Denis Aptula Ekmel Intze

**COMPREHENSIVE Azure and AD Audit Plus Deployment**

We are pleased to present our "Comprehensive Azure and AD Audit Plus Deployment" report, detailing our work on configuring and testing the Manage Engine tool - AD Audit Plus. Our efforts aim to create a reliable and compliant IT infrastructure ready to support our organisation’s needs and future growth.

Table of Contents

[Introduction 3](#_Toc170816924)

[1. Creating a Windows Server Virtual Machine in Azure 3](#_Toc170816925)

[1.1. Log in to the Azure Portal: 3](#_Toc170816926)

[1.2. Create a Windows Server Virtual Machine: 3](#_Toc170816927)

[1.3. Conclusion: 6](#_Toc170816928)

[2. Configuring Network Security Groups (NSGs) 6](#_Toc170816929)

[2.1. Add Inbound Ports: 6](#_Toc170816930)

[2.2. Confirm the added open ports with the Nmap tool. 9](#_Toc170816931)

[2.3. Conclusion 9](#_Toc170816932)

[3. Securing RDP 10](#_Toc170816933)

[3.1. Verify Network Security Group (NSG) Rules 10](#_Toc170816934)

[3.2. Changing the RDP Port on the VM and Azure (Optional) 10](#_Toc170816935)

[3.3. Enable Network Level Authentication (NLA) 12](#_Toc170816936)

[3.4. Configure RDP Settings to Force Credential Prompt 13](#_Toc170816937)

[3.5. Client-Side 14](#_Toc170816938)

[3.6. Conclusion 15](#_Toc170816939)

[4. Setting up Event Hub on Azure 16](#_Toc170816940)

[Conclusion: 18](#_Toc170816941)

[5. Configuring VM as a Domain Controller 18](#_Toc170816942)

[5.1. Configure Domain Controller: 18](#_Toc170816943)

[5.2. Conclusion: 21](#_Toc170816944)

[6. Configuring Internet Control Message Protocol (ICMP) settings 22](#_Toc170816945)

[6.1. Allow ICMP: 22](#_Toc170816946)

[6.2. Confirming Configuration: 22](#_Toc170816947)

[6.3. Conclusion: 23](#_Toc170816948)

[7. Creating a Snapshot on Azure for the VM 23](#_Toc170816949)

[7.1. Step-by-Step: 23](#_Toc170816950)

[7.2. Conclusion: 24](#_Toc170816951)

[8. Configuring Audit Policies for Active Directory Auditing 25](#_Toc170816952)

[8.1. Access Group Policy Management Console (GPMC) 25](#_Toc170816953)

[8.2. Add a new Policy 25](#_Toc170816954)

[8.3. Configure Audit Policies 26](#_Toc170816955)

[8.4. Set Advanced Audit Policies (For Windows Server 2008 and above) 26](#_Toc170816956)

[8.5. Enforce Advanced Audit Policy Configuration 28](#_Toc170816957)

[8.6. Apply and Verify 29](#_Toc170816958)

[8.7. Conclusion 30](#_Toc170816959)

[9. Setting up the Simple Mail Transfer Protocol Secure (SMTPS) Server 30](#_Toc170816960)

[9.1. Creating a SendGrid Resource 30](#_Toc170816961)

[9.2. Create SendGrid Account 31](#_Toc170816962)

[9.3. Creating a Twilio SendGrid Account 33](#_Toc170816963)

[9.4. Adding an API Key 34](#_Toc170816964)

[9.5. Configuring Sender Authentication 35](#_Toc170816965)

[9.6. SMTPS Configuration 38](#_Toc170816966)

[9.7. Conclusion 40](#_Toc170816967)

[10. Report Summary 40](#_Toc170816968)

## Introduction

Welcome to the "Comprehensive Azure and AD Audit Plus Deployment " report. In this project, our primary aim is to configure and test the Manage Engine tool: AD Audit Plus. To achieve this, we need to set up a Windows Server virtual machine on Microsoft Azure and perform all necessary security configurations.

We start by creating a Windows Server virtual machine, configuring network security groups (NSGs), and securing Remote Desktop Protocol (RDP) to ensure a safe and efficient environment. Following this, we set up an Azure Event Hub for efficient log management and established a domain controller to manage network operations.

Additionally, we implement advanced audit policies, enable HTTPS for AD Audit Plus, and configure a secure SMTP server with SSH. These steps are crucial for enhancing network security, ensuring reliable communication, and enabling comprehensive monitoring and analysis through AD Audit Plus.

By following this structured approach, we aim to create a robust and secure IT infrastructure that meets industry standards and regulatory requirements. This setup will enable us to effectively monitor, manage, and protect our IT environment, providing a solid foundation for future growth and success.

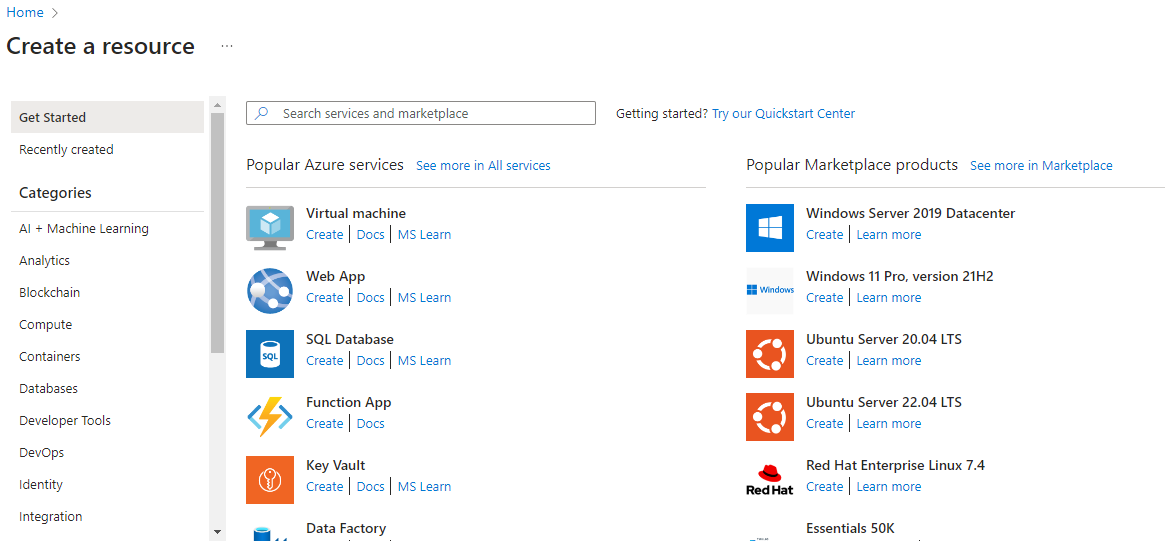
## 1. Creating a Windows Server Virtual Machine in Azure

### 1.1. **Log in to the Azure Portal**:

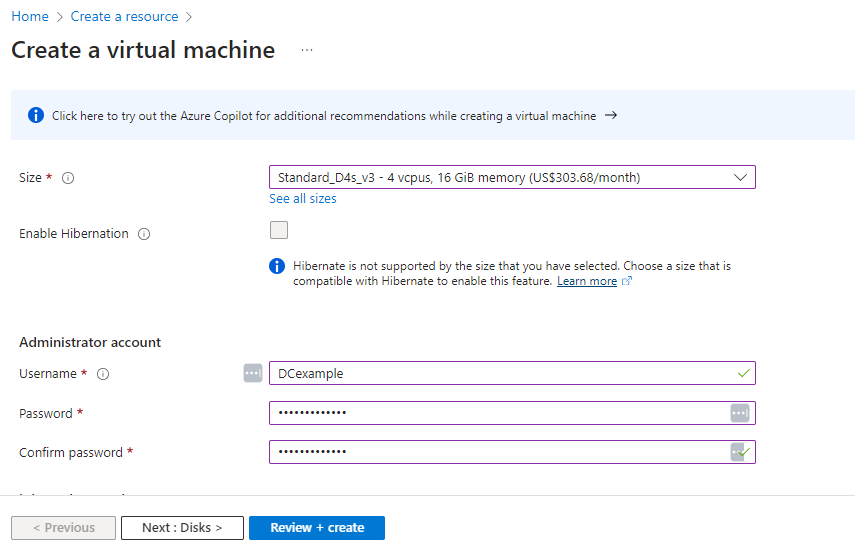
* Open a web browser and navigate to [https://portal.azure.com](https://portal.azure.com" \t "_new).

### 1.2. **Create a Windows Server Virtual Machine**:

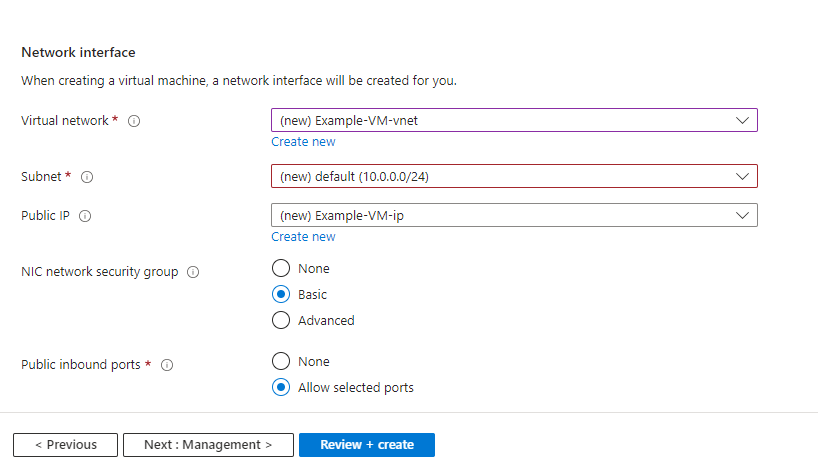
* Navigate to the **Resources** section in the Azure Portal.
* Under **Virtual Machine**, Click **Create** to create a new virtual machine.



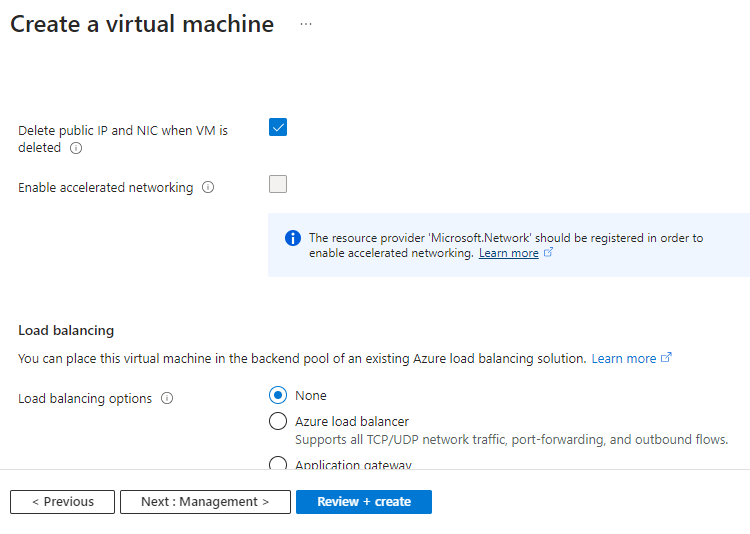
* **Basics**:
  + Select your subscription.
  + Click **Create New** and enter a name for the resource group.
  + Choose a name for your virtual machine.
  + Select the region.
  + Choose "Windows Server" from the dropdown.
  + Select an appropriate VM size based on your needs.
* **Administrator Account**:
  + Create an admin username.
  + Create a password.



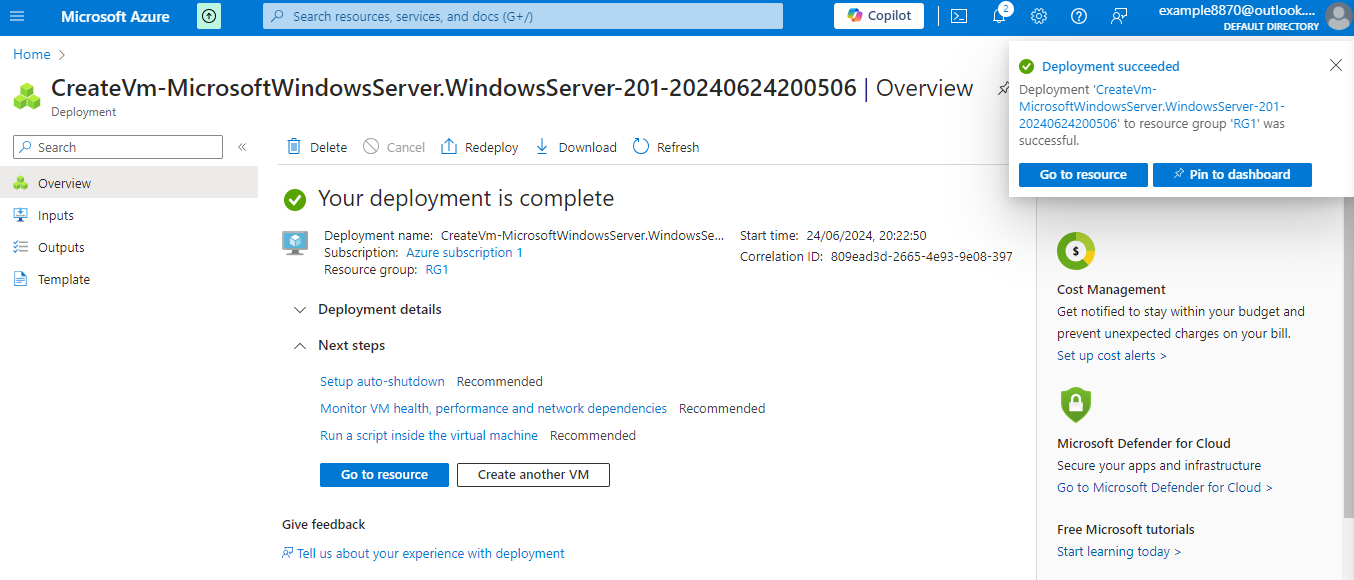
* **Networking**:
  + **Virtual network**: Click **Create New** and enter a name for the virtual network.



* + Define the IP address range for the virtual network.
  + Tick the box on “Delete public IP and NIC when VM is deleted” so when you delete the VM, the public IP and NIC will be automatically deleted.



