AC HUNTER™

ANALYZE. IDENTIFY. HUNT.

Welcome!

We're glad you've chosen to purchase AC-Hunter on the Azure platform. This guide will walk you through setting up AC-Hunter and provide pointers on where to go next.

Once you've purchased AC-Hunter, please email support@activecountermeasures.com and we'll provide an account for our portal. Once you receive your account information, please go to "AC-Hunter Getting Started" (https://portal.activecountermeasures.com/start-here/). This has links to AC-Hunter downloads, the User Guide (you don't need the Pre-Install Guide and Install Guide), FAQ's, Training courses, Blogs, YouTube channels, and multiple ways to get support if needed.

If you did not purchase AC-Hunter through the Azure Marketplace, see Appendix A for instructions on how to get started.

What you're getting

A full AC-Hunter installation will include the following:

- An AC-Hunter Azure cloud instance. You reach this through a web browser (at its hostname or IP address) and use that interface to review network traffic, looking for malicious traffic like beacons or other communication with a Command and Control server.
- Monitored systems. As part of the upcoming setup you'll place software on your other Windows and/or Linux Azure cloud instances. This software self-reports on the network traffic going to and coming from each instance. The network traffic reports are automatically sent to AC-Hunter, and from there AC-Hunter looks for Threats.
    - We officially support the following Linux distributions as Azure instances: Ubuntu 18.04, Ubuntu 20.04, and Centos 7.x
    - We officially support the following Windows distributions: Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10, and Windows 11

The monitoring software should not interfere with the normal operation of your servers.

Setting Up Your New AC-Hunter Environment

Setting Up Azure

We assume that you have some Linux and/or Windows systems in the Azure cloud that you want to inspect for Threats. During this install we'll install the software on these systems to make this Threat Hunting possible.

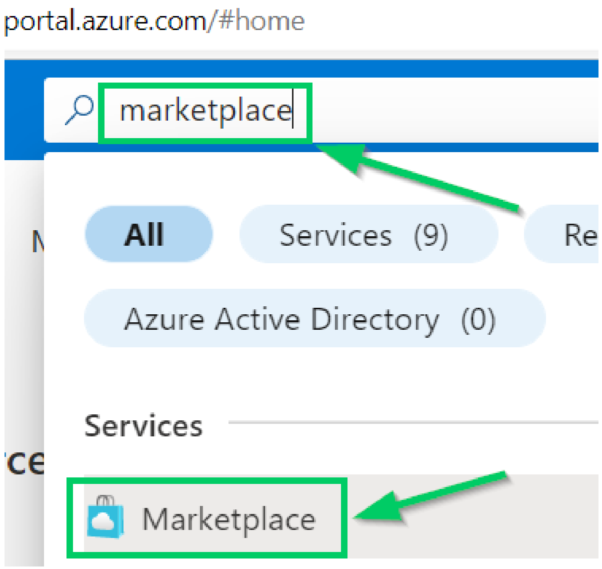
Firewall Settings

If you use one or more firewalls to protect your systems, you'll need to allow the following traffic types through them:

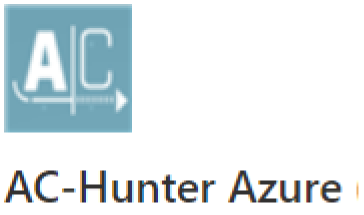
From	To	Port	Reason
Analyst laptops	AC-Hunter	TCP 22,443	Accessing AC-Hunter command line and web UI
Azure Windows systems	AC-Hunter	TCP 6379,9200	Reporting Windows network traffic
Azure Linux systems	AC-Hunter	TCP 22	Reporting Linux network traffic
AC-Hunter	Internet	UDP 53, TCP 53, 80, 443	Install process, updates, live lookups

Creating the AC-Hunter System

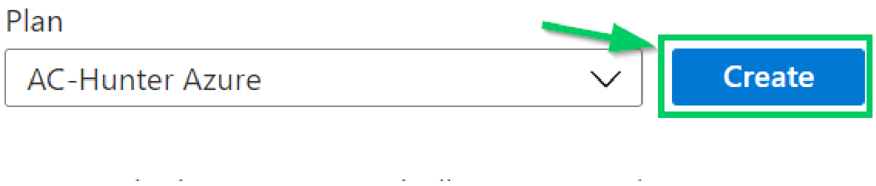
You'll need to purchase an AC-Hunter system from the marketplace. This is a cloud server that holds the AC-Hunter software. To purchase the VM, head to https://portal.azure.com and login with your Azure account. In the search bar, search for “Marketplace” and click “Marketplace” in the results.



