

## Automatisch toewijzen van een VLAN aan een gebruiker

## Contents

Figuren- en tabbellenlijst.....	4
1. Voorwoord.....	11
2. Inleiding .....	12
3. Fysieke setup.....	13
4. vSphere.....	15
4.1    Virtuele Switches .....	15
4.2 Templates .....	18
5. FortiGate firewall.....	20
5.1 Interfaces .....	20
5.2 VLAN-indeling .....	23
5.3 DHCP .....	24
5.4 Adressen .....	25
5.5 Virtual IPs.....	26
5.5.1 Configuratie virtuele IP (VIP) .....	26
5.5.2 Configuratie virtuele IP groep (VIPG). ....	28
5.5.3 Firewall policy rule RDP, SSH, ... .....	28
5.6 Schedules .....	29
5.7 SSID (Service Set Identifier) .....	30
5.8 AP profiel.....	32
5.9 Acces point (AP).....	35
6. Virtuele servers .....	37
6.1 Domain controller.....	37
6.1.1 Installatie AD.....	37
6.1.2 Installatie Certificaat services.....	41
6.1.3 Users and computers .....	48
6.1.4 Groep Policy .....	50
6.1.5 Extra – Linux Join active directory .....	65
6.2 RADIUS (Network policy server).....	69
6.2.1 Installatie NPS .....	69
6.2.2 Registreren van server .....	74
6.2.3 Configuratie RADIUS clients.....	74

## Automatisch toewijzen van een VLAN aan een gebruiker

6.2.4 connection request policies.....	75
6.2.5 Configuratie network policies.....	76
6.3 Fileserver .....	79
6.3.1 Installatie services .....	79
6.3.2 Toevoegen van een extra schijf.....	80
6.3.3 Aanmaken share.....	84
6.3.4 Users en computers groepen.....	87
6.3.5 Share rechten aanpassen.....	90
6.3.6 Rechten aan de mappen toekennen.....	91
6.4 Management.....	92
6.5 Back-up (Veeam).....	93
6.5.1 Installatie Veeam .....	93
6.5.2 Create Backup repository.....	98
6.5.3 Voeg servers toe voor back-up.....	102
6.5.4 Backup job aanmaken.....	104
6.6 Monitoring.....	107
6.6.1 Zabbix.....	107
6.7 Syslog logging .....	117
6.7.1 Schema.....	117
6.7.2 Installatie handleidingen .....	117
7. Switches.....	137
7.1 FortiSwitch .....	137
7.1.1 Opzet.....	137
7.1.2 Hostname.....	140
7.1.3 Instellen van RADIUS server .....	140
7.1.4 Groep aanmaken.....	142
7.1.5 Configuratie 802.1x poort .....	143
7.1.6 Configuratie voor syslogs.....	145
7.2 Aruba Switch.....	146
7.2.1 hostname.....	146
7.2.2 VLAN's .....	146
7.2.3 Trunk poort .....	147
7.2.4 Poort configuratie .....	149
7.2.5 Radius Configuratie .....	149

## Automatisch toewijzen van een VLAN aan een gebruiker

7.2.5 Poort toegangscontrole.....	150
7.2.3 Configuratie Syslog .....	152
8. FortiAnalyzer.....	154
8.1 Authorizatie hosts .....	154
8.2 Device Manager.....	155
8.3 Syslogs .....	156
8.4 Traffiek .....	157
8.5 Bedreigingen .....	157
9. Test-scenarios RADIUS 802.1x authentication.....	159
10. Conclusie.....	160
11. Bronnen .....	161

## **Figuren- en tabellenlijst**

Figuur 1: Fysieke setup.....	13
Figuur 2: Switches met aansluiting naar de laptops .....	13
Figuur 3: Netwerk indeling.....	14
Figuur 4: vSphere virtuele machines .....	15
Figuur 5: vSphere opstelling van de virtuele switch.....	15
Figuur 6: vSphere aanmaken van een virtuele switch (1) .....	16
Figuur 7: vSphere aanmaken van een virtuele switch (2) .....	16
Figuur 8: vSphere aanmaken van een virtuele switch (3) .....	17
Figuur 9: vSphere aanmaken van een virtuele switch (4) .....	17
Figuur 10: vSphere aanmaken van een virtuele switch (5).....	18
Figuur 11: vSphere aanmaken van een template .....	19
Figuur 12: Fortigate firewall fysieke poort.....	20
Figuur 13: Fortigate firewall vlan overzicht .....	20
Figuur 14: Fortigate firewall aanmaken VLAN (1) .....	21
Figuur 15: Fortigate firewall aanmaken VLAN (2) .....	22
Figuur 16: Fortigate firewall aanmaken VLAN (3) .....	23
Figuur 17: Fortigate firewall menu.....	24
Figuur 18: Fortigate firewall DHCP overzicht .....	25
Figuur 19: Fortigate firewall aanmaken van IP-adres (1) .....	25
Figuur 20: Fortigate firewall aanmaken van IP-adres (2) .....	26
Figuur 21: Fortigate firewall aanmaken van VIP.....	27
Figuur 22: Fortigate firewall VIP overzicht .....	27
Figuur 23: Fortigate firewall VIP groep overzicht .....	28
Figuur 24: Fortigate firewall aanmaken van VIP groep.....	28
Figuur 25: Fortigate firewall policy overzicht.....	28
Figuur 26: Fortigate firewall aanmaken van een policy .....	29
Figuur 27: Fortigate firewall aanmaken van een schedule .....	30
Figuur 28: Fortigate firewall aanmaken van SSID (1).....	30
Figuur 29: Fortigate firewall aanmaken van SSID (2).....	30
Figuur 30: Fortigate firewall aanmaken van SSID (3).....	31
Figuur 31: Fortigate firewall aanmaken van SSID (4).....	31
Figuur 32: Fortigate firewall aanmaken van SSID (5).....	32
Figuur 33: Fortigate firewall aanmaken van AP (1) .....	33
Figuur 34: Fortigate firewall aanmaken van AP (2) .....	33
Figuur 35: Fortigate firewall aanmaken van AP (3) .....	34
Figuur 36: Fortigate firewall aanmaken van AP (4) .....	34
Figuur 37: Fortigate firewall V51 overzicht.....	35
Figuur 38: Fortigate firewall autorizeren van AP (1).....	35
Figuur 39: Fortigate firewall autorizeren van AP (2).....	35
Figuur 40: Fortigate firewall autorizeren van AP (3).....	36
Figuur 41: Installatie van de DC (1) .....	37

## Automatisch toewijzen van een VLAN aan een gebruiker

Figuur 42: Installatie van de DC (2) .....	37
Figuur 43: Installatie van de DC (3) .....	38
Figuur 44: Installatie van de DC (4) .....	38
Figuur 45: Installatie van de DC (5) .....	39
Figuur 46: Installatie van de DC (6) .....	39
Figuur 47: Installatie van de DC (7) .....	39
Figuur 48: Installatie van de DC (8) .....	40
Figuur 49: Installatie van de DC (9) .....	41
Figuur 50: Installatie van de certificaat services (1) .....	41
Figuur 51: Installatie van de certificaat services (2) .....	42
Figuur 52: Installatie van de certificaat services (3) .....	43
Figuur 53: Installatie van de certificaat services (4) .....	43
Figuur 54: Installatie van de certificaat services (5) .....	43
Figuur 55: Installatie van de certificaat services (6) .....	44
Figuur 56: Installatie van de certificaat services (7) .....	44
Figuur 57: Installatie van de certificaat services (8) .....	45
Figuur 58: Installatie van de certificaat services (9) .....	45
Figuur 59: Installatie van de certificaat services (10) .....	46
Figuur 60: Installatie van de certificaat services (11) .....	47
Figuur 61: Installatie van de certificaat services (12) .....	47
Figuur 62: Installatie van de certificaat services (13) .....	48
Figuur 63: Aanmaken van OU (1) .....	48
Figuur 64: Aanmaken van OU (2) .....	49
Figuur 65: Aanmaken van OU (3) .....	49
Figuur 66: Aanmaken van OU (4) .....	50
Figuur 67: Aanmaken van OU (5) .....	50
Figuur 68: Navigeren naar GPO .....	51
Figuur 69: GPO aanmaken voor NTP (1) .....	51
Figuur 70: GPO aanmaken voor NTP (2) .....	52
Figuur 71: GPO aanmaken voor NTP (3) .....	52
Figuur 72: GPO aanmaken voor NTP (4) .....	53
Figuur 73: GPO aanmaken voor drives (1) .....	53
Figuur 74: GPO aanmaken voor drives (2) .....	54
Figuur 75: GPO aanmaken voor drives (3) .....	54
Figuur 76: GPO aanmaken voor drives (4) .....	54
Figuur 77: GPO aanmaken voor drives (5) .....	55
Figuur 78: GPO aanmaken voor drives (6) .....	55
Figuur 79: GPO aanmaken voor 802.1 auth (1) .....	56
Figuur 80: GPO aanmaken voor 802.1 auth (2) .....	56
Figuur 81: GPO aanmaken voor 802.1 auth (3) .....	57
Figuur 82: GPO aanmaken voor 802.1 auth (4) .....	57
Figuur 83: GPO aanmaken voor 802.1 auth (5) .....	58
Figuur 84: GPO aanmaken voor 802.1 auth (6) .....	58
Figuur 85: GPO aanmaken voor 802.1 auth (7) .....	58
Figuur 86: GPO aanmaken voor 802.1 auth (8) .....	59
Figuur 87: GPO aanmaken voor 802.1 auth (9) .....	59

## Automatisch toewijzen van een VLAN aan een gebruiker

Figuur 88: GPO aanmaken voor 802.1 auth (10).....	60
Figuur 89: GPO aanmaken voor 802.1 auth (11).....	60
Figuur 90: GPO aanmaken voor 802.1 auth (12).....	61
Figuur 91: GPO aanmaken voor certificaten (1).....	62
Figuur 92: GPO aanmaken voor certificaten (2).....	62
Figuur 93: GPO aanmaken voor certificaten (3).....	62
Figuur 94: GPO aanmaken voor certificaten (4).....	63
Figuur 95: GPO aanmaken voor certificaten (5).....	63
Figuur 96: GPO aanmaken voor certificaten (6).....	64
Figuur 97: GPO aanmaken voor certificaten (7).....	64
Figuur 98: Domein joinen via linux (1) .....	65
Figuur 99: Domein joinen via linux (2) .....	65
Figuur 100: Domein joinen via linux (3).....	66
Figuur 101: Domein joinen via linux (4).....	66
Figuur 102: Domein joinen via linux (5).....	67
Figuur 103: Domein joinen via linux (6).....	67
Figuur 104: Domein joinen via linux (7).....	68
Figuur 105: Domein joinen via linux (8).....	68
Figuur 106: Domein joinen via linux (9).....	68
Figuur 107: Installatie van de NPS (1).....	69
Figuur 108: Installatie van de NPS (2).....	69
Figuur 109: Installatie van de NPS (3).....	70
Figuur 110: Installatie van de NPS (4).....	70
Figuur 111: Installatie van de NPS (5).....	71
Figuur 112: Installatie van de NPS (6).....	71
Figuur 113: Installatie van de NPS (7).....	72
Figuur 114: Installatie van de NPS (8).....	72
Figuur 115: Installatie van de NPS (9).....	73
Figuur 116: Installatie van de NPS (10) .....	73
Figuur 117: Configuratie van de NPS (1) .....	74
Figuur 118: Configuratie van de NPS (2) .....	74
Figuur 119: Configuratie van de NPS (3) .....	75
Figuur 120: Configuratie van de NPS (4) .....	76
Figuur 121: Configuratie van de NPS (5) .....	77
Figuur 122: Configuratie van de NPS (6) .....	77
Figuur 123: Configuratie van de NPS (7) .....	78
Figuur 124: Configuratie van de NPS (8) .....	78
Figuur 125: Installatie van de fileserver (1).....	79
Figuur 126: Installatie van de fileserver (2).....	79
Figuur 127: Installatie van de fileserver (3).....	79
Figuur 128: Installatie van de fileserver (4).....	80
Figuur 129: Installatie van de fileserver (5).....	80
Figuur 130: vSphere extra drive aanmaken (1).....	81
Figuur 131: vSphere extra drive aanmaken (2).....	81
Figuur 132: vSphere extra drive aanmaken (3).....	81
Figuur 133: vSphere extra drive aanmaken (4).....	82

## Automatisch toewijzen van een VLAN aan een gebruiker

Figuur 134: vSphere extra drive aanmaken (5).....	82
Figuur 135: vSphere extra drive aanmaken (6).....	82
Figuur 136: vSphere extra drive aanmaken (7).....	82
Figuur 137: vSphere extra drive aanmaken (8).....	83
Figuur 138: vSphere extra drive aanmaken (9).....	83
Figuur 139: vSphere extra drive aanmaken (10) .....	83
Figuur 140: vSphere extra drive aanmaken (11) .....	84
Figuur 141: File share aanmaken (1) .....	84
Figuur 142: File share aanmaken (2) .....	84
Figuur 143: File share aanmaken (3) .....	85
Figuur 144: File share aanmaken (4) .....	85
Figuur 145: File share aanmaken (5) .....	86
Figuur 146: File share aanmaken (6) .....	86
Figuur 147: File share aanmaken (7) .....	87
Figuur 148: File share aanmaken (8) .....	87
Figuur 149: Overzicht van de groepen.....	88
Figuur 150: Overzicht van de ACL groepen .....	88
Figuur 151: Members van de groep LSY-ACL (1).....	89
Figuur 152: Members van de groep LSY-ACL (2).....	89
Figuur 153: Members van de groep LSY-ACL (3).....	90
Figuur 154: Members van de groep LSY-ACL (4).....	90
Figuur 155: Groepen toekennen aan een folder (1).....	91
Figuur 156: Groepen toekennen aan een folder (2).....	92
Figuur 157: Groepen toekennen aan een folder (3).....	92
Figuur 158: Installatie van VEEAM (1).....	93
Figuur 159: Installatie van VEEAM (2).....	93
Figuur 160: Installatie van VEEAM (3).....	93
Figuur 161: Installatie van VEEAM (4).....	94
Figuur 162: Installatie van VEEAM (5).....	94
Figuur 163: Installatie van VEEAM (6).....	95
Figuur 164: Installatie van VEEAM (7).....	95
Figuur 165: Installatie van VEEAM (8).....	96
Figuur 166: Installatie van VEEAM (9).....	96
Figuur 167: Installatie van VEEAM (10) .....	97
Figuur 168: Installatie van VEEAM (11) .....	97
Figuur 169: Configuratie van VEEAM (1) .....	98
Figuur 170: Configuratie van VEEAM (2) .....	98
Figuur 171: Configuratie van VEEAM (3) .....	99
Figuur 172: Configuratie van VEEAM (4) .....	99
Figuur 173: Configuratie van VEEAM (5) .....	100
Figuur 174: Configuratie van VEEAM (6) .....	100
Figuur 175: Configuratie van VEEAM (7) .....	101
Figuur 176: Configuratie van VEEAM (8) .....	101
Figuur 177: Configuratie van VEEAM (9) .....	102
Figuur 178: Configuratie van VEEAM (10) .....	102
Figuur 179: Configuratie van VEEAM (11).....	102

## Automatisch toewijzen van een VLAN aan een gebruiker

Figuur 180: Configuratie van VEEAM (12).....	103
Figuur 181: Configuratie van VEEAM (13).....	103
Figuur 182: Configuratie van VEEAM (14).....	104
Figuur 183: Configuratie van VEEAM (15).....	104
Figuur 184: Configuratie van VEEAM (16).....	105
Figuur 185: Configuratie van VEEAM (17).....	105
Figuur 186: Configuratie van VEEAM (18).....	106
Figuur 187: Configuratie van VEEAM (19).....	106
Figuur 188: Configuratie van VEEAM (20).....	106
Figuur 189: Configuratie van VEEAM (21).....	107
Figuur 190: Installatie van zabbix (1).....	109
Figuur 191: Installatie van zabbix (2).....	109
Figuur 192: Installatie van zabbix (3).....	110
Figuur 193: Configuratie van zabbix (1) .....	111
Figuur 194: Configuratie van zabbix (2) .....	111
Figuur 195: Configuratie van zabbix (3) .....	112
Figuur 196: Configuratie van zabbix (4) .....	113
Figuur 197: Configuratie van zabbix (5) .....	113
Figuur 198: Configuratie van zabbix (6) .....	113
Figuur 199: Configuratie van zabbix (7) .....	114
Figuur 200: Configuratie van zabbix (8) .....	114
Figuur 201: Configuratie van zabbix (9) .....	115
Figuur 202: Configuratie van zabbix (10) .....	115
Figuur 203: Zabbix graph filters (1).....	116
Figuur 204: Zabbix graph filters (2).....	116
Figuur 205: Syslog schema.....	117
Figuur 206: Installatie van grafana (1) .....	118
Figuur 207: Installatie van grafana (2) .....	119
Figuur 208: Installatie van loki (1).....	119
Figuur 209: Installatie van loki (2).....	121
Figuur 210: Grafana koppelen met loki (1).....	121
Figuur 211: Grafana koppelen met loki (2).....	122
Figuur 212: Grafana koppelen met loki (3).....	122
Figuur 213: Grafana koppelen met loki (4).....	122
Figuur 214: Grafana koppelen met loki (5).....	123
Figuur 215: Installatie van promtail (1) .....	123
Figuur 216: Installatie van promtail (2) .....	124
Figuur 217: Installatie van promtail (3) .....	124
Figuur 218: Installatie van promtail (4) .....	124
Figuur 219: Installatie van promtail (5) .....	124
Figuur 220: Installatie van promtail (6) .....	125
Figuur 221: Installatie van promtail (7) .....	125
Figuur 222: Installatie van promtail (8) .....	125
Figuur 223: Installatie van kiwi syslog manager (1) .....	125
Figuur 224: Installatie van kiwi syslog manager (2) .....	126
Figuur 225: Installatie van kiwi syslog manager (3) .....	126

## Automatisch toewijzen van een VLAN aan een gebruiker

Figuur 226: Installatie van kiwi syslog manager (4) .....	126
Figuur 227: Installatie van kiwi syslog manager (5) .....	127
Figuur 228: Installatie van kiwi syslog manager (6) .....	127
Figuur 229: Installatie van kiwi syslog manager (7) .....	127
Figuur 230: Installatie van kiwi syslog forwarder (1).....	128
Figuur 231: Installatie van kiwi syslog forwarder (2).....	128
Figuur 232: Installatie van kiwi syslog forwarder (3).....	129
Figuur 233: Installatie van kiwi syslog forwarder (4).....	129
Figuur 234: Installatie van kiwi syslog forwarder (5).....	130
Figuur 235: Installatie van kiwi syslog forwarder (6).....	130
Figuur 236: Installatie van kiwi syslog forwarder (7) .....	130
Figuur 237: Installatie van kiwi syslog forwarder (8) .....	131
Figuur 238: Installatie van kiwi syslog forwarder (9) .....	131
Figuur 239: Installatie van kiwi syslog forwarder (10).....	131
Figuur 240: Installatie van kiwi syslog forwarder (11).....	132
Figuur 241: Logs van kiwi syslog .....	132
Figuur 242: Logs geschreven naar bestanden .....	132
Figuur 243: Flowchart Powershell script .....	133
Figuur 244: Powershell script (1).....	134
Figuur 245: Dashboard aanmaken .....	134
Figuur 246: Dashboard importeren .....	135
Figuur 247: Dashboard importeren .....	135
Figuur 248: Grafana dashboard (1).....	135
Figuur 249: Dashboard met data .....	136
Figuur 250: Grafana variables (1).....	136
Figuur 251: Grafana variables (2).....	136
Figuur 252: FortiSwitch fysiek interface (1).....	137
Figuur 253: FortiSwitch fysiek interface (2).....	138
Figuur 254: FortiSwitch fysiek interface (3).....	138
Figuur 255: FortiSwitch Interfaces (1) .....	139
Figuur 256: FortiSwitch Interfaces (2) .....	139
Figuur 257: FortiSwitch hostname.....	140
Figuur 258:FortiSwitch NTP .....	140
Figuur 259: FortiSwitch Radius.....	141
Figuur 260: FortiSwitch Radius (2) .....	141
Figuur 261: FortiSwitch Radius (3) .....	141
Figuur 262: FortiSwitch Radius (4) .....	142
Figuur 263: FortiSwitch Radius (5) .....	142
Figuur 264: FortiSwitch groepen aanmaken (1) .....	142
Figuur 265: FortiSwitch groepen aanmaken (2) .....	143
Figuur 266: FortiSwitch interface (1) .....	143
Figuur 267: FortiSwitch poortbeveiliging .....	144
Figuur 268: FortiSwitch configuratie syslog.....	146
Figuur 269: Aruba Switch hostname.....	146
Figuur 270: Aruba Switch hostname .....	147
Figuur 271: Aruba Switch Management VLAN.....	147

## Automatisch toewijzen van een VLAN aan een gebruiker

Figuur 272: Aruba Switch VLAN configuration op interface (1) .....	148
Figuur 273: Aruba Switch VLAN configuration op interface (2) .....	148
Figuur 274: Aruba Switch IP statisch instellen .....	148
Figuur 275: Aruba Switch poort configuratie (1) .....	149
Figuur 276: Aruba Switch poort configuratie (2) .....	149
Figuur 277: Aruba Switch Radius configuratie (1).....	150
Figuur 278: Aruba Switch Radius configuratie (2).....	150
Figuur 279: Aruba Swich poort toegangscontrole (1) .....	151
Figuur 280: Aruba Swich poort toegangscontrole (2) .....	151
Figuur 281: Aruba Swich poort toegangscontrole (3) .....	152
Figuur 282: Aruba Swich syslog configuratie (1) .....	152
Figuur 283: Aruba Switch configuratie saven .....	153
Figuur 284: FortiAnalyser niet-geauthoriseerde apparaten .....	154
Figuur 285: FortiAnalyser niet-geauthoriseerde apparaten autoriseren (1) .....	154
Figuur 286: FortiAnalyser niet-geauthoriseerde apparaten autoriseren (2).....	155
Figuur 287: FortiAnalyser niet-geauthoriseerde apparaten autoriseren (3).....	155
Figuur 288: FortiAnalyser Device Manager (1).....	155
Figuur 289: FortiAnalyser Device Manager (2).....	156
Figuur 290: FortiAnalyser Device Manager (3).....	156
Figuur 291: FortiAnalyser Device Manager (4).....	156
Figuur 292: FortiAnalyser Syslog .....	157
Figuur 293: FortiAnalyser Traffiek.....	157
Figuur 294: FortiAnalyser Bedreigingen (1) .....	158
Tabel 1: Test-scenarios Radius.....	159

## I. Voorwoord

Na een intensieve en leerzame periode van 13 weken, zijn wij verheugd om te presenteren wat we hebben bereikt met ons project gericht op het efficiënter en veiliger maken van netwerktoegang door middel van geautomatiseerde VLAN-toewijzing en geavanceerde logvisualisatie. Dit document biedt een uitgebreide beschrijving van onze aanpak en de implementatie van verschillende technologieën om een toekomstbestendige netwerkomgeving te realiseren.

In moderne netwerkomgevingen zijn veiligheid en efficiëntie cruciale factoren. Ons project richt zich op het optimaliseren van deze aspecten door het gebruik van netwerkapparatuur en -software. Centraal in deze implementatie staan diverse belangrijke componenten zoals de Fortigate Firewall, de domein controller, de RADIUS server, en netwerkapparatuur zoals Aruba Switches of FortiSwitches. Daarnaast speelt logbeheer en -visualisatie een cruciale rol, met tools zoals Kiwi Syslog van SolarWinds, Grafana, en FortiAnalyzer, die ons helpen bij het snel identificeren van trends, problemen en beveiligingsincidenten.

Dit project zou niet mogelijk zijn geweest zonder de steun en begeleiding van onze collega's. Daarnaast ook het aanmaken van de labo-omgeving door Dieter V. Daarnaast willen we ook Fons N. bedanken voor het voorzien van de middelen en het vertrouwen om dit project tot een succes te maken.

## Automatisch toewijzen van een VLAN aan een gebruiker

## 2. Inleiding

In de moderne netwerkomgevingen, waar veiligheid en efficiëntie cruciale factoren zijn, is het automatisch toewijzen van VLANs aan gebruikers een noodzakelijke verbetering. Dit project richt zich op het efficiënt laten verlopen en beveiligen van netwerktoegang door gebruik te maken van netwerkapparatuur en -software.

Centraal in deze implementatie staan verschillende belangrijke componenten. De Fortigate Firewall biedt een beveiligingslaag voor ons netwerk en fungeert als de eerste verdedigingslinie tegen ongeautoriseerde toegang en bedreigingen. De domein controller beheert gebruikersauthenticatie en -autorisatie, en speelt een cruciale rol in het toewijzingsproces van VLANs door gebruikers te verifiëren. De RADIUS server (Remote Authentication Dial-In User Service) is verantwoordelijk voor de centrale authenticatie, autorisatie en accounting van gebruikers. Deze server integreert met de domein controller en helpt bij het automatisch toewijzen van VLANs op basis van gebruikersrollen en beleidsregels. De Aruba Switch of FortiSwitch maakt dynamische netwerksegmentatie mogelijk door VLANs automatisch toe te wijzen aan gebruikers zodra ze zich aanmelden, wat zorgt voor een efficiënte en veilige netwerkstructuur.

Naast de netwerkcomponenten speelt logbeheer en -visualisatie een cruciale rol in dit project. Kiwi syslog van SolarWinds wordt gebruikt om alle syslogs te verzamelen van de verschillende netwerkapparaten. Het zorgt voor een gecentraliseerde opslag van loggegevens, wat essentieel is voor netwerkbeheer en -monitoring. Met Grafana worden de verzamelde loggegevens gevisualiseerd, wat helpt bij het snel identificeren van trends, problemen en beveiligingsincidenten. Deze visuele weergave maakt het netwerkbeheer intuïtiever en proactiever.

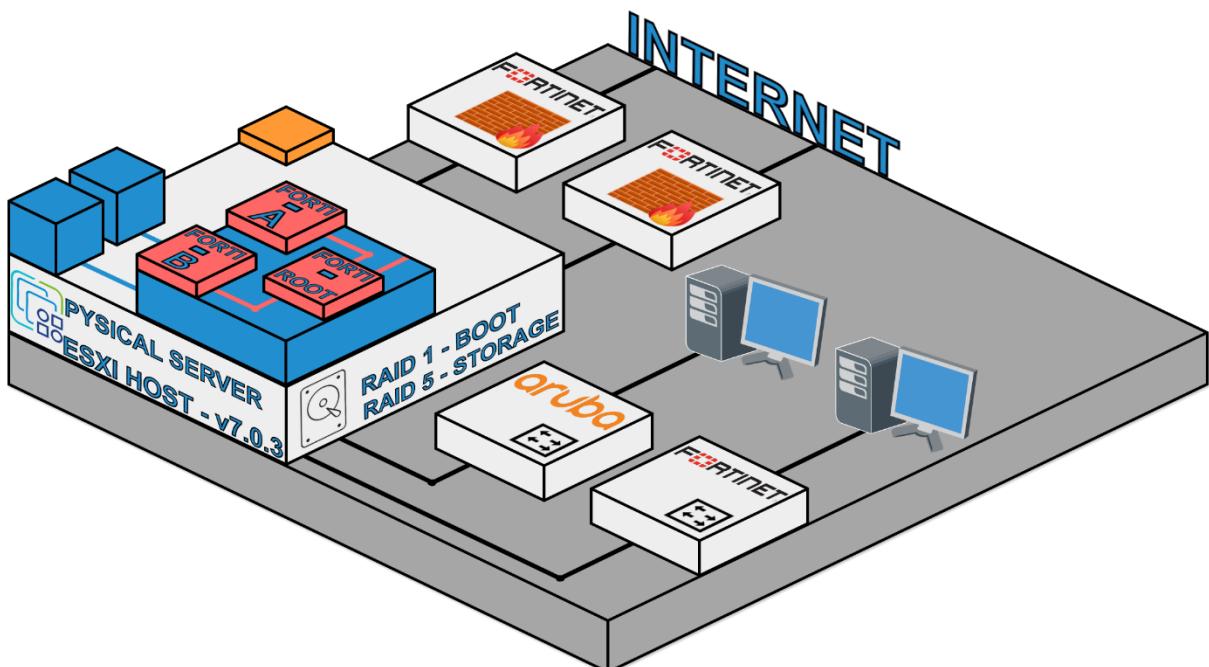
Daarnaast wordt FortiAnalyzer ingezet voor uitgebreide analyse en rapportage van loggegevens. FortiAnalyzer biedt geavanceerde mogelijkheden voor het correleren van loggegevens en kan gedetailleerde rapporten genereren, wat helpt bij het identificeren van bedreigingen en het naleven van beveiligingsbeleid.

Het doel van dit project is om een efficiënte, veilige en eenvoudig beheren van een netwerkomgeving te creëren door middel van geautomatiseerde VLAN-toewijzing en geavanceerde logvisualisatie. Met behulp van de genoemde technologieën kunnen we niet alleen de operationele efficiëntie verbeteren, maar ook de algehele netwerkbeveiliging versterken.

Door de combinatie van deze krachtige tools en technieken, zetten we een belangrijke stap richting een toekomstbestendig netwerkbeheer. Ik nodig u uit om door dit document te bladeren en de gedetailleerde aanpak en implementatie van dit innovatieve project te ontdekken.

## Automatisch toewijzen van een VLAN aan een gebruiker

### **3. Fysieke setup**



Figuur 1: Fysieke setup

Kijken we naar de setup, dan zien we een fysieke server, deze heeft twee schijven in raid één staan. Deze schijven zullen voor het boot en besturingssysteem zorgen. Het gebruik maken van twee schijven zorgt voor failover: als er één van de twee uitvalt heb is er de andere schijf nog. De rest van de schijven staan geconfigureerd in raid vijf. Dit is de storage van de virtuele machines die we later bespreken en configureren in de documentatie.

Deze fysieke server heeft vier poorten. Twee poorten hiervan zijn verbonden met een switch van CISA, zodat deze naar buiten kunnen (de twee fortinet firewalls, staan in high availability), Een van de poorten is voor Labo A en de andere voor Labo B. De andere twee poorten zijn voor de switch waar we de VLAN toewijzing zullen gaan doen. Hier hangen ook computers aan zodat we onze configuraties kunnen testen. Hieronder zie je de setup in het prep lokaal van beide labo's.



Figuur 2: Switches met aansluiting naar de laptops

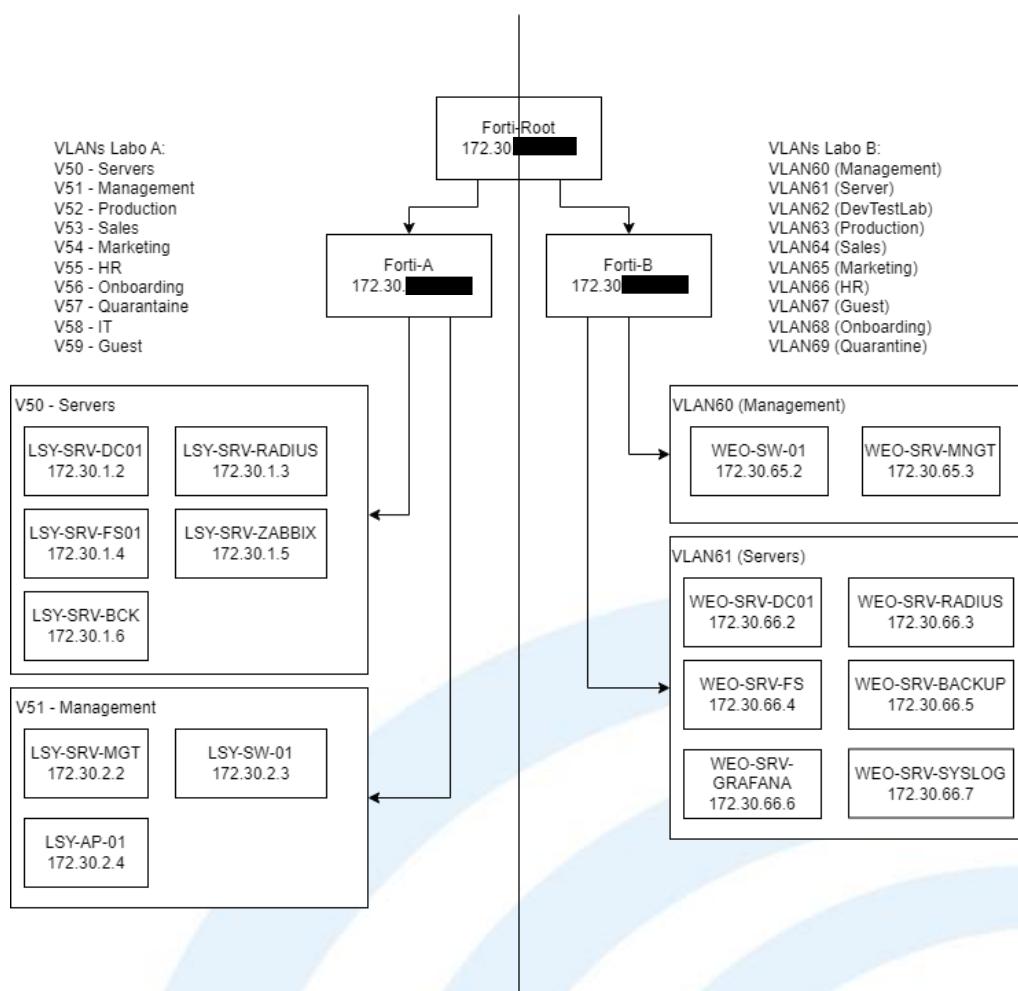
## Automatisch toewijzen van een VLAN aan een gebruiker

Als we dan verder gaan kijken naar wat er op de fysieke server staat zien we blauwe vakken. Dit stellen onze virtuele machines voor die we gaan integreren in het project, zoals een domain controller, radius server, fileserver, back-up server, ... .

Het grootste blok is de fortigate virtuele machine. Dit is de firewall die we gebruiken om het netwerk te controleren. Daarop zien we drie rode blokken dit zijn de virtuele domeinen (VDOM's). VDOM's worden gebruikt om een FortiGate op te delen in virtuele eenheden die onafhankelijk functioneren. VDOM's kunnen afzonderlijk beveiligingsbeleid bieden en, in de NAT-modus, volledig afzonderlijke configuraties voor routering en VPN-services bieden voor elk verbonden netwerk.

Wij gebruiken deze virtuele domeinen voor het aanmaken van onze eigen rules, interfaces(vlans), etc. Forti-ROOT wordt gebruikt door CISA om de VDOMs verder te beheren.

Daarnaast is dit de VLAN-indeling.

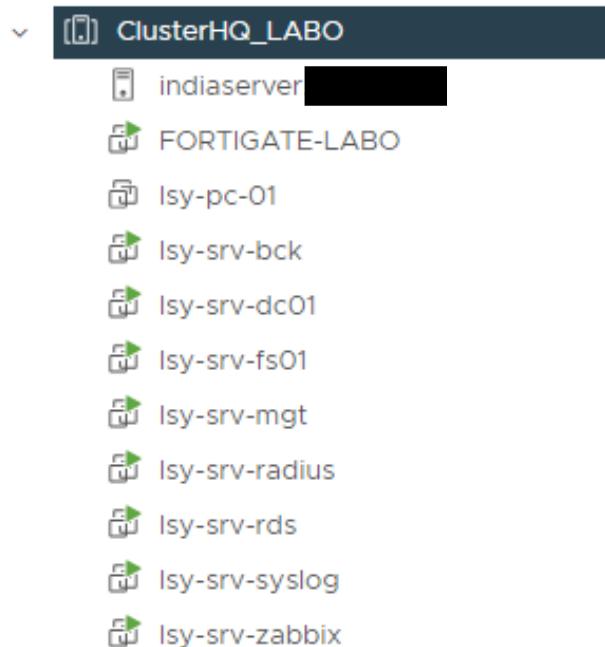


Figuur 3: Netwerk indeling

## Automatisch toewijzen van een VLAN aan een gebruiker

### 4. vSphere

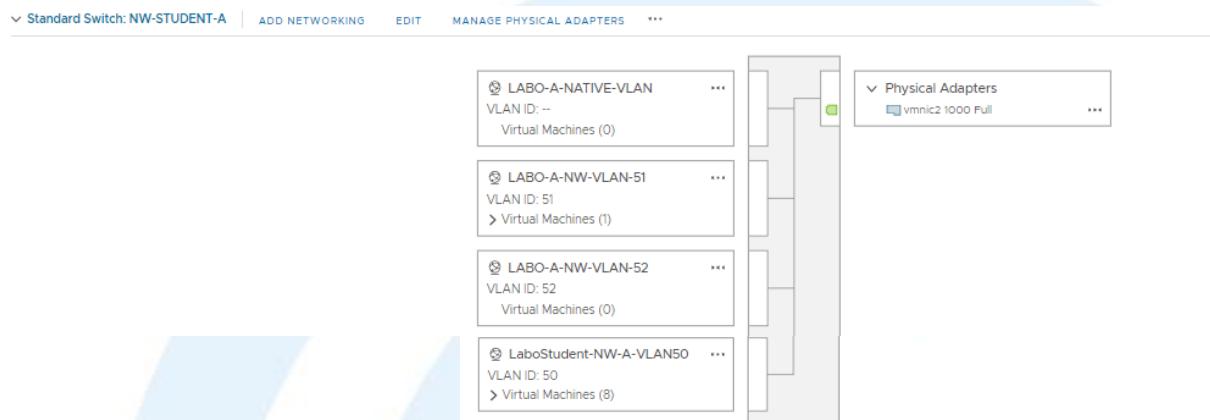
We gebruiken vSphere om de servers aan te maken en te beheren. Het cluster dat we gebruiken is van het labo. Zoals te zien op onderstaande afbeeldingen staan onze virtuele machines op dit cluster (ClusterHQ\_Labo) en de Indiaserver:



Figuur 4: vSphere virtuele machines

#### 4.1 Virtuele Switches

Om de connectie van virtuele machines naar fysieke setups te hebben, zetten we virtuele switchen op in de vSphere.



Figuur 5: vSphere opstelling van de virtuele switch

## Automatisch toewijzen van een VLAN aan een gebruiker

Dit is hetzelfde voor beide labo omgevingen met aan de ene kant een fysieke adapter waar de switches aan hangen. Aan de andere kant hebben we alle VLAN's zodat trafiek dat van de fysieke LAN-kant komt ook weet naar waar deze moet of kan gaan, en natuurlijk andersom is dit ook zo om van de virtuele naar de fysieke kant te gaan. Voor Labo A is dit VLAN 50-59 en voor Labo B is dit VLAN 60-69.

Om de instellingen van de switch goed te zetten om het mogelijk te maken voor virtuele inter VLAN routing, drukt men op 'edit' van de switch.

▼ Standard Switch: NW-STUDENT-A | ADD NETWORKING | **EDIT** | MANAGE PHYSICAL ADAPTERS | ...

Figuur 6: vSphere aanmaken van een virtuele switch (1)

Als we naar de properties van de switch gaan kijken zien we bij security enkele modussen. Zoals te zien bij figuur 7 zullen deze allemaal aangepast moeten worden naar 'accept'.

### NW-STUDENT-A - Edit Settings

Properties	
<b>Security</b>	Promiscuous mode      Accept
Traffic shaping	MAC address changes      Accept
Teaming and failover	Forged transmits      Accept

Figuur 7: vSphere aanmaken van een virtuele switch (2)

Promiscuous mode is een security policy die wordt gedefineerd op virtuele switch of poort group niveau. Wie de promiscuous mode toestaat, kan al het netwerkverkeer zien dat erdoor gaat. Forged transmits zullen ervoor zorgen dat de ESXi niet de bron en effectief MAC-adres zal controleren. MAC-adres change zal de virtele machine toelaten om frames te verkrijgen van een MAC-adres dat anders is dan de geconfigureerd in de VMX (virtual machine configuration files). Door forged transmits en MAC-adres veranderingen aan te zetten verhoog men wel de kans voor MAC-spoofing.

Het toevoegen van extra networking kan via de knop 'add networking'. Bij het selecteren van connectie type, kies hier voor 'virtual machine port group for a standard switch'. Druk na het kiezen op next.

## Automatisch toewijzen van een VLAN aan een gebruiker

Indiaserver.cisanet.be - Add Networking X

**1 Select connection type** Select connection type

2 Select target device Select a connection type to create.

3 Connection settings

4 Ready to complete

VMkernel Network Adapter  
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

Virtual Machine Port Group for a Standard Switch  
A port group handles the virtual machine traffic on standard switch.

Physical Network Adapter  
A physical network adapter handles the network traffic to other hosts on the network.

CANCEL BACK NEXT

Figuur 8: vSphere aanmaken van een virtuele switch (3)

Als we op de knop ‘add networking’ drukken bij de correcte switch staat die al goed. Zo niet, kan men via de browse knop de juiste switch selecteren.

indiaserver.cisanet.be - Add Networking X

✓ 1 Select connection type Select target device

**2 Select target device** Select a target device for the new connection.

3 Connection settings

4 Ready to complete

Select an existing standard switch  
NW-STUDENT-A BROWSE ...

New standard switch

MTU (Bytes) 1500

CANCEL BACK NEXT

Figuur 9: vSphere aanmaken van een virtuele switch (4)

Na de selectie van een bestaande switch ga je de connectie settings aanpassen. Je geeft het een naam naar keuze, de X is het vlan ID dat je graag wil gebruiken in de opstelling.

## Automatisch toewijzen van een VLAN aan een gebruiker

indiaserver.cisanet.be - Add Networking X

<span style="color: green;">✓</span> 1 Select connection type <span style="color: green;">✓</span> 2 Select target device <b>3 Connection settings</b> 4 Ready to complete	<b>Connection settings</b> Use network labels to identify migration-compatible connections common to two or more hosts.  Network label: LABO-A-NW-VLAN-X VLAN ID: X <span style="color: red;">!</span>
---	--

CANCEL
NEXT

Figuur 10: vSphere aanmaken van een virtuele switch (5)

Daarna klikt u op next en ziet u een overzicht van wat uw net heeft meegegeven, of de poort die u gaat aanmaken op de switch. Op dit scherm kan u op ‘finish’ drukken om de poort groep aan te maken.

## 4.2 Templates

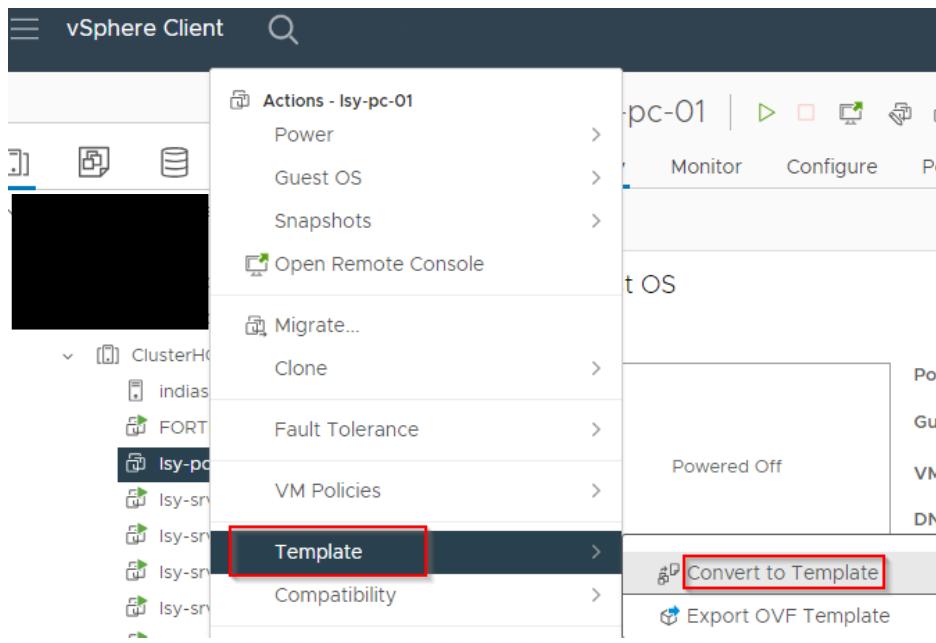
We hebben een template gemaakt van een Windows Server 2022 om het makelijker te maken om een nieuwe server te deployen. Hiervoor hebben we een installatie van Windows Server 2022 gedaan en deze gesysprepped.

Een sysprep zal ervoor zorgen dat de server wordt gegeneraliseerd, dit wil zeggen dat de unieke systeem informatie zoals security identifiers (SIDs) en computernamen worden verwijderd. Dit zorgt ervoor dat het systeem kan worden geimed en deployed met een nieuwe, unieke identiteit.

Voor het het syspreppen openen we de opdrachtenprompt als administrator. Daarna navigeren we met het commando cd naar het pad “C:\Windows\System32\Sysprep”. En hier voeren we sysprep.exe uit. In het scherm van deze tool kiezen we voor “Out-of-Box Experience” en selecteren we ook de box naast Generalize. Daarna kiezen we hier voor shutdown in de shutdown opties en klikken op OK om het sysprep proces te starten.

## Automatisch toewijzen van een VLAN aan een gebruiker

Voor het aanmaken van een template in vCenter drukken de rechter muisknop op de virtuele machine in. Hier kiezen we template en daarna convert to template zoals te zien in onderstaande figuur 11.



Figuur 11: vSphere aanmaken van een template

Na het klikken op convert to template zal je een scherm krijgen om te bevestigen dat je deze virtuele machine wilt converteren. Als je virtuele machine gesysprepped is druk je op yes.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 5. FortiGate firewall

De opzet tot een met het aanmaken van de virtuele domeinen is gedaan door CISA. Vanaf toen zijn wij aan de slag gegaan met het aanmaken van VLANs, het configureren van DHCP, het aanmaken van virtuele IP en groepen om connectie te maken vanuit CISA met de servers van de labo-omgeving. Daarnaast maken we ook firewall policies regels aan om het netwerk te beheren.

#### 5.1 Interfaces

In de onderstaande afbeelding zien we momenteel alleen poort 2, wat de fysieke interface is. Poort 2 van de fysieke server is verbonden met de switch in het voorbereidingslokaal, zoals te zien is op de foto van de fysieke opstelling.

Physical Interface (1)								
	Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Virtual Domain
	port2	Physical Interface		172.30.0.1/255.255.255.0	PING			LABO-A 10

Figuur 12: Fortigate firewall fysieke poort

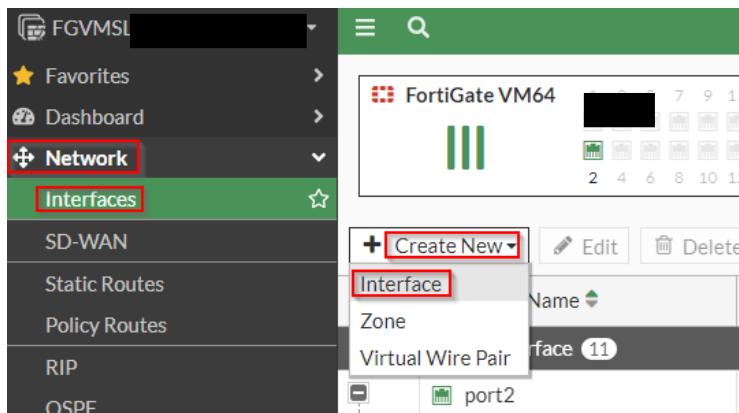
We zullen op deze poort de VLANs aanmaken waarmee we graag willen werken.

Physical Interface (1)								
	Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Virtual Domain
	port2	Physical Interface		172.30.0.1/255.255.255.0	PING			LABO-A 10
•	V50 Servers	VLAN		172.30.1.1/255.255.255.0	PING HTTPS SNMP HTTP	7	172.30.1.2-172.30.1.254	LABO-A 25
•	V51 Management	VLAN		172.30.2.1/255.255.255.0	PING HTTPS SSH HTTP Security Fabric Connection	2	172.30.2.2-172.30.2.254	LABO-A 9
•	V52 Production	VLAN		172.30.3.1/255.255.255.0	PING		172.30.3.2-172.30.3.254	LABO-A 5
•	V53 Sales	VLAN		172.30.4.1/255.255.255.0	PING		172.30.4.2-172.30.4.254	LABO-A 5
•	V54 Marketing	VLAN		172.30.5.1/255.255.255.0	PING		172.30.5.2-172.30.5.254	LABO-A 5
•	V55 HR	VLAN		172.30.6.1/255.255.255.0	PING	1	172.30.6.2-172.30.6.254	LABO-A 4
•	V56 Onboarding	VLAN		172.30.7.1/255.255.255.0	PING		172.30.7.2-172.30.7.254	LABO-A 4
•	V57 Quarantine	VLAN		172.30.8.1/255.255.255.0	PING		172.30.8.2-172.30.8.254	LABO-A 4
•	V58 IT	VLAN		172.30.9.1/255.255.255.0	PING HTTPS HTTP		172.30.9.2-172.30.9.254	LABO-A 5
•	V59 Guest	VLAN		172.30.10.1/255.255.255.0			172.30.10.2-172.30.10.254	LABO-A 3

Figuur 13: Fortigate firewall vlan overzicht

Voor het aanmaken van een VLAN op de fortigate, klik je op ‘Netwerk’, daarna op ‘Interfaces’. Hier druk je op de knop ‘Create New’ en kies je in de drop-down voor ‘Interface’.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 14: Fortigate firewall aanmaken VLAN (I)

We kiezen een naam voor de VLAN. We vonden het hier duidelijker om te werken via V(ID) (Naam) (bv. V50 Servers). Deze lijn trekken we door voor alle VLAN's die zijn aangemaakt.

De interface die we kiezen is voor ons de connectie van de fysieke server met de switch. Daarna geef je het VLAN id mee dat je wilt gebruiken. Vanuit CISA kregen we VLAN 50-59 voor Labo A en VLAN 60-69 voor Labo B. Het IP-adres dat je ingeeft is het IP-adres van de firewall van de VLAN of de default gateway.

Voor administratieve toegang kiezen we voor HTTP(s), ping en SNMP zodat we aan de gebruikersinterface van de firewall kunnen en natuurlijk ping voor eventuele debug. SNMP hebben we hier geactiveerd voor de integratie met Zabbix. Dit is nu aangepaast naar HTTPS.

## Automatisch toewijzen van een VLAN aan een gebruiker

Edit Interface

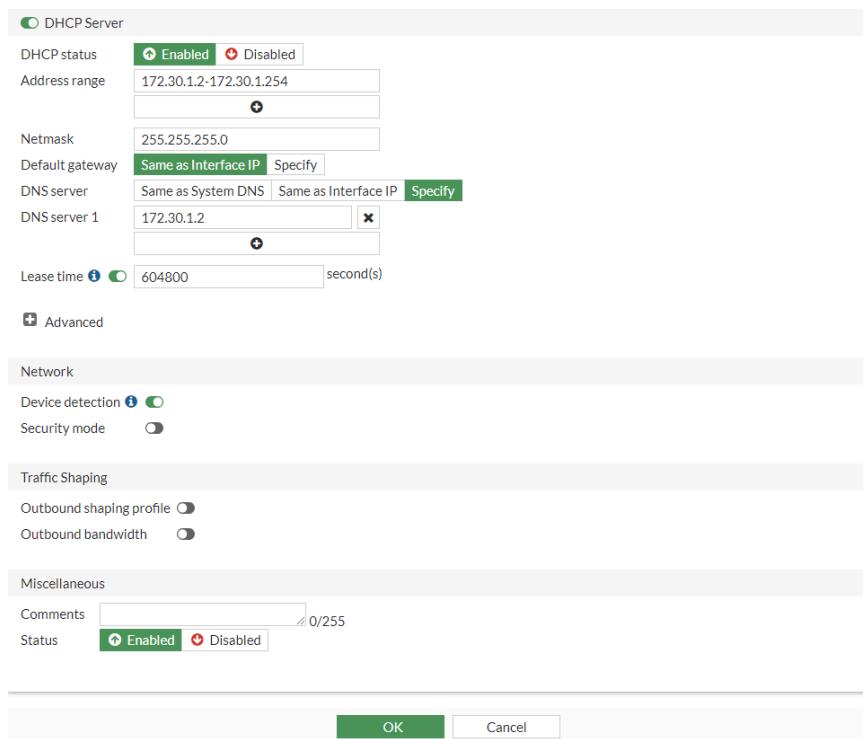
Name	V50 Servers		
Alias	VLAN		
Type	VLAN		
VLAN protocol	802.1Q		
Interface	port2		
VLAN ID	50		
VRF ID	0		
Virtual domain	LABO-A		
Role	LAN		
Address			
Addressing mode	<b>Manual</b>		
IP/Netmask	172.30.1.1/255.255.255.0		
Create address object matching subnet	<input checked="" type="checkbox"/>		
<small>The interface-subnet address associated to this interface is currently in use and will not be deleted.</small>			
Name	V50 Servers address		
Destination	172.30.1.0/24		
Secondary IP address	<input type="radio"/>		
Administrative Access			
IPv4	<input checked="" type="checkbox"/> HTTPS <input type="checkbox"/> FMG-Access <input type="checkbox"/> FTM	<input checked="" type="checkbox"/> HTTP <small>i</small> <input type="checkbox"/> SSH <input type="checkbox"/> RADIUS Accounting	<input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> Security Fabric Connection <small>i</small>
	<input type="checkbox"/> Speed Test		

Figuur 15: Fortigate firewall aanmaken VLAN (2)

Daarnaast configureren we ook een DHCP server die automatisch de IP-adressen zal verdelen over bepaalde leaseperioden. We specificeren ook de DNS server: dit is de domein controller die onze DNS zal beheren.

Hou voor de DHCP wel rekening met welke VLAN je de DNS server zult implementeren omdat niet alle VLAN's toegang nodig hebben tot de domein controller.

## Automatisch toewijzen van een VLAN aan een gebruiker



*Figuur 16: Fortigate firewall aanmaken VLAN (3)*

### 5.2 VLAN-indeling

Voor de VLAN-indelingen kreeg elk Labo tien VLANs om te gebruiken. Voor Labo A was dit 50 tot en met 59, voor Labo B 60 tot en met 69. We delen deze als volgt op.

We gebruiken één VLAN om onze servers in te zetten. Dit gaat dan over de virtuele machines zoals de domain controller, radius server, fileserver enzovoort.

Daarnaast gebruiken we een management VLAN om een management server in te plaatsen en de netwerk apparatuur zodat deze allemaal gemanaged kunnen worden door de management server. De management VLAN krijgt ook de toegang tot de andere VLANs.

Daarnaast hebben we VLANs die specifiek zijn toegewezen aan verschillende afdelingen binnen het bedrijf, zoals productie, verkoop, marketing, HR en IT. We hebben deze VLANs gekozen om nauwkeurige controle te hebben over welke afdeling toegang heeft tot welke specifieke resources, zoals de fileserver voor IT, voor HR of Sales, en andere toepassingen zoals afdeling specifieke servers.

Verder hebben we nog een onboarding VLAN. Dit VLAN zal zorgen voor de mogelijkheid om nieuwe PC's klaar te maken voor het bedrijf. Deze kan enkel en alleen communiceren met de domain controller.

## Automatisch toewijzen van een VLAN aan een gebruiker

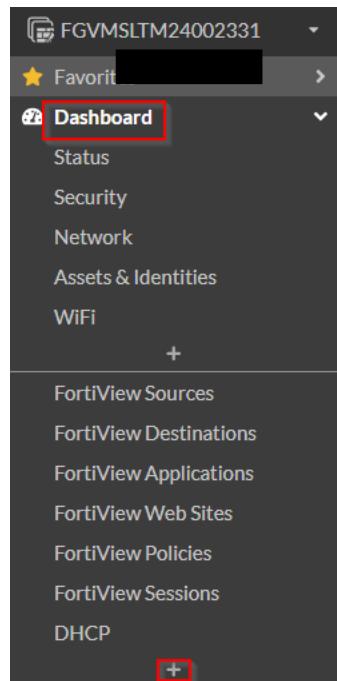
We hebben ook een quarantaine VLAN voorzien. Indien er PCs geïnfeceteerd worden met een virus, of zouden er rogue devices worden aangesloten op het netwerk zullen deze in het quarantaine netwerk geplaatst worden om zo de schade te beperken.

Als laatste beschikken we ook nog over een gast-netwerk of VLAN. Er komen altijd mensen langs die niet tot het bedrijf behoren. Dezen zullen enkel de mogelijkheid krijgen om naar het internet te gaan. In onze opstelling gaat dit alleen maar met draadloos netwerk.

