# Implementatie

Sedric Yaovi Lodonou

Opgesteld op 20/5/2020

Versie 2

Er is dus geen implementatie documentatie gemaakt maar verschillende scripts. Voor elke oplossing is er een script gecreëerd. Deze scripts kunnen in de toekomst geïmplementeerd worden wanneer het mogelijk is.

De scripts bestaan uit 4 delen. Deel a van het script is het script die uitgevoerd moet worden voor de implementatie voor de verschillende problemen, deel b is een kleine deel die zorgt voor het controleren van de resultaten van het uitgevoerde script. Deel c en d zijn deel a en b maar met uitleg over de code.

# Bittorent - Implementatie

.

### Scavenger met Nbar

### Script: implementatie

!

*ip cef*

*class-map match-any CM-SCAVENGER-BT*

*match protocol bittorrent*

*match protocol kazaa2*

*match protocol gnutella*

*exit*

*policy-map PM- SCAVENGER -BT-POLICY*

*class CM- SCAVENGER -BT*

*set ip DSCP CS1*

*exit*

*exit*

*exit*

*int gig 0/2*

*ip nbar protocol-discovery*

*service-policy output PM- SCAVENGER -BT-POLICY*

*end*

*!*

*!*

### Script: Controle

show policy-map interface gig 0/1

Show running-config policy-map

Show running-config class-map

### Script: implementatie uitleg

* + - CEF1 moet aangezet worden, Peer-to-Peer kan niet geblokkeerd worden als dit uitstaat.

ip cef

* + - Maak een clasc-map genaamd CM-BLOCK-BT

  class-map match-any CM-BLOCK-BT

* + - Macht de class map met de verschillende protocollen die verwerkt moeten worden. We gaan hier niet alleen bittorrent zetten, maar ook twee andere grote P2P protocollen.

  match protocol bittorrent

  match protocol kazaa2

match protocol gnutella

  exit

* + - Maak een policy map. Hierin worden alle regels omtrent de actie die genomen moeten worden, prioriteiten etc… eerste stap is de gemaakte policy erin te steken.

  policy-map PM-BLOCK-BT-POLICY

* + - Hiermee krijgt alle verkeer die gelijk is aan het verkeer van de map CM-Block-BT de DSCP waarde van CS1. Hierdoor kijgt deze class 1% prioriteit van de bandbreedte.

  class CM-BLOCK-BT

*set DSCP CS1*

  exit

  exit

  exit

* + - Ga naar de interface waar dit toegepast moet worden in het netwerk, want daar moet nbaar aangezet worden

  Int gig 0/2

  ip nbar protocol-discovery

* + - The policy map moet toegepast worden op deze interface. Hier kan er ook vermelden worden of het een input of output is.

  service-policy output PM-BLOCK-BT-POLICY

### Script: Controle uitleg

* + - Voor alle statistieken voor pakketjes die geconfigureerd zijn voor alle service policies op deze interface.

show policy-map interface gig 0/1

* + - Voor alle policy map configuraties

Show running-config policy-map

* + - Voor class map configuraties

Show running-config class-map

# Telephonie / VOIP - Implementatie

### LLQ

### Script: Implamentatie

!

