**A computer network diagram on a black background

Description automatically generated with low confidence**

**Domain Name Registration**

To register a domain name, follow these steps:

1. Choose a domain registrar service provider. For this example, we will use GoDaddy as the registrar.
2. Visit the GoDaddy website or any other domain registrar of your choice.
3. Search for the desired domain name, [DomainName] using the registrar's domain search feature.
4. If the domain name is available, proceed with the registration process. If not, try different variations or consider choosing a different domain name.
5. Follow the instructions provided by the registrar to complete the domain registration process. This typically involves providing your contact information, selecting the registration duration, and making the necessary payment.
6. During the registration process, you may be asked to provide the public IP address from your Internet Service Provider (ISP). This information helps associate the domain name with the correct server or website.
7. Once the registration is complete, you will become the owner of the domain name for the specified duration. It is important to renew the registration before it expires to retain ownership of the domain.

**Active Directory and Domain Controller Setup**

Follow these steps to set up Active Directory and a Domain Controller:

1. Install Active Directory and Domain Services:

a. Open Server Manager and navigate to "Server Roles."

b. Select "Active Directory Domain Services" and click on "Add Feature."

c. Choose the required features like DNS Server and install them.

d. Once the installation is complete, click on "Promote this server as a domain controller" in the same window.

e. Select "Add a new forest" and enter the root domain name, such as "[DomainName] ."

f. Configure the domain controller options and set the DSRM (Directory Services Restore Mode) password.

g. Proceed with the installation, and the server will be rebooted.

1. Create Organizational Units (OUs) and Users:

a. Open "Active Directory Users and Computers" and right-click on "[DomainName] ."

b. Create a new OU (Organizational Unit) named "MonGuardiansOrg."

c. Within the new OU, create another OU named "Users."

d. Create new user accounts within the "Users" OU, such as Monday, Tuesday, Wednesday, Exchangeadmin, Thursday, Friday, Saturday.

1. Verify Active Directory Sites and Services:

a. Open "Active Directory Sites and Services."

b. Verify that the server and domain controller are created under the appropriate site.

1. Configure DNS Management:

a. Open "DNS Management" and create a forward lookup zone for "[DomainName] ."

b. Verify that the Host A record is created correctly.

**Preparing Active Directory for Exchange 2016**

Before installing Exchange 2016, make sure to complete the following steps:

1. Install the required software:

a. Install .NET Framework 4.8.

b. Install the Visual C++ Redistributable Package for Visual Studio 2012.

1. Ensure the installation account has the necessary permissions:

a. Enterprise Admins group membership: Required if this is the first Exchange server in the organization.

b. Schema Admins group membership: Required if the Active Directory schema hasn't been extended or prepared for Exchange 2016.

c. Exchange Organization Management role group membership: Required if the Active Directory domain already contains Exchange servers.

**Installing and configuring Exchange Server 2016**

Exchange Server 2016 Prerequisites

Network and Update:

1. Network Configuration:
   * Network card: Main on Hyper-V
   * IP address: 192.168.xx
     + Gateway: 192.168.y.y
     + DNS: 192.168.1.zz, 8.8.8.8
   * Exclude IP ranges 192.168.1.xx , and 192.168.1.yy in the network router DHCP settings to prevent other devices from being assigned the server's static IP.
   * Change the computer name to "ADDC-Server1."
2. Update Windows:
   * Install the latest Windows updates.

Exchange Server 2016 Prerequisites:

1. Log in to the Exchange server with local admin credentials.
2. Run the following command in Windows PowerShell to install the required Windows components:

Install-WindowsFeature NET-Framework-45-Features, Server-Media-Foundation, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS

1. Install the following software in order:
   * .NET Framework 4.8
   * December 13, 2016 (KB3206632) security update (if applicable)
   * Visual C++ Redistributable Package for Visual Studio 2012
   * Visual C++ Redistributable Package for Visual Studio 2013
   * IIS URL Rewrite Module (for Cumulative Update 22 or later)
   * Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit
2. If installing Exchange 2016 Edge Transport servers on Windows Server 2016:
   * Run the following command in Windows PowerShell to install the required Windows components:
   * Install-WindowsFeature ADLDS  
     Install .NET Framework 4.8
   * Install Visual C++ Redistributable Package for Visual Studio 2012

Install Exchange Server Cumulative Update 19:

* Log in as a domain admin.
* Reboot after the server installation is complete.

Create Exchange Admin Roles group:

* Go to ECP -> Permissions -> Admin Roles.
* Click on the "+" sign to add a new group named "Exchange Admin Users."
* Add roles: Databases, Disaster Recovery, E-Mail Address Policies, Migration.
* Add "exchangeadmin" and "administrator" users as members.

