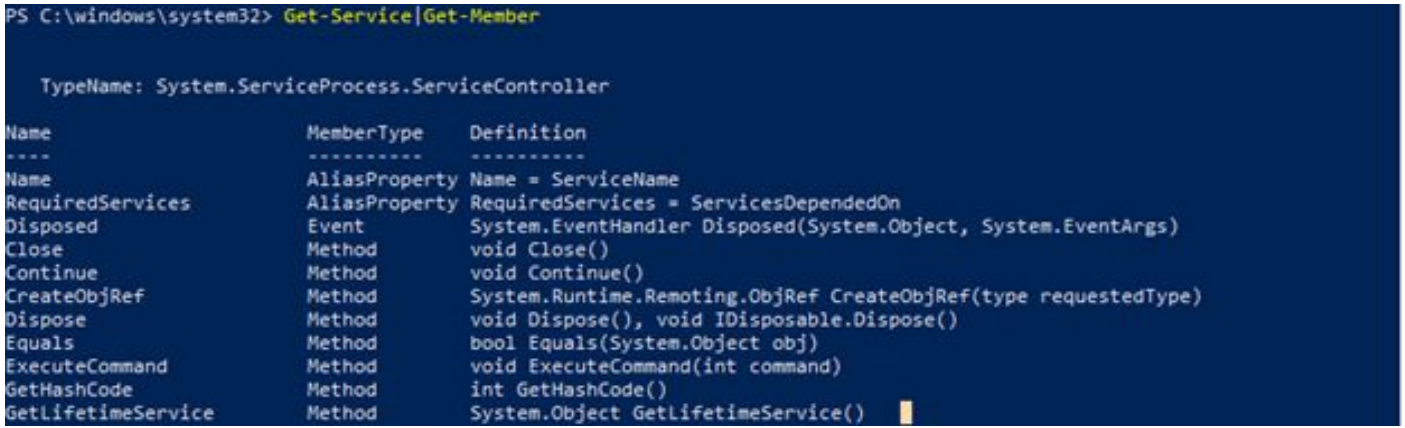
PS> Get-Process| Format-Table



Basic PS: Killing Process, Listing Object methods

PS > Get-Process -name chrome | Stop-Process

PS> Get-Service | Get-Member



Org. Units vs Containers

- Cannot apply GPOs to containers.
- Containers present by default. Not possible to containers in AD directly.
- Computer-default location of new computers joining domain
- Foreign Security Principal - trusted objects from other domains
- MSA- for services. Virus scanner, update, etc.
- Users, Built-in (cannot delete these groups)
- OU-organize and separate objects in AD. Marketing users and computers in marketing OUs. Specific permissions to OUs. Picking wrong OU for AD objects can cause issues.
- Create, delete OU, advanced features from view, properties, uncheck accidental deletion.

User Account Management

Tools-AD Users and Computers

Create and Manage Groups

Saved Query - check users not logged in 30 days

New - Query

LDAP Query

Group Policy

- Make configuration changes - restrict users to login to computers, access to files, background image to user.
- GP works by applying GPO to OUs. Settings in GPO applied to users and computers. Security filtering can be used for selective filtering. Applied recursively.
- Tools - Group Policy Management
- Link existing GPO
- Group Policy Precedence. Local GP-> Site GP -> Domain -> OU / Sub OU (applied last) - > enforce GPO. Last GPO to be applied takes precedence (LSDOE).
- Computer Config. -> User Configuration.
- OU can block inheritance.

PowerShell

RSAT - windows feature or DC

PS ISE