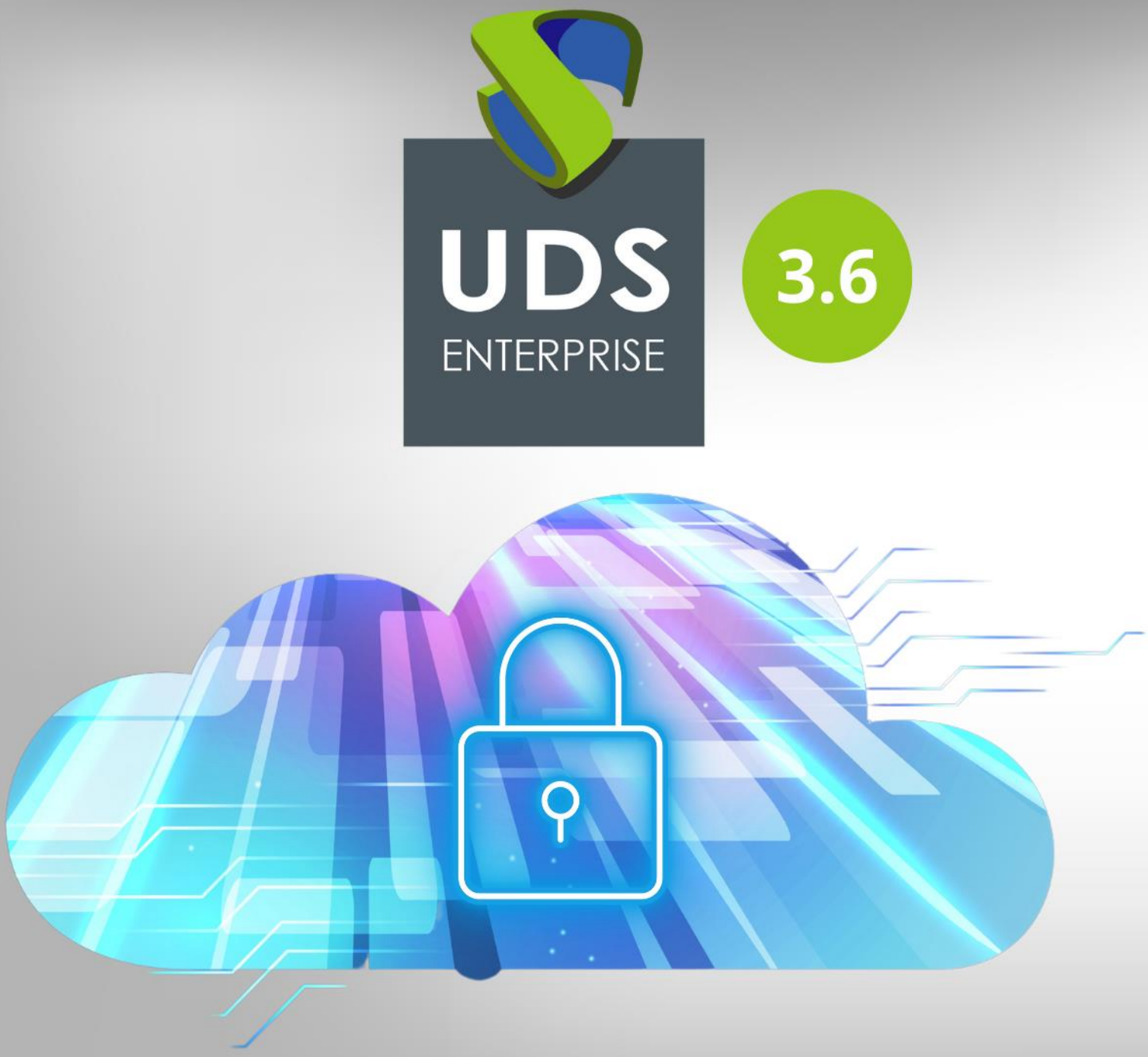
VIRTUAL CABLE

VDI with UDS Enterprise 3.6 and Microsoft Azure



Index

Introduction

Azure is a proprietary Microsoft platform that provides cloud services. Some of its advanced features include the ability to run virtual machines, virtual applications, databases, backups, and many other tasks. It integrates countless cloud services that are necessary to develop, test, implement and manage virtual machines (VMs).

This guide "**VDI with UDS Enterprise and Microsoft Azure"** will help you understand the procedure to deploy and configure the UDS Enterprise components on the platform. This document shows, through real examples, how to create resource groups, storage accounts, containers and any necessary resources so that UDS Enterprise can deploy virtual desktops on this platform.

Also, one of the procedures to create virtual machines (which will be used as base machine or template), the steps to migrate machines from an existing environment (VMware, Hyper-V, etc...) to Microsoft Azure and the simplest way of converting a MV disk to .vhd format (disk format recognized in Azure) are detailed.

UDS Enterprise on Microsoft Azure

Before carrying out the integration, it is worth investing time in knowing the different configurable parts of UDS Enterprise (for more information visit our website. In the Documentation section you will find the Installation, administration and user manual of UDS Enterprise). Two of them are **Service Providers** and **Authenticators**, elements of utmost importance for the configuration of Azure in UDS Enterprise.

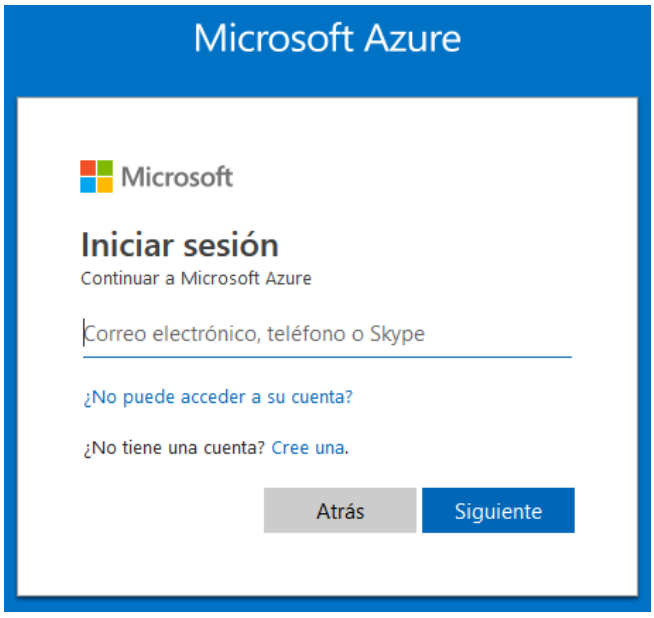
UDS Enterprise will allow to deploy self-generated virtual desktops and virtual application sessions on the Microsoft Azure platform.

To install and configure UDS Enterprise, you must request VirtualCable its components (UDS-Server, UDS-Tunnel and MySQL Database –optional-) and a serial number (Free/ Evaluation/ Enterprise).

You must have a valid Microsoft Azure subscription on which to deploy UDS Enterprise components, virtual desktops, or Windows/Linux application servers.

Where to begin

First, you must have an account with administrator privileges on the Azure platform. If you already have it, Login to the portal.



Once you have logged in and before uploading the UDS Enterprise components, you will need a series of elements available on the Azure platform ("***Resource Groups***", "***Storage Accounts***", "***Container***", "***Network Security Groups***").

Below are examples of how you should create and configure these elements for the proper functioning of UDS Enterprise on an Azure platform.

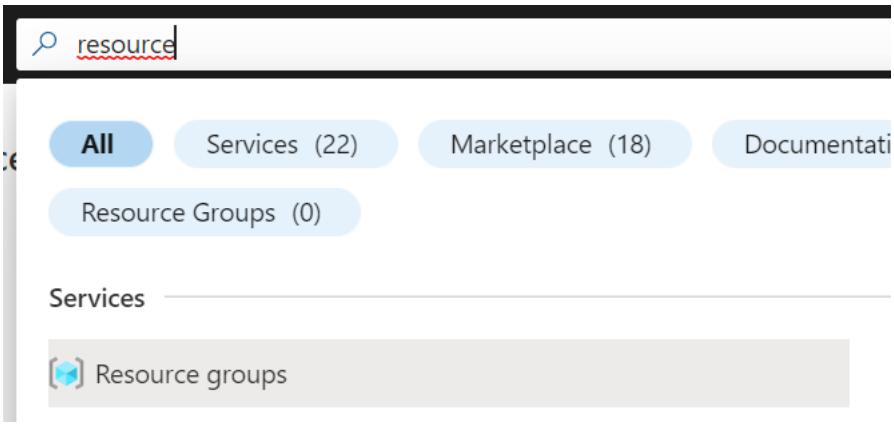
1. Necessary elements

- Resource Groups

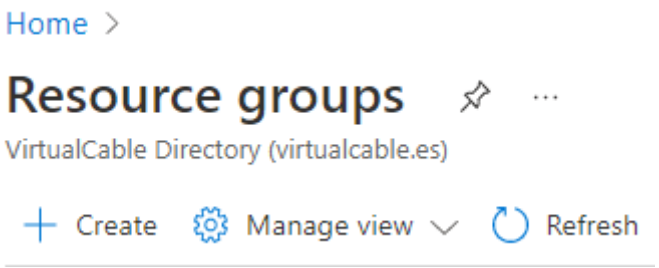
A "***Resource Group***" in Azure groups a collection of assets into logical groups for provisioning, monitoring and access control easily or even automatically, for more effective management.

You will need to have at least one "***Resource Group***" on which to deploy and configure all the requirements and components of UDS Enterprise. If you don't have one, you can create it by following these steps:

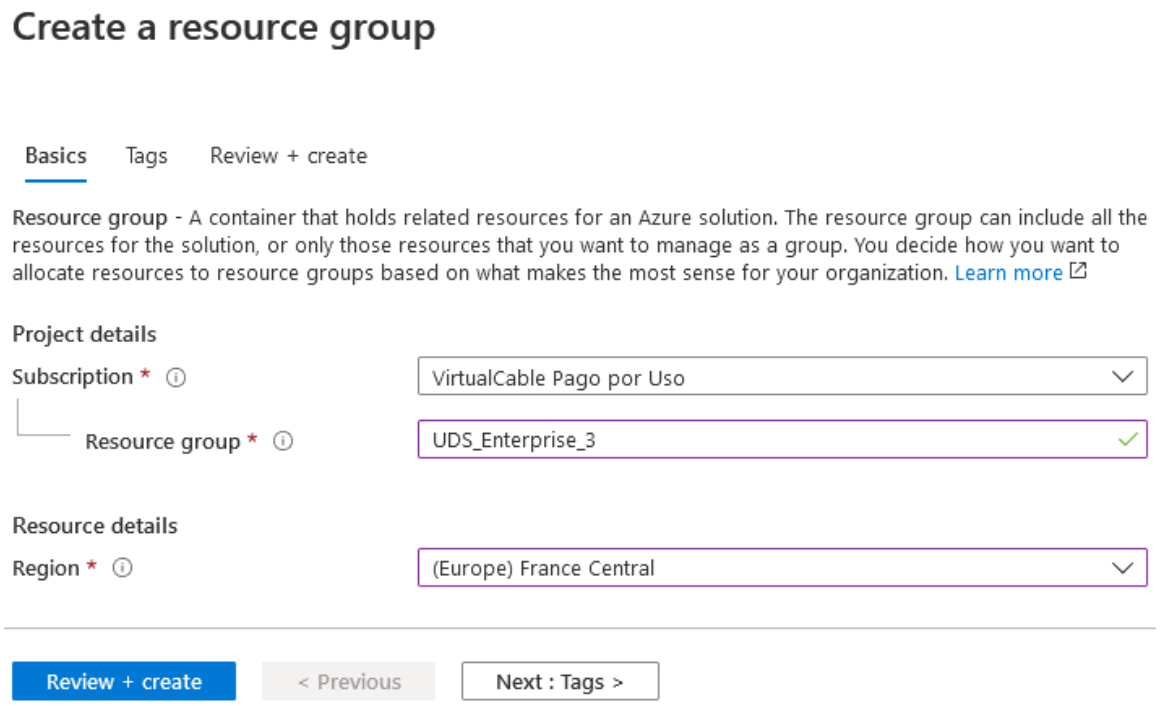
1. In the "***Services***" list, search for "***Resources groups***" and click on it:



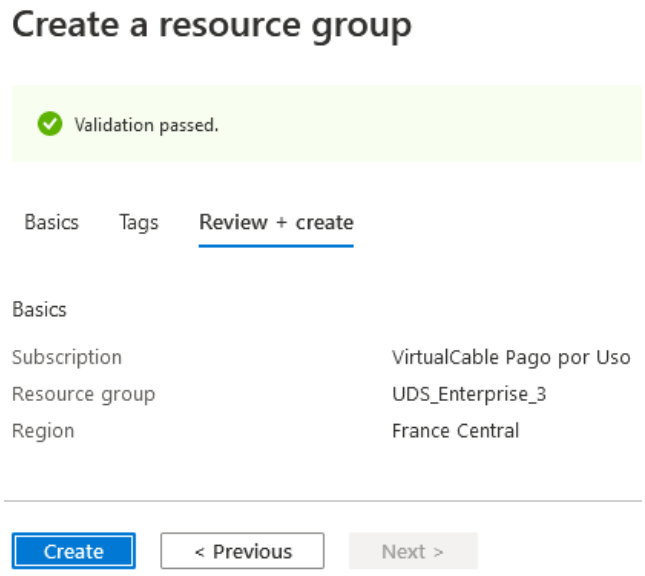
2. Once inside, click on "***add***" to create a new one.



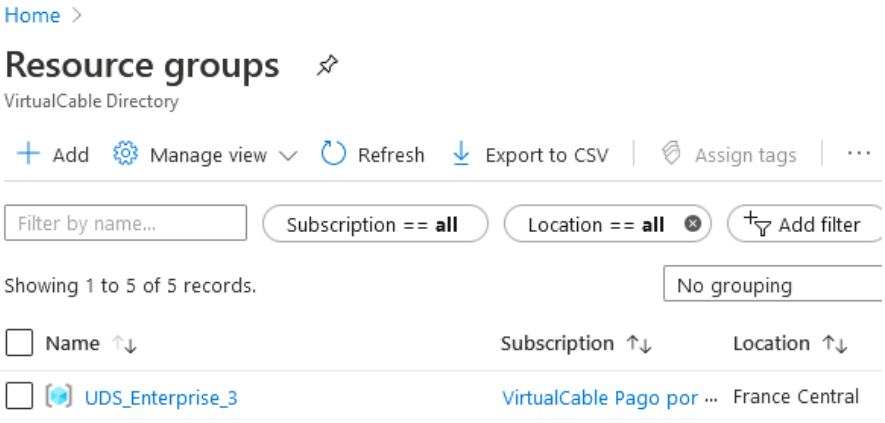
3. In the "***Basics***" section, select the subscription on which it will be registered, indicate a descriptive name for the element, and choose a "***Resource group location***". Click on "***Review + Create***".



4. Review all the data and if they are correct, click on "***Create***":



5. Confirm that the "***Resource Group***" has been created correctly.

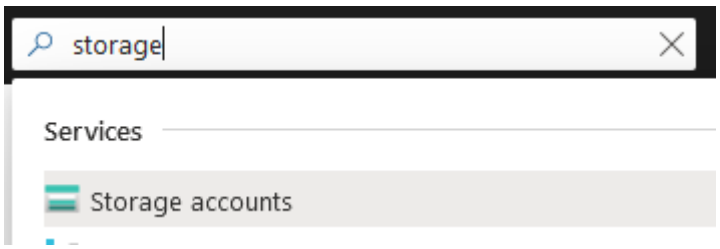


- Storage Accounts

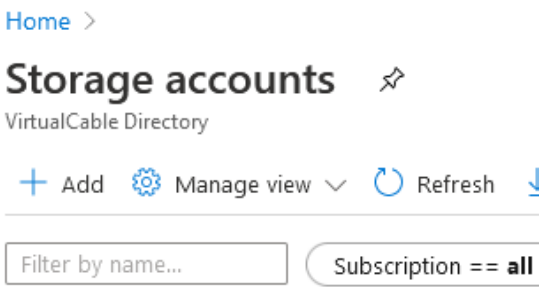
The next item you will need will be a "***Storage account***". This element will allow you to import the UDS components and generate the virtual disks to later deploy the UDS virtual servers.

If you don't have one, you can create it by following these steps:

1. In the "***Services***" list, search for "***Storage accounts***" and click on it:

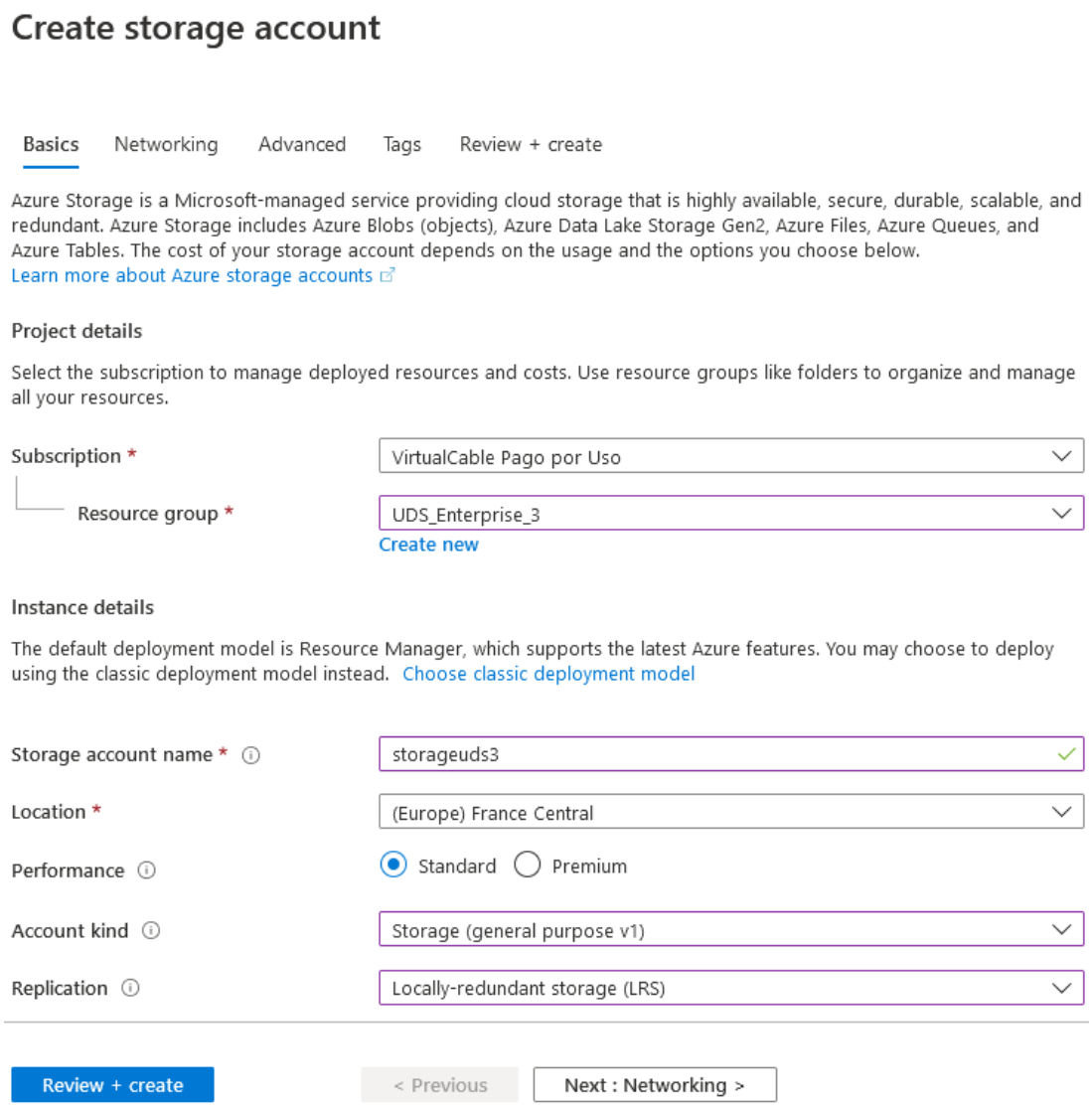


2. Once inside, click on "***Create***" to create a new one.

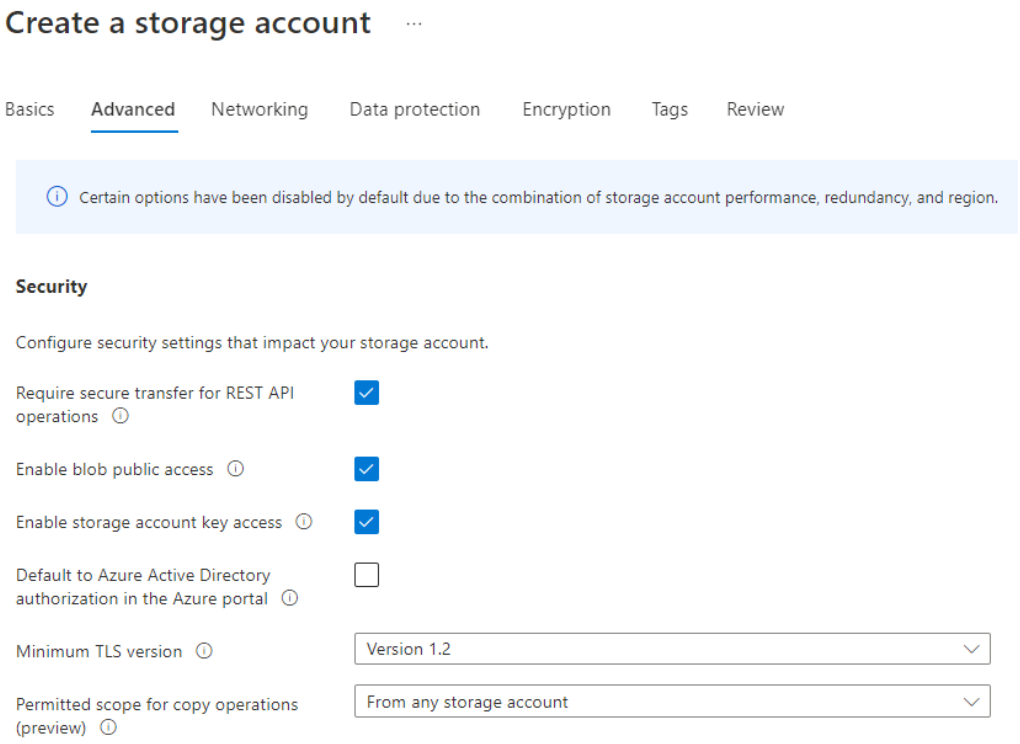


3. In the "***Basics***" section, select the subscription on which it will be registered, choose the "***Resource group***" previously created and indicate a descriptive name.

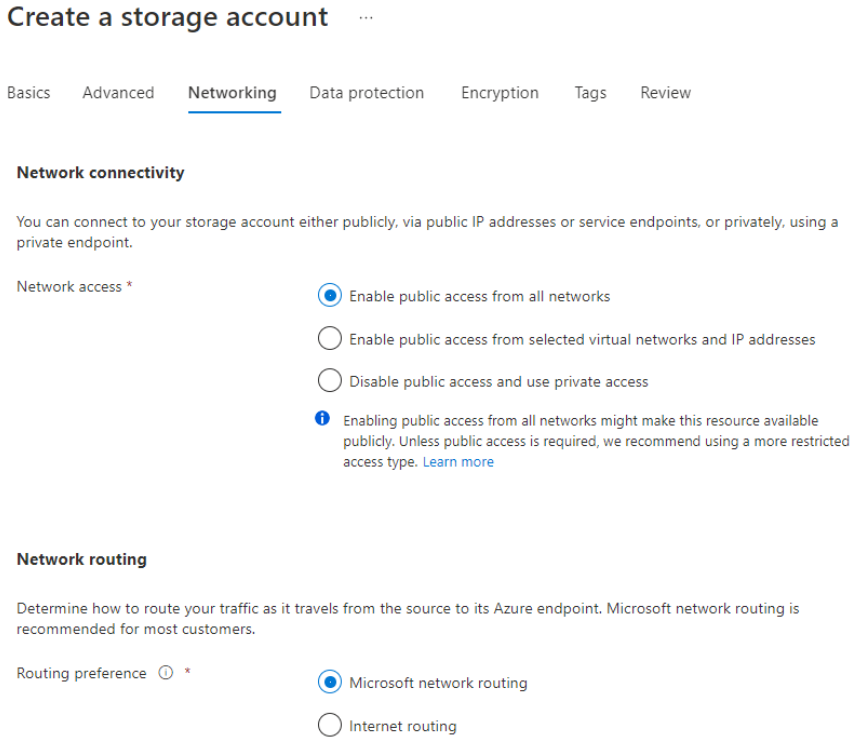
   Choosing the rest of the available options "***Performance***", "***Region***", "***Redundancy***") do not affect the operation/deployment of UDS, but they can affect the final cost.



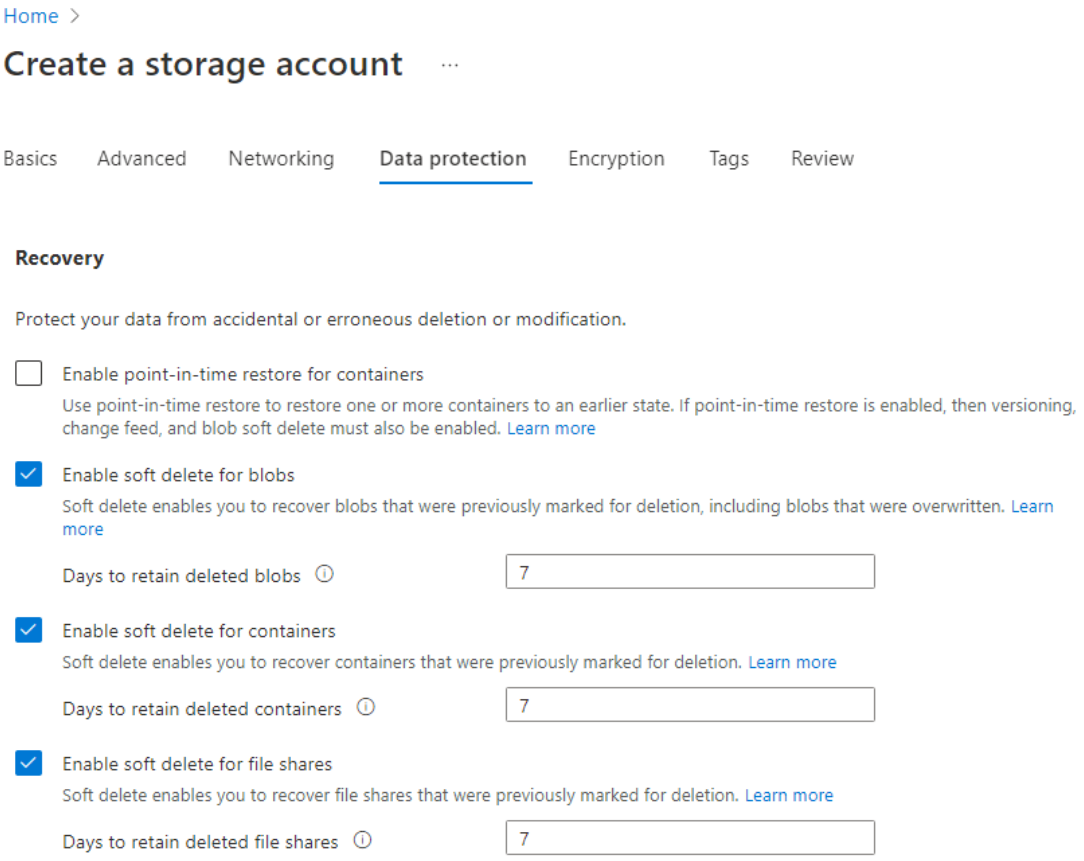
4. In the "***Advanced***" section, mark the options that interest you.



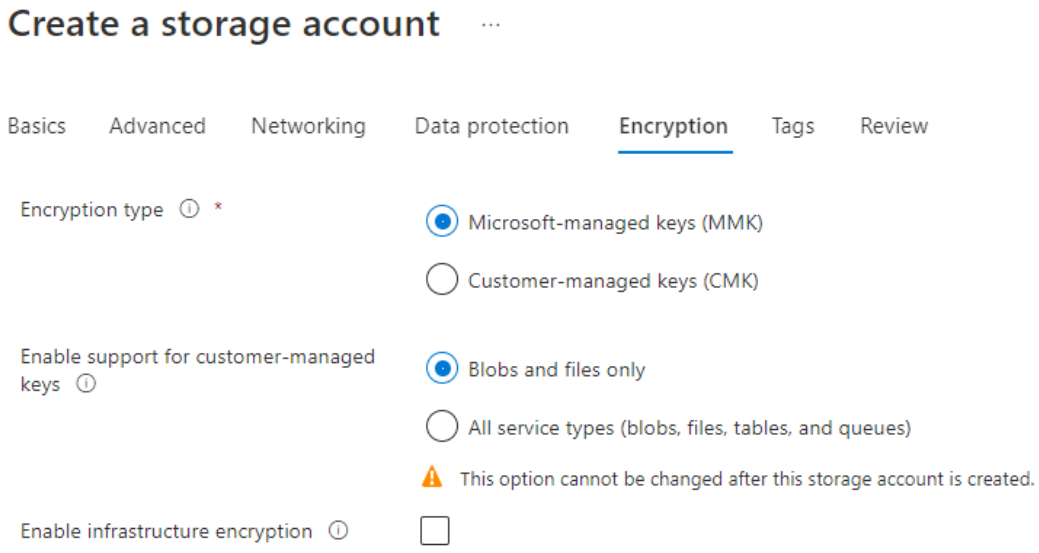
5. In the "***Networking***" section, select the options that interest you.



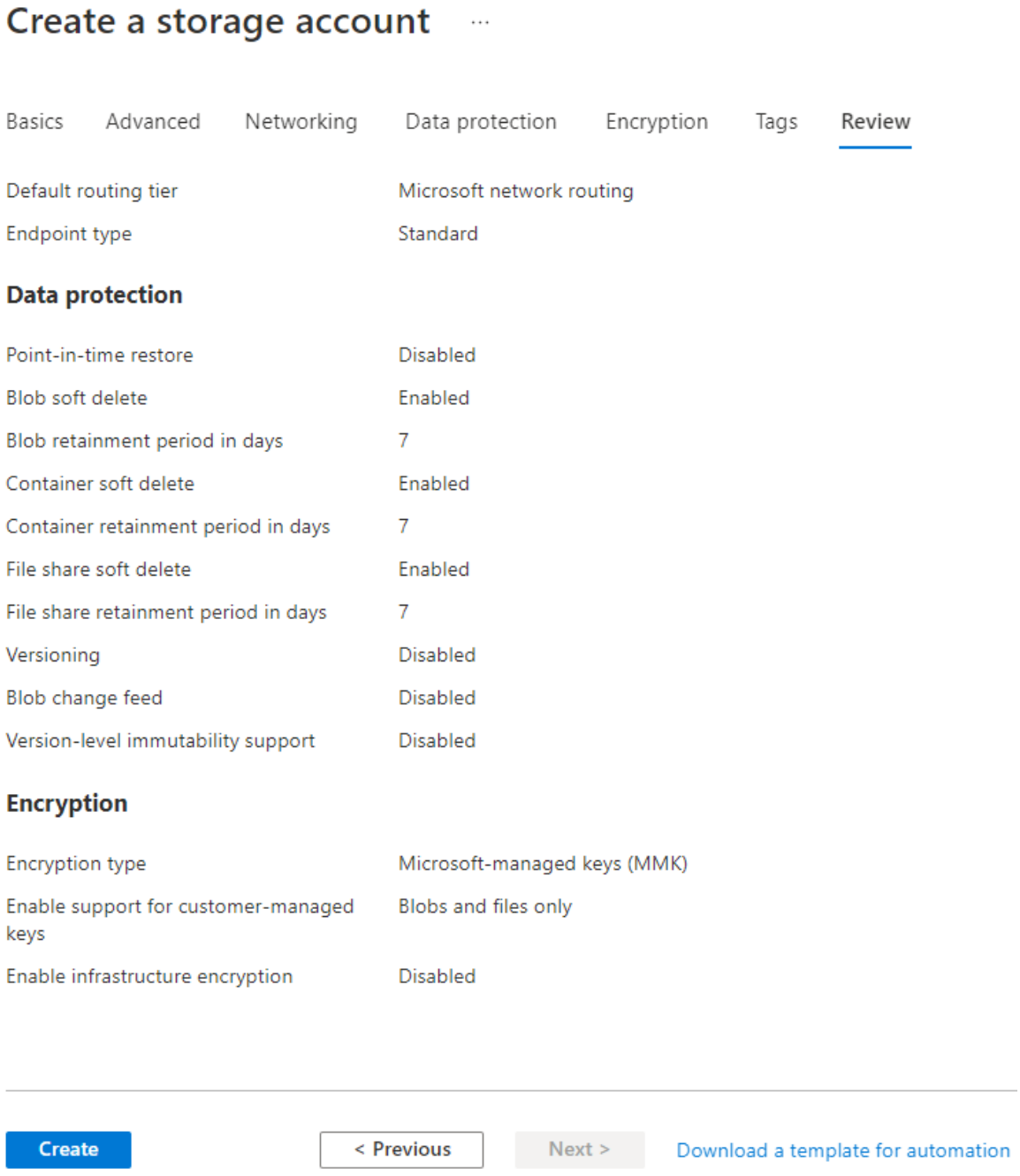
6. In the "***Data protection***" section, select the options that interest you



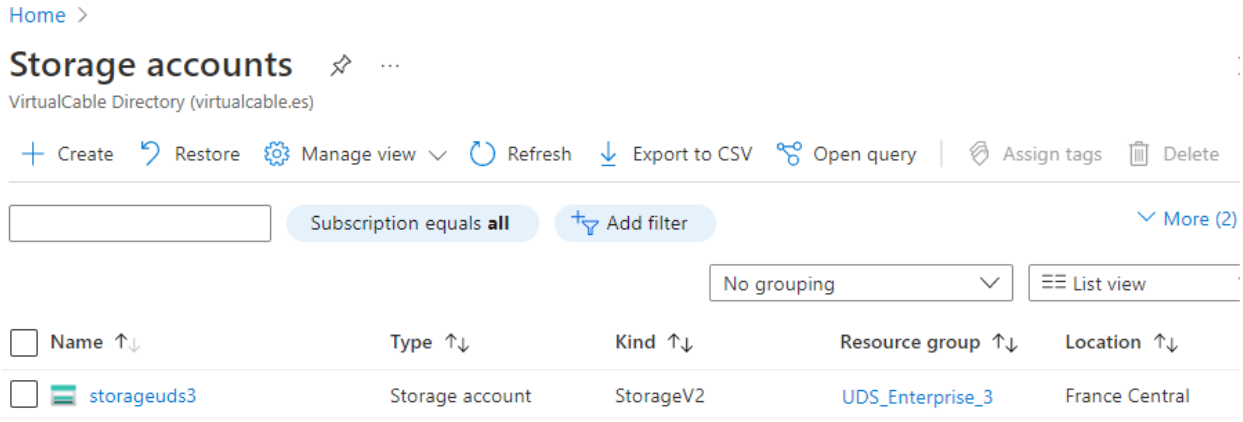
7. In the "***Encryption***" section, select the options that interest you.



8. In the "***Review***" section, confirm that all the data is correct and click on "***create***":



9. Confirm that the "***Storage account***" has been created correctly.

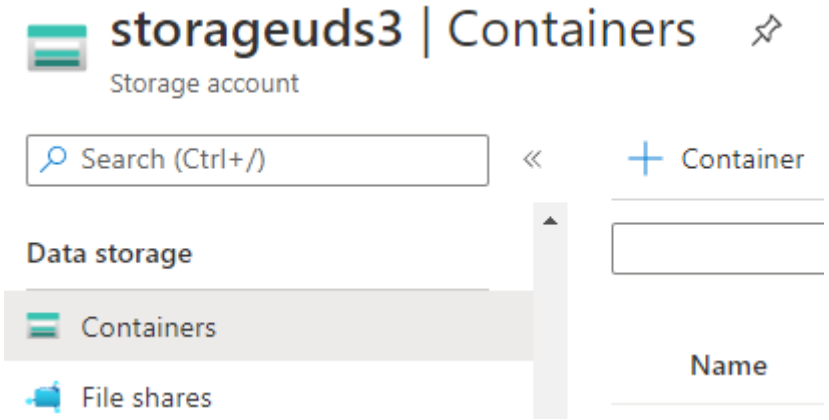


- Container

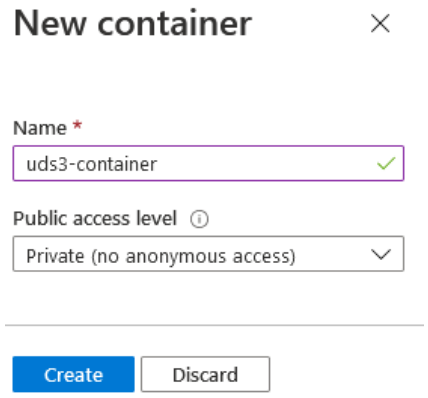
Once you have a valid "***Storage account***" you will need to have a "***Container***" to upload the disk images from the UDS servers.