Create User Mailbox:

* Log in to the Exchange Admin Center via a browser: https://<exchange server host name>/ecp/
* Go to Recipients -> Mailboxes.
* Click on the "+" sign to add new mailboxes for the AD users (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).

Test Mail Flow between domain users:

* If encountering HTTP error 404 to access OWA login, run the following commands:

Set-Owavirtualdirectory -identity "Exchange-Server\owa (Exchange Back End)" -WindowsAuthentication $True -Basicauthentication $false -Formsauthentication $false  
iisreset

* Launch the URL: https://<exchange server host name>/owa
* Login to OWA as a mailbox user.
* Send a new email from and to internal email users to confirm proper internal email flow.

Note: If mail flow is not working properly (unable to send and receive emails internally), configure the local DNS server IP on the exchange server's DNS lookups via ECP:

* Go to Exchange Control Panel (ECP) and navigate to 'Servers.'
* Select your Exchange server and press Edit.
* Select DNS Lookups in the left-side menu.
* For internal DNS lookups, select Custom settings and add the local DNS server IP.
* Restart the Exchange Transport Service.

**Configure AutoDiscover, ActiveSync, Outlook Anywhere, MAPI Over HTTP**

1. Prerequisites:

Add a host A record in the Domain Name Service.

1. Configure the name space by creating a host A record in the DNS [DomainName] domain: mymail.[DomainName] - 192.168.1.xx
2. Configure AutoDiscover URL for internal:
   * Open Exchange Management Shell (EMS).
   * Check the current AutoDiscover service URL:

Get-ClientAccessService | fl name.auto\*

* Set the AutoDiscoverServiceInternalUri to:

Get-ClientAccessService | set-ClientAccessService -AutoDiscoverServiceInternalUri [https://mymail.[DomainName] /Autodiscover/Autodiscover.xml](https://mymail.monguardians.com/Autodiscover/Autodiscover.xml)

1. Configure Internal and External URLs for OWA in Exchange Admin Center (EAC):
   * Go to EAC -> Servers -> Virtual Directories.
   * Edit OWA (Default Web Site).
   * Set Internal URL: mymail.[DomainName] /owa, External URL: mymail.[DomainName] /owa, then save the changes.
2. Configure Internal and External URLs for MAPI:

* In EMS, check the current virtual directory settings:

Get-MapiVirtualDirectory

1. Set the internal and external URLs for MAPI:

Get-MapiVirtualDirectory | Set-MapiVirtualDirectory -InternalURL [https://mymail.[DomainName] /mapi](https://mymail.monguardians.com/mapi) -ExternalURL [https://mymail.[DomainName] /mapi](https://mymail.monguardians.com/mapi)

1. Reset the IIS service:

Iisreset

**Send Emails to the Internet (Gmail, Yahoo, Hotmail, etc.,) - Configure Send Connector**

**Prerequisites:**

To configure the Send Connector in Exchange Server for using AuthSMTP as the outgoing SMTP email service for the domain "[DomainName] ," follow these steps:

1. Open the Exchange Admin Center (EAC) and navigate to "Mail Flow" and then "Send Connectors."
2. Click on the "+" sign to add a new send connector. In the type options, select "Internet" and click "Next."
3. Provide a name for the send connector, such as "EmailsToInternet," and click "Next."
4. Select the option "MX record associated with recipient domain" and click "Next."
5. In the "New Send Connector" section, click on the "+" sign to add a domain.
6. In the "Add Domain" section, select the type as "SMTP" and enter the Fully Qualified Domain Name (FQDN) as "\*". This wildcard FQDN allows sending emails to any domain. Click "Save" and then click "Next."
7. Click the "+" sign to add the Exchange server hostname. Select the appropriate Exchange server from the list and click "Add," then click "OK."
8. Click "Finish" to complete the configuration of the send connector.

**Configure the SmartHost in Exchange Server**

To configure the SmartHost in Exchange Server for the "EmailsToInternet" send connector using AuthSMTP as the outgoing SMTP email service, follow these steps:

a. Go to the Exchange Admin Center (EAC) and navigate to "Mail Flow" and then "Send Connectors." Select the "EmailsToInternet" send connector and click on "Edit."

b. In the "Delivery" section, select the option "Route mail through smart hosts." Click the "+" sign to add a smart host.

c. Enter the smart host name as "mail.authsmtp.com." Enable basic authentication and provide the username and password of the AuthSMTP service. Click "Save" to save the configuration.

d. By default, the send connector in Exchange Server uses port 25. To change the default port to one of the ports provided by AuthSMTP (such as 2525, 23, or 26), you can use Exchange Shell.

e. Open Exchange Shell and run the following commands:

Get-SendConnector | fl Port  
Set-SendConnector -Identity "EmailsToInternet" -Port 2525  
This will change the port of the "EmailsToInternet" send connector to 2525. You can replace 2525 with the desired port provided by AuthSMTP.

f. To verify that the port has been set correctly, run the following command in Exchange Shell:

Get-SendConnector | fl Port  
Ensure that the port is now set at 2525.

