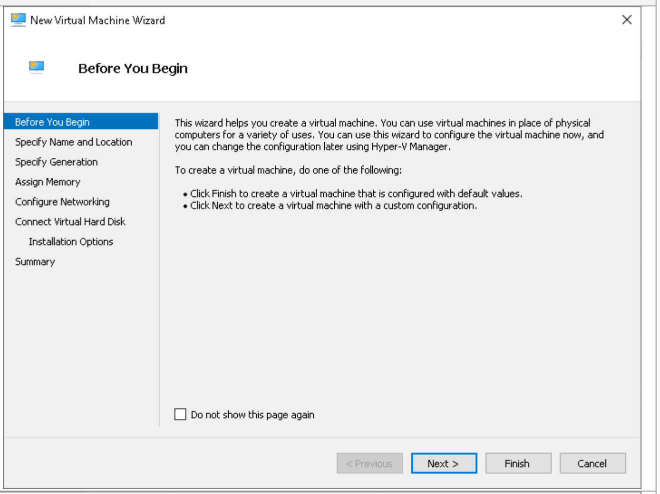
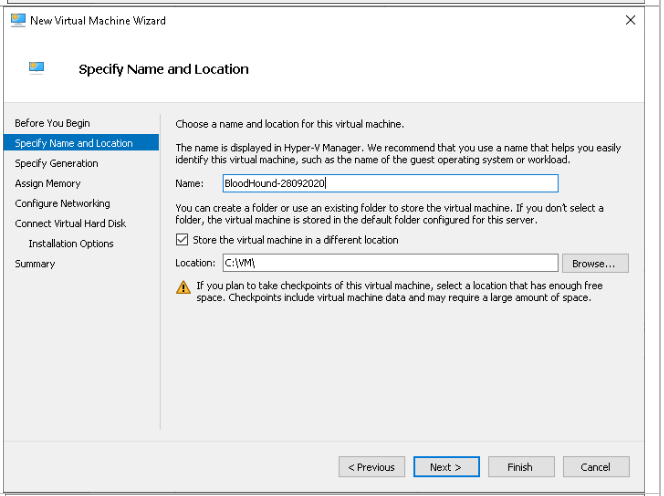
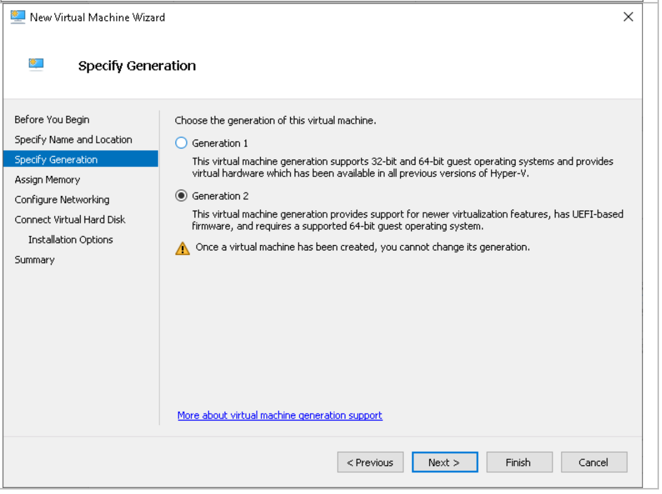
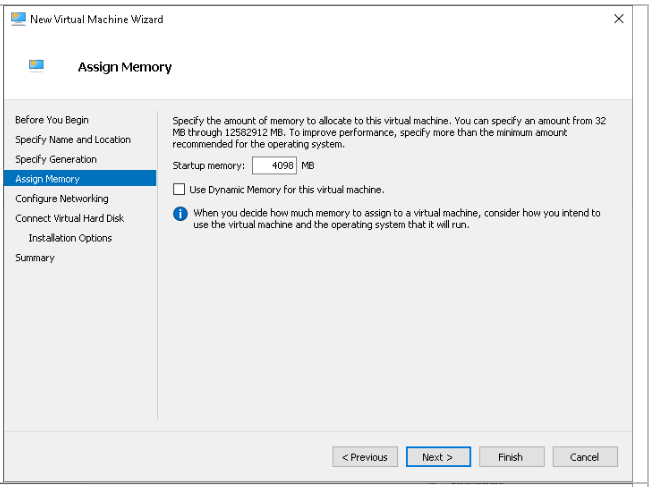
Assessment VM

Create and Prepare a VM

	 New Virtual Machine Wizard Before You Begin Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary < Previous Next > Finish Cancel This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager. To create a virtual machine, do one of the following: • Click Finish to create a virtual machine that is configured with default values. • Click Next to create a virtual machine with a custom configuration. □ Do not show this page again
	 New Virtual Machine Wizard Specify Name and Location Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary Browse... < Previous Next > Finish Cancel Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload. Name: BloodHound-28092020 You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server. ☑ Store the virtual machine in a different location Location: C:\VM\ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.
	 New Virtual Machine Wizard Specify Generation Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary More about virtual machine generation support < Previous Next > Finish Cancel Choose the generation of this virtual machine. ○ Generation 1 This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V. ● Generation 2 This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system. Once a virtual machine has been created, you cannot change its generation.



New Virtual Machine Wizard

Assign Memory

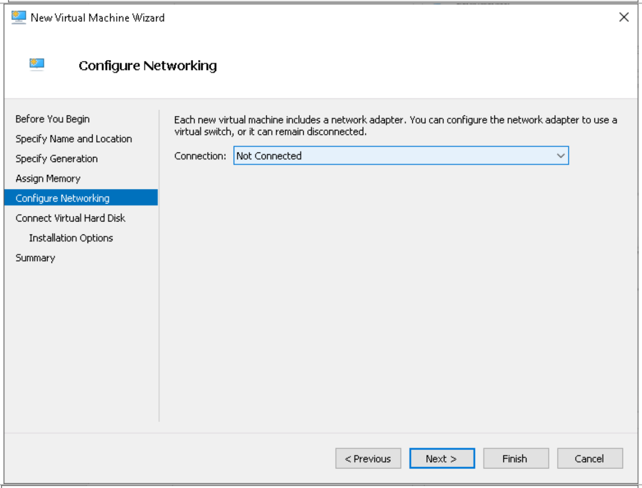
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 4098 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

Chose “Not Connected” for the moment

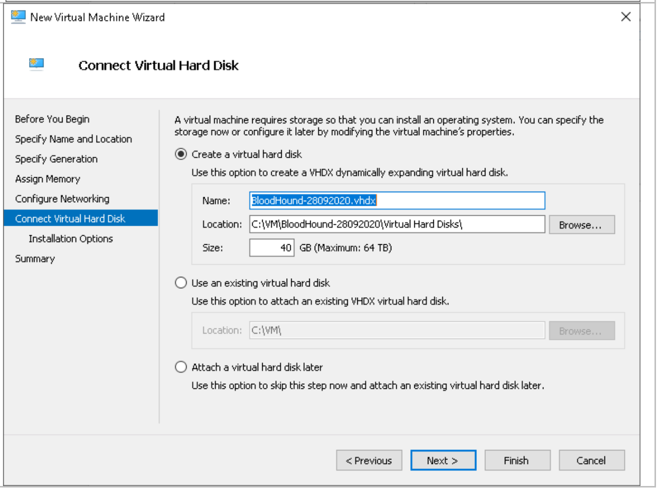


New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine’s properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: BloodHound-28092020.vhdx

Location: C:\VM\BloodHound-28092020\Virtual Hard Disks\ Browse...

