Lab Manual- Administrating Azure Virtual Machine

Prepared for:

Date: 18th March 2022

Prepared by:

Document Name: Lab Manual

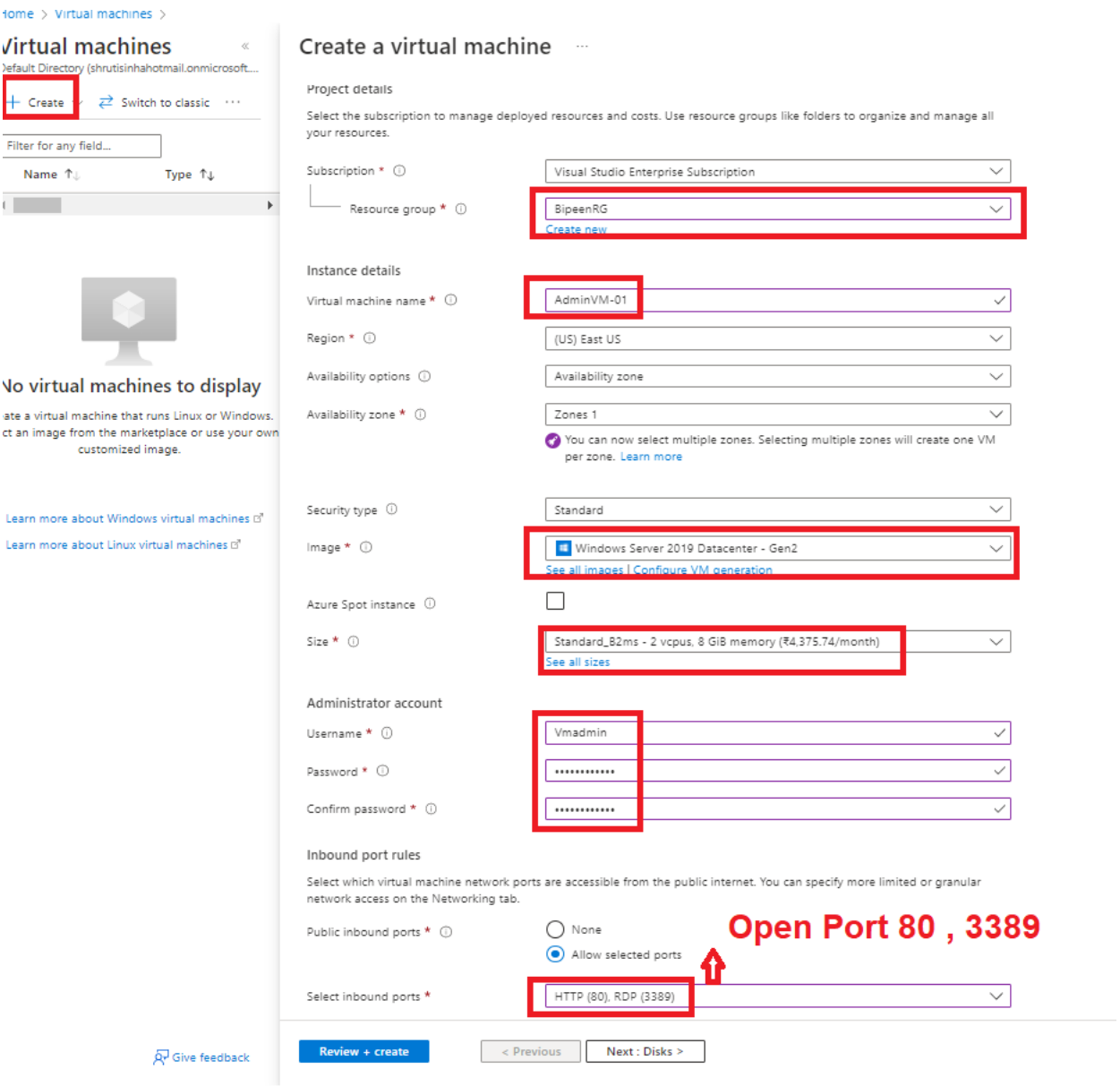
Document Number AZLabn990

Contributor:

Contents

1. Lab 1: Launch Azure Virtual Machine

1. Sign in to Azure Portal
2. In the Search Bar type Virtual Machine and Select Virtual Machine
3. Click Create to Create a VM
4. Use below parameter in the wizard
    - **Resource Group : Your Resource Group**
    - **Virtual Machine Name : AdminVM-01-<any other charater>**
    - **Image : Windows Server 2019**
    - **Size : Default**
    - **Username : VMAdmin**
    - **Password : Password@123**
    - **Ports : 80,3389**



5. Click Review and Create

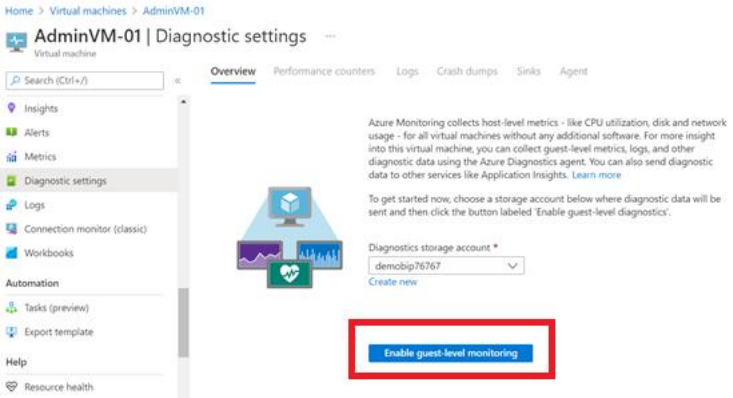
2. Lab 2: Enable Diagnostic Setting

Azure Diagnostics extension is one of the agents available to collect monitoring data from the guest operating system of compute resources. The primary scenarios addressed by the diagnostics extension are:

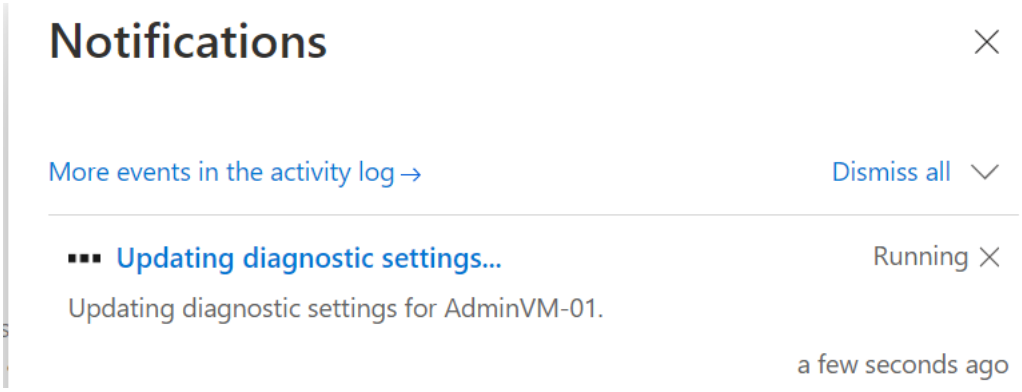
- Collect guest metrics into Azure Monitor Metrics.
- Send guest logs and metrics to Azure storage for archiving.
- Send guest logs and metrics to Azure event hubs to send outside of Azure.

Note : While the configuration for diagnostics extension can be formatted in either JSON or XML, any configuration done in the Azure portal will always be stored as JSON

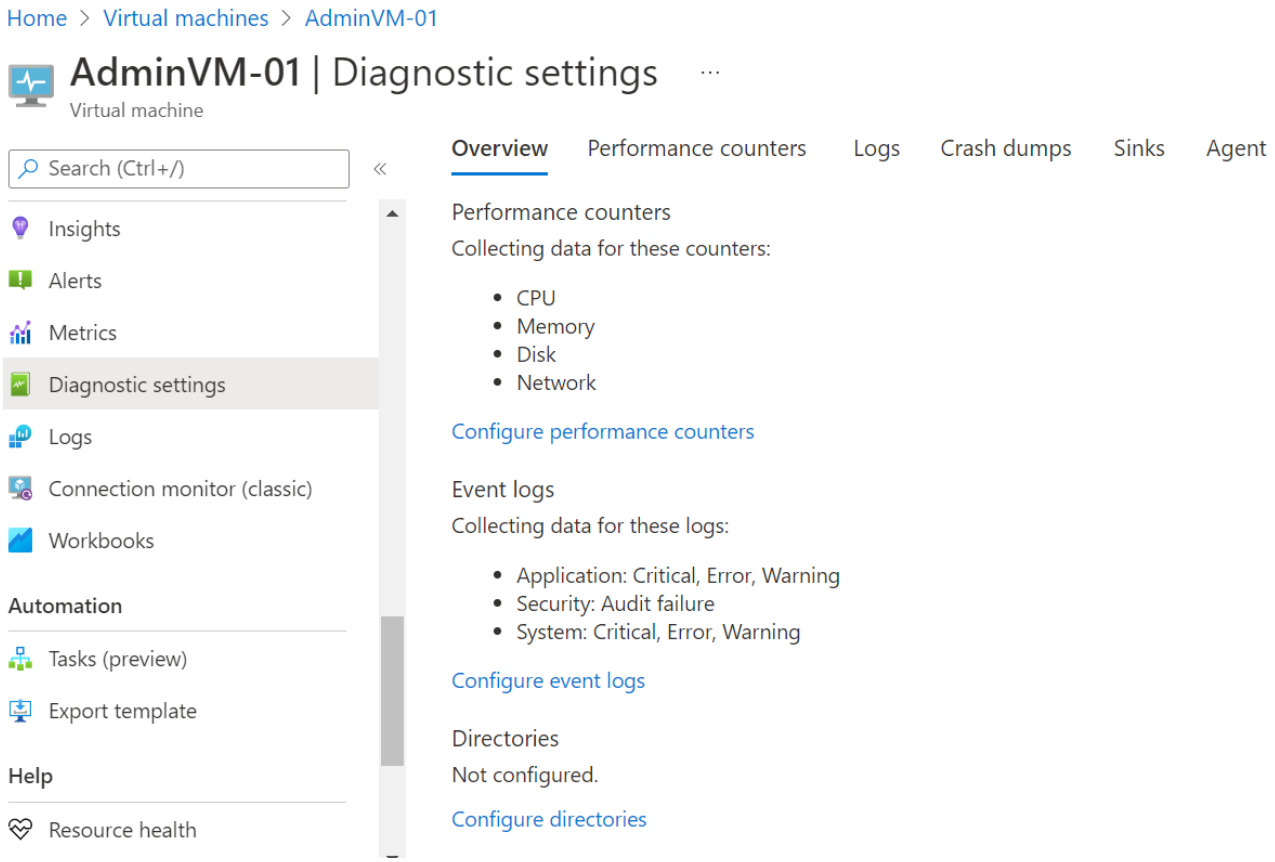
1. Open the menu for a virtual machine in the Azure portal.
2. Click on **Diagnostic settings** in the **Monitoring** section of the VM menu.
3. Click **Enable guest-level monitoring** if the diagnostics extension hasn't already been enabled.