* **Management, Disks, and Advanced Settings**: Configure these settings as needed. Otherwise, leave it as default.
* Click **Review + Create** and then **Create** to provision the virtual machine, resource group, and virtual network.



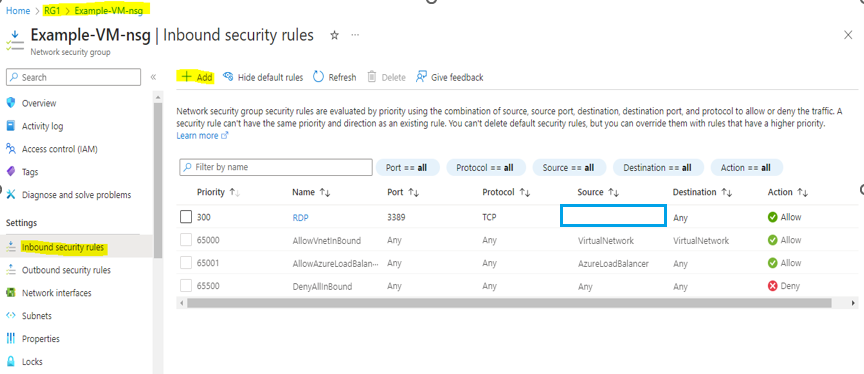
### 1.3. Conclusion:

By following the steps, we successfully created a Windows Server virtual machine, established the necessary resource group, and configured a virtual network through the Azure Portal. This structured approach ensures that all components are organized and manageable, laying a solid foundation for scalable and efficient cloud infrastructure.

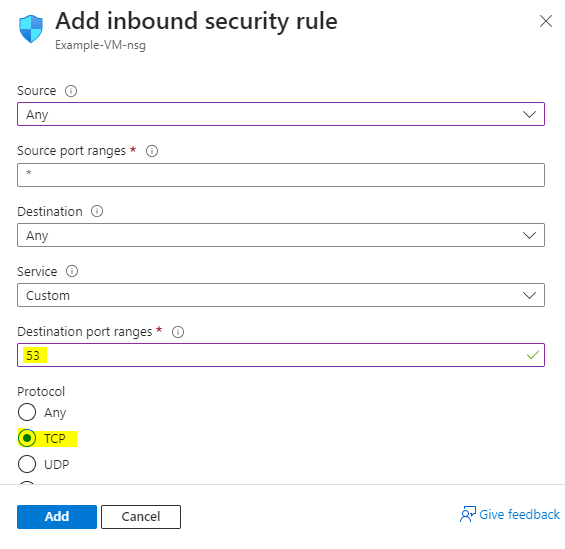
## ****2. Configuring Network Security Groups (NSGs)****

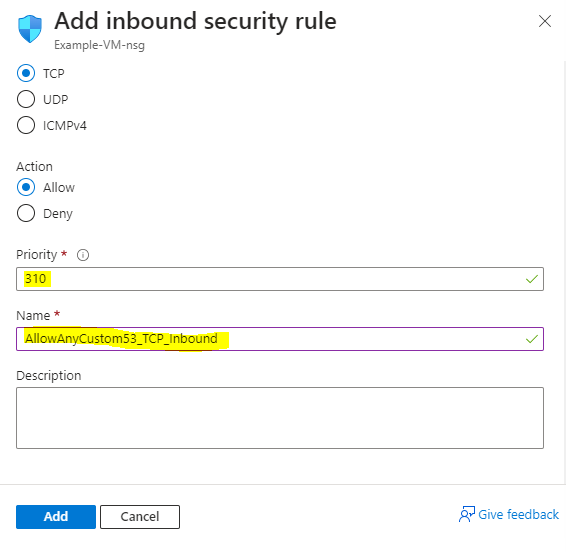
### 2.1. Add Inbound Ports:

* On the newly created Resource Group (RG1), Navigate to the NSG associated with the virtual machine's network interface and click “Add” to add security rules.



* Add inbound security rules to allow necessary traffic:
  + **TCP 53** and **UDP 53** (for DNS)  
    - Source: Any  
    - Source port ranges: \*  
    - Destination: Any  
    - Destination port ranges: 53  
    - Protocol: TCP  
    - Action: Allow  
    - Priority: Set an appropriate priority number  
    - Name: AllowAnyCustom53\_TCP\_Inbound

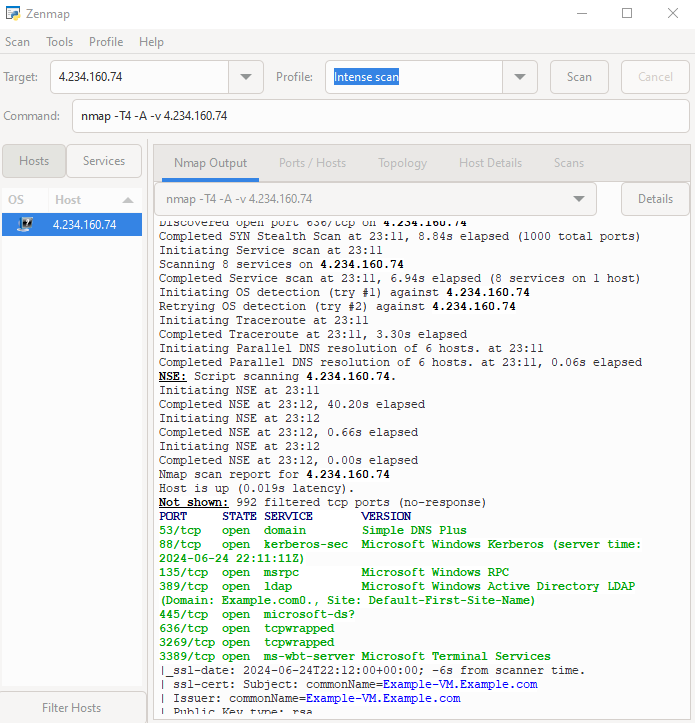


* Carefully plan the priority values to ensure there are no conflicts and that rules are evaluated in the correct order. Leave gaps between priority values (e.g., 110, 120, 130,) to allow for future rules to be added without needing to renumber existing rules.  
    
  

Do the same for UDP 53 and for all the rules below:

* + **TCP 88** and **UDP 88** (Kerberos)
  + **TCP 135** (RPC)
  + **TCP 445** (SMB)
  + **UDP 123** (NTP)
  + **TCP 389** and **UDP 389** (LDAP)
  + **TCP 636** (LDAP SSL)
  + **TCP 3268** and **3269** (Global Catalog)

### 2.2. Confirm the added open ports with the Nmap tool.



### ****2.3. Conclusion****

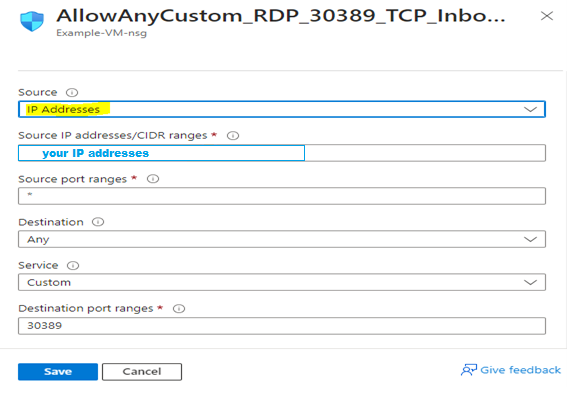
**Configuring Network Security Groups (NSGs) with specific inbound rules is essential for securing network communications. By allowing only necessary traffic on designated ports, we minimize potential attack vectors and enhance our virtual environment's security. Verifying these settings with tools like Nmap ensures they are correctly applied, preventing unauthorized access and maintaining a robust, secure network infrastructure.**

## ****3. Securing RDP****

### ****3.1.**** Verify Network Security Group (NSG) Rules

Ensure that the NSG attached to your Azure VM's network interface and subnet allows traffic only from trusted IP addresses on the new RDP port.

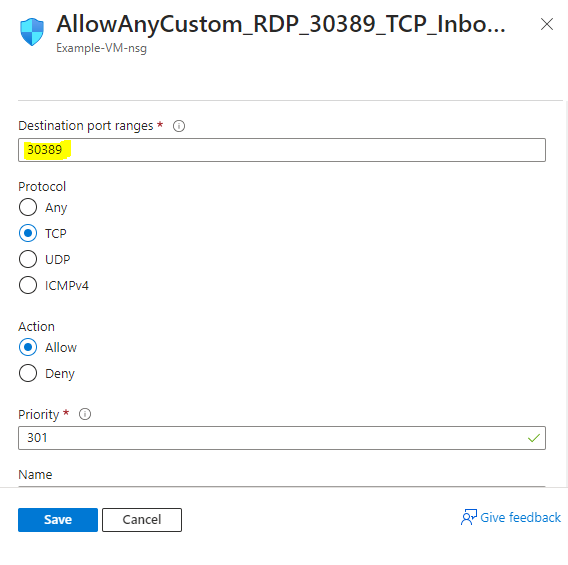
1. **Go to the Azure portal.**
2. **Navigate to your VM's Networking settings.**
3. **Check the Inbound port rules** and ensure the new RDP port is open only to specific IP addresses.
4. Click Source” and choose “IP Addresses”. Then on the “Source IP addresses” write the specific IP address which will be allowed to connect to the VM.



### 3.2. ****Changing the RDP Port on the VM and Azure (Optional)****

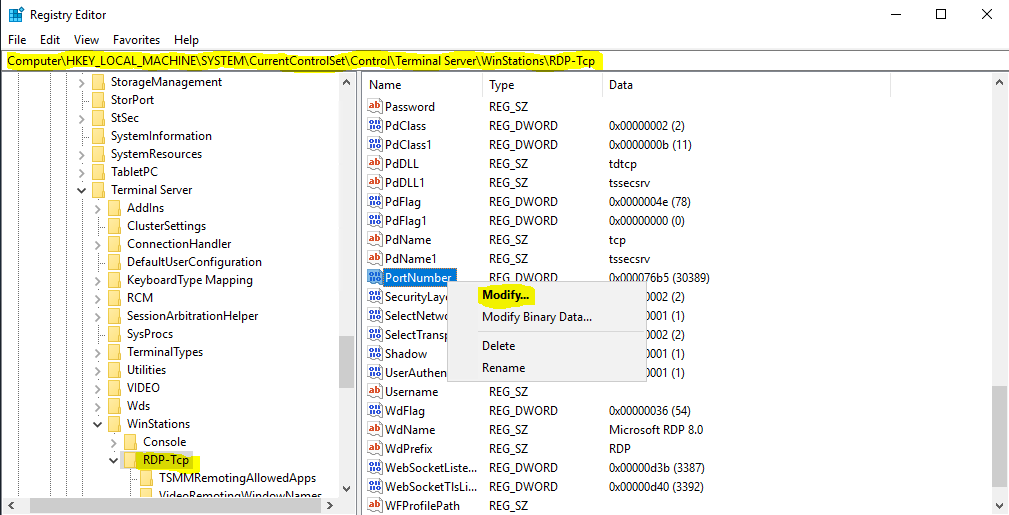
**On the Azure Portal:**

1. Access the Azure portal and navigate to your VM.
2. Locate the networking settings.
3. Update the network security group (NSG) rules to allow traffic on the new RDP port 30389 instead of the default 3389.



**On the VM:**

1. Connect to the VM using the existing RDP port 3389.
2. Open the Registry Editor by typing **regedit** in the Run dialogue (Win + R).
3. Navigate to: **HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp.**
4. Change the value of the PortNumber registry key to **30389.**

****

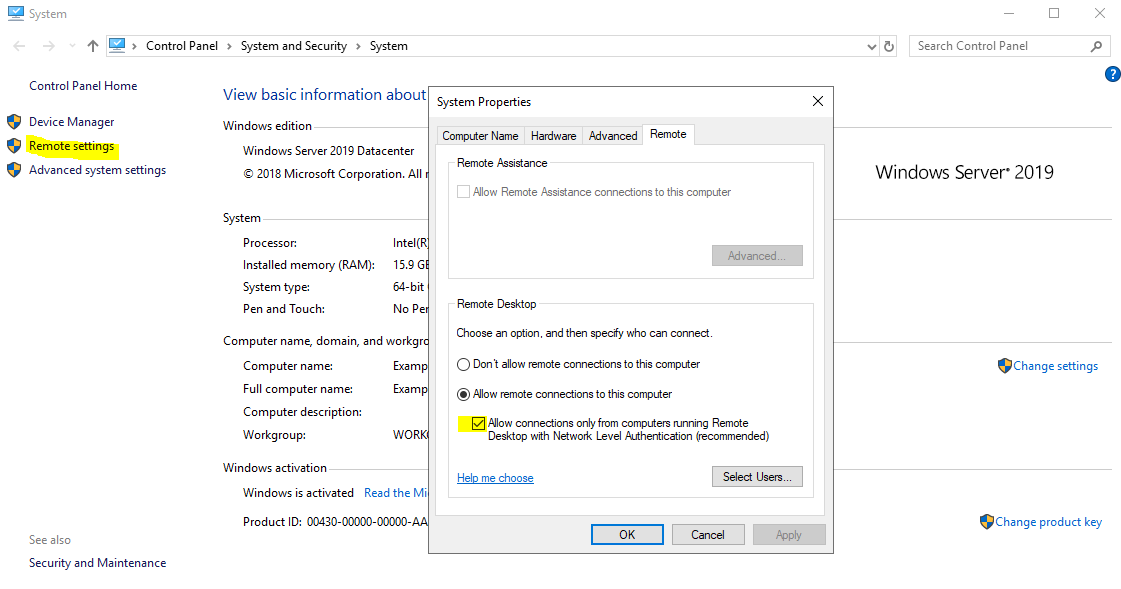
1. Restart the VM to apply the changes.

Changing the default RDP port to 30389 reduces the risk of automated attacks and brute-force attempts targeting the default RDP port, enhancing overall security by ensuring consistency across both network and local VM settings.

### 3.3. Enable Network Level Authentication (NLA)

Network Level Authentication adds an additional layer of security before establishing a full RDP connection.

