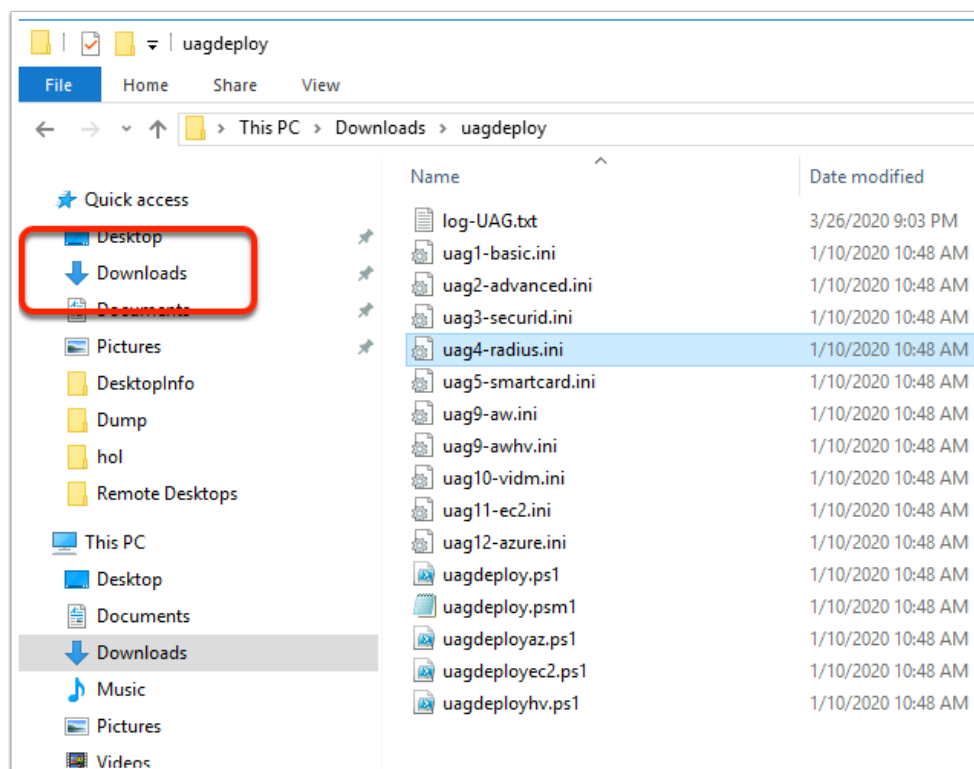


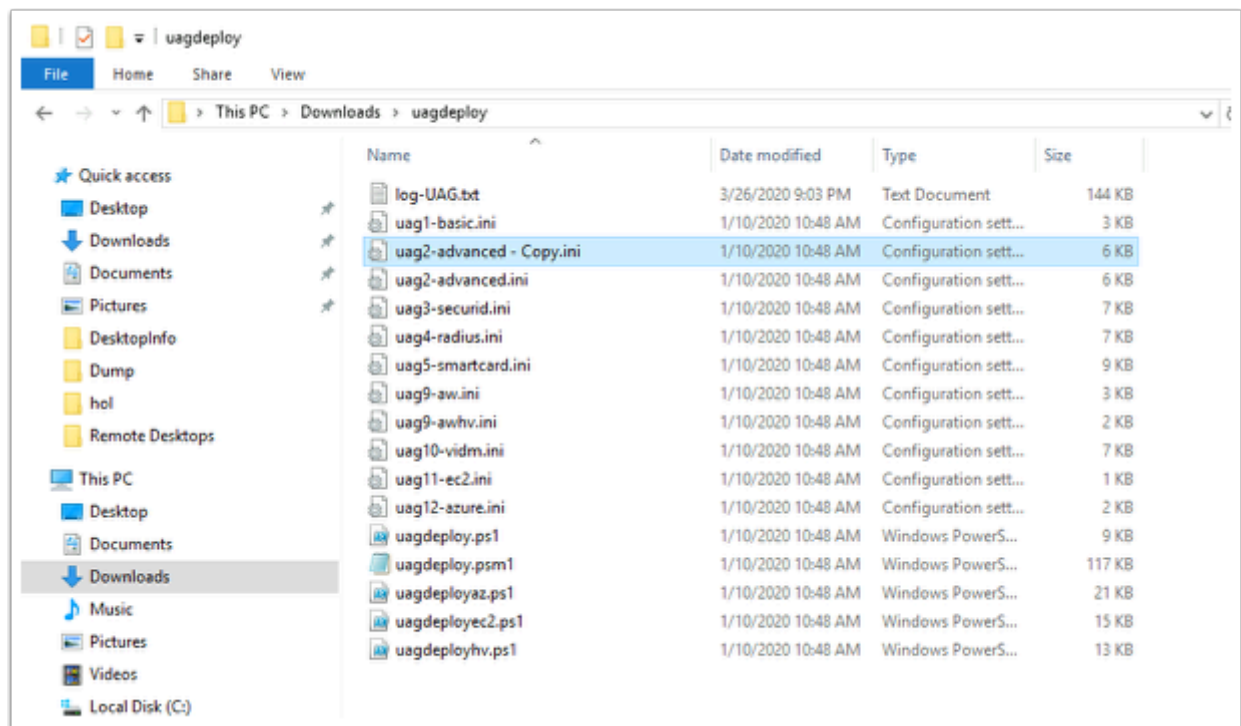
# Chapter 6: Unified Access Gateway deployment using the PowerShell