Size: 40 GB (Maximum: 64 TB)

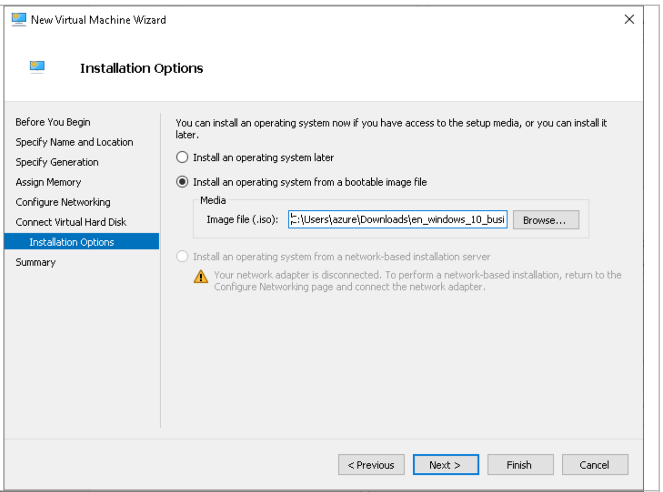
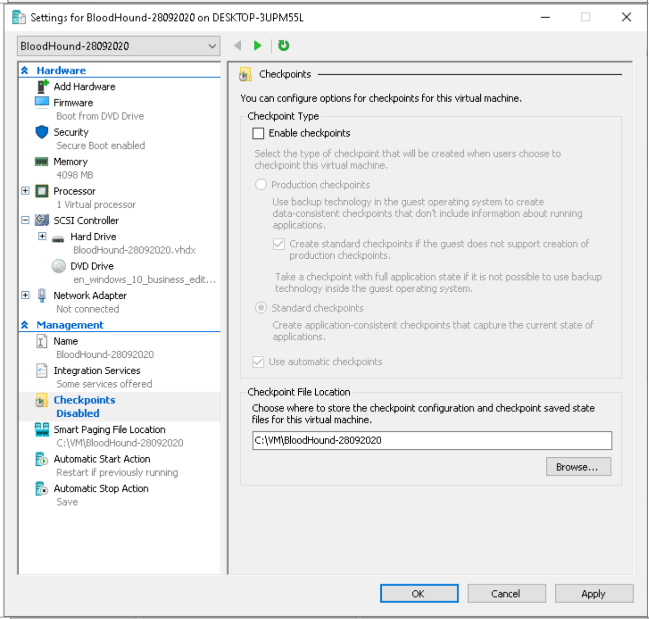
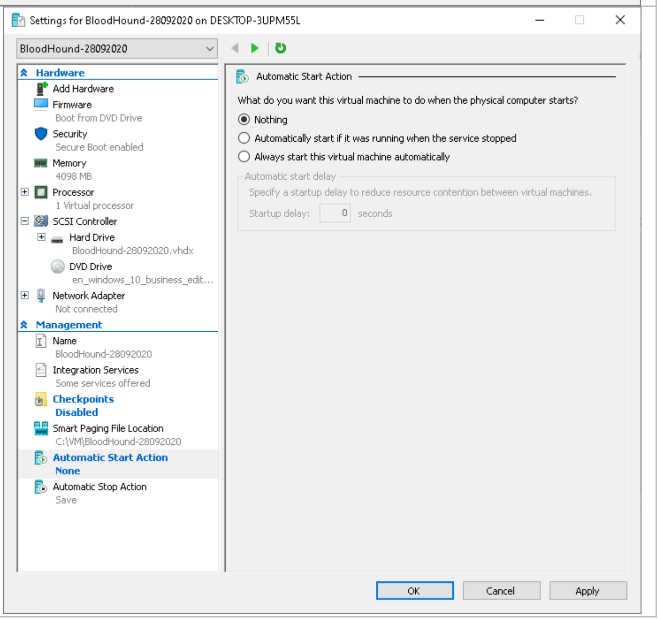
○ Use an existing virtual hard disk

Use this option to attach an existing VHDX virtual hard disk.

Location: C:\VM\ Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

	
Checkpoints: Disable Checkpoints (Optional)	
Automatic Start Action: Turn off Automatically start	

New Virtual Machine Wizard

Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable image file

Media

Image file (.iso): C:\Users\azure\Downloads\en_windows_10_busi

○ Install an operating system from a network-based installation server

Your network adapter is disconnected. To perform a network-based installation, return to the Configure Networking page and connect the network adapter.

Settings for BloodHound-28092020 on DESKTOP-3UPM55L

Checkpoints

You can configure options for checkpoints for this virtual machine.

Checkpoint Type

□ Enable checkpoints

Select the type of checkpoint that will be created when users choose to checkpoint this virtual machine.

○ Production checkpoints

Use backup technology in the guest operating system to create data-consistent checkpoints that don't include information about running applications.

☑ Create standard checkpoints if the guest does not support creation of production checkpoints.

Take a checkpoint with full application state if it is not possible to use backup technology inside the guest operating system.

● Standard checkpoints

Create application-consistent checkpoints that capture the current state of applications.

☑ Use automatic checkpoints

Checkpoint File Location

Choose where to store the checkpoint configuration and checkpoint saved state files for this virtual machine.

C:\VM\BloodHound-28092020

Settings for BloodHound-28092020 on DESKTOP-3UPM55L

Automatic Start Action

What do you want this virtual machine to do when the physical computer starts?

● Nothing

○ Automatically start if it was running when the service stopped

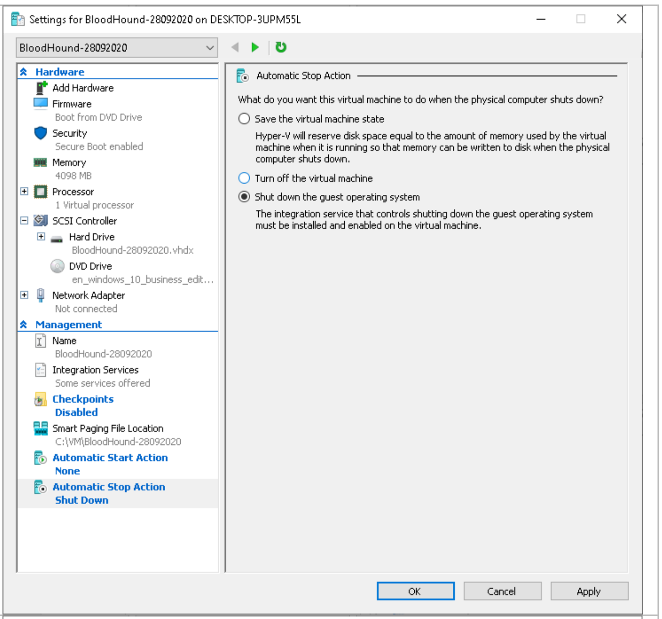
○ Always start this virtual machine automatically

Automatic start delay

Specify a startup delay to reduce resource contention between virtual machines.

Startup delay: 0 seconds

Automatic Stop Action: Shut down the guest operating system



Settings for BloodHound-28092020 on DESKTOP-3UPM55L

BloodHound-28092020

Hardware
- Add Hardware
- Firmware: Boot from DVD Drive
- Security: Secure Boot enabled
- Memory: 4098 MB
- Processor: 1 Virtual processor
- SCSI Controller
  - Hard Drive: BloodHound-28092020.vhdx
  - DVD Drive: en_windows_10_business_edit...
- Network Adapter: Not connected

Management
- Name: BloodHound-28092020
- Integration Services: Some services offered
- Checkpoints: Disabled
- Smart Paging File Location: C:\VM\BloodHound-28092020
- Automatic Start Action: None
- Automatic Stop Action: Shut Down

Automatic Stop Action

What do you want this virtual machine to do when the physical computer shuts down?

○ Save the virtual machine state

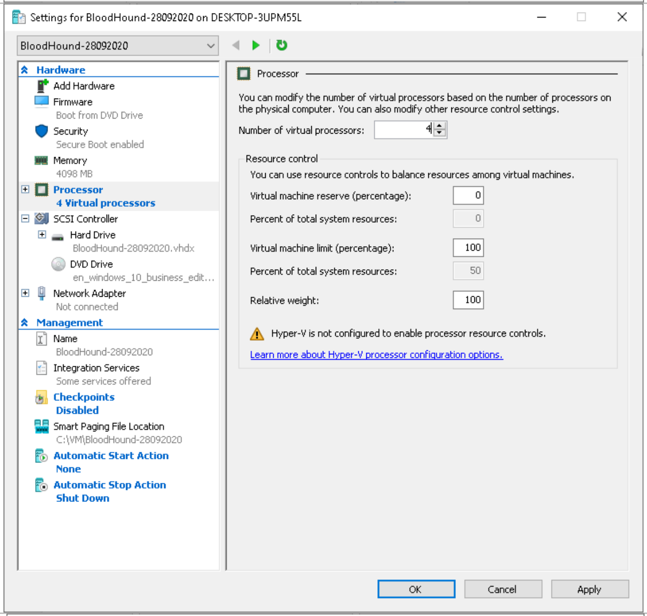
Hyper-V will reserve disk space equal to the amount of memory used by the virtual machine when it is running so that memory can be written to disk when the physical computer shuts down.