If you don't have one, you can create it by following these steps:

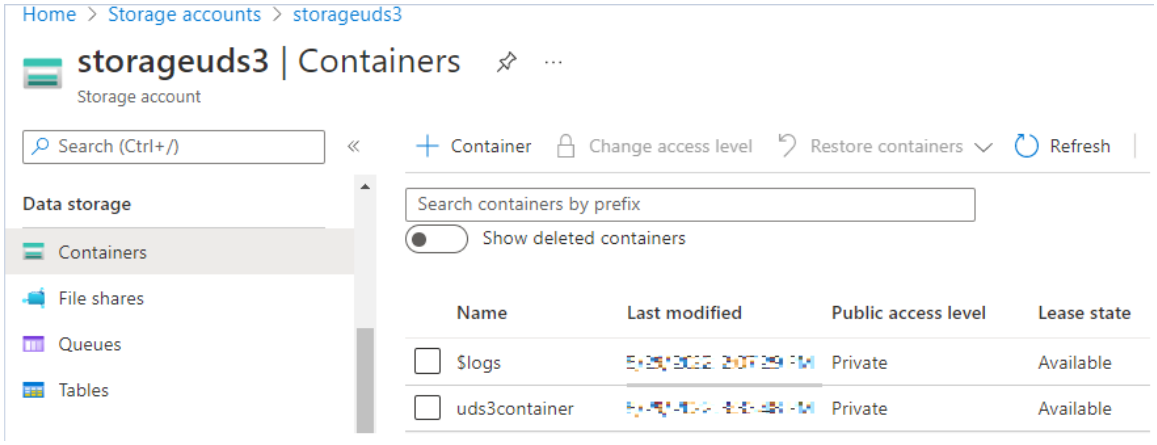
1. Access the "***Storage account***" on which you will upload the UDS images. Within the "***Data Storage***" menu, select "***Containers***" and click on "***Container***" to create a new one:



2. Indicate a descriptive name for the new "***Container***" and select the "***Public access level***" appropriate to your needs. Click on "Create" to finish its creation.



3. Confirm that the "***Container***" has been created correctly:

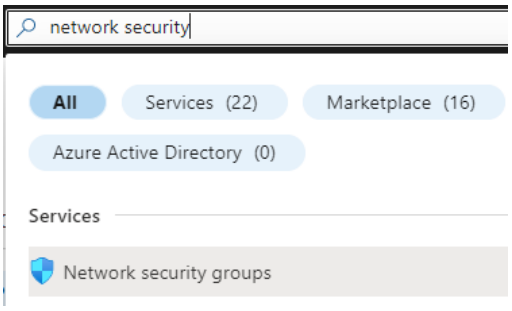


- Network security groups

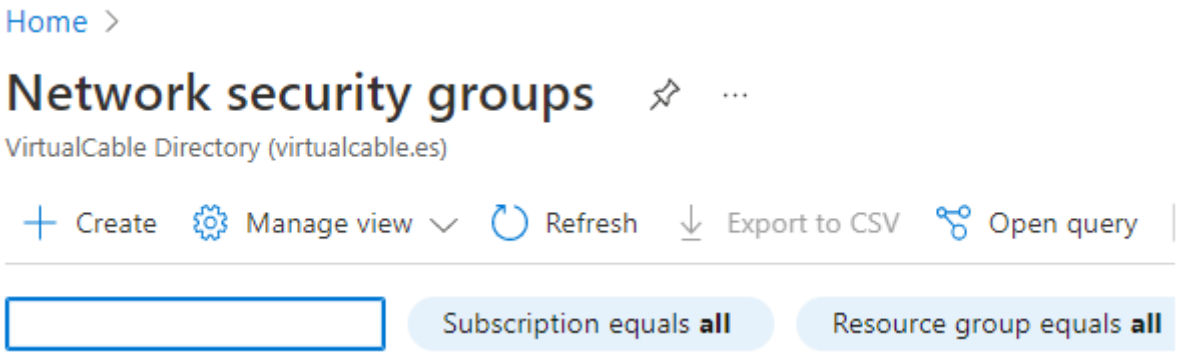
Another of the elements necessary for the deployment of UDS will be the "***Network security groups***", which will perform the firewall function.

For the different UDS elements, specific ports will be required. Below are the ports that must be configured for the correct operation of UDS:

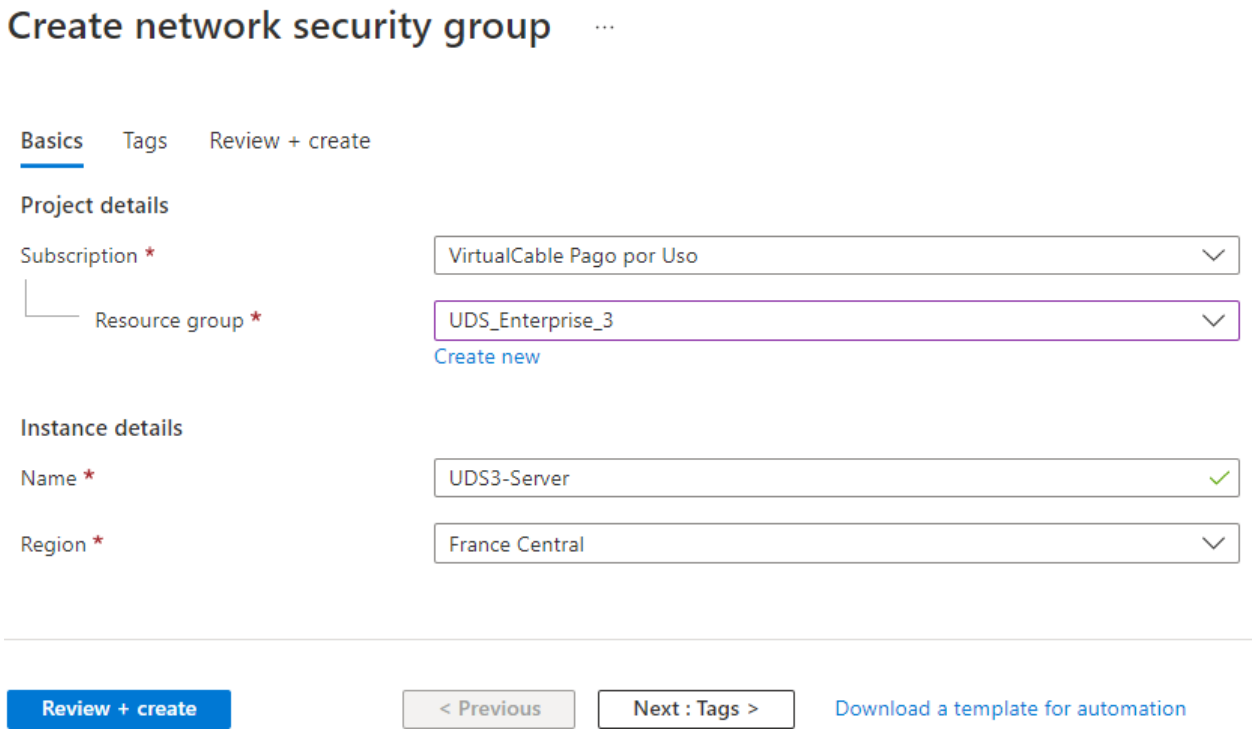
1. In the "***Services***" list, search for "***Network security groups***" and click on it:



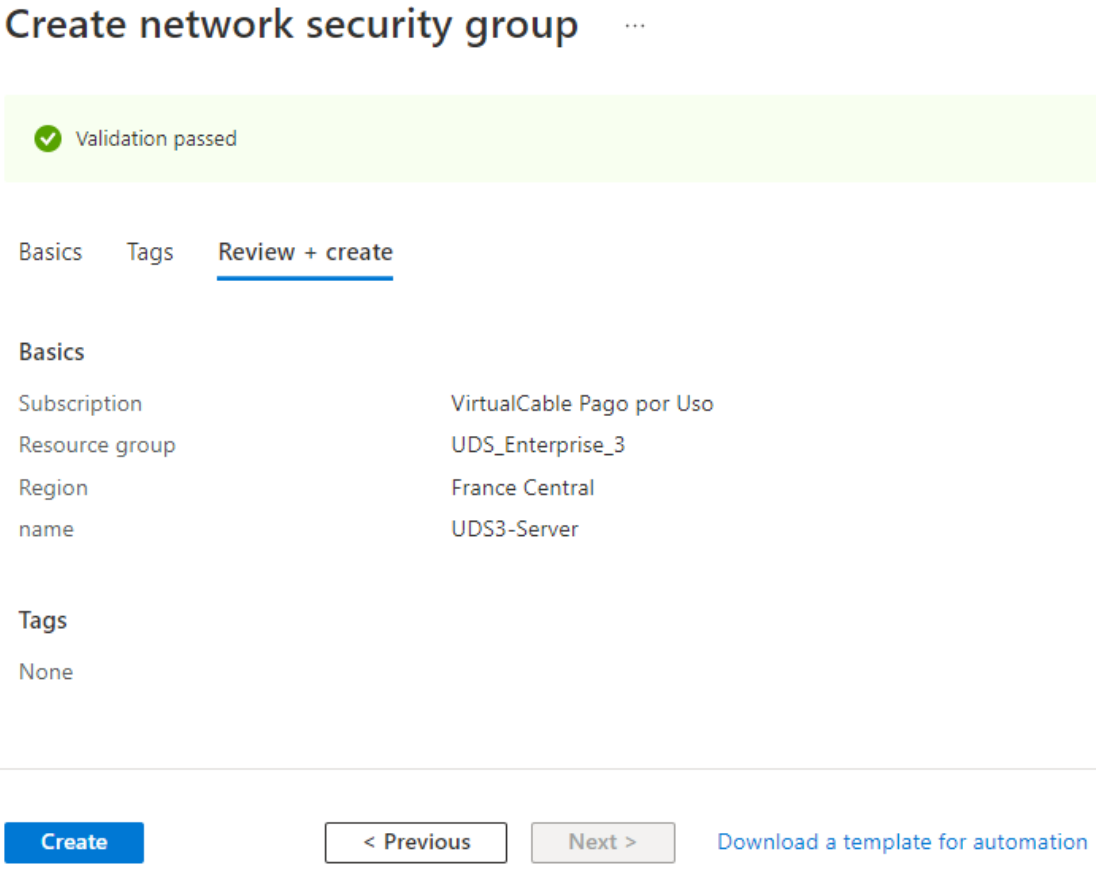
Once inside, click on "*Create*" to create a new one.



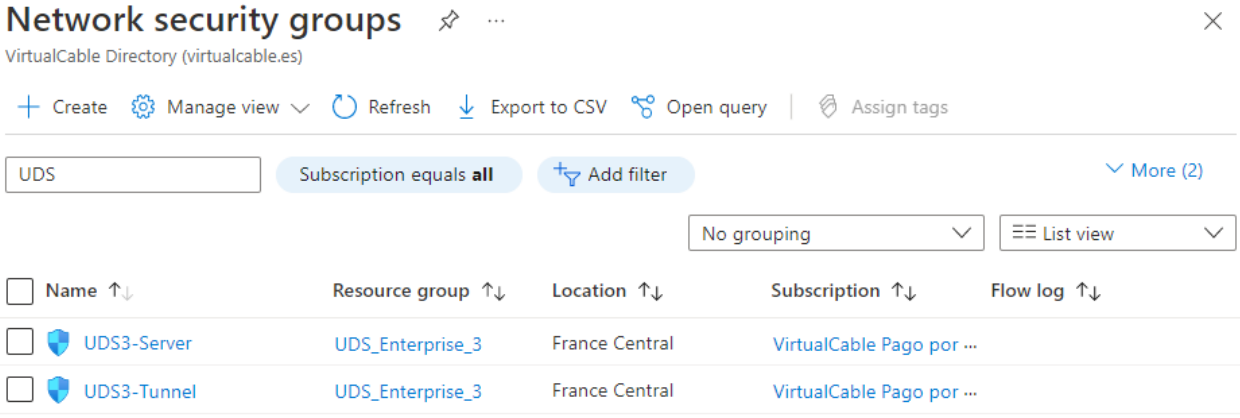
2. In the "*Basics*" section, select the subscription and the "*Resource group*" on which it will be registered. Indicate a descriptive name for the element, and choose a "*Region*". Click on "*Review + Create*".



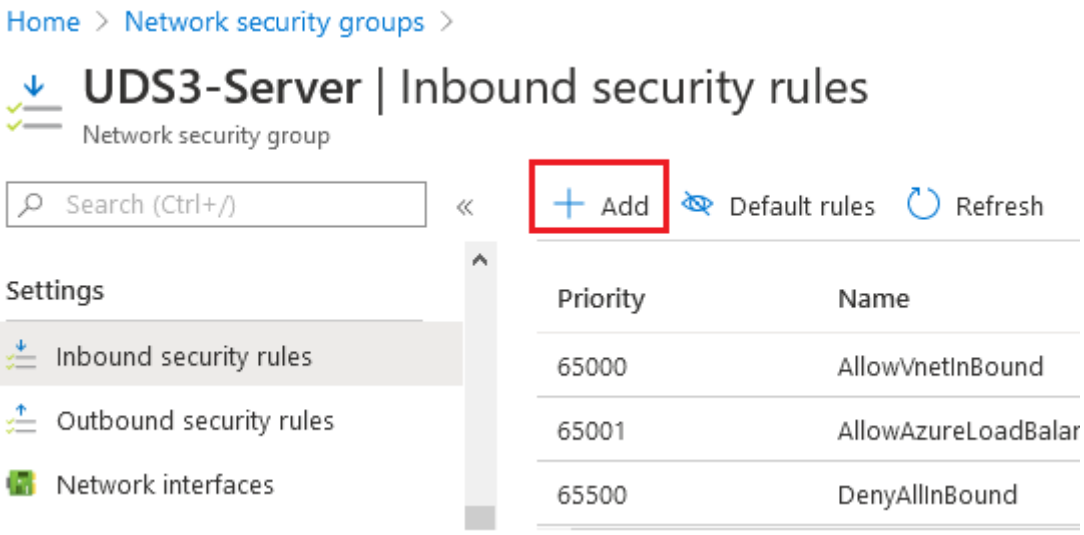
3. Review all the data and if they are correct click on "***Create***":



4. Confirm that the "***Network security group***" has been created correctly. It will be necessary to create two: one for the UDS server and one for the UDS Tunnel server:



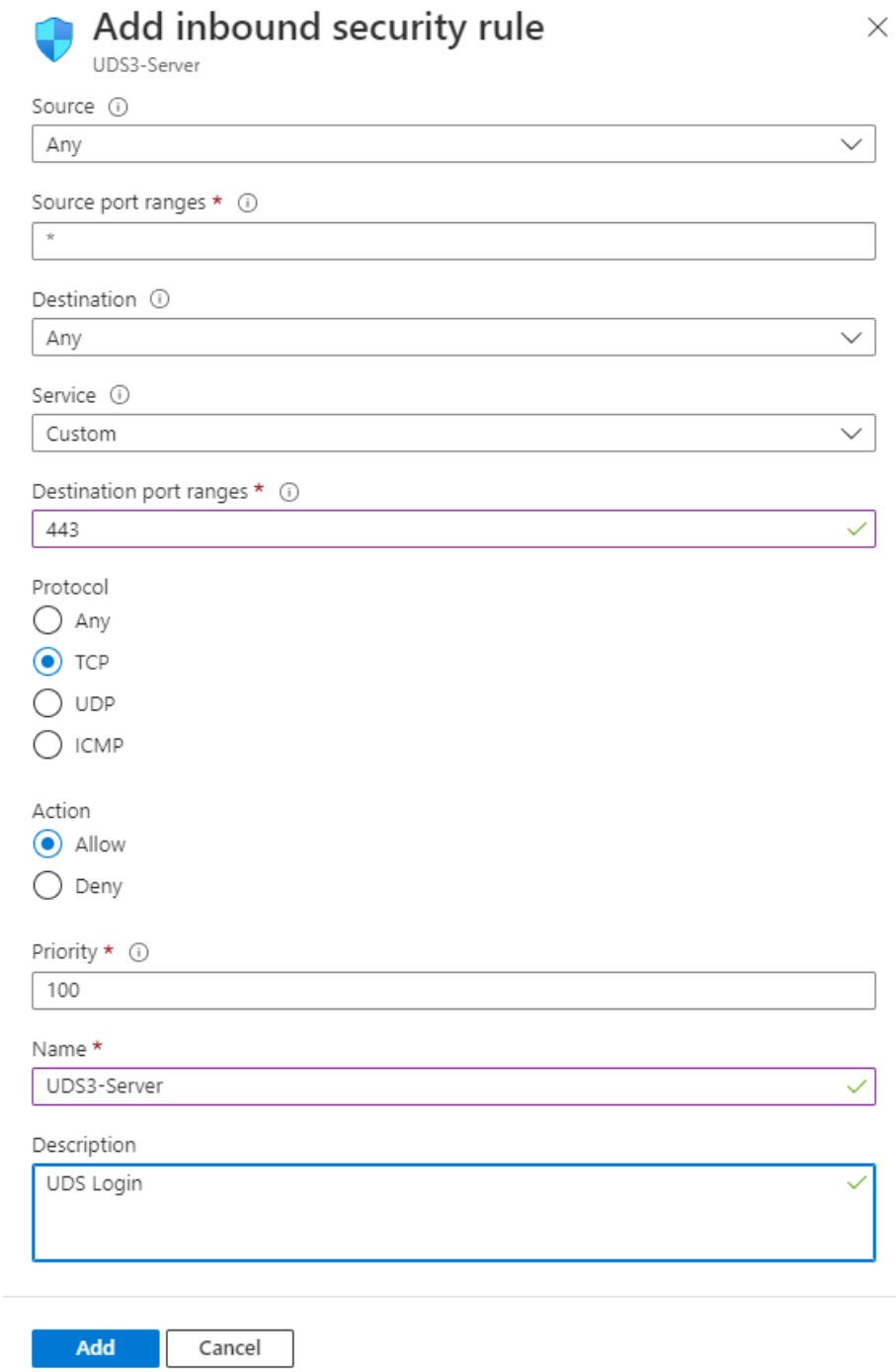
5. Access the newly created "***Network security group***". In the "***Settings***" menu, select "***Inbound security rules***" and click on "Add" to create the necessary access rules:



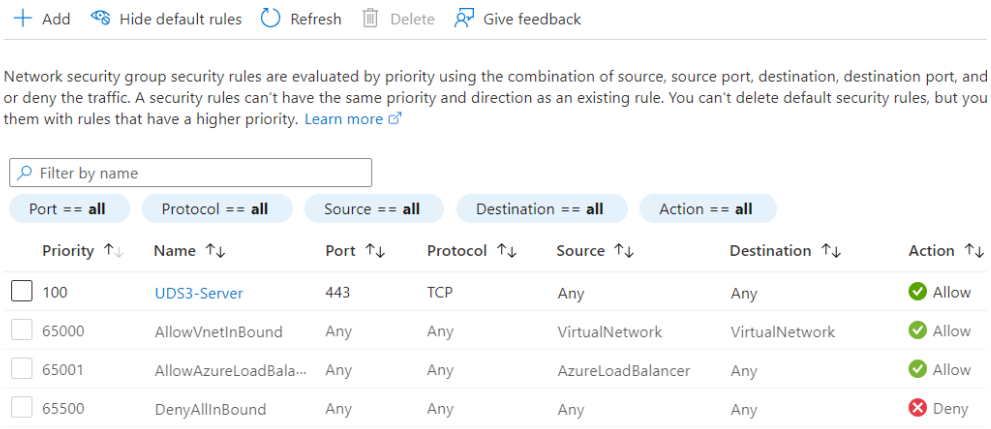
6. You will need to configure two "***Network security groups***": one for the UDS server and one for the UDS Tunnel server, each with its corresponding rule in "***Inbound security rules***". In the following table, you can check the ports necessary to access the UDS components and the service they will offer:

Component	Port	Role
UDS Server	443	Login panel access
UDS Tunnel	443, 10443	Access to servicies and HTML5

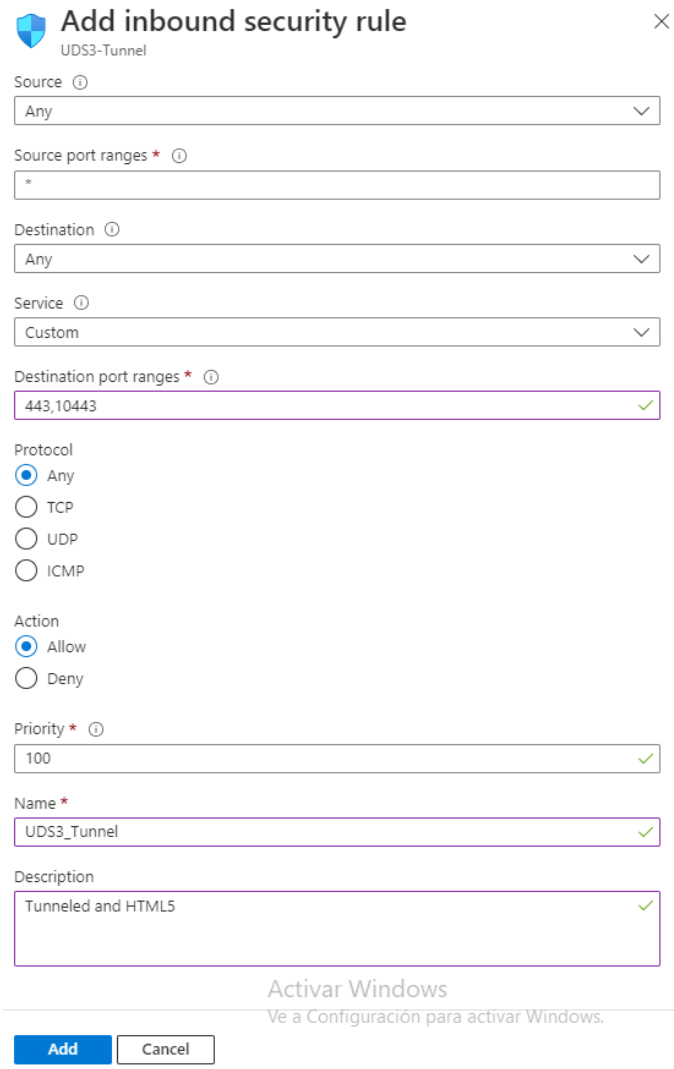
a) **UDS-Server:** You must create an access rule to the UDS server where you allow traffic through 443 TCP port:



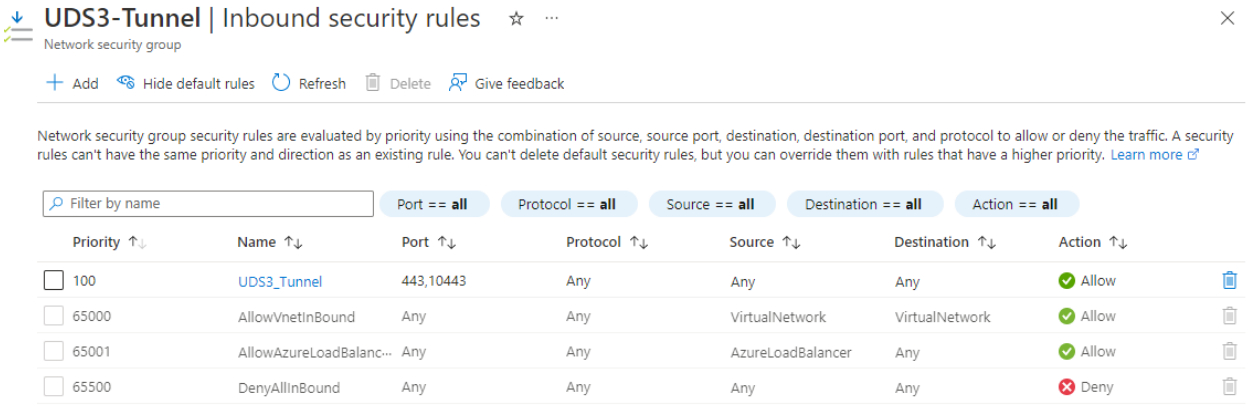
Once you have entered the data as shown in the screenshot, click on "***Add***" to create the rule and confirm its correct creation:



b) **UDS Tunnel:** You must create an access rule to the UDS Tunnel server where you allow traffic through 443 TCP and 10443 TCP ports:



Once you indicate the data as shown in the screenshot, click on "***Add***" to create the rule and confirm its correct creation:



Deploy UDS servers

Below is an example of how to deploy the servers that make up the UDS Enterprise environment on an Azure platform. The steps to upload and create the UDS Server component are detailed in this guide. The same tasks should be performed for the UDS Tunnel server and the MySQL database.

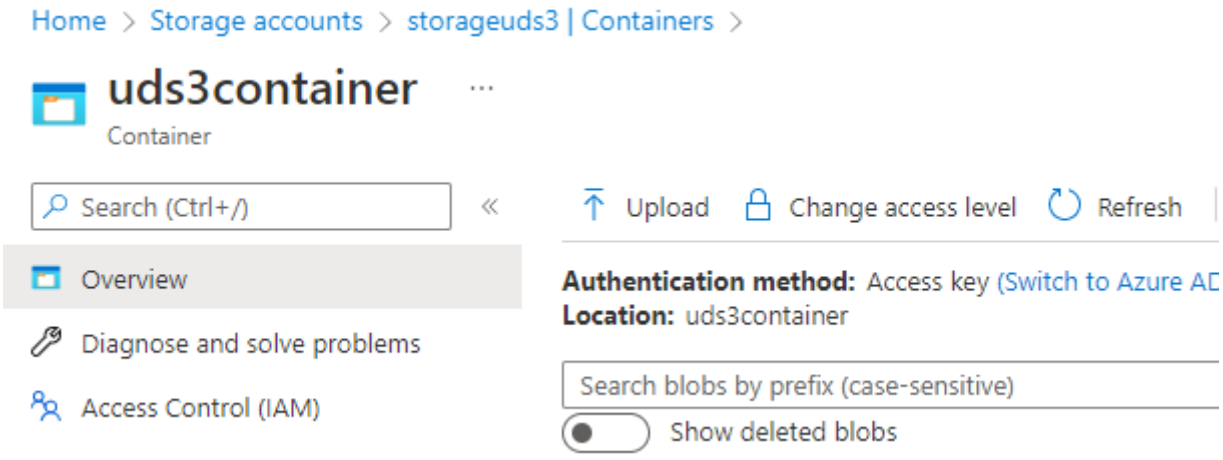
If the version of UDS to install is Enterprise, you should also upload the MySQL database server to the platform (if you use the UDS Enterprise Evaluation Edition version, you can activate a local database included in the UDS server).

The UDS servers will be provided by the VirtualCable team in disk image format (.vhd)

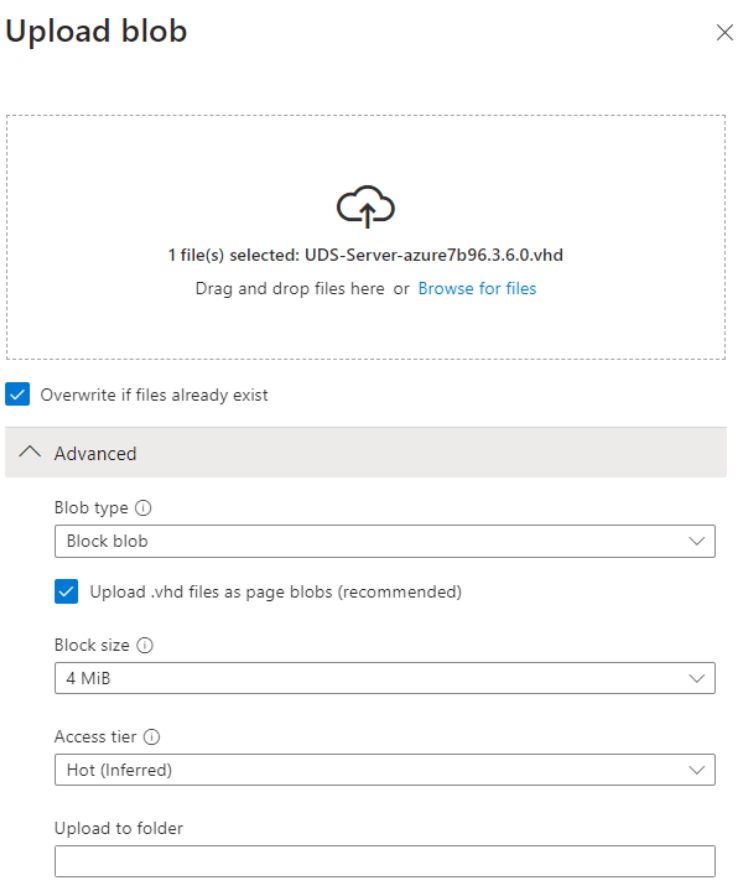
▪ Upload disk images

The first task you will perform will be to import the UDS Server disk image. In order to do this, you must have a "***Container***" and the disk image of the UDS Server in .vhd format

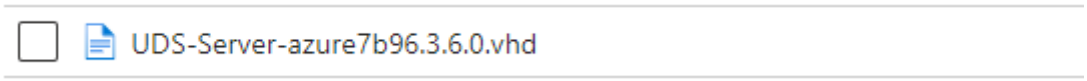
1. Access the "***Container***" ("***Storage accounts***", in the "***Data Storage***" section, click on the existing "***Container***") and click on "***Upload***":



2. Indicate the disk image in the "*Files*" section. In "*Blob type*" select "*Page blob*" and click on "*Upload*":



3. The image will start to be imported and you will have to wait until the upload process finishes. Once finished, you will proceed to the next task, which will consist of generating a disk from the image:



NOTE:
Depending on the size of the disk images and the connection speed, this process can take several minutes.

This process will need to be repeated with the UDS Tunnel component and with the MySQL Database server (in case you want to use this element).

Finally, you will see that within the "***Container***" you will have the UDS images available.

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
UDS-Dbserver-azured994.3.6.0.vhd	[redacted]			Page blob	10 GiB	Available
UDS-Server-azure7b96.3.6.0.vhd	[redacted]			Page blob	8 GiB	Available
UDS-Tunnel-azure7a78.3.6.0.vhd	[redacted]			Page blob	14 GiB	Available

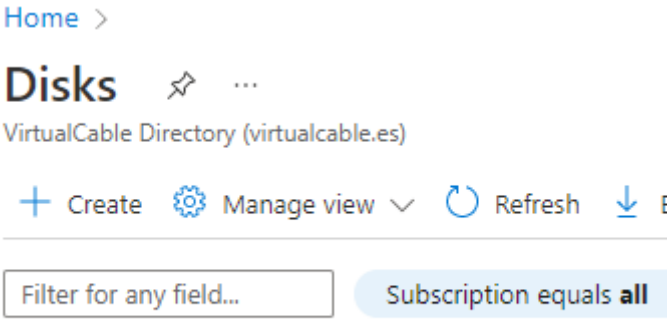
Disk creation

Once you have the images of the different UDS components uploaded to the Azure platform, you will proceed to deploy virtual disks based on these images.

From the virtual disks that we will create next, you will generate the virtual machines that will form the UDS environment:

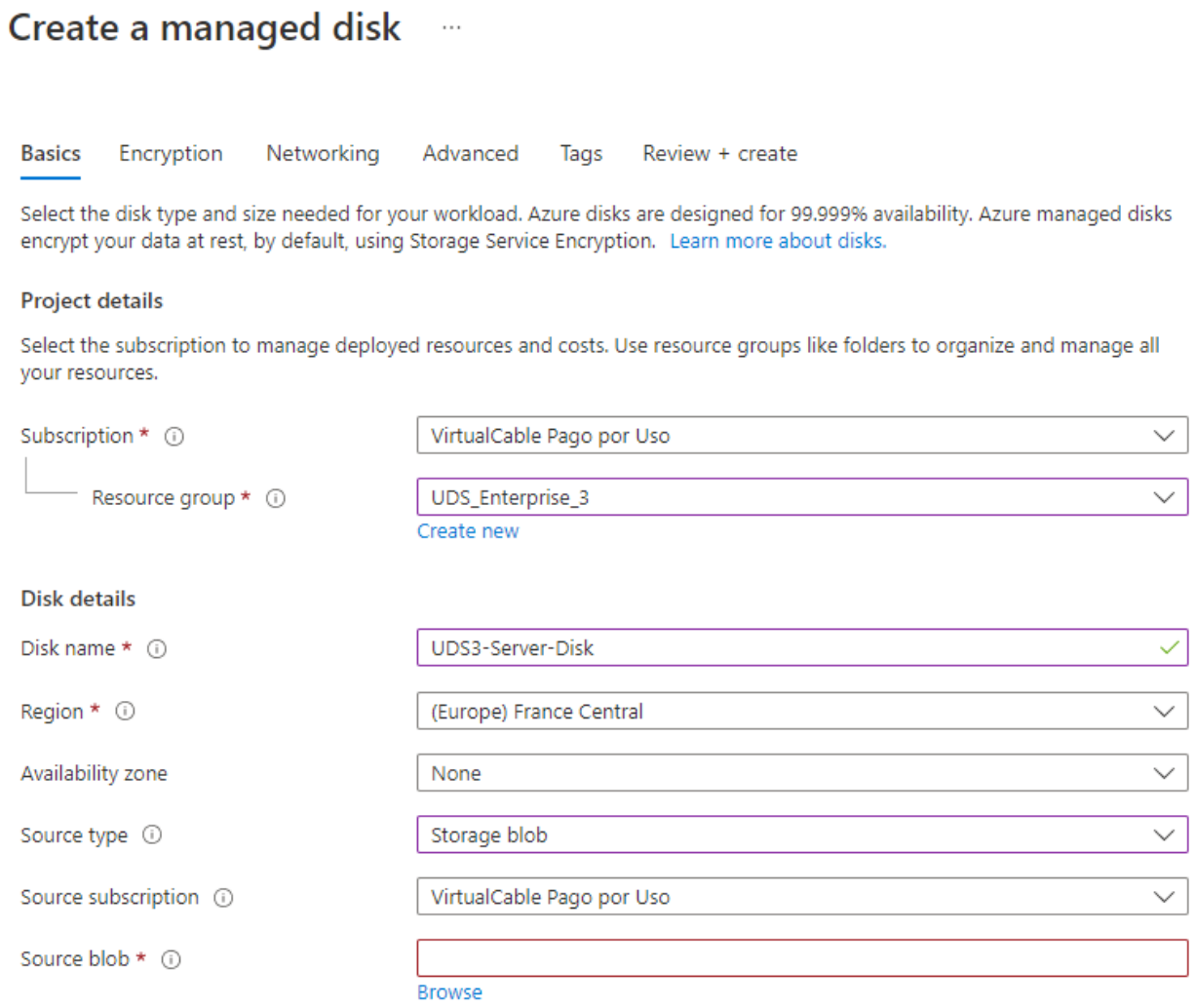
1. In the list of "***Services***", look for "***Disk***" and click on it:

2. Click on "***Add***" to add a new disk.



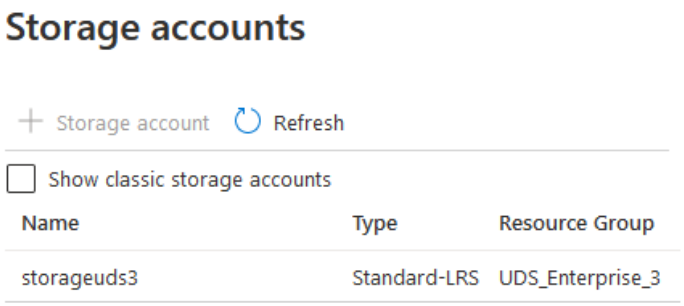
3. In the "***Basics***" section, select the subscription and the "***Resource group***" on which it will be registered. Indicate a descriptive name for the element, the "***Region***", and in "***Source type***", indicate "***Storage blob***".