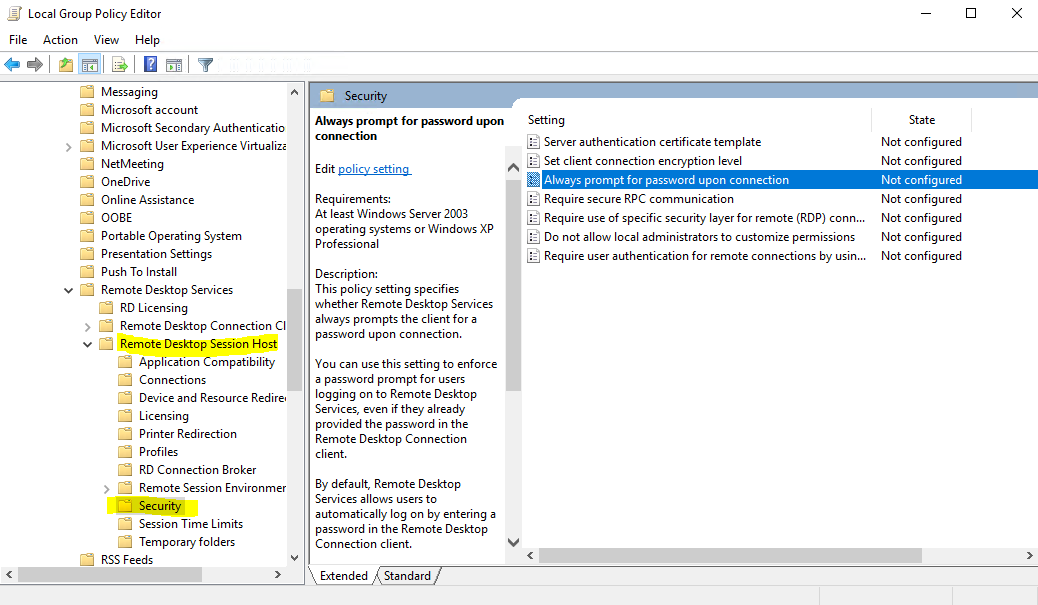
1. **Log into your VM.**
2. **Open the System properties** (Right-click on ‘This PC’ -> Properties -> Remote settings.
3. **Under Remote Desktop**, ensure "Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)" is checked.



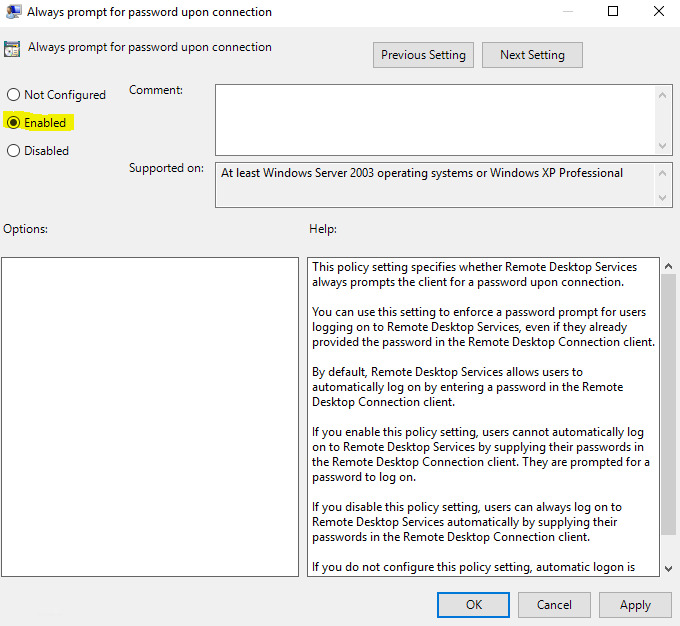
### 3.4. Configure RDP Settings to Force Credential Prompt

If the RDP connection isn't prompting for credentials, you might need to enforce credential protection on the client and server sides.

1. **Open Group Policy Editor** (gpedit.msc).
2. **Navigate to:** Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security.



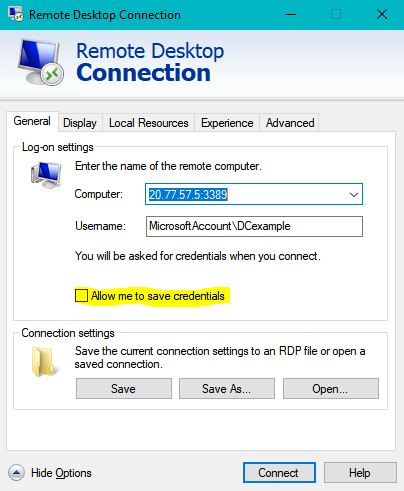
**On the** "Always prompt for password upon connection" policy, click **Edit** to **Enable** the policy



### 3.5. Client-Side

When setting up the RDP client, ensure that the option to save credentials is not used:

1. **Open Remote Desktop Connection.**
2. **Enter the IP address and new port.**
3. **Click on Show Options.**
4. **Ensure the "Always ask for credentials" is not checked.**

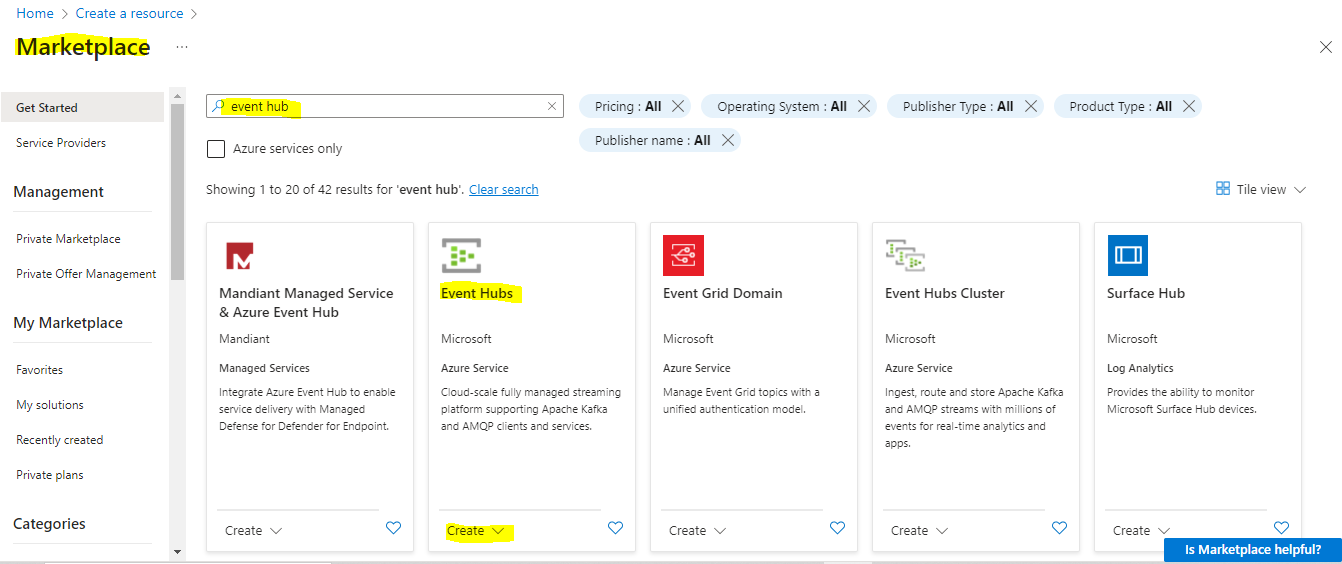


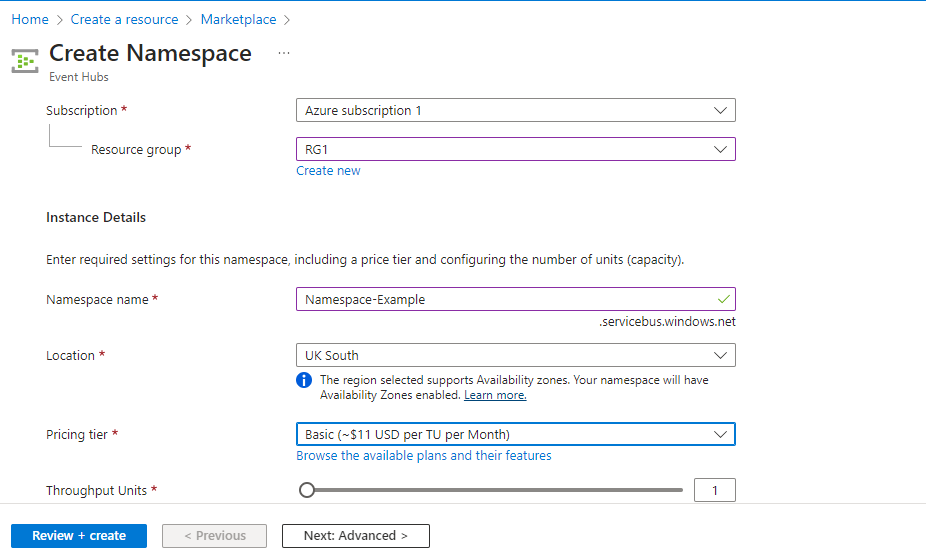
### 3.6. Conclusion

Securing RDP access involves meticulous steps to safeguard your Azure VM. By verifying NSG rules to allow traffic only from trusted IPs and changing the default RDP port, we mitigate the risks of automated attacks and brute-force attempts. Enabling Network Level Authentication (NLA) and enforcing credential prompts further bolster security, ensuring that only authenticated connections are established. These measures collectively enhance the overall security posture of your virtual environment, protecting it from unauthorized access.

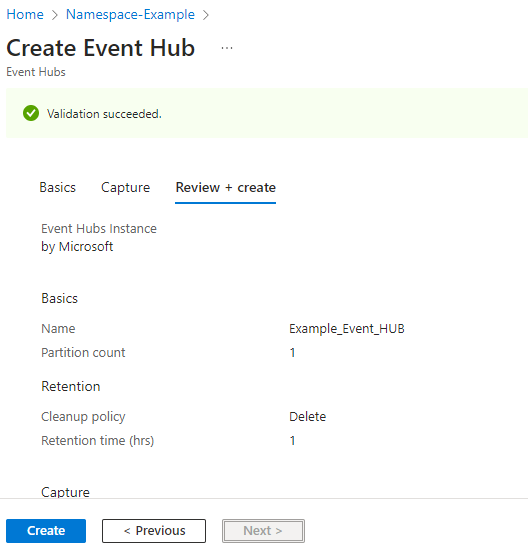
## ****4. Setting up Event Hub on Azure****

4.1. Navigate to Marketplace and search for “Event Hubs”.

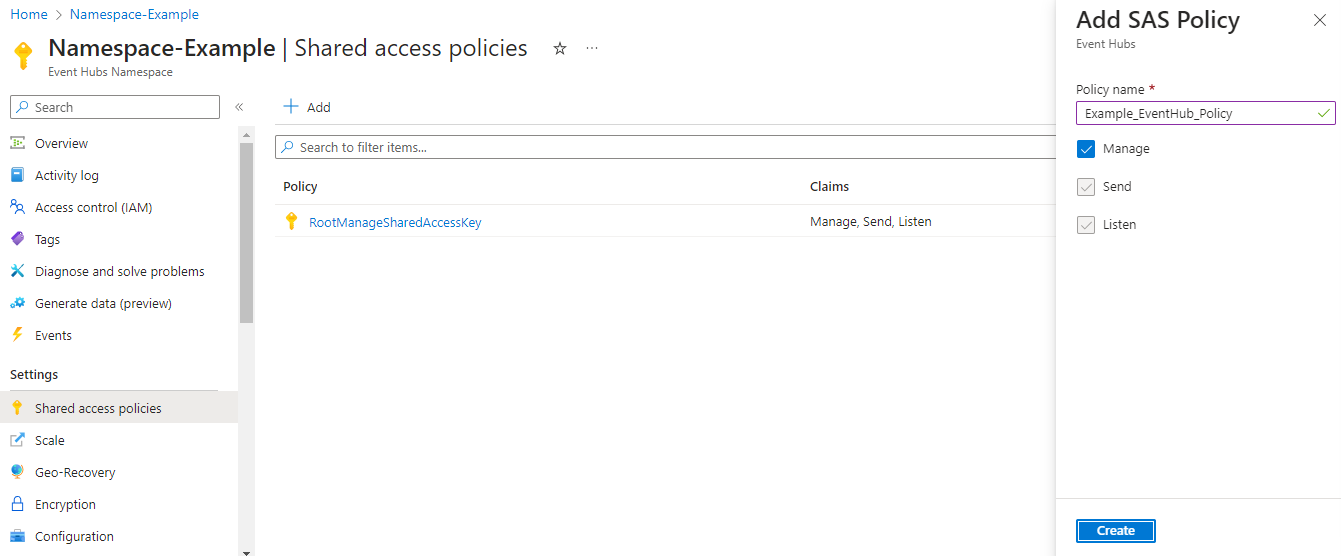


4.2. Create an Event Hub namespace. 

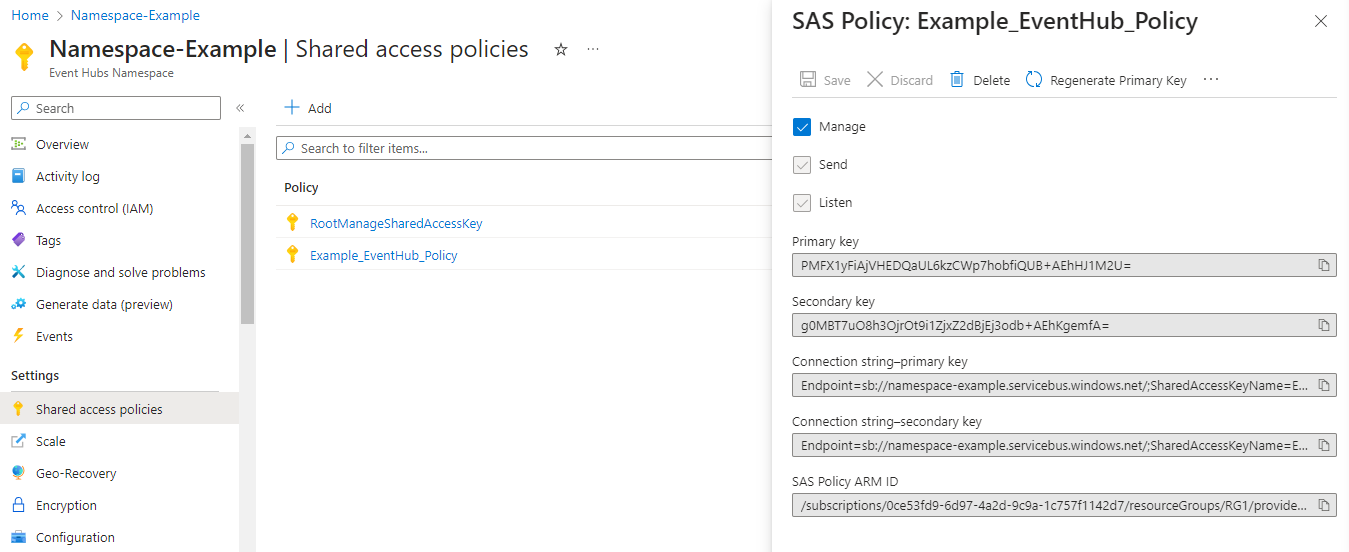
4.3. Within the created Even Hub Namespace create Event Hub.



