



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	3
2.	Lab 2: Enable Diagnostic Setting	4
3.	Lab 3: Enable Insight.....	8
4.	Lab 4: Configure VM Alerts.....	13
5.	Lab 5: Enable diagnostics on a virtual machine created using the Azure Portal.....	15
6.	Lab 6: Serial Console for Virtual Machines	17
7.1	Enable Serial Console functionality for Windows Server	17
7.2	Launch Serial Console for Windows Server	19
7.3	Launch Serial Console for Windows Server	22
1.	Verify RDP is enabled	22
2.	View service state	22
3.	Stop service.....	22
4.	Start service.....	23
7.4	Manage Networking Features using CMD.....	23
7.5	Manage Users and Groups using CMD.....	24
7.6	File System Management using CMD.....	25
1.	Scan for system file corruption	25

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**

Home > Virtual machines >

Virtual machines

Default Directory (shrutisinhahotmail.onmicrosoft...)

[+ Create](#) [Switch to classic](#) ...

Filter for any field...

Name ↑ Type ↑

No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

[Learn more about Windows virtual machines](#) [Learn more about Linux virtual machines](#)

Create a virtual machine

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Availability zone *

☒ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type

Image * [See all images](#) [Configure VM generation](#)

Azure Spot instance ☐

Size * [See all sizes](#)

Administrator account

Username *

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ☐ None ☒ Allow selected ports

Select inbound ports * [Open Port 80 , 3389](#)

[Review + create](#) [< Previous](#) [Next : Disks >](#)

5. Click Review and Create

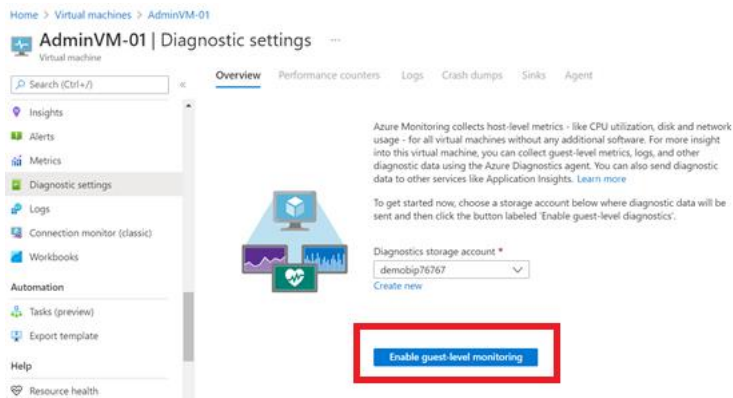
2. Lab 2: Enable Diagnostic Setting

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:

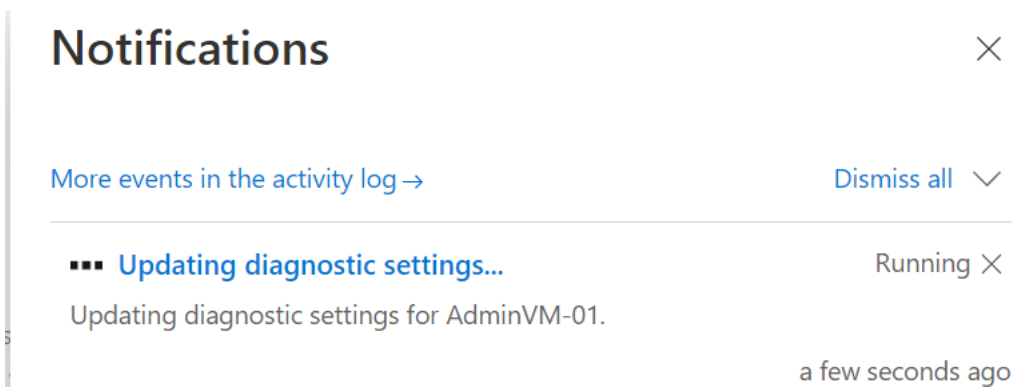
- Collect guest metrics into Azure Monitor Metrics.
- Send guest logs and metrics to Azure storage for archiving.
- Send guest logs and metrics to Azure event hubs to send outside of Azure.

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.



AdminVM-01 | Diagnostic settings

Virtual machine

- Insights
- Alerts
- Metrics
- Diagnostic settings**
- Logs
- Connection monitor (classic)
- Workbooks

Automation

- Tasks (preview)
- Export template

Help

- Resource health

Overview

Performance counters

Logs

Crash dumps

Sinks

Agent

Performance counters

Collecting data for these counters:

- CPU
- Memory
- Disk
- Network

[Configure performance counters](#)

Event logs

Collecting data for these logs:

- Application: Critical, Error, Warning
- Security: Audit failure
- System: Critical, Error, Warning

[Configure event logs](#)

Directories

Not configured.

