Cyber Defense Organization

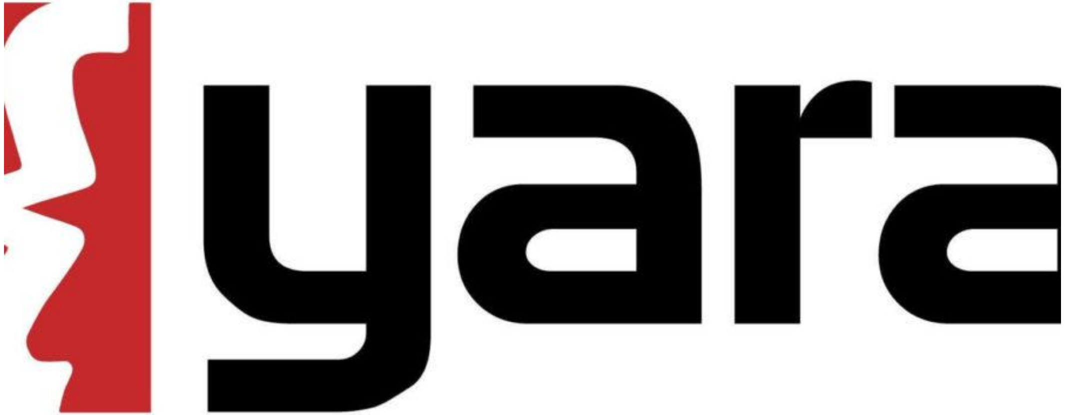
Fall 2018 - Windows Defense

Stuff for intro...

https://www.youtube.com/watch?v=s_razQwH0Ok

https://www.dailymotion.com/video/x6vp9um

Word of the Week



WTF is…. YARA

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic.