○ Turn off the virtual machine

● Shut down the guest operating system

The integration service that controls shutting down the guest operating system must be installed and enabled on the virtual machine.

Processor:
Switch to 4 virtual CPU’s (depends on the machine)



Settings for BloodHound-28092020 on DESKTOP-3UPM55L

BloodHound-28092020

Hardware
- Add Hardware
- Firmware: Boot from DVD Drive
- Security: Secure Boot enabled
- Memory: 4098 MB
- Processor: 4 Virtual processors
- SCSI Controller
  - Hard Drive: BloodHound-28092020.vhdx
  - DVD Drive: en_windows_10_business_edit...
- Network Adapter: Not connected

Management
- Name: BloodHound-28092020
- Integration Services: Some services offered
- Checkpoints: Disabled
- Smart Paging File Location: C:\VM\BloodHound-28092020
- Automatic Start Action: None
- Automatic Stop Action: Shut Down

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 4

Resource control

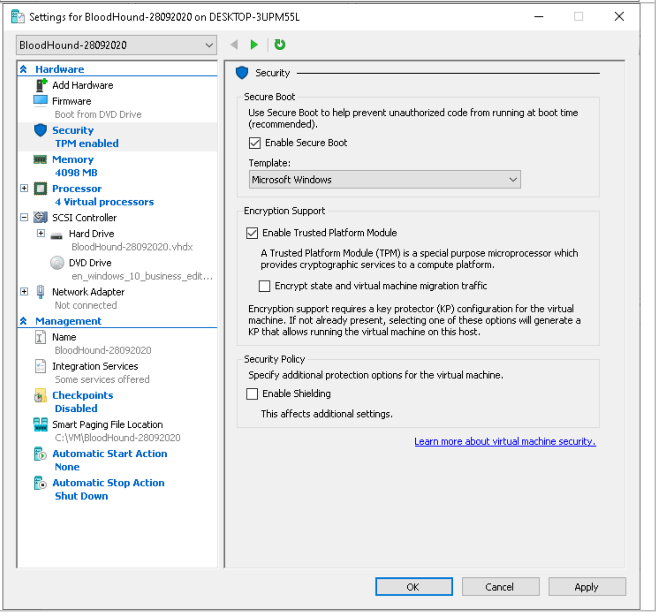
You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage):	0
Percent of total system resources:	0
Virtual machine limit (percentage):	100
Percent of total system resources:	50
Relative weight:	100

⚠ Hyper-V is not configured to enable processor resource controls.

Learn more about Hyper-V processor configuration options.

Security: Enable Secure Boot and Enable TPM



Settings for BloodHound-28092020 on DESKTOP-3UPM55L

BloodHound-28092020

Hardware
- Add Hardware
- Firmware: Boot from DVD Drive
- Security: TPM enabled
- Memory: 4098 MB
- Processor: 4 Virtual processors
- SCSI Controller
  - Hard Drive: BloodHound-28092020.vhdx
  - DVD Drive: en_windows_10_business_edit...
- Network Adapter: Not connected

Management
- Name: BloodHound-28092020
- Integration Services: Some services offered
- Checkpoints: Disabled
- Smart Paging File Location: C:\VM\BloodHound-28092020
- Automatic Start Action: None
- Automatic Stop Action: Shut Down

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template: Microsoft Windows

Encryption Support

☑ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

☐ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

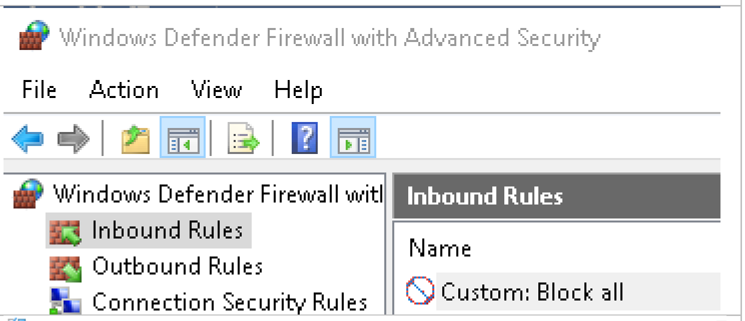
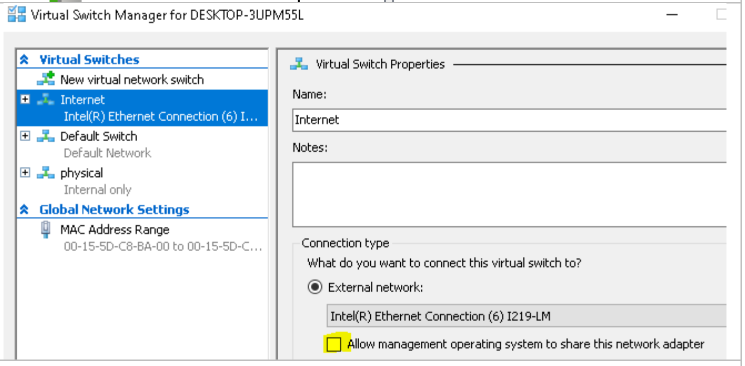
Specify additional protection options for the virtual machine.

☐ Enable Shielding

This affects additional settings.

Learn more about virtual machine security.

Install OS

Detach any Network Cable (No Internet Connection required at this stage)	
Install Windows OS (Most recent version)	
Create an inbound rule a block all the traffic	 Windows Defender Firewall with Advanced Security File Action View Help Windows Defender Firewall witl Inbound Rules Outbound Rules Connection Security Rules Inbound Rules Name Custom: Block all
If a VM is used, assign a dedicated VM Switch and don't share it with the host.	 Virtual Switch Manager for DESKTOP-3UPM55L Virtual Switches New virtual network switch Internet Intel(R) Ethernet Connection (6) I... Default Switch Default Network physical Internal only Global Network Settings MAC Address Range 00-15-5D-C8-BA-00 to 00-15-5D-C... Virtual Switch Properties Name: Internet Notes: Connection type What do you want to connect this virtual switch to? ● External network: Intel(R) Ethernet Connection (6) I219-LM ☐ Allow management operating system to share this network adapter
Install Security Updates	Disconnect after update is complete. Exposure to the Network must be as minimal as possible.

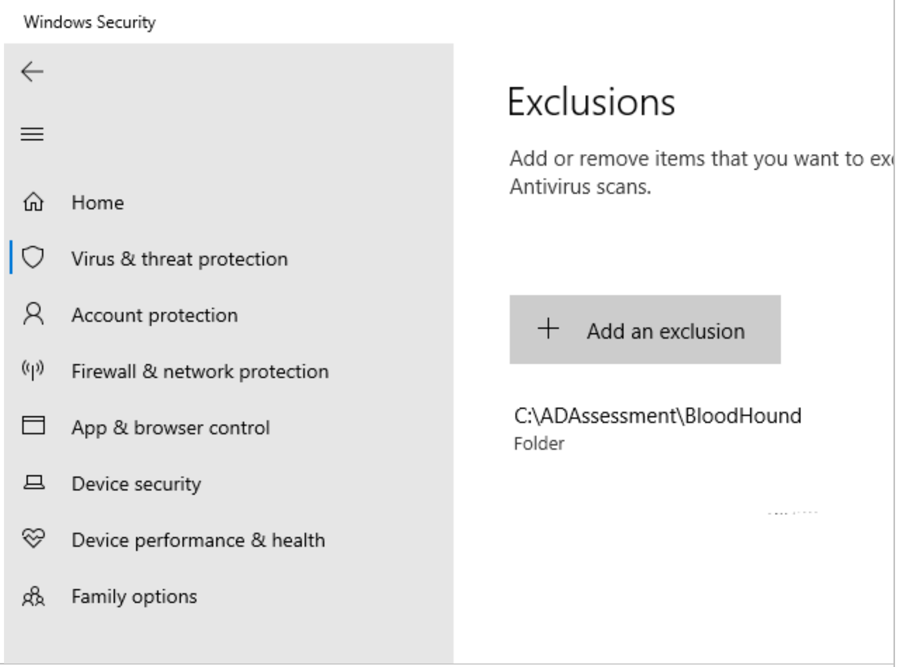
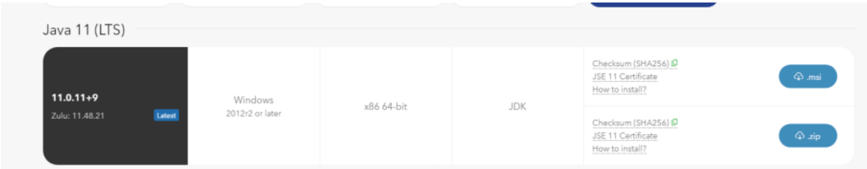
BloodHound (AD + Azure Assessment)