NOTE: The machines may only contain one disk

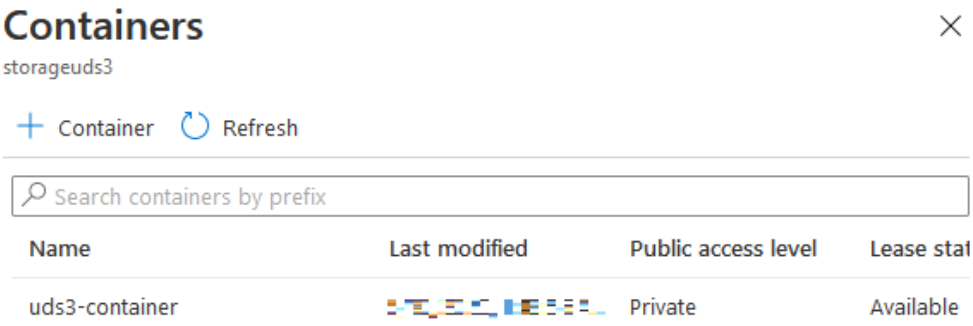


In "***Source blob***" click on "***Browse***" to select the previously imported disk.

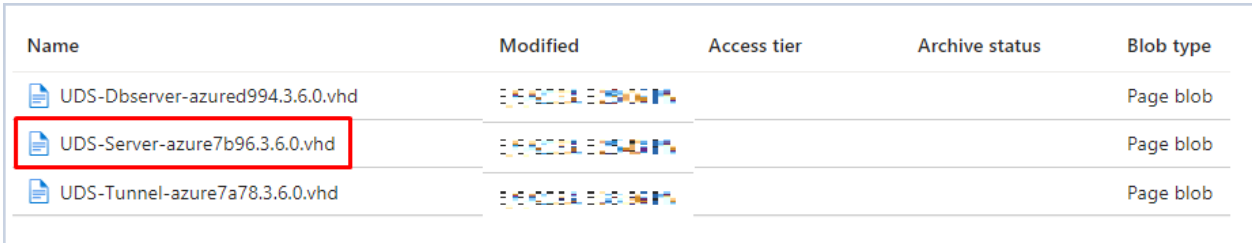
You must select the "***Storage accounts***" that contains the disk images:



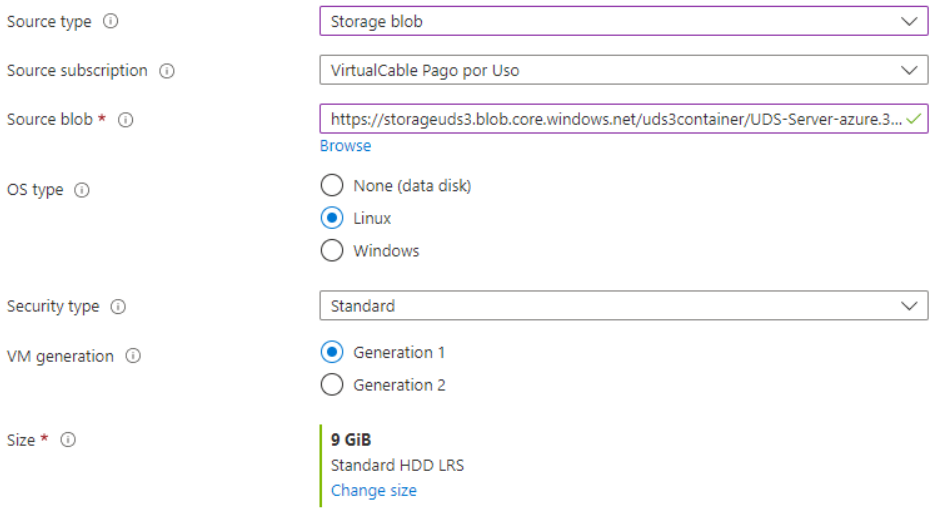
Once inside, select the "*Container*" previously created.



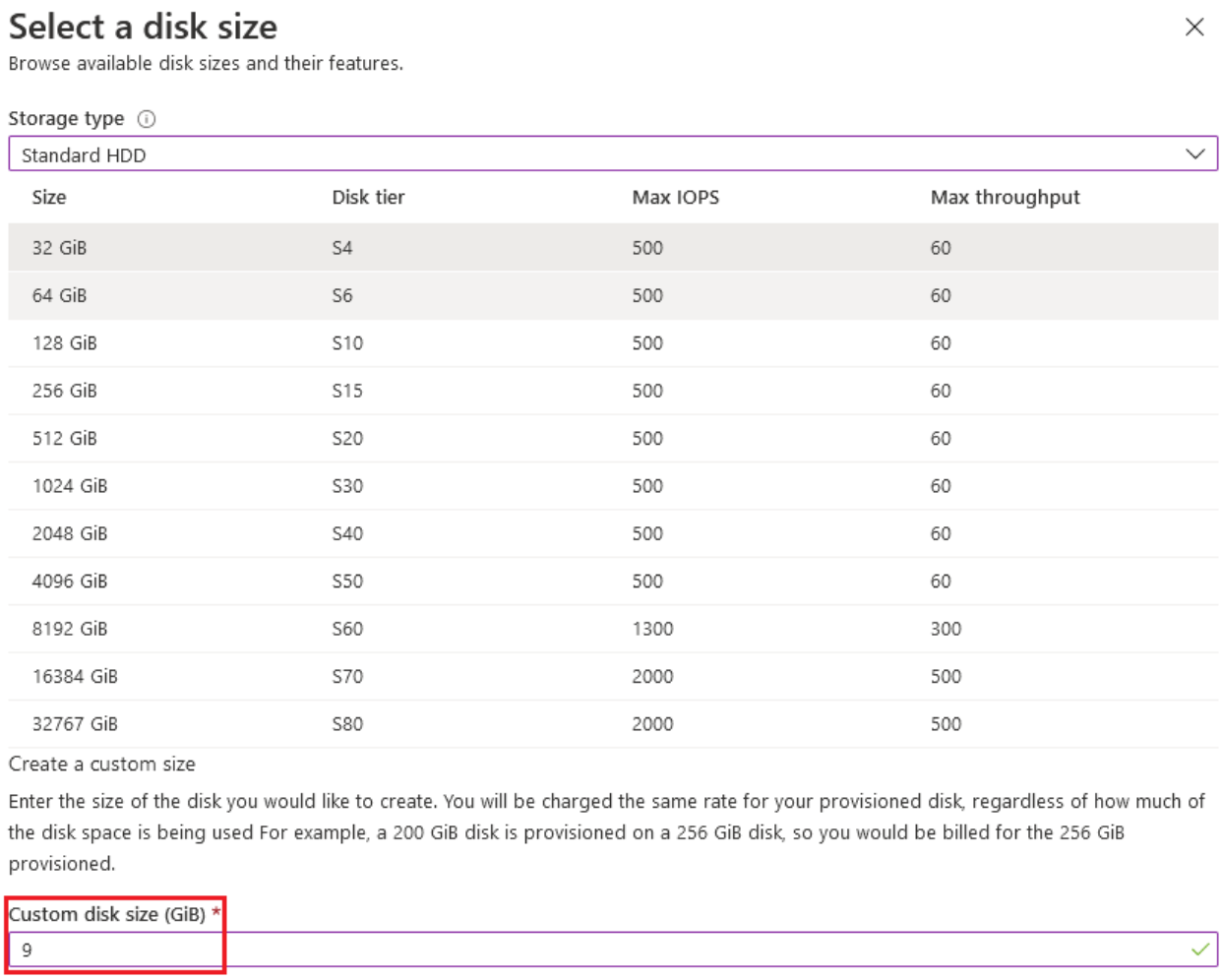
Finally, select the imported image in the previous step (in this case for the UDS-Server) and click on "*Select*".



In "*OS type*", indicate that it is "*Linux*" and in "*Size*" click on "*Change size*".



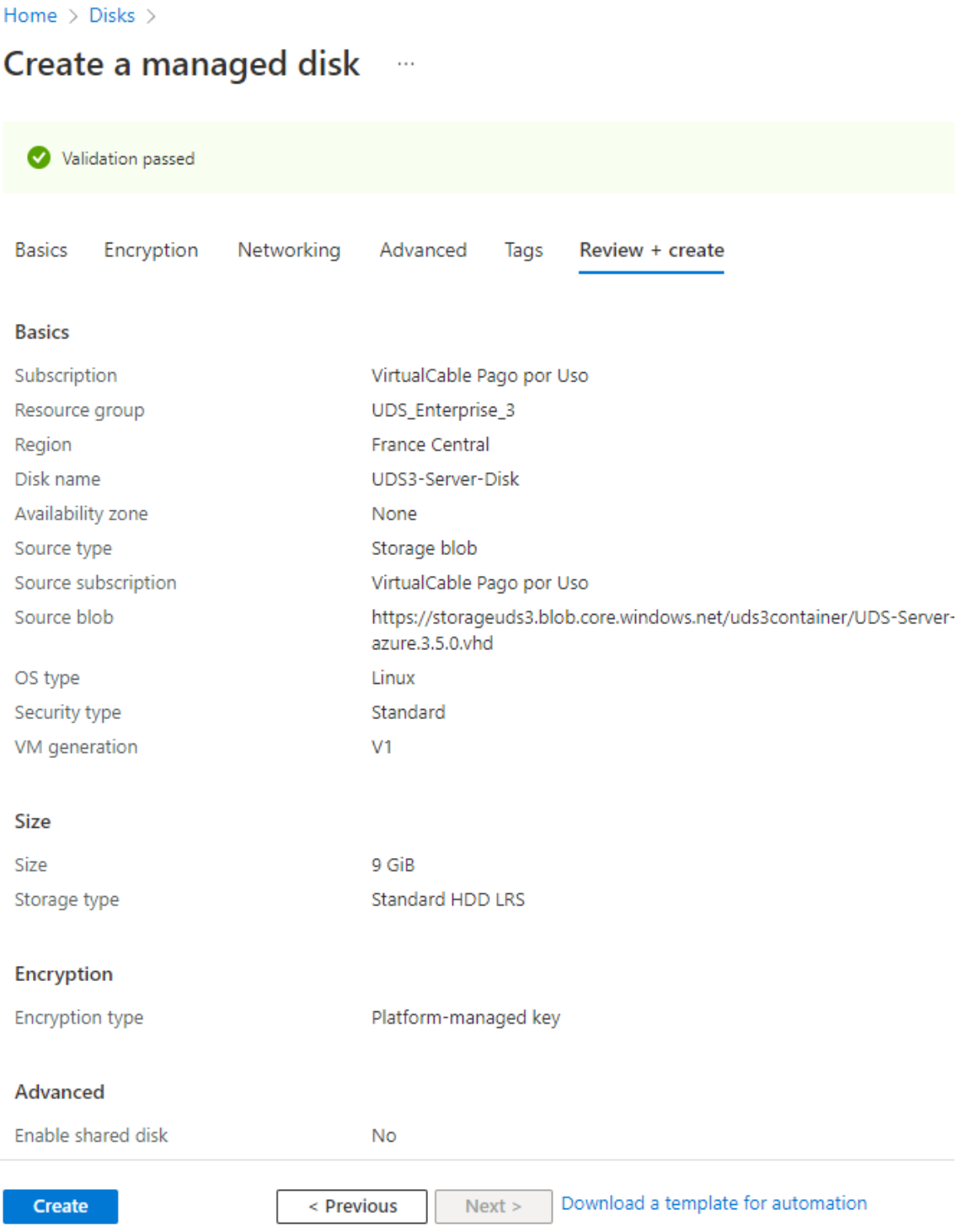
You select the "*Storage type*" and in "*Custom disk size (GB)*" you indicate 9 as the disk size for the UDS-Server component:



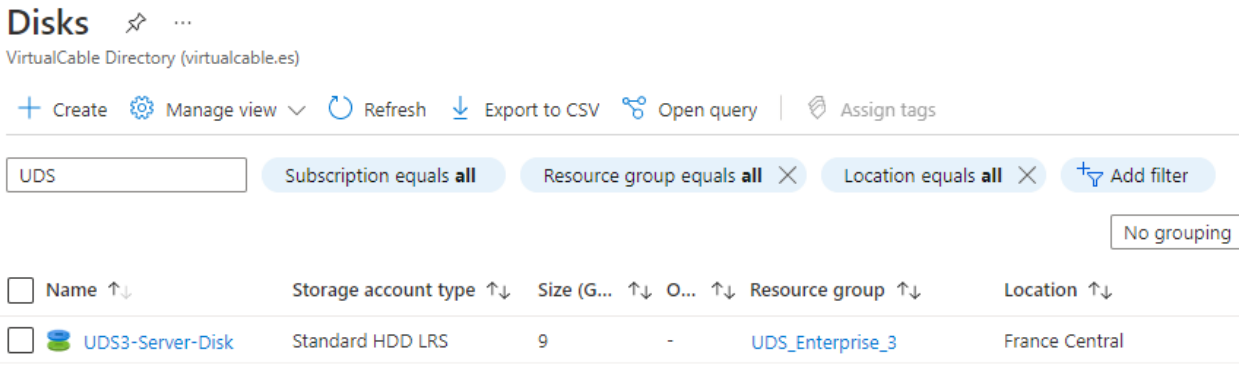
NOTE:
The disk sizes for the different UDS Enterprise 3.6 components will be as follows

Component	Size in GB
UDS-Server	9
UDS-Tunnel	14
MySQL	9

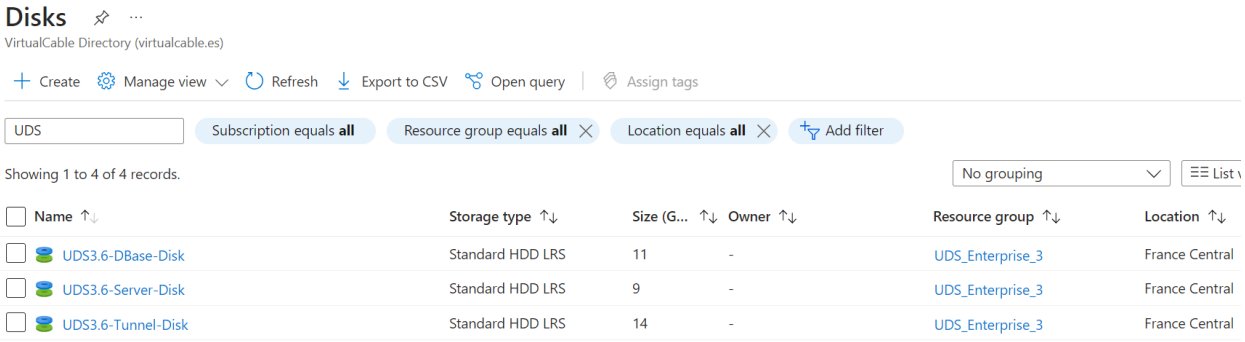
Click on "***Review + Create***", check that all the data is correct and click on "***Create***":



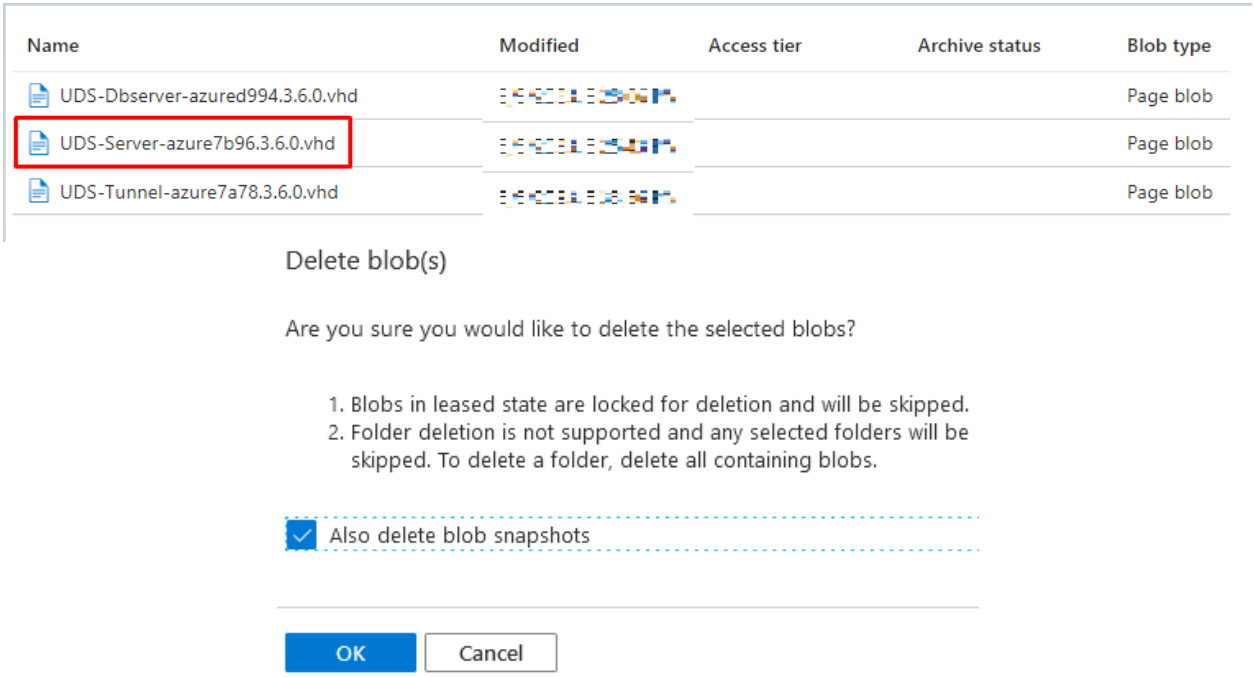
4. You will wait for the disk to be created and, once the task is finished, you will see that it is available to later generate the virtual machines.



5. You will repeat the process with the UDS-Tunnel component and, if necessary, also with the MySQL Database server.



NOTE:
Once the disks are deployed, you can delete the images from the "**Container**" to avoid causing an unnecessary cost.

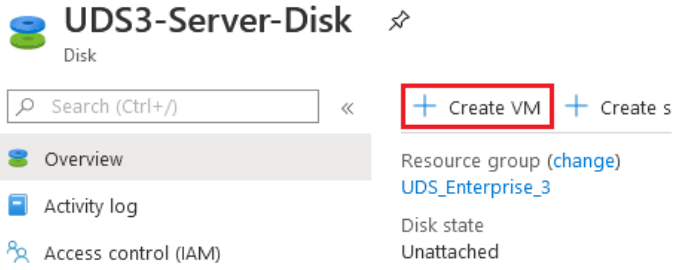


Create UDS virtual servers

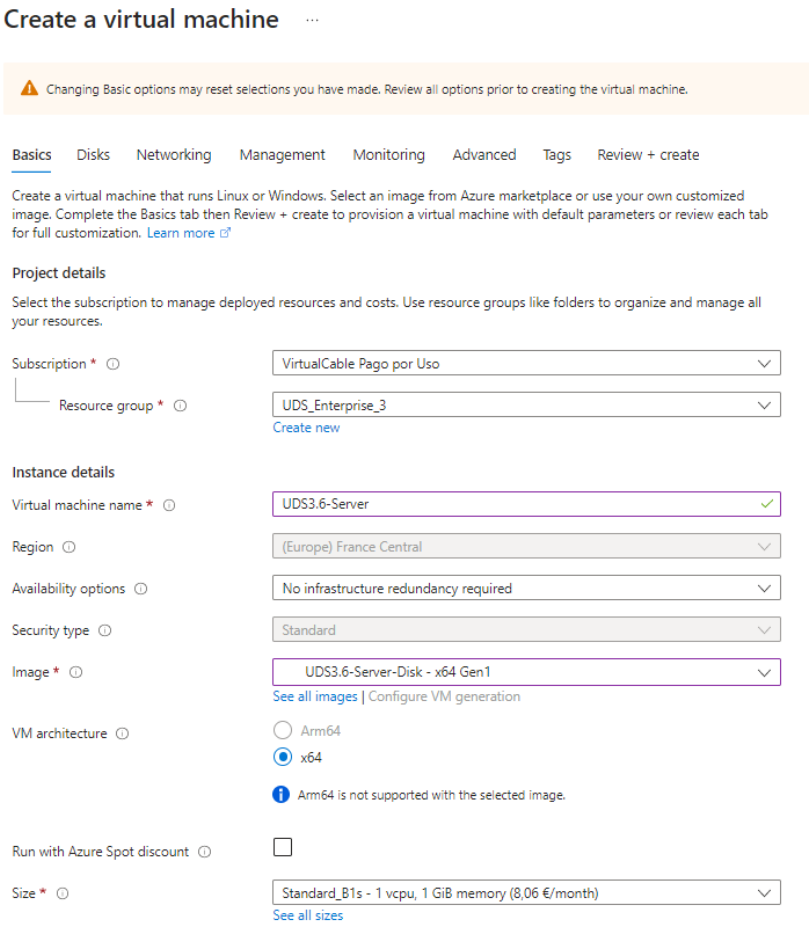
The last task that you will perform in the process of importing/creating the UDS components will be the creation of the virtual machines based on the disks created in the previous step.

The machines will be created from the disks themselves:

1. Select the previously created disk (from the "***Disk*** service) and click on "***Create VM***":



In the "***Basics***" section, select the "***Resource group***" on which it will be registered, indicate a descriptive name for the new virtual machine (in this case for the UDS-Server component), confirm that "***Image***" is selected in the virtual disk previously selected and, finally, indicate the "***Size***" of the virtual machine.



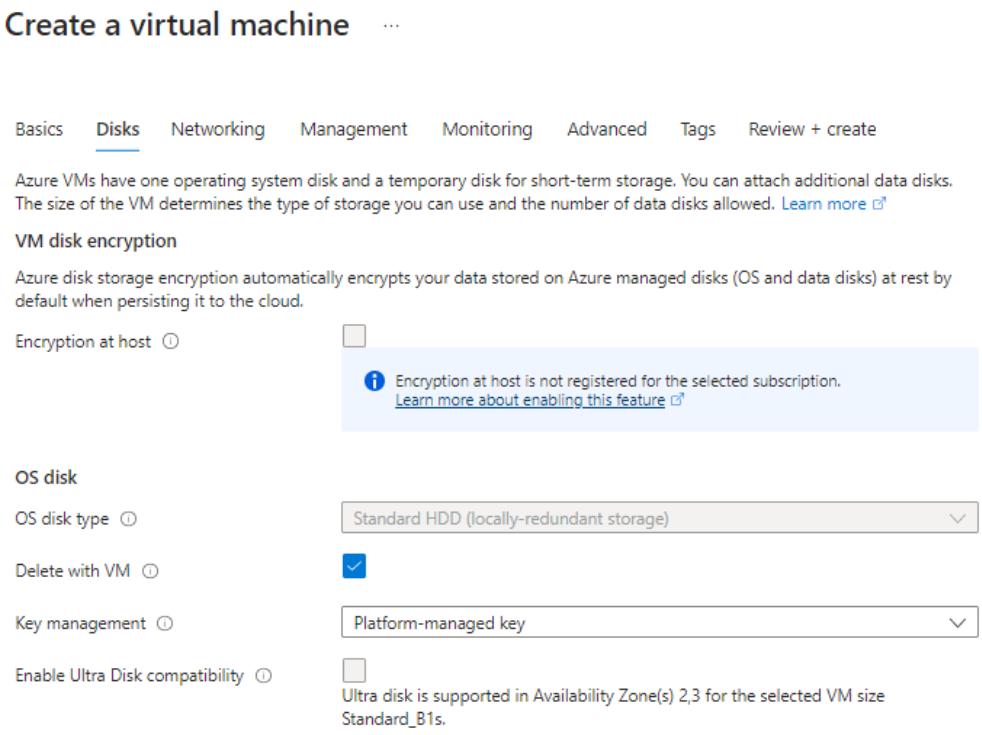
NOTE:

The recommended resources for the installation of the UDS components are shown in the following table (even if very small deployments are going to be carried out, we can reduce these resources, being able to choose the type B1s, 1vCPU and 1 GB of vRAM, for all items).

Component	vCPU	vRAM (GB)
UDS-Server	2	2
UDS-Tunneler	2	2
MySQL	2	1

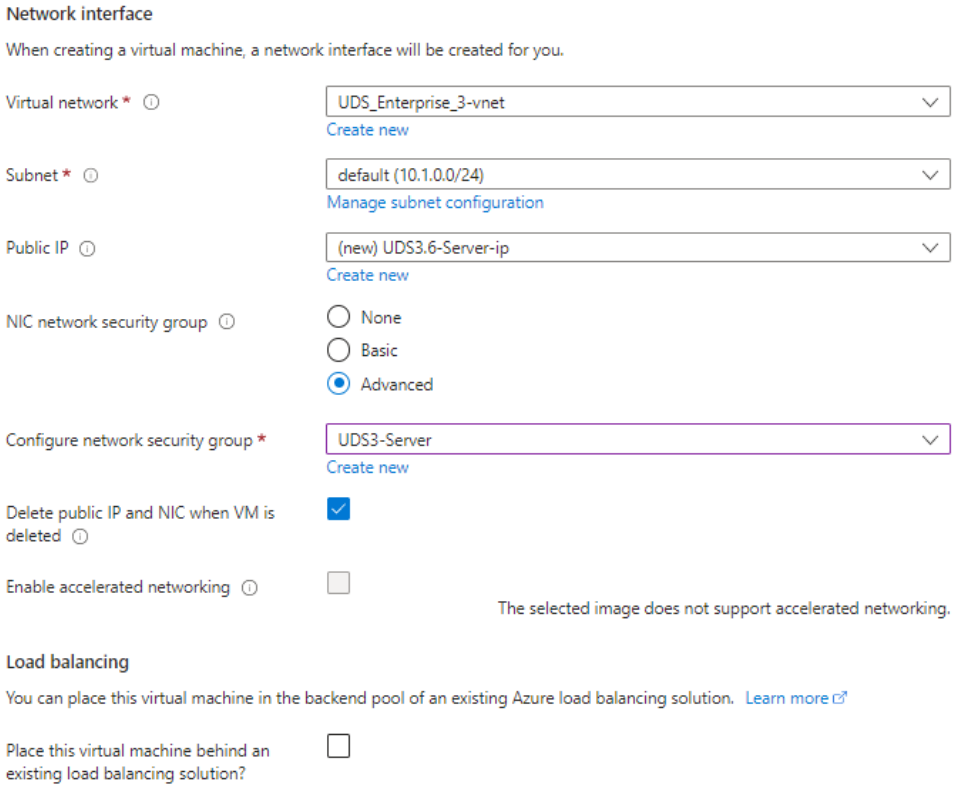
2. In the "***Disks***" section, leave all the options by default since it is not necessary to add an extra disk.

If we select the "Delete with VM" option, the disk will also be deleted when the virtual machine is deleted.



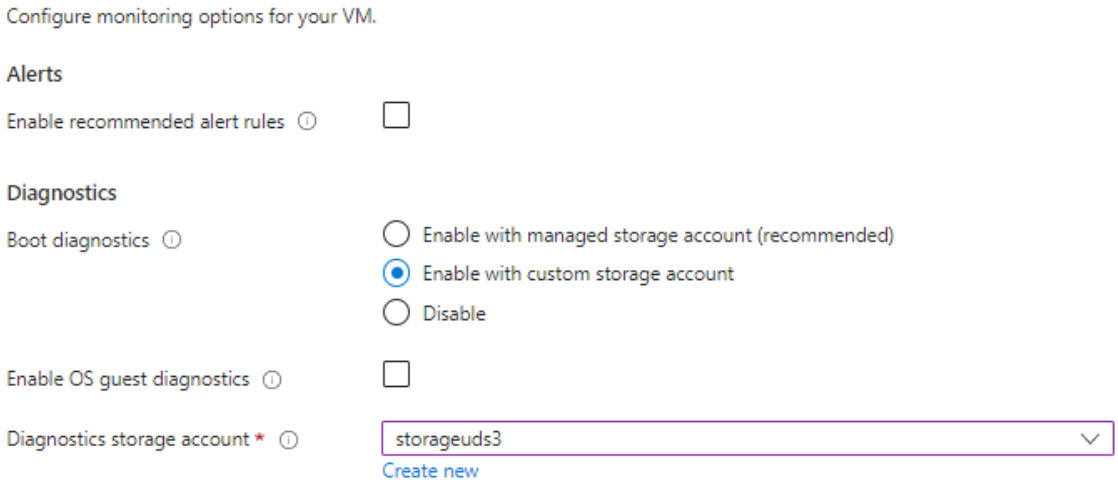
3. In the "***Networking***" section, you must indicate a "***Virtual network***" to connect the server (if you do not have one created, you will need to create one), a "***subred***", and for the UDS-Server and UDS-Tunnel components you will assign a new "***Public IP***".

   In "***NIC network security group***" you will select "***Advanced***" and you will choose the appropriate "***Security group***" created in previous steps for each server.

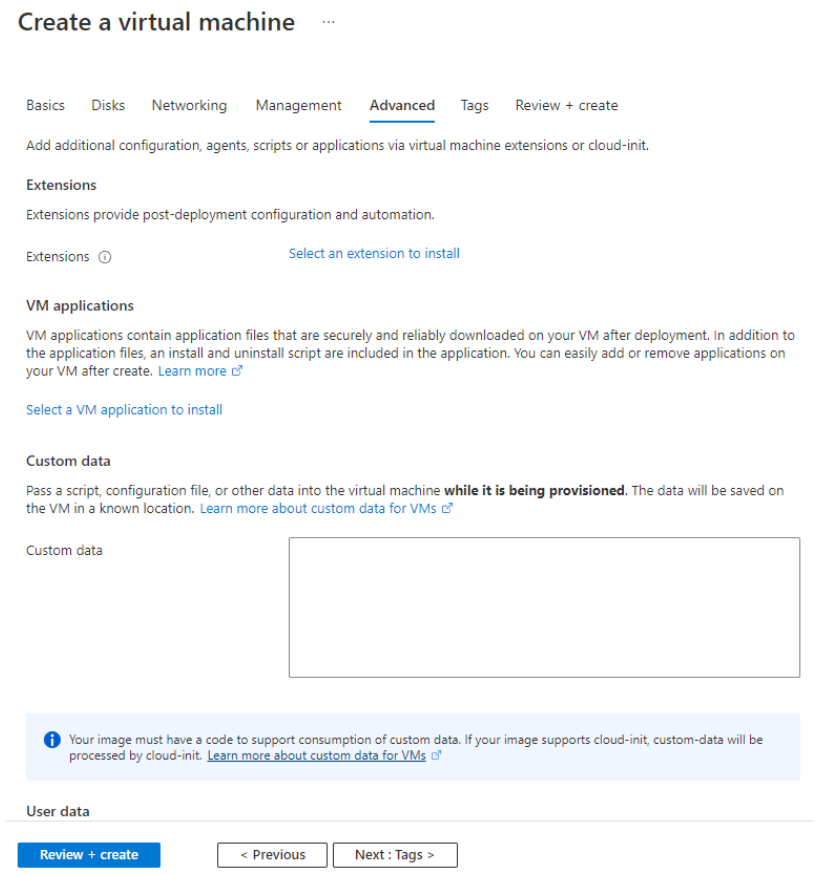


NOTE:
The public IP addresses assigned by default will be dynamic. Although once the VMs is created, you can generate a DNS name associated with this IP or even force the machine to have a static public IP (the UDS-Tunnel component will also need to be assigned a public IP, but for the MySQL database it will not be necessary. Therefore, in this case, you will select "None").

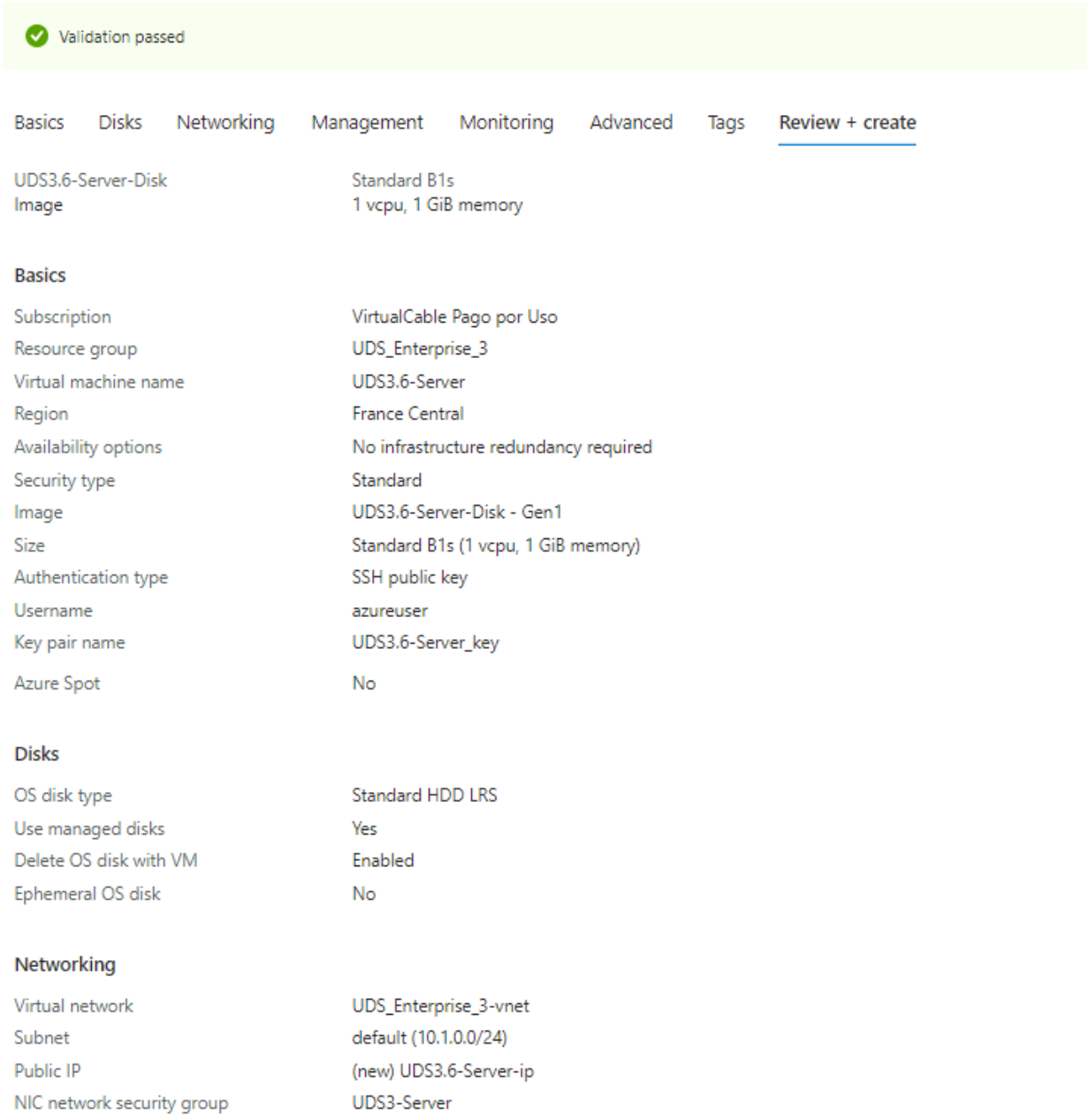
4. In the "***Management***" tab, enable the "***Boot diagnostics***" option that will allow you to view a screenshot of the boot and subsequent state of the virtual machine. Also, this option is necessary to access the "***Serial console***" (when enabling "***Boot diagnostics***" it will be necessary to indicate a "***Storage account***". In this case, select the one created previously to avoid creating a new one).