4.4. Create a Policy within the Event Hub.



4.5. Later on you will need the Connection String – Primary key from the created policy



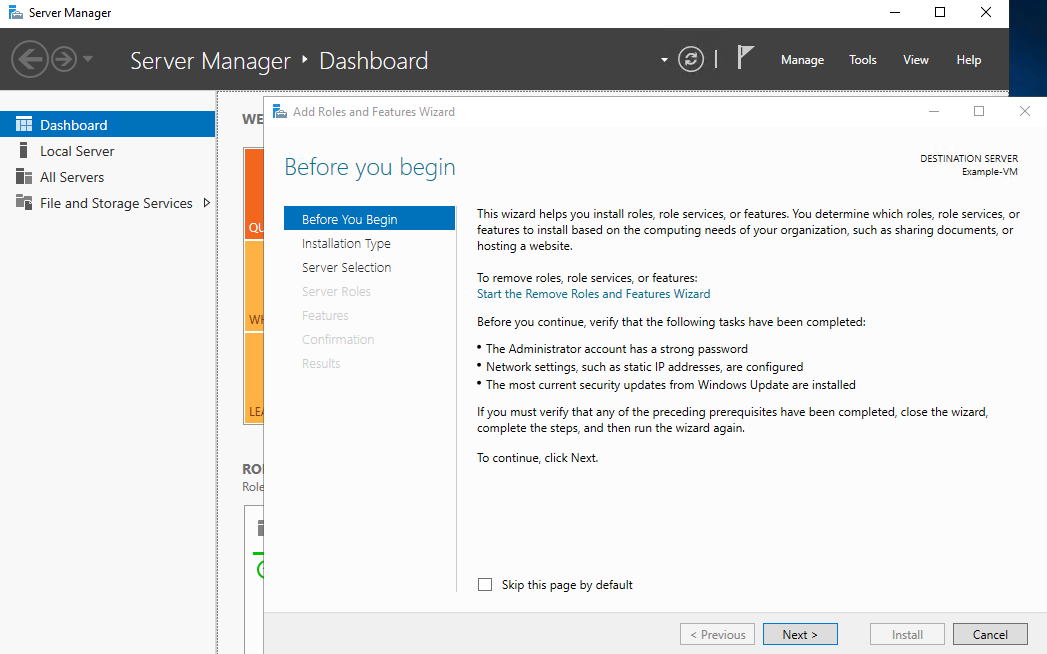
### Conclusion:

We set up an Azure Event Hub to enable smooth communication, log collection, and analysis using tools like AD Audit. By using the Azure Marketplace, we created an Event Hub namespace, an Event Hub, set up an access policy, and retrieved the connection string. Azure Event Hubs can handle and analyze large amounts of event data in real-time. This setup ensures that logs from your virtual machine are efficiently collected and analyzed, giving you comprehensive monitoring and better security insights.

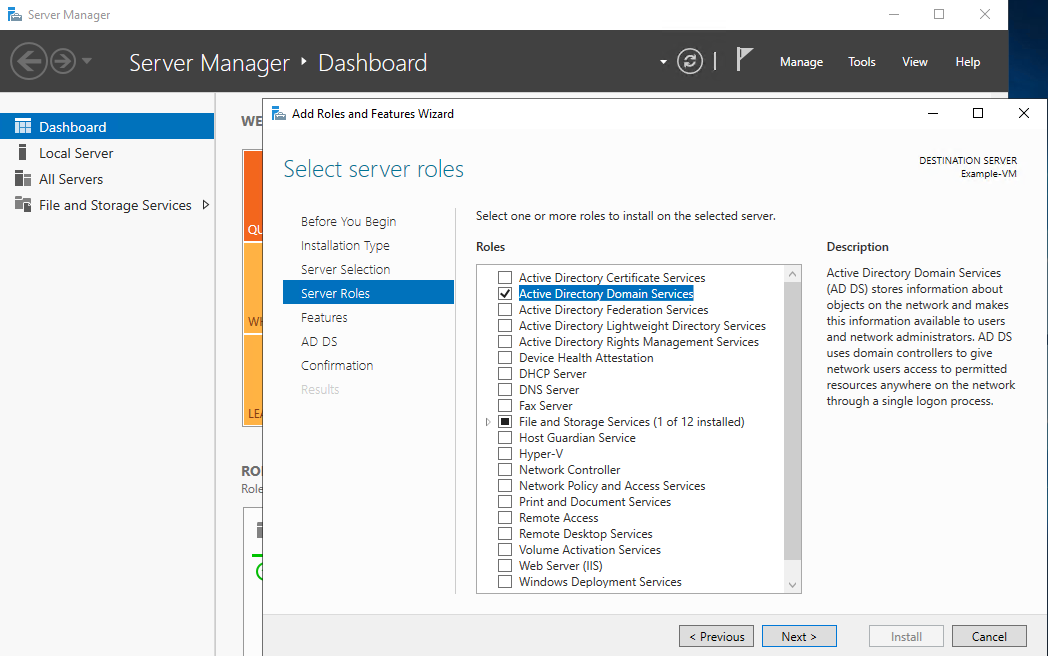
## ****5. Configuring VM as a Domain Controller****

### 5.1. Configure Domain Controller:

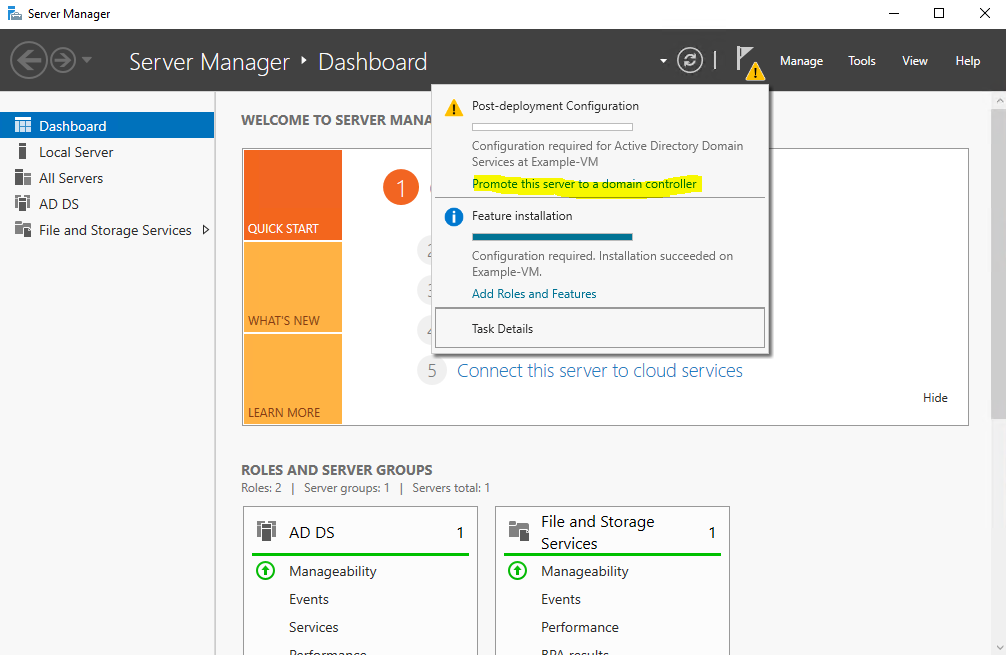
* Connect to the VM via Remote Desktop Protocol (RDP).
* Open Server Manager and navigate to "Add roles and features".



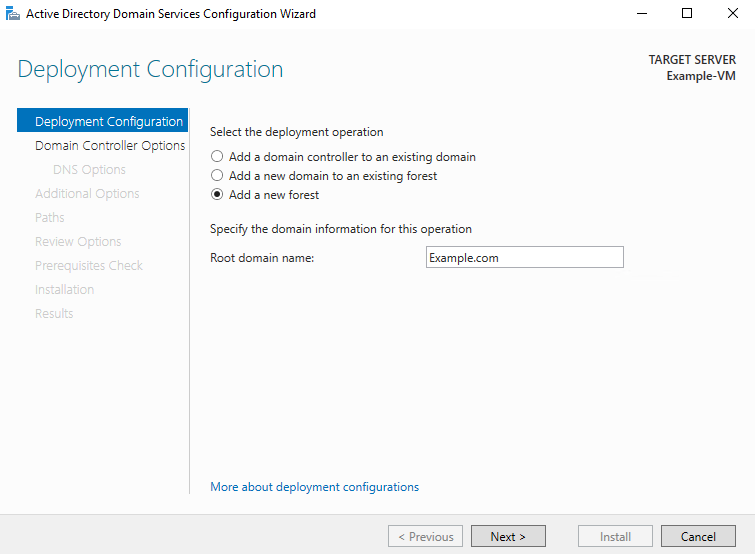
Select "Active Directory Domain Services" and follow the wizard to install the necessary features.



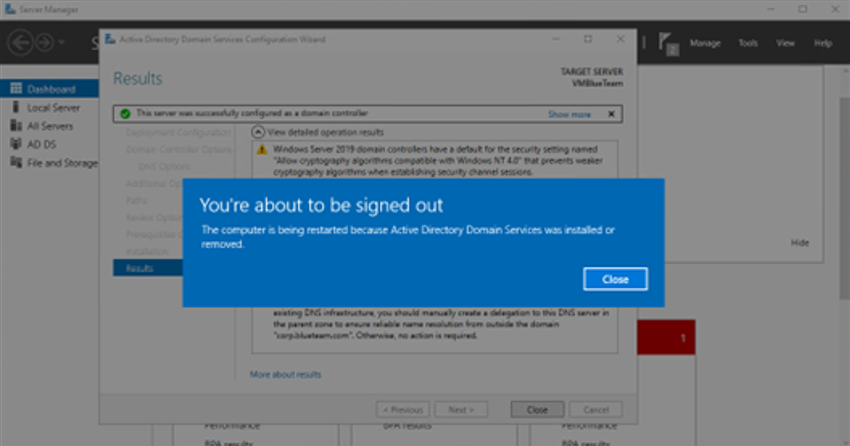
* Promote the server to a domain controller by configuring Active Directory.



* Mark “Add New Forest” and enter the name of your Root Domain.



* Follow the required steps.
* If the configuration is successful the VM will restart automatically.



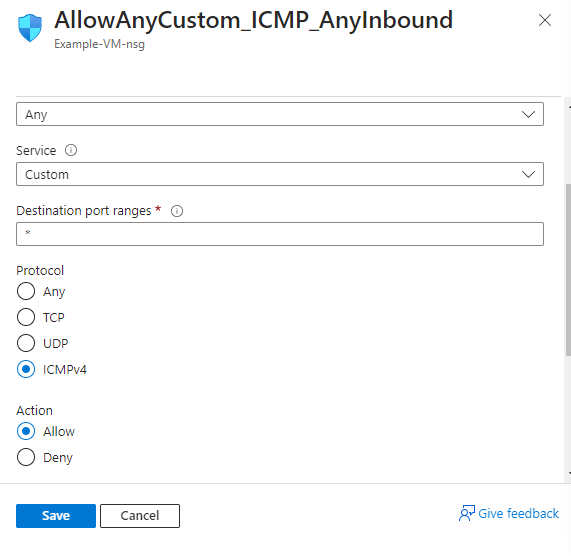
### 5.2. Conclusion:

Configuring your virtual machine as a domain controller was done to set up a central system to manage the network. By installing the Active Directory Domain Services role and promoting the server, we made sure the network can securely handle user logins and permissions. This setup helps keep everything organized and safe, making it easier to control who can access different parts of the network. Following these steps means your virtual machine is now ready to manage the network efficiently, which is important for keeping things running smoothly and securely.

## ****6. Configuring Internet Control Message Protocol (ICMP) settings****

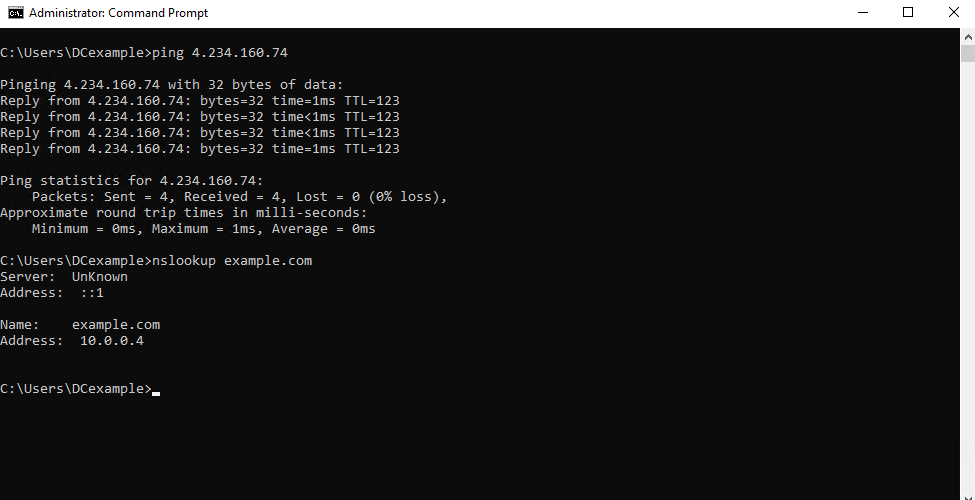
### 6.1. Allow ICMP:

1. **Allow ICMP Traffic through NSG:**
   * In the Azure portal, go to "Network Security Groups".
   * Select your NSG and add an inbound rule to allow ICMP traffic.