ip cef

class-map match-any cl\_RTVIDEO

match dscp af41

match protocol rtp video

exit

class-map match-any cl\_TRANSACTIONAL\_OUT

match access-group name acl\_APP\_SECR\_OUT

exit

class-map match-any cl\_IPTEL

match dscp ef

match protocol rtp audio

exit

class-map match-any cl\_TRANSACTIONAL

match dscp af21

exit

class-map match-any cl\_TRANSACTIONAL\_IN

match access-group name acl\_APP\_SECR\_IN

exit

policy-map pol\_LETHAS\_QOS\_APPLY

class cl\_IPTEL

priority percent 10

class cl\_RTVIDEO

bandwidth remaining percent 20

class cl\_TRANSACTIONAL

bandwidth remaining percent 40

random-detect

class class-default

fair-queue

policy-map pol\_LETHAS\_QOS\_SET\_LAN\_IN

class cl\_IPTEL

set ip dscp ef

class cl\_TRANSACTIONAL\_IN

set ip dscp af21

class cl\_TRANSACTIONAL\_OUT

set ip dscp af21

class cl\_RTVIDEO

set ip dscp af41

exit

exit

exit

int gig 0/0

ip nbar protocol-discovery

service-policy output pol\_LETHAS\_QOS\_APPLY

exit

int gig 0/1

ip nbar protocol-discovery

service-policy output pol\_LETHAS\_QOS\_SET\_LAN\_INexit

int gig 0/2

  ip nbar protocol-discovery

service-policy output pol\_LETHAS\_QOS\_APPLY

### Script: Controle

show policy-map interface gig 0/o

show policy-map interface gig 0/1

show policy-map interface gig 0/2

Show running-config policy-map

Show running-config class-map

### Script: implamentatie uitleg

* + - Cef moet aangezet worden voor express fowarding.

ip cef

* + - Een class-maps worden aangemaakt, de verschillende verkeerstypes worden in geclassificeerd. De matches worden gedaan met protocol zelf maar ook de DSCP-waarde.

class-map match-any cl\_RTVIDEO

match dscp af41

match protocol rtp video

exit

class-map match-any cl\_TRANSACTIONAL\_OUT

match access-group name acl\_APP\_SECR\_OUT

exit

class-map match-any cl\_IPTEL

match dscp ef

match protocol rtp audio

exit

class-map match-any cl\_TRANSACTIONAL

match dscp af21

exit

class-map match-any cl\_TRANSACTIONAL\_IN

match access-group name acl\_APP\_SECR\_IN

exit

* + - Nu wordt de policy aangemaakt, hierin wordt verteld wat er moet gebeuren met een bepaalde verkeerstype. Bij deze policy krijgt VoIP 10% van de bandbreedte. Video krijgt 20% en alle transactie krijgen 40%.

policy-map pol\_LETHAS\_QOS\_APPLY

class cl\_IPTEL

priority percent 10

class cl\_RTVIDEO

bandwidth remaining percent 20

class cl\_TRANSACTIONAL

bandwidth remaining percent 40

* + - Dit berekent gebruikt hierdoor de DSCP-waarde om de *drop probability* te bereken. De andere classes hebben al een gereserveerde bandbreedtes dus, bij opstopping worden ze nooit gedropt worden.

random-detect

class class-default

* + - Bij beperking in de netwerkbronnen zorgt fair-queue ervoor dat de beschikbare bronnen gelijk verdeelt zijn.

fair-queue

* + - Nu wordt weer een policy gemaakt, maar dit keer met DSCP waarden. Deze waarden hebben al een prioriteit ingebouwd. Bij de vorige opdracht was duidelijk dat de Scavengern (CS1) maar 1% had.

policy-map pol\_LETHAS\_QOS\_SET\_LAN\_IN

class cl\_IPTEL

set ip dscp ef

class cl\_TRANSACTIONAL\_IN

set ip dscp af21

class cl\_TRANSACTIONAL\_OUT

set ip dscp af21

class cl\_RTVIDEO

set ip dscp af41

exit

exit

exit

* + - Hier worden de policies op interfaces geïmplanteerd.

int gig 0/0

ip nbar protocol-discovery

service-policy output pol\_LETHAS\_QOS\_APPLY

exit

int gig 0/1

ip nbar protocol-discovery

service-policy output pol\_LETHAS\_QOS\_SET\_LAN\_INexit

int gig 0/2

ip nbar protocol-discovery

service-policy output pol\_LETHAS\_QOS\_APPLY

### Script: Controle uitleg

* + - Voor alle statistieken voor pakketjes die geconfigureerd zijn voor alle service policies op deze interface.

