

# Azure - Microsoft Sentinel Lab

## 1. Creating Resource Group (rg-sentinel-lab) and VM (vm-004)

- Deployed Ubuntu Server VM with SSH key authentication.

The screenshot shows the Azure Resource Group Overview page for 'rg-sentinel-lab'. The left sidebar contains navigation links like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Insights (preview), Alerts, Metrics, Diagnostic settings, Logs, Advisor recommendations, Workbooks, Automation, Export template, Help, and Support + Troubleshooting. The main area displays 'Essentials' information: Subscription (move) to 'Azure subscription 1', Deployment status 'No deployments', and Location 'West US 3'. Below this is a table of resources:

Name	Type	Location
vm-003_key	SSH key	West US 3
vm004	Virtual machine	West US 3
vm004-ip	Public IP address	West US 3
vm004-rsg	Network security group	West US 3
vm004279	Network Interface	West US 3
vm004_key	SSH key	West US 3
vm004_OsDisk_1_90f574d6fb7448f904eed67c885d	Disk	West US 3
vnet-westus3	Virtual network	West US 3

- Configured NSG to allow SSH only from your IP.

The screenshot shows the 'SSH' configuration for the NSG 'vm004-rsg'. A success message 'Updated security rule' and 'Successfully saved security rule 'SSH''. The configuration fields are as follows:

- Source: IP Addresses
- Source IP addresses/CIDR ranges: (empty field)
- Source port ranges: \*
- Destination: Any
- Service: SSH
- Destination port ranges: 22
- Protocol: TCP (selected)
- Action: Allow (selected)
- Priority: 100

## 2. Connecting to VM server

- Used ssh azureuser@ with SSH key

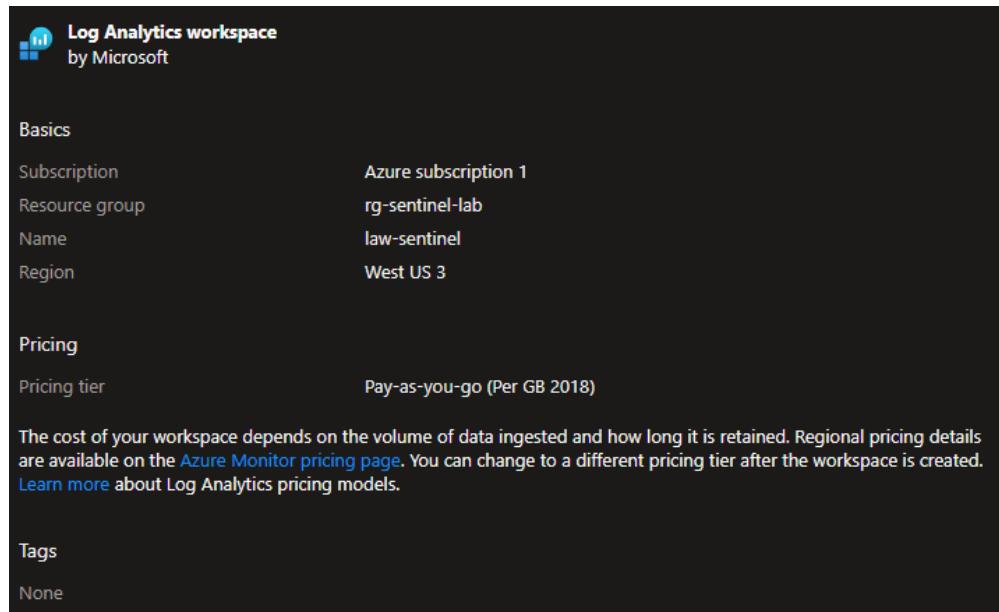
```
PS C:\Users\██████████ ssh -i "C:\Users\██████████ Downloads\vm004.key.pem" azureuser@██████████
The authenticity of host '██████████ (██████████)' can't be established.
ED25519 key fingerprint is SHA256:██████████.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '██████████' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1017-azure x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Mon Feb 23 00:26:06 UTC 2026
System load: 0.01      Processes:          137
Usage of /: 5.6% of 28.02GB   Users logged in:     0
Memory usage: 31%           IPv4 address for eth0: ██████████
Swap usage:  0%
```