Search for “AC-Hunter” and click the offering with the image similar to the following image.



After clicking the offering, click “Create”.

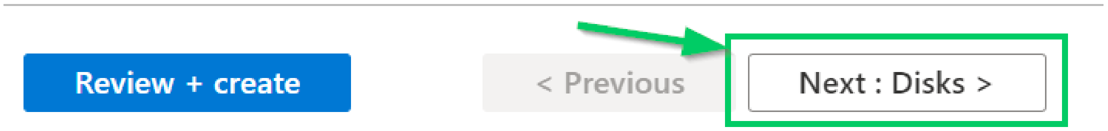


Fill in the following fields and leave the others as default (unless business requirements necessitate changing them):

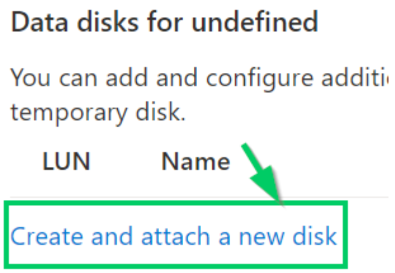
- **Subscription:** This is your Azure subscription under which the VM will run. This should be the same subscription that contains the VMs that AC-Hunter will be monitoring.
- **Resource Group:** Create a new resource group to hold the AC-Hunter VM.
- **Virtual Machine Name:** Choose a name for this AC-Hunter VM
- **Region:** Choose a region where the AC-Hunter VM will be located. This does not have to be the same region as the VMs that AC-Hunter will be monitoring.
- **Size:** It needs a minimum of 32GB of memory and 4 processor cores (64GB and at least 8 processor cores are recommended for heavy loads). Do not worry about the size of the "Temp storage" that is specified alongside the cores and memory specifications; you will add a storage volume that will hold all of your data.
- **Administration Account:** Fill in the details for the account and authentication mechanism that you will be using to connect to the AC-Hunter VM (note: this is not the account that will be used to login to the AC-Hunter web interface; this is the account for gaining shell access to the AC-Hunter VM).

Now we add the storage volume that will hold all of your sensor logs and data. This should be at least 500GB, and if you know you will be 1) watching high volumes of traffic on your other servers or 2) need to preserve daily snapshots for more than a few months due to a data retention policy, this should be 1TB or more.

Click the "Next: Disks >" button at the bottom of the Azure page.

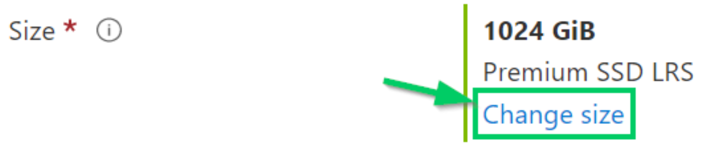


Towards the bottom of the page, click the "Create and attach a new disk" link.


Data disks for undefined

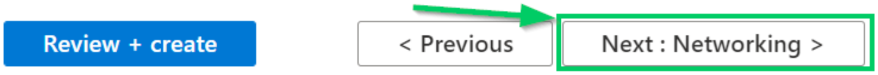
You can add and configure additi
temporary disk.

Click the "Change size" link to select the disk size.

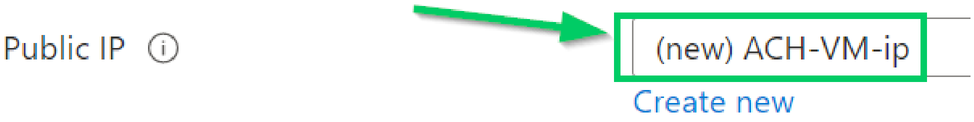

Size * ⓘ 1024 GiB
Premium SSD LRS

Choose a size, click “Ok” at the bottom of the page, and then click “Ok” on the bottom of the “Create a new disk” page. Note that the storage volume for AC-Hunter **must** be on SSDs (Solid-State Drives). The Azure choices for this are "Ultra Disk Storage", "Premium SSD", and "Standard SSD". Please do **not** choose "Standard HDD"; this would bottleneck the AC-Hunter system, making it unusably slow.

