YouTestMe

Installation and Support Manual
for Windows Server

Contents

1 Introduction

YouTestMe GetCertified is a Java-based web application. The Standard Edition requires the following software components to be installed on the Windows Server 2022 host: Java Runtime Environment (JRE), Tomcat application server, and PostgreSQL database.

2 System (Host) Hardware Requirements

Hardware	Typical	Enhanced
CPU	4 vCPU cores	8 vCPU cores
RAM	16 GB	32 GB
Storage (SSD)	128 GB	256 GB (2x128)
Network Connection	Yes	Yes

2.1 Network Bandwidth Requirements

Ensuring optimal network performance is crucial for a seamless and efficient experience on the GetCertified application. This chapter outlines the network requirements for users engaging in basic/lightweight tests.

We recommend a minimum network bandwidth of 1 Mbit/s per user for users participating in lightweight tests. This estimate is based on typical usage scenarios involving text-based questions and minimal multimedia content.

Several factors can influence the network bandwidth required, including the complexity of test content, the frequency of interactions, and the presence of multimedia elements. It's advisable to monitor network usage during peak periods and adjust bandwidth accordingly.

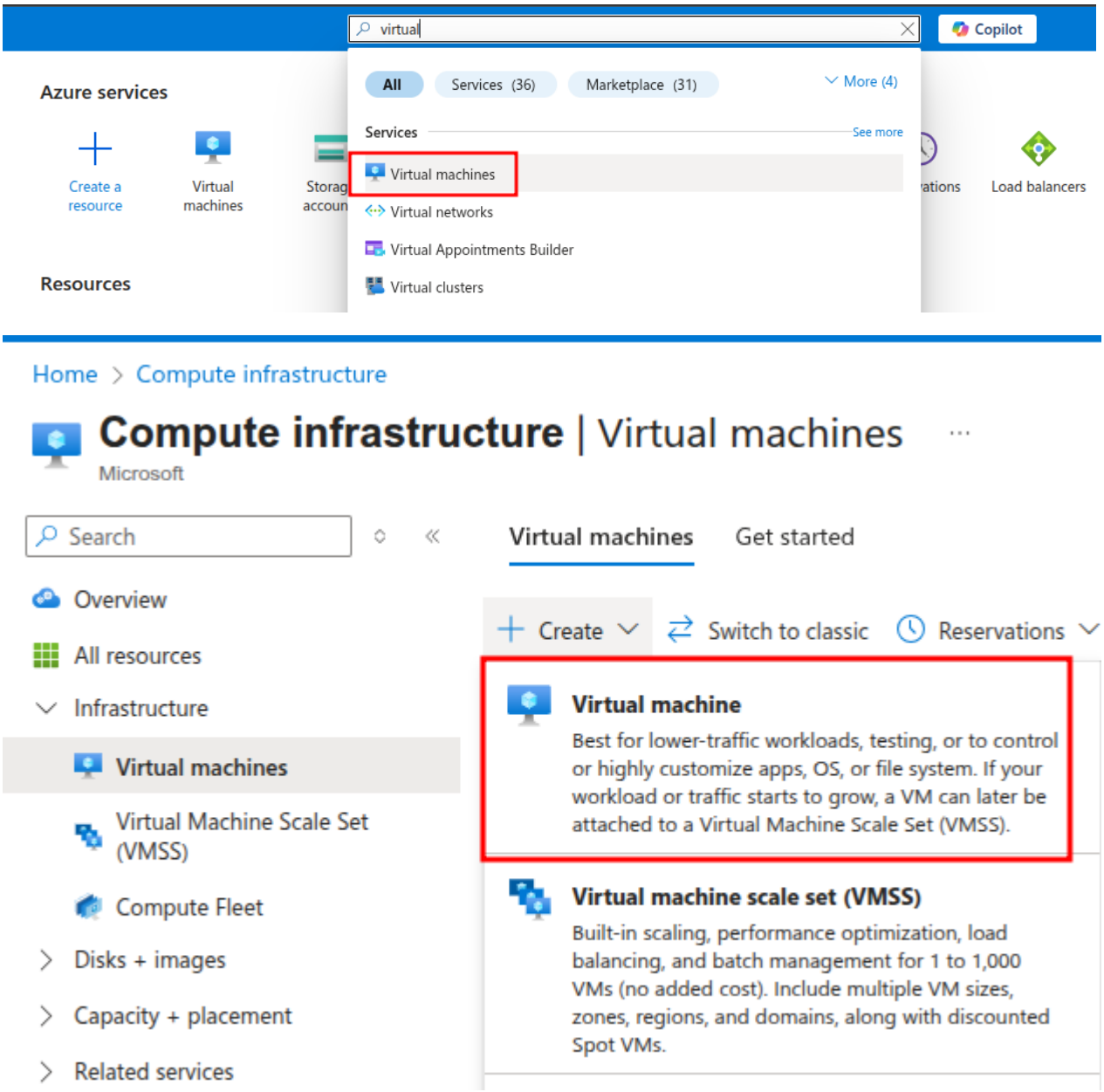
Recommendations for Users:

To ensure an optimal testing experience, we recommend the following:

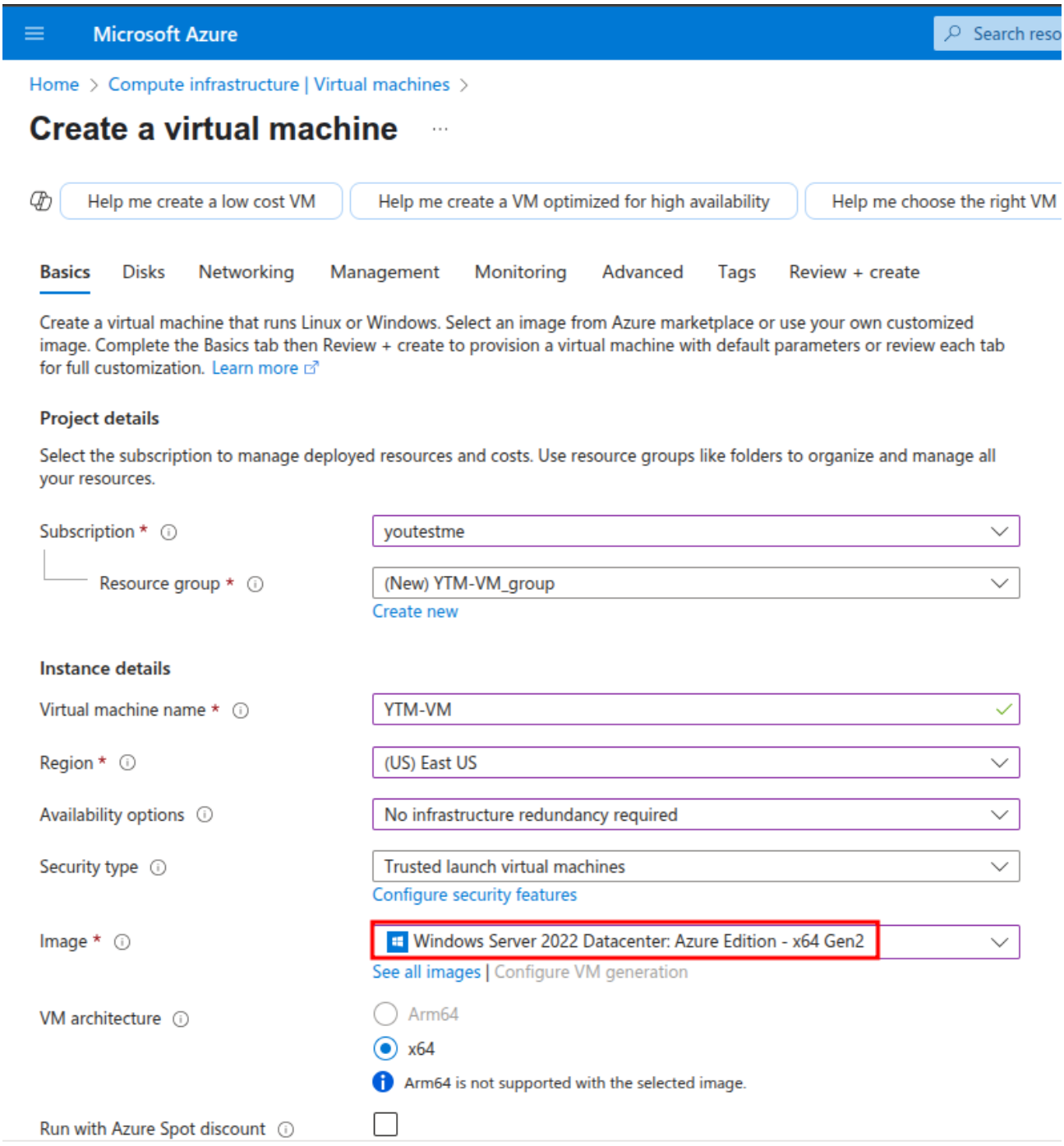
- Stable Internet Connection: Users should connect to a stable and reliable internet connection to minimize disruptions during the testing session.
- Pre-Test Network Check: Before starting a test, users can perform a pre-test network check to ensure their internet connection meets the recommended bandwidth requirements.
- Test Environment Considerations: Consider the test environment, especially for proctoring-enabled tests, and ensure the necessary bandwidth is available for a smooth proctoring experience.