### 6.2. Confirming Configuration:

1. **Verify DNS and ICMP:**
   * Open PowerShell on the VM.
   * Use the “**nslookup”** command to check DNS resolution.
   * Use the “**ping**” command to check ICMP connectivity.



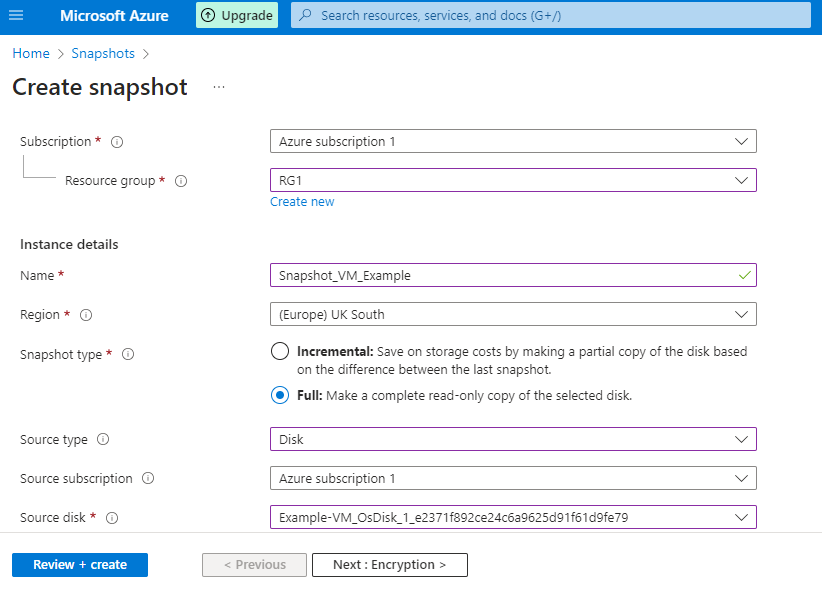
### 6.3. Conclusion:

By following these steps, we have ensured that our VM can properly resolve domain names and communicate over the network. Configuring DNS settings and allowing ICMP traffic is essential for maintaining network reliability and troubleshooting connectivity issues. Verifying with nslookup and ping confirms that our setup is correct, providing a solid foundation for efficient network operations.

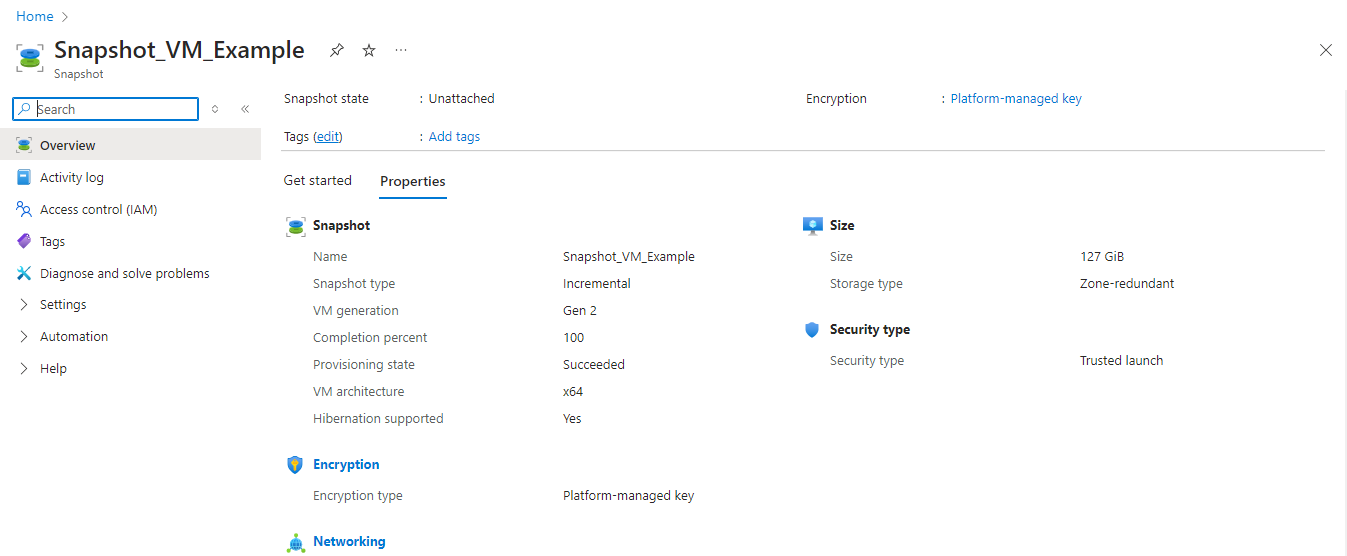
## ****7. Creating a Snapshot on Azure for the VM****

### ****7.1. Step-by-Step****:

* + Navigate to the 'Snapshots' section in the Azure portal.
  + Select 'Create a snapshot'.
  + Choose the VM disk you want to snapshot.



* + Configure the rest of the snapshot settings if required.
  + Review the configured settings and create.



### ****7.2. Conclusion:****

Creating a snapshot of the VM provides a point-in-time image of the disk, which can be useful for backup purposes or to quickly restore the VM to a previous state in case of failure or other issues. These updated steps incorporate the changes made directly on the VM as well as on Azure, providing a comprehensive overview of the security enhancements and backup measures implemented in your project.

## ****8. Configuring Audit Policies for Active Directory Auditing****

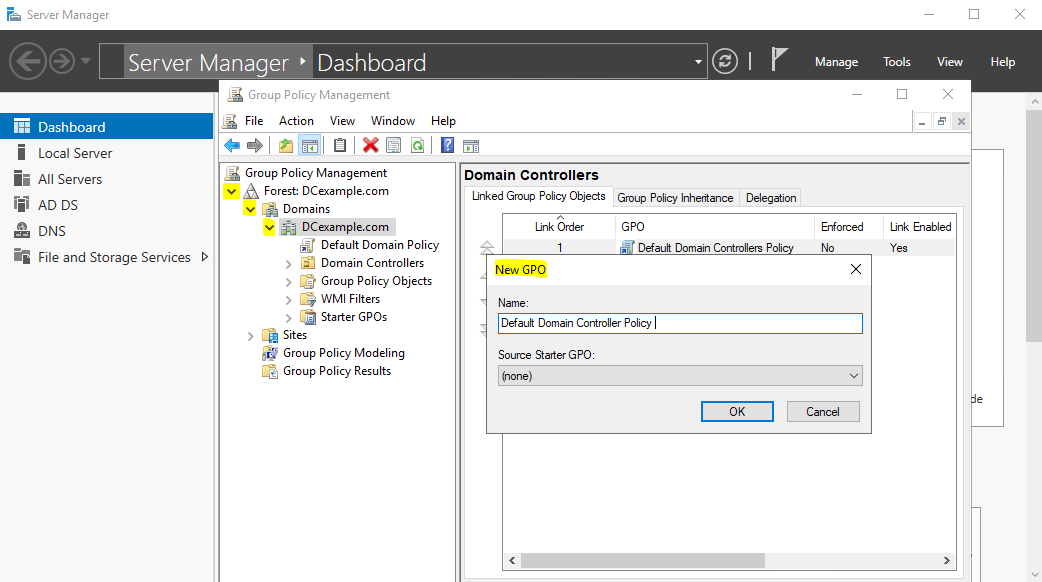
After downloading, installing the AD Audit Plus tool and activating the license follow the steps below to configure the policies:

### ****8.1. Access Group Policy Management Console (GPMC)****

* Open the Group Policy Management Console from your server's administrative tools.

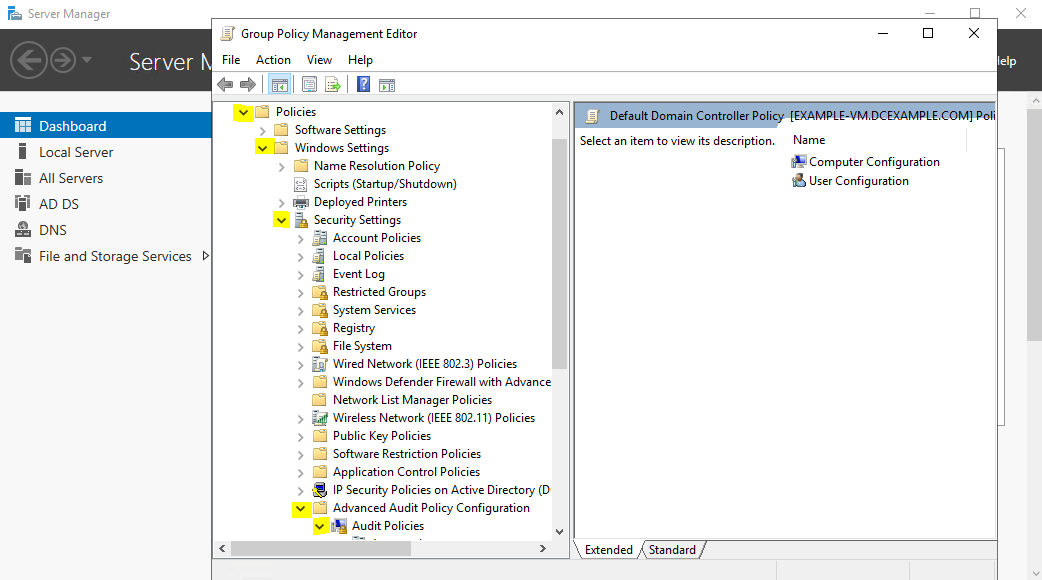
### ****8.2. Add a new Policy****

* Right-click on **Group Policy Objects** and select **New**.
* Enter a name for your new GPO, such as "Default Domain Controllers Policy" (if not already listed).



### ****8.3. Configure Audit Policies****

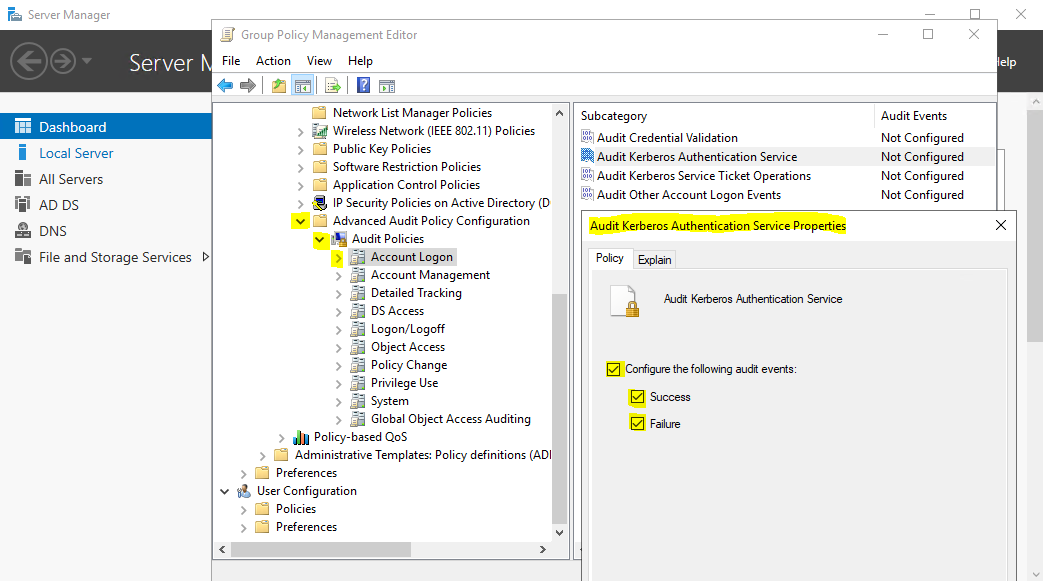
* For **Windows Server 2008 and later**:
  + Go to: Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies.



* + Configure necessary security settings such as Account Policies, Local Policies, Event Log settings, and more as per your organization’s requirements.

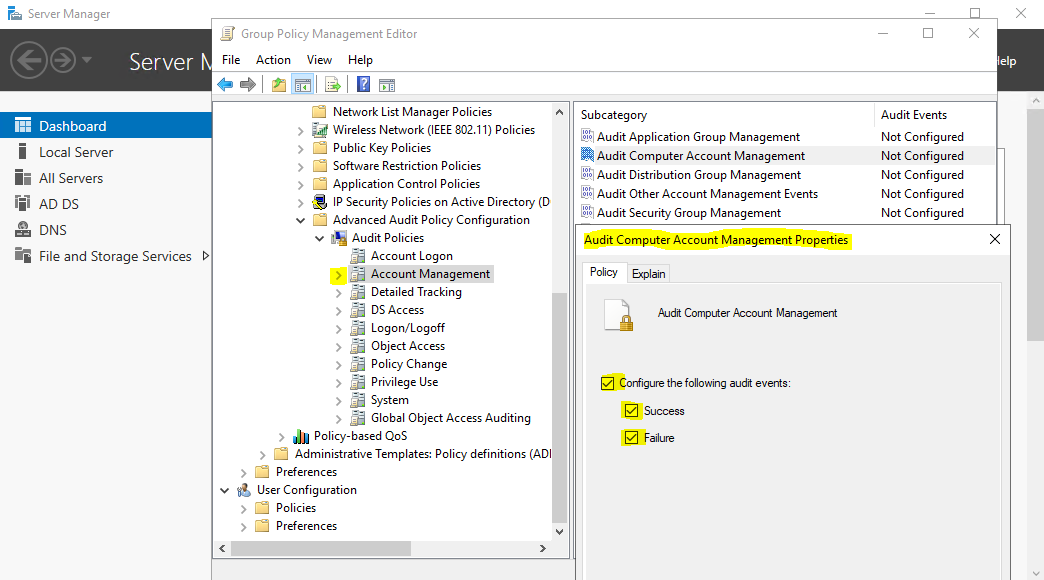
### ****8.4. Set Advanced Audit Policies (For Windows Server 2008 and above)****

* **Audit Logon Events**:
  + Select “Account Logon”
  + Expand Audit Policies and select Account Logon.
  + In the right pane, find and double-click on Audit Kerberos Authentication Service.
  + Select both Success and Failure checkboxes.
  + Click OK to save the changes.