### 5.3 DHCP

Zoals hierboven beschreven hebben we op de interface VLAN DHCP geconfigureerd. Wij zullen dus DHCP gebruiken via de fortigate en niet via een DHCP server. Binnen de fortigate verkrijg je een heel goed overzicht over welke IP-adressen geleased zijn, welke hiervan gereserveerd zijn, daarnaast kan je ook met het cirkeldiagram filteren op de bepaalde VLANs.

Maar dit dashboard kan je niet zomaar zien. Dit zal je in de fortigate eerst moeten aanzetten voor je het kan bekijken. Dit kan je doen door te navigeren naar Dashboard in de fortigate en daarna op het plusteken te drukken. Als je je muis houdt op het plusteken dan zal dit vragen om een monitor toe te voegen aan de fortigate.



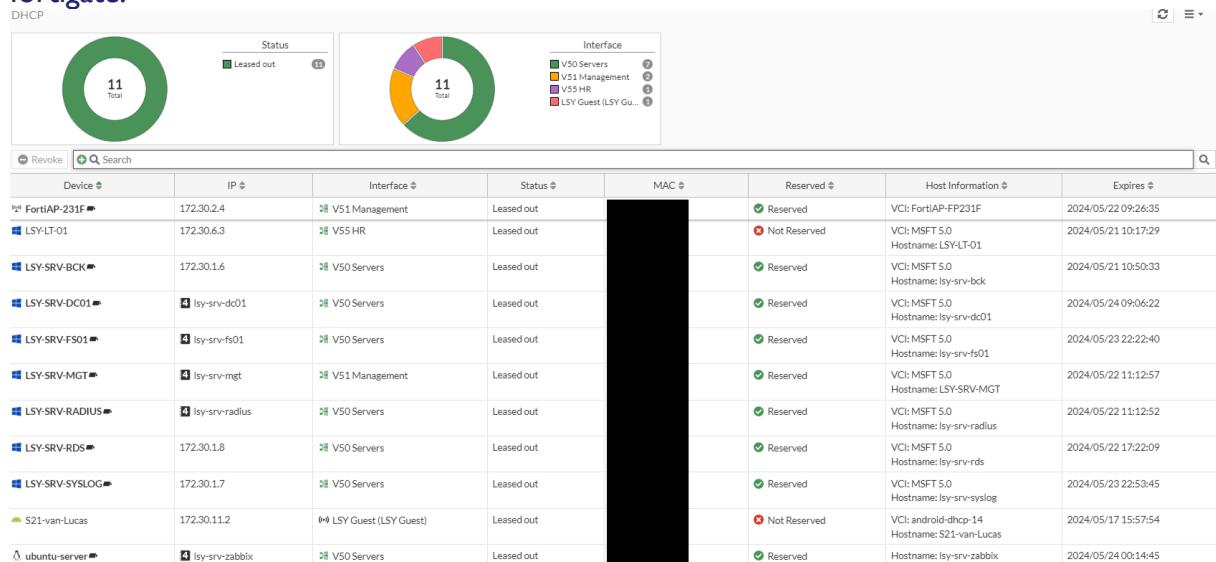
Figuur 17: Fortigate firewall menu

Eenmaal als je hier op hebt gedrukt komt er een extra scherm tevoorschijn waar je heel wat extra monitors kunt toevoegen aan de fortigate. In de zoekbalk kan je zoeken op DHCP of kan je door scrollen naar het netwerk. Dan klik je op DHCP, je geeft dit een naam en kiest u

## Automatisch toewijzen van een VLAN aan een gebruiker

de fortigate. Deze zou normaal al goed staan. Eenmaal als je op ‘Done’ hebt gedrukt zou er een monitor aan toegevoegd zijn. Als je deze opent verkrijg je extra informatie van je DHCP.

Bovenaan zie je een zoekbalk via hier kan je zoeken naar MAC-adressen of andere zaken. Daarnaast kan je ook zelf filters toevoegen, en je kan ook filteren door op het circkeldiagram te drukken. Daarnaast zie je nog andere informatie zoals hostnames, lease periodes, IP-adres. Maar het is ook mogelijk om hier een adres te zien, dit zijn geconfigureerde adressen in de fortigate.

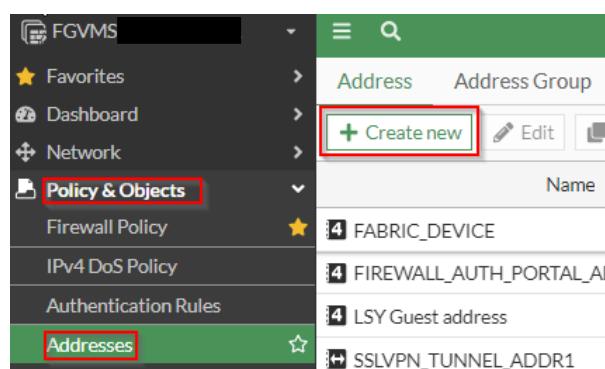


Figuur 18: Fortigate firewall DHCP overzicht

## 5.4 Adressen

Adressen worden aangemaakt in de fortigate om in de firewall policy regels te plaatsen aangezien hier geen IP-adressen kunnen worden genoteerd.

Het aanmaken van adressen gaat ook tijdens het maken van firewall policy regels of via de addresses tab onder policy & objects zelf.



Figuur 19: Fortigate firewall aanmaken van IP-adres (I)

## Automatisch toewijzen van een VLAN aan een gebruiker

Voor het aanmaken van een adres kies je een naam waarvan je weet wat deze inhoudt, en koppelt hier het interface aan waar deze staat. Je geeft het IP-adres en netmask aan. We kiezen in het voorbeeld hieronder voor het IP van de domain controller en daarnaast een netmask dat gelijk is aan prefix /32 of te wel enkel dit IP-adres.

Edit Address

Name	Isy-srv-dc01
Color	<input type="button" value="Change"/>
Interface	V50 Servers
Type	Subnet
IP/Netmask	172.30.1.2 255.255.255.255
Static route configuration	<input checked="" type="radio"/>
Comments	Write a comment... <span style="float: right;">0/255</span>

Figuur 20: Fortigate firewall aanmaken van IP-adres (2)

## 5.5 Virtual IPs

Als je van buiten het netwerk naar een server via RDP of SSH wil gaan, kan je ook gebruik maken van andere services. Dit gebruiken wij om gemakkelijk aan onze eigen servers of tools te kunnen vanuit het CISA-netwerk. Dit zal gaan via port forwarding, of poorten openzetten naar de buitenwereld. Het is aanbevolen om dit te doen door gebruik te maken van virtuele IP-adressen, zodat de interne zaken gemaskeerd blijven.

**NOTE:** Wel rekening houden dat je servers niet zomaar open zet naar de buitenwereld toe maar dit doen we vooral voor gemakkelijk te werken en omdat dit een test-omgeving is.

### 5.5.1 Configuratie virtuele IP (VIP)

Voor het aanmaken van een virtueel IP-adres kiezen we voor een naam die beschrijft waarvoor het virtuele IP-adres staat. Hier kiezen we voor de interface: in ons geval is dit de link naar de root VDOM of terwijl als het verkeer van WAN-kant naar LAN-kant komt.

We configureren het externe IP-adres naar het IP-adres van de firewall. Daarna mappen we dit naar het interne IP-adres. We zetten hier ook port forwarding op: dit zal ervoor zorgen dat wij het IP-adres van de firewall en de poort die staat bij externe service port kunnen verbinden vanuit het CISA netwerk met de virtuele machines, in dit geval de domein controller.

## Automatisch toewijzen van een VLAN aan een gebruiker

The screenshot shows the 'Virtual IP' configuration page. The 'Name' field is set to 'VIP-RDP-LABO-A-DC01'. Under the 'Network' section, the 'Interface' is 'LINK-ROOT-A1', 'Type' is 'Static NAT', and 'External IP address/range' is '172.30. [REDACTED]'. Under 'Port Forwarding', the 'Protocol' is 'TCP', 'Port Mapping Type' is 'One to one', 'External service port' is '3390', and 'Map to IPv4 port' is '3389'. At the bottom right, the 'OK' button is highlighted with a red box.

Figuur 21: Fortigate firewall aanmaken van VIP

Dit is een lijst van onze configuraties voor de virtuele IP-adressen:

Virtual IP						
Virtual IP		Virtual IP Group				
<a href="#">+ Create new</a>		<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Delete</a>	<a href="#">Search</a>	<a href="#">Export</a>
Name	Interface	Mapped From	Mapped To	Hit Count	Ref.	
VIP-RDP-LABO-A-DC01	LINK-ROOT-A1	172.30. [REDACTED]:3390)	172.30.1.2 (TCP: 3389)	0	1	
VIP-RDP-LABO-A-RADIUS	LINK-ROOT-A1	172.30. [REDACTED]:3391)	172.30.1.3 (TCP: 3389)	0	1	
VIP-RDP-LABO-A-MGT	LINK-ROOT-A1	172.30. [REDACTED]:3392)	172.30.2.2 (TCP: 3389)	212	1	
VIP-RDP-LABO-A-FS01	LINK-ROOT-A1	172.30. [REDACTED]:3393)	172.30.1.4 (TCP: 3389)	0	1	
VIP-SSH-LABO-A-ZABBIX	LINK-ROOT-A1	172.30. [REDACTED]:2222)	172.30.1.5 (TCP: 22)	7	1	
VIP-RDP-LABO-A-BCK	LINK-ROOT-A1	172.30. [REDACTED]:3394)	172.30.1.6 (TCP: 3389)	0	1	
VIP-RDP-LABO-A-SYLOG	LINK-ROOT-A1	172.30. [REDACTED]:3395)	172.30.1.7 (TCP: 3389)	0	1	
VIP-HTTP-LABO-A-ZABBIX	LINK-ROOT-A1	172.30. [REDACTED]:8080)	172.30.1.5 (TCP: 80)	0	1	
VIP-HTTPS-LABO-A-SYLOG	LINK-ROOT-A1	172.30. [REDACTED]:4430)	172.30.1.7 (TCP: 443)	0	1	
VIP-RDP-LABO-A-RDS	LINK-ROOT-A1	172.30. [REDACTED]:3396)	172.30.1.8 (TCP: 3389)	0	1	

Figuur 22: Fortigate firewall VIP overzicht

We hebben hier al onze windows servers in opgeliist. Daarnaast hebben we ook een zabbix server. Deze server is een linux ubuntu server, hier zullen we naartoe verbinden met SSH. Daarnaast is het ook makkelijk om het dashboard van zabbix en de web access van de kiwi syslog server rechtstreeks te zien via het CISA-netwerk en via het CISA-netwerk ook te werken. Daarom hebben we ervoor gekozen om deze poorten open te zetten.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 5.5.2 Configuratie virtuele IP groep (VIPG).

Daarnaast kiezen we er ook voor om de virtuele IP-adressen te groeperen in een virtuele IP-groep, per service en per VLAN. Dit zal ervoor zorgen dat je de firewall policy regels hier ook naartoe kunt configureren en beheren.

Name	Members	Interface	Ref.
VIPG-HTTP-V50-SERVERS	VIP-HTTP-LABO-A-ZABBIX VIP-HTTPS-LABO-A-SYSLOG	LINK-ROOT-A1	1
VIPG-RDP-V50-SERVERS	VIP-RDP-LABO-A-DC01 VIP-RDP-LABO-A-RADIUS VIP-RDP-LABO-A-FS01 VIP-RDP-LABO-A-BCK	LINK-ROOT-A1	1

Figuur 23: Fortigate firewall VIP groep overzicht

Voor het aanmaken van een virtuele IP groep kiezen we een naam die weergeeft wat deze doet, zodat het in de firewall policy regel duidelijk zal zijn wat deze doet. Daarnaast kiezen we ook een interface waar het verkeer binnen zal komen. Tot slot geven we ook de leden mee die tot deze groep zullen behoren.

Figuur 24: Fortigate firewall aanmaken van VIP groep

### 5.5.3 Firewall policy rule RDP, SSH, ...

Nu we de voorbereidingen hebben getroffen om te connecteren kunnen we momenteel nog niet connecteren naar onze server omdat hiervoor firewall policy rules ontbreken. Hieronder ziet u een overzicht van de regels die we hebben ingesteld.

LINK-ROOT-A1 → V50 Servers										
#	ID	Service	Action	Protocol	Port	Enabled	Profile	SSL	Inspection	Size
1	RDP-OUT-V50	all	VIPG-RDP-V50-SERVERS	always	RDP	✓ ACCEPT	Disabled	Standard	no-inspection	All 783.28 MB
13	SSH-OUT-V50	all	VIP-SSH-LABO-A-ZABBIX	always	SSH	✓ ACCEPT	Disabled	Standard	no-inspection	All 2.73 MB
18	HTTP-OUT-V50	all	VIPG-HTTP-V50-SERVERS	always	HTTP	✓ ACCEPT	Disabled	Standard	no-inspection	All 1.67 GB

LINK-ROOT-A1 → V51 Management										
#	ID	Service	Action	Protocol	Port	Enabled	Profile	SSL	Inspection	Size
3	RDP-OUT-V51	all	VIP-RDP-LABO-A-MGT	always	RDP	✓ ACCEPT	Disabled	Standard	no-inspection	All 425.81 MB

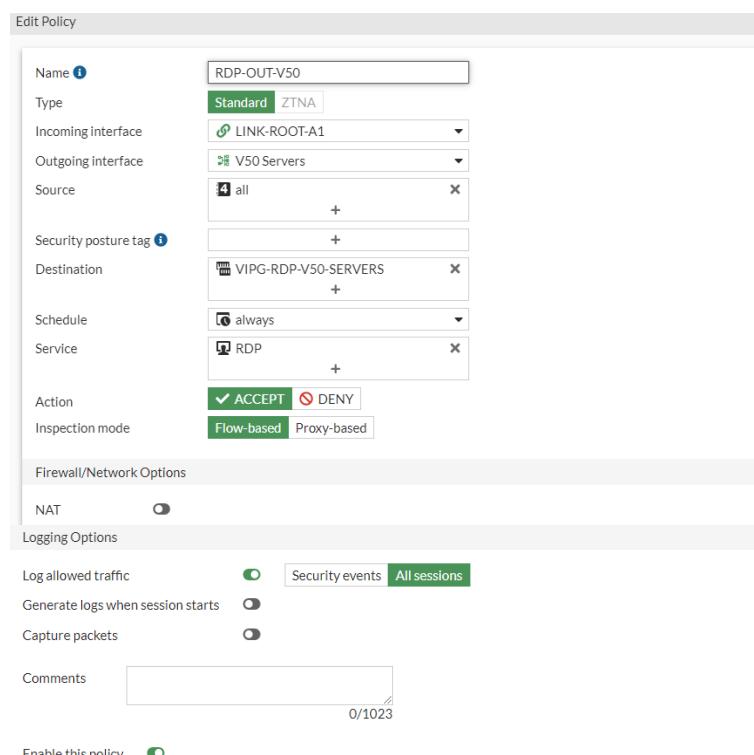
Figuur 25: Fortigate firewall policy overzicht

We kiezen voor een naam. We hebben hier gekozen om de service eerst te melden. In dit geval is dit RDP. Het verkeer komt van buiten naar VLAN 50 (Server VLAN). Het verkeer kan van overal komen en we gaan naar de virtuele IP-groep die als eerste is aangemaakt met

## Automatisch toewijzen van een VLAN aan een gebruiker

onze servers. We kunnen hier ook altijd kiezen om wanneer deze regel van kracht is hiervoor kan je ook nog altijd extra schedules maken onder policy & objects schedules. Momenteel is het altijd van kracht. We schakelen NAT uit. De adres informatie moet niet veranderd worden.

We kiezen bij de logging opties om alle sessies te loggen zodat we hier zeker via de logs kunnen monitoren.



The screenshot shows the 'Edit Policy' configuration window. The policy is named 'RDP-OUT-V50'. The configuration includes:

- Name:** RDP-OUT-V50
- Type:** Standard ZTNA
- Incoming interface:** LINK-ROOT-A1
- Outgoing interface:** V50 Servers
- Source:** all
- Destination:** VIPG-RDP-V50-SERVERS
- Schedule:** always
- Service:** RDP
- Action:** ACCEPT (checked)
- Inspection mode:** Flow-based

**Logging Options:**

- Log allowed traffic: Security events (selected)
- Generate logs when session starts: Off
- Capture packets: Off

**Comments:** (empty)

Figuur 26: Fortigate firewall aanmaken van een policy

## 5.6 Schedules

Als je graag een regels wil die enkel tijdens bepaalde dagen of uren beschikbaar is dan kan je hier altijd schedules voor aanmaken. Voor een schedule aan te maken kan je via policy & objects navigeren naar schedules. Als je hier bij recurring schedule een nieuwe aanmaakt door op create new te drukken, dan kom je op de onderstaande afbeelding terecht.

Als voorbeeld hebben we een schedule aangemaakt voor een werkweek. Nu kunnen we dit toepassen op regels, zodat de regels enkel maar van kracht zijn tijdens deze dagen en uren. Zie figuur 27.

Daarnaast heb je ook de mogelijkheid om een eenmalige planning te maken en groepen te maken van deze schedules.

## Automatisch toewijzen van een VLAN aan een gebruiker

Edit Schedule

Type	Recurring
Name	Working Week
Color	<span style="color: #0070C0;">Change</span>
Days	All days <span style="background-color: #00A050; color: white; padding: 2px 5px;">Specify</span>
	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday
	<input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday
	<input type="checkbox"/> Sunday
Time	All day <span style="background-color: #00A050; color: white; padding: 2px 5px;">Specify</span>
Start	06:00 <span style="border: 1px solid #ccc; padding: 2px 5px;">(i)</span>
Stop <span style="color: #0070C0;">(i)</span>	19:00 <span style="border: 1px solid #ccc; padding: 2px 5px;">(i)</span>

Figuur 27: Fortigate firewall aanmaken van een schedule

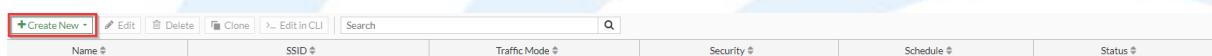
### 5.7 SSID (Service Set Identifier)

We willen graag draadloos netwerk met behulp van access points. Voor we dit kunnen doen zullen we eerst een service set identifier (SSID) aanmaken. Dit kunnen we zien als de naam van het netwerk. Om een SSID aan te maken in de fortigate navigeren we naar Wifi & Switch Controller. Hierin navigeren we naar SSID.



Figuur 28: Fortigate firewall aanmaken van SSID (1)

Als je in dit scherm bent aangekomen kan je een nieuwe SSID aanmaken via de knop 'Create New':



Figuur 29: Fortigate firewall aanmaken van SSID (2)

## Automatisch toewijzen van een VLAN aan een gebruiker

Hier gaan we onze nieuwe SSID aanmaken. Aangezien we ervoor kiezen om het netwerk van de gasten draadloos op te zetten maken we nu het SSID aan voor de gasten. We kiezen voor een gepaste naam. Daarna geef je ook een management poort mee met een vertrouwde host. Daarnaast geven je het IP-adres mee wat de default gateway gaat zijn voor dit netwerk. Als administratieve toegang geven we enkel ping. Van het gasten netwerk moet je niet aan de firewall geraken, ping kan wel helpen om debug redenen.

Figuur 30: Fortigate firewall aanmaken van SSID (3)

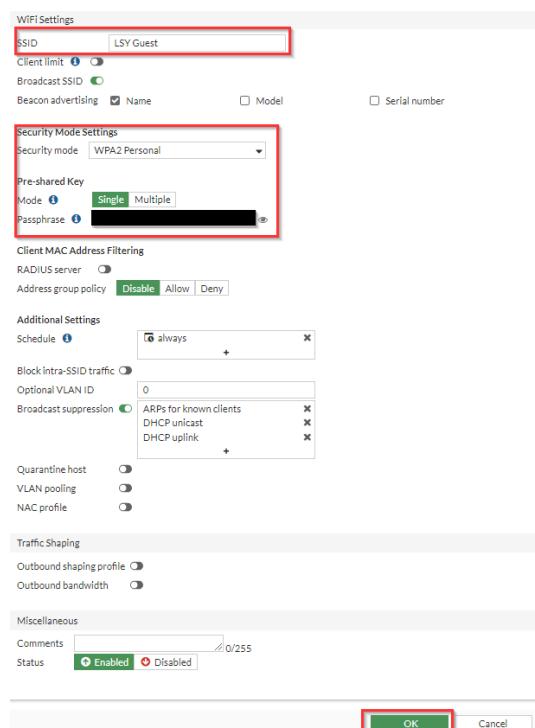
Daarnaast zal er van deze SSID ook een DHCP server zijn. Deze geeft in deze range – 172.30.11.2-254 - IP-adressen. Daarnaast is de DNS server 8.8.8.8 van Google. We kiezen voor een lease time van 28800s voordat de gebruikers een nieuwe aanvraag moeten doen. Deze tijd in seconde is 8 uur. Als gast zal je normaal niet langer dan een werkdag aanwezig zijn.

Figuur 31: Fortigate firewall aanmaken van SSID (4)

## Automatisch toewijzen van een VLAN aan een gebruiker

Uiteindelijk gaan we de WiFi settings zelf instellen. Als naam kiezen we voor ‘LSY guest’ kan ook een andere nuttige betekenisvolle naam zijn. Je kan er ook voor kiezen om een limiet van toestellen in te stellen, dit zal ervoor zorgen dat er een gelimiteerd aantal toestellen kunnen verbinden met het netwerk. De advertising – te voorschijn komen bij de WiFi settings van de client toestellen – gebeurt via de naam, je kan er ook voor kiezen om dit via model of serie nummer te doen.

Als security mode kiezen we ervoor om dit met een wachtwoord te doen. Hier geven we dan ook het wachtwoord mee dat je zal moeten ingeven bij het verbinden met de WiFi. Daarna druk je op OK.

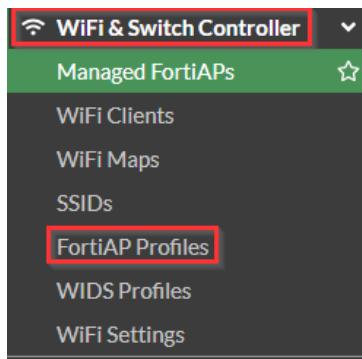


Figuur 32: Fortigate firewall aanmaken van SSID (5)

### 5.8 AP profiel

Met deze aangemaakt SSID ben je alleen niks. Om netwerk met FortiAPs beschikbaar te maken – zodat je kan verbinden met de WiFi - zal je eerst een AP profiel moeten aanmaken waar deze SSID in uitgezonden zullen worden. Hiervoor ga je ook naar WiFi & Switch Controller, vervolgens naar FortiAP profiles.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 33: Fortigate firewall aanmaken van AP (1)

Als je bent aangekomen bij de profielen van de APs, kan je een nieuw profiel aanmaken door te drukken op create new. We kiezen hier al voor een passende naam. We zetten een wachtwoord zodat dit voor elke AP waar dit profiel aan wordt gekoppeld hetzelfde is. De toegangen zijn HTTPS en SSH.

Name	Test-LSY-AP
Comments	Write a comment... 0/255
Platform	FAP231F
Dedicated scan	<input checked="" type="radio"/>
Indoor / Outdoor	<input checked="" type="radio"/> Default (Indoor) <input type="radio"/> Override Use default (Belgium)
Country / Region	<input checked="" type="radio"/> Belgium <input type="radio"/> Set <input type="radio"/> Leave Unchanged
AP login password	[REDACTED]
Administrative access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP
Client load balancing	<input type="checkbox"/> Frequency Handoff <input type="checkbox"/> AP Handoff
802.1X authentication	<input checked="" type="radio"/>

Figuur 34: Fortigate firewall aanmaken van AP (2)

Daarna komen we bij de configuratie van de radio's: dit zal de AP effectief uitstralen. Radio 1 is een band van 2.4 GHz en radio 2, 5 GHz. Hier koppelen we manueel de aangemaakte SSID aan toe, in mijn geval is dat het gast netwerk. Radio 3 houden we zoals default aangegeven op 'dedicated monitor'. Daarnaast houden we al de rest ook op default en drukken op OK om het profiel aan te maken.

## Automatisch toewijzen van een VLAN aan een gebruiker

Radio 1

Mode	<input type="button" value="Disabled"/> <input checked="" type="button" value="Access Point"/>
Radio resource provision	<input type="checkbox"/>
Band	2.4 GHz <input type="button" value="802.11ax/n/g"/>
Channel width	20MHz
Channel plan	<input type="button" value="Three Channels"/> <input type="button" value="Four Channels"/> <input type="button" value="Custom"/>
Channels	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13
Short guard interval	<input type="checkbox"/>
Transmit power mode	<input checked="" type="radio"/> <b>Percent</b> Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
Transmit power	<input checked="" type="radio"/> <b>dBm</b> Power is setting using a dBm value.
SSIDs	<input type="button" value="Tunnel"/> <input type="button" value="Bridge"/> <input checked="" type="button" value="Manual"/> (●) LSY Guest (LSY Guest) <input type="button" value="X"/> <input type="button" value="+"/>
Monitor channel utilization	<input type="checkbox"/>

Figuur 35: Fortigate firewall aanmaken van AP (3)

Radio 2

Mode	<input type="button" value="Disabled"/> <input checked="" type="button" value="Access Point"/>
Radio resource provision	<input type="checkbox"/>
Band	5 GHz <input type="button" value="802.11ax/ac/n/a"/>
Channel width	<input type="button" value="20MHz"/> <input checked="" type="button" value="40MHz"/> <input type="button" value="80MHz"/>
Channels	<input type="button" value="Set Channels"/> 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 149 153 157 161
Short guard interval	<input type="checkbox"/>
Transmit power mode	<input checked="" type="radio"/> <b>Percent</b> Transmit power is determined by multiplying set percentage with maximum available power determined by region and FortiAP device.
Transmit power	<input checked="" type="radio"/> <b>dBm</b> Power is setting using a dBm value.
SSIDs	<input type="button" value="Tunnel"/> <input type="button" value="Bridge"/> <input checked="" type="button" value="Manual"/> (●) LSY Guest (LSY Guest) <input type="button" value="X"/> <input type="button" value="+"/>
Monitor channel utilization	<input type="checkbox"/>

Radio 3

Mode	<input type="button" value="Disabled"/> <input checked="" type="button" value="Dedicated Monitor"/>
WIDS profile	<input type="checkbox"/>

LAN Port

Figuur 36: Fortigate firewall aanmaken van AP (4)

## Automatisch toewijzen van een VLAN aan een gebruiker

### 5.9 Acces point (AP)

Voor een access point is het belangrijk waar je dit gaat aansluiten. Wij doen dit in de switch op een poort die staat op de VLAN van management zodat deze een IP-adres krijgt die behoort tot het management VLAN. Wel is het belangrijk dat je op de VLAN waar je APs wilt opzetten de administratieve toegang ‘security fabric connection’ inschakelt.

	V51 Management	VLAN		172.30.2.1/255.255.255.0	PING HTTPS SSH HTTP Security Fabric Connection	2	172.30.2.2-172.30.2.254	LABO-A
--	----------------	------	--	--------------------------	--	---	-------------------------	--------

Figuur 37: Fortigate firewall V5 I overzicht

Daarna gaan we naar WiFi & Switch controller > Managed FortiAPs.



Figuur 38: Fortigate firewall autorizeren van AP (1)

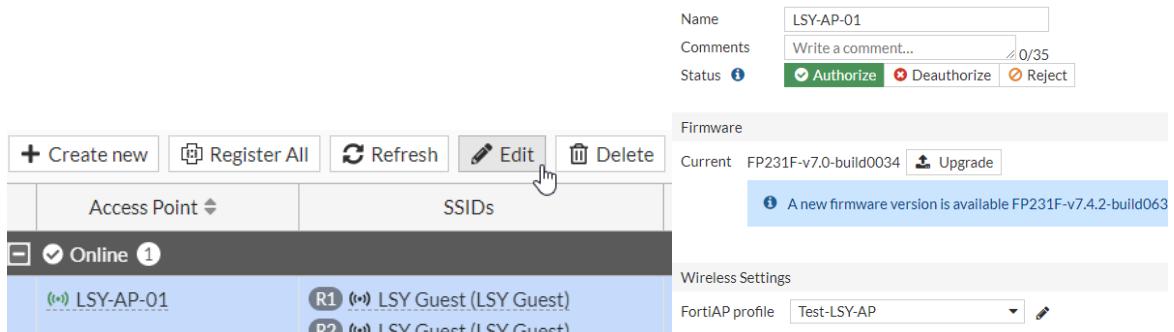
Hier zou je access point dan te komen staan. Dit zal je eerste moeten autorizeren door te drukken op de AP, daarna op de knop authorization en hier op authorize.

Access Point		SSIDs	Authorization				
<input checked="" type="checkbox"/>	Online 1		<input checked="" type="radio"/> Authorize	<input type="radio"/> Reject	<input type="radio"/> Deauthorize		
(W) LSY-AP-01	R1 (W) LSY Guest (LSY Guest)	R1 1	0	v7.0.0 build0034	Ian1:lsy-sw-01 - port1	Test-LSY-AP	V51 Management
	R2 (W) LSY Guest (LSY Guest)	R2 132					
	R3 N/A	R3 N/A					

Figuur 39: Fortigate firewall autorizeren van AP (2)

Na de autorisatie kunnen we de naam van de AP aanpassen door op de AP te drukken en daarna op edit. Hier kunnen we ook de status van AP veranderen. Bij wire settings voegen we het aangemaakte fortiAP profiel toe de rest kunnen we zoals default laten staan. Nadat dit gesaved wordt zal de AP rebooten om het nieuwe profiel aan te nemen.

## Automatisch toewijzen van een VLAN aan een gebruiker



The screenshot shows the Fortigate firewall interface for managing Access Points. At the top, there are buttons for 'Create new', 'Register All', 'Refresh', 'Edit' (with a cursor pointing to it), and 'Delete'. Below this is a table with columns 'Access Point' and 'SSIDs'. A row for 'LSY-AP-01' is selected, showing two SSIDs: 'R1 (••) LSY Guest (LSY Guest)' and 'R2 (••) LSY Guest (LSY Guest)'. In the top right, there's a 'Name' field set to 'LSY-AP-01', a 'Comments' field with placeholder 'Write a comment...', a 'Status' section with 'Authorize' checked, and buttons for 'Deauthorize' and 'Reject'. A 'Firmware' section shows 'Current' as 'FP231F-v7.0-build0034' with a 'Upgrade' button. A blue banner at the bottom right says 'A new firmware version is available FP231F-v7.4.2-build063'.

Figuur 40: Fortigate firewall autorizeren van AP (3)

## Automatisch toewijzen van een VLAN aan een gebruiker

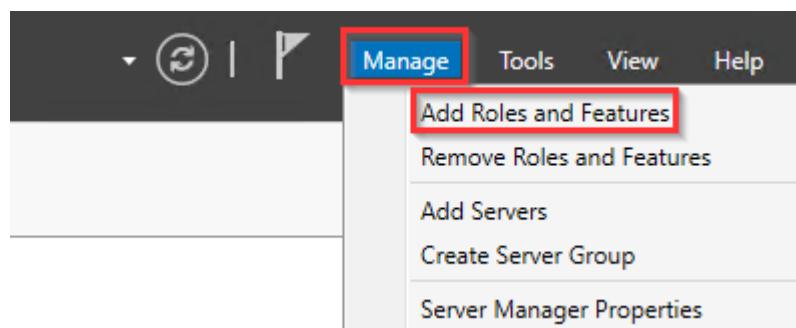
## 6. Virtuele servers

### 6.1 Domain controller

Een domein controller is een essentieel onderdeel in een netwerkbeheeromgeving. In onze opdracht gebruiken we dit voor centraal beheer van gebruikers en groepen. Daarnaast ook voor de beveiliging zoals groep policy, maar ook DNS. We hebben natuurlijk ook in elk labo een domein (LSY.be en WEO.be)

#### 6.1.1 Installatie AD

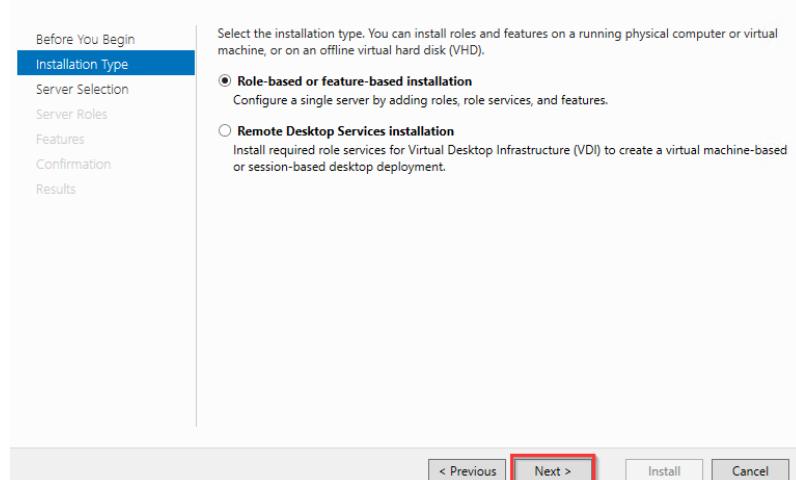
Voor het installeren van Active directory domein services navigeren we naar manage en daarna naar 'add roles and features'.



Figuur 41: Installatie van de DC (1)

We kiezen hier voor role-based or feature-based installatie en drukken daarna op next.

Select installation type



Figuur 42: Installatie van de DC (2)

Bij het selecteren kan je verder drukken op next. Dit zal normaal de server zijn die je graag wilt promoveren to domain controller. In het volgende scherm selecteer je de server rol,

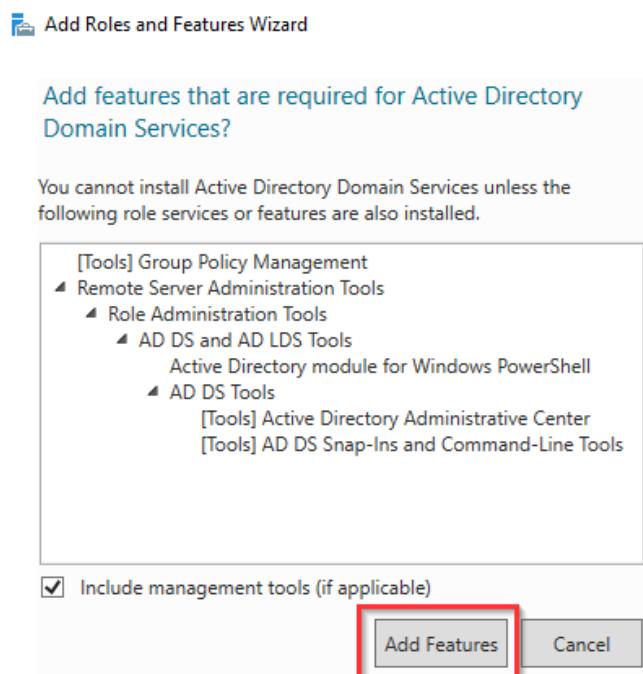
## Automatisch toewijzen van een VLAN aan een gebruiker

voor AD is dit active directory domain services. Daarnaast komt er een pop-up hier druk je op add features.

### Roles



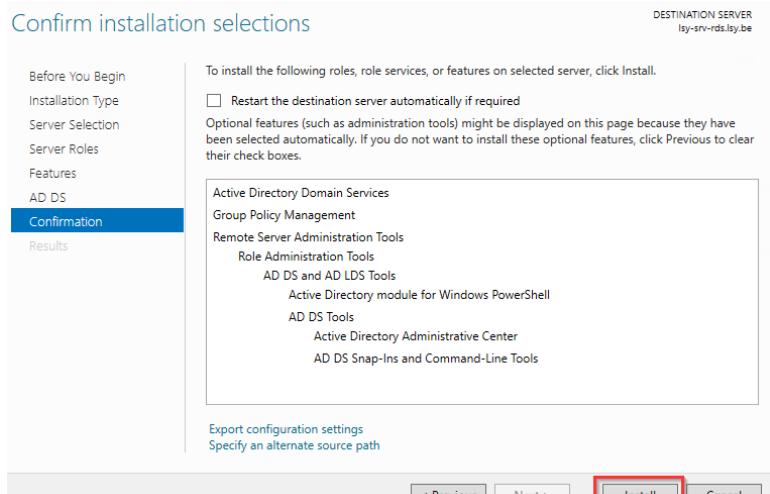
Figuur 43: Installatie van de DC (3)



Figuur 44: Installatie van de DC (4)

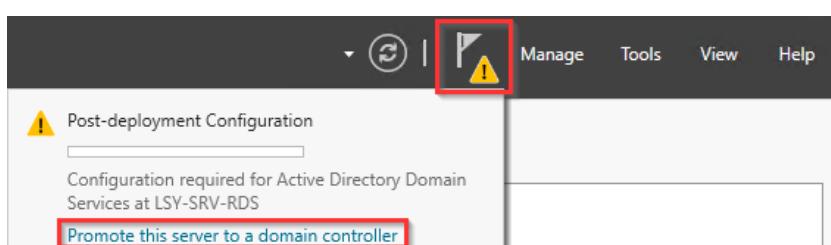
In het volgende scherm druk je op next, hier heb je geen extra features voor nodig. Daarnaast kan je op de volgende schermen ook op next drukken en uiteindelijk druk je op 'Install'.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 45: Installatie van de DC (5)

Daarna drukken we op de vlag met een uitroepteken, en selecteren hier ‘Promote this server to a domain controller’.



Figuur 46: Installatie van de DC (6)

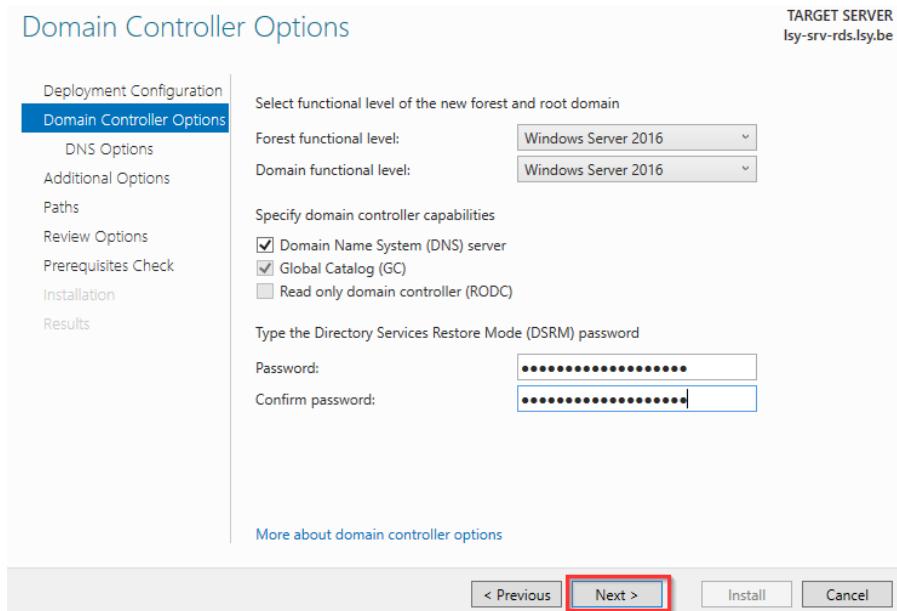
We kiezen hier voor root domein naam. Daarnaast hebben we al een domein, maar voor de documentatie lopen we door de wizard. Na het invullen van de root domein naam druk je op next.



Figuur 47: Installatie van de DC (7)

In het volgende scherm staan de opties correct, kies voor een makkelijk te onthouden wachtwoord of gebruik een wachtwoordmanager om je wachtwoorden in op te slaan. Wij gebruiken hiervoor Passwork. Druk op next na het invullen van het wachtwoord.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 48: Installatie van de DC (8)

Bij de DNS opties druk je op next. Dan kom je bij het scherm van extra opties, hier druk je ook op next. Bij paths druk je ook op next. Bij review druk je ook op next.

Daarna worden alle vereisten gecontroleerd. Normaal zouden deze controle succesvol moeten zijn. Als deze succesvol zijn kan je op 'Install' drukken om de server te promoveren naar een domein controller.

## Automatisch toewijzen van een VLAN aan een gebruiker

### Prerequisites Check

TARGET SERVER  
lsy-srv-rds.lsy.be

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more 

<a href="#">Deployment Configuration</a> <a href="#">Domain Controller Options</a> <a href="#">DNS Options</a> <a href="#">Additional Options</a> <a href="#">Paths</a> <a href="#">Review Options</a> <span style="background-color: #0070C0; color: white; padding: 2px 5px;">Prerequisites Check</span> <a href="#">Installation</a> <a href="#">Results</a>	<p>Prerequisites need to be validated before Active Directory Domain Services is installed on this computer</p> <p><a href="#">Rerun prerequisites check</a></p> <p><span style="font-size: 1.5em;">▲</span> <a href="#">View results</a></p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p><span style="color: yellow;">⚠</span> Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.</p> <p>For more information about this setting, see Knowledge Base article 942564 (<a href="http://go.microsoft.com/fwlink/?LinkId=104751">http://go.microsoft.com/fwlink/?LinkId=104751</a>).</p> <p><span style="color: yellow;">⚠</span> This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System</p> <p><span style="color: yellow;">⚠</span> If you click Install, the server automatically reboots at the end of the promotion operation.</p> <p><a href="#">More about prerequisites</a></p> </div> <p style="text-align: right; margin-top: 10px;"> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">&lt; Previous</span> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Next &gt;</span> <span style="border: 2px solid #c00; padding: 2px 10px; background-color: #fff; color: #c00;">Install</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Cancel</span> </p>
---	--

Figuur 49: Installatie van de DC (9)

### 6.1.2 Installatie Certificaat services

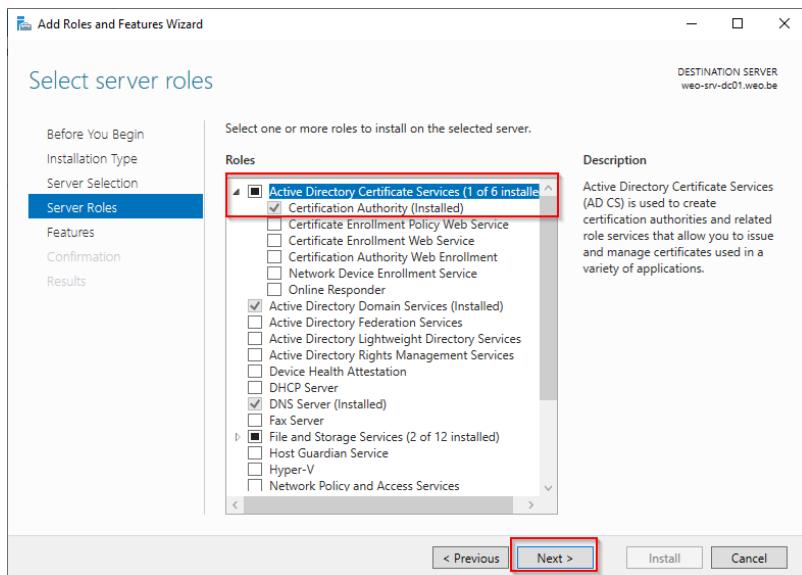
Allereerst gaan we onze domein controller configureren als een certificaatserver. Om dit te doen, moeten we eerst de rol 'Active Directory Certificate Services' toevoegen. Raadpleeg de foto's voor de configuratie in de wizard.



Figuur 50: Installatie van de certificaat services (1)

Hier selecteer je 'Active Directory Certificate Services'. Laat de rest van de instellingen op de standaardwaarden staan en klik op 'Next' totdat je de wizard hebt voltooid.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 51: Installatie van de certificaat services (2)

Je certificaatserver is nu operationeel en je kunt zelf ondertekende certificaten aanmaken.

### 6.1.2.1 Aanmaken certificaten

We gaan certificaten templates voor zowel computers als gebruikers aanmaken om te gebruiken in het kader van 802.1x IEEE-authenticatie. Deze templates bieden een gestandaardiseerde en geautomatiseerde methode voor het uitgeven van certificaten binnen ons netwerk, specifiek gericht op het authenticatieproces.

Voor computers kunnen we bijvoorbeeld certificaatvereisten instellen die nodig zijn voor 802.1x-authenticatie, zoals het gebruik van een specifiek algoritme voor het versleutelen van communicatie tussen de computer en het netwerk. Dit zorgt voor een veilige en gecontroleerde toegang tot het netwerk voor alle computers in ons domein.

Aan de gebruikerskant kunnen we certificaattemplates configureren die worden gebruikt voor de authenticatie van individuele gebruikers bij het verbinden met het netwerk. Deze certificaten kunnen bijvoorbeeld worden gebruikt om de identiteit van de gebruiker te verifiëren en de toegang tot specifieke netwerkresources te beheren.

Door aparte templates te gebruiken voor zowel computers als gebruikers, kunnen we het proces van certificaatuitgifte beter beheren en aanpassen aan de specifieke eisen van 802.1x-authenticatie. Dit verhoogt niet alleen de beveiliging van ons netwerk, maar biedt ook een geautomatiseerde en gecontroleerde methode voor het beheren van de toegang tot ons netwerk op basis van certificaat gebaseerde authenticatie.

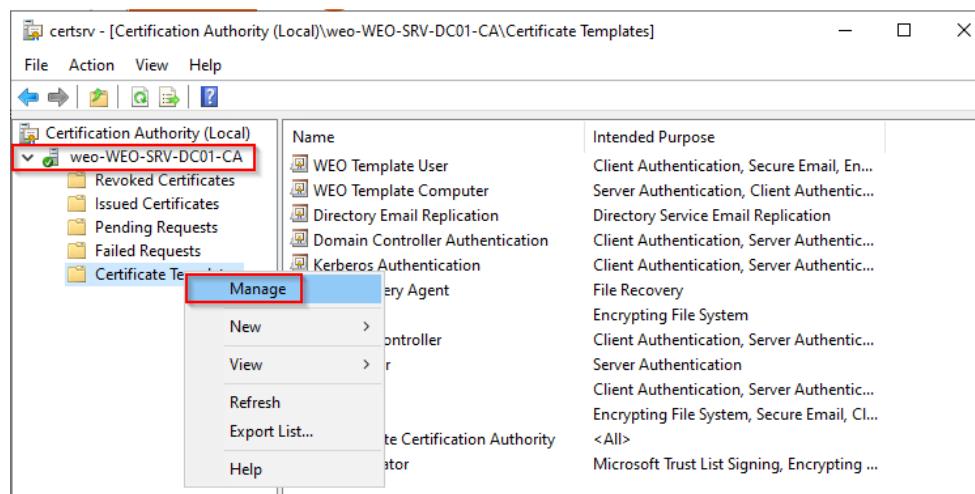
## Automatisch toewijzen van een VLAN aan een gebruiker

**Open 'certificate authority'**



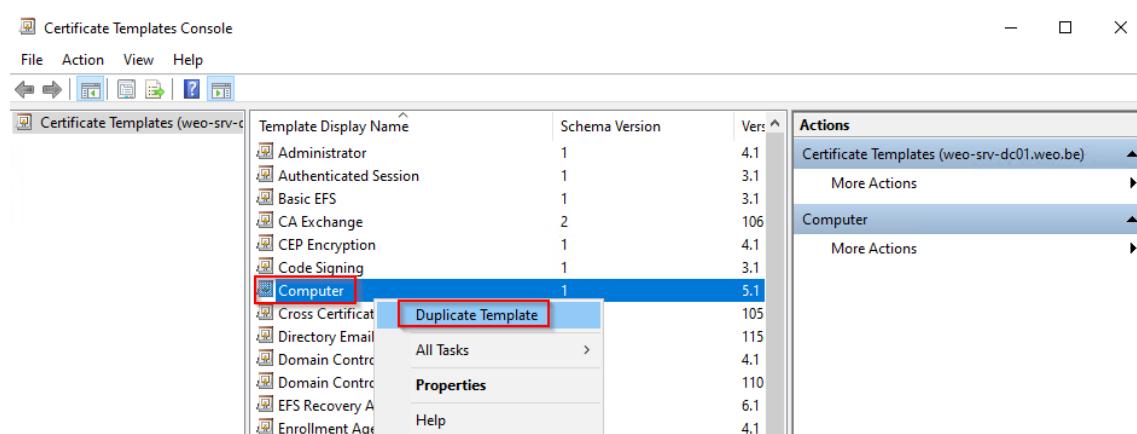
Figuur 52: Installatie van de certificaat services (3)

**Recht klik op 'Certificate Templates' en selecteer vervolgens 'Manage'.**



Figuur 53: Installatie van de certificaat services (4)

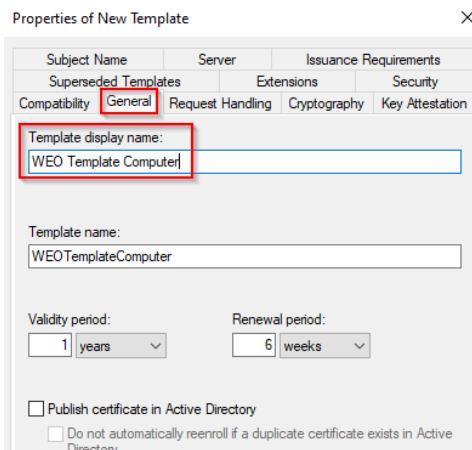
**Vervolgens rechter klik je op 'Computer' en selecteer je 'Duplicate Template'.**



Figuur 54: Installatie van de certificaat services (5)

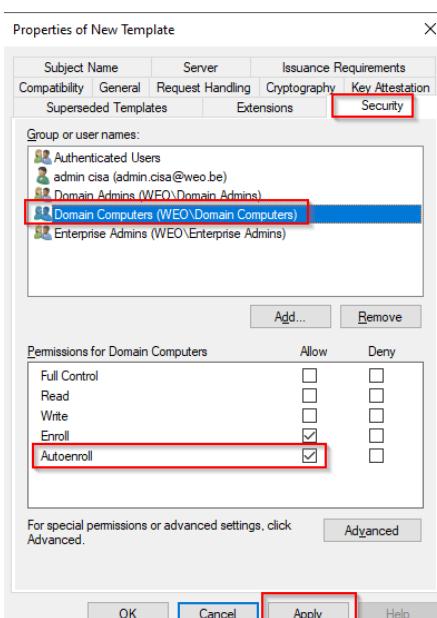
**Klik hier op 'General' en geef je computer template een zinvolle naam.**

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 55: Installatie van de certificaat services (6)

Vervolgens klik je ook op 'Security', selecteer je 'Domain Computers', en sta je toe dat deze automatisch inschrijven ('autoenroll') mogen uitvoeren.



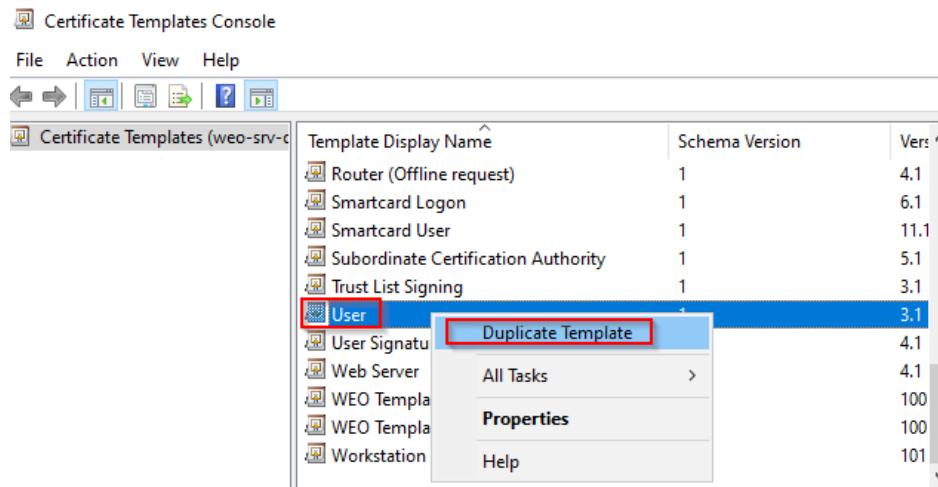
Figuur 56: Installatie van de certificaat services (7)

**Belangrijk:** We staan toe dat 'Domain Computers' automatisch inschrijvingen ('autoenroll') kunnen uitvoeren om ervoor te zorgen dat computers binnen ons domein automatisch de benodigde certificaten kunnen verkrijgen zonder handmatige tussenkomst. Dit is belangrijk omdat het proces van certificaatuitgifte stroomlijnt en automatiseert, waardoor de administratieve last wordt verminderd en de efficiëntie wordt verhoogd. Met auto-enroll kunnen computers naadloos en zonder menselijke tussenkomst certificaten verkrijgen die nodig zijn voor verschillende doeleinden, zoals authenticatie, beveiligde communicatie, of andere netwerktoepassingen. Dit verhoogt niet alleen de beveiliging, maar minimaliseert ook

## Automatisch toewijzen van een VLAN aan een gebruiker

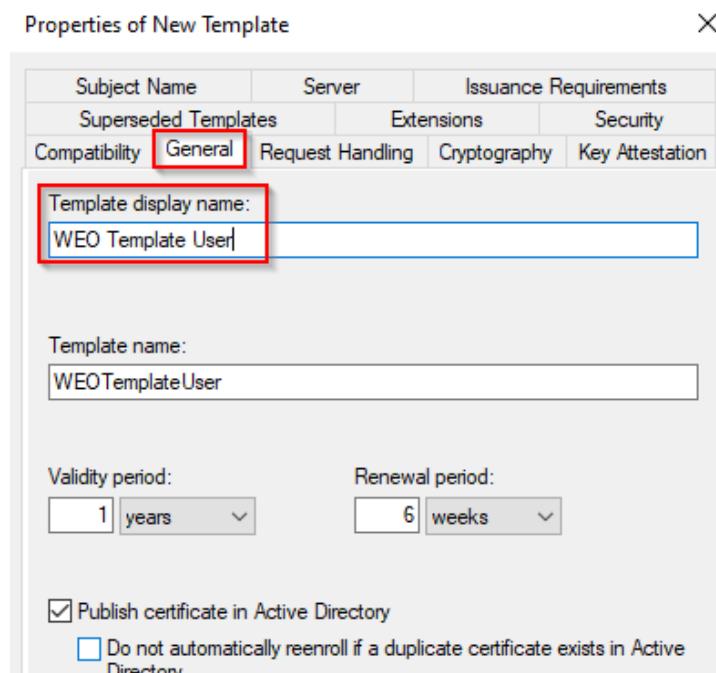
de kans op menselijke fouten en verhoogt de consistentie van het certificaatbeheer binnen ons netwerk.

Nu gaan we ook een template maken voor gebruikers. Klik met de rechtermuisknop op 'Users' en selecteer 'Duplicate Template'.



Figuur 57: Installatie van de certificaat services (8)

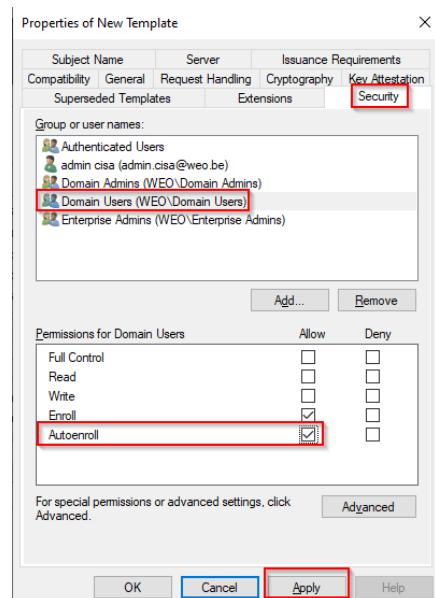
Klik hier op 'General' en geef je user template een zinvolle naam.



Figuur 58: Installatie van de certificaat services (9)

## Automatisch toewijzen van een VLAN aan een gebruiker

Vervolgens klik je ook op 'Security', selecteer je 'Domain Users', en sta je toe dat deze automatisch inschrijven ('autoenroll') mogen uitvoeren.

