



Azure Home Lab

In this lab, I set up a basic home SOC in Azure from scratch. Using a free Azure subscription, I walk through creating a virtual machine (VM), opening it to the internet as a honeypot, and forwarding logs to a central repository. I then integrate Microsoft Sentinel to analyse real-world attack data.

In this lab I cover the following:

- Creating an Azure subscription and setting up a VM
- Configuring Log Analytics Workspace
- Forwarding logs and integrating with Sentinel
- Querying failed login attempts and visualizing attack sources
- Building an attack map to track real-time hacker activity

This project is great for cybersecurity personnel, like myself, looking to practice log analysis, threat detection, and SOC operations in a real-world cloud environment.

The initial steps will encompass the setting up of all the resources I need for this lab.

Step 1:

After signing up for my Azure free tier account, the first step is to create a **Resource Group** within the Azure portal. The Resource Group will house all my resources for this lab.

The screenshot shows the 'Create a resource group' wizard in the Azure portal. The 'Basics' tab is selected. The form includes fields for Subscription (set to 'Azure for Students'), Resource group name ('Azure-SOC_lab'), and Region ('(Africa) South Africa North'). At the bottom, there are 'Previous' and 'Next' buttons, and a prominent 'Review + create' button.

Microsoft Azure Search resources, services, and docs (G+/) Copilot 53208765@myle.unisa....
UNIVERSITY OF SOUTH AFRICA (...)

Home > Resource Manager

Resource Manager | Resource groups

University of South Africa

Search + Create Manage view Refresh Export to CSV Open query Assign tags

You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field... Subscription equals all Location equals all + Add filter

Name ↑	Subscription	Location
Azure-SOC_lab1	Azure for Students	South Africa North

Showing 1 - 1 of 1. Display count: auto Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Next, I created a **Virtual Network**. In essence, a virtual network uses software to create and manage a virtual version of a physical computer network. This allows devices to communicate with each other over the internet or a cloud infrastructure, offering greater flexibility and scalability than traditional hardware-based networks.

Microsoft Azure Search resources, services, and docs (G+/) Copilot 53208765@myle.unisa....
UNIVERSITY OF SOUTH AFRICA (...)

Home > Network foundation

Network foundation | Virtual networks

Preview

Search + Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all + Add filter

Showing 0 to 0 of 0 records.

Name ↑	Resource group ↑	Location ↑	Subscription ↑
--------	------------------	------------	----------------

No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.

+ Create virtual network Learn more Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure Search resources, services, and docs (G+) Copilot Home > Network foundation | Virtual networks > Create virtual network ...

Basics Security IP addresses Tags Review + create

Subscription * Azure for Students ✓
Resource group * Azure-SOC_lab1 ✓
[Create new](#)

Instance details

Virtual network name * V-Net_Lab1
Region * (Africa) South Africa North ⓘ
[Deploy to an Azure Extended Zone](#)

Previous Next Review + create Give feedback

Microsoft Azure Search resources, services, and docs (G+) Copilot Home > Network foundation | Virtual networks > Create virtual network ...

Validation passed

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription Azure for Students
Resource Group Azure-SOC_lab1
Name V-Net_Lab1
Region South Africa North

Security

Azure Bastion Disabled

Previous Next Create Download a template for automation Give feedback

Microsoft Azure Search resources, services, and docs (G+) Copilot Home > V-Net_Lab1-1761330542721 | Overview >

Deployment

Search Delete Cancel Redeploy Download Refresh

Overview

Deployment is in progress

Deployment name : V-Net_Lab1-1761330542721 Start time : 10/24/2025, 8:29:01 PM
Subscription : Azure for Students Correlation ID : da75c2c2-1d51-4fed-8cb1-cb3...
Resource group : Azure-SOC_lab1

Deployment details

Resource	Type	Status	Operation
V-Net_Lab1	Virtual network	Created	Operation

Give feedback Tell us about your experience with deployment

Microsoft Defender for Cloud
Secure your apps and infrastructure [Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

Below, you will notice that my **Virtual Network** has been created within my **Resource Group**.