show policy-map interface gig 0/0

show policy-map interface gig 0/1

show policy-map interface gig 0/2

* + - Voor alle policy map configuraties

Show running-config policy-map

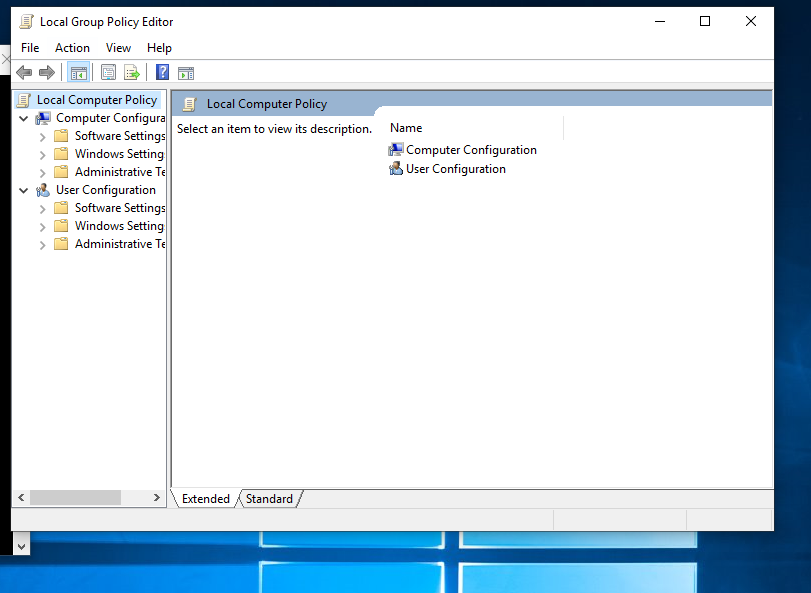
* + - Voor class map configuraties

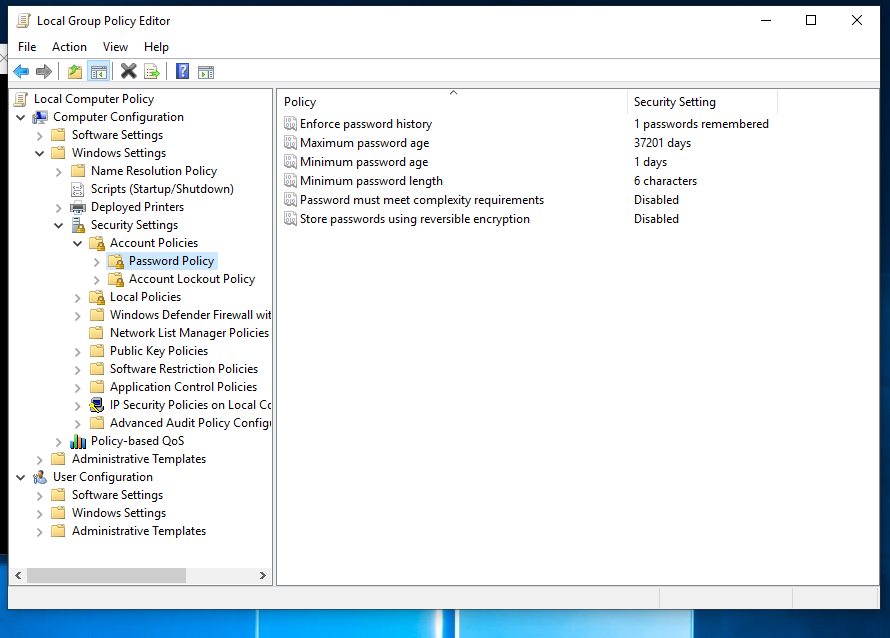
Show running-config class-map

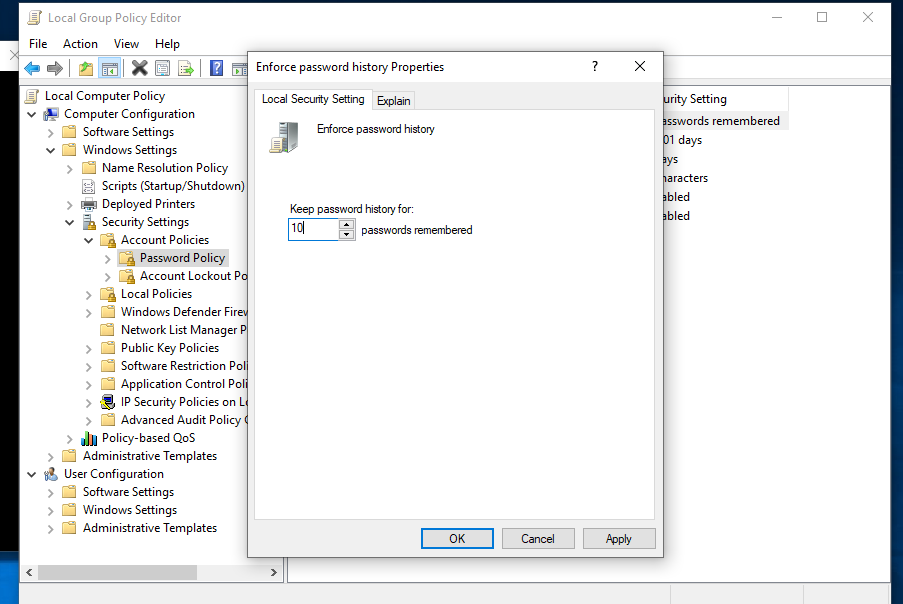
# Wachtwoorden- Implementatie

### Enforce password history

Hierdoor worden alle vorige wachtwoorden onthouden. Dit betekent dat er geen oude passorden opnieuw gebruikt kunnen