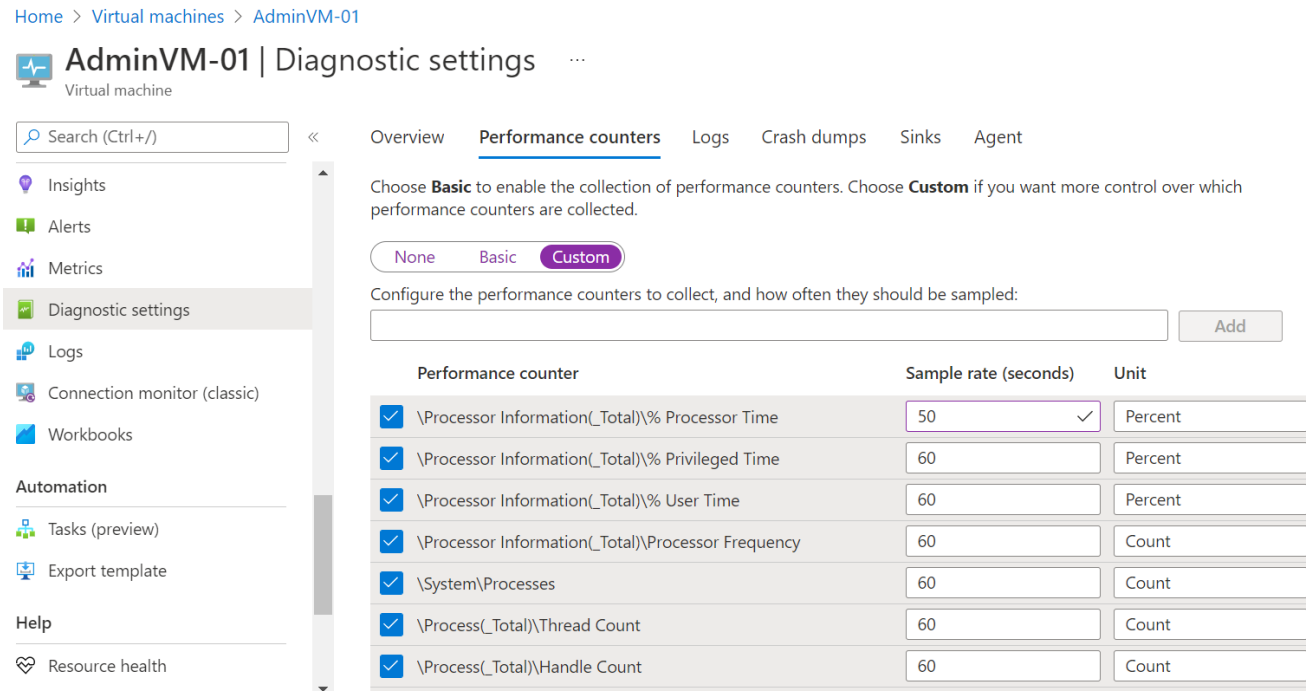
4. It may take few minutes



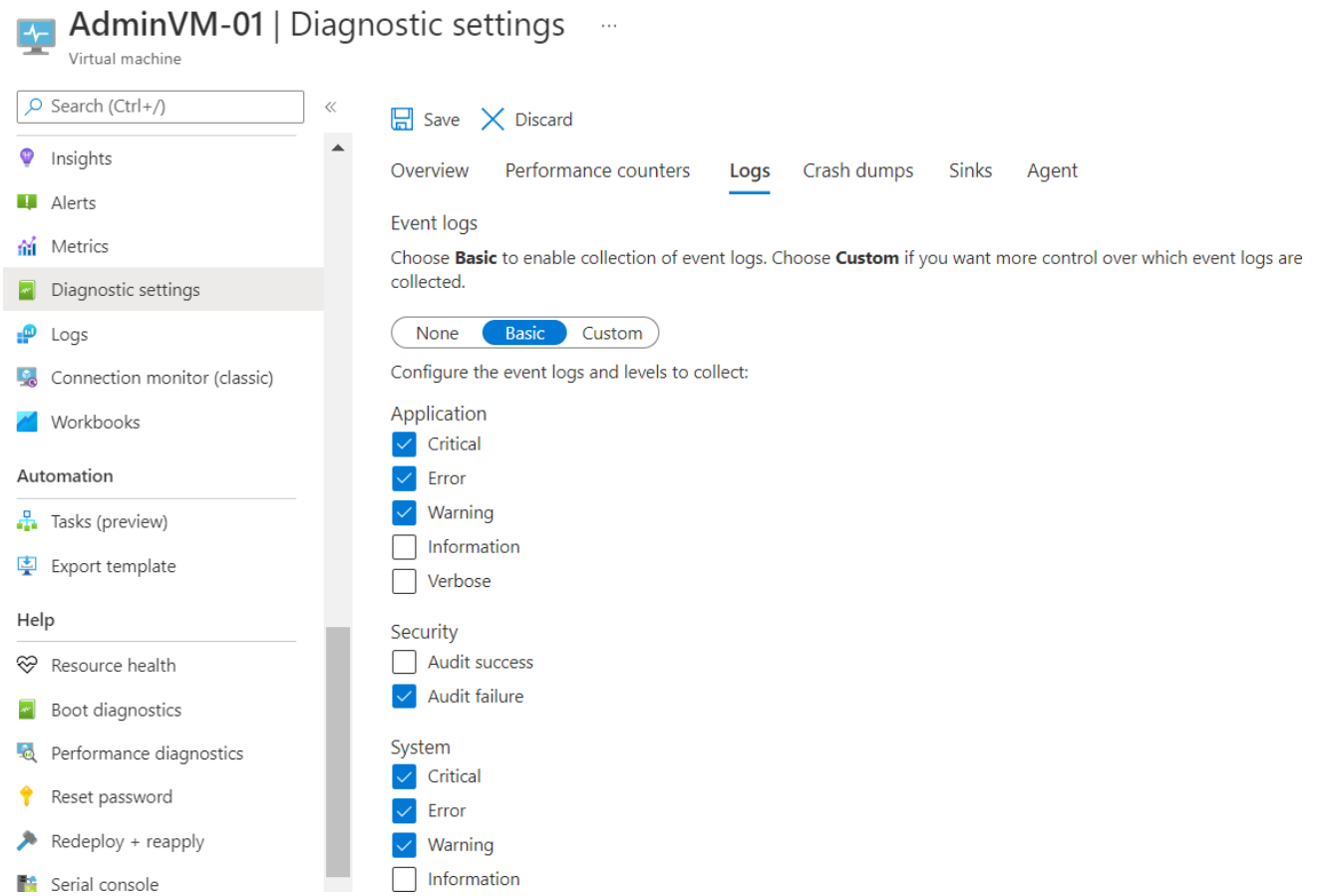
5. A new Azure Storage account will be created for the VM with the name will be based on the name of the resource group for the VM, and a default set of guest performance counters and logs will be selected.



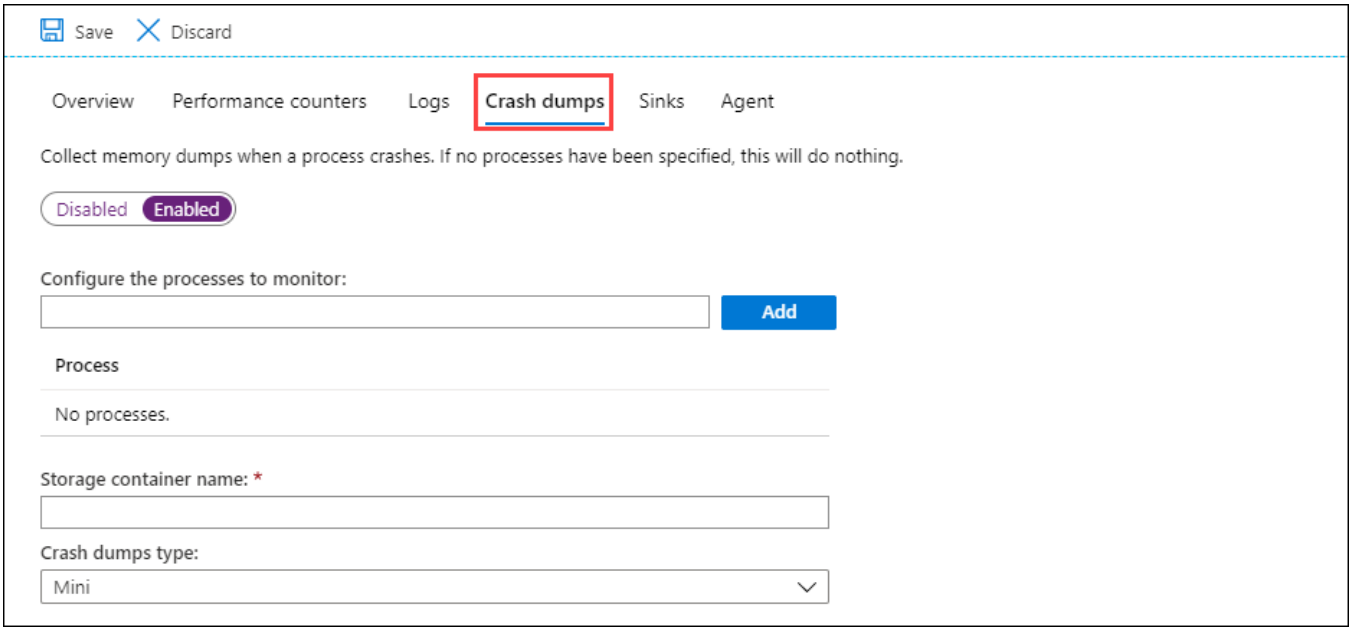
6. In the **Performance counters** tab, select the guest metrics you would like to collect from this virtual machine. Use the **Custom** setting for more advanced selection.