The screenshot shows the Microsoft Azure Resource Manager interface. In the left sidebar, under the 'Essentials' section, there is a table listing resources. One entry is 'V-Net_Lab1' of type 'Virtual network' located in 'South Africa North'. The table includes columns for Name, Type, and Location.

Next, I will create a **Virtual Machine** which will act as the **honey pot**. In cybersecurity, a **honey pot** is a decoy system set up to attract and trap cyber attackers.

The screenshot shows the 'Create a virtual machine' wizard. On the first step, 'General', the user has selected 'Standard' as the security type, 'Windows 10 Enterprise 2016 LTSB - x64 Gen1' as the image, and 'x64' as the VM architecture. The 'Size' dropdown is set to 'Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$92.71/month)'. Buttons at the bottom include '< Previous', 'Next : Disks >', and 'Review + create'.

The screenshot shows the 'Networking' step of the 'Create a virtual machine' wizard. Under the 'Network interface' section, the user has selected 'V-Net_Lab1 (Azure-SOC_lab1)' for the virtual network, 'default' for the subnet, and '(new) CorpNET-1-ip' for the public IP. Buttons at the bottom include '< Previous', 'Next : Management >', and 'Review + create'.

Create a virtual machine

Validation passed

You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Azure for Students
Resource group	Azure-SOC_Lab1
Virtual machine name	CorpnetLabVM1
Region	South Africa North
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1

< Previous Next > Create Download a template for automation Give feedback

CreateVm-MicrosoftWindowsDesktop.Windows-10-rs1-e-20251028125417 | Overview

Your deployment is complete

Deployment name : CreateVm-MicrosoftWindows... Start time : 10/28/2025, 1:13:26 PM
 Subscription : Azure for Students Correlation ID : fbc896dc-fae1-4ee6-989c-d0...
 Resource group : Azure-SOC_lab1

Deployment details

Next steps

Set up 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

Give feedback Tell us about your experience with deployment

After successful deployment I went to my **Resource Group** to confirm that everything is in order.

Azure-SOC_lab1 Resource group

Overview

Activity log Access control (IAM) Tags Resource visualizer Events Settings Cost Management Monitoring Automation Help

How to manage these changes more efficiently with deployment tools? Help me generate Terraform for this resource group configuration. +1

+ Create Manage view Delete resource group Refresh Export to CSV Open query ... Group by none JSON View

Filter for any field... Type equals all Location equals all + Add filter

Name ↑	Type	Location
CorpNET-1-nsg	Network security group	South Africa North
CorpnetLabVM1	Virtual machine	South Africa North
CorpnetLabVM1-ip	Public IP address	South Africa North
CorpnetLabVM1-nsg	Network security group	South Africa North
corpnetlabvbm1440_z1	Network Interface	South Africa North
CorpnetLabVM1_OsDisk_1_3505878ab8744cc08ca193bb8c9b76c6	Disk	South Africa North
V-Net Lab1	Virtual network	South Africa North

Add or remove favorites by pressing Ctrl+Shift+F

Step 2

Now that my initial resources have been created, I will edit my **Network Security Group** and open it up to the internet. I do this so that my network is accessible from all traffic and make it discoverable to potential attackers as part of the honey trap.

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBal...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

I continued to delete my default **Remote Desktop Protocol (RDP)** inbound rule and create a new inbound rule that allows all inbound traffic.

Priority ↑	Name ↑	Port ↑
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBal...	Any
65500	DenyAllInBound	Any

CorpNetLabVM1-nsg | Inbound security rules

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Priority ↑	Name ↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	DANGER_rule_All...	Any	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Step 3

I proceeded to my Virtual Machine (VM) to disable the internal Windows Firewall. I start this process by first remote connecting my Virtual Machines Public IP Address.