5. In the "***Advanced***" tab you will leave all the default options and click on "***Review + create***".

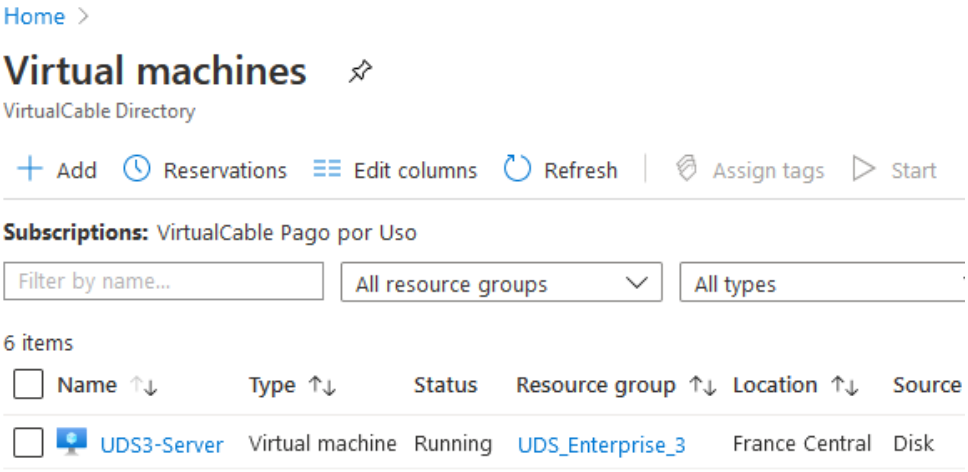


6. Check that all the configuration is correct and click on "***Create***" to create the virtual machine.



7. Once the process of creating the new VM is finished, you will verify that you already have the new machine within the "*Virtual machines*". service. To view it, you must search in the list of "*Services*": "*Virtual machines*" and click on it:

You will see the new virtual machine created and powered on:



8. Repeat the process with the UDS-Tunnel component and also with the MySQL Database server if necessary.

-

Name	Type	Subscription	Resource group	Location	Status
UDS-DBbase	Virtual machine	VirtualCable Pago por ...	UDS_Enterprise_3	France Central	Running
UDS3.6-Server	Virtual machine	VirtualCable Pago por ...	UDS_Enterprise_3	France Central	Running
UDS3.6-Tunnel	Virtual machine	VirtualCable Pago por ...	UDS_Enterprise_3	France Central	Running

NOTE:
In the database server, it will not be necessary to indicate a "Public IP" or a "Security Group", since it will not be accessible from the outside and only the UDS server will need access to it.

UDS server configuration

Once you have all the UDS components deployed as virtual machines, you will proceed to configure them.

To do this, access the "***Virtual machines***" service. If you have the MySQL component, you will start configuring it.

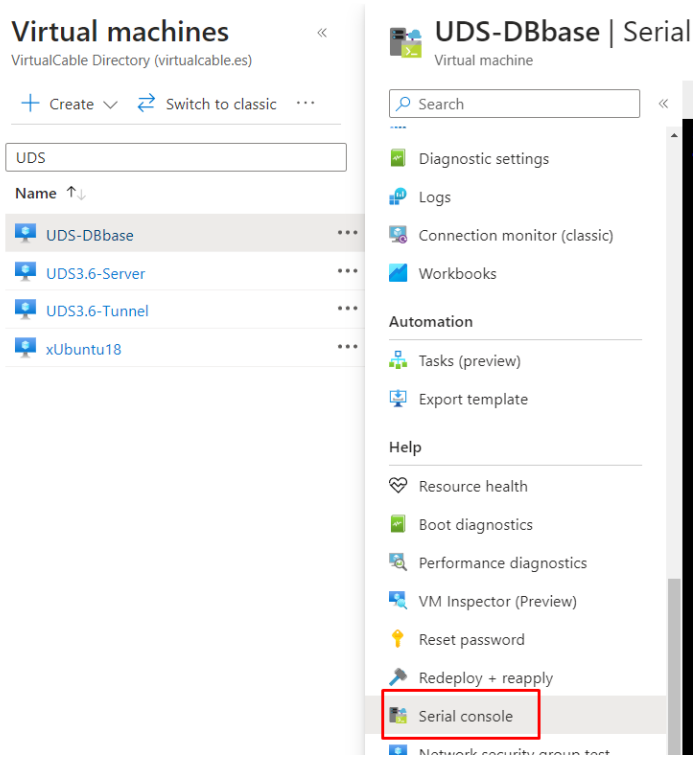
MySQL database configuration

If you are using the MySQL database provided by the VirtualCable team, it will already be pre-configured and you will only have to verify that you have IP connectivity (by default the network is configured by DHCP).

This MySQL server has created a DB instance ready to use with UDS Enterprise with the following data:

- **Instance name:** uds
- **User:** uds
- **Password:** uds

To confirm that the server has a valid IP assigned via DHCP you will have to connect via "***Serial console***". You will access the "***Virtual machines***" service, you will select the virtual machine that contains the MySQL DB and in the "***Support + troubleshooting***" menu you will select "***Serial console***".



NOTE:
The connection will take a few seconds to establish.Once connected, you must place the mouse on it and press the "enter" key.

You will validate on the MySQL server with the following credentials:

- **User:** root
- **Password:** uds

It will directly indicate the assigned IP address and relevant information about the security and configuration of the server itself.

```
* This machine is provided as a very basic mysql server, without any security ad
don.
* Change root password (ssh root login is ENABLED by default)
* Provide a custom name for this machine. you can use hostnamectl set-hostname -
-static YOUR_SERVER_NAME to do this.
* Protect access to this machine, because it contains defaults that are publicy
available, such as root password and database passwords.
* By default, cockpit is installed and available at https://SERVER_IP:9090. You
can uninstall it if desired with apt-get remove cockpit
* Consider updating the software (using apt, dselect, etc..) as a first step bef
ore using it in any environment (production or not)
* Update the keyboard layout if needed: use dpkg-reconfgure keyboard-configurati
on, then service keyboard-setup restart for this. Default keyboard lang is Spani
sh
* Set the timezone: use dpkg-reconfigure tzdata

* THIS MACHINE IS INTENDED ONLY TO BE USED IN AN INTERNAL AND TRUSTED LAN.

You will need to take securty actions (such as changing passwords, enabling fire
wall, etc...) in order to secure this machine.

Default mysql root password: Without password
Default uds database password: uds
Default listen address of mysql server: 0.0.0.0 (all addresses)

Default network mode: DHCP

Detected IP: 10.1.0.6
Cockpit interface is at https://10.1.0.6:9090
root@dbbroker-360:~#
```

If you want to confirm that the network configuration is correct, you can use the command:

ip a

```
root@dbbroker-360:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
t 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
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP grou
ult qlen 1000
    link/ether 60:45:bd:6c:3a:32 brd ff:ff:ff:ff:ff:ff
    inet 10.1.0.6/24 brd 10.1.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@dbbroker-360:~#
```

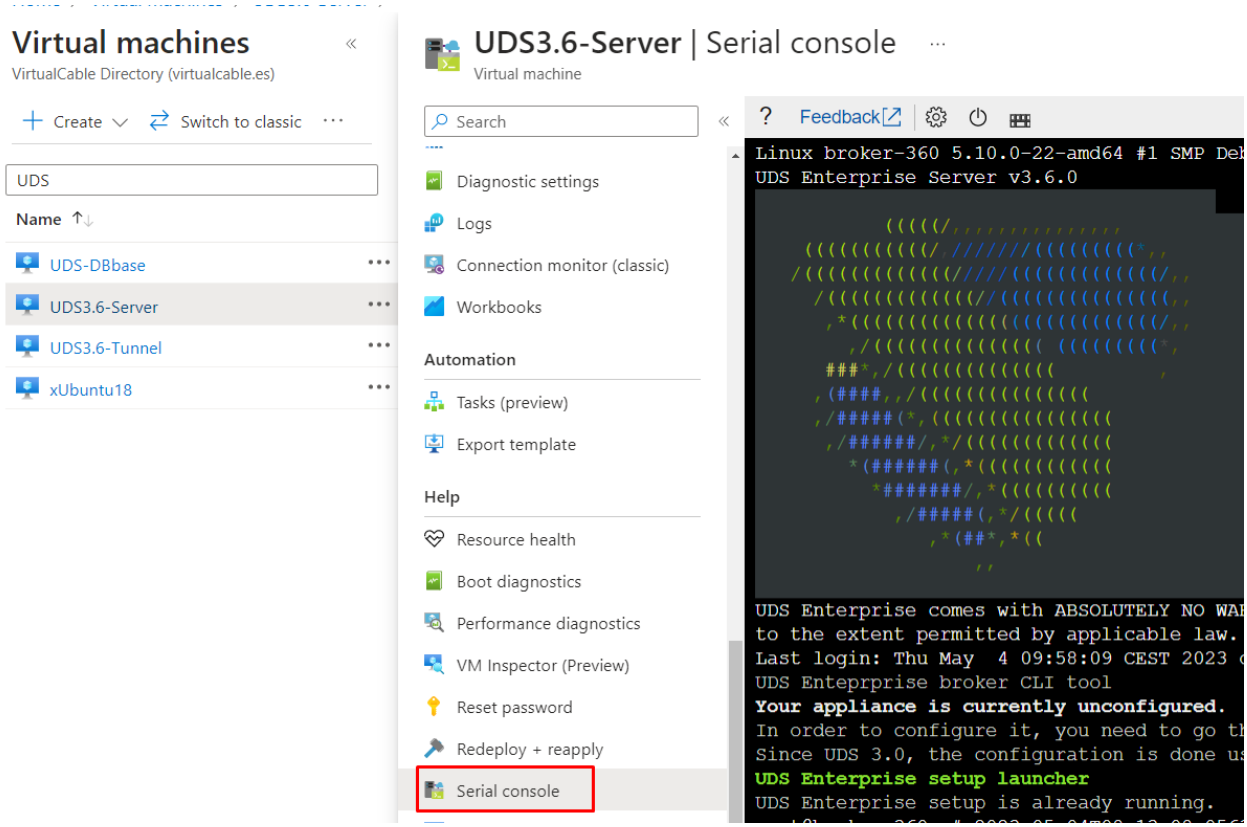
Once you confirm that you have network connectivity, you will proceed to configure the UDS Server component.

NOTE:
The use of fixed IPs is recommended for all UDS components

UDS Server Configuration

The UDS-Server component is the main element of the UDS environment. It has a configuration wizard accessible via web browser. Before accessing this configuration wizard you will need to confirm that the server has been assigned an IP address.

To confirm that the server has a valid IP assigned via DHCP, you will have to connect via "***Serial console***". You will access the "***Virtual machines***" service, you will select the virtual machine that contains the UDS server, and in the "***Support + troubleshooting***" menu you will select "***Serial console***".

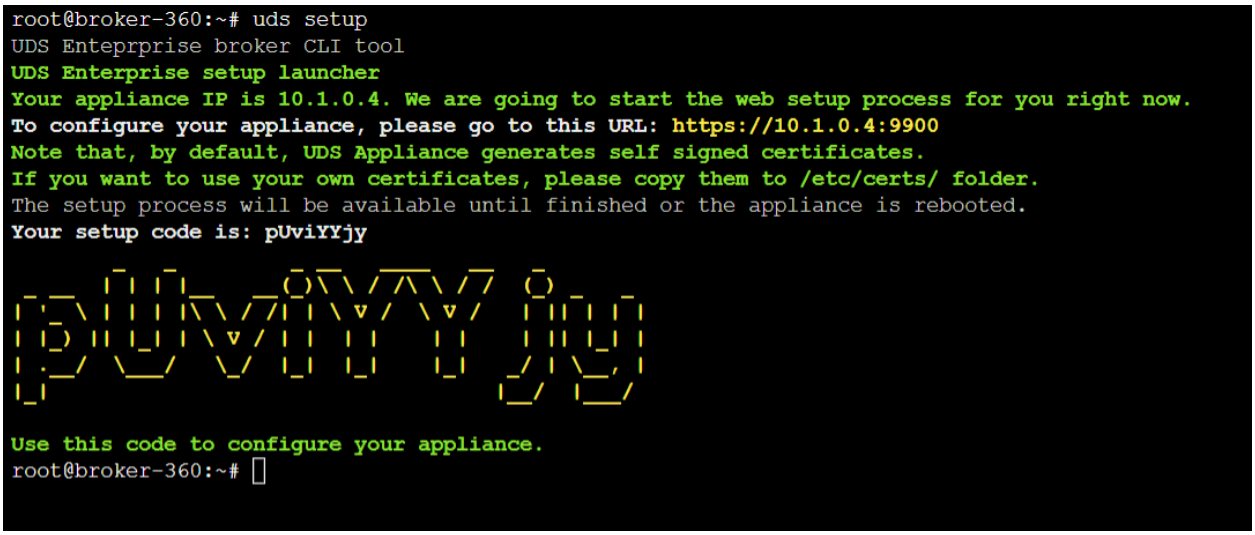


NOTE:
The connection will take a few seconds to establish. Once connected, you must place the mouse on it and press the "enter" key.

You will validate on the UDS server with the following credentials:

- **User:** root
- **Password:** uds

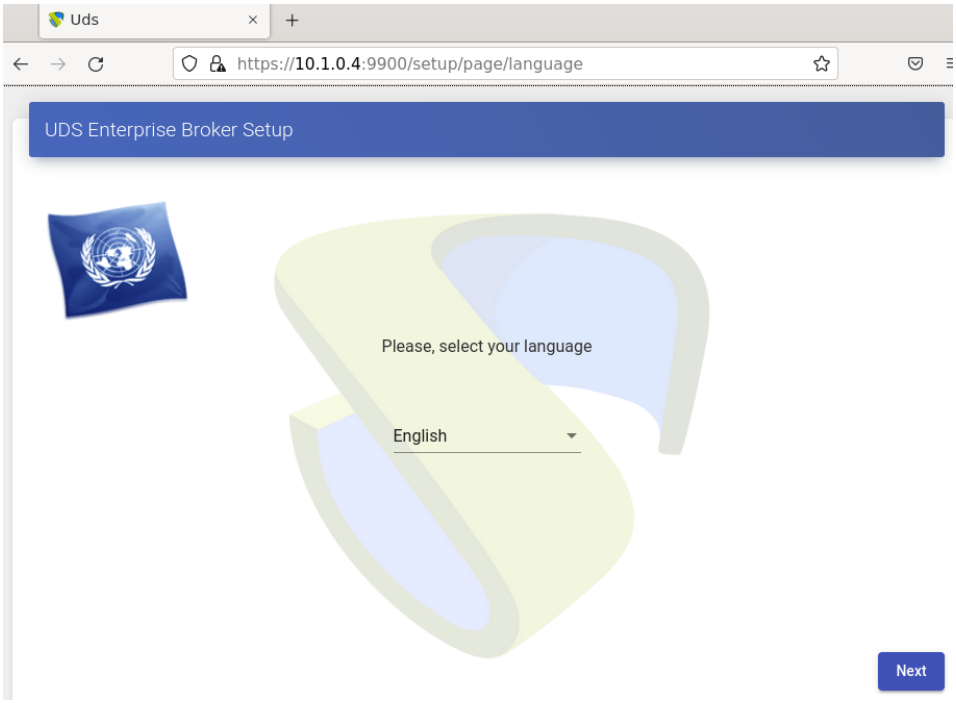
It will directly indicate the assigned IP address and information to access the server configuration wizard (through port 9900).



If the server has not been assigned an IP address automatically, you must do so through the command: **uds ip**

NOTE:
For more information on the uds ip command, consult the UDS Enterprise 3.6 Installation, administration and user manual in the Documentation section of our website.

You will need a virtual machine within the Azure environment and in the UDS server subnet to access the server configuration wizard via web browser. In the browser, you must enter the IP address of the UDS server and port 9900.



Here you will indicate all the necessary data (IP data, serial to activate the subscription, credentials, etc ...) to configure the server.

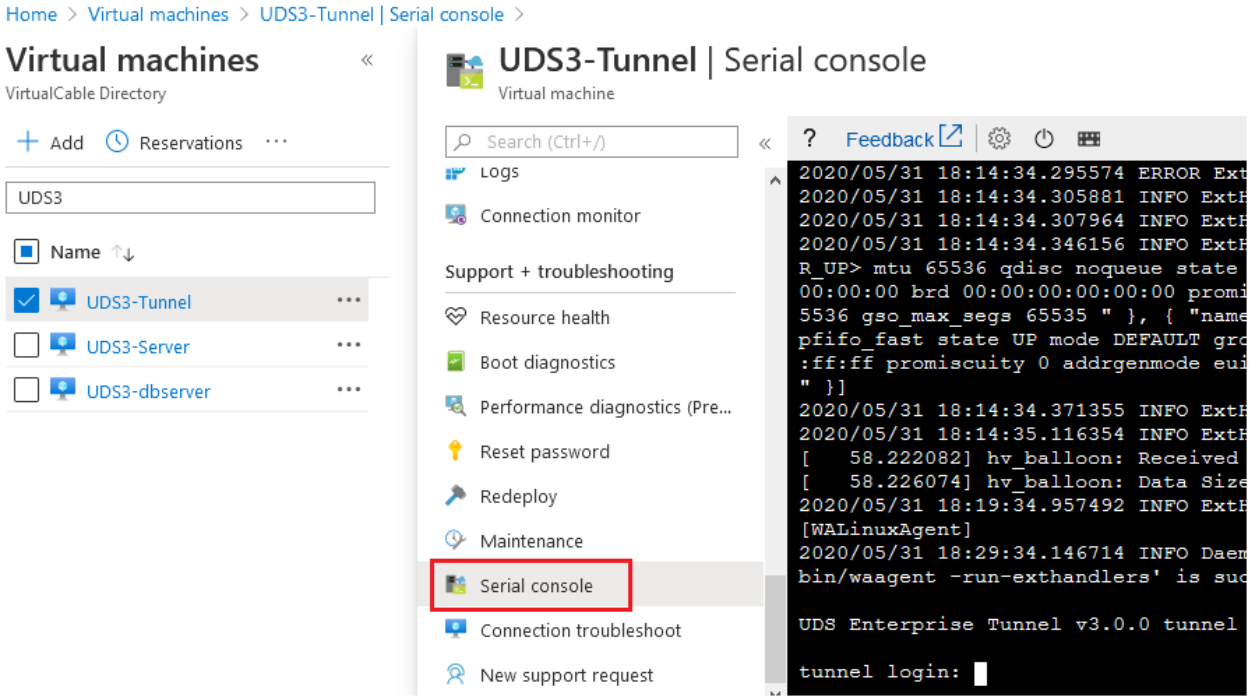
For more information on the UDS server configuration, consult the UDS Enterprise 3.5 installation, administration and user manual.

NOTE:
During the wizard configuration procedure, it will request the configuration data from the database server. In the case of using an external server, you must indicate the data of the previously configured MySQL server (IP address, instance, user and password).

○ UDS Tunnel Configuration

The UDS Tunnel component is the element that will provide you with secure access to virtual desktops through the Internet. It will also be responsible for establishing the HTML5 connection (HTM5 Transport for desktops and vApps). It has a configuration wizard accessible via web browser. Before accessing this configuration wizard you will need to confirm that the server has been assigned an IP address.

To confirm that the server has a valid IP address assigned via DHCP, you will have to connect via "***Serial console***". You will access the "***Virtual machines***" service, you will select the virtual machine that contains the UDS Tunnel server and in the "***Support + troubleshooting***" menu you will select "***Serial console***".

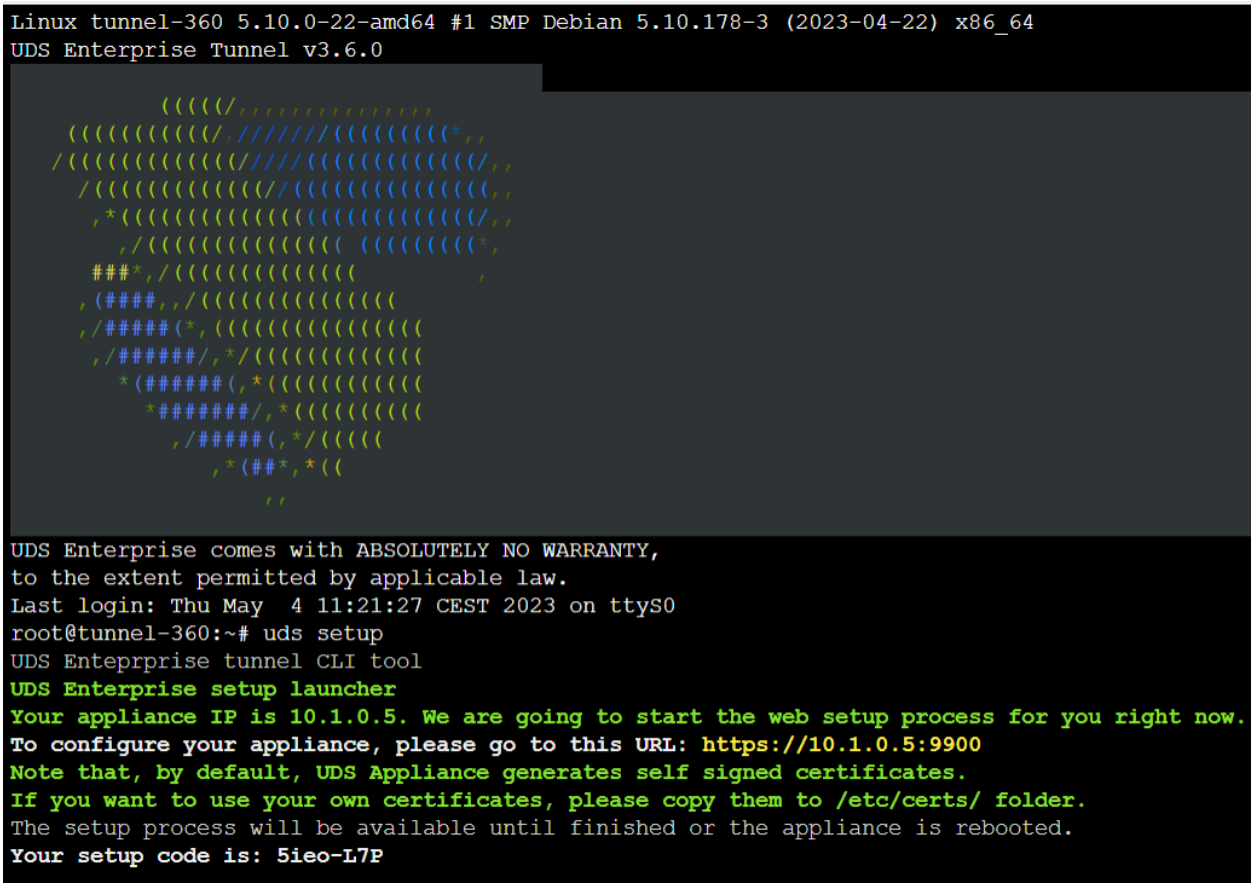


NOTE:
The connection will take a few seconds to establish. Once connected, you must place the mouse on it and press the "enter" key.

You will validate on the UDS Tunnel server with the following credentials:

- **User:** root
- **Password:** uds

It will directly indicate the assigned IP address and information to access the server configuration wizard (through port 9900):



If the server has not been assigned an IP address, you should automatically do so through the command: **uds ip**

In order for the UDS Tunnel to trust the self-signed certificate of the UDS Server and to be able to validate the connection, we will have to use the "uds trust" command.

```
root@tunnel-360:~# uds trust -h
UDS Enteprprise tunnel CLI tool
usage: uds trust [-h] [-c] HOSTNAME PORT

positional arguments:
  HOSTNAME     Hostname of the remote server.
  PORT         Port of the remote server.

optional arguments:
  -h, --help   show this help message and exit
  -c, --chain  Trust the certificate full chain.
root@tunnel-360:~#
```

```
root@tunnel-360:~# uds trust 10.1.0.4 443
UDS Enteprprise tunnel CLI tool
Reading certificate from server 10.1.0.4:443 done
Certificate name: uds
Valid from: 2023-05-03 13:45:58
Valid until: 2033-04-30 13:45:58
Fingerprint: 45c4057ccfb7868c46a7a380d14eb7469154aae7ba01eac02e3fbd6e6b3158b5
Issuer: CN=uds,O=UDS Enterprise Self Signed Certificate,L=Madrid,ST=Madrid,C=ES
Subject: CN=uds,O=UDS Enterprise Self Signed Certificate,L=Madrid,ST=Madrid,C=ES
Serial number: 964377329676414671361997497992543456138676985 68
Self signed: Yes
Writing certificate to trust file (/usr/local/share/ca-certificates/uds.crt)... done
Ensuring that the name uds resolves to the IP 10.1.0.4...
updating /etc/hosts... done
Updating trusted database...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

done.
done.
Trusted certificate installed
```

Once done we will have to tell the UDS Tunnel the name of our UDS Server "uds"

```
Ensuring that the name uds resolves to the IP 10.1.0.4...
```

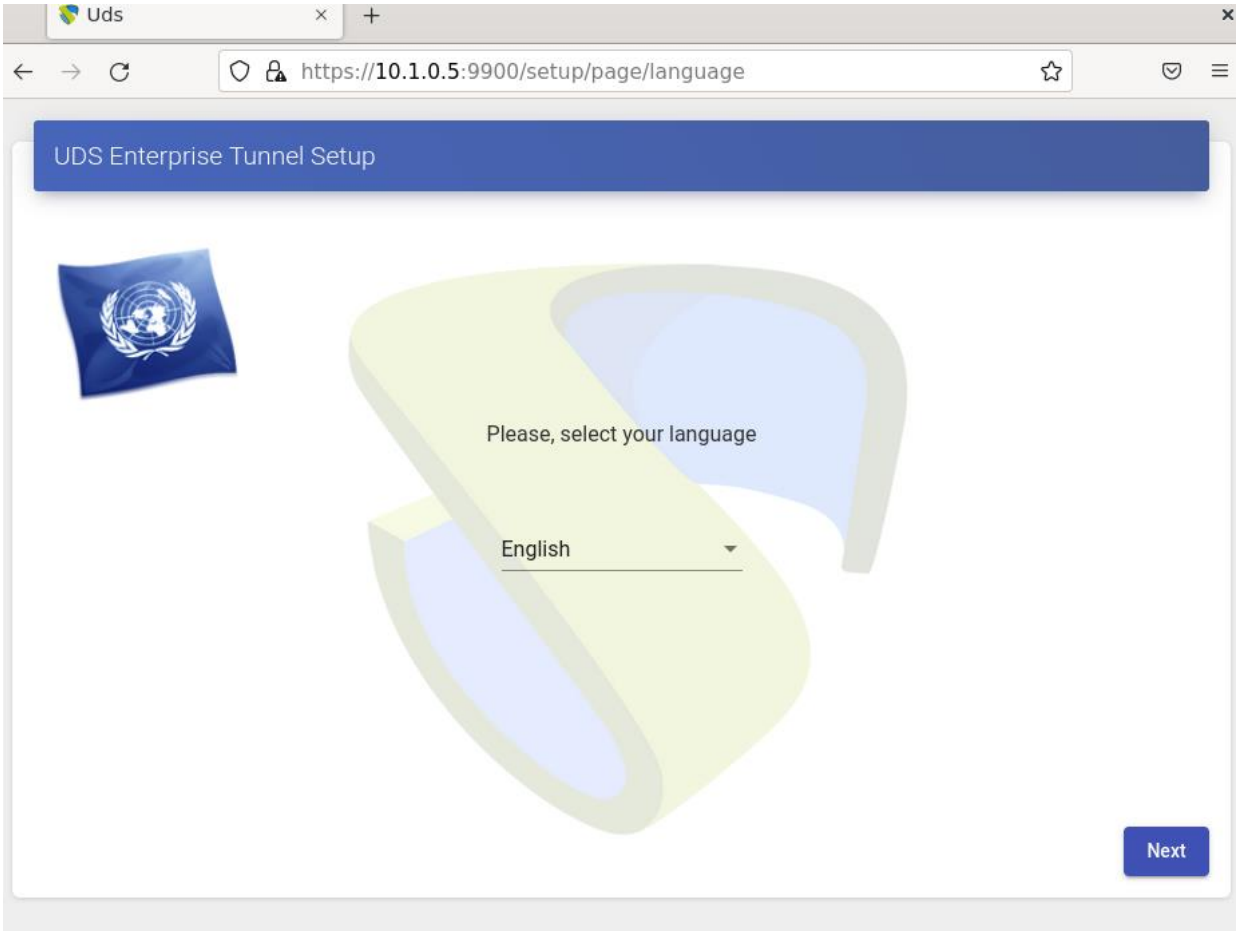
Editing the /etc/hosts file

```
# Autogenerated by UDS installer
127.0.0.1       localhost
127.0.1.1       tunnel-360.domain.local tunnel-360
10.1.0.4        uds
```

Once the process is done we can continue with the Tunnel configuration

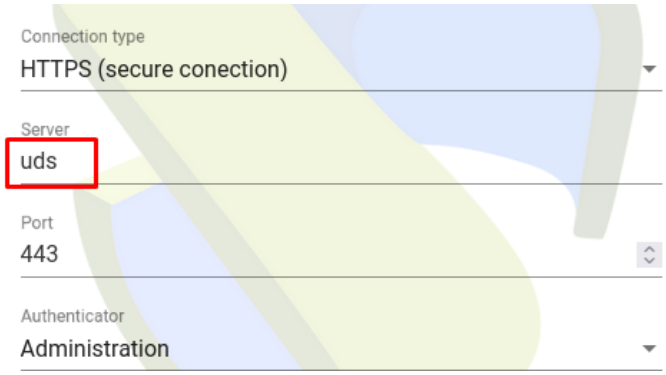
NOTE:
For more information on the uds ip command, consult the UDS Enterprise 3.6 installation, administration and user manual.

You will need a virtual machine within the Azure environment and in the subnet of the UDS Tunnel server to access the server configuration wizard via web browser. In the browser, you must indicate the IP address of the UDS Tunnel server and port 9900:



Here, you will indicate all the necessary data (IP data, credentials, certificates, etc...) to configure the server.

It will be necessary to take into account that in the connection section with the UDS Server, we will have to indicate the hostname of the Server indicated in the previous step.



For more information on the UDS Tunnel server configuration, see the UDS Enterprise 3.6 installation, administration and user manual.

NOTE:
During the wizard configuration procedure, it will request the UDS server connection data.

Create base machines or templates in Microsoft Azure

For UDS to deploy virtual desktops on the Azure platform, it is necessary to have a base machine or template on which the new UDS self-generated desktops will be based. This base machine can be deployed in different ways. Below you can find a procedure that will allow you to migrate templates already installed and configured on other virtual platforms (vSphere, KVM, etc...) to the Azure platform.

The first thing you should do is have a disk image of the base virtual machine in .vhd format. There are many free tools (such as StarWind converter, qemu-img, etc...) that allow you to convert disks of different formats (vmdk from VMware, qcow2/raw from KVM, etc...) to .vhd format. It is very important to keep in mind that the disk image needs to have the total size (Fixed Size). "Thin" (Dynamically Expanding) format is not supported.

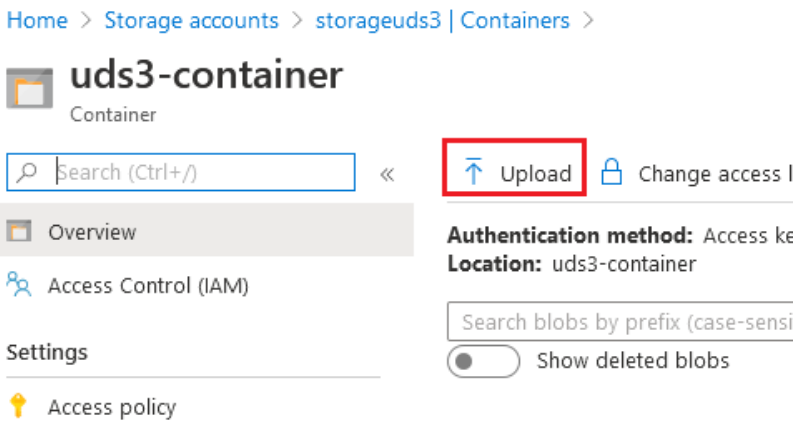
Before migrating the template machine, you must ensure that it will have a valid access mode (type SSH or RDP) to be able to access it once it is hosted on the Azure platform (this platform does not have a console to manage, configure and modify the machines). The base machine used in this example has access enabled/installed via SSH and RDP.

Another important point to keep in mind is the network configuration. It needs to be configured to take IP address via DHCP. In Windows O.S. templates, it is necessary to have the valid network driver installed to detect it on the Azure platform (if the machine is exported from a Hyper-V platform it will already be embedded).

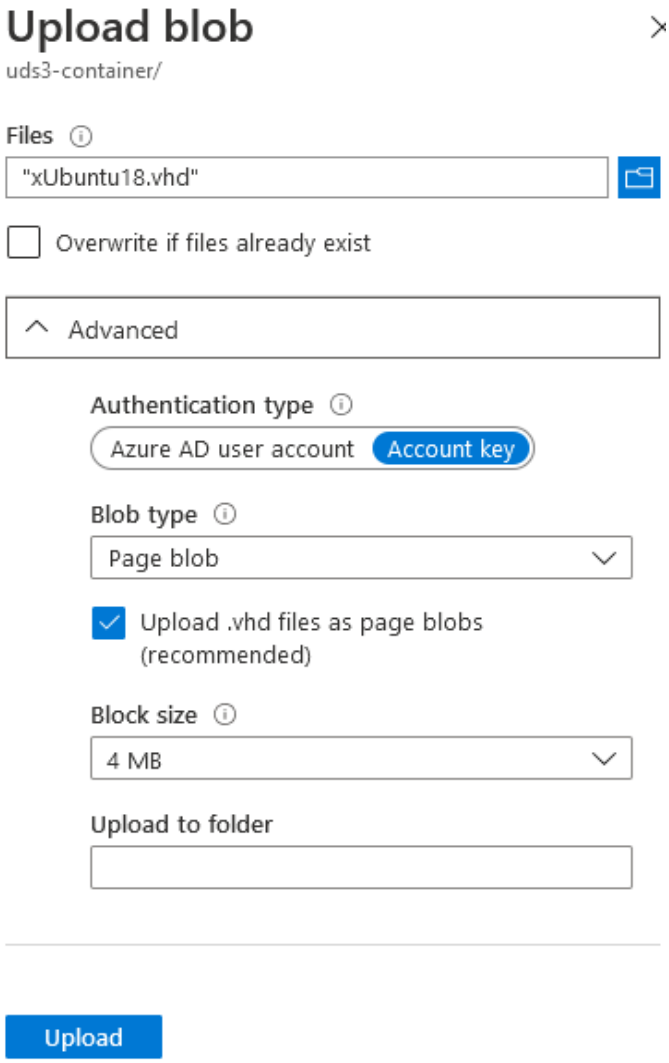
Once you have the disk image converted to the format supported by Azure (.vhd), you will proceed to upload it to the platform and deploy the new base machine. You will perform the following tasks described below (the procedure will be very similar to the one you used to deploy the UDS component Appliances):

- Upload .vhd disk image to a "Container"

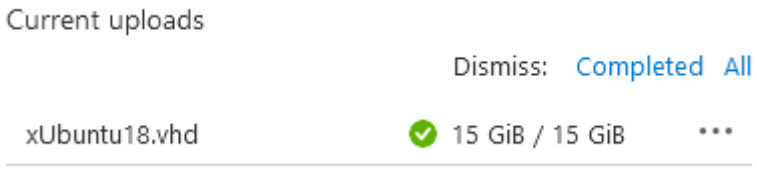
1. Access the "***Container***" ("***Storage accounts***", in the "***Blob service***" section, click on the existing "***Container***") and click on "***Upload***":



2. Indicate the disk image in the "***Files***" section. In "***Blob type***" select "***Page blob***" and click on "***Upload***".

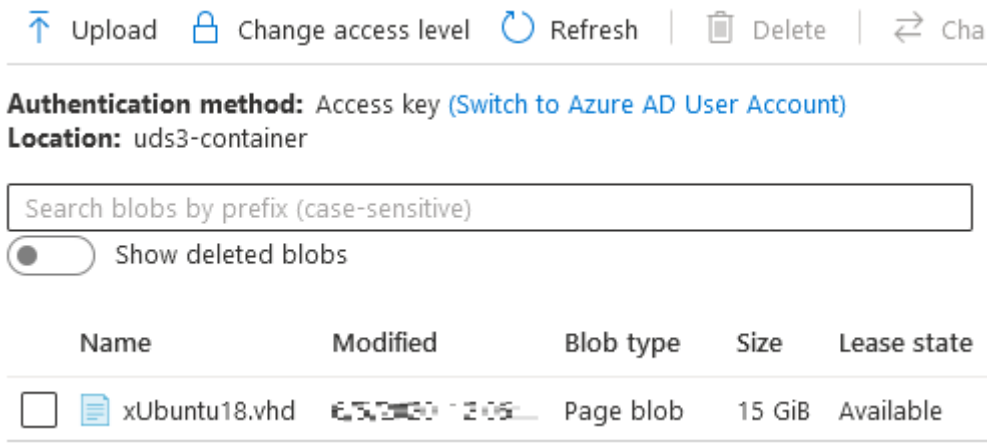

Upload blob
uds3-container/
Files
"xUbuntu18.vhd"
Overwrite if files already exist
Advanced
Authentication type
Azure AD user account
Account key
Blob type
Page blob
Upload .vhd files as page blobs (recommended)
Block size
4 MB
Upload to folder
Upload

3. The image will start to be imported and you will have to wait until the upload process finishes. Once finished, you will proceed to the next task: generating a disk from the image.