Click the “Next: Networking >” button at the bottom of the page.

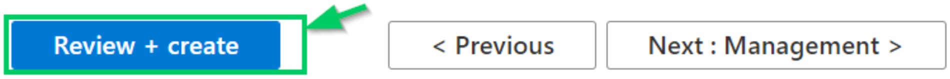


On the networking page, you can choose to place AC-Hunter in an existing subnet or let Azure create a new subnet for this system. Note that if AC-Hunter is on a subnet that is not reachable by the VMs that it is monitoring, then the monitored VMs will need to communicate with AC-Hunter via its Public IP address. If systems will be communicating to AC-Hunter via its public IP, ensure that the Public IP option on this page is either set to create a new IP or use an existing public IP. You will also need to assign a Public IP address in the case that you’d like to reach the AC-Hunter VM via shell access or the AC-Hunter VM’s web console outside of your Azure internal network.

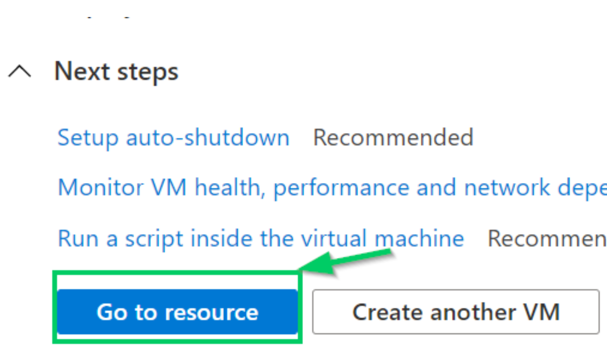


Public IP: (new) ACH-VM-ip

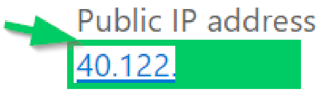
The options in the remaining menus can likely be left to their defaults. You may review them, if desired, by continuing to click the “Next: [Options Page Title] >” buttons at the bottom of the pages. Otherwise, click the “Review + create” button at the bottom of the page to proceed to the final creation page.



On the final screen, review the details of the VM. If satisfied with the parameters of the VM, click the “Create” button at the bottom of the page. It may take 5-10 minutes for the VM to be deployed. Once it is deployed, the page will be refreshed. Click the “Go to resource” button at the bottom of the page.

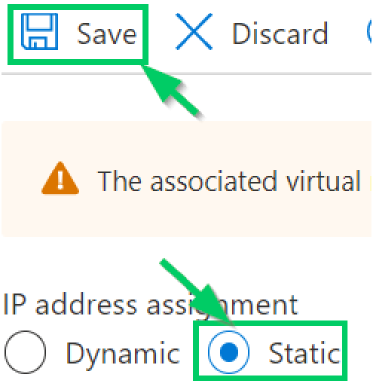

Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM

On this page, you will be able to view and modify various details of the VM. If you assigned a Public IP address to this system, we require that you set its IP address to be static. Click on the Public IP address.



Public IP address
40.122.[redacted]

Click the radio button next to “Static” and then click the “Save” button at the top of the page:



The associated virtual

IP address assignment
○ Dynamic ● Static

Make a note of the Public IP as you will use it in the following steps.

Setting Up AC-Hunter

Once your cloud server is set up, please ssh to that system using the Public IP address that you noted down in the previous step. If you've logged in as a non-root user, please run

```
sudo bash
```

to become root.