CorpNetLabVM1 Virtual machine

Networking

- Public IP address: 102.37.145.129 (Network corpNetlabvm1440_z1 interface)
- 1 associated public IPs
- Public IP address (IPv6): -
- Private IP address: 172.16.0.4
- Private IP address (IPv6): -
- Virtual network/subnet: vnet-southafricanorth/snet-southafricanorth-1
- DNS name: Configure

Size

- Size: Standard D2s v3
- vCPUs: 2
- RAM: 8 GiB

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name:

- Name in the certificate from the remote computer: CorpnetLabVM1

Certificate errors:

The following errors were encountered while validating the remote computer's certificate:

- The certificate is not from a trusted certifying authority.

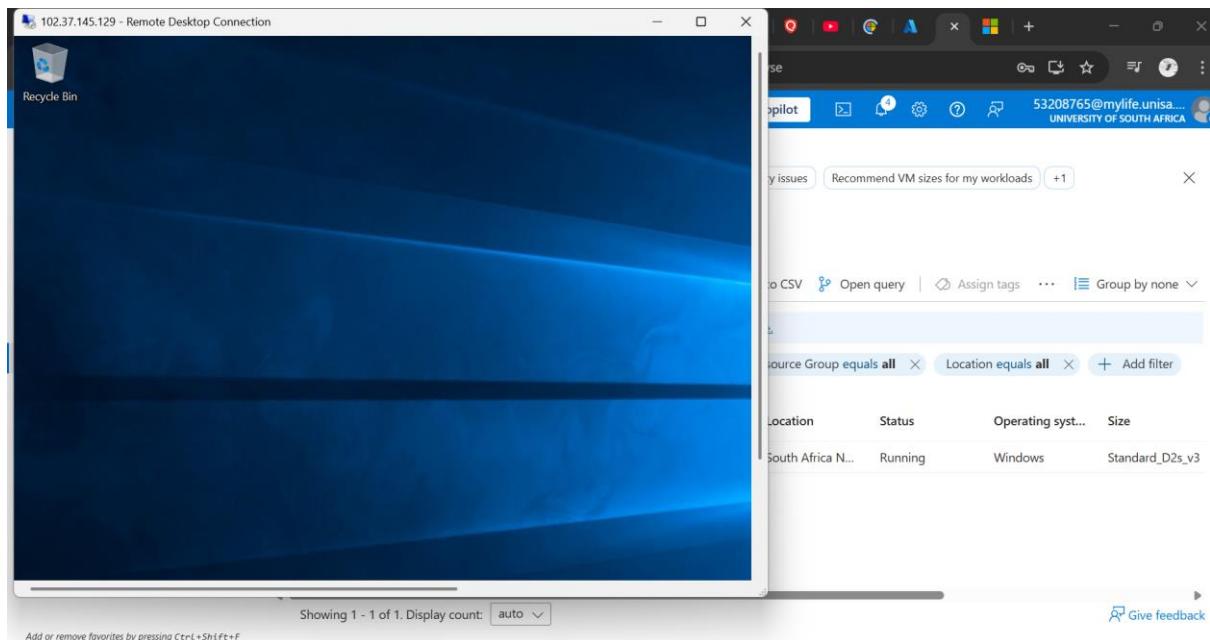
Do you want to connect despite these certificate errors?