worden. Bij het ingeven van een nieuw wachtwoord wordt eerst de lijst van opgeslagen wachtwoorden gecontroleerd, als het gekozen wachtwoord niet in de lijst is dan wordt het nieuwe wachtwoord geaccepteerd. Momenteel moeten de 10 vorige wachtwoorden opgeslagen worden.

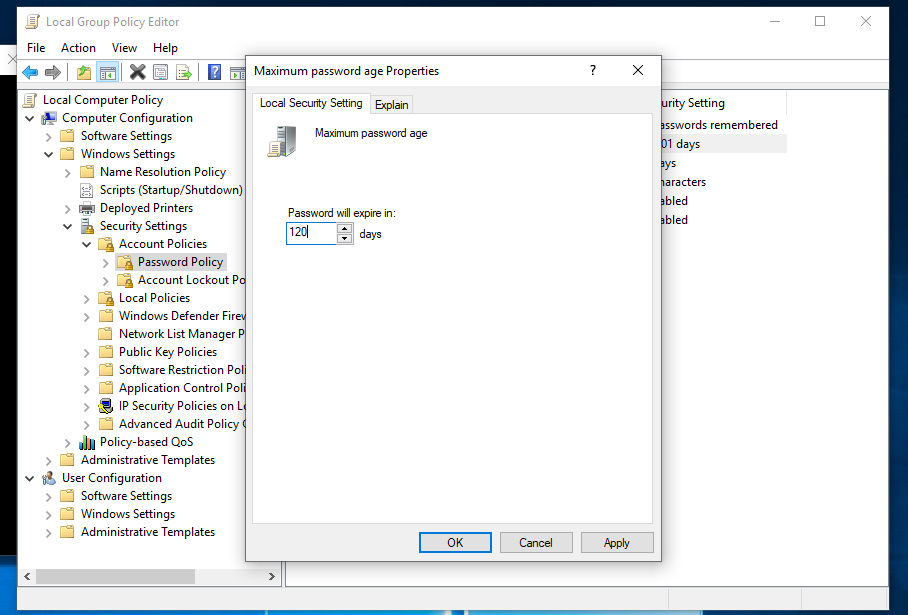






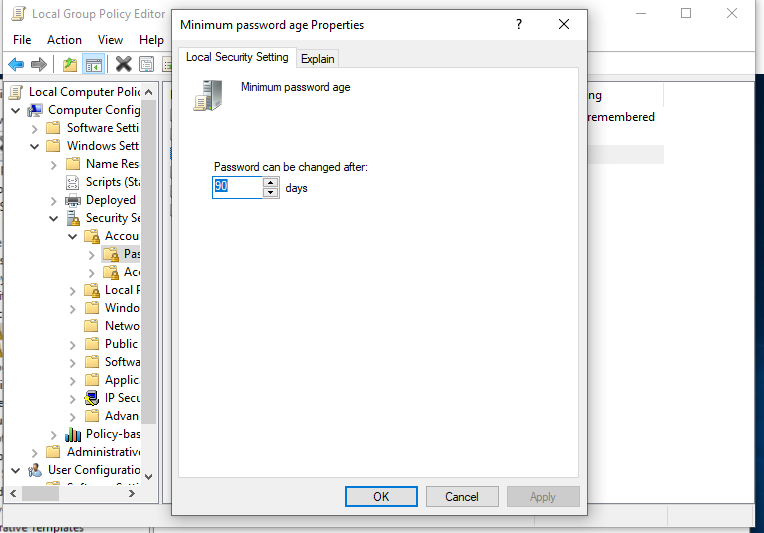
### “Max Password age”

Het wachtwoord moet ten laatste in 150dagen (5 maanden is de beste optie. Momenteel staat alles op 4 maanden omdat dit het eerste advies was) veranderd worden.



