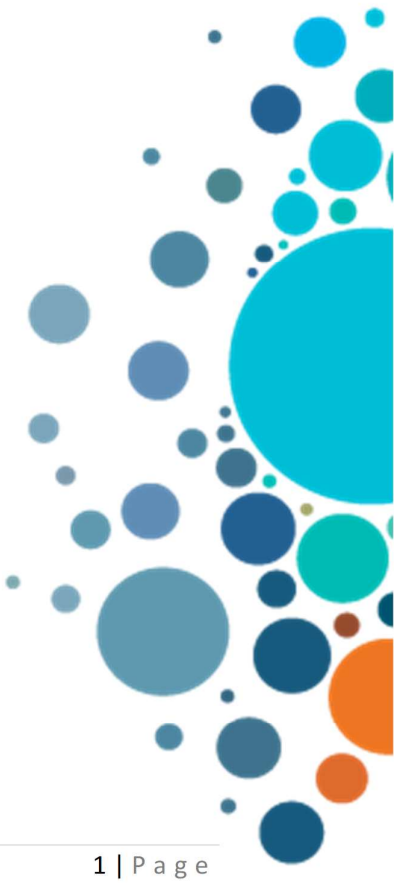
CISCO Live!
Las Vegas + Digital | June 12-16, 2022

Migrate UCS to Intersight Managed Mode using IaC

HOLDCN-2012

Tyson Scott & Patrick LeMaistre



Learning Objectives

Upon completion of this hands-on lab, you will become familiar with migrating an existing UCS Managed Mode domain (brownfield) as well as configuring a new Intersight Managed Mode domain (greenfield). As a bonus, you can deploy a Kubernetes cluster using the Intersight Kubernetes Service.

Specifically, you will perform the following tasks:

- Brownfield – Transition an existing UCS domain to Intersight Infrastructure Service from UCS Manager leveraging Terraform infrastructure as code (IaC) practices.
- Greenfield – Use the python wizard to generate Terraform Infrastructure as Code (IaC), that will enable you to build a new UCS domain utilizing Intersight Infrastructure Services to manage the Domain.
- Deploy a Kubernetes cluster in Intersight using the Intersight Kubernetes Service (IKS) and familiarize yourself with the Intersight Virtualization Service (IVS) as well as IKS [BONUS]

Outline

Scenario 0: Initiate Your Hands on Lab Session via dCloud

Use these steps to connect to the dCloud lab environment.

Step 1 Initiate your dCloud session: [show me how]

Step 2 Connect to the dCloud desktop workstation using one of the following connection methods:

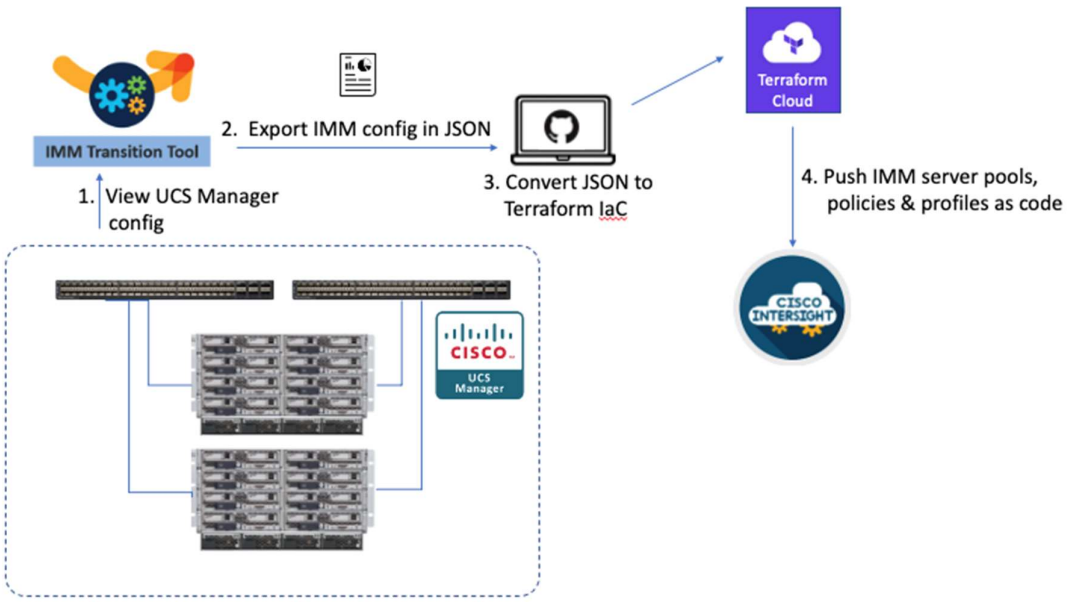
- Cisco AnyConnect VPN [Show me how] and the local RDP client on your laptop [Show me how] (Workstation: 198.18.133.12, Username administrator, Password: C1sco12345)
- Cisco dCloud Remote Desktop Client [Show me how]

NOTES: When the session starts setup scripts may still be running. Please wait until these complete before beginning your lab.

Scenario 1: Domain to Intersight Managed Mode

In this lab activity, you will learn how to transition an existing UCS domain that is running in UCS Manager Mode (UMM) to Intersight Managed Mode (IMM).

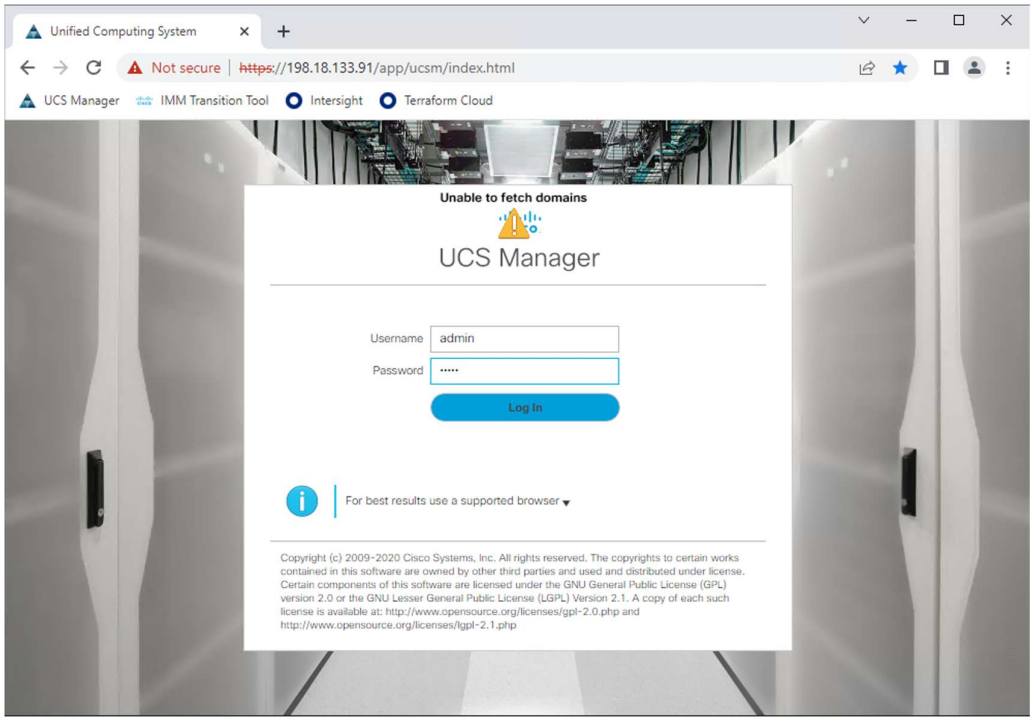
To perform this migration, the IMM Transition Tool will be used to gather your existing UCSM configuration and export it to JSON format. This JSON file will then be converted to HashiCorp Config Language (HCL) so it can be managed like code. Finally Terraform Cloud will be used to push the converted configuration into Intersight so servers and fabric interconnects can be now managed in IMM mode.



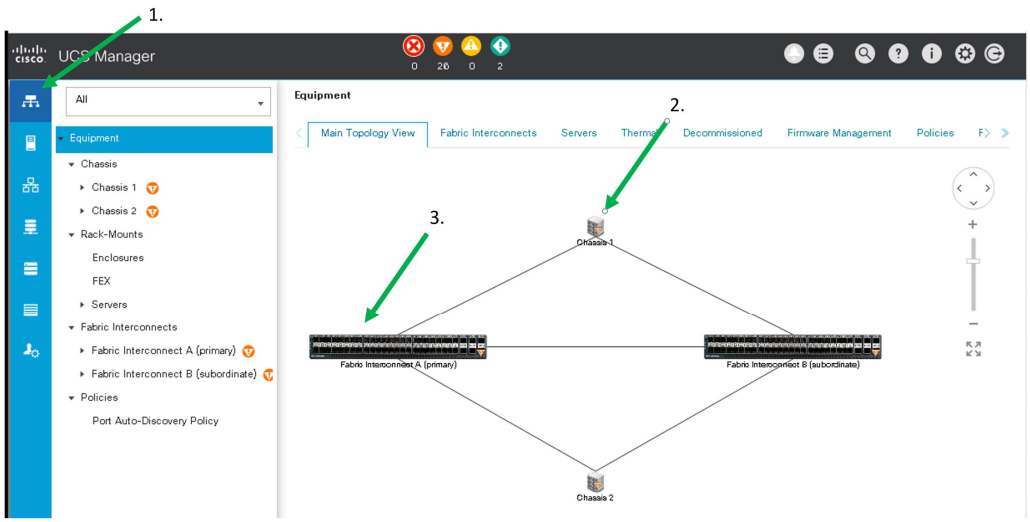
Task 1: Log into the Brownfield UCS Manager Domain

In this task you will connect to the brownfield UCS Manager and familiarize yourself with the existing UCS domain configuration that is to be migrated to Intersight.

Step 1 Log into the brownfield UCS Manager GUI by opening Chrome on the dcloud desktop and click the UCS Manager bookmark (https://198.18.133.91/app/ucsm/index.html) and login with a username **`admin`** and password **`admin.`**

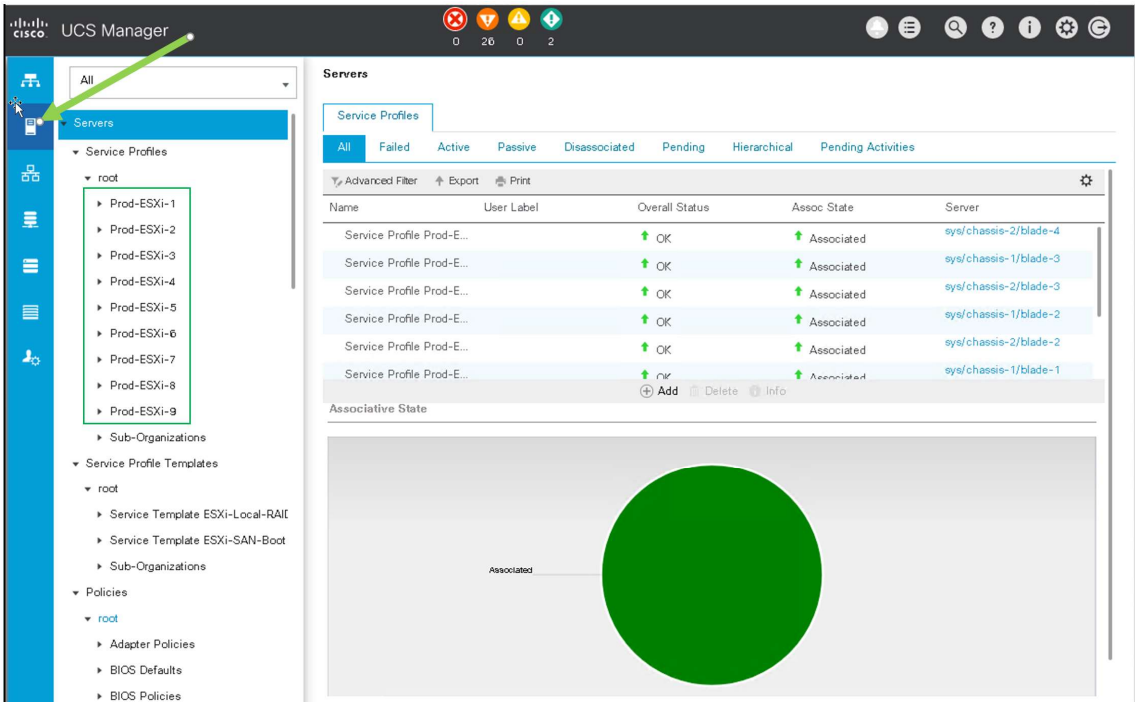


Step 2 Click on the **Equipment** tab in UCS Manager and take note that your pod has a pair of UCS 6454 Fabric Interconnects as well as a two UCS 5108 chassis as well as 16 x B200 M5 servers.



Note: some alarms will be in your pod, these should not affect your lab.

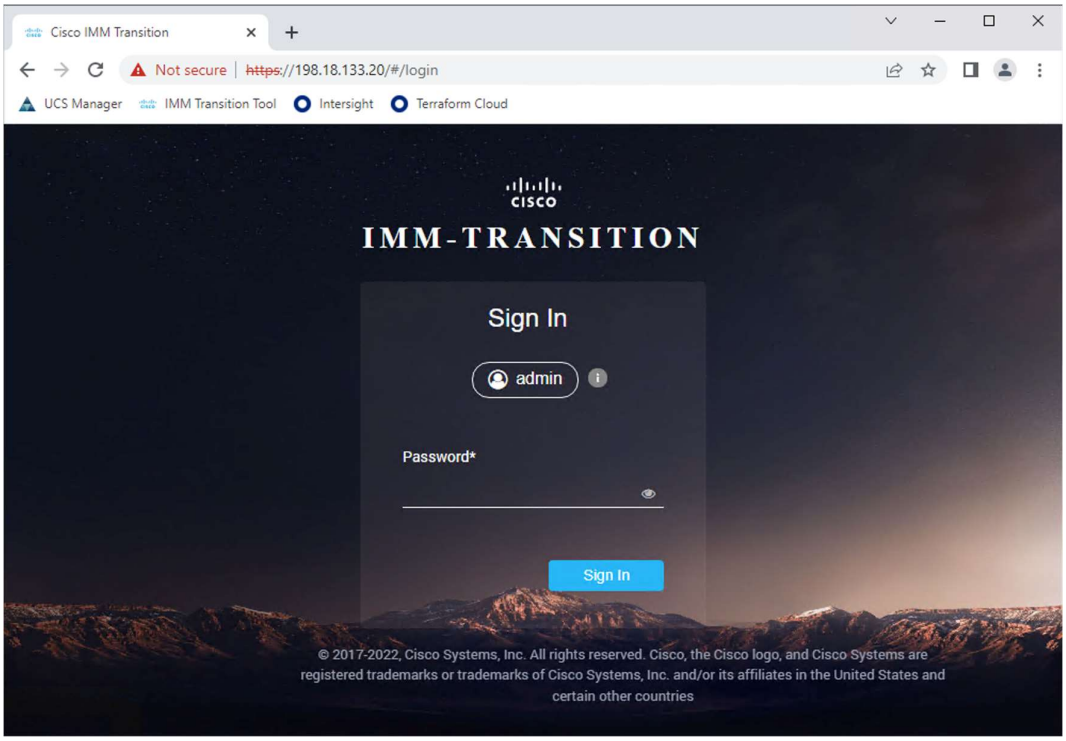
Step 3 Click on the **Servers** tab and notice that your pod has 9 Service Profiles as well as two Service Profile Templates. View the templates and service profiles to see how your pod is configured.



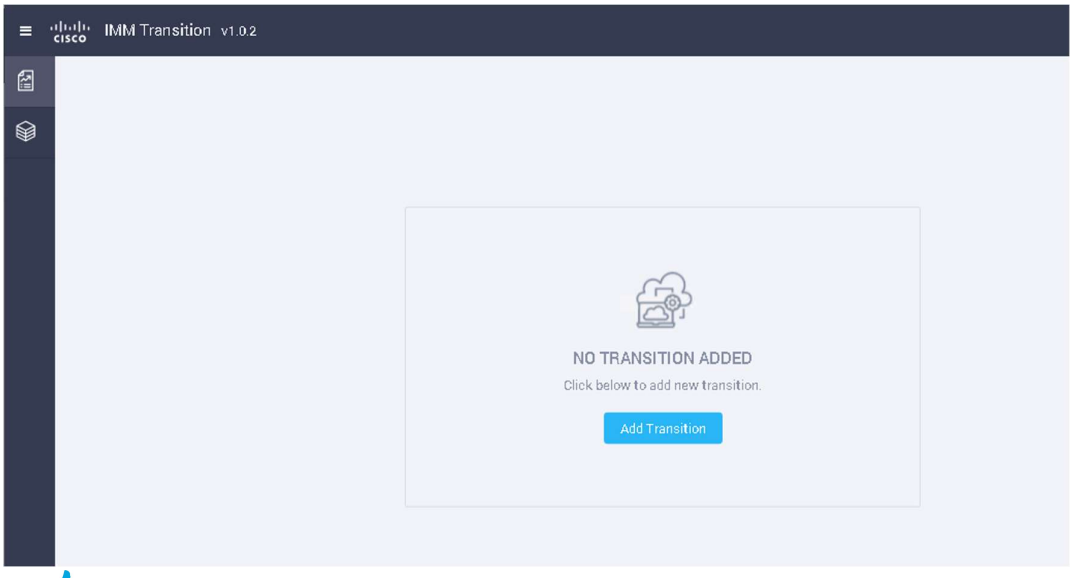
Task 2: Export the Brownfield UCS Config using the IMM Transition Tool

In this task you will connect to the IMM Transition Tool, import the UCS Manager configuration, create a readiness report and then convert the config for Intersight. You will then download this converted configuration in JSON format so that it can be manipulated using infra as code practices.

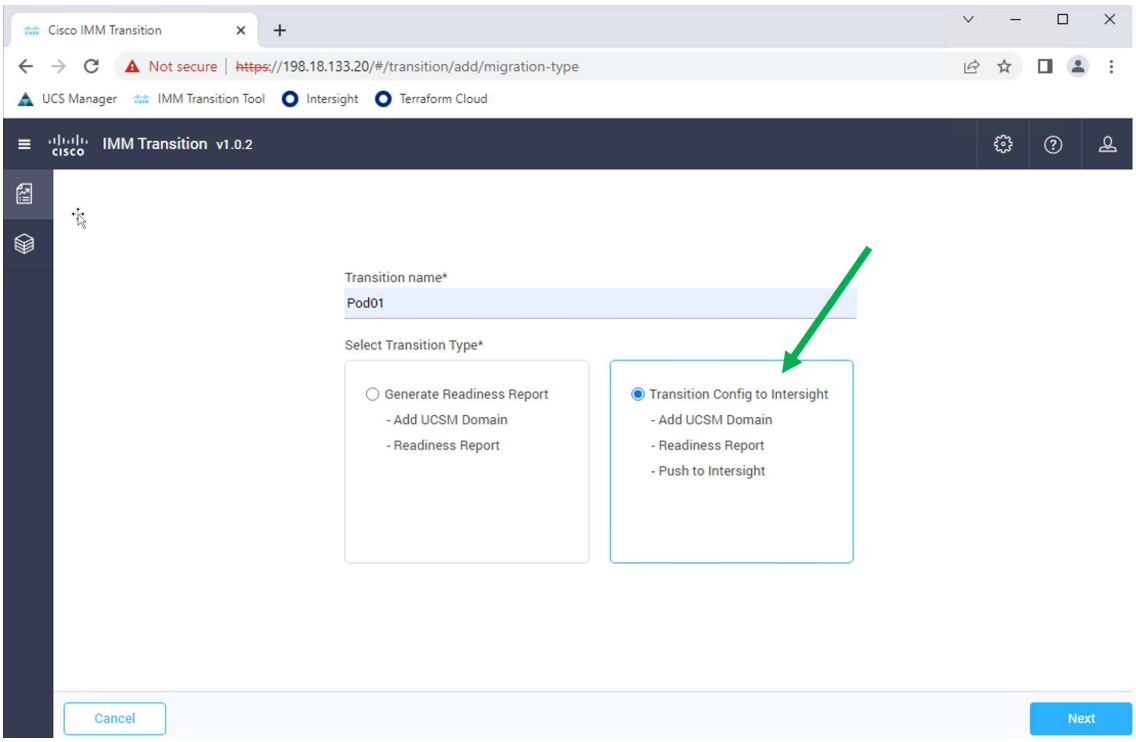
Step 1 Log into the IMM Transition Tool by opening Chrome on the dCloud desktop and click the IMM Transition Tool bookmark (https://198.18.133.20) and login with a username/password of **`admin/C1sco12345`**



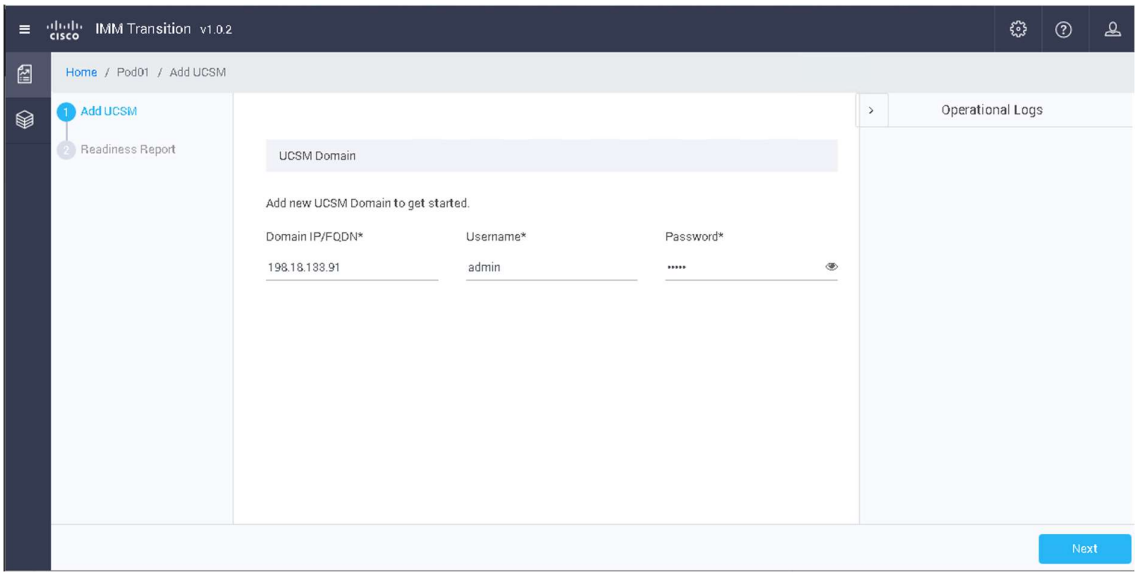
Step 2 Click Add Transition



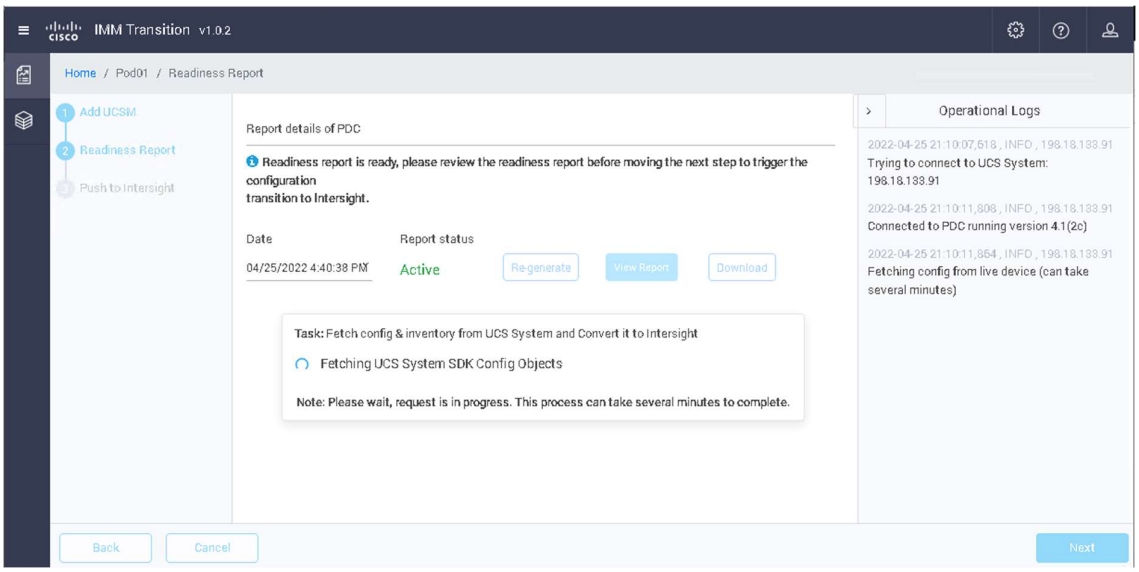
Step 3 Enter a **Transition name** of Pod1XX (where XX is your pod number 01-20), select **Transition Config to Intersight** and click **Next**



Step 4 Enter a **Domain IP** of 198.18.133.91, username **admin** and password **admin** and click **Next.**

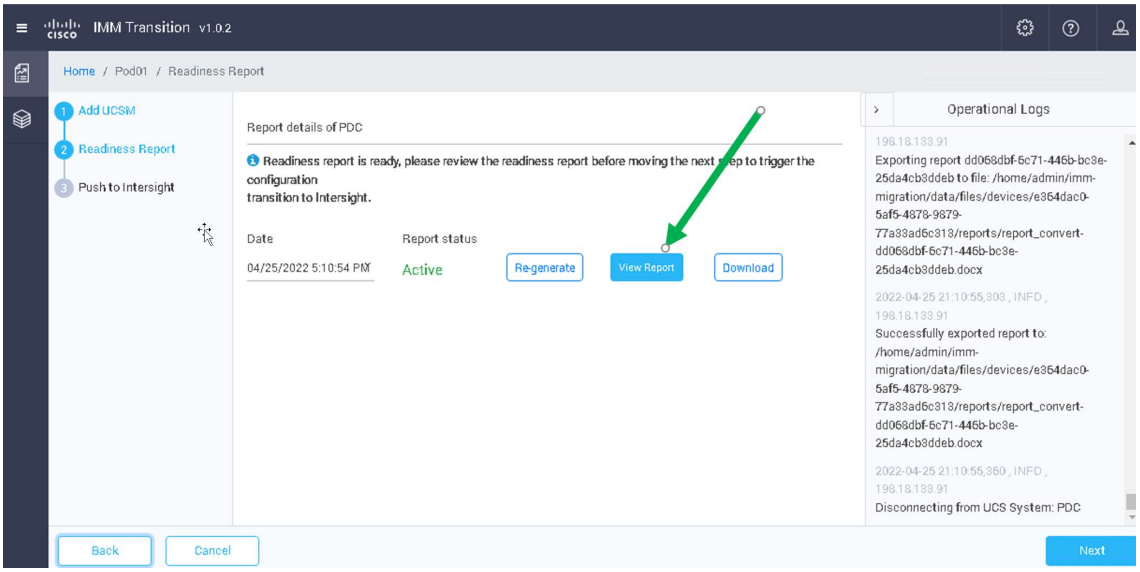


The tool should connect to UCS Manager and fetch the config and inventory:

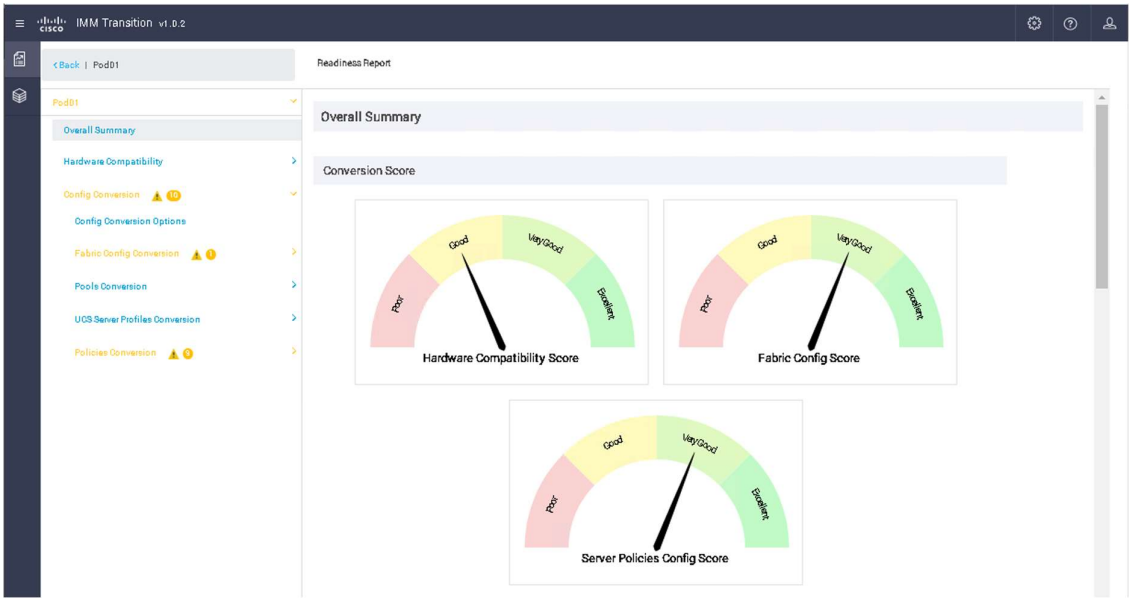


NOTE: If the **Next** button remains greyed out click the  icon in the top left and then select the transition for your Pod # and then the next button should appear.