https://yara.readthedocs.io/en/v3.7.0/a

TL;DR De Facto standard for malware examination

Agenda

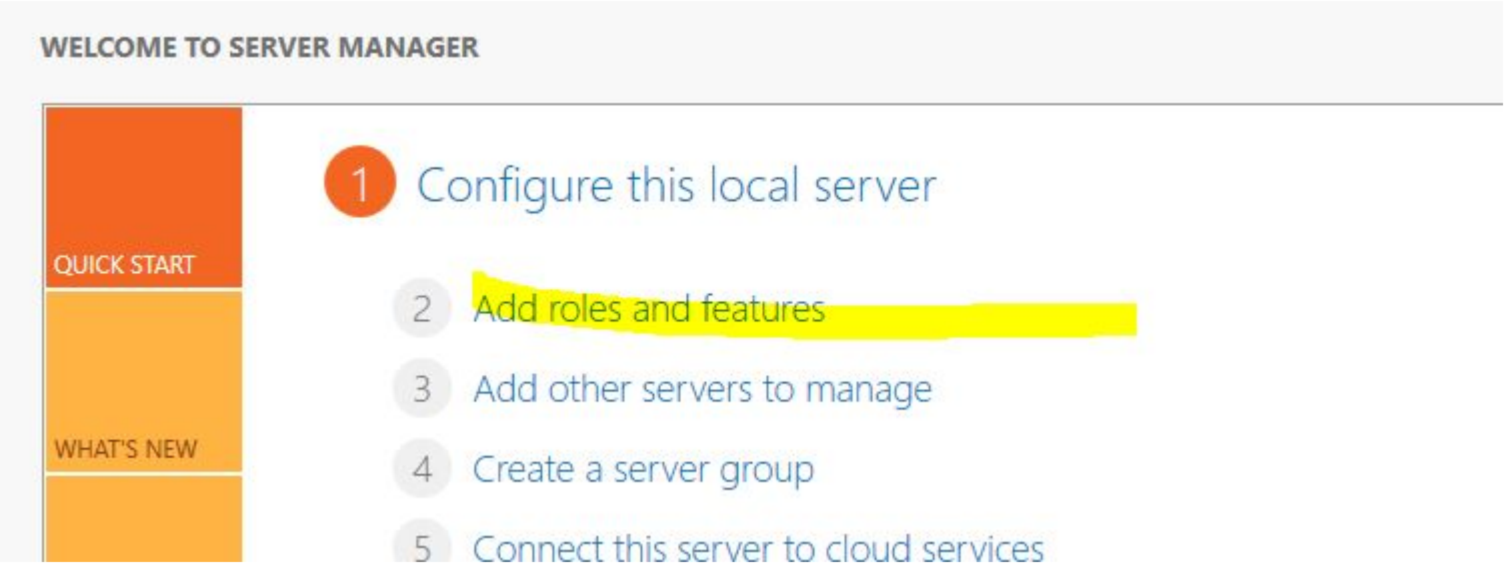
Install a role

Play with Active Directory

Threat hunt

Run a powershell script

Install a feature



WELCOME TO SERVER MANAGER

1 Configure this local server

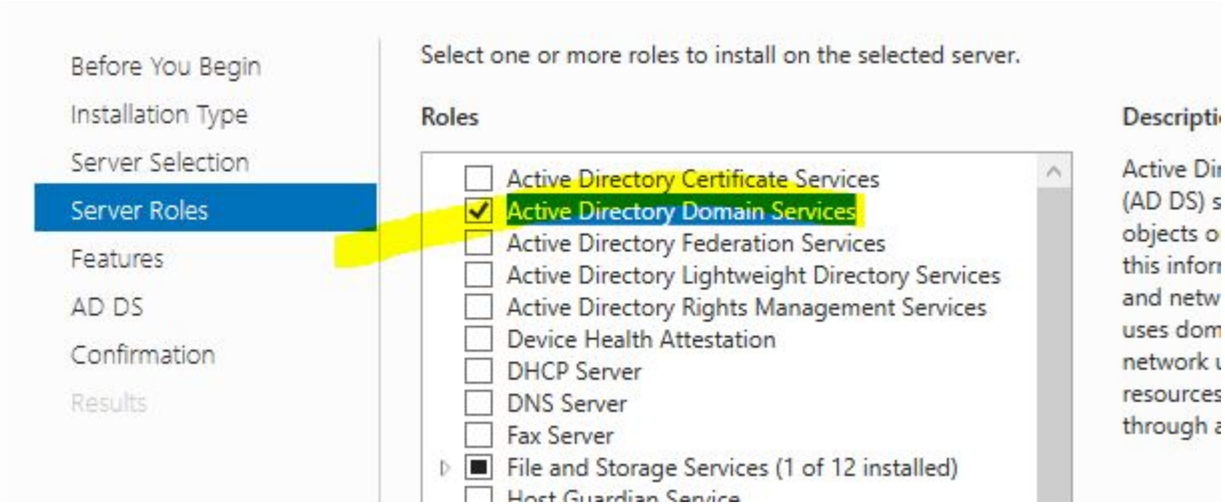
2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

Click until



Select one or more roles to install on the selected server.

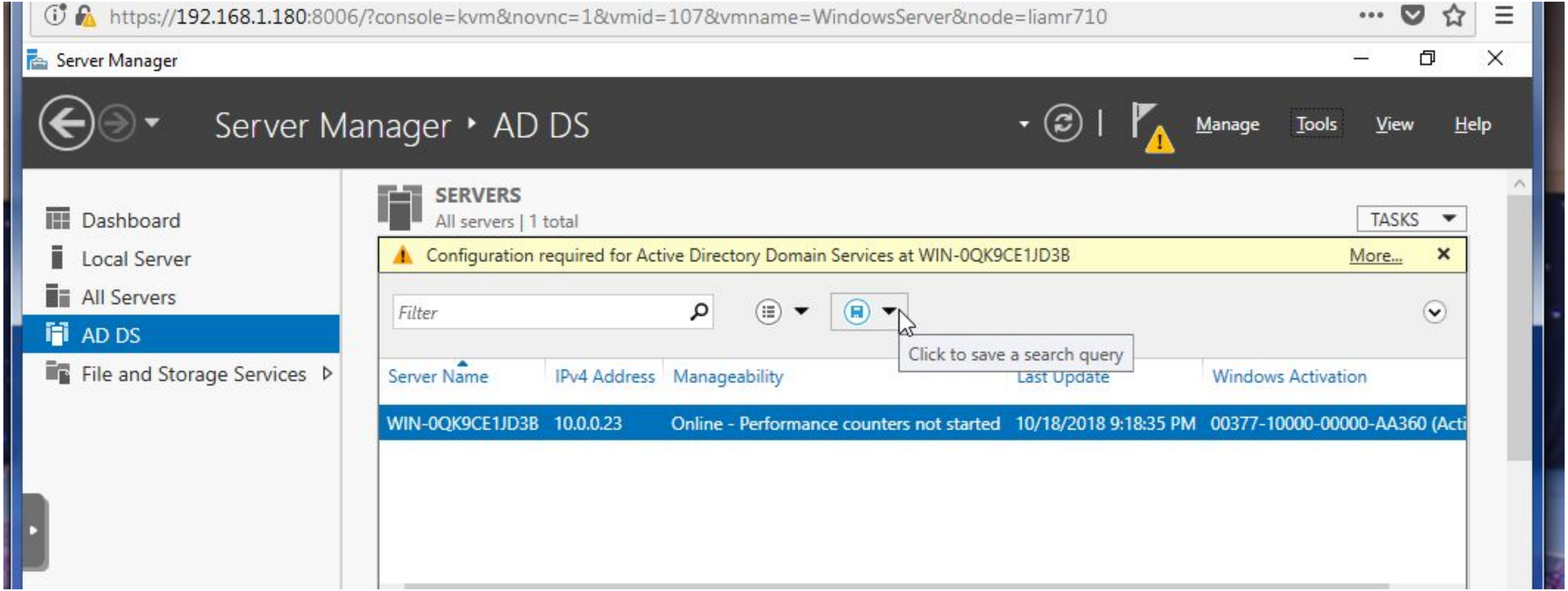
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service