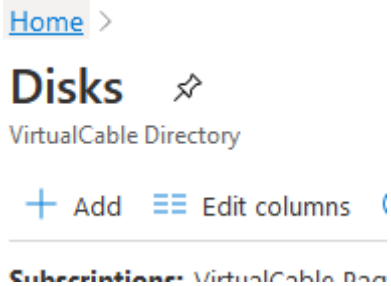
NOTE:
Depending on the size of the disk images and the speed of the connection, this process can take several minutes.

Finally, you will see that within the "***Container***" you will have available the disk image of our base machine/template.

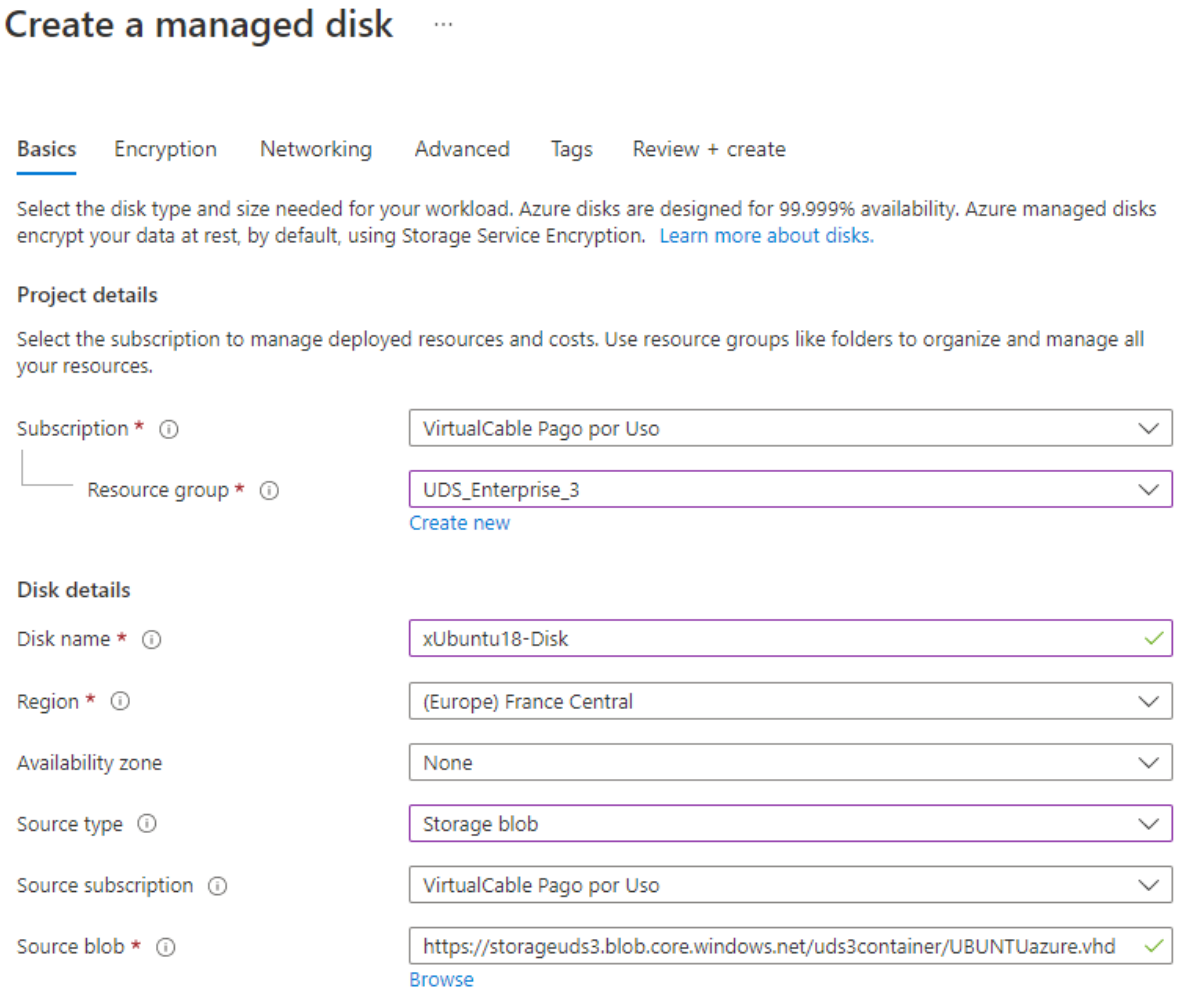


- Virtual disk creation

1. Access the "***Disk***" service and click on "***Add***" to add a new disk.

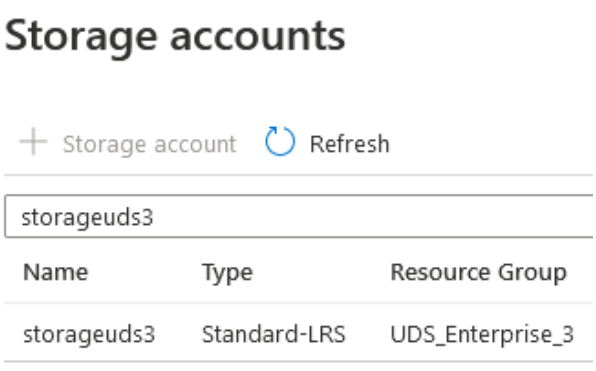


2. In the "***Basics***" section, select the subscription, the "***Resource group***" on which it will be registered, indicate a descriptive name for the element, the "***Region***", and in "***Source type***" indicate "***Storage blob***":

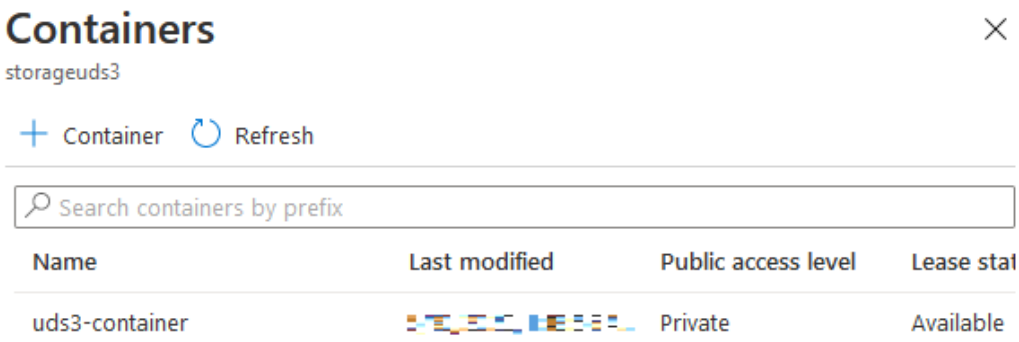


In "***Source blob***" click on "***Browse***" to select the previously imported disc.

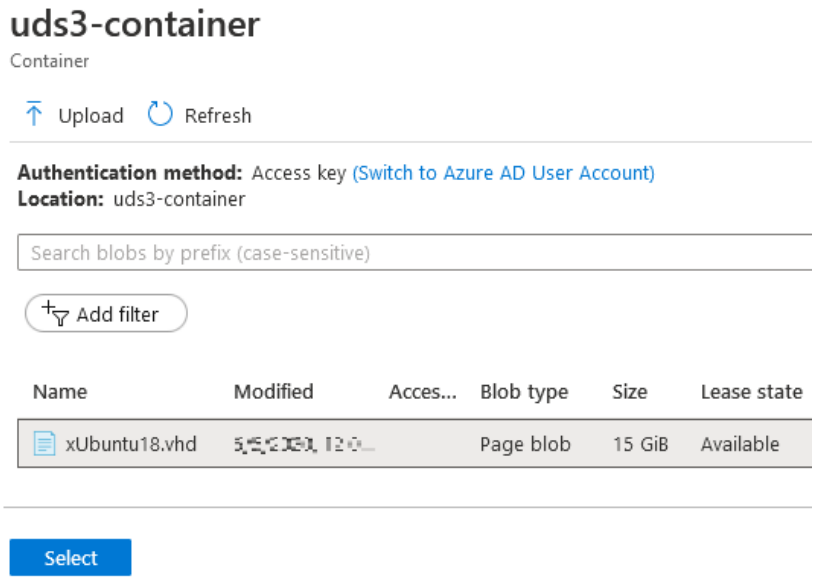
You must select the "***Storage accounts***" that contains the disk images:



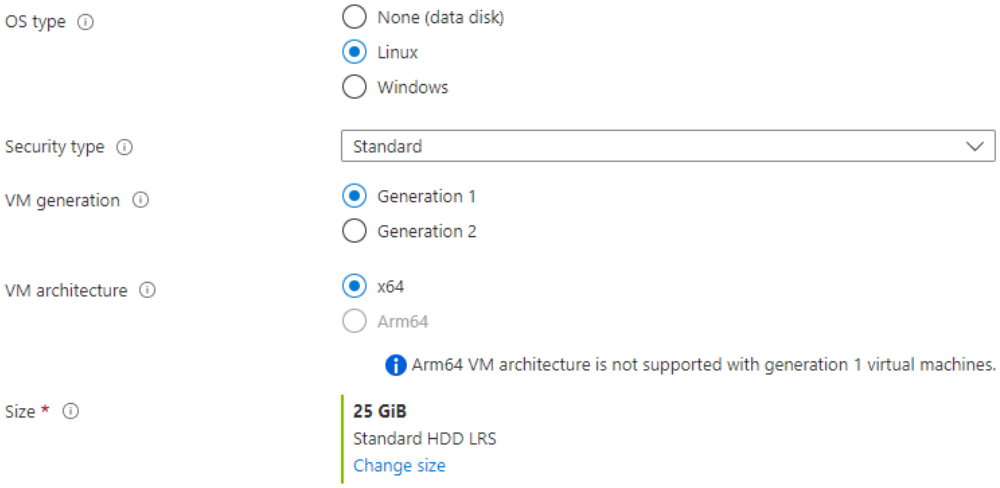
Once inside, you select the "***Container***" previously created.



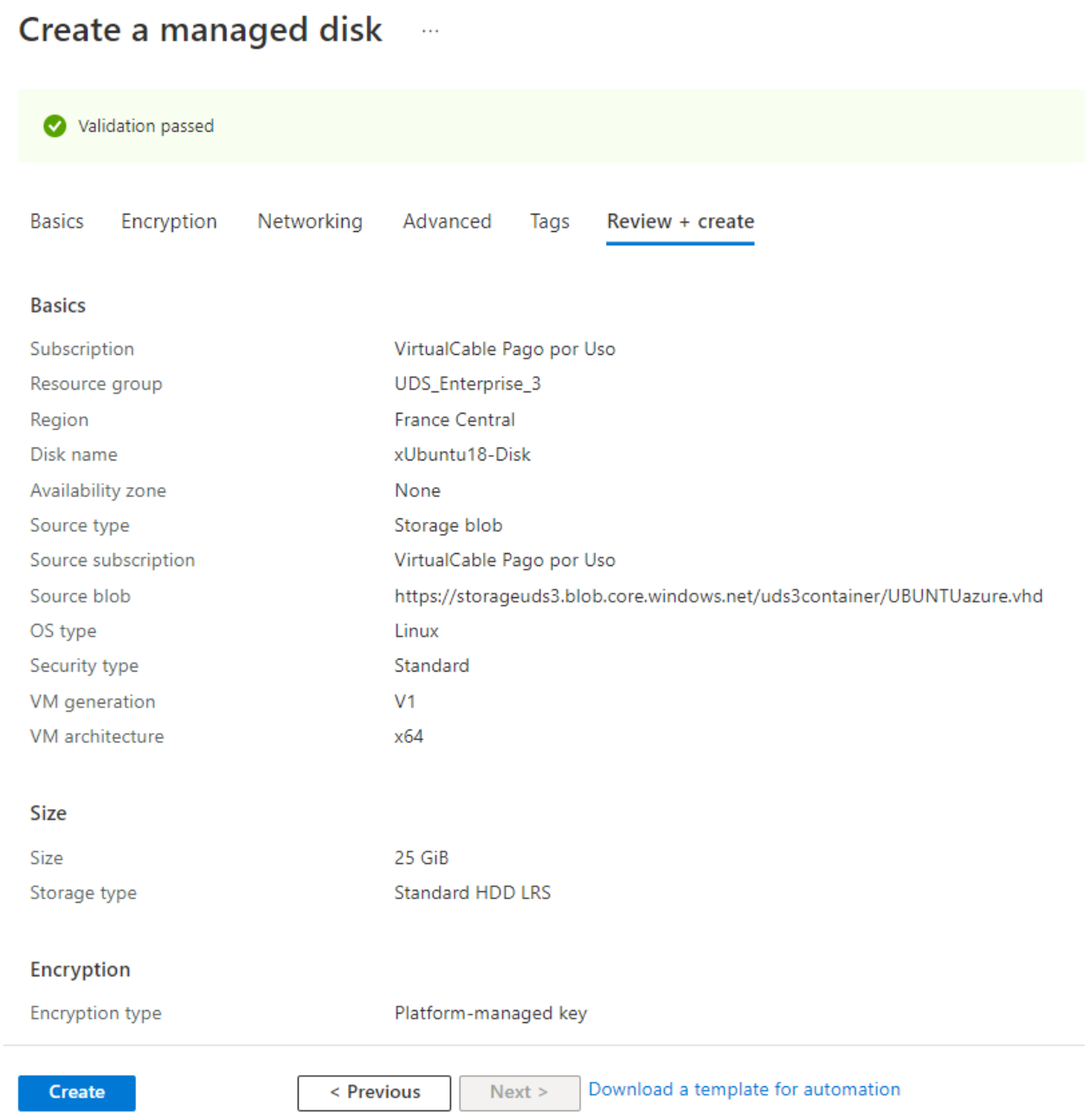
Finally, select the imported image in the previous step (in this case for the UDS-Server) and click on "***Select***".



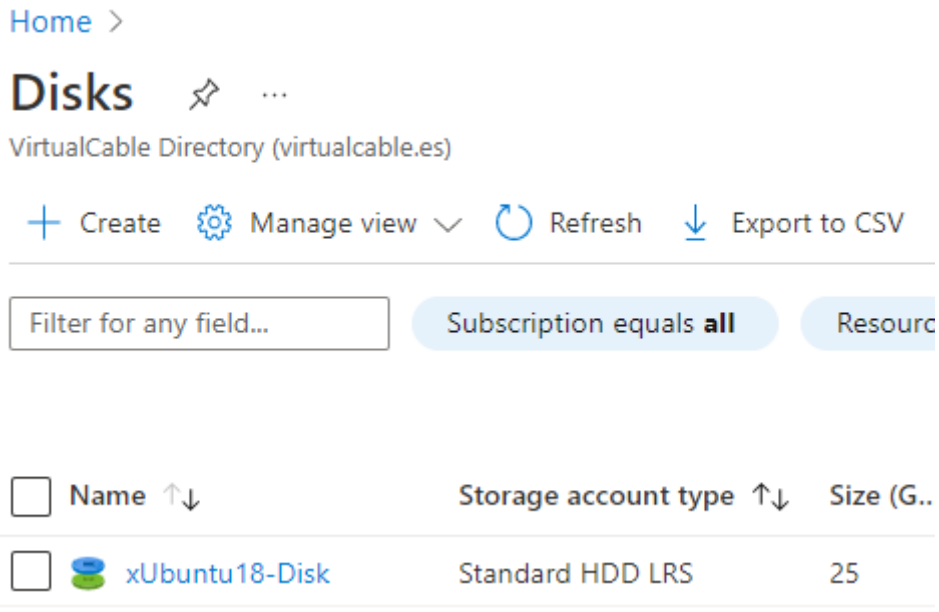
In "***OS type***" you will indicate the O.S. In "***Size***", click on "***Change size***" and choose the resources of your template machine (in the size of the disk, indicate always 1 GB more).


OS type
None (data disk)
Linux
Windows
Security type
Standard
VM generation
Generation 1
Generation 2
VM architecture
x64
Arm64
Arm64 VM architecture is not supported with generation 1 virtual machines.
Size *
25 GiB
Standard HDD LRS
Change size

3. Click on "***Review + Create***", check that all the data is correct and click on "***Create***":



4. You will wait for the disk to be created and, once this task is finished, you will see that you have it available to later generate the template virtual machine.

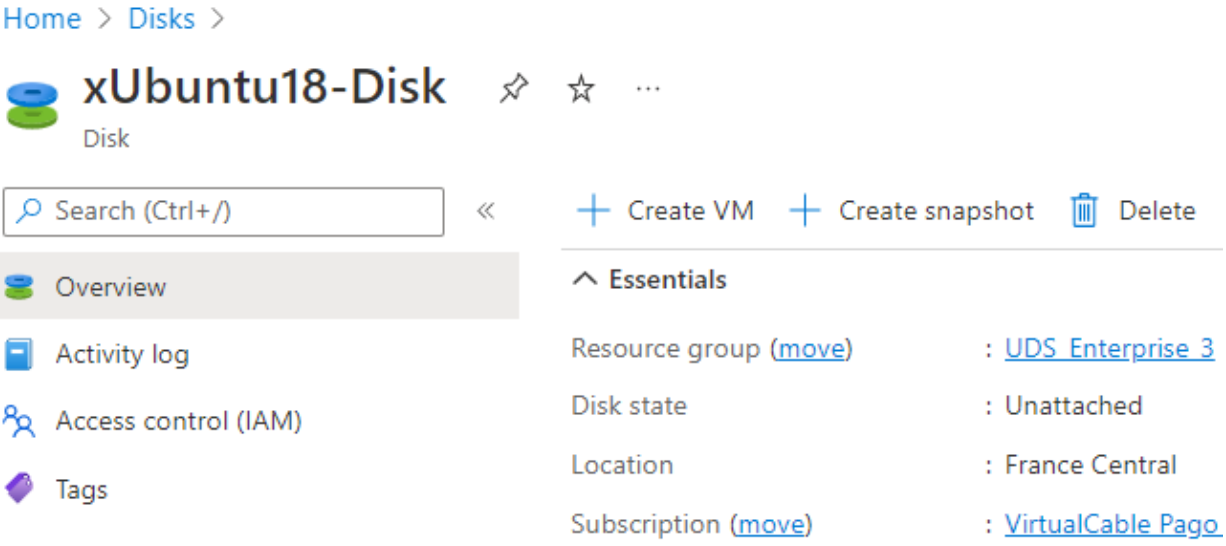


NOTE:
Once the disk is unfolded, you can delete the image of the "Container" to avoid it causing an unnecessary cost.

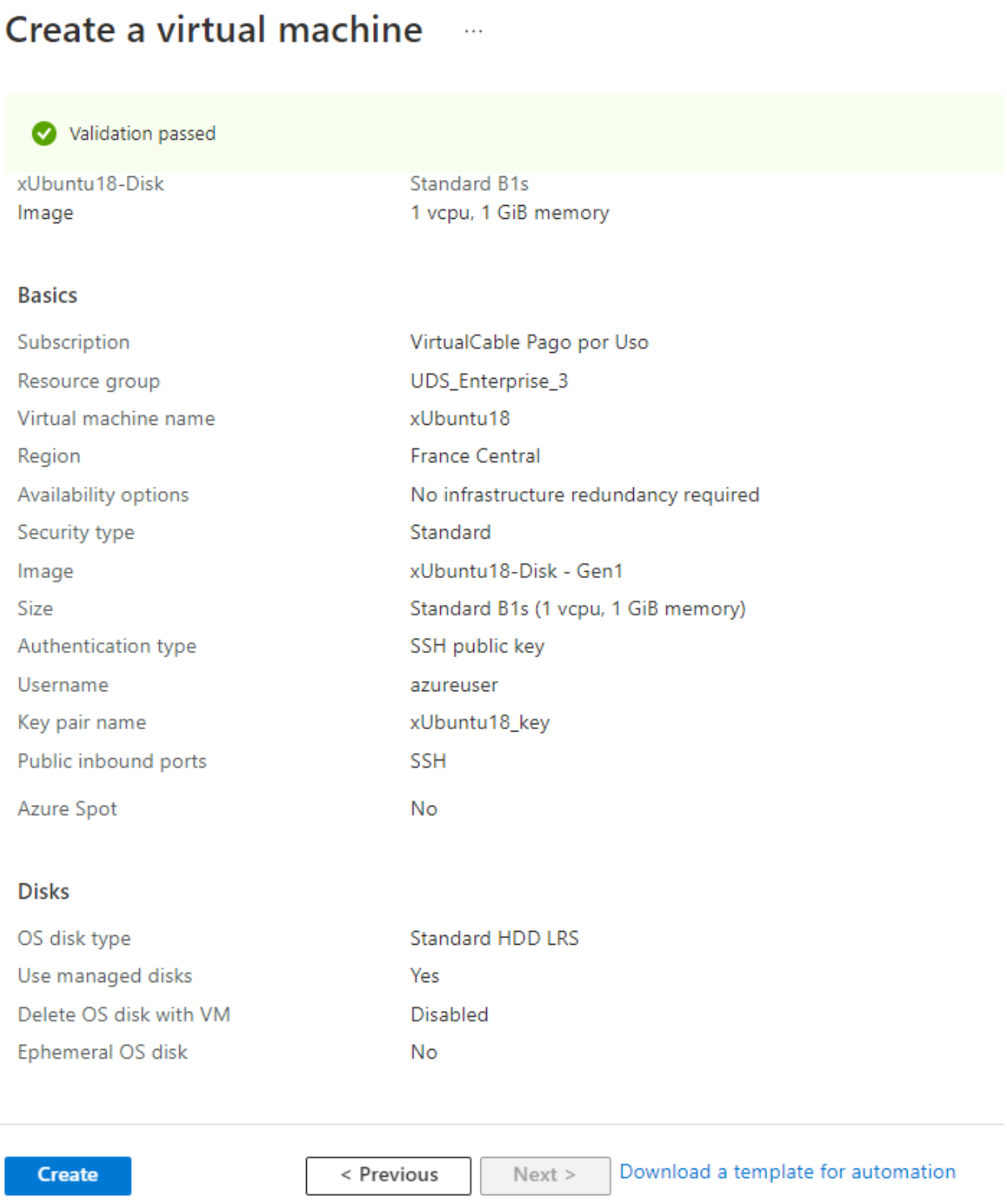
- Base machine creation

You will create the base machine/template from the disk itself:

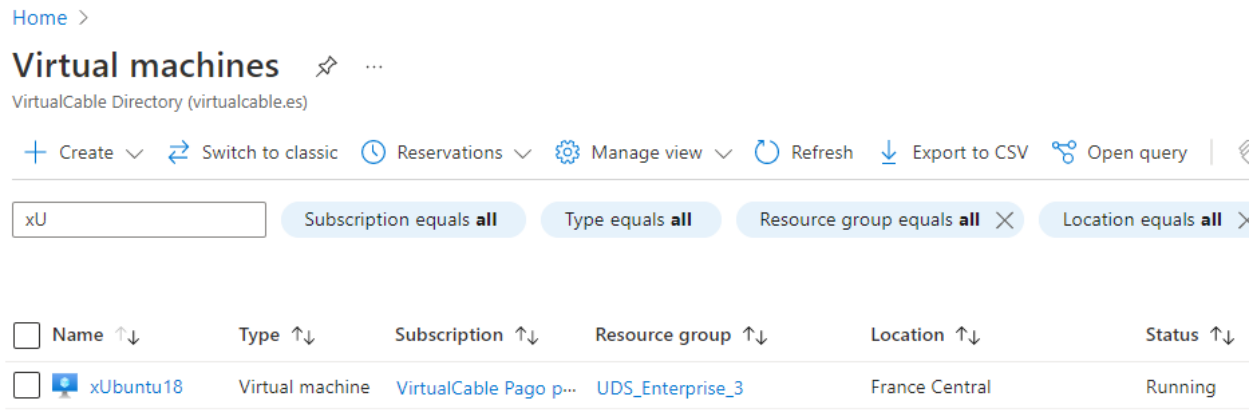
Select the previously created disk (from the "***Disk***" service) and click on "***Create VM***":


Home > Disks >
xUbuntu18-Disk
Disk
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Create VM
Create snapshot
Delete
Essentials
Resource group (move) : UDS_Enterprise_3
Disk state : Unattached
Location : France Central
Subscription (move) : VirtualCable Pago

In the virtual machine creation wizard, you will choose the options that best suit your needs. Once finished, you will check that all the configuration is correct and click on "*Create*"to create the virtual machine.



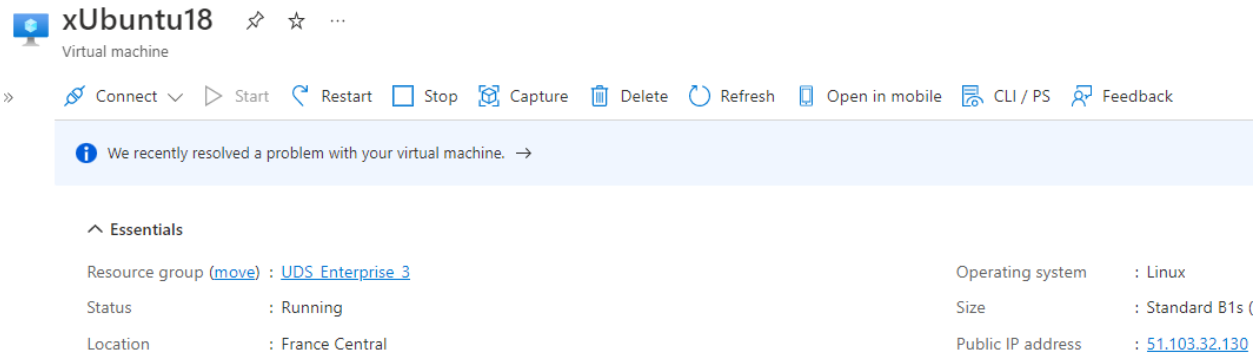
Once the process of creating the new VM is finished, verify that you already have the new machine within the "***Virtual machines***" service.



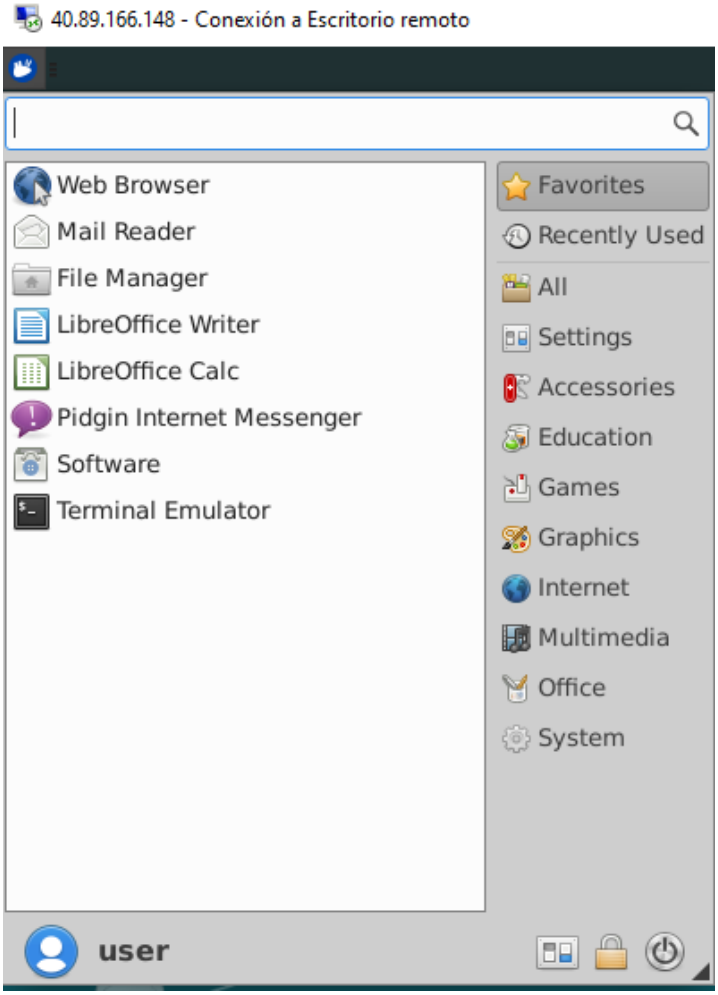
NOTE:
The template name cannot start with the letters "UDS". If you start with these letters, it will not be displayed or available in the UDS administration to be used as "base machine".
It is recommended to create a specific "Network Security Group" for this machine allowing ports to access it. For example, 22 (SSH) or RDP (3389).

- Base machine access and configuration

Once the virtual machine is deployed, you should be able to access it. To know what the public IP address of the machine is, you will click on it in the "***Virtual machines***" service. In the "***Overview***" section you will look at the value "***Public IP address***".



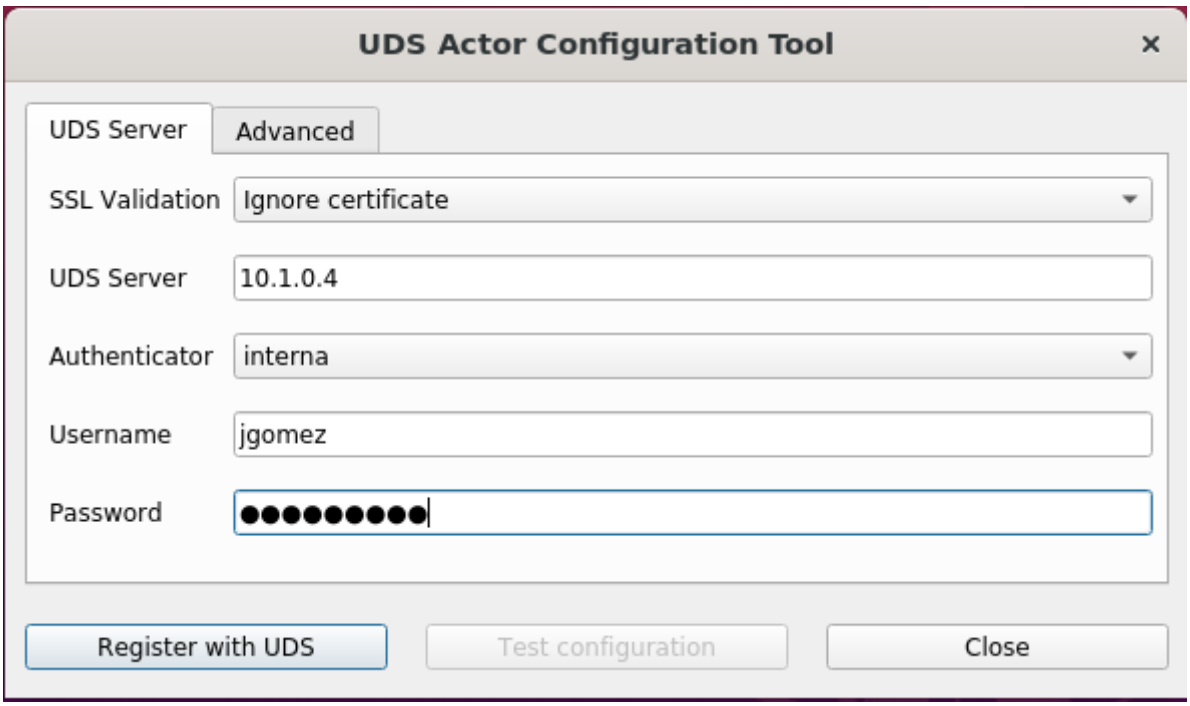
In this example, you will connect via RDP to access the template and install and configure the UDS Actor:



NOTE:
You can consult the UDS Enterprise installation, administration and user manual in the Documentation section of the UDS Enterprise website for more details on the installation of the UDS Actor.

During the configuration of the UDS Actor, you can indicate in the connection data against the UDS Server the local DNS address/name or also the public IP or DNS (in the case of using IP addresses instead of names, it is necessary to ensure that these addresses are not dynamic since they can change with the on/off of the virtual machines).

In this example, you will use the local IP address of the UDS Server:



NOTE:
If you want to view the configuration of the UDS Actor in an Ubuntu OS through RDP, you will have to execute the following command from a console:

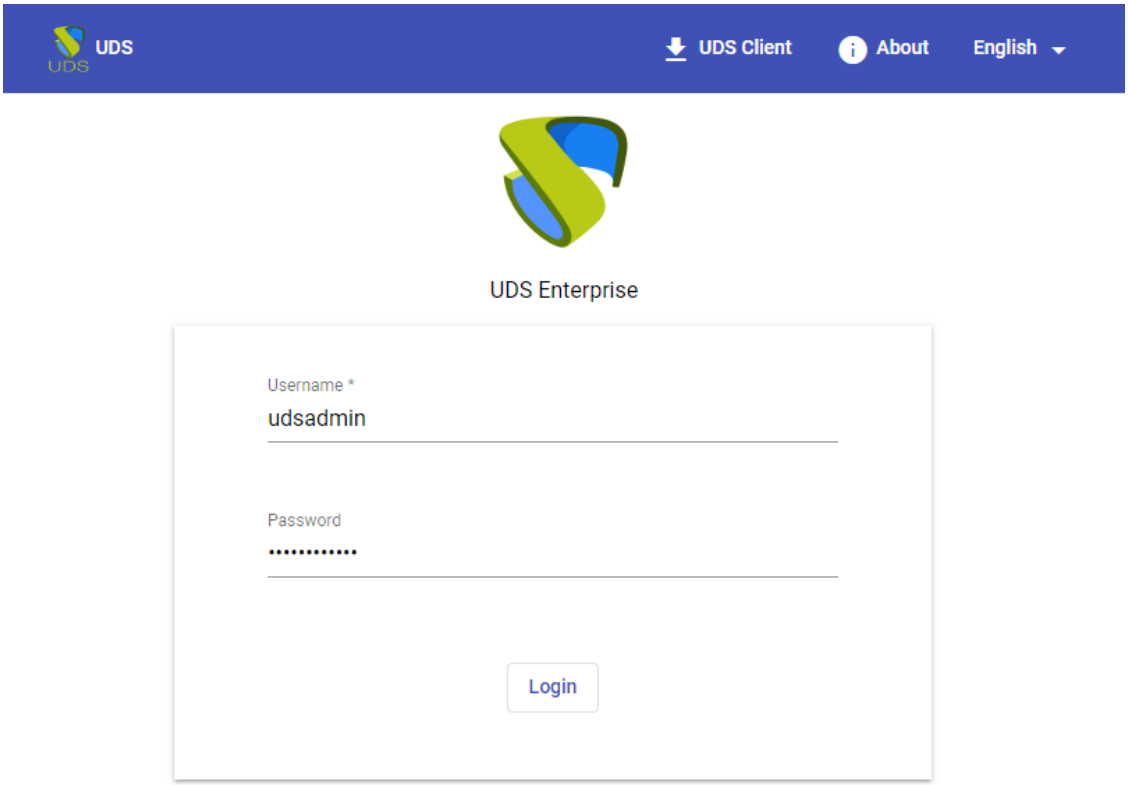
```
xhost + && sudo QT_X11_NO_MITSHM=1 /usr/sbin/UDSActorConfig
```

Once all these tasks are completed, you can now turn off the base or template machine to use it with UDS Enterprise (it is not possible to publish a service if the base or template machine is turned on).