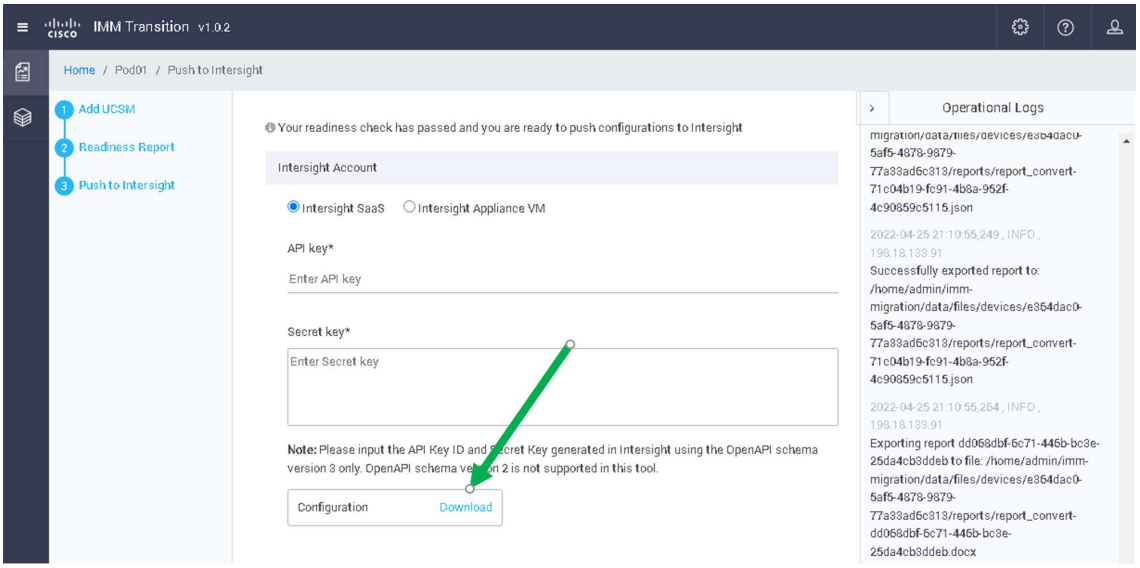
Step 5 Click **Next** to generate the readiness report. Before hitting Next, be sure to **View Report**:



The report will give you a score on hardware compatibility, fabric config and server policies config. Examine the report and the various sections.



Step 6 When done looking at the report, select **Back** and then **Next** which will take you to the **Push to Intersight** screen. Select the **Configuration Download** option which will download your IMM configuration in JSON format into your Downloads folder.



Note: you cannot select Next at the Push to Intersight screen. This is expected proceed to the next step.

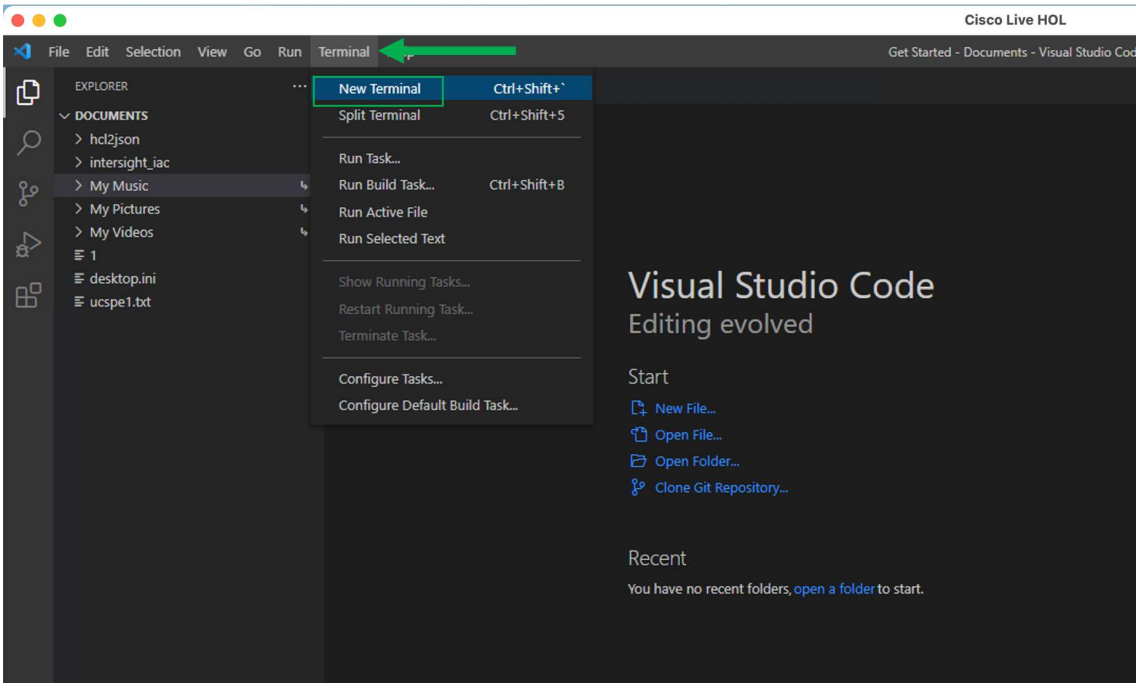
Step 7 Once the JSON config download is complete, you can now select the **Cancel** option in the IMM Transition Tool and go back to the main screen.

NOTE: Although you could have pushed the converted config exactly as it was downloaded from the IMM Transition Tool using the UI, in the next task we will instead switch to a code editor to look at the configuration using infrastructure as code practices.

Task 3: Use Infra as Code Practices to Work with your Imported Brownfield Configuration before pushing it to Intersight

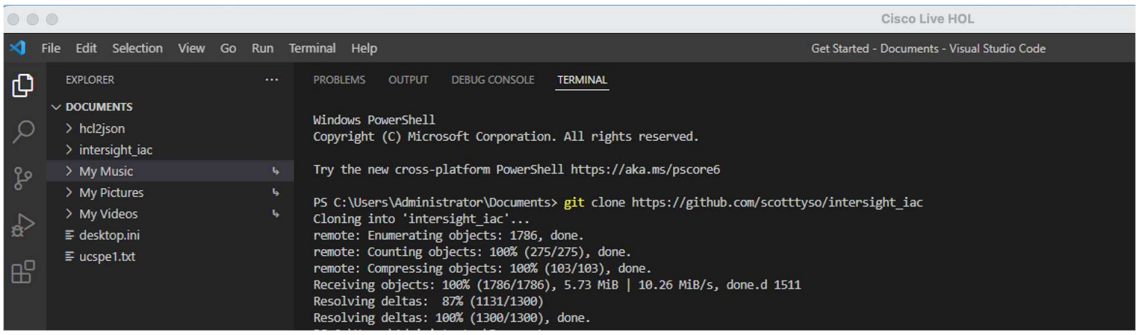
In this task you will download the Intersight IaC Wizard (written in python) by cloning a GitHub code repository. This code will be used to convert your IMM Transition Tool downloaded JSON config from the previous step into Terraform HCL format so your so you can use infrastructure as code practices.

Step 1 Open **Visual Studio Code** from the dCloud workstation desktop and open a **New Terminal** window:



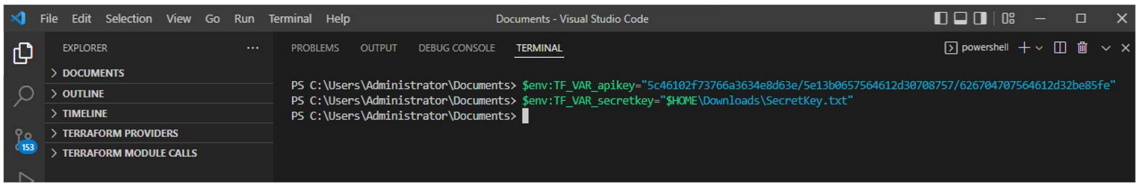
Step 2 From the **Visual Studio Code** terminal, clone the intersight_iac GitHub repository by running the command:

```
git clone https://github.com/scotttyso/intersight_iac
```



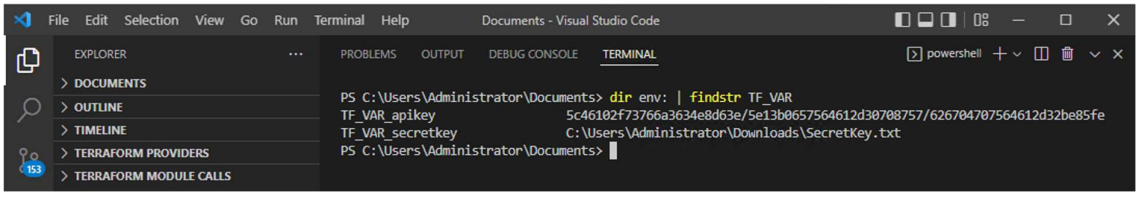
Step 2 Set two environment variables. One for your **Intersight API key ID** and another for the **API secret key filename**. These variables are used by the Intersight IaC Wizard so need to be set prior to running it:

```
$env:TF_VAR_apikey="5c46102f73766a3634e8d63e/5e13b0657564612d30708757/626704707564612d32be85fe"
$env:TF_VAR_secretkey="$HOME\Downloads\SecretKey.txt"
```



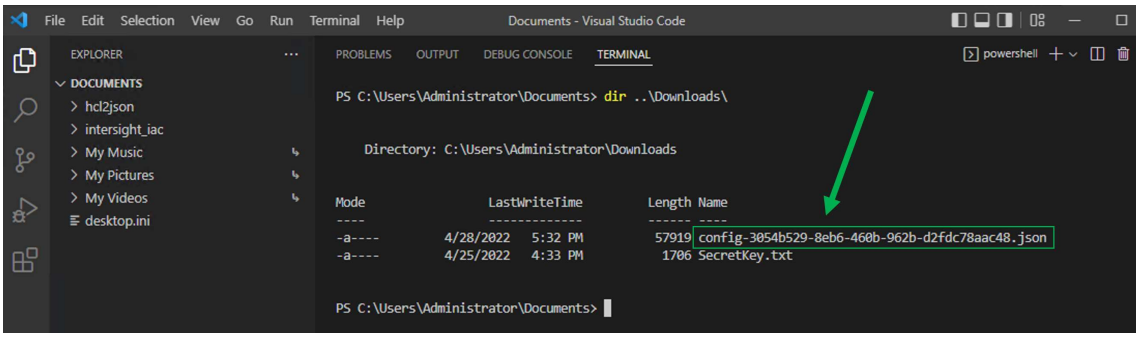
Step 3 Confirm your environment variables are set with the command:

```
dir env: | findstr TF_VAR
```



Step 4 Run the "**dir**" command in the **Downloads** directory to get the filename of the JSON config file you downloaded in the previous task and **copy it to the clipboard**:

```
dir $HOME\Downloads\
```



Step 5 Change to the intersight_iac directory and run the main.py python script on the exported UCS Manager configuration. Change the area in yellow to the filename you downloaded from the IMM Transition Tool in the previous task. Check the Downloads directory for your exact filename.

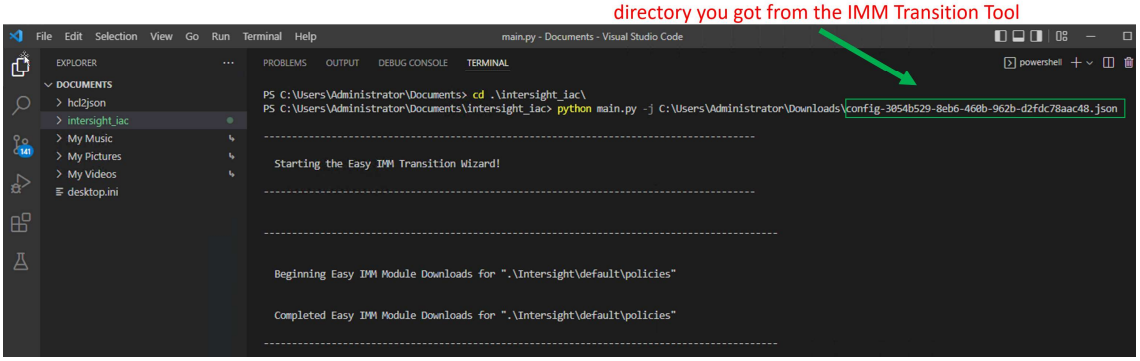
```
cd intersight_iac
python main.py -j $HOME\Downloads\config<press TAB>.json
```

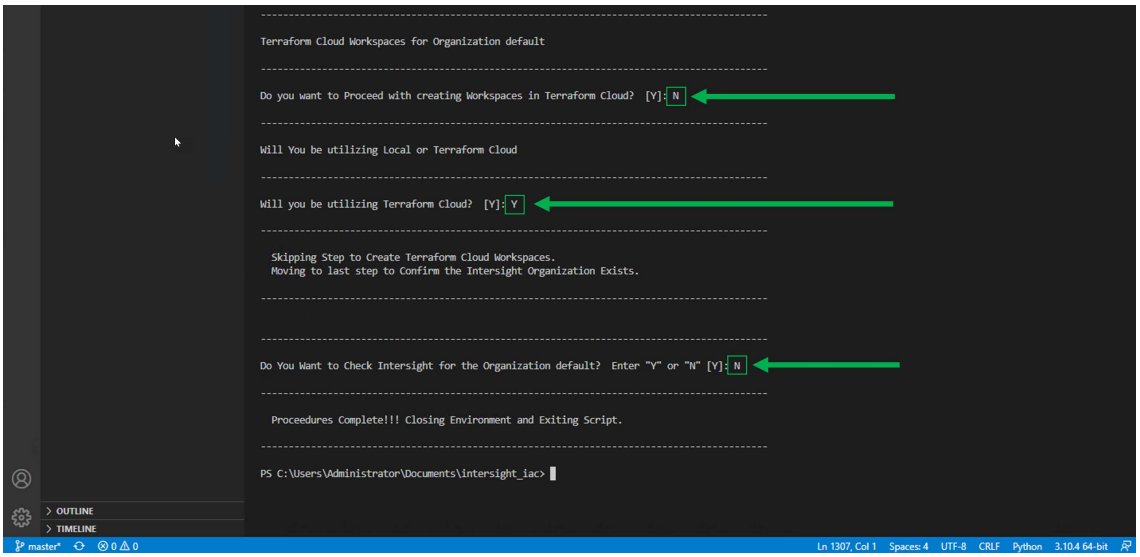
Answer **N** when asked to create the workspaces in Terraform Cloud. The workspaces have already been created for you, so this is not required.

Answer **Y** when asked if you will be utilizing Terraform Cloud. Terraform Cloud will be used later.

Answer **N** when asked "Do you want to Check Intersight for the Organization default".

Replace with your specific config file in your Downloads directory you got from the IMM Transition Tool

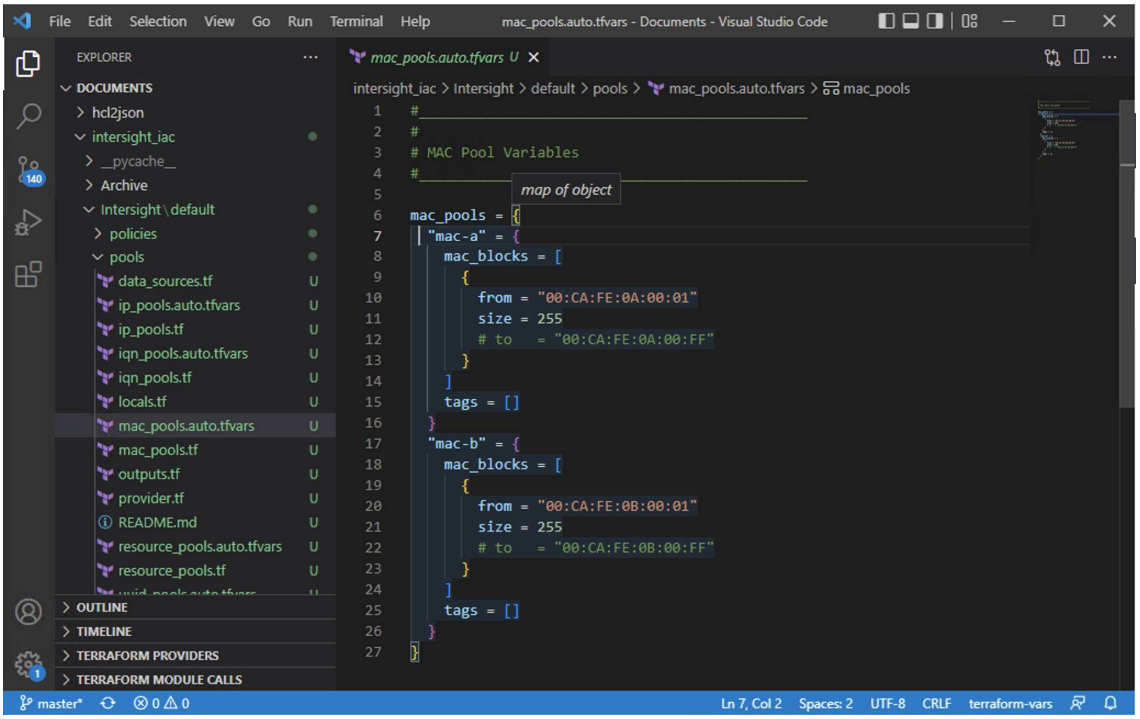




Step 6 Using VS Code, you can now look at your UCS Manager settings that have been converted into Terraform HCL language. For example, look at the following files on the dCloud workstation:

```
intersight_iac > Intersight > default > pools > mac_pools.auto.tfvars
```

Contains two blocks of 255 MAC addresses for each of the sides of your fabric (A and B) called "**mac-a**" and "**mac-b**".



```
intersight_iac > Intersight > default > pools > wwnn_pools.auto.tfvars
```

Contains a block of 255 WWNN addresses so one can be allocated to each host.

```
intersight_iac > Intersight > default > pools > wwpn_pools.auto.tfvars
```

Contains a block of 255 WWPN addresses for each of the sides of your fabric (A and B) called "**wwpn-a**" and "**wwpn-b**".

```
intersight_iac > Intersight > default > profiles >
ucs_server_profiles.auto.tfvars
```

Contains 9 server profiles (Prod-ESXi-1 through 9) all configured for SAN booting.

```
intersight_iac > Intersight > default > ucs_domain_profiles >
ucs_domain_profiles.auto.tfvars
```

Contains a profile for your fabric interconnects and references additional policies for NTP, DNS, QoS, VLAN and VSAN settings.

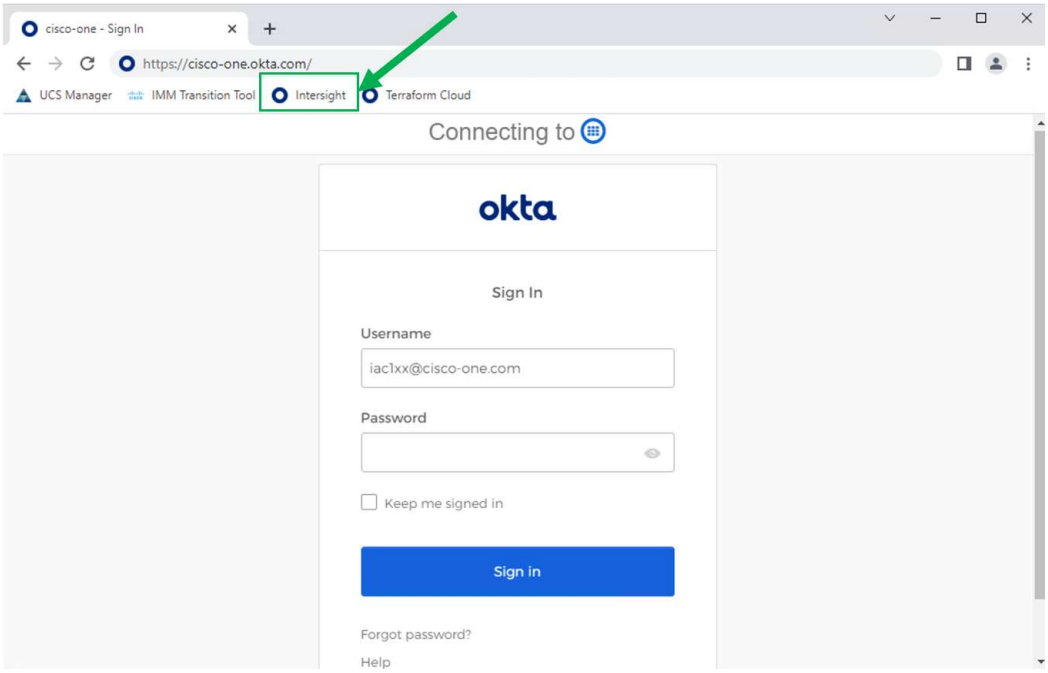
Note that files ending in "`.auto.tfvars`" contain the configurations imported from your UCS Manager domain.

Summary Now that you have converted your UCS Manager domain configuration to Terraform code, you can begin to manage your UCS infrastructure as code.

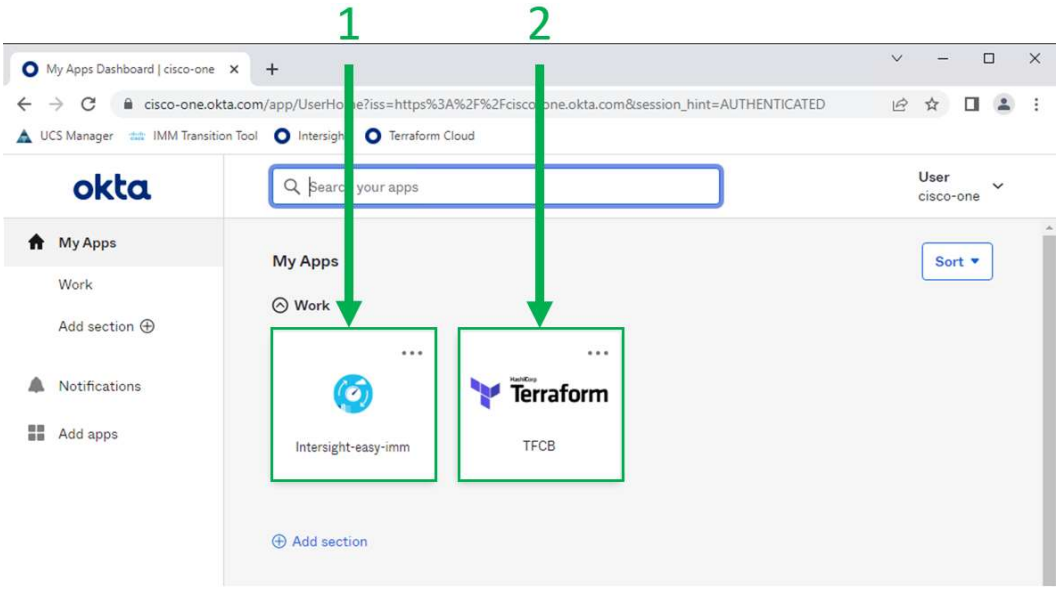
Task 4: Upload Terraform Code UCS Configuration to Intersight using Terraform Cloud

In this task you will now upload Terraform code representing your UCS configuration to Intersight using Terraform Cloud for Business.

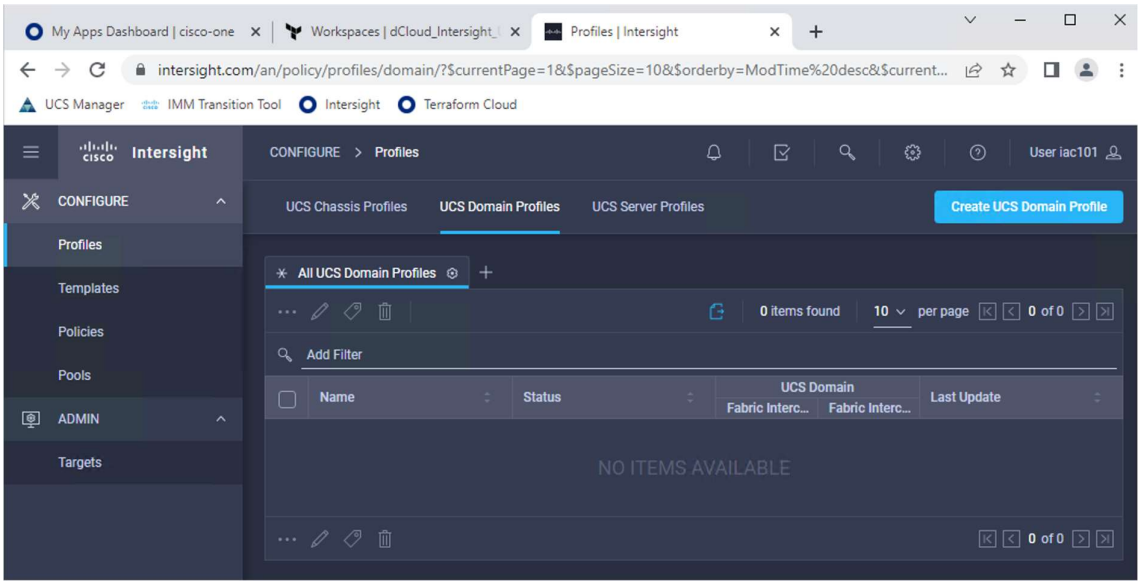
Step 1 From Chrome click on the **Intersight** bookmark (or browse to https://cisco-one.okta.com) and log in with username **iac1XX@cisco-one.com** (where XX is your Pod number 01-20) and password will be "**C1sco12345**".



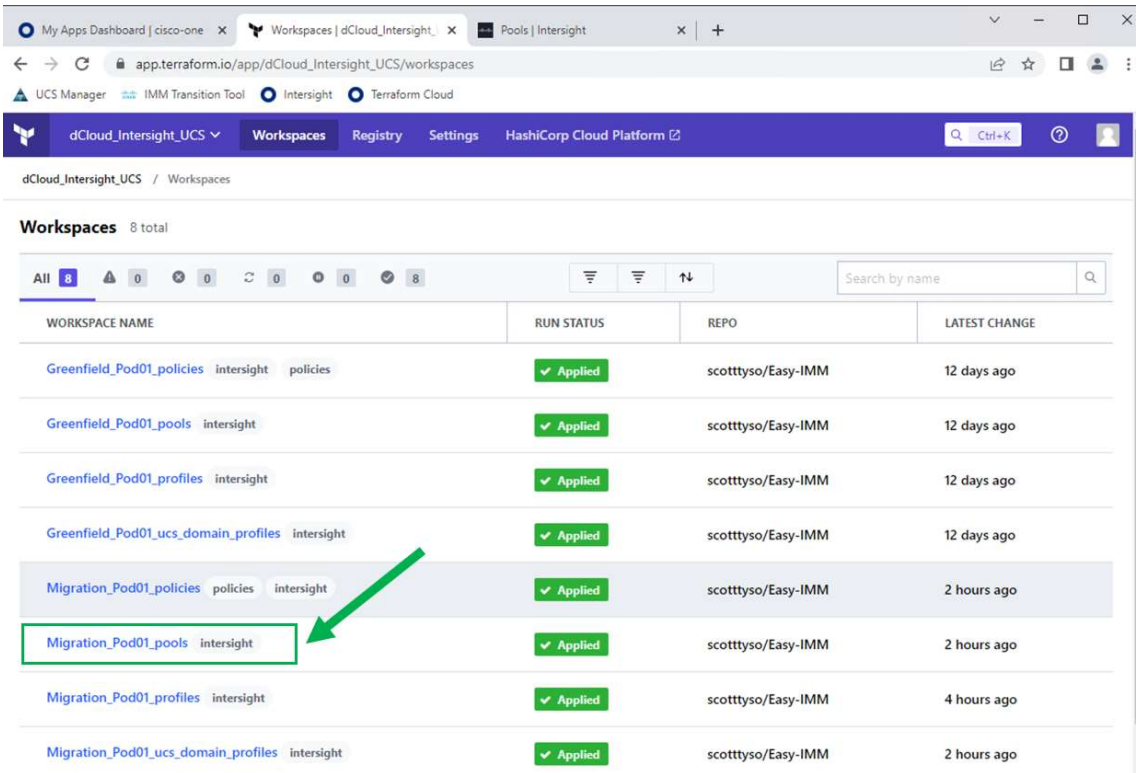
Step 2 From the okta dashboard, open two tabs. One for "**Intersight-easy-imm"** and the other for "**Terraform Cloud for Business"** (TFCB).



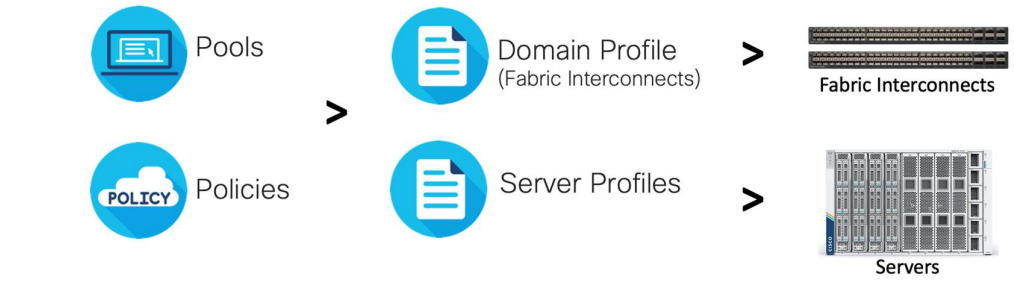
Step 2 From **Intersight**, browse the UCS Domain Profiles, UCS Server Profiles, Policies and Pools and notice that they are all empty.



