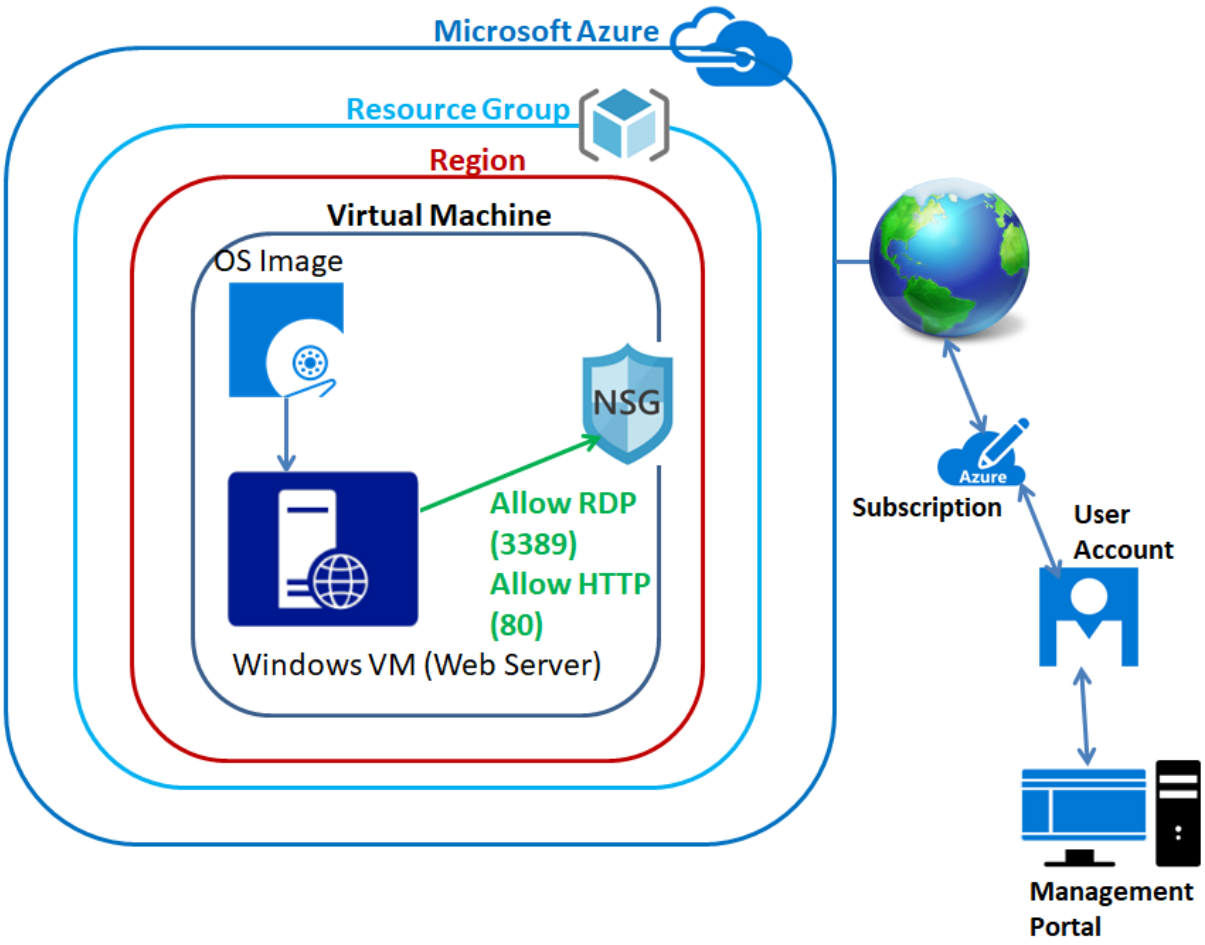
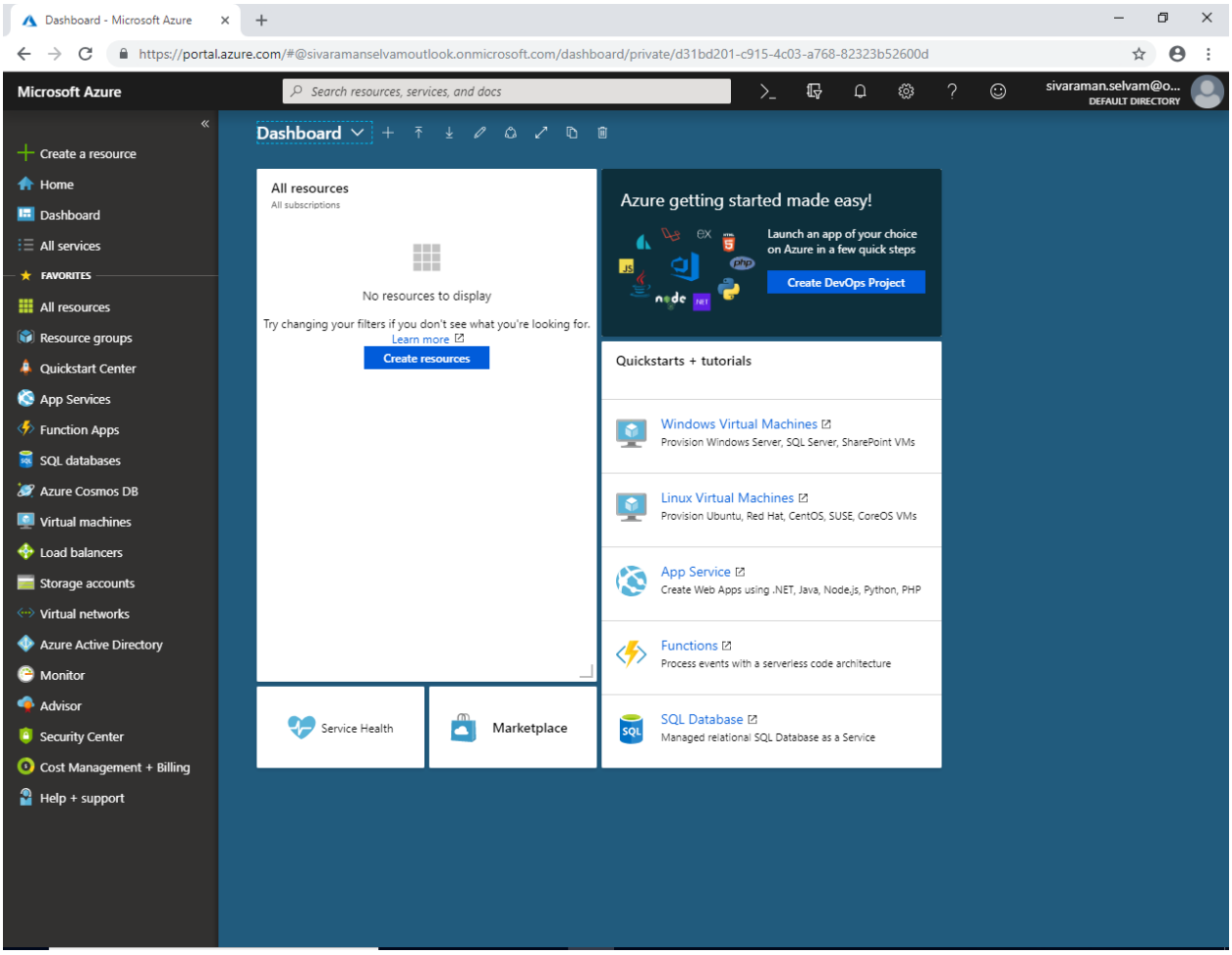
Lab3 – Installing IIS in Windows Virtual Machine - Azure

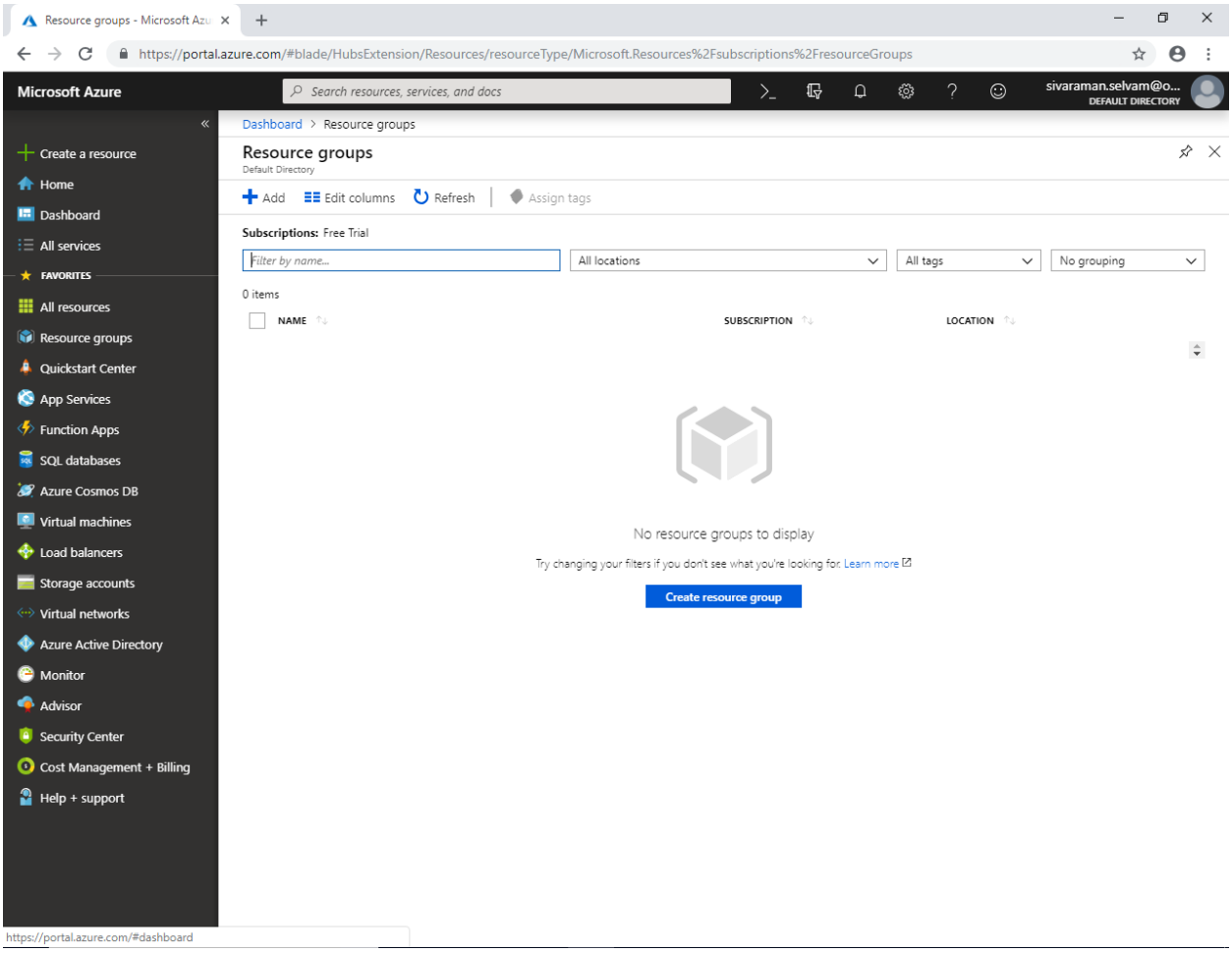
Topology



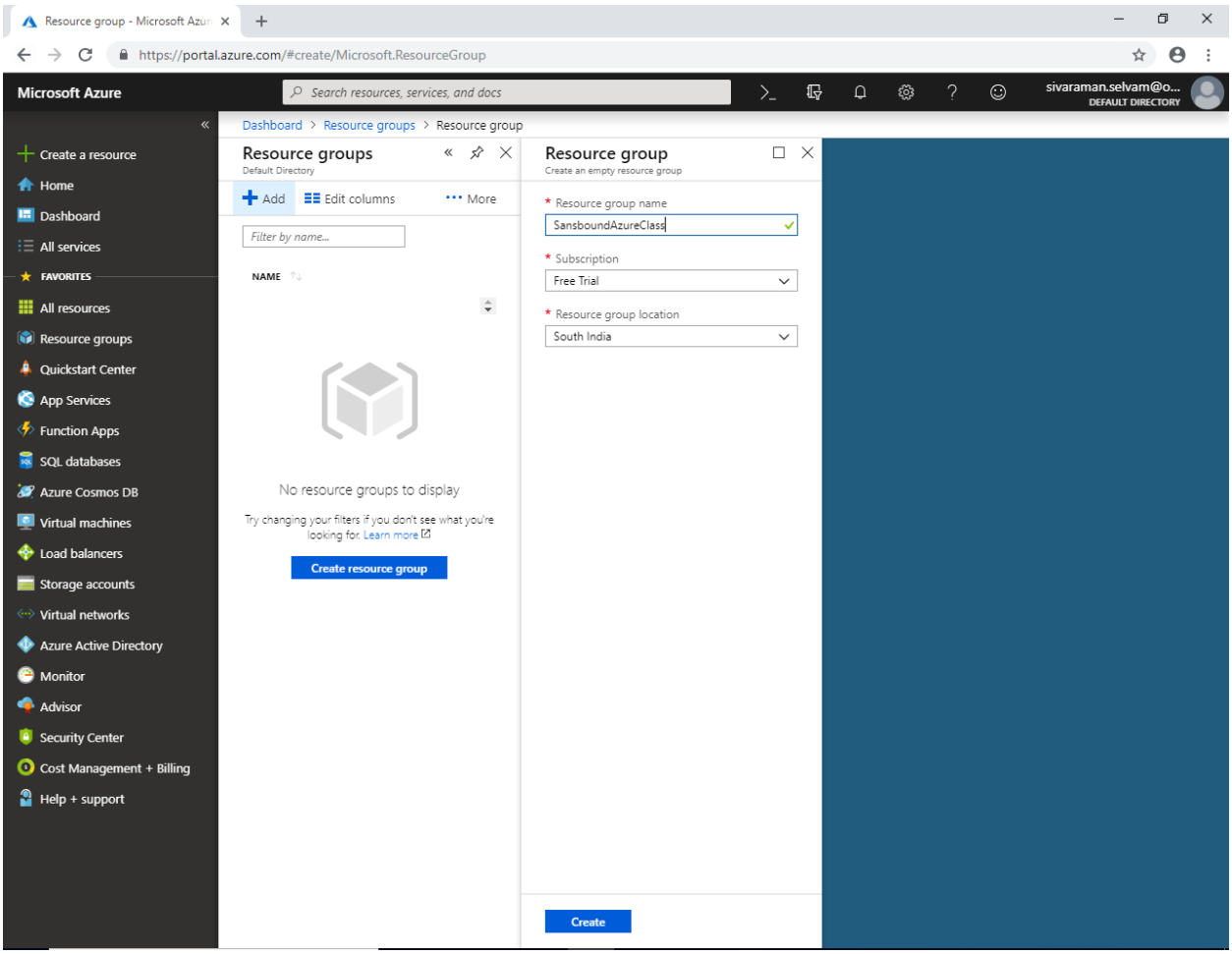
In Azure portal, click **"Resource Groups"**.



In “Resource Groups” click **“Add”.**

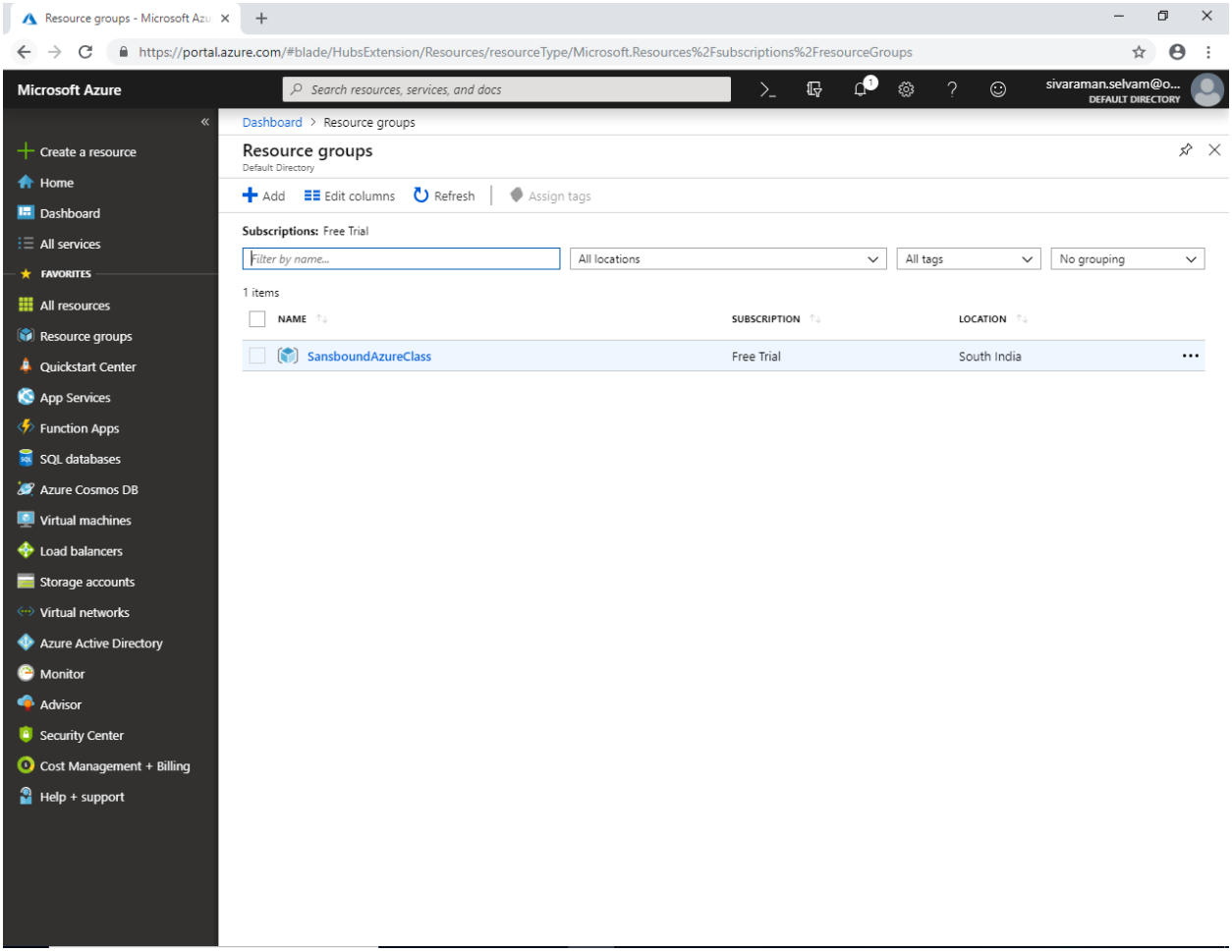


In “Resource Groups”, Type **“SansboundAzureClass”** as Resource group name.