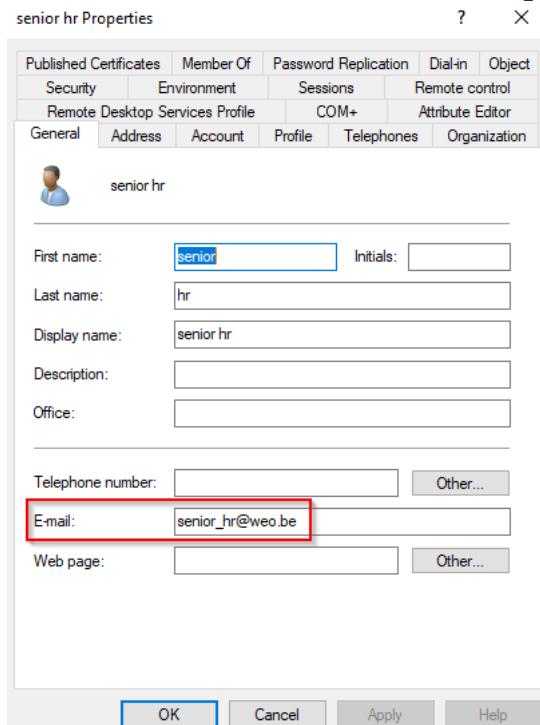


Figuur 59: Installatie van de certificaat services (10)

**Belangrijk:** We moeten ervoor zorgen dat we voor elke gebruiker een e-mailadres toevoegen, zelfs als het een nepadres is dat niet bestaat. Dit is essentieel om fouten te voorkomen bij het uitdelen van de user certificaten in een later stadium.

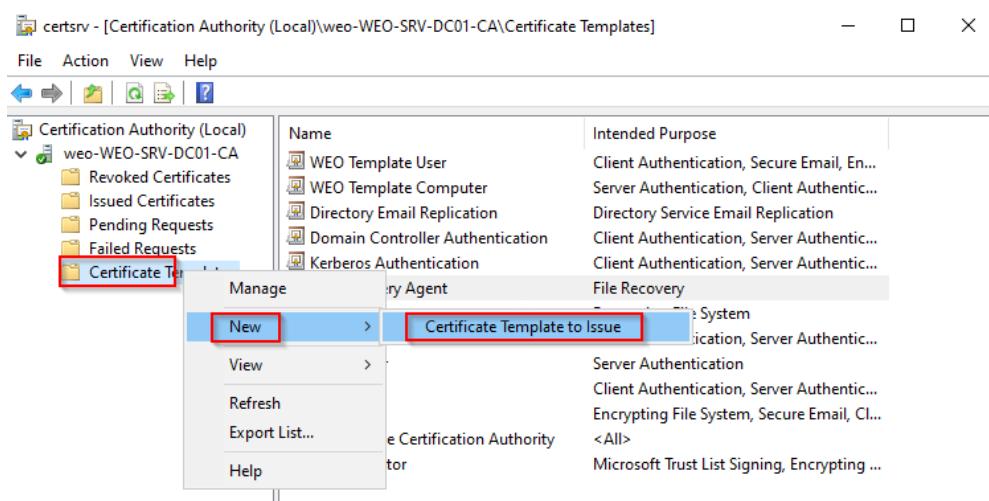
## Automatisch toewijzen van een VLAN aan een gebruiker

Dit kan worden bereikt door 'Active Directory Users en Computers' te openen. Zoals je kunt zien, is er een fictief e-mailadres ingevoerd in het betreffende veld.



Figuur 60: Installatie van de certificaat services (11)

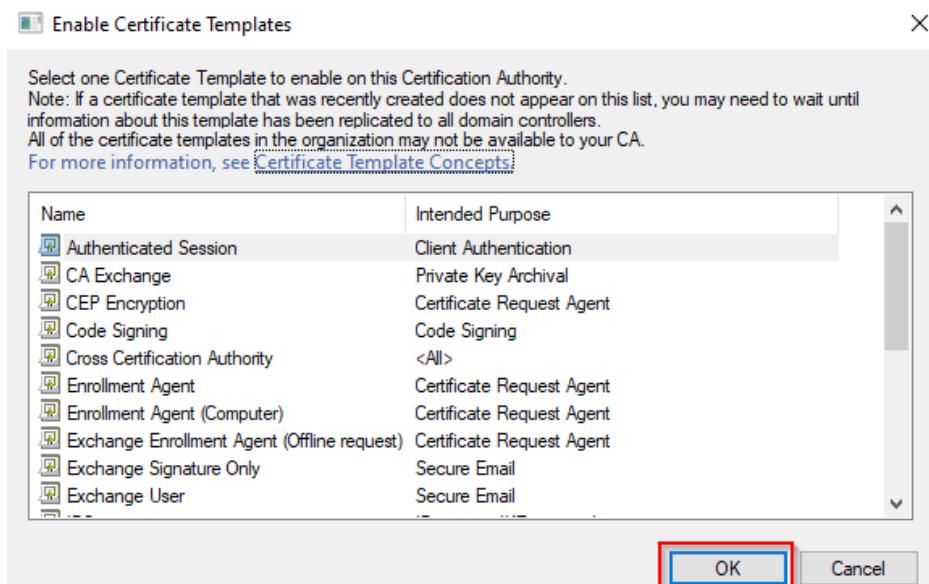
Als laatste stap moeten we nu ook onze twee templatecertificaten uitgeven. We doen dit om ervoor te zorgen dat de certificaten beschikbaar zijn voor gebruik binnen ons netwerk. Dit kan worden gedaan door te klikken op 'Certificate Templates > new > Certificate Template to Issue'.



Figuur 61: Installatie van de certificaat services (12)

## Automatisch toewijzen van een VLAN aan een gebruiker

Vervolgens klik je op de twee template certificaten die je net hebt gemaakt en klik je op 'OK'.



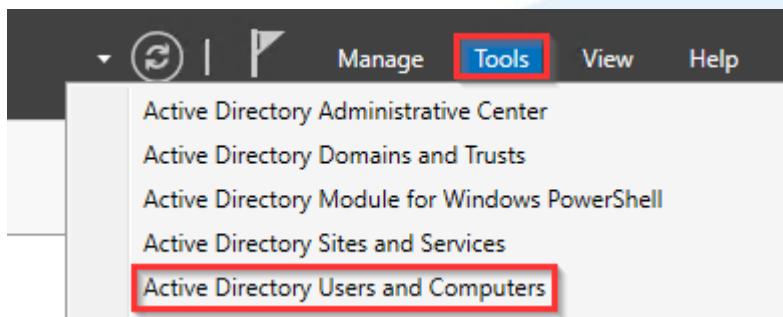
Figuur 62: Installatie van de certificaat services (13)

Hoewel we auto-enroll al hebben ingeschakeld, moeten we ook een GPO(Group policy) aanmaken om ervoor te zorgen dat de certificaten worden bijgewerkt en vernieuwd wanneer nodig. Je kunt de stappen voor het pushen van certificaten terugvinden in de sectie over '5.1.4 Groep policy > 5.1.4.4 Certificaatbeheer en Automatische Vernieuwing'.

### 6.1.3 Users and computers

In active directory users en computers (ADUC) zullen we de organizational units (OU's), groepen, gebruikers etc aanmaken.

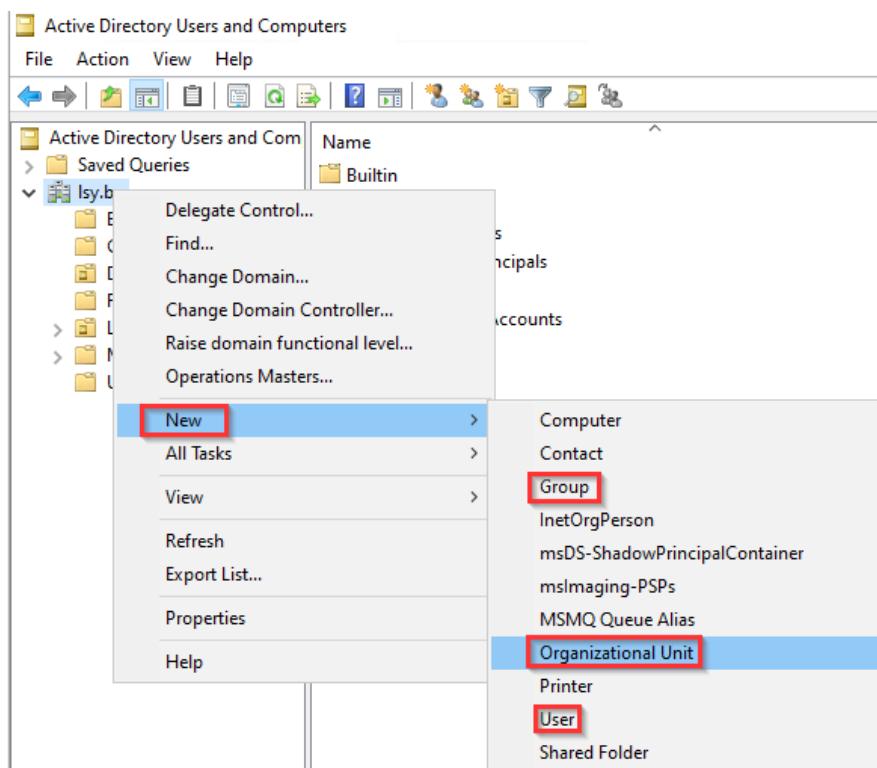
Om te navigeren naar de ADUC kan je in de server manager naar tools gaan en daarna naar active directory users en computers.



Figuur 63: Aanmaken van OU (1)

## Automatisch toewijzen van een VLAN aan een gebruiker

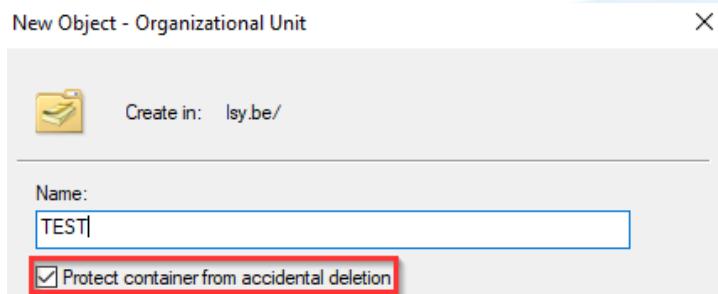
Voor het aanmaken van OU's, gebruikers en groepen kan je rechter muisknop drukken op waar je deze wilt toevoegen daarna op "new", uit deze lijst kies je dan wat je wilt aanmaken.



Figuur 64: Aanmaken van OU (2)

Het aanmaken van de OU structuur, users en computers kan manueel zoals hierboven getoond. Bij de OU structuur hebben we ervoor gekozen om deze via powershell te laten gaan. Op deze manier hebben we een gemakkelijke manier om de structuur op te zetten en overal hetzelfde te houden.

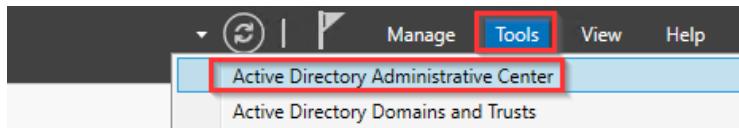
Er kan ook gekozen worden om de optie 'Protect container from accidental deletion' uit te schakelen bij het aanmaken van de OU. Mocht er in deze OU nog een object zetten met ook bescherming tegen per ongeluk verwijderen zal je dit voor elk object moeten uitschakelen.



Figuur 65: Aanmaken van OU (3)

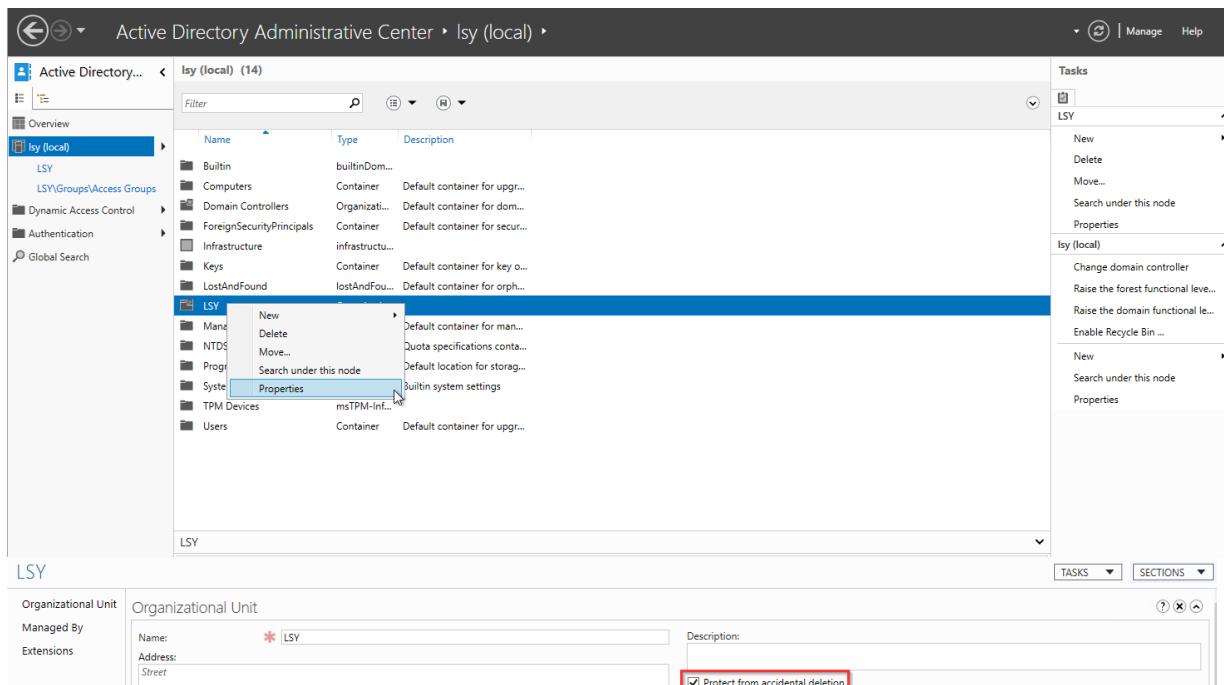
## Automatisch toewijzen van een VLAN aan een gebruiker

Voor het verwijderen van OU is het de bedoeling dat de bescherming eerst wordt uitgeschakeld. Dit kunnen we doen door te navigeren in de server manager naar tools en daarna active directory administrative center.



Figuur 66: Aanmaken van OU (4)

Eenmaal in het center aangekomen navigeer je onder overview naar je domein (local). Als je daar bent navigeer je in de lijst naar de OU die je wilt verwijderen en drukt daarna op properties. Dan komt er een pop-up met extra informatie over de organizational unit. Hier kan je ook de optie “protect from accidental deletion” uitschakelen.



Figuur 67: Aanmaken van OU (5)

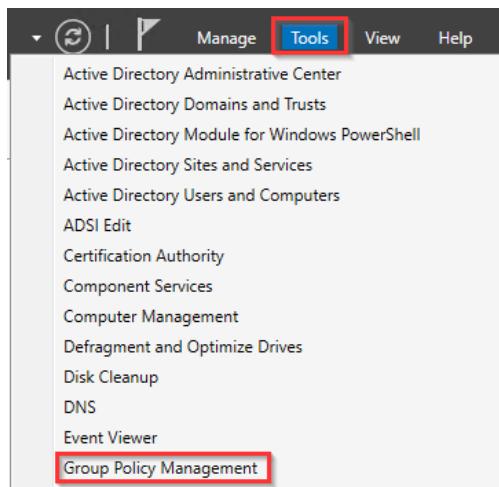
Aangezien dit omslachtig is als je heel wat OU's moet/wilt verwijderen hebben we voor onze OU-structuur ook een script dat zorgt voor het verwijderen van deze structuur.

Deze scripts zijn voorzien in de zip.

### 6.1.4 Groep Policy

Om GPO's aan te maken of aan te passen gaan we in de server manager naar tools en daarna openen we groep policy management.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 68: Navigeren naar GPO

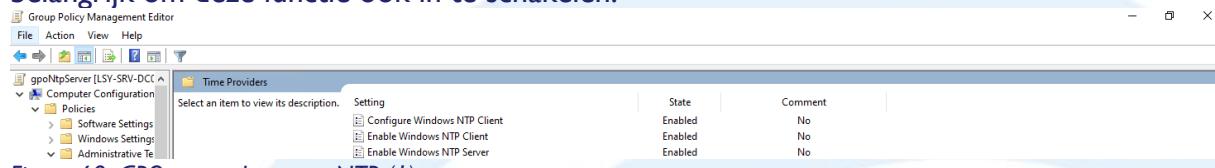
### 6.1.4.1 NTP

Network Time Protocol (NTP) is zeer belangrijk voor kritieke functies en systeem binnen netwerken en computers. NTP zal ervoor zorgen dat de klokken van alle systemen binnen een netwerk op dezelfde tijd lopen. Dit is van cruciaal belang voor bijvoorbeeld logbestanden waarbij de volgorde van gebeurtenissen nauwkeuring moet worden geregistreerd.

Om hierbij aan te sluiten maken we gebruik van GPO's voor zowel servers als computers. Voor de domain controller en andere servers maken we gebruik van de gpoNtpServer en daarnaast bij de computers maken we gebruik van de gpoNtpClient.

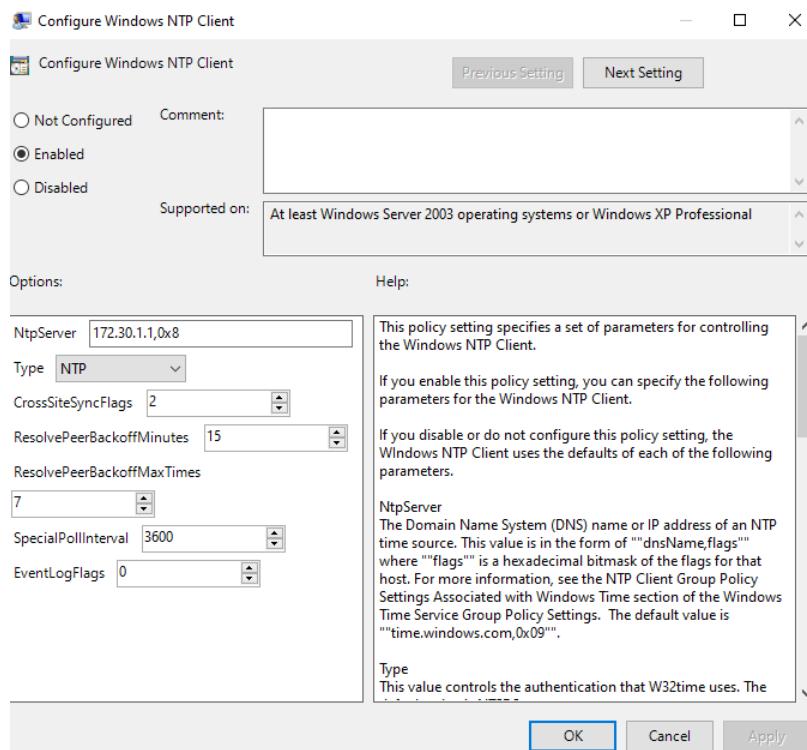
Om de NTP goed in te stellen voor de server navigeren we naar ‘computer configuration > policies > Administrative templates > System > Windows Time Service > Time Providers’.

Hierin zetten we enable windows NTP client en server aan. Voor het configureren van de client; nemen we het IP van de firewall als NtpServer met als flag 0x8. Deze flag zal de clientmodus gebruiken tijdens het synchroniseren van de tijd met een externe tijdborn. Wel zeggen we erbij dat de firewall geen externe tijdborn is. Het type dat we gebruiken is NTP. De andere configuraties kan je overnemen van de onderstaande afbeelding. Het is wel belangrijk om deze functie ook in te schakelen.



Figuur 69: GPO aanmaken voor NTP (1)

## Automatisch toewijzen van een VLAN aan een gebruiker

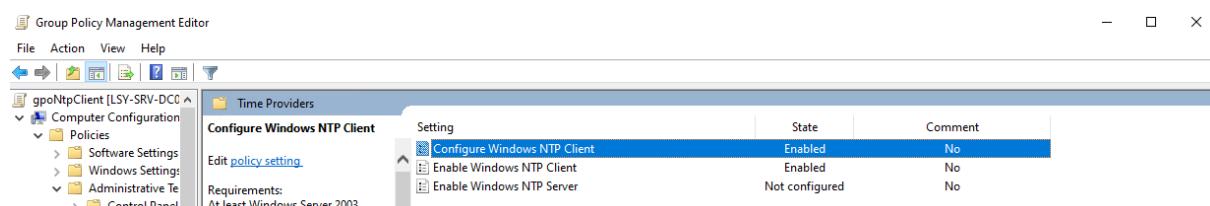


Figuur 70: GPO aanmaken voor NTP (2)

Daarna druk je op apply.

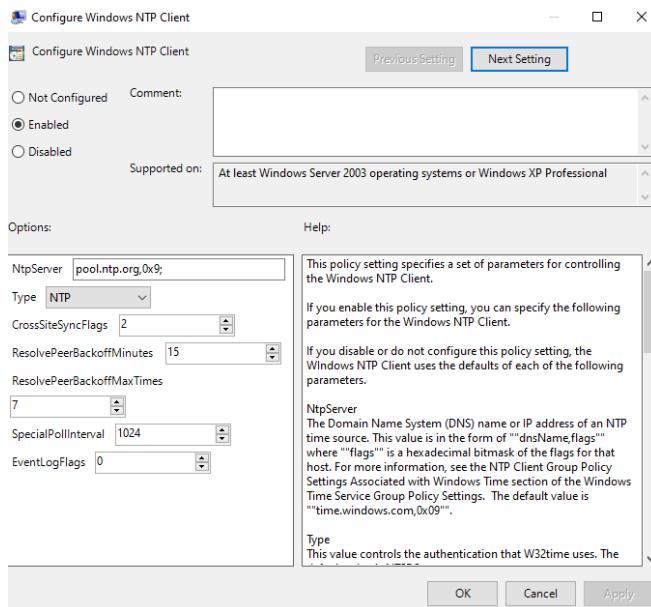
Voor de client schakelen we configure windows NTP client en daarnaast ook het inschakelen van NTP client. We laten inschakelen windows NTP server staan zoals deze staat op niet geconfigureerd.

Als ntp server nemen we hier 'pool.ntp.org,0x9;', met als type NTP. De 0x9 vertelt de server om een client-mode associatie te gebruiken met speciaal interval.



Figuur 71: GPO aanmaken voor NTP (3)

## Automatisch toewijzen van een VLAN aan een gebruiker

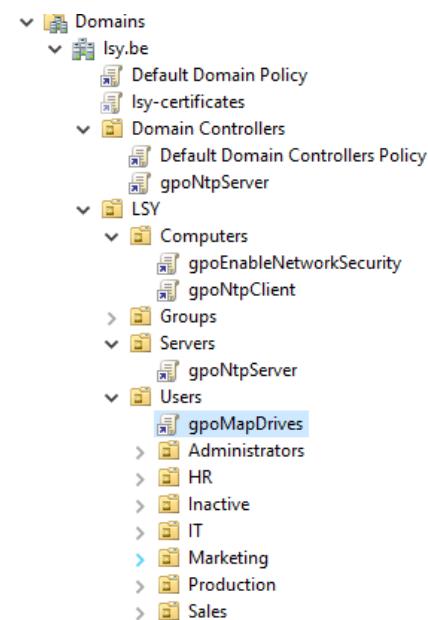


Figuur 72: GPO aanmaken voor NTP (4)

Daarna druk je op apply. Door het gekozen interval kan het even duren voor de tijden effectief allemaal zijn gesyncroniseerd.

### 6.1.4.2 Map drives

Als we de drives automatisch willen laten halen door de gebruikers gaan we op user niveau een nieuwe gpo aanmaken met naam gpoMapDrives. Deze plaatsen we op het niveau van de user.



Figuur 73: GPO aanmaken voor drives (1)

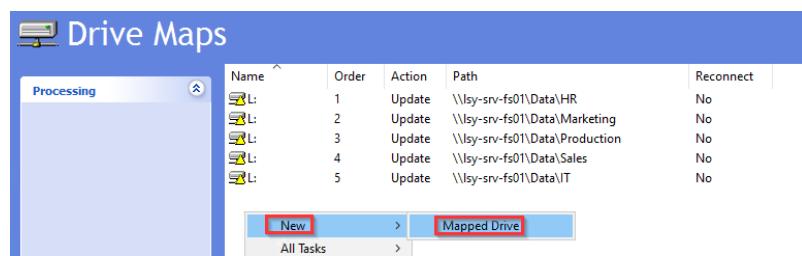
## Automatisch toewijzen van een VLAN aan een gebruiker

Eenmaal in de editor aangekomen na het aanmaken van deze GPO navigeren we naar user configuration > preferences > windows settings en daarna drive maps. Hier zullen we de mappings maken naar de fileserver.



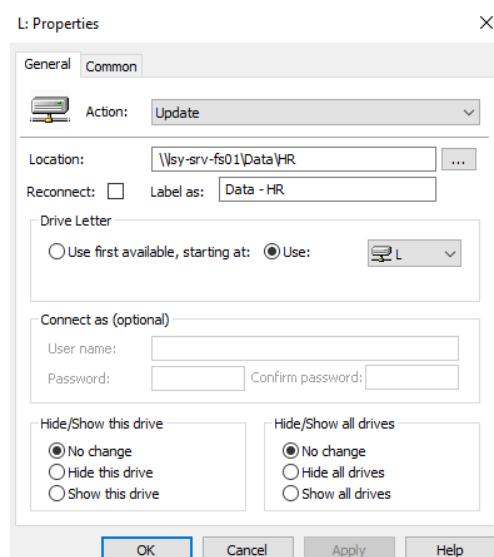
Figuur 74: GPO aanmaken voor drives (2)

Voor het aanmaken van een nieuwe mapped drive, drukken we op rechtermuisknop daarna selecteren we nieuw en daarna kiezen we voor mapped drive.



Figuur 75: GPO aanmaken voor drives (3)

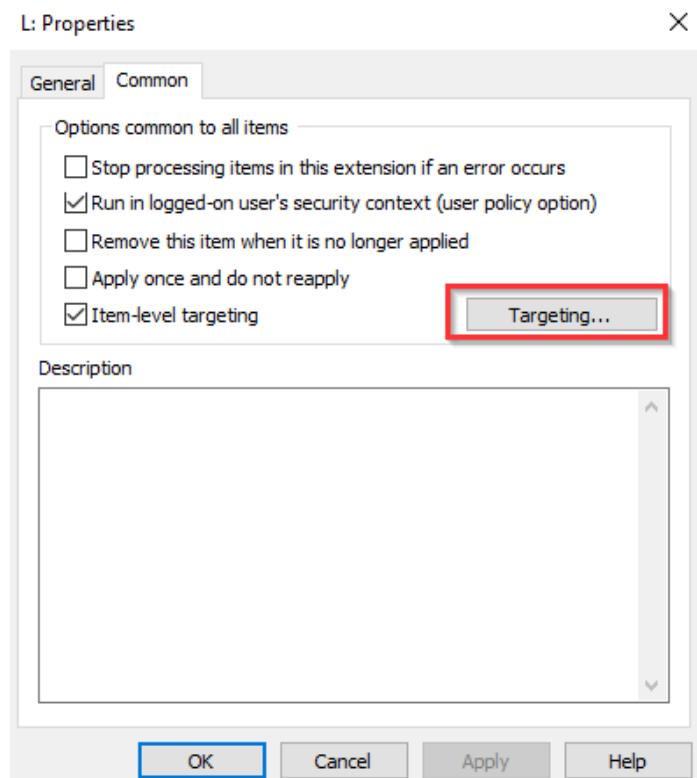
We zetten in de general tab de actie op update, daarnaast komt de locatie op het pad waar de share zich bevindt. Dit is op de fileserver. Om te navigeren naar een netwerk pad gebruiken we 2 maal de backslash. Naast de domein naam kan dit ook het IP van de server zijn. Daarna geven de share een label. Aangezien dit de data share is kiezen we voor data koppelteken en daarna de afdeling. Als letter gebruik ik dezelfde als we gekozen hebben voor de disk. In ons geval is dit de L-schijf. Hide/show this/all drives blijven allebei staan op geen veranderingen.



Figuur 76: GPO aanmaken voor drives (4)

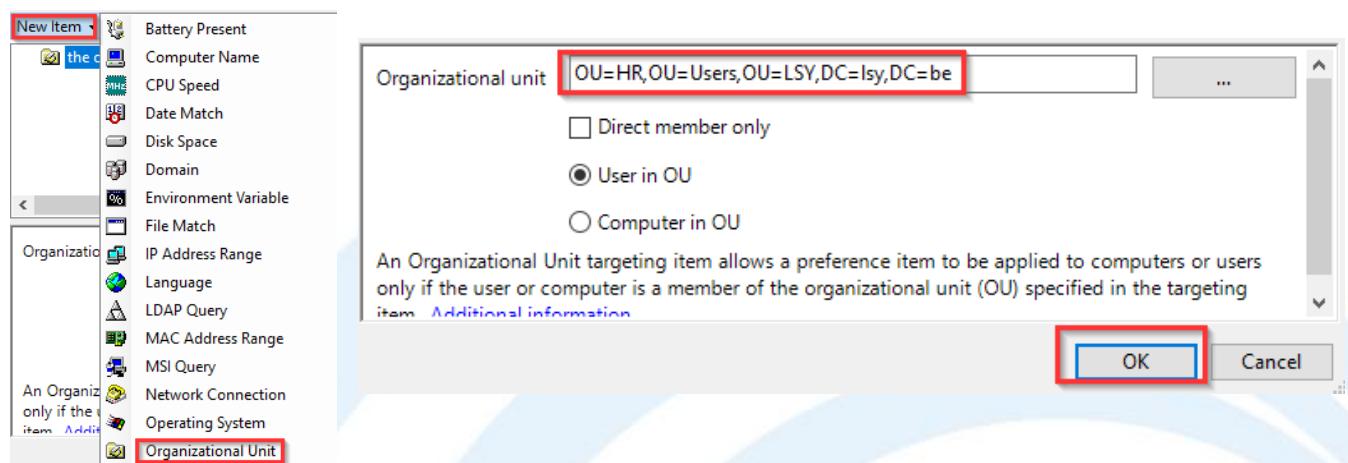
## Automatisch toewijzen van een VLAN aan een gebruiker

In de common tab selecteren we “run in logged-on user’s security context”. Maar daarnaast selecteren we ook item-level targeting. Als we dan op targeting drukken kunnen we OU selecteren om aan te geven welke gebruikers deze map moeten krijgen.



Figuur 77: GPO aanmaken voor drives (5)

We kiezen in deze nieuwe tab new item en daarna organization unit (OU). Voor het kiezen van de OU kan je drukken op de drie puntjes. In de pop-up die je krijgt selecteer je welke OU. In dit geval zal die de OU HR zijn. Daarna druk je op OK. Eenmaal je terug in het vorige scherm bent druk je op OK. Dit herhaal je voor elke afdeling.



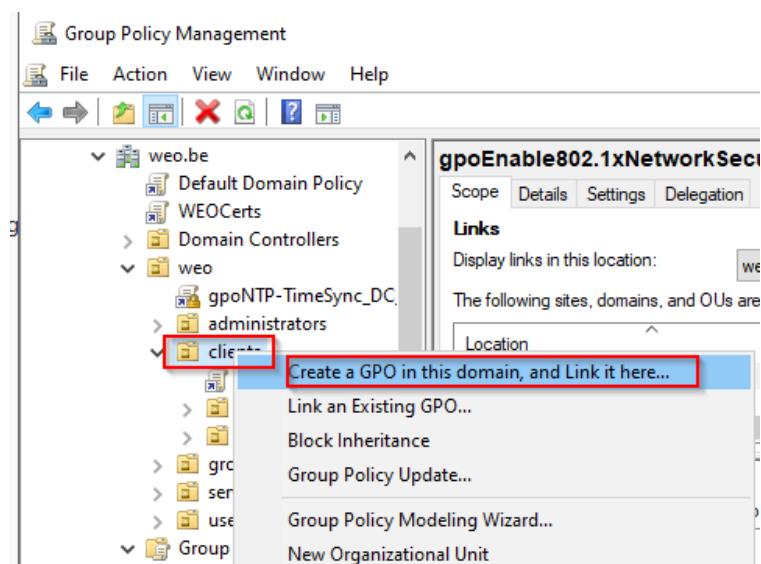
Figuur 78: GPO aanmaken voor drives (6)

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.1.4.3 Enable 802.1x

De Group Policy is ontworpen om automatisch 802.1 port security in te schakelen voor gebruikers binnen ons netwerk. Door deze policy toe te passen, worden gebruiker automatisch geauthentiseerd en toegang verleend tot netwerkpoorten volgens de 802.1x-standaard.

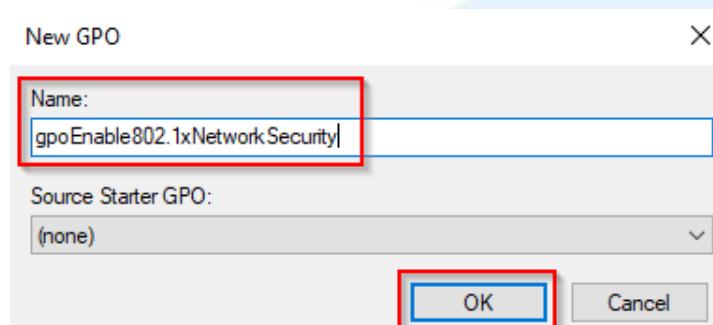
Open eerst 'Group Policy Management'. Vervolgens maak je een nieuwe GPO aan op het niveau van je OU waar alle clients onder staan door met de rechtermuisknop op de OU te klikken en te kiezen voor 'Create a GPO in this domain, and Link it here...'.!



Figuur 79: GPO aanmaken voor 802.1 auth (1)

Het is belangrijk om te vermelden dat de virtuele machines en servers niet in deze map mogen worden opgenomen. Ze bevinden zich namelijk niet achter de switch, maar achter de firewall, en hebben daarom geen 802.1 port security nodig.

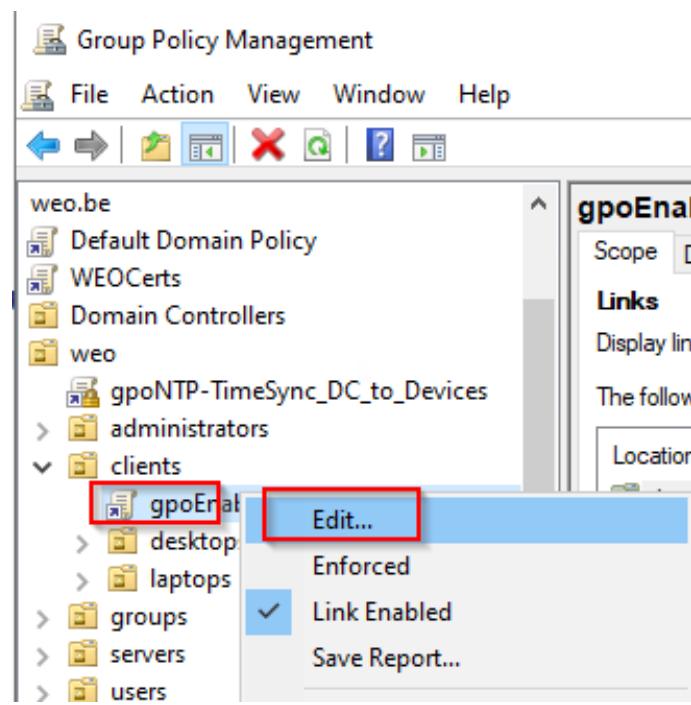
Geef je GPO een duidelijke naam.



Figuur 80: GPO aanmaken voor 802.1 auth (2)

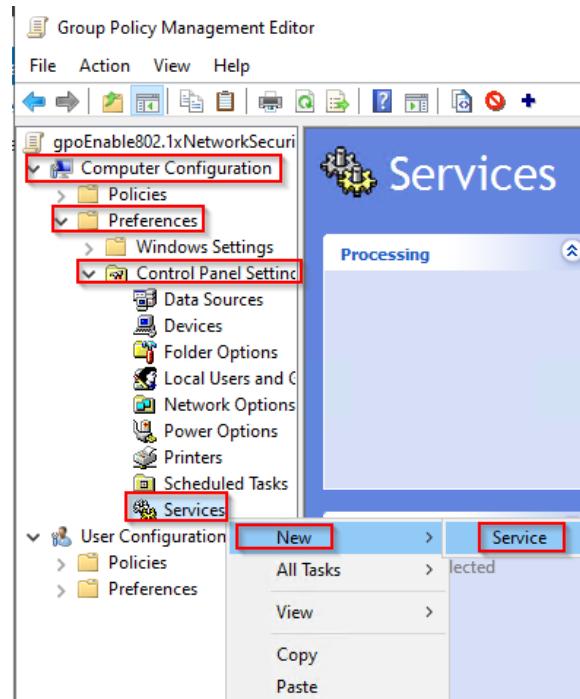
## Automatisch toewijzen van een VLAN aan een gebruiker

Klik daarna met de rechtermuisknop op je nieuwe GPO en selecteer 'Edit' om deze te bewerken.



Figuur 81: GPO aanmaken voor 802.1 auth (3)

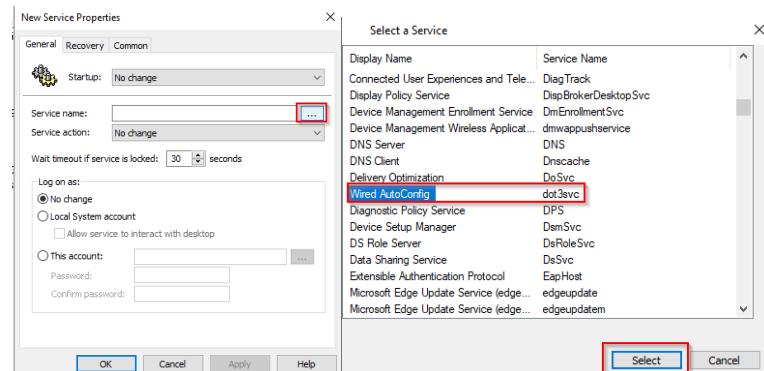
Navigeer vervolgens naar 'Computer Configuration > Preferences > Control Panel Settings'. Klik met de rechtermuisknop op 'Services' en selecteer 'New' > 'Service'.



Figuur 82: GPO aanmaken voor 802.1 auth (4)

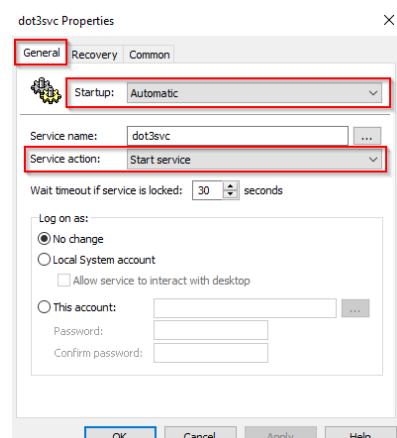
## Automatisch toewijzen van een VLAN aan een gebruiker

Selecteer daarna de service 'dot3svc'.



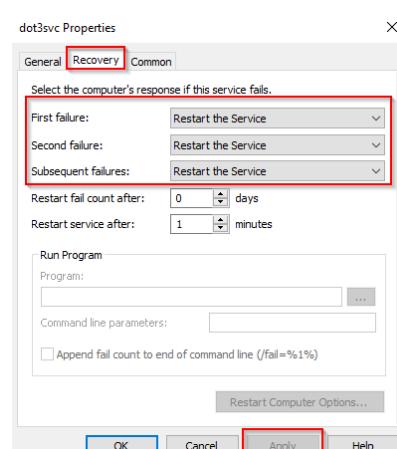
Figuur 83: GPO aanmaken voor 802.1 auth (5)

In het tabblad 'General' wijzig je de opstartinstelling naar 'Automatisch', en bij 'Service Action' selecteer je 'Start Service'. Zie de foto voor referentie.



Figuur 84: GPO aanmaken voor 802.1 auth (6)

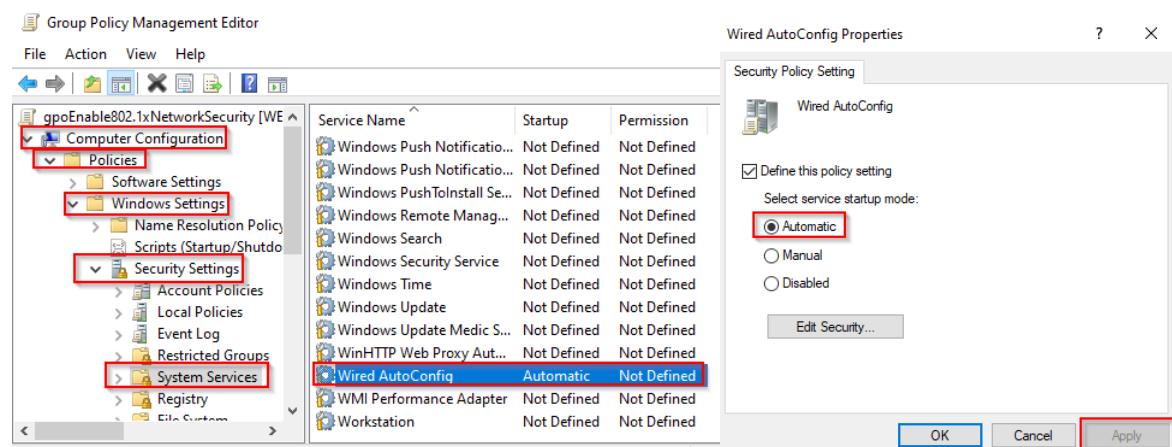
In het tabblad 'Recovery' wijzig je alle opties bij 'Failures' in het vervolgmenu naar 'Herstart de service'.



Figuur 85: GPO aanmaken voor 802.1 auth (7)

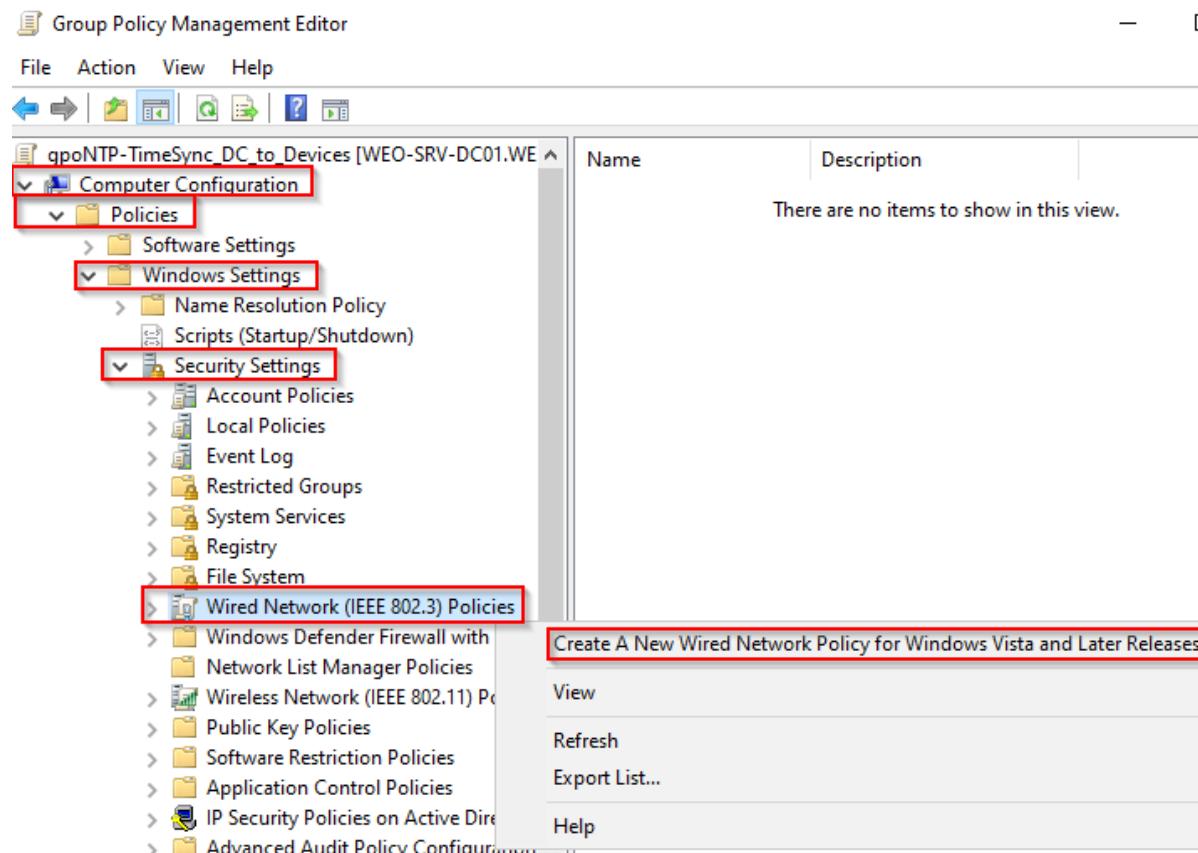
## Automatisch toewijzen van een VLAN aan een gebruiker

Naveer nu naar 'Computer Configuration > Policies > Windows Settings > Security Settings > System Services'. Zoek hier naar 'Wired AutoConfig' en wijzig dit naar 'Automatisch'.



Figuur 86: GPO aanmaken voor 802.1 auth (8)

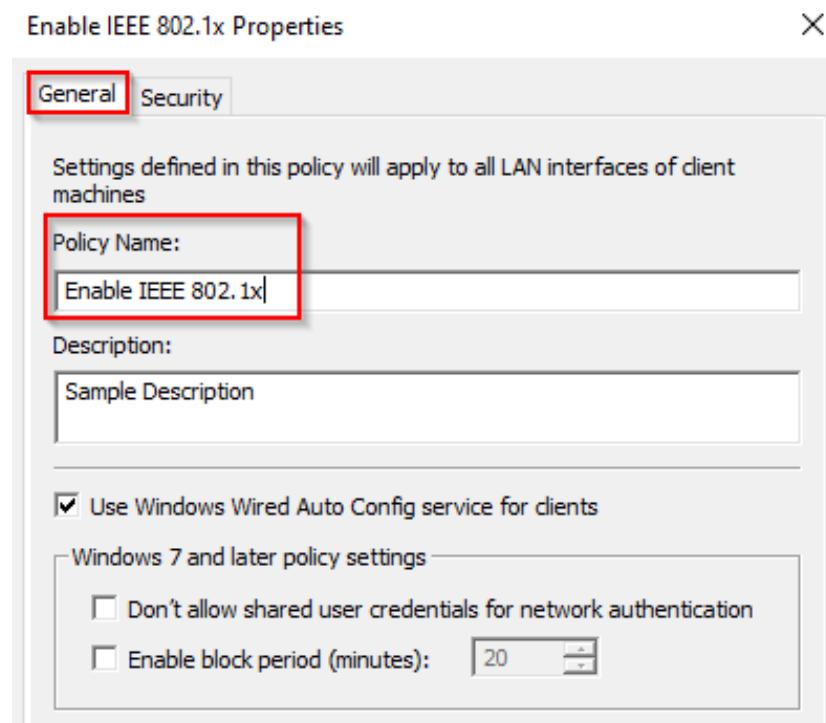
Naveer nu naar 'Computer Configuration > Policies > Windows Settings > Security Settings' rechtersklik 'Wired Network' en selecteer hier 'Create a new wired...'



Figuur 87: GPO aanmaken voor 802.1 auth (9)

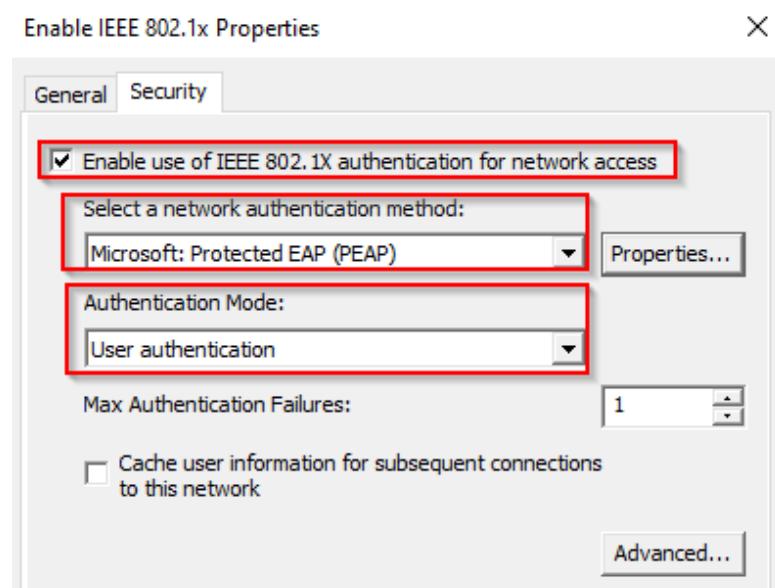
## Automatisch toewijzen van een VLAN aan een gebruiker

In het tabblad 'General' geef je de beleidsnaam een duidelijke en beschrijvende naam.



Figuur 88: GPO aanmaken voor 802.1 auth (10)

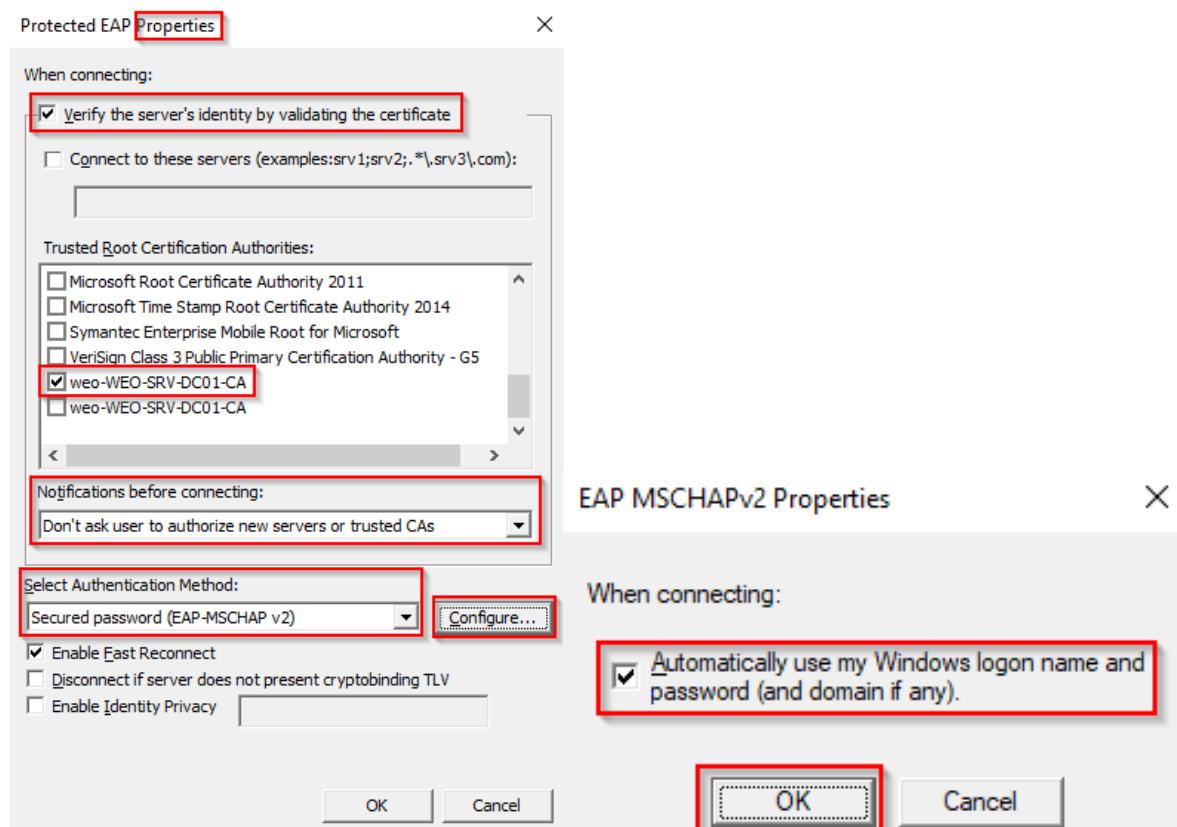
In het tabblad 'Security' vink je de optie aan om 802.1x-authenticatie in te schakelen. Vervolgens selecteer je in het vervolgkeuzemenu onder select a network authentication method: 'Microsoft: Protected EAP (PEAP)' en onder Authentication Mode:s selecteer je 'User authentication'. Zie de foto voor referentie.



Figuur 89: GPO aanmaken voor 802.1 auth (11)

## Automatisch toewijzen van een VLAN aan een gebruiker

Daarna klik je op 'Properties...' en selecteer je 'Verify the server's identity by validationg the certificate'. Selecteer ook bij 'Trusted Root Certification Authorities' je eigen rootcertificaat. Bij 'notifications before connectiong' selecteer je de optie die ervoor zorgt dat de gebruiker geen melding krijgt. Vervolgens selecteer je bij 'select Authentication method' 'secured password (EAP-MSCHAP v2)'. Ten slotte, bij 'properties', klik je op 'Configureren...' en vink je het selectievakje aan. Zie de twee foto's voor referentie.



Figuur 90: GPO aanmaken voor 802.1 auth (12)

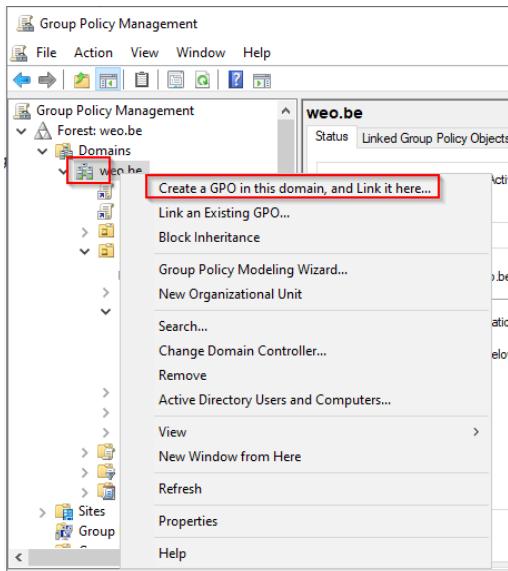
Nu hebben we met succes 802.1x-authenticatie geconfigureerd met behulp van de gewenste beveiligingsinstellingen en certificaatverificaties.

### 6.1.4.4 Certificaatbeheer en Automatische Vernieuwing

Hieronder leggen we uit hoe je een GPO instelt om certificaten up-to-date te houden en automatisch te vernieuwen wanneer nodig.

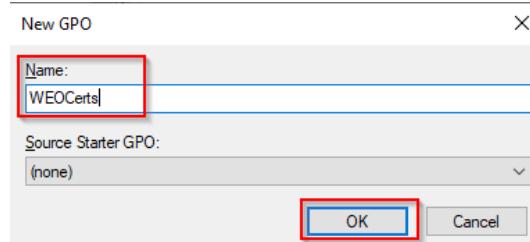
Open eerst 'Group Policy Management'. Vervolgens maak je een nieuwe GPO aan op het niveau van je domein door met de rechtermuisknop op het domein te klikken en te kiezen voor 'Create a GPO in this domain, and Link it here...'.

## Automatisch toewijzen van een VLAN aan een gebruiker



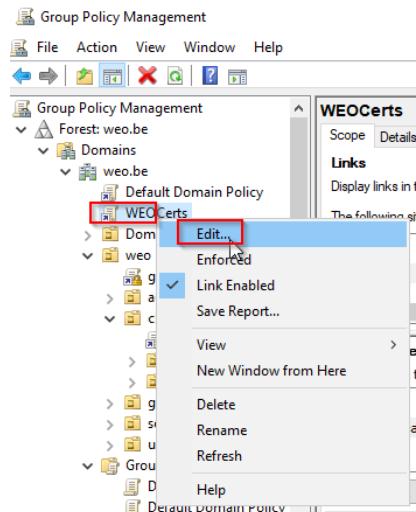
Figuur 91: GPO aanmaken voor certificaten (1)

Geef je GPO een duidelijke naam.