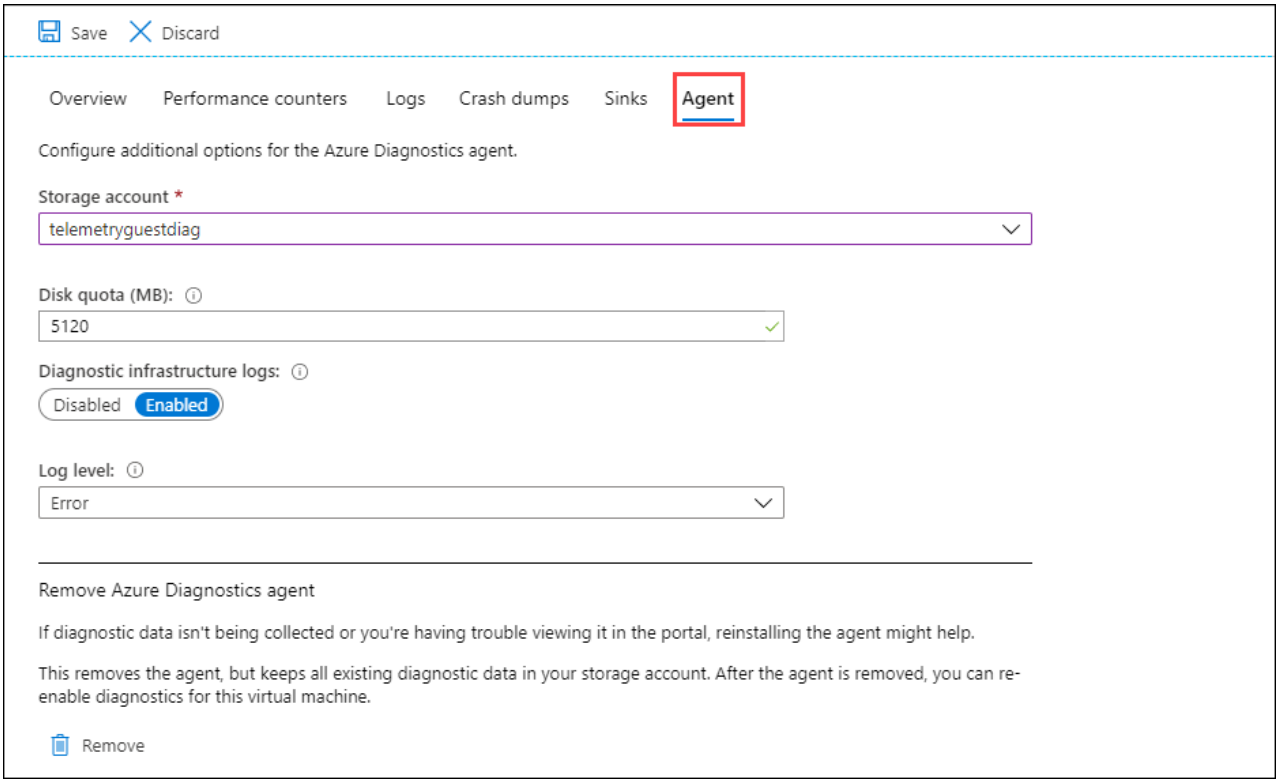
7. In the **Logs** tab, select the logs to collect from the virtual machine. Logs can be sent to storage or event hubs, but not to Azure Monitor. Use the Log Analytics agent to collect guest logs to Azure Monitor.



8. In the **Crash dumps** tab, specify any processes to collect memory dumps after a crash. The data will be written to the storage account for the diagnostic setting, and you can optionally specify a blob container.



9. In the **Agent**, you can change the storage account, set the disk quota, and specify whether to collect diagnostic infrastructure logs.



10. Click **Save** to save the configuration.

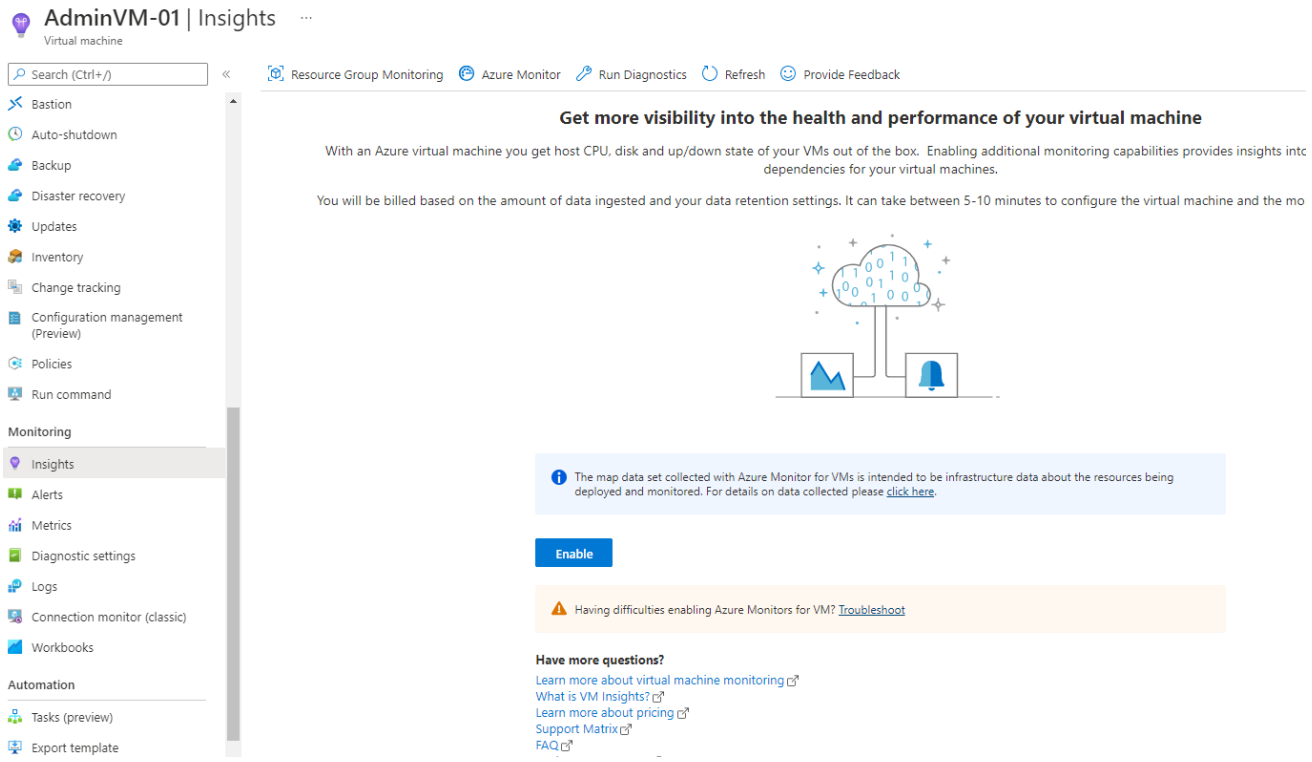
3. Lab 3: Enable Insight

VM insights monitors the performance and health of your virtual machines and virtual machine scale sets, including their running processes and dependencies on other resources. It can help deliver predictable performance and availability of vital applications by identifying performance bottlenecks and network issues and can also help you understand whether an issue is related to other dependencies.

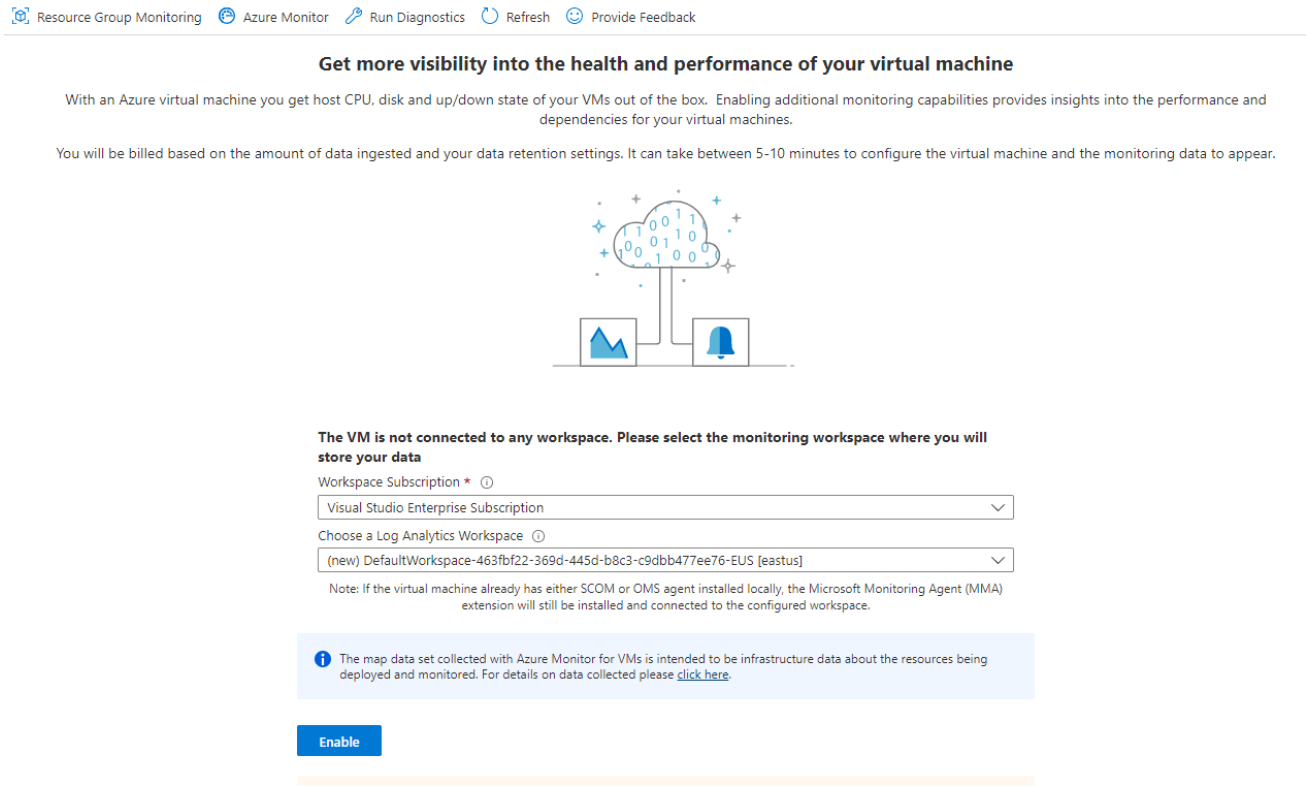
VM insights supports Windows and Linux operating systems on the following machines:

- Azure virtual machines
- Azure virtual machine scale sets
- Hybrid virtual machines connected with Azure Arc
- On-premises virtual machines
- Virtual machines hosted in another cloud environment