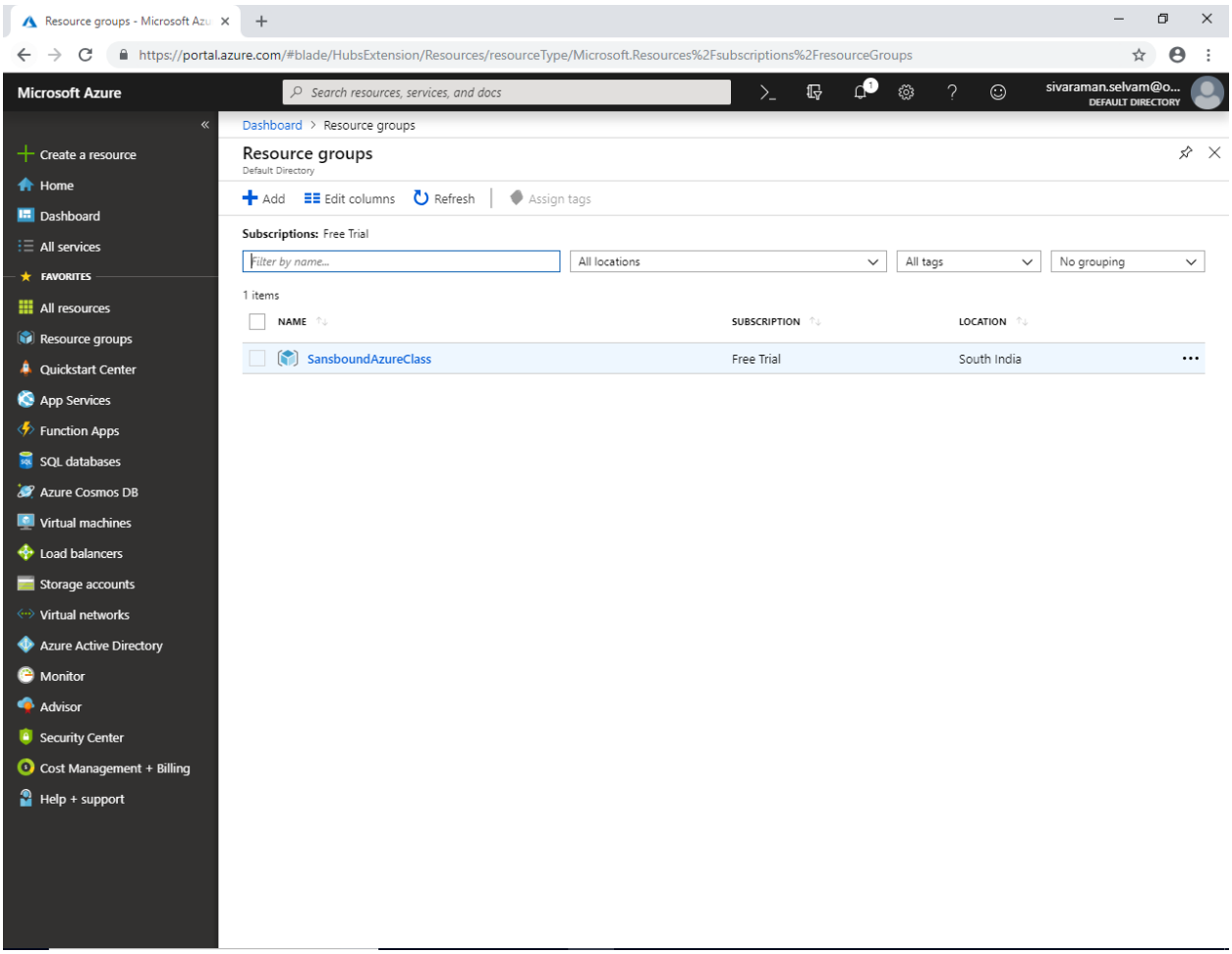


Click “Refresh” to view Resource groups.

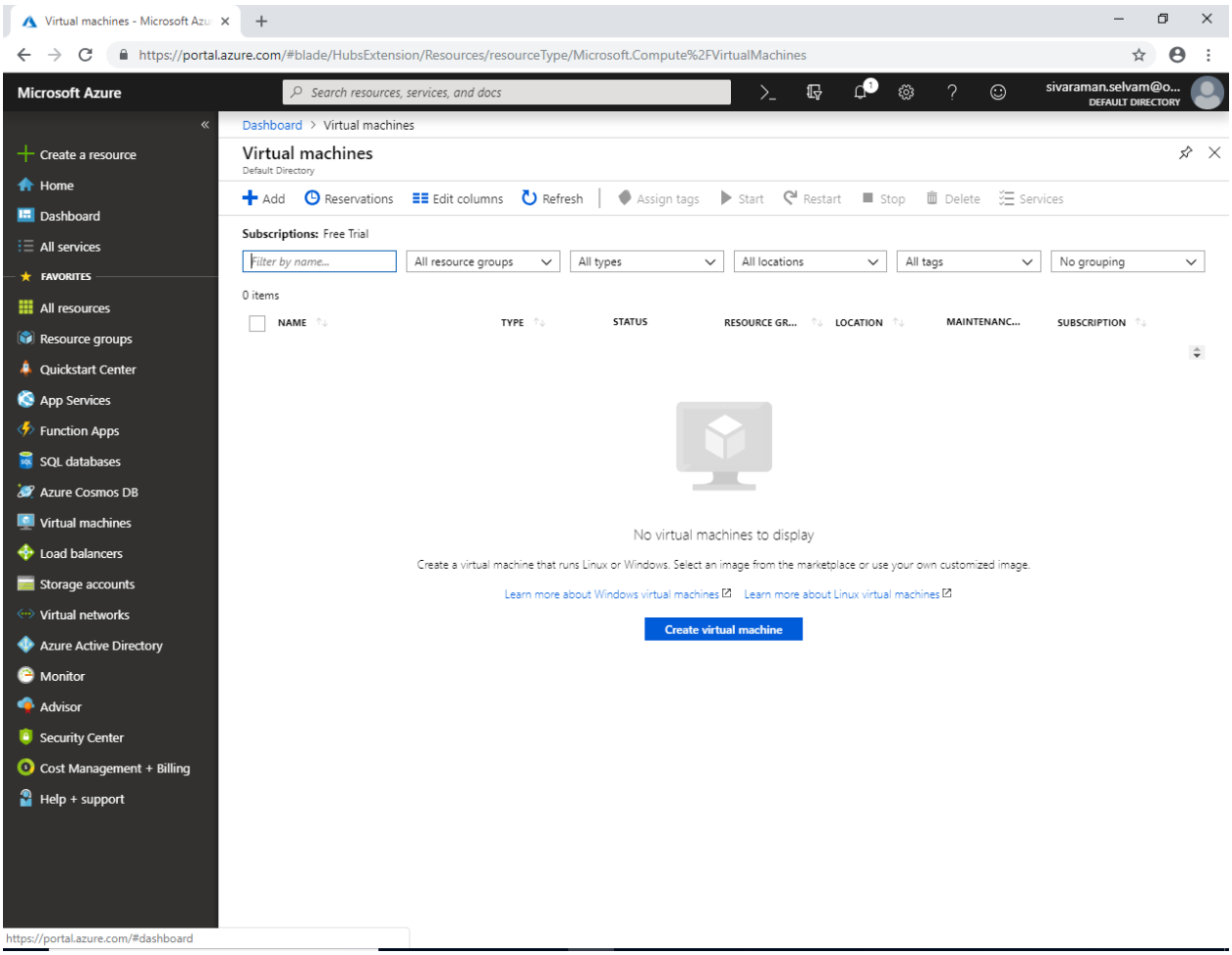
You are able to see that created “Resource Groups” named as **“SansboundAzureClass”**.



Click **“Virtual machines”** in left side panel.



In **“Virtual machines”** click **“Add”**.



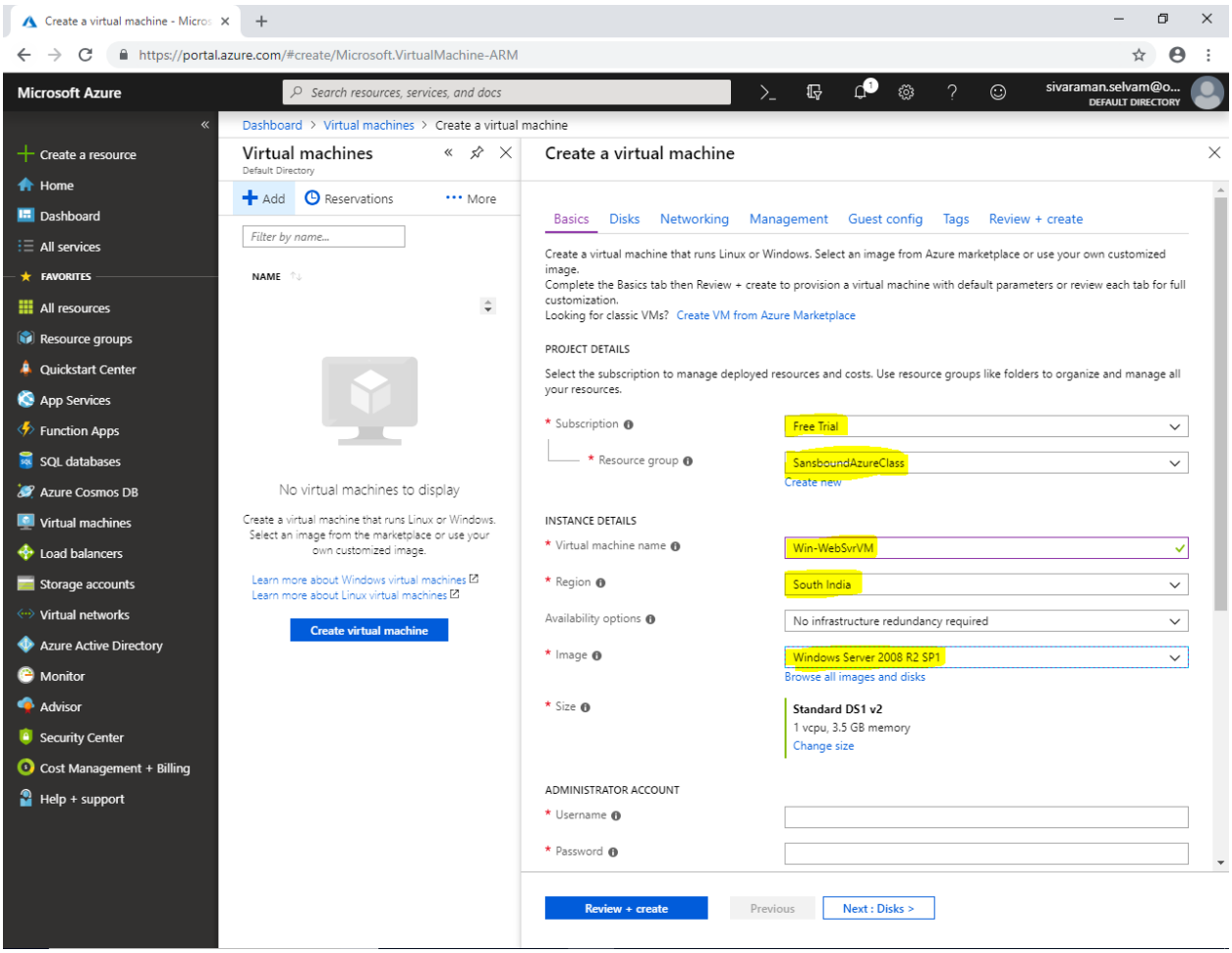
Select “Subscription”

Select “Resource Group” name as “SansboundAzureClass”.

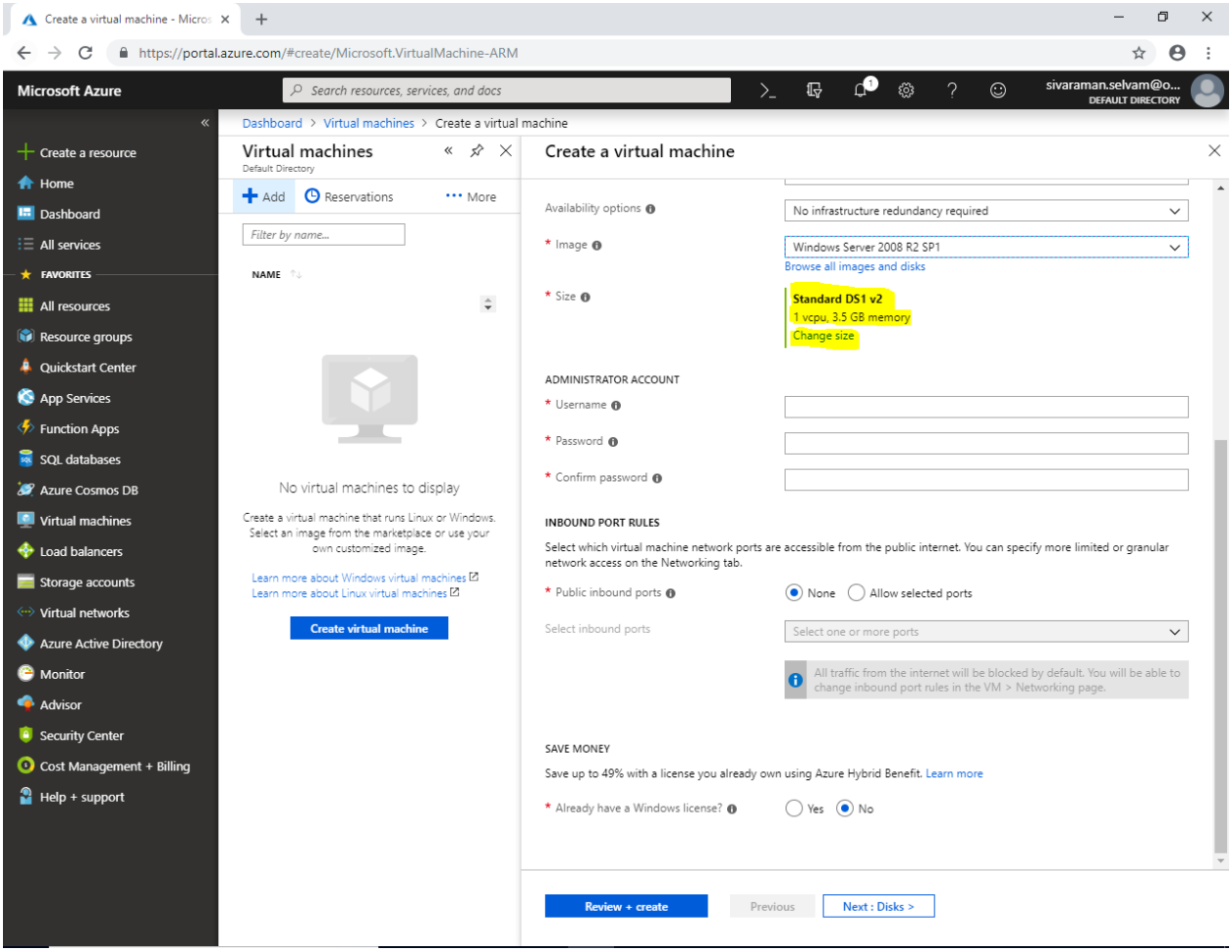
Type “Virtual machine name” as “Win-WebSvrVM”.

Select “Region” as “South India”.

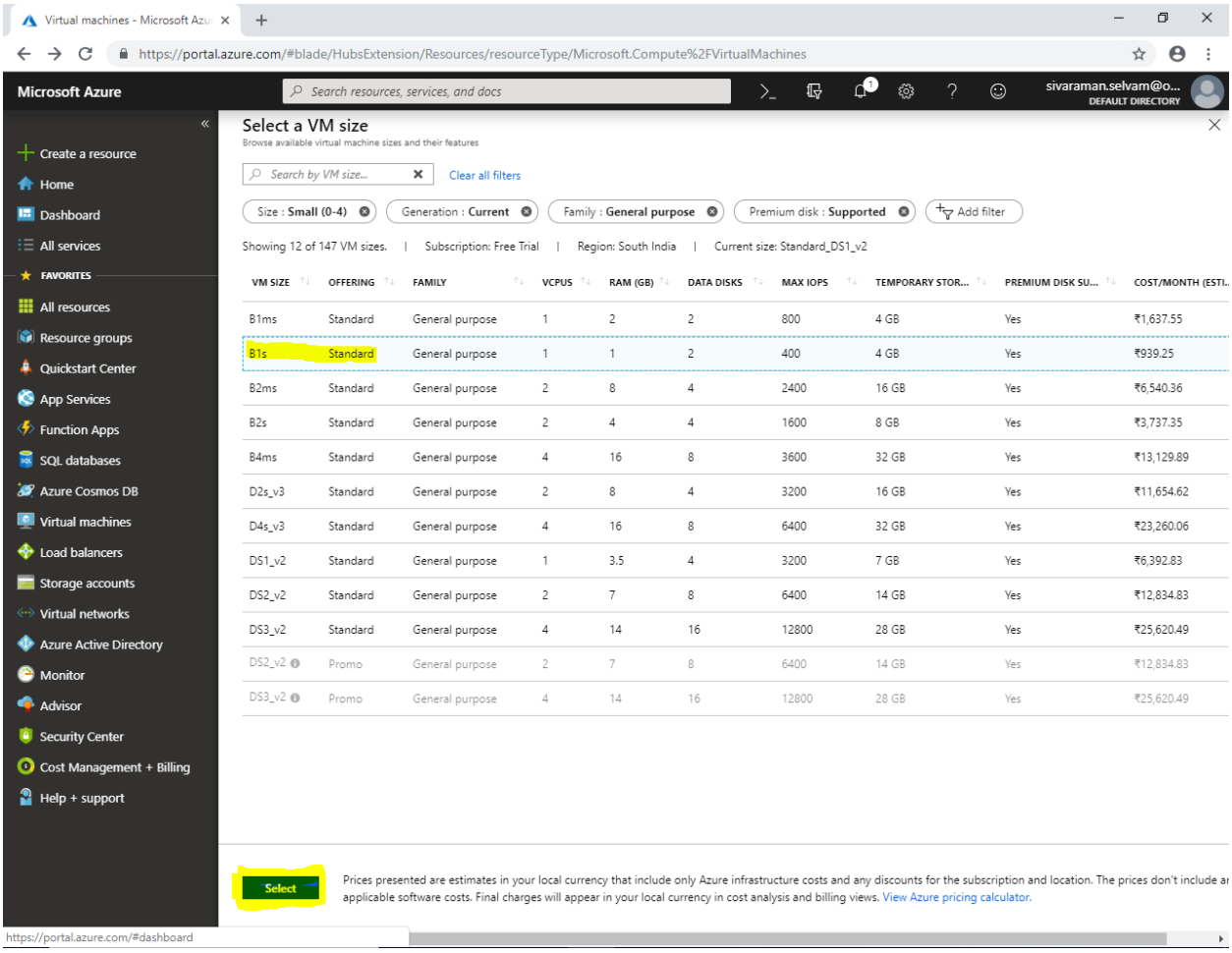
Select OS Image “Windows Server 2008 R2 SP1”.



By default VM Size is as **"Standard DS1 v2"** and 1 vCPU and 3.5 GB memory. You should change the VM Size by click **"Change Size"**.

