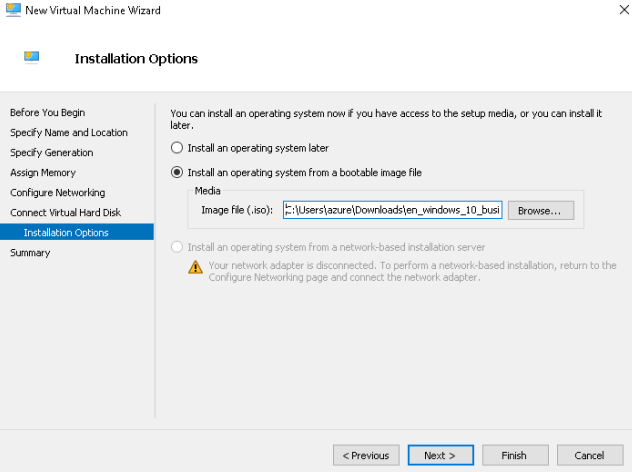
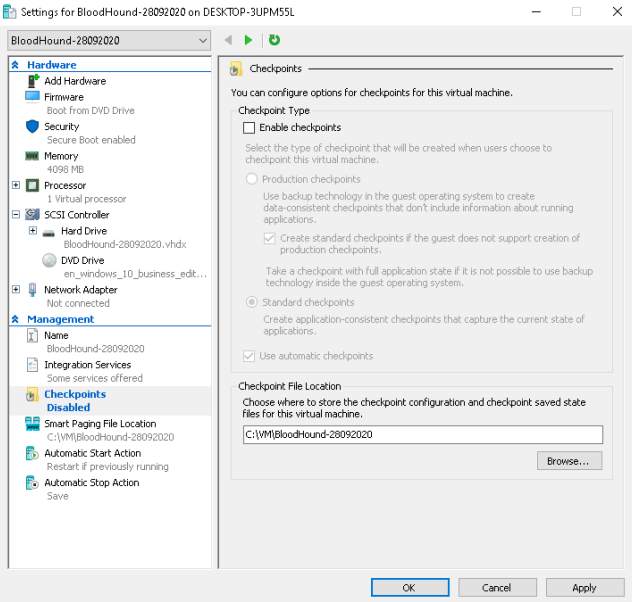
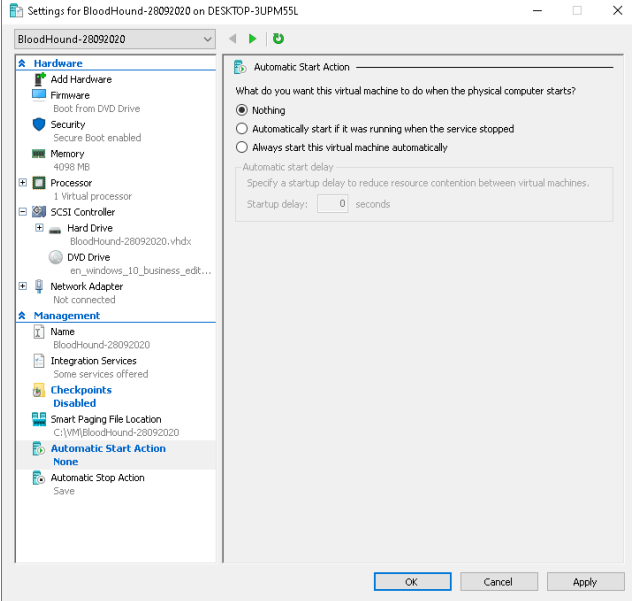