Descripti

Active Di
(AD DS) s
objects o
this infor
and netw
uses dom
network u
resources
through a

Next



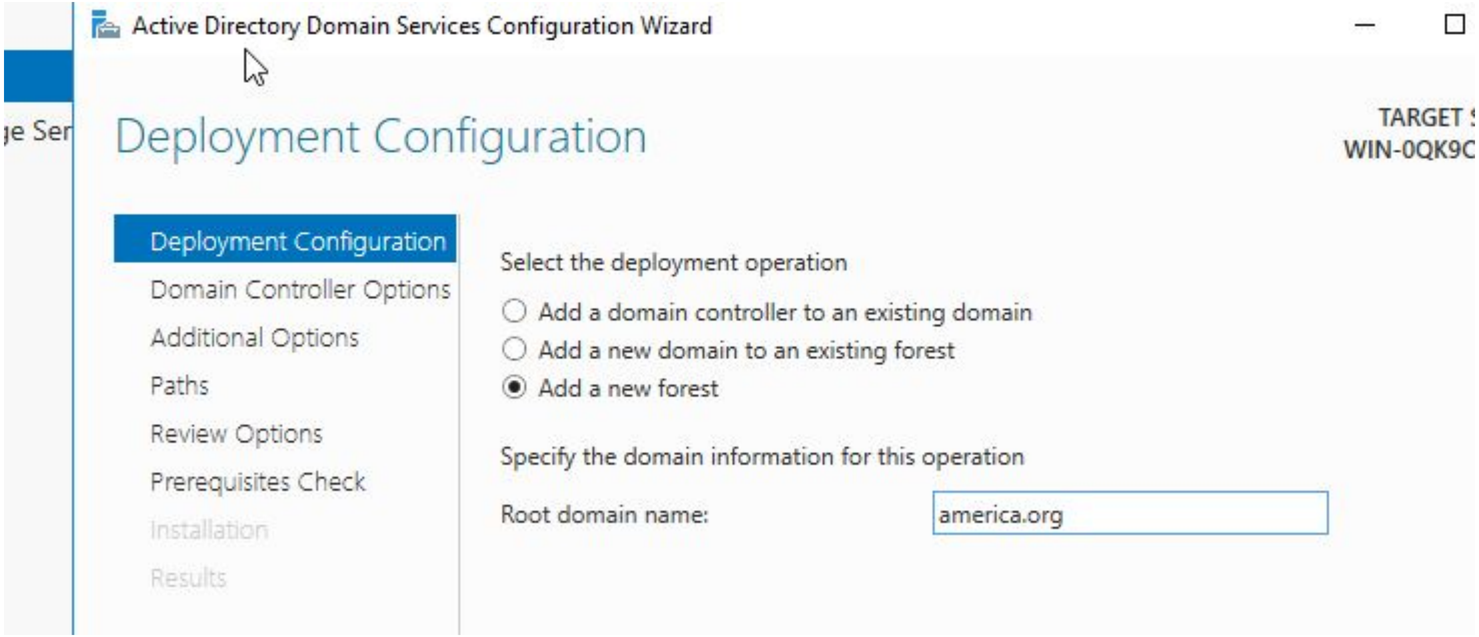
https://192.168.1.180:8006/?console=kvm&novnc=1&vmid=107&vmname=WindowsServer&node=liamr710

SERVERS

All servers | 1 total

Configuration required for Active Directory Domain Services at WIN-0QK9CE1JD3B More...