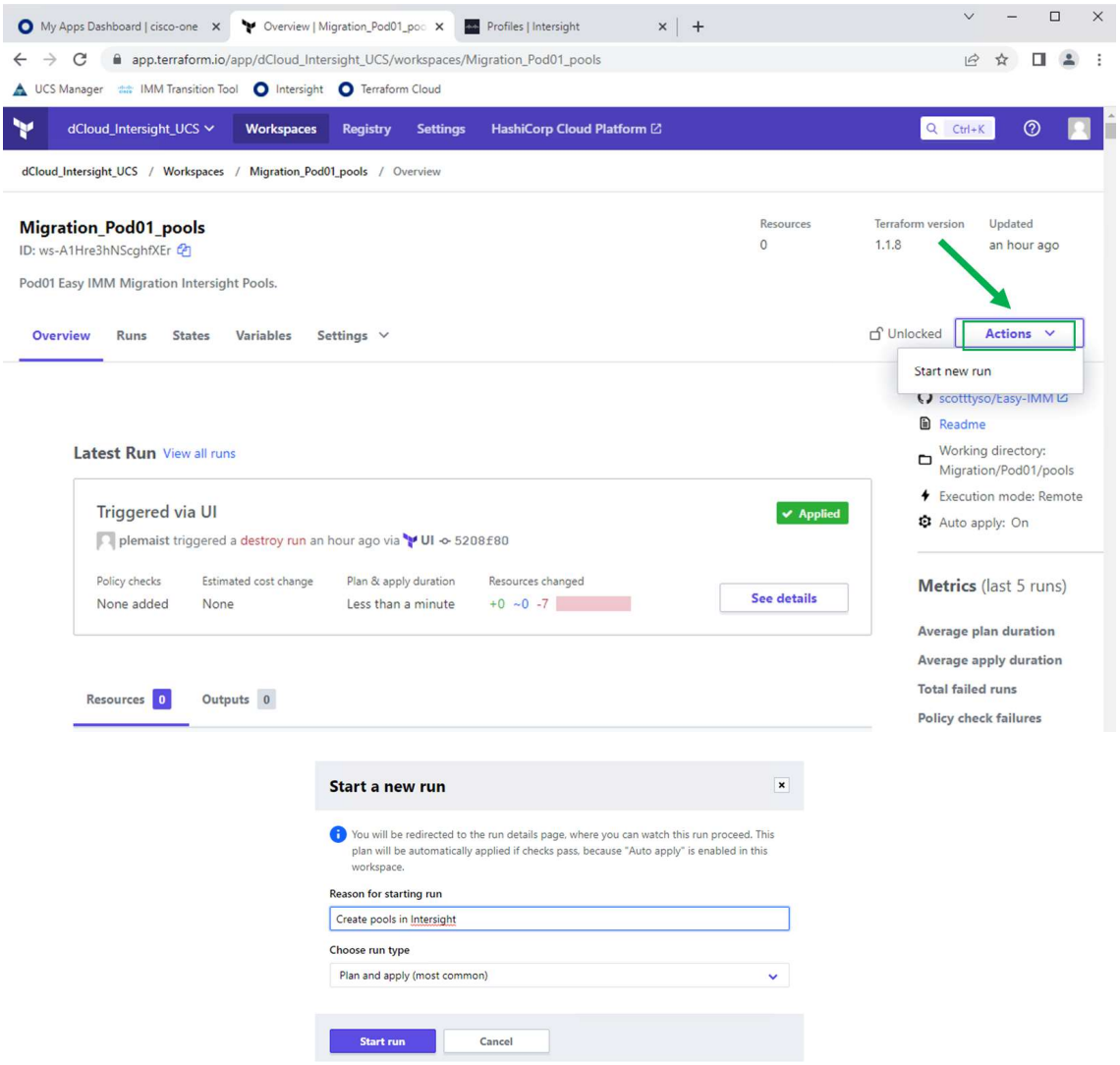
Step 3 From **Terraform Cloud** notice that your pod has 8 workspaces. Four for greenfield and four for IMM migration. Click on the **Migration_Pod_XX_pools** (where XX is your Pod number 01-20) workspace to go into that workspace:



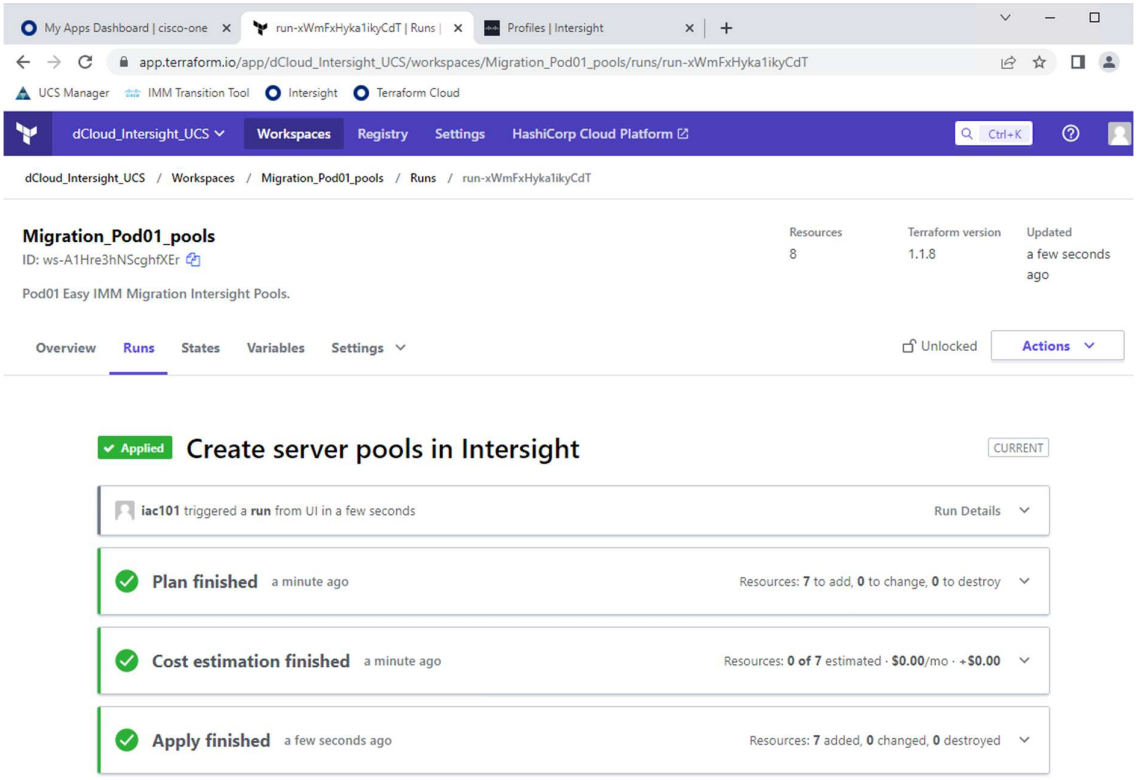
You will use the migration workspaces to create all the pools, domain-policy, policies, and profiles in Intersight. They need to be created in the correct order as the some of the elements are dependent on others. See the diagram below for how they relate to the fabric interconnect and actual server configuration:



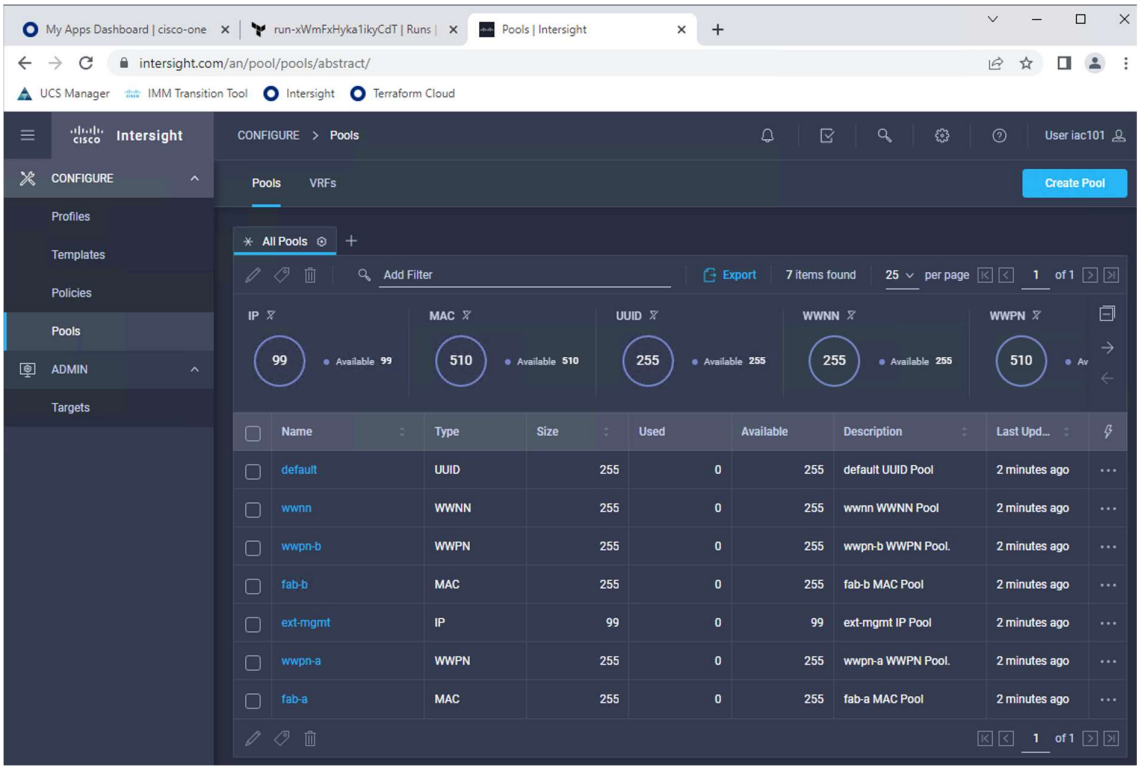
Step 4 From the migration **pools** workspace, select **Action** and then **Start new run.** Specify a **Reason for starting the run** (IE: Create pools in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.



Watch the output shown while the Terraform code from the workspace is both run and applied. Warnings are OK, but errors are not. Upon completion you should see a green checkmark indicating that the apply finished.



Step 5 Now go into **Intersight** and verify that all 7 pools have been created for UUIDs, MAC addresses (fabric a and b), WWNN, WWPN (fabric a and b) and IP addresses for management.

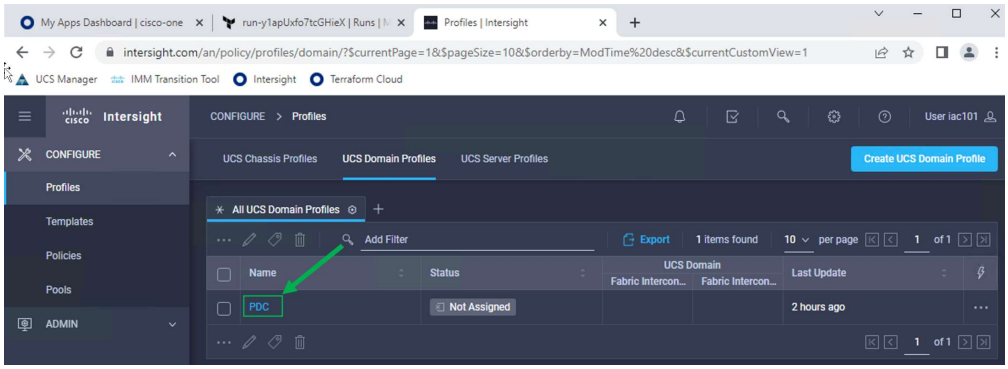


Step 6 Back in **Terraform Cloud**, now go into the **Migration_PodXX_domain_profiles** workspace, click **Actions** and **Start a new run** (where XX is your Pod number 01-20). Specify a **Reason for starting the run** (IE: Create domain-profiles in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.

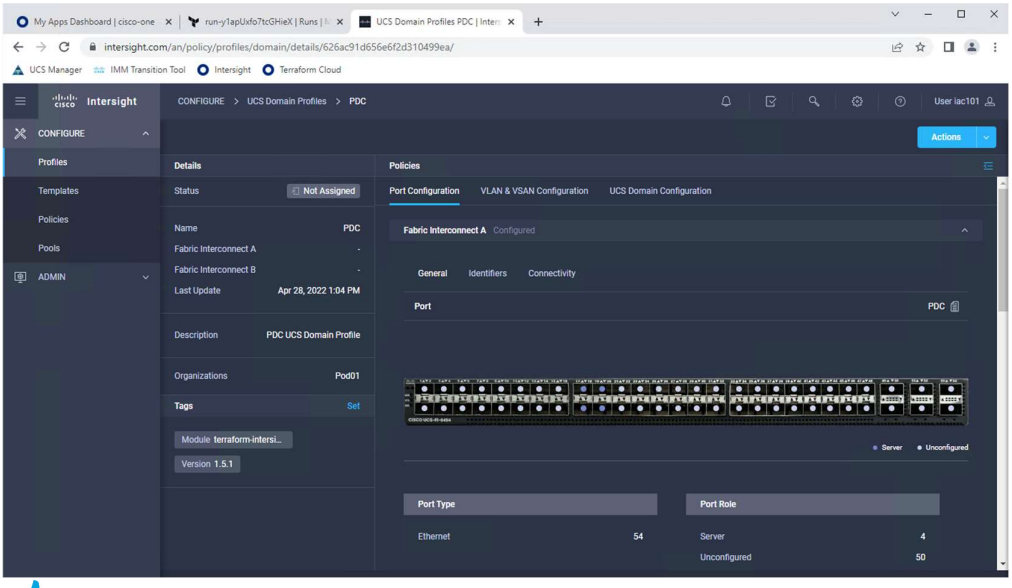
Step 7 In **Terraform Cloud**, now go into the **Migration_PodXX_policies** workspace, click **Actions** and **Start a new run** (where XX is your Pod number 01-20). Specify a **Reason for starting the run** (IE: Create policies in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.

Step 8 In **Terraform Cloud**, now go into the **Migration_PodXX_profiles** workspace, click **Actions** and **Start a new run** (where XX is your Pod number 01-20). Specify a **Reason for starting the run** (IE: Create profiles in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.

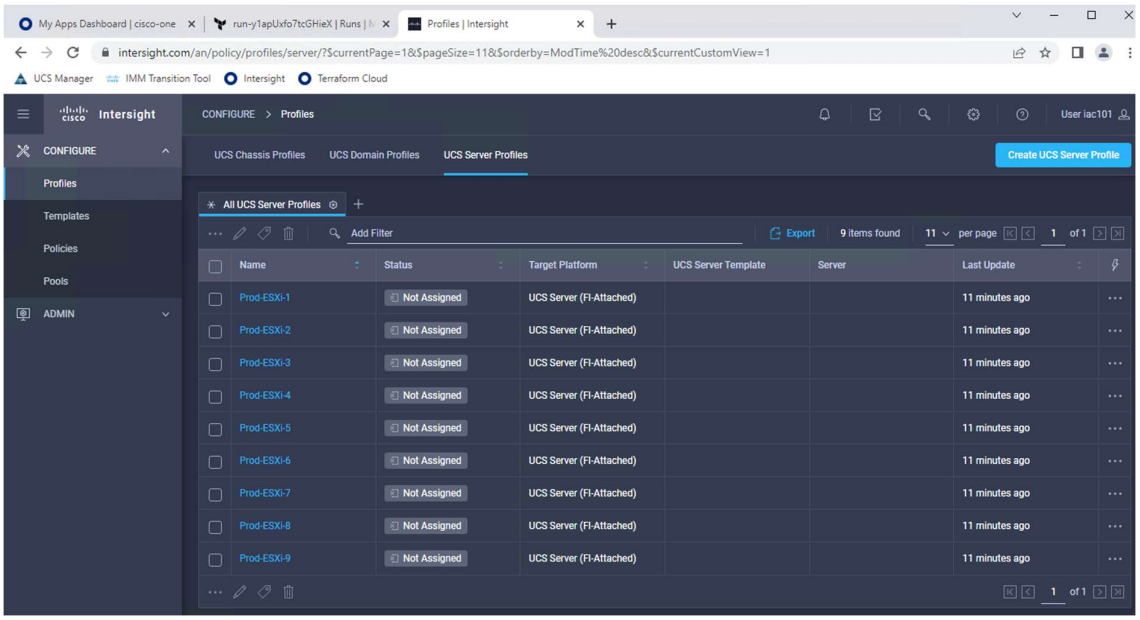
Step 9 In **Intersight**, check that you have a UCS Domain Profile called PDC (short for Primary Data Center).



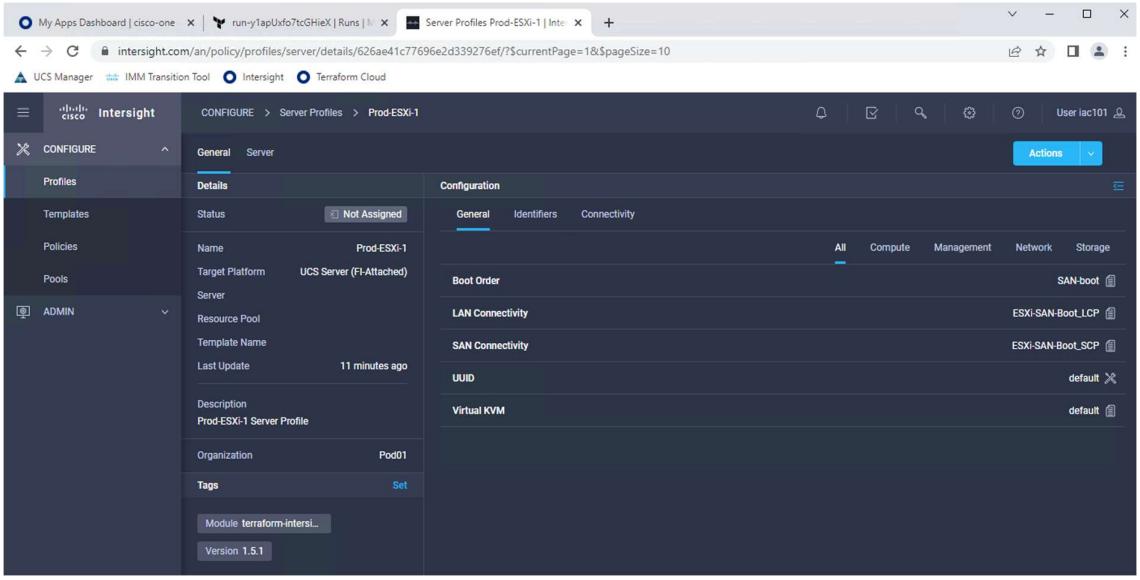
Step 10 Click on the **PDC** domain profile and verify that a port configuration, VLAN & VSAN configuration and domain configuration has taken place because of your domain-profile run in Terraform Cloud.



Step 11 Click on the **UCS Server Profiles** and verify that 9 server profiles (Prod-ESXi-1 through -9) have been created.



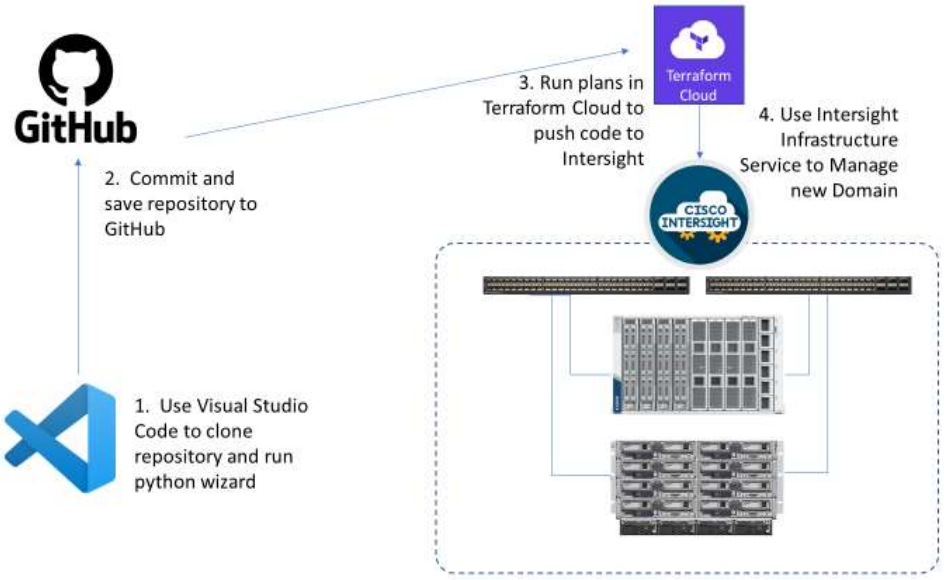
Step 12 Click on one of the UCS Server Profiles and verify the configuration has been created.



Summary Now that you have built server profiles via Terraform in Intersight, these profiles can be assigned to physical servers.

Scenario 2: Build a New UCS Domain in Intersight Managed Mode (IMM)

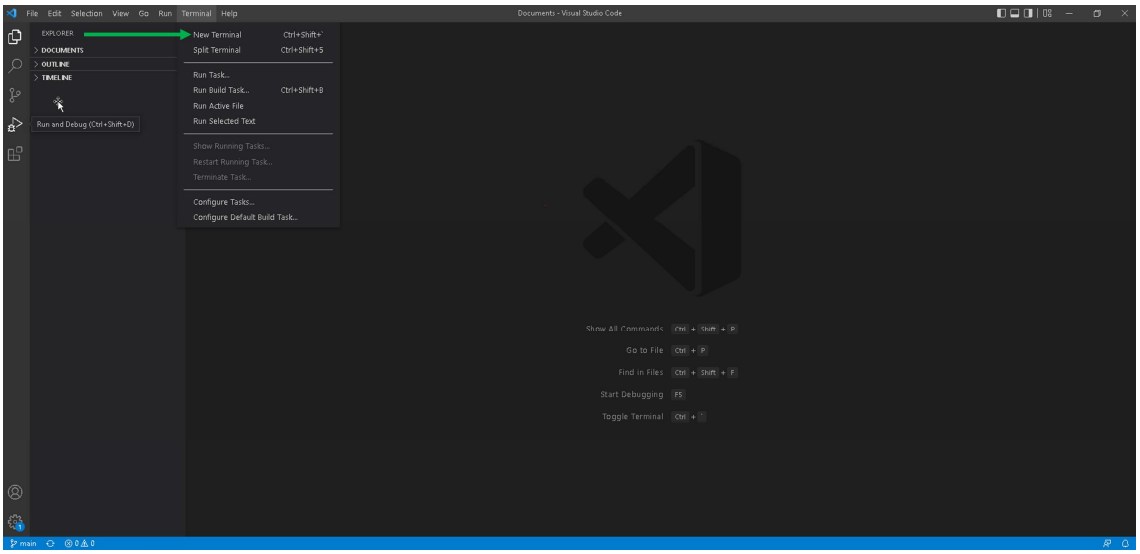
Diagram



In this scenario you will build out an Infrastructure as Code (IaC) repository to deploy a greenfield domain, including server profiles via the python intersight_iac wizard. The purpose of the wizard is to assist customers in building their first domain. Once the first domain is deployed you can continue to build additional domains in a different folder, but you can also build additional domains in the repository via the generated HCL files with the more traditional IaC methodologies. But often the hardest part of adopting automation/IaC is setting it up for the first time and build/test scenarios. The wizard is built to help you get past that initial hurdle of your first step.

Task 1: Setup the environment with the repository and variables

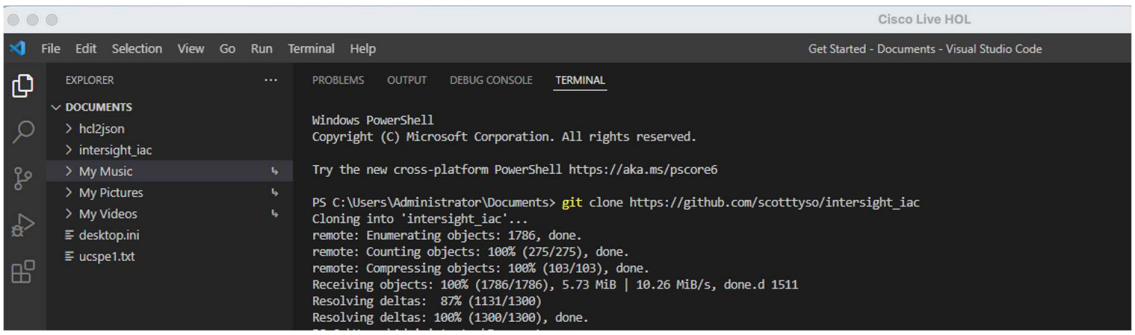
Step 1 If you already completed **Scenario 1**, and Visual Studio Code is still open, skip to **Step 4**. If not, Open **Visual Studio Code** from the dCloud workstation desktop and open a **New Terminal** window:



Note: The dCloud Jump Station has already been pre-configured with Python, Visual Studio Code, git, and other pre-requirements. If you want to perform these same steps within your own environment, make sure to follow the step-by-step instructions in the intersight_iac README file to prepare your system.

Step 2 If you already completed **Scenario 1**, skip to **Step 4**. If not already complete, from the **Visual Studio Code** terminal, clone the intersight_iac GitHub repository by running the command:

```
git clone https://github.com/scotttyso/intersight_iac
```

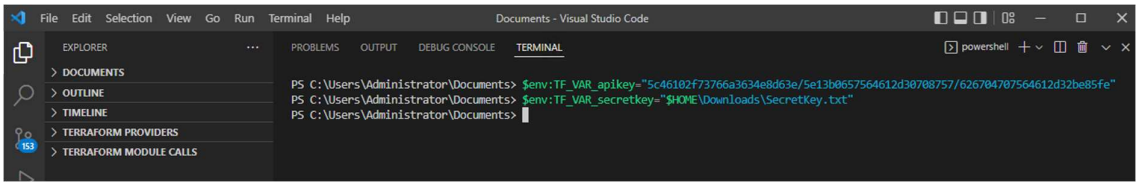


Step 3 If you completed **Scenario 1** and still have your terminal session open, skip to **step 4**. Otherwise, set two environment variables. One for your **Intersight API key ID** and another for the **API secret key filename**. These variables are used by the Intersight IaC Wizard, so they need to be set prior to running the wizard:

```
$env:TF_VAR_apikey="5c46102f73766a3634e8d63e/5e13b0657564612d30708757/626704707564612d32be85fe"
$env:TF_VAR_secretkey="$HOME\Downloads\SecretKey.txt"
```

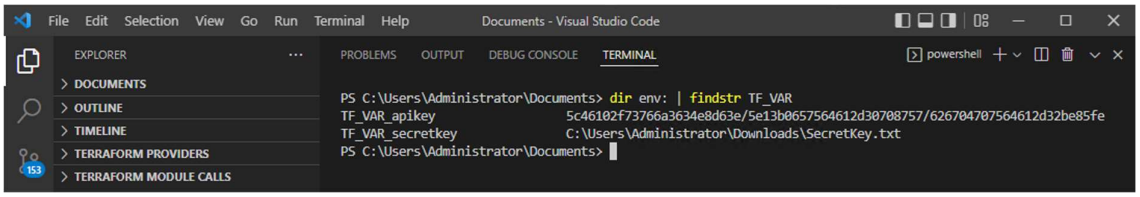
Note: The API key and Secret Key are not valid values. These were generated in Intersight but have since been invalidated. If you were to run these same steps for your environment, you would want to generate an API key and Secret to authenticate to your Organization's Intersight instance. The script will prompt for the API key and Secret if they are not entered before running the wizard, which is why we are entering them in this step, even if they are invalid.

The API key version for the Intersight Terraform provider is Version 2. Version 2 and Version 3 can be used by the Python SDK.



Step 4 Confirm your environment variables are set with the command:

```
dir env: | findstr TF_VAR
```



Step 5 Change to the intersight_iac directory

```
cd intersight_iac
```

Step 6 In the previous scenario we used the **"-j config-[unique-value].json"** option when running the script. The -j option tells the script to run the IMM transition process. Without the -j option it will run the traditional wizard to build a new environment. There are additional options that you can specify as well as is shown below:

```
PS C:\Users\Administrator\Documents\intersight_iac> ./main --help
usage: main.py [-h] [-a API_KEY_ID] [-d DIR] [-i] [-j JSON_FILE] [-s API_KEY_FILE] [-u URL] [-v]

Intersight Easy IMM Deployment Module

options:
  -h, --help            show this help message and exit
  -a API_KEY_ID, --api-key-id API_KEY_ID
                        The Intersight API client key id for HTTP signature scheme
  -d DIR, --dir DIR     The Directory to Publish the Terraform Files to.
  -i, --ignore-tls      Ignore TLS server-side certificate verification
  -j JSON_FILE, --json-file JSON_FILE
                        The IMM Transition Tool JSON Dump File to Convert to HCL.
  -s API_KEY_FILE, --api-key-file API_KEY_FILE
                        Name of file containing The Intersight secret key for the HTTP signature scheme
  -u URL, --url URL     The Intersight root URL for the API endpoint. The default is https://intersight.com
  -v, --api-key-v3      Flag for API Key Version 3.
PS C:\Users\Administrator\Documents\intersight_iac>
```

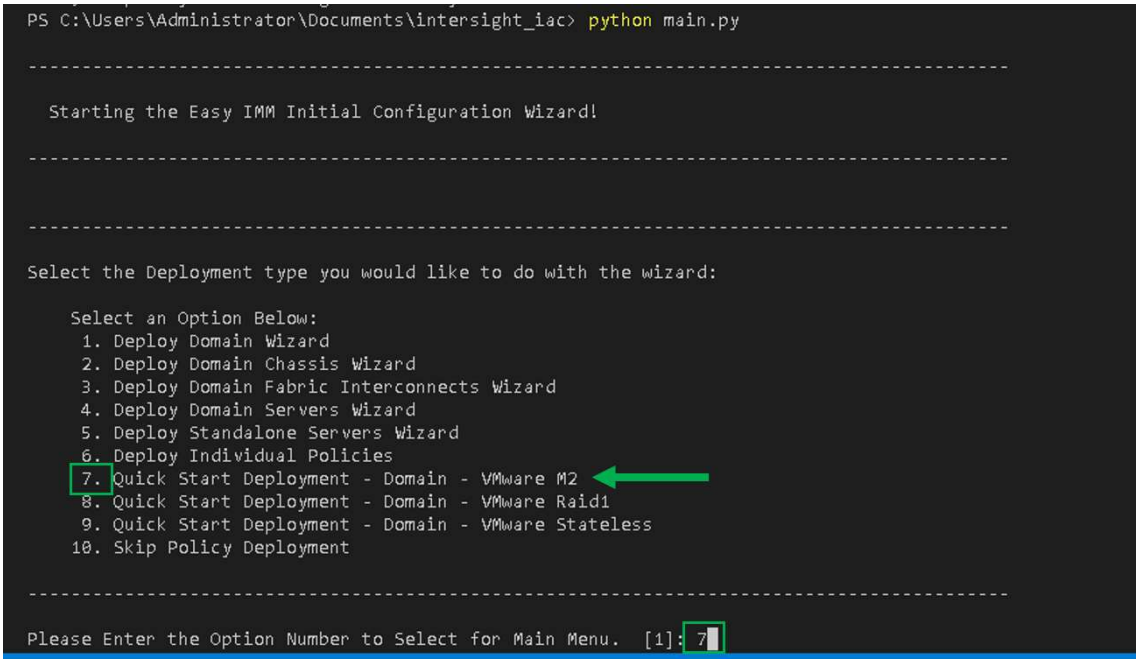
For example, if you are using a private or connected virtual appliance instead of the SaaS delivered service via Intersight.com, you can use the -u option to specify the URL for your environment. Or if you have a separate repository that you want the wizard to create the files in you can use the -d (--dir) option to tell the script to create your files in a different directory on the system.

Note: If the secret key filename is different than **"$HOME\Downloads\SecretKey.txt"** or **"~/Downloads/SecretKey.txt"** on a Linux based system, you need to specify the filename with **"-s secret_file_location"**. The Python SDK credentials function, used by the script, uses the file location instead of the file contents for the authentication process. So, if you are running this in your environment and you do not use the default SecretKey file location, then you need this option to tell the script where the file is located. In this demonstration because we are not using a valid API key, we will be skipping the step of checking Intersight for the existence of the Organization.

Task 2: Run the Python Wizard to build the Domain Pools, Policies, and Profiles.

Step 1 Start the wizard by executing the command in the Visual Studio Code PowerShell Session:

```
python main.py
```



There are multiple options that you can choose when running the wizard, and you can play around with any of these that you want to generate the tfvars files. Options 1 – 6 asks more questions than the "Quick Start Deployments" because they are meant to allow you to fully customize the pools, policies, and profiles to your environment. But the wizards for these are much longer (100's of questions longer) because it will ask for all the customized inputs. We will use the VMware M2 quick start as this will provide a good demonstration of the tool. Notice that the wizard can do deployments for domain-based servers or standalone deployments (options 1 – 4 versus option 5).