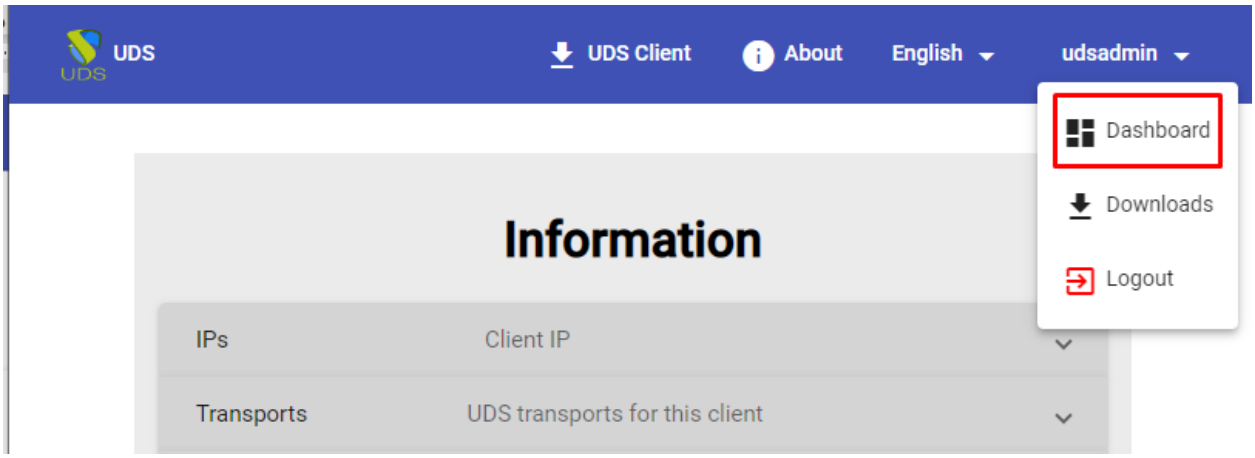
UDS Enterprise Administration

Azure service provider integration

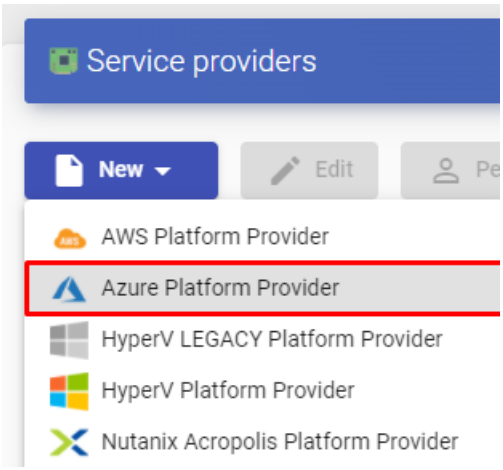
To integrate Azure as a UDS Enterprise service provider, you must access the UDS administration. In order to do this, access the public IP address or name of the UDS Server component via web browser using port 443 and validate yourself with an administrator user (in the first access, use the system administrator user indicated in the UDS server configuration wizard).



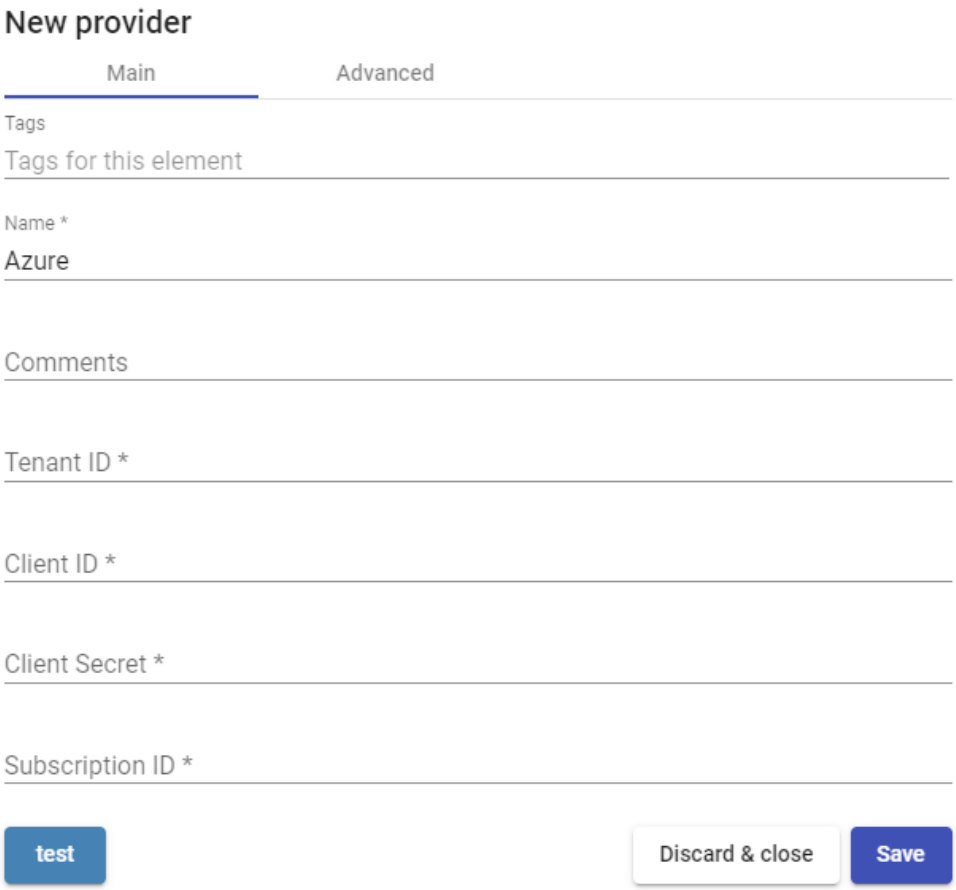
Once validated in the UDS login portal, access the "***Dashboard***" from the user menu.


UDS
UDS Client
About
English
udsadmin
Dashboard
Downloads
Logout
Information
IPs
Client IP
Transports
UDS transports for this client

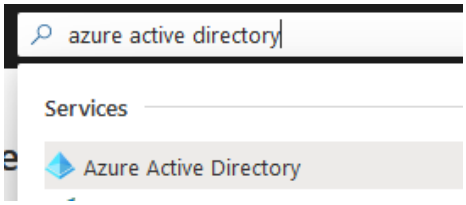
Within the UDS administration, access the "***Services***" menu and click on "***New***" to register a new "***Service provider***". Select "***Azure Platform Provider***".

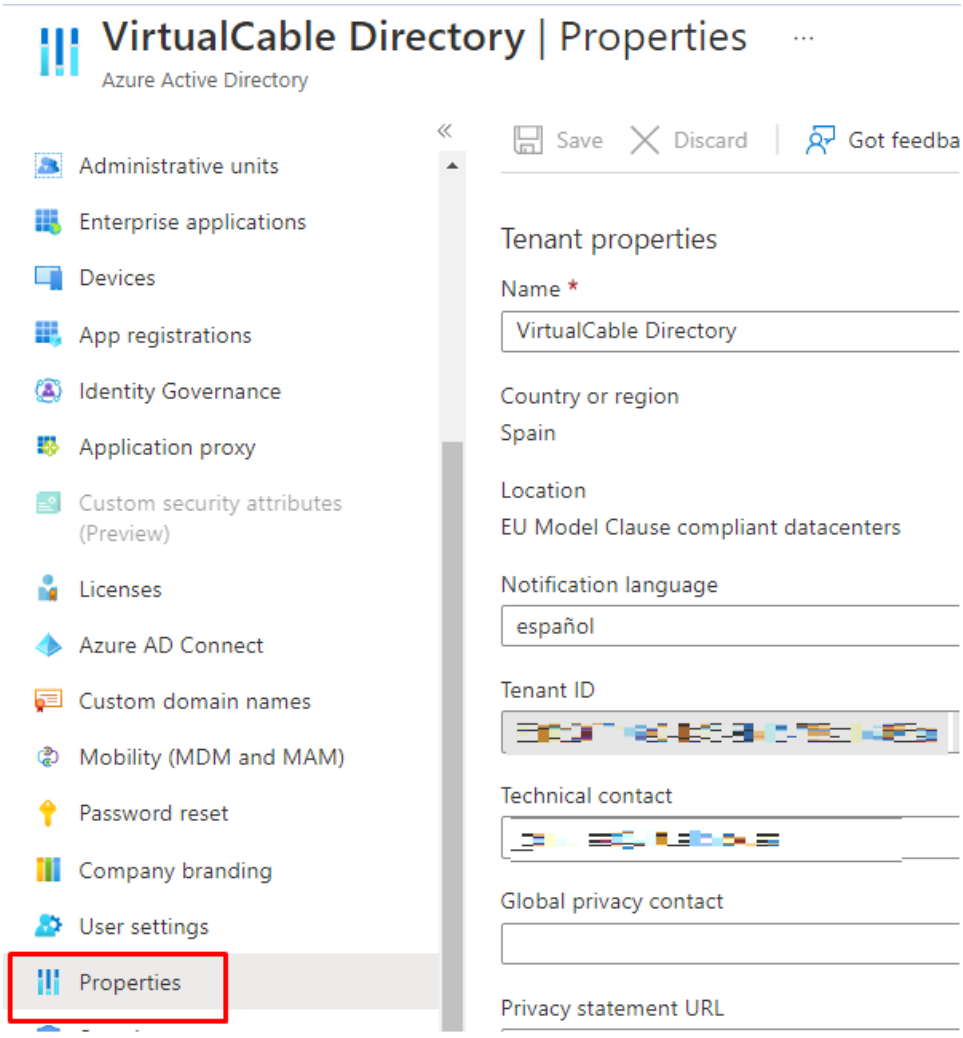


To make it possible for UDS to connect to the Azure platform, and to be able to automatically deploy virtual desktops, it will be necessary to indicate a descriptive name and a series of data that you can obtain directly from said platform:


New provider
Main
Advanced
Tags
Tags for this element
Name *
Azure
Comments
Tenant ID *
Client ID *
Client Secret *
Subscription ID *
test
Discard & close
Save

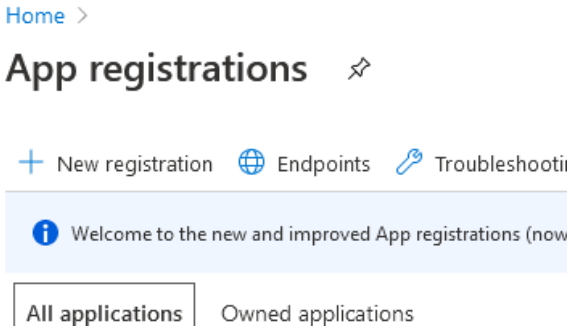
- **Tenant ID:** This value can be obtained from the "***Azure Active Directory***", "***Properties***", and "***Directory ID***".





- **Client ID:** To obtain this value, it will be necessary to create a new "***Application registration***" and give it permissions on our Azure subscription.

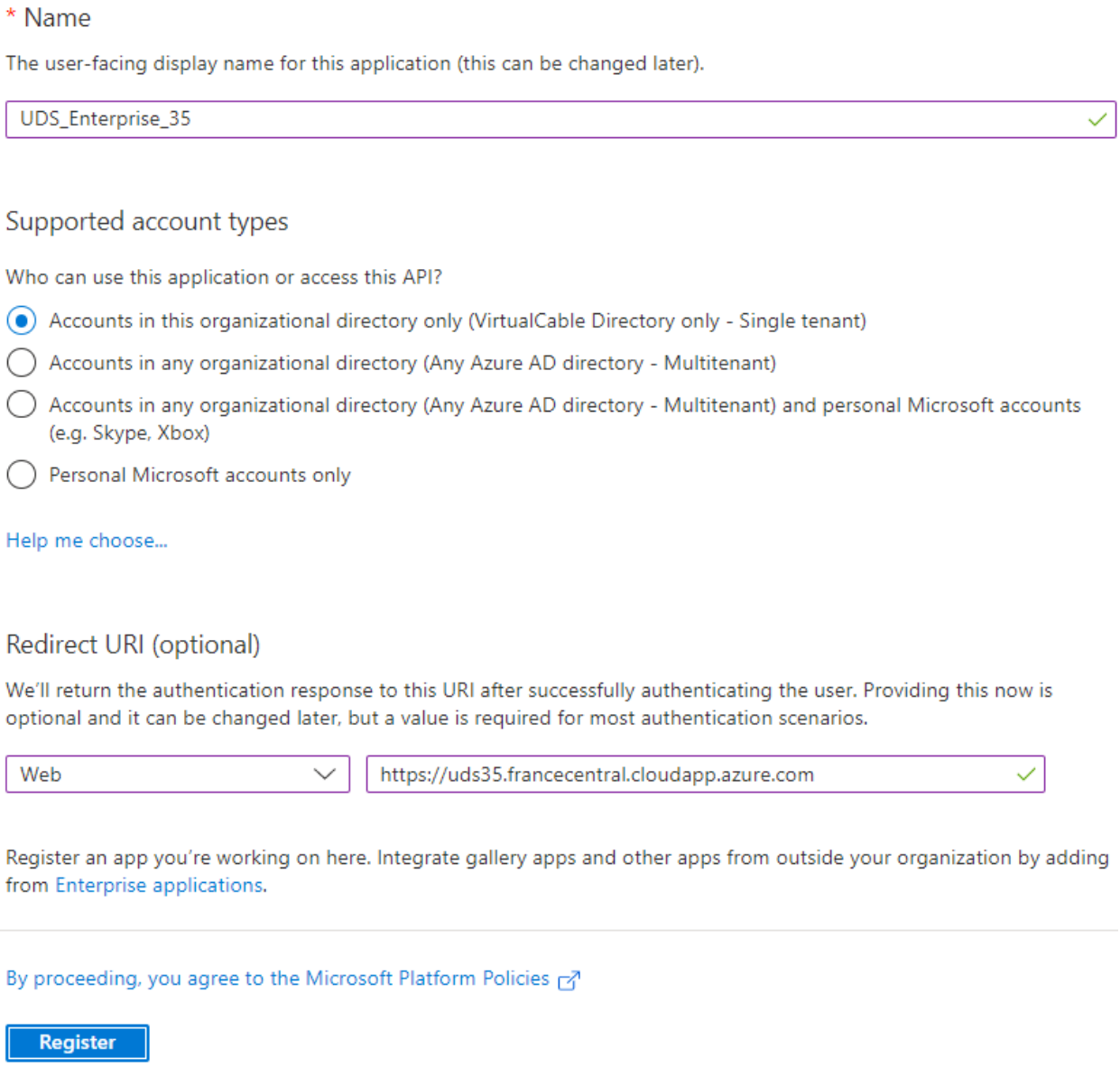
To register the application you will go to the service "***App registrations***" and click on "***New application registration***".



In the creation wizard, indicate a name, select a "***Supported account types***" and a "***Redirect URI***".

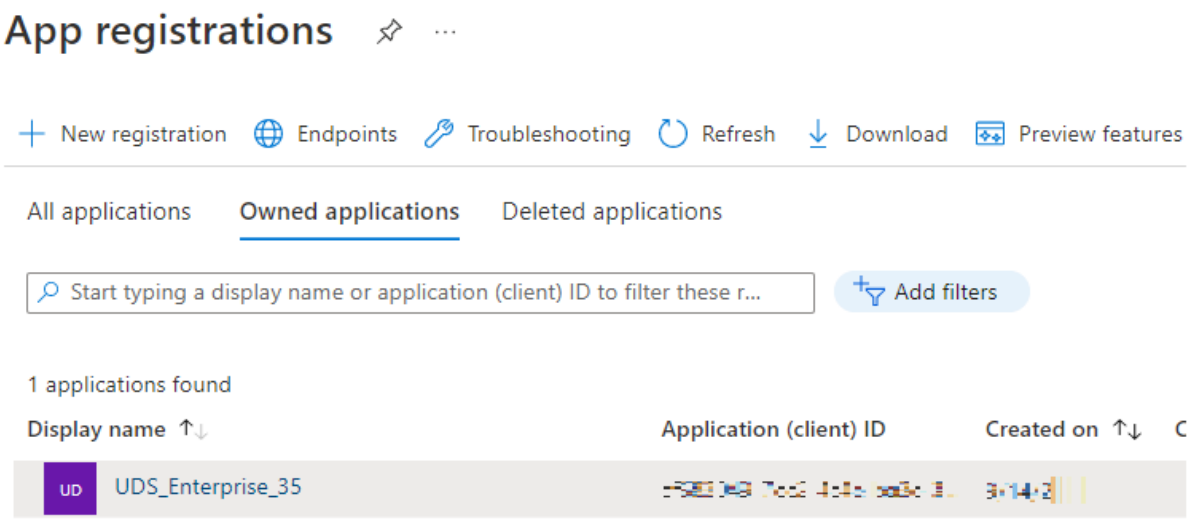
This last value will be extracted from the DNS name of the UDS server:

Once the data is indicated, click on "***Register***":



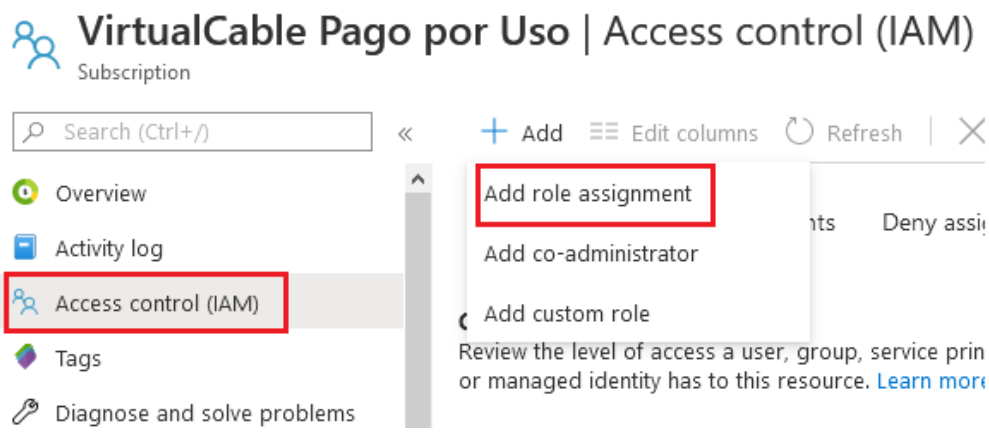
NOTA: El campo URI puede ser la dirección local del servidor UDS

Once registered, you will check that it has been correctly created:

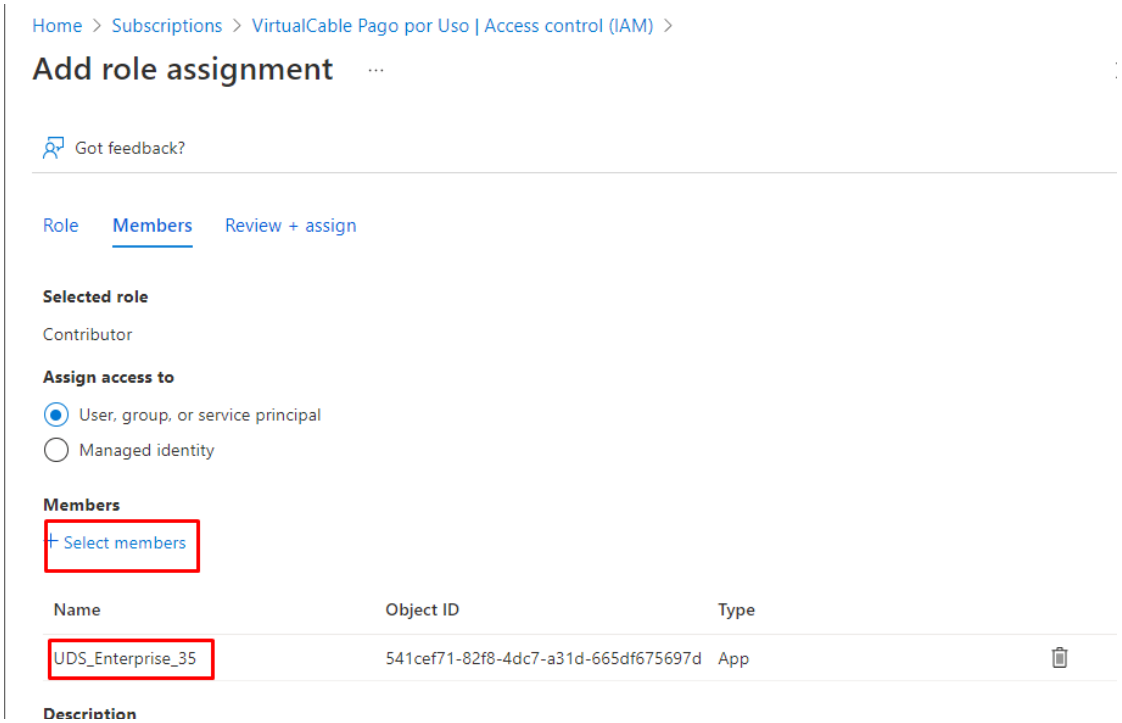


The column "***Application (client) ID***" will indicate the "***Client ID***" that you must copy to UDS.

To have a valid "***Client ID***" that can be used by UDS, you must give UDS permissions on your subscription. To do this, select your Azure subscription ("***Subscriptions***" service) and in the "***Access control (IAM)***" option, click on "***Add***", selecting "***Add custom role***".

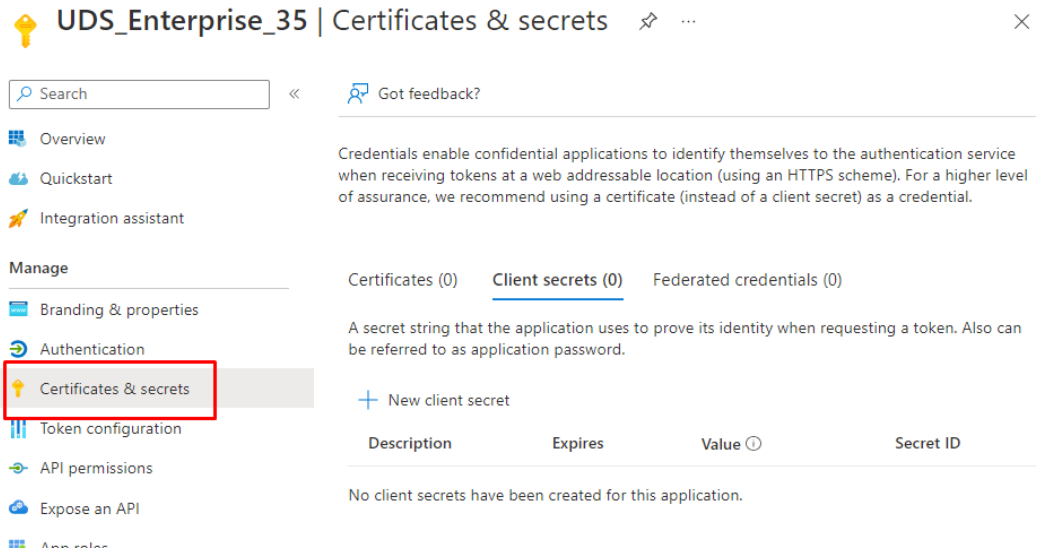


Indicate the role, in this case "***Contributor***", select that the access will be for "***Azure AD user, group, or service principal***" and write the start of the registered application name in the previous step. Once it appears as available, select it and click on "***Save***":

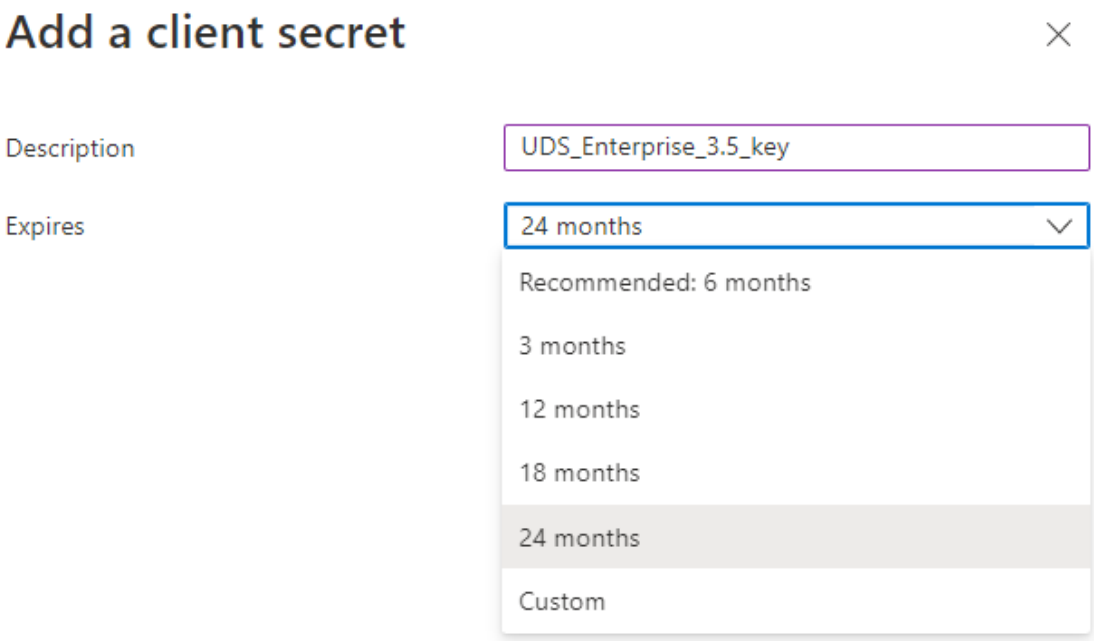


You can see the App with the assigned role:

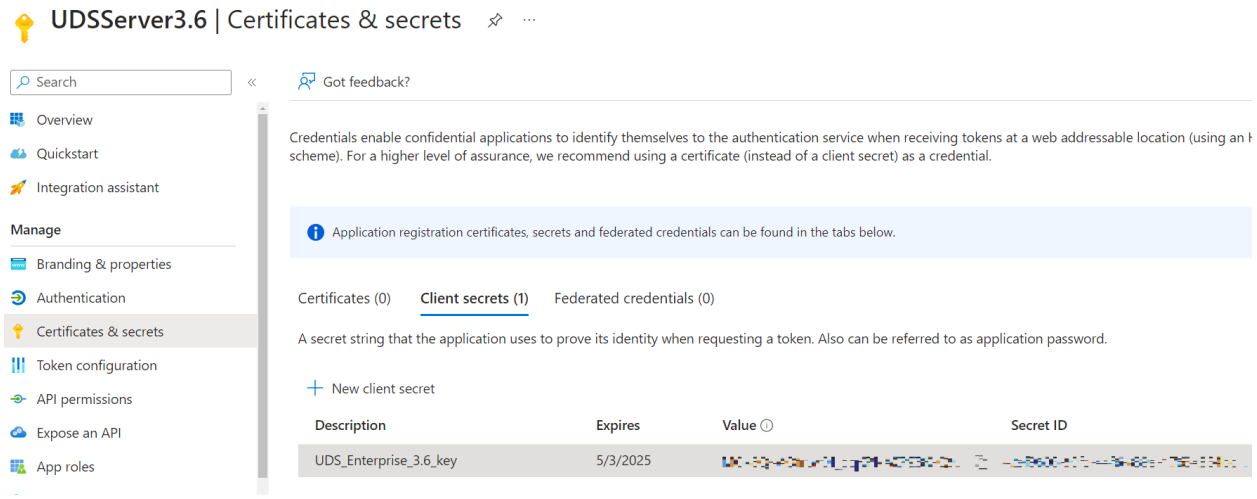
- **Client Secret:** This value will be obtained from the previously registered application. Click on it (in the "*App registrations*" service) and access "*Certificates & secrets*".



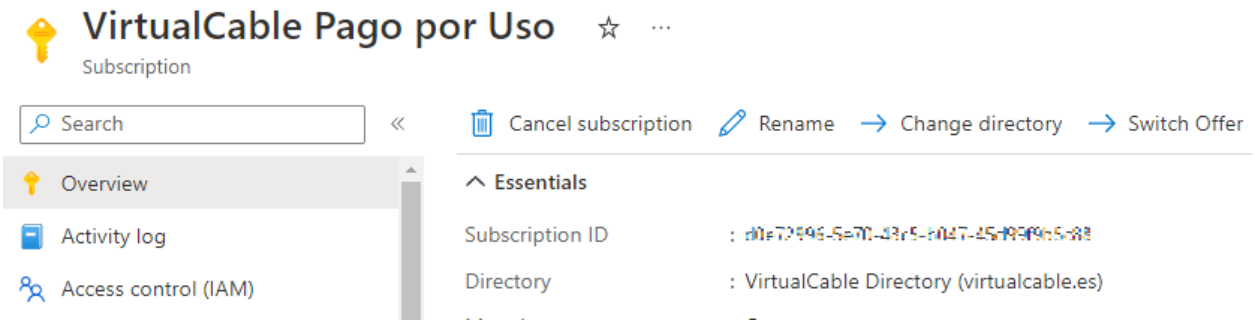
Within "*Certificates & secrets*" click on "*New client secret*". Add a description, select when it expires and click on "*Add*" to be able to copy the "*key*":



Once added, it will allow you to copy the value (once this window is closed, you will not be able to copy this value again, although you will be able to generate a new one if necessary). You will use this value as "*Client Secret*" in UDS.

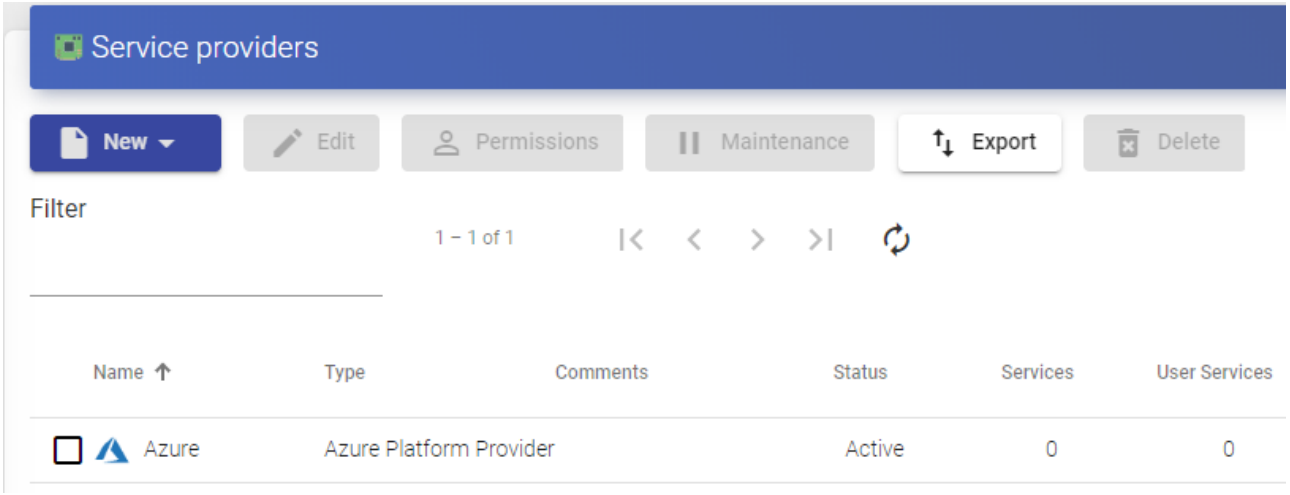


Subscription ID: To obtain this value, access the "***Subscriptions***" service. Identify your subscription and copy the value of "***Subscription ID***":



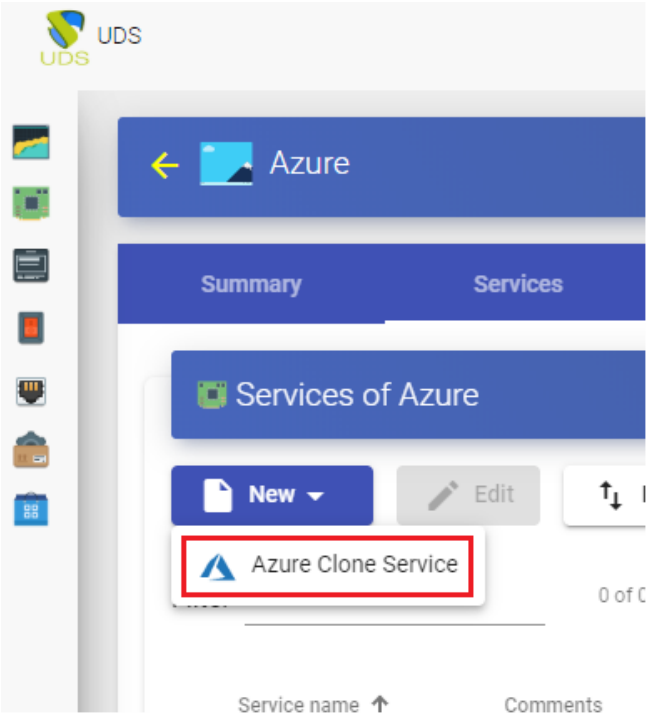
Once you have all the fields filled in, you will click on "***Test***" to verify that all the data is correct, and you will save the parameters.

NOTE:
Although the test does not come out correct, you can save the provider and thus not lose the indicated data. Subsequently, you can check which of the values is wrong (the "Client Secret" will only be visible during its creation).



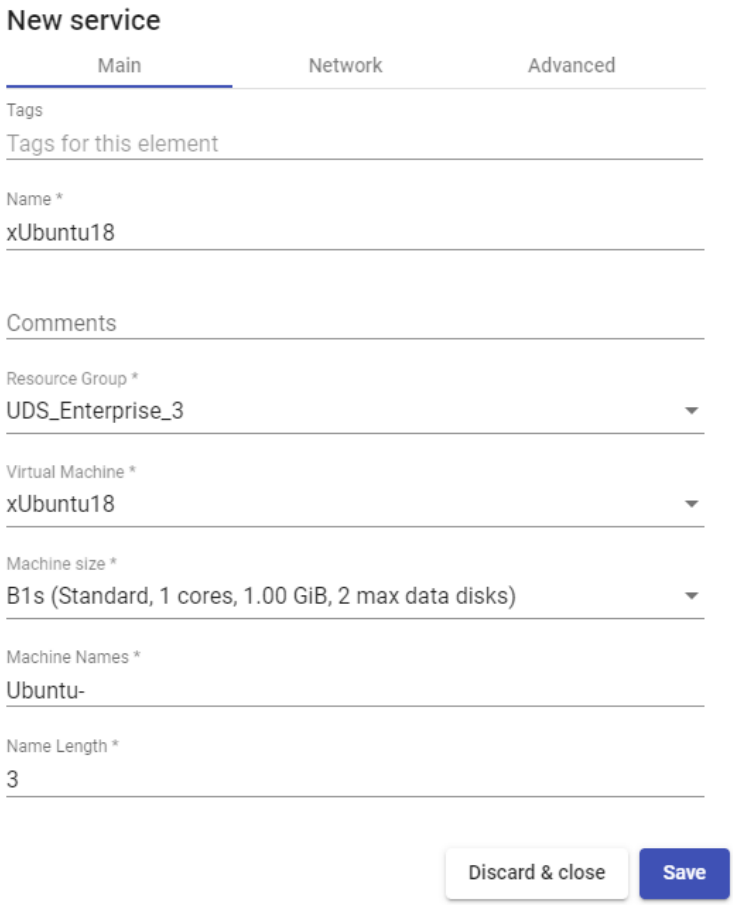
Creation of base services

When you have a valid "***Service provider***" connected to the Azure platform, you can create services based on templates. In order to do this, access the provider (with a double click or right button – "***Detail***") and in the "***Services***" tab click on "***New***" – "***Azure Clone Service***".