[Configure directories](#)

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.



AdminVM-01 | Diagnostic settings

Virtual machine

- Insights
- Alerts
- Metrics
- Diagnostic settings**
- Logs
- Connection monitor (classic)
- Workbooks

Automation

- Tasks (preview)
- Export template

Help

- Resource health

Overview

Performance counters

Logs

Crash dumps

Sinks

Agent

Choose **Basic** to enable the collection of performance counters. Choose **Custom** if you want more control over which performance counters are collected.

None **Basic** **Custom**

Configure the performance counters to collect, and how often they should be sampled:

Performance counter		Sample rate (seconds)	Unit
<input checked="" type="checkbox"/>	\Processor Information(_Total)\% Processor Time	50	Percent
<input checked="" type="checkbox"/>	\Processor Information(_Total)\% Privileged Time	60	Percent
<input checked="" type="checkbox"/>	\Processor Information(_Total)\% User Time	60	Percent
<input checked="" type="checkbox"/>	\Processor Information(_Total)\Processor Frequency	60	Count
<input checked="" type="checkbox"/>	\System\Processes	60	Count
<input checked="" type="checkbox"/>	\Process(_Total)\Thread Count	60	Count
<input checked="" type="checkbox"/>	\Process(_Total)\Handle Count	60	Count

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.

AdminVM-01 | Diagnostic settings ...

Virtual machine

Search (Ctrl+ /)

Save Discard

Overview Performance counters **Logs** Crash dumps Sinks Agent

Event logs

Choose **Basic** to enable collection of event logs. Choose **Custom** if you want more control over which event logs are collected.

None Basic Custom

Configure the event logs and levels to collect:

Application

- ☒ Critical
- ☒ Error
- ☒ Warning
- ☐ Information
- ☐ Verbose

Security

- ☐ Audit success
- ☒ Audit failure

System

- ☒ Critical
- ☒ Error
- ☒ Warning
- ☐ Information

Insights

Alerts

Metrics

Diagnostic settings

Logs

Connection monitor (classic)

Workbooks

Automation

Tasks (preview)

Export template

Help

Resource health

Boot diagnostics

Performance diagnostics

Reset password

Redeploy + reapply

Serial console

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.

Save Discard

Overview Performance counters Logs **Crash dumps** Sinks Agent

Collect memory dumps when a process crashes. If no processes have been specified, this will do nothing.

Disabled Enabled

Configure the processes to monitor:

Add

Process

No processes.

Storage container name: *

Crash dumps type:

Mini

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

Save Discard

Overview Performance counters Logs Crash dumps Sinks **Agent**

Configure additional options for the Azure Diagnostics agent.

Storage account *
telemetryguestdiag

Disk quota (MB): ①
5120

Diagnostic infrastructure logs: ①
Disabled Enabled

Log level: ①
Error

Remove Azure Diagnostics agent

If diagnostic data isn't being collected or you're having trouble viewing it in the portal, reinstalling the agent might help.

This removes the agent, but keeps all existing diagnostic data in your storage account. After the agent is removed, you can re-enable diagnostics for this virtual machine.

Remove

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.

- Bastion
- Auto-shutdown
- Backup
- Disaster recovery
- Updates
- Inventory
- Change tracking
- Configuration management (Preview)
- Policies
- Run command
- Monitoring
 - Insights
 - Alerts
 - Metrics
 - Diagnostic settings
 - Logs
 - Connection monitor (classic)
 - Workbooks
- Automation
 - Tasks (preview)
 - Export template

Get more visibility into the health and performance of your virtual machine

With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into dependencies for your virtual machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the virtual machine and the mo



i The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please [click here](#).

Enable

! Having difficulties enabling Azure Monitors for VM? [Troubleshoot](#)

Have more questions?

[Learn more about virtual machine monitoring](#) [↗](#)
[What is VM Insights?](#) [↗](#)
[Learn more about pricing](#) [↗](#)
[Support Matrix](#) [↗](#)
[FAQ](#) [↗](#)

✓ It by default create a Log Analytics workspace

Get more visibility into the health and performance of your virtual machine

With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance and dependencies for your virtual machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the virtual machine and the monitoring data to appear.