Note: When the wizard has the brackets, [], at the end of the question, this means the value shown is the default value selected by pressing enter. We will be using mostly the default values in this demo but, if you are using this for your own environment, you should enter the values that would be suitable for your systems.

Step 2 Enter the Organization Name **"Greenfield"**, which is the name of the Intersight Organization where the objects will be created. We are using this name just for demonstration purposes, as the repo will be pre-configured with the Organization of "**PodXX**" (where XX is your Pod number 01-20), as the Organization Name:

```
What is your Intersight Organization Name?  [default]: Greenfield
```

Note: The Organization name is used in a few capacities related to the wizard. First it will become the first level folder in the destination directory where the files will be stored. Second it is the Intersight organization. In this lab the pre-created code in GitHub is assigned based on your Pod ID, "Pod1XX". In the previous scenario we used the default organization, as we are only going through the steps for demonstration, but here we will use the Pod ID to not overwrite what we already did for our Brownfield migration.

At the beginning of each section the script will provide guidance towards what it is creating, and where you can find the files it will create. The purpose for this, is to allow you to review the outputs and to guide you on how you can maintain these files without the use of the wizard, as your comfort level grows.

```
--------------------------------------------------------------------------------

  The Quick Deployment Module - Pools, will configure pools for a UCS Server Profile
  connected to an IMM Domain.

  This wizard will save the output for these pools in the following files:

  - Intersight\Greenfield\pools\ip_pools.auto.tfvars
  - Intersight\Greenfield\pools\mac_pools.auto.tfvars
  - Intersight\Greenfield\pools\uuid_pools.auto.tfvars
  - Intersight\Greenfield\pools\wwnn_pools.auto.tfvars
  - Intersight\Greenfield\pools\wwpn_pools.auto.tfvars

--------------------------------------------------------------------------------

Do You Want to run the Quick Deployment Module - Pools?  Enter "Y" or "N" [Y]:
```

Step 3 Press Enter to select the default value of [Y] to start the Pools section of the wizard. For each of the questions in the Pools section you can select the default value or enter your own value. The purpose of this walkthrough is for you to see what it can do, so feel free to enter whatever you would like in response to each of the questions. But come back to the instructions once you are asked for the prefix of the MAC/WWNN/WWPN Pools. Below is the output from selecting the default values:

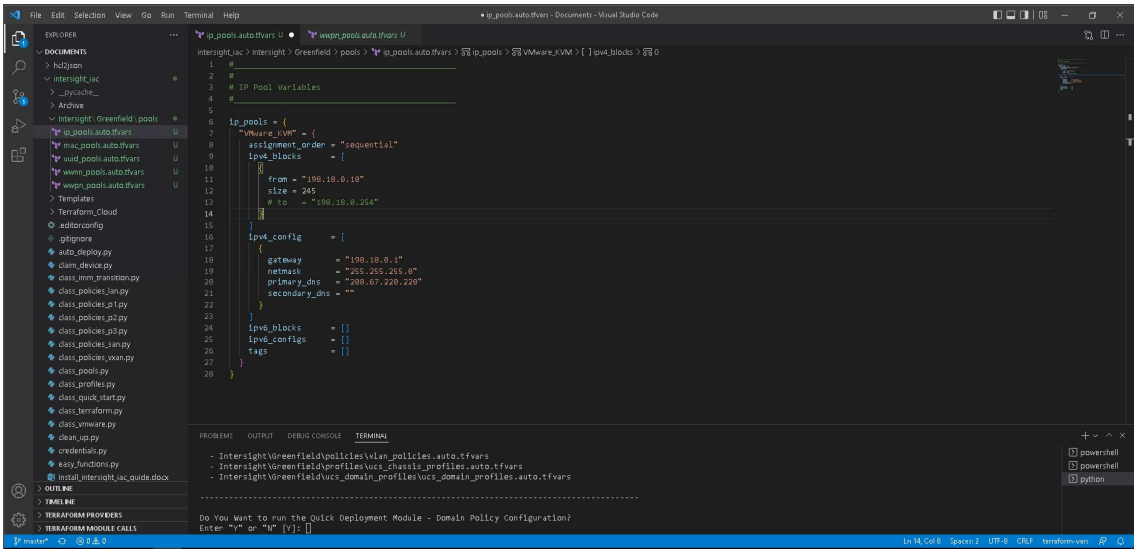
```
--------------------------------------------------------------------------------

IP address of the default IPv4 gateway.

--------------------------------------------------------------------------------

What is the Gateway for the KVM IP Pool? [198.18.0.1]:

--------------------------------------------------------------------------------

A subnet mask is a 32-bit number that masks an IP address and divides the IP address
into network address and host address.

--------------------------------------------------------------------------------

What is the Netmask for the KVM IP Pool? [255.255.255.0]:

--------------------------------------------------------------------------------

IP Address of the primary Domain Name System (DNS) server.

--------------------------------------------------------------------------------

What is the Primary Dns for the KVM IP Pool? [208.67.220.220]:

--------------------------------------------------------------------------------

IP Address of the secondary Domain Name System (DNS) server.

--------------------------------------------------------------------------------

What is the Secondary Dns for the KVM IP Pool? [press enter to skip]:

--------------------------------------------------------------------------------

First IPv4 address of the block.

--------------------------------------------------------------------------------

What is the First IP Address for the KVM IP Pool? [198.18.0.10]:

--------------------------------------------------------------------------------

Last IPv4 address of the block.

--------------------------------------------------------------------------------
```

```
--------------------------------------------------------------------------------------------

What is the Last IP Address for the KVM IP Pool? [198.18.0.254]:

--------------------------------------------------------------------------------------------

Prefix to assign to Pools

--------------------------------------------------------------------------------------------

What is the 2 Digit (Hex) Prefix to assign to the MAC, UUID, WWNN, and WWPN Pools? [00]:

--------------------------------------------------------------------------------------------

  KVM IP Pool Variables:"
    Gateway       = "198.18.0.1"
    Netmask       = "255.255.255.0"
    Primary DNS   = "208.67.220.220"
    Secondary DNS = ""
    Starting IP   = "198.18.0.10"
    Ending IP     = "198.18.0.254"
  Pool Prefix for the rest of the Pools = "00"

--------------------------------------------------------------------------------------------

Do you want to accept the above configuration?  Enter "Y" or "N" [Y]:
```

After you enter the prefix for the pool the script will prompt you to confirm the values you have entered for the section. This is an opportunity to run through the section again if you entered any information incorrectly or to confirm that you want to accept the values. The script will pause for confirmation at the end of each section. If you choose to answer no, then the script will run through all the questions of that section again.

Step 4 After selecting [Y] to accept the configuration, pause for a moment, and review the files the script has created. In Visual Studio code browse to the following folder location:

```
intersight_iac > Intersight > Greenfield > pools
```



In the screenshot on the previous page the "ip_pools.auto.tvars" file is displayed. Note that the values entered answered during the wizard have been entered into the file in the HCL format. This file is created using a map of objects, which means that this is just one block of values. If you wanted to create another IP Pool in the file, it is a straightforward process to copy the VMware_KVM block and paste another object block. Also note that the pool supports IPv6, but we are not using IPv6 in this demo. They are there if you are using IPv6 in your environment.

You are more than welcome to review the other pool files to review as well but just note that they are there as well. We will now move on to the Domain Policies Section.

Step 5 Press enter [Y] to begin the Domain Policies Wizard Section. Enter the name for the UCS domain. For the demo we will use **"greenfield-ucs"**:

```
What is the name for this UCS Domain? greenfield-ucs
```

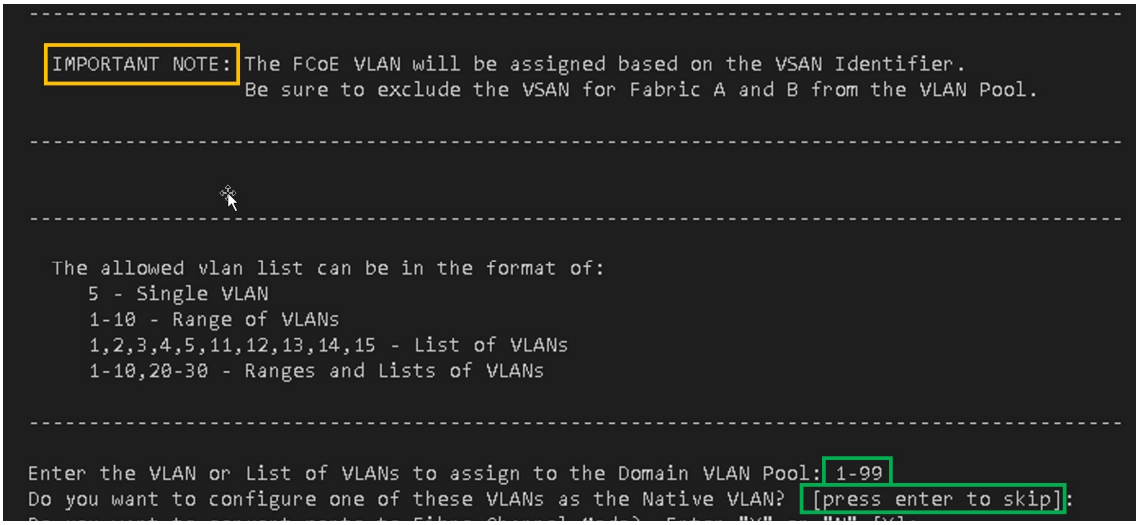
Step 6 We will select the default FI Model of **UCS-FI-6454**:

```
    Select an Option Below:
      1. UCS-FI-64108
      2. UCS-FI-6454
      3. unknown

------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Device Model.  [2]:

------------------------------------------------------------------------------------------
```

Step 7 Because we are not assigning the Domain Profile to equipment, for this demo we will press enter to skip the Serial Number entry. The Serial Number is used by Terraform to assign the Physical resource to the profile when the plan is applied. But since our environment does not yet have physical resources, we will create the profile without the serial numbers. This is meant to provide the ability to pre-provision an environment before resources are available. Or in our case, we will use this for demonstration purposes:

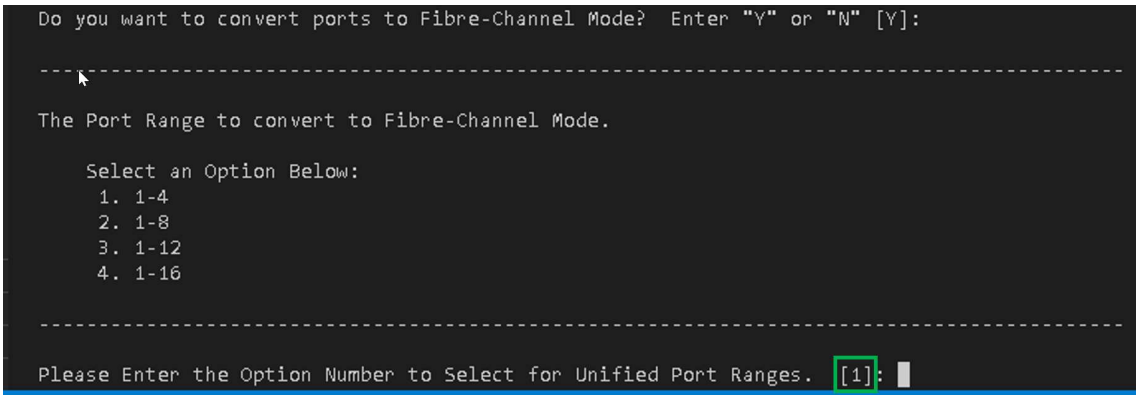
```
  Note: If you do not have the Serial Number at this time you can manually add it to the:
        - ucs_domain_profiles/ucs_domain_profiles.auto.tfvars file later.

------------------------------------------------------------------------------------------

What is the Serial Number of Fabric A? [press enter to skip]:
What is the Serial Number of Fabric B? [press enter to skip]:

------------------------------------------------------------------------------------------
```

Step 8 Enter a range of VLANs to assign to the VLAN Pool, below we have entered 1-99:



Note: There are guidance notes throughout the wizard. Like the above "IMPORTANT NOTE". In this case the guidance is that the FCoE VLAN, which will be based on the VSAN identifier, cannot be included in the VLAN pool range, so the wizard is warning you to make sure to exclude your VSAN ids from the pool range.

Step 9 Configure the Unified ports for Fibre-Channel Mode. The ASIC Port groups on the 6400 FI's are groups of four. That is why the ranges are displayed as groups of four. We will select the default "1-4" range:

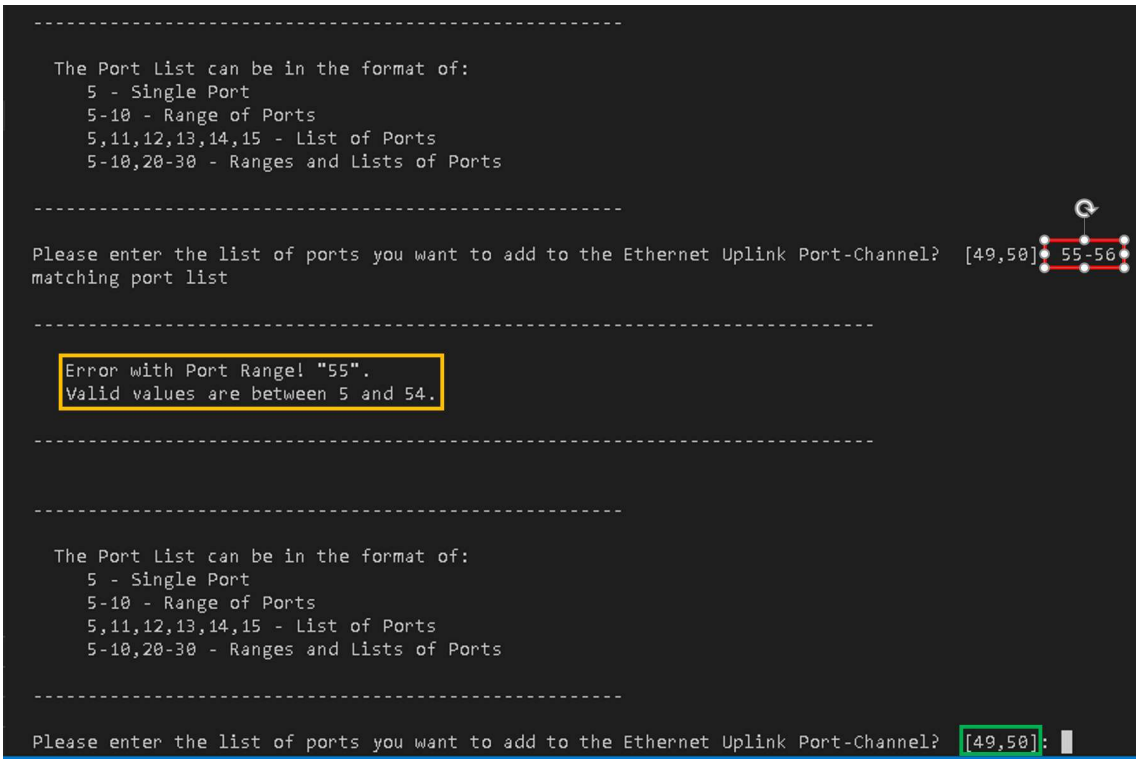


Step 10 Enter the VSAN's for Fabric A and Fabric B. Default is 100 and 200, which you can choose or enter the values for your environment:

Step 11 The Next section will start the configuration for the Port-Channels. Press Enter on the "**Do you want to configure an Ethernet Uplink**." Now enter the range of ports to assign to the Uplink Port-Channel. To Demonstrate error checks, we entered 55-56, which are invalid port ranges for the 6454:

Note: The script is intelligent enough to validate the values you are entering will work with your setup, to a degree 😉. In this case, because a 6454 is 54 ports, it knows that the last available port is 54; 55 and 56 are invalid ports. Also note that in the error message, it tells us the valid range is between 5 and 54. Remember, we have already converted ports 1-4 to Fibre-Channel Mode, they are no longer available as Ethernet Ports. These types of checks will occur for other attributes throughout the wizard. I cannot say there is nothing you can do that I did not cover though. If you find problems, please open a Bug request on GitHub or submit a pull request.

We will move forward, accepting the default value of [49,50], and move to the next step.



Step 12 Select the Speed for the individual ports in the port-channel. We will select Auto [1]:

```
---------------------------------------------------------------------------------------------

Admin configured speed for the port.
 * `Auto` - Admin configurable speed AUTO ( default ).
 * `1Gbps` - Admin configurable speed 1Gbps.
 * `10Gbps` - Admin configurable speed 10Gbps.
 * `25Gbps` - Admin configurable speed 25Gbps.
 * `40Gbps` - Admin configurable speed 40Gbps.
 * `100Gbps` - Admin configurable speed 100Gbps.

    Select an Option Below:
     1. Auto
     2. 1Gbps
     3. 10Gbps
     4. 25Gbps
     5. 40Gbps
     6. 100Gbps

---------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Admin Speed.  [1]:

---------------------------------------------------------------------------------------------
```

Step 13 Now we need to assign the Ethernet Network Group, Flow Control Policy, Link Aggregation Policy, and Link Control Policies to assign to the Port-Channel. The script could have automatically assigned these values for the Quick Start options but with the full deployment options you might have multiple policies that you might want to choose from. These steps are a remnant of the more in-depth wizards where you would be creating multiple policies. In this case just select "**1**" for each of them and confirm to accept:

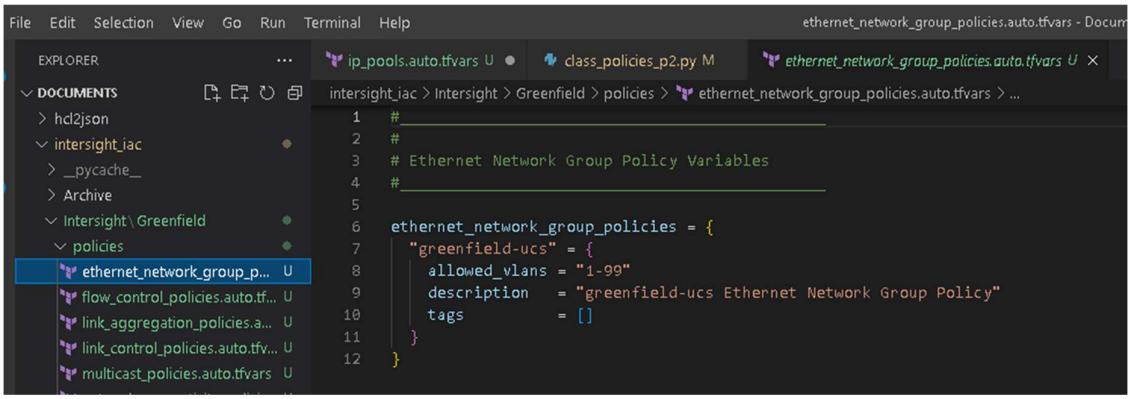
```
---------------------------------------------------------------------------------------------

  Ethernet Network Group Policy Options:
     1. greenfield-ucs
     100. Create a New Ethernet Network Group Policy.

---------------------------------------------------------------------------------------------

Select the Option Number for the Ethernet Network Group Policy to Assign to greenfield-ucs: 1

---------------------------------------------------------------------------------------------

  Flow Control Policy Options:
     1. greenfield-ucs
     100. Create a New Flow Control Policy.

---------------------------------------------------------------------------------------------

Select the Option Number for the Flow Control Policy to Assign to greenfield-ucs: 1

---------------------------------------------------------------------------------------------

  Link Aggregation Policy Options:
     1. greenfield-ucs
     100. Create a New Link Aggregation Policy.

---------------------------------------------------------------------------------------------

Select the Option Number for the Link Aggregation Policy to Assign to greenfield-ucs: 1

---------------------------------------------------------------------------------------------
```

```
------------------------------------------------------------------------------------------

  Link Control Policy Options:
     1. greenfield-ucs
     100. Create a New Link Control Policy.

------------------------------------------------------------------------------------------

Select the Option Number for the Link Control Policy to Assign to greenfield-ucs: 1

------------------------------------------------------------------------------------------

    admin_speed                    = "Auto"
    ethernet_network_group_policy  = "greenfield-ucs"
    flow_control_policy            = "greenfield-ucs"
    link_aggregation_policy        = "greenfield-ucs"
    link_control_policy            = "greenfield-ucs"
    interfaces = [
      {
        port_id = 49
        slot_id = 1
      }
      {
        port_id = 50
        slot_id = 1
      }
    ]
    pc_id     = 49

------------------------------------------------------------------------------------------

Do you want to accept the configuration above?  Enter "Y" or "N" [Y]:
Would You like to Configure another Ethernet Uplink Port-Channel?  Enter "Y" or "N" [N]:
Do you want to configure a Fibre-Channel Port-Channel?  Enter "Y" or "N" [Y]:

------------------------------------------------------------------------------------------
```

Pause: Stepping Away from the Wizard for a Moment: Now that we have finished the ethernet uplink port configuration section, we can review some of the files, and talk about a few use cases you may want to update the attributes in the variable files for.

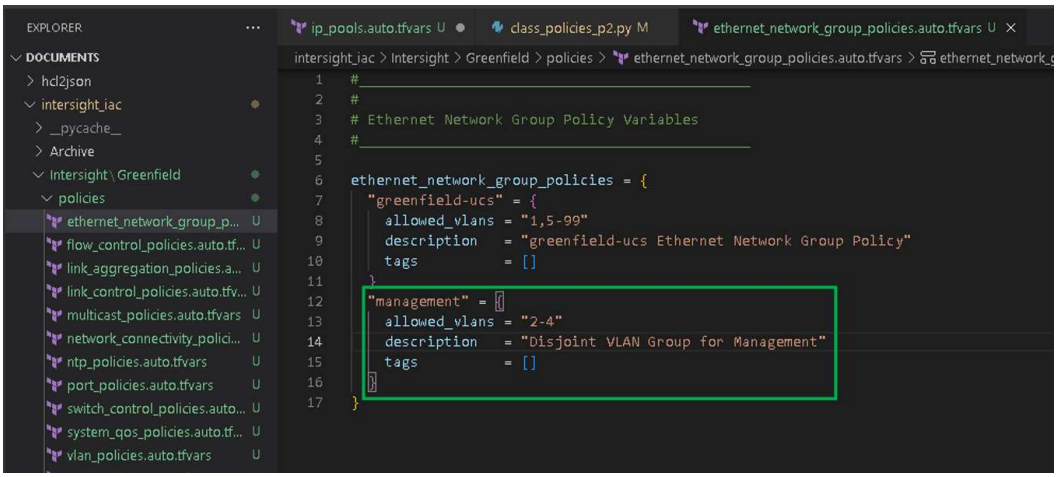
Open the following file:

```
intersight_iac > Intersight > Greenfield > policies >
ethernet_network_group_policies.auto.tfvars
```



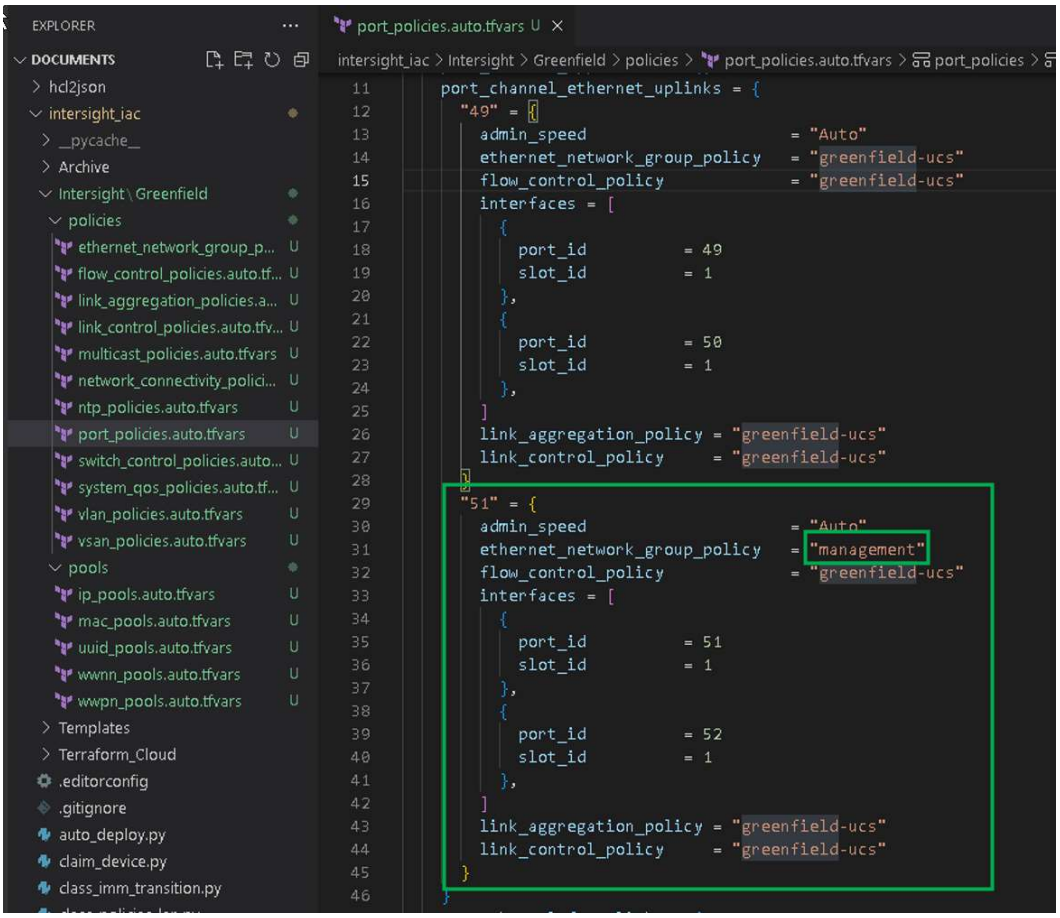
If your environment is utilizing disjoint layer2 for out-of-band management, a DMZ, or other use case. In the full wizard you would have the option of creating multiple policies and you would not need to edit these files manually, but since we ran the quick

start, it created the policies without asking as many questions. What you could do from here is modify the file above and split your VLAN range between the policies. Something like below:



As shown above, I split the VLAN list and moved VLANs "2-4" to the management group.

I can now go and edit the port policies and add the additional uplink to my management environment with this new policy. Like so:



Note: One thing you may notice above is the port_id and slot_id lines have the values way-out to the right. That is because there are other options like breakout ports that might be in the map from the template. The base jinja template lines up the columns

based on all values being entered. But when the optional fields are not shown in the file, this looks out of sorts.

For formatting issues like this, when the wizard is finished, it will run the "**`terraform fmt`**" command in the folders to fix any formatting problems. You can come back to these files after the wizard is complete to confirm, if desired.

Step 14 Configure the Fibre-Channel port-channel:

```
Do you want to configure a Fibre-Channel Port-Channel?  Enter "Y" or "N" [Y]

----------------------------------------------------------------------------------------

    Please Select a Port for the Port-Channel:

     1. 1
     2. 2
     3. 3
     4. 4

----------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Unified Port: 1
Would you like to add another port to the Fibre-Channel Port-Channel?  Enter "Y" or "N" [Y]:

----------------------------------------------------------------------------------------

    Please Select a Port for the Port-Channel:

     1. 1
     2. 2
     3. 3
     4. 4

----------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Unified Port: 2
Would you like to add another port to the Fibre-Channel Port-Channel?  Enter "Y" or "N" [N]:

----------------------------------------------------------------------------------------
```

This is a little more clunky than the ethernet port-channel section. Part of the reason is it needs to verify the port selections against the converted port list. As such, the easier way to make sure the user enters the information correctly is to request values from a menu. Someone could debate other ways would have been better, but this is what I thought would be best when I wrote it.

```
----------------------------------------------------------------------------------------

Admin configured speed for the port.
* `Auto` - Admin configurable speed AUTO ( default ).
* `8Gbps` - Admin configurable speed 8Gbps.
* `16Gbps` - Admin configurable speed 16Gbps.
* `32Gbps` - Admin configurable speed 32Gbps.

    Select an Option Below:
     1. 8Gbps
     2. 16Gbps
     3. 32Gbps

----------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Admin Speed. [3]:

----------------------------------------------------------------------------------------
```

Note: There are times when you see the description and the options available do not match. Like in the example above. The default option is **Auto**, but **Auto** is not an option to select. The reason is the description is from the API documentation, located in the "Templates/variables" folder but the Auto option is not currently supported. I am using the API documentation as much as possible to keep the descriptions accurate as to what Intersight GUI will display, but there are cases like this that show inconsistencies.

```
--------------------------------------------------------------------------------

Fill pattern to differentiate the configs in NPIV.
* `Idle` - Fc Fill Pattern type Idle.
* `Arbff` - Fc Fill Pattern type Arbff.
For Cisco UCS 6400 Series fabric interconnect, if the FC uplink speed is 8 Gbps, set the
fill pattern as IDLE on the uplink switch. If the fill pattern is not set as IDLE, FC
uplinks operating at 8 Gbps might go to an errDisabled state, lose SYNC intermittently,
or notice errors or bad packets.  For speeds greater than 8 Gbps we recommend Arbff.
Belowis a configuration example on MDS to match this setting:

mds-a(config-if)# switchport fill-pattern IDLE speed 8000
mds-a(config-if)# show port internal inf interface fc1/1 | grep FILL
  FC_PORT_CAP_FILL_PATTERN_8G_CHANGE_CAPABLE (1)
mds-a(config-if)# show run int fc1/16 | incl fill

interface fc1/16
  switchport fill-pattern IDLE speed 8000

mds-a(config-if)#


    Select an Option Below:
     1. Arbff
     2. Idle

--------------------------------------------------------------------------------

Please Enter the Option Number to Select for Fill Pattern.  [1]:

--------------------------------------------------------------------------------
```

Those lovely gotchas that you spend time scouring the documentation to find. In the example above, this is an important configuration that you need to configure on the MDS when deploying the FI's if using 8G optics. Again, I hope you will take time to read the tips as there are hidden gems that will save you time if you read along. We will select option "**1**" as we set the speed to 32G above.

Note: I noticed the "**Belowis**" above as well. Fixed in the code but screenshot is good enough for now.