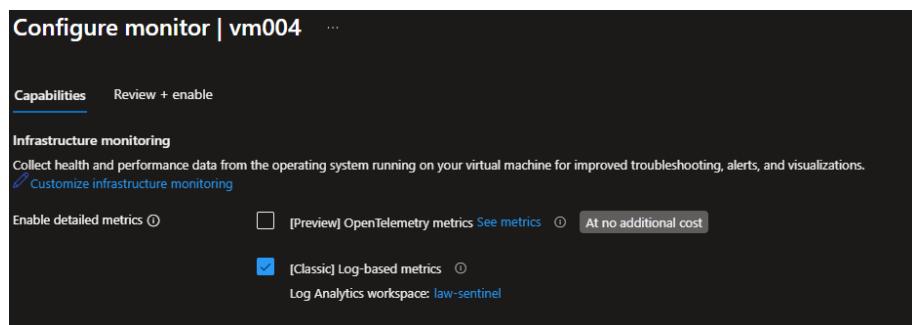
## 3. Create Log Analytics Workspace (law-sentinel)

- Created LAW in the same region as VM.



## 4. Install Azure Monitor Agent (AMA)

- a. - Onboarded VM from Monitor -> Virtual Machines.



- b. AMA is installed ✓
- c. Confirmed LAW is working properly with VM via heartbeat

Query: Heartbeat | sort by TimeGenerated desc

The screenshot shows the Log Analytics workspace interface. On the left, there's a navigation pane with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Resource visualizer, Settings, Tables, Agents, Usage and estimated costs, Data export, Network isolation, and Identity. The main area has a search bar and a query history section. A query editor window is open with the following command:

```
Heartbeat | sort by TimeGenerated desc
```

The results table shows three rows of data:

TimeGenerated [UTC]	SourceComputerId	ComputerIP	Computer	Category	OStype	OSName	OSMajor
2/23/2026, 12:40:13.650 AM	b0365de-1808-45a5-939c-3b159045972	vm004	Azure Monitor Agent	Linux	Ubuntu	24	
2/23/2026, 12:39:13.618 AM	b0365de-1808-45a5-939c-3b159045972	vm004	Azure Monitor Agent	Linux	Ubuntu	24	
2/23/2026, 12:38:13.675 AM	b0365de-1808-45a5-939c-3b159045972	vm004	Azure Monitor Agent	Linux	Ubuntu	24	

## 5. Create Microsoft Sentinel: Syslog Data Collection Rule (DCR)

The screenshot shows the Microsoft Sentinel Content hub. It displays various metrics: 465 Solutions, 324 Standalone contents, 0 Installed, and 0 Updates. A search bar at the top is set to "syslog". The main area lists data connectors, with "Syslog via AMA" being the selected item. The right side provides a detailed view of the "Syslog via AMA" connector.

**Syslog via AMA**

**Description:** Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace.

**Content source:** Syslog

**Status:** Not installed

**Provider:** Microsoft

**Support:** Microsoft

**Category:** IT Operations

**Prerequisites:** To integrate with Syslog via AMA make sure:

- Workspace data sources: read and write permission
- To collect data from non-Azure VMs; they must be running the Azure Monitor Agent.

**Configuration:** Enable data collection rule

**Facility:** LOG\_ALERT, LOG\_AUDIT, LOG\_AUTH, LOG\_AUTHPRIV, LOG\_CRON, LOG\_DAEMON, LOG\_CLOCK, LOG\_FTP, LOG\_KERN, LOG\_LOCAL0, LOG\_LOCAL1, LOG\_LOCAL2, LOG\_LOCAL3, LOG\_LOCAL4, LOG\_LOCAL5

**Minimum log level:** none

- a. - Enabled syslog facilities: auth, authpriv, daemon, syslog.

The screenshot shows the Data collection rule management page for the "Syslog via AMA" connector. It has tabs for Basic, Resources, Collect, and Review + create. The Collect tab is active.

**Prerequisites:** Select the checkbox to collect messages with no facility and no severity.  Collect messages without PRI header (facility and severity).