Assessment VM

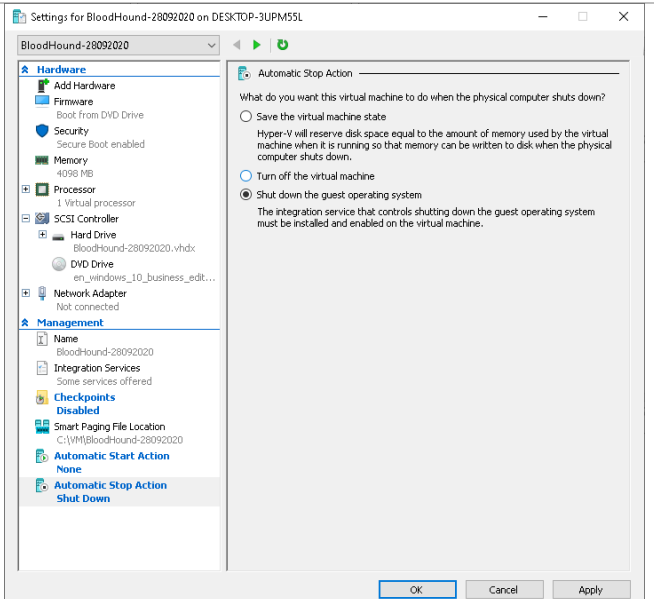
Create and Prepare a VM

	<div><div>New Virtual Machine Wizard</div><div><div>Before You Begin</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><p>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.</p><p>To create a virtual machine, do one of the following:</p><ul style="list-style-type: none">Click Finish to create a virtual machine that is configured with default values.Click Next to create a virtual machine with a custom configuration.<p><input type="checkbox"/> Do not show this page again</p></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>
	<div><div>New Virtual Machine Wizard</div><div><div>Specify Name and Location</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><p>Choose a name and location for this virtual machine.</p><p>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.</p><p>Name: <input type="text" value="Bloodhound-28092020"/></p><p>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.</p><p><input checked="" type="checkbox"/> Store the virtual machine in a different location</p><p>Location: <input type="text" value="C:\VM\"/> <input data-bbox="1305 1099 1369 1120" type="button" value="Browse..."/></p><p>⚠ 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.</p></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>
	<div><div>New Virtual Machine Wizard</div><div><div>Specify Generation</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><p>Choose the generation of this virtual machine.</p><p><input type="radio"/> Generation 1</p><p>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.</p><p><input checked="" type="radio"/> Generation 2</p><p>This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.</p><p>⚠ Once a virtual machine has been created, you cannot change its generation.</p><p>More about virtual machine generation support</p></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>

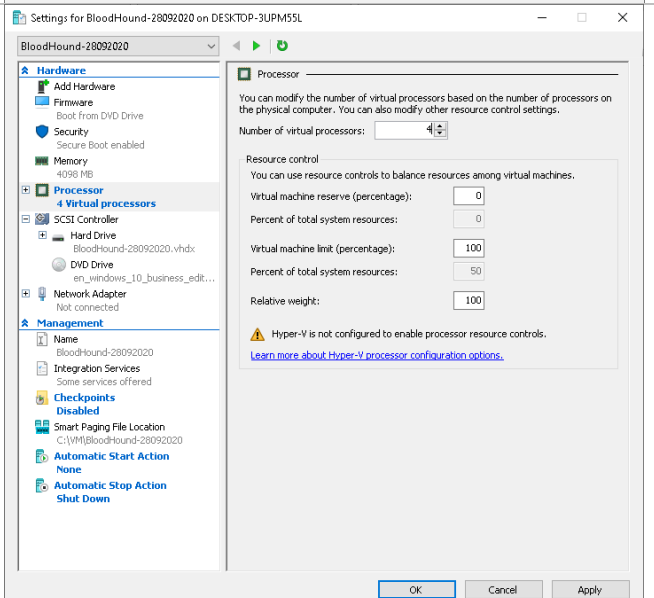
	<div><div>New Virtual Machine Wizard</div><div><div>Assign Memory</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><div>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.</div><div>Startup memory: 4096 MB</div><div><input type="checkbox"/> Use Dynamic Memory for this virtual machine.</div><div><div>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.</div></div></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>
Chose "Not Connected" for the moment	<div><div>New Virtual Machine Wizard</div><div><div>Configure Networking</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><div>Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.</div><div>Connection: Not Connected</div></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>
	<div><div>New Virtual Machine Wizard</div><div><div>Connect Virtual Hard Disk</div><div><div>Before You Begin</div><div>Specify Name and Location</div><div>Specify Generation</div><div>Assign Memory</div><div>Configure Networking</div><div>Connect Virtual Hard Disk</div><div>Installation Options</div><div>Summary</div></div><div><div>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.</div><div><input checked="" type="radio"/> Create a virtual hard disk</div><div>Use this option to create a VHDX dynamically expanding virtual hard disk.</div><div><div>Name: BloodHound-28092020.vhdx</div><div>Location: C:\VM\BloodHound-28092020\Virtual Hard Disks\ Browse...</div><div>Size: 40 GB (Maximum: 64 TB)</div></div><div><input type="radio"/> Use an existing virtual hard disk</div><div>Use this option to attach an existing VHDX virtual hard disk.</div><div><div>Location: C:\VM\ Browse...</div></div><div><input type="radio"/> Attach a virtual hard disk later</div><div>Use this option to skip this step now and attach an existing virtual hard disk later.</div></div><div><div>< Previous</div><div>Next ></div><div>Finish</div><div>Cancel</div></div></div></div>