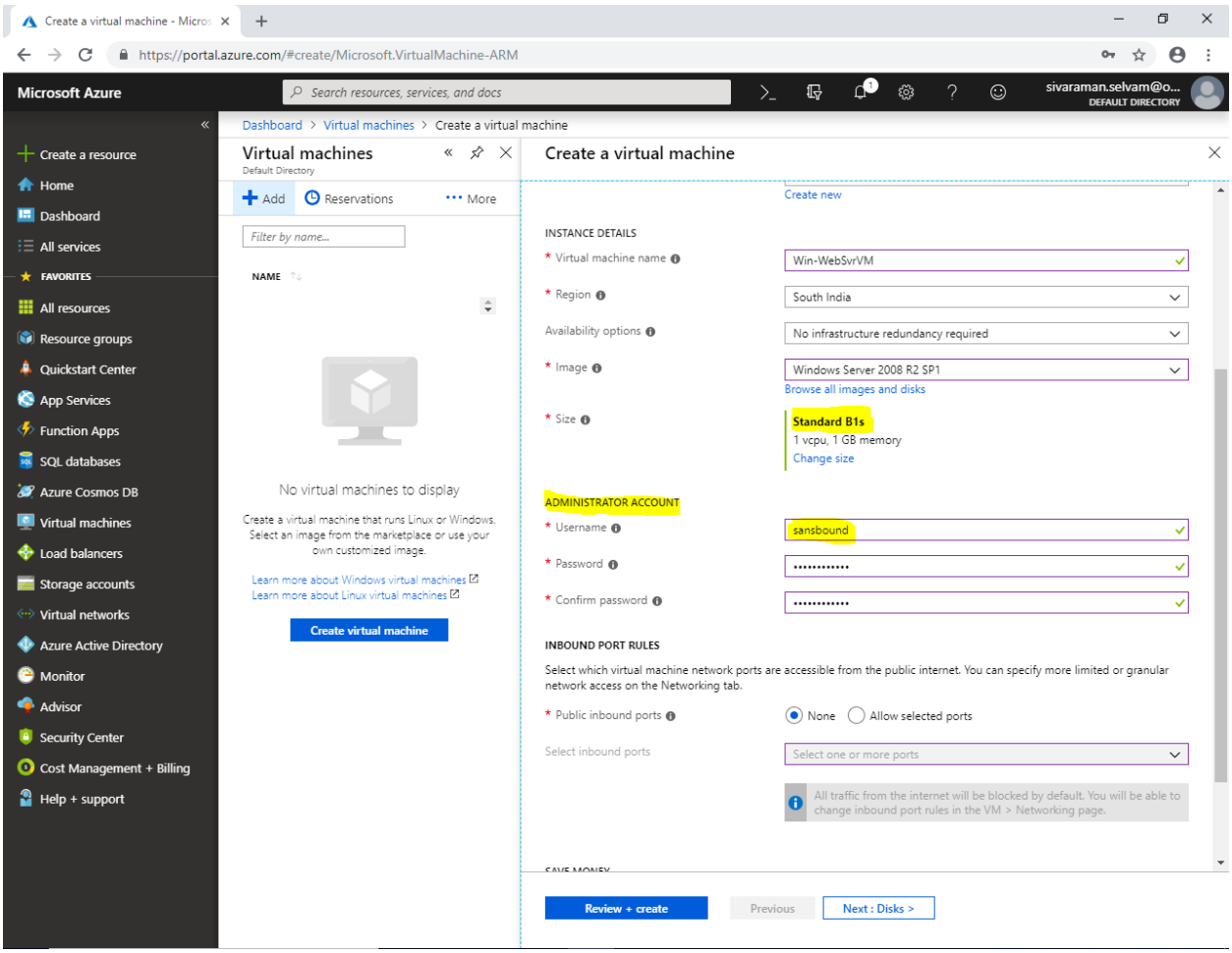


In **"VM Size"** click on **"B1s - Standard"** **and click "Select".**



Ensure that **"Standard B1s"** VM Size is selected.

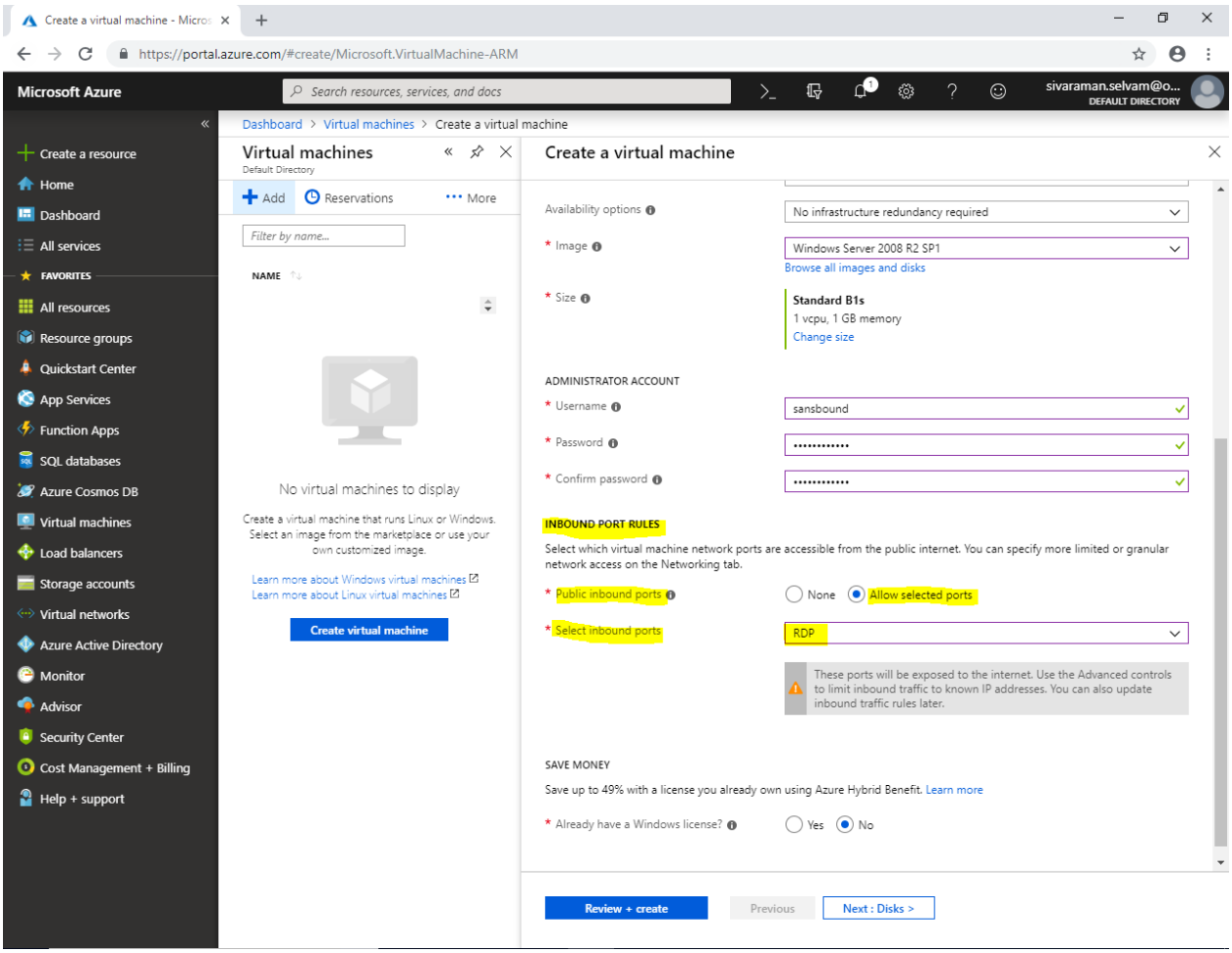
In **"Administrator Account"** type username as **"sansbound"** and type your own password.



In **“Inbound Port Rules”**

In **“Public inbound ports”** click **“Allow selected ports”**.

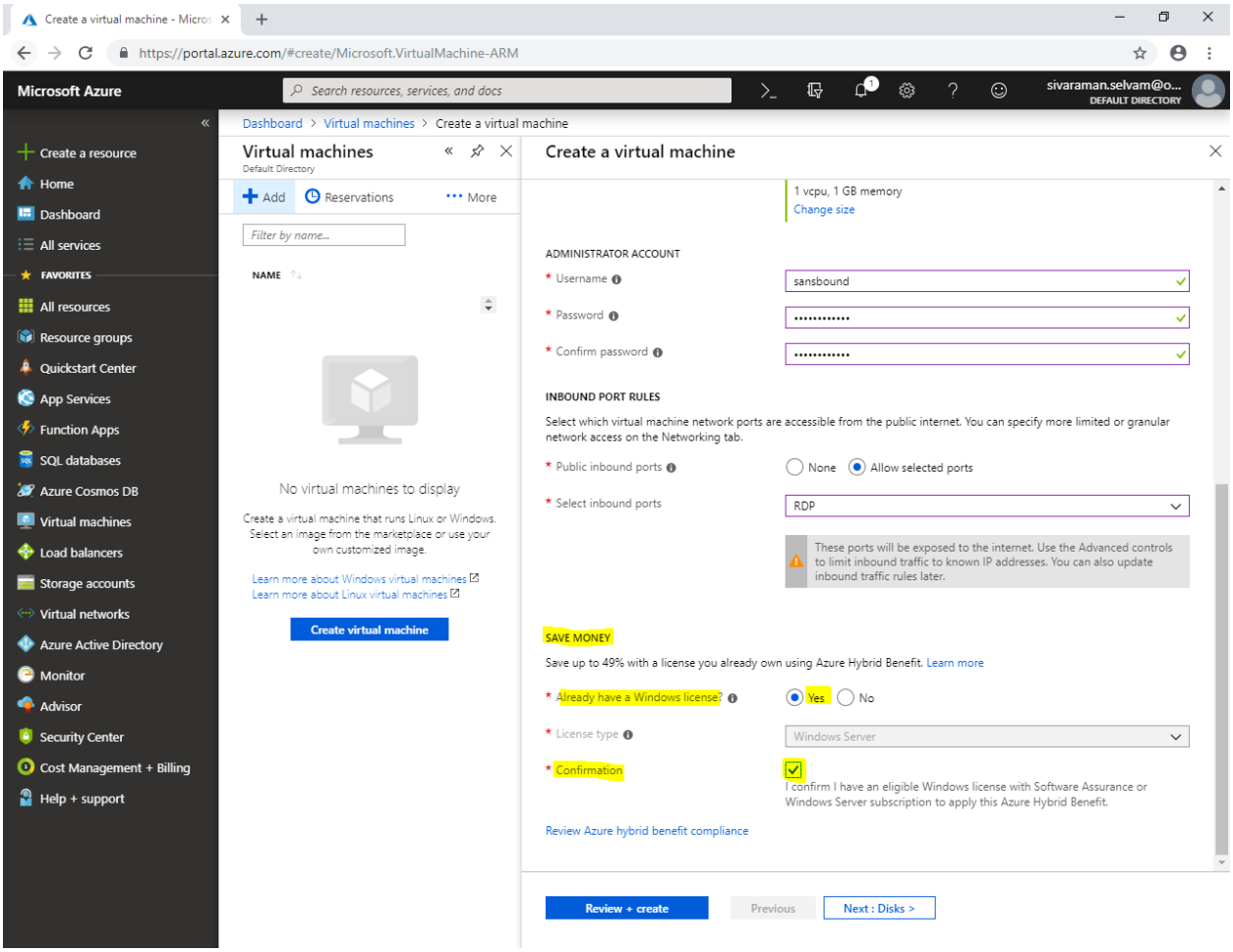
In **“Select inbound ports”** select **“RDP (3389)”** from the drop down list.



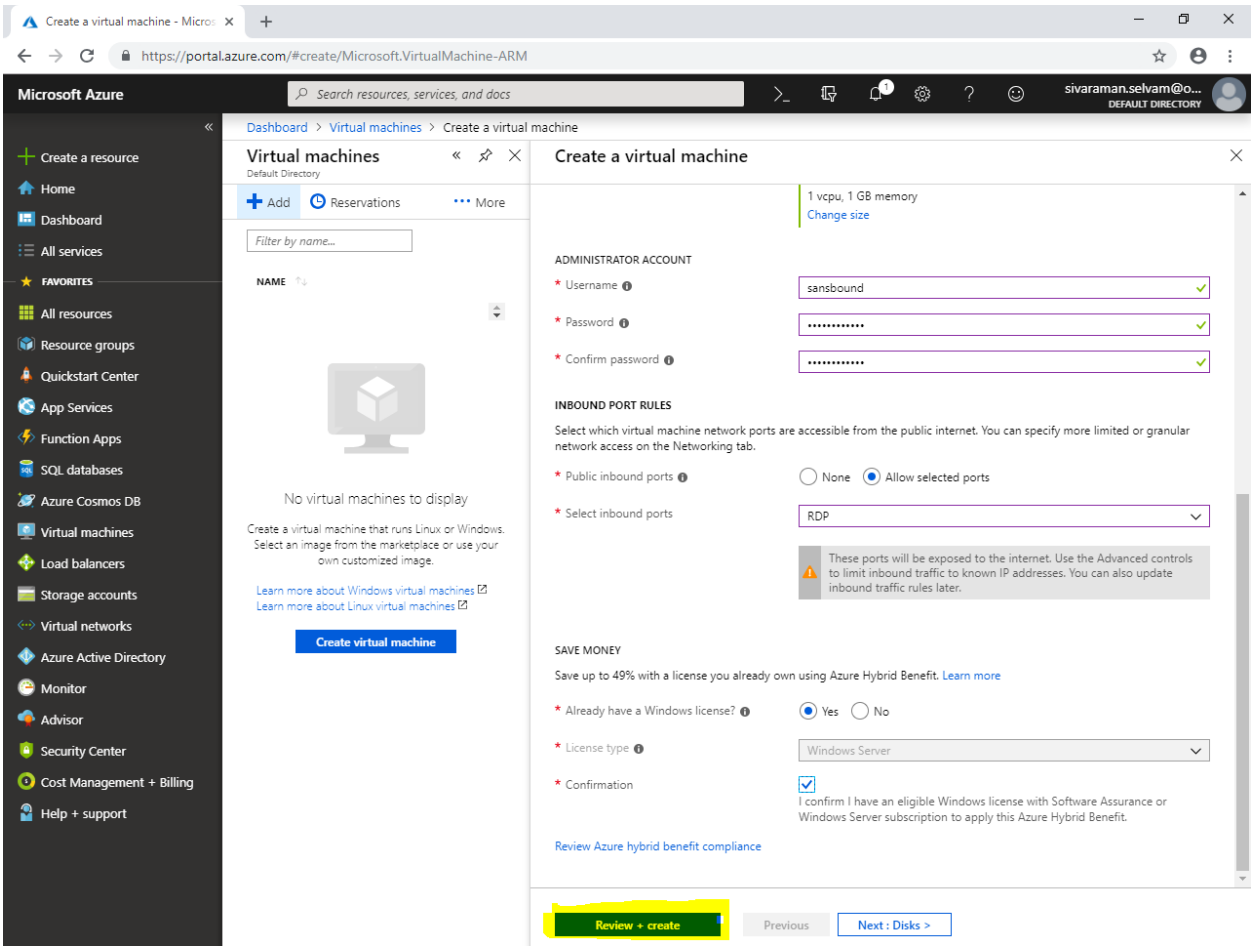
In “Save Money”,

Always have a Windows license as **“Yes”**.

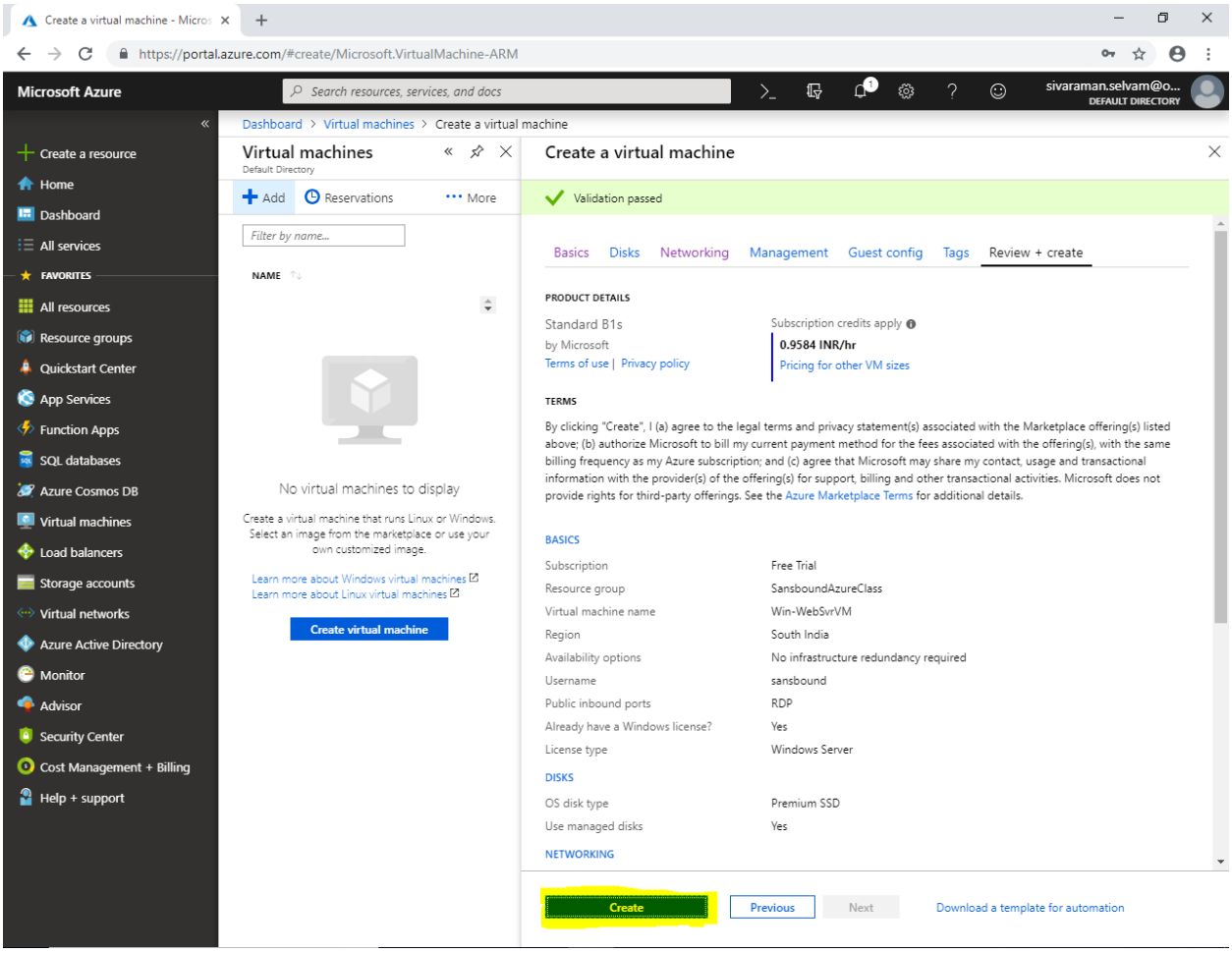
Check the **“Confirmation”** box.



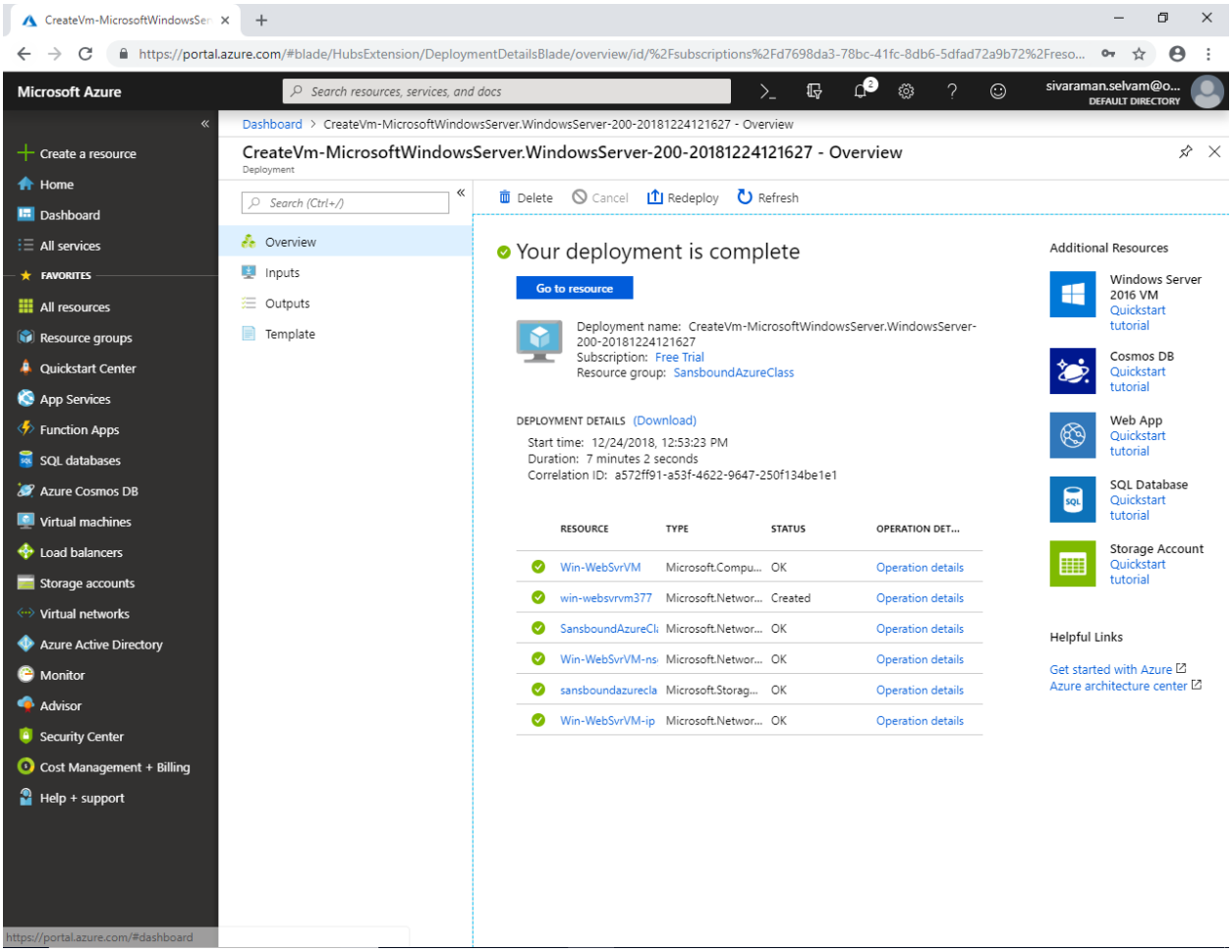
Then click **“Review + Create”**.