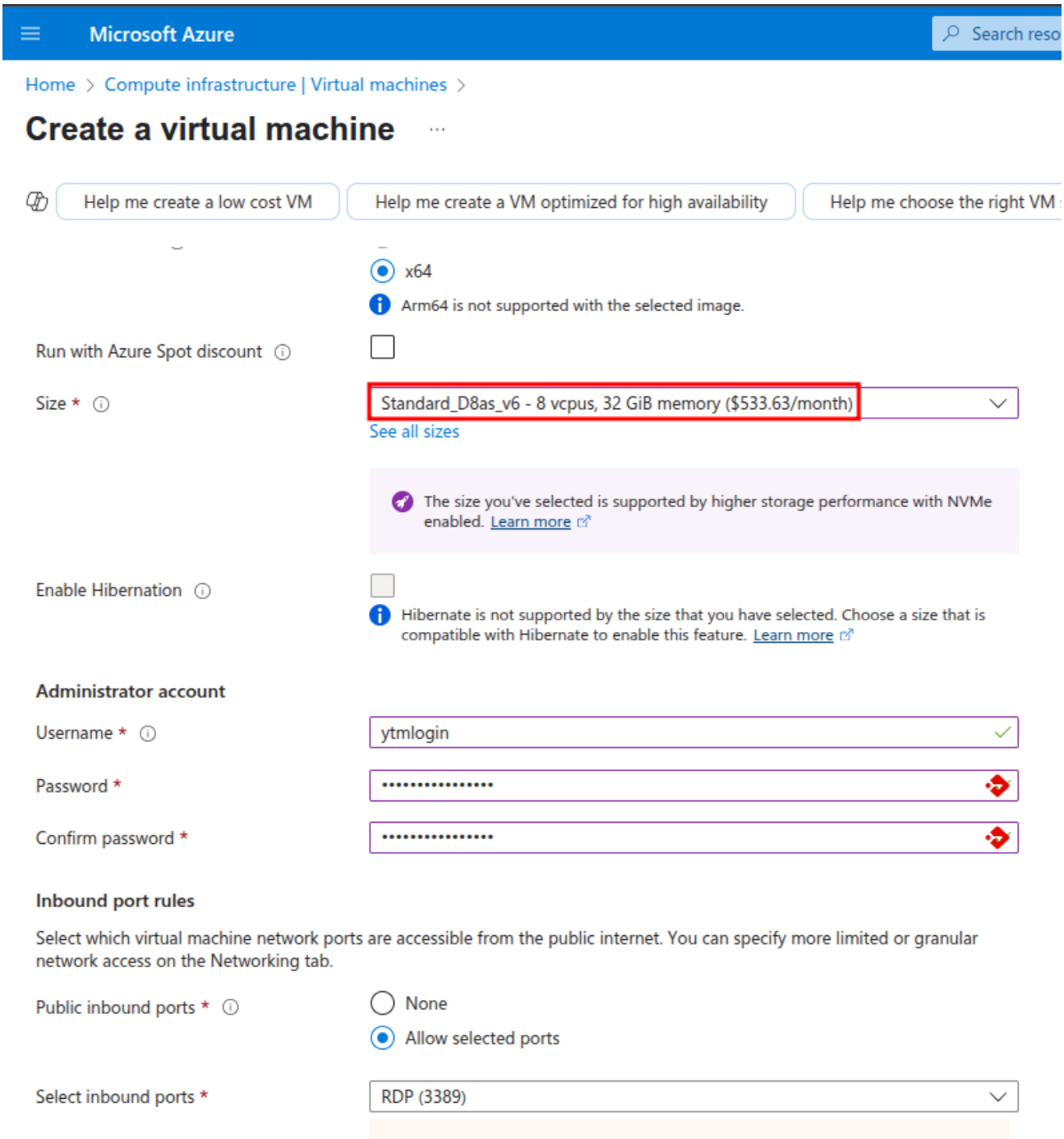
3 Azure Virtual Machine Installation

1. Search for “Virtual machine” in Azure Portal to create a new one:



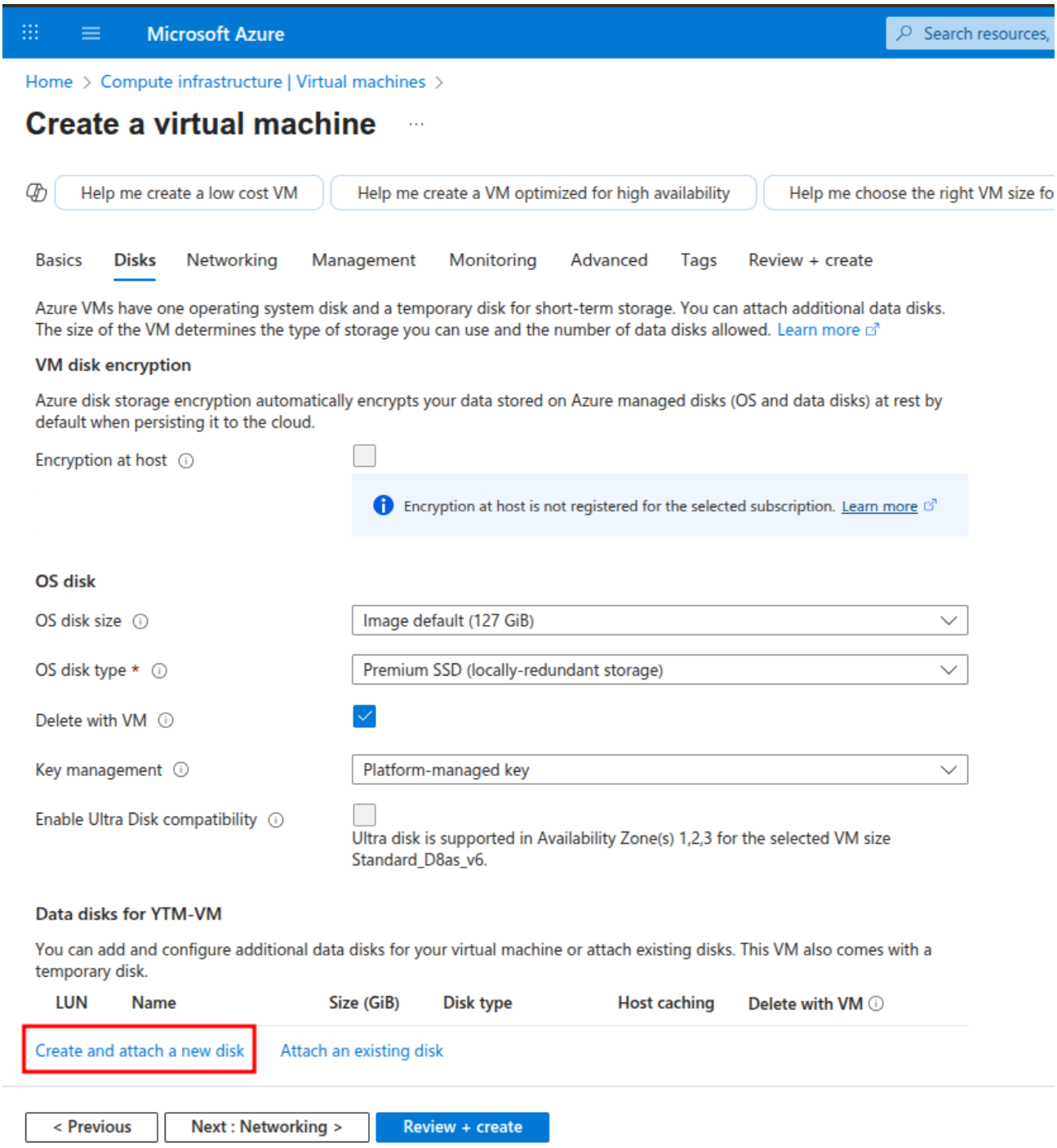
2. Select “Project details” and “Instance details” parameters according to your deployment plan. It is essential to select “Windows Server 2022 Datacenter Azure Edition - x64 Gen2” for the Image type. The recommended hardware configuration is 8 vcpus and 32 GiB RAM, and the most suitable type is “D” - General Purpose. **D8as_v6** or similar will work for you.

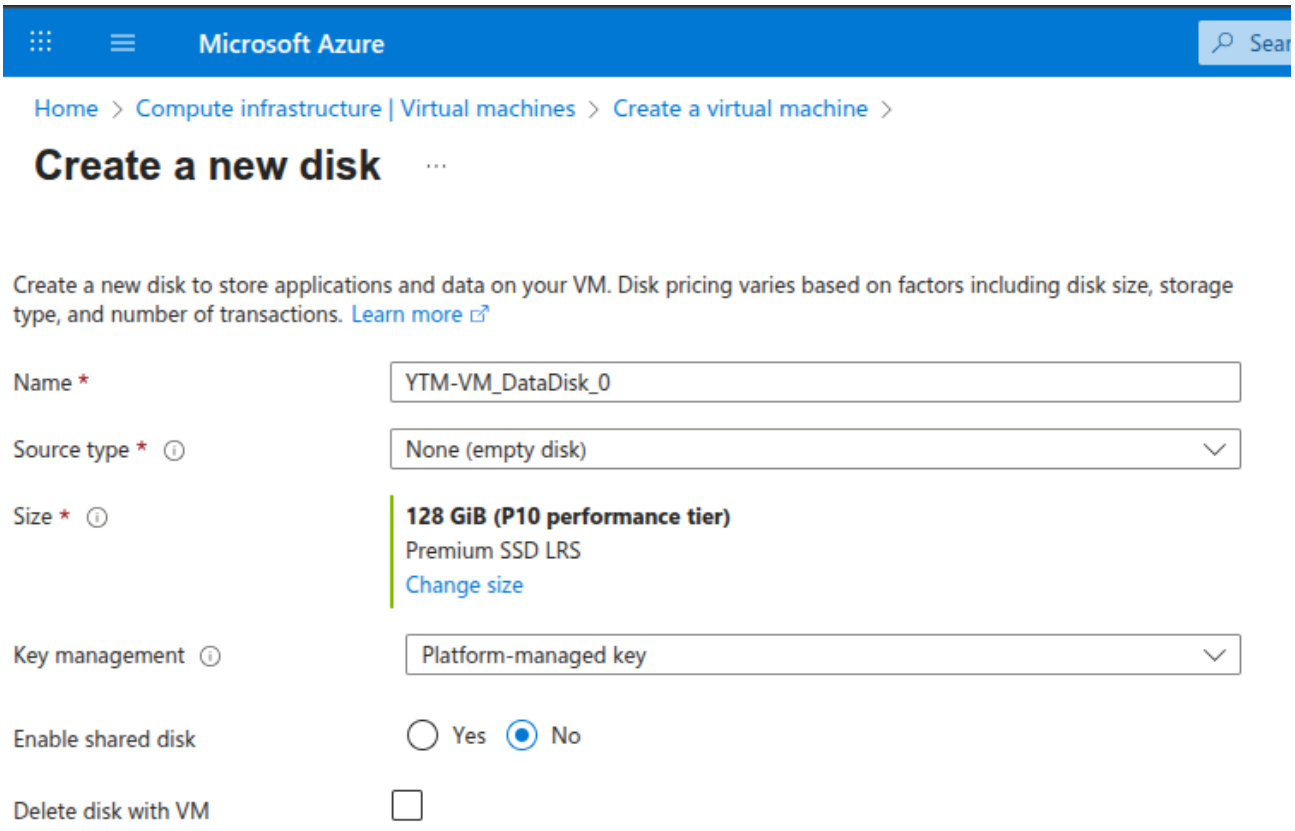

Microsoft Azure
Search reso
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
youtestme
Resource group *
(New) YTM-VM_group
Create new
Instance details
Virtual machine name *
YTM-VM
Region *
(US) East US
Availability options
No infrastructure redundancy required
Security type
Trusted launch virtual machines
Configure security features
Image *
Windows Server 2022 Datacenter: Azure Edition - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount



3. Under the “Disks” section, you can create and attach a new data disk. It is not mandatory, but it is a good practice to separate user data from system data in a different storage. The premium SSD disk type is recommended, but a standard SSD will also work.

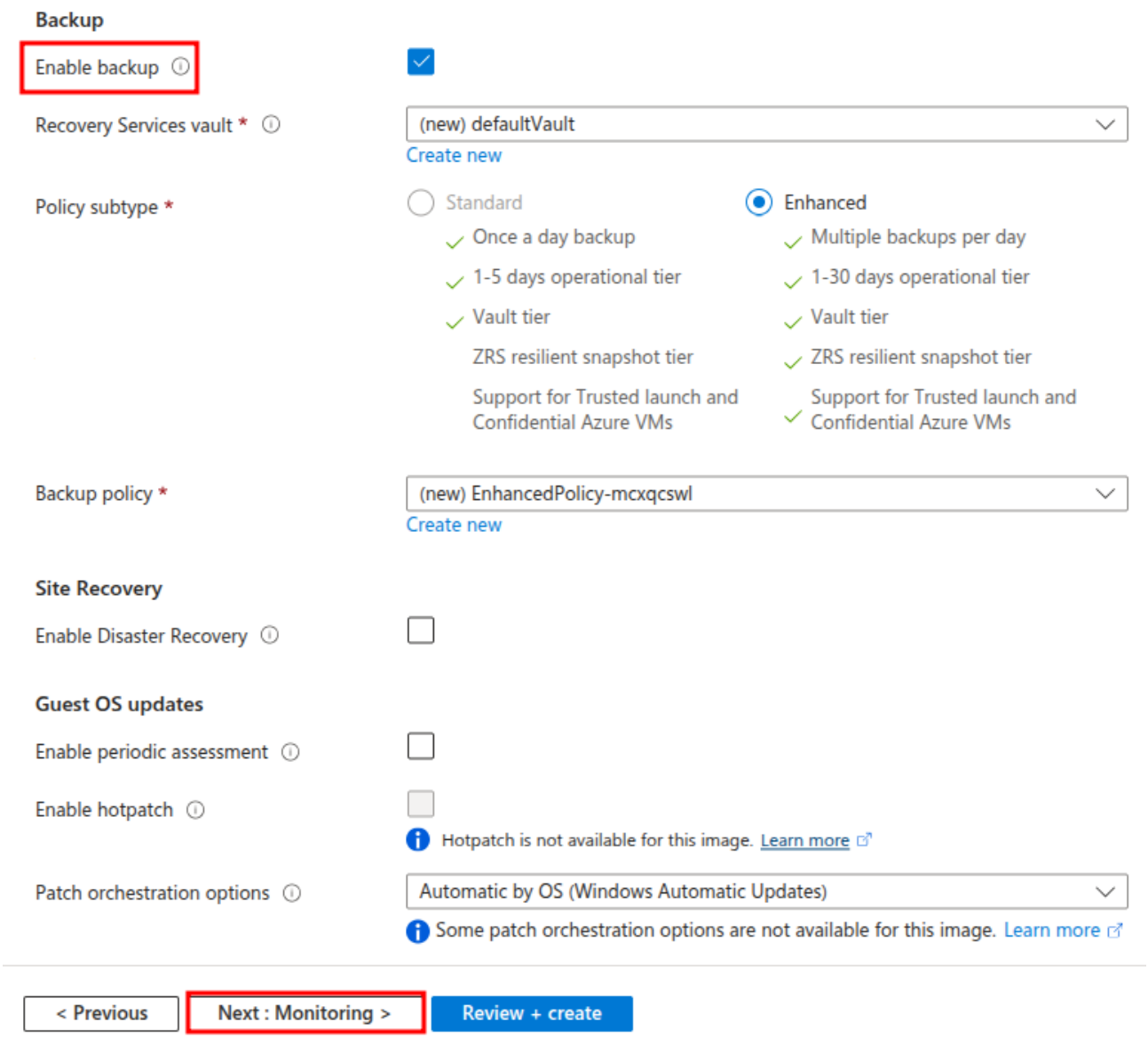
   To calculate data disk size, you can use the following relation: 1000 test attempts generate approximately 1 GB of data on the storage (disk). It does not include multimedia that can be attached to the test.