	
<p>Checkpoints: Disable Checkpoints (Optional)</p>	
<p>Automatic Start Action: Turn off Automatically start</p>	

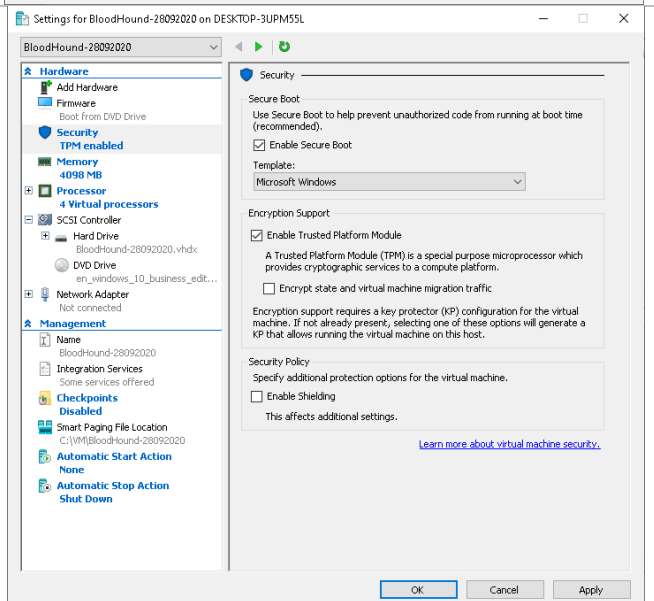
Automatic Stop Action: Shut down the guest operating system



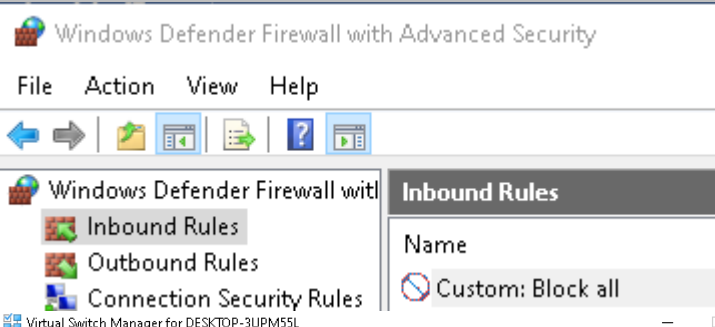
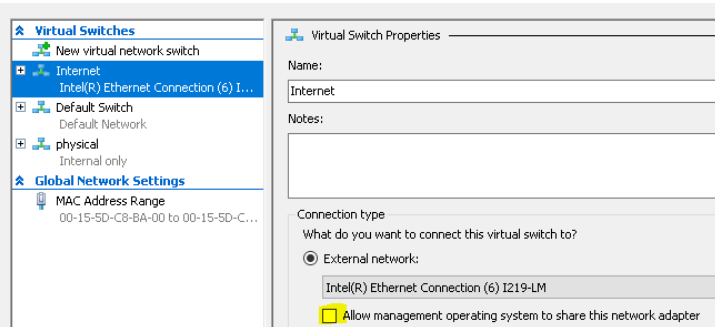
Processor:
Switch to 4 virtual CPU's (depends on the machine)



Security: Enable Secure Boot and Enable TPM



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	
If a VM is used, assign a dedicated VM Switch and don't share it with the host.	
Install Security Updates	Disconnect after update is complete. Exposure to the Network must be as minimal as possible.