Click **"Create"** in bottom of the portal.

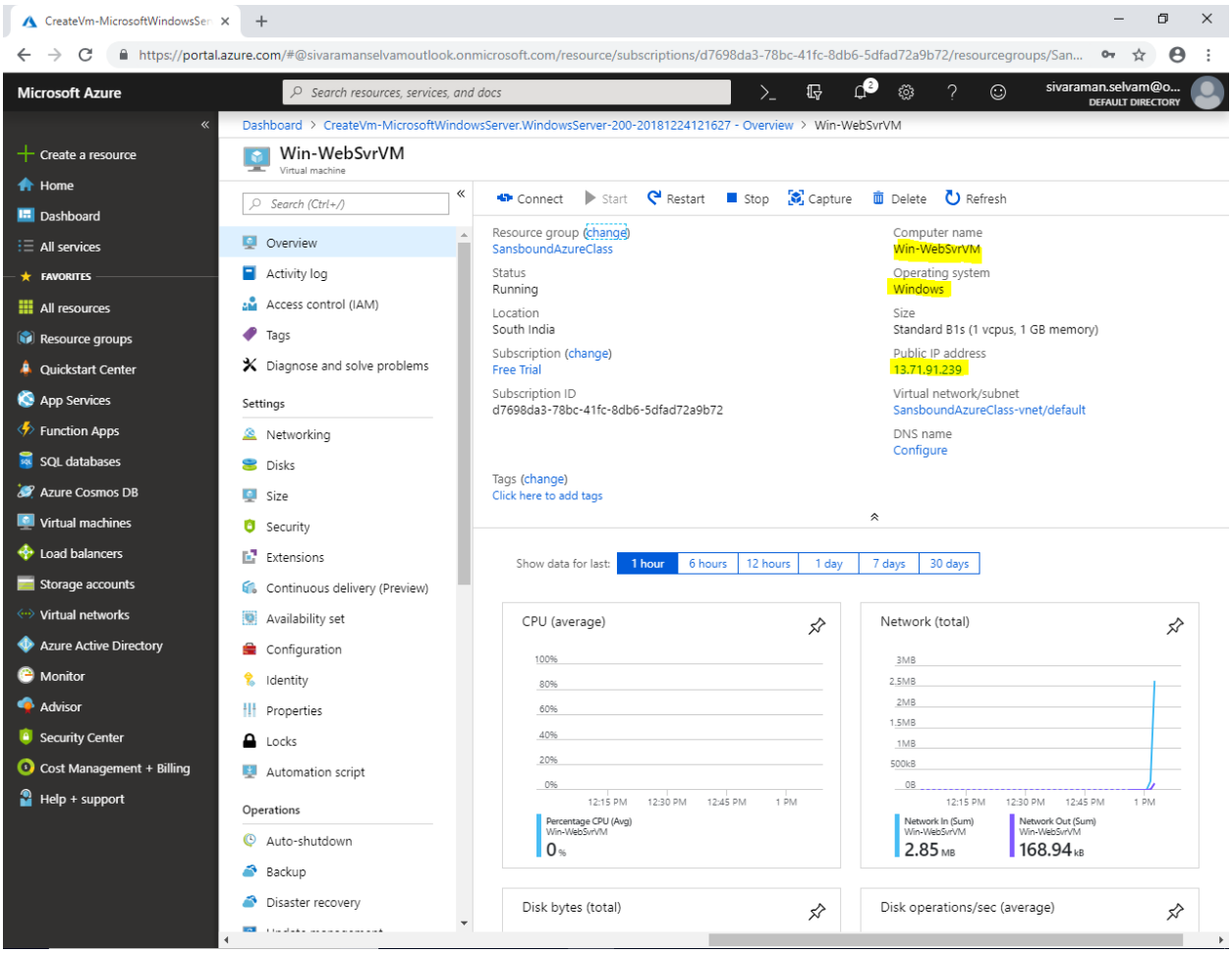


Click “Go to resource”.

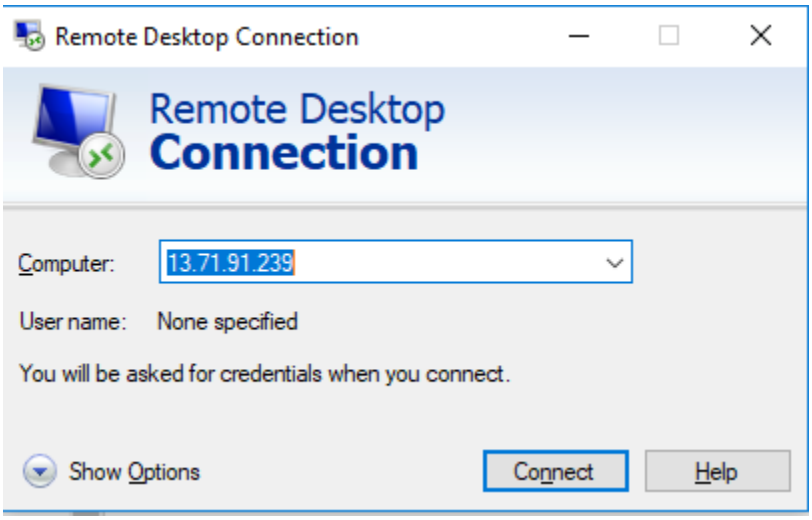


We have selected “Windows 2008 R2 Sp1”.

Kindly note the public IP address of the Windows VM which has been created for Web server.



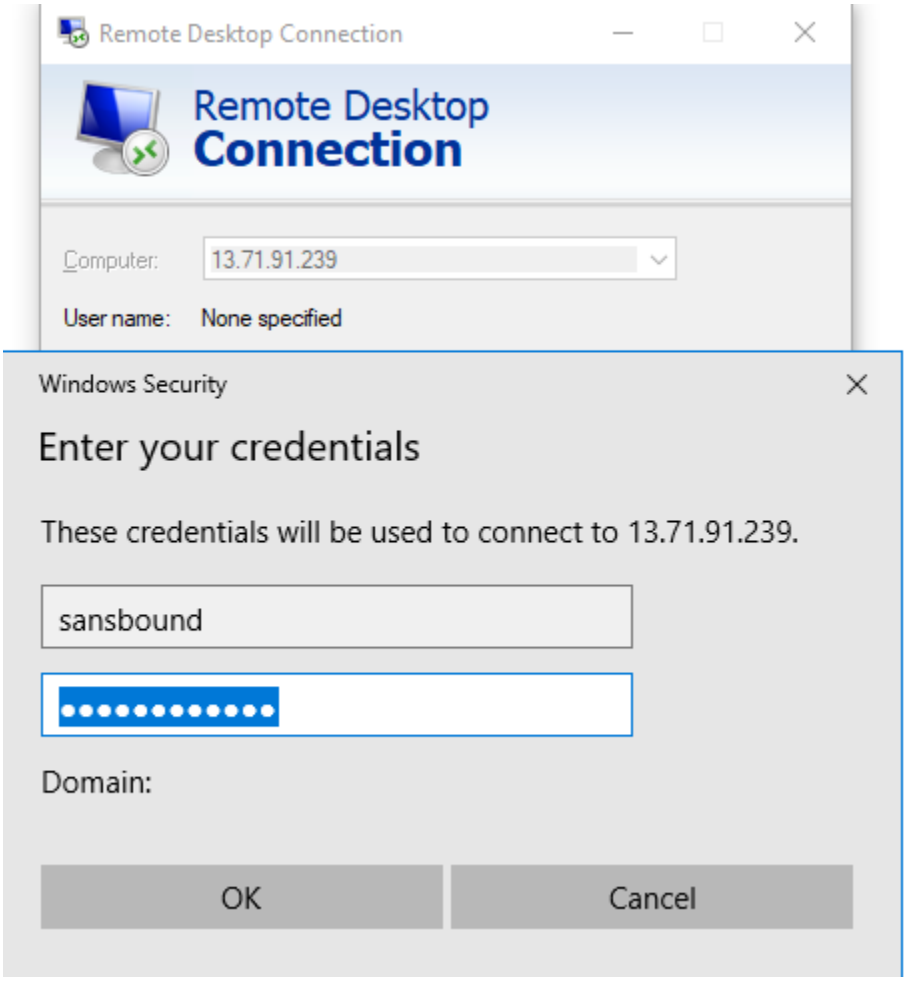
Type **“mstsc”** in run box and press “Enter”.



Click **”Connect”**

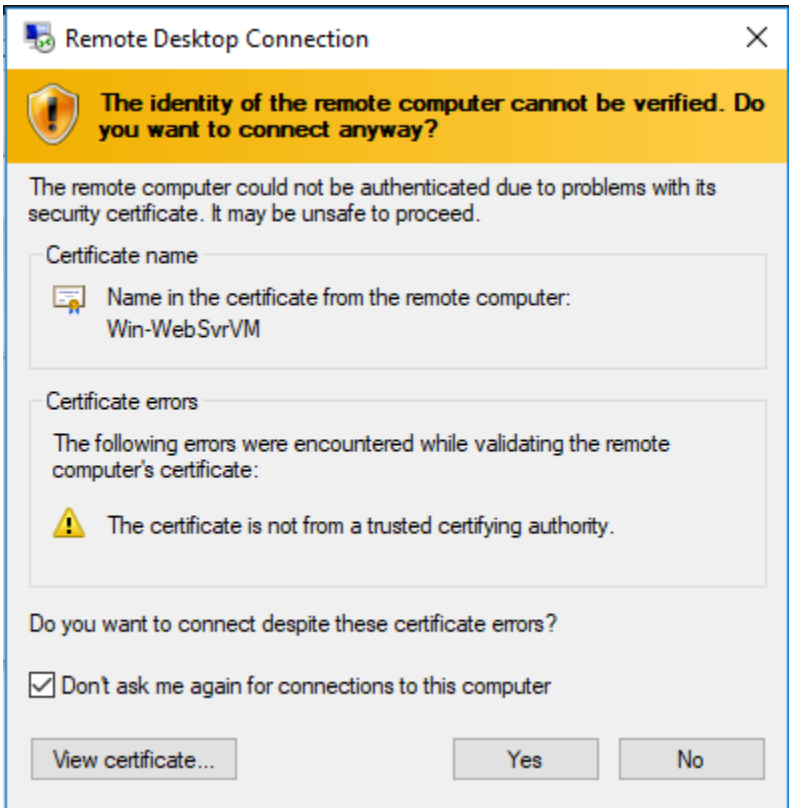
Type username as “sanbound”

Type password for the server which you have specified in the Azure portal while creating VM.

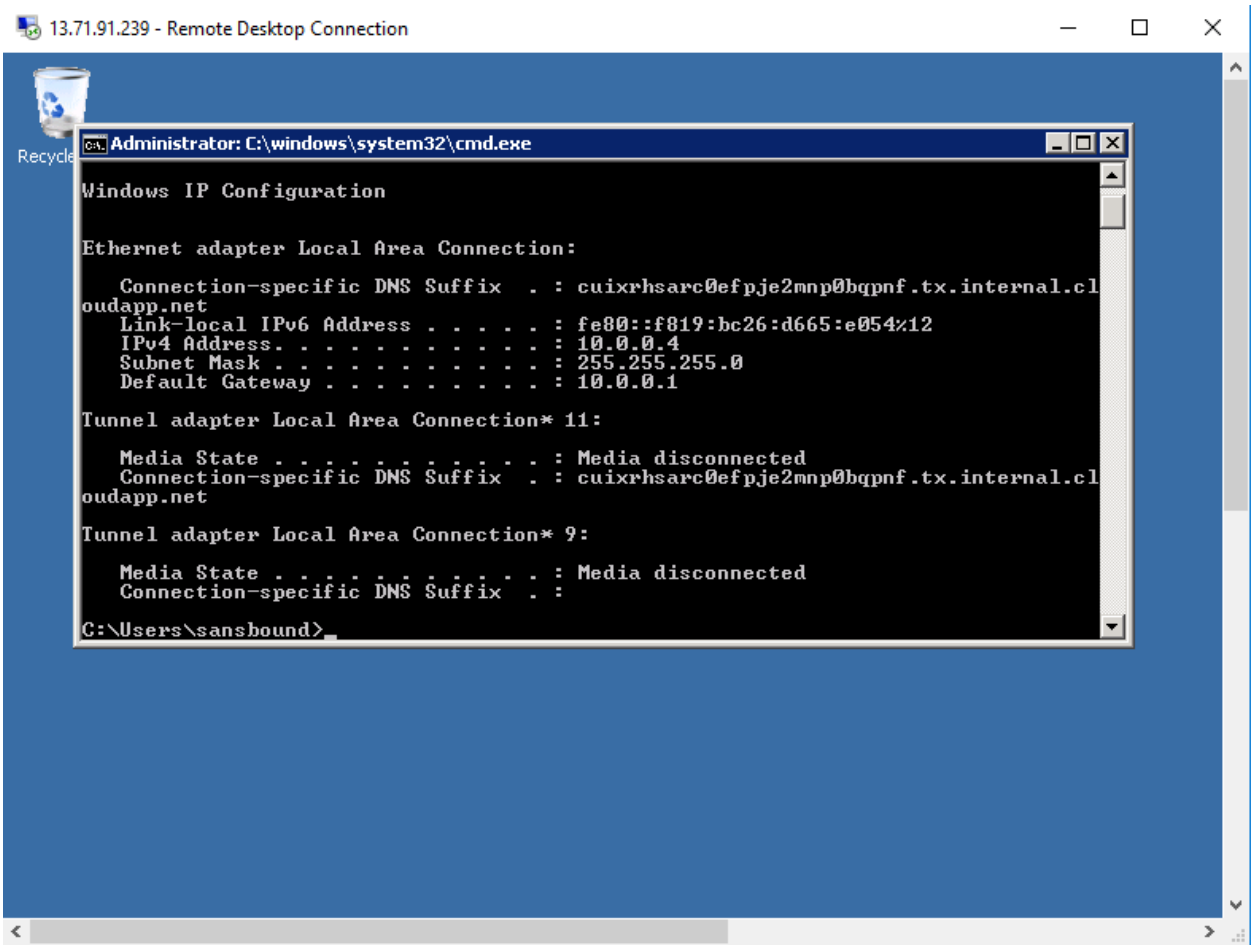


Click **”Ok”.**

Click “Yes”.

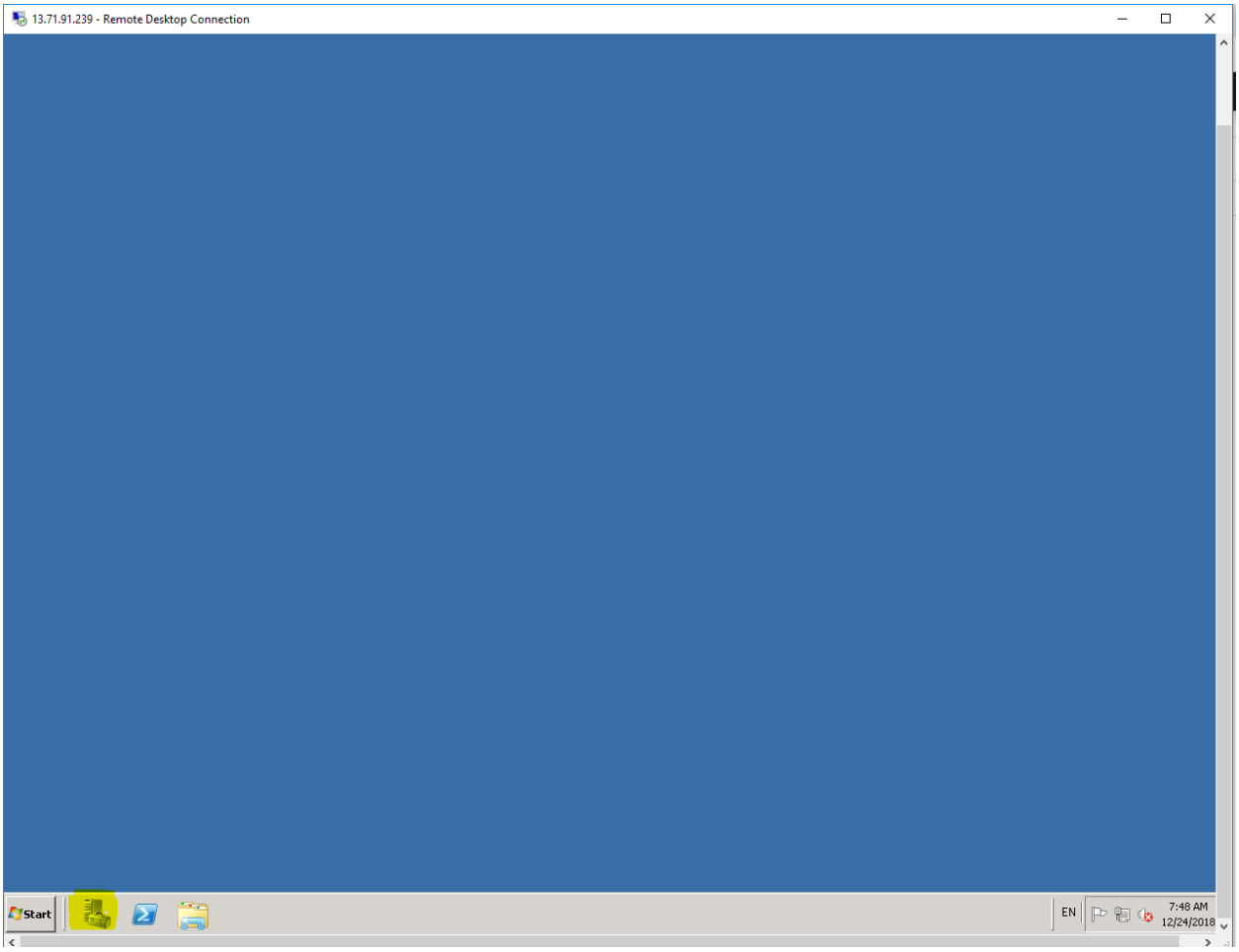

Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
Win-WebSvrVM
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No

I have got **10.0.0.4** IP address for the **Windows 2008 R2 Sp1** server.