Microsoft Azure
Search resources,
Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size fo
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks.
The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more
VM disk encryption
Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.
Encryption at host
Encryption at host is not registered for the selected subscription. Learn more
OS disk
OS disk size
Image default (127 GiB)
OS disk type *
Premium SSD (locally-redundant storage)
Delete with VM
Key management
Platform-managed key
Enable Ultra Disk compatibility
Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_D8as_v6.
Data disks for YTM-VM
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.
LUN
Name
Size (GiB)
Disk type
Host caching
Delete with VM
Create and attach a new disk
Attach an existing disk
< Previous
Next : Networking >
Review + create

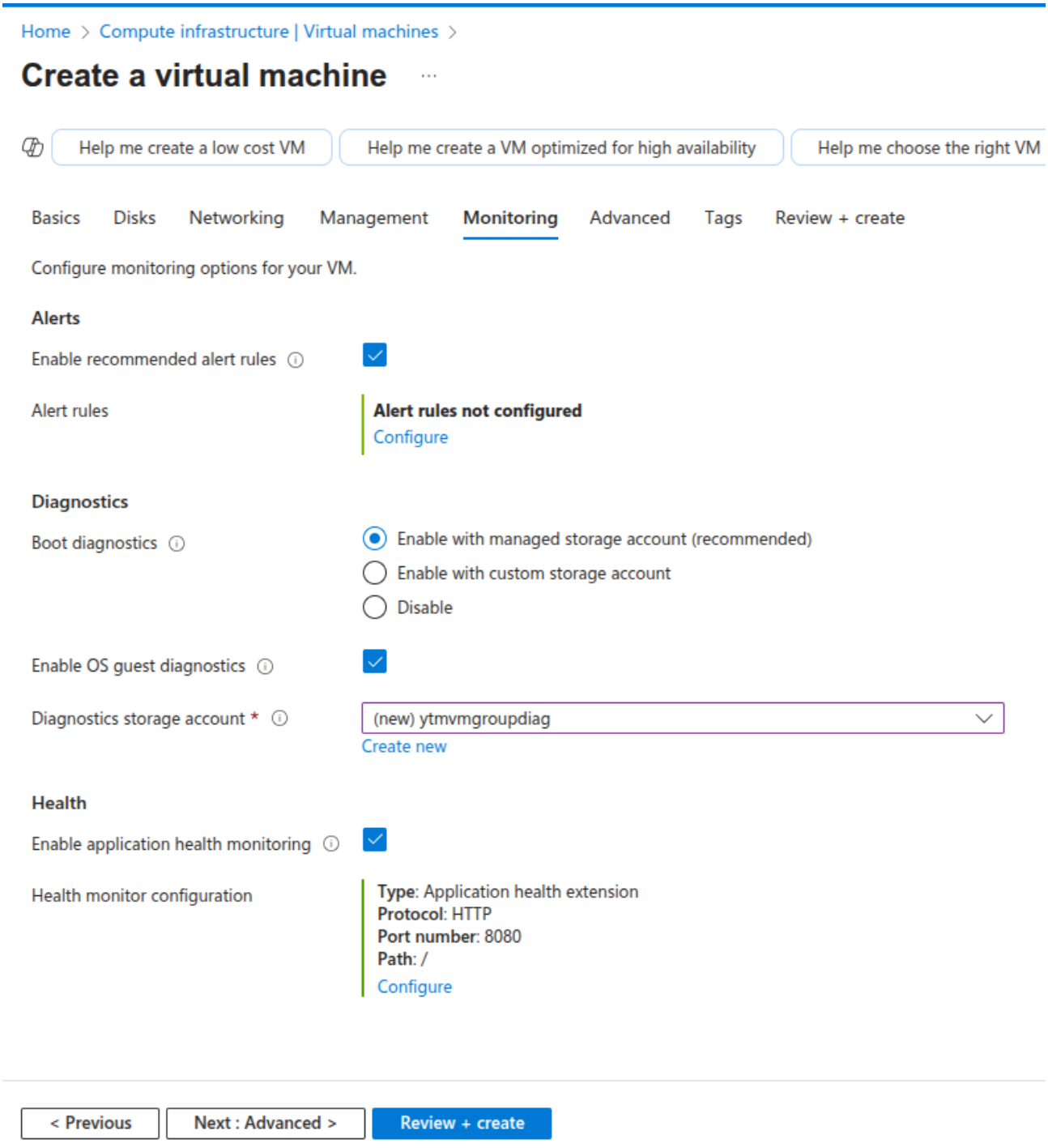


4. Create a new Virtual Network and Subnet if necessary, or place the server in the existing ones. Avoid using public IP addresses attached to the VM in the production environment; instead, use Azure VPN or Azure Bastion to connect to the VM using its private IP address.

5. Under the “Management” section, select the “Enable backup” option if you are not sure about the correct backup strategy that can be applied to the VM.



6. Regarding the **Monitoring** section, you can activate all options. The Health Monitor configuration should include the default Tomcat HTTP port 8080.



7. You can skip the remaining sections and proceed to the “Review+create” step. After the final examination of the specified configuration, confirm that you are ready to start Azure VM creation.

4 Azure VM Remote Desktop Connection

4.1 Prerequisites

To connect via private IP (strongly recommended), ensure the following:

1. The Azure VM is running and has a private IP address.
2. You have network-level access to the VM (via the same virtual network, vNet peering, VPN, or ExpressRoute).
3. RDP (TCP port 3389) is allowed in the Network Security Group (NSG) for the VM.
4. You have the VM's username and password.

4.2 Common Scenarios That Allow Private Access

You can connect via private IP if:

- You're on another Azure VM in the same vNet or peered vNet
- You're on-premises and connected to Azure via VPN Gateway or ExpressRoute
- You're using an Azure Bastion host
- You're connecting via a jump host (bastion/jump VM) that has public access

4.3 Step-by-Step Instructions

4.3.1 Find the VM's Private IP

- Go to the **Azure Portal**
- Navigate to Virtual Machines → Select your VM
- Under the Networking section of the **Overview** tab, find the Private IP address

4.3.2 Check NSG Inbound Rule for RDP

Ensure the VM's Network Security Group allows RDP:

- Go to Networking → Inbound Port Rules
- Confirm a rule exists:
  Port: 3389
  Protocol: TCP
  Source: Your private network range
  Action: Allow

- If not, click the + Add inbound port rule and allow TCP 3389 from your subnet or specific IP.

4.3.3 ◈Ensure Network Access

You must be connected to the same private network as the VM.

Choose the method that fits your setup:

- If you're on another Azure VM, verify it's in the same vNet or peered vNet.
- If on-prem: ensure VPN or ExpressRoute is active.
- If using a jump host: connect to it first, then RDP into the target VM from there.

4.3.4 ◈Connect via RDP

On the machine with network access (local PC or jump host):

- Open Remote Desktop Connection **(mstsc** on Windows)
- In the Computer field, enter the private IP (e.g., 10.0.1.5)
- Enter the Username and Password for the VM
- Click **Connect** and accept any certificate warning

5 GetCertified Deployment on Windows Server

5.1 Mount a New Disk on Azure Windows VM (optional)

5.1.1 Attach the Disk in Azure (if not done yet)

If you haven't attached the disk yet:

- Go to Azure Portal → Virtual Machines
- Select your VM
- Navigate to Disks → + Add data disk
- Choose an existing disk or create a new one
- Click Save

The disk is now attached at the Hyper-V (virtual controller) level, but it has not been mounted inside Windows yet.

5.1.2 Log into the Windows VM

- Use RDP to connect to your Azure Windows VM.
- Open Server Manager or Run > diskmgmt.msc to launch Disk Management.

5.1.3 Initialize the Disk

In Disk Management:

- You will see a new disk marked as “Offline” or “Not Initialized” (typically something like Disk 1).
- Right-click the new disk and choose:
  - "Online" (if it's offline)
  - Then "Initialize Disk"
- Choose GPT (recommended for Azure/modern OS) or MBR (legacy).

5.1.4 Create New Volume

- After initialization, right-click on the unallocated space → New Simple Volume
- Use the wizard to:
  - Assign a drive letter
  - Format with NTFS
  - Set volume label (e.g., Data, Backup, etc.)
  - Perform a quick format

5.1.5 Verify Mount

- The new disk will appear in File Explorer with the assigned drive letter.
- You can now use it like any other drive.

5.2 Software Download

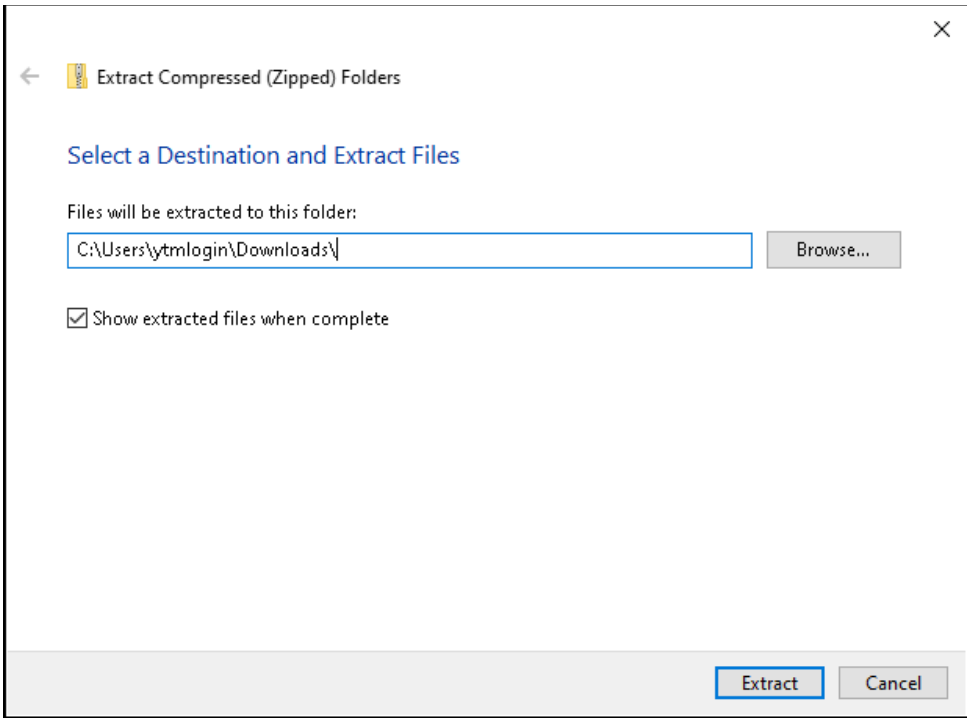
Use the URL below to download the resource files required for the software installation:

YouTestMe Software Download

Copy the URL above in the Azure VM browser and download the ZIP archive that contains the following components:

- JRE 21 installation file (.exe)
- PostgreSQL Server 16 installation file (.exe)
- Apache Tomcat v10 (portable version)
- Initial Postgres data (.dmp) - the minimal set of data required for the GetCertified to work
- PostgreSQL configuration files

Decompress the downloaded archive and move (copy) the "apache-tomcat-10.1.39" directory to the "C:" partition.