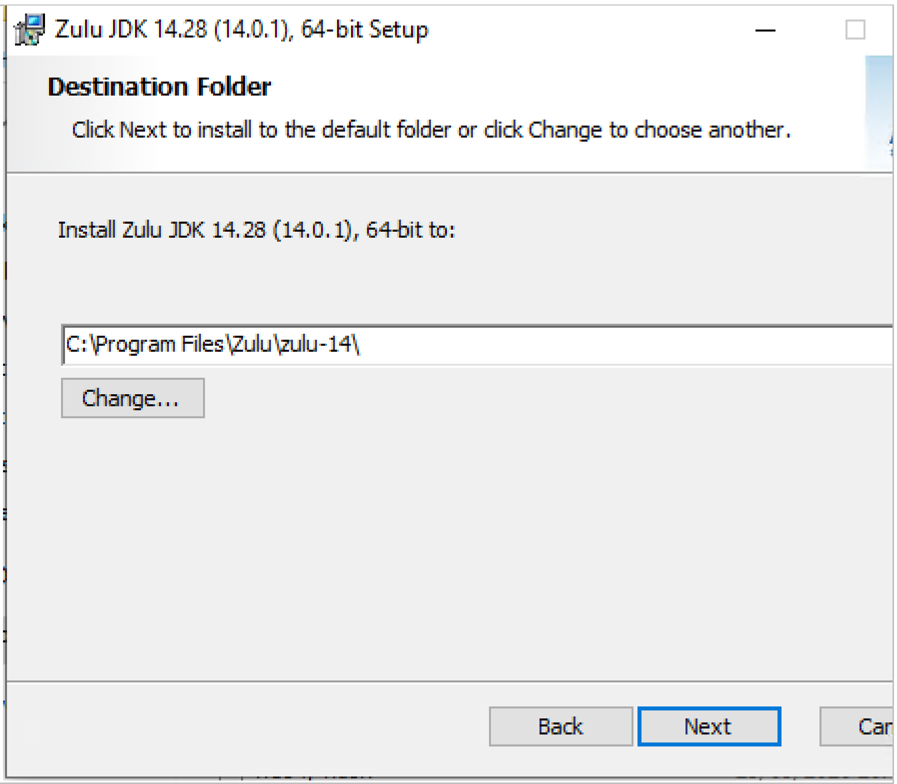
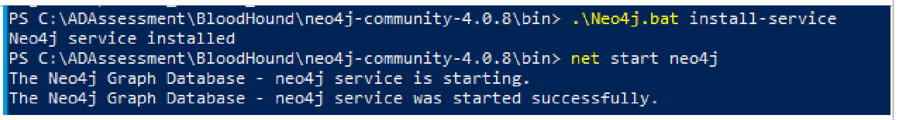
Prepare Assessment Client (Windows)

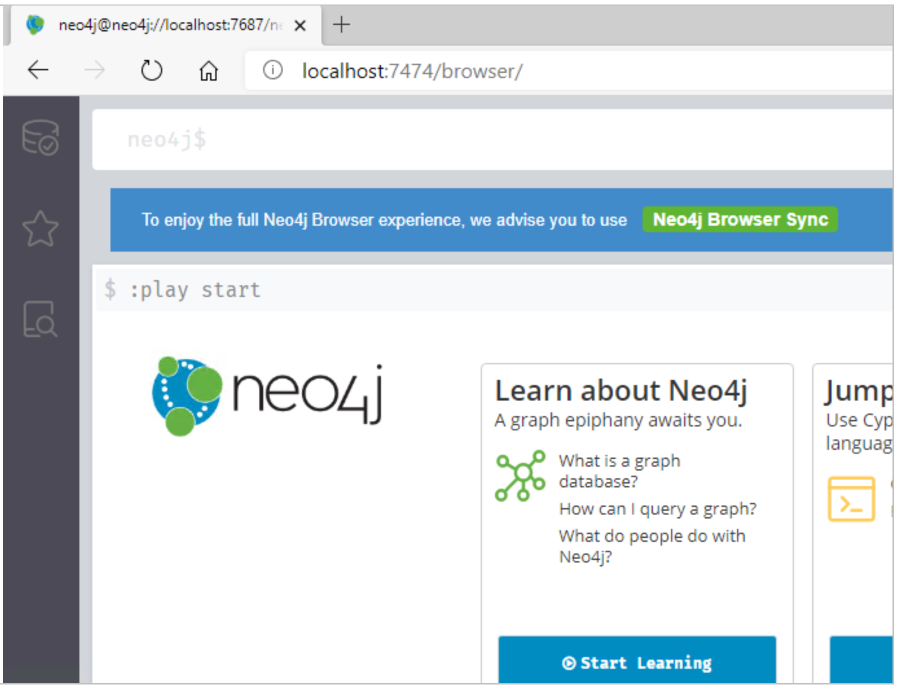
Either use a dedicated machine for the assessment or create a VM on an assessment machine.

See First Chapter for VM preparation: **Error! Reference source not found.**

Create a C:\ADAssessment directory	
Create a C:\ADAssessment\BloodHound directory	

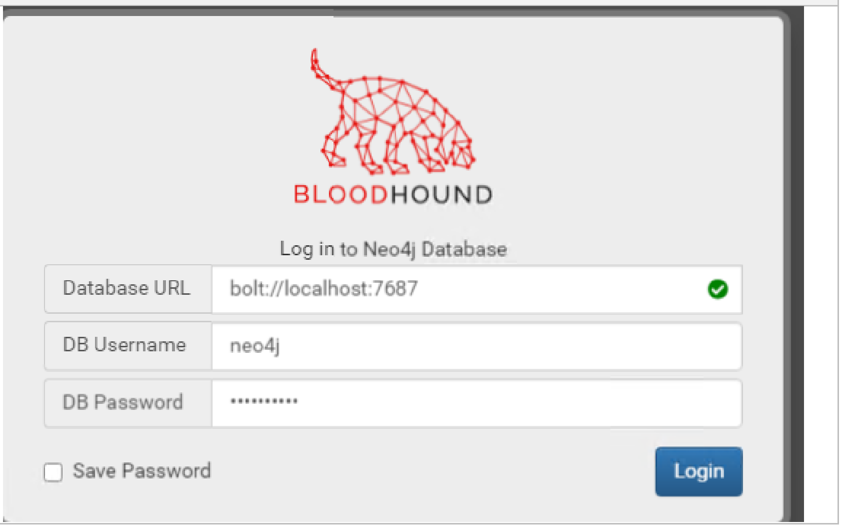
Create a Defender exclusion for the Folder. Virus & Threat protection settings > Exclusions: C:\ADAssessment\BloodHound	 Windows Security Home Virus & threat protection Account protection Firewall & network protection App & browser control Device security Device performance & health Family options + Add an exclusion Exclusions Add or remove items that you want to ex Antivirus scans. C:\ADAssessment\BloodHound Folder
Create folder: C:\ADAssessment\source You can place all the following source files into that folder	
Download Neo4j Community Edition database engine	https://neo4j.com/download-center/#community
Download the latest version of the BloodHound GUI + Source Code	Releases · BloodHoundAD/BloodHound (github.com)
Download CustomFilter	Bloodhound-Custom-Queries/customqueries.json at master · hausec/Bloodhound-Custom-Queries (github.com)
Download Zulu JDK 11	Java Download | Java 8, Java 11, Java 13 - Linux, Windows & macOS (azul.com)  Java 11 (LTS) 11.0.11+9 Zulu: 11.48.21 Latest Windows 2012r2 or later x86 64-bit JDK Checksum (SHA256) JSE 11 Certificate How to install? .msi Checksum (SHA256) JSE 11 Certificate How to install? .zip