The VM is not connected to any workspace. Please select the monitoring workspace where you will store your data

Workspace Subscription * ⓘ

Visual Studio Enterprise Subscription

Choose a Log Analytics Workspace ⓘ

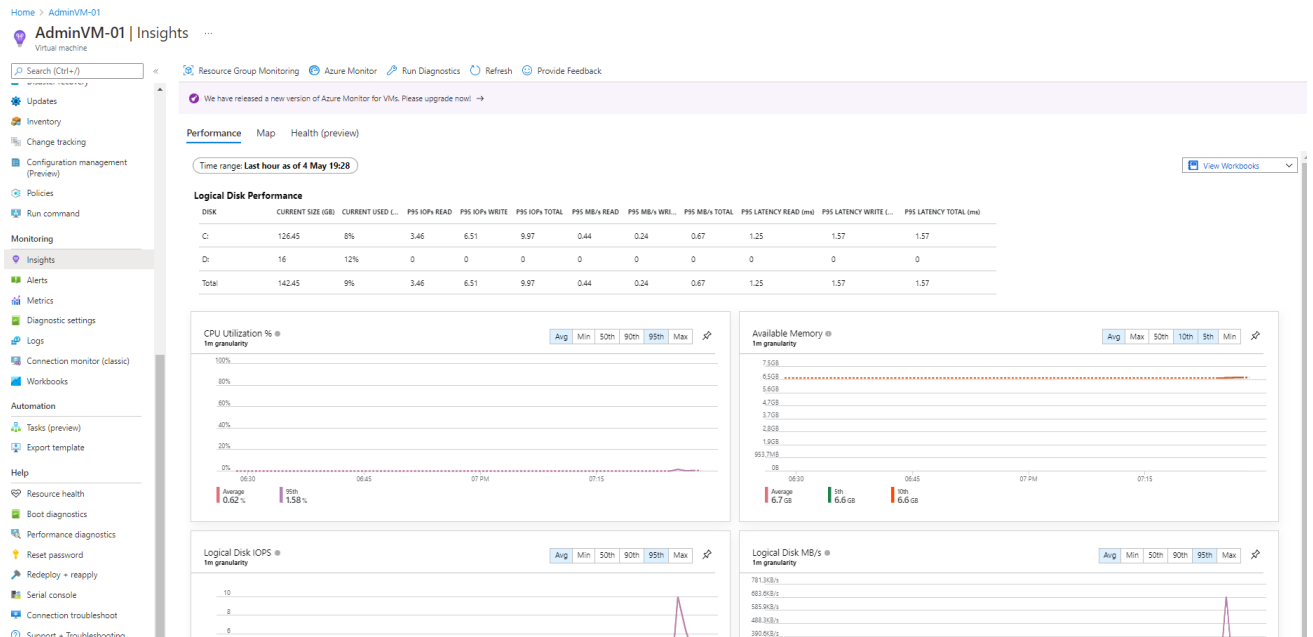
(new) DefaultWorkspace-463fbf22-369d-445d-b8c3-c9dbb477ee76-EUS [eastus]

Note: If the virtual machine already has either SCOM or OMS agent installed locally, the Microsoft Monitoring Agent (MMA) extension will still be installed and connected to the configured workspace.

i The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please [click here](#).