5.3 JRE and PostgreSQL Server Installation

Install Java Runtime Environment (JRE) and PostgreSQL 16 Database Server using the executable files downloaded from the YouTestMe Nextcloud server.

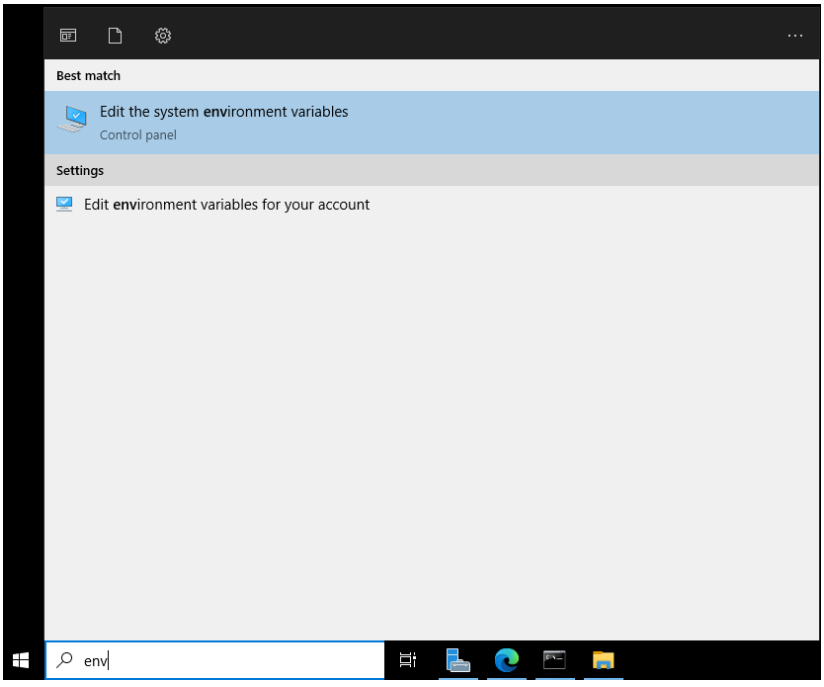
During the installation process, keep the default settings. Specify and keep the database administrative password for user **postgres** in a secure place. You can also skip the installation of some database components (pgAdmin 4 and Stack Builder).

5.4 Edit System Environment Variables

It is mandatory to define %CATALINA_BASE% and %JAVA_HOME% user variables and to modify the system %PATH% variable by adding the paths to the following "bin" directories ("bin" directories contain executable files of the primary system components):

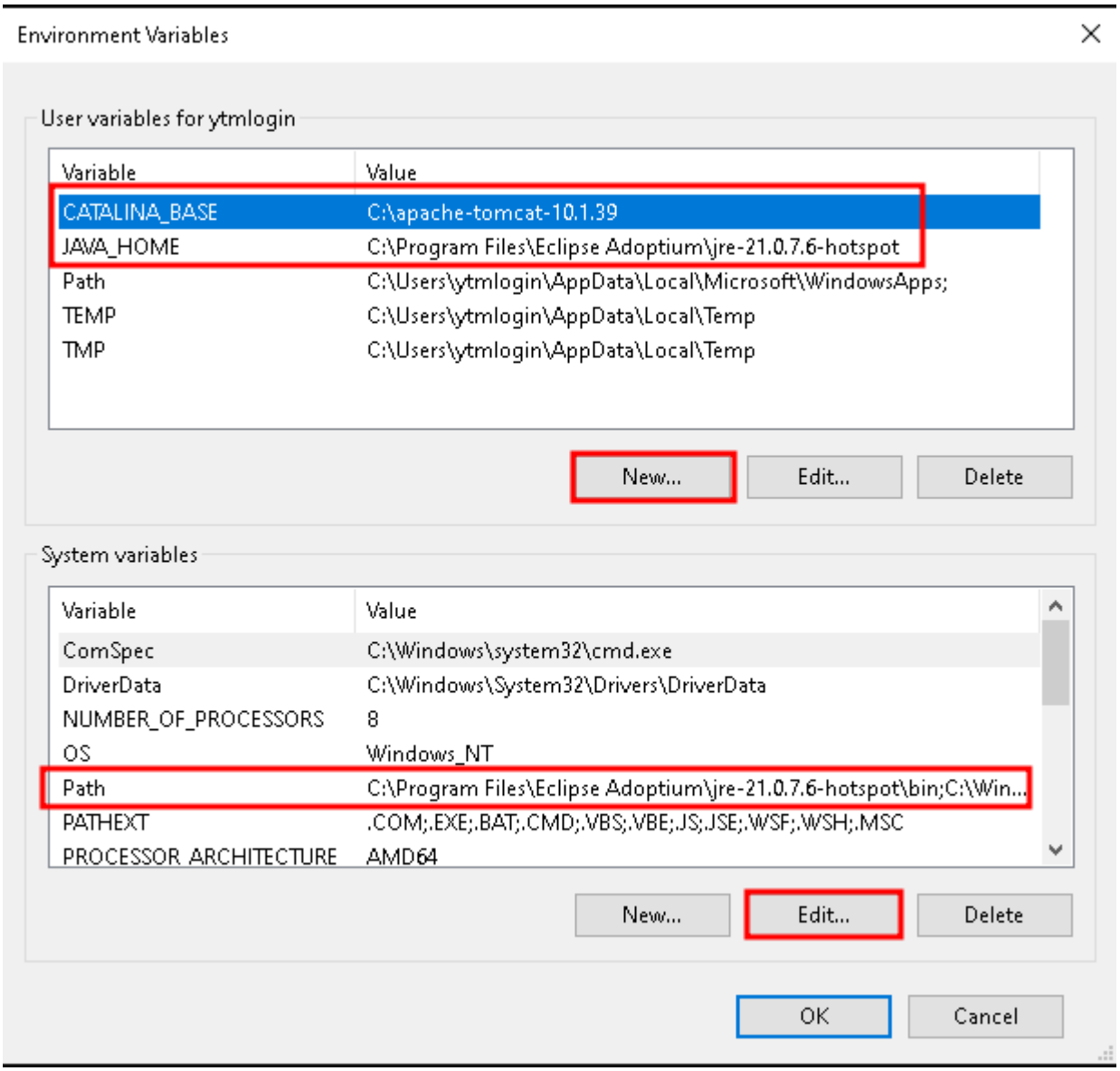
- %CATALINA_BASE%\bin
- %JAVA_HOME%\bin
- C:\Program Files\PostgreSQL\16\bin

1. Search for "Edit the system environment variables" dialog:

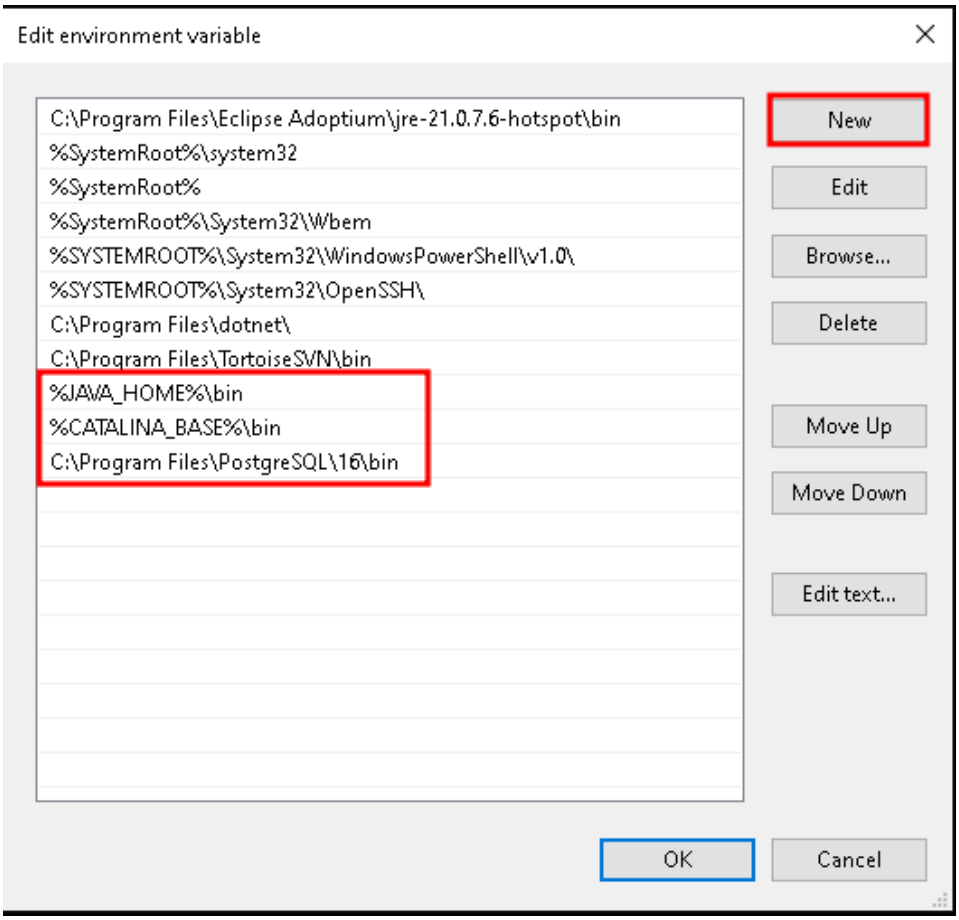


2. Click on the "Environment Variables…" button

3. Create the new system variables by clicking on the "New…" button. To edit the system variable **Path**, highlight it and click on "Edit…"



4. Edit the system variable %PATH% and add the specific system paths:



5.5 PostgreSQL Configuration

5.5.1 Replace Default Configuration Files

- Stop PostgreSQL Service
- Replace default PostgreSQL configuration files “pg_hba.conf” and “postgresql.conf” from the PostgreSQL data directory:

  C:\Program Files\PostgreSQL\16\data

  with the preconfigured database configuration files located in the “Downloads” folder.
- Start PostgreSQL Service