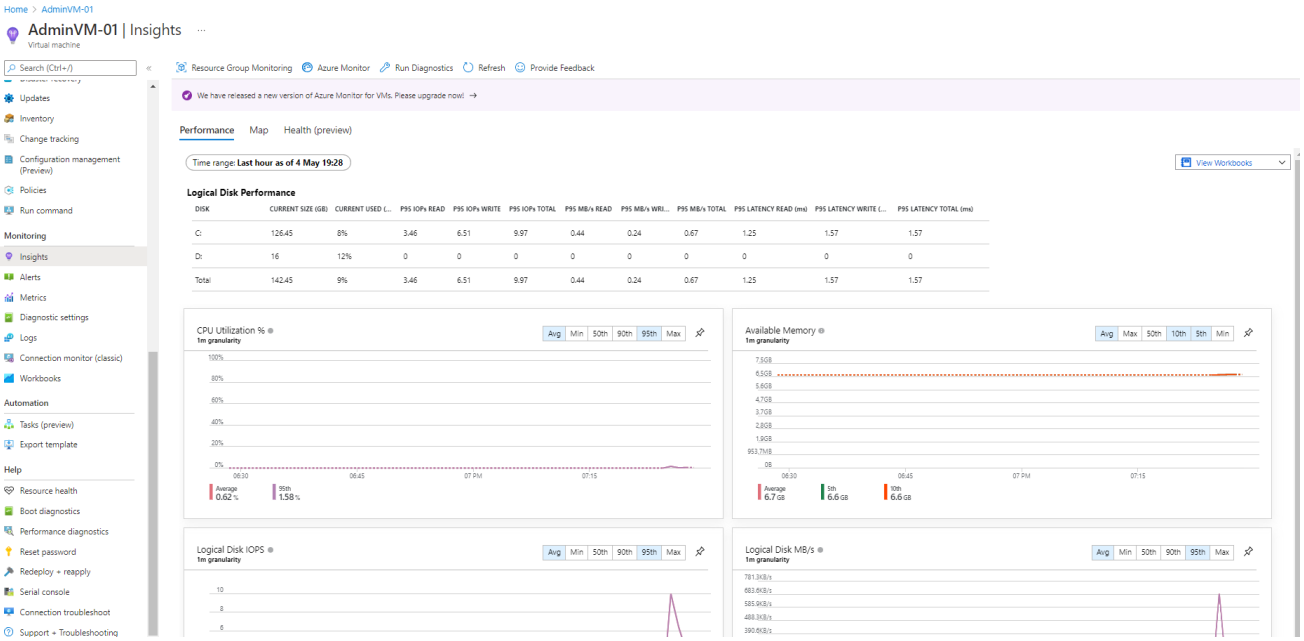
✓ In the Monitoring section of the menu, select **Insights** and then Enable.



✓ It by default create a Log Analytics workspace

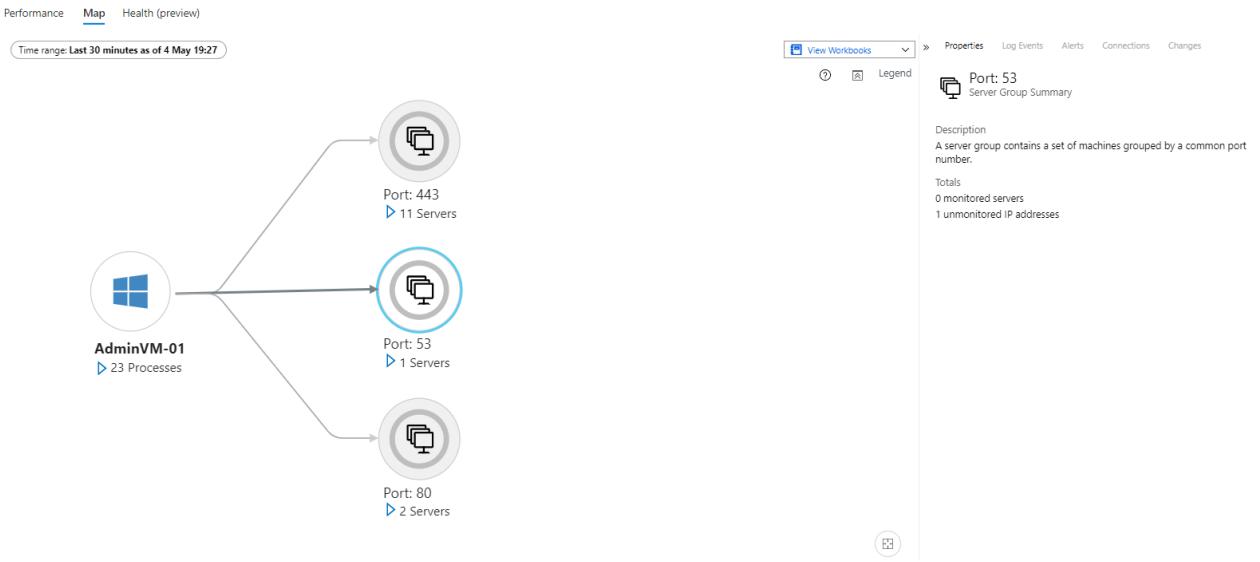


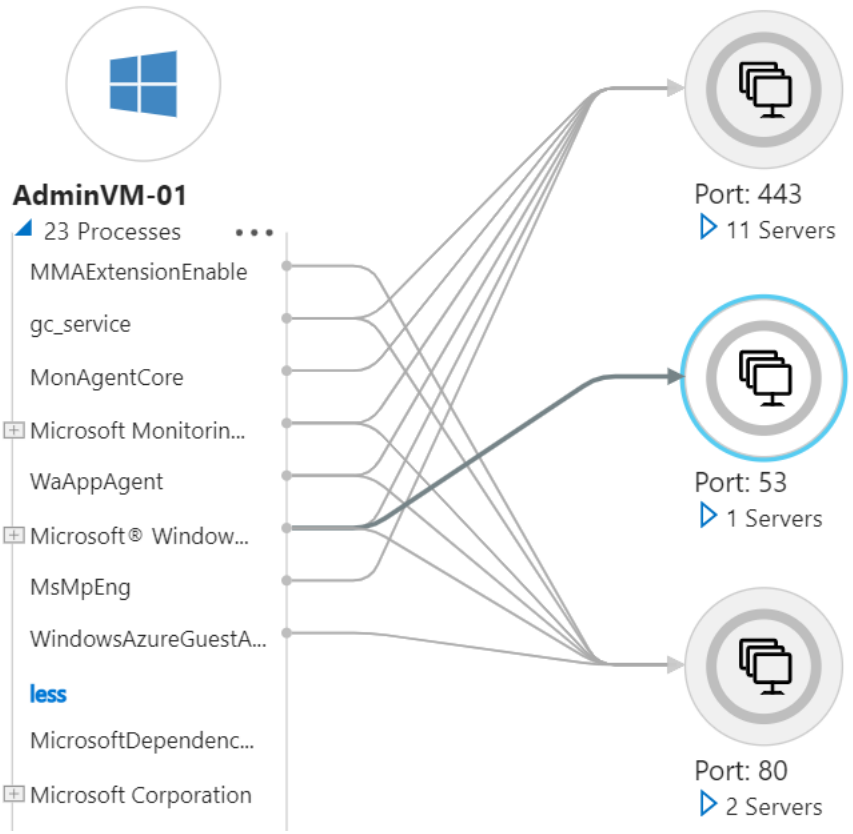
✓ You will receive status messages as the configuration is performed.



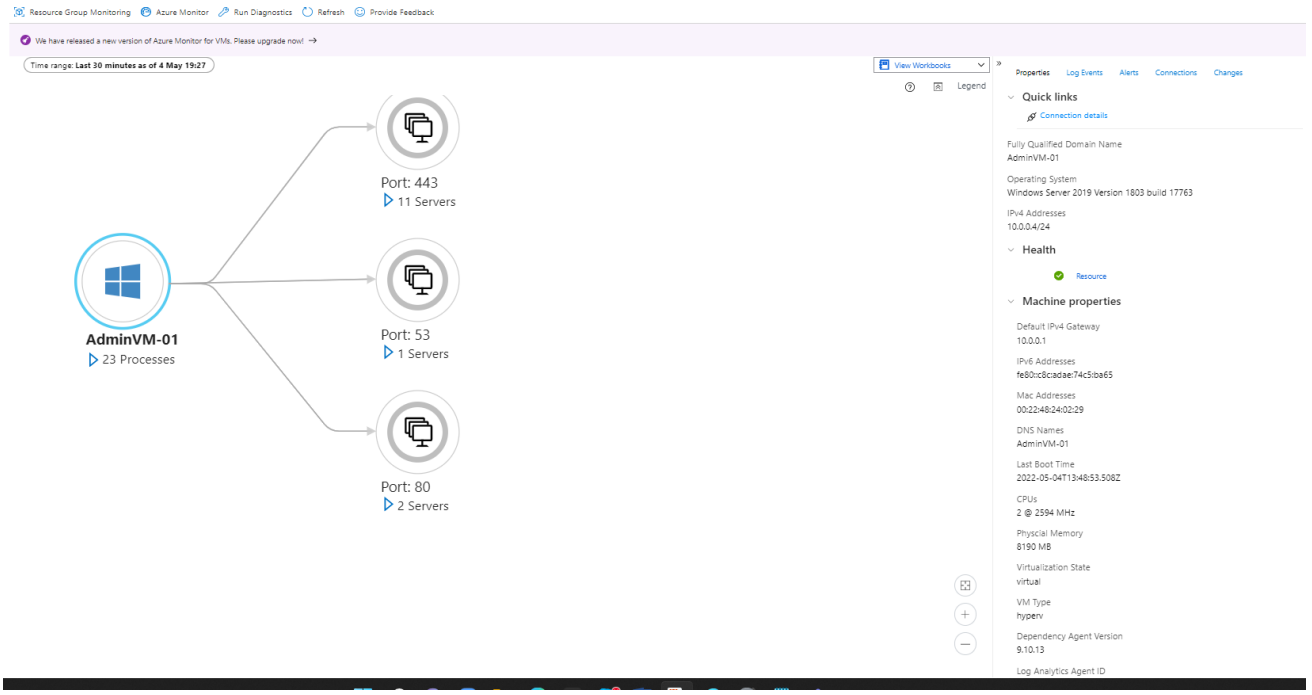
✓ The Map feature visualizes the VM dependencies by discovering running processes that have:

- Active network connections between servers.
- Inbound and outbound connection latency.
- Ports across any TCP-connected architecture over a specified time range.