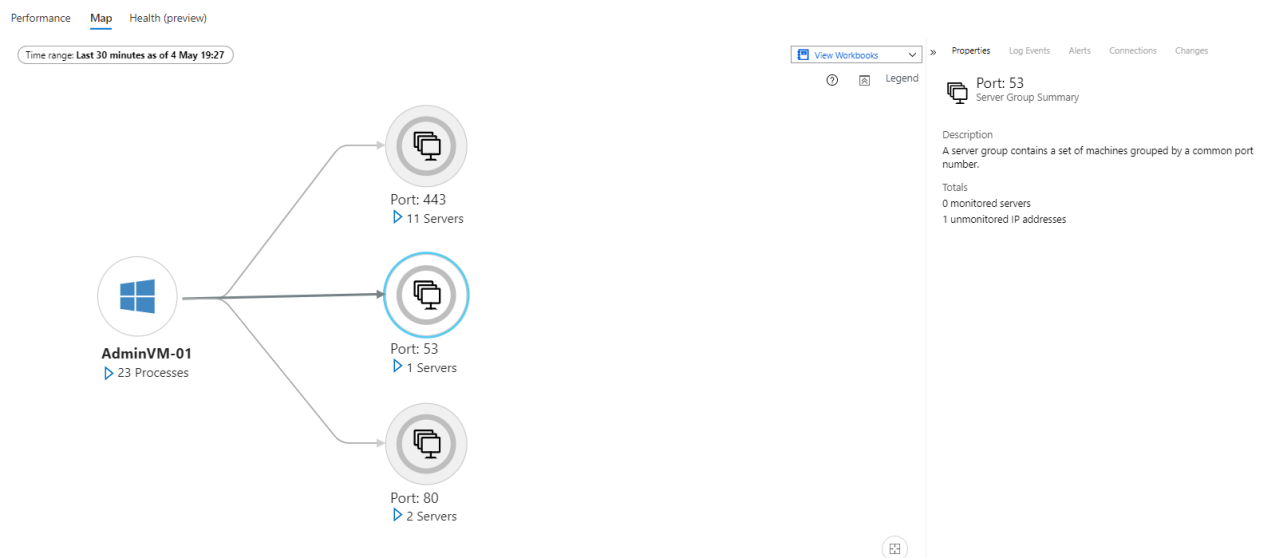
Enable

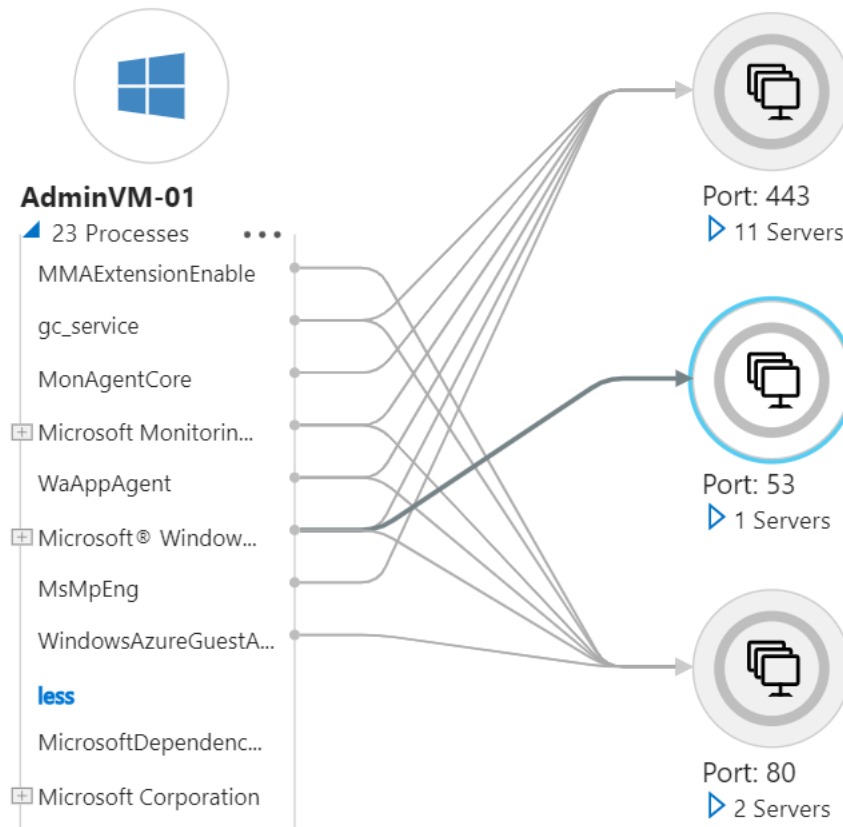
✓ You will receive status messages as the configuration is performed.



✓ 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

Resource Group Monitoring Azure Monitor Run Diagnostics Refresh Provide Feedback

We have released a new version of Azure Monitor for VMs. Please upgrade now! →

Time range: Last 30 minutes as of 4 May 19:27

View Workbooks Legend

AdminVM-01
 23 Processes

Port: 443
 11 Servers

Port: 53
 1 Servers

Port: 80
 2 Servers

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:nc8ca0ae:74c5ba65

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

DNS Names
 AdminVM-01

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

CPU
 2 @ 2594 MHz

Physical Memory
 8190 MB

Virtualization State
 virtual

VM Type
 hyperv

Dependency Agent Version
 9.10.13

Log Analytics Agent ID

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::c8cdaae: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

Physical Memory
8190 MB

Virtualization State
virtual

VM Type
hyperv

Dependency Agent Version
9.10.13

»

 AdminVM-01
Machine Alerts








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


 **AdminVM-01** | Alerts  ...


Virtual machine


Search (Ctrl+J)


«


+ Create ▾


 Alert rules

 Action groups

 Alert processing rules

 Columns

 Refresh

 Export to CSV

Bastion

Auto-shutdown

Backup

Disaster recovery

Updates

Inventory

Change tracking

Configuration management (Preview)

Policies

Run command

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Logs

Connection monitor (classic)

Workbooks

Set up alert rules on this resource

Get notified on important monitoring events by enabling commonly used alert rules or creating your own custom rules.