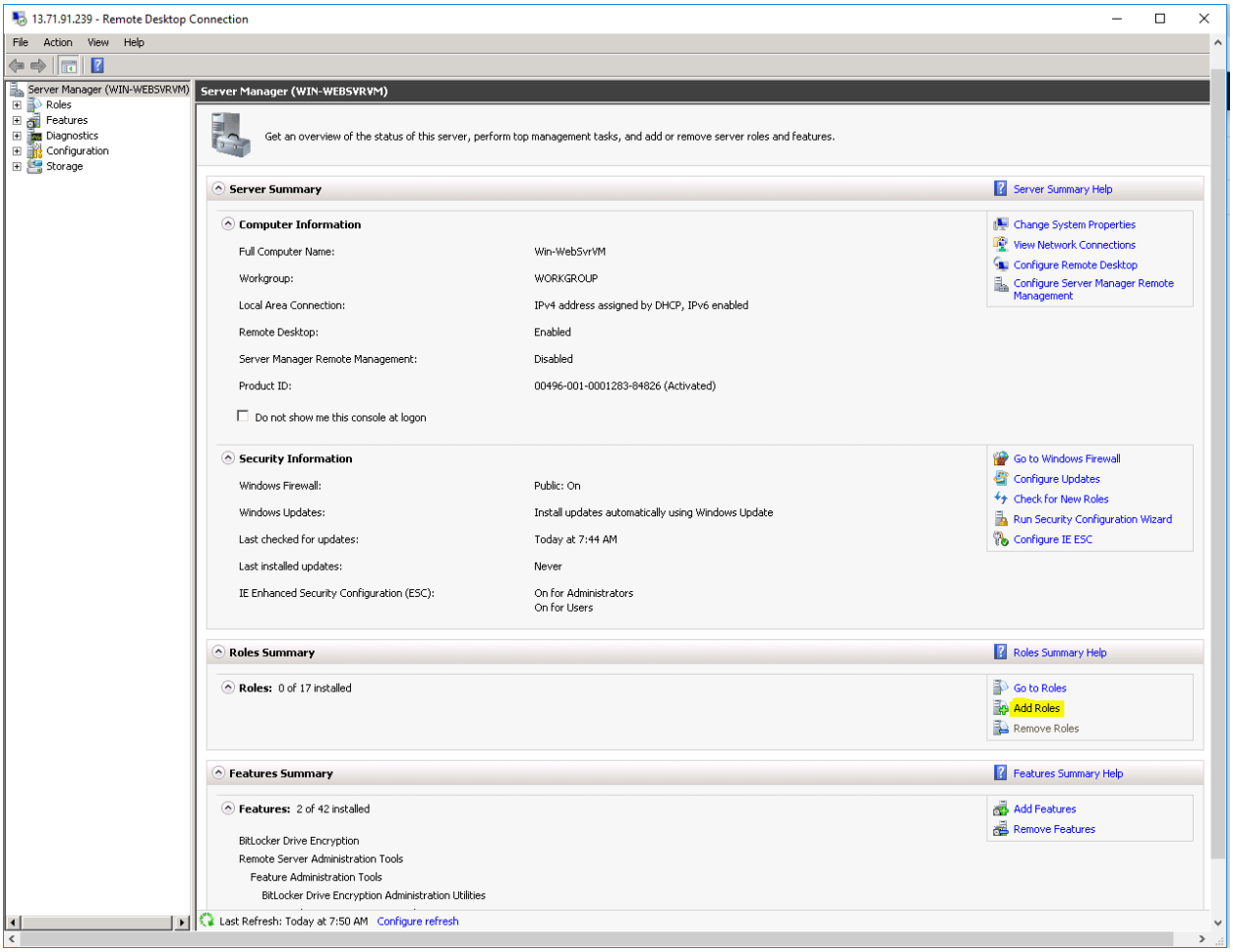


Now I have required to install "IIS" in Windows 2008 R2 Sp1 Server to configure as "Web server".

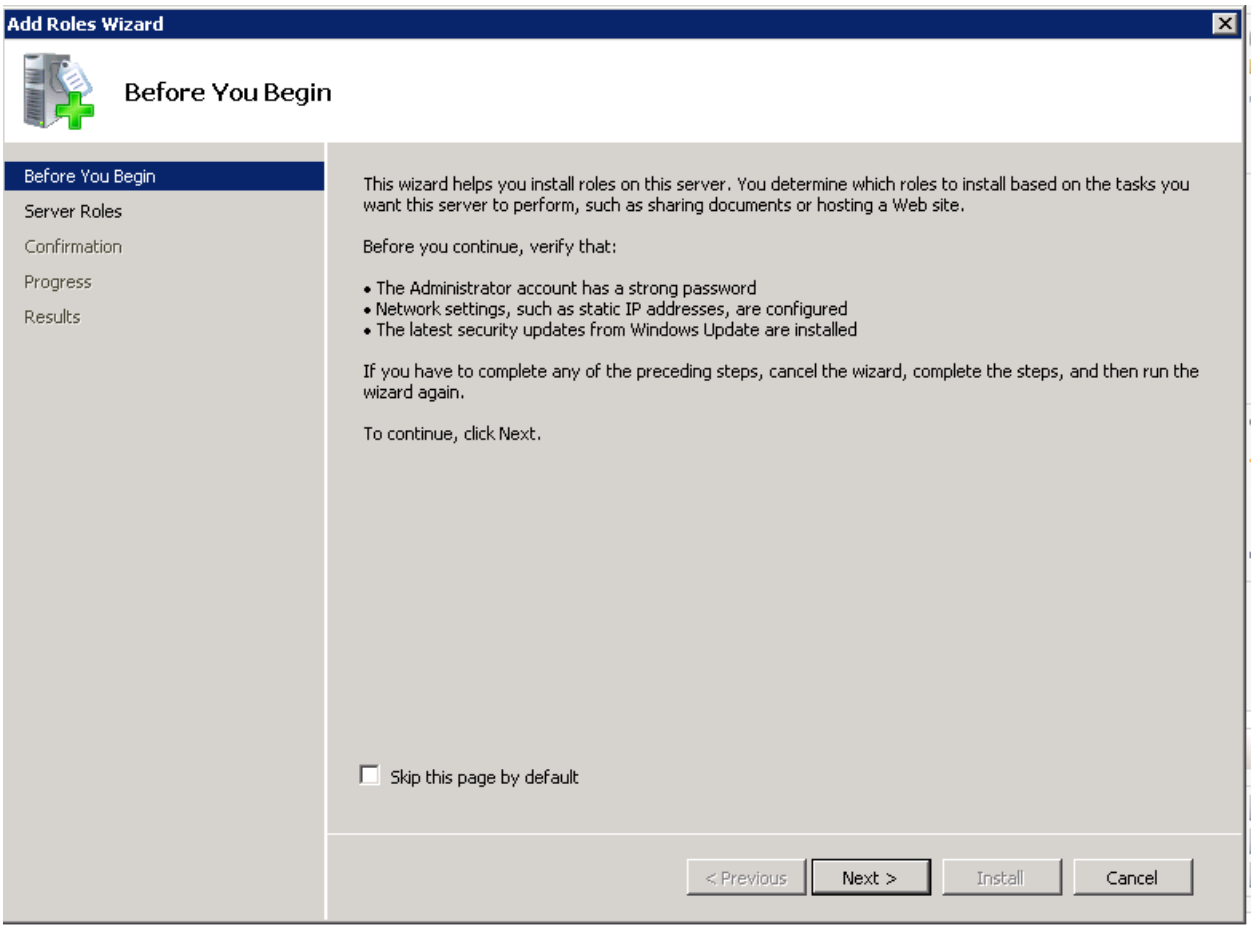
In "Windows 2008 R2 Server" click the high lighted icon of "Server Manager" in quick launch near start menu to launch it.



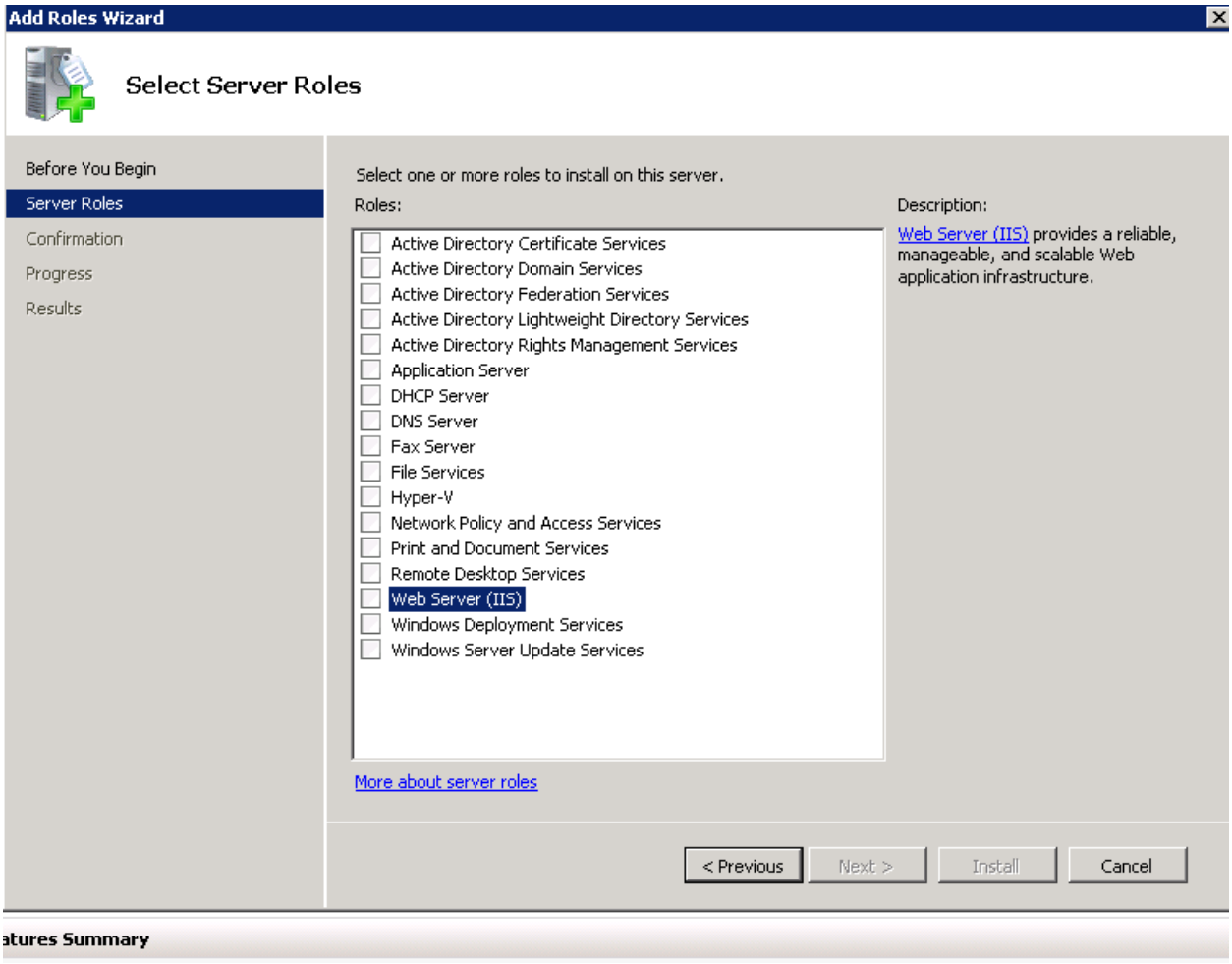
In “Roles Summary” click “Add Roles”.



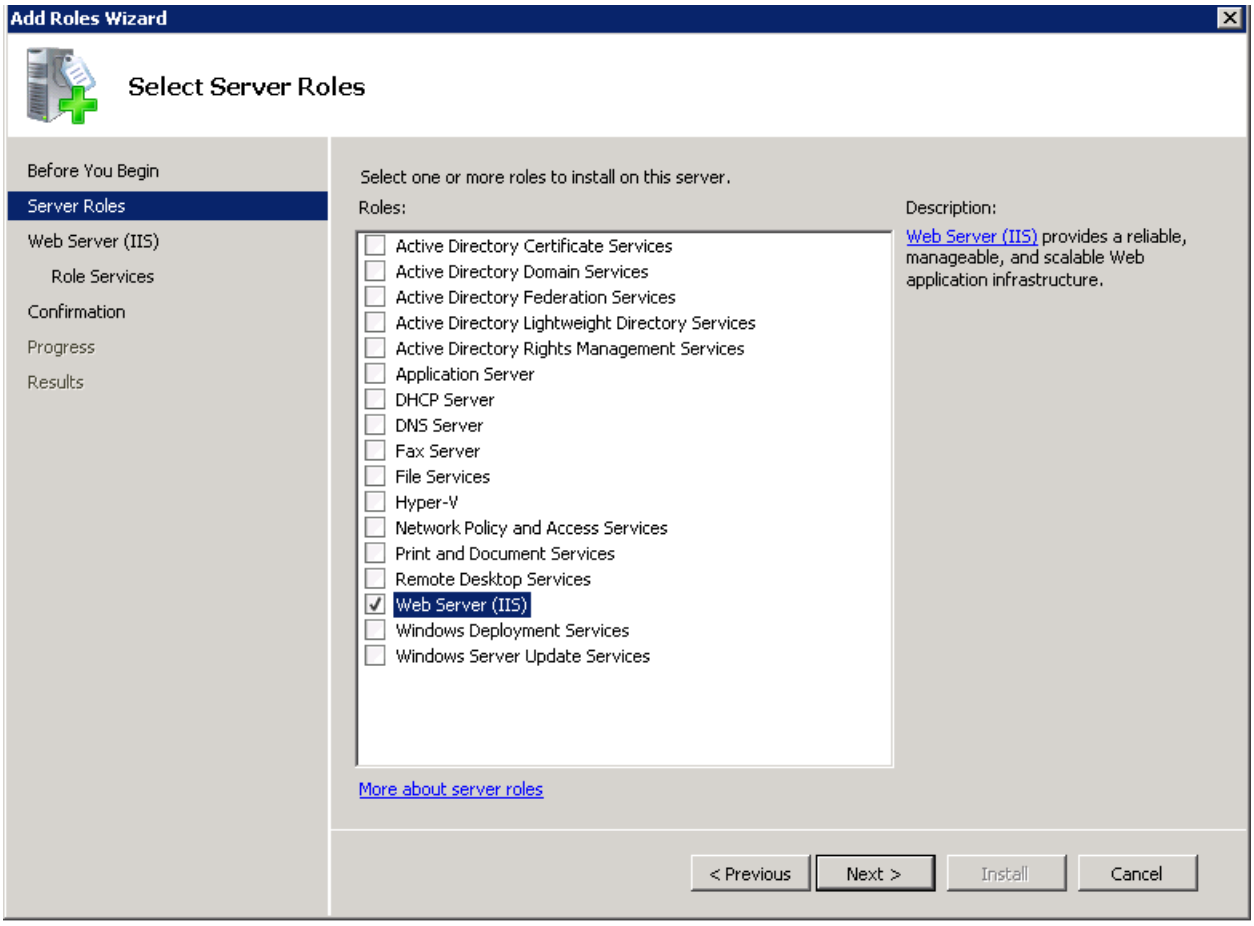
Click ”Next”.


Add Roles Wizard
Before You Begin
Before You Begin
Server Roles
Confirmation
Progress
Results
This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.
Before you continue, verify that:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The latest security updates from Windows Update are installed
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

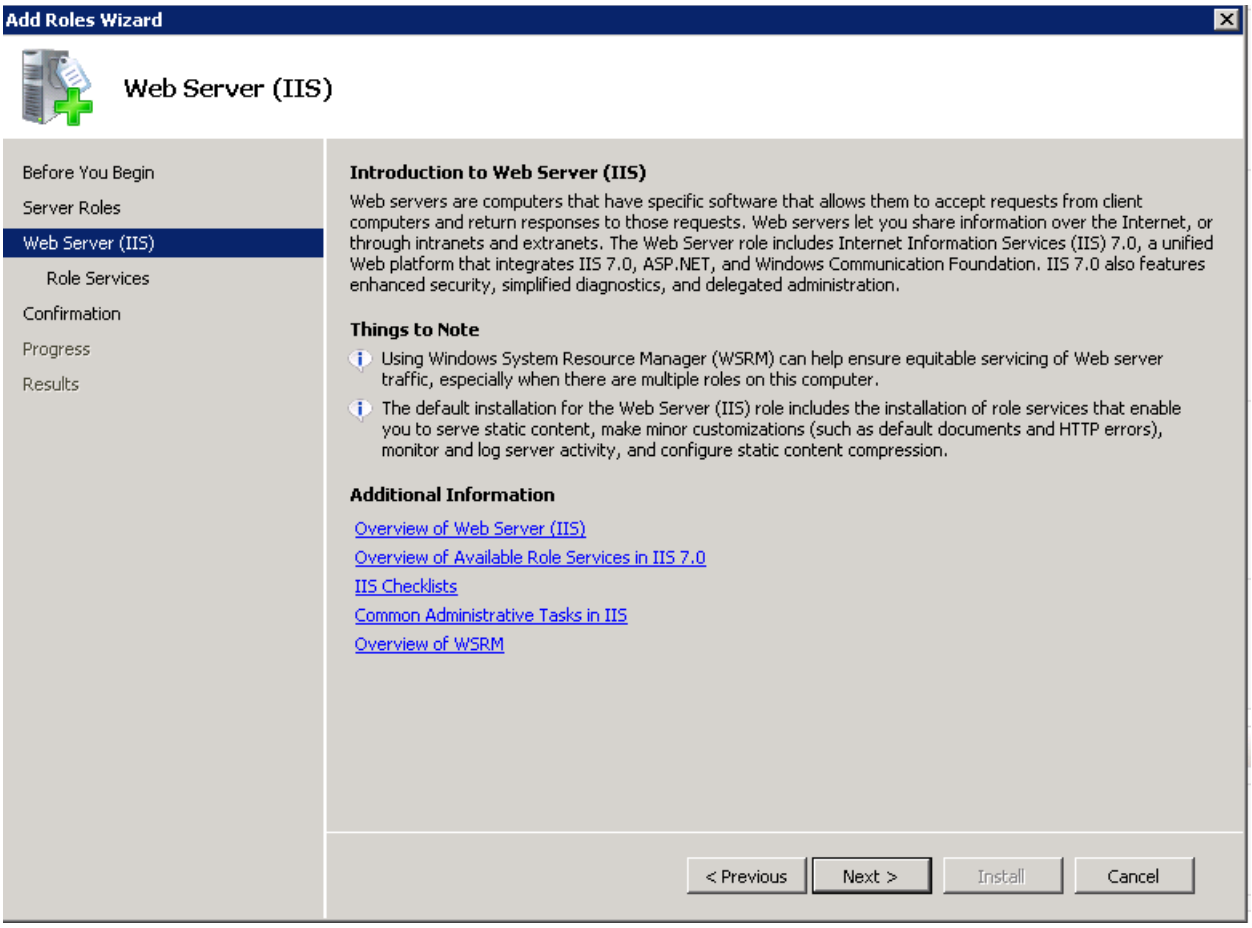
In "Web server" you need to Check it.