**Configuration:** To use your AMA installed machine as a collector, run the command: sudo wget -O Forwarder\_AMA\_installer.py https://

Facility	Minimum log level
LOG_ALERT	none
LOG_AUDIT	none
LOG_AUTH	LOG_INFO
LOG_AUTHPRIV	LOG_INFO
LOG_CRON	none
LOG_DAEMON	LOG_INFO
LOG_CLOCK	none
LOG_FTP	none
LOG_KERN	none
LOG_LOCAL0	none
LOG_LOCAL1	none
LOG_LOCAL2	none
LOG_LOCAL3	none
LOG_LOCAL4	none
LOG_LOCAL5	none

- Destination: law-sentinel.
- Query test syslog integration: Syslog | take 20

TimeGenerated [UTC]	Computer	EventTime [UTC]	Facility	HostName	Severity
> 2/23/2026, 2:27:00.013 AM	vm004	2/23/2026, 2:27:00.000 AM	daemon	vm004	info
> 2/23/2026, 2:27:00.013 AM	vm004	2/23/2026, 2:27:00.000 AM	daemon	vm004	info
> 2/23/2026, 2:27:00.013 AM	vm004	2/23/2026, 2:27:00.000 AM	daemon	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info
> 2/23/2026, 2:26:57.471 AM	vm004	2/23/2026, 2:26:57.000 AM	syslog	vm004	info

b. - Associated VM to DCR

## 6. Enable PasswordAuthentication on VM

```
PS C:\Users\***** > for ($i=1; $i -le 15; $i++) {
>>     ssh wronguser@172.17.0.10 # this will fail
>> }
wronguser@172.17.0.10: Permission denied (publickey).
PS C:\Users\*****
```

- a. - Edited /etc/ssh/sshd\_config and /etc/ssh/sshd\_config.d/60-cloudimg-settings.conf.

i. Set password authentication on so we can test brute force

```
azureuser@vm004:~$ # See all places that set it
sudo grep -Rin 'PasswordAuthentication' /etc/ssh/sshd_config /etc/ssh/sshd_config.d/
/etc/ssh/sshd_config:66:PasswordAuthentication yes
/etc/ssh/sshd_config:88:# PasswordAuthentication. Depending on your PAM configuration,
/etc/ssh/sshd_config:92:# PAM authentication, then enable this but set PasswordAuthentication
/etc/ssh/sshd_config.d/50-cloud-init.conf:1:PasswordAuthentication no
/etc/ssh/sshd_config.d/60-cloudimg-settings.conf:1:PasswordAuthentication no

azureuser@vm004:~$ sudo nano /etc/ssh/sshd_config.d/60-cloudimg-settings.conf
azureuser@vm004:~$ sudo systemctl reload ssh
azureuser@vm004:~$ exit
Logout
```

- b. - Set PasswordAuthentication yes, restarted SSH.

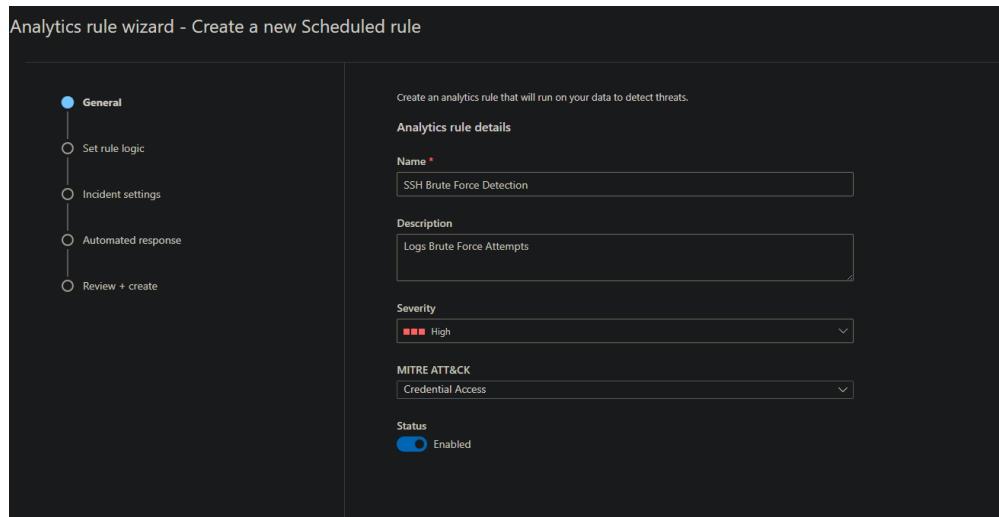
## 7. Run brute-force simulation from local machine

- Used PowerShell loop to generate failed SSH password attempts.

```
wronguser@[REDACTED]:~$ password:  
PS C:\Users\wronguser> for ($i=1; $i -le 15; $i++) {  
>> ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no wronguser@[REDACTED]  
>> }  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
wronguser@[REDACTED]:~$ Permission denied (publickey,password).  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
wronguser@[REDACTED]:~$ Permission denied (publickey,password).  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
wronguser@[REDACTED]:~$ Permission denied (publickey,password).  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.  
wronguser@[REDACTED]:~$ password:  
Permission denied, please try again.
```

## 8. Build Sentinel Analytic Rule (SSH Brute Force Detection)

- Created Scheduled Query Rule in Defender portal.