✓ When you select the VM, the **Properties** pane on the right shows the VM's properties



Properties Log Events Alerts Connections Changes

Quick links

Connection details

Fully Qualified Domain Name
AdminVM-01

Operating System
Windows Server 2019 Version 1803 build 17763

IPv4 Addresses
10.0.0.4/24

Health

Resource

Machine properties

Default IPv4 Gateway
10.0.0.1

IPv6 Addresses
fe80::c8c:adae:74c5:ba65

Mac Addresses
00:22:48:24:02:29

DNS Names
AdminVM-01

Last Boot Time
2022-05-04T13:48:53.508Z

CPUs
2 @ 2594 MHz

Physcial Memory
8190 MB

Virtualization State
virtual

VM Type
hyperv

Dependency Agent Version
9.10.13

AdminVM-01
Machine Alerts

Properties Log Events Alerts Connections Changes

Only alerts with signal type = Resource are displayed.

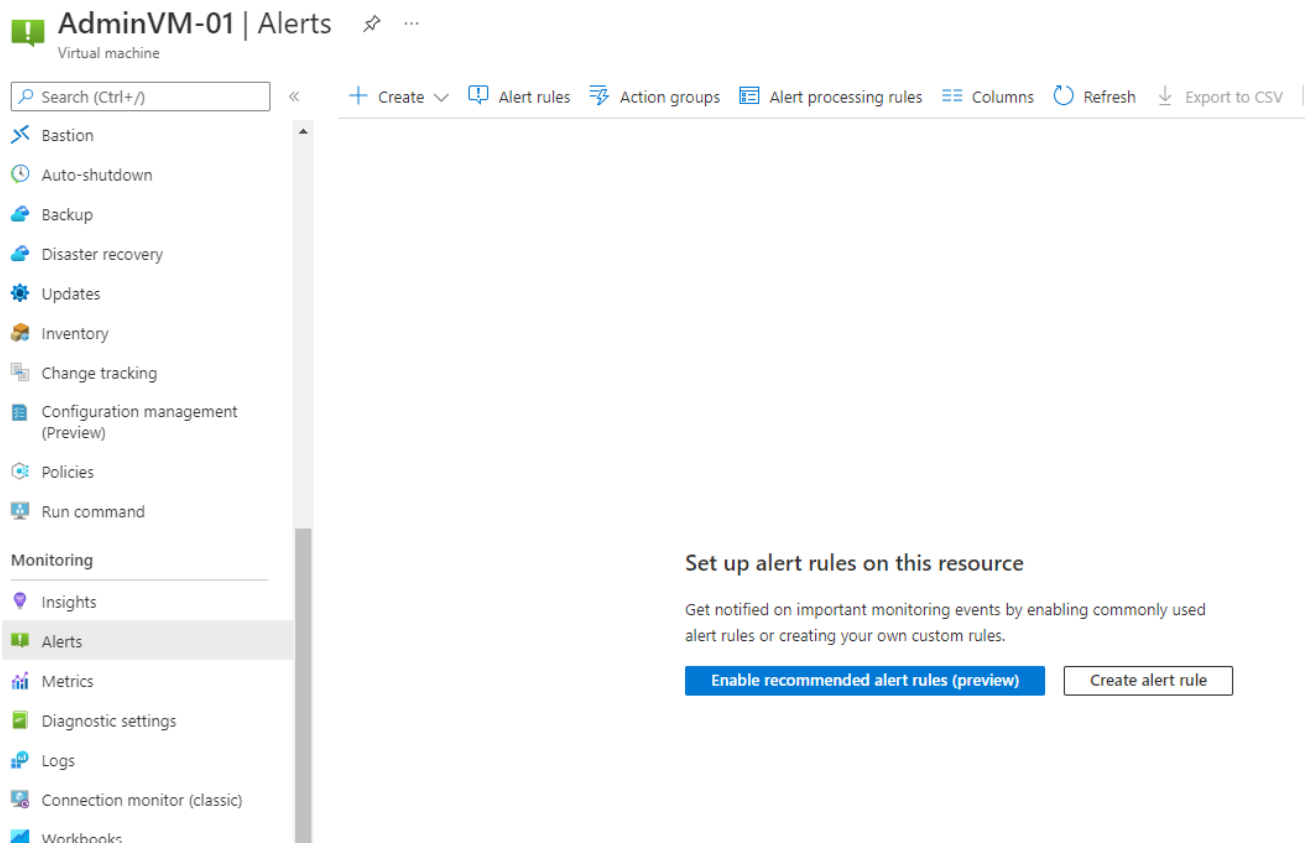
Total alerts
0

Fired Alerts By Severity

SEVERITY	COUNT
Sev 0	0
Sev 1	0
Sev 2	0
Sev 3	0
Sev 4	0

Investigate Alerts

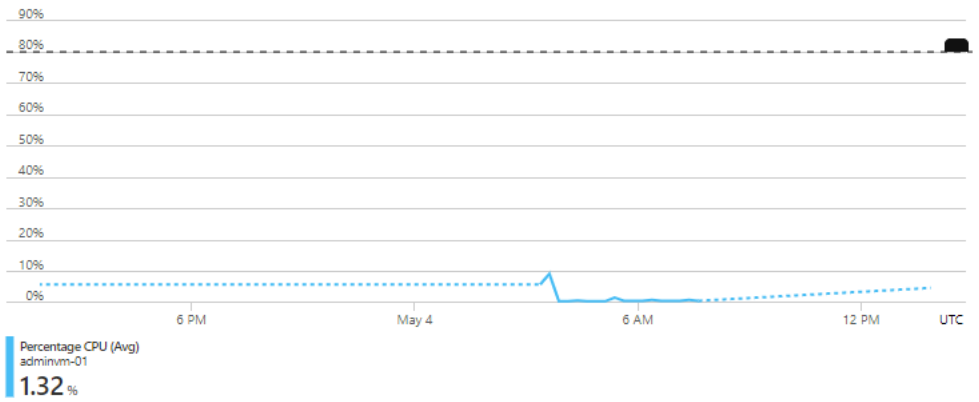
4. Lab 4: Configure VM Alerts



Enable recommended alert rules (preview)

Alert me if

Percentage CPU is greater than 80 %



Alert rule name * Percentage CPU - AdminVM-01

Severity 0 - Critical

Threshold type Static Dynamic

Available Memory Bytes is less than 1 GB

Data Disk IOPS Consumed Percentage is greater than 95 %

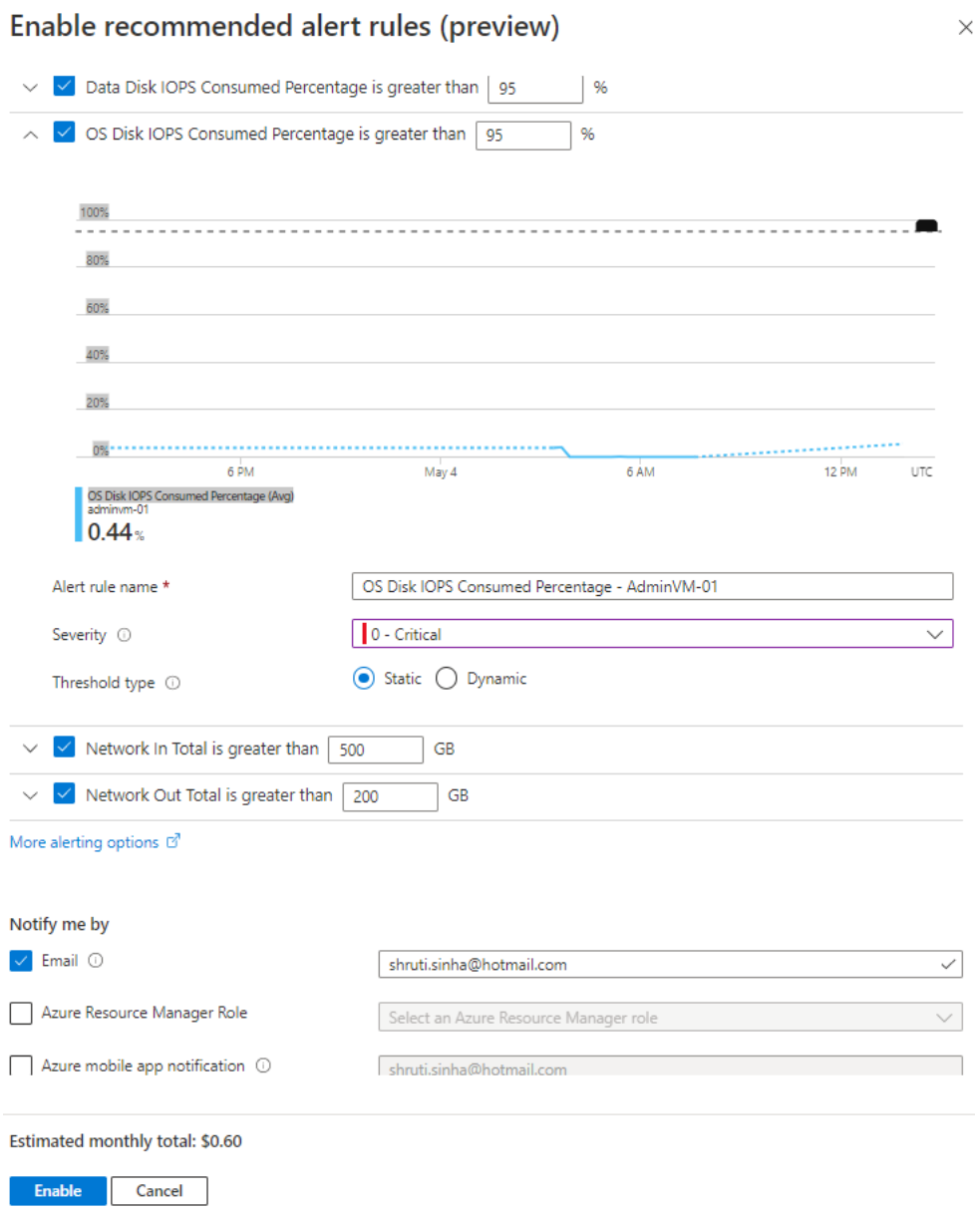
OS Disk IOPS Consumed Percentage is greater than 95 %