Step 15 Assign the VSAN Policies, created in the background, to each of the Fabric Interconnects and select the VSAN to assign to each policy. There will only be one VSAN in each policy with the quick start:

```
--------------------------------------------------------------------------------

  Vsan Policy Options:
     1. greenfield-ucs-A
     2. greenfield-ucs-B
     100. Create a New Vsan Policy.

--------------------------------------------------------------------------------

Select the Option Number for the Vsan Policy to Assign to greenfield-ucs: 1

--------------------------------------------------------------------------------
```

```
Please Select a VSAN for the Port-Channel:

 1. 100

Please Enter the Option Number to Select for VSAN: 1

  Please Select the VSAN Policy for Fabric_B

  Vsan Policy Options:
    1. greenfield-ucs-A
    2. greenfield-ucs-B
    100. Create a New Vsan Policy.

Select the Option Number for the Vsan Policy to Assign to greenfield-ucs: 2

    Please Select a VSAN for the Port-Channel:

     1. 200

Please Enter the Option Number to Select for VSAN: 1
```

Step 16 Accept the Fibre-Channel Configuration and select the default server port assignment. As mentioned above, the script has again excluded ports "1-4" as they are already in use.

```
    admin_speed      = "32Gbps"
    fill_pattern     = "Arbff"
    vsan_id_fabric_a = 100
    vsan_id_fabric_b = 200
    interfaces = [
      {
        port_id          = 1
        slot_id          = 1
      }
      {
        port_id          = 2
        slot_id          = 1
      }
    ]

Do you want to accept the configuration above?  Enter "Y" or "N" [Y]:
Would You like to Configure another Fibre-Channel Port-Channel?  Enter "Y" or "N" [N]:
Do you want to configure an Server Ports?  Enter "Y" or "N" [Y]:
```

```
Please enter the list of ports you want to add to the Server Ports?  [5-18]:
matching port list

------------------------------------------------------------------------------------------

  port_list = 5-18

------------------------------------------------------------------------------------------

Do you want to accept the configuration above?  Enter "Y" or "N" [Y]:
Would You like to Configure another Server Ports?  Enter "Y" or "N" [N]:

------------------------------------------------------------------------------------------

This option will set the MTU to 9216 if answer is "Y" or 1500 if answer is "N".

------------------------------------------------------------------------------------------

Do you want to enable Jumbo MTU?  Enter "Y" or "N"  [Y]:
```

Note: The last item related to Jumbo MTU will configure the system QoS class and enable each of the queues. The Server VNIC templates will also be configured with the MTU based on the answer here. The queue settings can always be changed in the variable files, but the goal of the quick start is to be quick.

Step 17 Now finish off the domain policies with the NTP configuration. Set the NTP servers and select your time-zone. The script does divide the time-zones by region.

```
What is your Primary NTP Server [0.north-america.pool.ntp.org]:
Do you want to Configure an Alternate NTP Server?  Enter "Y" or "N" [Y]:
What is your Alternate NTP Server? [1.north-america.pool.ntp.org]:

------------------------------------------------------------------------------------------
```

```
------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Time Region.  [2]:

------------------------------------------------------------------------------------------
```

Option 2 is America and Options 48 is America/New_York, but we do not need to display all the output here.

```
------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Region Timezones: 48

------------------------------------------------------------------------------------------
```

And you can review the domain configuration but for this document we are only showing the acceptance.

```
------------------------------------------------------------------------------------------

Do you want to accept the above configuration?  Enter "Y" or "N" [Y]:

------------------------------------------------------------------------------------------
```

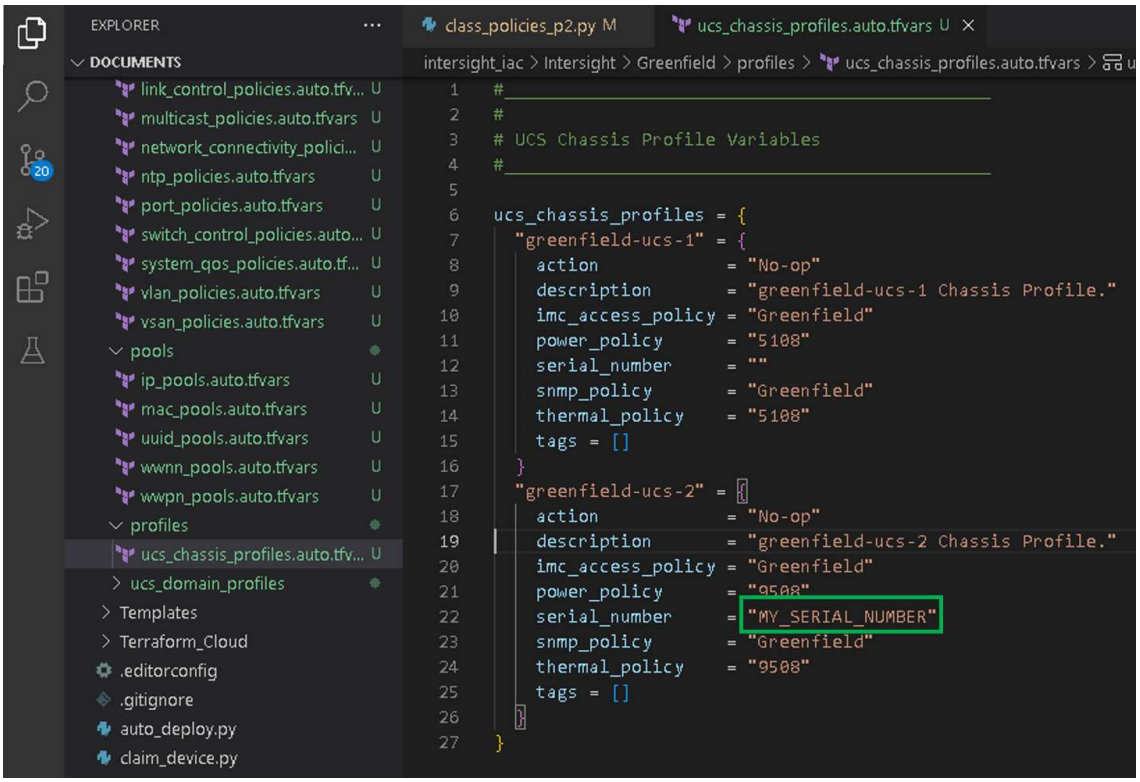
Step 18 Configure the profiles for the chassis in the domain. We will select 2 chassis so the policies for a 5108 and a 9508 (X-Series) will be configured. Power and thermal policies support different settings per model.

```
----------------------------------------------------------------------------------------------

Enter the Number of Chassis attached to greenfield-ucs:  [1]: 2

----------------------------------------------------------------------------------------------

The Type of Chassis to Apply this Policy to.

    Select an Option Below:
     1. 5108
     2. 9508

----------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Chassis Model.  [2]: 1

----------------------------------------------------------------------------------------------

Serial Number of the Chassis to assign to the Profile.

----------------------------------------------------------------------------------------------

What is the Serial Number of Chassis 1? [press enter to skip]:

----------------------------------------------------------------------------------------------

The Type of Chassis to Apply this Policy to.

    Select an Option Below:
     1. 5108
     2. 9508

----------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Chassis Model.  [2]: 2

----------------------------------------------------------------------------------------------
```

```
----------------------------------------------------------------------------------------------

What is the Serial Number of Chassis 2? [press enter to skip]:

----------------------------------------------------------------------------------------------
```

We do not have physical hardware, this is being assigned to, we are skipping the serial number value. But to add the serial number to the variables file go to the chassis_profiles file:

```
intersight_iac > Intersight > Greenfield > profiles >
ucs_chassis_profiles.auto.tfvars
```



As is shown above you would replace insert your serial number into the serial_number attribute.

Step 19 Configure the server policies. Press enter to select the default option of [Y].

```
---------------------------------------------------------------------------------------------

Do You Want to run the Quick Deployment Module - Policy Configuration?  Enter "Y" or "N" [Y]:

---------------------------------------------------------------------------------------------

  Below are the Questions that will be asked by the Policies Portion of the wizard.
   - VLAN ID for IMC Access Policy.
   - Local User Policy (Required for direct KVM Access).
     * user and role
     * user password (strong passwords enforced)
   - SNMP Policy
     * Contact
     * Location
     * SNMPv3 Users (optional)
     * SNMPv3 Trap Servers (optional)
   - Syslog Policy - (Optional)
     * Remote Syslog Server(s)

---------------------------------------------------------------------------------------------
```

As is shown above we are going to create the policies of IMC Access (KVM), Local User Policy (This is the user(s) that will be used to login through KVM if Intersight were down (By default KVM access in Intersight does not require additional login), SNMP, and Syslog Policies. Each of these policies are about management control of the servers and domain.

Step 20 Configure the IMC Access Policy. We can select the default values for this demo of inband and assigning the VLAN identifier. As a note with this the lowest VLAN id that can be assigned to the IMC Access inband policy is VLAN 4, thus the default value. VLAN1-3 cannot be used.

```
--------------------------------------------------------------------------------

  Now Starting the IMC Access Policy Section.

--------------------------------------------------------------------------------

--------------------------------------------------------------------------------

The type of configuration, In-Band and/or Out-Of-Band to be configured on the CIMC.

    Select an Option Below:
     1. inband
     2. out_of_band

--------------------------------------------------------------------------------

Please Enter the Option Number to Select for IMC Access Type. [1]:

--------------------------------------------------------------------------------

IMC Access VLAN Identifier

--------------------------------------------------------------------------------

Enter the VLAN ID for the IMC Access Policy. [4]:

--------------------------------------------------------------------------------
```

Step 21 Configure the IPMI over LAN Policy. Here we are only entering a password for the IPMI policy. Note that the password must be a hexadecimal value, be an even number of characters, and no longer than 40 characters. We used "**BEEF**" below.

```
--------------------------------------------------------------------------------

  The ipmi_key Must be in Hexidecimal Format [a-fA-F0-9] and no longer than 40 characters.

--------------------------------------------------------------------------------

Enter the ipmi_key: ****
Please re-enter ipmi_key: ****

--------------------------------------------------------------------------------
```

Step 22 Configure the Local User Policy. As mentioned above we need to create a local user for backup access to KVM (Or if you choose to launch KVM from the domain). We will enter a user of "**admin**" and assign to this user the "**admin**" role.

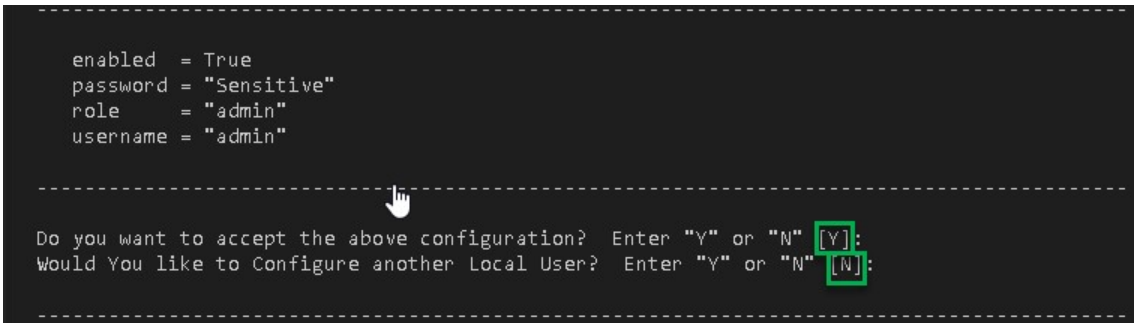
```
---------------------------------------------------------------------------------------------

Would you like to configure a Local user?  Enter "Y" or "N" [Y]:

---------------------------------------------------------------------------------------------

Name of the user to be created on the endpoint. It can be any string that adheres to the
following constraints. It can have alphanumeric characters, dots, underscores and
hyphen. It cannot be more than 16 characters.

---------------------------------------------------------------------------------------------

What is the Local username? admin

---------------------------------------------------------------------------------------------

The Role to Assign to the Local User.

    Select an Option Below:
     1. admin
     2. readonly
     3. user

---------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for User Role.  [1]:

---------------------------------------------------------------------------------------------
```

Step 23 The policy created by the wizard will enable strong password enforcement. The password must adhere to the strong password rules. Enter any strong password you want.

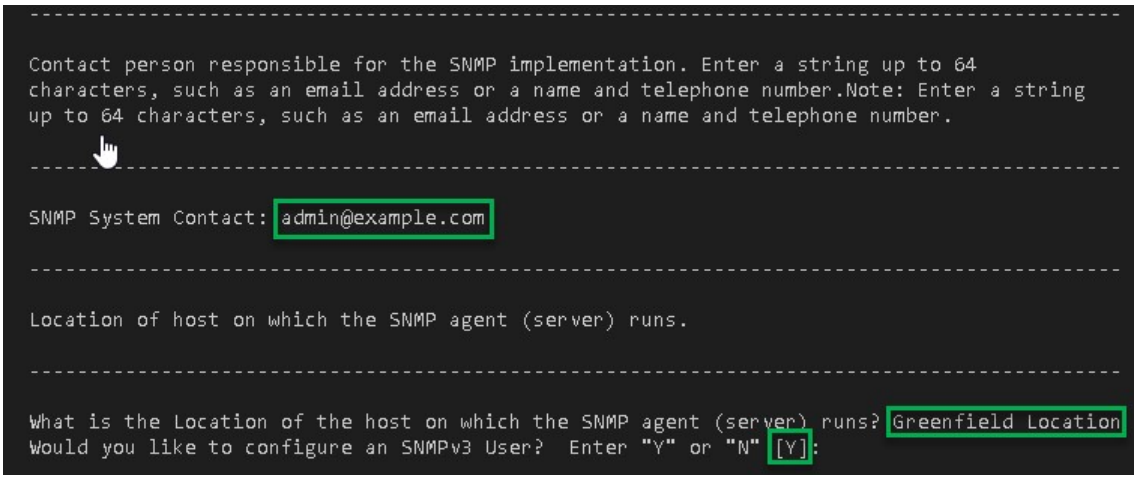
```
---------------------------------------------------------------------------------------------

Enforce Strong Password is enabled so the following rules must be followed:
  - The password must have a minimum of 8 and a maximum of 20 characters.
  - The password must not contain the User's Name.
  - The password must contain characters from three of the following four categories.
    * English uppercase characters (A through Z).
    * English lowercase characters (a through z).
    * Base 10 digits (0 through 9).
    * Non-alphabetic characters (! , @, #, $, %, ^, &, *, -, _, +, =)

What is the password for admin? ********
Please re-enter the password for admin? ********

---------------------------------------------------------------------------------------------

Error with admin's password! The password failed one of the following complexity rules:
  - The password must have a minimum of 8 and a maximum of 20 characters.
  - The password must not contain the User's Name.
  - The password must contain characters from three of the following four categories.
    * English uppercase characters (A through Z).
    * English lowercase characters (a through z).
    * Base 10 digits (0 through 9).
    * Non-alphabetic characters (! , @, #, $, %, ^, &, *, -, _, +, =)

---------------------------------------------------------------------------------------------

What is the password for admin? **********
Please re-enter the password for admin? **********

---------------------------------------------------------------------------------------------
```

Note: The output above shows us entering a password that does not meet the complexity requirements and we needed to enter the password again.

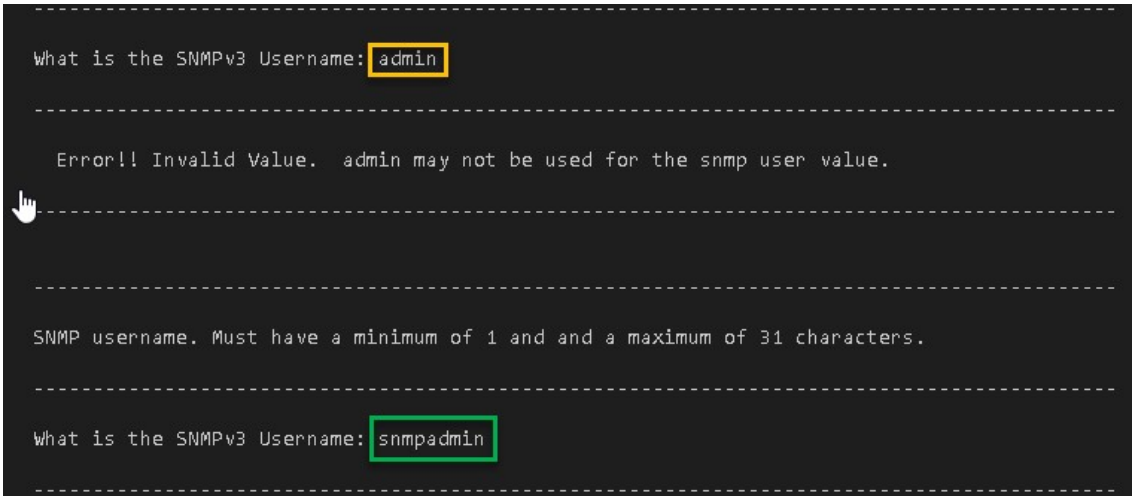
Step 24 Finish the Local User Policy section by accepting the user. You can create additional users if you want to, but we will select **[N]** and continue to the next section.



Step 25 Start the SNMP Policy section by assigning a SNMP Contact and Location information. Below we used the values of "admin@example.com" and "**Greenfield Location**".



Step 26 Configure a SNMPv3 user. The SNMP Policy in Intersight does support SNMP Communities but we have chosen for the quick start wizard to use the more secure method of SNMP users.



Note: "**admin**" is not allowed to be used as the username in the SNMP Policy.

Step 27 Assign the Security Level to the user. Descriptions below provide more color on what each level provides. The wizard default is the most secure level.

```
----------------------------------------------------------------------------------------------

Security mechanism used for communication between agent and manager.
* `AuthPriv` - The user requires both an authorization password and a privacy password.
* `NoAuthNoPriv` - The user does not require an authorization or privacy password.
* `AuthNoPriv` - The user requires an authorization password but not a privacy password.

    Select an Option Below:
     1. AuthNoPriv
     2. AuthPriv
     3. NoAuthNoPriv

----------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for SNMP Security Level.  [2]:

----------------------------------------------------------------------------------------------

Authorization protocol for authenticating the user.
* `NA` - Authentication protocol is not applicable.
* `MD5` - MD5 protocol is used to authenticate SNMP user.
* `SHA` - SHA protocol is used to authenticate SNMP user.
* `SHA-224` - SHA-224 protocol is used to authenticate SNMP user.
* `SHA-256` - SHA-256 protocol is used to authenticate SNMP user.
* `SHA-384` - SHA-384 protocol is used to authenticate SNMP user.
* `SHA-512` - SHA-512 protocol is used to authenticate SNMP user.

    Select an Option Below:
     1. MD5
     2. SHA

----------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for SNMP Auth Type.  [2]:
What is the authorization password for snmpadmin? ********
Please re-enter the authorization password for snmpadmin? ********

----------------------------------------------------------------------------------------------
```

Note: The SNMP User password must be between 8 and 32 characters. It has the same rules as the SNMP Community string.

Step 28 If you chose "**AuthPriv**" as the security level configure the Privilege Password.

```
----------------------------------------------------------------------------------------------

Privacy protocol for the user.
* `NA` - Privacy protocol is not applicable.
* `DES` - DES privacy protocol is used for SNMP user.
* `AES` - AES privacy protocol is used for SNMP user.

    Select an Option Below:
     1. AES
     2. DES

----------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for SNMP Auth Type.  [1]:
What is the privacy password for snmpadmin? ********
Please re-enter the privacy password for snmpadmin? ********

----------------------------------------------------------------------------------------------
```

Step 29 Accept the configured attributes. You can create additional users if you want to, but we will select **[N]** and continue to the SNMP Trap Section.

```
   auth_password    = "Sensitive"
   auth_type        = "SHA"
   privacy_password = "Sensitive"
   privacy_type     = "AES"
   security_level   = "AuthPriv"
   snmp_user        = "snmpadmin"

Do you want to accept the above configuration?  Enter "Y" or "N" [Y]:
Would You like to Configure another SNMP User?  Enter "Y" or "N" [N]:
Would you like to configure SNMP Trap Destionations?  Enter "Y" or "N" [Y]:
```

Step 30 The SNMP Trap section will only happen if an SNMPv3 user has been configured. And since the user was already configured, we will select the V3 option. The wizard will display the users that have been configured, which we will select below with option "**1**".

```
SNMP version used for the trap.
* `V3` - SNMP v3 trap version notifications.
* `V2` - SNMP v2 trap version notifications.

    Select an Option Below:
     1. V2
     2. V3

Please Enter the Option Number to Select for SNMP Version.  [2]:

    Please Select the SNMP User to assign to this Destination:

     1. snmpadmin

Please Enter the Option Number to Select for SNMP User: 1
What is the SNMP Trap Destination Hostname/Address? server1.example.com
Enter the Port to Assign to this Destination.  Valid Range is 1-65535.  [162]
```

server1.example.com is not a valid FQDN, it is just used here for example.

Step 31 Finish the SNMP Policy section by accepting the trap configuration. The wizard supports the ability to add as many trap destinations as you need to configure.

```
    destination_address = "server1.example.com"
    enable              = True
    trap_type           = "Trap"
    snmp_version        = "V3"
    user                = "snmpadmin"

Do you want to accept the above configuration?  Enter "Y" or "N" [Y]:
Would You like to Configure another SNMP Trap Destination?  Enter "Y" or "N" [N]:
```

Step 32 The wizard will now begin the Syslog Policy configuration. A few important notes. You can only configure two Syslog destinations in the Syslog Policy. It is not supported to configure more. If you only configure one syslog server, the second server will show up as "**0.0.0.0**" in the policy and be in a disabled state. Same rule applies if you configure no syslog destinations but create a policy, which you should as the policy will set the local syslog level as well, as shown in the screenshot below.

```
Do you want to configure Remote Syslog Servers?  Enter "Y" or "N" [Y]:

Lowest level of messages to be included in the local log.
* `warning` - Use logging level warning for logs classified as warning.
* `emergency` - Use logging level emergency for logs classified as emergency.
* `alert` - Use logging level alert for logs classified as alert.
* `critical` - Use logging level critical for logs classified as critical.
* `error` - Use logging level error for logs classified as error.
* `notice` - Use logging level notice for logs classified as notice.
* `informational` - Use logging level informational for logs classified as
    informational.
* `debug` - Use logging level debug for logs classified as debug.

    Select an Option Below:
     1. alert
     2. critical
     3. debug
     4. emergency
     5. error
     6. informational
     7. notice
     8. warning

Please Enter the Option Number to Select for Syslog Local Minimum Severity.  [8]:
Enter the Hostname/IP Address of the Remote Server: server1.example.com
```

Step 33 The syslog policy supports TCP or UDP as the transmission protocol. Select the necessary protocol, as shown below.

```
Transport layer protocol for transmission of log messages to syslog server.
* `udp` - Use User Datagram Protocol (UDP) for syslog remote server connection.
* `tcp` - Use Transmission Control Protocol (TCP) for syslog remote server connection.

    Select an Option Below:
     1. tcp
     2. udp

Please Enter the Option Number to Select for Syslog Protocol.  [2]:
Enter the Port to Assign to this Policy.  Valid Range is 1-65535.  [514]:
```

Step 34 We will configure just the one syslog server by changing the default answer to **[N]** below.

```
    hostname     = "server1.example.com"
    min_severity = "warning"
    port         = 514
    protocol     = "udp"

Do you want to accept the configuration above?  Enter "Y" or "N" [Y]:
Would You like to Configure another Remote Host?  Enter "Y" or "N" [Y]: N
```

Step 35 Accept the Syslog configuration.

```
    remote_clients = [
      {
        enabled      = True
        hostname     = "server1.example.com"
        min_severity = "warning"
        port         = 514
        protocol     = "udp"
      }
      {
        enabled      = False
        hostname     = "0.0.0.0"
        min_severity = "warning"
        port         = 514
        protocol     = "udp"
      }
    ]

Do you want to accept the above configuration?  Enter "Y" or "N" [Y]:
```

Step 37 The wizard is now ready to begin the LAN and SAN policies. Press enter, **[Y]**, to begin the configuration.

```
---------------------------------------------------------------------------------------

  The Quick Deployment Module - Network Configuration, will configure policies for the
  Network Configuration of a UCS Server Profile connected to an IMM Domain.

  This wizard will save the output for these pools in the following files:

  - Intersight\Greenfield\policies\ethernet_adapter_policies.auto.tfvars
  - Intersight\Greenfield\policies\ethernet_network_control_policies.auto.tfvars
  - Intersight\Greenfield\policies\ethernet_network_group_policies.auto.tfvars
  - Intersight\Greenfield\policies\ethernet_qos_policies.auto.tfvars
  - Intersight\Greenfield\policies\fibre_channel_adapter_policies.auto.tfvars
  - Intersight\Greenfield\policies\fibre_channel_network_policies.auto.tfvars
  - Intersight\Greenfield\policies\fibre_channel_qos_policies.auto.tfvars
  - Intersight\Greenfield\policies\lan_connectivity_policies.auto.tfvars
  - Intersight\Greenfield\policies\san_connectivity_policies.auto.tfvars

---------------------------------------------------------------------------------------

Do You Want to run the Quick Deployment Module - Network Configuration?  Enter "Y" or "N" [Y]

---------------------------------------------------------------------------------------
```

Note: The Quick start wizard is going to configure the Ethernet Network policies in the same manner the Hyperflex deployment tool does as well. It will create eight vNIC's, two redundant vNIC's for each virtual switch. What is helpful about this approach is it allows the traffic from a host to be assigned different QoS classes based on the traffic assigned to the virtual switch. MGMT is assigned to the "Silver" class. vMotion is assigned to the "Bronze" class. Storage is assigned to the "Platinum" class. And DATA (Virtual Machine Networks or DVS) is assigned to the "Gold" class. The Platinum class has a class of service (CoS) of "5" and is assigned to the Priority Flow Control Queue. This is very important for technologies like ROCEv2 or NVMeoF, where you want to guarantee packets are not dropped and receive immediate queue attention. All of these are more advanced tuning practices but there is no harm in enabling them by default, which is why the wizard is doing this.

```
---------------------------------------------------------------------------------------

  Below are the Questions that will be asked by the Policies Portion of the wizard.
    - Choice to use CDP or LDP for Device Discovery.
    - Choice to enable Jumbo MTU (9000 MB) or Run standard 1500 MB MTU for vNICs.
    - LAN Connectivity Policy (vNICs):
      * VLAN ID for ESXi MGMT
      * VLAN ID for ESXi vMotion
      * VLAN ID for ESXi Storage
      * VLAN List for DATA (Virtual Machines)
    - SAN Connectivity Policy (vHBAs):
      * VSAN ID for Fabric A
      * VSAN ID for Fabric B
      ** Note: This should not overlap with any of the VLANs assigned to the
               LAN Connectivity Policies.

---------------------------------------------------------------------------------------
```

Step 39 The neighbor discovery protocol is part of the Ethernet Network Control Policy. Most deployments do not tune the other attributes. Enabling CDP or LLDP is helpful for end-to-end visibility through the domain.

```
---------------------------------------------------------------------------------------------

Neighbor Discovery Protocol.

    Select an Option Below:
     1. CDP
     2. LLDP
     3. None

---------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Neighbor Discovery Protocol.  [2]:

---------------------------------------------------------------------------------------------
```

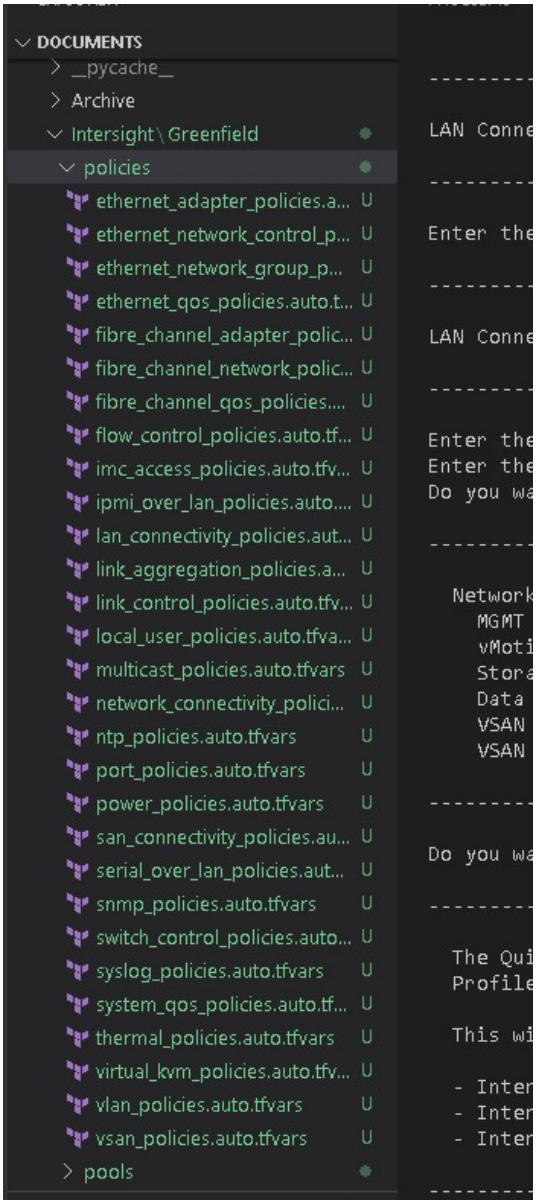
Step 40 For each of the virtual switches to be assigned to the host, based on the policy, select a VLAN to be configured on the vNIC pair. Note that for the MGMT, vMotion, and Storage vNIC's the VLAN selected will be configured as the default Native VLAN. This would mean that for the virtual switches for these networks do not need to be assigned a VLAN tag in vCenter. This is especially important for the MGMT network when the desire is to use something like auto-deploy to PXE boot the OS for deployment.

```
---------------------------------------------------------------------------------------------

LAN Connectivity Policy vNICs - MGMT VLAN Identifier

---------------------------------------------------------------------------------------------

Enter the VLAN ID for MGMT:  [1]:

---------------------------------------------------------------------------------------------

LAN Connectivity Policy vNICs - vMotion VLAN Identifier

---------------------------------------------------------------------------------------------

Enter the VLAN ID for vMotion:  [2]:

---------------------------------------------------------------------------------------------

LAN Connectivity Policy vNICs - Storage VLAN Identifier

---------------------------------------------------------------------------------------------

Enter the VLAN ID for Storage:  [3]:
Enter the VLAN or List of VLANs to add to the DATA (Virtual Machine) vNICs: 1-99
Do you want to Configure one of the VLANs as a Native VLAN?  [press enter to skip]

---------------------------------------------------------------------------------------------
```

Note: You can only assign VLAN values that were assigned to the VLAN Policy in the previous sections. Thus "1-99" is what we entered here, as that is what was defined in the VLAN Policy. If you try to enter VLANs that were not already defined the script will display an error message.