Figuur 92: GPO aanmaken voor certificaten (2)

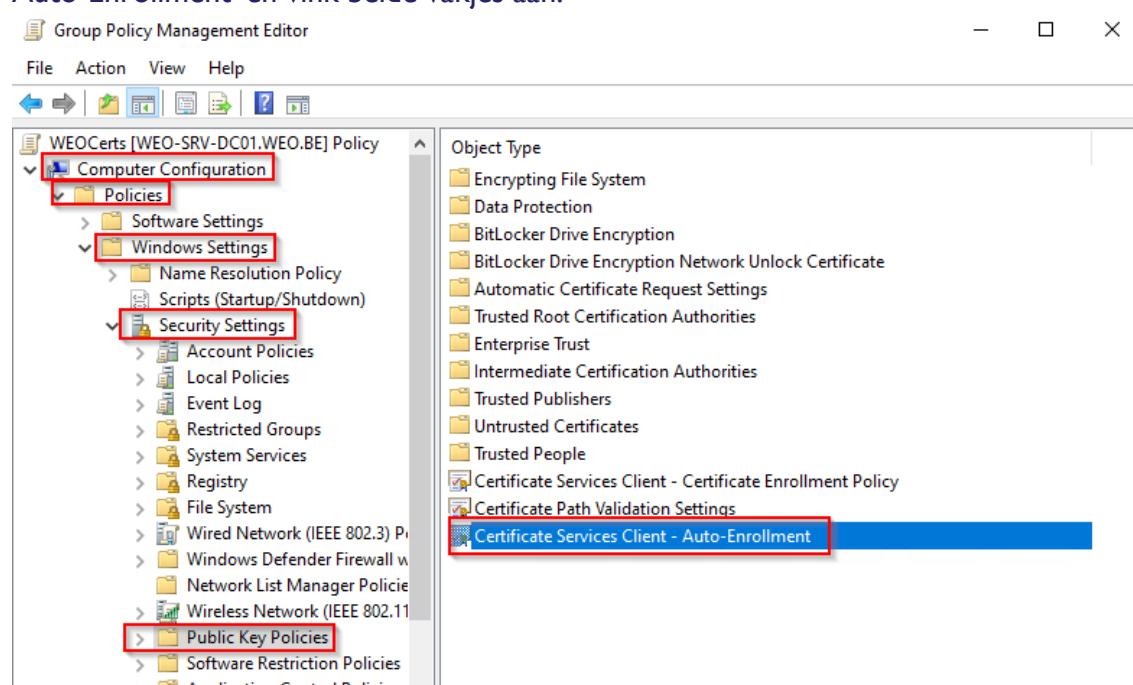
Klik daarna met de rechtermuisknop op je nieuwe GPO en selecteer 'Edit' om deze te bewerken.



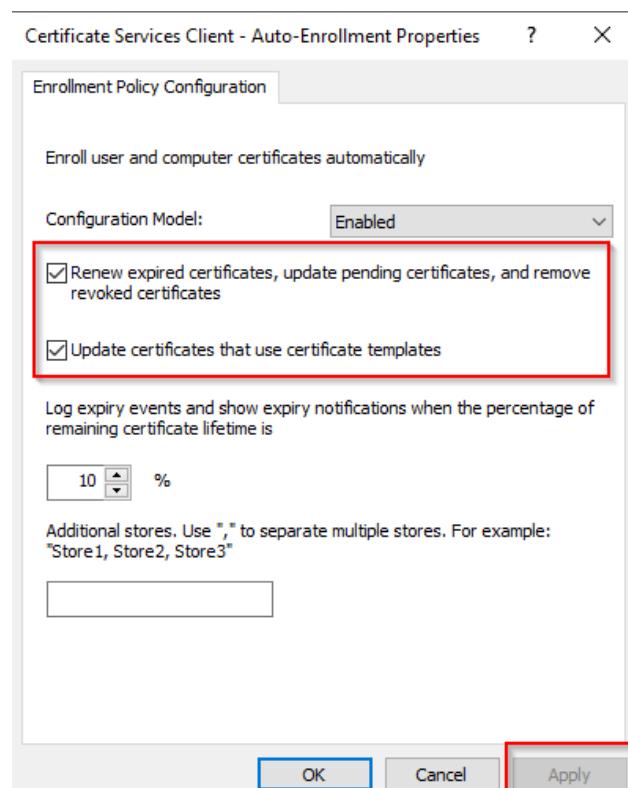
Figuur 93: GPO aanmaken voor certificaten (3)

## Automatisch toewijzen van een VLAN aan een gebruiker

Navigeer vervolgens naar 'Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies'. Dubbelklik daarna op 'Certificate Services Client - Auto-Enrollment' en vink beide vakjes aan.



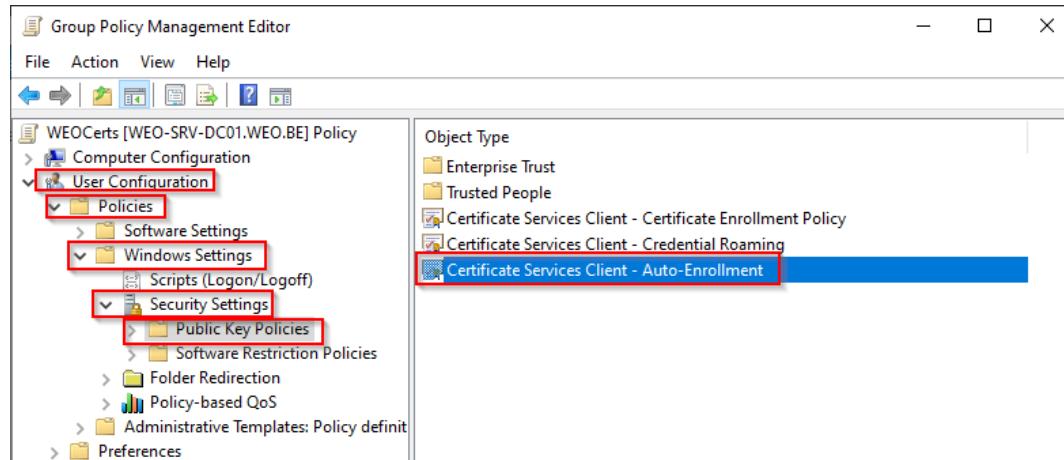
Figuur 94: GPO aanmaken voor certificaten (4)



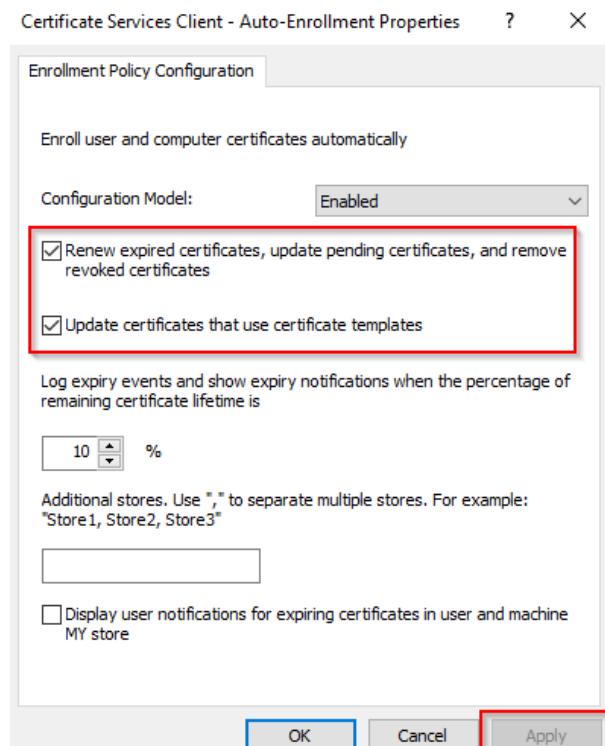
Figuur 95: GPO aanmaken voor certificaten (5)

## Automatisch toewijzen van een VLAN aan een gebruiker

Nu moeten we dit ook instellen voor de gebruikerscertificaten. Navigeer naar 'User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies'. Dubbelklik vervolgens op 'Certificate Services Client - Auto-Enrollment' en vink beide vakjes aan.



Figuur 96: GPO aanmaken voor certificaten (6)



Figuur 97: GPO aanmaken voor certificaten (7)

Nu staat je GPO klaar om certificaten automatisch bij te werken en te vernieuwen voor zowel computers als gebruikers binnen je domein. Deze instellingen zorgen voor een gestroomlijnd en geautomatiseerd proces van certificaatbeheer, waardoor de beveiliging van je netwerk wordt versterkt en de administratieve last wordt verminderd.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.1.5 Extra – Linux Join active directory

- Aanzetten van NTP synchronisatie

```
$ sudo timedatectl set-ntp true
```

- De server IP-Adres van DHCP naar STATIC zetten.

```
$ sudo nano /etc/netplan/00-installer-config.yaml
```

Zo moet het bestand eruit zien.

```
GNU nano 6.2
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens192:
      dhcp4: false
      addresses: [172.30.66.6/24] -> Server IP-Adres
      routes:
        - to: 0.0.0.0/0
          via: 172.30.66.1 -> Default-Gateway
      nameservers:
        addresses: [172.30.66.2] -> IP-Adres van de DC [DNS]
version: 2
```

Figuur 98: Domein joinen via linux (1)

Vervolgens sla je het bestand op door op Ctrl+O te drukken en verlaat je het bestand met Ctrl+X.

- De Netwerkconfiguratie toepassen.

```
$ sudo netplan apply
$ ip a
```

```
wes@wes-srv-zabbix:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether 00:50:56:bf:e9:8e brd ff:ff:ff:ff:ff:ff
    altname enp1s0
    inet 172.30.66.6/24 brd 172.30.66.255 scope global ens192
      valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe98:6/64 scope link
      valid_lft forever preferred_lft forever
```

Figuur 99: Domein joinen via linux (2)

- Alle package updaten en upgraden.

```
$ sudo apt update -y && sudo apt upgrade -y
```

## Automatisch toewijzen van een VLAN aan een gebruiker

- Installeer de benodigde pakketten om ervoor te zorgen dat je machine zich bij het domein kan aansluiten.

```
$ sudo apt install sssd-ad sssd-tools realmd adcli -y
```

- Zoek de Active Directory-informatie met behulp van het volgende commando

```
$ realm -v discover weo.be
```

Selecteer de 'realm-name' uit de verkregen gegevens, die je in de volgende stap zult gebruiken. **Let op: deze naam is hoofdlettergevoelig.**

```
weo@weo-srv-zabbix:~$ realm -v discover weo.be
* Resolving: _ldap._tcp.weo.be
* Performing LDAP DSE lookup on: 172.30.66.2
* Successfully discovered: weo.be
weo.be
  type: kerberos
  realm-name: WEO.BE
  domain-name: weo.be
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
```

Figuur 100: Domein joinen via linux (3)

- Voeg de Kerberos-configuratie toe, zodat je kunt verbinden met de Active Directory.

```
$ sudo nano /etc/krb5.conf
```

Zo moet het bestand eruit zien.

```
GNU nano 6.2
[libdefaults]
  default_realm = WEO.BE
  rdns = false
```

Figuur 101: Domein joinen via linux (4)

Vervolgens sla je het bestand op door op Ctrl+O te drukken en verlaat je het bestand met Ctrl+X.

- Voeg de computer toe aan het Active Directory-domein.

```
$ sudo realm join -v WEO.BE --user=admin.cisa
```

## Automatisch toewijzen van een VLAN aan een gebruiker

```
weo@weo-srv-zabbix:~$ sudo realm join -v WEO.BE --user=admin.cisa
* Resolving: _ldap._tcp.weo.be
* Performing LDAP DSE lookup on: 172.30.66.2
* Successfully discovered: weo.be
Password for admin.cisa:
* Unconditionally checking packages
* Resolving required packages
* /usr/sbin/update-rc.d sssd enable
* /usr/sbin/service sssd restart
* Successfully enrolled machine in realm
weo@weo-srv-zabbix:~$
```

Figuur 102: Domein joinen via linux (5)

- Voeg de server hostnaam toe aan het SSSD-configuratiebestand.

```
$ sudo nano /etc/sssd/sssd.conf
```

Voeg de regel toe:

```
GNU nano 6.2

[sssd]
domains = weo.be
config_file_version = 2
services = nss, pam

[domain/weo.be]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = WEO.BE
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = weo.be
use_fully_qualified_names = True
ldap_id_mapping = True
access_provider = ad
ad_server = weo-srv-dc01
```

Figuur 103: Domein joinen via linux (6)

Vervolgens sla je het bestand op door op Ctrl+O te drukken en verlaat je het bestand met Ctrl+X.

- Voeg DC-naam toe aan het hosts-bestand.

```
$ sudo nano /etc/hosts
```

## Automatisch toewijzen van een VLAN aan een gebruiker

```
GNU nano 6.2
127.0.0.1 localhost
127.0.1.1 weo-srv-zabbix
172.30.66.2 weo-srv-dc01
```

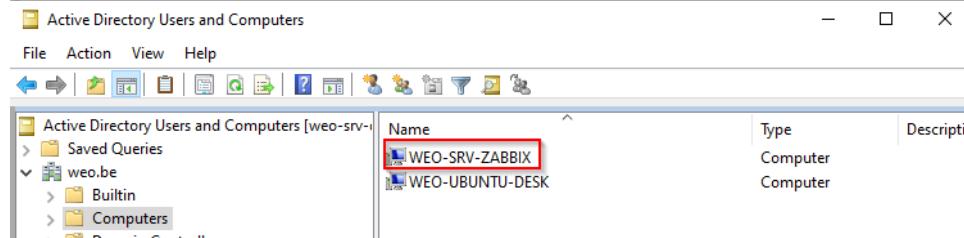
Figuur 104: Domein joinen via linux (7)

Vervolgens sla je het bestand op door op Ctrl+O te drukken en verlaat je het bestand met Ctrl+X.

- Herstart het systeem.

```
$ sudo reboot now
```

- Als je nu kijkt in je Active Directory, zou je de computer moeten zien verschijnen.



Figuur 105: Domein joinen via linux (8)

- Activeer het maken van een home directroy voor elke nieuwe AD-gebruiker die zich aanmeldt op het systeem.

```
$ sudo pam-auth-update --enable mkhomedir
```

- Meld je aan met een gebruiker van Active Directory.

```
$ su - admin.cisa@weo.be
```

```
weo@weo-srv-zabbix:~$ su - admin.cisa@weo.be
Password:
Creating directory '/home/admin.cisa@weo.be'.
admin.cisa@weo.be@weo-srv-zabbix:~$
```

Figuur 106: Domein joinen via linux (9)

Door je Linux-systeem succesvol in je Active Directory-domein te integreren, heb je een naadloze verbinding tot stand gebracht tussen beide omgevingen. Dit opent de deur naar gecentraliseerd gebruikersbeheer en verbeterde beveiliging.

Gebruikers kunnen nu moeiteloos inloggen op het Linux-systeem met hun Active Directory-gegevens, terwijl systeembeheerders profiteren van geconsolideerd beheer over het hele netwerk.

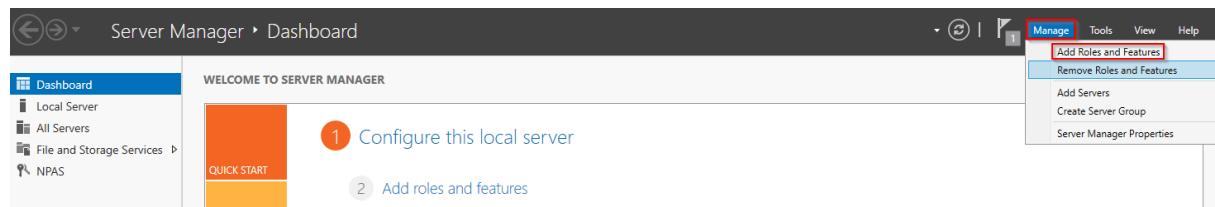
Kortom, de integratie biedt een efficiëntere en beter beheersbare omgeving voor zowel gebruikers als beheerders.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.2 RADIUS (Network policy server)

#### 6.2.1 Installatie NPS

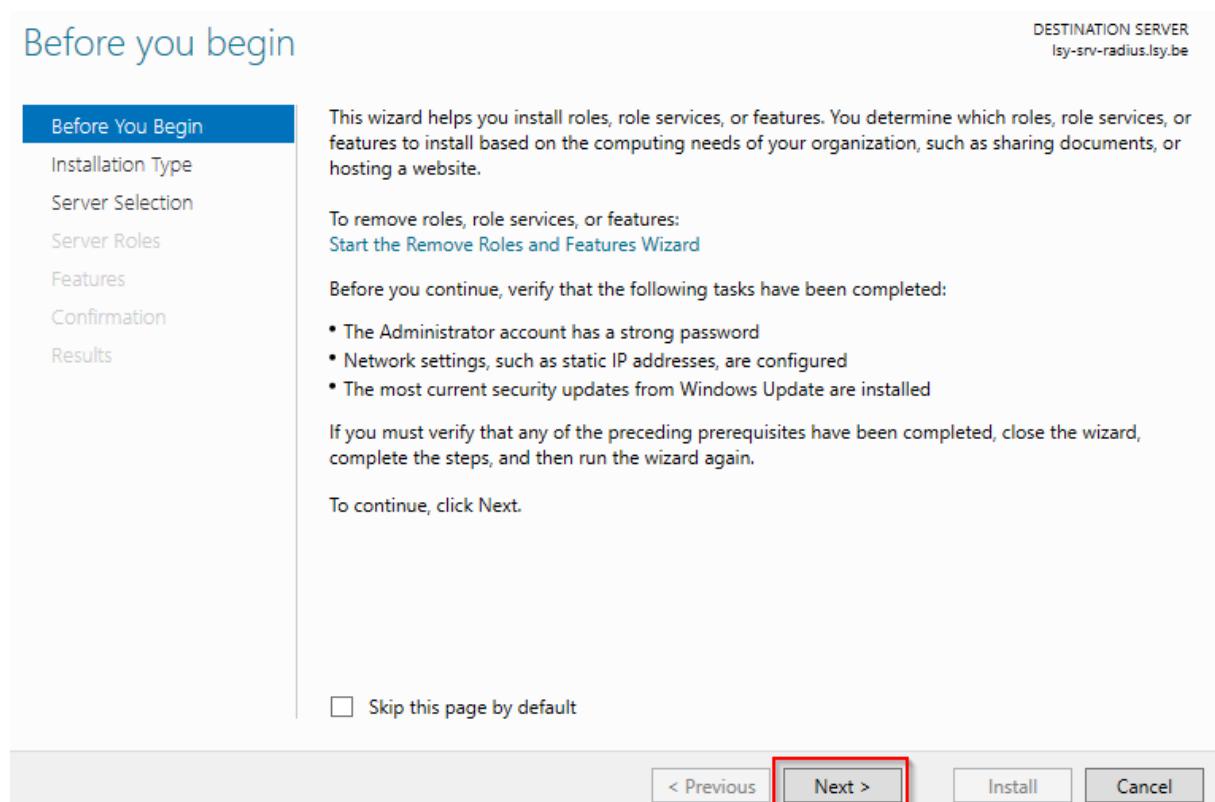
Navigeer in de server manager naar “Add roles and Features”.



Figuur 107: Installatie van de NPS (1)

In de volgende wizard zullen we de network policy and access services installeren. Deze services zullen ons helpen om de beveiling van ons netwerk te bewaren.

In onderstaand scherm drukken we op “next”.



Figuur 108: Installatie van de NPS (2)

In het volgende scherm kiezen we voor role-based or feature-based installation. Druk daarna op “next”.

## Automatisch toewijzen van een VLAN aan een gebruiker

## Select installation type

 DESTINATION SERVER  
 lsy-srv-radius.ls.y.be

Before You Begin  
**Installation Type**  
 Server Selection  
 Server Roles  
 Features  
 Confirmation  
 Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

**Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

**Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous **Next >** Install Cancel

Figuur 109: Installatie van de NPS (3)

Daarna kiezen we de server uit de server pool waar we de services willen gaan installeren. De server waarop je dit gaat installeren staat normaal gezien in de lijst van de server pool. Daarna drukken we op next om de server rol te kiezen.

## Select destination server

 DESTINATION SERVER  
 lsy-srv-radius.ls.y.be

Before You Begin  
 Installation Type  
**Server Selection**  
 Server Roles  
 Features  
 Confirmation  
 Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool  
 Select a virtual hard disk

Server Pool

Name	IP Address	Operating System
lsy-srv-radius.ls.y.be	172.30.1.3	Microsoft Windows Server 2022 Standard Evaluation

1 Computer(s) found

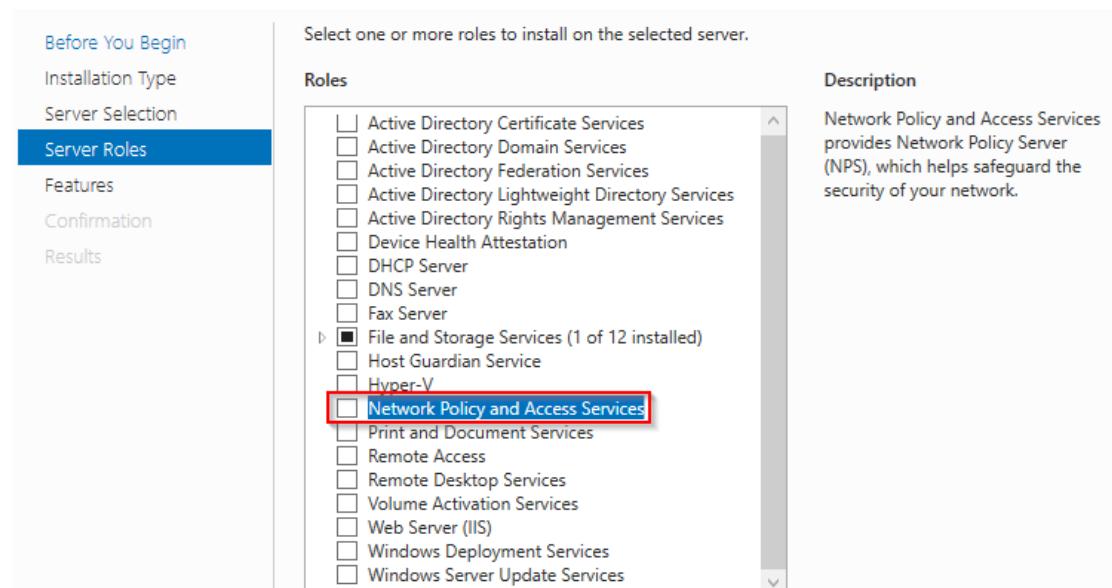
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous **Next >** Install Cancel

Figuur 110: Installatie van de NPS (4)

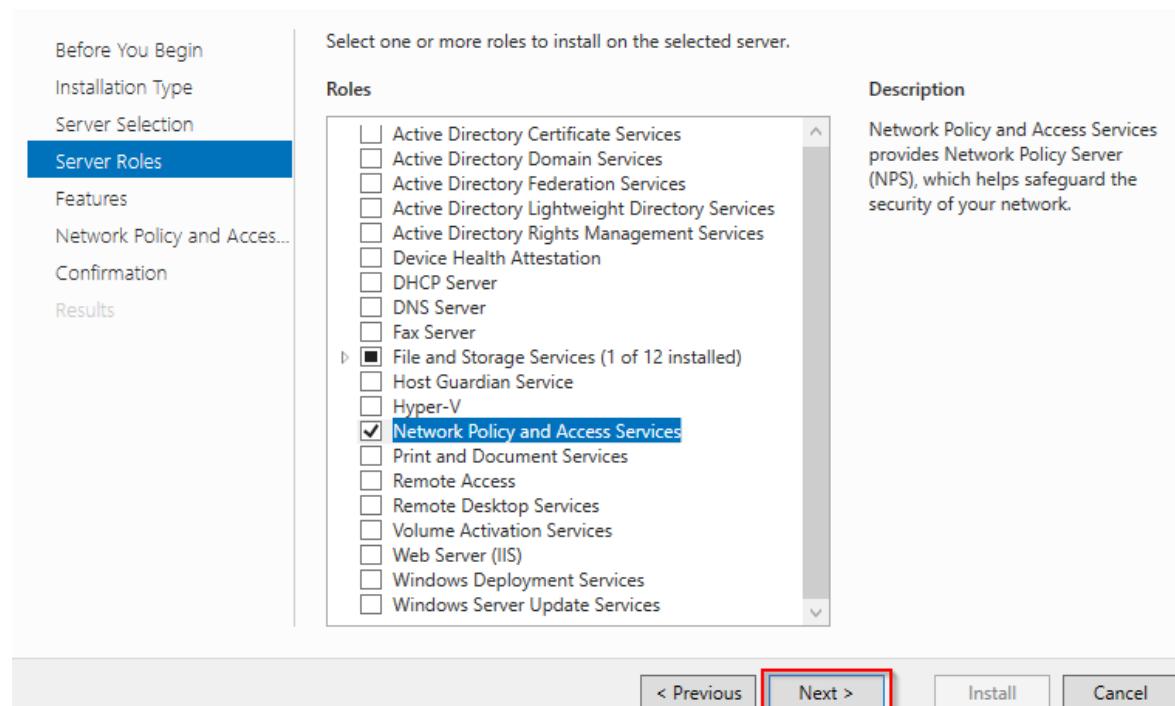
## Automatisch toewijzen van een VLAN aan een gebruiker

In het geval van de network policy server kiezen we voor network policy and access services.



Figuur 111: Installatie van de NPS (5)

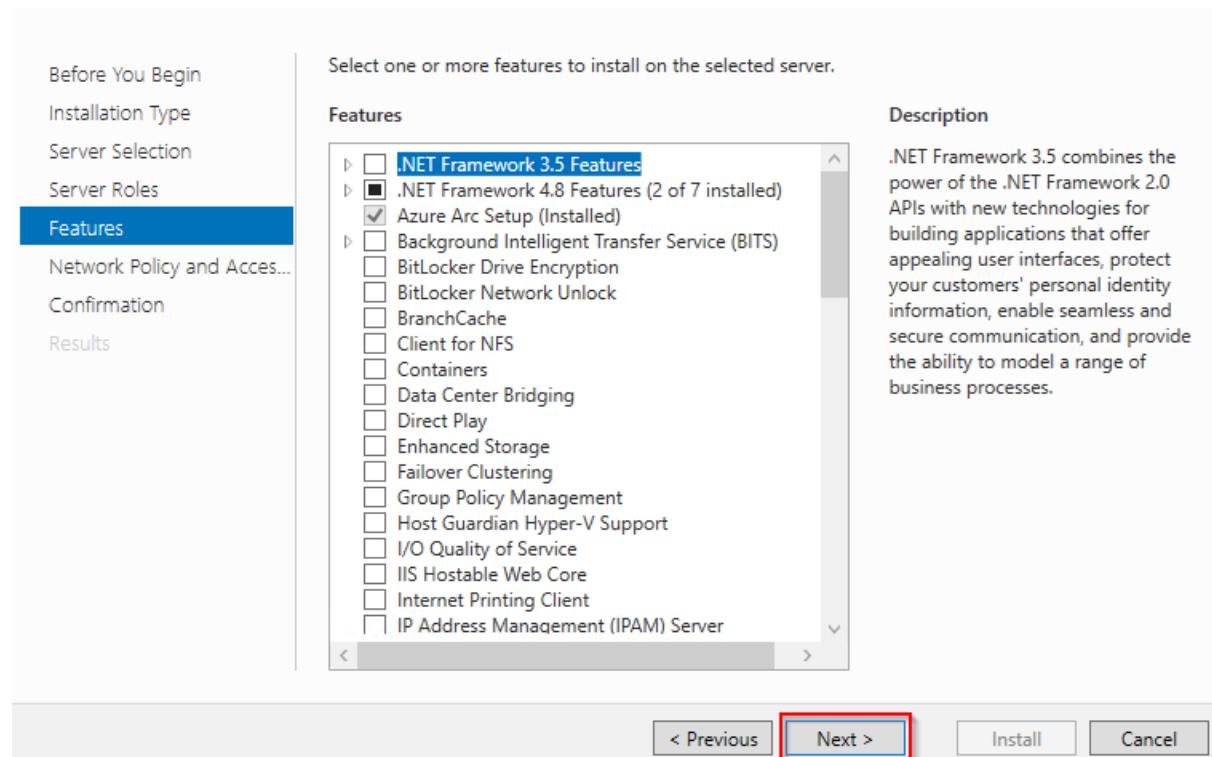
Daarna krijg je een pop-up om nog andere tools toe te voegen. Deze tools zijn vereist om met de services te werken. Hier druk je op “Add features”. In ondestaand scherm – na het kiezen van services/tools – druk je op next.



Figuur 112: Installatie van de NPS (6)

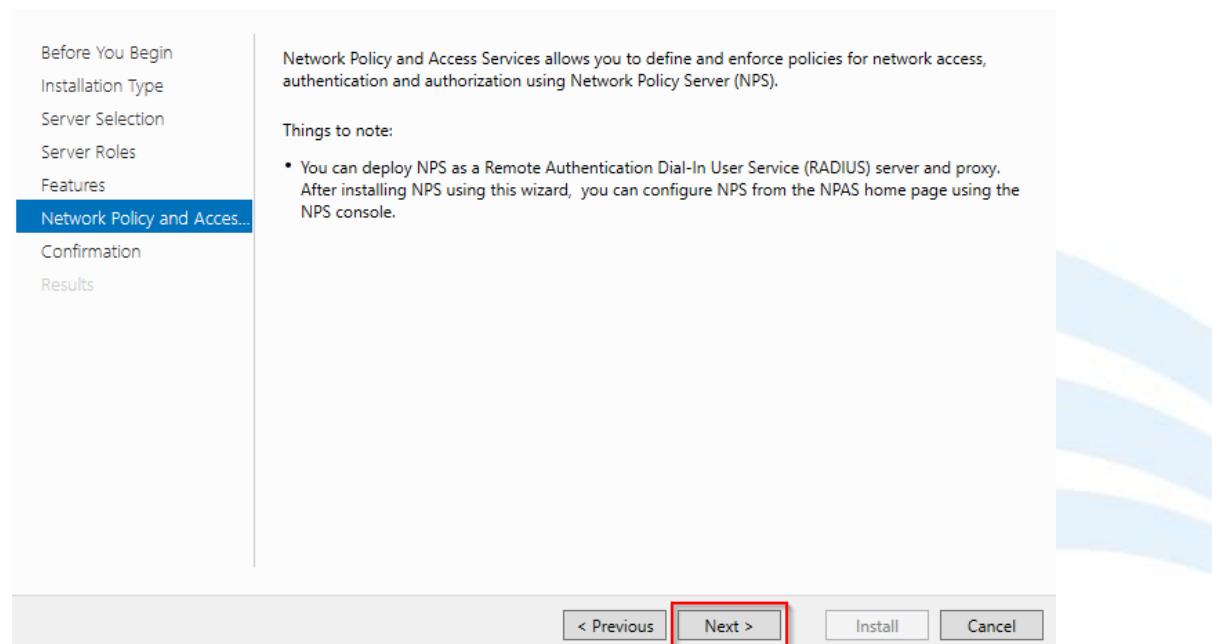
## Automatisch toewijzen van een VLAN aan een gebruiker

Er zijn geen extra features nodig voor de server. In dit scherm kunnen we op next drukken.



Figuur 113: Installatie van de NPS (7)

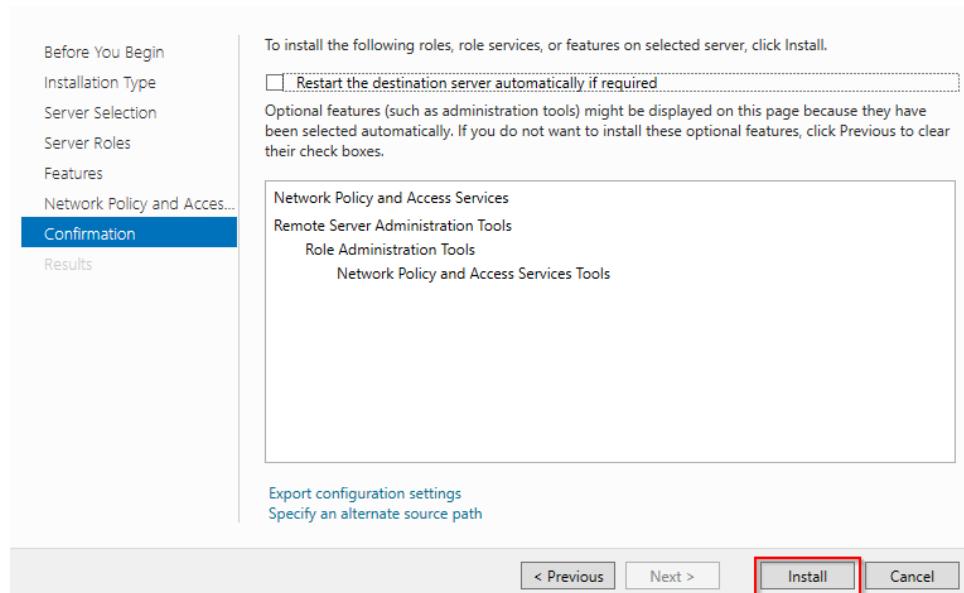
Er wordt in het volgende scherm informatie gegeven over wat de network policy server doet. Deze services die worden geïnstalleerd zullen het mogelijk maken om policy's te definieren en af te dwingen voor netwerk toegang. We drukken hier op next.



Figuur 114: Installatie van de NPS (8)

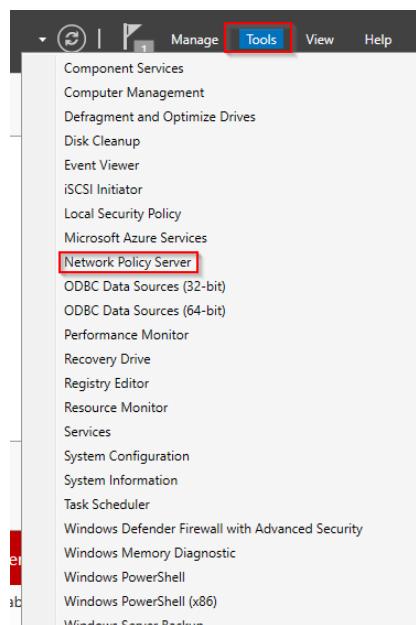
## Automatisch toewijzen van een VLAN aan een gebruiker

Daarna drukken we op install. Dan zullen de nodige services en tools geïnstalleerd worden om er een Network Policy Server van te maken. U kan er zelf voor kiezen om het herstarten van de server aan te vinken.



Figuur 115: Installatie van de NPS (9)

Na het installeren van de services en tools kan je in de server manager nageren naar de tools, in deze oplijsting zal je nu Network Policy server zien staan. Dit betekent dat de installatie succesvol is verlopen.

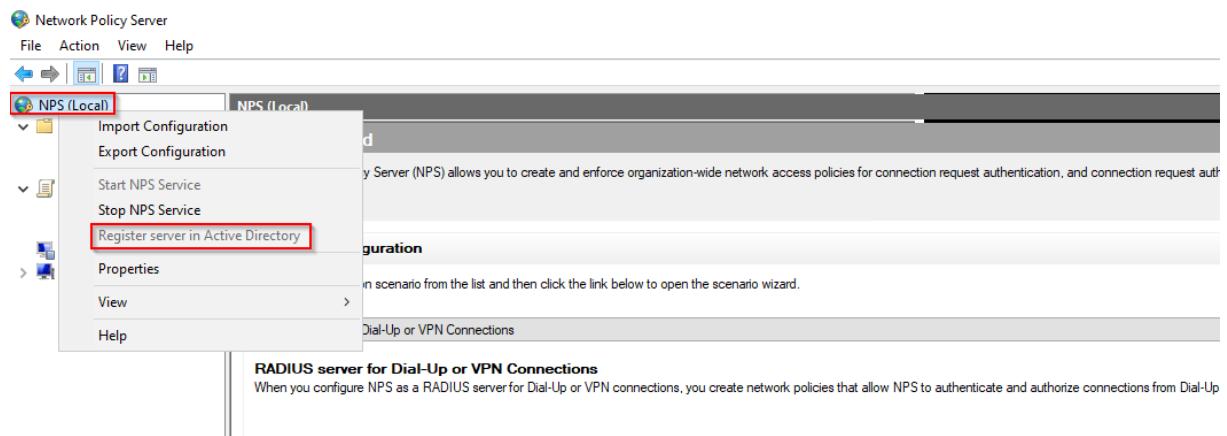


Figuur 116: Installatie van de NPS (10)

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.2.2 Registreren van server

We willen eerst de network policy server registreren in de active directory. We drukken op de rechtermuisknop en daarna registreren we de server in active directory.



Figuur 117: Configuratie van de NPS (1)

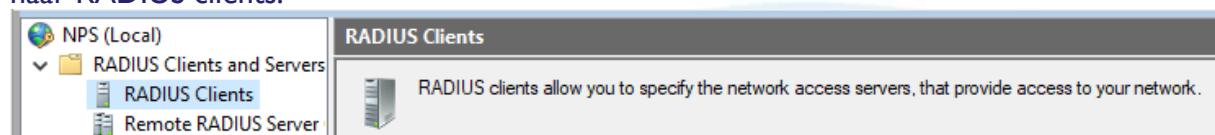
U klikt in de wizard 2-maal op ok.

Dit is verplicht omdat dit ervoor zal zorgen dat de server toegang heeft tot het lezen van dial-in properties van de users accounts tijdens het autorisatie process. Door het toevoegen wordt de NPS toegevoegd aan de RAS en IAS Server groepen in de active directory.

### 6.2.3 Configuratie RADIUS clients

RADIUS (Remote authentication dial-in user service) clients zullen u de toegang geven voor het verbinden van laptops waar gebruikers in zullen loggen. Deze clients zullen requests sturen naar de RADIUS server. Dit zijn switches, routers, access points maar kan ook VPN zijn. Deze zullen zorgen voor netwerktoegang.

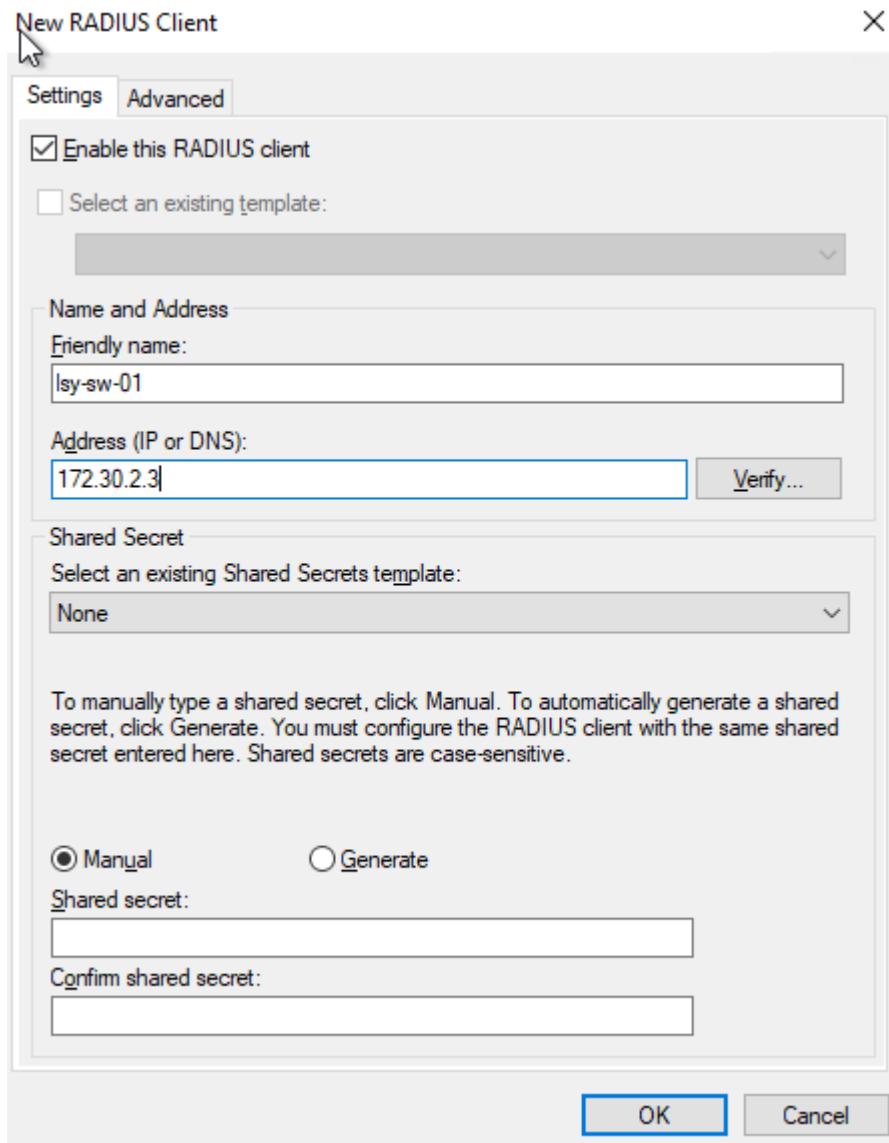
Voor het configureren van je radius client open je ‘radius clients and servers’ en navigeer je naar RADIUS clients:



Figuur 118: Configuratie van de NPS (2)

Voor een nieuwe aan te maken druk je op rechtermuisknop en daarna op nieuw. We kiezen hier voor een friendly name, zodat we weten welke netwerktoegangserver het is. Daarna geef je het IP adres mee. Na het ingeven van het IP adres gaan we een secret aanmaken, deze kan je genereren maar ook zelf manueel instellen. Het is belangrijk dat je deze goed bewaard omdat je deze nodig hebt voor de configuratie van de RADIUS server in de firewall en/of switch. Daarna druk je op OK.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 119: Configuratie van de NPS (3)

Bij het geavanceerd scherm kan je ook kiezen voor een vendor. RADIUS standard was oke hiervoor, maar je kan natuurlijk ook meer in het specifieke gaan mocht je een toestel hebben voor netwerktoegang voor een van deze vendors.

### 6.2.4 connection request policies

Connection request policies kun je angeven of verbindingsverzoeken lokaal worden verwerkt of doorgestuurd naar een remote radius server.

Deze kan je default laten staan: Use windows authentication for all users zou voldoende moeten zijn.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.2.5 Configuratie network policies

Netwerk policies laten je toe om aan te duiden wie geautorizeerd is om verbinding te maken met het netwerk en onder welke omstandigheden ze verbinding kunnen maken. Hiervoor hebben we momenteel 5 policy's opgesteld.

Elke gebruiker moet aan de gegeven conditie voldoen om op het netwerk te mogen. In dit geval plaatsen we de gebruikers in een groep op de domain controller zoals op onderstaande afbeelding te zien is de user group V52 production, iedereen die in deze groep zit zal een IP verkrijgen van het subnet dat aan deze VLAN is toegewezen.

In de instellingen helemaal beneden van de afbeelding worden er 3 belangrijke attributen meegegeven, het tunnel-medium-type, tunnel-pvt-group-id en het type van de tunnel. Dit is om aan te geven om de VLAN te wijzigen naar 52.

Het protocol dat gebruikt zal worden voor de authenticaties is MS-CHAP v2.

**Network Policies**

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
V52 Production Policy	Enabled	1	Grant Access	Unspecified
V53 Sales Policy	Enabled	2	Grant Access	Unspecified
V54 Marketing Policy	Enabled	3	Grant Access	Unspecified
V55 HR Policy	Enabled	4	Grant Access	Unspecified
V58 IT Policy	Enabled	5	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	6	Deny Access	Unspecified
Connections to other access servers	Enabled	7	Deny Access	Unspecified

**V52 Production Policy**

Conditions - If the following conditions are met:

Condition	Value
User Groups	LSY\V52 Production

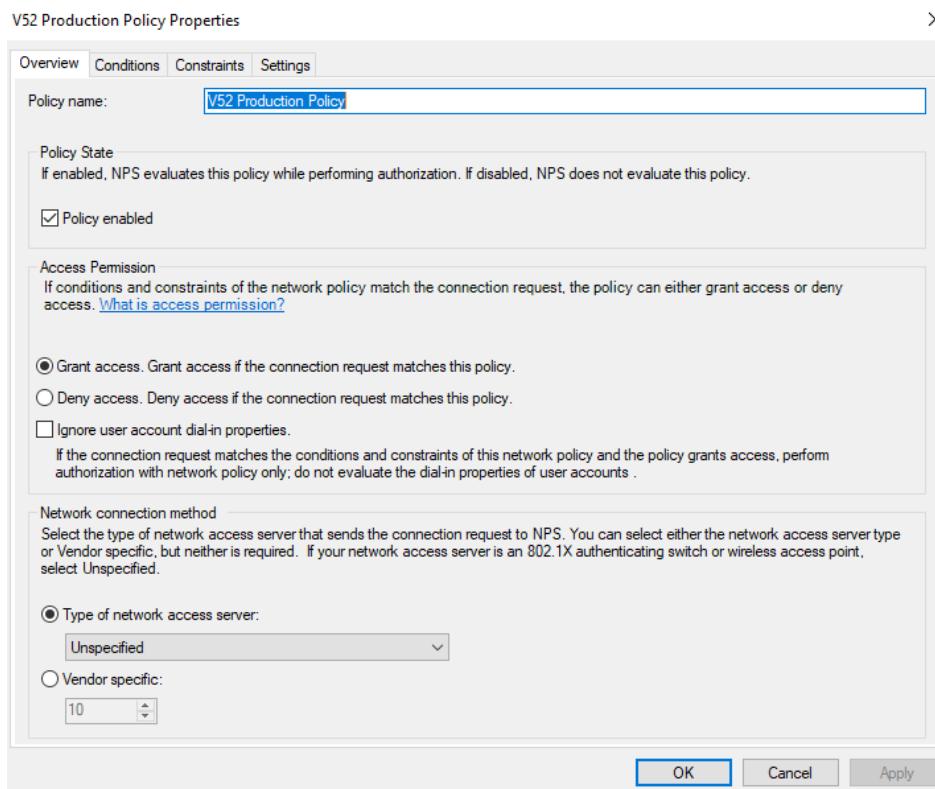
Settings - Then the following settings are applied:

Setting	Value
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
Authentication Method	EAP OR Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2...
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	52
Tunnel-Type	Virtual LANs (VLAN)

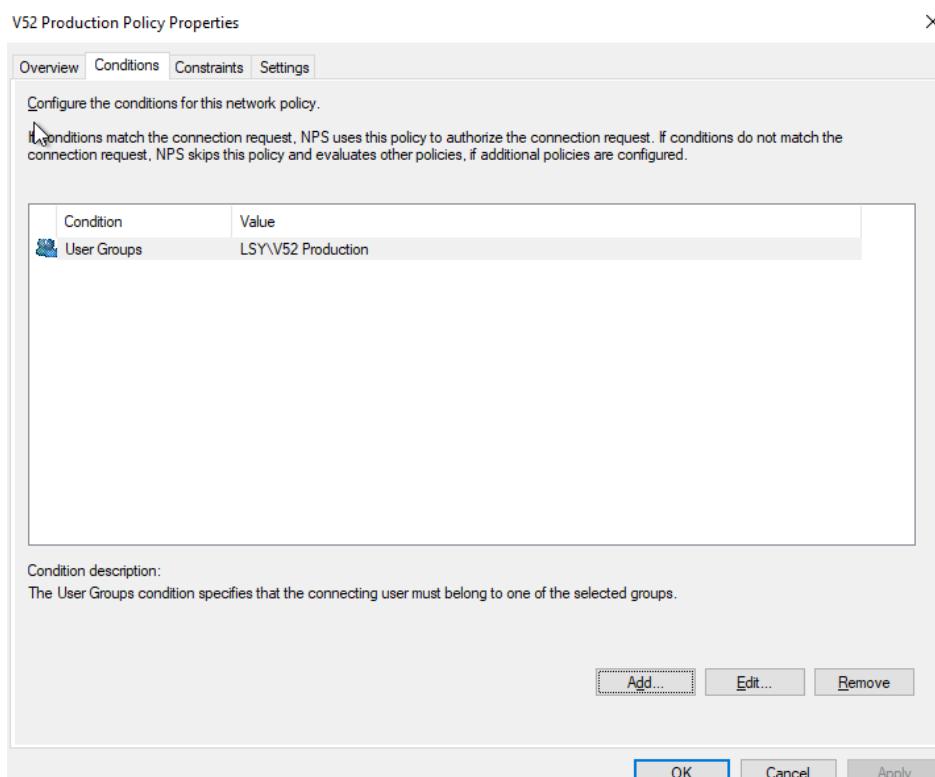
Figuur 120: Configuratie van de NPS (4)

Dit is voor het configureren van de policy.

## Automatisch toewijzen van een VLAN aan een gebruiker

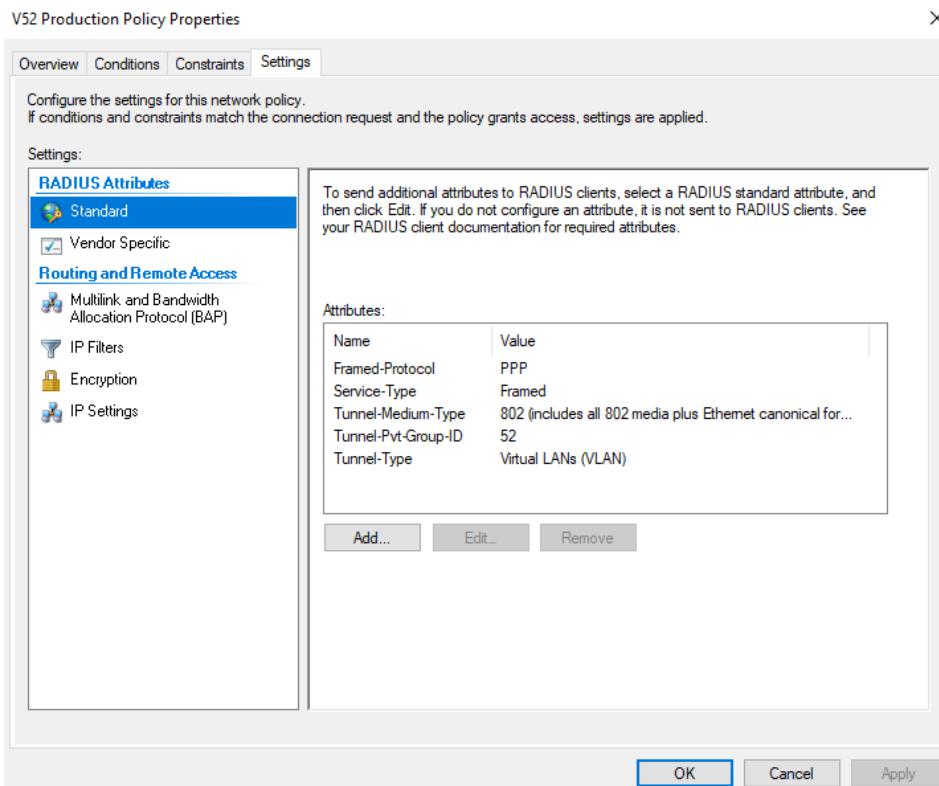


Figuur 121: Configuratie van de NPS (5)

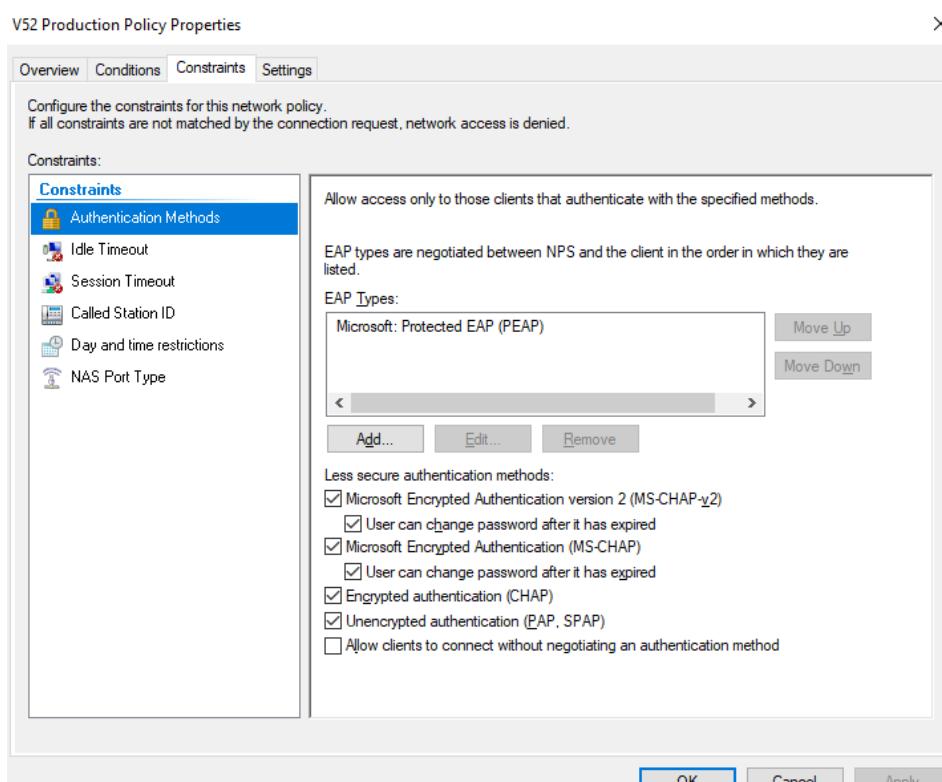


Figuur 122: Configuratie van de NPS (6)

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 123: Configuratie van de NPS (7)



Figuur 124: Configuratie van de NPS (8)

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.3 Fileserver

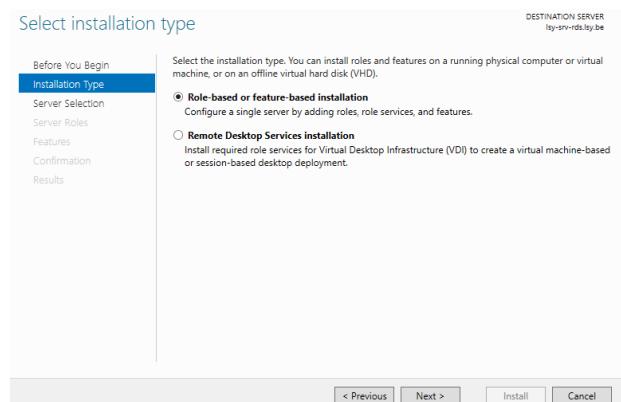
#### 6.3.1 Installatie services

Navigeer in de server manager naar “Add roles and Features”.



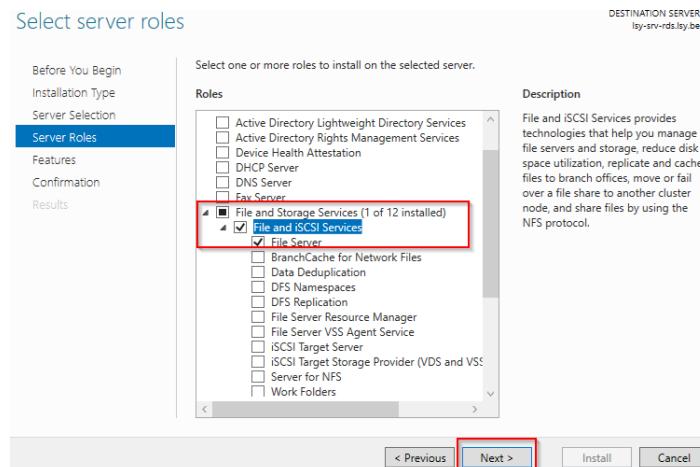
Figuur 125: Installatie van de fileserver (1)

Daarna krijgen we een wizard waar we kiezen voor role-based or feature-based installatie. Klik daarna op next.



Figuur 126: Installatie van de fileserver (2)

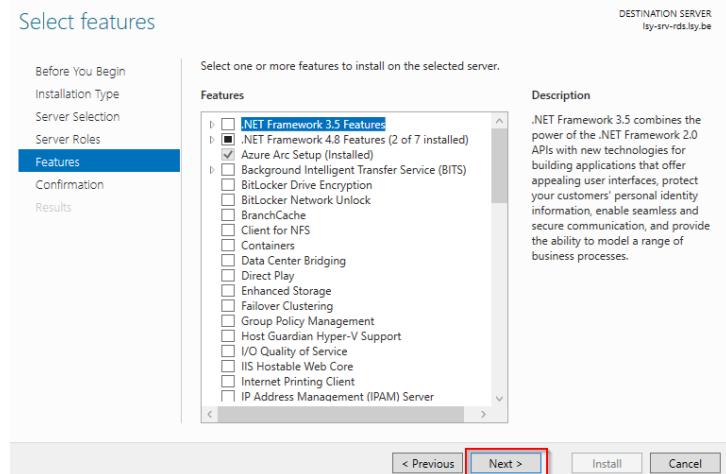
In het volgende scherm selecteren we de server waarop we de file and iSCSI server roles gaan installeren, deze staat normaal default correct, druk hier op next. Daarna krijgen we het scherm voor het selecten van de server roles, we open file and storage services verder en selecteren hier file and iSCSI services, als we deze verder openen staat enkel file server aangeduid, dit is voldoende voor installatie. We drukken daarna op next.