5.5.2 Move PostgreSQL Data to Partition 2 (optional)

1. **Stop PostgreSQL Service**

2. Copy the Existing PostgreSQL Data Directory to partition number 2 (Data disk), e.g.:

   C:\Program Files\PostgreSQL\16\data ->(copy)-> **E:\PostgreSQLData**

3. Update Windows Service Parameters:

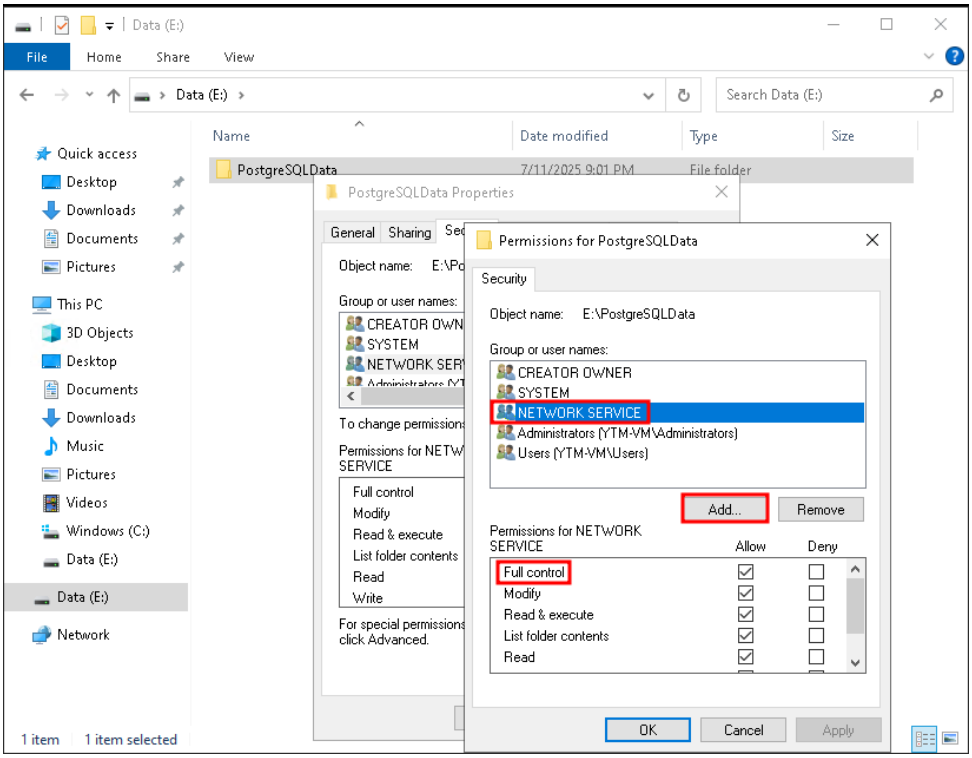
   a) Open Registry Editor (regedit)
   b) Navigate to: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-x64-16**
   c) Edit the ImagePath value by changing the **-D** parameter to point to the new data path:

   "C:\Program Files\PostgreSQL\16\bin\pg_ctl.exe" runservice -N "postgresql-x64-16" -D "**E:\PostgreSQLData**"

4. Set Folder Permissions:

   Ensure the postgres service user (usually **NETWORK SERVICE**) has Full Control on E:\PostgreSQLData.

   a) Right-click the new folder → Properties
   b) Go to Security → Edit → Add the service user
   c) Grant Full Control



5. Start PostgreSQL Service

6. Verify the New Location

   a) Run **psql** from the command line and confirm it works: **psql -U postgres**
   b) From within **psql,** run: **SHOW data_directory;**
   c) You should see: **E:/PostgreSQLData**

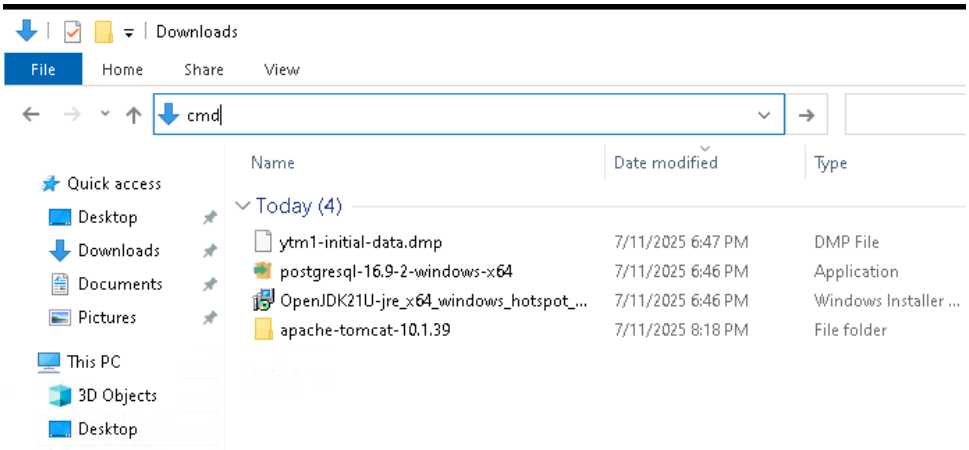
7. (Optional) Delete Old Data Folder

Once everything is working correctly and you've backed up your data:

- You can delete the old **C:\Program Files\PostgreSQL\16\data** folder to free space.

5.5.3 Data Import

Open the Windows terminal (Command Prompt) and navigate to the “Downloads” directory where the downloaded file “ytm1-initial-data.dmp” is located.



Execute the following commands (marked as bold text):

- **`psql -U postgres postgres`** (connecting to the local database; entering **psql** shell)
- `postgres=#` **`create database ytmdb1;`**
- `postgres=#` **`create role ytm1 with password '2ytm1';`**
- `postgres=#` **`alter role ytm1 with login;`**
- `postgres=#` **`alter database ytmdb1 owner to ytm1;`**
- `postgres=#` **`\q`** (exit psql shell)
- **`pg_restore -v -U postgres -d ytmdb1 ytm1-initial-data.dmp`**

5.5.4 Restart (Start/Stop) PostgreSQL Service

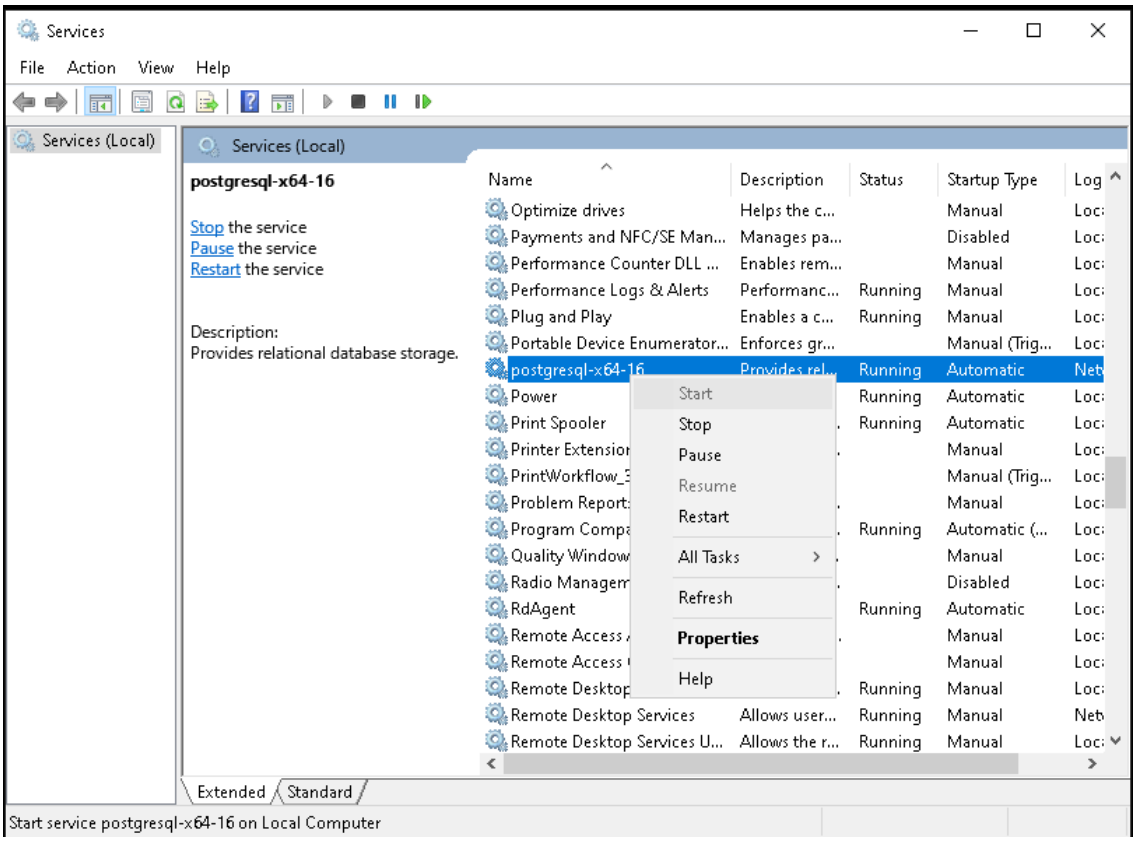
Method 1:

Open the command prompt as an administrator and type one of the following commands:

- **`net stop postgresql-x64-16`**
- **`net start postgresql-x64-16`**
- **`net restart postgresql-x64-16`**

Method 2:

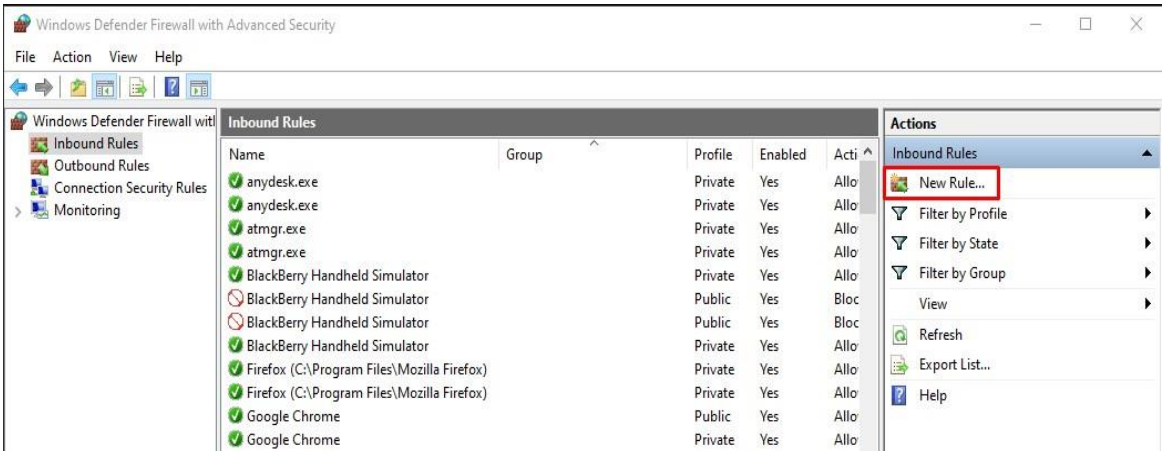
Search for the keyword **Services**, locate PostgreSQL service, highlight it, right-click and select "Restart/Stop/Start” operation:



6 Windows Firewall

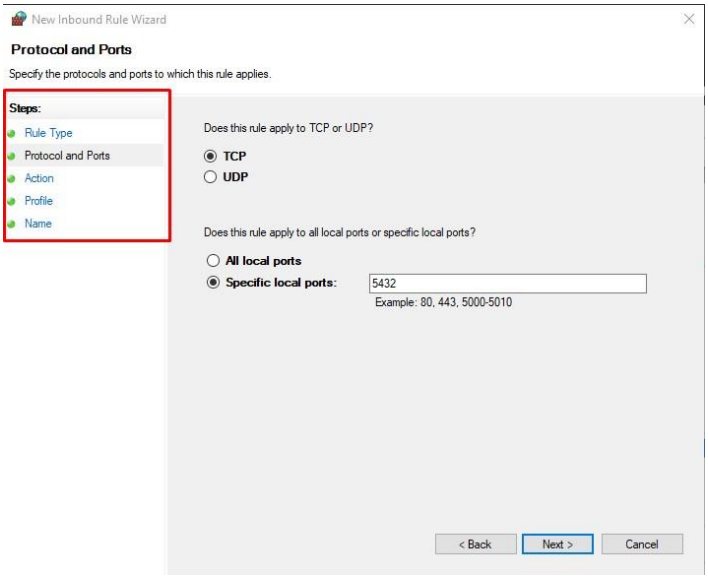
If it is necessary to allow database connection on port 5432 within the private network, you need to modify Windows Firewall rules:

1. Search for the "Windows Defender Firewall with Advanced Security" prompt and select "Inbound Rules" from the left menu. Proceed by clicking the "New Rule..." option from the right menu:



2. Select the following options for the steps listed on the left:

a) **Rule Type** -> select "port"
b) **Protocols and Ports** -> select "TCP" and type "5432" in the "Specific local ports:" field
c) **Action** -> select "Allow the connection"
d) **Profile** -> check "Private" ("Domain" is optional)
e) **Name** -> specify custom rule name ("PGRULE", for example)



3. Click "Finish" and test the database connection from the different nodes located in the same private network.

4. The same procedure can be applied to open the Tomcat HTTP port (8080) for access within the private network.

7 Starting YouTestMe Server Application

Open the Command Line (CMD), navigate to the Tomcat binary folder, and execute Tomcat **startup.bat** script:

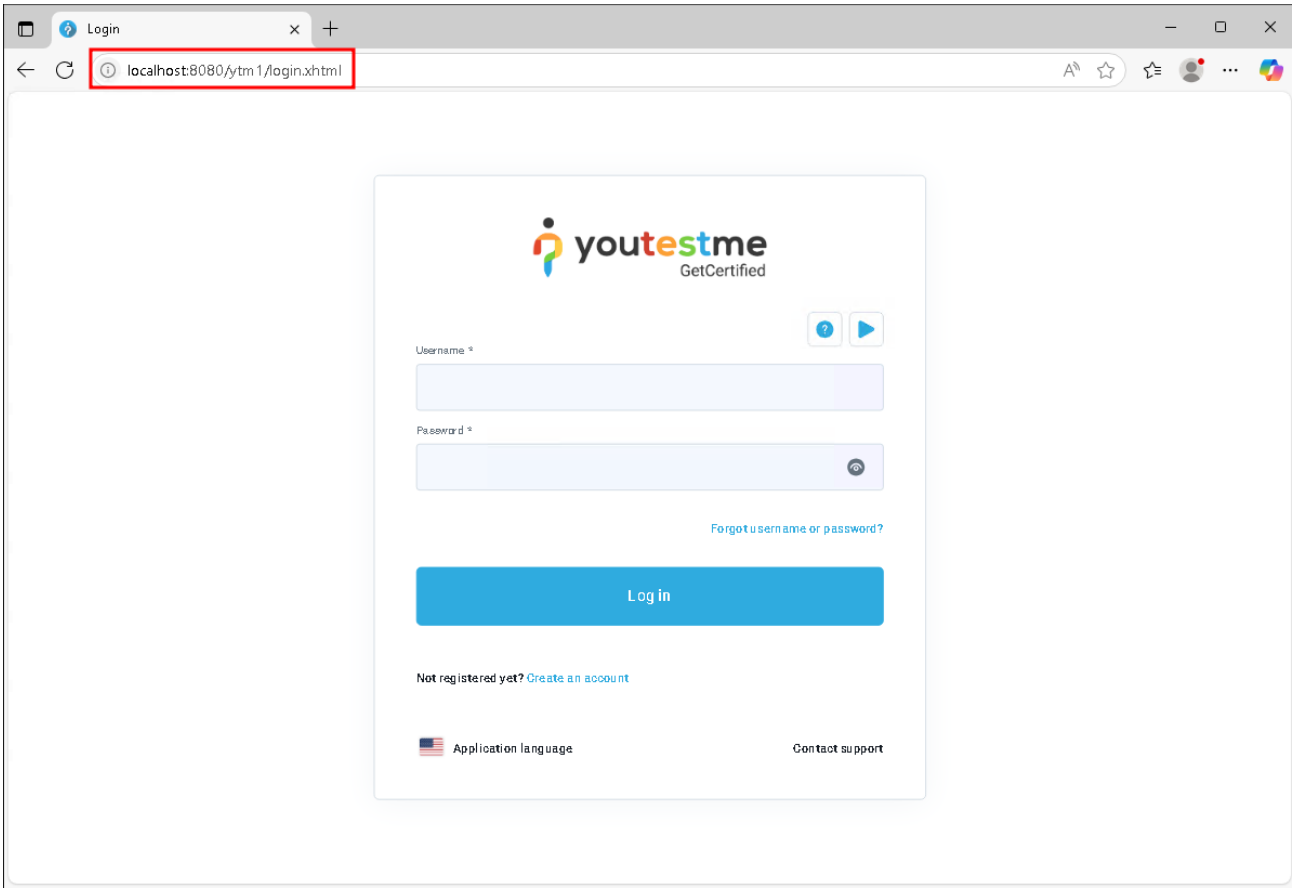
- C:\Users\ytmlogin> **cd C:\apache-tomcat-10.1.39\apache-tomcat-10.1.39\bin**
- C:\apache-tomcat-10.1.39\apache-tomcat-10.1.39\bin> **startup.bat**

When executed, the **startup.bat** script starts the Tomcat application server and launches a new console window that displays the live output of the server. Wait up to 5 minutes for the application deployment after you start the Tomcat server.

To access the application, type (copy) the following string in the VM browser's address bar:

http://localhost:8080/ytm1/login.xhtml

Login information and the instructions for configuring recommended initial settings can be found in the document **Instructions for First Time Use.pdf.**



8 Changing Application Default Port (optional)

1. Check ports that are currently in use by executing the following command:

   C:\Users\ytmlogin> **netstat -an | findstr LISTEN**

2. Choose the port that is not currently used:

   a) Edit file: **C:\apache-tomcat-10.1.39\conf\server.xml**
   b) Change the port in the line below:

```
-->
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           compression="on"
           redirectPort="8443"
           maxParameterCount="1000"
           />
```

   c) Save file
   d) Restart Tomcat Server

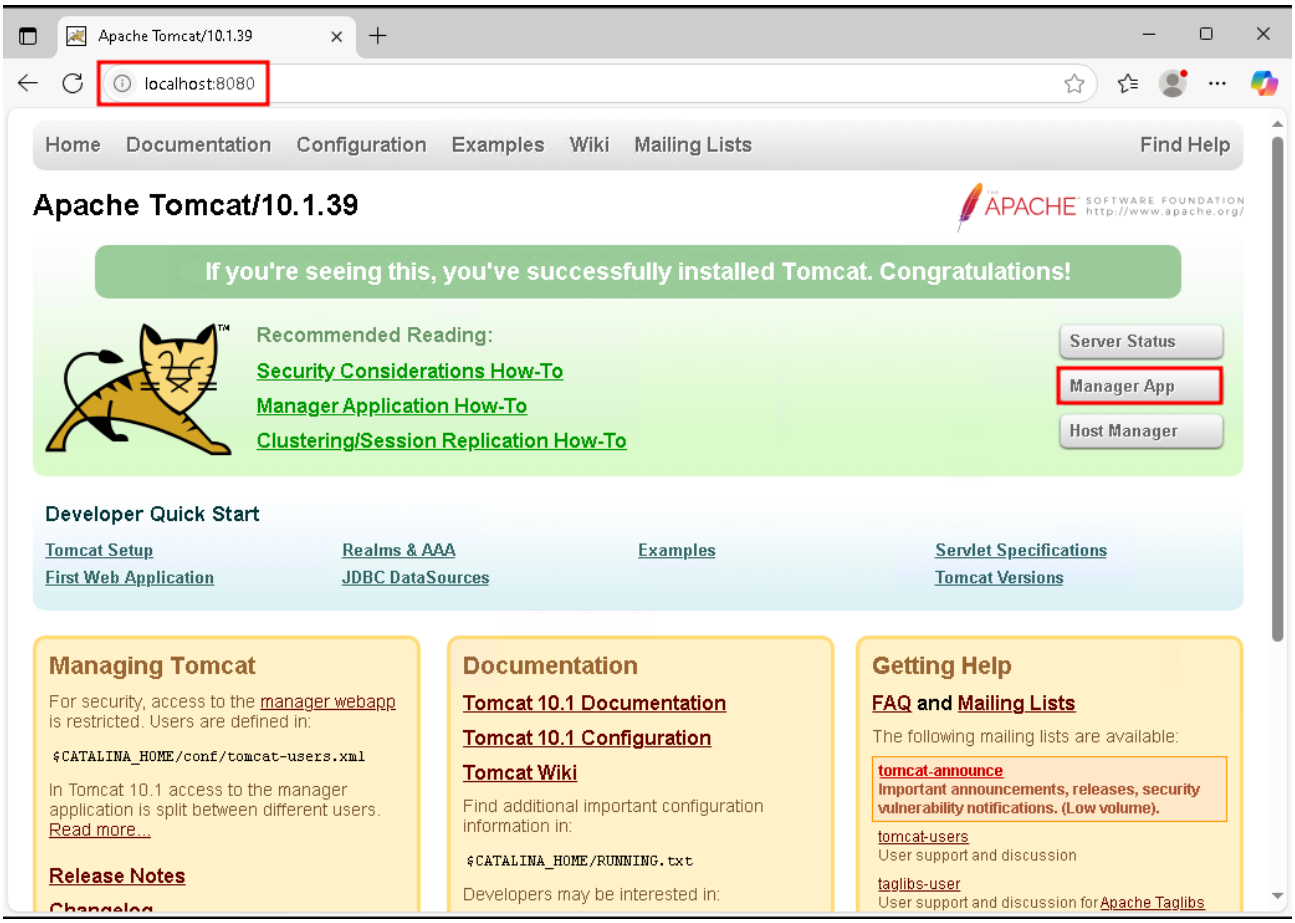
9 Tomcat Manager

Tomcat Manager App is a web application packaged with the Tomcat server and provides us with the basic functionality we need to manage our deployed web applications.

To access the Tomcat Manager application, do the following steps:

1. Open a browser on the Azure Virtual Machine and type the following URL:

   `http://localhost:8080`



2. Access to Tomcat Manager is allowed only from localhost by default for security reasons. To change it, do the following:

   Edit the following configuration file (**Valve** component) and specify the IP address of your workstation.