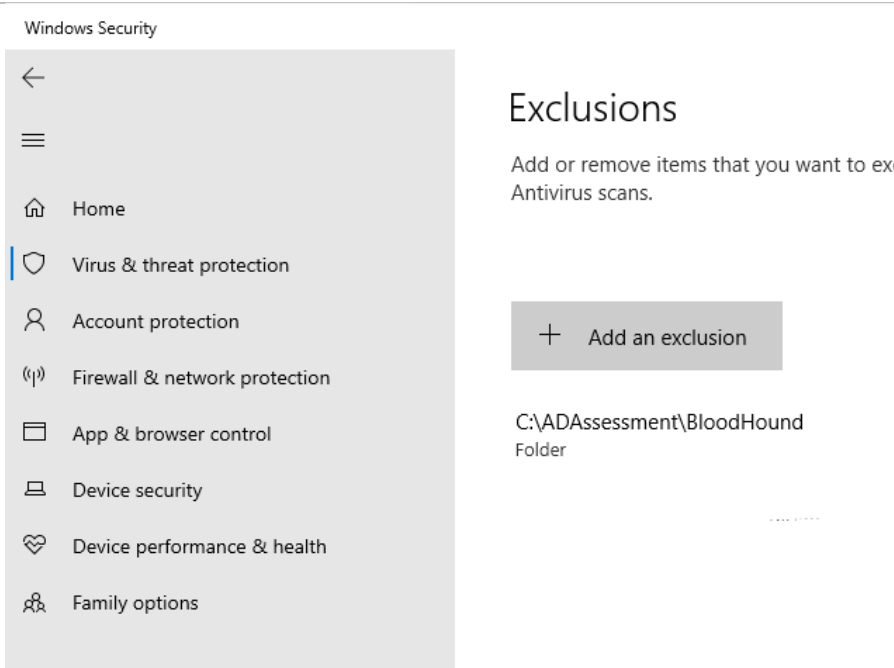
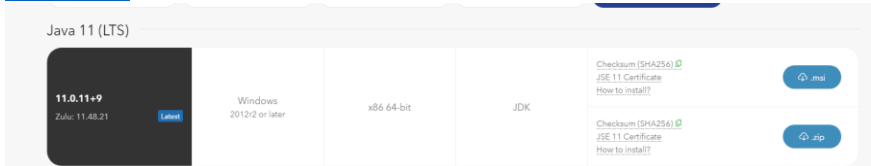
BloodHound (AD + Azure Assessment)

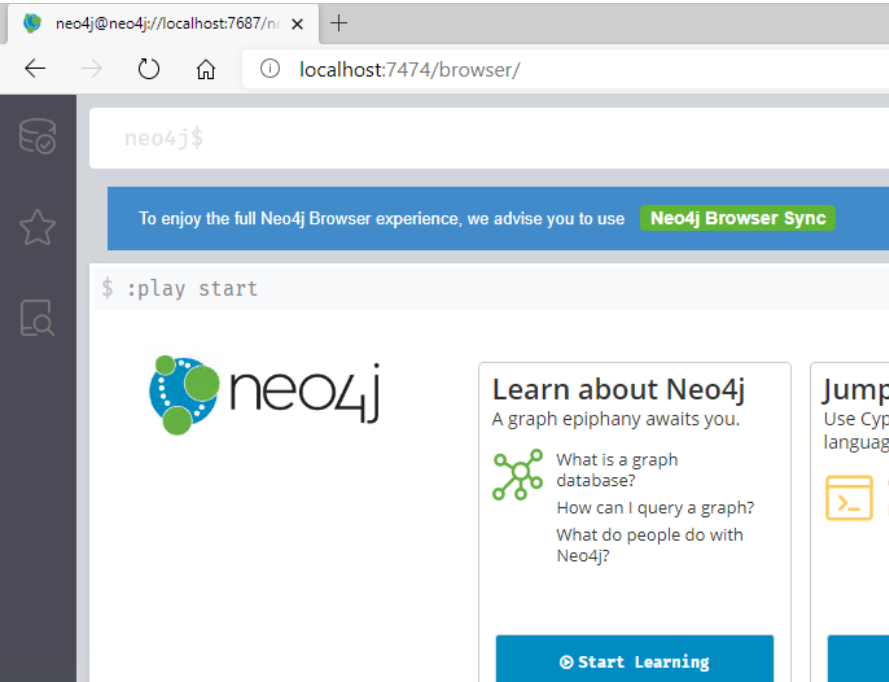
Prepare Assessment Client (Windows)