Figuur 127: Installatie van de fileserver (3)

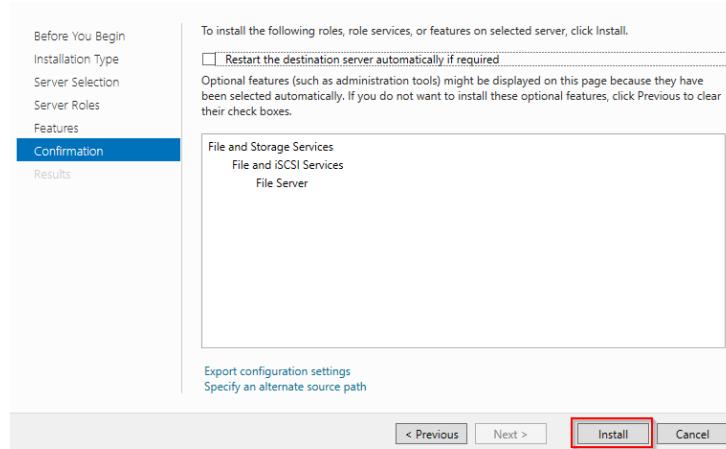
## Automatisch toewijzen van een VLAN aan een gebruiker

In het volgende scherm komen we in het features scherm, hier selecteren we geen extras en drukken op next.



Figuur 128: Installatie van de fileserver (4)

Dan komen we aan bij het bevestigen van de installatie. We kiezen ervoor om de bestemmingsserver te herstarten, door op de box te klikken. Dit zou normaal niet nodig zijn.

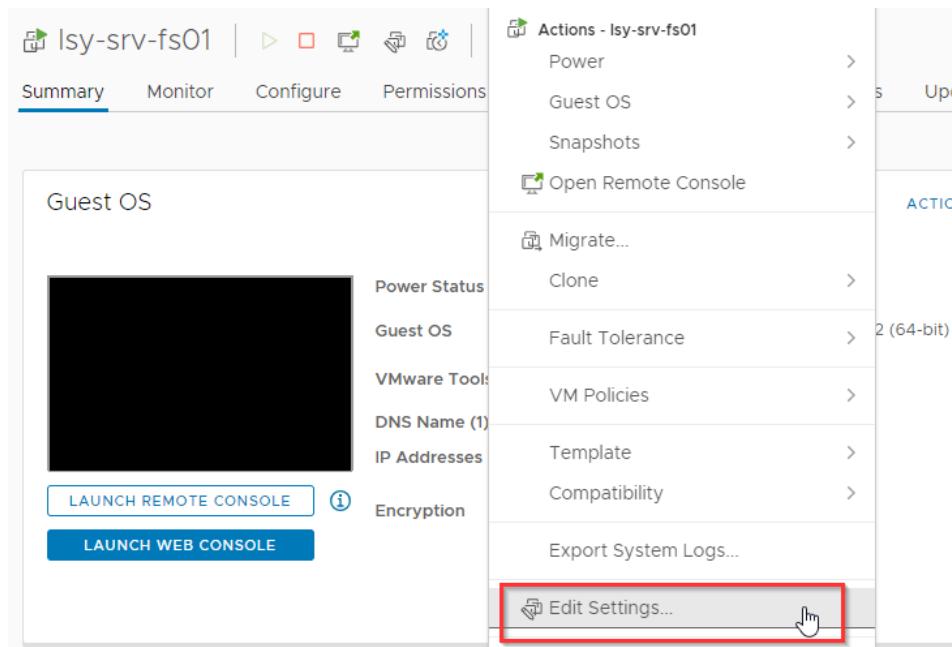


Figuur 129: Installatie van de fileserver (5)

### 6.3.2 Toevoegen van een extra schijf

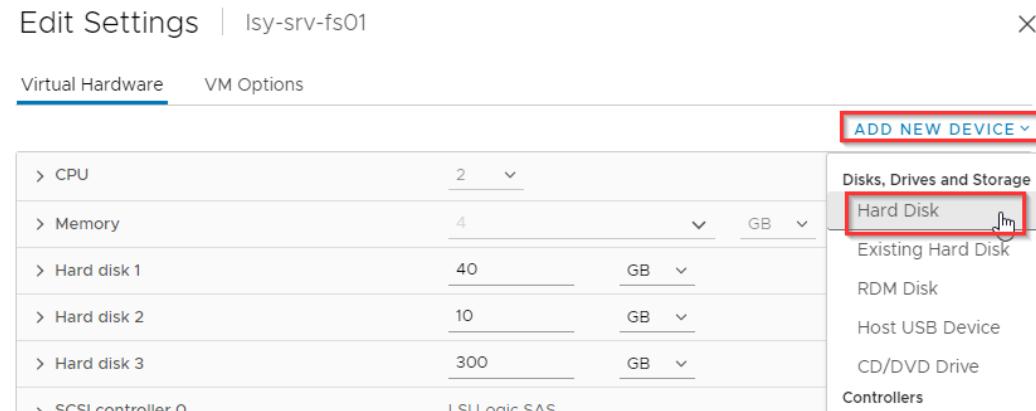
Voor het toevoegen van een extra schijf aan de fileserver, gaan we naar de vCenter. In vCenter zullen we gaan naar de virtuele machine. Als we bij de virtuele machine zijn gaan we de instellingen editeren.

## Automatisch toewijzen van een VLAN aan een gebruiker



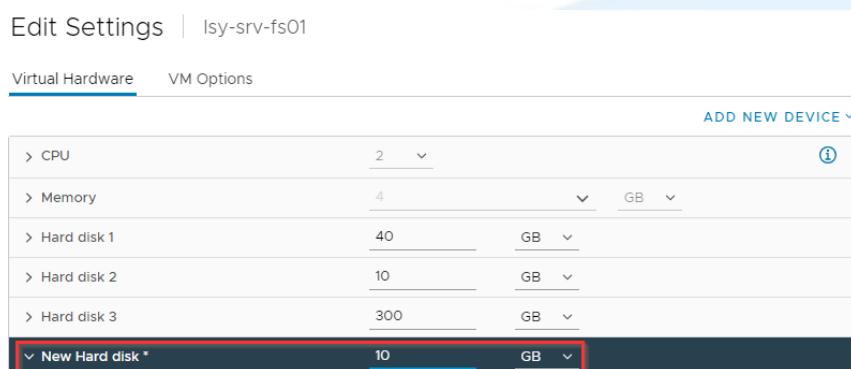
Figuur 130: vSphere extra drive aanmaken (1)

In de instellingen van de virtuele machine voegen we een nieuwe harde schijf aan toe.



Figuur 131: vSphere extra drive aanmaken (2)

Deze nieuwe harde schijf geven we 10 GB vrije ruimte. Daarna drukken we op OK.



Figuur 132: vSphere extra drive aanmaken (3)

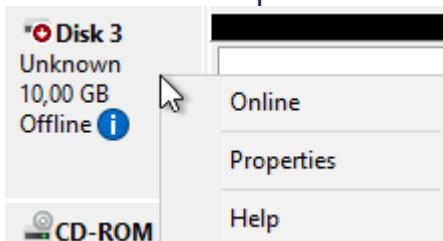
## Automatisch toewijzen van een VLAN aan een gebruiker

Na het aanmaken van de virtuele harde schijf gaan we terug op de fileserver en hier gaan we naar disk management. Hierin zal er een offline disk zijn, deze moeten we online gaan brengen om de schijf te kunnen gebruiken.



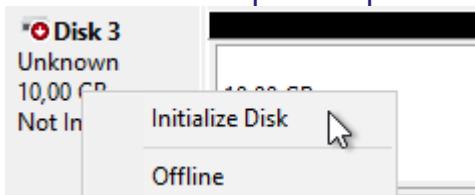
Figuur 133: vSphere extra drive aanmaken (4)

Het online brengen doen we door de rechter muisknop te drukken op het vak van de schijf. We drukken hier op online.



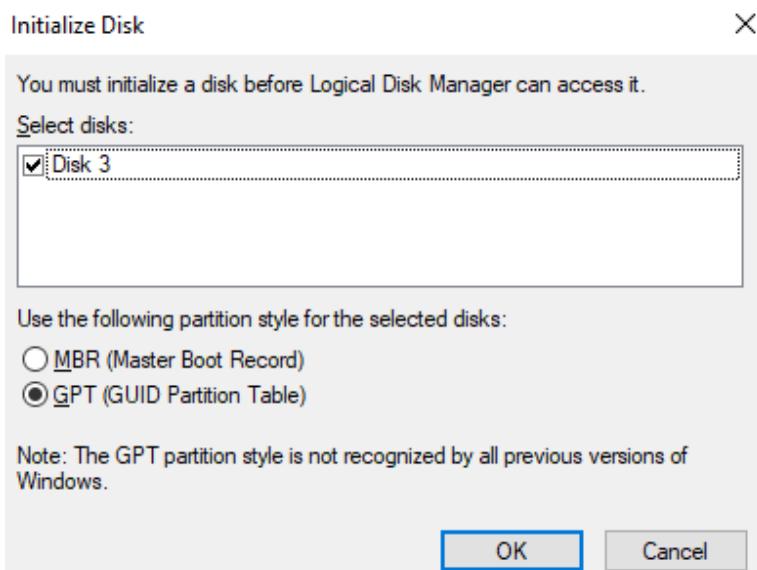
Figuur 134: vSphere extra drive aanmaken (5)

Na de schijf online te brengen zien we dat deze nog niet geïnitialiseerd is en zullen deze initialiseren door op de knop initialize disk te drukken.



Figuur 135: vSphere extra drive aanmaken (6)

Daarna krijg je een pop-up, hierin kan je op OK drukken.



Figuur 136: vSphere extra drive aanmaken (7)

## Automatisch toewijzen van een VLAN aan een gebruiker

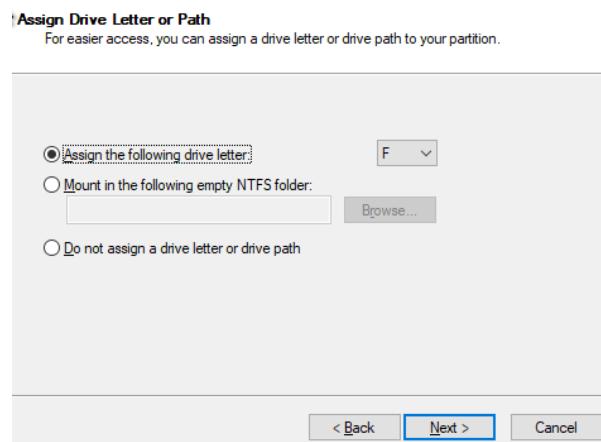
We zien dat de disk nu online is gebracht maar de vrij ruimte is er nog niet aan toegekend. Hiervoor zullen we met rechter muisknop drukken op de vrije ruimte waar unallocated staat. Daarna op new simple volume.



Figuur 137: vSphere extra drive aanmaken (8)

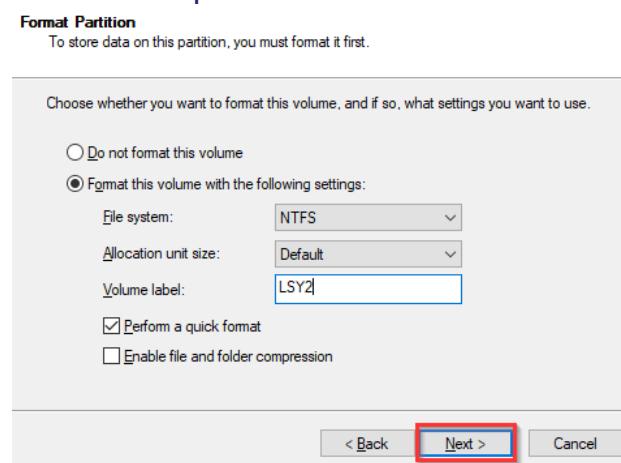
Nu komen we in een wizard terecht voor het opzetten van het volume. In het eerste scherm druk je op next. Daarna weer op next, in het scherm kan je nog een bepaalde grootte in megabytes meegeven hoe groot de schijf mag zijn. Normaal staat dit op de gehele vrije ruimte.

Daarna gaan we de schijf een letter toekennen. Dit zal direct al een vrije beschikbare letter geven. Je kan via de drop-down van de letter een andere letter naar keuze kiezen. Na het kiezen van de letter druk je op next.



Figuur 138: vSphere extra drive aanmaken (9)

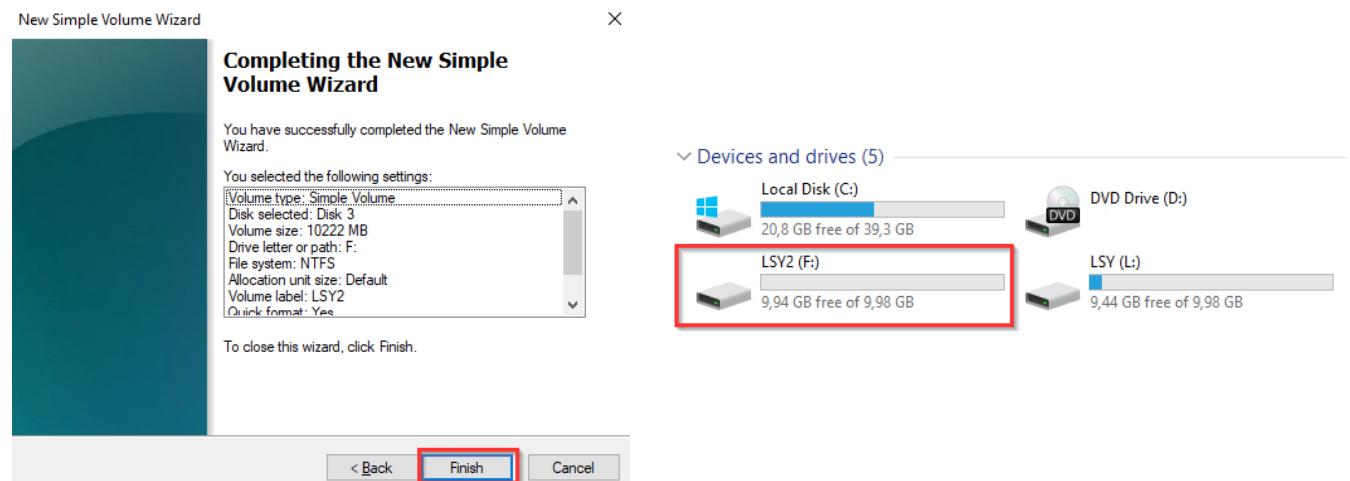
In het volgende scherm geven we mee welke naam of label we het volume geven. Daarna drukken we op next.



Figuur 139: vSphere extra drive aanmaken (10)

## Automatisch toewijzen van een VLAN aan een gebruiker

In de laatste stap zien we een overzicht van de instellingen. Hier klikken we op finish om het volume te finaliseren. Dan zal de schijf formatteren en dan is de schijf online. Dit kan je daarnaast ook controleren in de file explorer van de fileserver.

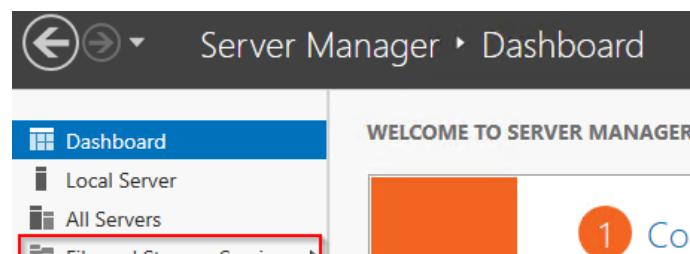


Figuur 140: vSphere extra drive aanmaken (1)

### 6.3.3 Aanmaken share

Na de installatie van de fileserver gaan we een share aanmaken. Deze share zal het mogelijk maken om bestanden op te slaan in deze map die ook toegankelijk voor meerdere gebruikers.

We navigeren naar file and storage services, en vervolgens naar shares.



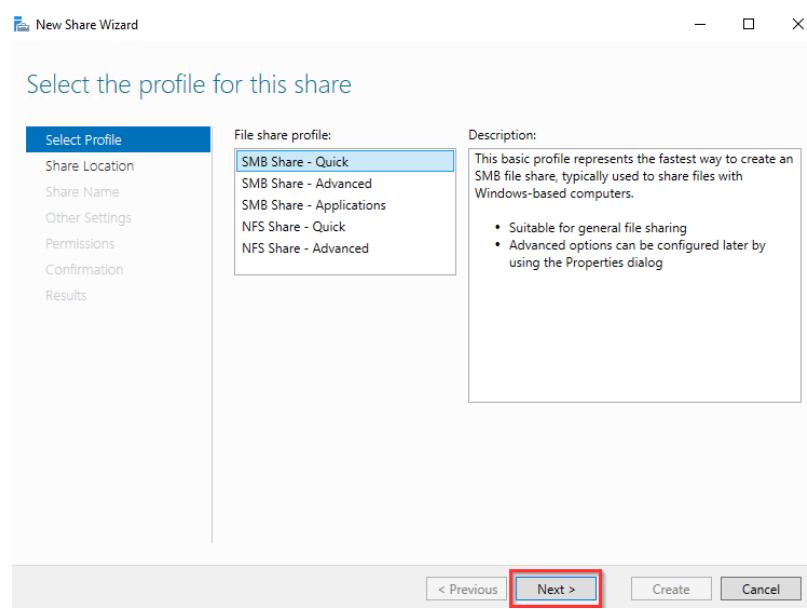
Figuur 141: File share aanmaken (1)

Share	Local Path	Protocol	Availability Type
lsy-srv-fs01 (2)	L:\Shares\Data	SMB	Not Clustered

Figuur 142: File share aanmaken (2)

## Automatisch toewijzen van een VLAN aan een gebruiker

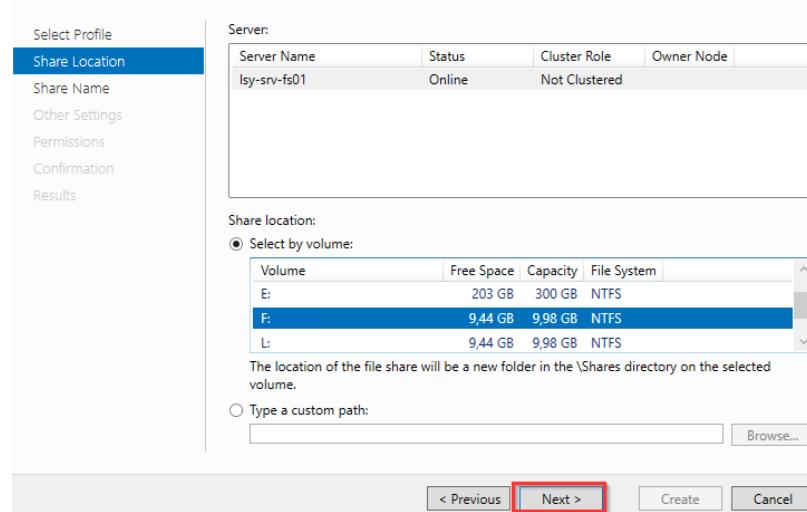
Voor het aanmaken van een nieuwe share drukken we op rechter muisknop onder de fileserver en drukken op new share. Als je hier op hebt gedrukt kom je terecht in een wizard voor het aanmaken van een share. In het eerste scherm van de wizard kiezen we voor een SMB share – Quick en daarna drukken we op next.



Figuur 143: File share aanmaken (3)

Als we op next hebben gedrukt kiezen we het aangemaakt volume. In dit geval is dit de F-schijf. Daarna klikken we op next.

### Select the server and path for this share



Figuur 144: File share aanmaken (4)

Daarna kiezen we een naam. Aangezien dit een extra share is voor ons, zullen we als share naam Data2 gebruiken. Na het kiezen van een gepaste naam van de share drukken we op next.

## Automatisch toewijzen van een VLAN aan een gebruiker

### Specify share name

Select Profile  
Share Location  
**Share Name**  
Other Settings  
Permissions  
Confirmation  
Results

Share name: Data2  
Share description:  
Local path to share: F:\Shares\Data2  
If the folder does not exist, the folder is created.  
Remote path to share: \\lsy-srv-fs01\Data2

< Previous **Next >** Create Cancel

Figuur 145: File share aanmaken (5)

We gaan nu nog extra instellingen instellen op de share. We drukken het vakje van “enable access-based enumeration”. Dit zal er voor zorgen dat wanneer een gebruiker niet minimaal lees rechten heeft voor een folder, zal deze verborgen worden voor de gebruiker. Daarnaast staat chaching van de share automatisch al ingeschakeld wat ervoor zal zorgen dat de content in de fileshare ook voor offline gebruikers zichtbaar is.

### Configure share settings

Select Profile  
Share Location  
Share Name  
**Other Settings**  
Permissions  
Confirmation  
Results

Enable access-based enumeration  
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

Allow caching of share  
Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

Enable BranchCache on the file share  
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Encrypt data access  
When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

< Previous **Next >** Create Cancel

Figuur 146: File share aanmaken (6)

Momenteel laten we de rechten zo staan, we zullen deze aanpassen na de groepen voor de mappen hebben aangemaakt te hebben, in dit scherm mag je op next drukken.

## Automatisch toewijzen van een VLAN aan een gebruiker

### Specify permissions to control access

Select Profile  
Share Location  
Share Name  
Other Settings  
**Permissions**  
Confirmation  
Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu..	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

[Customize permissions...](#)

< Previous **Next >** Create Cancel

Figuur 147: File share aanmaken (7)

Bij het bevestigen van de share drukken we op create. Daarna op close. Na deze stap zal ik verder gaan met de aangemaakte data share.

### Confirm selections

Select Profile  
Share Location  
Share Name  
Other Settings  
Permissions  
**Confirmation**  
Results

Confirm that the following are the correct settings, and then click Create.

SHARE LOCATION	
Server:	Igy-srv-fs01
Cluster role:	Not Clustered
Local path:	F:\Shares\Data2

SHARE PROPERTIES	
Share name:	Data2
Protocol:	SMB
Access-based enumeration:	Enabled
Caching:	Enabled
BranchCache:	Disabled
Encrypt data:	Disabled

< Previous **Create** Next > Cancel

Figuur 148: File share aanmaken (8)

### 6.3.4 Users en computers groepen

Daarna gaan we naar de Active Directory users and computers op de domain controlleren en hebben hier een OU aangemaakt genaamd groups met hierin access groups en ACL. Deze ACLs gaan we gebruiken voor het toekennen van rechten op de mappen in de share. In de access groep gaan we de laagste mogelijk rechten geven.

De access groepen zijn van het type security en de scope is universeel. We hebben hier steeds de functie en hier medewerker of manager. De manager zal steeds meer rechten verkrijgen bij elke functie.

## Automatisch toewijzen van een VLAN aan een gebruiker

Name	Type
HR Employee	Security Group - Universal
HR Manager	Security Group - Universal
IT Employee	Security Group - Universal
IT Manager	Security Group - Universal
Marketing Employee	Security Group - Universal
Marketing Manager	Security Group - Universal
Production Employee	Security Group - Universal
Production Manager	Security Group - Universal
Sales Employee	Security Group - Universal
Sales Manager	Security Group - Universal

**Active Directory Users and Computers**  
> **Saved Queries**  
**Isy.be**  
> **Builtin**  
> **Computers**  
> **Domain Controllers**  
> **ForeignSecurityPrincipals**  
**LSY**  
> **Computers**  
> **Groups**  
> **Access Groups**  
> **ACL**  
> **RADIUS**  
> **Servers**  
> **Users**  
> **Managed Service Accounts**  
> **Users**

Figuur 149: Overzicht van de groepen

Daarnaast hebben we ook nog ACLs aangemaakt in de OU van de access control lists. De groepen zijn van het type security en de scope domein lokaal. Als belangrijkste voegen we hier de LSY-ADM fs01 aan toe. Dit is een universele groep. Deze zal ervoor zorgen dat de administrators van het systeem altijd rechten hebben tot elke folders en bestanden die nieuw worden aangemaakt.

Name	Type	Description
LSY-ACL DataLX	Security Group - Domain Local	\\\isy-srv-fs01\Data\
LSY-ACL DataHR L	Security Group - Domain Local	\\\isy-srv-fs01\Data\HR\
LSY-ACL DataHREmployee M	Security Group - Domain Local	\\\isy-srv-fs01\Data\HR\Employee
LSY-ACL DataHrManager M	Security Group - Domain Local	\\\isy-srv-fs01\Data\HR\Manager
LSY-ACL DataIT L	Security Group - Domain Local	\\\isy-srv-fs01\Data\IT\
LSY-ACL DataITEmployee M	Security Group - Domain Local	\\\isy-srv-fs01\Data\IT\Employee
LSY-ACL DataITManager M	Security Group - Domain Local	\\\isy-srv-fs01\Data\IT\Manager
LSY-ACL DataMarketing L	Security Group - Domain Local	\\\isy-srv-fs01\Data\Marketing\
LSY-ACL DataMarketingEmployee M	Security Group - Domain Local	\\\isy-srv-fs01\Data\Marketing\Employee
LSY-ACL DataMarketingManager M	Security Group - Domain Local	\\\isy-srv-fs01\Data\Marketing\Manager
LSY-ACL DataProduction L	Security Group - Domain Local	\\\isy-srv-fs01\Data\Production\
LSY-ACL DataProductionEmployee M	Security Group - Domain Local	\\\isy-srv-fs01\Data\Production\Employee
LSY-ACL DataProductionManager M	Security Group - Domain Local	\\\isy-srv-fs01\Data\Production\Manager
LSY-ACL DataSales L	Security Group - Domain Local	\\\isy-srv-fs01\Data\Sales\
LSY-ACL DataSalesEmployee M	Security Group - Domain Local	\\\isy-srv-fs01\Data\Sales\Employee
LSY-ACL DataSalesManager M	Security Group - Domain Local	\\\isy-srv-fs01\Data\Sales\Manager
LSY-ADM Isy-srv-fs01	Security Group - Universal	

Figuur 150: Overzicht van de ACL groepen

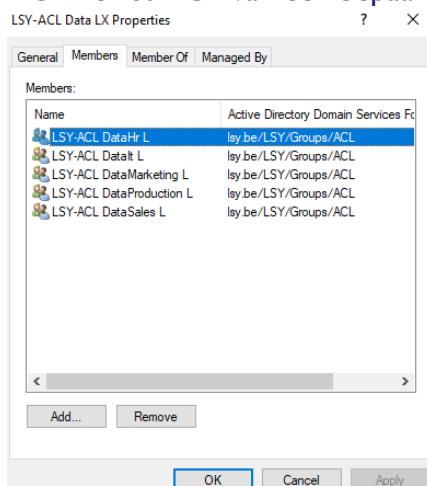
De domein lokale groepen zullen ervoor zorgen dat de machtigingen enkel worden toegewezen aan middelen binnen hetzelfde domein. Daarentegen zorgen de universele groepen ervoor dat je toegang kan bieden over meerde domeinen. Globale groepen zorgen dan weer voor gebruikers die vergelijkbare netwerktoegangsvereisten delen binnen hetzelfde domein.

In deze opstelling staat L voor list en M voor modify, de X na de L die toebehoort tot het hoogste niveau van de bestandstructuur staat ervoor dat overerving is uitgeschakeld.

Daarnaast geven we elke ACL ook een descriptie van waar deze in de filestructuur is toegepast. Dit geeft nuttige informatie van waar je deze kan terugvinden mocht er een probleem zijn.

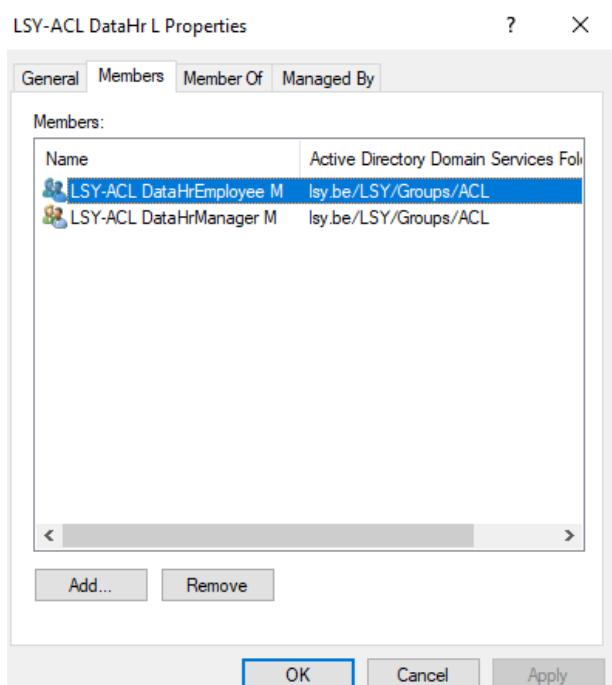
## Automatisch toewijzen van een VLAN aan een gebruiker

Als we de ACLs verder gaan bekijken dan gaan we deze ook in elkaar steken. Zo gaan we een slang van rechten creëren. Zo behoort – in deze opstelling – elke list(L) ACL tot deze in de map erboven. Zoals in onderstaande afbeelding te zien is zijn de leden van de Data LX ACL de list ACL van een bepaalde afdeling.



Figuur 151: Members van de groep LSY-ACL (1)

Daarnaast heeft de list ACL van elke afdeling ook de andere rechten van deze afdeling met als voorbeeld Hr.

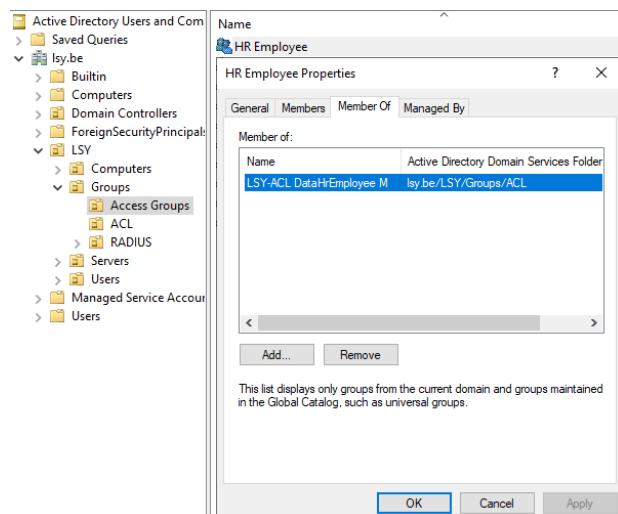


Figuur 152: Members van de groep LSY-ACL (2)

In andere woorden wil dit zeggen dat een gebruiker beschikt over één van deze modify rechten, hij/zij de list rechten mee krijgt van de mappen daarboven. Als we dan naar onze structuur gaan kijken zal deze enkel de map van HR kunnen zien in de data map, niet de marketing, production enzovoort.

## Automatisch toewijzen van een VLAN aan een gebruiker

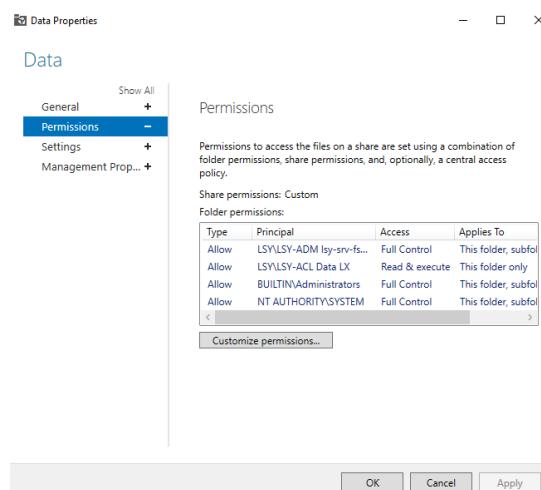
Het laagste niveau van ACL wordt ook enkel toegevoegd in de access groepen. Dit zijn de modify (M) rechten op het laagste niveau van de mappen. In onderstaande afbeeldingen zie je dat de groep HR employee enkel de modify rechten bevat van de medewerker.



Figuur 153: Members van de groep LSY-ACL (3)

### 6.3.5 Share rechten aanpassen.

Om de share rechten aan te passen gaan we in de server manager naar file and storage services en daarna naar de shares. We drukken de rechter muisknop op de share die we hebben toegevoegd en navigeren hier naar de permissies. Daarna customize permissions en als eerste gaan we overerving uitschakelen.



Figuur 154: Members van de groep LSY-ACL (4)

We verwijderen de principal BUILTIN\Users van de share. Dit doen we zodat niet elke domain users in elke map kan. Daarnaast verwijderen we ook Creator owner van de rechten. Mochten we creator owner niet verwijderen dan zou dit een hoog security risico

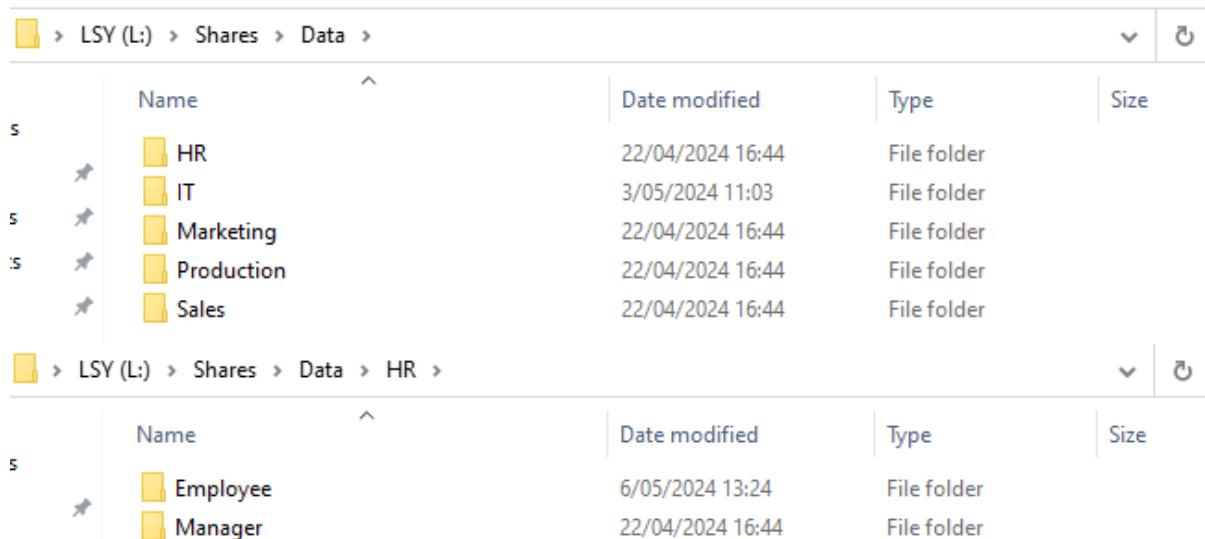
## Automatisch toewijzen van een VLAN aan een gebruiker

zijn: er zouden namelijk mensen, gebruikers van de fileserver de mogelijkheid kunnen krijgen om een eigen “fileserver” van de fileserver te maken waar de admins geen rechten meer over hebben aangezien de creator owner full control heeft en de rechten op deze map gewoon kan aanpassen.

We voegen ook groepen toe aan de share zelf. We voegen de list groep van het hoogste niveau toe aan deze map. Dit is de ACL data LX, deze wordt enkel op de data map toegevoegd. Deze groep krijgt lees en execute rechten op deze map zodat alle gebruikers die rechten hebben op de fileserver in de data map geraken. Daarnaast voegen we de LSY-ADM lsy-srv-fs01 ook toe met volledige controle met overerving ('this folder, subfolder en files'). Deze zal full control krijgen over de hele structuur, dit is enkel voor de administrator die eventueel rechten moeten aanpassen etc.

### 6.3.6 Rechten aan de mappen toekennen.

Als we gaan kijken naar onze bestandstructuur hebben we de data map als share ingesteld. In deze map staat er een map voor elke afdeling. In elke afdeling staat er een map voor de werknemers en één voor manager(s) van de afdeling.



	Name	Date modified	Type	Size
s	HR	22/04/2024 16:44	File folder	
s	IT	3/05/2024 11:03	File folder	
s	Marketing	22/04/2024 16:44	File folder	
s	Production	22/04/2024 16:44	File folder	
s	Sales	22/04/2024 16:44	File folder	

	Name	Date modified	Type	Size
s	Employee	6/05/2024 13:24	File folder	
s	Manager	22/04/2024 16:44	File folder	

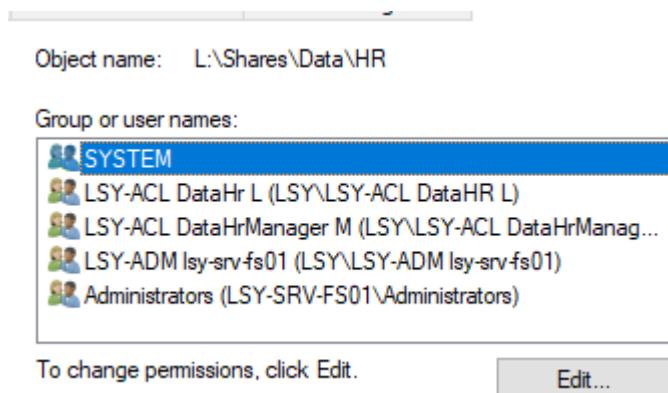
Figuur 155: Groepen toekennen aan een folder (I)

De rechten van de map Data hebben we al eerder veranderd in de server manager zelf. Voor elke afdeling zal je steeds op dezelfde manier rechten toekennen. Ik neem als voorbeeld de map van HR.

Op elke afdeling plaatsen we minstens als de rechten de list (read, list folder contents en read & execute) van deze afbeelding maar daarnaast voegen we aan de afdelingsmap ook de manager modify rechten toe.

In de mappen van de afdelingen voegen we de employee modify rechten toe aan de map van de employee. In de manager map voegen we deze ook toe maar dan als deny.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 156: Groepen toekennen aan een folder (2)

Permissions for LSY-ACL DataHrEmployee M		
	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Figuur 157: Groepen toekennen aan een folder (3)

## 6.4 Management

We gebruiken de management server om overal toegang te hebben en ook om configuraties uit te voeren binnen het netwerk. Dit biedt ook een extra beveiligingslaag, omdat alleen bepaalde gebruikersgroepen toegang krijgen voor beheerdoeleinden.

Stel dat je naar een klant gaat voor onderhoud en zij maken gebruik van netwerksegmentatie. Door jezelf in de beheergroep in de domain controller te plaatsen, krijg je toegang tot het VLAN wanneer je verbinding maakt met het bekabelde netwerk. Hierdoor kun je de management server bereiken en toegang krijgen tot alle benodigde resources om het onderhoud uit te voeren.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.5 Back-up (Veeam)

#### 6.5.1 Installatie Veeam

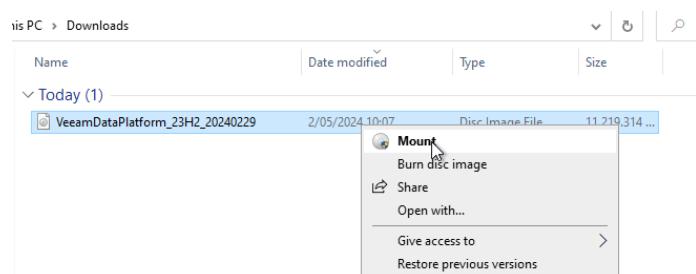
- Begin met het downloaden van Veeam vanaf de officiële website.

Je kunt het vinden op: <https://www.veeam.com/data-platform-trial-download.html>



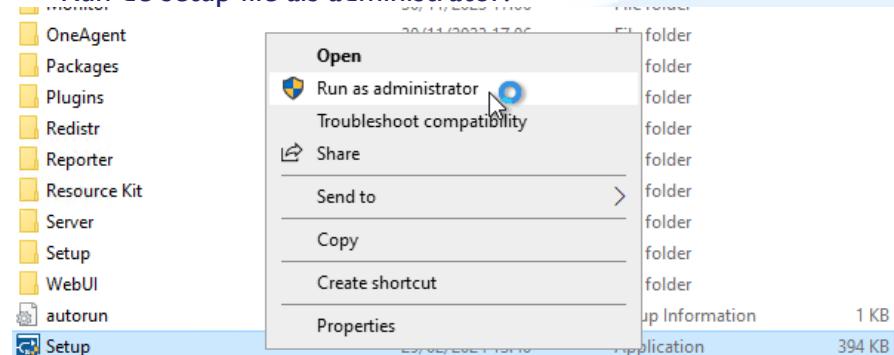
Figuur 158: Installatie van VEEAM (1)

- Nadat je het hebt gedownload, gaan we het installatiebestand mounten op onze computer.



Figuur 159: Installatie van VEEAM (2)

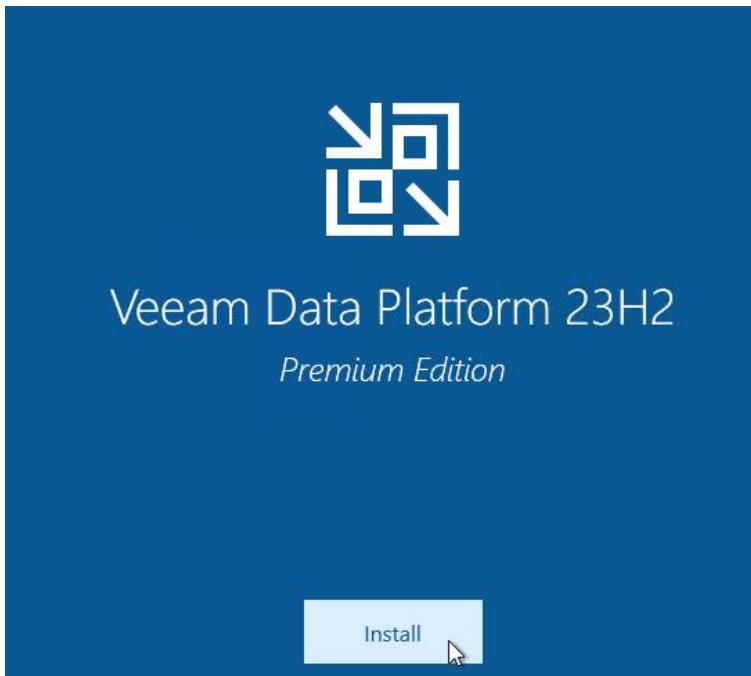
- Run de setup file als administrator.



Figuur 160: Installatie van VEEAM (3)

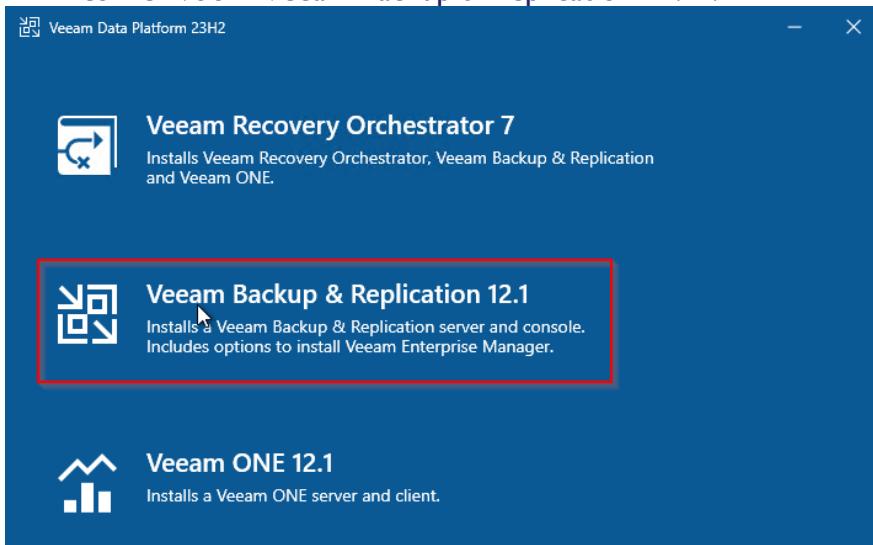
## Automatisch toewijzen van een VLAN aan een gebruiker

- Druk op install



Figuur 161: Installatie van VEEAM (4)

- Kies hier voor “Veeam Backup & Replication 12.1”.



Figuur 162: Installatie van VEEAM (5)

- Hier gaan we “Veeam Backup & Replication” installeren.

## Automatisch toewijzen van een VLAN aan een gebruiker

Veeam Backup & Replication

- X



## Install Veeam Backup &amp; Replication

Veeam Backup & Replication combines fast, flexible and reliable backup, recovery and replication for all your workloads and data.



## Install Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager is an optional web-based management and reporting console for Veeam Backup & Replication. It provides a single pane of glass for larger environments with multiple backup servers.



## Install Veeam Backup &amp; Replication Console

Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.

Figuur 163: Installatie van VEEAM (6)

Veeam Backup & Replication

- X

## License Agreement

Read the license agreements and accept them to proceed.

Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of [Veeam License Agreement](#) and [licensing policy](#)
- Agree and consent to each of the license agreements of [3rd party components](#) used
- Agree and consent to each of the license agreements of [required software](#)

Back I Accept Cancel

Figuur 164: Installatie van VEEAM (7)

- Voeg, indien beschikbaar, de licentiesleutel toe. Als je er geen hebt, kunnen we gebruikmaken van de community sleutel.

## Automatisch toewijzen van een VLAN aan een gebruiker

Veeam Backup & Replication

### License

Provide license file for Veeam Backup & Replication.

Select license provisioning method:

Sign in with Veeam |  Browse license file

License details:

Community edition, 10 instances, limited functionality & personal use only

Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

**i** Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

Back  Cancel

Figuur 165: Installatie van VEEAM (8)

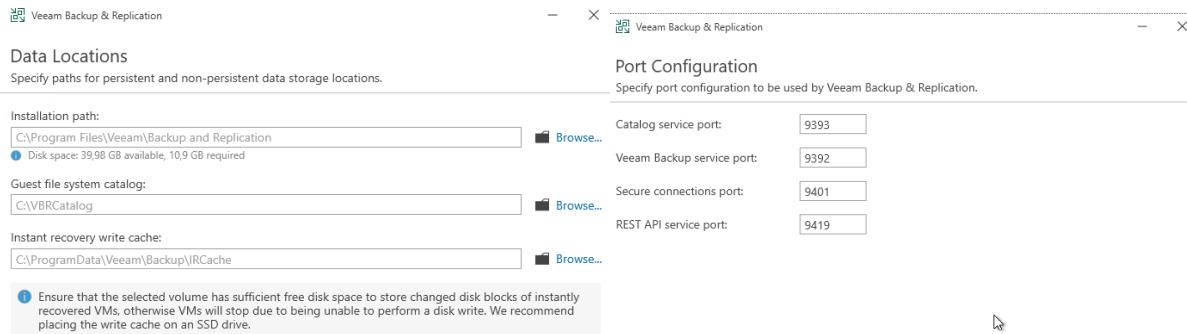
- Volg nu de afbeeldingen voor de volgende stappen.

The screenshot shows two side-by-side configuration windows. On the left, the 'Service Account' step asks for a service account for Veeam Backup & Replication. It has two options: 'LOCAL SYSTEM account (Recommended)' (selected) and 'The following user account'. Below are fields for 'User name' (WEO\administrator.cisa), 'Password', and 'Choose...'. On the right, the 'Database' step asks to choose a database engine and instance. It shows 'PostgreSQL' selected as the engine, 'Install new instance' selected, and 'weo-srv-backup:5432' entered as the instance. It also shows 'VeeamBackup' as the database name. Both windows have 'Back', 'Next', and 'Cancel' buttons at the bottom, with the 'Next' button in both boxes highlighted with a red border.

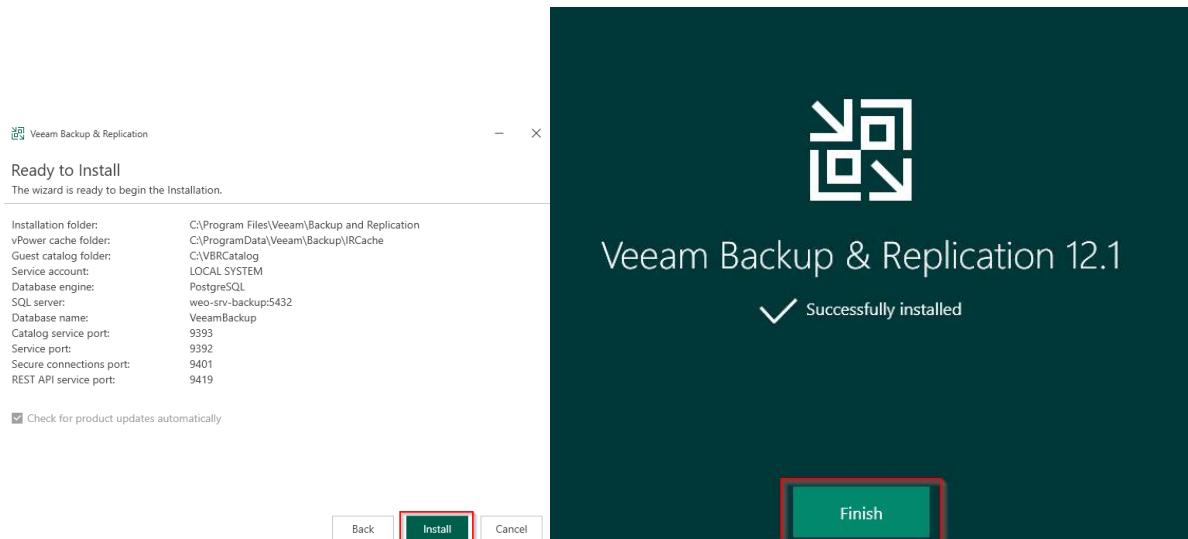
Figuur 166: Installatie van VEEAM (9)

## Automatisch toewijzen van een VLAN aan een gebruiker

**Zorg zeker voor genoeg ruimte op de C-schijf wanneer je Veeam back-up en replicatie gaat installeren. Het iso-bestand is 10,9 GB groot en dit vraagt het ook voor de setup zelf van Veeam.**



Figuur 167: Installatie van VEEAM (10)



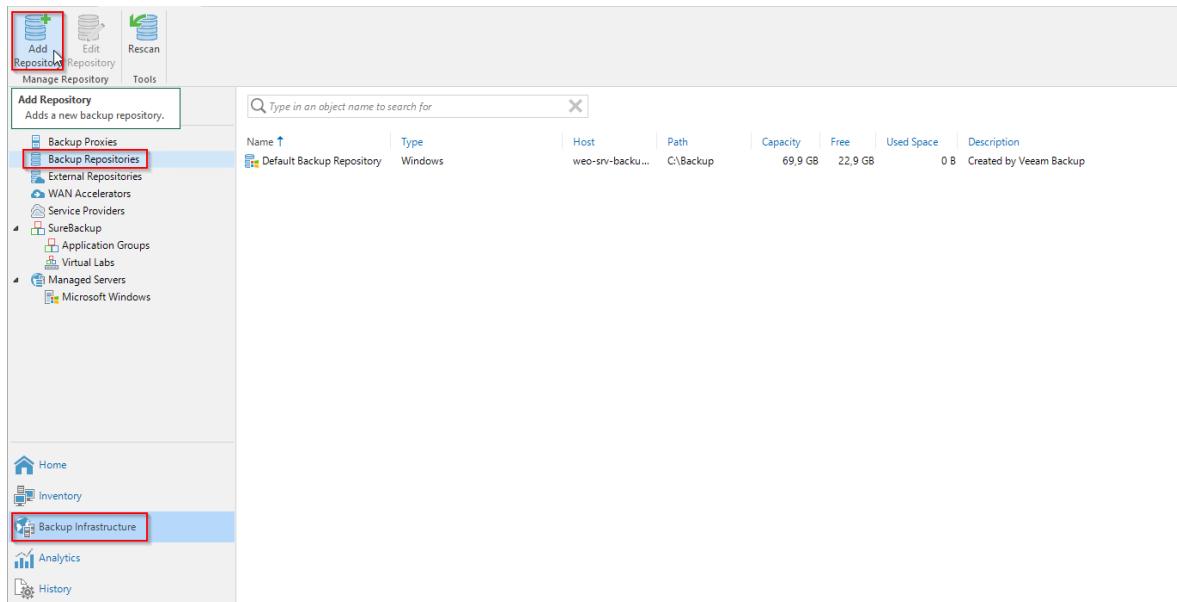
Figuur 168: Installatie van VEEAM (11)

Na de installatie kan je het toegevoegde installatiebestand ontkoppelen en de installatie van het .iso bestand kan je ook weer verwijderen zodat er weer ruimte zal vrijkomen op de schijf.

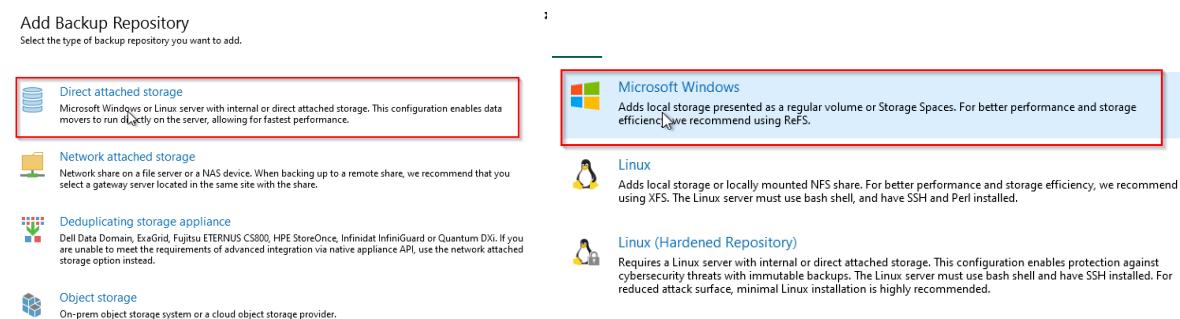
## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.5.2 Create Backup repository

- Nu Veeam is geïnstalleerd, gaan we eerst een back-up repository aanmaken waar we onze back-ups kunnen opslaan.