Do the same for the following policies below:

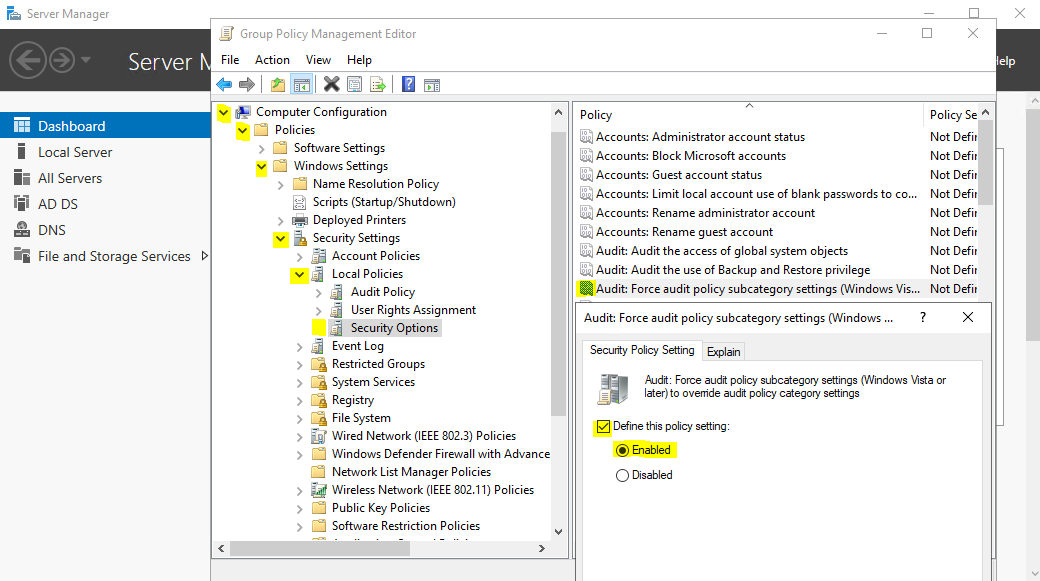
* **Audit User, Group, Computer Activities**:
  + Navigate to Account Management -> Audit activities like 'Computer Account Management' (Success), and 'User Account Management' (Success & Failure).



* **Audit Tracking Processes**:
  + Select Detailed Tracking -> Audit 'Process Creation' and 'Process Termination' (Success).
* **Audit DS Access**:
  + Choose DS Access -> Audit 'Directory Services Changes' and 'Directory Service Access' (Success).
* **Audit Logon / Logoff Activities**:
  + Go to Logon / Logoff -> Audit 'Logon' and 'Logoff' events (Success & Failure), including 'Network Policy Server' events.
* **Audit Scheduled Tasks**:
  + Select Object Access -> Audit 'Other Object Access Events' (Success).
* **Audit Local Policy Changes**:
  + Navigate to Policy Change -> Audit 'Authentication Policy Change' and 'Authorization Policy Change' (Success).
* **Audit System Events**:
  + Choose System -> Audit 'Security State Change' (Success).

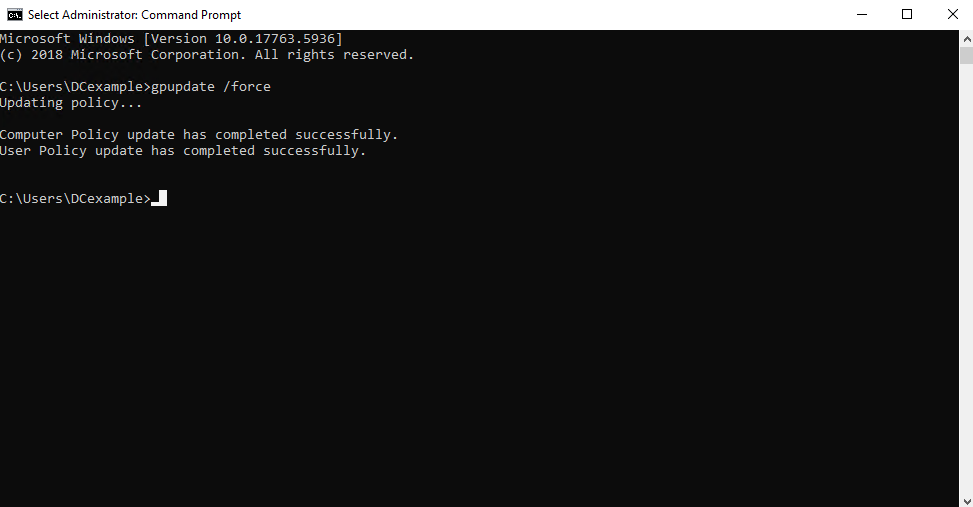
### ****8.5. Enforce Advanced Audit Policy Configuration****

* + In the Group Policy Management Editor, expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
  + In the right pane, find the setting named **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings**.
  + Double-click on this setting to open its properties and Select **Enabled**.
  + Click **Apply**, then **OK** to save the changes.



### ****8.6. Apply and Verify****

* Force Group Policy Update: Open Command Prompt on a domain controller or any relevant computer within the domain.
* Run the command **gpupdate /force** to ensure the new settings are applied immediately.



* Verify the Settings: Use the command **auditpol /get /category:\*** to verify that the auditing settings are correctly applied according to the subcategory settings.

### 8.7. Conclusion

Using the Group Policy Management Console (GPMC), we added a new Group Policy Object (GPO) named "Default Domain Controllers Policy" and navigated to the Advanced Audit Policy Configuration. We then set essential security settings, including Account Policies, Local Policies, and Event Log settings, to meet our organization’s requirements. Advanced audit policies were configured to track critical activities such as logon events, user and group activities, process tracking, directory service access, logon/logoff events, scheduled tasks, local policy changes, and system events. By enabling and enforcing these policies, we established detailed tracking to detect unauthorized access, identify security breaches, and maintain a secure and compliant Active Directory environment. The new settings were applied using **gpupdate /force** and verified with **auditpol** to ensure correct implementation.

## 9. Setting up the Simple Mail Transfer Protocol Secure (SMTPS) Server

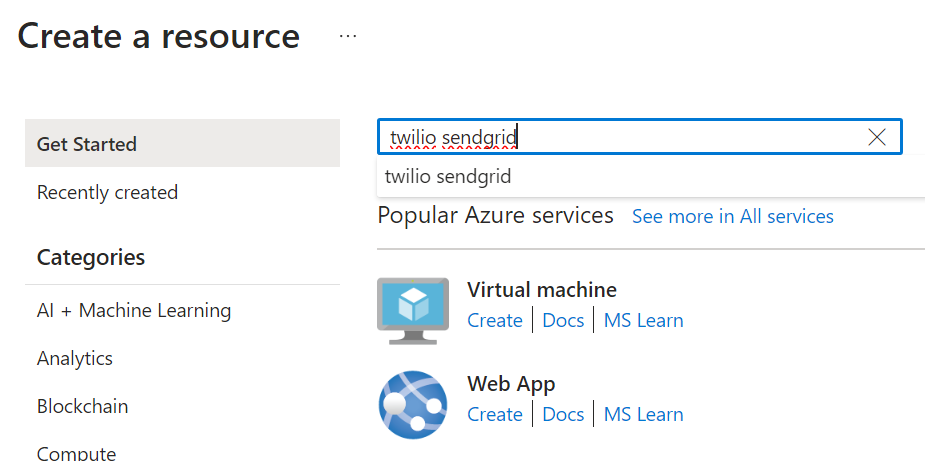
### 9.1. Creating a SendGrid Resource

#### Step 1: Log in to Azure Portal

* **Access Azure Portal**: Open [Azure Portal](https://portal.azure.com/).
* **Log In**: Use your Azure account credentials to log in.

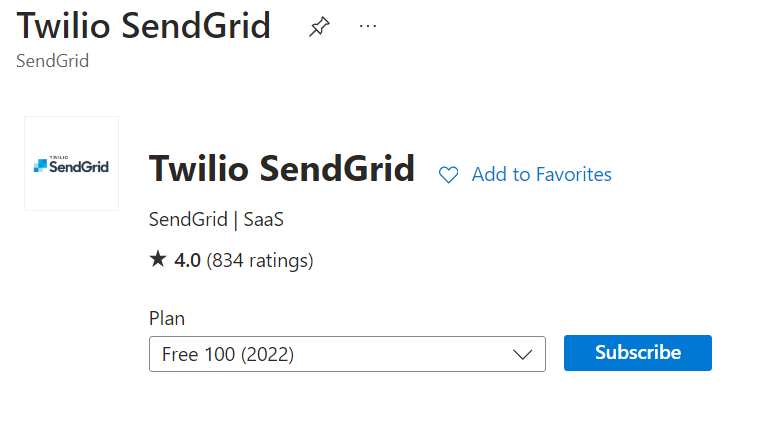
#### Step 2: Navigate to the Azure Marketplace

* **Azure Marketplace**: Select **Create a resource** from the left-hand menu.
* **Search for SendGrid**: Type “SendGrid” in the search bar and press Enter.



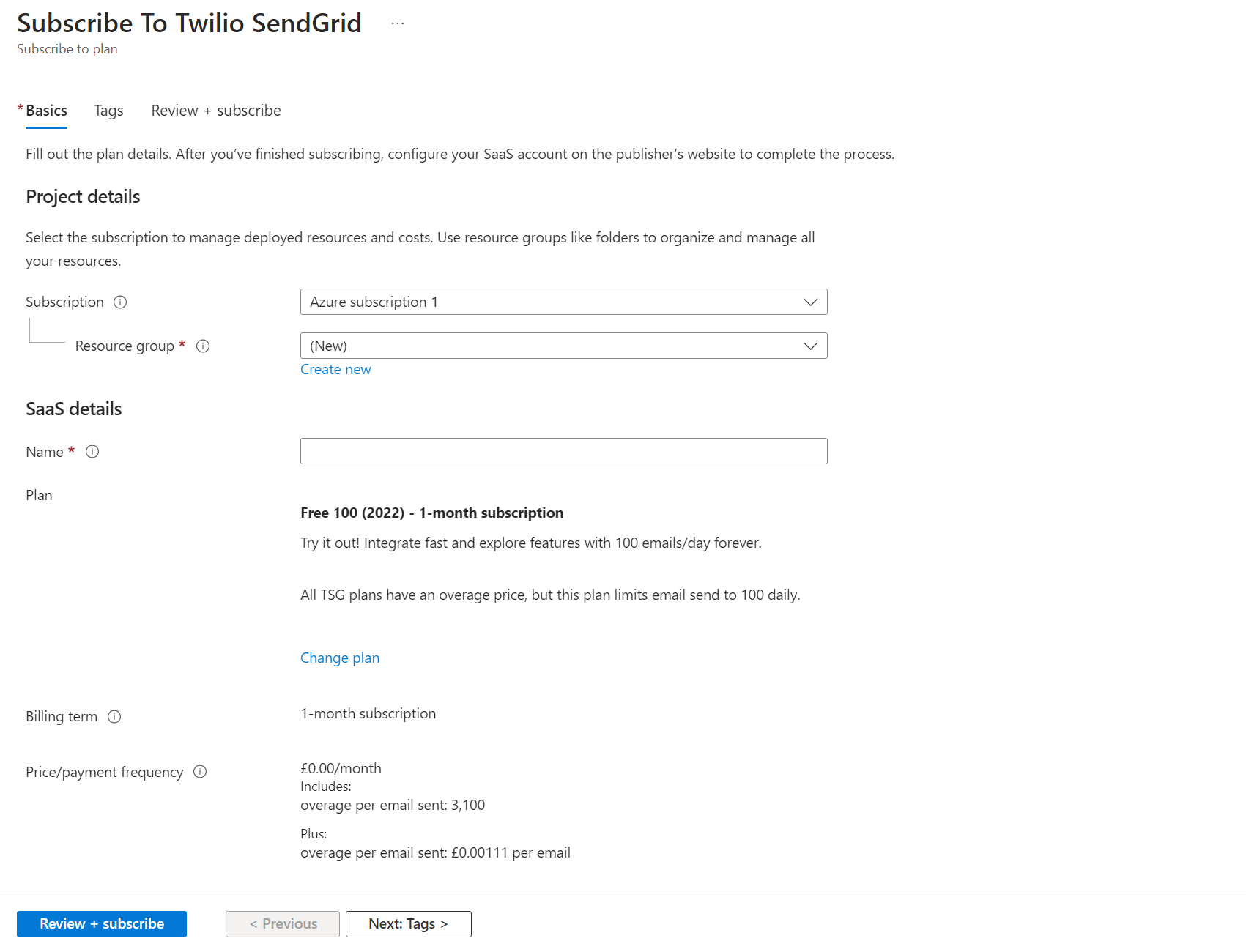
### 9.2. Create SendGrid Account

* **Select SendGrid**: Choose **SendGrid** by Twilio from the search results.
* **Create Account**: Click the **Create** button.



#### Step 1: Configure SendGrid Account

* **Subscription**: Choose your Azure subscription for billing.
* **Resource Group**: Select an existing resource group or create a new one.
* **Name**: Provide a unique name for your SendGrid resource.
* **Pricing Tier**: Select the desired pricing tier.
* **Contact Information**: Enter your contact details.
* **Password**: Set a password for your SendGrid account.