Step 41 Finish the LAN/SAN Policy section by accepting the configuration. If you did enter anything you want to change, this is the opportunity for you to re-run the section again.

```
----------------------------------------------------------------------------------------

  Network Configuration Variables:
    MGMT VLAN     = 1
    vMotion VLAN  = 2
    Storage VLAN  = 3
    Data VLANs    = "1-99"
    VSAN Fabric A = 100
    VSAN Fabric B = 200

----------------------------------------------------------------------------------------

Do you want to accept the above configuration?  Enter "Y" or "N" [Y]:

----------------------------------------------------------------------------------------
```



Now that we have finished the above policies, you can go to the folder "**Intersight > Greenfield > Policies**" and view all the polices that have been created.

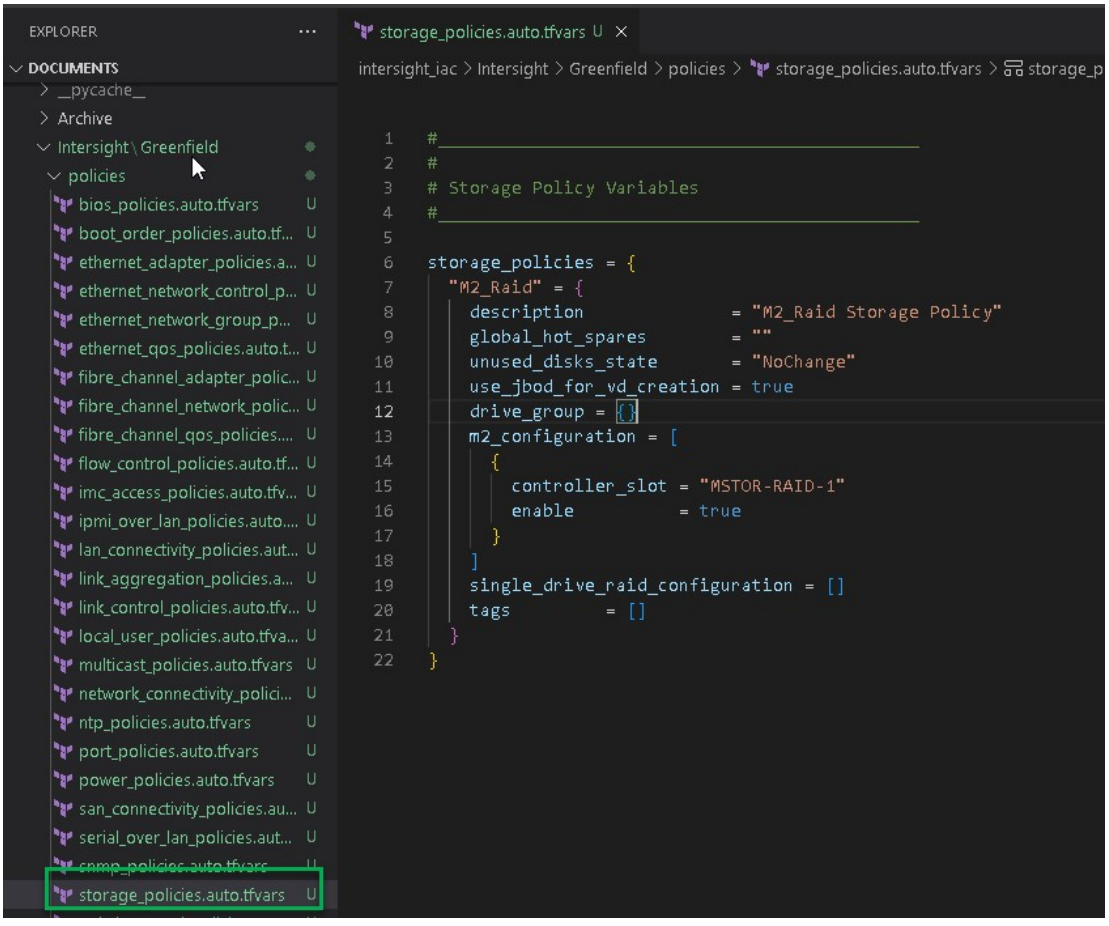
It is not a requirement, but this provides you the opportunity to see how the data has been entered into each of the files. You can change any values you want from these files.

The purpose of the wizard is not to be a permanent tool for managing Intersight. The purpose of it is to help you take the initial step towards infrastructure as code. Generate the base pools, policies, and profiles. The hardest part of starting any coding project is knowing where to start and understanding the nuances of the API. Hopefully, this gets you past those initial challenges.

Step 42 Configure the BIOS, boot, and Storage Policies. The only question that will be asked here is if servers will have the TPM module installed. This determines which BIOS templates should be assigned.

```
The Quick Deployment Module - Boot/Storage, will configure policies for a UCS Server
Profile connected to an IMM Domain.

This wizard will save the output for these pools in the following files:

- Intersight\Greenfield\policies\bios_policies.auto.tfvars
- Intersight\Greenfield\policies\boot_order_policies.auto.tfvars
- Intersight\Greenfield\policies\storage_policies.auto.tfvars

Do You Want to run the Quick Deployment Module - Boot/Storage Configuration?  Enter "Y" or "N" [Y]:

Flag to Determine if the Servers have a TPM Installed.

Will any of these servers have a TPM Module Installed?  [Y]:
```

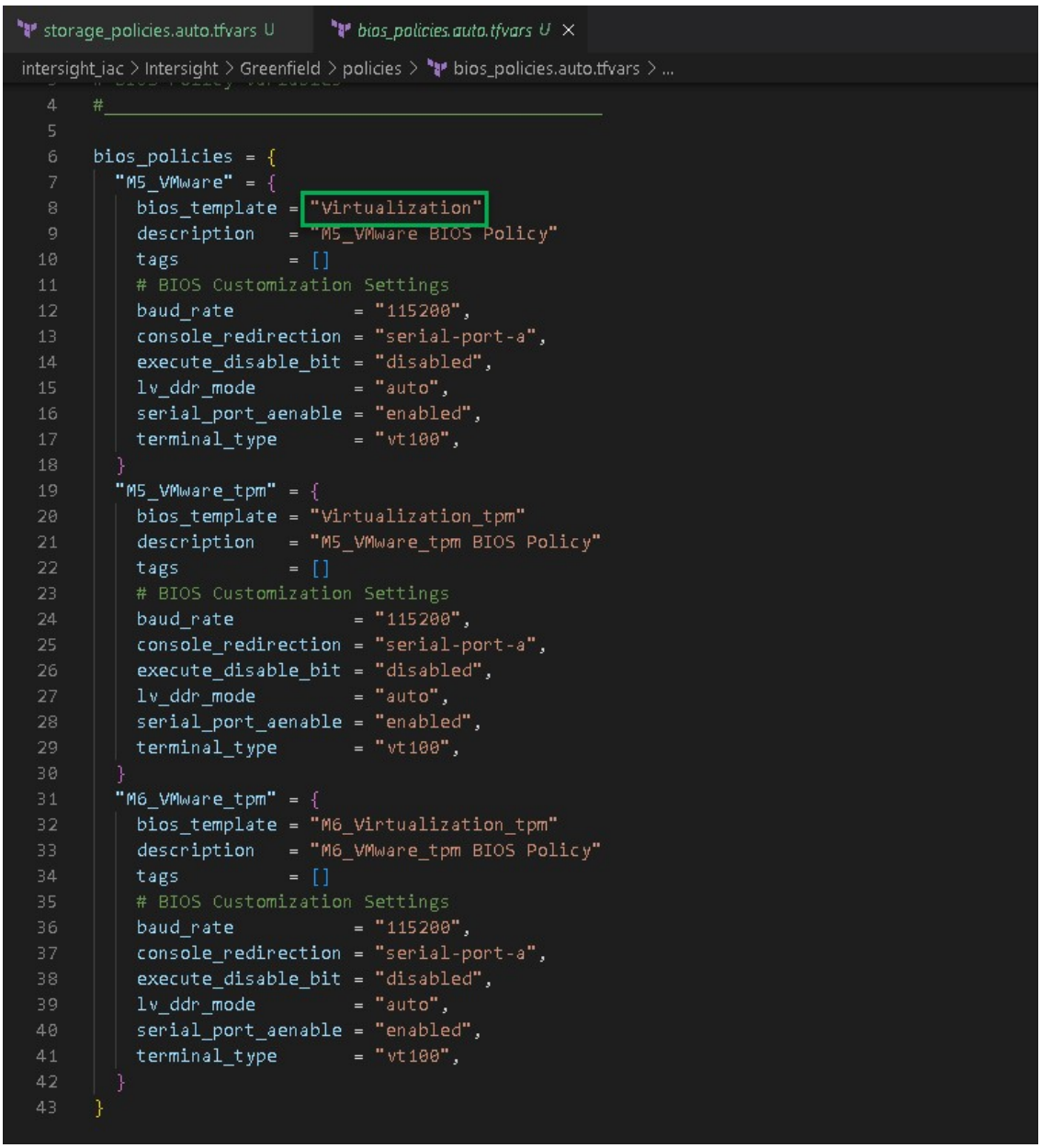
We chose the option "**Quick Start Deployment – Domain – VMware M2**", at the beginning of the wizard. That is what determined the Storage Policy to be configured, shown below.



The M6 generation servers ship by default with the TPM module. You can of course remove it from the server before ordering, but we are trying to hit the 95% most common deployments, not the exceptions. Also notice below the attribute of "**bios_template**". This is not a BIOS attribute but is an attribute used by the script to determine the BIOS tokens to modify based on the Performance tuning guide of each the different Generation of servers.

Performance Tuning Guide for Cisco UCS M5 Servers
Performance Tuning Guide for Cisco UCS M6 Servers

There are differences between generations. The terraform library has been configured to set the best practice attributes using the template defined here. There are templates for each of the workloads defined in the guides, but we only assigned policies based on the type of deployment selected. You can always add more through the terraform files or run the individual policies wizard.



Step 43 The wizard is now ready to create the server profiles. An important note, which is a break from the UCS norm related to the script. Although the script will assign the policies to the "ucs_server_profile_templates.auto.tfvars". The script is not going to create templates in Intersight. The reason that I have chosen not to utilize templates is in my experience in the field most customers build either many templates with only a few small differences, or they generate all the profiles from a few master templates and then detach and make policy changes to the profiles. In my experience this is because a template cannot have any override policies.

The approach with the script is it will use the template file as a policy holder. Anything specified in the template will be assigned to the server profile. But if a server profile needs a different policy (say LAN Policy), then assigning a policy to the server profile will override the template.

```
-------------------------------------------------------------------------------------------

  The Quick Deployment Module - Domain Policies, will configure pools for a UCS Domain
  Profile.

  This wizard will save the output for these pools in the following files:

  - Intersight\Greenfield\profiles\ucs_server_profile_templates.auto.tfvars
  - Intersight\Greenfield\profiles\ucs_server_profiles.auto.tfvars

-------------------------------------------------------------------------------------------

Do You Want to run the Quick Deployment Module - Server Profiles Configuration?
Enter "Y" or "N" [Y]:

-------------------------------------------------------------------------------------------

  Below are the Questions that will be asked by the Server Profiles Portion of the wizard.
   - Number of Servers you are going to deploy.
   - Name of the Server Profile(s).
   - Serial Number of the Server Profile(s).

-------------------------------------------------------------------------------------------
```

Step 44 For this demo we will create "**4**" server profiles. For "**esx01**" and "**esx02**" we will assign M5 servers, and for "**esx03**" and "**esx04**" we will assign M6 server type. The output for the first and last server profile is shown below. But it is the same procedure for the 2nd and 3rd as well.

```
-------------------------------------------------------------------------------------------

Number of Server Profiles.

-------------------------------------------------------------------------------------------

Enter the Number of Server Profiles to Create:  [1]: 4
What is the Name for the Server Profile? esx01

-------------------------------------------------------------------------------------------

Serial Number of the Server Profile esx01.

-------------------------------------------------------------------------------------------

What is the Serial Number of esx01? [press enter to skip]:

-------------------------------------------------------------------------------------------

The Generation of UCS to Apply these Policies to.

    Select an Option Below:
     1. M5
     2. M6
     3. M7

-------------------------------------------------------------------------------------------

Please Enter the Option Number to Select for Generation of UCS Server.  [2]: 1

-------------------------------------------------------------------------------------------

Flag to Determine if the Server has TPM Installed.

-------------------------------------------------------------------------------------------

Is a Trusted Platform Module installed in this Server and do you want to enable secure-boot?  [N]:
```

Note: Because we are not assigning this to actual hardware, we are skipping the serial number for the servers. For your environment you can follow the same approach to pre-provision the profiles or you can assign the serial numbers if you are ready for installation.

```
--------------------------------------------------------------------------------

Is a Trusted Platform Module installed in this Server and do you want to enable secure-boot?  [N]:
What is the Name for the Server Profile? esx03

--------------------------------------------------------------------------------

Serial Number of the Server Profile esx03.

--------------------------------------------------------------------------------

What is the Serial Number of esx03? [press enter to skip]:

--------------------------------------------------------------------------------

The Generation of UCS to Apply these Policies to.

    Select an Option Below:
     1. M5
     2. M6
     3. M7

--------------------------------------------------------------------------------

Please Enter the Option Number to Select for Generation of UCS Server.  [2]:
What is the Name for the Server Profile? esx04

--------------------------------------------------------------------------------
```

Once the last server profile has been created the script will begin to download the terraform resource files. The script is controlling this by checking the repository and if the version.txt matches the current version in the repository then it will not download updated configurations. If the version.txt is not created yet or is an older release, then the script will download the files again. This is to make sure the files are always the most current but not to download them if the files are already current.

```
--------------------------------------------------------------------------------


   Beginning Easy IMM Module Downloads for ".\Intersight\Greenfield\policies"

   Downloading "README.md"
   "README.md" Download Complete!

   Downloading "adapter_configuration_policies.tf"
   "adapter_configuration_policies.tf" Download Complete!

   Downloading "bios_policies.tf"
   "bios_policies.tf" Download Complete!

   Downloading "boot_order_policies.tf"
   "boot_order_policies.tf" Download Complete!

   Downloading "certificate_management_policies.tf"
   "certificate_management_policies.tf" Download Complete!
```

After the last server profile has been created, the script will begin to download the terraform resource files. The script is checking the repository against a local file version.txt. If it matches the current version in the repository, then it will not download updated the files. If the version.txt is not created yet or is an older release, then the script will download the files again. This is to make sure the files are always the most current but not to download them if the files already exist and are the most current release.

```
  Completed Easy IMM Module Downloads for ".\Intersight\Greenfield\policies"

--------------------------------------------------------------------------------------------



--------------------------------------------------------------------------------------------


  Beginning Easy IMM Module Downloads for ".\Intersight\Greenfield\pools"

  Downloading "README.md"
  "README.md" Download Complete!

  Downloading "data_sources.tf"
  "data_sources.tf" Download Complete!

  Downloading "ip_pools.tf"
  "ip_pools.tf" Download Complete!
```

Once the downloads are complete, the script will finish by running “terraform fmt” to line up indentations in the files it created. This is important because, based on user input, the indentations in the files may differ, thus the default indentation needs to be adjusted.

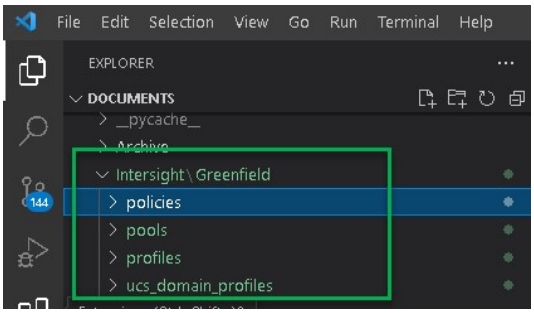
```
--------------------------------------------------------------------------------------------

  Running "terraform fmt" in folder ".\Intersight\Greenfield\policies",
  to correct variable formatting!

--------------------------------------------------------------------------------------------

Format updated for the following Files:
- Intersight\Greenfield\policies\bios_policies.auto.tfvars
- Intersight\Greenfield\policies\boot_order_policies.auto.tfvars
- Intersight\Greenfield\policies\ethernet_adapter_policies.auto.tfvars
- Intersight\Greenfield\policies\fibre_channel_adapter_policies.auto.tfvars
- Intersight\Greenfield\policies\flow_control_policies.auto.tfvars
- Intersight\Greenfield\policies\ipmi_over_lan_policies.auto.tfvars
- Intersight\Greenfield\policies\link_control_policies.auto.tfvars
- Intersight\Greenfield\policies\local_user_policies.auto.tfvars
- Intersight\Greenfield\policies\network_connectivity_policies.auto.tfvars
- Intersight\Greenfield\policies\ntp_policies.auto.tfvars
- Intersight\Greenfield\policies\port_policies.auto.tfvars
- Intersight\Greenfield\policies\power_policies.auto.tfvars
- Intersight\Greenfield\policies\serial_over_lan_policies.auto.tfvars
- Intersight\Greenfield\policies\snmp_policies.auto.tfvars
- Intersight\Greenfield\policies\storage_policies.auto.tfvars
- Intersight\Greenfield\policies\switch_control_policies.auto.tfvars
- Intersight\Greenfield\policies\syslog_policies.auto.tfvars
- Intersight\Greenfield\policies\system_qos_policies.auto.tfvars
- Intersight\Greenfield\policies\vlan_policies.auto.tfvars
- Intersight\Greenfield\policies\vsan_policies.auto.tfvars

--------------------------------------------------------------------------------------------
```

Step 45 For this demo, because the user environment is setup with "dummy" API credentials we will skip the step to create the Terraform Cloud Workspaces by entering "**N**". If this was for your own environment, select [**Y**] to create the workspaces. Please move ahead to Task 3 for a walkthrough of creating the workspaces.

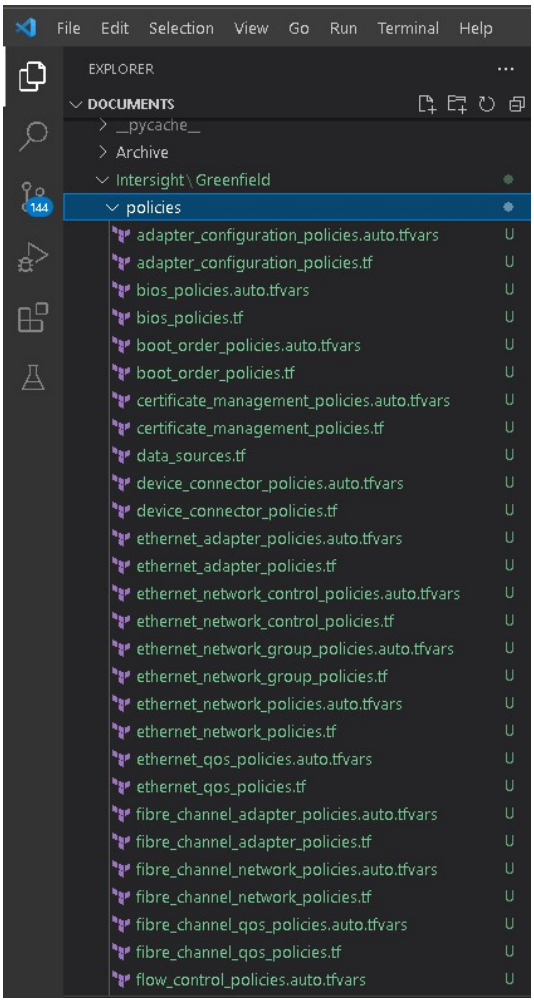
Step 46 Select [**Y**] that you will be utilizing Terraform Cloud and enter "**N**" to checking for the Intersight Organization.

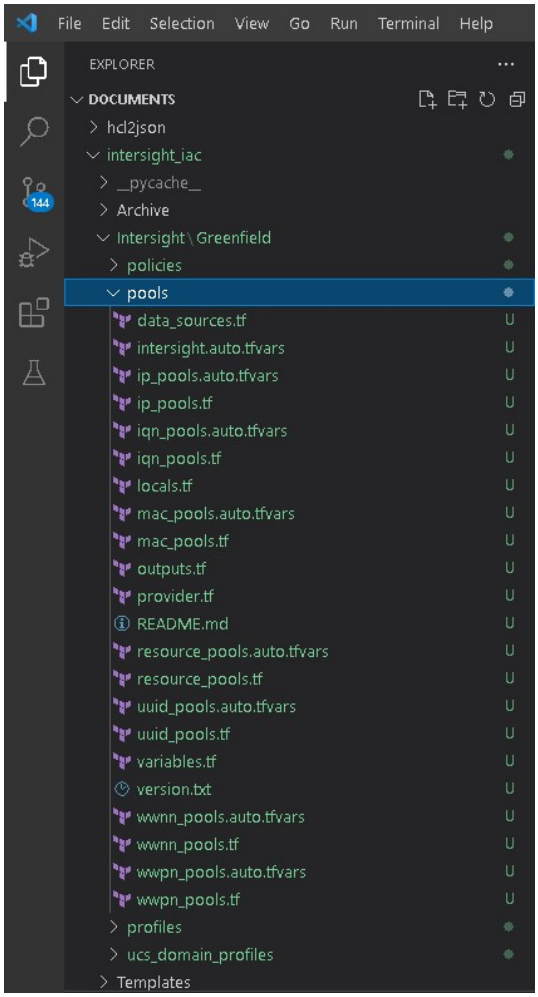
```
--------------------------------------------------------------------------------

Do you want to Proceed with creating Workspaces in Terraform Cloud?  [Y]: N

--------------------------------------------------------------------------------

Will You be utilizing Local or Terraform Cloud

--------------------------------------------------------------------------------

Will you be utilizing Terraform Cloud?  [Y]:

--------------------------------------------------------------------------------

  Skipping Step to Create Terraform Cloud Workspaces.
  Moving to last step to Confirm the Intersight Organization Exists.

--------------------------------------------------------------------------------


--------------------------------------------------------------------------------

Do You Want to Check Intersight for the Organization Greenfield?  Enter "Y" or "N" [Y]: N

--------------------------------------------------------------------------------

  Proceedures Complete!!! Closing Environment and Exiting Script.

--------------------------------------------------------------------------------

PS C:\Users\Administrator\Documents\intersight_iac>
```

Now we should see that all 4 folders are created and have the files necessary to run the script through Terraform Cloud.

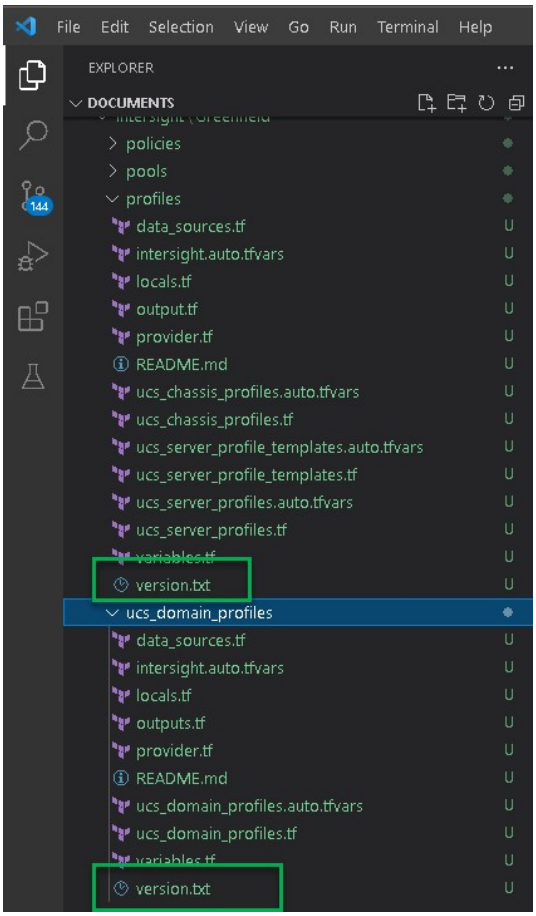


This is another good opportunity to browse the files and see the data that has been entered. Feel free to check whatever you would like at this point.

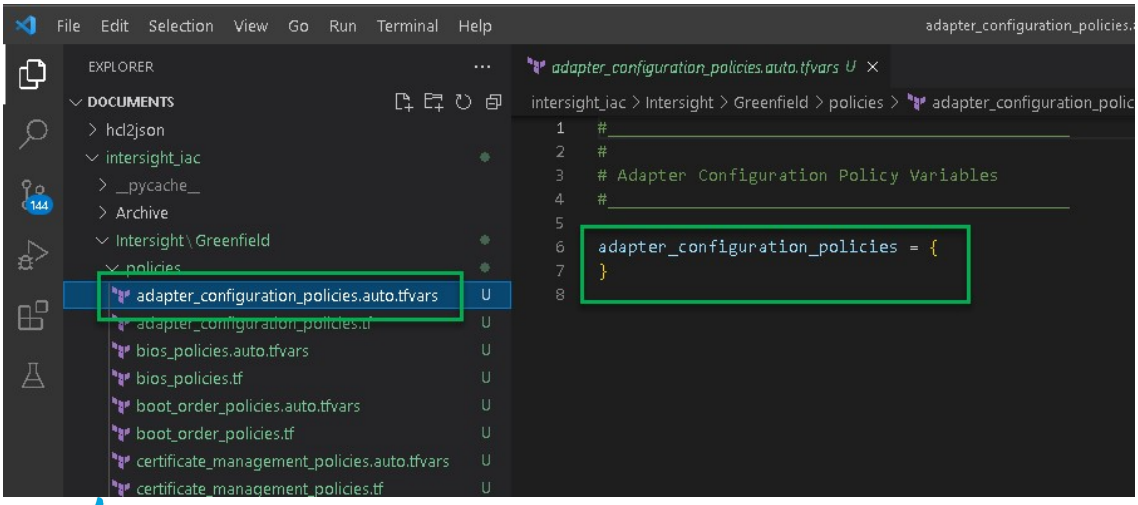




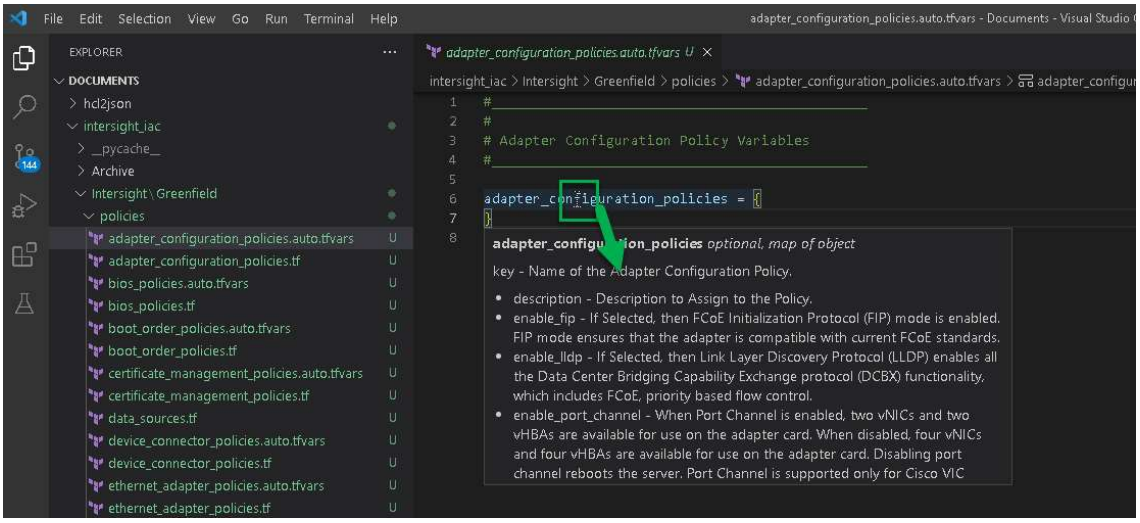
As mentioned previously the version.txt files shown below are used by the python wizard. They are not needed by Terraform Cloud.



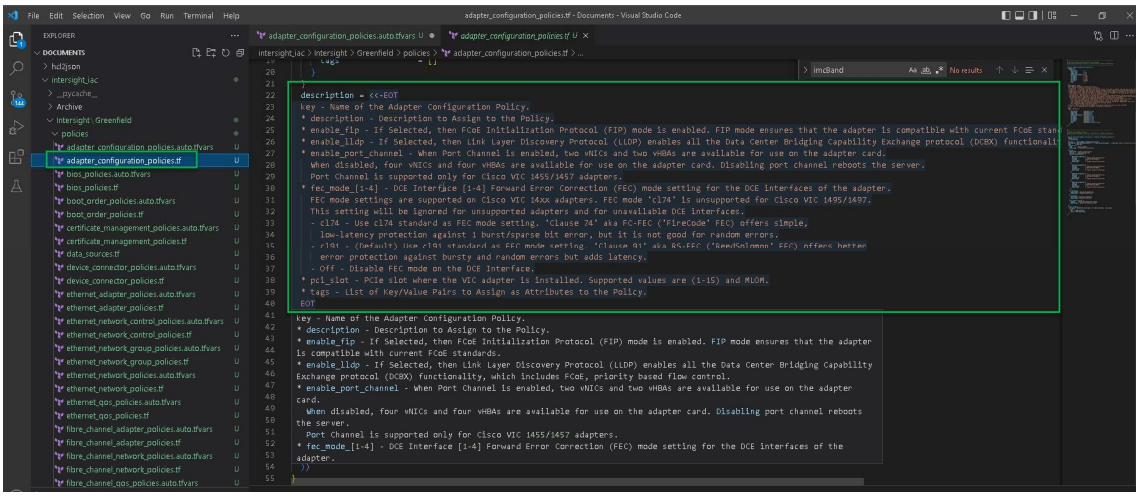
The workspaces have been created to work with domain and standalone server profiles. Because of this all server/domain policies are in place. When a policy is not utilized in an environment, like with the adapter configuration policies shown below, an empty map of objects for the policy needs to be created so that Terraform will not try to create these policies or pools. An empty map of objects is shown below for the adapter_configuration_policies.



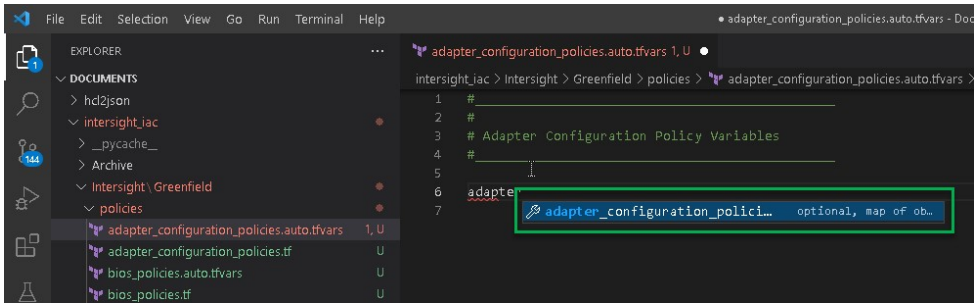
While we are in these files, we can also talk about some features that are helpful with Visual Studio Code. Now that the "**.tf**" files have been downloaded from the "terraform-intersight-easy-imm" repository when we are in one of the "auto.tfvars" files, if you hover over the map of objects, the Intersight documentation will be displayed.