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	

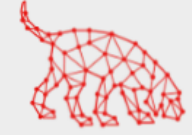
<p>Create a Defender exclusion for the Folder.</p> <p>Virus & Threat protection settings > Exclusions: C:\ADAssessment\BloodHound</p>	
<p>Create folder: C:\ADAssessment\source</p> <p>You can place all the following source files into that folder</p>	
<p>Download Neo4j Community Edition database engine</p>	https://neo4j.com/download-center/#community
<p>Download the latest version of the BloodHound GUI + Source Code</p>	Releases · BloodHoundAD/BloodHound (github.com)
<p>Download CustomFilter</p>	Bloodhound-Custom-Queries/customqueries.json at master · hausec/Bloodhound-Custom-Queries (github.com)
<p>Download Zulu JDK 11</p>	<p>Java Download Java 8, Java 11, Java 13 - Linux, Windows & macOS (azul.com)</p> 
<p>Install Zulu JDK</p>	
<p>Extract Bloodhound binaries to C:\ADAssessment\BloodHound</p>	
<p>Extract neo4j into the C:\ADAssessment\BloodHound directory</p>	
<p>Open cmd</p>	
<p>Change folder to:</p>	

C:\ADAssessment\BloodHound\neo4j...	
Run: Neo4j.bat install-service net start neo4j	<pre>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.</pre>
Open the administrative web interface in the browser by going to http://localhost:7474 ➔ Username: neo4j ➔ Password: neo4j	
Change Password to "Bloodhound"	

BloodHound – Configuration (Windows)

--	--

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



BLOODHOUND

Log in to Neo4j Database

Database URL	bolt://localhost:7687	✓
DB Username	neo4j	
DB Password	*****	

☐ Save Password Login

Switch to Dark Mode

Settings

Node Collapse Threshold	5	<input type="range"/>
Edge Label Display	Threshold Display	
Node Label Display	Threshold Display	
Query Debug Mode	<input type="checkbox"/>	
Low Detail Mode	<input type="checkbox"/>	
Dark Mode	<input checked="" type="checkbox"/>	

Settings

Load CustomFilters

Start typing to search for a node...

A

K

Database Info

Node Info

Queries

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

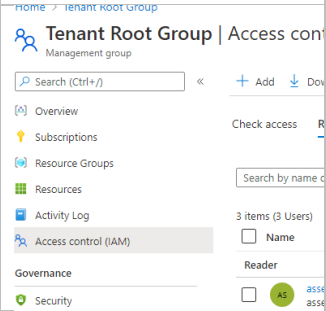
Open CMD	
cd \Ingestors	
SharpHound.exe --domain <domain name> --CollectionMethod Session --Loop --Loopduration 03:00:00	3h Loop to collect only session data
Before loading the data decompress the main zip file (e.g. 20201014101654_BloodHoundLoopResults.zip) to get the result zip files. Import of the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