   C:\apache-tomcat-10.1.39\webapps\manager\META-INF\context.xml

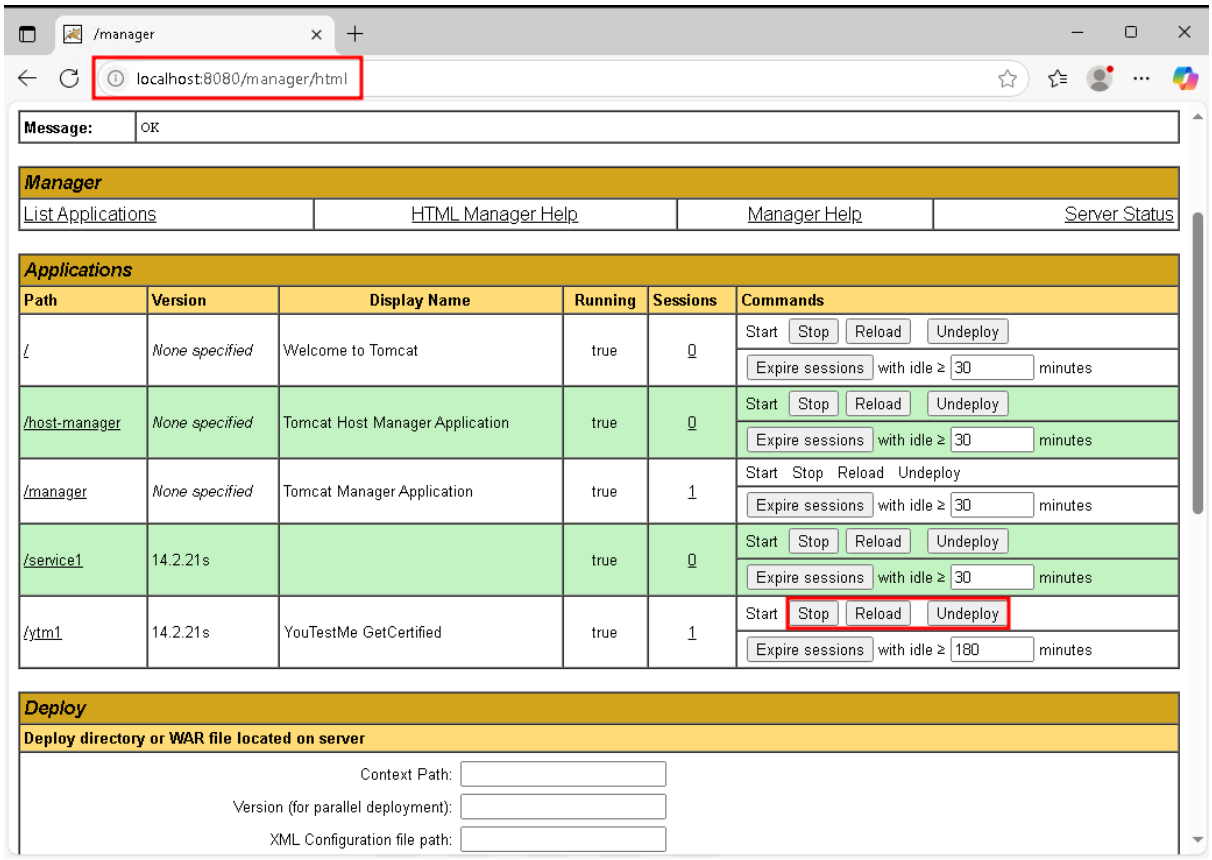
   Example: Allow Tomcat manager access from the private IP address 192.168.1.80.

   ```
   <Valve className="org.apache.catalina.valves.RemoteAddrValve"
          allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1|192\.168\.1\.80" />
   ```

3. Click on the "Manager App" button and enter the default login credentials:

   - Username: ytmadmin
   - Password: 2youtestme1

4. Now, you can easily manage the YouTestMe application using the GUI:



Check the official documentation for more details about Tomcat Manager functionality.

9.1 Change Login Credentials

To change Tomcat Manager login credentials, perform the following operation:

1. Edit the following configuration file and set up your username and password values.

   C:\apache-tomcat-10.1.39\conf\tomcat-users.xml

```
  <role rolename="manager-status"/>
  <role rolename="manager-gui"/>
  <role rolename="manager-jmx"/>
  <role rolename="manager-script"/>

  <user username="ytmadmin" password="2youtestme1" roles="manager-gui"/>
  <user username="ytmscript" password="2youtestme1" roles="manager-script"/>

</tomcat-users>
```

2. Restart Tomcat Server

10 Securing Network Access to the YouTestMe System

This section describes ensuring that only specific computers on your network can access the YouTestMe system.

10.1 YouTestMe Virtual Machine Active Ports

Port	Protocol	Purpose
3389	RDP	System support
5432	TCP	Access to the PostgreSQL database
8080	HTTP	Access to the YouTestMe Web Application using a web browser

10.2 Assumptions

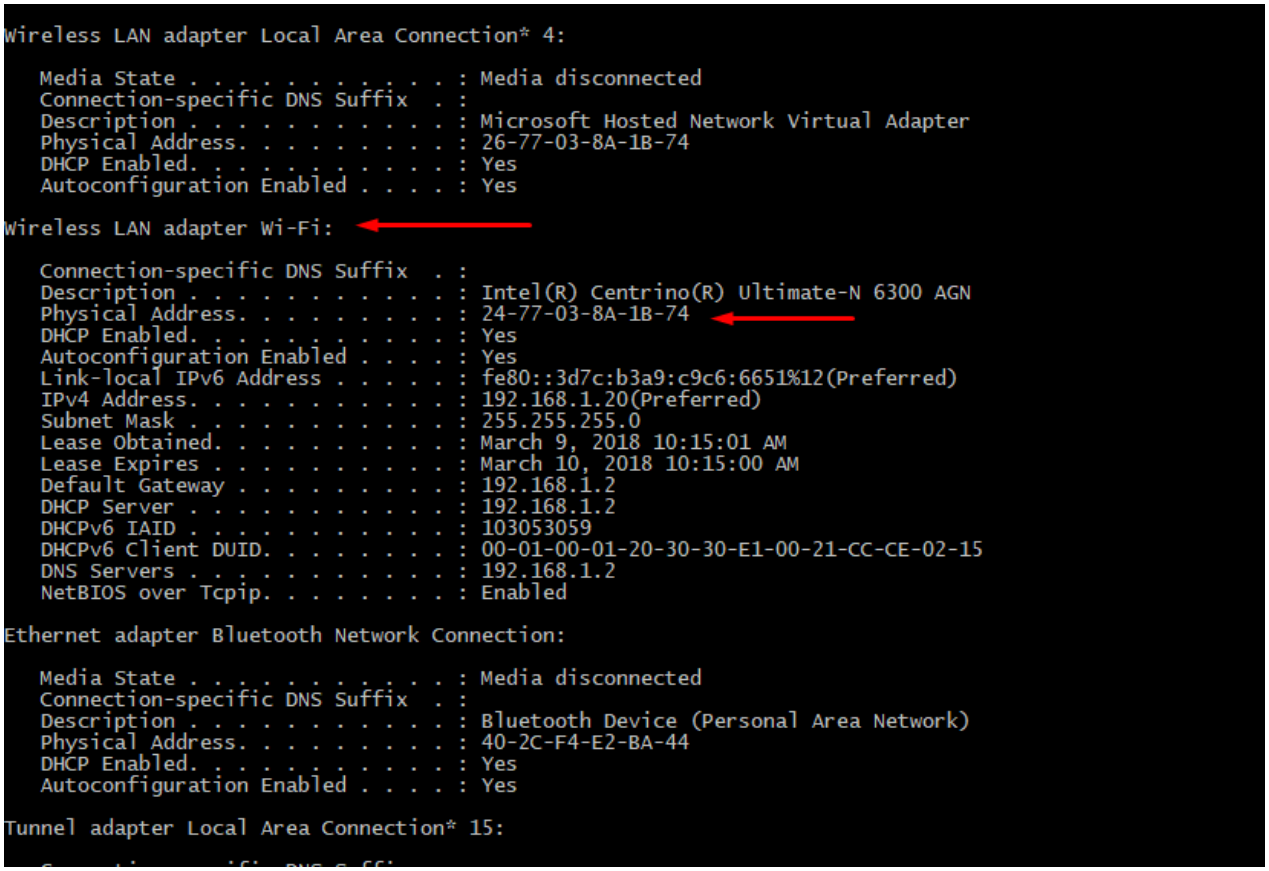
All computers are on the local network.

10.3 Step #1 - Determine a set of IP addresses with Access to the YouTestMe System

Determine the range of IP addresses permanently assigned to computers (devices) that will have access to the YouTestMe System. For example, suppose you have 30 computers (workstations) used for doing tests and for the application's administration. In that case, you could specify a range of related IP addresses from 192.168.1.100 to 192.168.1.129.

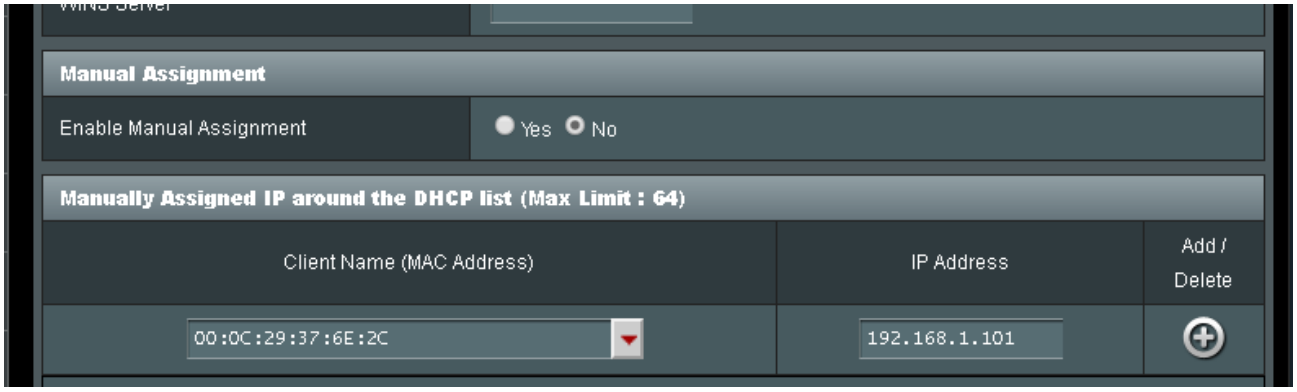
10.4 Step #1 - Collect MAC addresses

Collect MAC addresses from all computers (devices) that need access to the YouTestMe system.
Type "ipconfig /all" inside the DOS Window and search for Physical Address (picture below).



10.5 Step #3 - Set up your network (DHCP server)

Set up your DHCP server to reserve specific IP addresses to specific MAC addresses.
An example of one particular router (Asus RT-AC66U) is shown below:



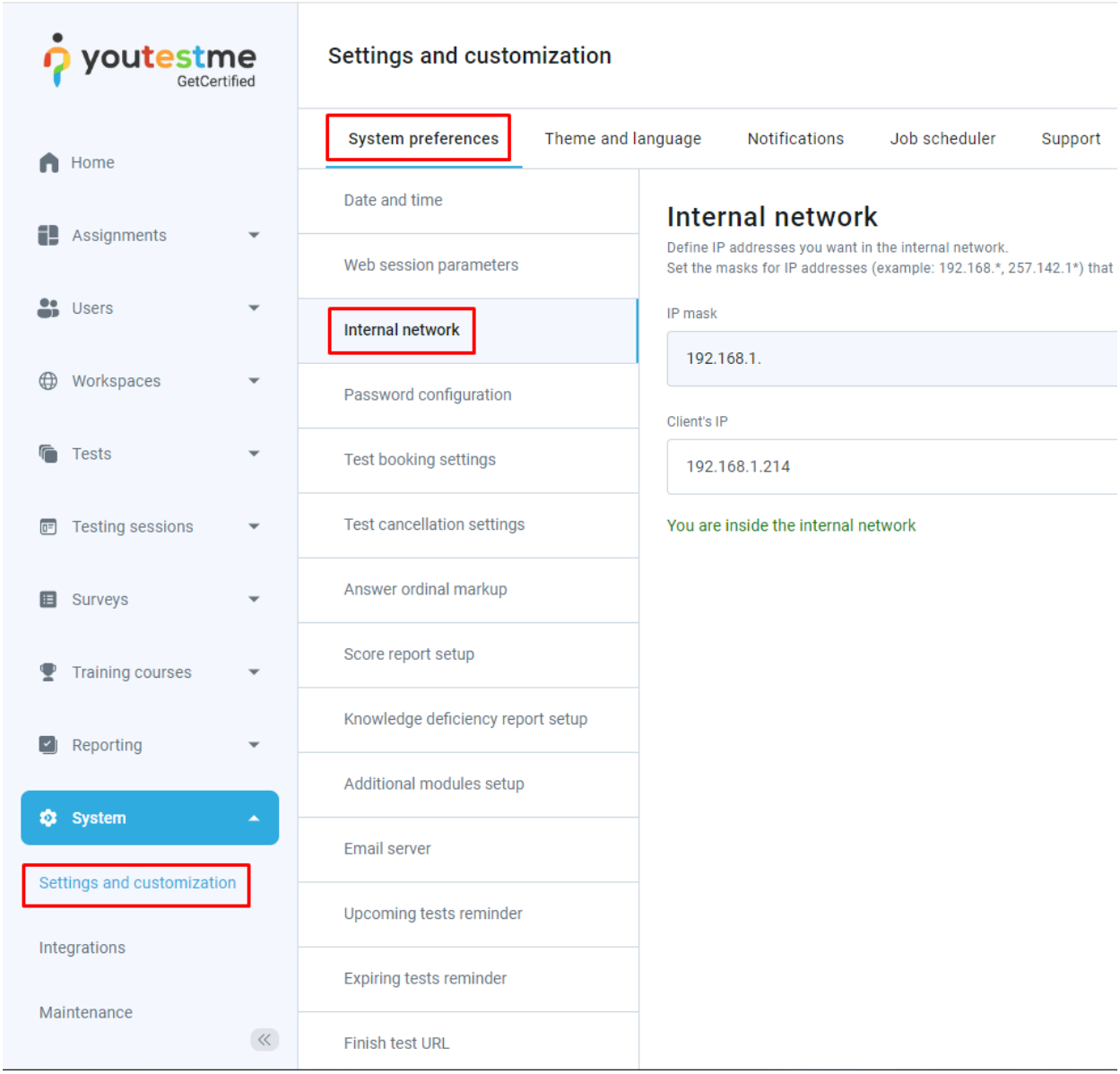
10.6 Step 4 - Verify your devices

Reboot your devices and make sure they are assigned IP addresses as set up in Step #3