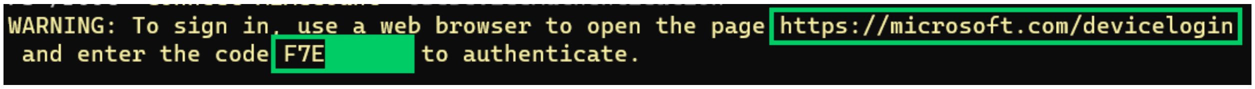
Now run:

```
/var/ACH-Azure/install_ACH-Azure.sh
```

to start the setup process. This will prepare the data storage volume and will install AC-Hunter and the Espy server (the module that accepts network traffic reports from your Windows Azure instances).

During the setup process you'll generate some passwords for the different services used in AC-Hunter. Please record these in a password vault for later use.

The setup script will then provision various resources in your Azure environment that will be needed for deploying Espy and Zeek to your systems in Azure. The script will prompt you for the IP address of the AC-Hunter system that monitored systems will use to send data to AC-Hunter. Enter the Public IP address of the AC-Hunter system. You will then be prompted to perform a browser-based login to Azure. Follow the link that it provides, enter the device code that was shown, and login with your Azure account. NOTE: The Azure account with which you login must have the ability to create resource groups and the ability to assign roles to users.



```
WARNING: To sign in, use a web browser to open the page https://microsoft.com/devicelogin
 and enter the code F7E[redacted] to authenticate.
```

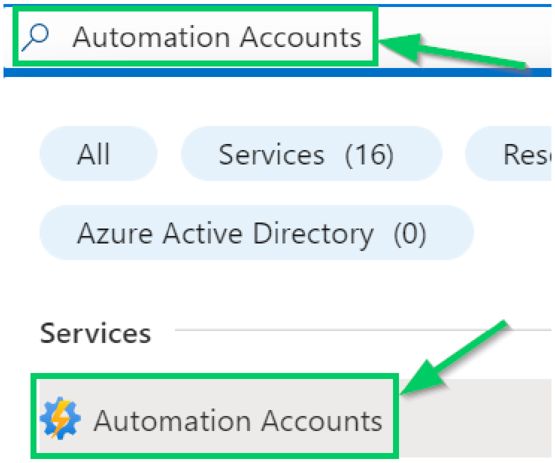
After authenticating, the setup will automatically perform the following tasks:

- Create a Resource Group: ACH-Azure-RG
- Create a Storage Account in ACH-Azure-RG
    - Will have a prefix of “achazure” that is followed by a string of randomly-generated characters
- Create a Storage Container named “achcontainer” in the above Storage Account
- Upload “install_zeek.sh” and “AC-Hunter.tar” to “achcontainer”
- Create an Automation Account in ACH-Azure-RG named “ACH-Automation”
- Create and populate a Runbook named “ACH-Azure-Deploy” under the ACH-Automation account

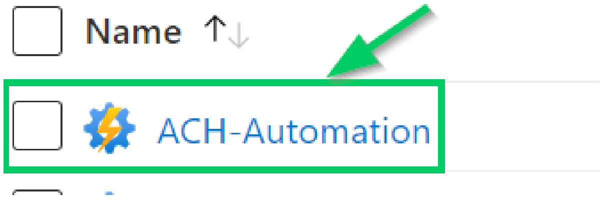
After the above Azure tasks have been completed, the script will delete the Azure token files from disk so that further Azure actions will require additional authentication to Azure.

Start Monitoring Azure Servers

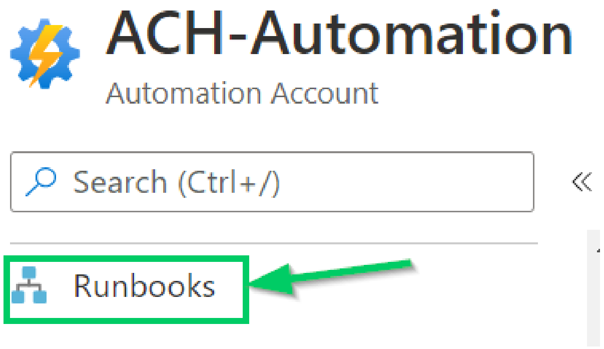
AC-Hunter has the ability to watch both Linux and Windows cloud instances in Azure. To start this, please login to the Azure portal. Use the search bar to search for “Automation Accounts” and click the “Automation Accounts” result.