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-0QK9CE1JD3B	10.0.0.23	Online - Performance counters not started	10/18/2018 9:18:35 PM	00377-10000-00000-AA360 (Acti



Deployment Configuration

Select the deployment operation

○ Add a domain controller to an existing domain

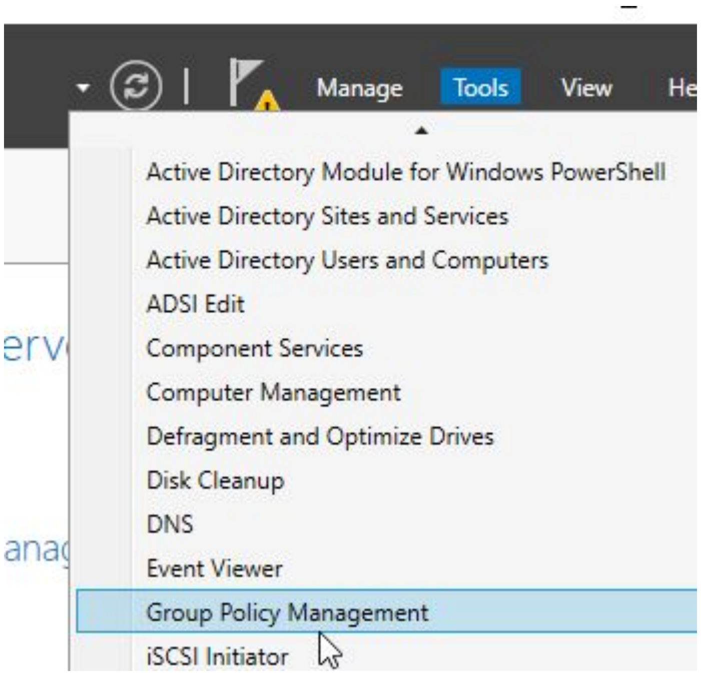
○ Add a new domain to an existing forest

● Add a new forest

Specify the domain information for this operation

Root domain name: america.org

Lets Create Group Policy



Manage
Tools
View
He
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
erv
anag