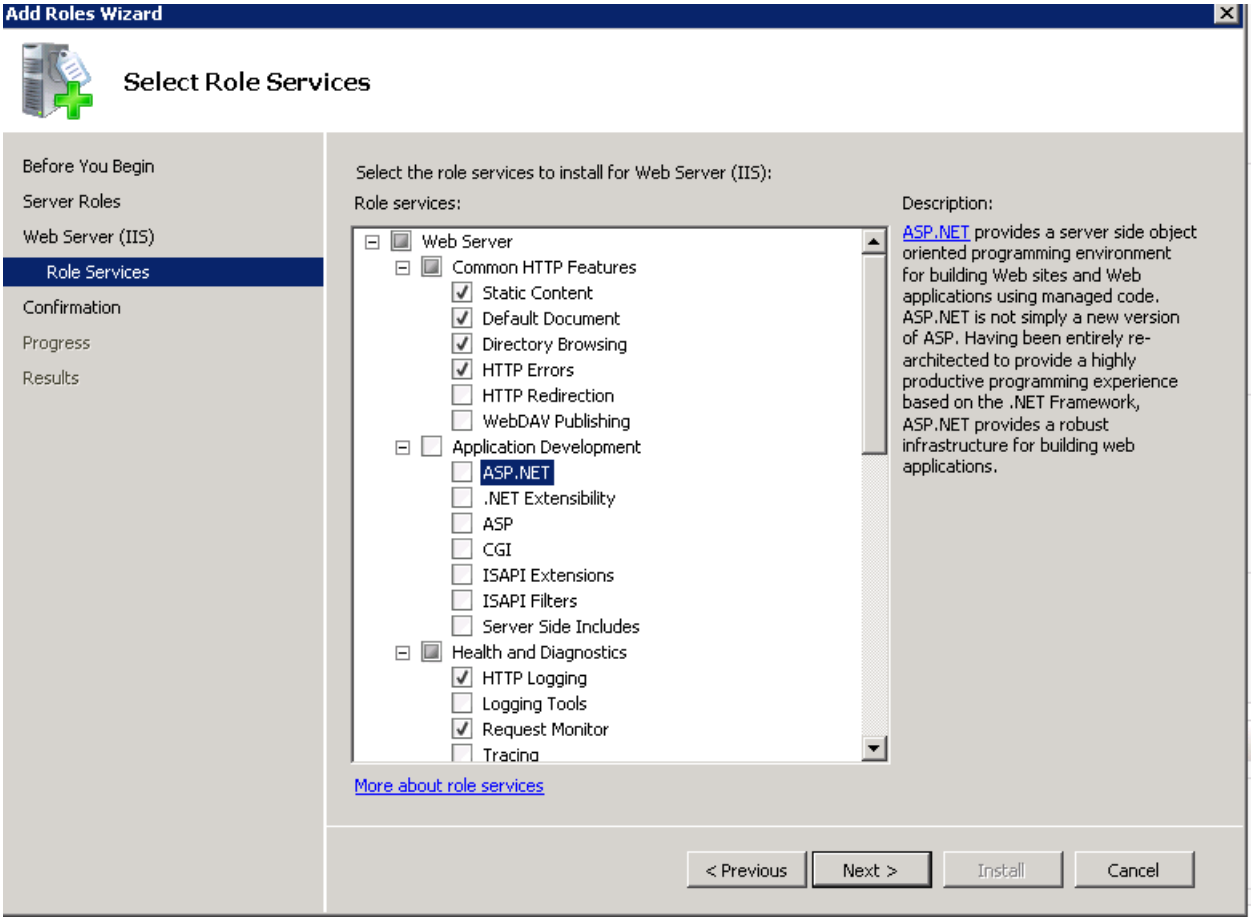
Ensure that “Web Server (IIS)” is selected and click “Next”.



Click “Next”.

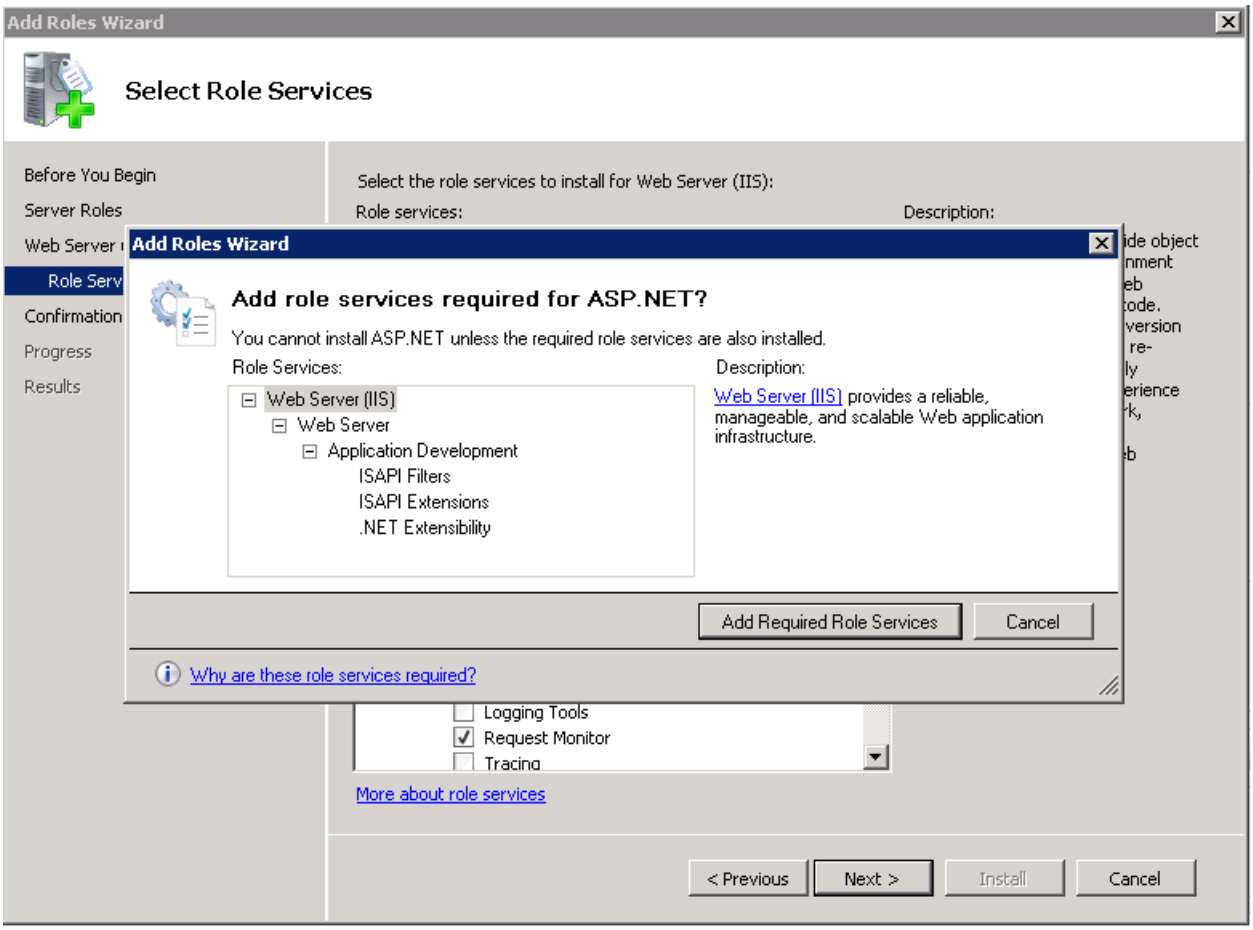

Add Roles Wizard
Web Server (IIS)
Before You Begin
Server Roles
Web Server (IIS)
Role Services
Confirmation
Progress
Results
Introduction to Web Server (IIS)
Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.
Things to Note
Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.
Additional Information
Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM
< Previous
Next >
Install
Cancel

In "Application Development", need to check "ASP .Net".

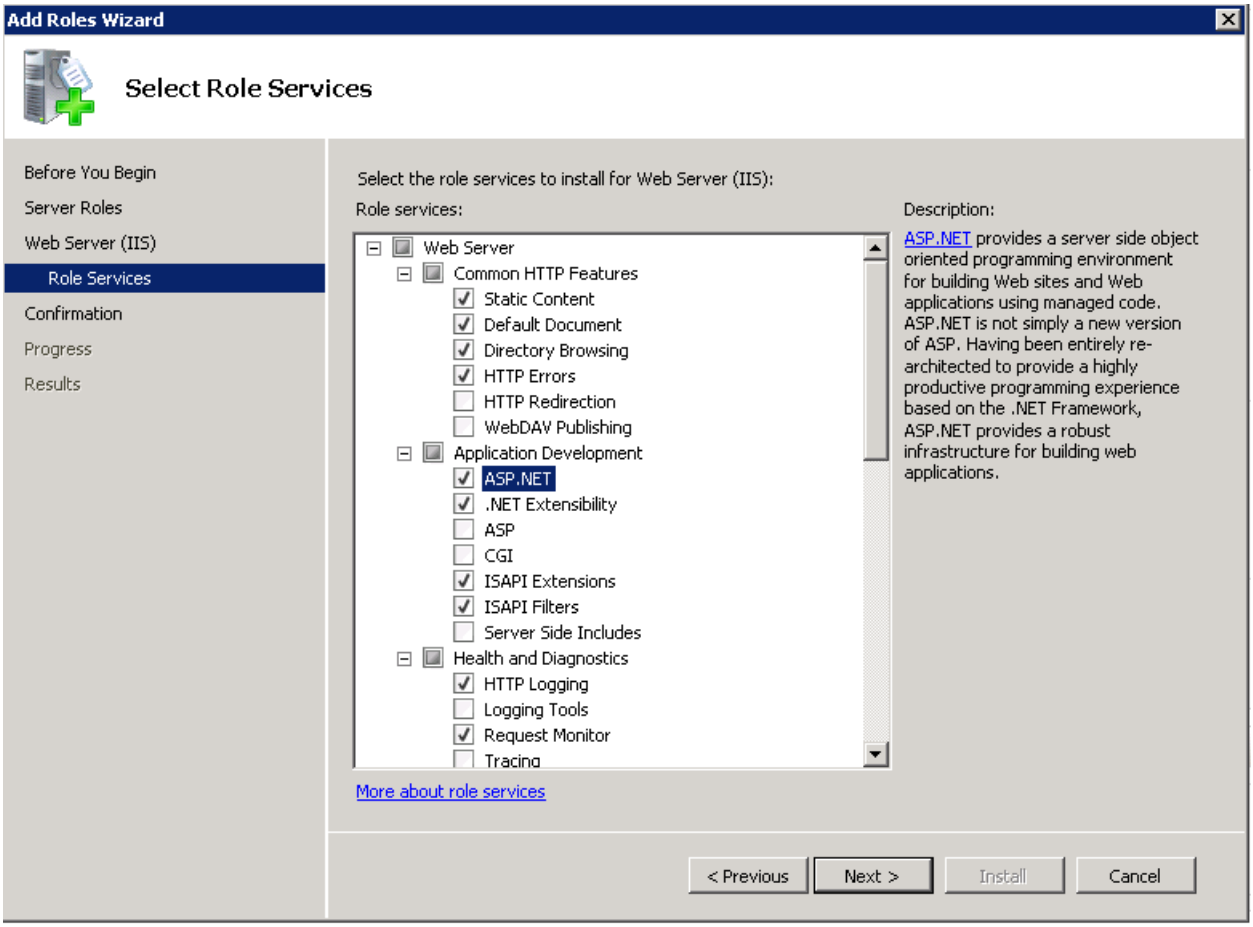


Once you have checked the ASP.NET check box, you will get below window.

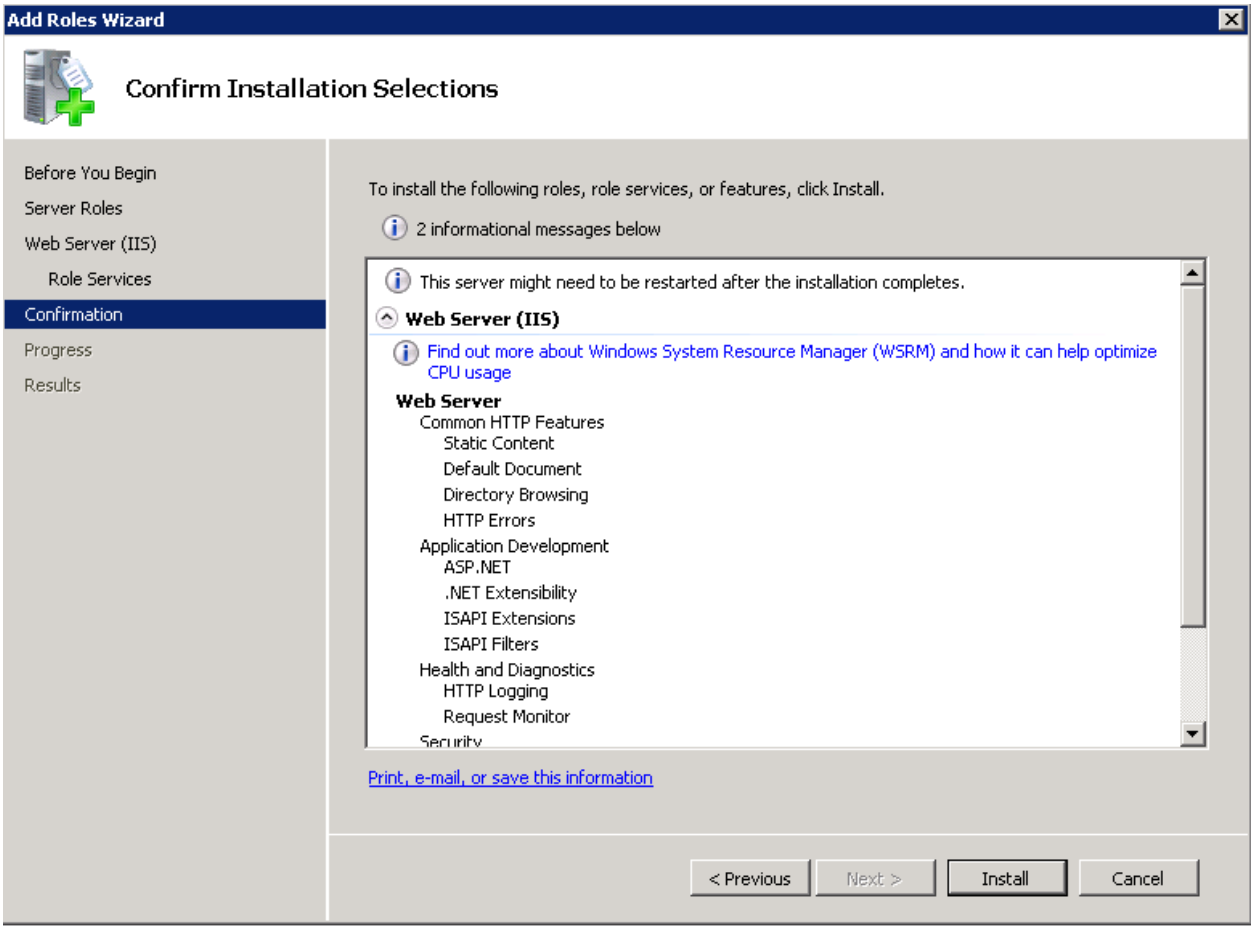
Click "Add required role services".



Click "Next".

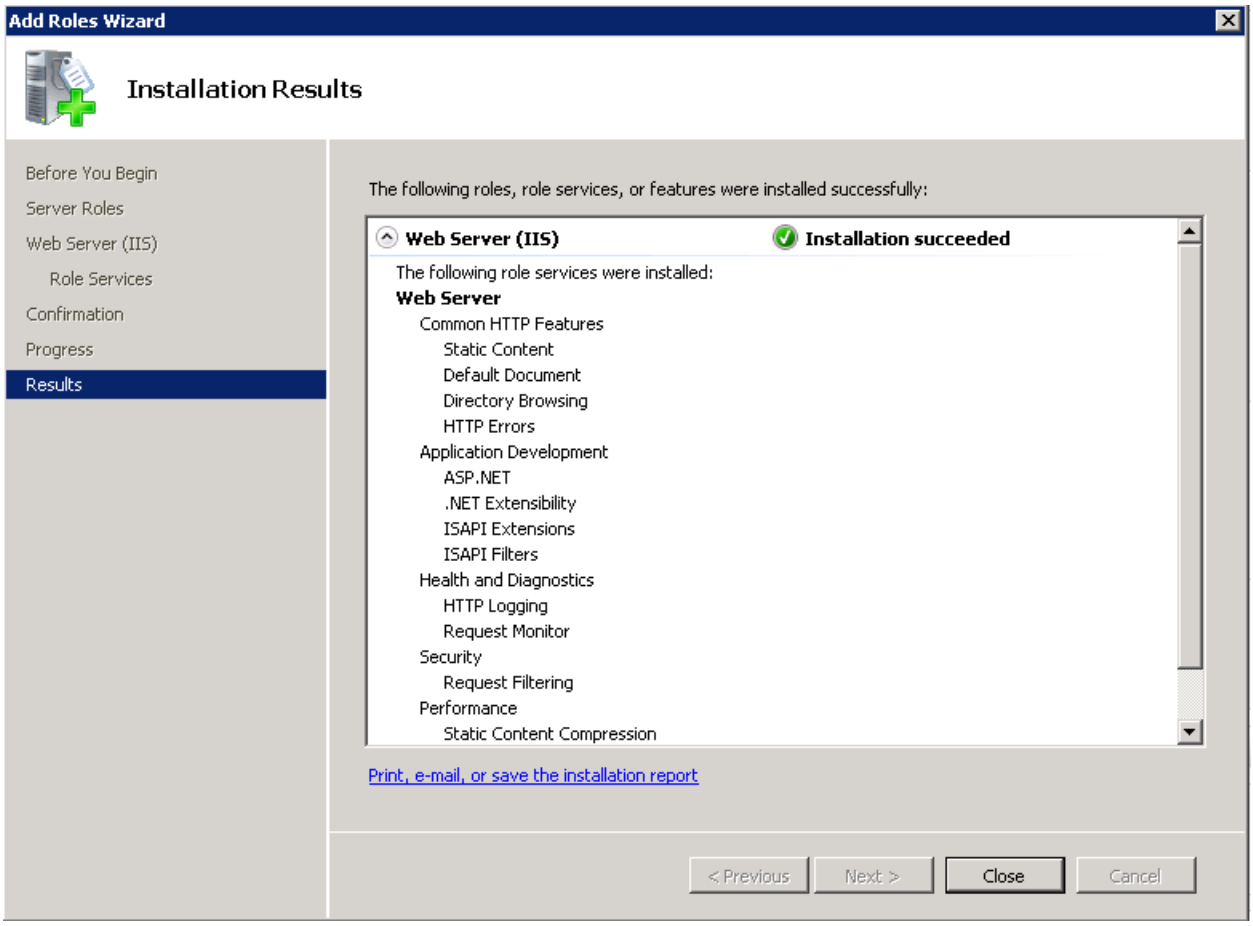

Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
Web Server (IIS)
Role Services
Confirmation
Progress
Results
Select the role services to install for Web Server (IIS):
Role services:
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
HTTP Redirection
WebDAV Publishing
Application Development
ASP.NET
.NET Extensibility
ASP
CGI
ISAPI Extensions
ISAPI Filters
Server Side Includes
Health and Diagnostics
HTTP Logging
Logging Tools
Request Monitor
Tracing
More about role services
Description:
ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.
< Previous
Next >
Install
Cancel

Click "Install".