Enable recommended alert rules (preview)

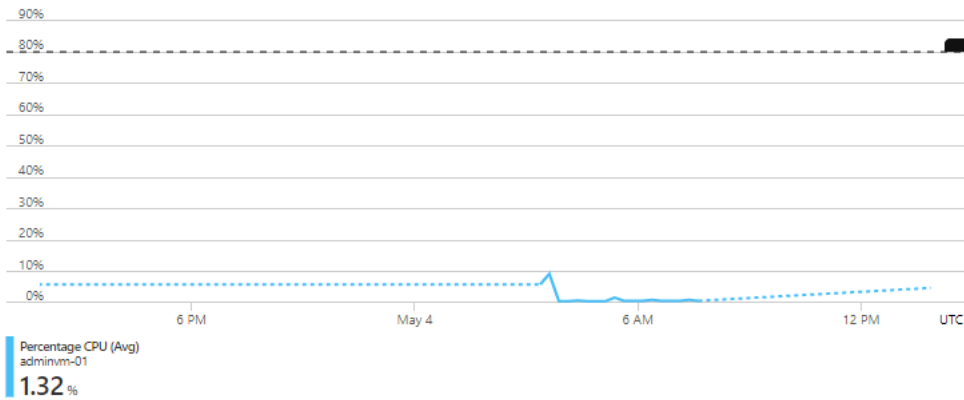
Create alert rule

Enable recommended alert rules (preview)



Alert me if

^ ☒ Percentage CPU is greater than %



Alert rule name *

Percentage CPU - AdminVM-01

Severity ⓘ

0 - Critical

Threshold type ⓘ

☒ Static ☐ Dynamic

v ☒ Available Memory Bytes is less than GB

v ☒ Data Disk IOPS Consumed Percentage is greater than %

v ☒ OS Disk IOPS Consumed Percentage is greater than %

v ☒ Network In Total is greater than GB

v ☒ Network Out Total is greater than GB

Estimated monthly total: \$0.60

Enable

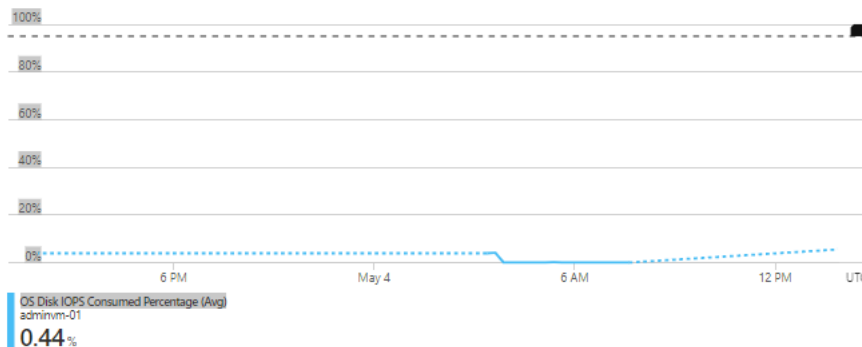
Cancel

Enable recommended alert rules (preview)



✓ ☒ Data Disk IOPS Consumed Percentage is greater than %

^ ☒ OS Disk IOPS Consumed Percentage is greater than %



Alert rule name *

Severity

Threshold type ☒ Static ☐ Dynamic

✓ ☒ Network In Total is greater than GB

✓ ☒ Network Out Total is greater than GB

[More alerting options](#)

Notify me by

☒ Email

☐ Azure Resource Manager Role

☐ Azure mobile app notification

Estimated monthly total: \$0.60

Enable

Cancel

AdminVM-01 | Alerts

Virtual machine

Search (Ctrl+/) << + Create Alert rules Action groups Alert processing rules Columns Refresh Export to CSV Change user response Feedback

Search Resource name: AdminVM-01 Time range: Past 24 hours Alert condition: Fired Severity: all Add filter