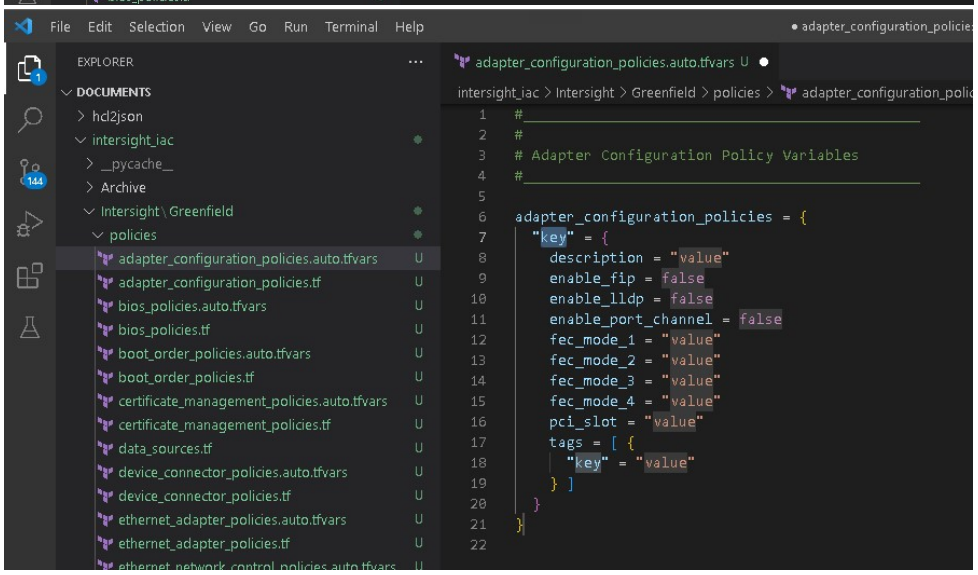


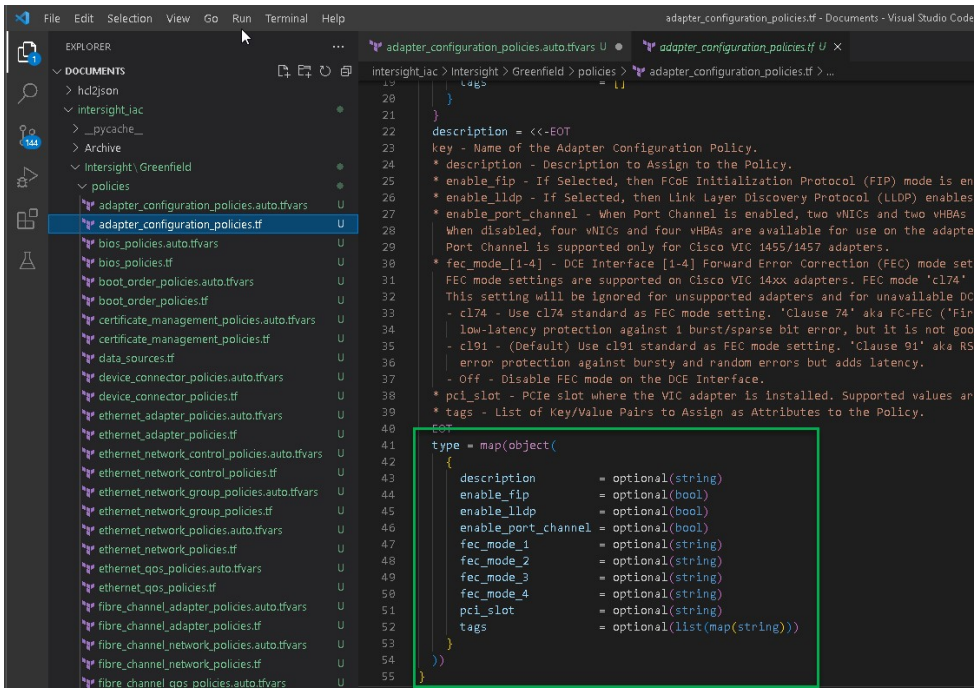
This is provided by the description in the map of object that was copied from the Intersight API documentation. The purpose is to help you know what the options are for each attribute as you work with each of the files.



Another feature is the auto completion. If you edit a file and create the first map of object. When you type out the variable name in the "**auto.tfvars** "file(s), Visual Studio Code will pull in the map of object dictionary from the variable with the type value set. You can then hover over the map to refer to the documentation to know what the values that you should utilize, as well as the defaults.







Task 3: Demo – Workspace and Organization Creation with the Wizard. (Optional Task)

Step 1 This section is for review only, related to the lab. Nothing you need to do. These steps would fail as you do not have a valid API key and Secret for Intersight. If you do not want to read through this section, go ahead and Skip ahead to Task 5.

But if you are running this in your own environment, please continue, this will provide the steps to create the Terraform Cloud Workspaces. For this Demo we need to specify the API key secret file with the main.py process as we are not pointing to the default location of "*C:\Users\Administrator\Downloads\SecretKey.txt*". We are skipping the policy deployment by selection option "**10**" from the menu and entering our organization again as "**Greenfield**".

```
PS C:\Users\Administrator\Documents\intersight_iac> python main.py -s "C:\Users\Administrator\Downloads\easy-imm-key-1.txt"

  Starting the Easy IMM Initial Configuration Wizard!

Select the Deployment type you would like to do with the wizard:

    Select an Option Below:
     1. Deploy Domain Wizard
     2. Deploy Domain Chassis Wizard
     3. Deploy Domain Fabric Interconnects Wizard
     4. Deploy Domain Servers Wizard
     5. Deploy Standalone Servers Wizard
     6. Deploy Individual Policies
     7. Quick Start Deployment - Domain - VMware M2
     8. Quick Start Deployment - Domain - VMware Raid1
     9. Quick Start Deployment - Domain - VMware Stateless
    10. Skip Policy Deployment

Please Enter the Option Number to Select for Main Menu.  [1]: 10
What is your Intersight Organization Name?  [default]: Greenfield
```

Step 2 We select [Y] to continue with the Terraform Cloud Workspace creation process and select the organization this configuration will be performed in.

```
Terraform Cloud Workspaces for Organization Greenfield

Do you want to Proceed with creating Workspaces in Terraform Cloud?  [Y]:

Terraform Cloud Organizations:

    Select an Option Below:
     1. atr
     2. Cisco-IST-TigerTeam
     3. Cisco-Richfield-Lab
     4. dCloud_Intersight_UCS
     5. deere-poc
     6. tyscott-training
     7. Tyson_Demo

Please Enter the Option Number to Select for Terraform Cloud Organization: 4
```

Step 3 We select the version control system (VCS) provider that has already been pre-configured in the Terraform Cloud Organization:

```
Terraform Cloud VCS Provider:

    Select an Option Below:
     1. GitHub.com

Please Enter the Option Number to Select for VCS Provider: 1
```

Step 4 Here we select the VCS Base Repository where our configuration will be stored, which is Option "**3**":

```
Terraform Cloud VCS Base Repository:

    Select an Option Below:
     1. DCMattyG/brahma
     2. DCMattyG/brahma-project
     3. scotttyso/Easy-IMM
     4. scotttyso/OKTA
     5. scotttyso/acipdt
     6. scotttyso/brahma
     7. scotttyso/deployments_intersight
     8. scotttyso/iac
     9. scotttyso/iac-easy-aci
```

<screen cropped for brevity>

```
Please Enter the Option Number to Select for VCS Base Repository: 3
```

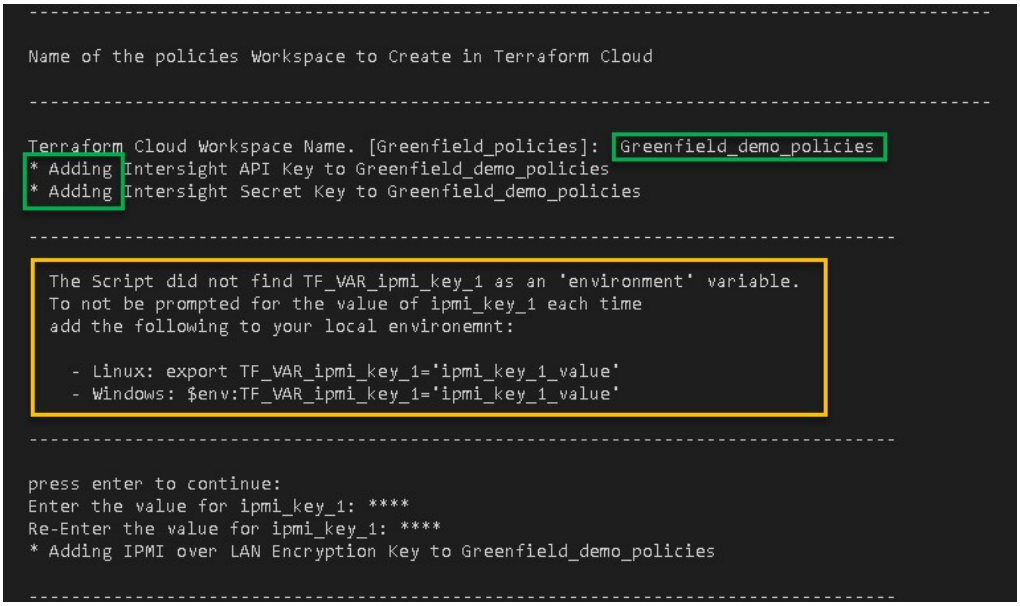
Step 5 we select the latest version of Terraform for the Workspace. If you had a specific need, you could select different versions, but typically the latest version is a good practice.

```
Terraform Version for Workspaces:

    Select an Option Below:
     1. 1.1.9
     2. 1.1.8
     3. 1.1.7
     4. 1.1.6
     5. 1.1.5
```

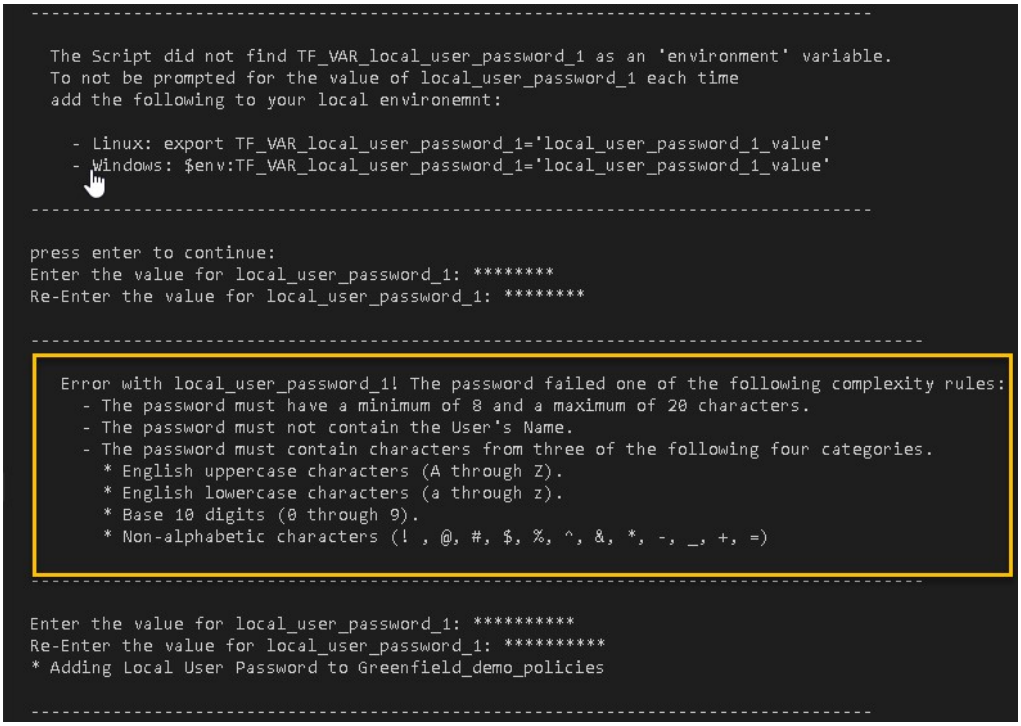
<screen cropped for brevity>

```
    18. 1.0.2
    19. 1.0.1
    20. 1.0.0

Please Enter the Option Number to Select for Terraform Version. [1]:
```

Step 6 By default the Workspace is going to be named {organization}_{folder}. For this demo I am choosing to change the name for simplicity in the Org Workspaces for finding it. If I searched by Greenfield or policies, it would show all 20 pod workspaces. An additional note here. Because I stopped the wizard and restarted, my environment variables from the wizard are no longer in place. As such I need to re-enter all the sensitive variables that will be added to the Terraform Cloud workspaces. As is shown in the orange box below I can enter these values in my environment before running the script to prevent from being prompted for them.



Step 7 The same checks will be applied to password policies as shown below.



Step 8 To bypass the requirement to re-enter the passwords I would use the following export/env commands to save these in the environment for the command line session.

```
Linux:

export TF_VAR_ipmi_key_1="MY_VALUE"
export TF_VAR_local_user_password_1="MY_VALUE"
export TF_VAR_snmp_auth_password_1="MY_VALUE"
export TF_VAR_snmp_privacy_password_1="MY_VALUE"

Windows:

$env:TF_VAR_ipmi_key_1="MY_VALUE"
$env:TF_VAR_local_user_password_1="MY_VALUE"
$env:TF_VAR_snmp_auth_password_1="MY_VALUE"
$env:TF_VAR_snmp_privacy_password_1="MY_VALUE"
```

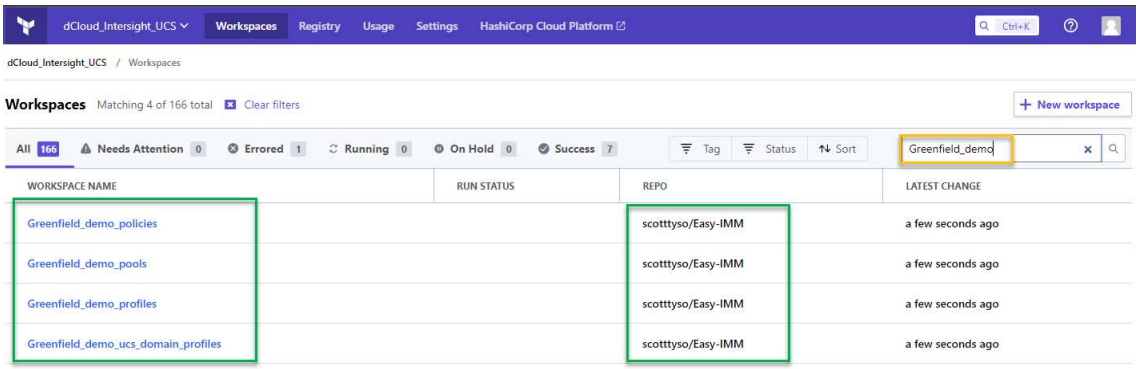
Step 9 Now we will create the folders for pools, profiles, and ucs_domain_profiles.

```
--------------------------------------------------------------------------------

Name of the pools Workspace to Create in Terraform Cloud

--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_pools]: Greenfield_demo_pools
* Adding Intersight API Key to Greenfield_demo_pools
* Adding Intersight Secret Key to Greenfield_demo_pools

--------------------------------------------------------------------------------

Name of the profiles Workspace to Create in Terraform Cloud

--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_profiles]: Greenfield_demo_profiles
* Adding Intersight API Key to Greenfield_demo_profiles
* Adding Intersight Secret Key to Greenfield_demo_profiles

--------------------------------------------------------------------------------

Name of the ucs_domain_profiles Workspace to Create in Terraform Cloud

--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_ucs_domain_profiles]: Greenfield_demo_ucs_domain_profiles
* Adding Intersight API Key to Greenfield_demo_ucs_domain_profiles
* Adding Intersight Secret Key to Greenfield_demo_ucs_domain_profiles

--------------------------------------------------------------------------------
```

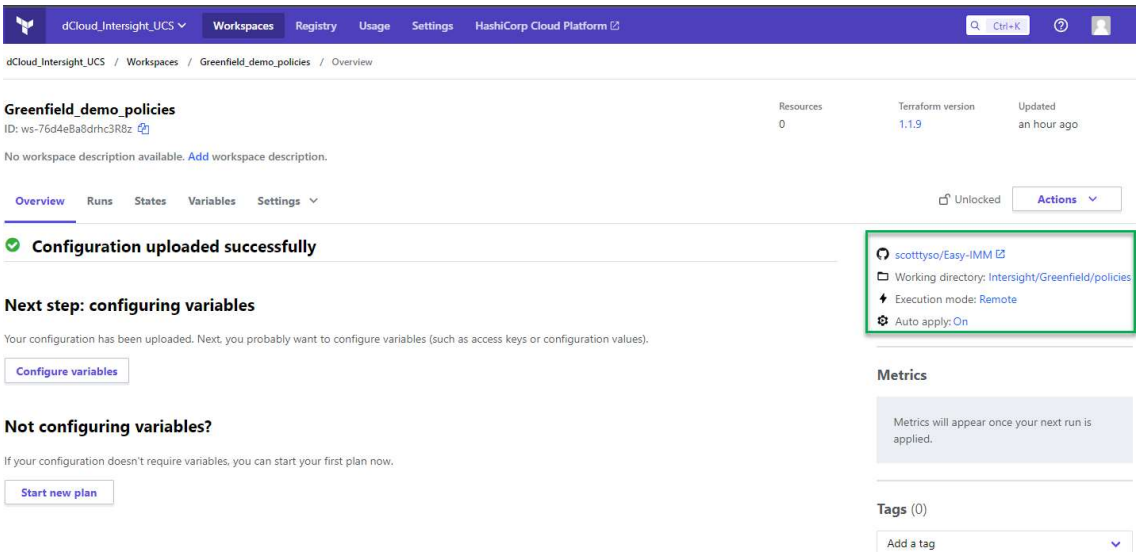
Step 10 We have completed the Workspace creation process, the last portion of the wizard is the option to check Intersight for the existence of the Organization. This is where the "-s" option was important as the current library requires the secret key file versus the terraform provider that wants the secret key content.

```
Do You Want to Check Intersight for the Organization Greenfield?  Enter "Y" or "N" [Y]:

Resource Group Greenfield_rg has the Moid of 627fe1fe6972652d32c0d212,
which was just Created.

did not find the organization

Organization Greenfield has the Moid of 627fe1ff6972652d32c0d23a,
which was just Created.

  Proceedures Complete!!! Closing Environment and Exiting Script.
```

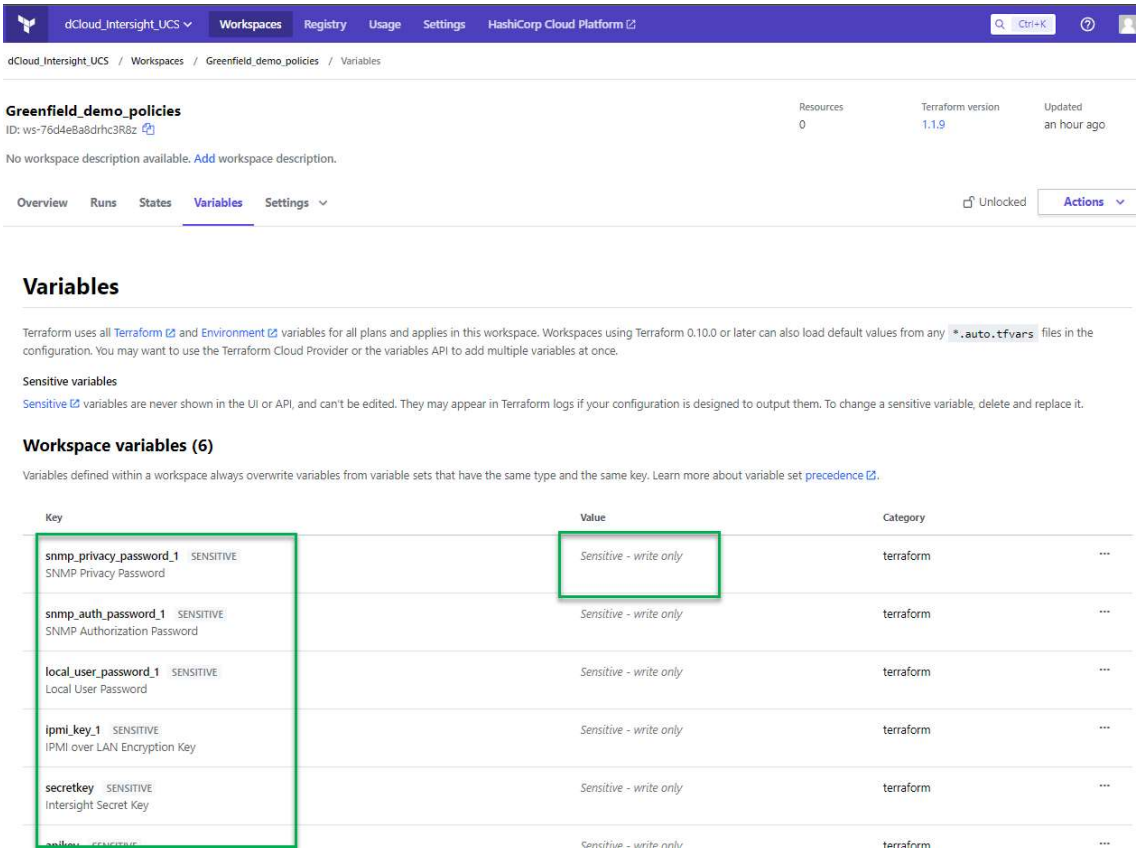
Step 11 We can now move over to Terraform Cloud and see that the Workspaces have been created. Note that we used the Greenfield_demo is used in the Filter and that is why we used the demo key in the Workspace Names. With the Flat Workspace structure it is helpful to have an attribute you can key off of.



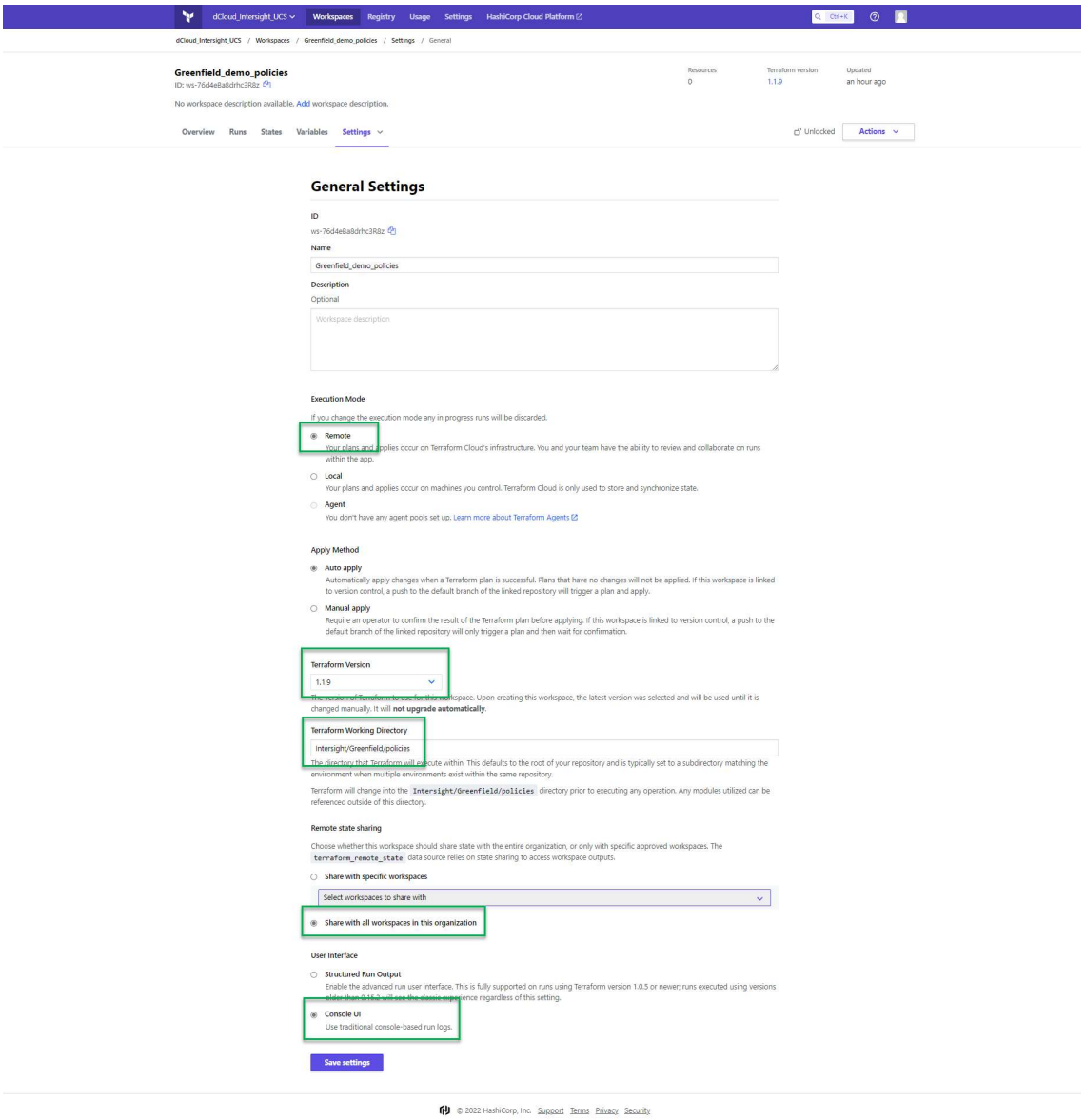
Step 12 Within the workspaces we can see several of the settings that have been pushed. We can see the VCS integration on the right-hand side.



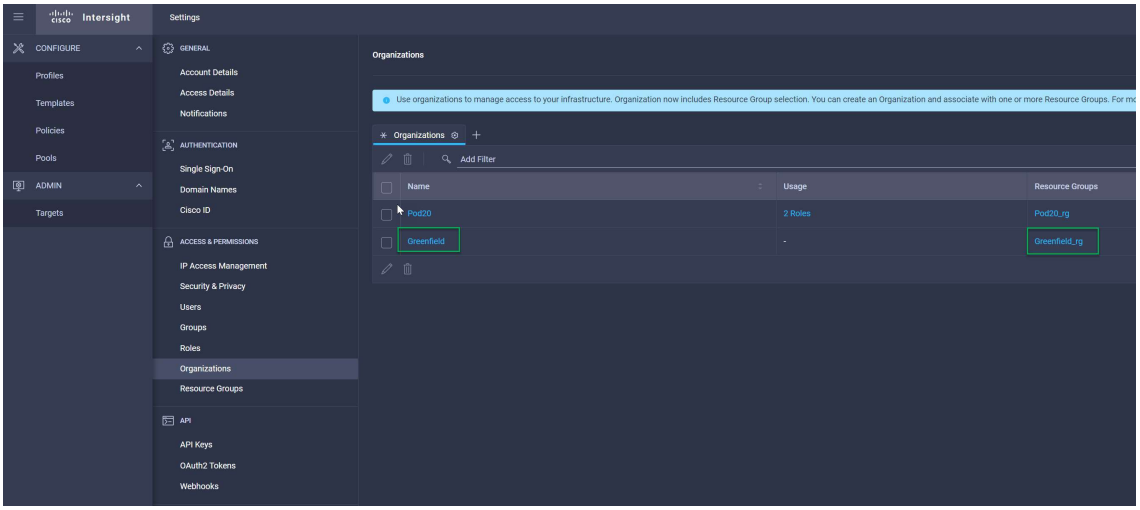
Step 13 Additionally going into the Variables we can see that the script pushed the sensitive variables into the workspace below.



Step 14 Below are a few more specifics from the General settings tab. Each of the highlighted settings were pushed by the script. The execution mode of "Remote" tells the workspace to run the plan/apply process in the cloud. We set the Terraform version based on the selected version above. The Terraform Working directory is the location inside the working directory. This can be changed by specifying the -d option at wizard startup to say the location these folders are going to be. It is important to recognize that the VCS base repository and the working directory are not the same. Each workspace will have their own working directory, that should be sub-folders within the root folder of the VCS base repository.



Step 15 In Intersight we can see the "**Greenfield**" folder that was created.