Install Zulu JDK	 Zulu JDK 14.28 (14.0.1), 64-bit Setup **Destination Folder** Click Next to install to the default folder or click Change to choose another. Install Zulu JDK 14.28 (14.0.1), 64-bit to: C:\Program Files\Zulu\zulu-14\\
Extract Bloodhound binaries to C:\ADAssessment\BloodHound	
Extract neo4j into the C:\ADAssessment\BloodHound directory	
Open cmd	
Change folder to: C:\ADAssessment\BloodHound directory\neo4j…	
Run: Neo4j.bat install-service net start neo4j	 PS C:\ADAssessment\BloodHound\neo4j-community-4.0.8\bin> .\Neo4j.bat install-service Neo4j service installed PS C:\ADAssessment\BloodHound\neo4j-community-4.0.8\bin> net start neo4j The Neo4j Graph Database - neo4j service is starting. The Neo4j Graph Database - neo4j service was started successfully.
Open the administrative web interface in the browser by going to http://localhost:7474 ➔ Username: neo4j ➔ Password: neo4j	

Change Password to “Bloodhound”	

neo4j@neo4j://localhost:7687/n
localhost:7474/browser/
neo4j$
To enjoy the full Neo4j Browser experience, we advise you to use
Neo4j Browser Sync
$:play start
neo4j
Learn about Neo4j
A graph epiphany awaits you.
What is a graph database?
How can I query a graph?
What do people do with Neo4j?
Start Learning
Jump
Use Cyp
languag

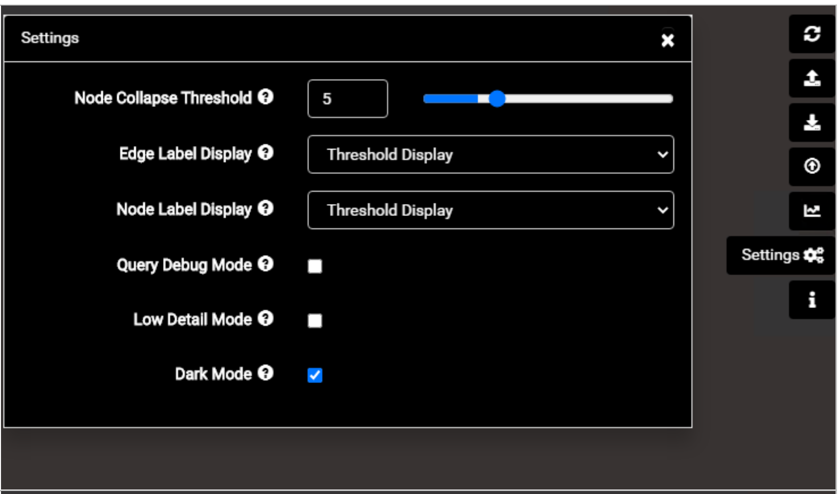
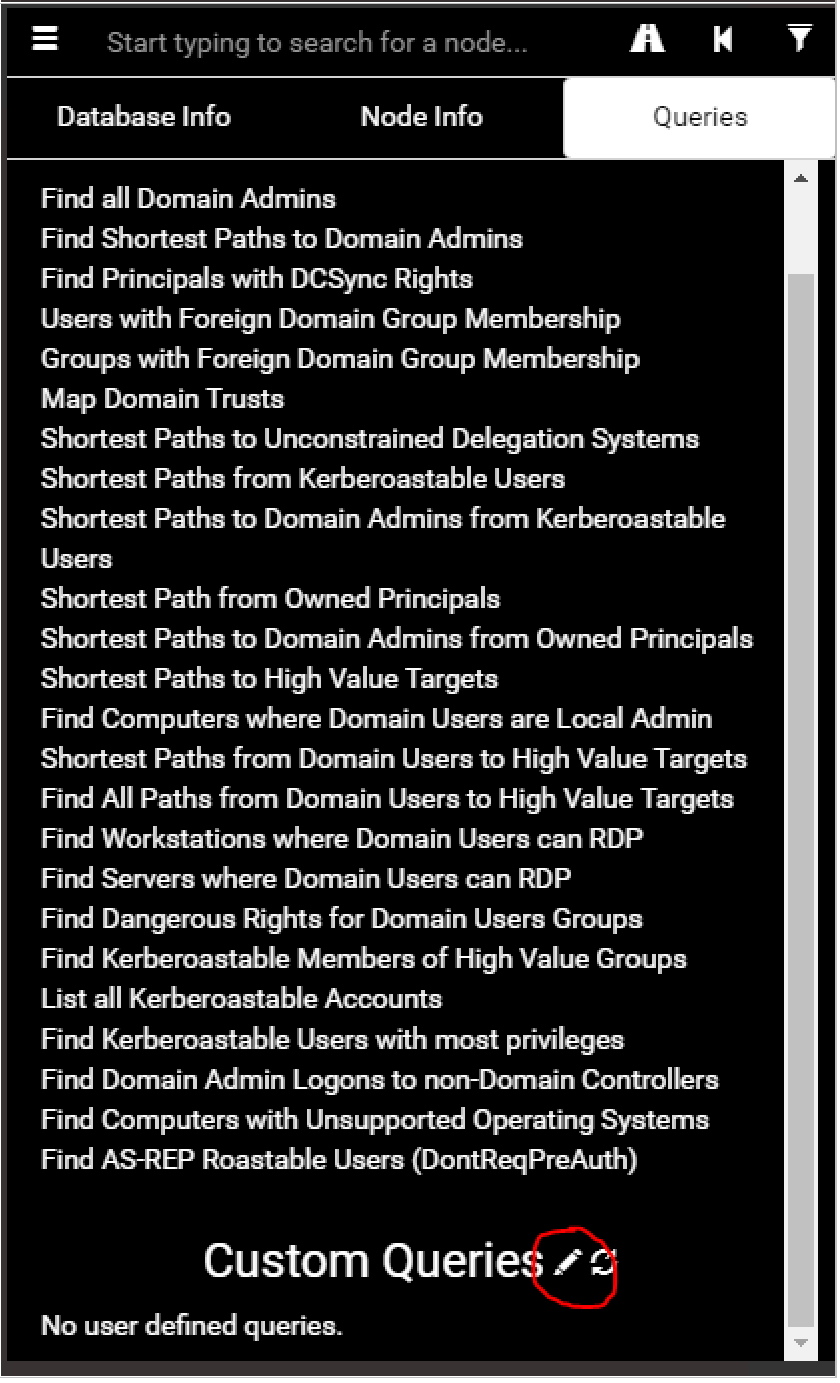
BloodHound – Configuration (Windows)

Start Bloodhound from C:\ADAssessment\BloodHound User: neo4j Pass: Bloodhound	

Database URL: bolt://localhost:7687

DB Username: neo4j

DB Password: ••••••••••

Switch to Dark Mode	 Settings Node Collapse Threshold: 5 Edge Label Display: Threshold Display Node Label Display: Threshold Display Query Debug Mode □ Low Detail Mode □ Dark Mode ☑
Load CustomFilters	 Start typing to search for a node... Find all Domain Admins Find Shortest Paths to Domain Admins Find Principals with DCSync Rights Users with Foreign Domain Group Membership Groups with Foreign Domain Group Membership Map Domain Trusts Shortest Paths to Unconstrained Delegation Systems Shortest Paths from Kerberoastable Users Shortest Paths to Domain Admins from Kerberoastable Users Shortest Path from Owned Principals Shortest Paths to Domain Admins from Owned Principals Shortest Paths to High Value Targets Find Computers where Domain Users are Local Admin Shortest Paths from Domain Users to High Value Targets Find All Paths from Domain Users to High Value Targets Find Workstations where Domain Users can RDP Find Servers where Domain Users can RDP Find Dangerous Rights for Domain Users Groups Find Kerberoastable Members of High Value Groups List all Kerberoastable Accounts Find Kerberoastable Users with most privileges Find Domain Admin Logons to non-Domain Controllers Find Computers with Unsupported Operating Systems Find AS-REP Roastable Users (DontReqPreAuth) Custom Queries No user defined queries.

	Copy content of downloaded customqueries file to opened editor Or copy file to: C:\Users\<user>\AppData\Roaming\bloodhound

AD: SharpHound – Run (Windows)

AD Pre-requisites

Create a temporary assessment user in AD	
User Right: Domain User	
SAM-R: If possible assign temporary rights to the user to read SAM-R from all available Clients in the network.	

Run SharpHound to collect data

Open CMD	
`cd C:\ADAssessment\Bloodhound\resources\app\Collectors`	

`SharpHound.exe --domain <domain name>`
If the assessment client is not domain joined:
`runas /user:<domain>\adassessment /netonly cmd`	

Run SharpHound to collect Session data

Open CMD	
cd \Ingestors	
SharpHound.exe --domain <domain name> --CollectionMethod Session --Loop --Loopduration 03:00:00	3h Loop to collect only session data
Before loading the data decompress the main zip file (e.g. 20201014101654_BloodHoundLoopResults.zip) to get the result zip files. Import of the main zip file will not work.	