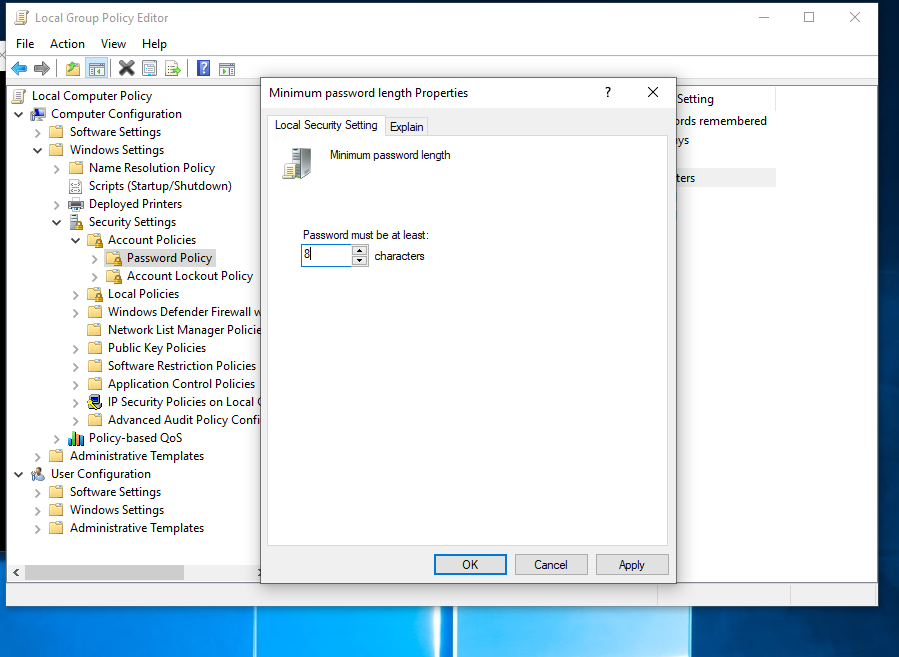
### Min Passwoord age

Na hoeveel maanden MAG het wachtwoord al veranderd worden. Voor drie maanden kunnen de gebruikers hun wachtwoord niet veranderen. Na 90 dagen kunnen de gebruikers hun wachtwoord veranderen tot de *Max Age*



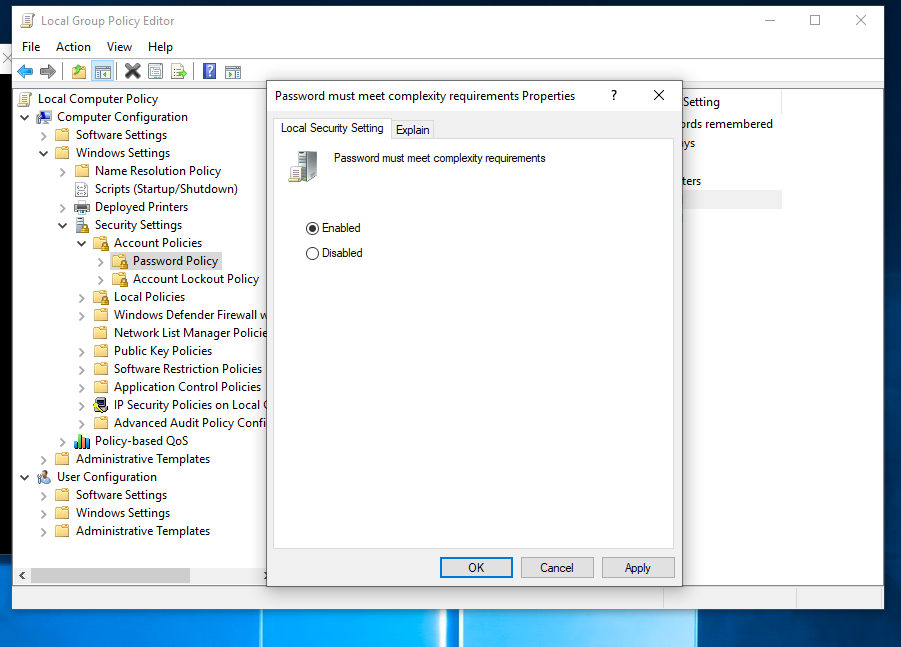
### Min Passwoord Length

Wachtwoord moet min een aantal karakters hebben. Die verhoogd de moeilijkheid graad van het wachtwoord. De min lengte hier is 8