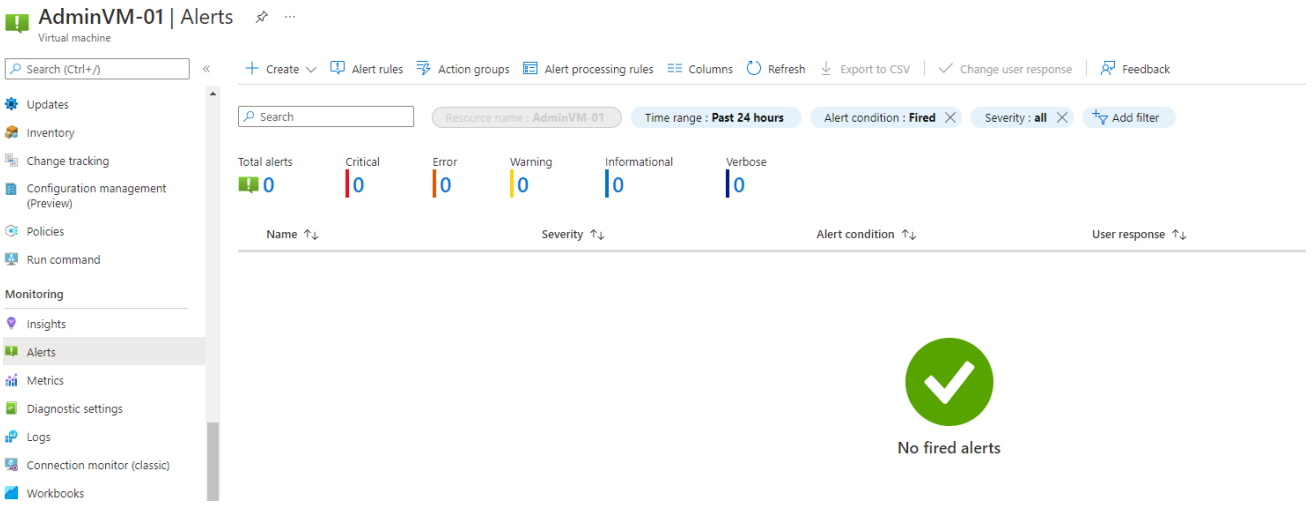
Network In Total is greater than 500 GB

Network Out Total is greater than 200 GB

Estimated monthly total: $0.60

Enable Cancel





5. Lab 5: Enable diagnostics on a virtual machine created using the Azure Portal

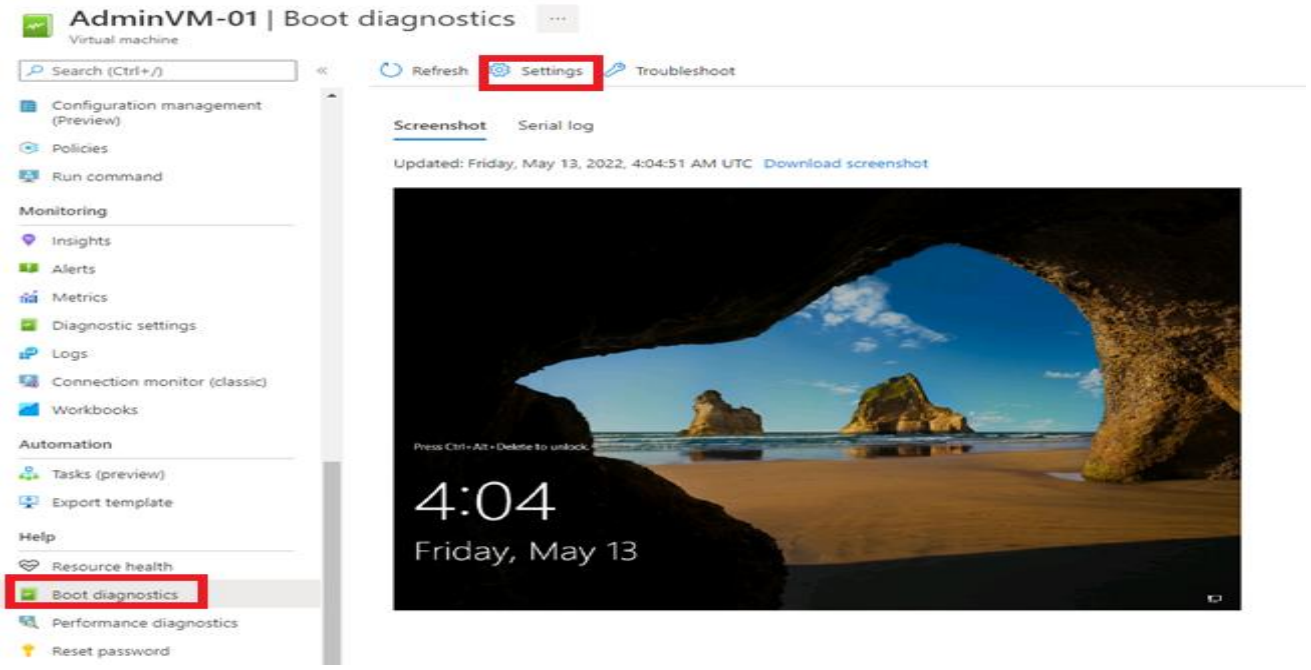
There can be many reasons that a virtual machine enters a non-bootable state.

To address issues with your virtual machines created using Resource Manager Deployment model, you can use the following debugging features for Azure virtual machines.

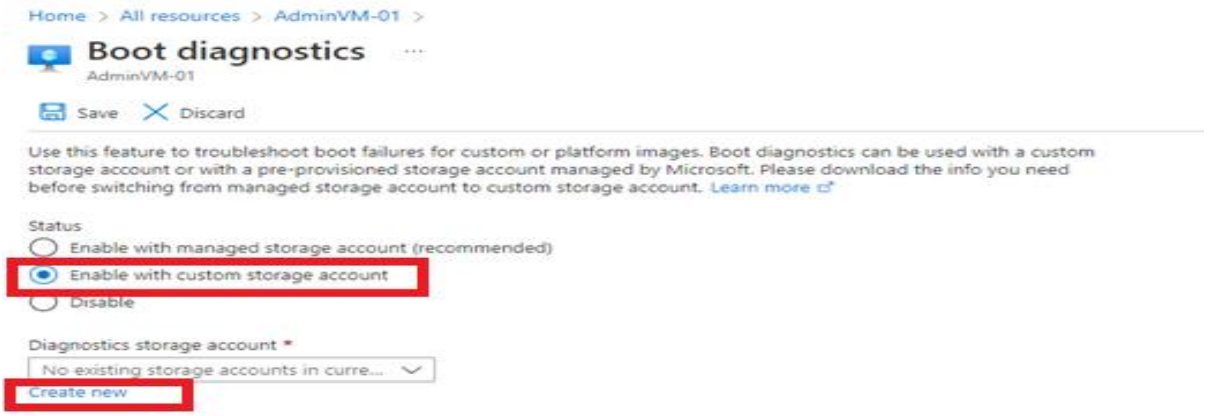
Console Output

Screenshot support

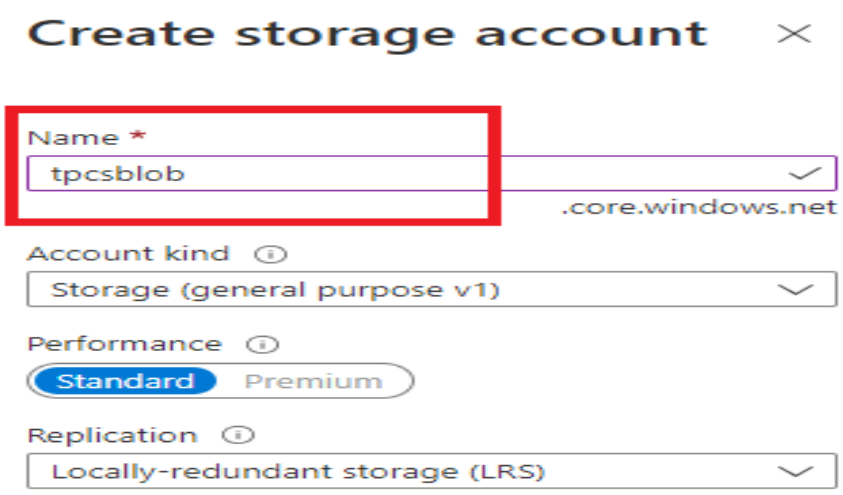
1. Sign in to the Azure portal, and then select the virtual machine.
2. In the **Support + troubleshooting** section, select **Boot diagnostics**,
3. Then select the **Settings** tab.



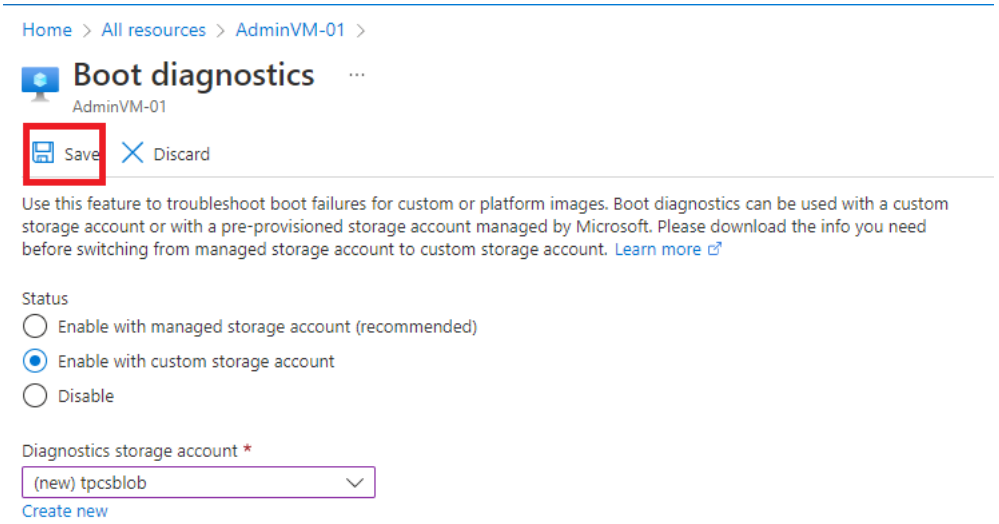
4. In **Boot diagnostics** settings, select **Enable with Custom Storage Account**
5. In Diagnostic Storage Account Click **Create New**