Don't ask me again for connections to this computer

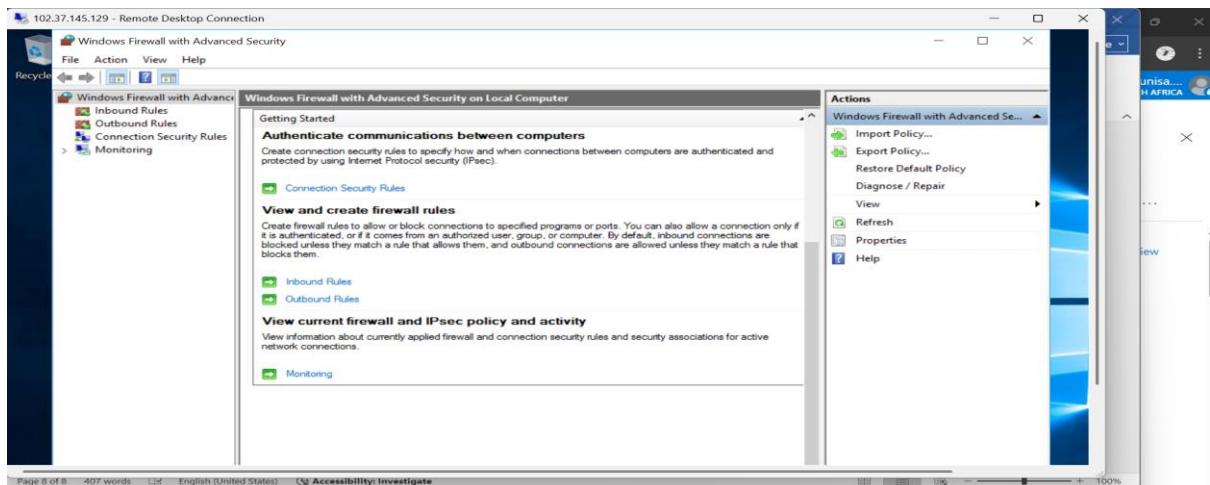
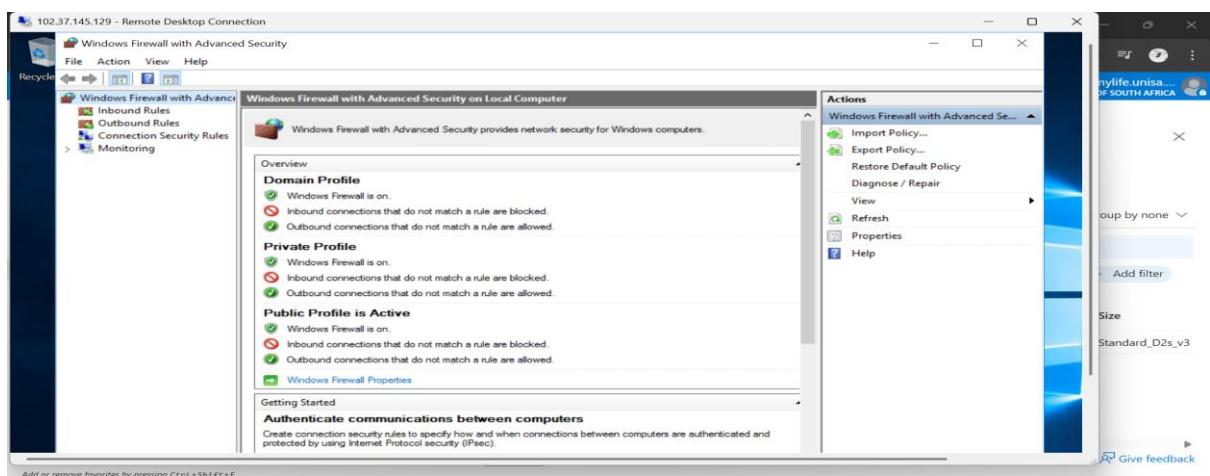
View certificate...

Yes **No**

I have successfully connected to my Windows Virtual Machine.



The next step was to turn off the **Windows Firewall** (VM) for my Virtual Machine.



I attempted to **ping** my VM, the **ping** was successful.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with options like Home, Compute infrastructure, Virtual machines, and others. In the center, a window titled 'CorpnetLabVM1' is open. Inside this window, a 'Command Prompt' tab is active, displaying the output of a 'ping' command to 102.37.145.129. The output shows four successful replies with round-trip times between 67ms and 77ms. To the right of the command prompt, there's a summary card for the VM. It shows the Public IP address as 102.37.145.129, associated with the interface corpnetlabvm1440_z1. It also lists 1 associated public IP (172.16.0.4), Private IP address (172.16.0.4), and other details like DNS name and size (Standard D2s v3, 2 vCPUs).