- Added KQL to detect >5 failures in 5 minutes.
- Entity mapping: SourceIP -> IP entity, HostName -> Host entity.
- Enabled alert grouping.

### Simple SSH Brute Force Detection Rule:

#### Syslog

```
| where ProcessName == "sshd"  
| where SyslogMessage has "Failed password"  
| extend SrcIp = extract(@"from\$\+(\d{1,3}\$\.\d{1,3})\$\{3\}", 1,  
SyslogMessage)  
| extend HostName = Computer  
| summarize FailedAttempts = count() by SrcIp, HostName,  
bin(TimeGenerated, 5m)  
| where FailedAttempts >= 5
```

**Analytics rule details**

Name	SSH Brute Force Detection
Description	Logs Brute Force Attempts
MITRE ATT&CK	Credential Access
Severity	High
Status	<input checked="" type="radio"/> Enabled

**Analytics rule settings**

Rule query	// Simple SSH Brute Force Detection Syslog   where ProcessName == "sshd"   where SyslogMessage has "Failed password"   extend SrcIp = extract(@"from\\$\+(\d{1,3}\\$\.\d{1,3})\\$\{3\}", 1, SyslogMessage)   extend HostName = Computer   summarize FailedAttempts = count() by SrcIp, HostName, bin(TimeGenerated, 5m)   where FailedAttempts >= 5
Rule frequency	Run query every <b>5 minutes</b>
Rule period	Last <b>5 minutes</b> data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns <b>more than 0</b> results
Event grouping	Group all events into a single alert
Suppression	Not configured

**Entity mapping**

Entity mapping	
Entity 1:	IP Identifier: Address, Value: SrcIp
Entity 2:	Host Identifier: HostName, Value: HostName
Custom details	Not configured
Alert details	Not configured
Incident settings	
Create incidents from this rule	<input checked="" type="radio"/> Enabled
Alert grouping	<input checked="" type="radio"/> Enabled
Grouping logic	Match selected entity types and details
Re-open closed incidents	<input checked="" type="radio"/> Disabled
Grouping period	Match from the last <b>5 Minutes</b>
Incident correlation	Tenant default
Automated response	
Automation rules	Not configured

## 9. Validate Incident Creation

### i. - Verified incidents in Microsoft Defender -> Incidents.

#### 1. Brute forced

```
Permission denied, please try again.  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] Permission denied (publickey,password).  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] Permission denied (publickey,password).  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] Permission denied (publickey,password).  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] Permission denied (publickey,password).  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] password:  
Permission denied, please try again.  
wronguser@[REDACTED] password:  
wronguser@[REDACTED] Permission denied (publickey,password).
```

### ii. - Confirmed high-severity brute-force detection triggered

The screenshot shows the Microsoft Defender XDR interface. On the left, the navigation pane includes Home, Exposure management, Investigation & response (selected), Incidents & alerts (selected), Hunting, Actions & submissions, Partner catalog, Threat intelligence, Assets, and Microsoft Sentinel. The main area is titled 'Alerts' and displays a list of 6 alerts. The first alert is highlighted: 'SSH Brute Force Detection' (Severity: High, Status: New, Category: Credential Access, Detection source: Scheduled detection, Product name: Microsoft Sentinel, Impacted assets: vm-002). The alert details pane on the right shows: Alert ID: sned52713e-a149-424e-97dd-dc73eeada2, Categories: Credential Access, Detection source: Scheduled detection, Service source: Microsoft Sentinel, Detection technology: Generated on Feb 22, 2026 4:56:28 PM, First activity: Feb 22, 2026 4:20:00 PM, Last activity: Feb 22, 2026 4:20:00 PM, Workspace: bchabbb0-abaf-4743-a119-bf9e0255371e, Evidence: Entity Name: [REDACTED], Remediation Status: Suspicious.