Total alerts Critical Error Warning Informational Verbose

0 0 0 0 0 0

Name ↑↓ Severity ↑↓ Alert condition ↑↓ User response ↑↓

No fired alerts

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

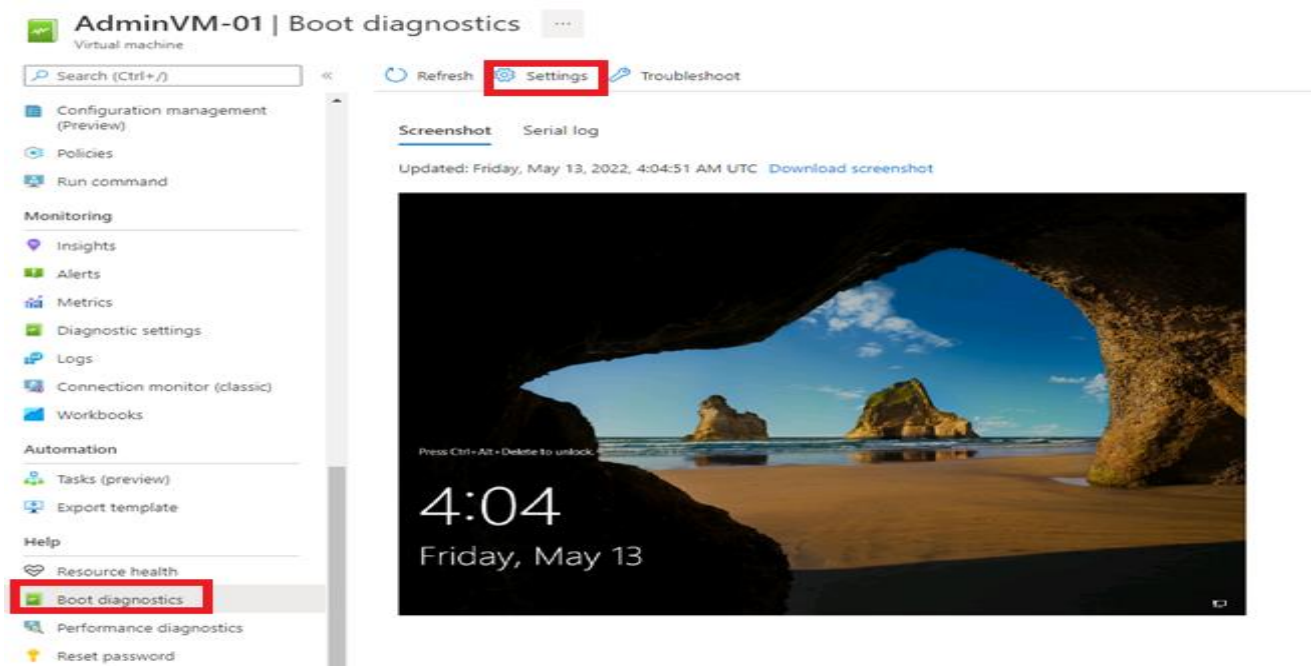
There can be many reasons that a virtual machine enters a non-bootable state.

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

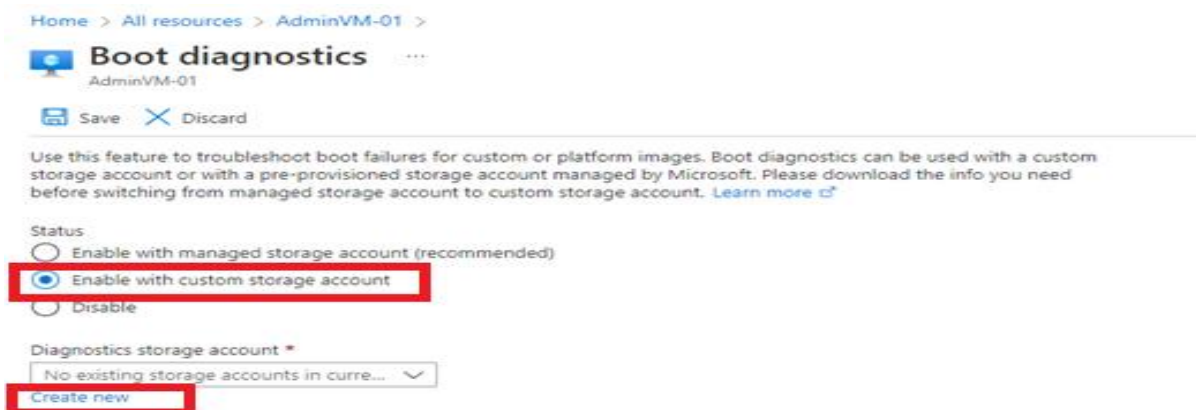
Console Output

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**

Create storage account ×

Name *

tpcsblob

✓

.core.windows.net

Account kind ⓘ
Storage (general purpose v1) ✓

Performance ⓘ
Standard Premium

Replication ⓘ
Locally-redundant storage (LRS) ✓

7. Click **Save**

[Home](#) > [All resources](#) > [AdminVM-01](#) >



Boot diagnostics ...

AdminVM-01



Save



Discard

Use this feature to troubleshoot boot failures for custom or platform images. Boot diagnostics can be used with a custom storage account or with a pre-provisioned storage account managed by Microsoft. Please download the info you need before switching from managed storage account to custom storage account. [Learn more](#)

Status

- ☐ Enable with managed storage account (recommended)
- ☒ Enable with custom storage account
- ☐ Disable

Diagnostics storage account *

(new) tpcsblob ✓

[Create new](#)

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)

AdminVM-01 | Run command

Virtual machine

Search (Ctrl+J)

Configuration management (Preview)

Policies

Run command

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Logs

Connection monitor (classic)

Workbooks

Run Command uses the VM agent to let you run a script inside this virtual machine. This can be helpful for troubleshooting and recovery, a maintenance. Select a command below to see details.