10.7 Set up networking in the YouTestMe application

Set up access to the YouTestMe application to be allowed for IP ranges from 192.168.1.100 to 192.168.1.129.

Navigate to "System -> Settings and customization -> System preferences" tab, and locate the "Internal network" settings, where you can set a range of your local IP addresses.



11 Configure HTTPS Using Apache Web Server

Requirements:

1. Apache HTTPD
2. Apache module **mod_ssl**
3. SSL certificate for your domain/subdomain

1. Copy your certificate file, the certificate key, and the certificate of the CA that signed the SSL certificate to the following directory: **C:\SSLCerts**

2. Navigate to Apache's **conf\extra** directory (commonly located at):

   cd C:\Apache24\conf\extra

   Adjust the path if your Apache installation directory is different.

3. Create a "***httpd-vhosts.conf***" file with a **Virtual Hosts** (your domain/subdomain should replace getcertified.example.com). The "secret" value should be the same as it is specified in the Tomcat file: C:\apache-tomcat-10.1.39\conf\server.xml (AJP connector)

```
<VirtualHost *:80>
        ServerName                      getcertified.example.com
        Redirect        /       https://getcertified.example.com/
</VirtualHost>

<VirtualHost *:443>

        ServerName                      getcertified.example.com

        SSLEngine on
        SSLCertificateFile "C:/SSLCerts/YOUR_CERTIFICATE.crt"
        SSLCertificateKeyFile "C:/SSLCerts/YOUR_key.key"
        SSLCACertificateFile "C:/SSLCerts/YOUR_CA.ca-bundle"

        ProxyPreserveHost on

        RewriteEngine on
        RewriteCond %{REQUEST_URI} ^/$
        RewriteRule (.*) /ytm1/ [R=301]

        RewriteCond %{HTTP:Upgrade} websocket [NC]
        RewriteCond %{HTTP:CONNECTION} Upgrade$ [NC]
        RewriteRule /(.*)  ws://Azure_VM_IP:8080/$1 [P,L]

        ProxyPass               /ytm1/ ajp://Azure_VM_IP:9101/ytm1/ secret=your_secret
        ProxyPassReverse   /ytm1/ ajp://Azure_VM_IP:9101/ytm1/
```

```
</VirtualHost>
```

4. Enable the Virtual Hosts file in httpd.conf:

    a. Open: **C:\Apache24\conf\httpd.conf**
    b. Ensure the following line is uncommented (remove # if present):
    Include conf/extra/httpd-vhosts.conf
    c. Also make sure the following modules are enabled in httpd.conf:

    LoadModule ssl_module modules/mod_ssl.so
    LoadModule proxy_module modules/mod_proxy.so
    LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
    LoadModule rewrite_module modules/mod_rewrite.so

5. Open Command Prompt as Administrator, then run:
httpd.exe -t

6. Reload HTTPD:
httpd.exe -k restart

7. Edit the Tomcat configuration file **server.xml** and uncomment AJP connector configuration. Change the default value for the "secret" parameter within the AJP connector settings. The new secret value should match the value specified in the Apache virtual host. Restart the Tomcat server to apply the changes.

    C:\apache-tomcat-10.1.39\conf\server.xml

```
<Connector protocol="AJP/1.3"
               address="0.0.0.0"
               port="9101"
               secretRequired="true"
               secret="your_secret"
               redirectPort="8443"
               maxParameterCount="1000"/>
```

12 System Troubleshooting and Maintenance

12.1 Enable Tomcat to Start on Boot

1. Run Command Prompt as Administrator:
   a) Click **Start**, search for "cmd".
   b) Right-click **Command Prompt** → **Run as Administrator**
2. Navigate to Tomcat's bin directory:
   cd C:\apache-tomcat-10.1.39\bin
3. Install Tomcat as a Windows service:
   service.bat install Tomcat10
4. Open Windows Services:
   a) Press **Win + R**, type services.msc, press **Enter**
   b) Look for a service named **Tomcat10**
5. Set the Service to Start Automatically:
   a) Right-click the Tomcat service -> Properties
   b) Set **Startup type** to **Automatic (Delayed Start) -** wait for PostgreSQL to start
   c) Click **Apply** and **OK**.
6. Start the Service (Optional):
   If Tomcat is not running yet:
   net start Tomcat10
7. How to Check if Tomcat Starts After Reboot:
   a) Reboot the server
   b) Open a browser on VM and navigate to: http://localhost:8080
   c) Or open **Services** again and confirm the Tomcat service is running

12.2 Tomcat Server Restart

- Stop YouTestMe applications (**ytm1** and **service1**) from the Tomcat Manager
- Stop Tomcat Server by executing **shutdown.bat** script:
  C:\apache-tomcat-10.1.39\bin\shutdown.bat
- Wait for 10-15 seconds for the server shutdown to complete
- Start Tomcat Server by executing **startup.bat** script:
  C:\apache-tomcat-10.1.39\bin\startup.bat

12.3 Export Database Data to a File

It is good practice to back up your data regularly by exporting it to a file, which can then be stored in a secure location. This backup can be invaluable in the event of data loss, as the saved data can be re-imported into the database.

It is sufficient to backup only the database schema containing your data by executing the following command from the Command Line:

C:\Users\ytmlogin> **pg_dump -v -Fc -U ytm1 -n ytm1 -b -d ytmdb1 > ytm1-backup.dmp**

12.4 Import Database Data from a File

The PostgreSQL data file can be restored from the backup via CLI (command-line interface) by performing the following procedure:

1. Copy your previously exported data file (***ytm1-backup.dmp***, for example) from the backup location and place it in the “Downloads” directory:

2. Navigate to the “Downloads” directory where you transferred the database backup file :

   ```
   cd C:\Users\ytmlogin\Downloads>
   ```

3. Backup your current database data (schema):

   ```
   pg_dump -v -U ytm1 -n ytm1 -b -Fc ytmdb1 > ytm1-backup2.dmp
   ```

4. Drop database schema "***ytm1***":

   ```
   psql -U postgres -d ytmdb1 -c 'drop schema ytm1 cascade';
   ```

5. Restore user data from the backup file "***ytm1-backup.dmp***":

   ```
   pg_restore -v -U postgres -d ytmdb1 < ytm1-backup.dmp
   ```

12.5 Database Parameters

Table showing default database parameters:

Setting	Value
Statistics gathering	automatic
Database Name	ytmdb1
Database administrative user	postgres
YouTestMe database schema (user data)	ytm1
Character Set	UTF8
Time Zone	UTC
Database Port	5432
Log Rotation	automatic

12.6 Virtual Machine Freezes

When a virtual machine freezes, the reason is usually that the host server is running out of memory or disk space. The solution is to shut down some processes on your host server or add more memory. If the cause runs out of disk space on the host server, adding disk space or cleaning unnecessary files will solve it.

12.7 Checking Tomcat Log

Tomcat's standard output and error are displayed in a separate window during startup. Application and API logs (e.g., ytm1.log, service1.log) can be found in the following directory:

C:\apache-tomcat-10.1.39\logs

12.8 Tomcat could not be stopped

Tomcat runs as a Java process, so you need to look for java.exe or javaw.exe. Use Command to execute the commands:

- Open Command Prompt as Administrator.
- Run the following command to list Java processes:

  tasklist /FI "IMAGENAME eq java.exe"

  Example output:

Image Name	PID	Session Name	Mem Usage
java.exe	12345	Services	150,000 K

- If multiple Java processes are running, identify the one related to Tomcat using this:
  wmic process where "name='java.exe'" get ProcessId,CommandLine

  Look for lines that include something like: ..org.apache.catalina.startup.Bootstrap...
  That process is Tomcat. Note the PID (Process ID).

- Kill the Tomcat Process:

  Once you have the PID, terminate the process:

  taskkill /PID <PID> /F

  Example: **taskkill /PID 12345 /F**
  /F forces the process to terminate. If successful, you'll see:

  SUCCESS: The process with PID 12345 has been terminated.

12.9 Running VACUUM ANALYZE on PostgreSQL

To ensure optimal performance and reliability of the PostgreSQL database installed on the Windows server, Windows administrators should periodically execute the VACUUM ANALYZE command. The task is especially important on systems with frequent data updates, inserts, or deletes.

To ensure regular execution, administrators can schedule the VACUUM ANALYZE command using a batch script and the Windows Task Scheduler.

Example batch script (vacuum.bat):

```
@echo off
psql -U postgres -d your_database_name -c "VACUUM ANALYZE;"
```

Use **Task Scheduler** to run this batch file weekly or nightly as part of your database maintenance plan.

12.10 Monitoring System Resources

To check resource utilization on a Windows Server, there are several built-in tools you can use depending on how detailed or real-time your monitoring needs to be:

12.10.1 Task Manager (Basic Monitoring)

- Press **Ctrl + Shift + Esc** or right-click the **taskbar** and select **Task Manager**.
- Click the **Performance** tab to view:
  - CPU usage per core
  - Memory (RAM) usage
  - Disk activity
  - Network traffic

Use the **Details** tab to see per-process usage.

12.10.2 Resource Monitor (Advanced GUI)

- Press **Win + R**, type resmon, and press **Enter**.
- Go to:
  - CPU tab: see services, threads, per-process usage
  - Memory: usage, hard faults, committed memory
  - Disk: I/O per file and process
  - Network: per-process network usage, ports

Very helpful for diagnosing which app is slowing down the system.

12.10.3 Performance Monitor (In-Depth & Historical Tracking)

- Press **Win + R**, type perfmon, and press **Enter**.
- Use:
  - Performance Monitor (real-time graphs)
  - Data Collector Sets (create logs over time)
  - Add counters for:
    - Processor(_Total)\% Processor Time
    - Memory\Available MBytes
    - PhysicalDisk\% Disk Time
    - Network Interface\Bytes Total/sec

Best for long-term monitoring and reporting.

13 Contact Information

If you encounter any difficulties during the process or have any questions, please do not hesitate to contact our support team at support@youtestme.com. Our dedicated team of experts is available to assist you with any issue that you may have.

https://www.youtestme.com/support-services/