Step 4

In this step, I'll review some raw logs from my VM. I started off by purposely attempting to log into the virtual machine using **incorrect** signing in **credentials**.

This screenshot shows a 'Windows Security' dialog box from a Remote Desktop Connection session. The title bar says 'Your credentials did not work'. The message in the box states: 'The credentials that were used to connect to 102.37.145.129 did not work. Please enter new credentials.' Below this, there's a 'Employee' field with a placeholder 'Password' and a checked 'Remember me' checkbox. At the bottom of the dialog are 'OK' and 'Cancel' buttons. To the right of the dialog, the Azure VM summary card is visible, showing the same information as the previous screenshot.

Below is the log with “all” the security events that place on the virtual machine.

This screenshot shows the Windows Event Viewer application running on the VM. The main pane displays a list of security events with 244 entries. One specific event is selected, showing details: 'Event 4672, Microsoft Windows security auditing.' The details pane shows that 'Special privileges assigned to new logon.' and the subject is listed. The right-hand pane, titled 'Actions', contains a context menu with options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To this Log..., View, Refresh, Help, Event 4672, Microsoft Windows s..., Event Properties, and Attach Task To This Event...'. The Azure VM summary card is partially visible at the top of the screen.

Step 5

Next, as I wait for potential attackers to try attack my VM, I'll configure a **Log Repository** in Azure and forward my VM logs into it.

The image consists of three vertically stacked screenshots from the Microsoft Azure portal, illustrating the step-by-step creation of a Log Analytics workspace.

Screenshot 1: Create Log Analytics workspace - Step 1

This screenshot shows the initial configuration steps:

- Project details:** Subscription is set to "Azure for Students" and Resource group is "Azure-SOC_lab1".
- Instance details:** Name is "VMlogs" and Region is "South Africa North".
- Buttons:** "Review + Create" (highlighted), "< Previous", and "Next : Tags >".

Screenshot 2: Create Log Analytics workspace - Step 2

This screenshot shows the validation results and basic configuration details:

- Validation:** "Validation passed".
- Log Analytics workspace by Microsoft:** A summary card with basic information.
- Basics:** Substitution: "Azure for Students", Resource group: "Azure-SOC_lab1", Name: "VMlogs", Region: "South Africa North".
- Pricing:** Pricing tier: "Pay-as-you-go (Per GB 2018)".
- Buttons:** "Create" (highlighted), "< Previous", and "Download a template for automation".

Screenshot 3: Microsoft.LogAnalyticsOMS | Overview

This screenshot shows the deployment status and additional resources:

- Overview:** Deployment status: "Your deployment is complete".
 - Deployment name: "Microsoft.LogAnalyticsOMS"
 - Subscription: "Azure for Students"
 - Resource group: "Azure-SOC_lab1"
 - Start time: "10/28/2025, 5:00:32 PM"
 - Correlation ID: "6218dd50-b897-4906-b212-49..."
- Deployment details:** A link to view deployment details.
- Next steps:** A link to "Go to resource".
- Right sidebar:**
 - Cost management:** "Get notified to stay within your budget and prevent unexpected charges on your bill." with a "Set up cost alerts >" link.
 - Microsoft Defender for Cloud:** "Secure your apps and infrastructure" with a "Go to Microsoft Defender for Cloud >" link.
 - Free Microsoft tutorials:** "Start learning today >"
 - Work with an expert:**

Next up, I create my **Sentinel** Instance and link my VM logs to the **Sentinel** workspace. Microsoft Sentinel a cloud-native security information and event management (**SIEM**) and security orchestration, automation, and response (**SOAR**) platform that provides a unified view of your organization's security posture. It uses AI and machine learning to help detect, investigate, and respond to security threats across multi-cloud and on-premises environments by collecting and analysing data from various sources.