Group Policy

GPO - Account Lockout policy

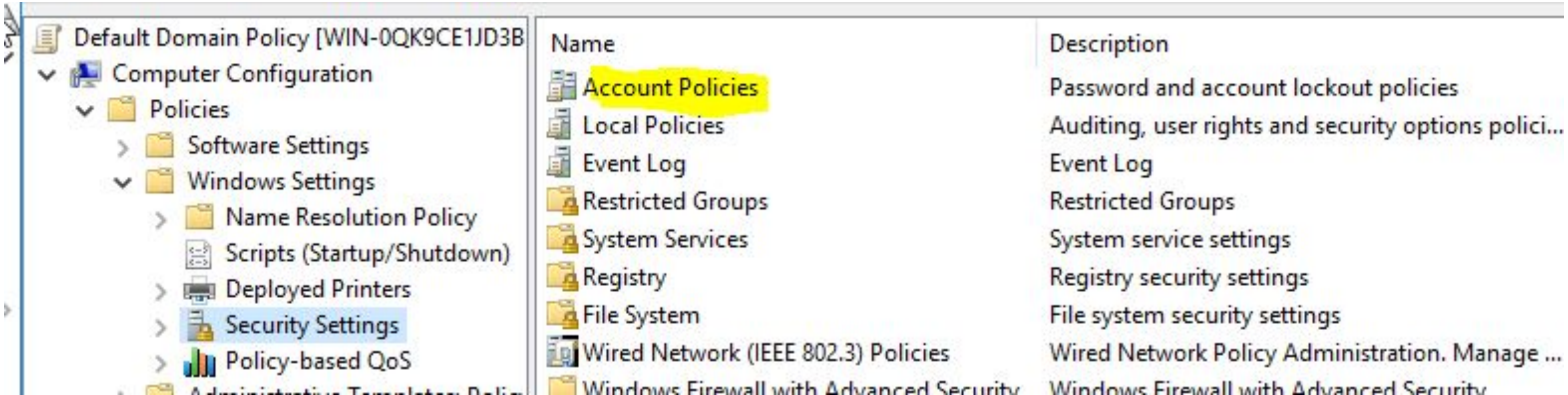
Lockout-

Account lockout duration - 120 mins

Account lockout attempts - 5

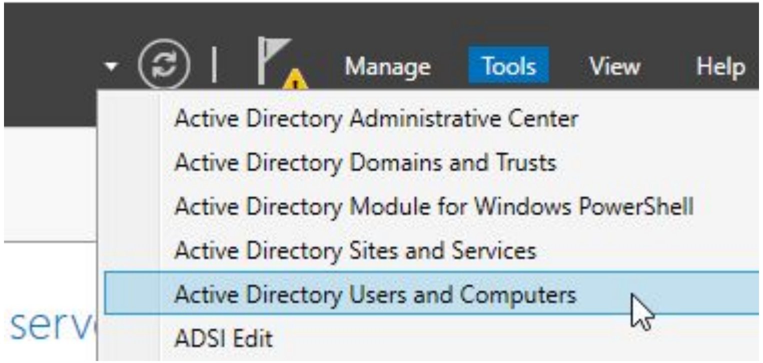
Once you have created the policy

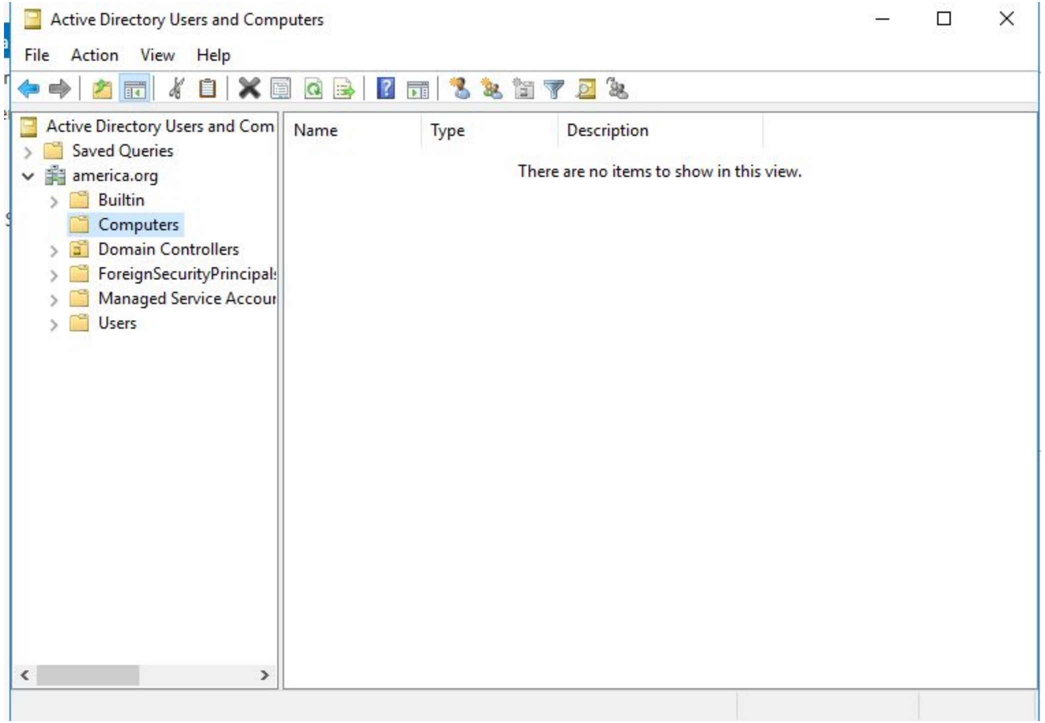
1. Open new powershell
2. gpupdate /force



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File system security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage ...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security

Make Some Users!


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
serv



There are no items to show in this view.

SysInternals

https://live.sysinternals.com/

Download:

Autoruns64.exe

procexp64.exe

Powershell Scripts!

Download AD Recon - https://github.com/sense-of-security/ADRecon

Start

powershell –ExecutionPolicy Bypass

UPDATES

Talk about your project - Workshop

Cya Next week!

Follow us on Twitter? Add on myInvolvement?

PWC 7:30PM Tuesday, BB129

Introduction to Routers

- Friday 3pm BB121

CCDC Meeting

- Monday 7:30PM BB121