6. Type the Name of Storage Account to be created (Name should be in small letter and globally unique) and click **OK**



7. Click **Save**

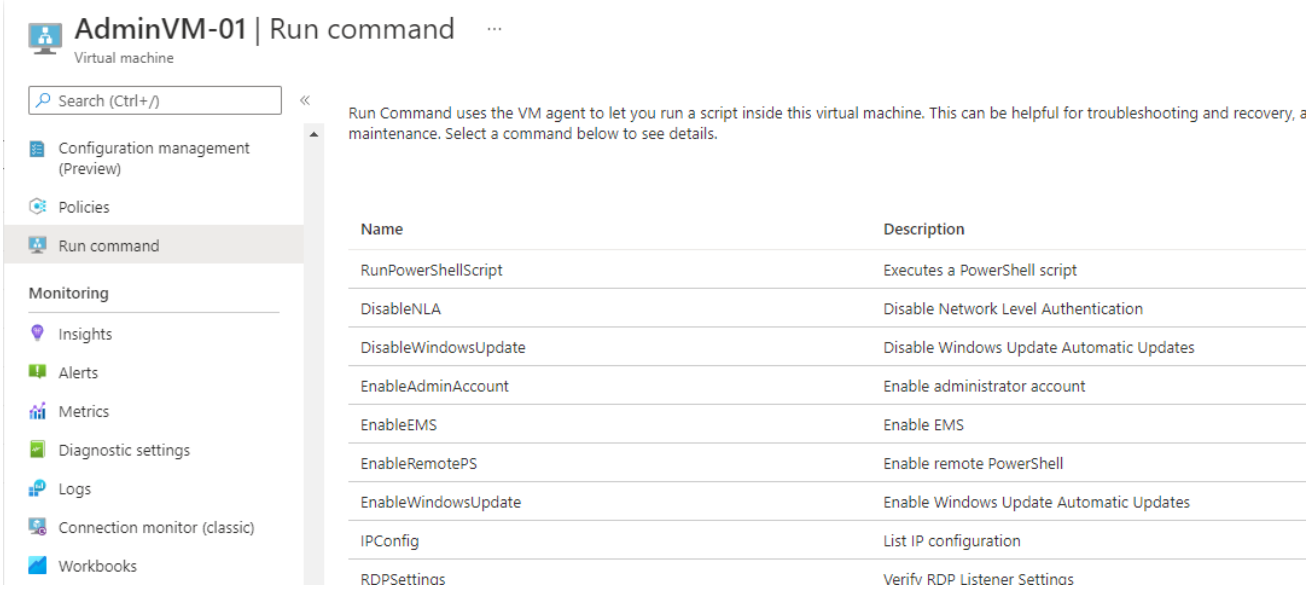


6. Lab 6: Serial Console for Virtual Machines

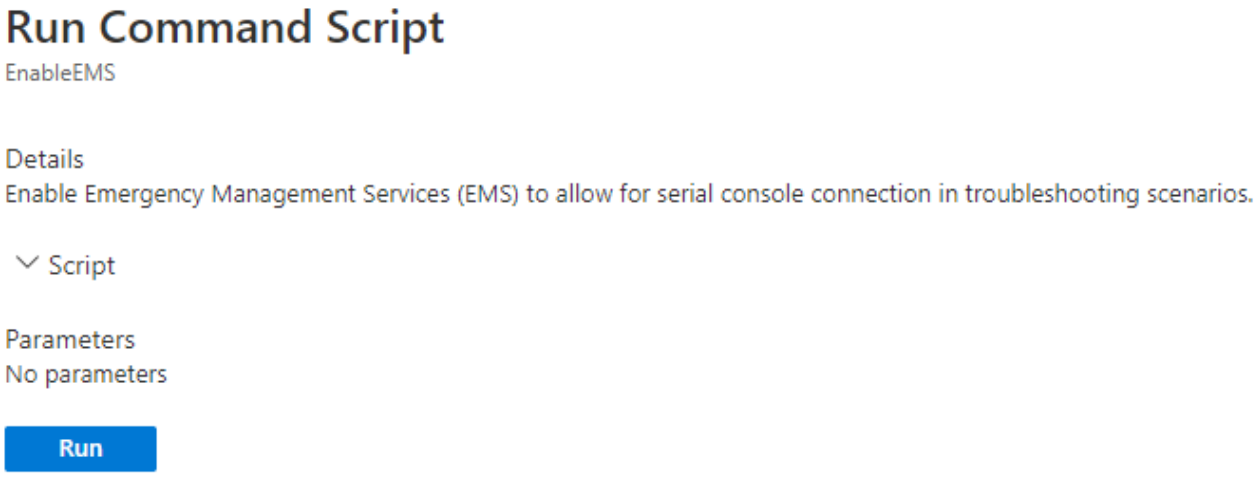
- ✓ The Serial Console in the Azure portal provides access to a text-based console for virtual machines (VMs) running either Linux or Windows.
- ✓ This serial connection connects to the **ttyS0 or COM1** serial port of the VM providing access independent of the network or operating system state.
- ✓ The serial console can only be accessed by using the Azure portal

7.1 Enable Serial Console functionality for Windows Server

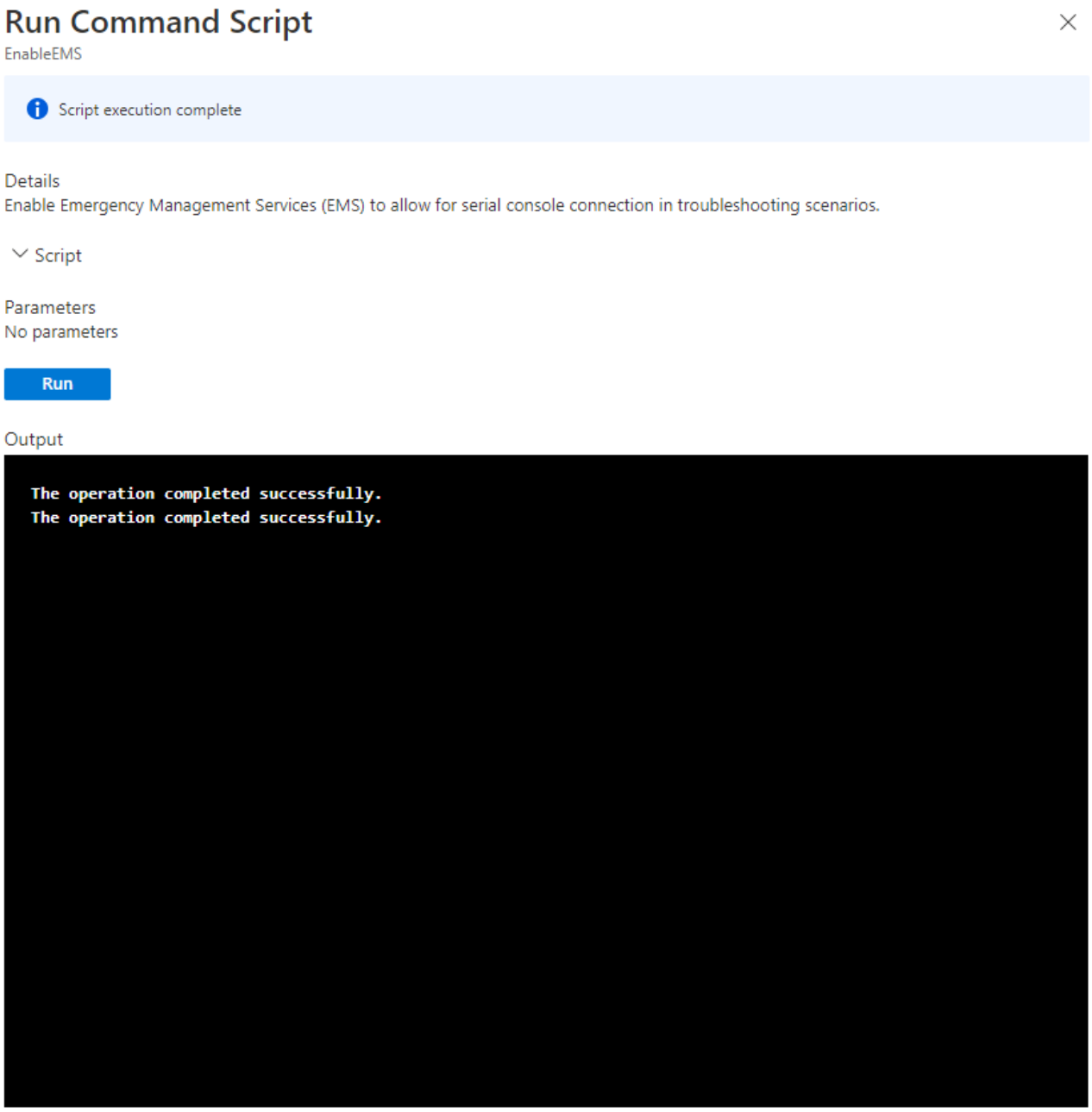
2. Enable SAC **(Special Administrative Console)**