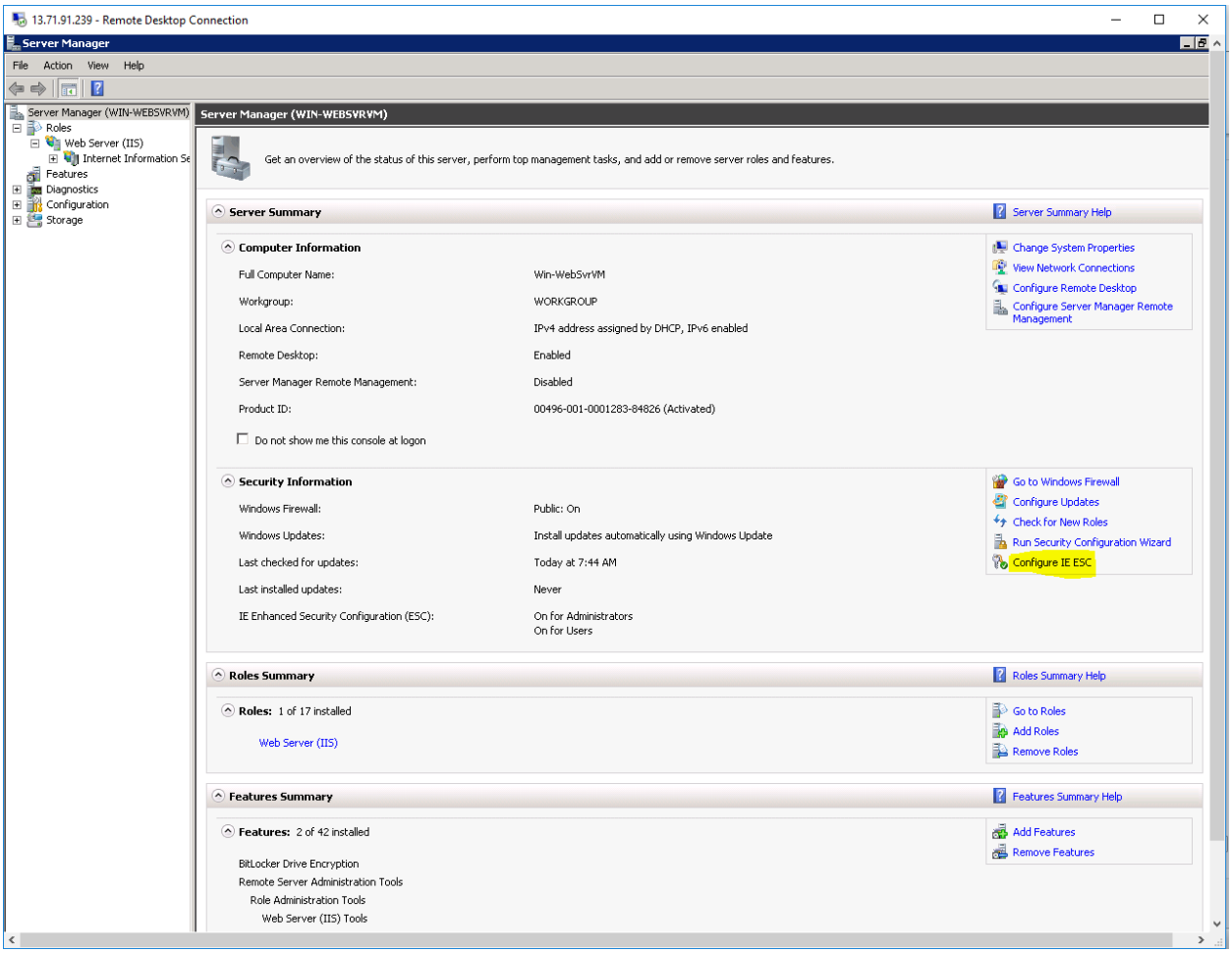
Click “Close”.

You have successfully created web server in Windows.



In Server manager,

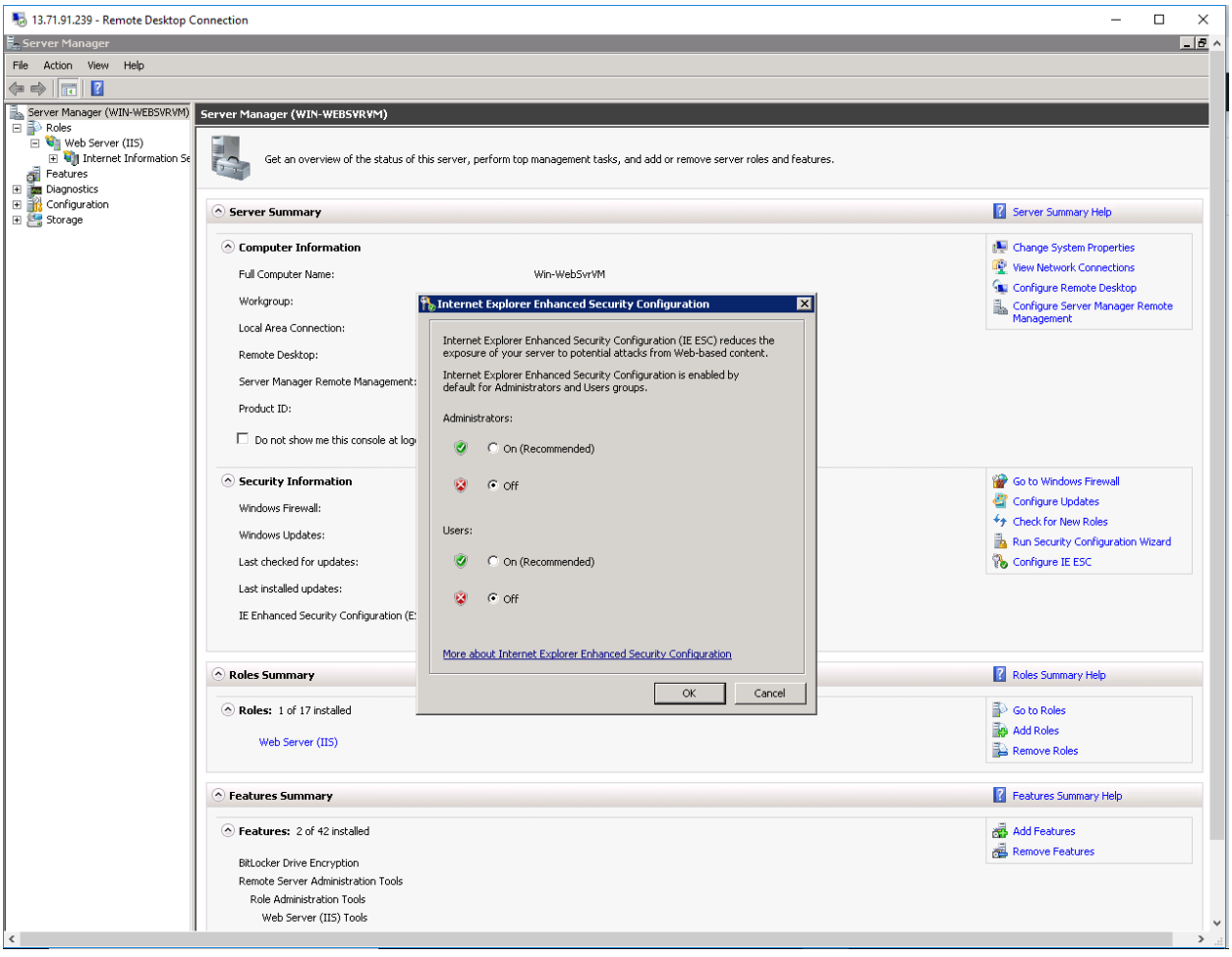
Click “Configure IE ESC”.



In IE Enhanced Security Configuration,

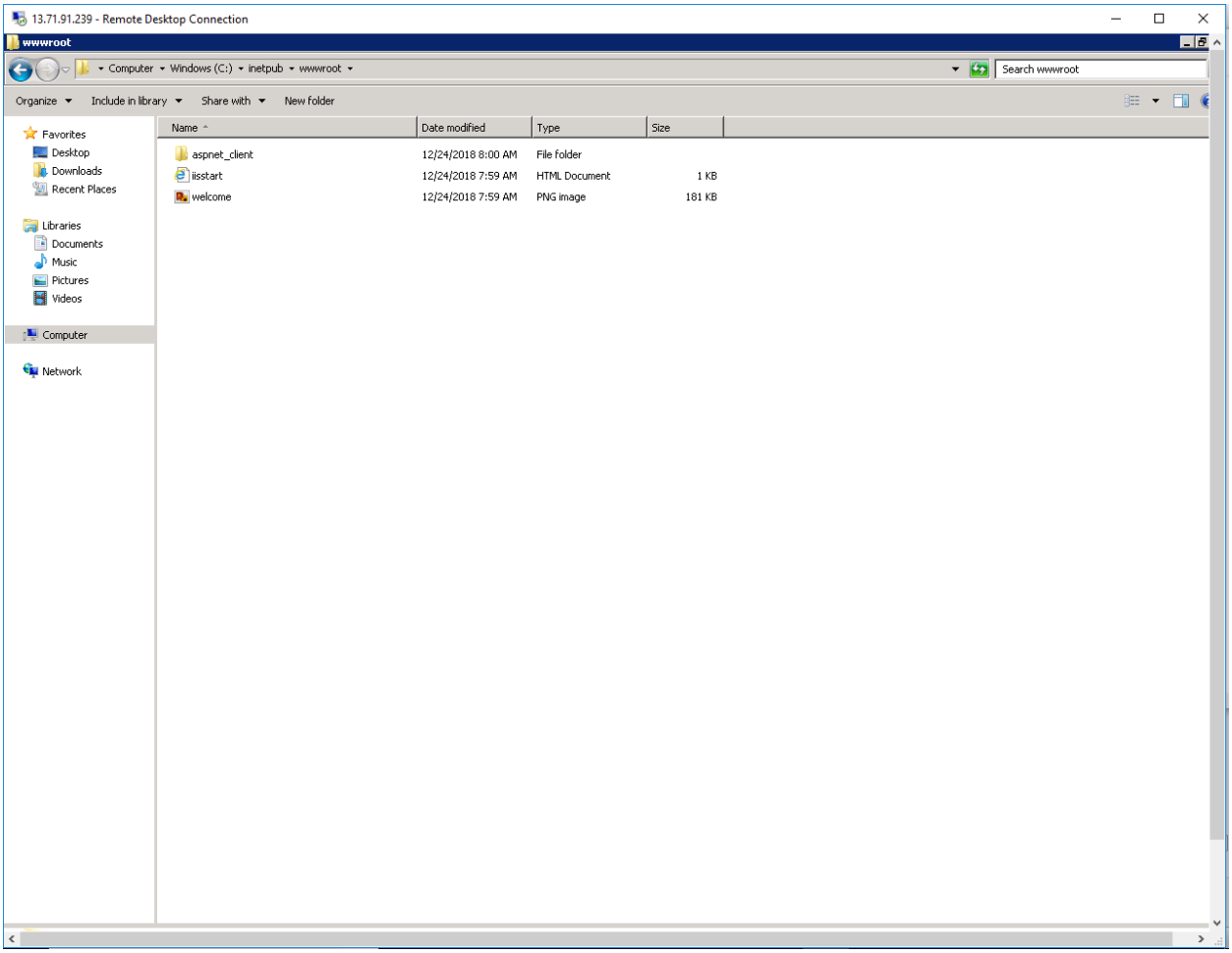
Set "Off" for Administrators

Set "Off" for Users and click "Ok".

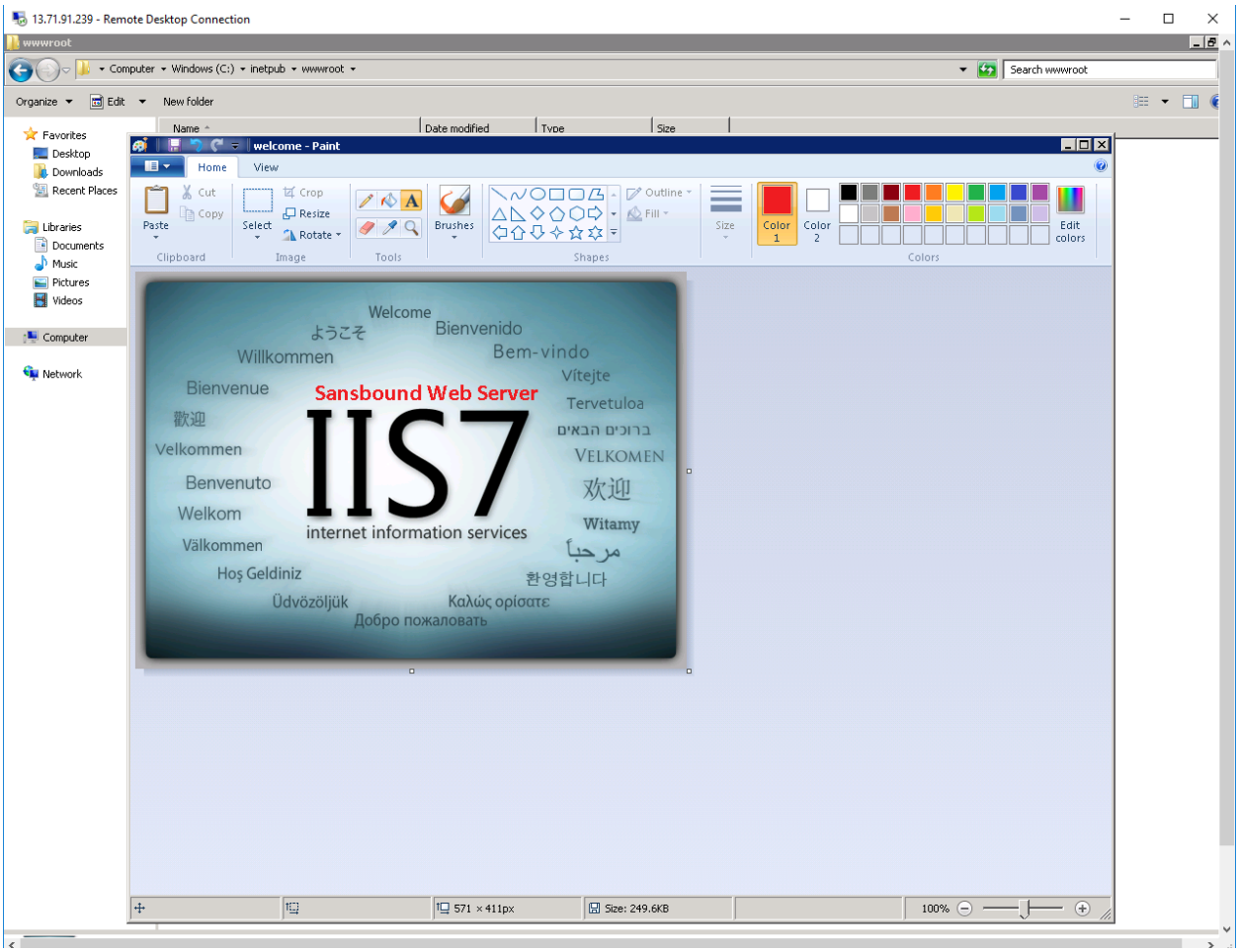


In Windows Server 2008 R2, go to C:\inetpub\wwwroot

Open "Welcome.png".

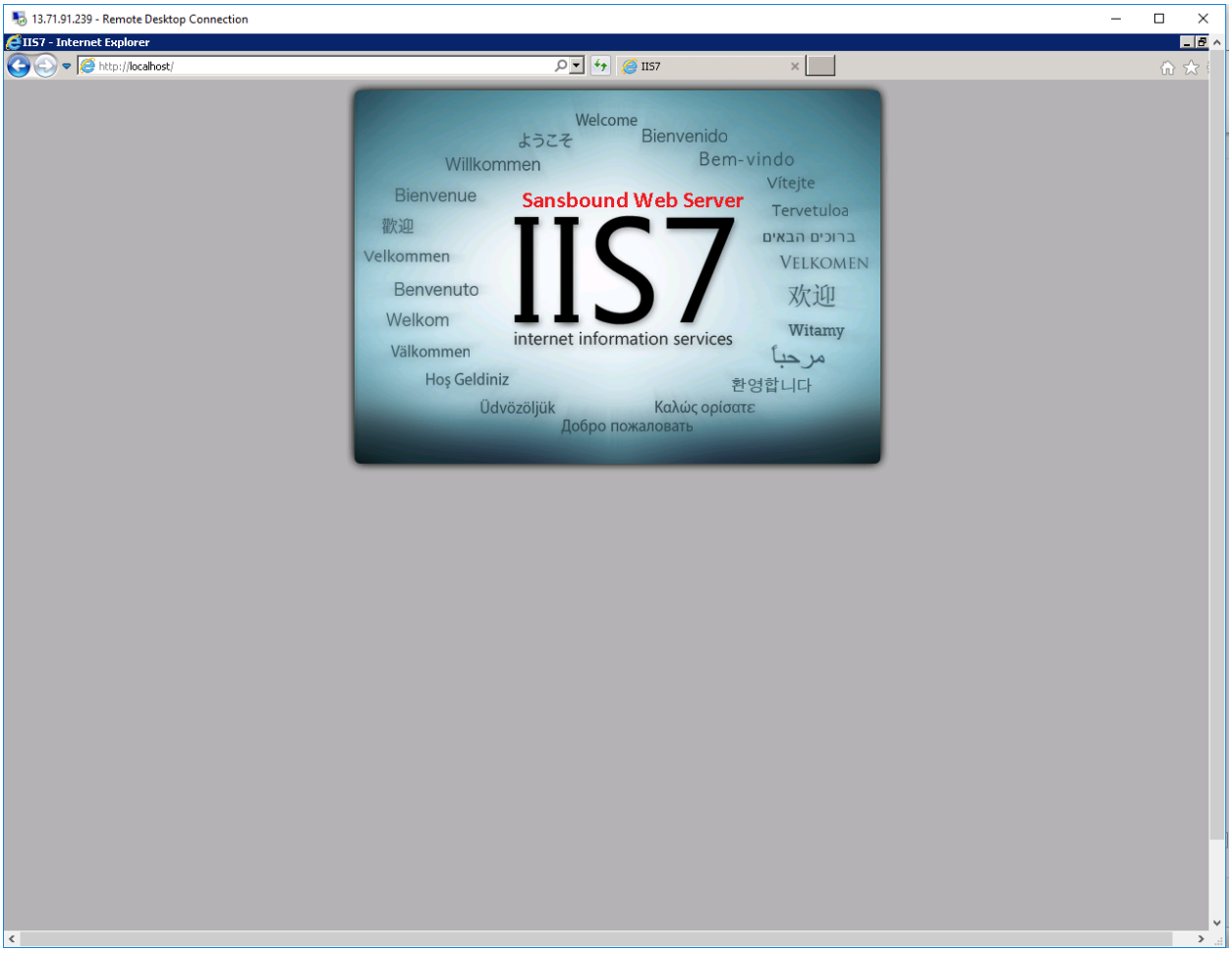


Modify the Welcome.jpg as per your wish and save it.



In Windows 2008 R2 server, in Internet explorer type “localhost” and press “Enter” to get the web page.

Yes, we have successfully got the web page with in the Azure VM.