## PART 1

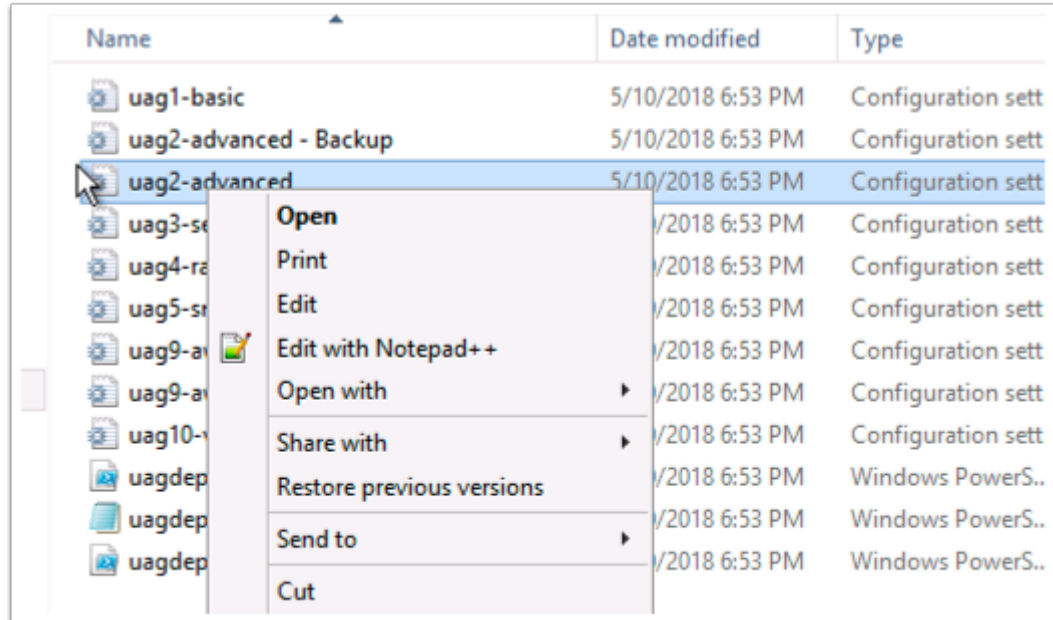
This is an overview of deploying the Unified Access Gateway script for VMware Horizon



1. On your **ControlCenter** server,
  - Go to the **Downloads** folder
  - Select and open the **uagdeploy** folder and observe the contents