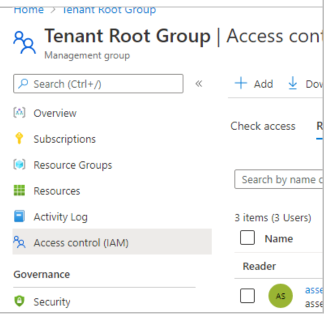
Azure: AzureHound

Pre-qreuisites

https://bloodhound.readthedocs.io/en/latest/index.html#collect-your-first-dataset

Open Powershell as Administrator	

Run:
`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
`Set-ExecutionPolicy bypass`	

Install Azure CLI `Install-Module -Name Az -Scope CurrentUser -Repository PSGallery -Force`	
Install AzureAD Powershell Module `Install-Module AzureAD -Scope CurrentUser -Repository PSGallery -Force`	
Import AzureHound Modules `Import-Module C:\ADAssessment\Bloodhound\resources\app\Collectors\AzureHound.ps1`	
Create a temporary assessment user in Azure AD	
Assign the Azure AD Role via PIM or permanent: Global Reader	
Assign the Reader Azure Role via PIM to the Tenant Root group	 Home > Tenant Root Group Tenant Root Group | Access con Management group Search (Ctrl+/) « + Add Dov Overview Subscriptions Resource Groups Resources Activity Log Access control (IAM) Governance Security Check access R Search by name c 3 items (3 Users) Name Reader AS asse asse

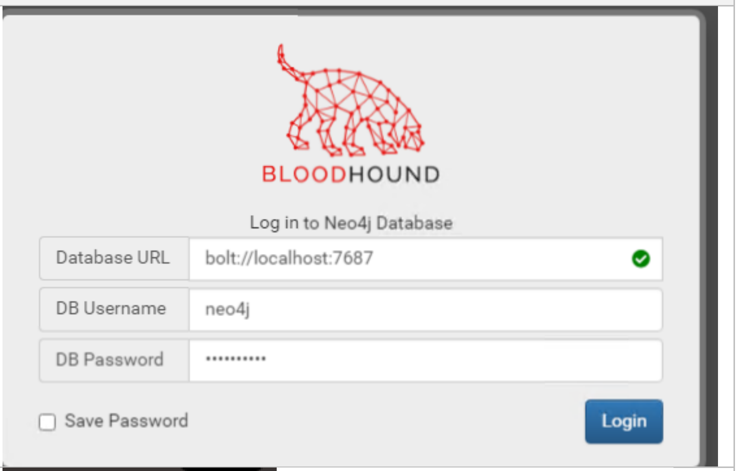
AzureHound – Run (Windows)

Open Powershell as Administrator	
login to Azure PowerShell `Connect-AzAccount`	
Login zu Azure AD `Connect-AzureAD`	

OPTIONAL:
It is also possible to steal the access tokens from a compromised machine if that machine has been used to login to Azure PowerShell before. Copy the existing files:
`C:\users\[Username]\.azure\AzureRmContextSettings.json`
`C:\users\[Username]\.azure\TokenCache.dat`	

And place them in your own .azure folder. Re-launch PowerShell and the token will now be used.	
Run `Invoke-AzureHound -TenantId <TenantID> -OutputDirectory C:\ADAssessment\Bloodhound\resources\app\Collectors`	

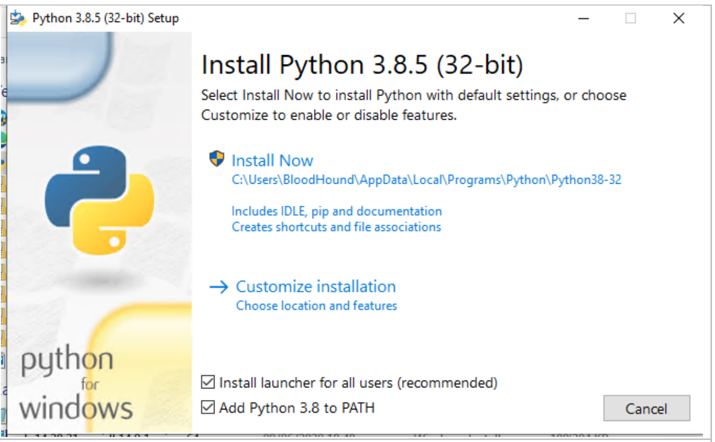
BloodHound – Load Data (Windows)

Start Bloodhound from C:\ADAssessment\BloodHound User: neo4j Pass: Bloodhound	 Log in to Neo4j Database Database URL: bolt://localhost:7687 DB Username: neo4j DB Password: •••••••••• □ Save Password
Once Bloodhound has logged in, you will have a huge blank window. We need to load data into this. Click Upload Data Select the zip file collected by Sharphound or AzureHound. <datatime>_azurecollection.zip <datatime>_BloodHound.zip	
Wait till the data is imported	
Mark all T0 services as High Value Target: Right click -> High Value	AADConnect, ADFS, etc.

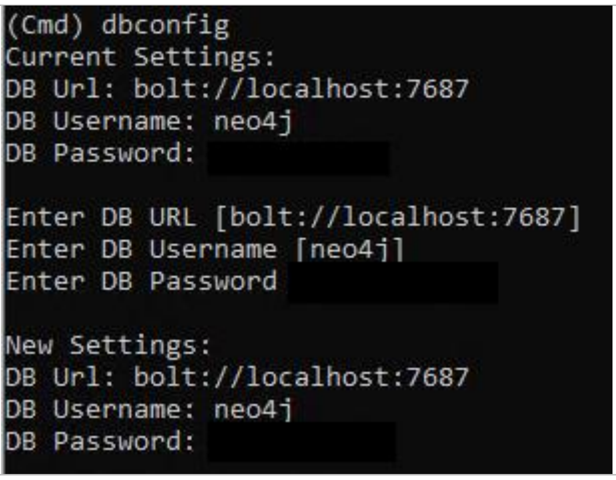
BloodHound – Create a Report (Windows)

Pre-requisites

Download Python (https://www.python.org/downloads)	

Install Python	 Python 3.8.5 (32-bit) Setup Install Python 3.8.5 (32-bit) Select Install Now to install Python with default settings, or choose Customize to enable or disable features. Install Now C:\Users\BloodHound\AppData\Local\Programs\Python\Python38-32 Includes IDLE, pip and documentation Creates shortcuts and file associations Customize installation Choose location and features ☑ Install launcher for all users (recommended) ☑ Add Python 3.8 to PATH Cancel
Open CMD and install the following modules: pip install neo4j pip install openpyxl	
Download BloodHound Analytics Python file from: [Bloodhound/bloodhoundanalytics.py at main · m8r1us/Bloodhound · GitHub]() Save to: C:\ADAssessment\Report	Script made for neo4j >=V4.0

Create Report

Run: python bloodhoundanalytics.py <domain>	
Type: dbconfig Check the connection settings	 (Cmd) dbconfig Current Settings: DB Url: bolt://localhost:7687 DB Username: neo4j DB Password: [redacted] Enter DB URL [bolt://localhost:7687] Enter DB Username [neo4j] Enter DB Password [redacted] New Settings: DB Url: bolt://localhost:7687 DB Username: neo4j DB Password: [redacted]
Type: Connect	

Type: startanalysis	
Excel is required to open the file	

Bloodhound – Review Graph

Open: C:\ADAssessment\Bloodhound\BloodHound.exe	

Cypher Queries (Azure)