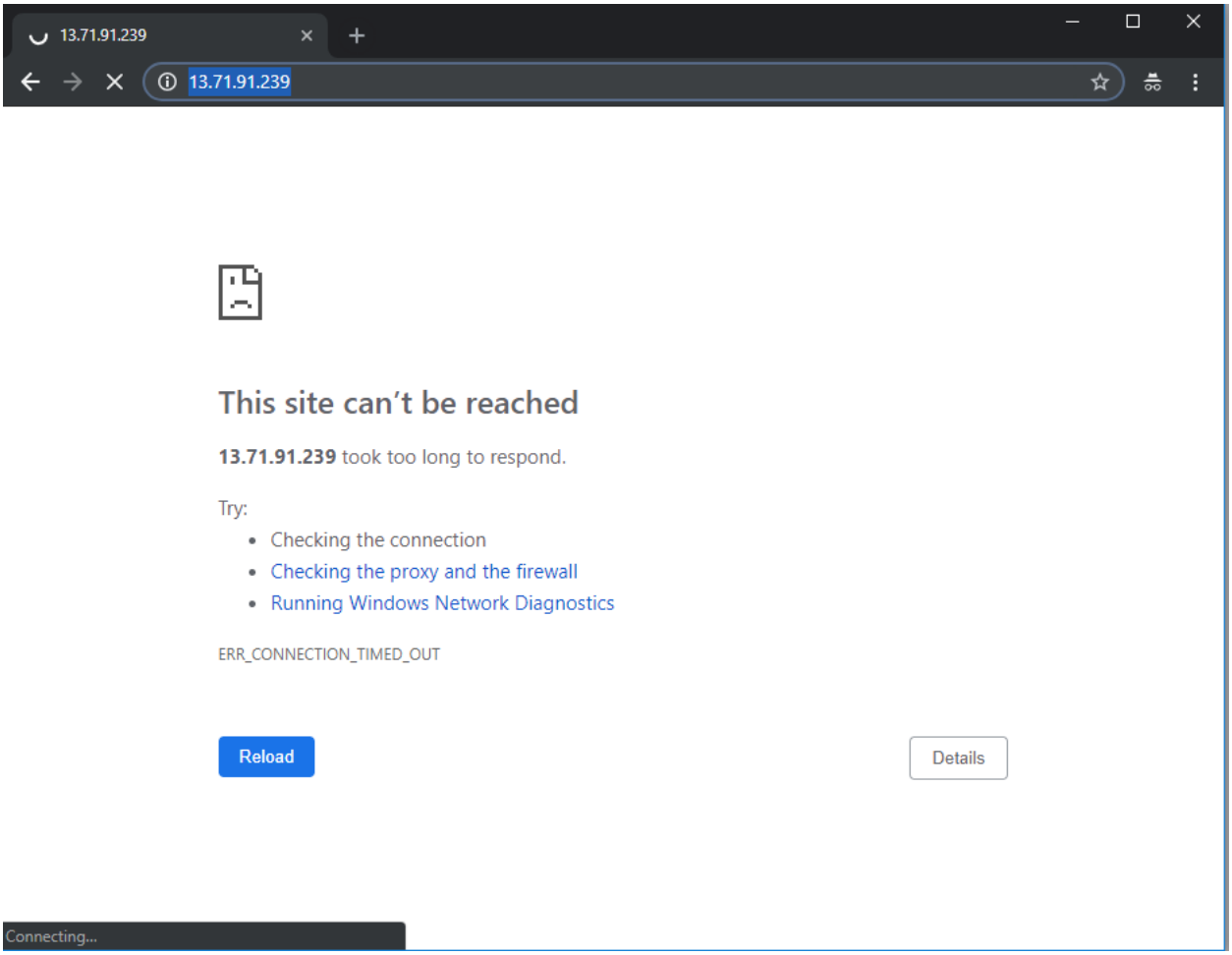
Now we have required to access the Web server through public.

Kindly note the Public IP of the Windows Virtual Machine (Win 2008 R2) and try to connect from local machine.

But, you are not able to got the web page.

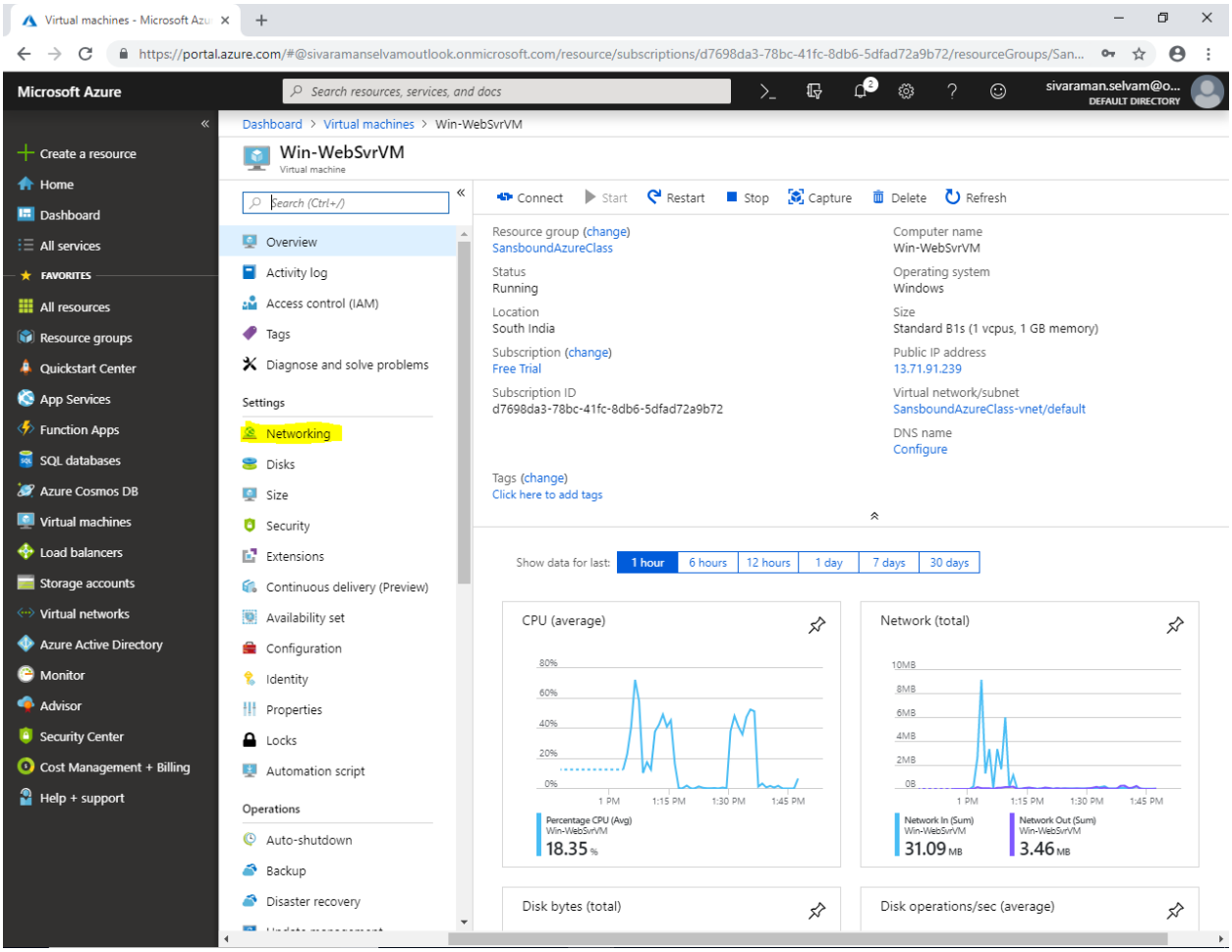
What could be the reason?

You have allowed only (RDP – 3389) Port only in inbound port rule to access selected ports from Public. That is the reason you are not able access the (HTTP – 80) Port through public. Hence you have required to permit HTTP (80).



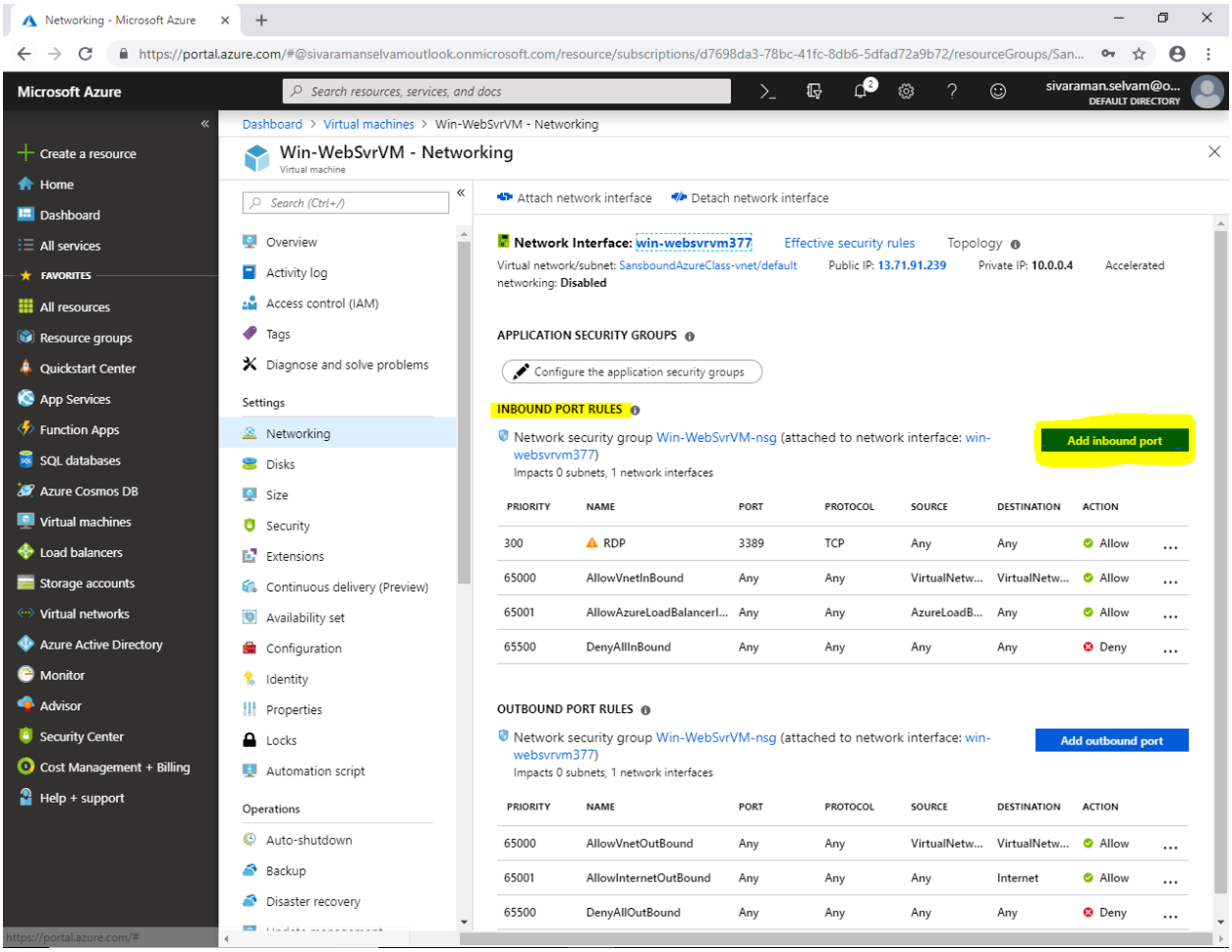
Select the virtual machine,

Click "Networking".

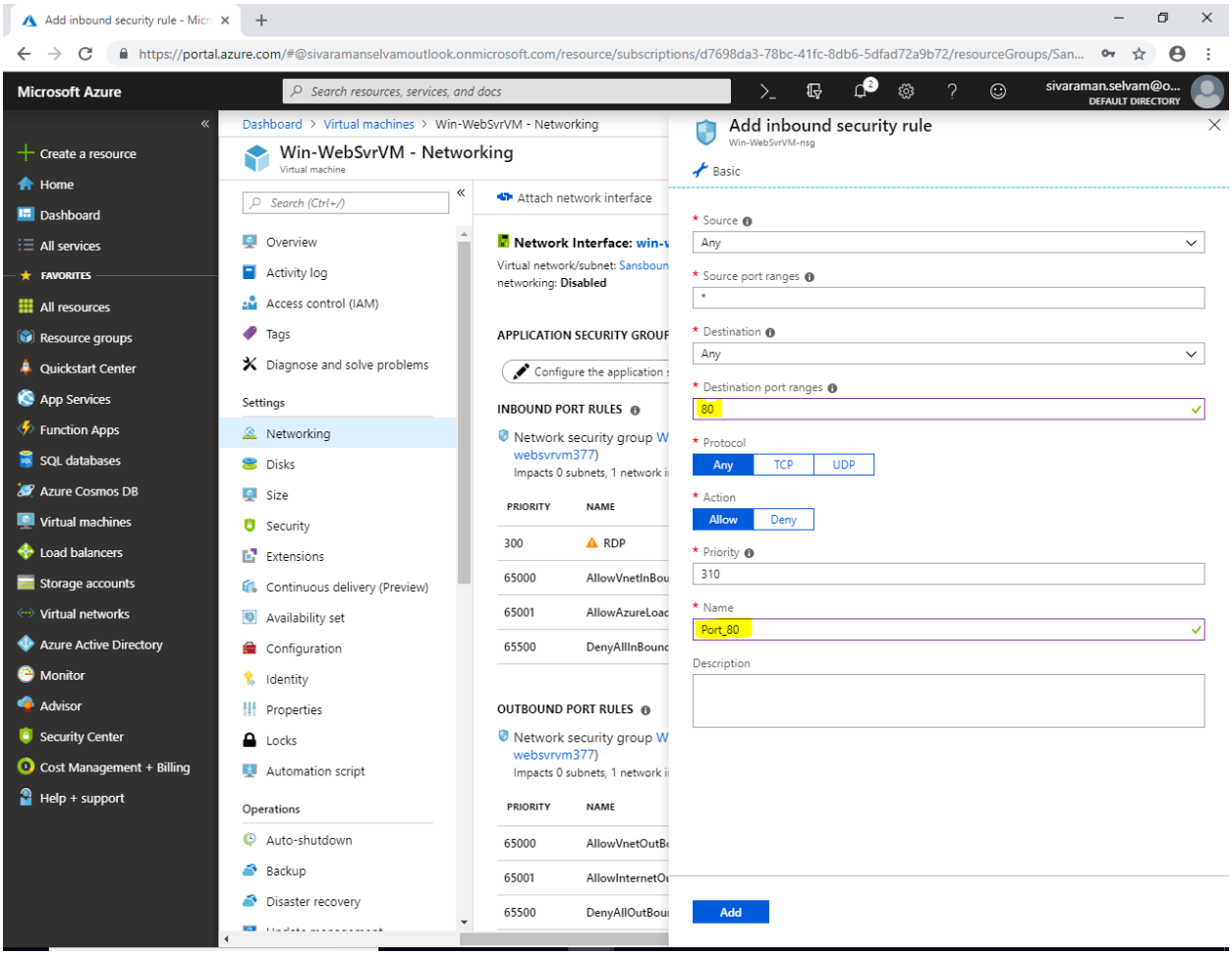


In “Networking”

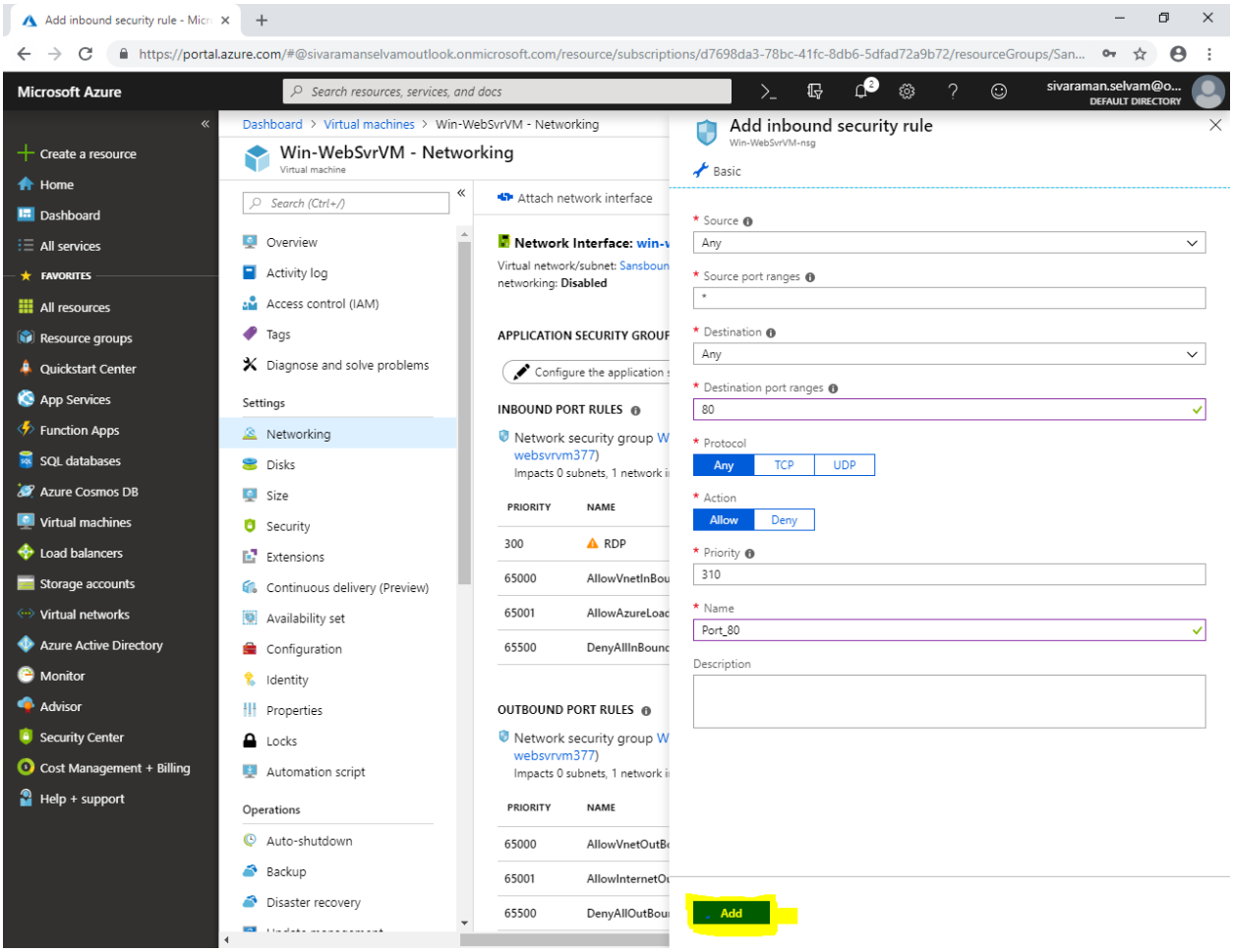
At “Inbound Port Rules” click “Add inbound port”.



Type "Destination port" range as "80"



Click "Add".


Add inbound security rule - Micr
https://portal.azure.com/#@sivaramanselvamoutlook.onmicrosoft.com/resource/subscriptions/d7698da3-78bc-41fc-8db6-5dfad72a9b72/resourceGroups/San...
Microsoft Azure
Search resources, services, and docs
sivaraman.selvam@o...
DEFAULT DIRECTORY
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Quickstart Center
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Dashboard > Virtual machines > Win-WebSvrVM - Networking
Win-WebSvrVM - Networking
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Disks
Size
Security
Extensions
Continuous delivery (Preview)
Availability set
Configuration
Identity
Properties
Locks
Automation script
Operations
Auto-shutdown
Backup
Disaster recovery
Attach network interface
Network Interface: win-v
Virtual network/subnet: Sansboun
networking: Disabled
APPLICATION SECURITY GROUP
Configure the application
INBOUND PORT RULES
Network security group W
websvrvm377)
Impacts 0 subnets, 1 network i
PRIORITY
NAME
300
RDP
65000
AllowVnetInBou
65001
AllowAzureLoad
65500
DenyAllInBound
OUTBOUND PORT RULES
Network security group W
websvrvm377)
Impacts 0 subnets, 1 network i
PRIORITY
NAME
65000
AllowVnetOutB
65001
AllowInternetOu
65500
DenyAllOutBou
Add inbound security rule
Win-WebSvrVM-nsg
Basic
* Source
Any
* Source port ranges
*
* Destination
Any
* Destination port ranges
80
* Protocol
Any
TCP
UDP
* Action
Allow
Deny
* Priority
310
* Name
Port_80
Description
Add

Go to browser click “Refresh” to connect the webserver.

Now you have successfully connected to the Web server.