2. Select the **uag2-Advanced.ini**,
  - **Copy and Paste** so that you have a backup of the original file .



3. Select **uag2-advanced** and then select **Edit with Notepad++**

```
#
name=UAG-HZN

#
# Full path filename of the UAG .ova virtual machine image
# The file can be obtained from VMware
#
source= \\horizon.euc-livefire.com\software\UAG\euc-unified-access-gateway-21.06.2.0-18528989_OVF10.ova

#
# target refers to the vCenter username and address/hostname and the ESXi host for deployment
# Refer to the ovftool documentation for information about the target syntax.
# See https://www.vmware.com/support/developer/ovf/
# PASSWORD in upper case results in a password prompt during deployment so that passwords do not need
# to specified in this .INI file.
# In this example, the vCenter username is administrator@vsphere.local
#           the vCenter server is 192.168.0.21 (this can be a hostname or IP address)
#           the ESXi hostname is esx1.myc0.int (this can be a hostname or IP address)
#
target=vi://administrator@vsphere.local:PASSWORD@192.168.110.25/RegionA01/host/RegionA01-COMP01/192.168.110.52

#
# vSphere datastore name
#
ds=CorpLUN
```

#### 4. In the **NotePad++** application

- Next to **name** change to **UAG-HZN**
- Next to **source** change

```
source=\\horizon.euc-livefire.com\software\UAG\euc-unified-access-gateway-21.06.2.0-18528989_OVF10.ova
```

- Next to **target** change it to:

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.110.25/RegionA01/host/RegionA01-COMP01/192.168.110.52
```

```
32 #
33
34 ds=CorpLUN
35
36 #
37 # Disk provisioning mode. Refer to OVF Tool doc
38 #
39
40 diskMode=thin
41
42 #
43 # vSphere Network names. For pre 3.3 UAG version
44 # network settings such as IPv4 subnet mask, ga
45 # value must be specified for each NIC. Normal
46 #
47
48 netInternet=VL-DMZ
49 netManagementNetwork=VL-DMZ
50 netBackendNetwork=VL-DMZ
51
52 defaultGateway=172.16.20.1
53
54 deploymentOption=onenic
55 ip0=172.16.20.11
56 netmask0=255.255.255.0
57 routes0=172.16.20.1/24 172.16.20.1
58
59 #deploymentOption=onenic
```

5. **Scroll down** in your NotePad++ window

- Next to **ds=Local Disk 1** change to **ds=CorpLUN**
- Next to **#diskMode=thin** change to **diskMode=thin**
- Change the following network settings to:
  - **netInternet=VL-DMZ**
  - **netManagementNetwork=VL-DMZ**
  - **netBackendNetwork=VL-DMZ**
  - **defaultGateway=172.16.20.1**
  - **deploymentOption=onenic**
  - **ip0=172.16.20.11**
  - **netmask0=255.255.255.0**
  - **routes0=172.16.20.0/24 172.16.20.1**

```
70 #ip1=192.168.0.91
71 #netmask1=255.255.255.0
72 #ip2=192.168.0.92
73 #netmask2=255.255.255.0
74 #routes0=192.168.1.0/24 192
75 #routes1=192.168.3.0/24 192
76 #routes2=192.168.5.0/24 192
77
78 dns=192.168.110.10
79
80 #syslogUrl=syslog://server.
81
82 #
83 # Setting honorCipherOrder 1
84 # UAG 2.7.2 and newer to fo
85 #
```

## 6. Scroll Down

- Change **dns=192.168.0.10** to

```
dns=192.168.110.10
```

```

97
98  [SSLCert]
99
100  #
101  # From UAG 3.0 and newer, you can specify
102  # any required intermediate certificates
103  # associated PEM certificates file and P
104  #
105
106  pfxCerts=C:\certificates\WildCard.pfx
107
108  #
109  # If there are multiple SSL certificates
110  # This is not necessary if there is only

```

7. Under **[SSLCert]** Change **pfxCerts=sslcerts.pfx** to

```
pfxCerts=C:\certificates\WildCard.pfx
```

```

133  #
134
135  [SSLCertAdmin]
136
137  pfxCerts=C:\certificates\WildCard.pfx
138  #pemCerts=sslcerts.pem
139  #pemPrivKey=sslcertsakey.pem
140
141  [Horizon]
142

```

8. In the **[SSLCertAdmin]** section , change **pfxCerts=sslcerts.pfx** to

```
pfxCerts=C:\certificates\WildCard.pfx
```

```
#
# proxyDestinationUrl refers to the backend Connection Server t
# It can either specify the name or IP address of an individual
# via a load balancer in front of multiple Connection Servers.
#

proxyDestinationUrl=https://horizon.euc-liveware.com

#
# proxyDestinationUrlThumbprints only needs to be specified if
# a trusted CA signed SSL server certificate installed (e.g. if
# This is a comma separated list of thumbprints in the format s
#
```

9. Under the **[Horizon]** section change **proxyDestinationUrl=https://192.168.0.209** to