Microsoft Azure Search resources, services, and docs (G+) Copilot ✉️ 5 🚧 ⚙️ ⓘ 💬 53208765@mylife.unisa... UNIVERSITY OF SOUTH AFRICA

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

[Create a new workspace](#) Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. [Learn more](#)

Filter by name...				
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
VMlogs	southafricanorth	azure-soc_lab1	Azure for Students	University of South Africa

[Add](#) [Cancel](#)

Below I install the **Windows Security Events** connector. **Microsoft security events** are logs of activities related to security in a Microsoft environment, including Windows operating systems and services. These events can include anything from successful or failed login attempts to file deletions, and they are collected to help detect threats, investigate incidents, and monitor security posture. They are also the data fed into platforms like [Microsoft Sentinel](#), which analyses them to identify potential security breaches.

The screenshot shows the Microsoft Sentinel Content hub interface. On the left, a sidebar lists navigation items: Home, Microsoft Sentinel, Add Microsoft Sentinel to a workspace, Microsoft Sentinel, General, Threat management, Content management (selected), Content hub (selected), Repositories, Community, and Configuration. The main content area displays four metrics: 436 Solutions, 324 Standalone contents, 1 Installed, and 0 Updates. A search bar contains the query "security event". Below it, a table lists content items with columns: Content title, Status, and Content source. One item, "Windows Security Events", is listed as Installed under Solution. To the right, a panel titled "Windows Security Events" shows details for the provider (Microsoft Provider, Microsoft Support, 3.0.9 Version) and a note about installing the solution.

I also configured the connector page (**Windows Security Events via AMA**) via the **Create Data Collection Rule**. These rules govern the communication between my VM and the **Logs Analytics workspace**, this then allows me to access these logs in **Sentinel**.

The screenshots illustrate the configuration of a Data Collection Rule for Windows Security Events via AMA and the extension settings for a virtual machine.

Screenshot 1: Create Data Collection Rule - Basic Tab

This screenshot shows the "Create Data Collection Rule" page in the Microsoft Azure portal. The "Basic" tab is selected. The rule name is "DCR-Windows". The subscription is set to "Azure for Students" and the resource group is "Azure-SOC_lab1". The "Description" section explains that security events from Windows machines connected to the Microsoft Sentinel workspace can be streamed using the Windows agent, enabling dashboards, alerts, and investigation. The "Last data received" status is shown as "Disconnected".

Screenshot 2: Create Data Collection Rule - Collect Tab

This screenshot shows the "Collect" tab of the "Create Data Collection Rule" page. It lists the selected machines for collecting data. A note indicates that this will enable System Assigned Managed Identity on these machines, in addition to existing User Assigned Identities (if any). The machines listed are "CorpnetLabVM1" (microsoft.compute/virtualmachines) located in "South Africa North".

Screenshot 3: CorpnetLabVM1 | Extensions + applications

This screenshot shows the "Extensions + applications" blade for the virtual machine "CorpnetLabVM1". The "Extensions" tab is selected, showing one extension named "AzureMonitorWindows...". The extension details are: Name: AzureMonitorWindows..., Type: Microsoft.Azure.Monitor..., Version: 1.38.1.0, Latest Version: 1.38.1.0, Status: Transitioning. The sidebar on the left shows other tabs like Overview, Activity log, and Resource visualizer.

Successfully connected to my Logs Analytics workspace.

The screenshot shows the Microsoft Azure Log Analytics workspaces interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and various icons. Below it, the main title is 'Log Analytics workspaces' with a subtitle 'University of South Africa'. A toolbar includes 'Create', 'Open recycle bin', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A message says 'You are viewing a new version of Browse experience. Click here to access the old experience.' Below this, there are filter options: 'Subscription equals all', 'Resource Group equals all', 'Location equals all', and '+ Add filter'. The main table lists one item: 'VMlogs' under 'Name', 'Azure-SOC_lab1' under 'Resource Group', 'South Africa North' under 'Location', and 'Azure for Students' under 'Subscription'. At the bottom, it says 'Showing 1 - 1 of 1. Display count: auto' and has a 'Give feedback' link.