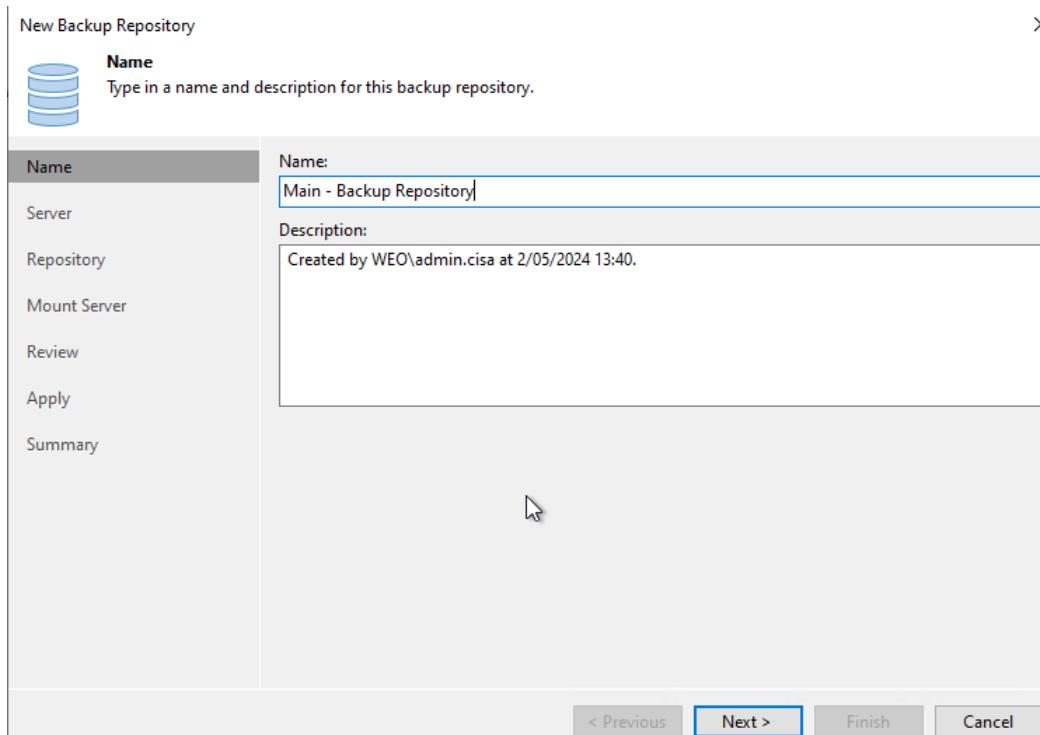
Figuur 169: Configuratie van VEEAM (1)



Figuur 170: Configuratie van VEEAM (2)

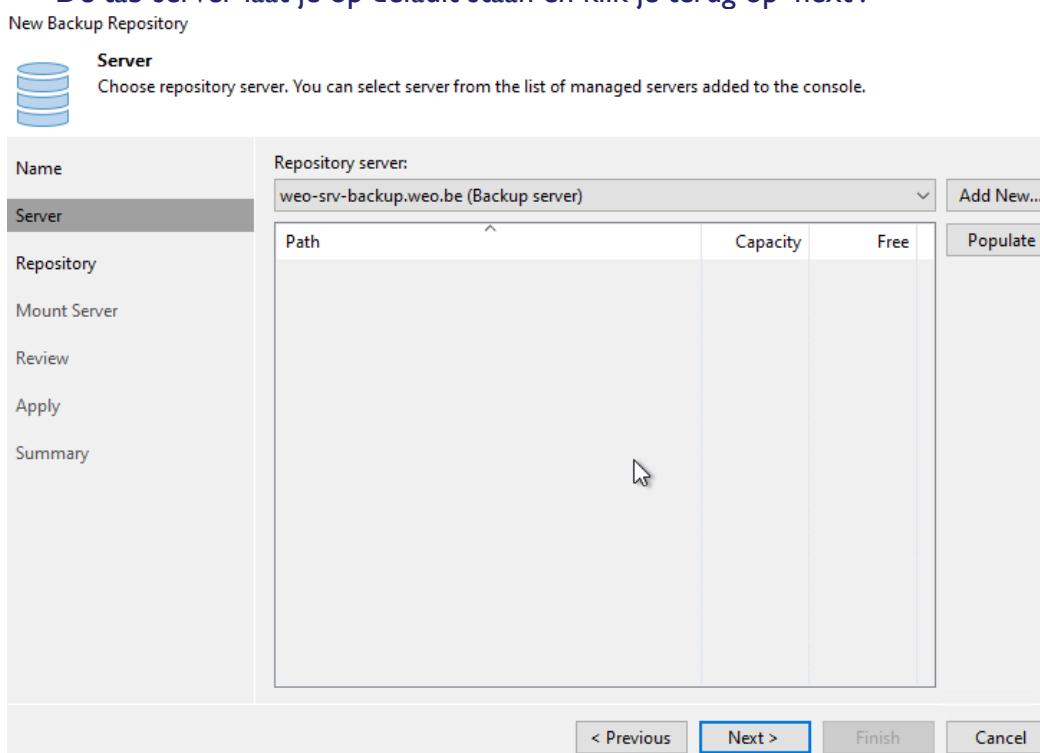
- Geef je back-up repository een zinvolle naam en klik vervolgens op 'next'.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 171: Configuratie van VEEAM (3)

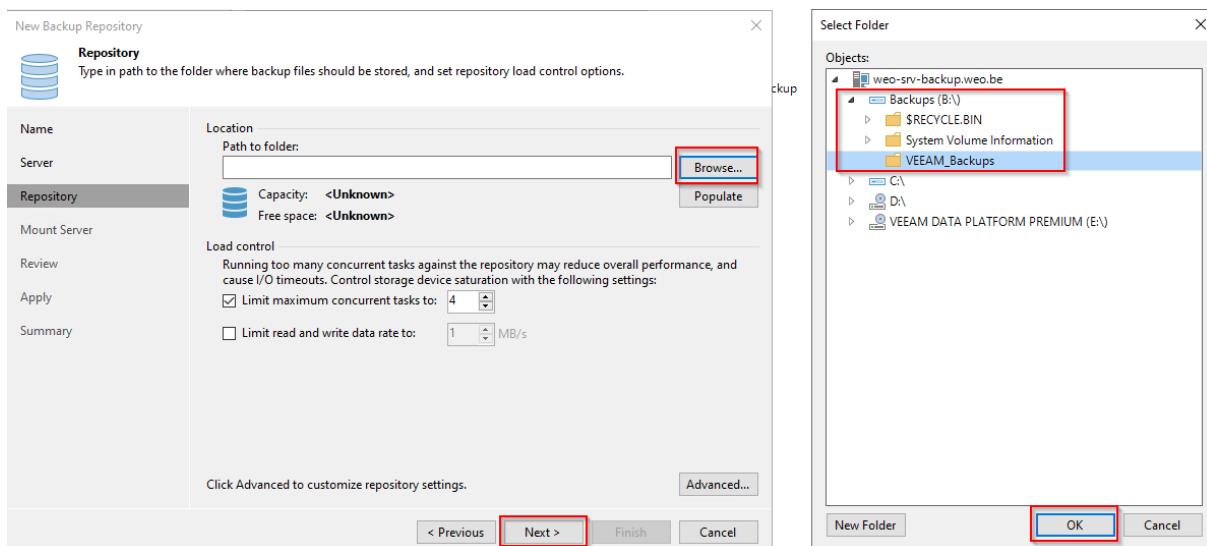
- De tab server laat je op default staan en klik je terug op ‘next’.



Figuur 172: Configuratie van VEEAM (4)

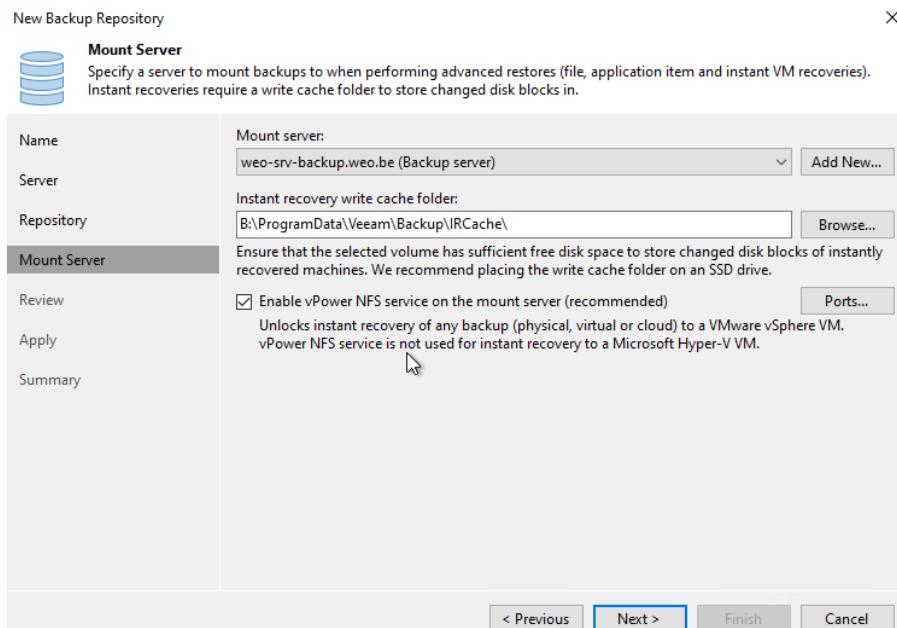
## Automatisch toewijzen van een VLAN aan een gebruiker

- Selecteer nu een locatie waar je back-ups wilt opslaan. Om de back-ups beter te managen kiezen we ervoor om een map aan te maken op de back-up



Figuur 173: Configuratie van VEEAM (5)

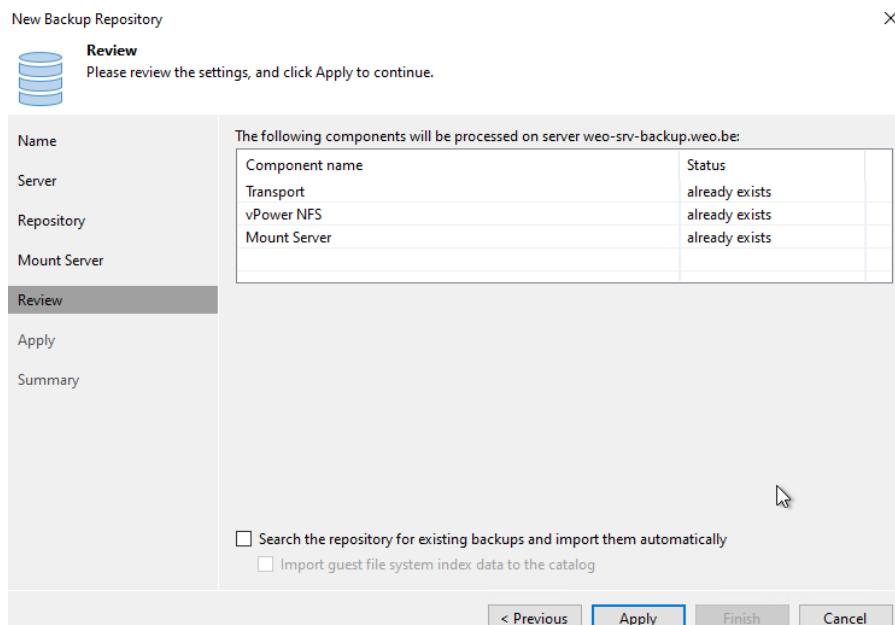
- Klik 'next'



Figuur 174: Configuratie van VEEAM (6)

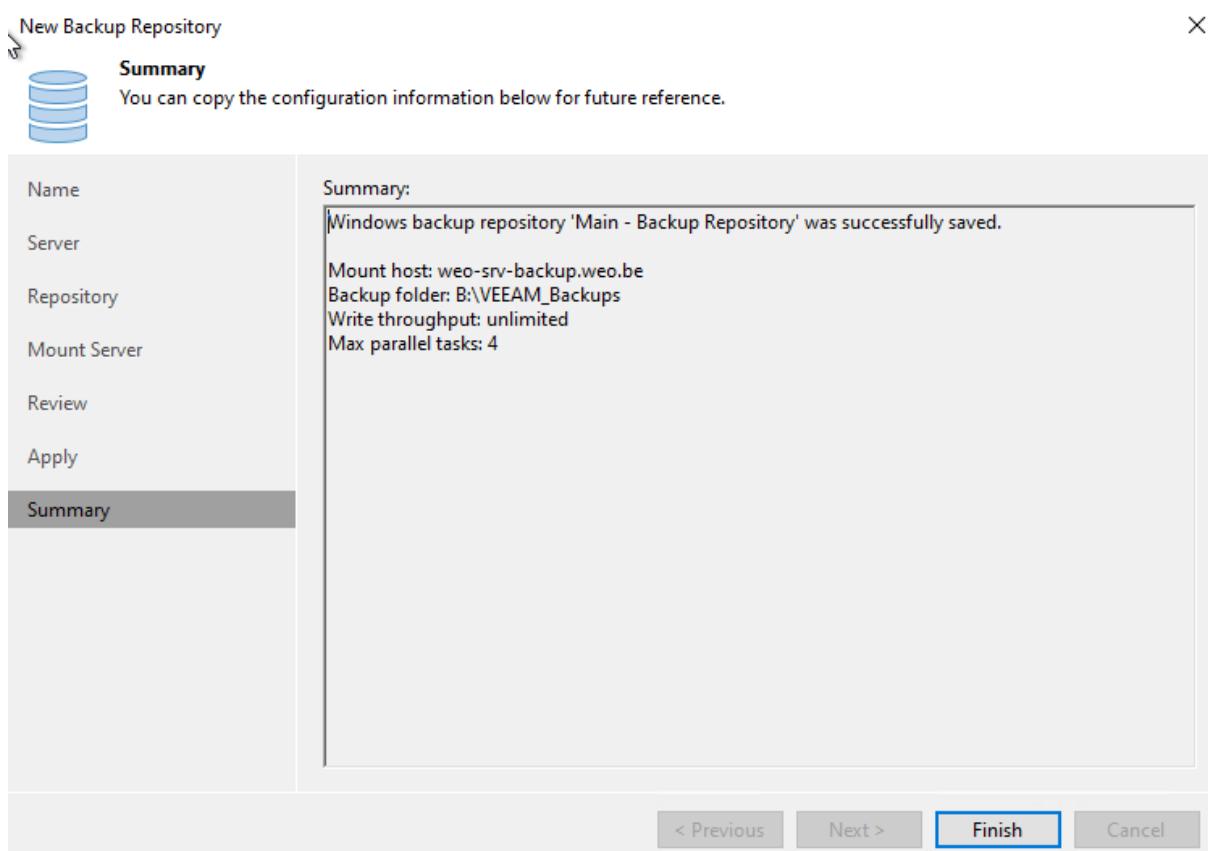
- Klik 'apply'. Het doel van de vPower NFS is een snelle en betrouwbare toegang te bieden tot de back-upgegevens via NFS, waardoor instant recovery- en verificatietaken efficiënt kunnen worden uitgevoerd zonder dat volledige herstelprocessen nodig zijn. Dit is enkel mogelijk voor Vmware vSphere virtuele machines.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 175: Configuratie van VEEAM (7)

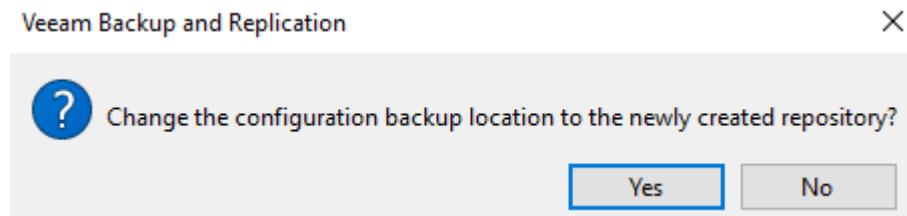
- Klik 'finish'



Figuur 176: Configuratie van VEEAM (8)

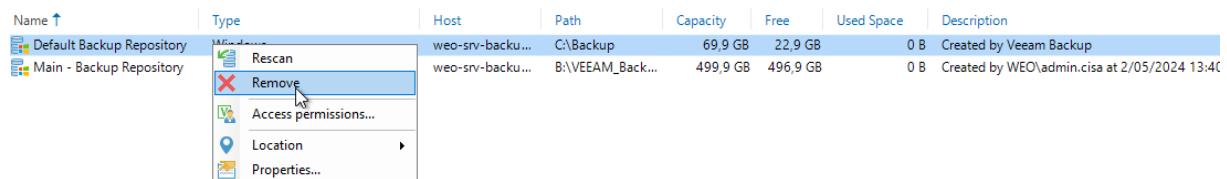
## Automatisch toewijzen van een VLAN aan een gebruiker

- Klik op 'yes'



Figuur 177: Configuratie van VEEAM (9)

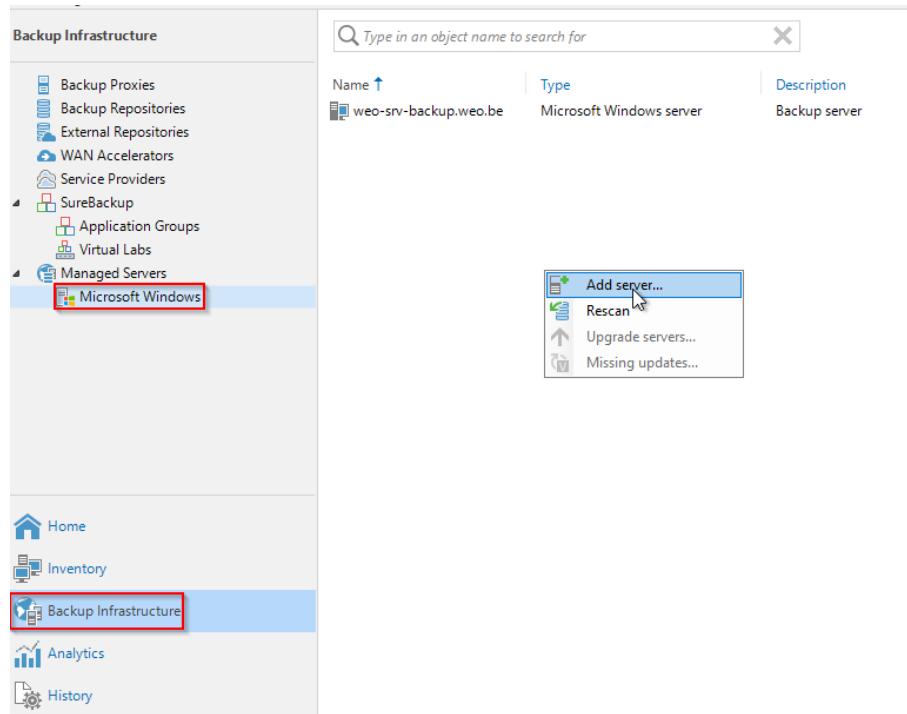
- Nu gaan we de oude back-up repository die is aangemaakt bij de installatie verwijderen.



Figuur 178: Configuratie van VEEAM (10)

### 6.5.3 Voeg servers toe voor back-up.

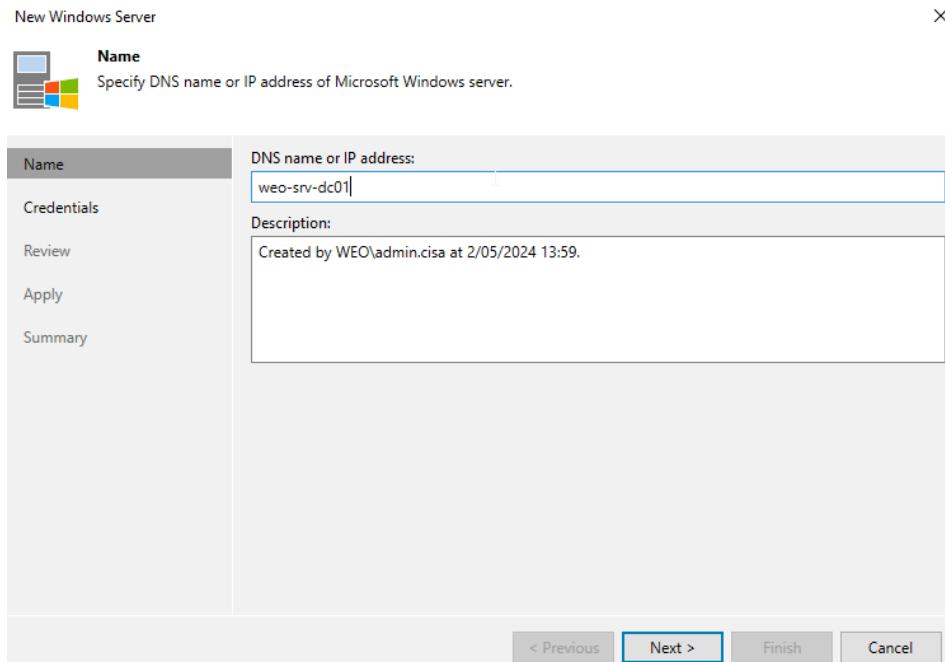
- Rechter muis klik hier om nieuwe servers toe te voegen.



Figuur 179: Configuratie van VEEAM (11)

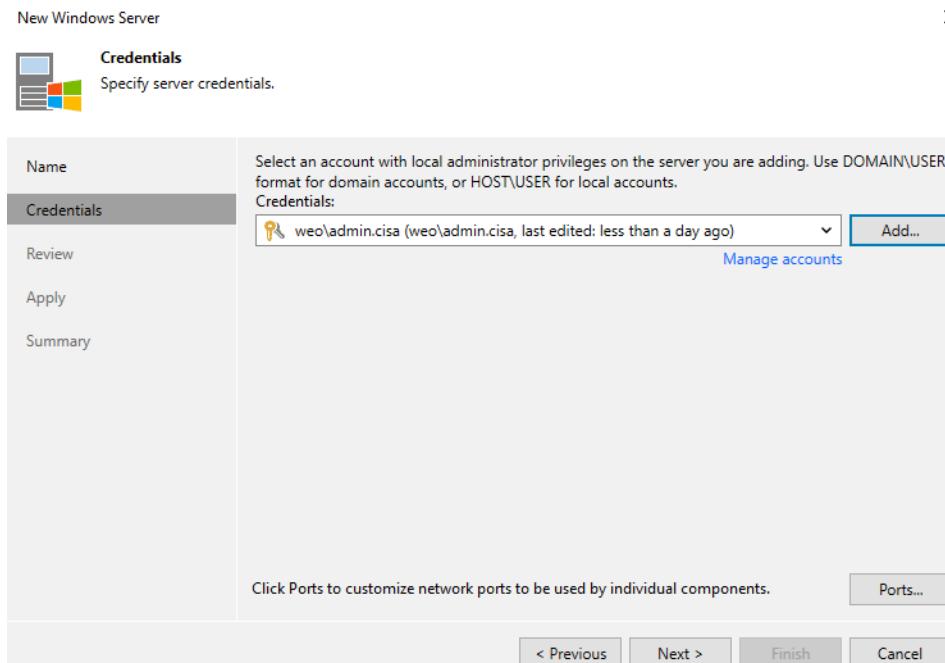
## Automatisch toewijzen van een VLAN aan een gebruiker

- Zet hier de DNS naam of het ip-adres van je server en klik daarna op 'next'.



Figuur 180: Configuratie van VEEAM (12)

- Kies hier een user waarmee de back-ups gaan gebeuren.

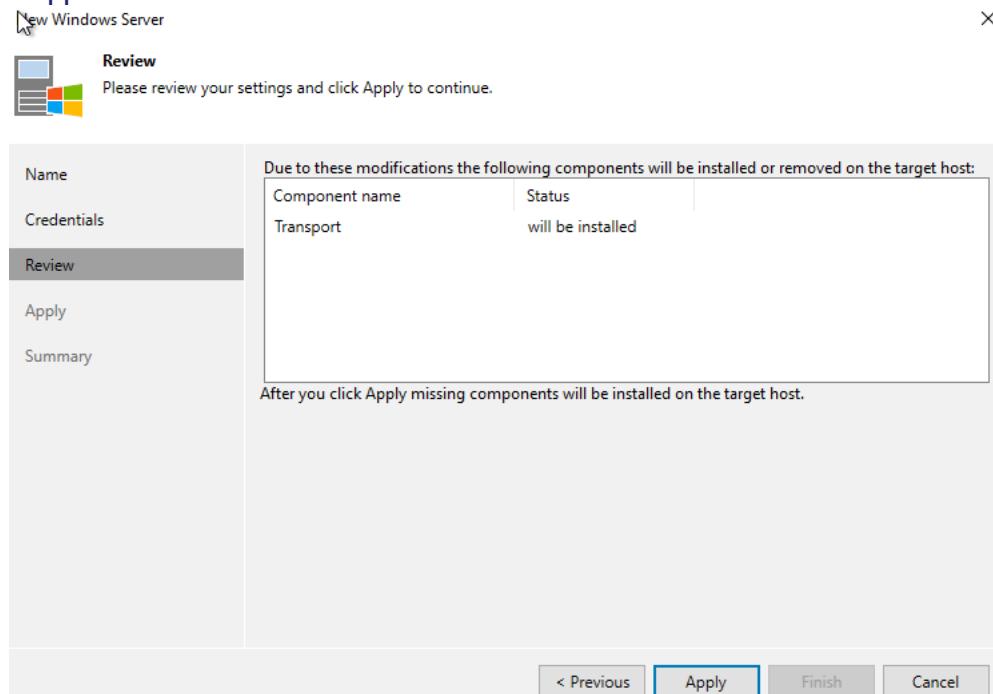


Figuur 181: Configuratie van VEEAM (13)

- Klik op 'apply'; er zullen op de server componenten worden geïnstalleerd die je gaat toevoegen. De transport component is verantwoordelijk voor het datatransport tijdens het maken van een back-up. Dit geldt zowel voor replicatie als voor het herstellen van

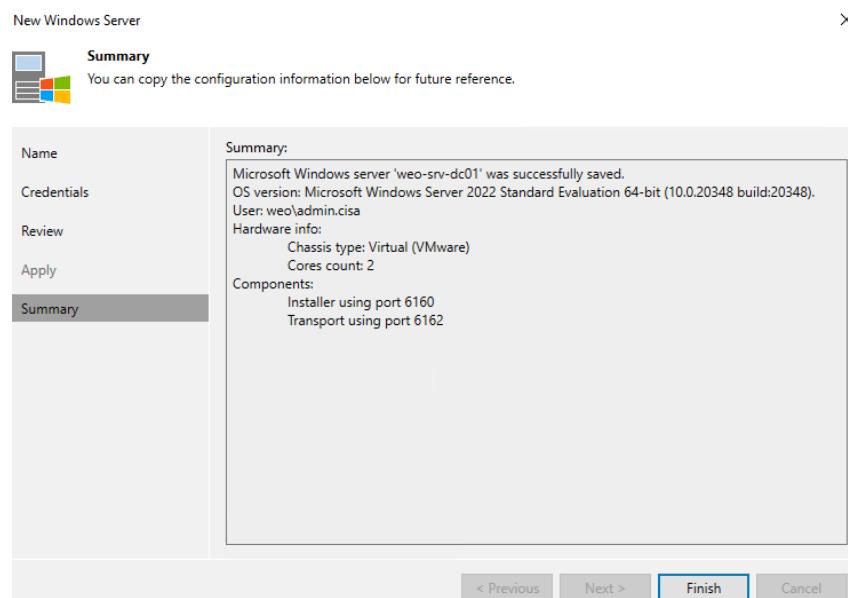
## Automatisch toewijzen van een VLAN aan een gebruiker

mappen en folders.



Figuur 182: Configuratie van VEEAM (14)

- Wanneer het proces klaar is klik je op ‘finish’.

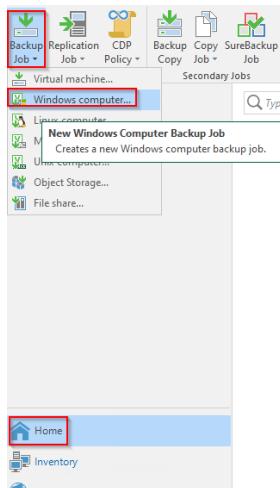


Figuur 183: Configuratie van VEEAM (15)

### 6.5.4 Backup job aanmaken.

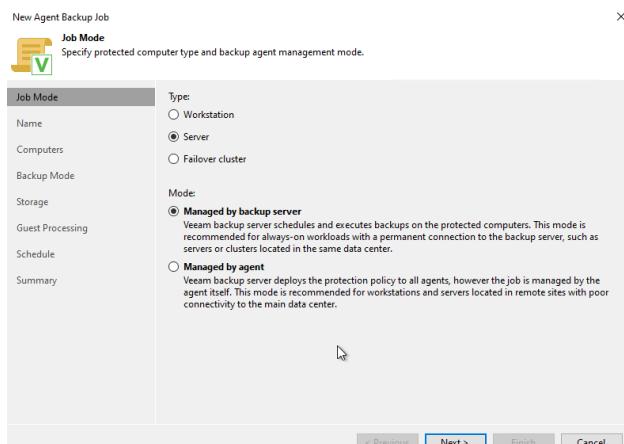
- Creëren van een nieuwe back-up job.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 184: Configuratie van VEEAM (16)

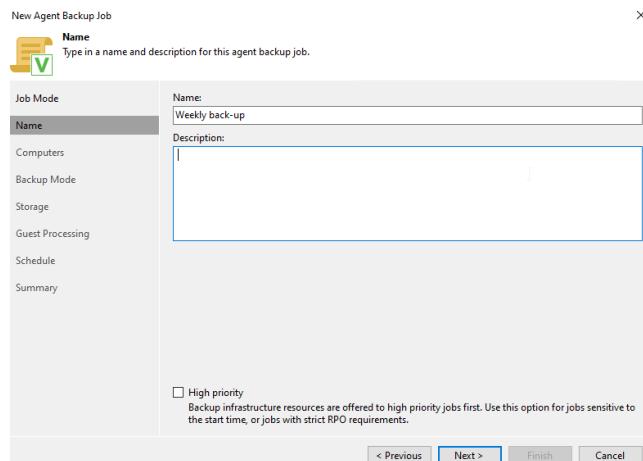
- Klik op 'next'



Figuur 185: Configuratie van VEEAM (17)

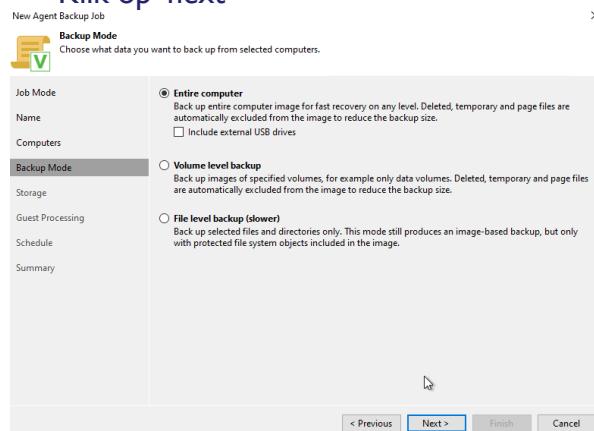
- Geef je back-up job een zinvolle naam.

## Automatisch toewijzen van een VLAN aan een gebruiker



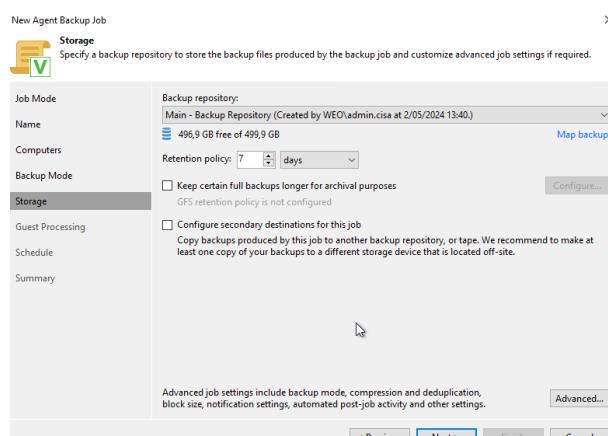
Figuur 186: Configuratie van VEEAM (18)

- Klik op 'next'



Figuur 187: Configuratie van VEEAM (19)

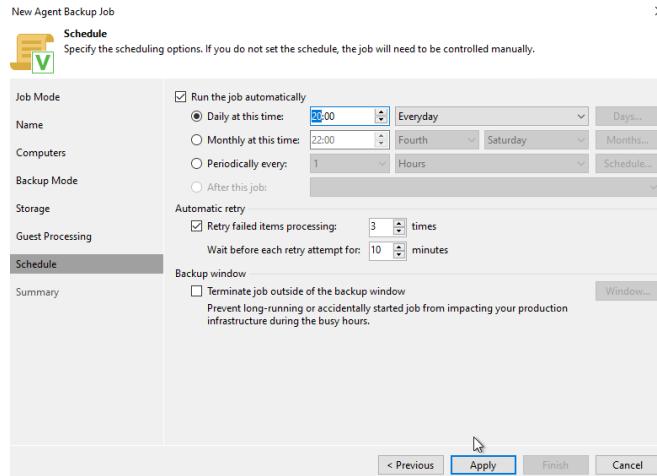
- Klik op 'next'



Figuur 188: Configuratie van VEEAM (20)

- Duid aan 'run the job automatically' en klik daarna op 'apply'. Je kan hier ook de tijd angeven wanneer de back-up zal starten.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 189: Configuratie van VEEAM (21)

## 6.6 Monitoring

Natuurlijk hebben we ook monitoring toevoegd in onze opstelling zodat we een centraal punt hebben waar meldingen binnenkomen. Om dit te realiseren gebruiken we Zabbix en daarnaast ook Grafana . Dit wordt verder besproken onder 5.7 logging.

### 6.6.1 Zabbix

#### 6.6.1.1 Installatie Server

Voor de installatie van zabbix gebruiken we een Linux server met ubuntu distributie.

De installatie van de Zabbix repository.

```
sudo wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
sudo apt update
```

Daarna komt de installatie van de zabbix server, frontend en agent:

```
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
zabbix-sql-scripts zabbix-agent
```

We gaan de initiële database maken voor de server, daarvoor installeerden we eerst de sql-server. We starten de service:

```
sudo apt-get install mysql-server
sudo systemctl start mysql
```

## Automatisch toewijzen van een VLAN aan een gebruiker

We maken de initiele database, de “placeholder” is je eigen **gekozen wachtwoord** dat je wil gebruiken om aan te melden op zabbix:

```
sudo mysql
create database zabbix character set utf8mb4 collate utf8mb4_bin;
create user zabbix@localhost identified by 'PLACEHOLDER';
grant all privileges on zabbix.* to zabbix@localhost;
set global log_bin_trust_function_creators = 1;
quit;
```

Op de Zabbix-serverhost importeer je daarna het initiële schema en de gegevens. Je wordt gevraagd het nieuw aangemaakte wachtwoord – ingegeven bij de placeholder - in te voeren. Dit commando kan zeker een 5-tal minuten duren:

```
sudo zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Schakel de optie `log_bin_trust_function_creators` uit na het importeren van databaseschema's.

```
sudo mysql
set global log_bin_trust_function_creators = 0;
quit;
```

Door `log_bin_trust_function_creators` op 0 te zetten na het importeren van het Zabbix-databaseschema, dwing je strengere beveiligingsmaatregelen af om te voorkomen dat ongeautoriseerde gebruikers potentieel schadelijke functies of triggers maken zonder dat ze daarvoor superuser-rechten nodig hebben. Dit helpt de integriteit en veiligheid van de Zabbix-database te behouden en zorgt tegelijkertijd voor compatibiliteit met MySQL replicatie setups.

Nu gaan we de database voor de zabbix server configureren:

```
sudo nano /etc/zabbix/zabbix_server.conf
```

In dit bestand zal je zoeken naar `DBPassword=`, deze staat in comments. Hier zal het aangemaakte “placeholder” invoeren zodat het `DBPassword=PLACEHOLDER` wordt. Door op `Ctrl+X` te drukken en daarna op `Y` sla je de aangepast configuratie op.

Nadat we het wachtwoord hebben toegevoegd aan het configuratie bestand start we de zabbix server en agent processen. We gaan de processen ook laten starten bij het opstarten van de server.

```
sudo systemctl restart zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent apache2
```

## Automatisch toewijzen van een VLAN aan een gebruiker

Na deze commando's uit te voeren kan je de zabbix UI web pagina openen. De URL die je gebruikt is <http://host-ip/zabbix>. Je kan aanloggen op de UI door de naam 'Admin' in te vullen en je eigen gekozen wachtwoord "placeholder".

### 6.6.1.2 Installatie agent

Je kan op heel wat besturingssystemen Zabbix agents installeren. Wij gebruiken in onze opstelling Windows servers. Dus hiervoor zal de windows agent geïnstalleerd worden op onze servers.

#### Download pre-compiled Zabbix agent binaries

For Agent DEBs and RPMs please visit [Zabbix packages](#)

Show legacy downloads

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	6.4	OpenSSL	MSI
Linux		i386	6.2	No encryption	Archive
macOS			6.0 LTS		
AIX			5.4		
FreeBSD			5.2		
OpenBSD			5.0 LTS		
Solaris			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

Figuur 190: Installatie van zabbix (1)

Je sturt naar [https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents) op de server. Hier zal je Zabbix agent v6.4.14 – wellicht is de versie al geupdate na het lezen van de documentatie – installeren.

Zabbix Release: 6.4.14

Zabbix agent v6.4.14		<a href="#">Read manual</a>
Packaging:	MSI	
Encryption:	OpenSSL	
Linkage:	Dynamic	
Checksum:	sha256: 4ec62619cff07aaeddc7d86f3013472aef975356dd295ac188b37480df92efb sha1: f85636eb277c9546551c78089ff23c50c13745a5 md5: 71894246bcace66d3aad375dbe2a027d	
<a href="#" style="background-color: green; color: white; padding: 5px 20px; border-radius: 5px;">DOWNLOAD</a>		https://cdn.zabbix.com/zabbix/binaries/stable/6.4/6.4.14/zabbix_agent-6.4.14-windows-amd64-openssl.msi

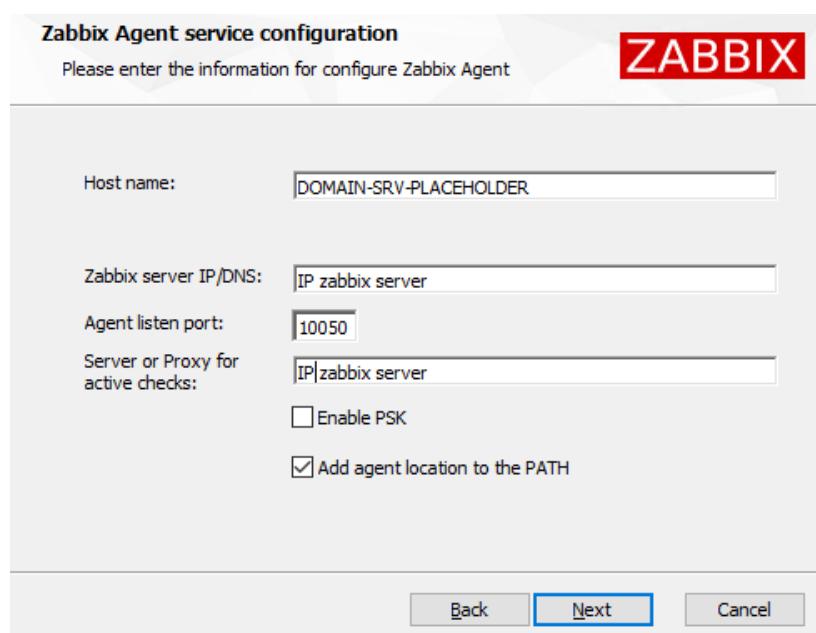
Figuur 191: Installatie van zabbix (2)

## Automatisch toewijzen van een VLAN aan een gebruiker

Na het uitvoeren van het installatiepakket zal je een wizard krijgen voor het doorlopen van de installatie. Druk op het eerste scherm op next, daarna vink je aan dat je het licentie akkoord accepteert en druk op next. Daarna krijg je een scherm voor hoe je de functies graag wilt installeren. Dit kan je laten staan en druk op next.

Na dit scherm krijg je het zabbix agent configuratiescherm. Als hostname kies je de naam van je server. Daarna vul je het ip van de zabbix server in, dit zal je ook voor de “active checks” doen. Vink “add agent location to the path” ook aan.

Dit zal er zo uit zien.



The screenshot shows the 'Zabbix Agent service configuration' wizard. The title bar says 'ZABBIX'. The main area has the heading 'Please enter the information for configure Zabbix Agent'. It contains the following fields:

Host name:	DOMAIN-SRV-PLACEHOLDER
Zabbix server IP/DNS:	IP zabbix server
Agent listen port:	10050
Server or Proxy for active checks:	IP zabbix server
<input type="checkbox"/> Enable PSK	
<input checked="" type="checkbox"/> Add agent location to the PATH	

At the bottom are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

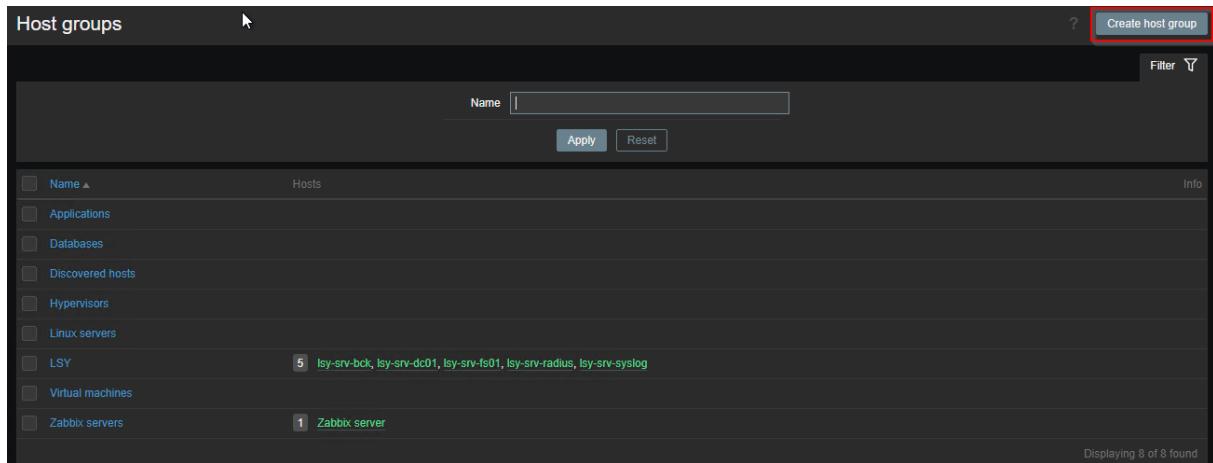
Figuur 192: Installatie van zabbix (3)

In het volgende scherm druk je op install om de agent te instaleren op de server.

#### 6.6.1.3 Hosts group

We gaan eerst een host group maken zodat we hier onze servers kunnen gaan groeperen. Zo kunnen we ook overzichten gaan creeëren in het Zabbix dashboard. Om een nieuwe groep aan te maken druk je rechts boven op “create host group”:

## Automatisch toewijzen van een VLAN aan een gebruiker



The screenshot shows the 'Host groups' configuration page in Zabbix. At the top right, there is a red box around the 'Create host group' button. Below it is a search bar with 'Name' and 'Apply' buttons. A sidebar on the left lists categories like 'Name', 'Applications', 'Databases', etc., with 'LSY' selected. Under 'Hosts', there are two entries: 'lsy-srv-bck' (5 hosts) and 'Zabbix server' (1 host). At the bottom right, it says 'Displaying 8 of 8 found'.

Figuur 193: Configuratie van zabbix (1)

Hier noteren we de groep naam waar we onze server willen groeperen.



The screenshot shows a 'New host group' dialog box. It has a field labeled '\* Group name' with 'PLACEHOLDER' placeholder text. At the bottom right are 'Add' and 'Cancel' buttons.

Figuur 194: Configuratie van zabbix (2)

Druk na het invullen van je groep naam op ‘add’ voor de groep toe te voegen.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.6.1.4 Hosts

Om een host te maken ga je naar data collection > hosts. Hier kan je hosts configureren maar ook krijg je een overzicht van je hosts of server die je aan het monitoren bent. Druk rechts boven op create host.

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	In
Isy-srv-bck	Items 142	Triggers 102	Graphs 16	Discovery 4	Web	172.30.1.6:10050		Windows by Zabbix agent	Enabled	ZBX	None	
Isy-srv-dc01	Items 123	Triggers 90	Graphs 11	Discovery 4	Web	172.30.1.2:10050		Windows by Zabbix agent	Enabled	ZBX	None	
Isy-srv-ls01	Items 123	Triggers 83	Graphs 16	Discovery 4	Web	172.30.1.4:10050		Windows by Zabbix agent	Enabled	ZBX	None	
Isy-srv-radius	Items 113	Triggers 80	Graphs 11	Discovery 4	Web	172.30.1.3:10050		Windows by Zabbix agent	Enabled	ZBX	None	
Isy-srv-syslog	Items 110	Triggers 77	Graphs 11	Discovery 4	Web	172.30.1.7:10050		Windows by Zabbix agent	Enabled	ZBX	None	
Zabbix server	Items 134	Triggers 74	Graphs 25	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None	

Figuur 195: Configuratie van zabbix (3)

Je kiest de hostname van je server. Als template hebben wij voor nu gekozen voor Templates/Operating systems als template groep en hier kiezen we voor Windows by Zabbix agent als template. Dit kan je doen door op select te drukken, de template group in te geven en te zoeken naar de correcte template. Of je vult in template windows by zabbix agent in en dan kan je deze template in de dropdown selecteren. Dit om te testen of er wel data van de hosts werden gehaald.

We voegen de daarnet gemaakte groep toe bij host groups zodat de host terecht komt in deze groep. Als je typt bij host groups kan je ook daar een nieuwe groep aanmaken. Bij interfaces druk je op add en kiest hier voor agent. Je vult het ip-adres van de server in. Dit zou voldoende moeten zijn voor interfaces. Het resultaat zou eruit moeten zien als de afbeelding hieronder:

## Automatisch toewijzen van een VLAN aan een gebruiker

The screenshot shows the 'New host' configuration dialog in Zabbix. The 'Host' tab is selected. The 'Host name' field contains 'domain-srv-placeholder'. The 'Visible name' field also contains 'domain-srv-placeholder'. Under 'Templates', 'Windows by Zabbix agent' is selected. In the 'Host groups' section, 'PLACEHOLDER' is chosen. An interface is defined with 'Agent' set to 'Ip van server' and port '10050'. At the bottom, there are buttons for 'Add', 'Cancel', and a large blue 'Save' button.

Figuur 196: Configuratie van zabbix (4)

Daarna druk je op “add” om de host toe te voegen. Na een tijdje zal de availability groen worden zodat je weet dat er connectie is tussen de zabbix server en de host.

The screenshot shows a list of hosts in Zabbix. The columns include Name, Items, Triggers, Graphs, Discovery, Web, Interface, Proxy, Templates, Status, Availability, Agent encryption, Info, and Tags. Most hosts have 'Availability' status as 'ZBX' (green). A red box highlights the 'Availability' column for all hosts. The Zabbix server has 'Availability' as 'ZBX' (green) and 'Agent encryption' as 'None'. The table shows various metrics for each host, such as item counts (e.g., 142 for Isy-srv-bck) and trigger counts (e.g., 102 for Isy-srv-bck).

Figuur 197: Configuratie van zabbix (5)

Voor het testen dat er data binnenkomt kan je gaan naar monitoring > latest data en scroll je naar onder. Hier zal je gegevens vinden van de server(s) die zijn toegevoegd.

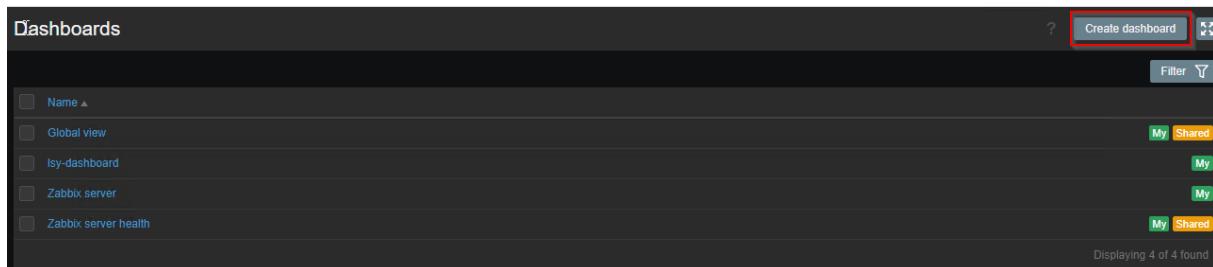
The screenshot shows the 'latest data' table in Zabbix. The columns are Host, Name, Last check, Last value, Change, Tags, and Info. The table lists various metrics for different hosts, such as file system data and space utilization. For example, 'Isy-srv-bck' has a 'Last check' of 41s and a 'Last value' of 51.658 %. The 'Tags' column includes components like 'component:raw', 'component:storage', and 'filesystem: C:'. The 'Info' column indicates whether it's a history entry or a graph.

Figuur 198: Configuratie van zabbix (6)

## Automatisch toewijzen van een VLAN aan een gebruiker

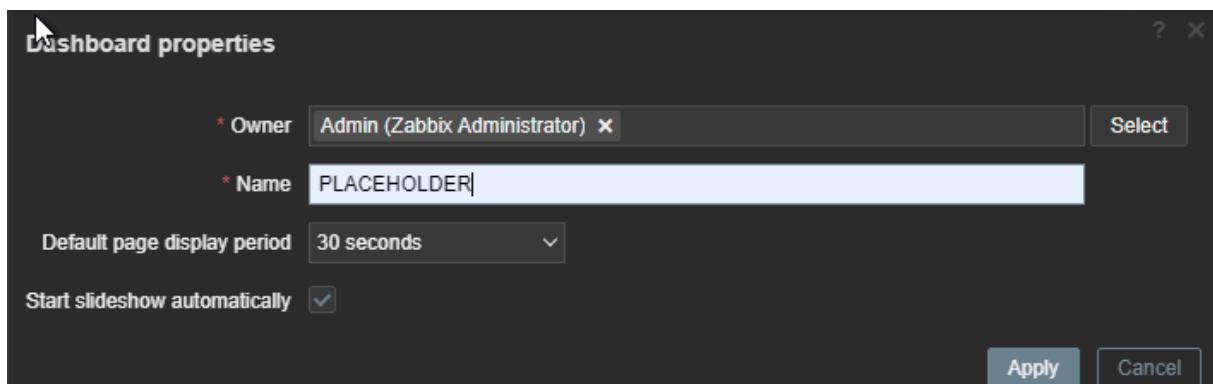
### 6.6.1.5 Dashboard

We gaan een eigen dashboard maken zodat we onze systemen goed, naar onze wil kunnen gaan monitoren.



Figuur 199: Configuratie van zabbix (7)

We kiezen een naam voor ons dashboard en drukken op apply.



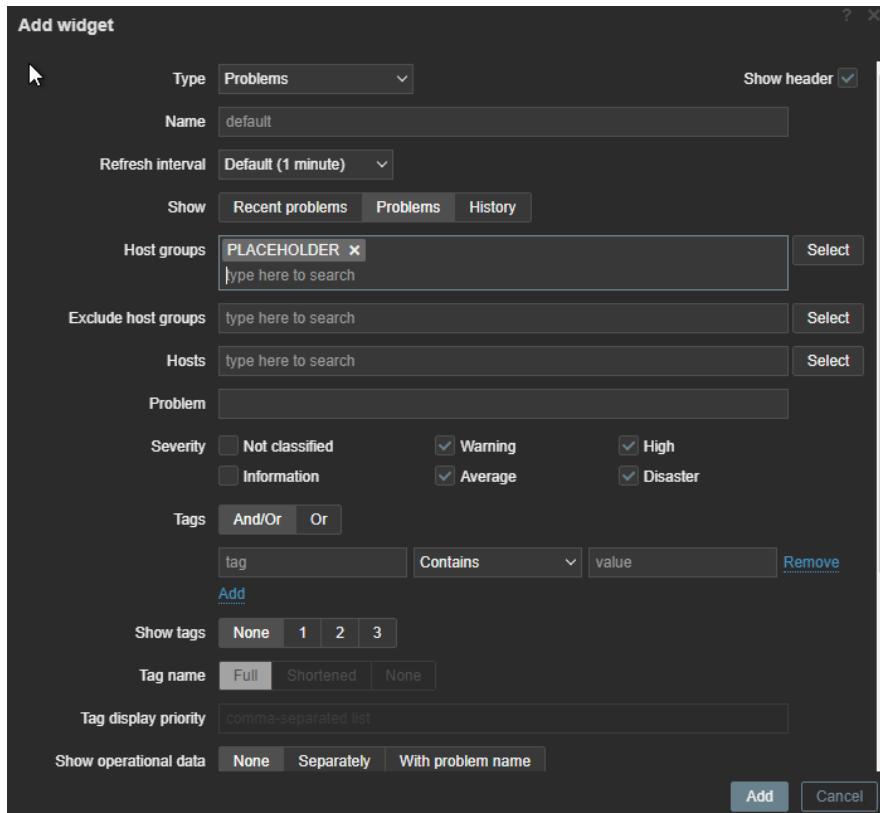
Figuur 200: Configuratie van zabbix (8)

We voegen een widget toe van het type problems. Dit zal er voor zorgen dat de problemen die zich eventueel voor doen op onze servers zich hier gaan tonen. De host groups van waar we de problemen willen weten is onze eerder gecreerde host group met hierin de host die we hebben toegevoegd.

Je kan zelf nog een naam kiezen voor de widget. Ook als je meerdere host groups hebt kan je er ook uitsluiten van de widget en je kan ook eventuele individuele hosts toevoegen.

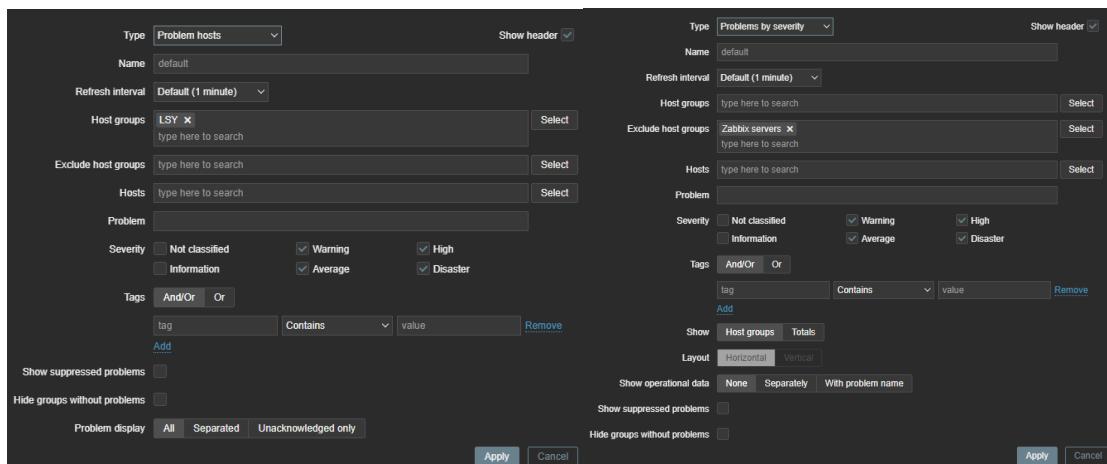
De severity of ernst van de problemen die zich gaan weergeven op de widget zijn warning, average, high en disaster.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 201: Configuratie van zabbix (9)

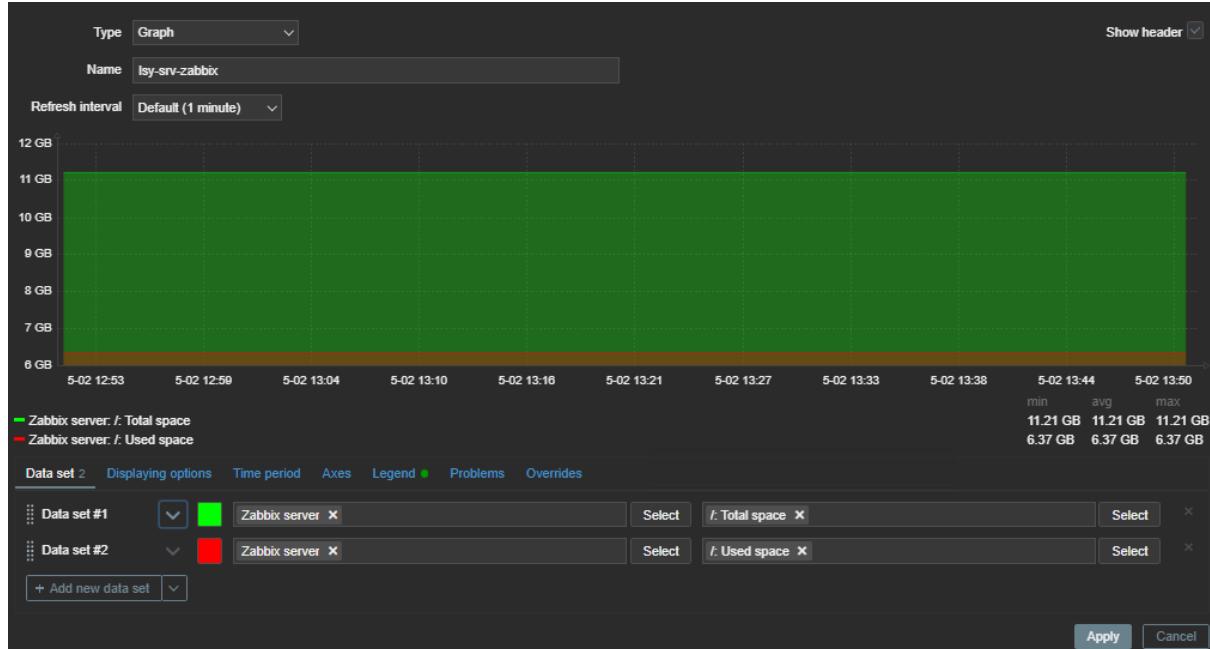
Daarnaast maken we nog een widget om de problemen per host group te zien; dan kunnen we zien hoeveel servers een problemen/meldingen hebben. Daarnaast nog een widget om de problemen per severity/ernst te laten zien.



Figuur 202: Configuratie van zabbix (10)

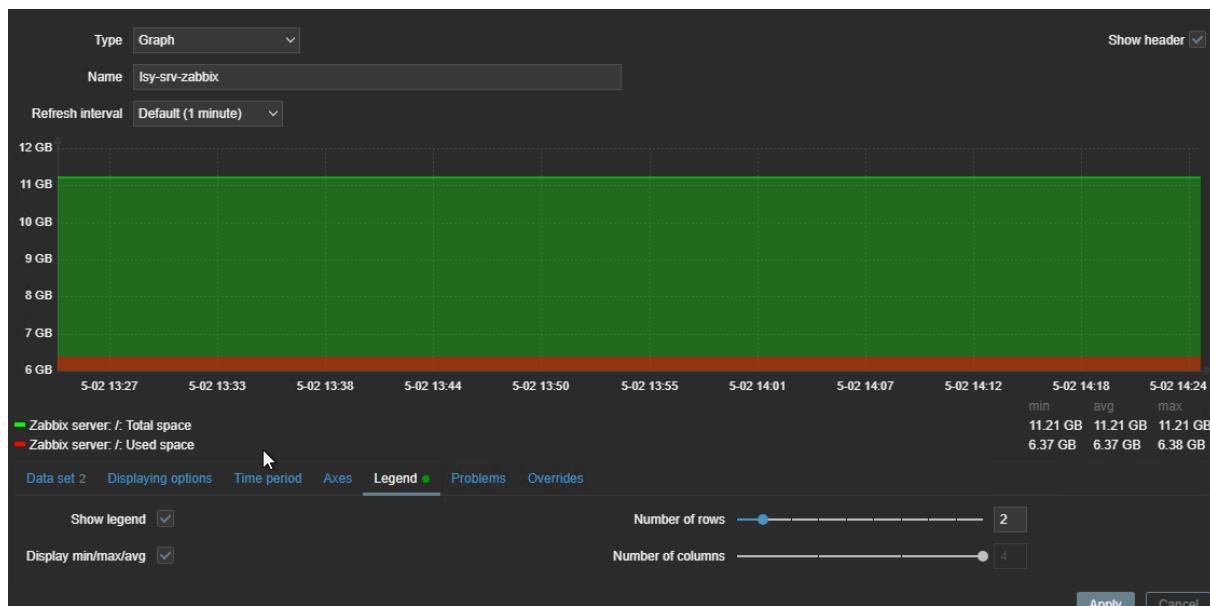
Het is ook belangrijk om de zabbix server te monitoren. Aangezien de data van op zabbix worden opgeslagen op de server is het goed om te weten hoeveel vrije schijfruimte er nog is. Daarvoor hebben we ook een widget aangemaakt:

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 203: Zabbix graph filters (1)

Als je de data sets opent, kan je hier nog extra aanpassingen doorvoeren. Dit is voor de grafiek naar je eigen wil te hebben. Daarna gaan we nog naar “legend”. Dan kiezen we weer om minimum, maxima, en het gemiddelde te tonen, we kiezen voor number of rows 2 zodat deze onder elkaar staan.



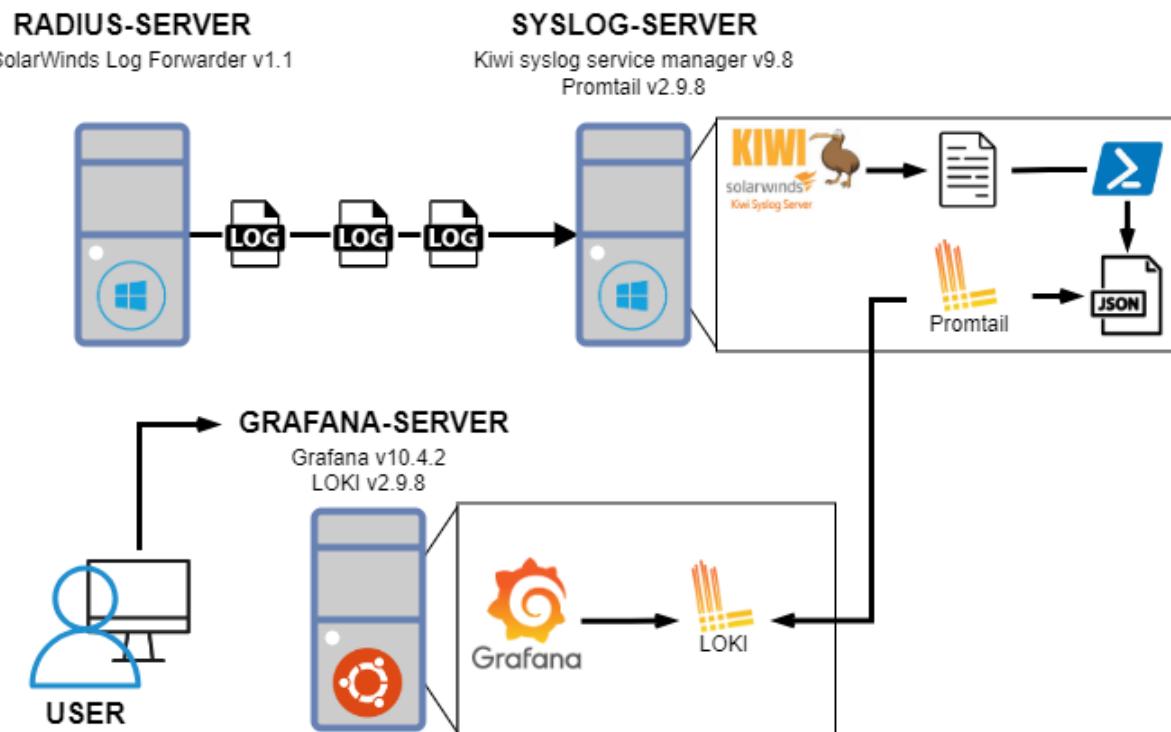
Figuur 204: Zabbix graph filters (2)

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.7 Syslog logging

Het is ook belangrijk om je logs bij te houden in een centrale plaats zodat je hier makkelijk kan zoeken naar fouten.

#### 6.7.1 Schema



Figuur 205: Syslog schema

#### 6.7.2 Installatie handleidingen

We gaan Grafana versie 10.4.2 en Loki versie 2.9.8 installeren op een Ubuntu 22.04 LTS-server. Daarnaast gaan we Promtail versie 2.9.8 op een Windows-machine installeren met behulp van een PowerShell-script.

**Note:** Deze volledige opstelling is gratis en vereist geen betaling. Het enige nadeel is dat de gratis versie van Kiwi Syslog Server berichten kan ontvangen van maximaal 5 apparaten.

##### 6.7.2.1 Grafana

- We gaan eerst de vereisten voor Grafana installeren.