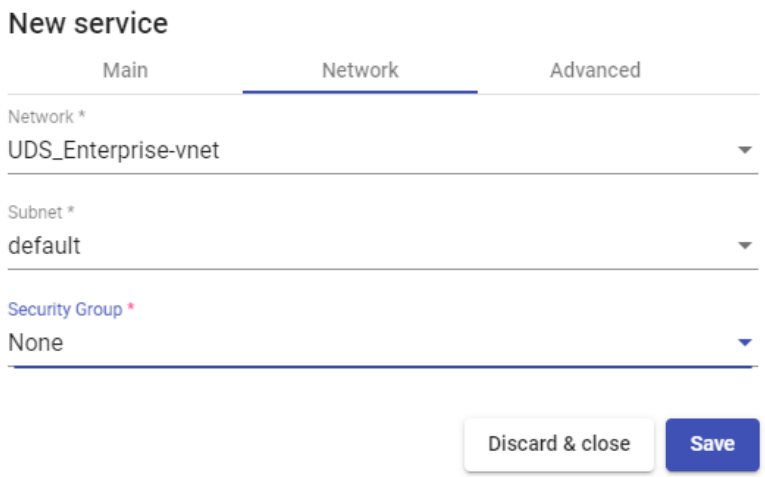

UDS
UDS
Azure
Summary
Services
Services of Azure
New
Edit
Azure Clone Service
Service name
Comments

To create a base service of type "***Azure Clone Service***" you will need to indicate:

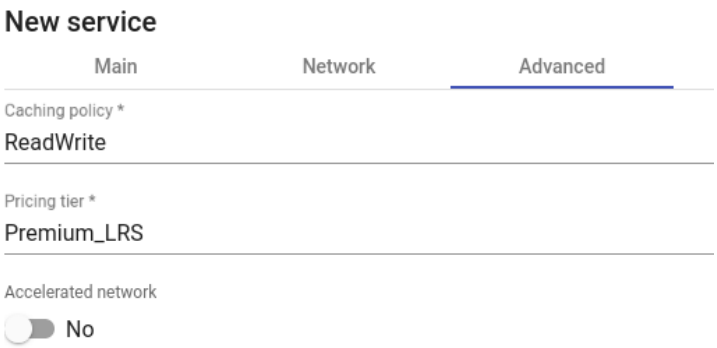
- Main:
  - **Name:** Descriptive name of the base service.
  - **Resource Group:** Select the Azure "***Resource Group***" under which you have your base machine or template.
  - **Virtual Machine:** base machine or template that you will use to deploy virtual desktops (with the UDS Actor installed and configured).
  - **Machine Size:** Amount of resources that the virtual desktops automatically deployed by UDS will have (this list will show all the types of machines available in Azure. Therefore, you must ensure that the chosen type is supported by your Azure subscription).
  - **Machine Names:** Root name of the virtual desktops generated by UDS.
  - **Name Length:** The number of digits of the counter for UDS machines. These digits will be joined to the "***machine names***" to form the DNS name of the virtual desktops (with 1 digit 9 machines can be created, with 2, 99, with 3, 999, etc...).


New service
Main
Network
Advanced
Tags
Tags for this element
Name *
xUbuntu18
Comments
Resource Group *
UDS_Enterprise_3
Virtual Machine *
xUbuntu18
Machine size *
B1s (Standard, 1 cores, 1.00 GiB, 2 max data disks)
Machine Names *
Ubuntu-
Name Length *
3
Discard & close
Save

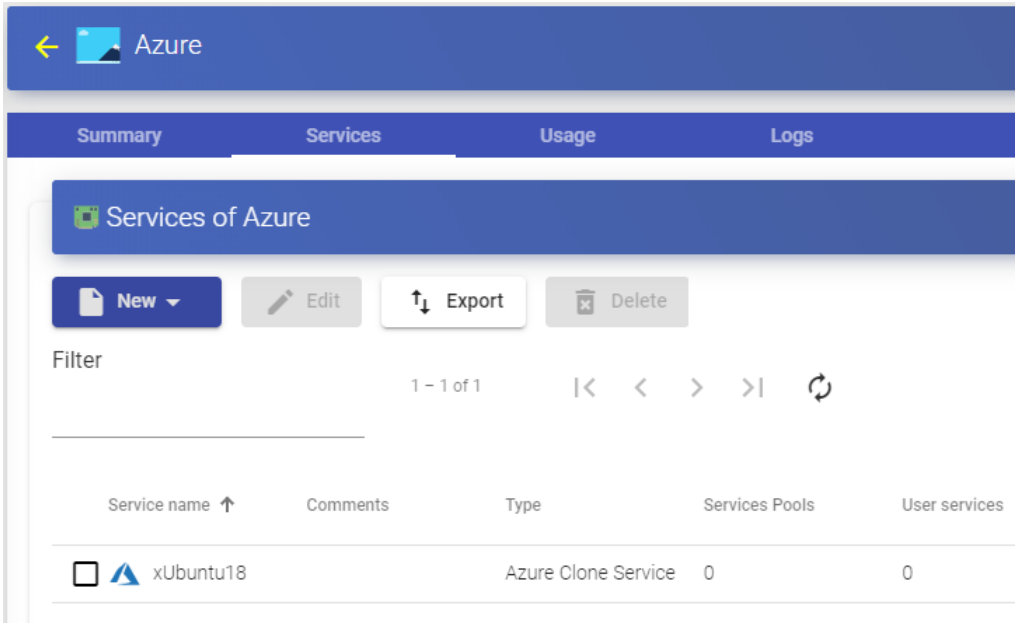
- Network:
  - **Network:** Existing virtual network in the Azure environment and associated with the selected "***Resource Group***" to which the virtual desktops will be connected (there must be connectivity with the UDS-Server component).
  - **Subnet:** Existing Azure environment subnet to which virtual desktops will connect.
  - **Security Group:** You can indicate a "***Security Group***"to assign to virtual desktops. In this example, when both the UDS components and the self-generated desktops are on the same network, you will select "***None***", since you do not want to apply any.



- Advanced:
  - **Caching policy:** Disk Cache Settings.
  - **Pricing tier:** Redundancy level applied.
  - **Accelerated network:** Enable the power to use this technology (it cannot be used with most types of machines, only with: D/DSv3, E/ESv3, Fsv2 and Ms/Mms and S.O. Linux).


New service
Main
Network
Advanced
Caching policy *
ReadWrite
Pricing tier *
Premium_LRS
Accelerated network
No

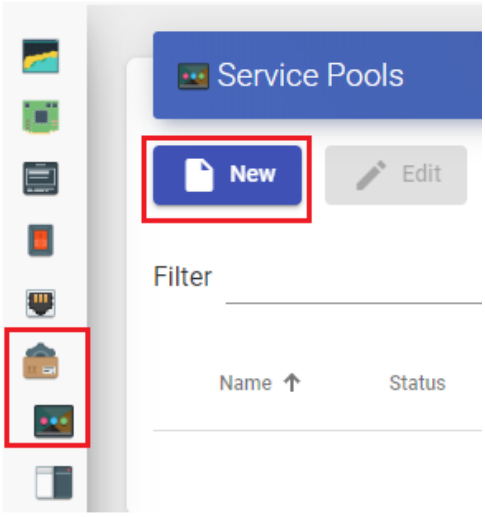
Click on "***Save***" and you will already have a valid base service to automatically deploy virtual desktops:



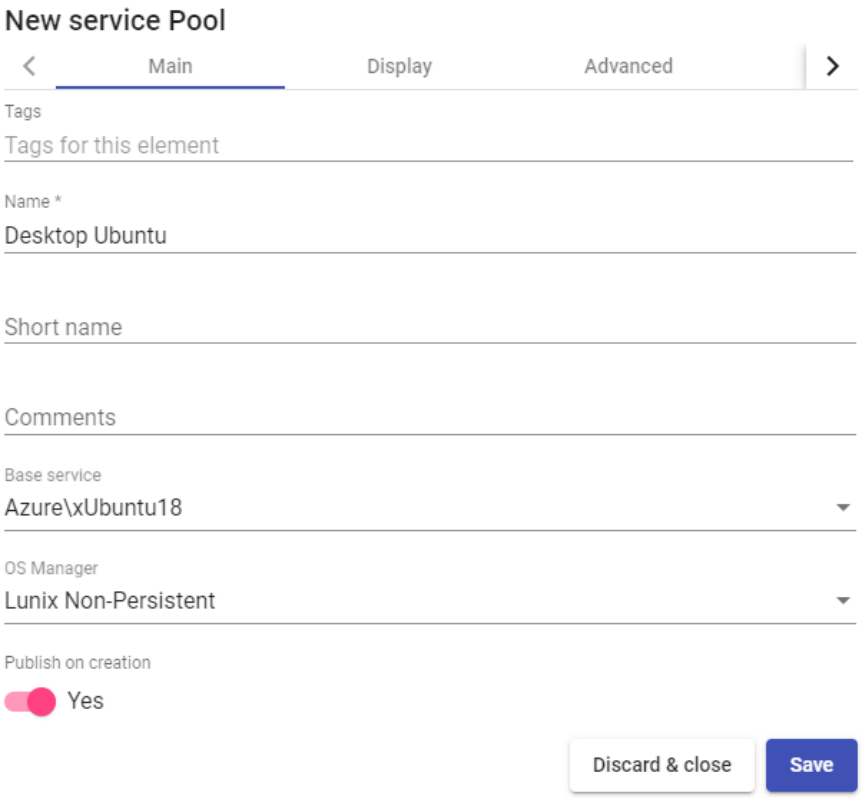
▪ Creation of a Service Pool

Before proceeding to create a service pool (to publish virtual desktops), it will be necessary to have at least one "***Authenticator***" with user groups (to validate and be able to assign the service to users), an "***OS Manager***" (to indicate the OS and the persistence policy of the generated desktops) and a "***Transport***" (to connect to the desktop) previously configured. To see more details on how to configure these elements, you can access the UDS Enterprise Installation, Administration and User Manual in the documentation section of our website.

When you have the elements mentioned above ("***Authenticator***", "***OS Manager***" and "***Transport***") you can create "***Service Pools***". In order to do this, access the "***Pools***", section, open the "***Service Pools***" tab and click on "***New***".

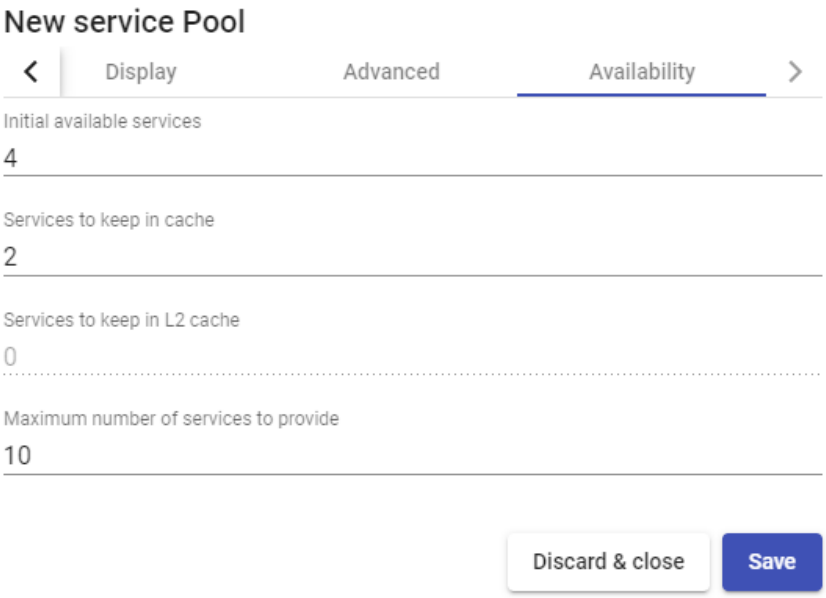

Service Pools
New
Edit
Filter
Name
Status

In the "*Main*" tab you will indicate the name of the service (this name will be visible to users) and select the previously created base service (in this case from the Azure platform and the xUbuntu18 base service) and an existing "*OS Manager*" (in this example we will use one for Linux O.S. and non-persistent type).



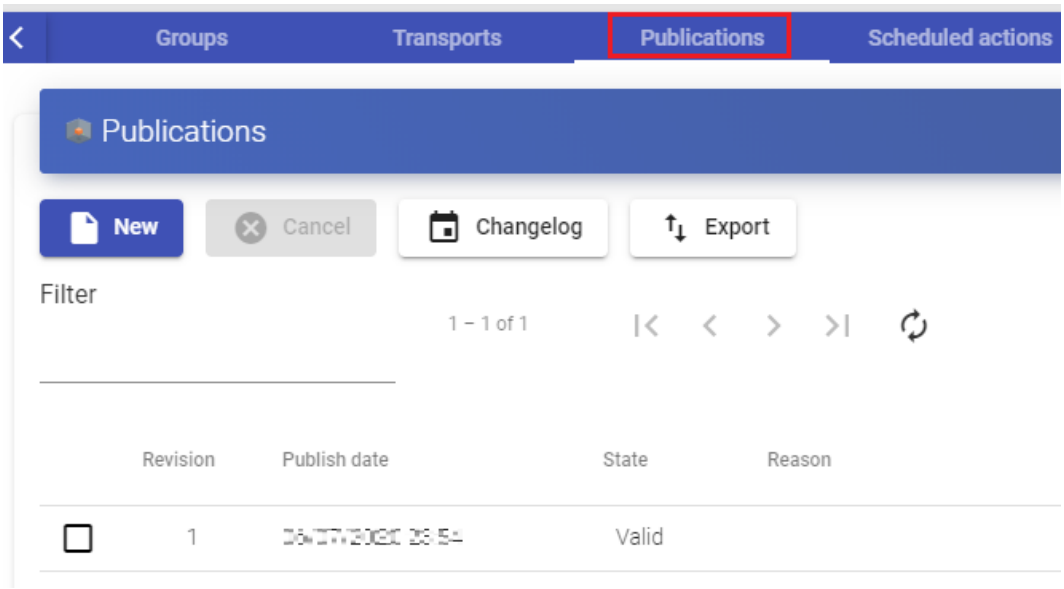
The parameters of the "*Advanced*" and "*Display*" tabs can be left by default. In the "*Availability*" tab, you will indicate the initial desktops that will generate UDS and those to be kept in the cache (in Azure the use of the L2 cache is not available).

In this example, we are going to indicate that UDS automatically creates 4 desktops and we always have at least 2 available in the cache.

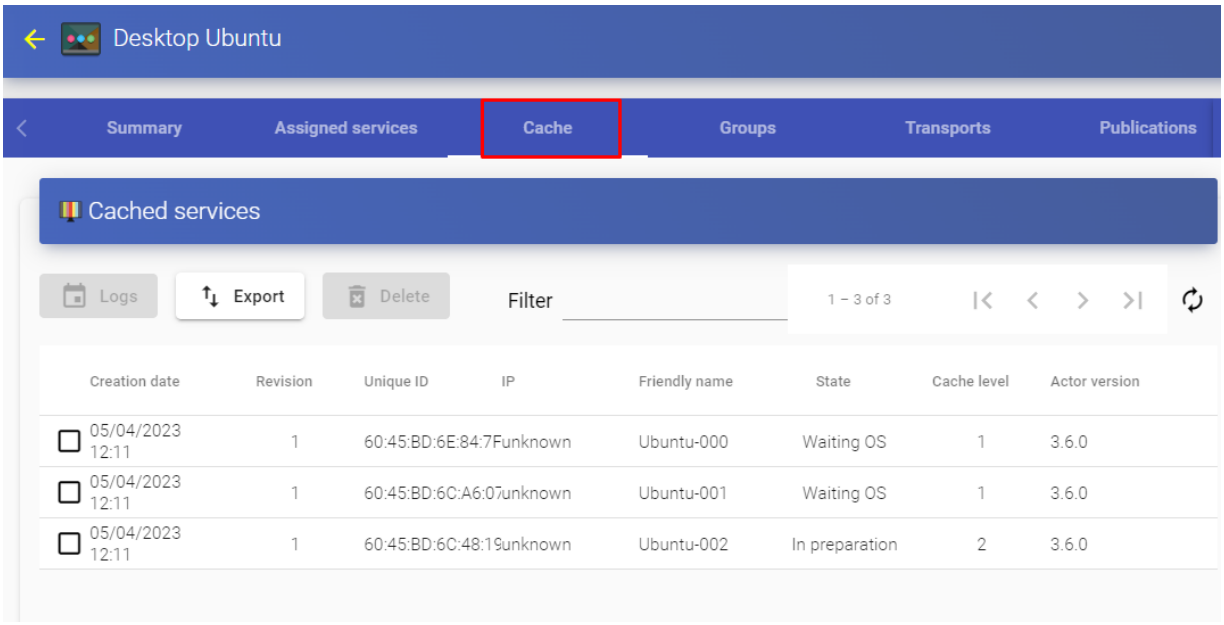

New service Pool
Display
Advanced
Availability
Initial available services
4
Services to keep in cache
2
Services to keep in L2 cache
0
Maximum number of services to provide
10
Discard & close
Save

NOTE:
When saving the configuration or publishing a new version, the base machine or template must be turned off.

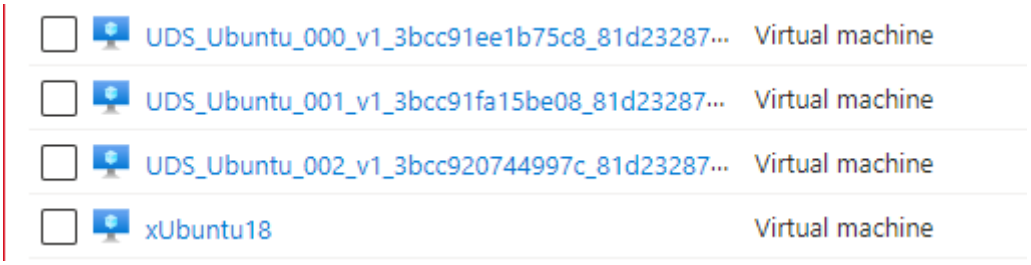
Selecting the "***Service Pool***" and opening the "***Publications***" tab you will check if the publication has been generated correctly. When in a "***Valid***" state, the system will start to auto-generate the virtual desktops indicated in the cache parameters.



In the "***Cache***" tab you can see how the desktops start to be generated.

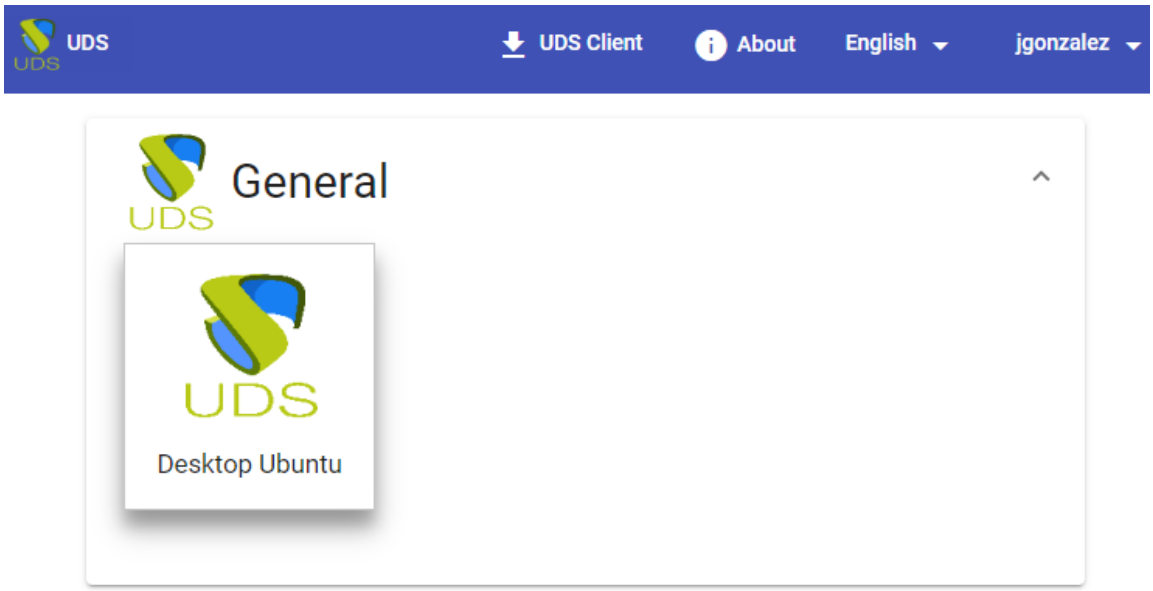

Desktop Ubuntu
Summary
Assigned services
Cache
Groups
Transports
Publications
Cached services
Logs
Export
Delete
Filter
1 – 3 of 3
Creation date
Revision
Unique ID
IP
Friendly name
State
Cache level
Actor version
05/04/2023 12:11
1
60:45:BD:6E:84:7F
unknown
Ubuntu-000
Waiting OS
1
3.6.0
05/04/2023 12:11
1
60:45:BD:6C:A6:07
unknown
Ubuntu-001
Waiting OS
1
3.6.0
05/04/2023 12:11
1
60:45:BD:6C:48:19
unknown
Ubuntu-002
In preparation
2
3.6.0

In the Azure environment you will also see how virtual desktops are generated:



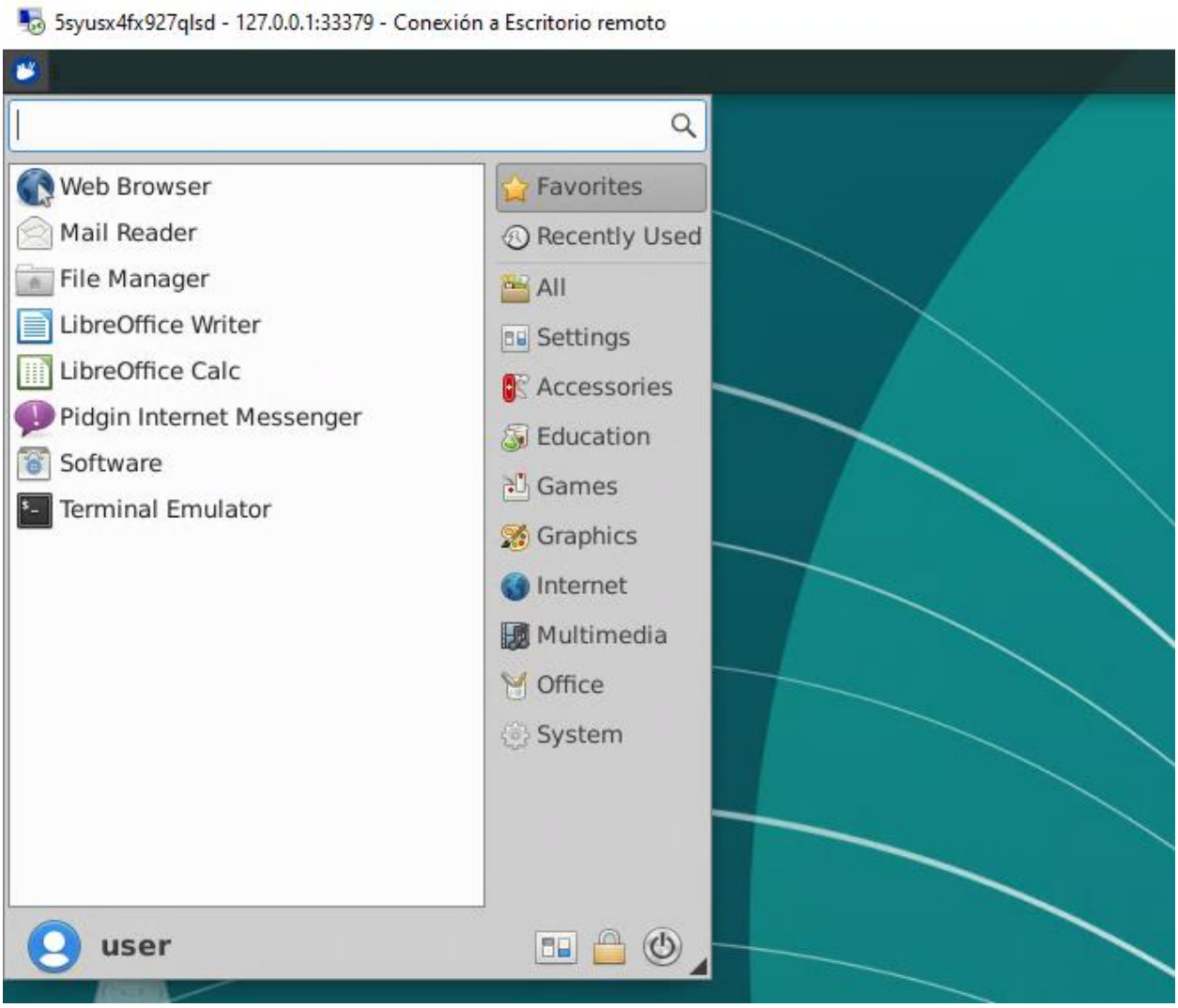
Once the desktops are in the "***Valid***" state (that is, the UDS Actor installed in the template has finished applying the necessary settings), they will be available for users to access.

You will access the services window with a user (it is not possible to use the system administrator super-user) and you will see the available service.



NOTE:
In order for the service to be viewed by users, the “Service Pool” created must have a user group (“Groups” tab) and a transport (“Transports” tab) assigned to it.

You access it by clicking on the image (in this example an RDP type transport has been configured).



NOTE:
If you are outside the network configured in Azure, it will be necessary to use tunnelled transport (as you can see in the screenshot of the connection example, it is connecting to 127.0.0.1 since the connection is made via Tunnel).

Azure AD integration as UDS Enterprise "Authenticator"

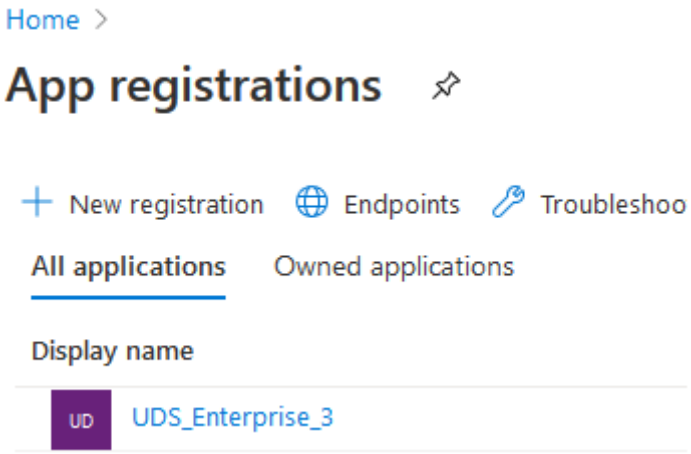
UDS allows integration with the Azure authentication system, called "***Azure Active Directory***". Through this integration, it will be possible to validate users registered in this authenticator in the UDS login portal and allow them to access desktop services and virtual applications.

To allow the correct integration between UDS and "***Azure Active Directory***" it will be necessary to carry out some preliminary tasks on the Azure platform.

Tasks to perform in Azure

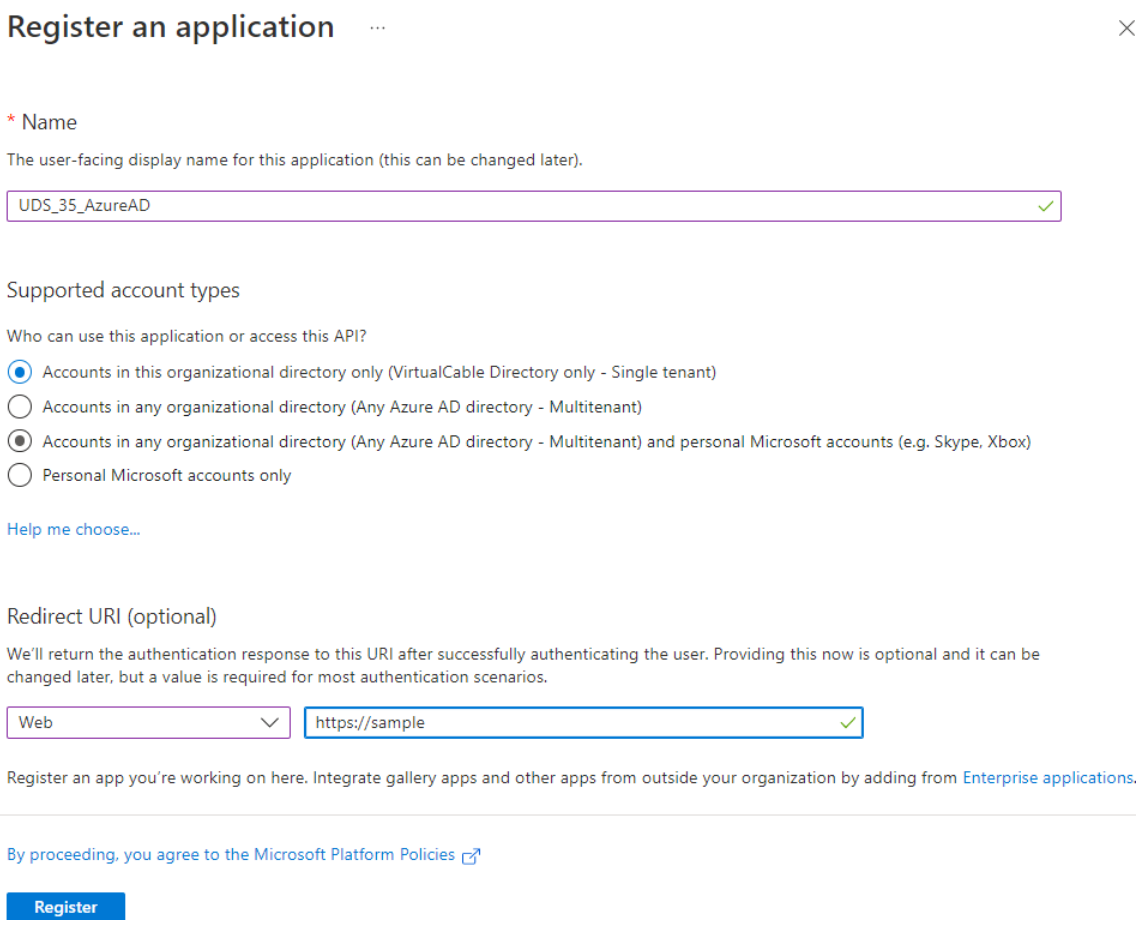
The first task you will perform in the Azure environment will be to create a valid "***App registrations***" to allow UDS to access the "***Azure Active Directory***".

To register the application you will go to the "***App registrations***" service and click on "***New registration***".

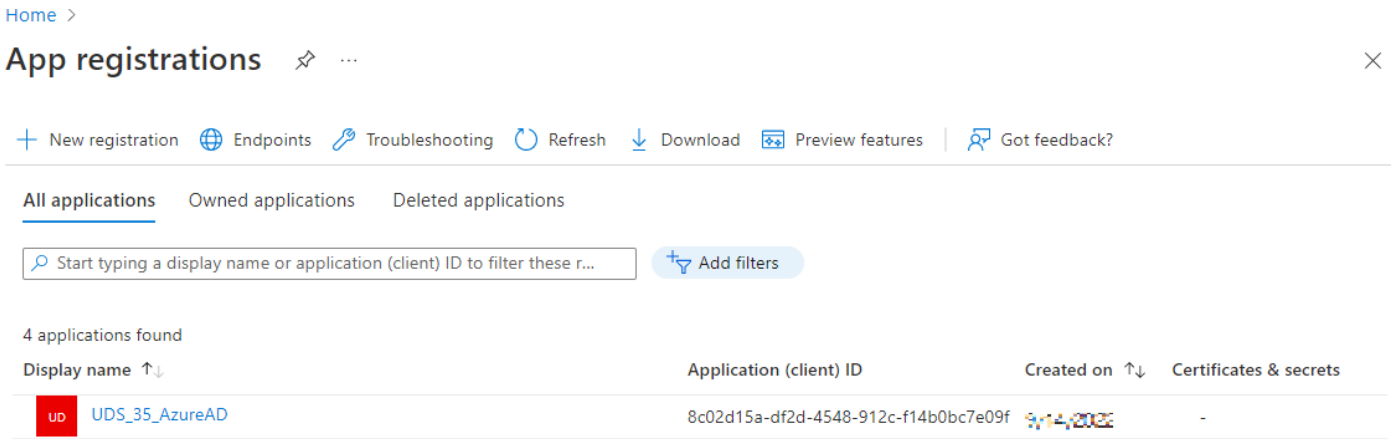


NOTE:
In some cases it will be necessary to click on "View all applications" in order to view all the existing ones.

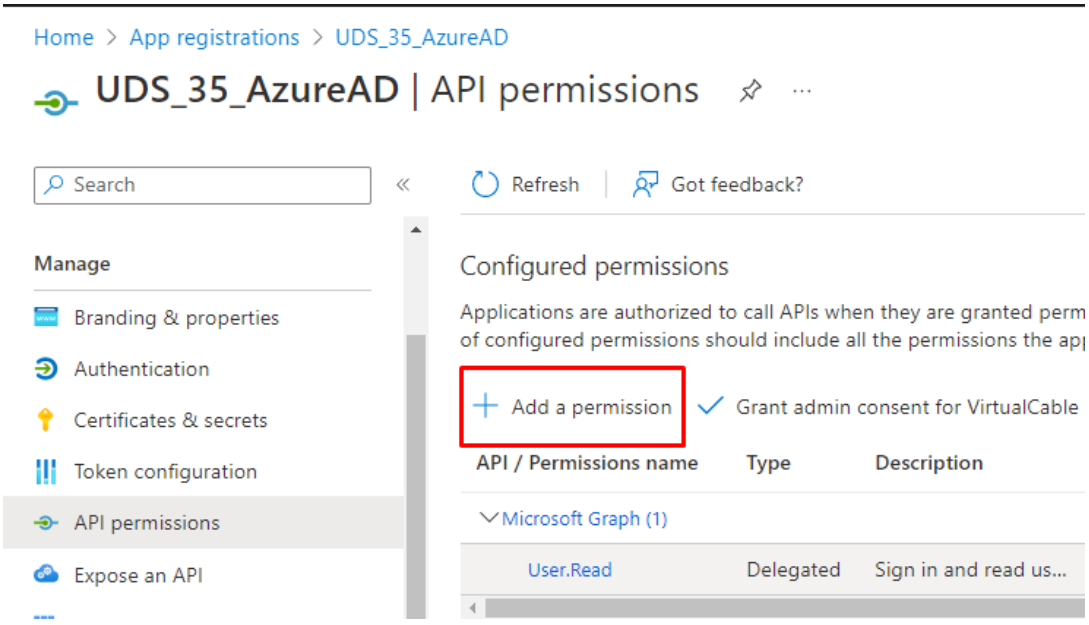
In the creation wizard, you will indicate the name of the application, who will be able to access it and in the "***Redirect URI***" section you will indicate "***Web***" with any URL (it does not need to exist, it will not be used).



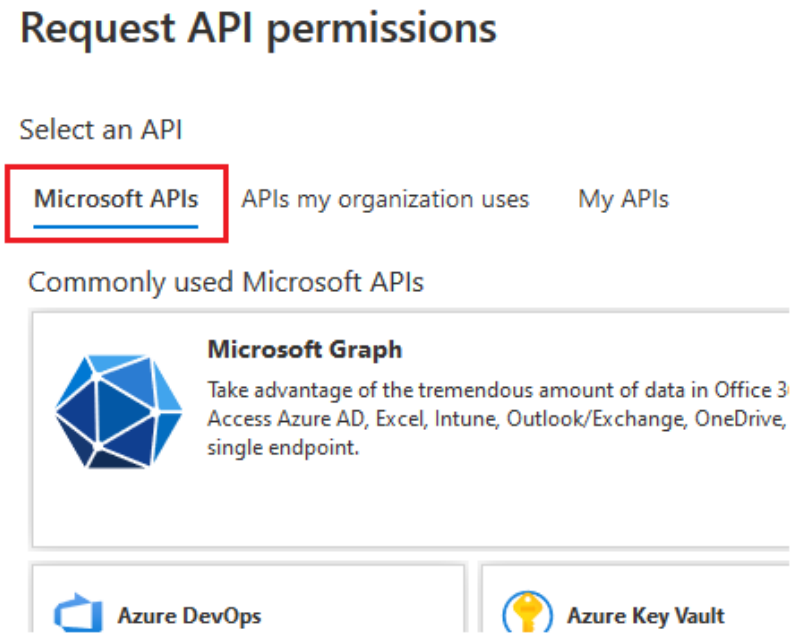
Once all the data of the application is indicated, you will click on "***Register***" and you will check that it has been created correctly (if you do not see it, you will click on "***View all applications***"):



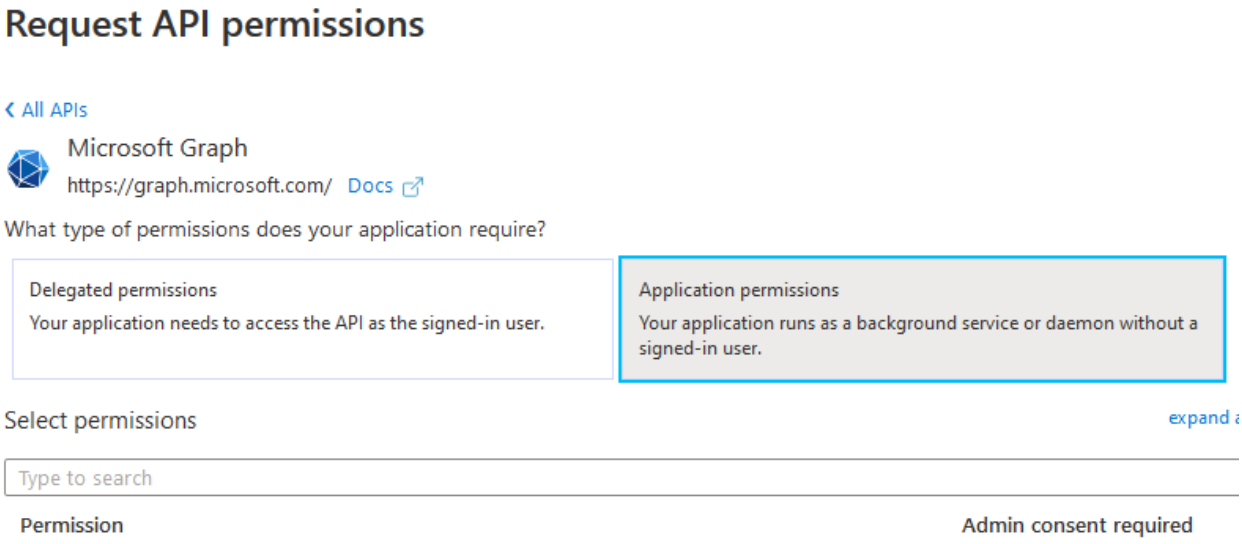
After checking that it has been created correctly, you will access the App. In the "***Manage***" menu, click on "***API permissions***" and select "***Add a permission***".