I ran a quick search (security event) to see which logs are being tracked. I went back to see the status of my connection and it was still transitioning. I then reattempted the search after the provisioning was successful in both **simple** and **KQL mode**

This screenshot shows the same interface as above, but with a search result for 'VMlogs'. The left sidebar shows 'Logs' is selected. The main pane displays a table titled 'Results' with two rows: 'EventID' and 'EventCount'. The first row has a value of '4624' and '1'. The second row has a value of '4672' and '1'. There are buttons for 'Search', 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', and 'Logs'. At the bottom, it says 'Showing 1 - 1 of 1. Display count: auto' and has a 'Query details' link.

This screenshot shows the same interface again, but with a search result for 'VMlogs' in KQL mode. The left sidebar shows 'Logs' is selected. The main pane displays a table titled 'Results' with three rows: 'TimeGenerated [UTC]', 'Account', 'AccountType', 'Computer', and 'EventSourceName'. The first row has a value of '10/28/2025, 5:31:33.589 PM', 'NT AUTHORITY\SYSTEM', 'Machine', 'CorpNetLabVM1', and 'Microsoft-Windows-Security/'. The second row has a value of '10/28/2025, 5:31:33.589 PM', 'NT AUTHORITY\SYSTEM', 'Machine', 'CorpNetLabVM1', and 'Microsoft-Windows-Security/'. There are buttons for 'New Query 1*', 'New Query 2*', 'Run', 'Save', 'Share', and 'Queries hub'. At the bottom, it says 'Showing 1 - 1 of 1. Display count: auto' and has a 'KQL mode' dropdown.

I expected to see more logs so I ran a ping and double checked my firewall settings on my VM. Everything seemed to be in order but for some reason my honey pot was not attracting any hits.

The screenshot shows two windows side-by-side. On the left is the Microsoft Azure Log Analytics workspace titled 'VMlogs'. It displays a table of log results with one entry:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel
> 10/28/2025, 5:31:33.589 PM	NT AUTHORITY\SYSTEM	Machine	CorpnetLabVM1	Microsoft-Windows-Security-Audit	Security
> 10/28/2025, 5:31:33.589 PM	NT AUTHORITY\SYSTEM	Machine	CorpnetLabVM1	Microsoft-Windows-Security-Audit	Security

On the right is a 'Windows Firewall with Advanced Security' window. The 'Monitoring' section shows that the Windows Firewall is off for all profiles (Domain, Private, Public). The 'Actions' pane includes options like Import Policy..., Export Policy..., and Diagnose / Repair.

After two hours I came back to run the “SecurityEvent” KQL command, I got some positive results. Unfortunately, none of the log results were hackers attempting to enter my VM.

The screenshot shows the Microsoft Azure Log Analytics workspace again, this time with four entries in the log table:

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel
> 10/28/2025, 7:21:26.011 PM	WORKGROUP\CorpnetLabVM1\\$	Machine	CorpnetLabVM1	Microsoft-Windows-Security-Audit	Security
> 10/28/2025, 7:21:23.729 PM	WORKGROUP\CorpnetLabVM1\\$	Machine	CorpnetLabVM1	Microsoft-Windows-Security-Audit	Security
> 10/28/2025, 7:21:23.728 PM	WORKGROUP\CorpnetLabVM1\\$	Machine	CorpnetLabVM1	Microsoft-Windows-Security-Audit	Security
> 10/28/2025, 7:21:23.727 PM	WORKGROUP\CorpnetLabVM1\\$	Machine	CorpnetLabVM1	Microsoft-Windows-Security-Audit	Security