3. **Click Run**

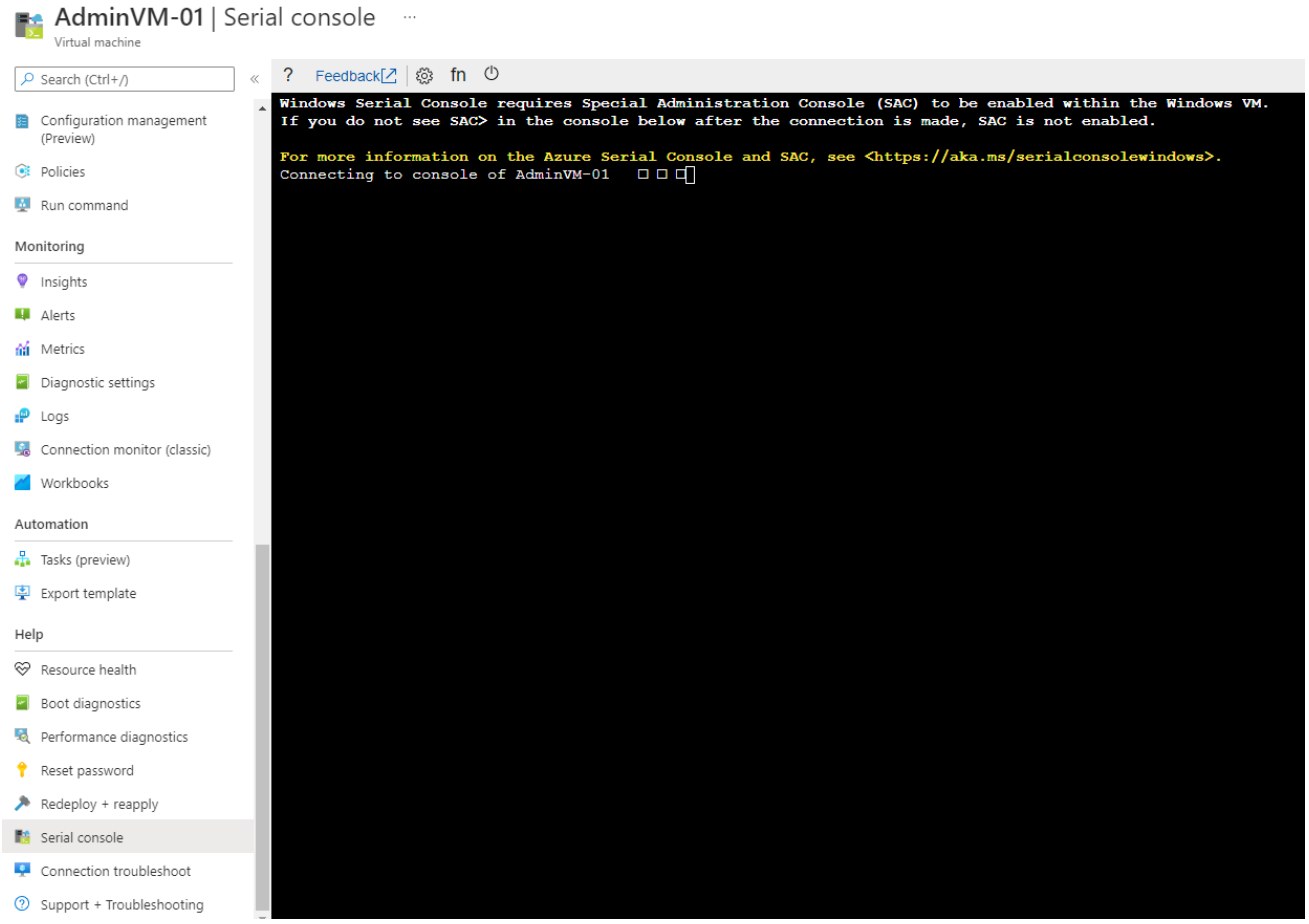


4. **You should see following output**

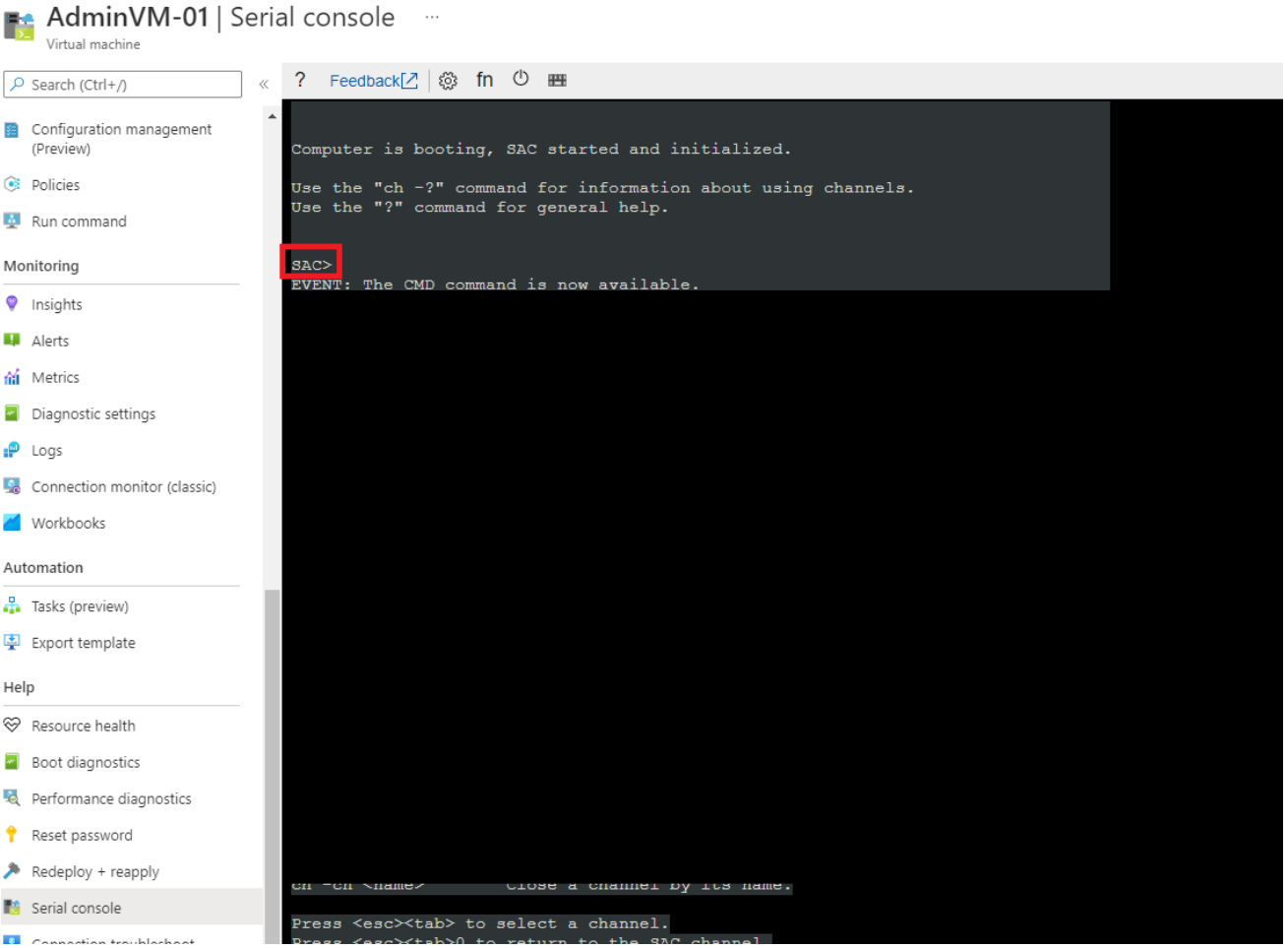


7.2 Launch Serial Console for Windows Server

1. The overview page for the VM opens.
2. Scroll down to the **Help** section and select **Serial console**. A new pane with the serial console opens and starts the connection.



3. Connect to the serial console. If you successfully connect, the prompt is **SAC**>:



4. Once SAC is open we can use **CMD** command to create CMD channel.

```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0002
SAC>ch
```

5. Then run **ch -si 1** to connect to the channel.

```
SAC>ch -si 1
SAC>
```

6. Then CMD channel will appear

```
Name:                   Cmd0002
Description:            Command
Type:                   VT-UTF8
Channel GUID:           288b58ef-d271-11ec-9622-002248240229
Application Type GUID:  63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

7. Press **enter** to continue and then it will ask for user name and password for the VM. (Leave domain Name Blank)

```
Please enter login credentials.
Username: vmadmin
Domain  :
Password: ************
```

8. Once session is authenticated, it will open the command prompt.

```
? Feedback fn
Microsoft Windows [Version 10.0.17763.2803]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

7.3 Launch Serial Console for Windows Server

1. Verify RDP is enabled

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections

reg query "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v
fDenyTSConnections
```

The second key (under \Policies) will only exist if the relevant group policy setting is configured.

```
C:\Windows\system32>reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Se
rver" /v fDenyTSConnections

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
    fDenyTSConnections    REG_DWORD    0x0


C:\Windows\system32>
```

2. View service state

sc query termservice

```
C:\Windows\system32>sc qc termservice
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: termservice
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\System32\svchost.exe -k termsvcs
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Remote Desktop Services
        DEPENDENCIES       : RPCSS
        SERVICE_START_NAME : NT Authority\NetworkService
```

3. Stop service

net stop termservice

```
C:\Windows\system32>net stop termservice
The following services are dependent on the Remote Desktop Services service.
Stopping the Remote Desktop Services service will also stop these services.

   Remote Desktop Services UserMode Port Redirector

Do you want to continue this operation? (Y/N) [N]: y
The Remote Desktop Services UserMode Port Redirector service is stopping.
The Remote Desktop Services UserMode Port Redirector service was stopped success
fully.

The Remote Desktop Services service is stopping.
The Remote Desktop Services service was stopped successfully.
```

4. Start service

net start termservice

```
C:\Windows\system32>net start termservice
The Remote Desktop Services service is starting.
The Remote Desktop Services service was started successfully.
```

7.4 Manage Networking Features using CMD

1. Show NIC properties

netsh interface show interface

```
C:\Windows\system32>netsh interface show interface

Admin State    State          Type             Interface Name
-------------------------------------------------------------------------
Enabled        Connected      Dedicated        Ethernet
```

2. Show IP properties

netsh interface ip show config

```
C:\Windows\system32>netsh interface ip show config

Configuration for interface "Ethernet"
    DHCP enabled:                         Yes
    IP Address:                           10.0.0.4
    Subnet Prefix:                        10.0.0.0/24 (mask 255.255.255.0)
    Default Gateway:                      10.0.0.1
    Gateway Metric:                       0
    InterfaceMetric:                      10
    DNS servers configured through DHCP:  168.63.129.16
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Loopback Pseudo-Interface 1"
    DHCP enabled:                         Yes
    IP Address:                           127.0.0.1
    Subnet Prefix:                        127.0.0.0/8 (mask 255.0.0.0)
    InterfaceMetric:                      75
    DNS servers configured through DHCP:  None
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None
```

3. Ping to google

ping 8.8.8.8

```
C:\Windows\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time<1ms TTL=56
Reply from 8.8.8.8: bytes=32 time<1ms TTL=56
Reply from 8.8.8.8: bytes=32 time<1ms TTL=56
Reply from 8.8.8.8: bytes=32 time=1ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

4. Test DNS name resolution

nslookup bing.com

```
C:\Windows\system32>nslookup bing.com
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    bing.com
Addresses:  2620:1ec:c11::200
          204.79.197.200
          13.107.21.200
```

5. Disable Windows Firewall

netsh advfirewall set allprofiles state off

```
C:\Windows\system32>netsh advfirewall set allprofiles state off
Ok.
```

7.5 *Manage Users and Groups using CMD*

1. Create local user account

net user /add demoadmin Password@123

```
C:\Windows\system32>net user /add demoadmin Password@123
The command completed successfully.
```

2. Add local user to local group

net localgroup Administrators demoadmin /add

```
C:\Windows\system32>net localgroup Administrators demoadmin /add
The command completed successfully.
```

3. Verify user account is enabled

net user demoadmin | find /i "active"

```
C:\Windows\system32>net user demoadmin | find /i "active"
Account active               Yes
```

4. View local groups

net localgroup

```
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Storage Replica Administrators
*System Managed Accounts Group
*Users
The command completed successfully.
```

7.6 File System Management using CMD

1. Scan for system file corruption

sfc /scannow

```
C:\Windows\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 12% complete.
```