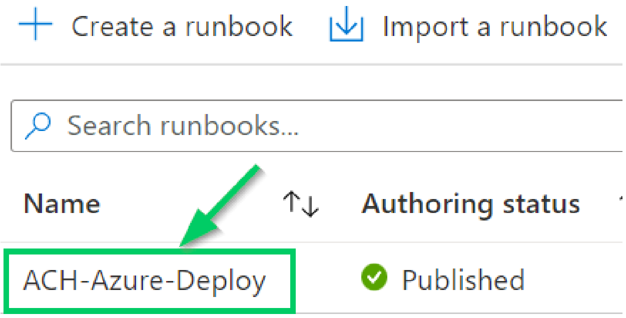
Click “ACH-Automation”.



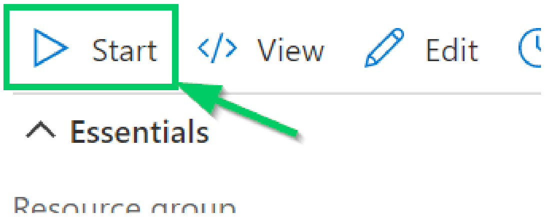
Find “Runbooks” in the left panel and click it.



Click the “ACH-Azure-Deploy” runbook.

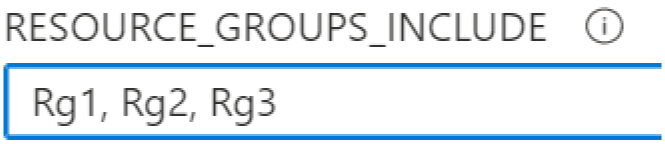


Click the “Start” button on the page.



You will be prompted with a series of parameters before starting the Runbook that will perform the Espy and Zeek deployment. By default, the script will target both Linux (Zeek install) and Windows (Espy install) systems in your Azure environment. You can disable one or the other by changing either “INSTALL_ZEEK” or “INSTALL_WINDOWS” parameters to “False” (found in the drop-down menu under the parameter names).

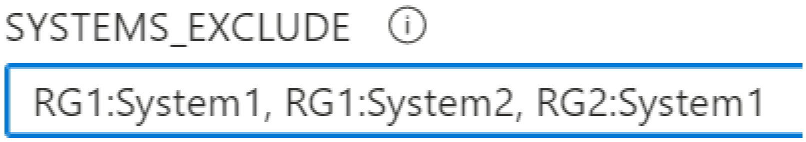
The RESOURCE_GROUPS_INCLUDE parameter must be filled in. This is used to tell the deployment Runbook which systems to target for installation. Provide a comma-separated list of the resource groups to include.