Azure: AzureHound

Pre-reqs

<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	

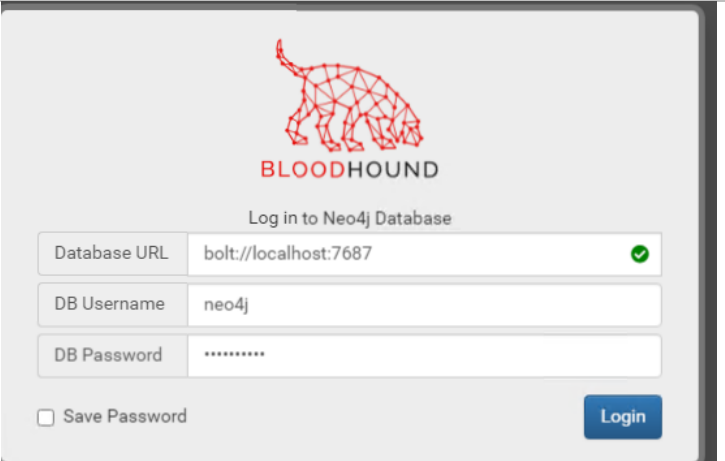
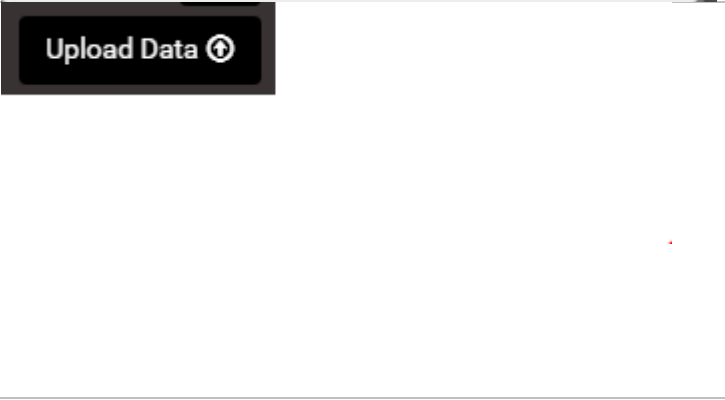
<p>Import AzureHound Modules</p> <pre>Import-Module C:\ADAssessment\Bloodhound\resources\app\Collectors\AzureHound.ps1</pre>	
Create a temporary assessment user in Azure AD	
Assign the Azure AD Role via PIM or permanent: Global Reader	
Assign the Reader Azure Role via PIM to the Tenant Root group	

AzureHound – Run (Windows)

Open Powershell as Administrator	
login to Azure PowerShell	
Connect -AzAccount	
Login zu Azure AD	
Connect -AzureAD	
<p>OPTIONAL:</p> <p>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:</p> <pre>C:\users\[Username]\.azure\AzureRmContextSettings.json C:\users\[Username]\.azure\TokenCache.dat</pre> <p>And place them in your own .azure folder. Re-launch PowerShell and the token will now be used.</p>	
Run	
<pre>Invoke-AzureHound -TenantId <TenantID> -OutputDirectory C:\ADAssessment\Bloodhound\resources\app\Collectors</pre>	

Load Data (Windows)

--	--

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


View Graph

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

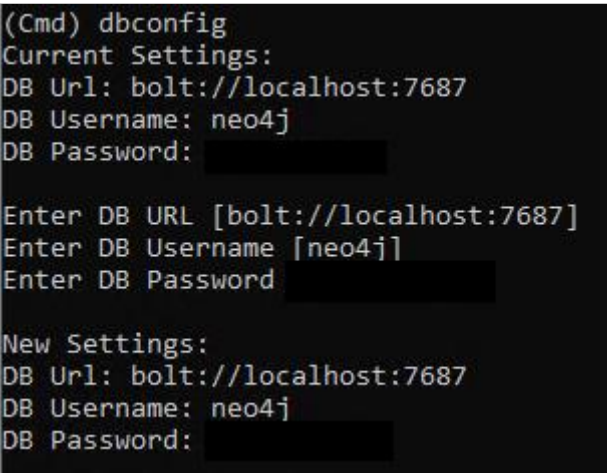
Create Excel Report (Windows)

Pre-requisites

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

Install Python	
<p>Open CMD and install the following modules:</p> <pre>pip install neo4j pip install openpyxl</pre>	
<p>Download BloodHound Analytics Python file from:</p> <p>Bloodhound/bloodhoundanalytics.py at main · m8r1us/Bloodhound · GitHub</p> <p>Save to: C:\ADAssessment\Report</p>	Script made for neo4j >=V4.0

Create Report

Run:	
<pre>python bloodhoundanalytics.py <domain></pre>	
<p>Type:</p> <p>dbconfig</p> <p>Check the connection settings</p>	
<p>Type:</p> <p>Connect</p>	

Type:	
startanalysis	
Excel is required to open the file	

Create Jupyter Notebook Report

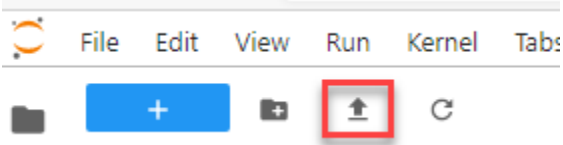
Jupyter: [Installation — JupyterLab 3.0.16 documentation](#)