```
proxyDestinationUrl=https://horizon.euc-liveware.com
```

```
160 # The following external URLs are used by Horizon Clients
161 # to this UAG appliance. If they reference a load balancer
162 # configured for source IP hash affinity otherwise the con
163 #
164
165 tunnelExternalUrl=https://uag-hzn.euc-liveware.com:443
166 blastExternalUrl=https://uag-hzn.euc-liveware.com:443
167
168 #
169 # pcoipExternalUrl must contain an IPv4 address (not a DNS
170 #
```

10. **Scroll down** and Change

- **tunnelExternalUrl=https://uag2.horizon.myco.com:443**
- **blastExternalUrl=https://uag2.horizon.myco.com:443**

To

```
tunnelExternalUrl=https://uag-hzn.euc-liveware.com:443
blastExternalUrl=https://uag-hzn.euc-liveware.com:443
```

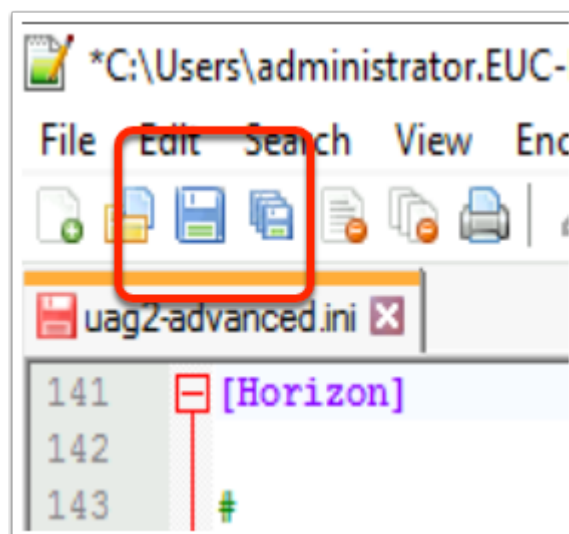


```
168 #
169 # pcoipExternalUrl must contain an IPv4 address
170 #
171
172 pcoipExternalUrl=172.16.20.11:4172
173 pcoipDisableLegacyCertificate=true
174
175
176
```

11. **Scroll down** and Change

- In the **pcoipExternalUrl** section change **pcoipExternalUrl=10.20.30.90:4172** to:

```
pcoipExternalUrl=172.16.20.11:4172
```

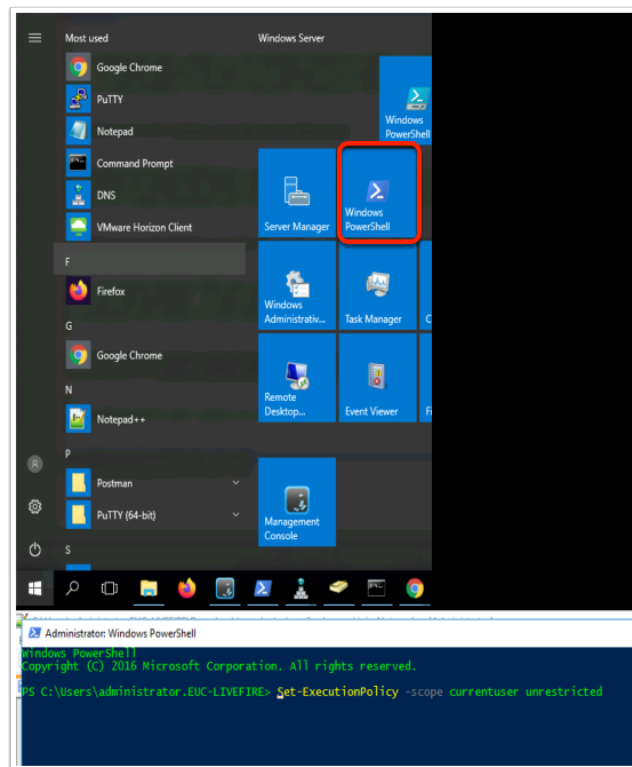


12. **SAVE** THE .ini File

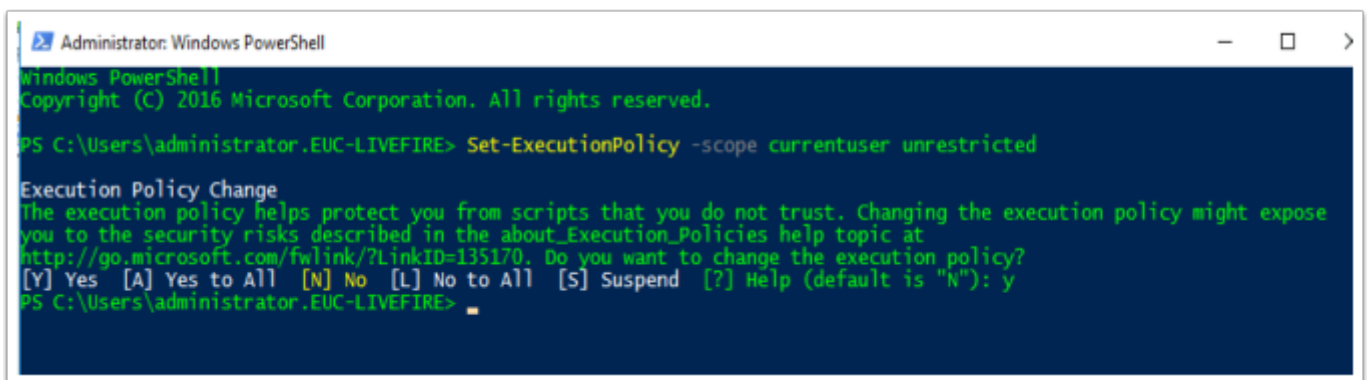
## Part 2

In this section, we will deploy the Unified Access Gateway using a Powershell Script





1. On your **ControlCenter** server ,
  - Launch the **powershell** shortcut from the **Start Menu**



2. We will set the script execution is set to unrestricted. Execute the following command.

```
Set-ExecutionPolicy -scope currentuser unrestricted
```

When Prompted select **Y**

```
PS C:\Users\administrator.EUC-LIVEFIRE> cd downloads\uagdeploy
PS C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy> █
```

3. Within the powershell interface type the following command

```
cd downloads\uagdeploy
```

```
PS C:\Users\administrator.EUC-LIVEFIRE> cd downloads\uagdeploy
PS C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy> .\uagdeploy.ps1 -iniFile uag2-advanced.ini

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy\uagdeploy.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy\uagdeploy.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r
Unified Access Gateway (UAG) virtual appliance deployment script
Enter a root password for UAG-HZN: *****
Re-enter the root password: ***** █
```

4. Execute the following command

```
.\uagdeploy.ps1 -iniFile uag2-advanced.ini
```

- When you get a security warning type: **R**
- When you get a second security warning type: **R**
- When prompted to **enter a root password for UAG-HZN**,
  - type:- **VMware1!**
  - when prompted to confirm type **VMware1!**

```

Enter an optional admin password for the Admin UI and REST API management access for UAG-HZN: *****
Re-enter the admin password: *****
Join the VMware Customer Experience Improvement Program?

This setting is supported in UAG versions 3.1 and newer.

VMware's Customer Experience Improvement Program (CEIP) provides VMware with information that enables VMware to
improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.

As part of the CEIP, VMware collects technical information about your organization's use of VMware products and
services on a regular basis in association with your organization's VMware license key(s). This information does
not personally identify any individual.

Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware
is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

If you prefer not to participate in VMware's CEIP for UAG 3.1 and newer, you should enter no.

You may join or leave VMware's CEIP for this product at any time. In the UAG Admin UI in System Configuration,
there is a setting 'Join CEIP' which can be set to yes or no and has immediate effect.