Task 4: Demo – Workspace and Organization deletion. (Optional Task)

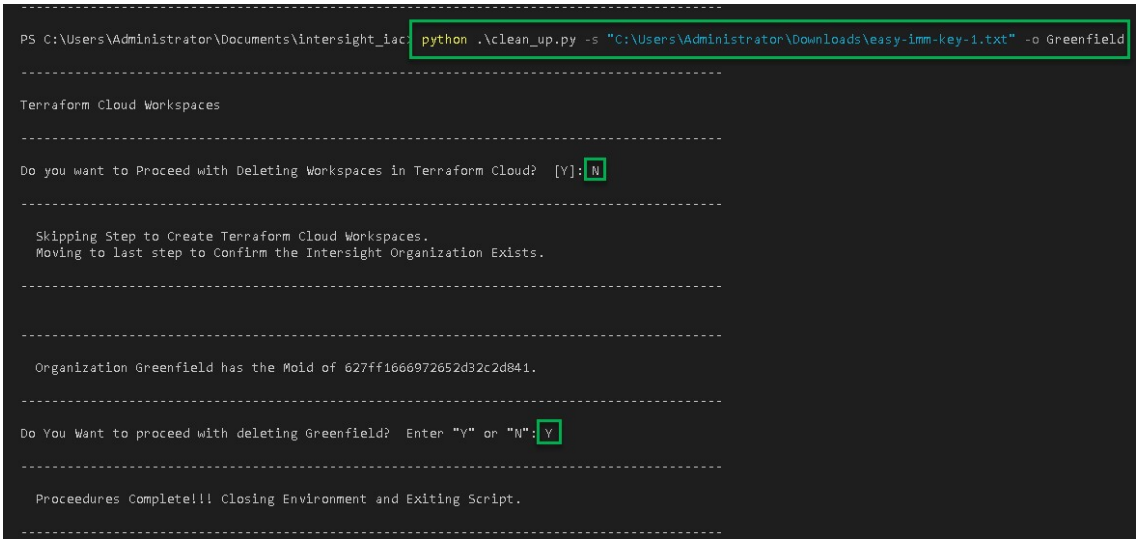
Step 1 In the intersight_iac repository there is a clean_up.py script that can be used to clean up the Workspaces and Organization in Intersight. The following steps are shown to show how to clean up the Workspaces in Terraform Cloud and the org in Intersight. You can see that there is one more argument in the command below with -o, which should be the Intersight organization but it also ties to the name of the workspaces so I am using it here to specify the prefix for the workspace names.

```
PS C:\Users\Administrator\Documents\intersight_iac> python .\clean_up.py -s "C:\Users\Administrator\Downloads\easy-imm-key-1.txt" -o Greenfield_demo

--------------------------------------------------------------------------------

Terraform Cloud Workspaces

--------------------------------------------------------------------------------

Do you want to Proceed with Deleting Workspaces in Terraform Cloud? [Y]:

--------------------------------------------------------------------------------

Terraform Cloud Organizations:

    Select an Option Below:
     1. atr
     2. Cisco-IST-TigerTeam
     3. Cisco-Richfield-Lab
     4. dCloud_Intersight_UCS
     5. deere-poc
     6. tyscott-training
     7. Tyson_Demo

--------------------------------------------------------------------------------

Please Enter the Option Number to Select for Terraform Cloud Organization 4

--------------------------------------------------------------------------------
```

Step 2 Below we delete all the Terraform Cloud workspaces.

```
--------------------------------------------------------------------------------

Please Enter the Option Number to Select for VCS Base Repository: 3

--------------------------------------------------------------------------------

Name of the Workspace to Delete in Terraform Cloud

--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_demo_policies]:

--------------------------------------------------------------------------

    Successfully Deleted Workspace "Greenfield_demo_policies".

--------------------------------------------------------------------------


--------------------------------------------------------------------------------

Name of the Workspace to Delete in Terraform Cloud

--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_demo_pools]:

--------------------------------------------------------------------------

    Successfully Deleted Workspace "Greenfield_demo_pools".

--------------------------------------------------------------------------


--------------------------------------------------------------------------------
--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_demo_profiles]:

--------------------------------------------------------------------------

    Successfully Deleted Workspace "Greenfield_demo_profiles".

--------------------------------------------------------------------------


--------------------------------------------------------------------------------

Name of the Workspace to Delete in Terraform Cloud

--------------------------------------------------------------------------------

Terraform Cloud Workspace Name. [Greenfield_demo_ucs_domain_profiles]:

--------------------------------------------------------------------------

    Successfully Deleted Workspace "Greenfield_demo_ucs_domain_profiles".

--------------------------------------------------------------------------


--------------------------------------------------------------------------------

  Proceedures Complete!!! Closing Environment and Exiting Script.

--------------------------------------------------------------------------------
```

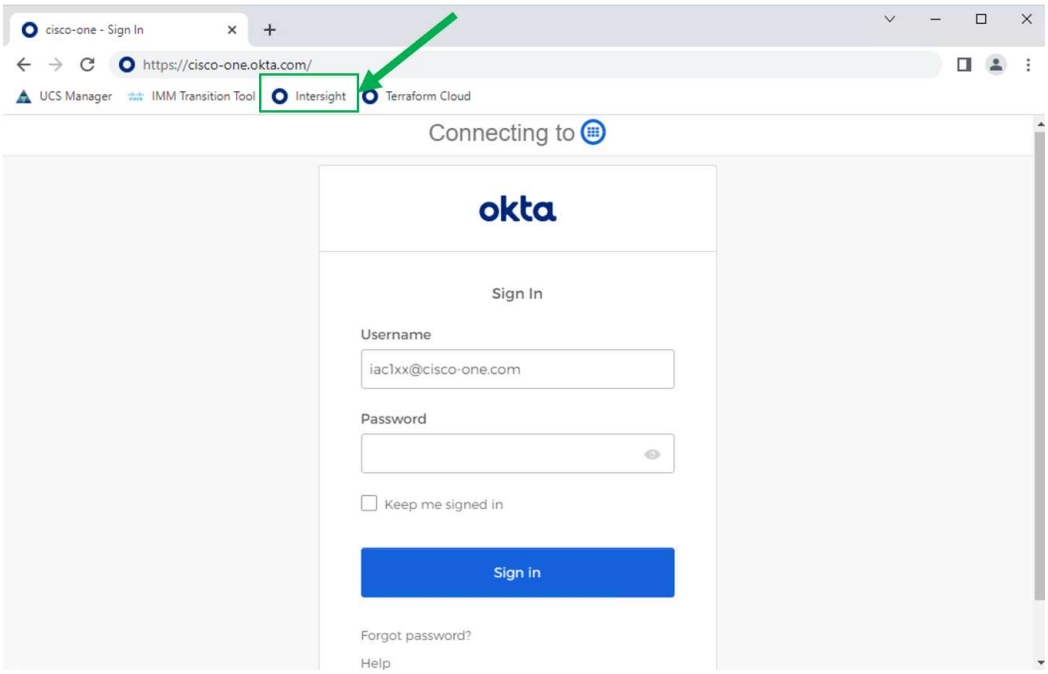
Step 3 Now we will run the clean_up.py again to clean up the “org” in Intersight.



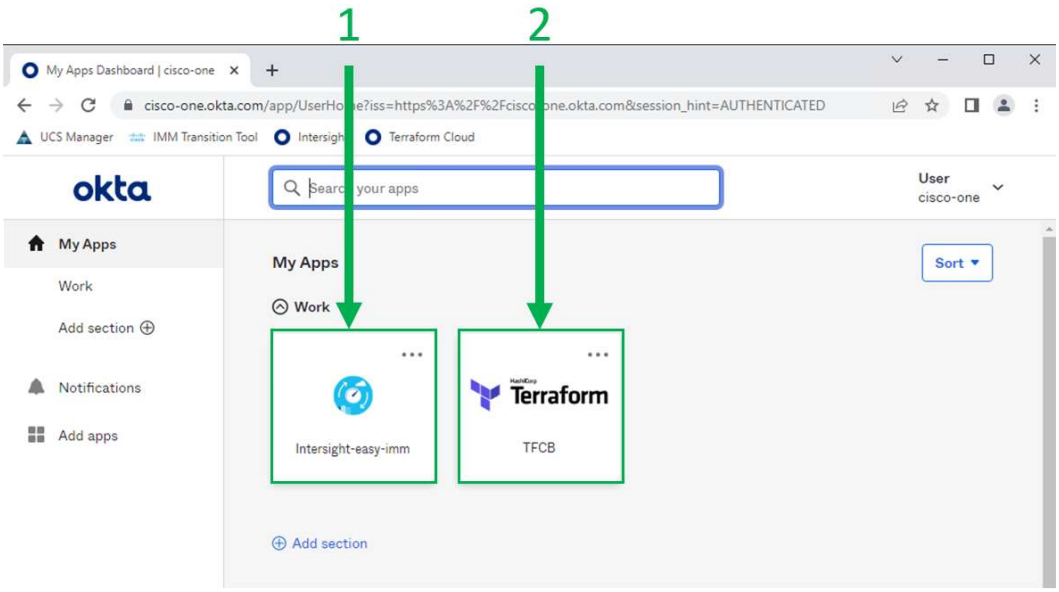
Task 5: Execute the Workspaces in Terraform Cloud

In this task you will now run an apply in the Terraform Cloud workspaces which will create the objects in Intersight.

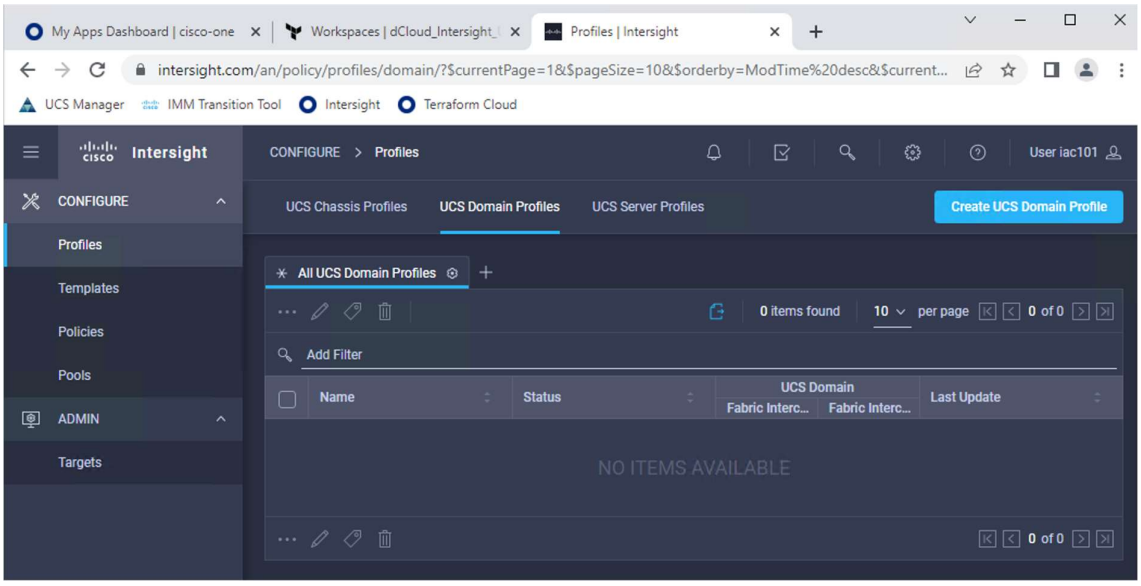
Step 1 From Chrome click on the **Intersight** or **Terraform Cloud** bookmark(s) (or browse to https://cisco-one.okta.com) and log in with username **iac1XX@cisco-one.com** (where XX is your Pod number 01-20) and password **C1sco12345**.



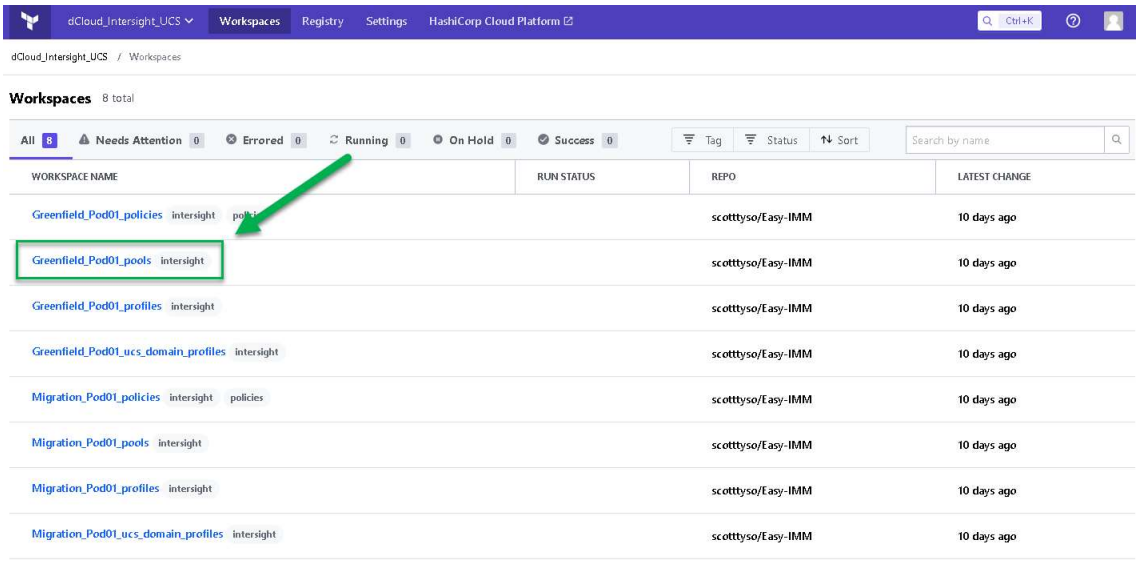
Step 2 From the okta dashboard, open two tabs. One for "**Intersight-easy-imm"** and the other for "**Terraform Cloud for Business"** (TFCB).



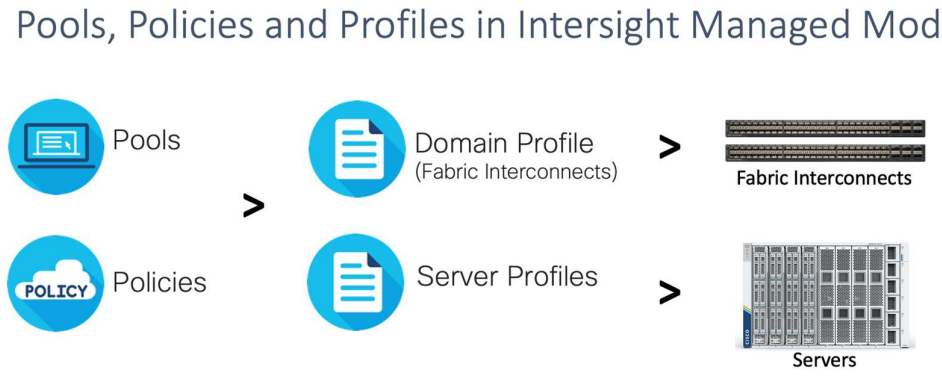
Step 3 From **Intersight**, browse the UCS Domain Profiles, UCS Server Profiles, Policies and Pools and notice that they are all empty.



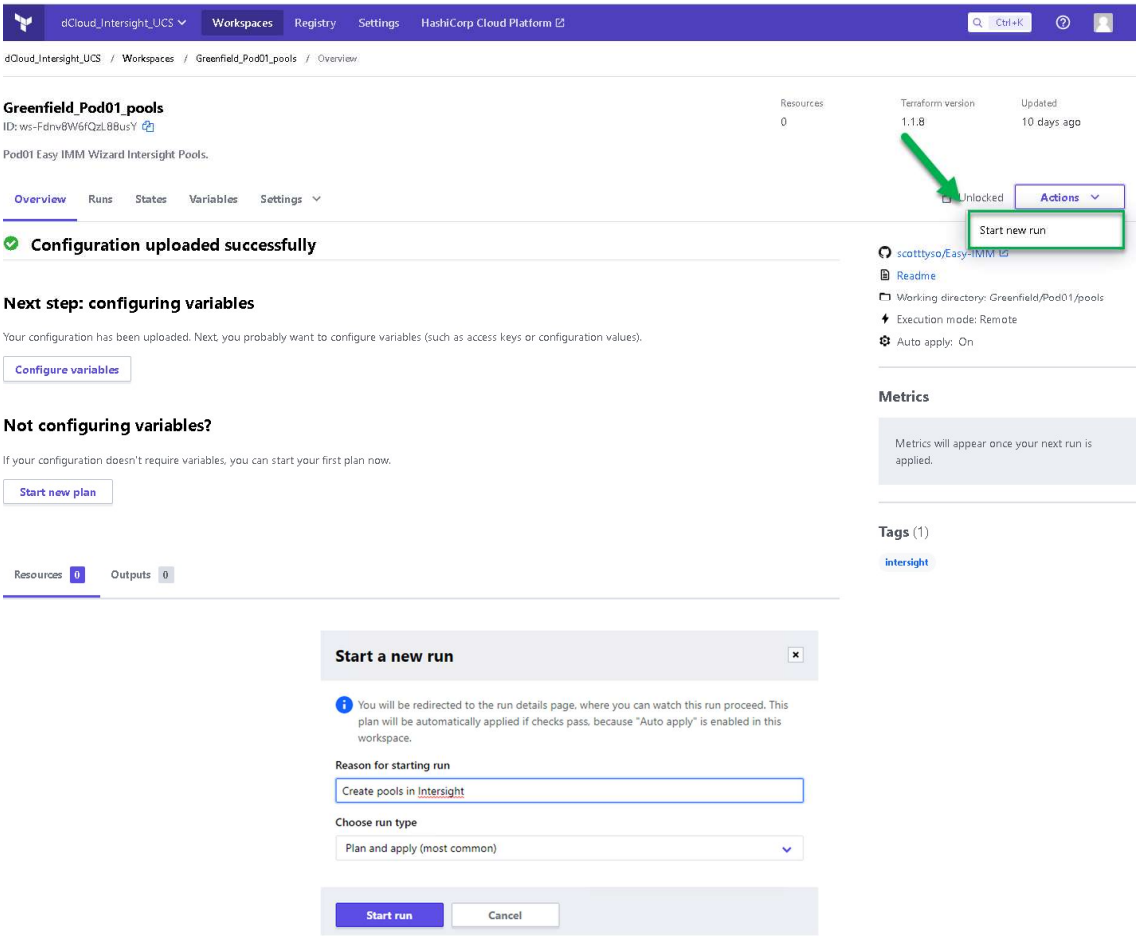
Step 4 From **Terraform Cloud** notice that your pod has 8 workspaces. Four for greenfield and four for IMM migration. Click on the **Greenfield_Pod_XX_pools** (where XX is your Pod number 01-20) workspace to go into that workspace:



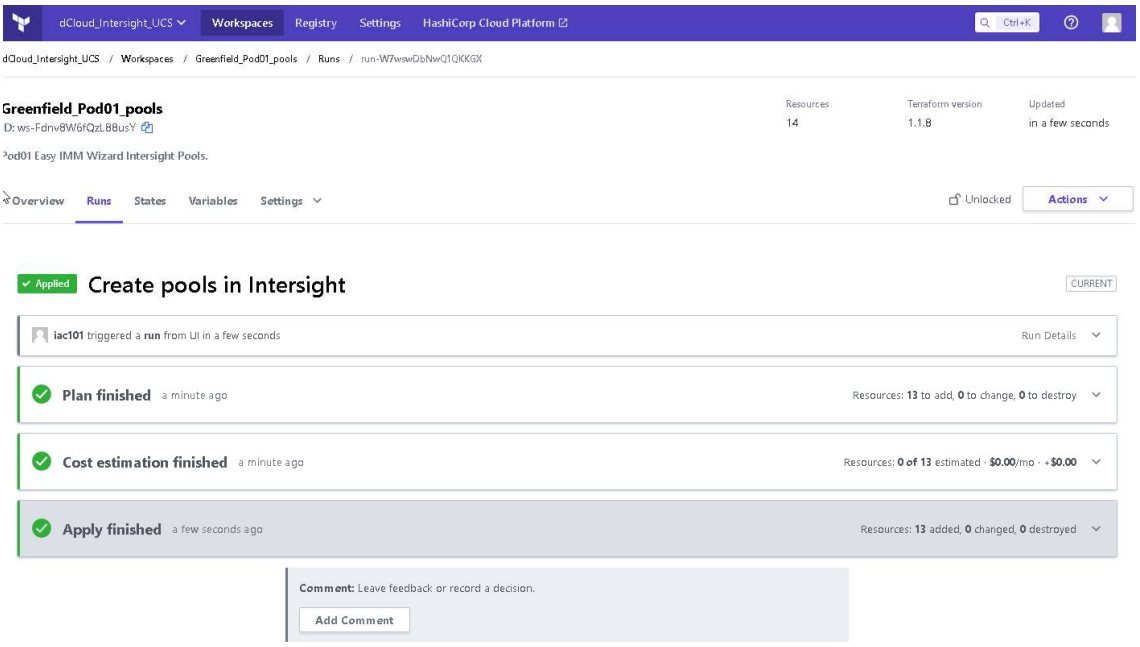
You will use the Greenfield workspaces to create all the pools, domain-policy, policies, and profiles in Intersight. They need to be created in the correct order as policies like IMC Access, and LAN Connectivity (as examples) need to consume the MOID of the MAC and IP Pools to complete the policy configuration. See the diagram below for how they relate to the fabric interconnect and actual server configuration:



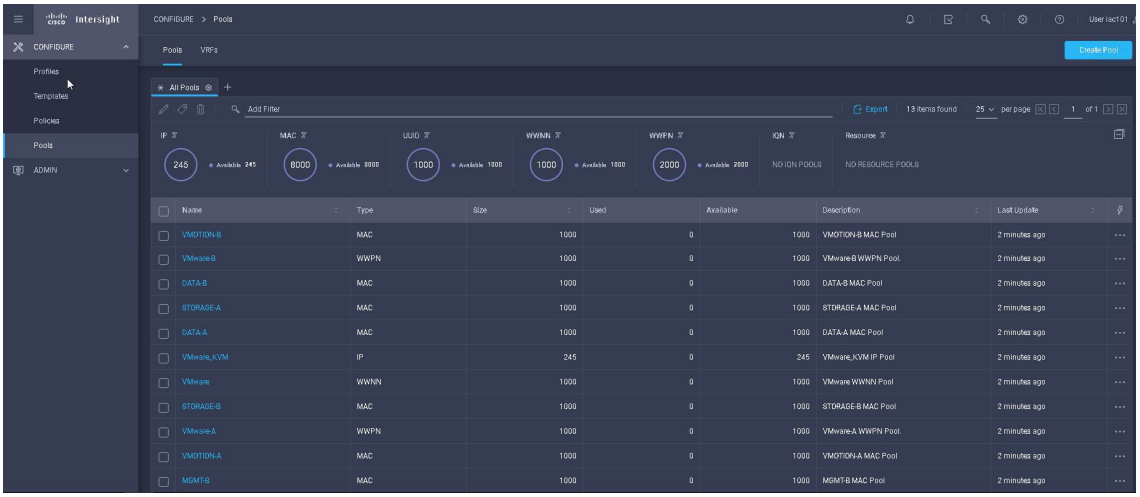
Step 5 From the Greenfield **pools** workspace, select **Action** and then **Start new run.** Specify a **Reason for starting the run** (IE: Create pools in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.



Watch the output shown while the Terraform code from the workspace is both run and applied. Warnings are OK, but errors are not. Upon completion you should see a green checkmark indicating that the apply finished.



Step 6 Now in **Intersight**, verify that all the pools have been created for UUIDs, MAC addresses (Fabric a and b), WWNN, WWPN (Fabric a and b) and IP addresses for management. Note that the screenshot below only shows pools for Greenfield. You will have a mix of Migration and Greenfield in here so your screen will look slightly different than below.

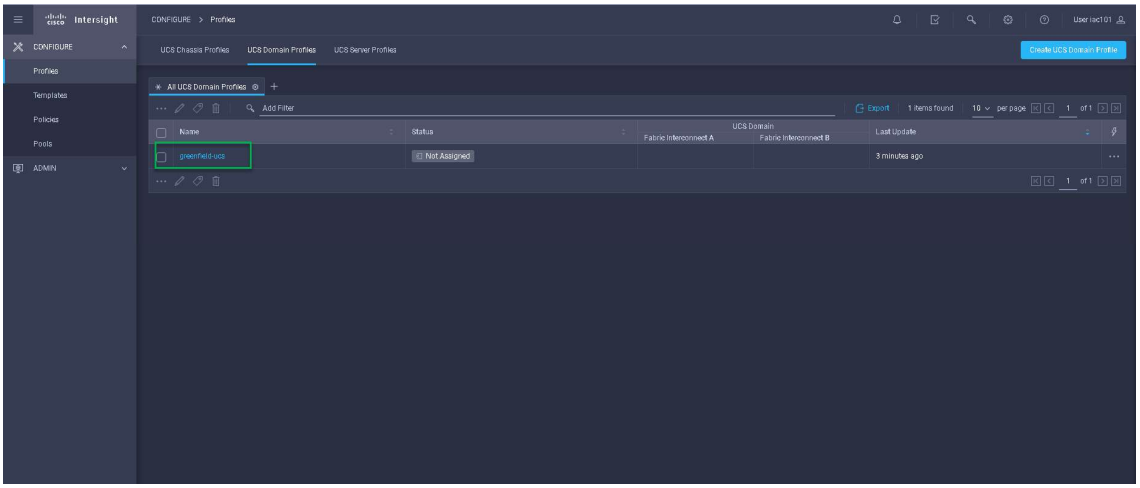


Step 7 Back in **Terraform Cloud**, now go into the **Greenfield_PodXX_domain_profiles** workspace, click **Actions** and **Start a new run** (where XX is your Pod number 01-20). Specify a **Reason for starting the run** (IE: Create domain-profiles in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.

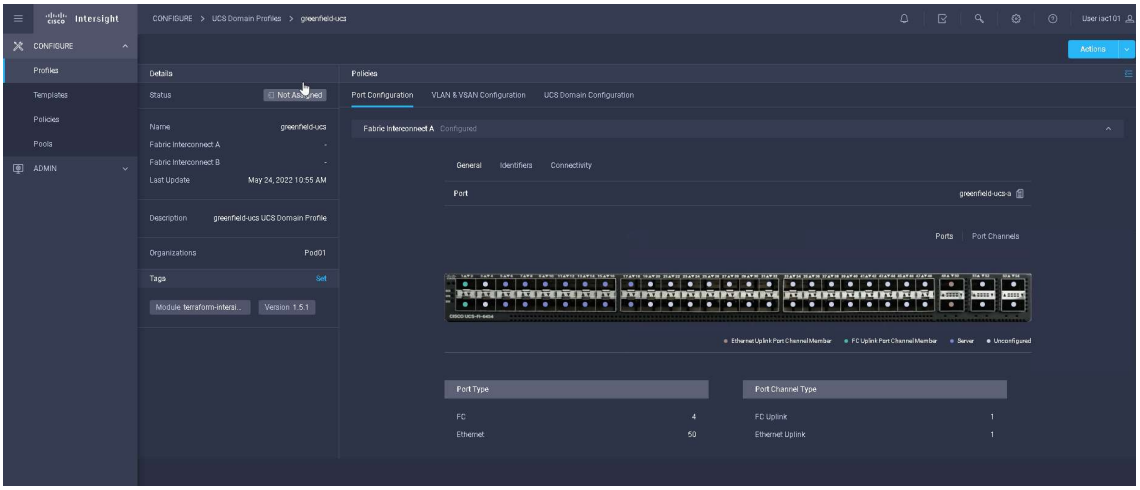
Step 8 In **Terraform Cloud**, now go into the **Greenfield_PodXX_policies** workspace, click **Actions** and **Start a new run** (where XX is your Pod number 01-20). Specify a **Reason for starting the run** (IE: Create policies in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.

Step 9 In **Terraform Cloud**, now go into the **Greenfield_PodXX_profiles** workspace, click **Actions** and **Start a new run** (where XX is your Pod number 01-20). Specify a **Reason for starting the run** (IE: Create profiles in Intersight) and then choose run type of **Plan and apply** and then click **Start run**.

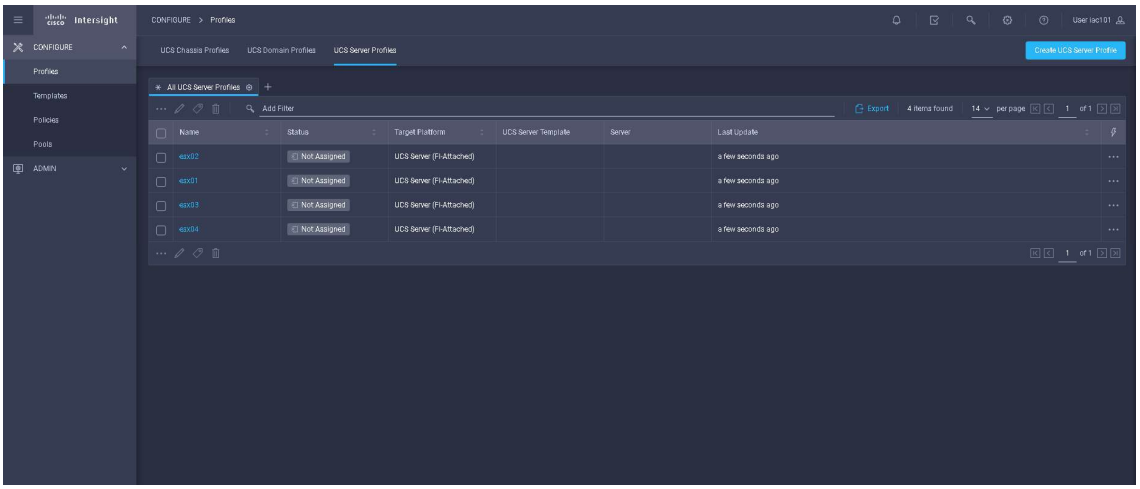
Step 10 In **Intersight**, check that you have a UCS Domain Profile called "**greenfield-ucs**".



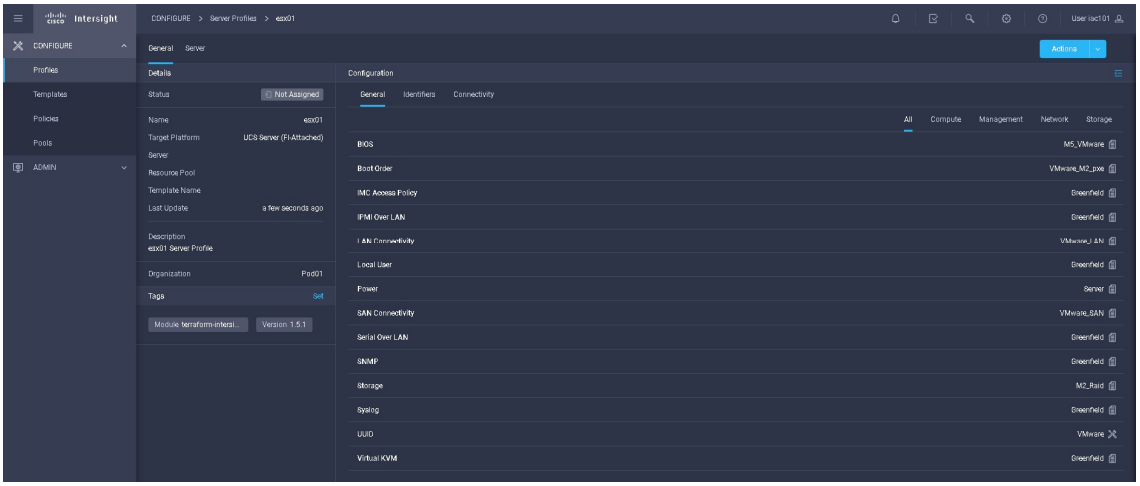
Step 11 Click on the "**greenfield-ucs**" domain profile and verify that a port configuration, VLAN & VSAN configuration and domain configuration has taken place because of your domain-profile run in Terraform Cloud.



Step 12 Click on the **UCS Server Profiles** and verify that 4 server profiles (esx01 through esx04) have been created.



Step 13 Click on one of the UCS Server Profiles and verify the configuration has been created.



Summary You have completed the process of both migrating a domain and building a new domain in Intersight. You will get the most out of this lab by spending some time reviewing the code in the files that were created. Both the wizard and the migration tool should not be a permanent method of managing the policies. Our recommendation would be to use the code in the workspaces to expand policies and or add additional pools/policies/profiles.