Return All Azure Users that are part of the 'Global Administrator' Role	MATCH p =(n)-[r:AZGlobalAdmin*1..]->(m) RETURN p
Return All On-Prem users with edges to Azure	MATCH p=(m:User)-[r:AZResetPassword|AZOwns|AZUserAccessAdministrator|AZContributor|AZAddMembers|AZGlobalAdmin|AZVMContributor|AZOwnsAZAvereContributor]->(n) WHERE m.objectid CONTAINS 'S-1-5-21' RETURN p
Find all paths to an Azure VM	MATCH p = (n)-[r]->(g:AZVM) RETURN p
Find all paths to an Azure KeyVault	MATCH p = (n)-[r]->(g:AZKeyVault) RETURN p
Return All Azure Users and their Groups	MATCH p=(m:AZUser)-[r:MemberOf]->(n) WHERE NOT m.objectid CONTAINS 'S-1-5' RETURN p
Return All Azure AD Groups that are synchronized with On-Premise AD	MATCH (n:Group) WHERE n.objectid CONTAINS 'S-1-5' AND n.azsyncid IS NOT NULL RETURN n
Find all Privileged Service Principals	MATCH p = (g:AZServicePrincipal)-[r]->(n) RETURN p
Find all Owners of Azure Applications	MATCH p = (n)-[r:AZOwns]->(g:AZApp) RETURN p
Return All Azure Users (Console)	MATCH (n:AZUser) return n.azname
Return All Azure Applications	MATCH (n:AZApp) return n.objectid
Return All Azure Devices	MATCH (n:AZDevice) return n.name
Return All Azure Groups	MATCH (n:AZGroup) return n.name
Return all Azure Key Vaults	MATCH (n:AZKeyVault) return n.name
Return all Azure Resource Groups	MATCH (n:AZResourceGroup) return n.name

Return all Azure Service Principals	MATCH (n:AZServicePrincipal) return n.objectid
Return all Azure Virtual Machines	MATCH (n:AZVM) return n.name
Find All Principals with the ‘Contributor’ role	MATCH p = (n)-[r:AZContributor]->(g) RETURN p

ROADTools (Azure Assessment)

dirkjanm/ROADtools: The Azure AD exploration framework. (github.com)

AzureAD / Azure Pre-requisites

Create a **temporary assessment user in Azure AD**	
Assign the Azure AD Role via PIM: Global Reader	
Assign the Reader Azure Role via PIM for Azure.	

Prepare Assessment Client (Windows)

Either use a dedicated machine for the assessment or create a VM on an assessment machine.

Create a folder: C:\AzureAssessment	
Create a folder: C:\AzureAssessment\roadtools	
Create a folder: C:\AzureAssessment\sources You can place all the following source files into that folder	
Download Python (https://www.python.org/downloads)	
Install Python	
Install Microsoft C++ Build Tools https://visualstudio.microsoft.com/thank-you-downloading-visual-studio/?sku=BuildTools&rel=16	
Download Roadtools from: Pipelines - Run 20210527.1 artifacts (azure.com) Or: dirkjanm/ROADtools: The Azure AD exploration framework. (github.com)	
Extract ROADtools.zip to: C:\AzureAssessment\roadtools\roadlib C:\AzureAssessment\roadtools\roadrecon	
Open cmd	
Run:	

Cd C:\AzureAssessment\roadtools pip install pipenv pipenv install roadlib/ pipenv install roadrecon/	

Run RoadRecon (Windows)

Open cmd Run: Cd C:\AzureAssessment\roadtools pipenv shell	
Use the created Azure AD Account Run: Roadrecon auth --device-code	
Run: Roadrecon gather	
Create Conditional Access Rule dump Run: Roadrecon plugin policies	

View Data with RoadRecon UI

Open cmd		
Cd C:\AzureAssessment\roadtools pipenv shell		
Roadrecon-gui		
Open Browser		

Export Data to BloodHound

Use the new Bloodhound Version with integrated Azure AD support.

~~Download the following repository~~ ~~https://github.com/dirkjanm/Bloodhound-AzureAD~~	
~~Extract to AzureAssessment\~~	
~~Download and install neo4j Community Edition (Follow installation guide from Bloodhound)~~	
~~Open Cmd~~ ~~Cd C:\AzureAssessment\roadtools~~ ~~Pipenv shell~~	

~~Roadrecon plugin bloodhound~~	
~~Download NodeJS/NPM (https://www.npmjs.com/get-npm)~~	
~~Open Cmd~~ ~~cd AzureAssessment\BloodHound-AzureAD-master~~ ~~NPM inall~~ ~~NPM run dev~~ ~~The application could be also compiled to an exe.~~	
~~Open the URL.~~ ~~Control +R if blank screen for refresh~~	
~~Import SharpHound Data~~	

Stormspotter (Azure Assessment)

https://github.com/Azure/Stormspotter

AzureAD / Azure Pre-requisites

Create a **temporary assessment user in Azure AD**	
Assign the Azure AD Role via PIM: Global Reader	
Assign the Reader Azure Role via PIM for Azure.	

Prepare Assessment Client (Windows - Docker)

Either use a dedicated machine for the assessment or create a VM on an assessment machine. Docker will maybe not run on a VM.

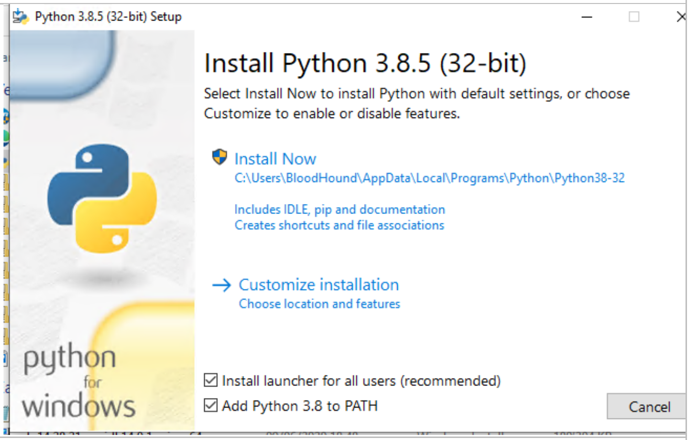
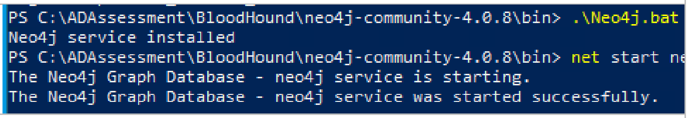
https://github.com/Azure/Stormspotter#with-docker

Download and Install Docker (Follow the instruction to Install WSL2) Docker Desktop for Mac and Windows | Docker	
git clone https://github.com/Azure/Stormspotter	
Adjust ports etc. in the docker-compose.yaml if required. (Conflict with installed neo4j version)	
docker-compose up	

Prepare Assessment Client (Windows – Without Docker)

Either use a dedicated machine for the assessment or create a VM on an assessment machine.

Create a folder: C:\AzureAssessment	
Create a folder: C:\AzureAssessment\stormspotter	

Create folder: C:\AzureAssessment\source You can place all the following source files into that folder	
Download Python (https://www.python.org/downloads)	
Install Python 3.8.0 (https://www.python.org/ftp/python/3.8.0/python-3.8.0-amd64.exe)	 Python 3.8.5 (32-bit) Setup Install Python 3.8.5 (32-bit) Select Install Now to install Python with default settings, or choose Customize to enable or disable features. Install Now C:\Users\BloodHound\AppData\Local\Programs\Python\Python38-32 Includes IDLE, pip and documentation Creates shortcuts and file associations → Customize installation Choose location and features ☑ Install launcher for all users (recommended) ☑ Add Python 3.8 to PATH
Download NodeJS/NPM (node-v14.17.0-x64) (https://www.npmjs.com/get-npm)	
Install NPM (NodeJS)	
Download Zulu JDK (https://www.azul.com/downloads/zulu-community/?architecture=x86-64-bit&package=jdk)	
Install Zulu JDK	
Download Neo4j (https://neo4j.com/download-center/#community)	
Extract neo4j into the C:\AzureAssessment\Stormspotter directory	
Open cmd	
Change folder to: C:\AzureAssessment\Stormspotter\neo4j-community-4.2.6\bin	
Run: Neo4j.bat install-service net start neo4j	 PS C:\ADAssessment\BloodHound\neo4j-community-4.0.8\bin> .\Neo4j.bat Neo4j service installed PS C:\ADAssessment\BloodHound\neo4j-community-4.0.8\bin> net start ne The Neo4j Graph Database - neo4j service is starting. The Neo4j Graph Database - neo4j service was started successfully.
Open the administrative web interface in the browser by going to http://localhost:7474 Username: neo4j Password: neo4j	
Change Password to “stormspotter”	