```
$ sudo apt update -y
$ sudo apt-get install -y apt-transport-https software-properties-common
- Importeer de Grafana GPG-sleutel.
```

## Automatisch toewijzen van een VLAN aan een gebruiker

```
$ sudo wget -q -O /usr/share/keyrings/grafana.key  
https://apt.grafana.com/gpg.key
```

- Voeg de Grafana "stable releases" repository toe.

```
$ echo "deb [signed-by=/usr/share/keyrings/grafana.key]  
https://apt.grafana.com stable main" | sudo tee -a  
/etc/apt/sources.list.d/grafana.list
```

- Werk de pakketten in de repository bij, inclusief het nieuwe Grafana-pakket.

```
$ sudo apt-get update -y
```

- Grafana installeren.

```
$ sudo apt-get install grafana -y
```

- Herlaad de systemctl daemon en activeer en start de Grafana-server. Met systemctl enable wordt de server geconfigureerd om Grafana te starten wanneer het systeem wordt opgestart.

```
$ sudo systemctl daemon-reload  
$ sudo systemctl enable grafana-server.service  
$ sudo systemctl start grafana-server
```

- Controleer de status van de Grafana-server en zorg ervoor dat deze actief is.

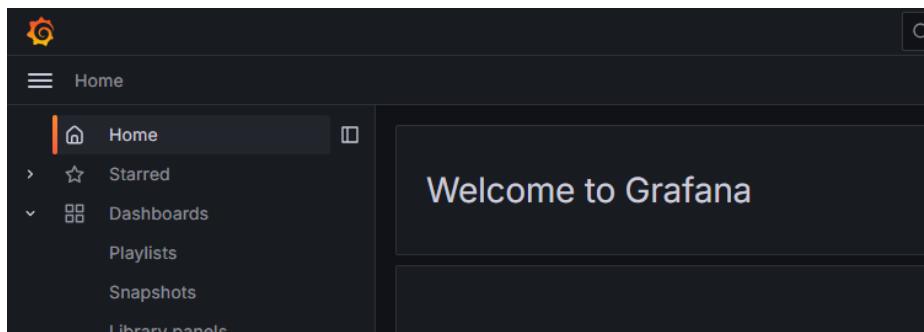
```
$ sudo systemctl status grafana-server  
[OUTPUT]
```

```
● grafana-server.service - Grafana instance  
  Loaded: loaded (/lib/systemd/system/grafana-server.service; enabled; vendor preset: enabled)  
  Active: active (running) since Thu 2024-05-16 14:48:47 UTC; 5 days ago  
    Docs: http://docs.grafana.org
```

Figuur 206: Installatie van grafana (1)

Grafana is nu geïnstalleerd en klaar voor gebruik. Je kunt naar het dashboard navigeren door naar <http://localhost:3000> te gaan. Log in met de gebruikersnaam 'admin' en het wachtwoord 'paswoord'. Grafana zal je vervolgens vragen om het wachtwoord te wijzigen, wat je het beste meteen kunt doen.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 207: Installatie van grafana (2)

### 6.7.2.2 Loki

- We gaan eerst de vereisten van Loki installeren.

```
$ sudo apt install unzip -y
```

- Downloaden van het Loki pakket.

```
$ curl -O -L "https://github.com/grafana/loki/releases/download/v2.9.8/loki-linux-amd64.zip"
```

- ZIP file unzippen.

```
$ unzip "loki-linux-amd64.zip"
```

- Ervoor zorgen dat we de file kunnen uitvoeren.

```
$ chmod a+x "loki-linux-amd64"
```

- Kopieer het binaire bestand naar /usr/local/bin/

```
$ sudo cp loki-linux-amd64 /usr/local/bin/loki
```

- Kijk nu dat loki staat geïnstalleerd.

```
$ loki --version
```

[OUTPUT]

```
wes@wes-srv-grafana:~$ loki --version
loki, version 2.9.8 (branch: release-2.9.x, revision: 94e0029)
  build user:      root@e4ac838ed4ad
  build date:    2024-05-02T22:28:14Z
  go version:   go1.21.9
  platform:     linux/amd64
  tags:         netgo
```

Figuur 208: Installatie van loki (1)

- User creëren waaronder loki gaat werken.

```
$ sudo useradd --system loki
```

- Files creëren onder /etc

```
$ sudo mkdir -p /etc/loki /etc/loki/logs
```

- Een standaard YAML-bestand creëren voor de Loki-configuratie.

```
$ sudo nano /etc/loki/loki-local-config.yaml
```

## Automatisch toewijzen van een VLAN aan een gebruiker

### Start - Dit mag in de file ###

```
auth_enabled: false

server:
  http_listen_port: 3100
  grpc_listen_port: 9096

common:
  path_prefix: /etc/loki
  storage:
    filesystem:
      chunks_directory: /etc/loki/chunks
      rules_directory: /etc/loki/rules
    replication_factor: 1
  ring:
    instance_addr: 0.0.0.0
    kvstore:
      store: inmemory

schema_config:
  configs:
    - from: 2020-10-24
      store: boltdb-shipper
      object_store: filesystem
      schema: v11
    index:
      prefix: index_
      period: 24h

ruler:
  alertmanager_url: http://localhost:9093
```

### End – Sla de file op ###

- Het eigendom van de map aanpassen.

```
$ sudo chown -R loki: /etc/loki
```

- Van loki een service maken.

```
$ sudo nano /etc/systemd/system/loki.service
```

## Automatisch toewijzen van een VLAN aan een gebruiker

### Start - Dit mag in de file ###

```
[Unit]
Description=Loki service
After=network.target

[Service]
Type=simple
User=loki
ExecStart=/usr/local/bin/loki -config.file /etc/loki/loki-local-config.yaml
Restart=on-failure
RestartSec=20
StandardOutput=append:/etc/loki/logs/loki.log
StandardError=append:/etc/loki/logs/loki.log

[Install]
WantedBy=multi-user.target
### End – Slaag de file op ###
```

- Nu gaan we Loki starten en ervoor zorgen dat het bij het opstarten van het systeem automatisch wordt gestart.

```
$ sudo systemctl daemon-reload
$ sudo systemctl start loki
$ sudo systemctl enable loki.service
$ sudo systemctl status loki
```

### [OUTPUT]

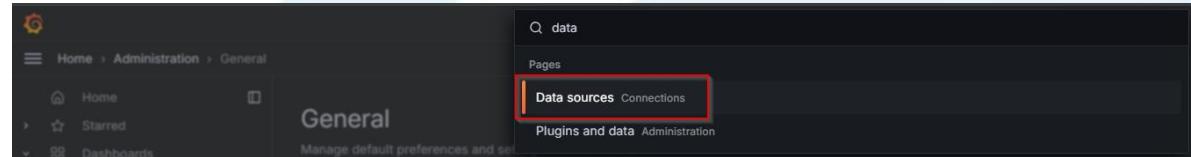
```
● loki.service - Loki service
  Loaded: loaded (/etc/systemd/system/loki.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-05-16 14:48:47 UTC; 5 days ago
    Main PID: 811 (loki)
      Tasks: 16 (limit: 4558)
     Memory: 256.7M
```

Figuur 209: Installatie van loki (2)

Loki is nu geïnstalleerd. Je kunt de installatie verifiëren door te nageren naar <http://localhost:3100/metrics> in je webbrowser.

### 6.7.2.3 Loki koppelen als een source aan Grafana

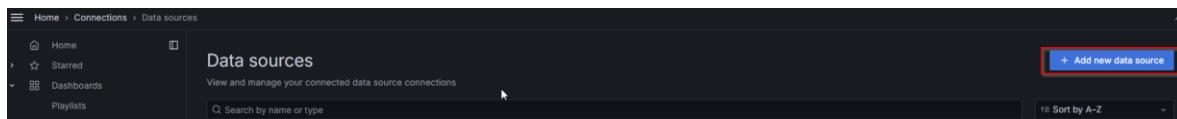
- Surf naar je grafana dashboard, en zoek naar ‘data sources’ in de zoek balk.



Figuur 210: Grafana koppelen met loki (1)

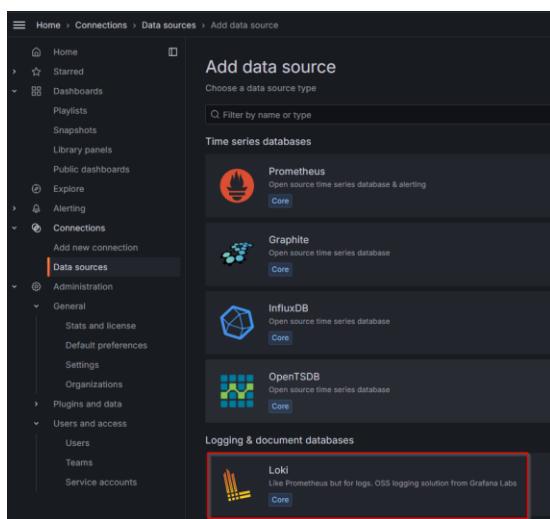
## Automatisch toewijzen van een VLAN aan een gebruiker

- Klik op 'add new data source'



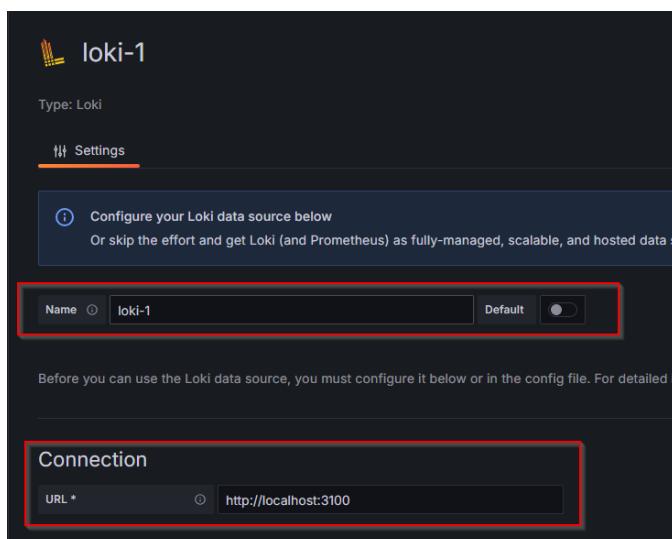
Figuur 211: Grafana koppelen met loki (2)

- Klik op 'loki'



Figuur 212: Grafana koppelen met loki (3)

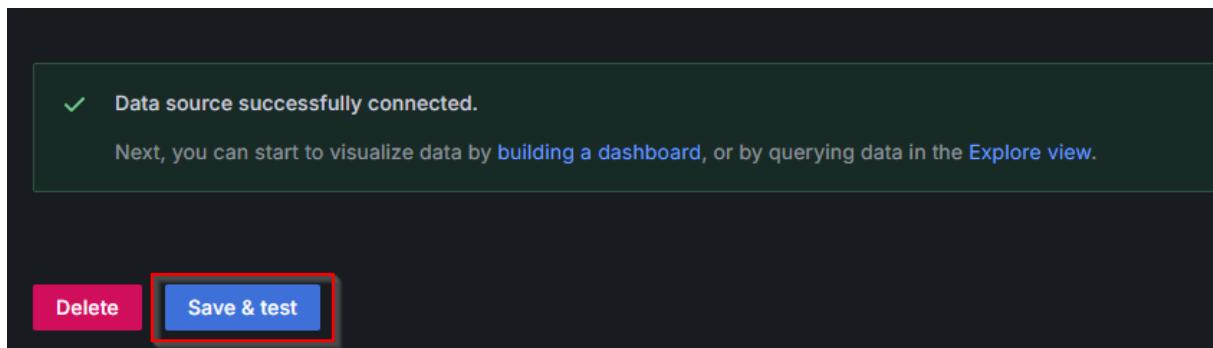
- Geef de data source een goede naam, en zet connectie URL goed.



Figuur 213: Grafana koppelen met loki (4)

- Laat de rest op default staan en klik op 'Save & Test'

## Automatisch toewijzen van een VLAN aan een gebruiker

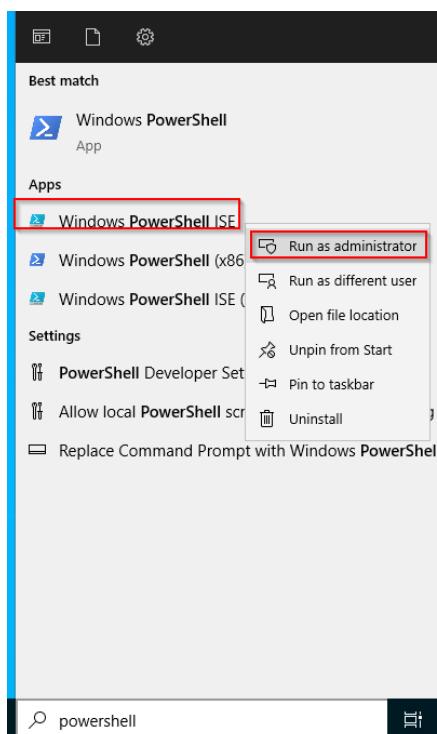


Figuur 214: Grafana koppelen met loki (5)

Je hebt nu een gegevensbron gecreëerd waaruit je later gegevens kunt opvragen en deze kunt weergeven op het dashboard.

#### 6.7.2.4 Promtail

- Kopieer het PowerShell-script dat in de ZIP-map van het project zit naar de server. (Install-PromtailOnWindows.ps1)
- Open Powershell ISE in administrator rechten.



Figuur 215: Installatie van promtail (1)

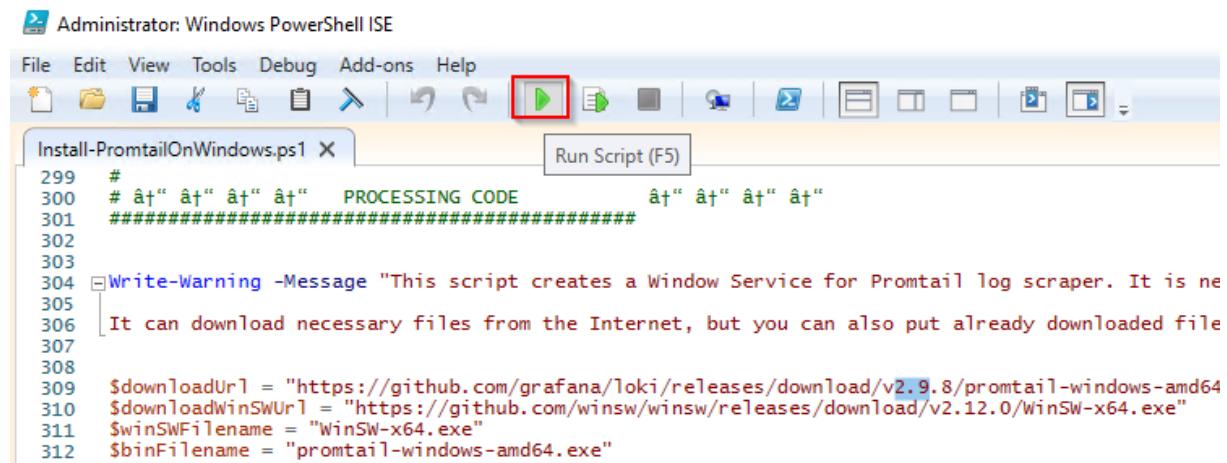
## Automatisch toewijzen van een VLAN aan een gebruiker

- Open het bestand in de teksteditor en zorg ervoor dat de betreffende regel dezelfde versie gebruikt als je Loki-server (hier wordt v2.9.8 gebruikt), zoals aangegeven in de handleiding die je volgt.

```
$downloadUrl = "https://github.com/grafana/loki/releases/download/v2.9.8/promtail-windows-amd64.exe.zip"
```

Figuur 216: Installatie van promtail (2)

- Voer het bestand uit door op de ‘run script’ button te klikken.

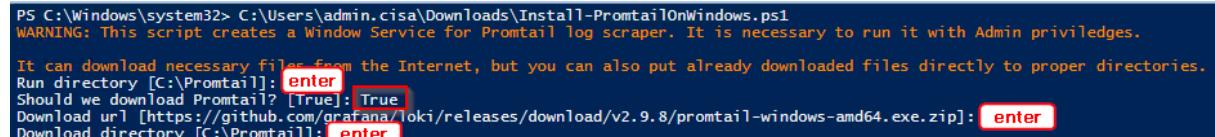


```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Run Script (F5)

Install-PromtailOnWindows.ps1
299  #
300  # PROCESSING CODE
301  #####
302
303
304 Write-Warning -Message "This script creates a Window Service for Promtail log scraper. It is ne
305 [It can download necessary files from the Internet, but you can also put already downloaded file
306
307
308
309 $downloadUrl = "https://github.com/grafana/loki/releases/download/v2.9.8/promtail-windows-amd64
310 $downloadWinSWUrl = "https://github.com/winsw/winsw/releases/download/v2.12.0/WinSW-x64.exe"
311 $winSWFilename = "WinSW-x64.exe"
312 $binFilename = "promtail-windows-amd64.exe"
```

Figuur 217: Installatie van promtail (3)

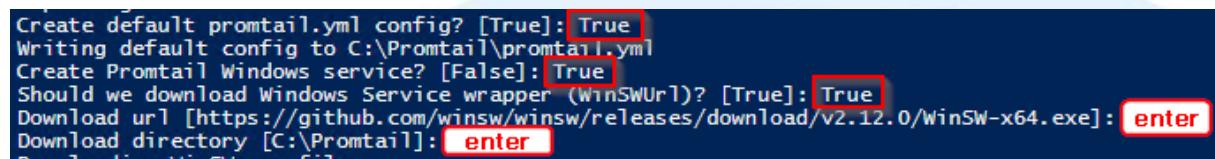
- Dit gedeelte van het PowerShell-script zorgt ervoor dat er een directory wordt aangemaakt voor Promtail. Vervolgens wordt een uitvoerbaar bestand gedownload vanuit GitHub.



```
PS C:\Windows\system32> C:\Users\admin.cisa\Downloads\Install-PromtailOnWindows.ps1
WARNING: This script creates a Window Service for Promtail log scraper. It is necessary to run it with Admin privileges.
It can download necessary files from the Internet, but you can also put already downloaded files directly to proper directories.
Run directory [C:\Promtail]: enter
Should we download Promtail? [True]: True
Download url [https://github.com/grafana/loki/releases/download/v2.9.8/promtail-windows-amd64.exe.zip]: enter
Download directory [C:\Promtail]: enter
```

Figuur 218: Installatie van promtail (4)

- Hier kies je de locatie van het Promtail-configuratiebestand en configureren je Promtail als een service.



```
Create default promtail.yml config? [True]: True
Writing default config to C:\Promtail\promtail.yml
Create Promtail Windows service? [False]: True
Should we download Windows Service wrapper (WinSWUrl)? [True]: True
Download url [https://github.com/winsw/winsw/releases/download/v2.12.0/WinSW-x64.exe]: enter
Download directory [C:\Promtail]: enter
```

Figuur 219: Installatie van promtail (5)

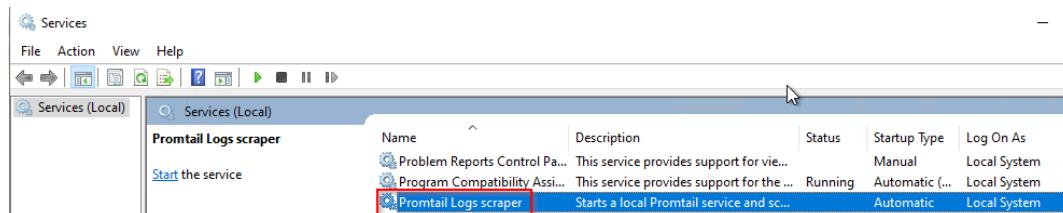
- In het laatste deel van het PowerShell-script wordt om toestemming gevraagd om WinSW te installeren. Dit programma maakt het mogelijk om een service aan te maken. Daarnaast geef je je Promtail-service een naam.

## Automatisch toewijzen van een VLAN aan een gebruiker

```
Create WinSW config as C:\Promtail\WinSW-x64.xml ? [True]: True
Service name [Promtail]: enter
Service name [Promtail Logs scraper]: enter
Writing default WinSW config to C:\Promtail\WinSW-x64.xml
Installing Promtail Windows Service
Promtail Windows Service Installed (hopefully)
```

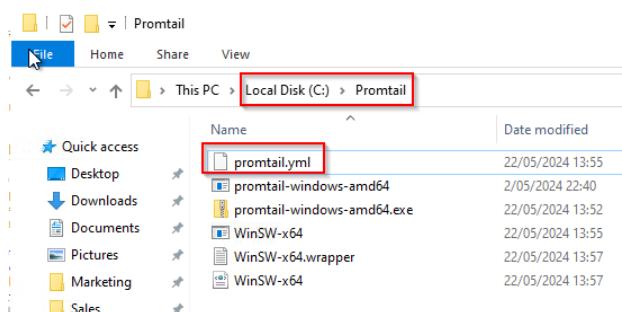
Figuur 220: Installatie van promtail (6)

Promtail is nu geïnstalleerd op de computer. Je kunt de installatie verifiëren door naar de services te gaan en de service "Promtail" op te zoeken.



Figuur 221: Installatie van promtail (7)

Je kunt het YAML-bestand van Promtail vinden in de map "promtail" op de C-schijf.



Figuur 222: Installatie van promtail (8)

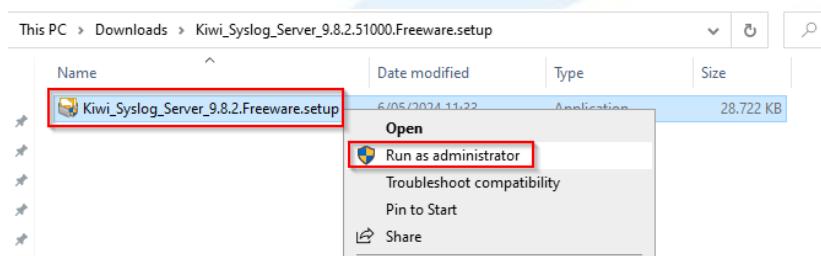
### 6.7.2.5 Kiwi syslog service manager

- Download de .exe file voor de syslog manager versie 9.8.2.

<https://www.solarwinds.com/downloads/SyslogServerFree.zip>

- Unzip de file 'Kiwi\_Syslog\_Server\_9.8.3.Freeware.setup'

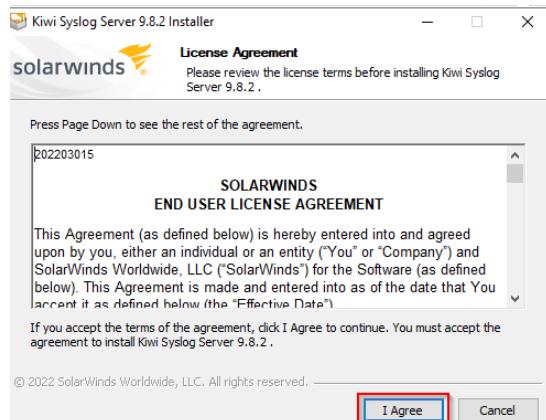
- Voer de .exe file uit als administrator om de wizard te volgen.



Figuur 223: Installatie van kiwi syslog manager (1)

## Automatisch toewijzen van een VLAN aan een gebruiker

- Klik 'I agree'



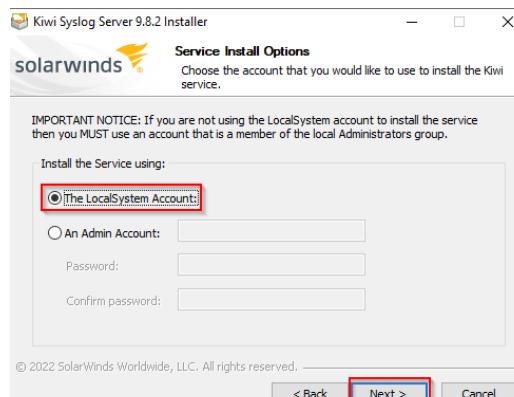
*Figuur 224: Installatie van kiwi syslog manager (2)*

- Duid aan dat kiwi syslog word gestart als een service, daarna klik je op 'next'.



*Figuur 225: Installatie van kiwi syslog manager (3)*

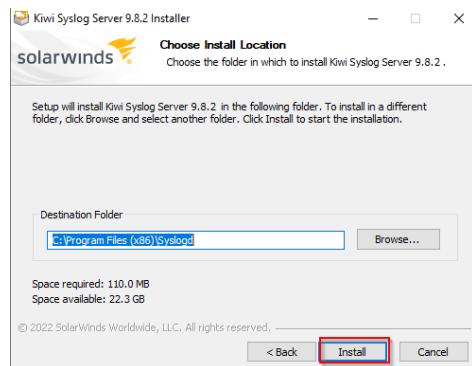
- Laat het op default staan en klik op 'next'.



*Figuur 226: Installatie van kiwi syslog manager (4)*

## Automatisch toewijzen van een VLAN aan een gebruiker

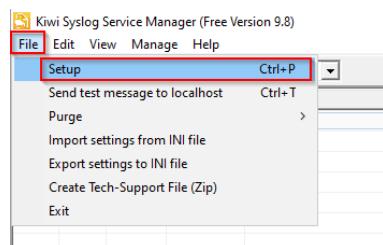
- Klik op 'Install'



Figuur 227: Installatie van kiwi syslog manager (5)

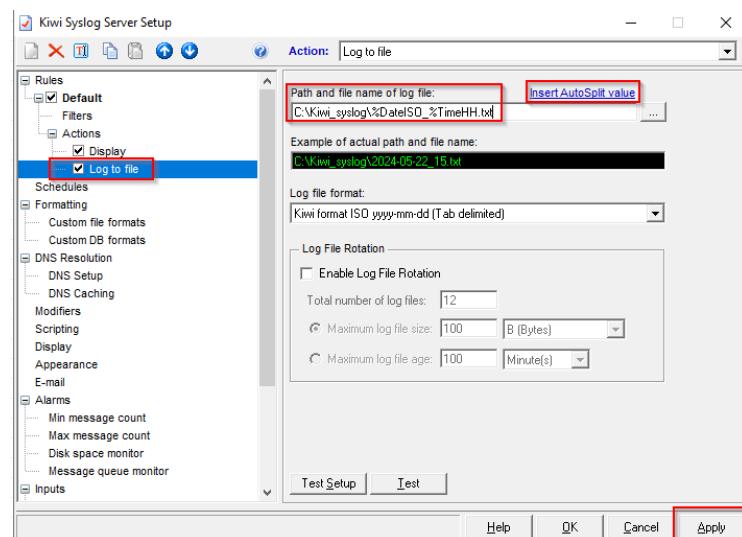
Nu heb je een Kiwi Syslog Manager opgezet, maar je moet er nog voor zorgen dat het zijn syslog op de juiste locatie opslaat, zodat het PowerShell-script het later kan lezen.

- Open kiwi syslog manager, klik daarna op 'file > Setup'.



Figuur 228: Installatie van kiwi syslog manager (6)

- Maak een folder in de C-schijf waarin je de kiwi syslogs gaat saven, verander daarna het path. Bij 'Insert AutoSplit Value' kan je ervoor zorgen dat hij de systeem datum overneemt.

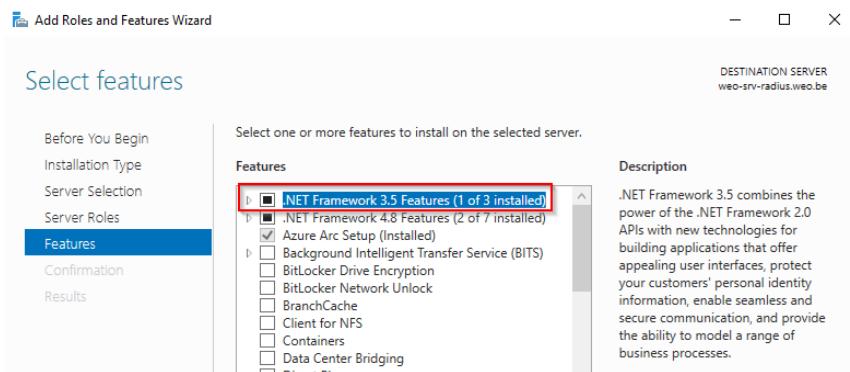


Figuur 229: Installatie van kiwi syslog manager (7)

## Automatisch toewijzen van een VLAN aan een gebruiker

### 6.7.2.6 Kiwi log forwarder

- Installeer eerst .NET 3.5 op de server, via roles en features. Op de radius server, als je graag nog andere servers wilt implementeren zal dit ook nodig zijn op deze server.

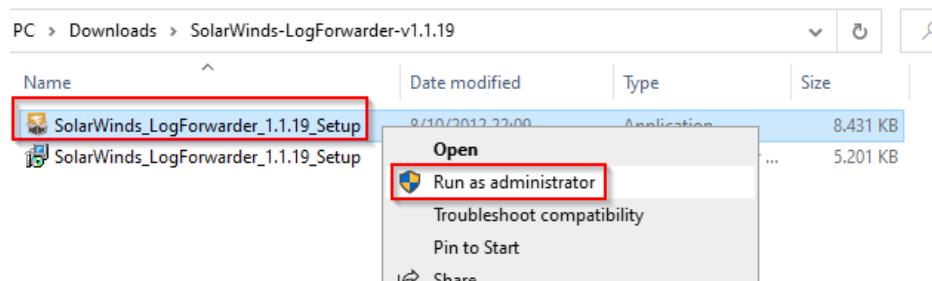


Figuur 230: Installatie van kiwi syslog forwarder (1)

- Download de .exe file voor de log forwarder versie 1.1.19.

<https://downloads.solarwinds.com/solarwinds/Release/Kiwi/LogForwarder/SolarWinds-LogForwarder-v1.1.19.zip>

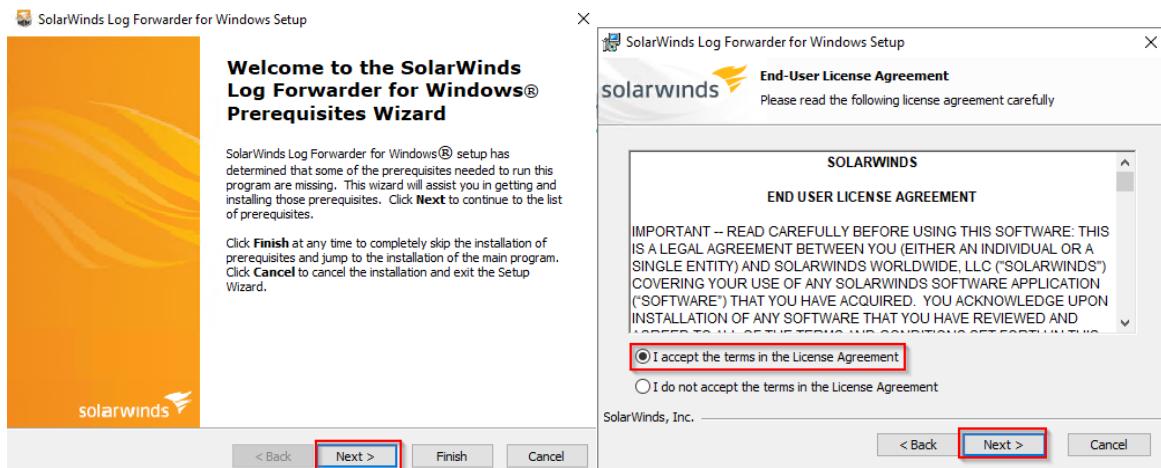
- Unzip de file 'SolarWinds-LogForwarder-v1.1.19'
- Voer de .exe file uit als administrator om de wizard te volgen.



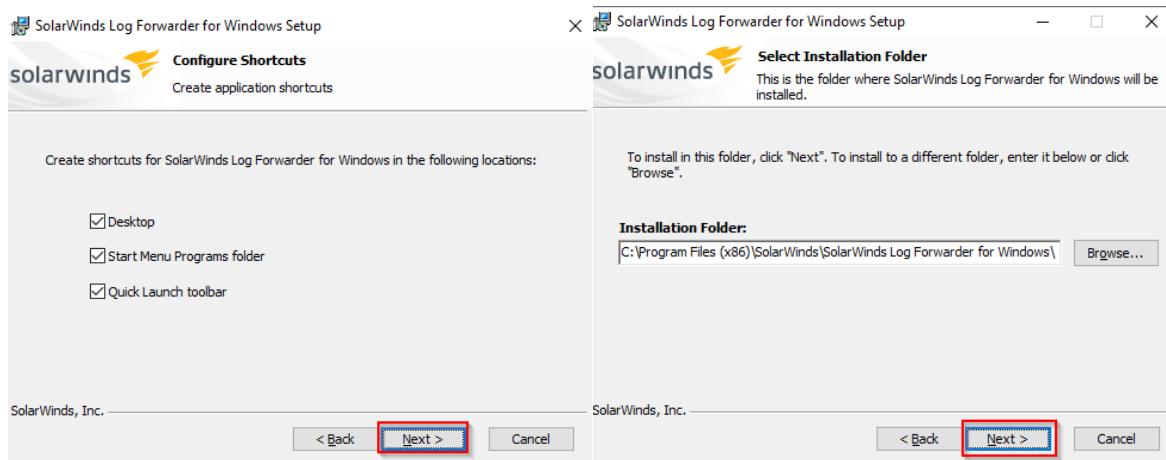
Figuur 231: Installatie van kiwi syslog forwarder (2)

- Klik 'next'

## Automatisch toewijzen van een VLAN aan een gebruiker



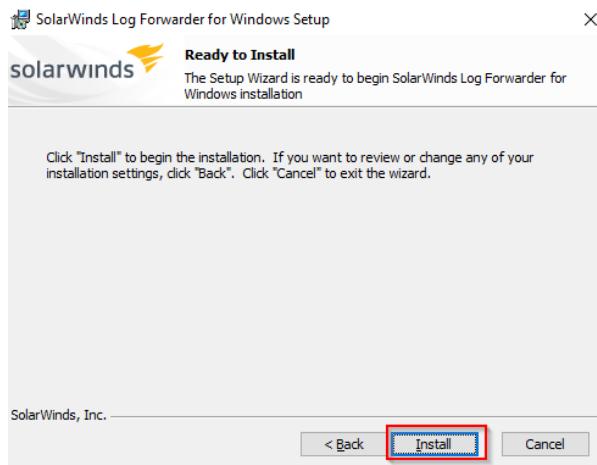
Figuur 232: Installatie van kiwi syslog forwarder (3)



Figuur 233: Installatie van kiwi syslog forwarder (4)

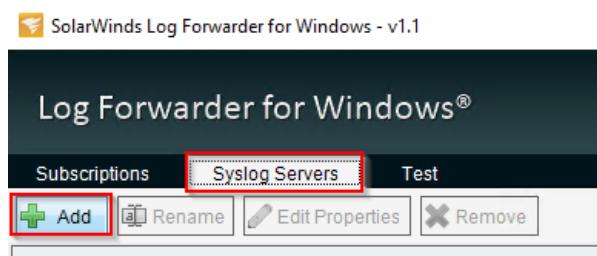
- Klik 'Install'

## Automatisch toewijzen van een VLAN aan een gebruiker



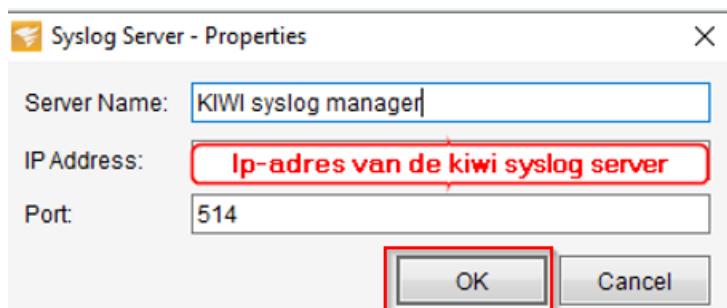
Figuur 234: Installatie van kiwi syslog forwarder (5)

- Open nu 'Solarwinds log forwarder for windows v1.1', daarna klik je op tab 'syslog servers'



Figuur 235: Installatie van kiwi syslog forwarder (6)

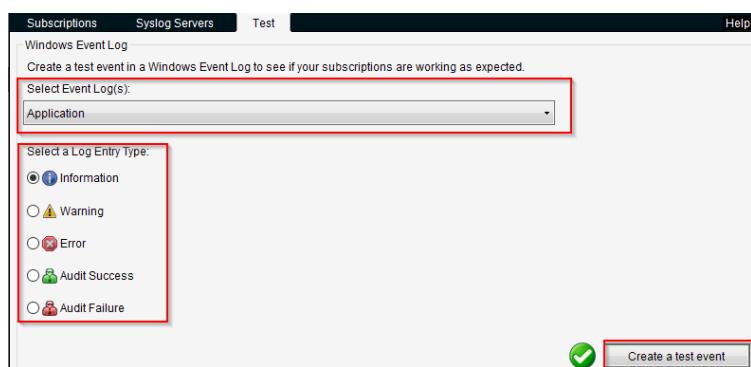
- Geef hier het ip-adres van je syslog server klik vervolgens op 'OK'.



Figuur 236: Installatie van kiwi syslog forwarder (7)

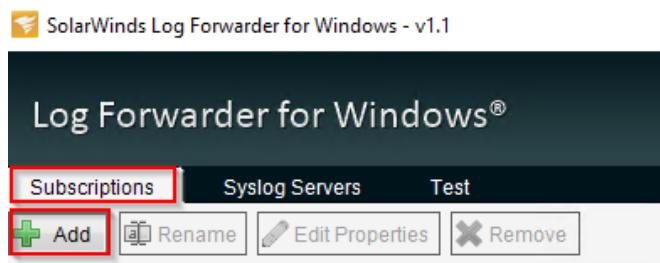
- Klik op het tab 'Test' selecteer een event en kies een entry type daarna kan je een test event sturen naar je syslog server.

## Automatisch toewijzen van een VLAN aan een gebruiker



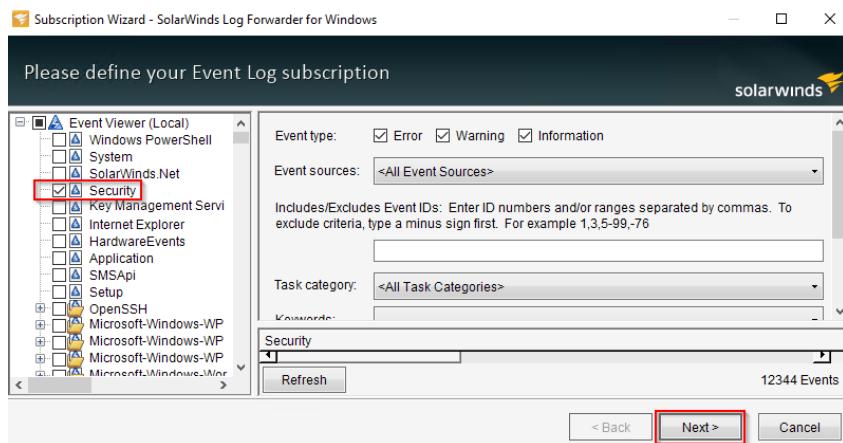
Figuur 237: Installatie van kiwi syslog forwarder (8)

- Nu gaan we ervoor zorgen dat onze security syslog wordt gestuurd naar de kiwi syslog server. Klik op de tab 'subscriptions' en daarna op 'add'.



Figuur 238: Installatie van kiwi syslog forwarder (9)

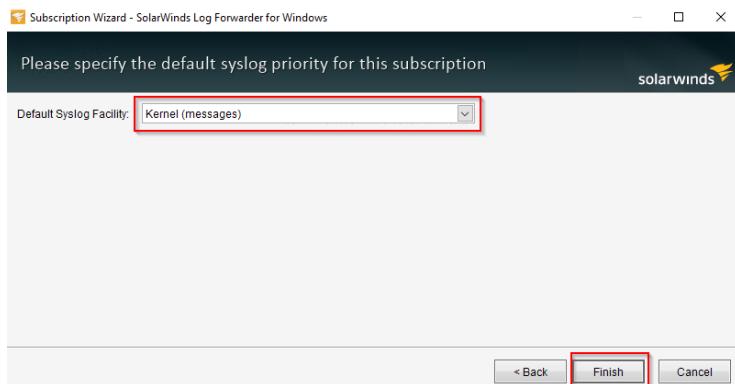
- Vervolgens selecteer je 'security' en daarna op 'Next'.



Figuur 239: Installatie van kiwi syslog forwarder (10)

- Selecteer 'Kernel (messages)' en klik op 'Finish'.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 240: Installatie van kiwi syslog forwarder (11)

Nu zou je op de Kiwi syslog service manager logs moeten zien binnen komen. Maar ook zouden ze moeten opgeslagen worden in de juiste folder.

Kiwi Syslog Service Manager (Free Version 9.8)				
File Edit View Manage Help				
Display 00 (Default)				
Date	Time	Priority	Hostname	Message
05-22-2024	15:48:20	Kernel Notice	127.0.0.1	mei 22 15:48:20 weo-srv-fs.weo.be MSWinEventLog 5 Security 2 wo mei assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
05-22-2024	15:48:20	Kernel Notice	127.0.0.1	mei 22 15:48:20 weo-srv-fs.weo.be MSWinEventLog 5 Security 1 wo mei successfully logged on. Subject: Security ID: S-1-5-18

Figuur 241: Logs van kiwi syslog

This PC > Local Disk (C:) > Kiwi_syslog			
Name	Date modified	Type	Size
2024-05-22_15	22/05/2024 15:48	Text	1,1 KB

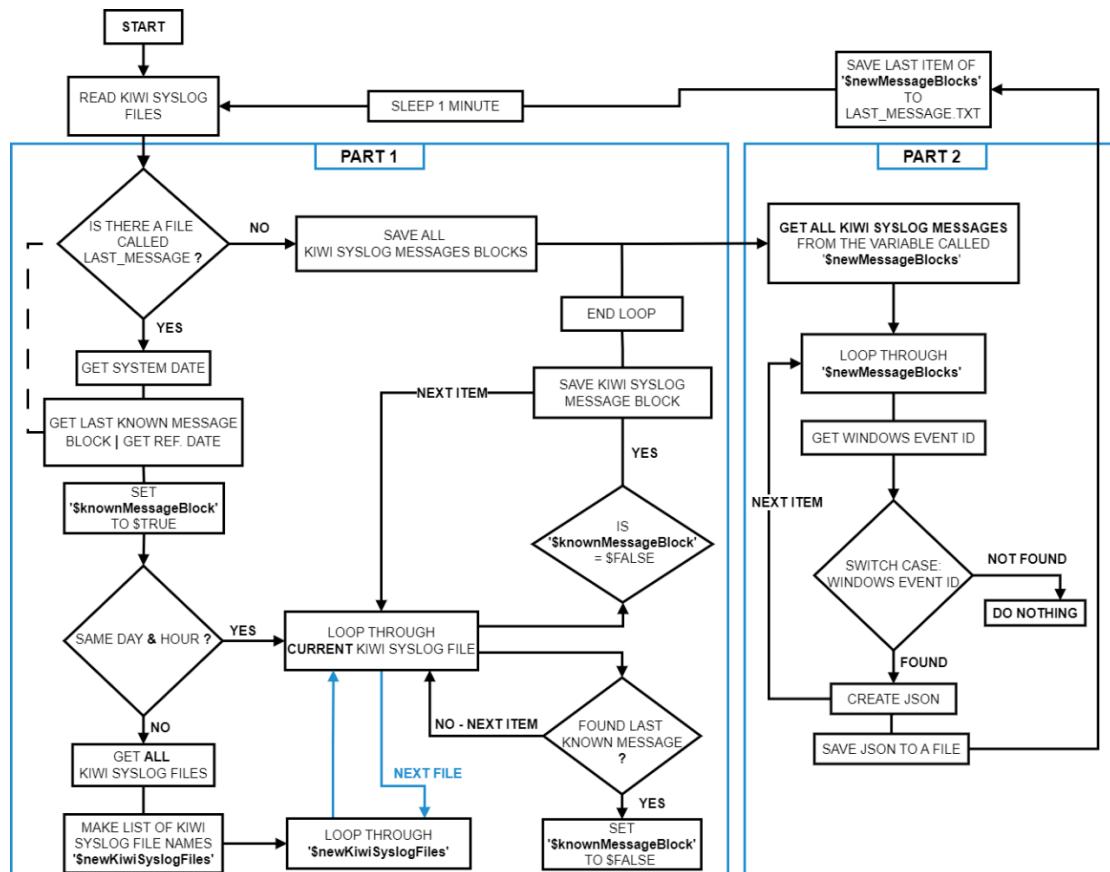
Figuur 242: Logs geschreven naar bestanden

## Automatisch toewijzen van een VLAN aan een gebruiker

## 6.7.2.7 Powershell

Nu we alles hebben geïnstalleerd, hebben we PowerShell nodig om alles met elkaar te verbinden.

## Flowchart van het PowerShell-script:



Figuur 243: Flowchart Powershell script

## Uitleg over het script:

- Je kan het powershell script terugvinden in het zip-bestand van dit project. (kiwi\_syslog\_promtail.ps1)
- Pas de variabelen aan naar jouw omgeving.

## Automatisch toewijzen van een VLAN aan een gebruiker

```

# Start - This the user can change -----
$fileExtension = ".txt"
$absolutePathToDirectory = "C:\Test\" 
$absolutePathToKiwiSyslogDirectory = $absolutePathToDirectory + "Kiwi_Syslogs" + "\"
$radiusFriendlyNameOfFirewall = "FortiGate-8"
$radiusFriendlyNameOfSwitch = "Aruba switch"

# This specifies the number of days after which syslog files are considered for deletion.
# Set this value to control the retention period for syslog files.
# Note: If $retentionPolicyDays is set to 0 or a negative value, no files will be deleted.
$retentionPolicyDays = 1