To Join the VMware Customer Experience Improvement Program with Unified Access Gateway version 3.1 and newer,
either enter yes or just hit return as the default for this setting is yes.
Join CEIP for UAG-HZN ? (default is yes for UAG 3.1 and newer): No
Enter the password for the specified [SSLCert] PFX certificate file WildCard.pfx:

```

5. When prompted to

- Enter an optional admin password for the REST API management access for UAG: type **VMware1!**
- When prompted to **Re-Enter an optional admin password** : type **VMware1!**
- When prompted whether or not to join the customer experience program type **No**

```

Join CEIP for UAG-HZN ? (default is yes for UAG 3.1 and newer): No
Enter the password for the specified [SSLCert] PFX certificate file WildCard.pfx: *****
Enter the password for the specified [SSLCertAdmin] PFX certificate file WildCard.pfx: *****
Opening OVA source: \\cs1-pd1.euc-livfire.com\software\UAG\euc-unified-access-gateway-3.10.0.0-16455273_OVF10.ova
The manifest validates
Source is signed and the certificate validates
Enter login information for target vi://192.168.110.22/
Username: administrator%40euc-livfire.com
Password:
Enter login information for target vi://192.168.110.22/
Username: administrator%40euc-livfire.com
Password: *****
Enter login information for target vi://192.168.110.22/
Username: administrator%40euc-livfire.com
Password: *****
Opening VI target: vi://administrator%40euc-livfire.com@192.168.110.22:443/Livfire/host/RegionA02-COMP02/
euc-livfire.com
Deploying to VI: vi://administrator%40euc-livfire.com@192.168.110.22:443/Livfire/host/RegionA02-COMP02/
euc-livfire.com
Disk progress: 17%

```

6. When prompted to

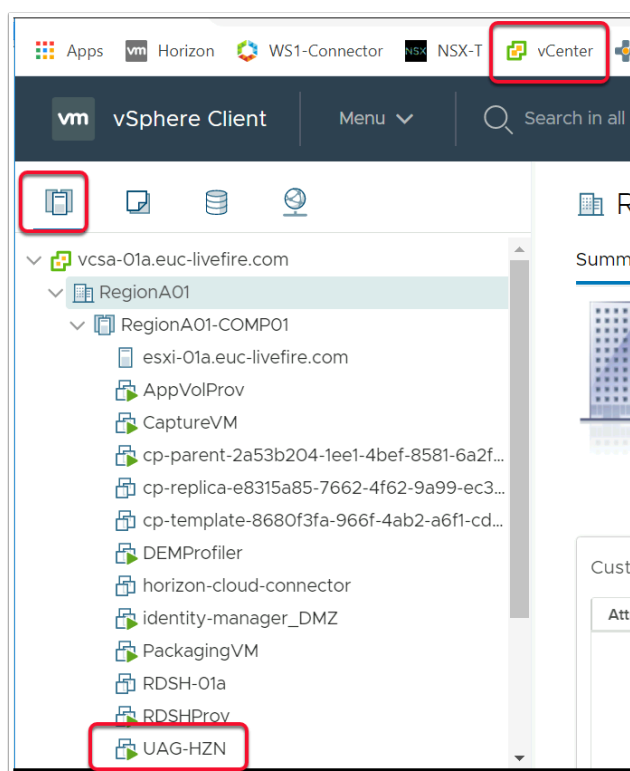
- Enter password for the **.pfx** type: **VMware1!**,
- When prompted to **confirm** type **VMware1!** again.
- When prompted the password for **administrator@vsphere.local**
  - Type **VMware1!**
- When prompted for **fingerprint will be added to the known host file** type **yes**
- **Your virtual Appliance deployment will now start , it will take between 5 - 10min to deploy. Proceed to step 8**

```

Deploying to VI: vi://administrator@euc-livefire.com@192.168.110.22:443/RegionA01/host/RegionA01-COMP01/esxi-01a.euc-
livefire.com
Transfer Completed
Powering on VM: UAG-HZN
Task Completed
Received IP address: 172.16.20.11
Completed successfully
Note that the IP addresses will be set to the specified IP addresses for each NIC
UAG virtual appliance UAG-HZN deployed successfully
MPS C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy>