RESOURCE_GROUPS_INCLUDE ⓘ

Rg1, Rg2, Rg3

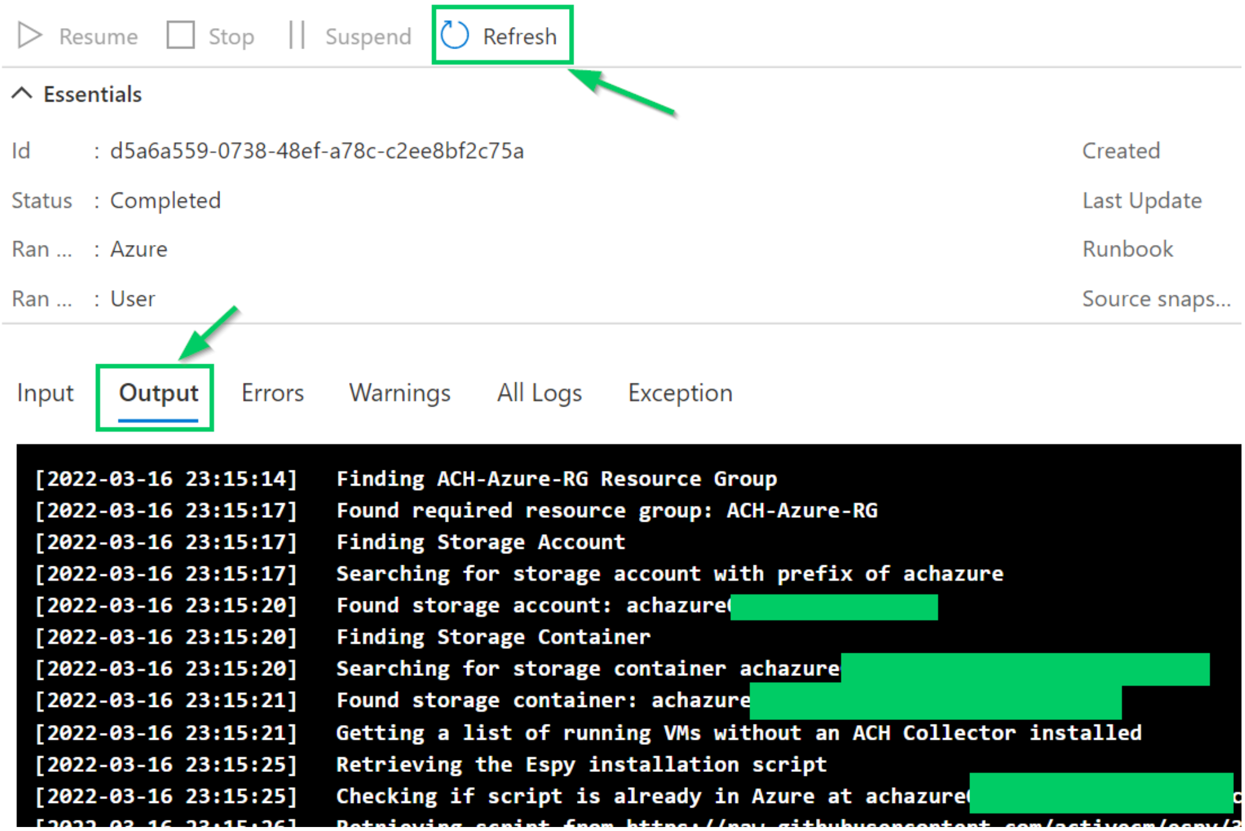
The SYSTEMS_EXCLUDE parameter can be used to exclude individual systems from installation. By default, the AC-Hunter VM is excluded from installation. To add systems to the list, use a format of ResourceGroupName:VMName for systems. Provide these systems as a comma-separated list in the SYSTEMS_EXCLUDE parameter.



SYSTEMS_EXCLUDE ⓘ

RG1:System1, RG1:System2, RG2:System1

After filling in the parameters, click the “Ok” button at the bottom of the page to begin deployment. You will be taken to a “Job” page where you can view the output of the deployment Runbook in the “Output” window (you may have to periodically click the “Refresh” button at the top of the page”).