Name	Description
RunPowerShellScript	Executes a PowerShell script
DisableNLA	Disable Network Level Authentication
DisableWindowsUpdate	Disable Windows Update Automatic Updates
EnableAdminAccount	Enable administrator account
EnableEMS	Enable EMS
EnableRemotePS	Enable remote PowerShell
EnableWindowsUpdate	Enable Windows Update Automatic Updates
IPConfig	List IP configuration
RDPSettings	Verify RDP Listener Settings

3. Click Run

Run Command Script

EnableEMS

Details

Enable Emergency Management Services (EMS) to allow for serial console connection in troubleshooting scenarios.

Script

Parameters

No parameters

Run

4. You should see following output

Run Command Script



EnableEMS

 Script execution complete

Details

Enable Emergency Management Services (EMS) to allow for serial console connection in troubleshooting scenarios.

✓ Script

Parameters

No parameters

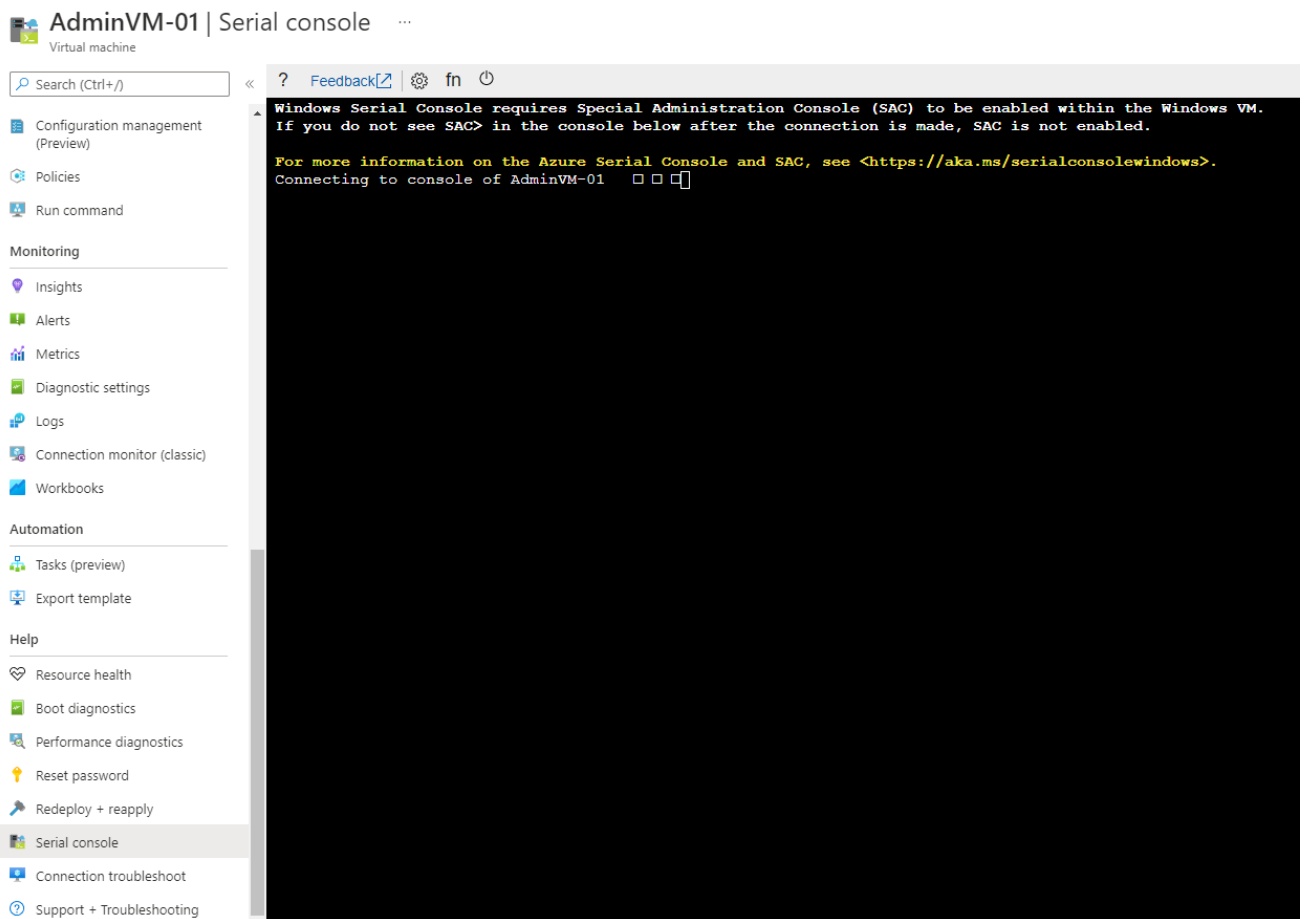
Run

Output

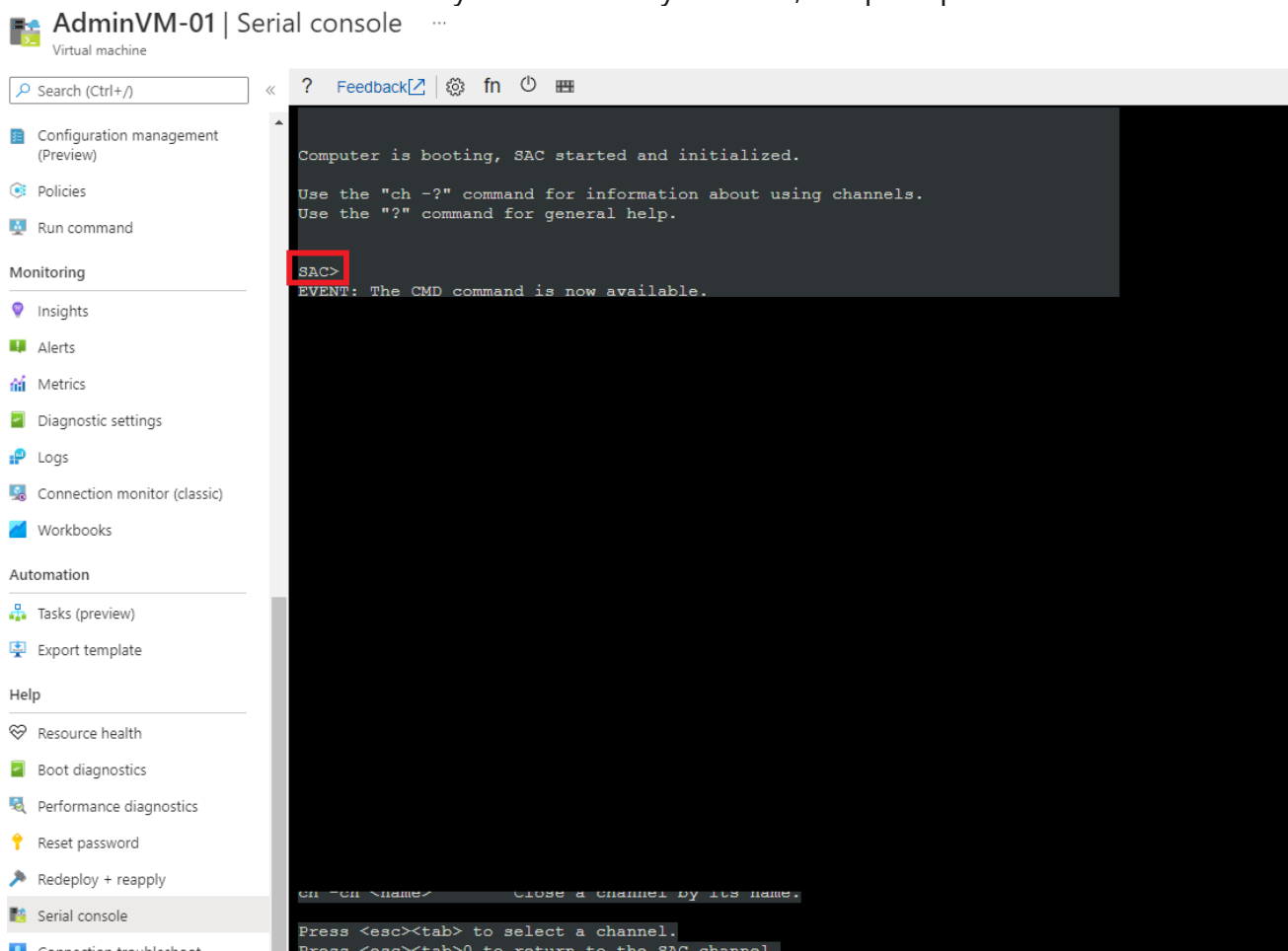
```
The operation completed successfully.  
The operation completed successfully.
```

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 | Settings fn Power
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 termsservice
```

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

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

3. Stop service

```
net stop termsservice
```

```
C:\Windows\system32>net stop termervice
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 successfully.

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

4. Start service

net start termervice

```
C:\Windows\system32>net start termervice
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.█
```