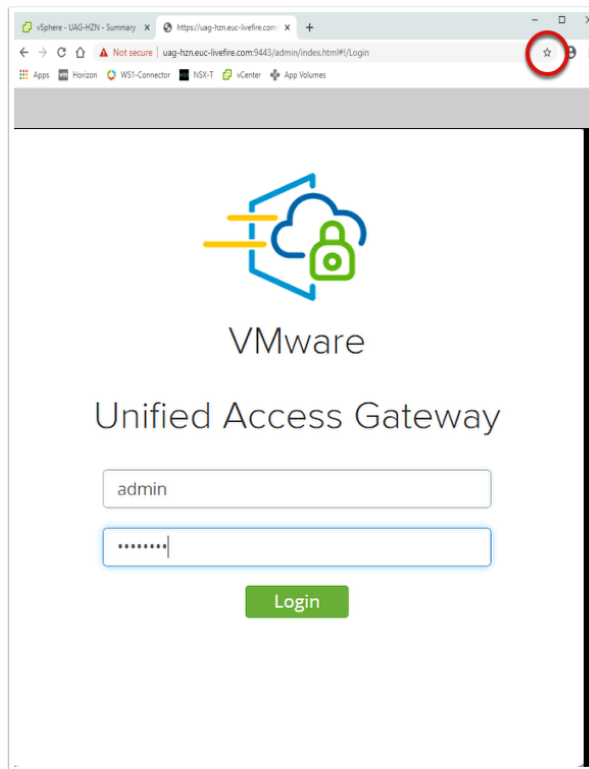
```

## 7. Review the deployment once the setup has completed



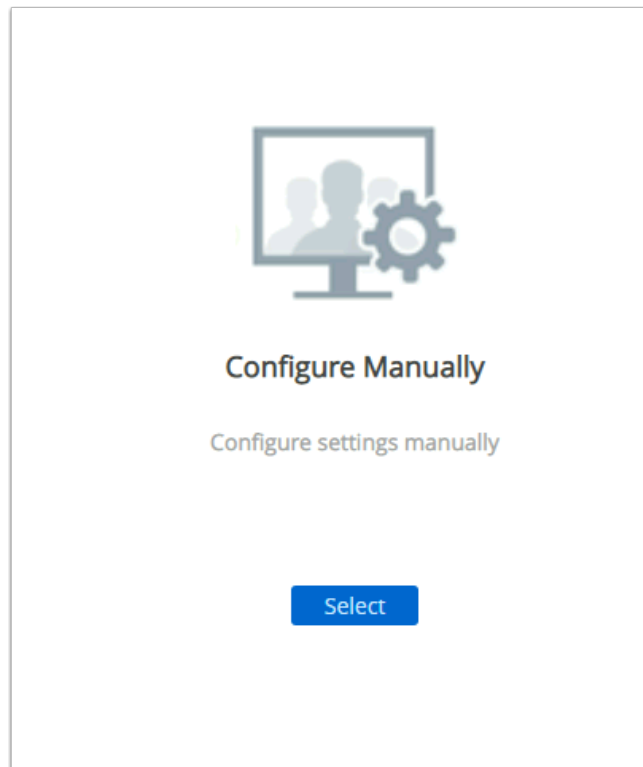
## 8. On your ControlCenter server

- Open your **Chrome Browser**. Select the **vCenter** shortcut
  - Login as **administrator** with the password **VMware1!**
  - Select the **Host & Clusters** Icon
  - In **Host & Clusters**, expand the **inventory** under **RegionA01-COMP01**
- Switch Back to your Powershell window to check if the deployment has completed.

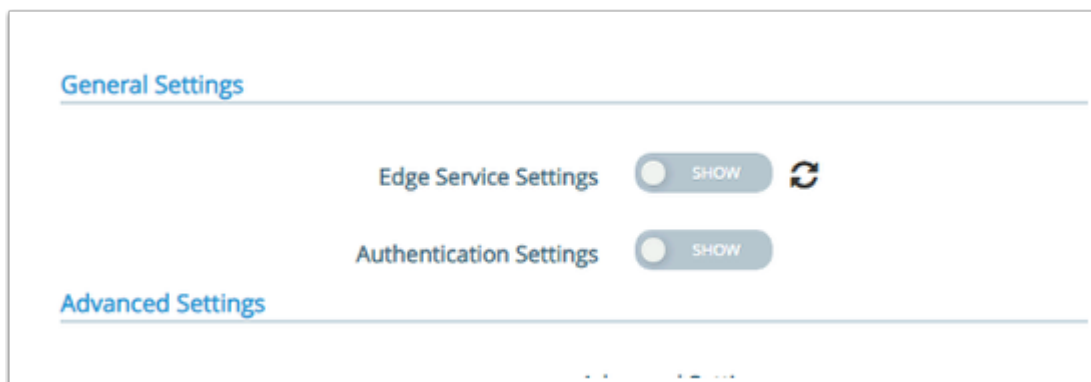


9. On your **ControlCenter** server

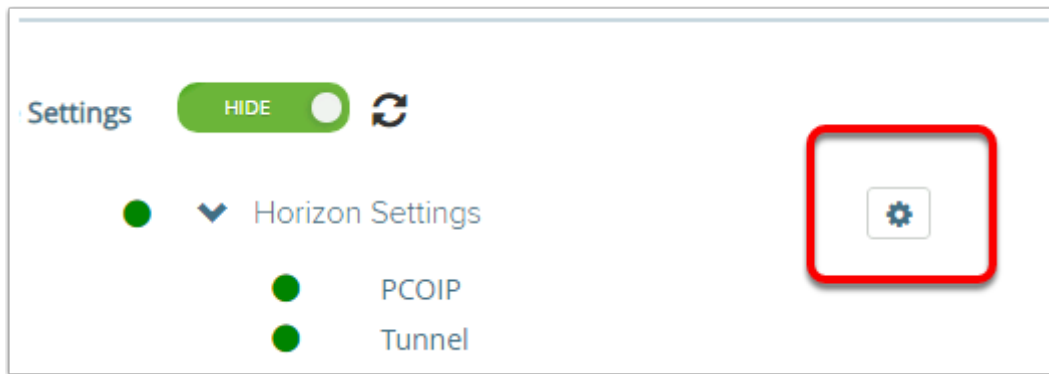
- On your **Chrome Browser** open a **new Tab**
- Enter the following URL into the address bar
  - <https://uag-hzn.euc-livewire.com:9443/admin/index.html#!/Login>
- In the right of your Chrome Browser . Add the following URL as Favourite in your Bookmarks, by selecting the **STAR**.
- Login to your UAG server by entering the following