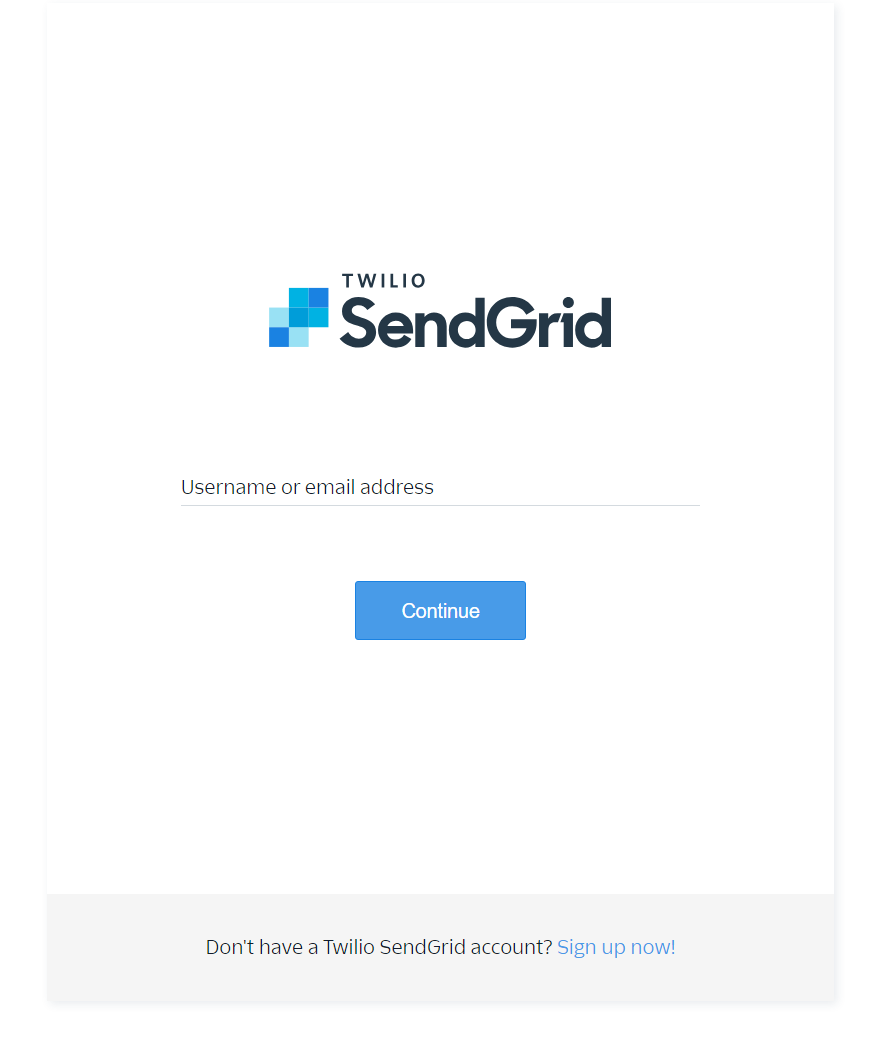
#### Step 2: Review and Create

* **Terms of Service**: Review the terms of service and privacy policy.
* **Review**: Click **Review + Create** to review your settings.
* **Validation**: Ensure all fields are validated.
* **Create**: Click **Create** to provision your SendGrid resource.

### 9.3. Creating a Twilio SendGrid Account

#### ****Step 1: Sign Up for Twilio SendGrid****

* Visit the [Twilio SendGrid website](https://sendgrid.com/).
* Click on the "Sign Up" button.
* Fill in the required details and create your account.



#### ****Step 2: Verify Your Email Address****

* After signing up, you will receive a verification email.
* Click the verification link in the email to activate your account.

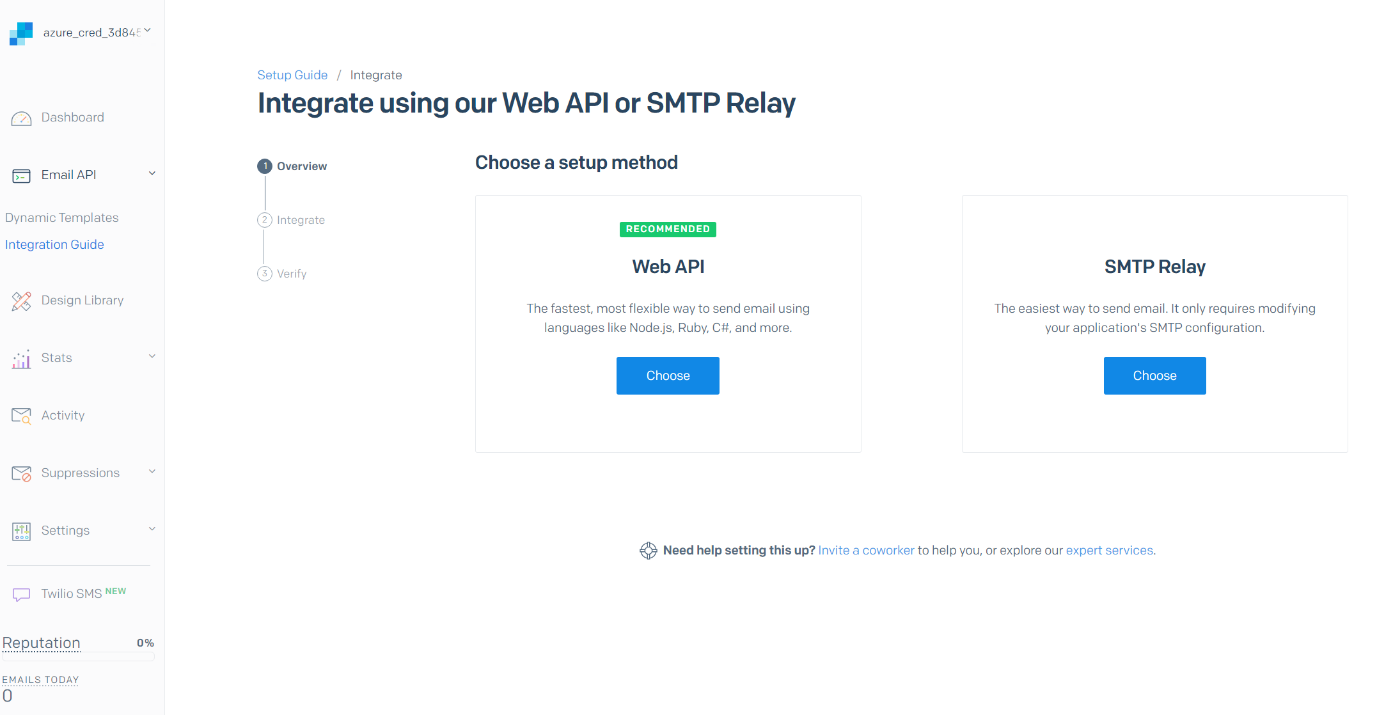
### 9.4. Adding an API Key

#### ****Step 1: Log in to Your Twilio SendGrid Account****

* Go to the Twilio SendGrid login page and log in with your credentials.

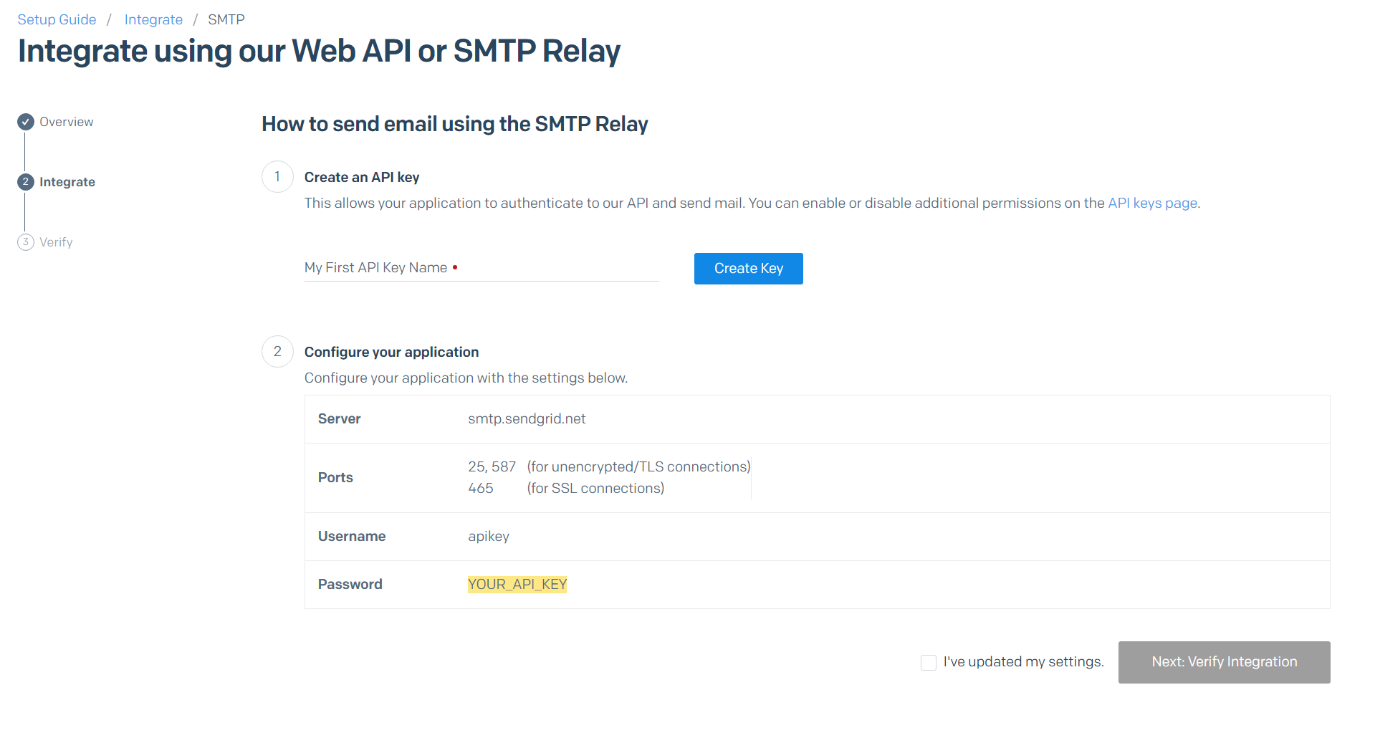
#### ****Step 2: Navigate to API Keys****

* In the dashboard, navigate to "Settings" and then select "API Keys."

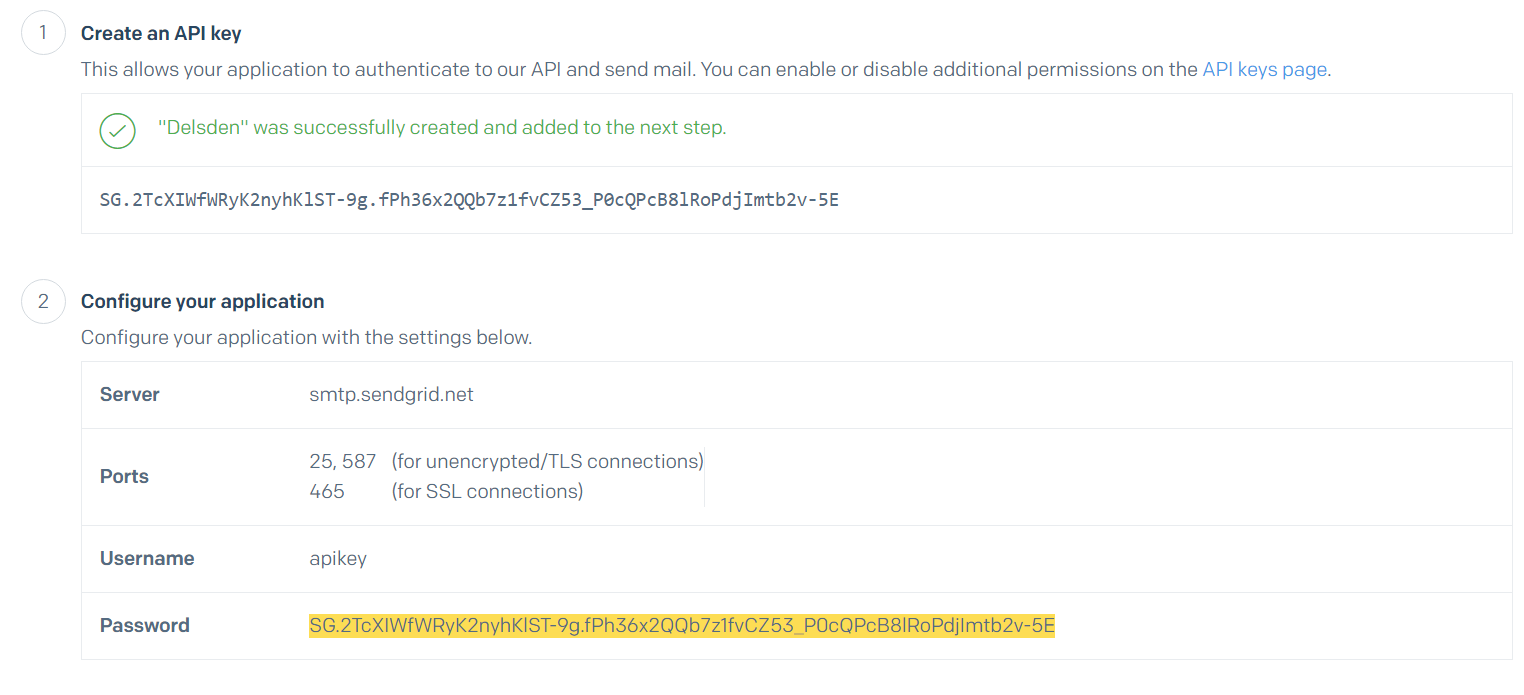


#### ****Step 3: Create an API Key****

* Click on the "Create API Key" button.
* Enter a name for your API key and set the permissions (e.g., Full Access).