Id : d5a6a559-0738-48ef-a78c-c2ee8bf2c75a

Status : Completed

Ran ... : Azure

Ran ... : User

Created

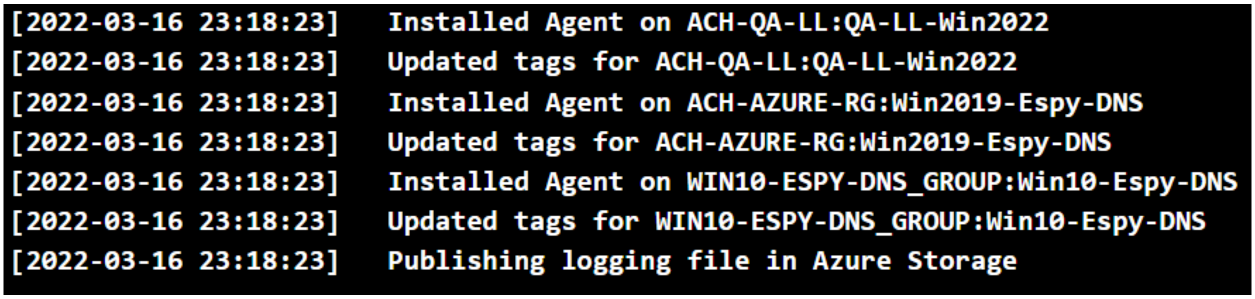
Last Update

Runbook

Source snaps...

```
[2022-03-16 23:15:14]   Finding ACH-Azure-RG Resource Group
[2022-03-16 23:15:17]   Found required resource group: ACH-Azure-RG
[2022-03-16 23:15:17]   Finding Storage Account
[2022-03-16 23:15:17]   Searching for storage account with prefix of achazure
[2022-03-16 23:15:20]   Found storage account: achazure[redacted]
[2022-03-16 23:15:20]   Finding Storage Container
[2022-03-16 23:15:20]   Searching for storage container achazure[redacted]
[2022-03-16 23:15:21]   Found storage container: achazure[redacted]
[2022-03-16 23:15:21]   Getting a list of running VMs without an ACH Collector installed
[2022-03-16 23:15:25]   Retrieving the Espy installation script
[2022-03-16 23:15:25]   Checking if script is already in Azure at achazure[redacted]c
[2022-03-16 23:15:26]   Retrieving script from https://raw.githubusercontent.com/activecm/espy/a
```

This process may take some time depending on the number of systems in your environment. Systems on which Zeek or Espy were successfully deployed will appear towards the bottom of the output after the Runbook has completed.



```
[2022-03-16 23:18:23]   Installed Agent on ACH-QA-LL:QA-LL-Win2022
[2022-03-16 23:18:23]   Updated tags for ACH-QA-LL:QA-LL-Win2022
[2022-03-16 23:18:23]   Installed Agent on ACH-AZURE-RG:Win2019-Espy-DNS
[2022-03-16 23:18:23]   Updated tags for ACH-AZURE-RG:Win2019-Espy-DNS
[2022-03-16 23:18:23]   Installed Agent on WIN10-ESPY-DNS_GROUP:Win10-Espy-DNS
[2022-03-16 23:18:23]   Updated tags for WIN10-ESPY-DNS_GROUP:Win10-Espy-DNS
[2022-03-16 23:18:23]   Publishing logging file in Azure Storage
```

This will install the needed software:

- On Windows 10 systems we'll install an Espy client. This package will report all network connections and DNS requests to AC-Hunter.
- On Ubuntu Linux (16.04, 18.04, and 20.04) and Centos Linux (7.x), we'll install the Zeek network monitoring package. This, too, will send reports on network traffic back to AC-Hunter.

Next steps

With the above steps complete, your cloud servers will send network traffic reports to AC-Hunter. Within a few hours, AC-Hunter will have new databases for these systems; one for all Windows systems, and individual databases for each Linux system. These databases will continue to fill up for the first 24 hours, and after that they'll drop the oldest hour when a new one is added.

To start working with these, connect to your AC-Hunter instance by going to the following in a web browser (we strongly recommend Chrome as it's the most heavily used and tested):

```
https://achunter.system.address.or.hostname
```

(When you connect, you'll be warned that your browser is unable to verify the certificate of that system. If you would like to assign a hostname to this system, our documentation provides the steps to later install a valid certificate for it.)

You'll be asked for the username and password generated during the install. The default username is "welcome@activecountermeasures.com", though you had the option of changing this. Please enter the username and password you chose.

You'll be asked to select a database. If you're logging in immediately after setup, you're likely to see the sample databases provided with AC-Hunter. Within a few hours you should see a new database named “localhost-rolling”. This database will contain all of the traffic from the Azure Windows and Azure Linux systems on which you installed agents.

At this point you can start Threat Hunting these systems. If you're new to AC-Hunter or Threat Hunting in general, we suggest you start at https://portal.activecountermeasures.com/start-here/ . If you want a quick introduction to how to use it, we suggest clicking on "Tutorials" there; each of the videos are short (around 10 minutes) introductions to different aspects of Threat Hunting with AC-Hunter.