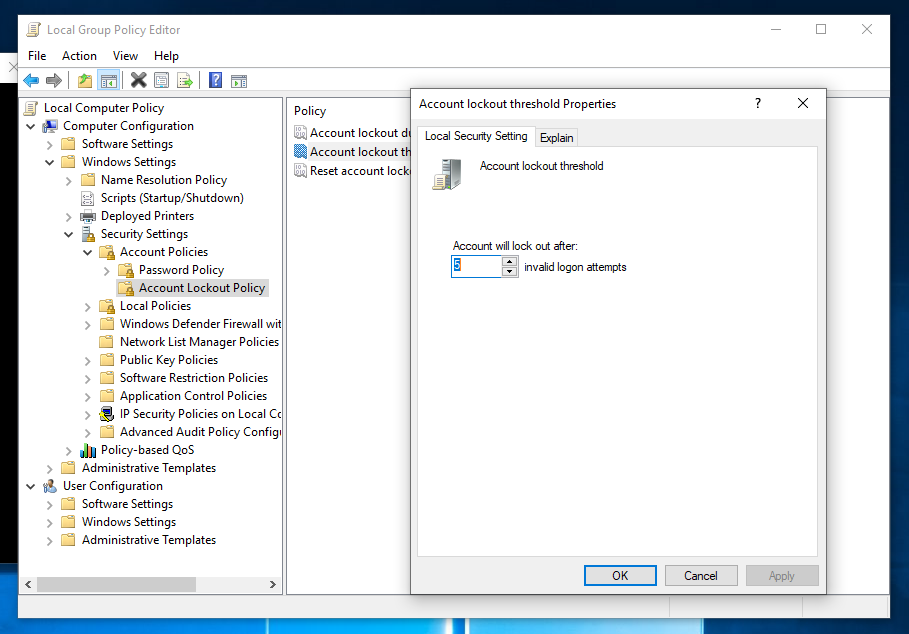
### Password complexity requirement

Dit zorgt ervoor dat er een wachtwoord gegeven wordt die een beetje moeilijker is dan gewoonlijks. Deze optie zorgt ervoor dat de wachtwoord verplicht een hoofdletter, kleinletter, symbool, cijfer etc bevat.



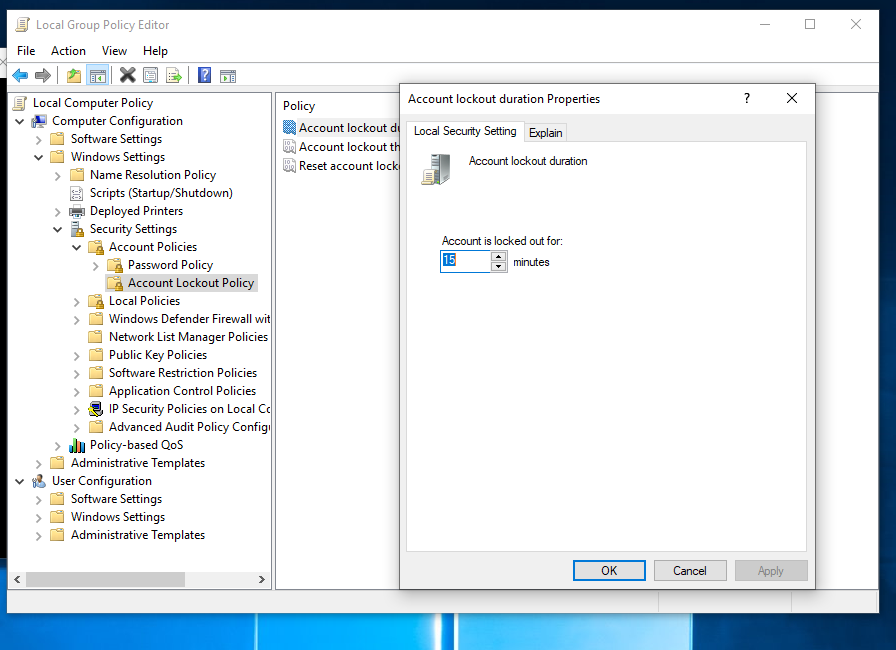
### Account Lockout Threshold

Na vijf pogingen zal de pc in lockdown gaan, dit is om attacks zoals brutforce attack tegen te gaan.