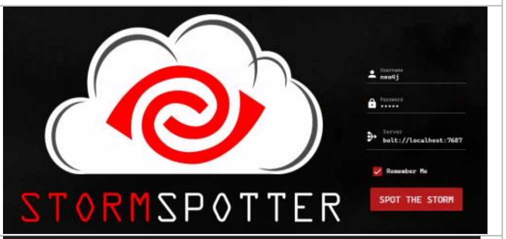
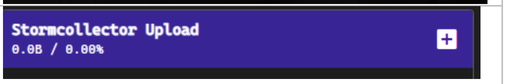
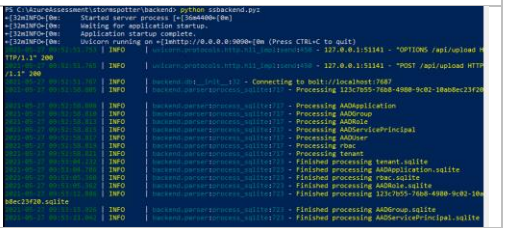
Download Stormspotter (Releases · Azure/Stormspotter (github.com))	
Extract C:\AzureAssessment\stormspotter	
Install az cli powershell (https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli)	
Install Fronted reuirements Run: cd C:\AzureAssessment\stormspotter\frontend\dist\spa npm install -g @quasar/cli	

Run Stormcollector

Open separate CMD and RUN:
 	
`cd C:\AzureAssessment\Stormspotter\stormcollector`
 	
Run to show the help menu:
`python sscollector.pyz -h`
 	
Common options for all authentication types
 	
`python sscollector.pyz cli`
`python sscollector.pyz spn -t <tenant> -c <clientID> -s <clientSecret>`
 	
`--cloud: Specify a different Azure Cloud (GERMAN, CHINA, USGOV)`
`--config: Specify a custom configuration for cloud environments`
`--azure: Only enumerate Azure Resource Manager resources`
`--aad: Only enumerate Azure Active Directory`
`--subs: Subscriptions you wish to scan. Multiple subscriptions can be added as a space deliminated list.`
`--nosubs: Subscriptions you wish to exclude. Multiple subscriptions can be excluded as a space deliminated list.`
`--json: Convert SQLite output to JSON (WARNING: STORMSPOTTER ONLY PARSES SQLITE FORMAT )`
`This option is useful if you want to parse the output for reasons other than Stormspotter.`
`--ssl-cert: Specify an SSL cert for Stormcollector to use for requests. Not a common option`
`--backfill: Perform AAD enumeration only for object IDs associated with RBAC enumeration. Only applicable when --azure is specified.`	

Run to collect data by using the created azure assessment account:
 	
`Az login`
`python sscollector.pyz cli`	

Load Data (Windows)

Start Frontend -> Open CMD Run: cd C:\AzureAssessment\stormspotter\frontend\dist\spa quasar serve -p 9091 --history	
Start Backend -> open CMD (Required for uploading data) Run: cd C:\AzureAssessment\stormspotter\backend python ssbackend.pyz	
Open: http://localhost:9091	 STORMSPOTTER Username neo4j Password ***** Server bolt://localhost:7687 ☑ Remember Me SPOT THE STORM
Upload to Stormcollector Upload -> results_<date>.zip Files collected are in the folder: C:\AzureAssessment\stormspotter\stormcollector\*.zip	
Check upload status in the Backend CMD Window	

```
PS C:\AzureAssessment\stormspotter\backend> python ssbackend.pyz
←[32mINFO←[0m:     Started server process [←[36m4400←[0m]
←[32mINFO←[0m:     Waiting for application startup.
←[32mINFO←[0m:     Application startup complete.
←[32mINFO←[0m:     Uvicorn running on ←[1mhttp://0.0.0.0:9090←[0m (Press CTRL+C to quit)
2021-05-27 09:52:51.753 | INFO     | uvicorn.protocols.http.h11_impl:send:458 - 127.0.0.1:51141 - "OPTIONS /api/upload H
TTP/1.1" 200
2021-05-27 09:52:51.765 | INFO     | uvicorn.protocols.http.h11_impl:send:458 - 127.0.0.1:51141 - "POST /api/upload HTTP
/1.1" 200
2021-05-27 09:52:51.767 | INFO     | backend.db:__init__:32 - Connecting to bolt://localhost:7687
2021-05-27 09:52:58.805 | INFO     | backend.parser:process_sqlite:717 - Processing 123c7b55-76b8-4980-9c02-10ab8ec23f20

2021-05-27 09:52:58.808 | INFO     | backend.parser:process_sqlite:717 - Processing AADApplication
2021-05-27 09:52:58.810 | INFO     | backend.parser:process_sqlite:717 - Processing AADGroup
2021-05-27 09:52:58.813 | INFO     | backend.parser:process_sqlite:717 - Processing AADRole
2021-05-27 09:52:58.815 | INFO     | backend.parser:process_sqlite:717 - Processing AADServicePrincipal
2021-05-27 09:52:58.817 | INFO     | backend.parser:process_sqlite:717 - Processing AADUser
2021-05-27 09:52:58.819 | INFO     | backend.parser:process_sqlite:717 - Processing rbac
2021-05-27 09:52:58.821 | INFO     | backend.parser:process_sqlite:717 - Processing tenant
2021-05-27 09:53:04.232 | INFO     | backend.parser:process_sqlite:723 - Finished processing tenant.sqlite
2021-05-27 09:53:04.706 | INFO     | backend.parser:process_sqlite:723 - Finished processing AADApplication.sqlite
2021-05-27 09:53:05.360 | INFO     | backend.parser:process_sqlite:723 - Finished processing rbac.sqlite
2021-05-27 09:53:05.362 | INFO     | backend.parser:process_sqlite:723 - Finished processing AADRole.sqlite
2021-05-27 09:53:12.806 | INFO     | backend.parser:process_sqlite:723 - Finished processing 123c7b55-76b8-4980-9c02-10a
b8ec23f20.sqlite
2021-05-27 09:53:13.026 | INFO     | backend.parser:process_sqlite:723 - Finished processing AADGroup.sqlite
2021-05-27 09:53:21.062 | INFO     | backend.parser:process_sqlite:723 - Finished processing AADServicePrincipal.sqlite
```

Review Graph

Start Frontend -> Open CMD Run: cd C:\AzureAssessment\stormspotter\frontend\dist\spa quasar serve -p 9091 --history	
Open in Edge http://localhost:9091	

Cypher Queries

Show ServicePrincipal Relationships	MATCH (a)-[r]-(t) Where a.type ="AADServicePrincipal" RETURN *

Show all Global Administrators	MATCH (a:AADRole)<-[r:MemberOf]-(t) WHERE a.name = ‘Global Administrator' RETURN *
Show all AAD Roles	MATCH (a:AADRole) RETURN *
Show full Tenant Relationships aka Christmastree	MATCH (a)-[r]-(t) Return *

AzureADAssessment

[GitHub - AzureAD/AzureADAssessment: Tooling for assessing an Azure AD tenant state and configuration]()

Prepare Assessment Client

Create a folder: C:\AzureAssessment	
Create a folder: C:\AzureAssessment\AzureADAssessment	

Open Powershell and run:
 	
`Install-module msal.ps`
`Install-Module AzureADAssessment -Force`	

## If you have already installed the module, run the following instead to ensure you have the latest version. `Update-Module AzureADAssessment -Force`	
Install PowerBi [Download Microsoft Power BI Desktop from Official Microsoft Download Center]()	

Run AzureADAssessment

Use the created Azure AD Assessment Account
cd C:\AzureAssessment\AzureADAssessment
 	
`Connect-AADAssessment`
`Invoke-AADAssessmentDataCollection "C:\AzureAssessment\AzureADAssessment"`	

Create PowerBI Report `Complete-AADAssessmentReports AzureADAssessmentData-<TenantName>.onmicrosoft.com.zip -OutputDirectory "C:\AzureAssessment\AzureADAssessment"` Open PowerBi Template AzureADAssessment.pbit	
In the popup provide the path to the Results folder: `C:\AzureAssessment\AzureADAssessment\AzureADAssessmentData-<tenant>.onmicrosoft.com\AAD-<tenant>.onmicrosoft.com`	

Run AzureADAssessment on Hybrid Components

Export Portable Module `Export-AADAssessmentPortableModule "C:\AzureAssessment\AzureADAssessment"`	

Import the module on each server running hybrid components.
`Import-Module "C:\AzureADAssessment\AzureADAssessmentPortable.psm1"`
Export Data into a single output package.
`Invoke-AADAssessmentHybridDataCollection "C:\AzureAssessment\AzureADAssessment"`	