  - **Admin Username :** [admin](#)
  - **Admin Password:** [VMware1!](#)
  - Select **Login**



10. On your UAG Admin Console
- Click the **Select** button under **Configure Manually**

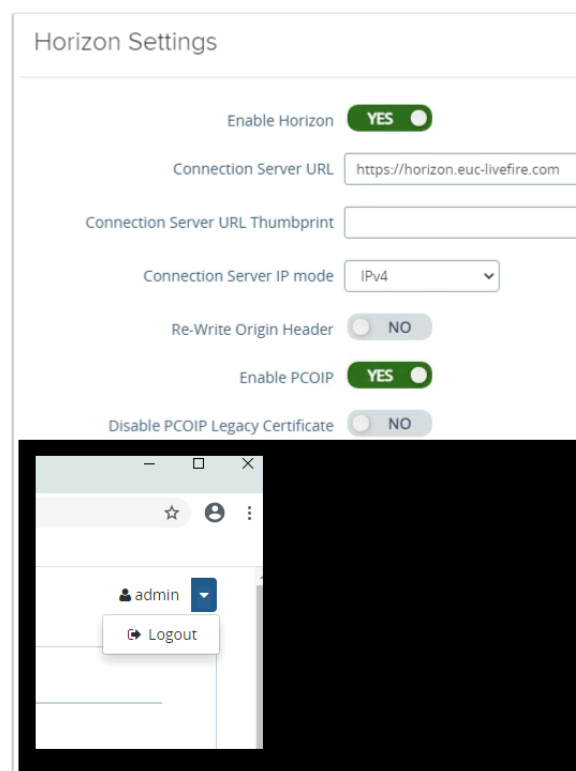


11. On your UAG Admin Console
- Under **General Settings**
    - Next to **Edge Service Settings**, move the **toggle** to the right



## 12. On your UAG Admin Console

- To the right of **Horizon Settings**, select the **Gearbox**



## 13. In your UAG Admin Console

- Under **Horizon Settings**
  - Browse and familiarize yourself with config, we will be changing some of the settings in a future exercise
  - **Logout** from the UAG Admin Console

This concludes the deployment of the Unified Access Gateway using a Powershell Script

## About the Author

About the Author Reinhart Nel

<https://www.livewire.solutions/meet-the-team/reinhartnel/>



For any questions please email Reinhart at **RACE-Livefire-EUC@vmware.com**