Now select the "***Microsoft APIs***" tab and click on "***Microsoft Graph***":

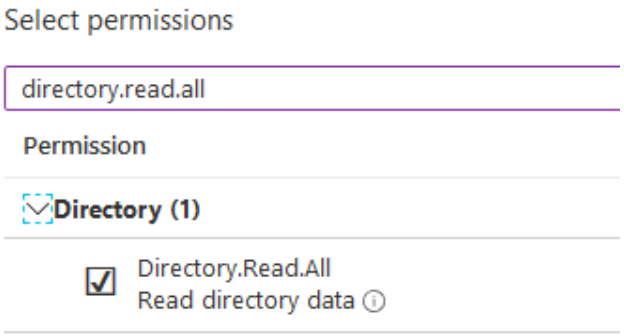


Within "*Microsoft Graph*", select "*Application permissions*" to apply for the necessary permissions:

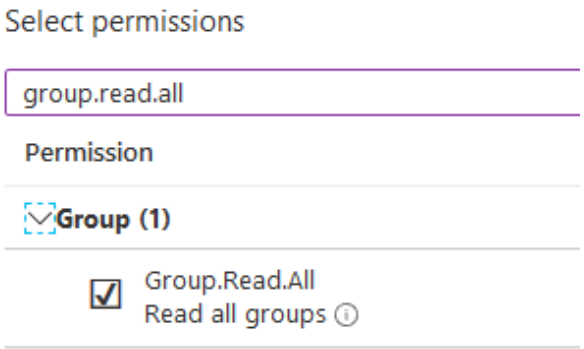


You will apply the permissions:

- "*Directory.Read.All*"

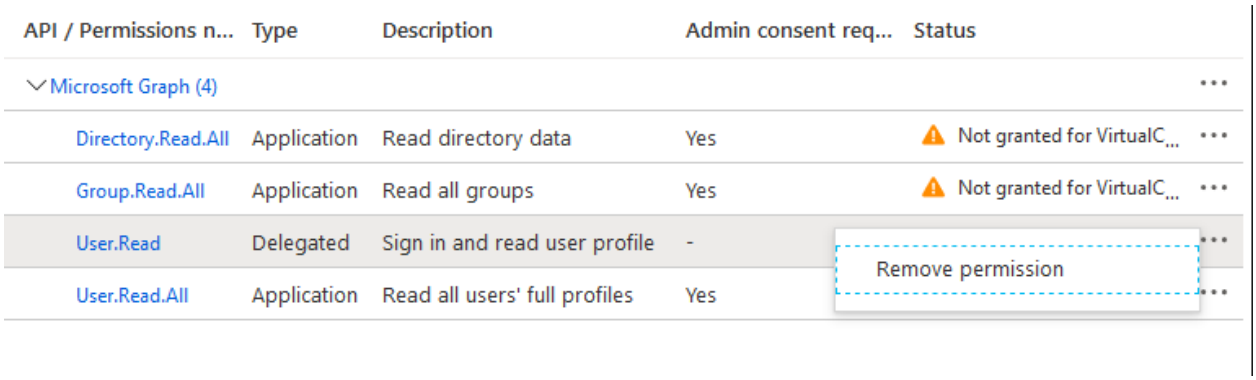


- "*Group.Read.All*"

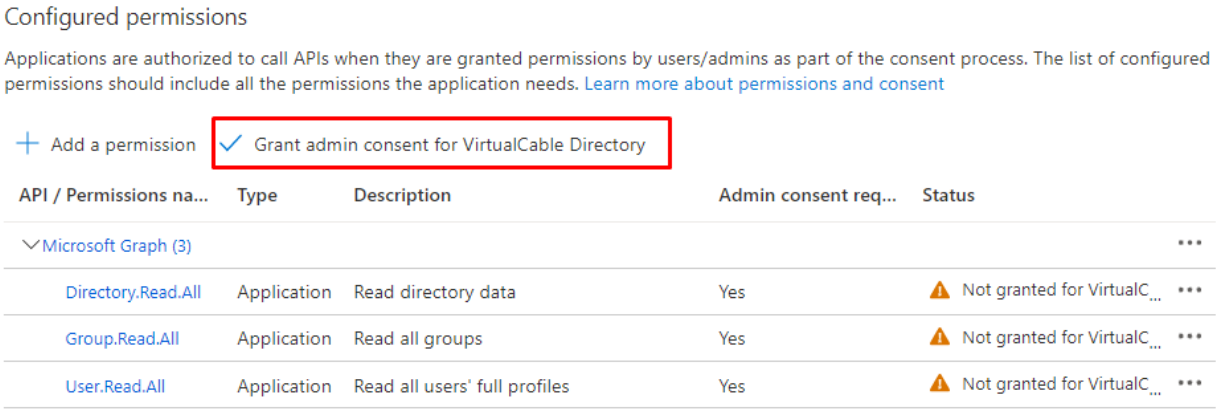


- "*User.Read.All*"

The "*User.Read*" permission, which is added by default, can be removed:



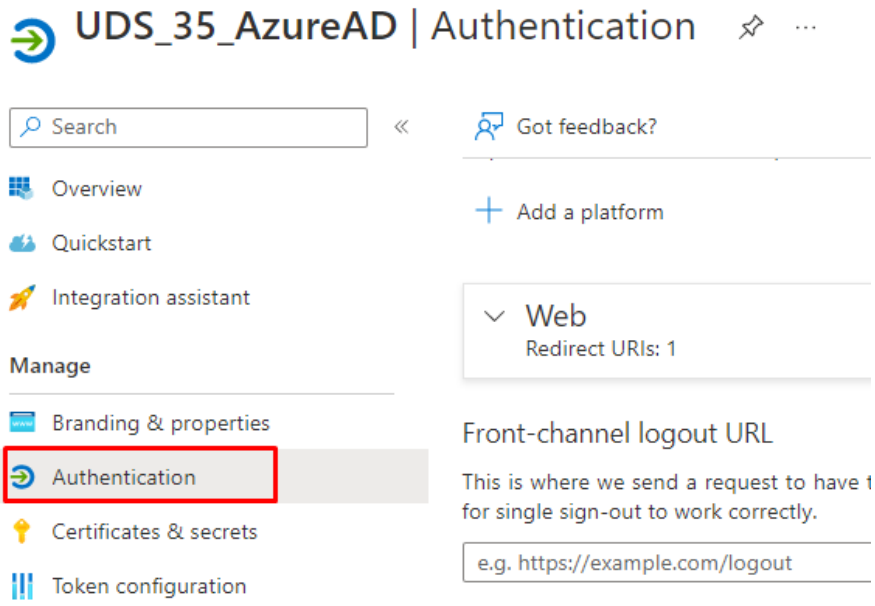
Once you have the necessary permissions, click on "*Grant admin consent for...*" and accept:



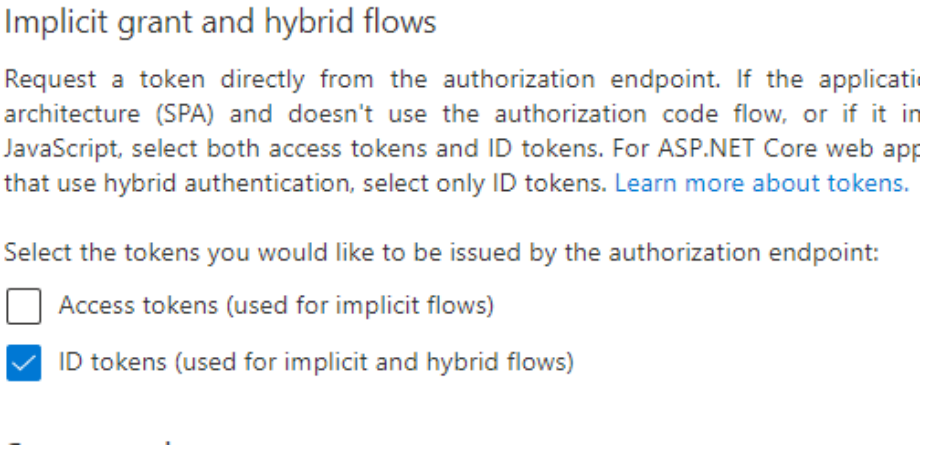
Confirm that the permissions have been applied:

API / Permissions n...	Type	Description	Admin c...	Status
Microsoft Graph (3)				
Directory.Read.All	Application	Read directory data	Yes	Granted for VirtualCable...
Group.Read.All	Application	Read all groups	Yes	Granted for VirtualCable...
User.Read.All	Application	Read all users' full profil...	Yes	Granted for VirtualCable...

To finish with the configuration of the App, you will need to access the "***Manage***" menu and select "***Authentication***":



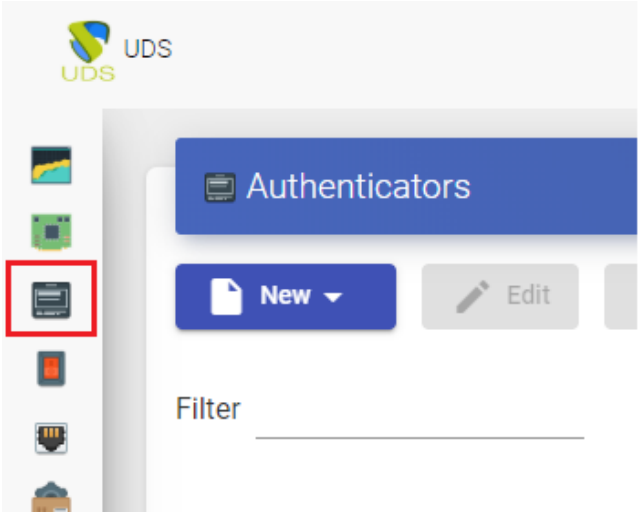
In the "***Implicit grant and hybrid flows***" section, you will select "***ID tokens***" and click on "***Save***" to apply the change.



The next task in the process of integrating "***Azure Active Directory***" with UDS will be carried out by the UDS administration itself.

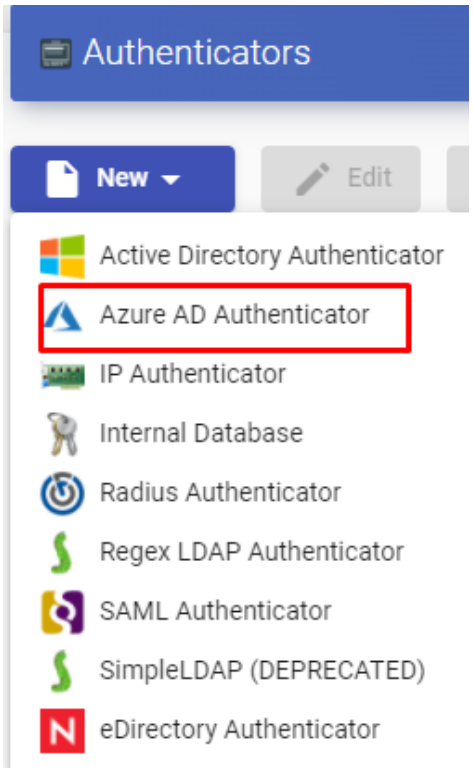
Tasks to perform in UDS Enterprise

From the UDS administration, you will proceed to register the new authenticator of type "***Azure Active Directory***". In order to do this, validate yourself on the UDS login portal with a user with administrative permissions and access the "***Authenticators***" section.



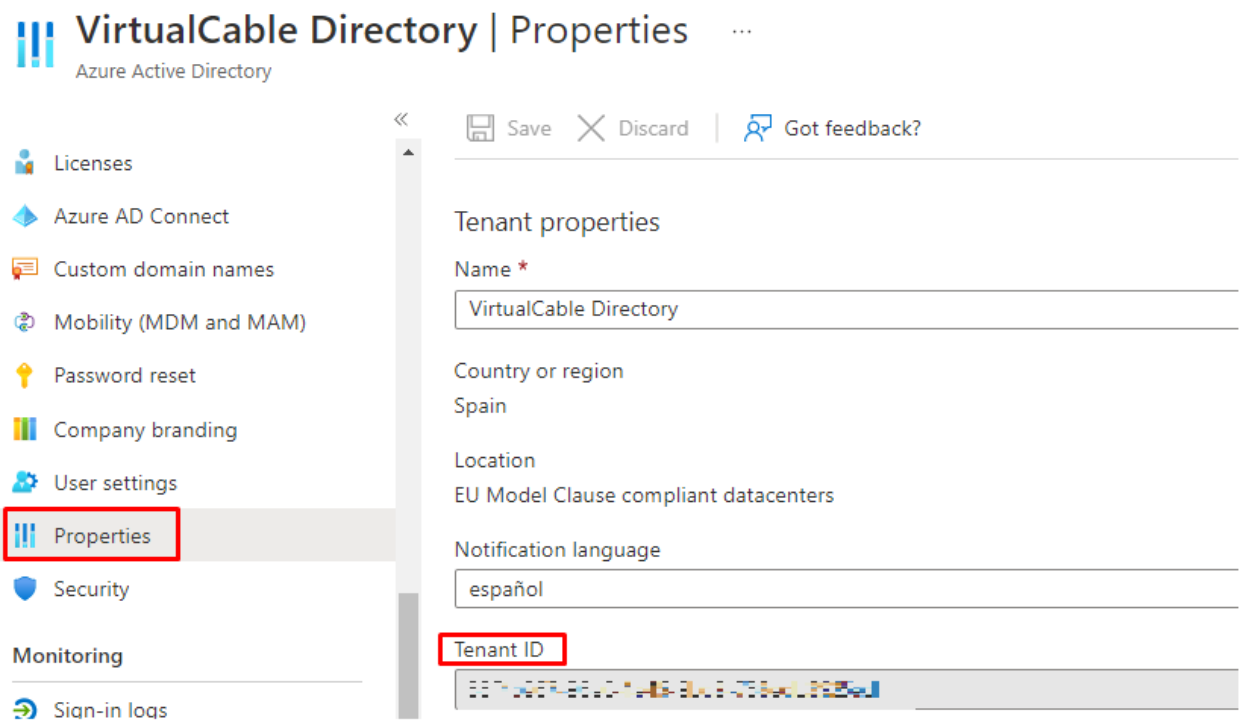
NOTE:
In UDS you can have different types of authenticators registered in the system. The priority field will define which authenticator will be shown to users by default.

Click on "***New***" and select "***Azure AD Authenticator***".

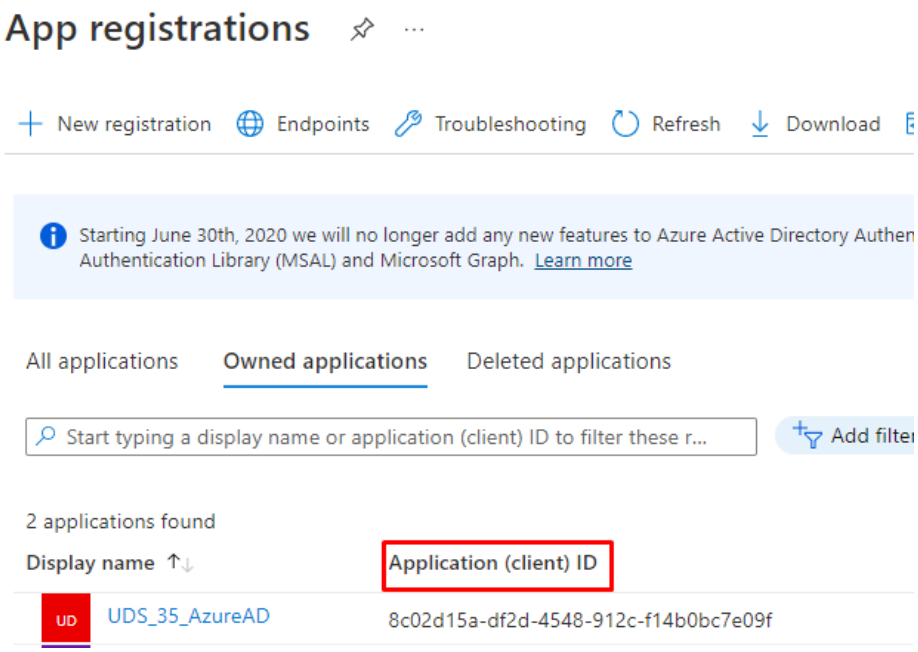

Authenticators
New
Edit
Active Directory Authenticator
Azure AD Authenticator
IP Authenticator
Internal Database
Radius Authenticator
Regex LDAP Authenticator
SAML Authenticator
SimpleLDAP (DEPRECATED)
eDirectory Authenticator

Within the wizard, you must indicate a series of necessary data:

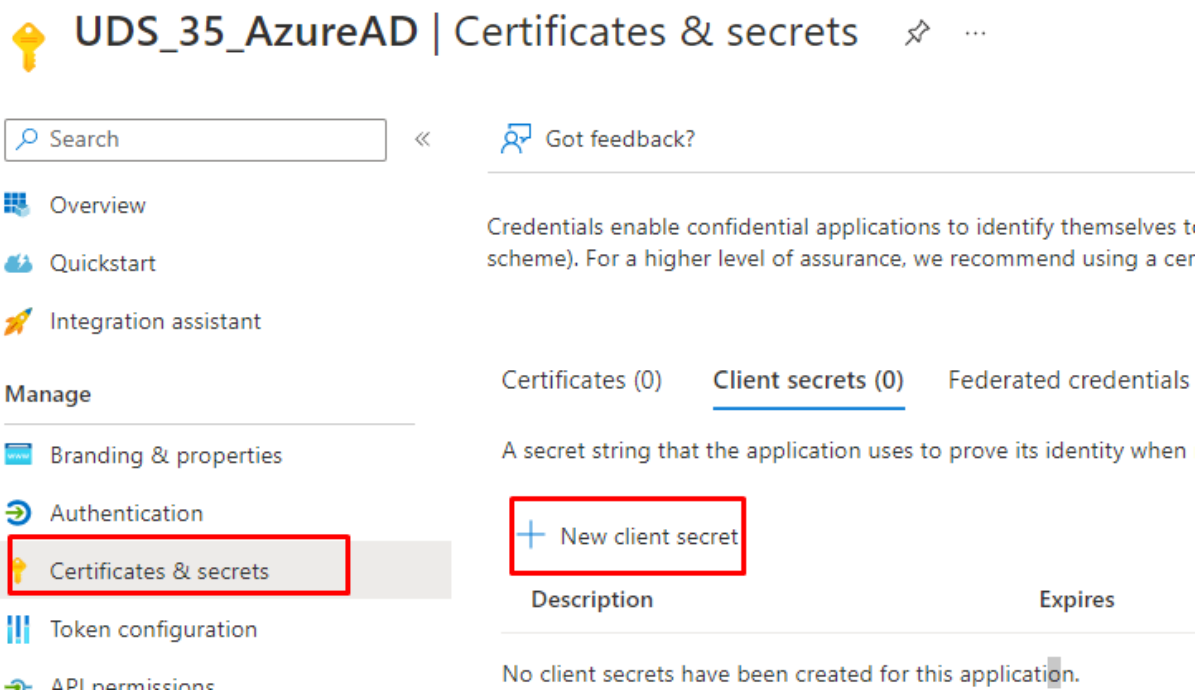
- **Main:**
  - **Name:** Authenticator name.
  - **Priority:** Priority, of this authenticator in the list of authenticators available. The lower the priority, the higher it is in the list of available authenticators (of all authenticators, the one with the lowest priority, including negative values, will be the default authenticator).
  - **Label:** Label assigned to this authenticator. You have to put it in the login URL to perform a direct validation without having to use the list of authenticators.
  - **Tenant ID:** This value can be obtained from the service "***Azure Active Directory***", "***Properties***", "***Directory ID***".



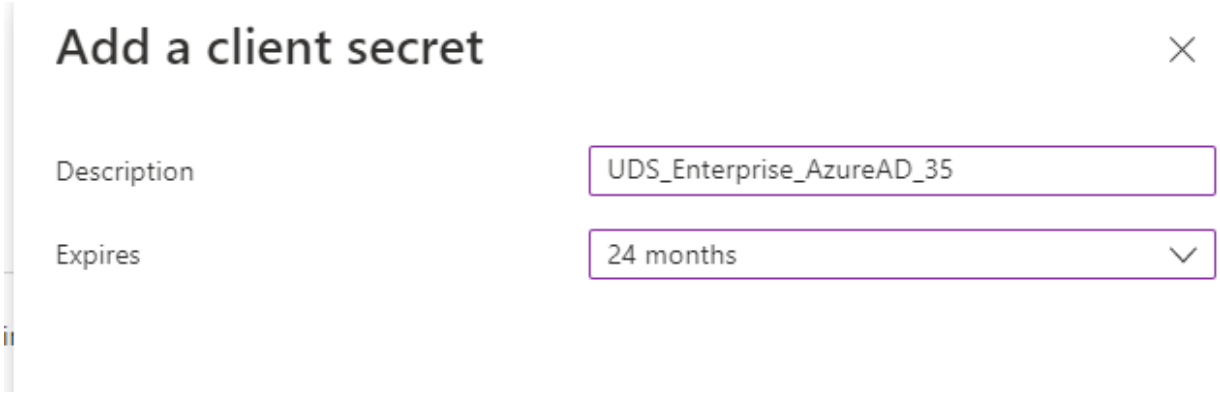
- **Client ID:** To obtain this value it will be necessary to access the "*Application registration*" previously created and copy the value of "*Application ID*".



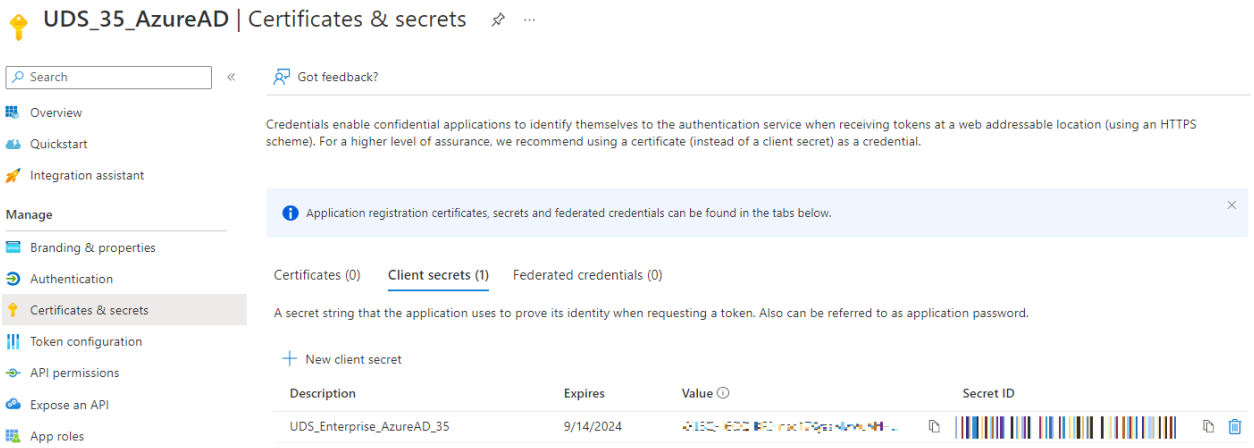
- **Client Secret:** This value will be obtained from the previously registered application. Click on it (in the "*App registrations*") and access "*Certificates & secrets*".



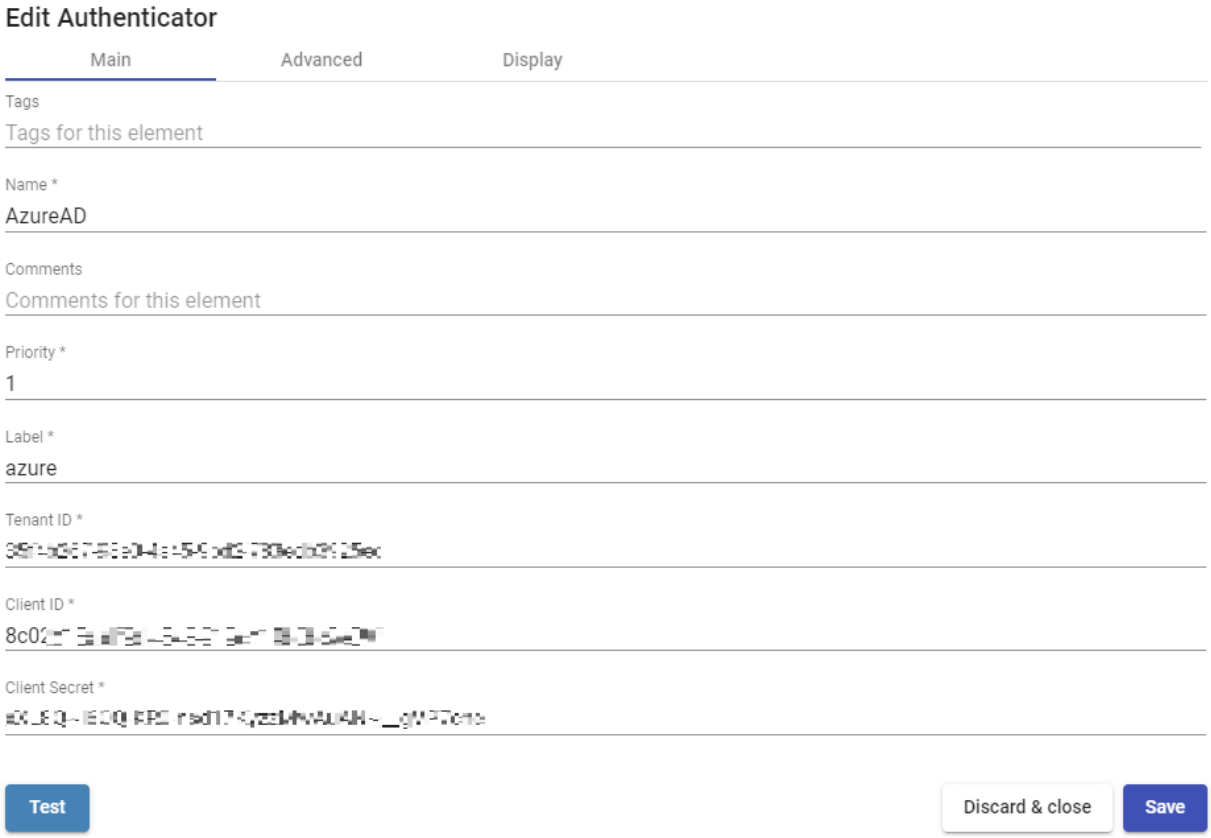
Within "***Certificates & secrets***" click on "***New client secret***". Add a description, select when it expires and click on "***Add***" to be able to copy the "***key***":



Once added, it will allow you to copy the value (once this window is closed, you will not be able to copy this value again, although you will be able to generate a new one if necessary). You will use this value as "***Client Secret***" in UDS.



Once you have all the fields filled in, you will click on "***Test***" to verify the correct integration.

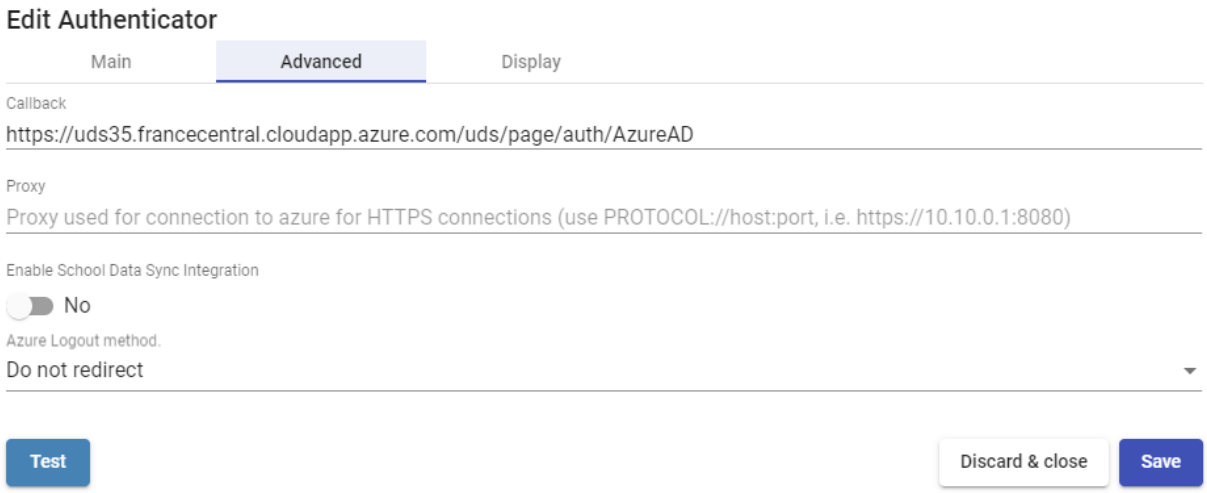


Once the correct connection has been verified, you will click on "***Save***" to save it.

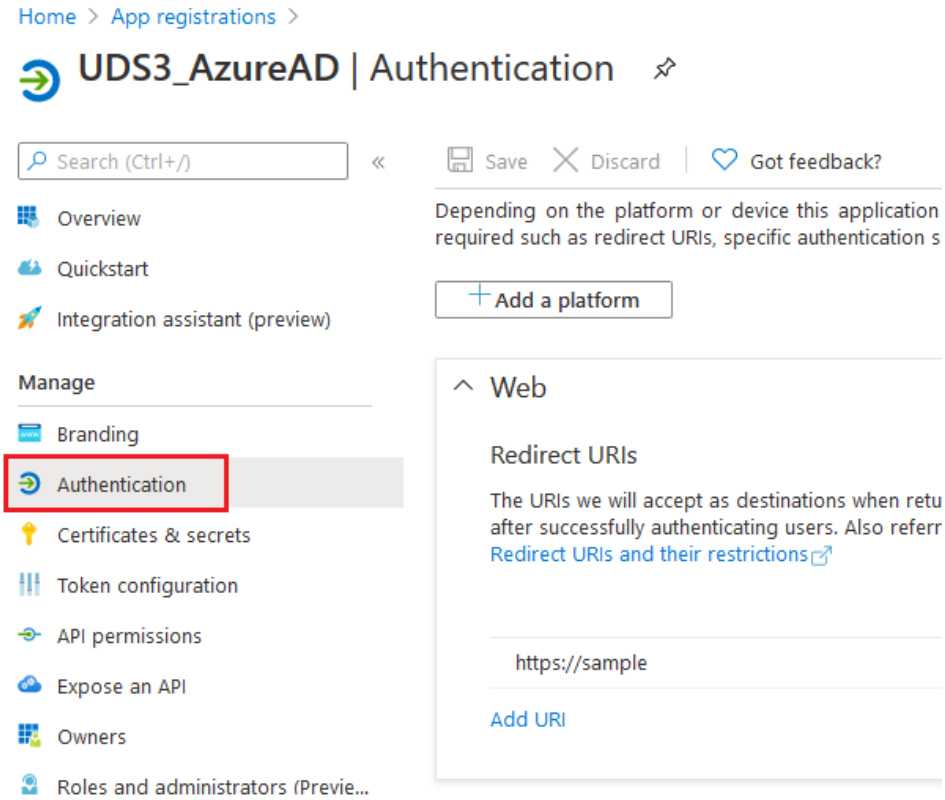
NOTE:
If the test indicates that there is an error, you can save the connector by clicking on "Save" to avoid losing data such as the "Client Secret" and, later, review the causes of the connection error.

The last task to complete the integration of UDS with the "***Azure Active Directory***" authenticator will be to indicate the access URL allowed in the Azure environment.

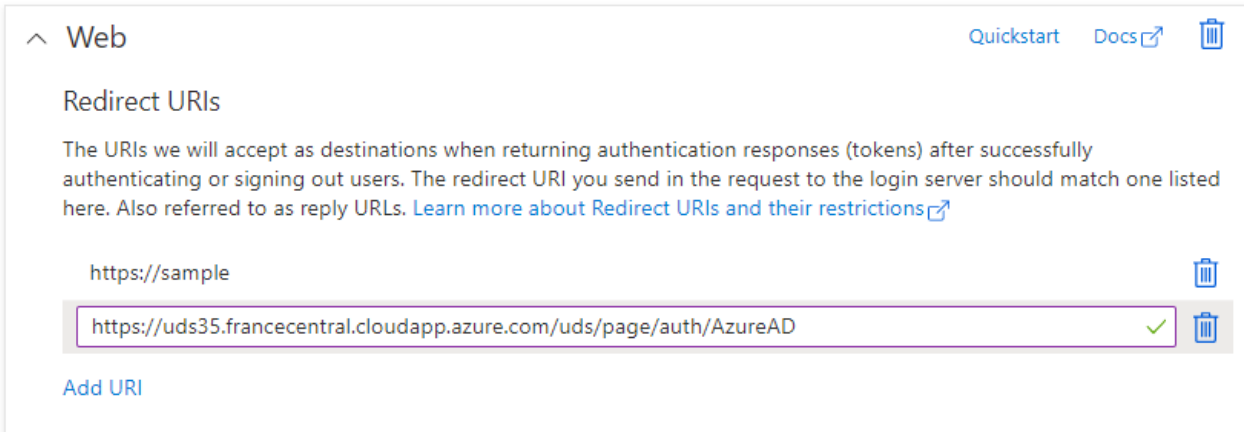
In the "***Authenticators***" section of UDS administration, select the authenticator previously created. Edit it by accessing the "***Advanced***"tab. You will need to copy the value of the "***Callback***" field.



Once you have the value copied, you will access the Azure platform. In "***App Registrations***", select the previously created application for the integration of Azure AD with UDS and in the "***Manage***" menu click on "***Authentication***".

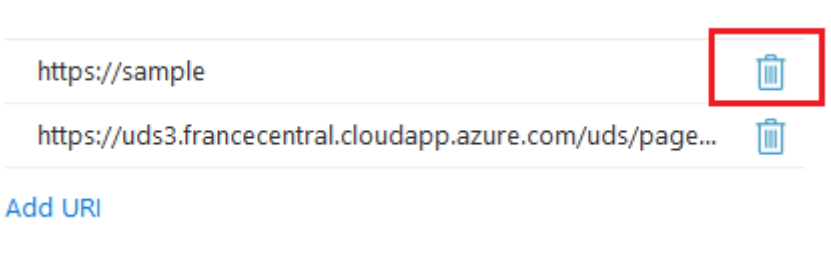


Within "***Authentication***", click on "***Add URI***" and paste the value copied from the UDS administration from the "***Callback***" field of the authenticator.



Click on "***Save***" to save the new "***URL***".

NOTE:
The URL indicated in the creation of the App can be removed (in this case https://sample). Click on the delete icon and then "Save".



After completing these steps, users can authenticate themselves with the user credentials configured in an "***Azure Active directory***" authenticator.

NOTE:
In order for a user to be able to validate in the UDS login portal with the Azure authenticator, he must belong to a group of users previously registered in the UDS administration.

About VirtualCable

Virtual Cable is a company specialized in the digital transformation of the workplace. The company develops, supports and markets UDS Enterprise. Its team of experts has designed VDI solutions tailored to each sector to provide a unique user experience fully adapted to the needs of each user profile. Virtual Cable professionals have more than 30 years of experience in IT and software development and more than 15 in virtualization technologies. Millions of Windows and Linux virtual desktops with UDS Enterprise are deployed all over the world every day.