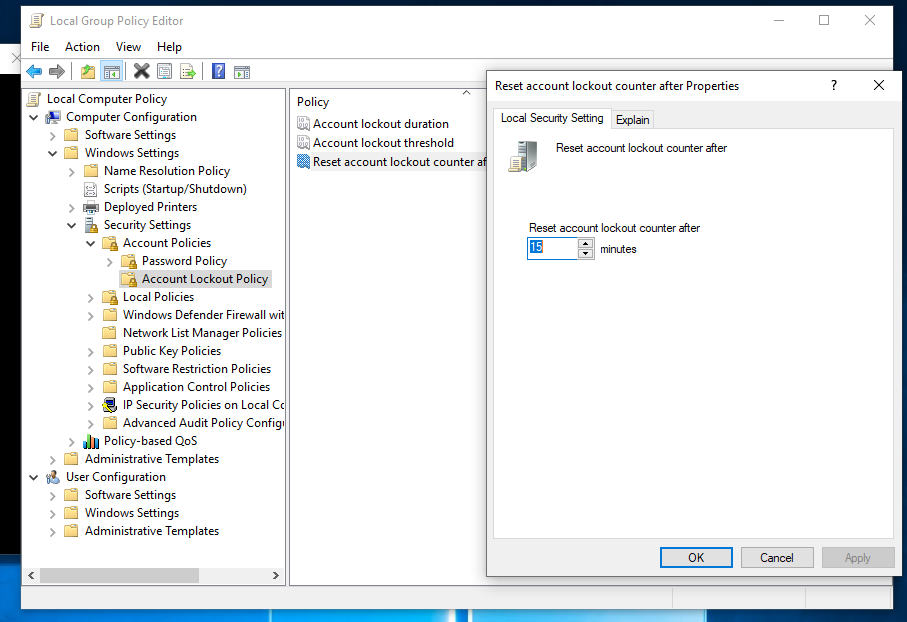
### Account Lockdown Duration

Hier kan de lengte van de lockdown ingesteld worden.



### Reset Lockdown counter

Na de lockdown duration timer op 0 is wordt de counter voor de ingegeven pogingen herstert.



# Per-Vlan Rapid Spaning Tree(PVST+)- Implementatie

### PVST+

### Script: Implamentatie

**!! LGL-FL1CR-Core-C3560v2-24p-Poe**

!

enable

config t

spanning-tree mode rapid-pvst

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

spanning-tree vlan 20,30,40,50,60,70,100,120 root secondary diameter 4

spanning-tree vlan 1,2,10,90,99 root primary diameter 4

end

!

**!!LGL-FL2-A213-Dist-C3560v2-24p-Poe**

!

*enable*

*config t*

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*spanning-tree vlan 20,30,40,50,60,70,100,120 root secondary diameter 4*

*spanning-tree vlan 1,2,10,90,99 root primary diameter 4*

*end*

*!*

***!!LGL-FL2-A201-C2860-24p***

*!*

*enable*

*Conf t*

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*end*

*!*

*!*

***!!LGL-FL4-FR-SF300-...***

*enable*

*Conf t*

*spanning-tree mode rapid-pvst*

*spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120*

*end*

*!*

### *Script: Controle*

*Show spanning-tree*

*Show spanning-tree active*

*Show spanning-tree bridge*

*Show spanning-tree brief*

*Show spanning-tree interface*

*Show spanning-tree root*

*Show spanning-tree summary*

*Show spanning-tree vlan*

### Script: implamentatie uitleg

!!LGL-FL2-A213-Dist-C3560v2-24p-Poe

!

enable

config t

* Zet spanning-tree aan. Laat het de mode pvst+ gebruiken

spanning-tree mode rapid-pvst

* Dit een spanning-tree methode waaring er meerdere vlans op een kables verkeer kunnen versturen. Nu moet de verschillende vlans ingeven die iver deze connecties moeten gaan.