# End - This the user can change -----

```

Figuur 244: Powershell script (1)

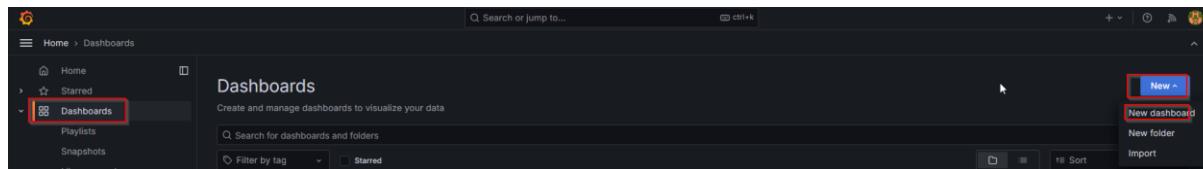
- Om het script te laten werken, moet je het uitvoeren als administrator.

### Verbeter punten:

- Het PowerShell-script kan worden geoptimaliseerd, vooral met betrekking tot de uitvoering van de for-lussen.
- Error handling moet nog worden toegevoegd in het powershell-script.
- Het PowerShell-script moet worden omgezet van handmatige uitvoering naar een service of een taakplanner.
- Er is een functie genaamd 'Get-IPMACFromMessageBlock' waarbij je nog code moet toevoegen zodat hij de DHCP server vraagt om het MAC-adres omzet naar een IP-adres of andersom.

### 6.7.2.8 Pre-build dashboard importeren naar Grafana.

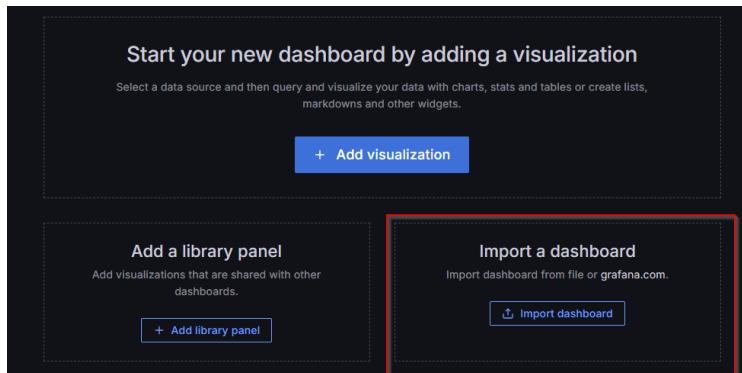
- Maak een nieuw dashboard.



Figuur 245: Dashboard aanmaken

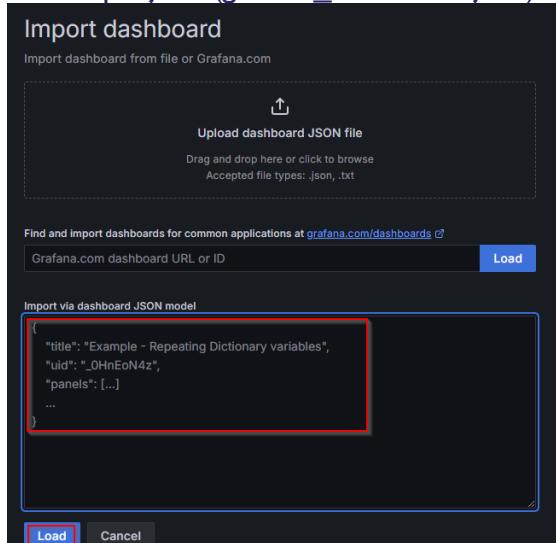
- Selecteer 'Import a dashboard'

## Automatisch toewijzen van een VLAN aan een gebruiker



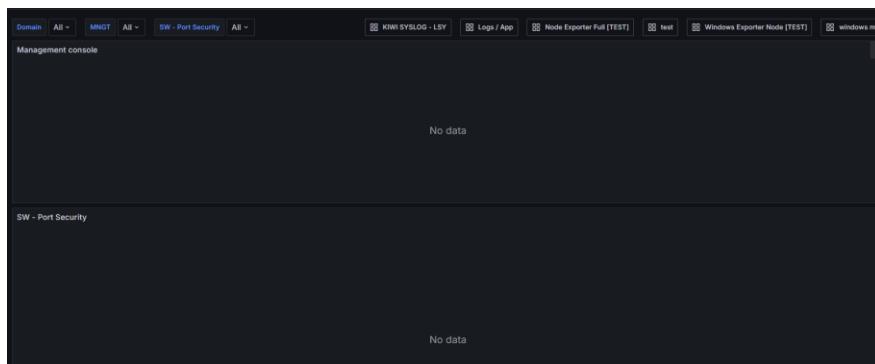
*Figuur 246: Dashboard importeren*

- Plak hier de volledige JSON van het dashboard, dat je kan terugvinden in het zip-bestand van dit project. (`grafana_dashboard.json`)



*Figuur 247: Dashboard importeren*

- Zodra je al deze stappen hebt voltooid, zou je iets moeten zien dat er ongeveer zo uitziet.



*Figuur 248: Grafana dashboard (I)*

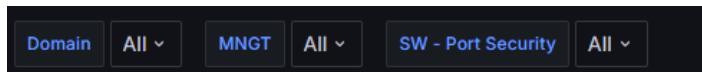
## Automatisch toewijzen van een VLAN aan een gebruiker

- Als je nu een syslog-activiteit zou uitvoeren, zoals aanmelden op een pc of aanmelden op de firewall, worden deze gebeurtenissen hier weergegeven.

Domain	All	MNGT	All	SW - Port Security	All	KIWI SYSLOG - ALL	KIWI SYSLOG - LSY	Logs / App	Node Exporter Full [TEST]	test	Windows Exporter Node [TEST]
<b>windows.mij</b>											
Management console											
Date (HH:MM:SS)	Priority	Win Event ID	Username	Access	Authentication_Type	Reason 1	IP 1	MAC 1	NAS_Identifier	NAS Port	
2024-05-16 00:55:42	Critical	6273	admin.cisa	DENIED							
2024-05-16 16:55:42	Notice	62720	admin.cisa	GRANTED							
2024-05-16 16:55:42	Notice	6272	admin.cisa	GRANTED							
2024-05-16 17:22:48	Critical	6273	admin.fogd	DENIED							
2024-05-17 17:37:02	Critical	6273	admin.cisa	DENIED							
2024-05-17 17:37:02	Critical	6273	admin.cisa	DENIED							
SW - Port Security											
Date (HH:MM:SS)	Priority	WIN Event ID	SOURCE - IP	SOURCE - MAC	USERNAME	Access	VLAN	Auth - Type	SW - PORT	Radius Client	Reason
2024-05-17 00:25:02	Critical	6273	null	E0-73-E7-30-70-31	admin	DENIED		EAP	3	Aruba switch	UNKNOWN USER
2024-05-17 00:00:04	Critical	6273	null	E0-73-E7-30-70-31	admin	DENIED		EAP	3	Aruba switch	UNKNOWN USER
2024-05-21 13:29:35	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	
2024-05-21 13:16:30	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	
2024-05-21 13:10:31	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	
2024-05-21 13:07:55	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	
2024-05-21 12:57:49	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	
2024-05-21 12:56:49	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	
2024-05-21 12:56:15	Notice	6272	null	E0-73-E7-30-70-31	WEO\hr.rookie	GRANTED	VLAN66 - HR	PEAP	4	Aruba switch	

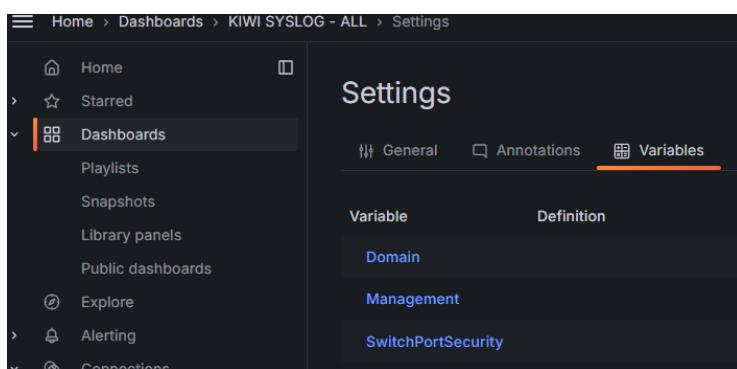
Figuur 249: Dashboard met data

- Dit zijn variabelen waarmee je kunt overschakelen tussen domeinen en andere parameters.



Figuur 250: Grafana variables (1)

- Je kan ze terug vinden bij de opties van het dashboard.



Figuur 251: Grafana variables (2)

## Automatisch toewijzen van een VLAN aan een gebruiker

## 7. Switches

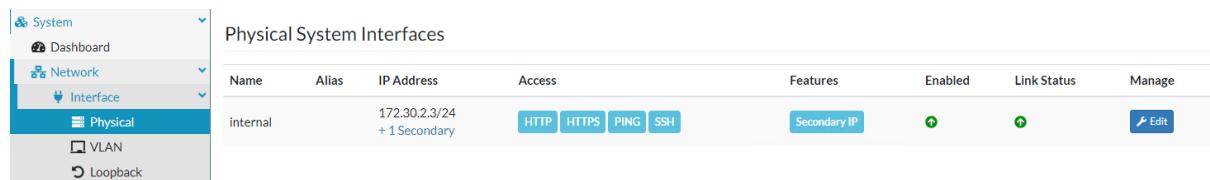
De switches gaan we gebruiken in de oplossing om onze test toestellen aan te koppelen. Om de authenticatie in gang te zetten. Labo A maakt gebruik van de fortiswitch en Labo B van een aruba switch.

### 7.1 FortiSwitch

#### 7.1.1 Opzet

Om het mogelijk te maken om aan de gebruikersinterface te geraken hebben we via CLI het interne IP-adress van de switch en de poort geconfigureerd die ook naar de fysieke server gaat zodat we traffiek hebben van onze fysieke omgeving naar de virtuele omgeving.

Om het interne IP adres aan te passen navigeren we naar system > network > interface > physical. Hier kunnen we de configuratie doen van het interne IP. Zoals in onderstaande afbeeldingen te zien is, hebben we administratieve toegang gegeven zodat we aan de user interface kunnen als ook de command line via SSH. We kunnen hier alleen maar naartoe via het management VLAN. Daarnaast hebben we ook een tweede IP-adress toegevoegd voor de mogelijkheid dat we aan de switch kunnen configureren zonder hiervoor bepaalde poorten op het management VLAN te zetten.



The screenshot shows the FortiSwitch management interface. On the left is a navigation sidebar with 'System' selected, followed by 'Dashboard', 'Network' (with 'Physical' selected), 'Interface', 'Physical', 'VLAN', and 'Loopback'. The main area is titled 'Physical System Interfaces' and contains a table with the following data:

Name	Alias	IP Address	Access	Features	Enabled	Link Status	Manage
internal		172.30.2.3/24 + 1 Secondary	HTTP HTTPS PING SSH	Secondary IP	Enabled	Link Up	

Figuur 252: FortiSwitch fysiek interface (1)

## Automatisch toewijzen van een VLAN aan een gebruiker

### Edit Physical Interface

Name	internal
MAC Address	[REDACTED]
Alias	<input type="text"/>
<b>IP Configuration</b>	
Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP/Netmask	<input type="text"/> 172.30.2.3 255.255.255.0
<b>Administration</b>	
Status	<input checked="" type="radio"/> Up <input type="radio"/> Down
Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input type="checkbox"/> RADIUS Accounting <input checked="" type="checkbox"/> SSH <input type="checkbox"/> TELNET

Figuur 253: FortiSwitch fysiek interface (2)

### Secondary IP

ID (1-65535)	Address	Access	Manage
1	192.168.1.99 255.255	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input type="checkbox"/> RADIUS Accounting <input checked="" type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP	<input type="button" value="Remove"/>
			<input type="button" value="Add IP"/>

### DHCP Relay

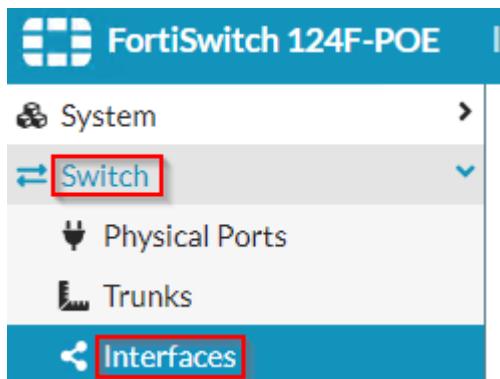
Enabled	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Figuur 254: FortiSwitch fysiek interface (3)

Daarnaast hebben we gekozen om de fysieke server te verbinden met poort 13 op de FortiSwitch. Deze poorten leveren geen PoE en dit is ook niet nodig voor deze verbinding; zo blijft er mee ruimte voor eventuele camera's of APs.

Voor de configuratie van deze poort navigeren we naar switch > interfaces.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 255: FortiSwitch Interfaces (1)

Daarna drukken we op poort 13 en daarna gaan we deze bewerken via edit:

Interfaces

<input type="checkbox"/> Select All	<input type="checkbox"/> Deselect All	<input checked="" type="button"/> Edit	Search: <input type="text"/>				
Name	Type	Traffic (Last Day)	VLAN(s)	STP	Edge Port	Packet Sampler	
Internal	Physical	19.16kbps	51	—	✓	—	
port1	Physical	69.15kbps	51/50-59	✓	✓	—	
port2	Physical	0.000bps	1	✓	✓	—	
port3	Physical	0.000bps	1	✓	✓	—	
port4	Physical	0.000bps	1	✓	✓	—	
port5	Physical	0.000bps	1	✓	✓	—	
port6	Physical	0.000bps	1	✓	✓	—	
port7	Physical	0.000bps	1	✓	✓	—	
port8	Physical	0.000bps	1	✓	✓	—	
port9	Physical	0.000bps	1	✓	✓	—	
port10	Physical	0.000bps	1	✓	✓	—	
port11	Physical	0.000bps	1	✓	✓	—	
port12	Physical	0.000bps	1	✓	✓	—	
port13	Physical	69.28kbps	1/1,50-58/1	✓	✓	—	

Figuur 256: FortiSwitch Interfaces (2)

Om netwerk door te laten van het virtuele gedeelte naar het fysieke deel en andersom zetten we ID's bij de toegelaten VLANs 50-59, dit zijn alle VLANs die tot ons bekabeld netwerk behoren. Daarnaast zetten we native, toegelaten en untagged VLAN 1.

Naast dat we dit met het gebruikersinterface configureren kunnen we dit ook configureren door gebruik te maken van de command line.

Het configureren van deze poort, poort 13 via CLI gebeurd als volgt:

```
config switch interface
edit port13
    set native-vlan 1
    set allowed-vlans 1,50-59
    set untagged-vlans 1
end
```

## Automatisch toewijzen van een VLAN aan een gebruiker

### 7.1.2 Hostname

We hebben de hostname van de switch aangepast. Dit hebben we gedaan door onze hostname in te typen en te updaten.



Figuur 257: FortiSwitch hostname

We hebben ook de tijd ingesteld op de switch, deze zal syncroniseren om de tien minuten.  
System Time

Figuur 258:FortiSwitch NTP

### 7.1.3 Instellen van RADIUS server

We hebben de RADIUS server ingesteld door te navigeren naar system > authentication > RADIUS. In dit scherm drukken we op add server. We kiezen een naam van de RADIUS server. De poort is 1812, dit is de authenticatie en autorisatie poort van RADIUS. Hier vullen we onze radius server aan en het serversecret dat we configureren bij het aanmaken van de RADIUS client in de network policy server.

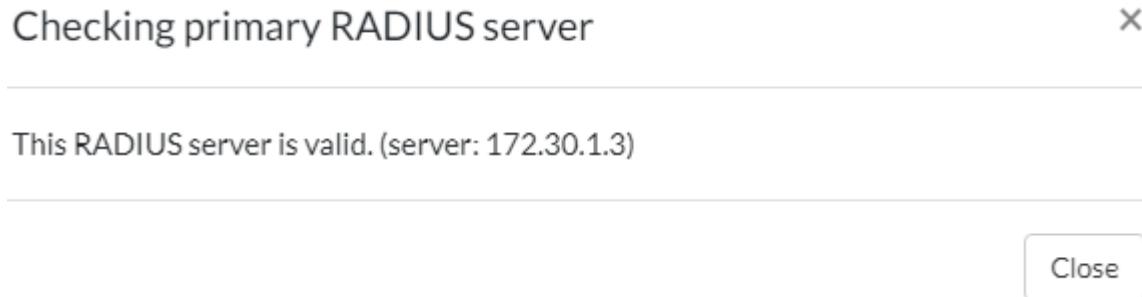
## Automatisch toewijzen van een VLAN aan een gebruiker

### Primary Server

Server Address	<input type="text" value="172.30.1.3"/>
Server Secret	<input type="text" value="*****"/>
<a href="#" style="color: blue; margin-right: 10px;"> Test Connectivity</a> <a href="#" style="color: blue;"> Test User Credentials</a>	

Figuur 259: FortiSwitch Radius

Met de knoppen weergegeven in bovenstaand screenshot (Figuur 259) kan je de connectiviteit naar de radius server testen; zo kan je zien dat je al aan de server kan:



Figuur 260: FortiSwitch Radius (2)

Je kan ook user credentials testen om te controleren of de RADIUS server werkt. Dit doen we door username en wachtwoord mee te geven van een users die in het domein zit:

<a href="#" style="color: blue; margin-right: 10px;"> Test Connectivity</a> <a href="#" style="color: blue;"> Test User Credentials</a>							
<p>Primary User Authentication</p> <table border="0"> <tr> <td style="vertical-align: top; padding-right: 10px;">Username</td> <td><input type="text" value="Sofie.Clercq"/></td> </tr> <tr> <td colspan="2" style="text-align: center; padding-top: 5px;"> <a href="#" style="color: blue; margin-right: 10px;">Test</a> </td> </tr> <tr> <td style="vertical-align: top; padding-right: 10px;">Password</td> <td><input type="password" value="*****"/></td> </tr> </table>		Username	<input type="text" value="Sofie.Clercq"/>	<a href="#" style="color: blue; margin-right: 10px;">Test</a>		Password	<input type="password" value="*****"/>
Username	<input type="text" value="Sofie.Clercq"/>						
<a href="#" style="color: blue; margin-right: 10px;">Test</a>							
Password	<input type="password" value="*****"/>						

Figuur 261: FortiSwitch Radius (3)

Na het testen kan je zien wat er succesvol of niet succesvol is:

## Automatisch toewijzen van een VLAN aan een gebruiker

## ×Primary User Authentication

Connection Status      Successful  
 User Credentials      Successful

AVP: I=6 t=Framed-Protocol(7) Value: 1  
 AVP: I=6 t=Service-Type(6) Value: 2  
 AVP: I=6 t=Tunnel-Medium-Type(65) Value: 00

Figuur 262: FortiSwitch Radius (4)

Als authentication scheme geven we MS-CHAP-v2 aan. Als NAS-IP geven we het internal IP van de switch mee.

Authentication Scheme	MS-CHAP-v2
NAS IP/Call Station ID	172.30.2.3
Include in Every User Group	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Figuur 263: FortiSwitch Radius (5)

#### 7.1.4 Groep aanmaken

Voor het aanmaken van een groep navigeren we in de interface naar system > user > group. Hier gaan we een nieuwe groep toevoegen via add group.

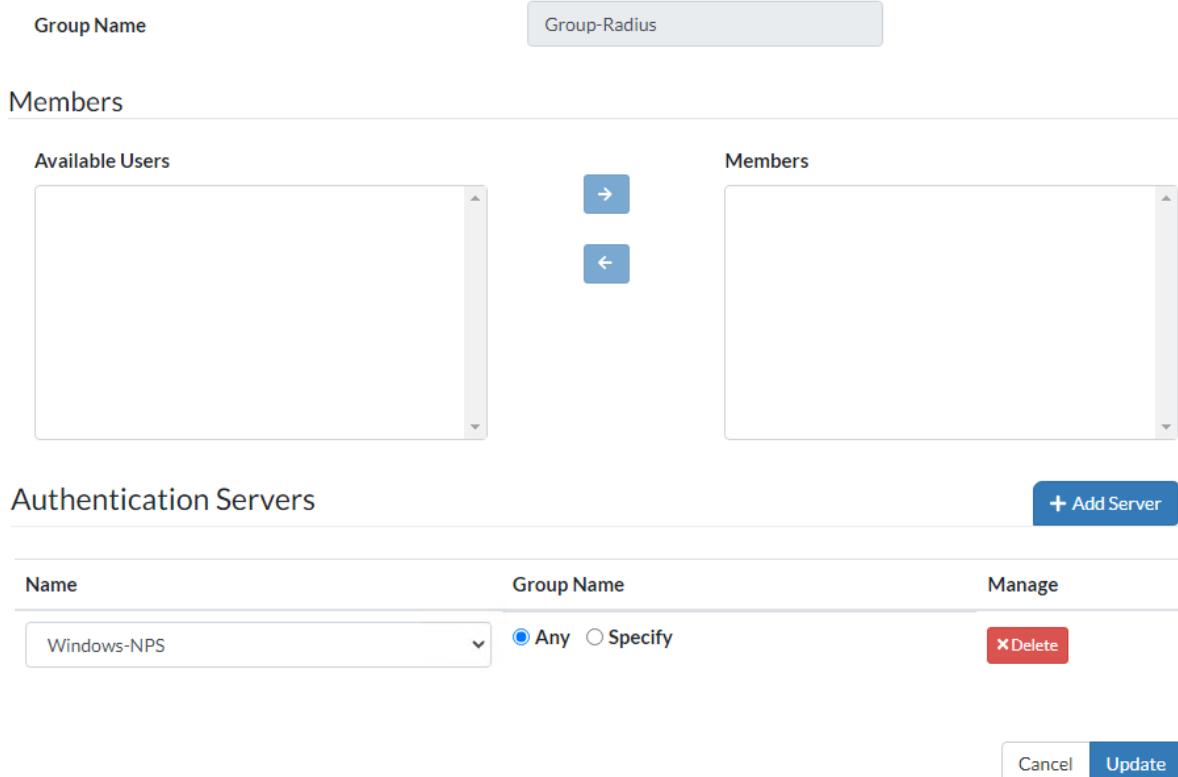
Group Name	Members	Authentication Servers	References	Manage
Group-RADIUS		Windows-NPS	0	<input type="button" value="Edit"/>

Figuur 264: FortiSwitch groepen aanmaken (1)

## Automatisch toewijzen van een VLAN aan een gebruiker

Hier heb ik een groep gemaakt “group-radius”. Daarnaast hebben we daar de authenticatie server aan toegevoegd namelijk de RADIUS server die we hier boven hebben aangemaakt. In mijn geval is dit Windows-NPS. Daarna kan je deze groep aanmaken.

### Edit Group



The screenshot shows two main sections: 'Edit Group' and 'Authentication Servers'.

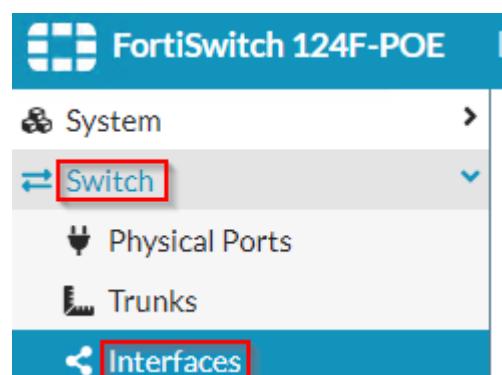
**Edit Group:** A 'Group Name' field contains 'Group-Radius'. Below it, a 'Members' section shows two lists: 'Available Users' (empty) and 'Members' (empty), with a double-headed arrow between them.

**Authentication Servers:** A table lists 'Windows-NPS' as the authentication server. It includes columns for 'Name', 'Group Name' (set to 'Any'), and 'Manage'. The 'Manage' row for Windows-NPS has a 'Delete' button. At the bottom right are 'Cancel' and 'Update' buttons.

Figuur 265: FortiSwitch groepen aanmaken (2)

### 7.1.5 Configuratie 802.1x poort

Voor het configureren van een poort, gaan we naar switch en daarna interfaces. Hier kiezen we een poort die we graag willen gebruiken. Dit kunnen er natuurlijk ook meerdere zijn.



The screenshot shows the FortiSwitch 124F-POE interface navigation menu. The 'Switch' and 'Interfaces' items are highlighted with red boxes.

- System
- Switch (highlighted)
- Physical Ports
- Trunks
- Interfaces (highlighted)

Figuur 266: FortiSwitch interface (1)

## Automatisch toewijzen van een VLAN aan een gebruiker

Ik doe dit op poort 17 van de switch. We gebruiken als native VLAN 1. Het maakt echter niet uit welke je hier gebruikt. Op de fortiswitch zal na een succesvolle autorisatie de native VLAN verandere door wat de netwerk policy server zal meegeven in de configuratie.

De configuratie die we nodig hebben voor de poortbeveiliging. We selecteren als modus 802.1X voor authenticatie. We selecteren hier ook de EAP pass-through mode die ervoor zal zorgen dat de EAP-pakketten tussen de eindapparaten en de authenticatie server doorgegeven worden zonder de pakketten zelf te verwerken of te wijzigen.

We kiezen ook voor een auth fail vlan, mocht de authenticatie niet lukken zal dit eindtoestel worden geplaatst in VLAN 57, dit VLAN wordt gebruikt voor quarantaine. Dan zal het niet mogelijk zijn om naar het internet te gaan noch mogelijk naar andere toestellen in dit netwerk.

Als laatste voegen we de eerder aangemaakte groep aan de port security toe; dit zal toelaten dat de pakketten worden doorgegeven aan de authenticatieserver, de radius server.

### Port Security

Security Mode <input type="radio"/> None <input checked="" type="radio"/> 802.1X <input type="radio"/> 802.1X MAC-Based  <input type="checkbox"/> MAC Auth Bypass <input checked="" type="checkbox"/> EAP Pass-Through Mode <input type="checkbox"/> Frame VLAN Apply <input type="checkbox"/> Open Authentication <input type="checkbox"/> Guest VLAN  Guest VLAN ID <input type="text" value="56"/> (1-4094)	<input type="checkbox"/> Guest Auth Delay <input type="text" value="1"/> (1-900)  <input checked="" type="checkbox"/> Auth Fail VLAN Auth Fail VLAN ID <input type="text" value="57"/> (1-4094)  <input type="checkbox"/> RADIUS Session Timeout Security Group <input type="text" value="Group-Radius"/>
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Figuur 267: FortiSwitch poortbeveiliging

Deze configuratie kunnen we ook doen via de CLI:

## Automatisch toewijzen van een VLAN aan een gebruiker

```
config switch interface
edit port17
    set security-groups "Group-Radius"
    config port-security
        set auth-fail-vlan enable
        set auth-fail-vlanid 57
        set authserver-timeout-period 3
        set authserver-timeout-vlan disable
        set dacl disable
        set eap-auto-untagged-vlans enable
        set eap-egress-tagged enable
        set eap-passthru enable
        set framevid-apply disable
        set guest-auth-delay 1
        set guest-vlan disable
        set mab-eapol-request 3
        set mac-auth-bypass disable
        set open-auth disable
        set port-security-mode 802.1X
        set quarantine-vlan enable
        set radius-timeout-overwrite disable
        set authserver-timeout-vlanid 300
        set guest-vlanid 56
    end
```

## 7.1.6 Configuratie voor syslogs

Als extra gaan we de syslogs sturen naar een syslog server, in mijn geval is dit de FortiAnalyzer.

We kiezen welke event types we willen sturen en vanaf welke graad we deze event sturen naar de FortiAnalyzer. We kiezen voor alle categorieën en we sturen vanaf informatie niveau naar de server. We geven het IP van de server waar we naar willen sturen mee. De poort van syslog is 514.

## Automatisch toewijzen van een VLAN aan een gebruiker

### Log Configuration

#### Event Type

 Enable

#### Categories

- Link
- POE
- Router
- Spanning Tree
- Switch
- Switch Controller
- System
- User

### Syslog

 Enable

#### Severity

(6) Information

#### Server

IP van syslog

#### Port

514 (0-65535)

Apply

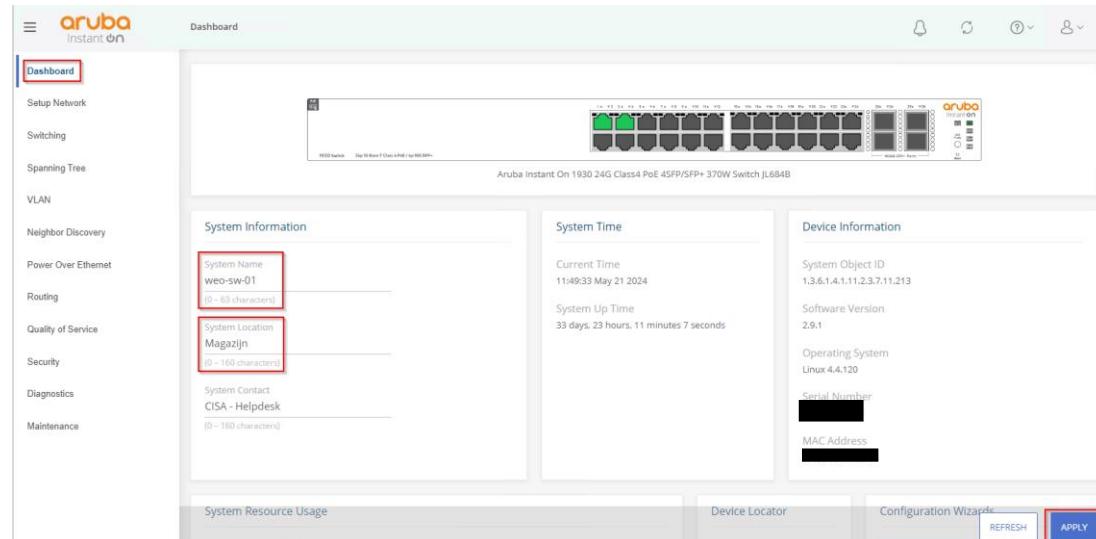
Figuur 268: FortiSwitch configuratie syslog

Uiteraard kunt u de volledige configuratie van de switch terugvinden in het zip-bestand van dit project.

## 7.2 Aruba Switch

### 7.2.1 hostname

Het is altijd handig om je switch een duidelijke naam te geven en de locatie correct aan te duiden. Zie de foto voor referentie.



Figuur 269: Aruba Switch hostname

### 7.2.2 VLAN's

We gaan ervoor zorgen dat alleen personen vanuit het management VLAN toegang hebben tot de switch. Maar voordat we dat doen, moeten we er natuurlijk voor zorgen dat we onszelf niet buiten sluiten.

## Automatisch toewijzen van een VLAN aan een gebruiker

Laten we eerst de VLANs aanmaken, zodat we ze later kunnen gebruiken. Ga hiervoor naar 'VLAN > VLAN Configuration' en klik vervolgens op het plus symbool om een nieuwe VLAN aan te maken. Zie de foto voor referentie.

VLAN ID	Name	Type
1	management	Default
60	management	Static
64	Sales	Static
65	Marketing	Static
66	HR	Dynamic
67	Guest	Static
68	Onboarding	Static
69	Quarantine	Static

Figuur 270: Aruba Switch hostname

In de wizard geef je natuurlijk zowel dezelfde VLAN ID als dezelfde VLAN naam in.

Figuur 271: Aruba Switch Management VLAN

Uiteraard kun je ook al je andere VLAN's aanmaken.

### 7.2.3 Trunk poort

Hierna zorgen we ervoor dat we de VLAN toelaten op de trunk poort zodat het verkeer van die specifieke VLAN door de trunkpoort kan passeren. Poort 1 van de switch gaat naar de ESXi-server en fungeert als de trunk poort. Bekijk de foto voor referentie.

## Automatisch toewijzen van een VLAN aan een gebruiker

The screenshot shows the 'VLAN Membership - By Interface' table. Interface 1 is selected and assigned to Tagged VLANs 60,64,65,66,67,68,69 and Untagged VLAN 1. Other interfaces (2-10) are listed with their respective VLAN assignments.

Interface	Tagged VLANs	Untagged VLAN
1	60,64,65,66,67,68,69	1
2		64
3		66,69
4		69
5		1
6		1
7		1
8		1
9		1
10		1

Figuur 272: Aruba Switch VLAN configuration op interface (1)

In de wizard geef je al je VLANs op bij 'Tagged VLANs' die via de trunk poort mogen. De 'Untagged VLAN' laat je op 1 staan.

The dialog box shows the configuration for interface 1. It lists 'Tagged VLAN(s)' as 60,64-69 and 'Untagged VLAN' as 1. A note at the bottom specifies the range syntax: 'A list of VLAN IDs in the range of 2 to 4092. Use "-" to specify a range of consecutive IDs and commas to separate ranges or VLAN IDs. For example: 2,4-10,16'. The 'APPLY' button is highlighted.

Figuur 273: Aruba Switch VLAN configuration op interface (2)

Als laatste stap kun je nu het management VLAN ID wijzigen van 1 naar 60. Daarnaast kun je de switch instellen van DHCP naar een statisch IP-adres. Zie de foto voor instructies.

The screenshot shows the 'Setup Network > Get Connected' interface. Under 'IPv4 Setup', 'Management Address Type' is set to 'Static' with IP 172.30.65.2/24 and Subnet Mask 255.255.255.0. Under 'Management VLAN', 'Management VLAN ID' is set to 60. The 'HTTP Management Settings' tab is also visible.

Figuur 274: Aruba Switch IP statisch instellen

## Automatisch toewijzen van een VLAN aan een gebruiker

Vanaf nu is het management dashboard van de switch alleen toegankelijk via VLAN 60 (Management).

### 7.2.4 Poort configuratie

Nu gaan we ervoor zorgen dat we één poort configureren voor het onboarding VLAN, terwijl we de rest configureren voor het quarantaine VLAN. Door deze poorten naar het quarantaine VLAN te zetten, zorgen we ervoor dat ongeautoriseerde gebruikers naar het quarantaine VLAN worden gestuurd. Later zullen we deze poorten wijzigen naar dynamic VLAN assignment.

Interface	Tagged VLANs	Untagged VLAN
1	60,64,65,66,67,68,69	1
2		68
3		69
4		69
5		69

Figuur 275: Aruba Switch poort configuratie (1)

In de wizard laat je het veld 'Tagged VLAN' leeg en verander je het veld 'Untagged VLAN' naar het juiste VLAN.

Figuur 276: Aruba Switch poort configuratie (2)

### 7.2.5 Radius Configuratie

We gaan de authenticatie van onze switch laten verlopen via de RADIUS-server, waardoor we port security kunnen implementeren.

Om dit te doen, stellen we de '**802.1x Authentication Mode**' in voor 802.1x-authenticatie en activeren we deze. Daarnaast schakelen we '**802.1x Accounting Mode**' in om auditing bij te houden. Ook activeren we '**RADIUS Management Authentication**' om aan te melden via gebruikers vanuit het domein.

## Automatisch toewijzen van een VLAN aan een gebruiker

De laatste optie is echter optioneel. Zie de foto (figuur 277) voor referentie.

Figuur 277: Aruba Switch Radius configuratie (1)

Zodra je alle gewenste instellingen hebt geselecteerd, klik je op het plusicoontje om een nieuwe RADIUS-server toe te voegen.

Figuur 278: Aruba Switch Radius configuratie (2)

### 7.2.5 Poort toegangscontrole

## Automatisch toewijzen van een VLAN aan een gebruiker

Nu gaan we ervoor zorgen dat port security wordt afgedwongen op de poorten waar het quarantaine VLAN is ingesteld.

Schakel hier de 'Admin Mode' in om 802.1x mode op de switch te kunnen gebruiken. Zie foto voor referentie.

The screenshot shows the Aruba Instant On web interface under the 'Security > Port Access Control' section. In the 'Global Configuration' panel, the 'Admin Mode' toggle switch is highlighted with a red box. In the 'Port Configuration' panel, the 'Interface' column lists ports 1 through 8, and the 'Control Mode' column for ports 1 and 2 is set to 'Force Authorized'. The 'Operating Control Mode' and 'PAE State' columns also show 'Force Authorized' for these ports. The 'Port Access Control' tab is selected in the navigation bar.

Figuur 279: Aruba Switch poort toegangscontrole (1)

Voor poorten 1 en 2 behouden we de instelling '**Force Authorized**', wat betekent dat de pc's op deze poorten automatisch worden toegewezen aan het juiste VLAN zonder port authenticatie. Voor de overige poorten zetten we de instelling op '**Auto**', wat betekent dat de pc's als 'unauthorized' worden beschouwd totdat ze succesvol zijn geautoriseerd.

Zie foto voor referentie.

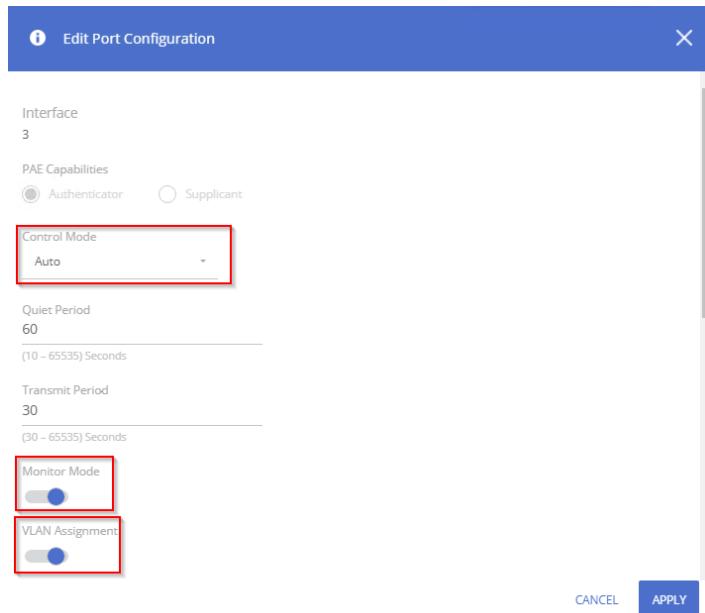
The screenshot shows the Aruba Instant On web interface under the 'Security > Port Access Control' section. In the 'Global Configuration' panel, the 'Guest VLAN Timeout' is set to 'Immediate'. In the 'Port Configuration' panel, the 'Control Mode' for ports 1 and 2 is set to 'Force Authorized', while for ports 3 through 8 it is set to 'Auto'. The 'Operating Control Mode' and 'PAE State' columns also show 'Force Authorized' for ports 1 and 2, and 'Initialize' for ports 3 through 8. The 'Port Access Control' tab is selected in the navigation bar.

Figuur 280: Aruba Switch poort toegangscontrole (2)

Zoals eerder vermeld, zetten we de 'Control Mode' op 'Auto'. Daarnaast schakelen we de 'Monitor Mode' in, zodat we de activiteiten in onze logs kunnen zien. Vergeet ook niet om 'VLAN Assignment' in te stellen, zodat VLANs correct kunnen worden toegewezen.

Zie foto voor referentie.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 281: Aruba Switch poort toegangscontrole (3)

### 7.2.3 Configuratie Syslog

Als laatste kunnen we er natuurlijk ook voor zorgen dat onze logs worden gestuurd naar onze algemene kiwi server.

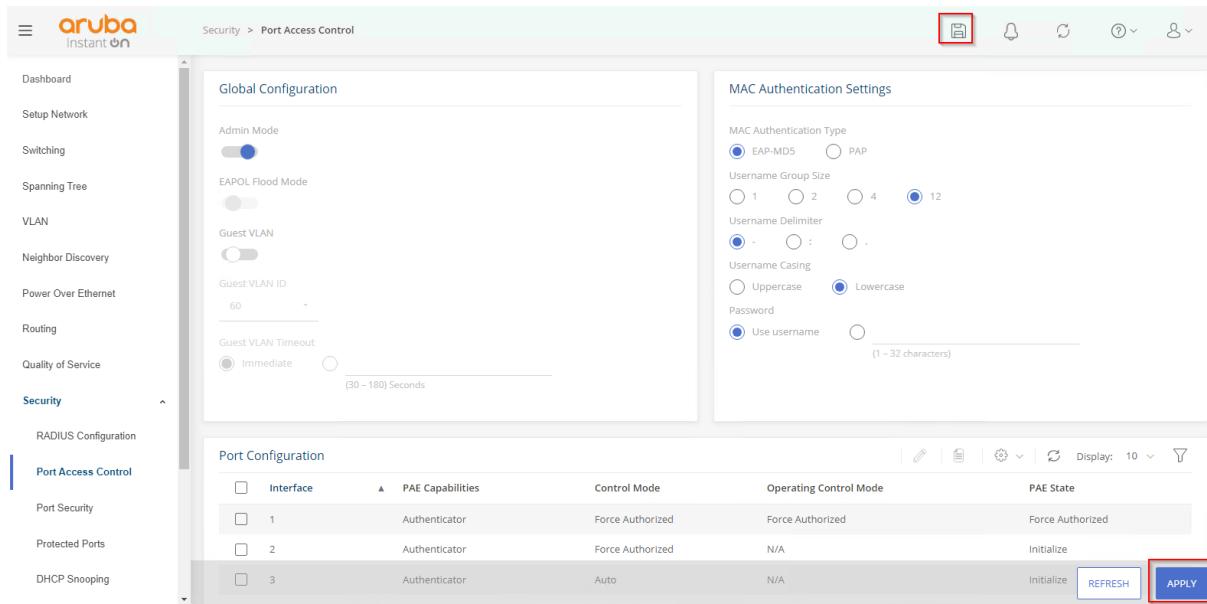
Zie foto voor referentie (figuur 282).

Figuur 282: Aruba Switch syslog configuratie (1)

Vergeet niet om op 'Apply' te klikken. Klik daarna bovenaan ook op 'Save', zodat je configuratie behouden blijft als de switch uitvalt.

Zie foto voor referentie (figuur 283).

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 283: Aruba Switch configuratie saven

Uiteraard kunt u de volledige configuratie van de switch terugvinden in het zip-bestand van dit project.

## Automatisch toewijzen van een VLAN aan een gebruiker

### 8. FortiAnalyzer

Eenmaal als de FortiAnalyzer logs binnenkrijgt, komen er in de root administratief domein niet-geautoriseerde apparaten te staan. Het uitsturen van de logs doen we op de machines met behulp van Solarwinds log forwarder zodat wij controle hebben over welke syslogs er allemaal worden gestuurd.

Wanneer FortiAnalyzer functies zijn ingeschakeld, geeft elke ADOM aan hoe lang en hoeveel schijfruimte te gebruiken voor zijn logs. U kunt het schijfgebruik voor elke ADOM controleren en indien nodig de opslaginstellingen voor logs aanpassen.

#### 8.1 Authorisatie hosts

We zullen deze apparaten eerst moeten autorizeren en plaatsen in ons administratief domein genaamd labostudent.

	Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode	
<input type="checkbox"/>	SYSLOG-AC1E0103	Syslog-Device	SYSLOG-AC1E0103	172.30.1.3	Standard	Logging Only	
<input type="checkbox"/>	SYSLOG-AC1E0104	Syslog-Device	SYSLOG-AC1E0104	172.30.1.4	Standard	Logging Only	
<input type="checkbox"/>	SYSLOG-AC1E0106	Syslog-Device	SYSLOG-AC1E0106	172.30.1.6	Standard	Logging Only	

Figuur 284: FortiAnalyzer niet-geautoriseerde apparaten

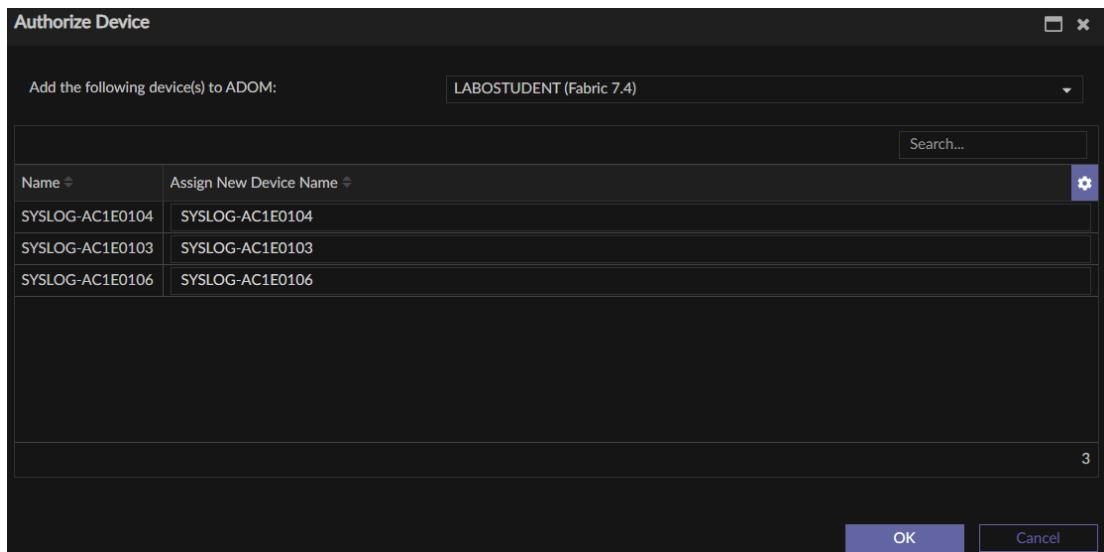
Dit doen we door de apparaten te selecteren en dan te drukken op de knop authorize.

	Device Name	Platform	Serial Number	IP Address	Firmware Version	Management Mode	
<input checked="" type="checkbox"/>	SYSLOG-AC1E0103	Syslog-Device	SYSLOG-AC1E0103	172.30.1.3	Standard	Logging Only	
<input checked="" type="checkbox"/>	SYSLOG-AC1E0104	Syslog-Device	SYSLOG-AC1E0104	172.30.1.4	Standard	Logging Only	
<input checked="" type="checkbox"/>	SYSLOG-AC1E0106	Syslog-Device	SYSLOG-AC1E0106	172.30.1.6	Standard	Logging Only	

Figuur 285: FortiAnalyzer niet-geautoriseerde apparaten autoriseren (I)

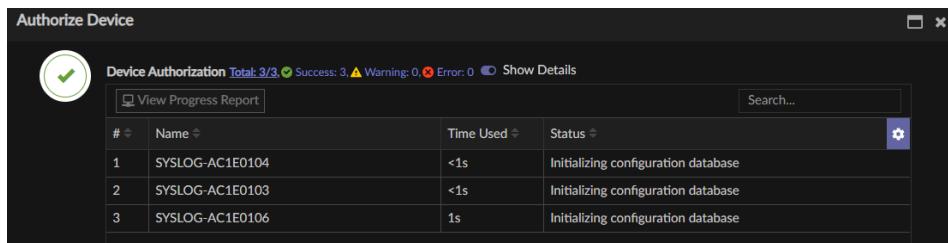
Daarna krijgen we volgend scherm te zien. Hier gaan we de apparaten toevoegen aan een bepaald administratief domein. In ons geval is dit labostudent. Daarna drukken we op OK.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 286: FortiAnalyzer niet-geautoriseerde apparaten autoriseren (2)

Na te drukken op OK zullen de apparaten geautoriseerd zijn zoals we dit links boven zien. In de tabel zien we dat de configuration database wordt aangemaakt.

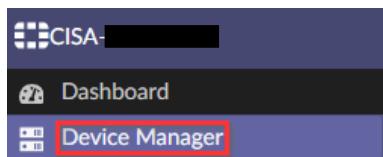


Figuur 287: FortiAnalyzer niet-geautoriseerde apparaten autoriseren (3)

## 8.2 Device Manager

Als we zo al onze apparaten hebben toegevoegd kunnen we ook zien wanneer de laatste log is gestuurd naar de FortiAnalyzer. We kunnen dan ook zien indien er iets mis zou zijn met de log forwarder, zodat we dit ook kunnen oplossen.

In je eigen administratief domein naveer naar device manager.



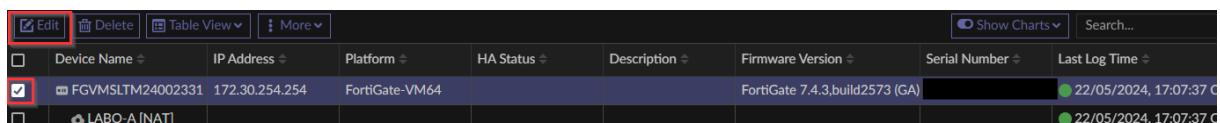
Figuur 288: FortiAnalyzer Device Manager (1)

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 289: FortiAnalyzer Device Manager (2)

In device manager kan je ook de namen aanpassen van de apparaten door te drukken op het apparaat en daarna op edit.



Figuur 290: FortiAnalyzer Device Manager (3)

Als je op edit hebt gedrukt kan je de naam aanpassen, daarna druk je op OK.

The screenshot shows the 'Edit Device' dialog box. The 'Name' field contains 'FortiGate-VM LABO'. The 'OK' button is highlighted with a red box.

Figuur 291: FortiAnalyzer Device Manager (4)

### 8.3 Syslogs

De syslogs kan je daarna bekijken als je navigeert naar log view en daarna syslog. Als je hier dubbel klikt op de één van de lijnen krijg je steeds meer informatie over de syslog. Links boven onder syslog zie je "all devices" in onderstaande afbeelding. Hier kan je filteren op devices, daaronder op het plusje kan je ook nog eens filteren op level, bericht, enzovoort.

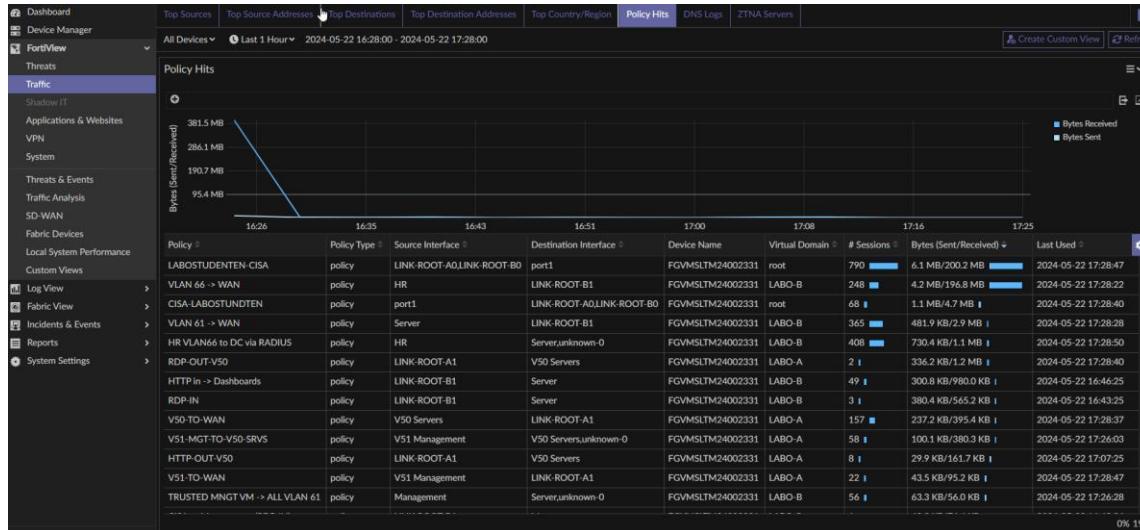
## Automatisch toewijzen van een VLAN aan een gebruiker

CISA FAZVM64			
Syslog			
All Devices	Last 7 Days	May 15 To May 22	
#	Date/Time	Device Name	Level
1	17:13:28	LSY-SRV-FS01	Information
2	17:13:28	LSY-SRV-FS01	Information
3	17:13:11	LSY-SRV-DC01	Notice
4	17:13:11	LSY-SRV-DC01	Notice
5	17:13:11	LSY-SRV-DC01	Notice
6	17:13:11	LSY-SRV-DC01	Notice
7	17:13:11	LSY-SRV-DC01	Notice
8	17:13:11	LSY-SRV-DC01	Notice
9	17:13:05	LSY-SRV-BCK	Information
10	17:12:53	LSY-SW-01	Notice
11	17:12:53	LSY-SRV-DC01	Notice
12	17:12:53	LSY-SRV-DC01	Notice
13	17:12:53	LSY-SRV-DC01	Notice
14	17:12:09	LSY-SRV-DC01	Notice
15	17:11:58	LSY-SRV-DC01	Notice
16	17:11:58	LSY-SRV-DC01	Notice
17	17:11:58	LSY-SRV-DC01	Notice
18	17:11:58	LSY-SRV-DC01	Notice
19	17:11:58	LSY-SRV-DC01	Notice

Figuur 292: FortiAnalysers Syslog

## 8.4 Traffiek

FortiAnalysers gaat nog veel verder dan alleen syslog binnenkrijgen. Je kan hier ook de traffiek met interfaces bekijken. Hier kan je ook onderscheid maken tussen policy hits, top country, top bestemmingen/adressen. Dit kan je bekijken in FortiView > Traffic.

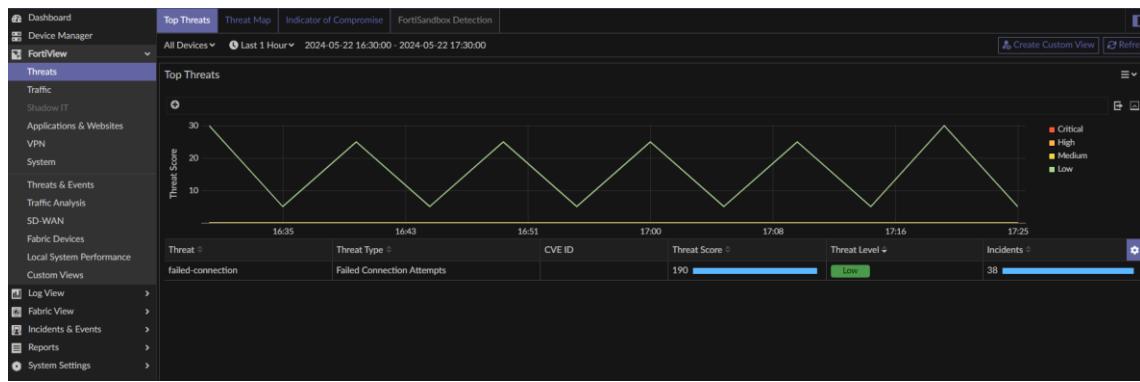


Figuur 293: FortiAnalysers Traffiek

## 8.5 Bedreigingen

Je kan in de fortiview ook naar de bedreigingen kijken die zich voordoen. Hier zal steeds de bedreiging staan, het type, hoe erg het is of het level van bedreiging, hoeveel keer dit incident is voor gevallen en eventueel ook een ID van de Common Vulnerabilities and Exposures (CVE). Dit kan je bekijken bij FortiView > threats.

## Automatisch toewijzen van een VLAN aan een gebruiker



Figuur 294: FortiAnalyser Bedreigingen (I)

## Automatisch toewijzen van een VLAN aan een gebruiker

## 9. Test-scenarios RADIUS 802.1x authentication.

Tabel 1: Test-scenarios Radius

	FortiSwitch	Aruba switch
Device is rogue (niet gekend)	Wordt geplaatst in het quarantaine netwerk (VLAN 57). Deze toestellen kunnen niet met elkaar communiceren noch naar het internet. Krijgen wel een IP-adres en kunnen we dan verder monitoren.	Ontvangt geen IP-adres.
Device is in het domein en logt in met een gebruiker	Dynamische VLAN-toewijzing wordt toegepast op de gebruiker. Afhankelijk van in welke groep hij zich bevindt in de domain controller. De gebruikers behoren tot een bepaalde groep van de afdelingen. Onze afdelingen zijn Production, Sales, Marketing, HR, IT.  Vanaf hier kunnen de afdelingen aan de nodige resources via de firewall policy regels.	
Device is in het domein en NIET valid (vb. ontslagen)	Wordt geplaatst in het quarantaine netwerk (VLAN 57). Deze toestellen kunnen niet met elkaar communiceren noch naar het internet. Krijgen wel een IP-adres en kunnen we dan verder monitoren.	Wordt geplaatst in het quarantaine netwerk (VLAN 69). Deze toestellen kunnen niet met elkaar communiceren noch naar het internet. Krijgen wel een IP-adres en kunnen we dan verder monitoren.
Gast device	Alleen via het WIFI-netwerk.	
Een nieuw apparaat dat klaargemaakt moet worden voor een gebruiker.	Aansluiten op een statische poort waarop static onboarding vlan op staat.	

## 10. Conclusie

Het automatisch toewijzen van VLANs aan gebruikers met behulp van een fortigate firewall, domein controller, radius server, en aruba switch of fortiswitch, biedt voordelen op het gebied van netwerkbeheer en beveiliging. Door deze technologieën te combineren, hebben we een netwerkstructuur gecreëerd die zowel flexibel als robuust is.

De fortigate firewall heeft bewezen een betrouwbare bescherming te bieden tegen ongeautoriseerde toegang en potentiële bedreigingen, terwijl de domein controller en radius server een naadloze gebruikersauthenticatie en -autorisatie mogelijk maken. De dynamische netwerksegmentatie door de aruba switch of fortiswitch zorgt ervoor dat gebruikers automatisch en veilig in de juiste VLANs worden geplaatst, wat de netwerkbeheerprocessen vereenvoudigt en de veiligheid verhoogt.

Het verzamelen van syslogs met kiwi syslog van SolarWinds en de visualisatie hiervan in grafana heeft onze mogelijkheden voor netwerkmonitoring en -beheer aanzienlijk verbeterd. Deze tools hebben ons in staat gesteld om snel trends te identificeren, problemen te diagnosticeren en incidenten proactief aan te pakken.

Daarnaast heeft de integratie van FortiAnalyzer onze mogelijkheden voor loganalyse uitgebreid. FortiAnalyzer biedt diepgaande inzicht in netwerkactiviteiten en bedreigingen, wat ons helpt om een beeld te krijgen van de netwerkbeveiling en om dreigingen te detecteren.

Samenvattend heeft dit project geleid tot een efficiëntere, veiligere en beter beheersbare netwerkomgeving. Door de inzet van geavanceerde technologieën en methoden zijn we in staat om onze netwerkinfrastructuur toekomstbestendig te maken, terwijl we de veiligheid en prestaties blijven optimaliseren. Dit project heeft aangetoond dat een strategische en goed geplande implementatie van netwerkbeheeroplossingen substantiële voordelen kan opleveren voor elke organisatie.

## **II. Bronnen**

*Virtual Domains | Administration Guide.* (n.d.).

<https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/109991/virtual-domains>

*Download and install Zabbix 6.4 for Ubuntu 22.04 (Jammy) Server, Frontend, Agent, MySQL, Apache.* (n.d.).

[https://www.zabbix.com/download?zabbix=6.4&os\\_distribution=ubuntu&os\\_version=22.04&components=server\\_frontend\\_agent&db=mysql&ws=apache](https://www.zabbix.com/download?zabbix=6.4&os_distribution=ubuntu&os_version=22.04&components=server_frontend_agent&db=mysql&ws=apache)

Airheads Broadcasting. (2019, February 13). Zero to EAP-TLS - Aruba Lab Build - “Grande Quad Shot” Edition [Video]. YouTube. <https://www.youtube.com/watch?v=klba-HxQJlk>

Grafana & Prometheus & Node-Exporter

<https://www.linode.com/docs/guides/how-to-install-prometheus-and-grafana-on-ubuntu/>

Fridberg, R. (2023, April 21). Segmenting Your Network with Dynamic VLAN. Portnox.

<https://www.portnox.com/blog/network-security/network-segmentation-dynamic-vlan-assignment/>

*Promiscuous mode operation.* (n.d.). <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-92F3AB1F-B4C5-4F25-A010-8820D7250350.html>

*MAC address changes.* (n.d.). <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-942BD3AA-731B-4A05-8196-66F2B4BF1ACB.html>

*Forged transmits.* (n.d.). <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-7DC6486F-5400-44DF-8A62-6273798A2F80.html>

Jonna. (2024, January 2). [Ultimate Guide] How to run Sysprep in Windows Server 2022. <https://www.ubackup.com/windows-server/sysprep-server-2022-6007-rc.html>

*Dynamic VLAN assignment | FortiSwitchOS Administration Guide.* (n.d.).

<https://docs.fortinet.com/document/fortiswitch/7.4.3/fortiswitchos-administration-guide/110505/dynamic-vlan-assignment>

root tech. (2023, August 13). How to map network drives using Group Policy Windows Server 2022 [Video]. YouTube. <https://www.youtube.com/watch?v=7iNY2GJcmEE>

David Dalton. (2021, November 4). Introduction to, and installation of, NPS [Video]. YouTube.

<https://www.youtube.com/watch?v=CpaN61SGyWU>

## Automatisch toewijzen van een VLAN aan een gebruiker

Patel, S. (2023, August 11). How to setup Loki in Ubuntu 20.04 - Sujit Patel - Medium. Medium. <https://psujit775.medium.com/how-to-setup-loki-in-ubuntu-20-04-f7aab49910fc>

Grafana. (n.d.). Docs: *installing Promtail on Windows isn't well documented* · Issue #9392 · grafana/loki. GitHub. <https://github.com/grafana/loki/issues/9392>

En de collega's bij CISA.