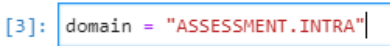
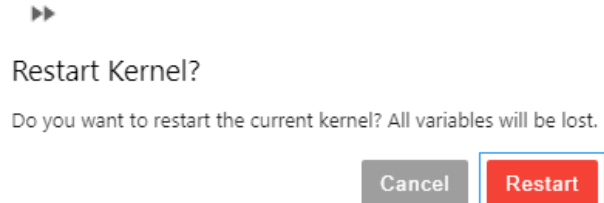
Plots: [plotly/plotly.py: The interactive graphing library for Python \(includes Plotly Express\) \(github.com\)](#)

Pre-requisites

Download Python (if not already done) (https://www.python.org/downloads)	
Install NPM: Node.js (nodejs.org)	
Open cmd as admin and run: <pre> pip install jupyterlab pip install py2neo pip install altair pip install pandas pip install psutil npm install --save plotlywidget jupyter labextension install jupyterlab-plotly@4.14.3 </pre>	
Create folder C:\ADAssessment\Reports	
Download bloodhound_report.ipynb from: https://github.com/m8r1us/Bloodhound/blob/main/bloodhound_report.ipynb and save the file to the Reports folder.	

Open Report

Open cmd as admin and run: <pre>jupyter-lab</pre>	
A browser should have opened automatically otherwise go to: http://localhost:8888/lab/workspaces	
Click on the upload file symbol and upload the "bloodhound_report.ipynb"	
Double-click or right click to open the bloodhound_report.ipynb file	

Change the connection string in step 2 accordingly.	<h3>Initialize BloodHound neo4j Database Connection</h3>  <p>The screenshot shows a configuration window for the Neo4j database connection. It includes a text box for the connection string, a dropdown for the database user, and a text box for the password. A red callout box points to the connection string, stating 'Neo4j connection URL See: http://localhost:7474/browser/'.</p>
Change the Domain to the domain to assess	<h3>Domain to assess</h3>  <p>The screenshot shows a configuration field for the domain to assess, with the value 'ASSESSMENT.INTRA' entered.</p>
Press the restart kernel button	 <p>The screenshot shows a dialog box titled 'Restart Kernel?' with the text 'Do you want to restart the current kernel? All variables will be lost.' and two buttons: 'Cancel' and 'Restart'.</p>

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. \(github.com\)](https://github.com/dirkjanm/ROADtools)

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 install 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)	
Download NodeJS/NPM (node-v14.17.0-x64) (https://www.npmjs.com/get-npm)	
Install NPM (NodeJS)	
Download Zulu JDK 11 (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	<pre>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 neo4j The Neo4j Graph Database - neo4j service is starting. The Neo4j Graph Database - neo4j service was started successfully.</pre>
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	



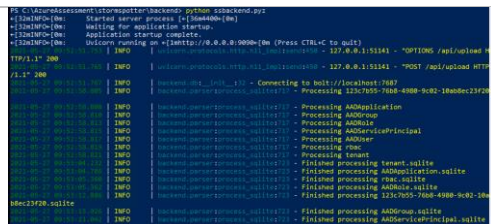
Run Stormcollector

<p>Open separate CMD and RUN:</p> <pre>cd C:\AzureAssessment\Stormspotter\stormcollector</pre> <p>Run to show the help menu:</p> <pre>python sscollector.pyz -h</pre> <p>Common options for all authentication types</p> <pre>python sscollector.pyz cli python sscollector.pyz spn -t <tenant> -c <clientID> -s <clientSecret></pre> <p>--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 delimited list. --nosubs: Subscriptions you wish to exclude. Multiple subscriptions can be excluded as a space delimited 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.</p>	

Run to collect data by using the created azure assessment account:

```
Az login
python sscollector.pyz cli
```

Load Data (Windows)

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

Review Graph

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

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 <i>! If there are msal.ps install errors follow the on-screen recommendations and try again to install msal.ps before installing the AzureADAssessment module.</i>	
## 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.pbix	
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"	