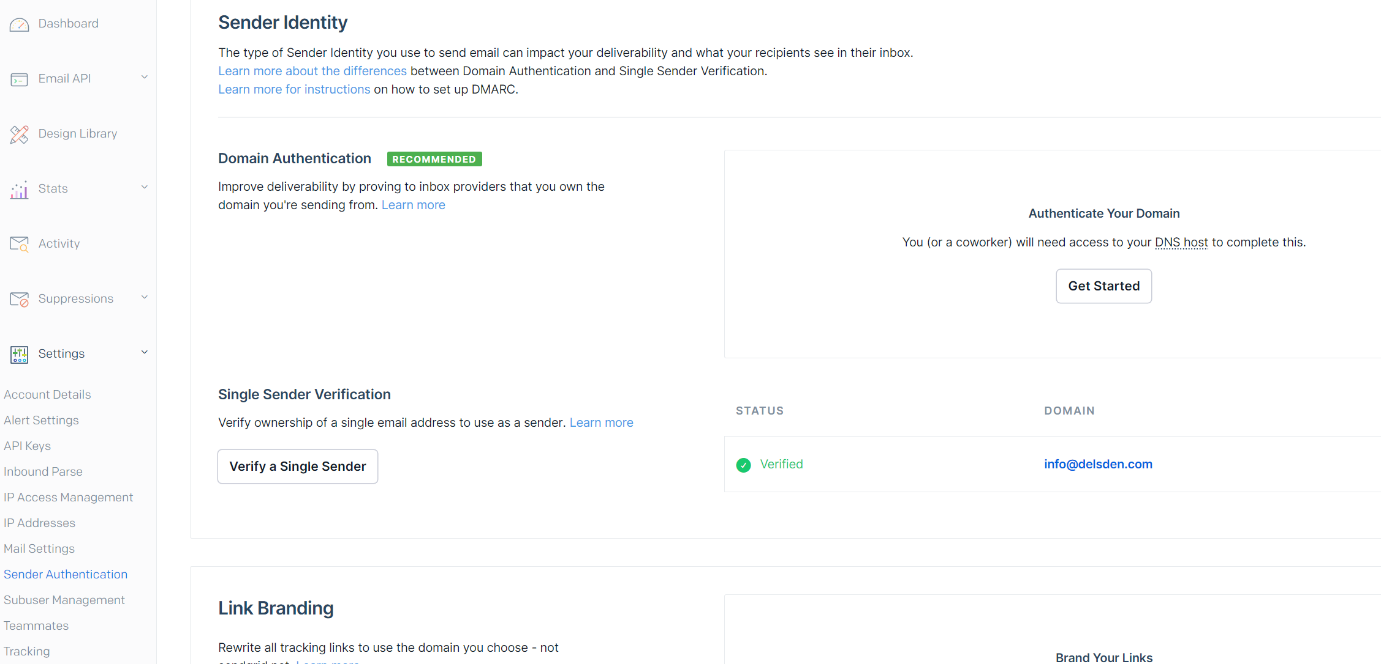
* Click "Create & View" to generate the API key.
* Copy the generated API key for use in your application.



### 9.5. Configuring Sender Authentication

#### ****Step 1: Navigate to Sender Authentication****

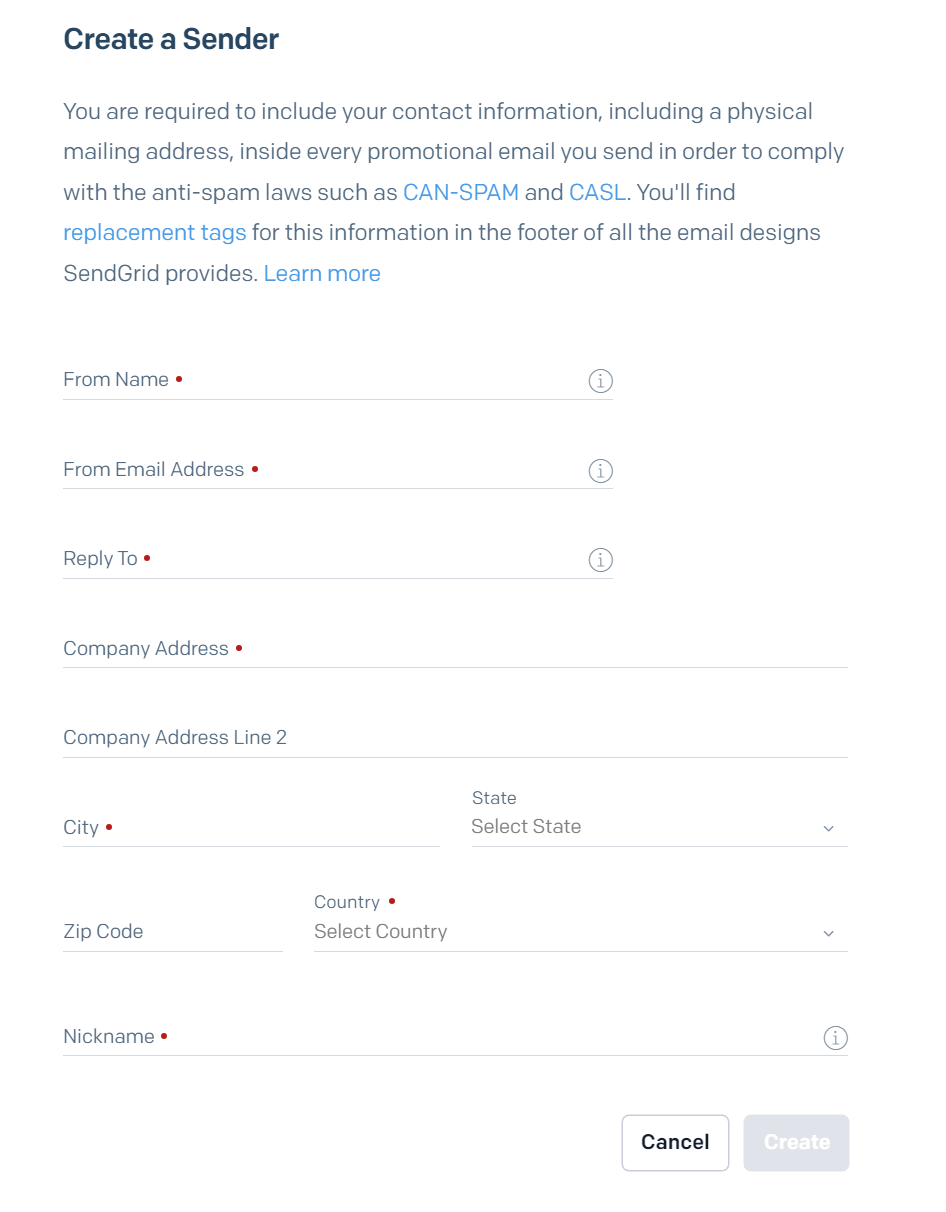
* In your Twilio SendGrid dashboard, go to "Settings" and select "Sender Authentication."



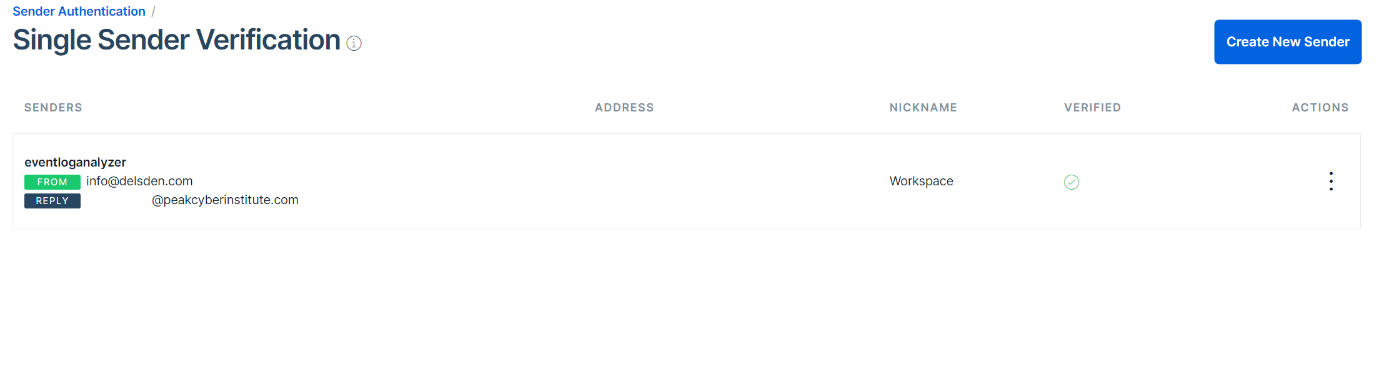
#### ****Step 2: Authenticate Your Domain****

* Choose the "Authenticate Your Domain" option.
* Follow the prompts to enter your domain information and DNS settings.
* Update your DNS records as provided by SendGrid to complete domain authentication.

#### ****Step 3: Verify Single Sender****

****

* Alternatively, you can verify a single sender email address.
* Choose the "Verify a Single Sender" option and enter the required details.
* Verify the email address by clicking the link sent to the specified address.



### 9.6. SMTPS Configuration

#### ****Step 1: Access the Admin Console****

* Open your application and log in with your admin credentials.
* From the application drop-down menu, select Admin Console.

#### ****Step 2: Navigate to Email Settings****

* In the Admin Console, navigate to Administrative Settings.
* Under Administrative Settings, find and select Email Settings.

#### ****Step 3: Configure SMTPS Mode****

* In the Email Settings, look for the Mode option.
* Select SMTP as the mode of email sending.

#### ****Step 4: Enter Mail Server Details****

* Enter the address of your mail server in the Mail Server field (e.g., smtp.example.com).
* Enter the port number your mail server uses for SMTPS in the Mail Port field (e.g., 465).

#### ****Step 5: Specify the From Address****

* In the From Address field, enter the email address you want to use as the sender for all notifications (e.g., no-reply@example.com).

#### ****Step 6: Test Email Address****

* Enter an email address to receive a test email in the Test Email Address field (e.g., test@example.com).

#### ****Step 7: Select Connection Security****

* Choose the connection security type from the available options.
* Select Use SSL if you want to use SSL for secure email transmission.

#### ****Step 8: Select Authentication Type****

* In the Authentication section, select the authentication type.
* Choose Basic Authentication.

#### ****Step 9: Enter Authentication Details****

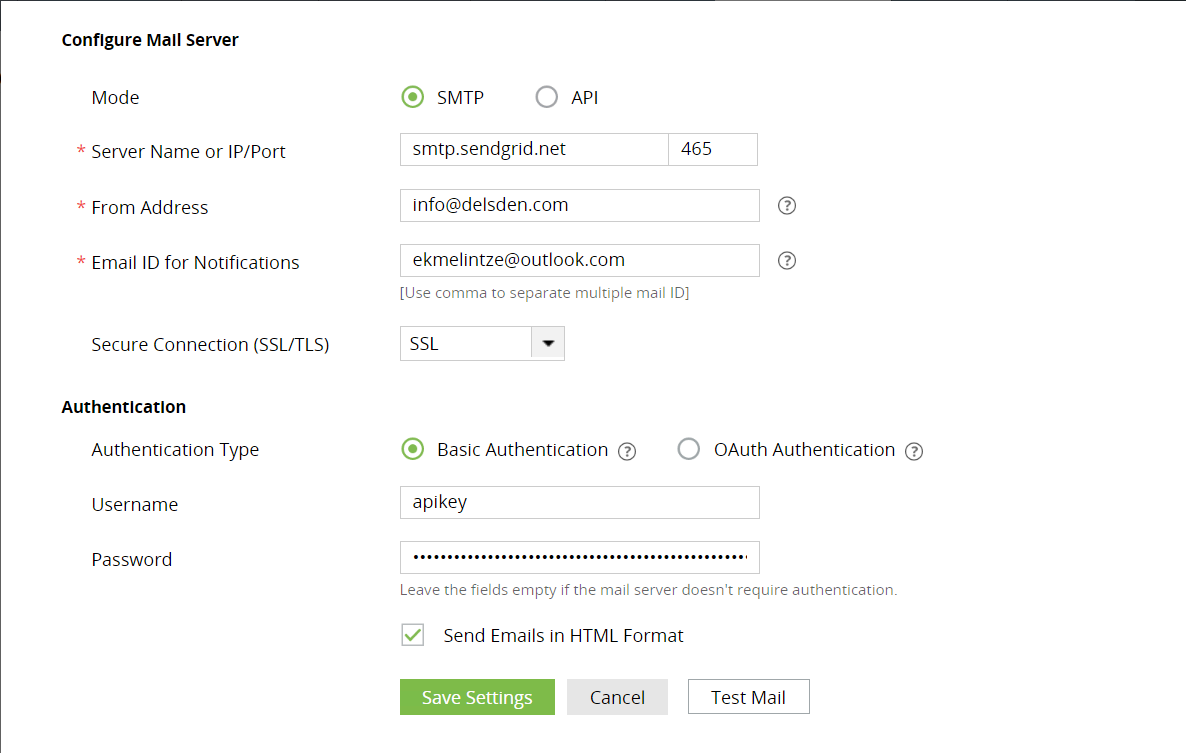
* If Basic Authentication is chosen, enter the Username and Password required to access the mail server.
* Leave these fields empty if your mail server does not require authentication.

#### ****Step 10: Enable HTML Format for Emails****

* Enable this option if you want to view all DataSecurity Plus notification content in a tabularized HTML format.

#### ****Step 11: Save Settings****

* After filling in all the details, click Save Settings to apply the changes.



### 9.7. Conclusion

By following these steps, you will have configured your email server using SMTP in your application. This setup will allow you to send notifications and other emails through your specified mail server, ensuring that your email communication is properly routed and delivered.

## ****10. Report Summary****

In the "Comprehensive Azure and AD Audit Plus Deployment" project we focused on configuring and testing two critical Manage Engine tools: AD Audit Plus. Our primary objective was to establish a reliable and compliant IT infrastructure that supports our organization’s needs and prepares us for future growth.

We began by creating a Windows Server virtual machine in Azure, ensuring a scalable and efficient cloud infrastructure. This foundational step allowed us to configure and secure network security groups (NSGs), essential for protecting our network by allowing only necessary traffic and minimizing potential attack vectors.

Securing Remote Desktop Protocol (RDP) was another crucial task. By verifying NSG rules, changing the default RDP port, enabling Network Level Authentication (NLA), and enforcing credential prompts, we significantly reduced the risk of automated attacks and ensured that only authenticated connections could be established.

Setting up an Azure Event Hub was vital for effective log management. This enabled us to collect and analyse large amounts of event data in real-time, providing comprehensive monitoring and better security insights.

Configuring the virtual machine as a domain controller was necessary for centralizing network management, handling user logins, and managing permissions securely. This setup streamlined our network operations and reinforced security.

We also allowed Internet Control Message Protocol (ICMP) traffic, which is essential for network reliability and troubleshooting connectivity issues. Verifying these settings confirmed our setup's accuracy, ensuring smooth network operations.

Creating snapshots of the virtual machine provided a reliable backup solution, allowing us to quickly restore the VM to a previous state in case of failure, thus ensuring data integrity and operational continuity.

Configuring advanced audit policies for Active Directory using the Group Policy Management Console enabled detailed tracking of critical activities. This step was crucial for detecting unauthorized access, identifying security breaches, and maintaining a secure and compliant Active Directory environment.

Enforcing HTTPS in AD Audit Plus and setting up a secure SMTP server using SendGrid ensured secure communication for notifications and alerts, further enhancing the overall security posture.

By meticulously following these steps, we achieved a robust and secure IT infrastructure. This comprehensive setup not only meets industry standards and regulatory requirements but also provides a solid foundation for effective monitoring, management, and protection of our IT environment, ensuring future growth and success.