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

* Laat de vlans 20,30,40,50,60,70,100,120 deze switch gebruiken als secondary root brigde

spanning-tree vlan 20,30,40,50,60,70,100,120 root secondary diameter 4

* Laat de vlans 1,2,10,90,99 deze switch gebruiken als root bridge

Spanning-tree vlan 1,2,10,90,99 root primary diameter 4

end

!

!!LGL-FL2-A201-C2860-24p

!

enable

Conf t

spanning-tree mode rapid-pvst

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

end

!

!

!!LGL-FL4-FR-SF300-...

enable

Conf t

spanning-tree mode rapid-pvst

spanning-tree vlan 2,10,20,30,40,50,60,70,80,90,99,100,120

end

!

### Script: Controle uitleg

* + - Weergave van STP informatie

*Show spanning-tree*

* + - Weergave van alle actieve STP interfaces

*Show spanning-tree active*

* + - Weergave van de bridge ID, timers, en protocol voor het lokale bridge op de switch

*Show spanning-tree bridge*

* + - Kleine samenvatting van STP

*Show spanning-tree brief*

* + - Weergave van STP-status en configuraties voor een specifieke interface

*Show spanning-tree interface*

* + - Weergave van status en configuratie van de root bridge van de switch

*Show spanning-tree root*

* + - Samenvatting voor de STP

*Show spanning-tree summary*

* + - Weergave van STP-information voor een specifieke VLAN

*Show spanning-tree vlan*

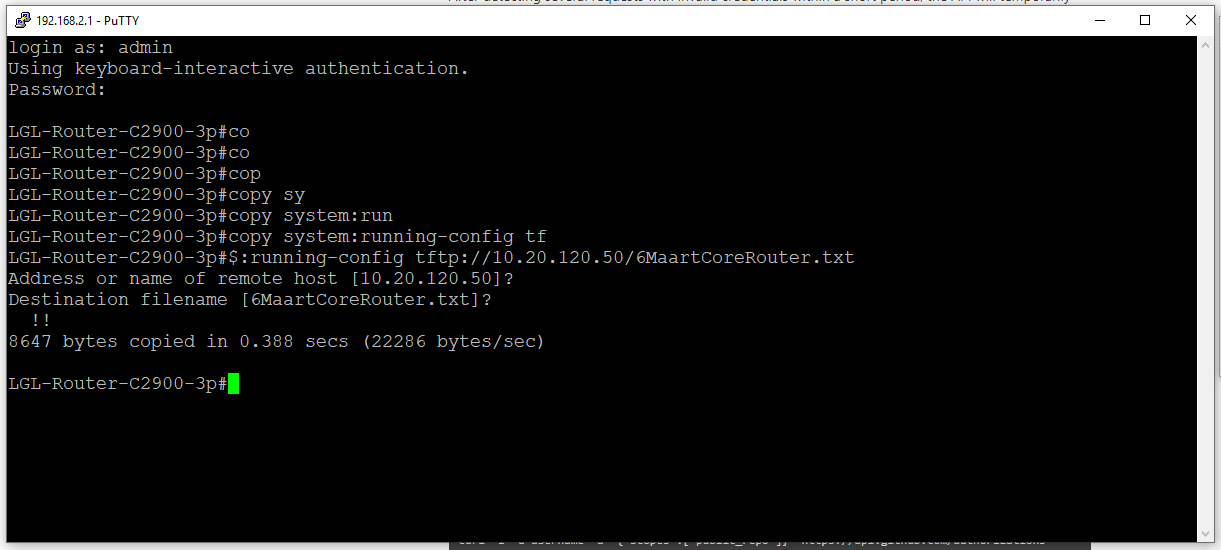
# Backup- Implementatie

### Configuratie tftpd

Current Directory 🡪 Locatie waar backup opgelagen moet worden.

Server Interface 🡪 de Interface die geconnecteerd met de router .

### Back-Up via command-line



!!verstuur een copie van de running config via de interface *Server Interface Address* en sla het op onder de naam  *DocumentNaam.txt*

copy system:running-config tftp://[*Server Interface Address*]/DocumentNaam.txt

!!Op 2000 series switches is het mogelijk dat de commando hiervoor anders is.

copy image tftp:// ://[*Server Interface Address*]/DocumentNaam.txt

!

CEF1: Cisco Express Forward is een switching techniek voor pakketjes op Cisco routers. Het optimaliseren van forwarden van de pekketen en het vergroten van de snelheid van het switching proces