Special Notes on Differences with ACH-Azure versus On-Premises AC-Hunter

Please note that as of AC-Hunter 6.1.0, the following modules will not work with data collected from Windows systems via Espy:

- Long Connections
- Client Signature

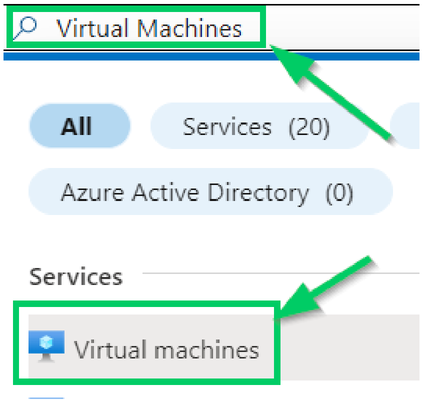
We are working to support these modules for Azure Windows systems in a future release. These features will still work for Linux systems in the Azure environment.

Appendix A

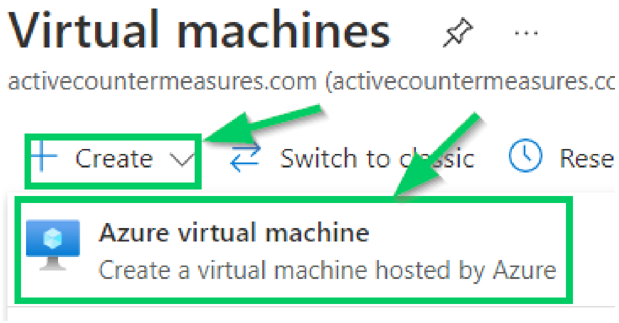
If you purchased AC-Hunter outside of the Azure Marketplace, you can still set up AC-Hunter within Azure.

Provision a VM in Azure

Sign into the Azure portal (https://portal.azure.com/) with an account that has the ability to provision VMs within the environment. Search “Virtual Machines” in the search bar and click the “Virtual Machines” result.



Click “Create” in the top-left and then select “Azure virtual machine”.


Virtual machines
activecountermeasures.com (activecountermeasures.cc
Create
Switch to classic
Rese
Azure virtual machine
Create a virtual machine hosted by Azure

For the VM settings, please refer to the “Creating the AC-Hunter System” section of this document. Ignore the paragraph about purchasing the VM in the Azure Marketplace and proceed to the paragraph that starts with “Fill in the following fields and leave the others as default…”. The only added setting is that you will need to select “Ubuntu Server 20.04 LTS Gen2” for the “Image”.

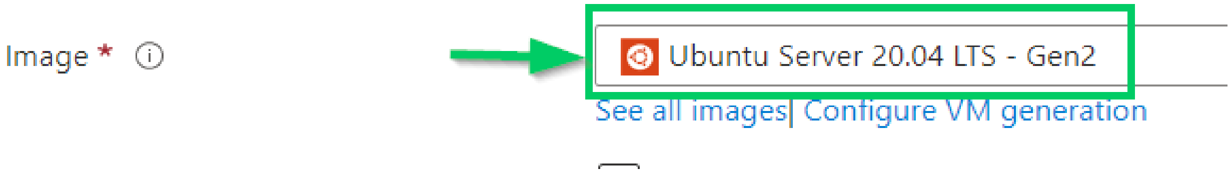


Image * Ubuntu Server 20.04 LTS - Gen2

Please follow the remaining steps in the “Creating the AC-Hunter System” before proceeding to the next section of this Appendix.

Install ACH-Azure

Obtain the ACH-Azure.tar file from the ACM portal (https://portal.activecountermeasures.com/). Transfer the ACH-Azure.tar file to the Azure Ubuntu 20.04 system you created in the “Provision a VM in Azure Section”. SSH to the Azure Ubuntu 20.04 system. Untar the ACH-Azure.tar file with the following command:

```
        sudo tar -C /var/ -xf ACH-Azure.tar
```

Enter the following commands to install PowerShell:

```
        sudo apt update
        sudo apt install -y wget apt-transport-https
software-properties-common

        wget -q
https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft
-prod.deb

        sudo dpkg -i packages-microsoft-prod.deb
        sudo apt update
        sudo apt install -y powershell
```

Next, install the PowerShell Az Cmdlet by using the following commands:

```
        sudo pwsh
        Install-Module -Name Az -Scope AllUsers -Repository PSGallery
-Force

        exit
```

With the prior steps completed, follow the steps in the “Setting Up AC-Hunter” section of this document for the remainder of the installation.