1. To test the SmartHost (AuthSMTP) configuration, send test emails to Internet recipients. Monitor the email delivery and check if the emails are being successfully routed through AuthSMTP.

### **Receive emails from the Internet (Gmail, Yahoo, Hotmail, etc.,) - Configure Receive Connector**

**Prerequisites**

To configure email redirection for the domain "[DomainName] " using DNSExit as the redirection service and port 940, follow these steps:

a. Create an MX record in the Domain Service (e.g., GoDaddy):

* Access the External DNS settings for your domain (e.g., GoDaddy).
* Create an MX record with the following details:
  + Type: MX
  + Name: @
  + Priority: 10
  + Value: smtp.dnsexit.com
  + TTL: 1 hour

This MX record tells incoming emails to route through DNSExit for redirection.

b. Configure the Receive connector in Exchange Server:

* Access the Exchange Control Panel (ECP) and go to "Mail Flow."
* Leave the default configurations (Client Frontend, Client Proxy, Default, Default Frontend, Outbound Proxy Frontend) unchanged.
* Add a new receive connector for DNSExit redirection:
  + Click the "+" sign.
  + Provide a name for the connector.
  + Set the Role as "FrontEnd Transport."
  + Select the Type as "Internet" and specify the Port as "940."

This configuration allows Exchange Server to listen for incoming emails on port 940 for redirection.

c. Verify network settings on the host machine:

* Ensure that the network settings on the host machine are correctly configured.
* Set the DNS server to point to the IP address of the DNS/Domain Controller (e.g., 192.168.1.zz).
* Leave the secondary DNS blank to avoid using an external DNS IP like 8.8.8.8.

This configuration ensures that the host machine uses the correct DNS server for name resolution.

d. Set up port forwarding on the network router:

* Access your network router's settings.
* Configure port forwarding to forward incoming traffic on port 940 to the IP address of the Exchange host machine.
* This step allows incoming emails from outside to reach Exchange Server through DNSExit.

e. Test the configurations using DNSExit's Mail Redirection Checking Tool:

* Use DNSExit's Mail Redirection Checking Tool to verify that the email redirection is functioning correctly.
* Send test emails to your domain and check if they are redirected as expected.

By following these steps, you will have configured email redirection for the domain "[DomainName] " using DNSExit as the redirection service on port 940.

## **SSL Certificates for Outlook client preparation**

### **Create a new self-signed certificate.**

To create a self-signed certificate for the Exchange Server host in the Exchange Admin Center (EAC), follow these steps:

1. Access the Exchange Admin Center (EAC) and navigate to "Servers" and then "Certificates."
2. Click on the "+" sign to create a new certificate.
3. Choose the option to create a self-signed certificate.
4. Provide a friendly name for the certificate. This name is used to identify the certificate within Exchange Server.
5. Select the root domain for which the certificate will be created. In this case, select the root domain associated with your Exchange Server.
6. Click on "Browse" to select the Exchange Server host for which the certificate will be created.
7. Once you have selected the Exchange Server host, click "Next" to proceed.
8. Review the certificate settings and click "Next" to continue.
9. On the final screen, click "Finish" to create the self-signed certificate.

### **Certificate binding in IIS Service Manager**

1. IIS Service Manager -> Expand the Host Name (EXCHANGE-SERVER) -> Expand Sites ->Default Web Site -> Click on “Bindings” in right column -> Add.. -> Type <https>, IP address <All Unassigned>, Host name <mymail.[DomainName] >, SSL Certificate <pick the new certificate just created>
2. Reset IIS by cmd “iisreset”

### **Install Certificate**

To install the certificate and add a CNAME record for Autodiscover in DNS Forward Lookup, follow these steps:

a. Open a web browser and browse to the OWA site, which in this example is "[https://mymail.[DomainName] /owa](https://mymail.monguardians.com/owa)."

b. Export the certificate from the browser:

* Click on the lock icon or the padlock symbol next to the website URL.
* Look for the option to export or view the certificate.
* Follow the prompts to export the certificate, saving it to a desired location on your computer.

c. Open the Certificate Manager:

* Press Windows Key + R to open the Run window.
* Type "certmgr.msc" and press Enter.
* This will open the Certificate Manager.

d. Install the exported certificate:

* In the Certificate Manager, expand the "Trusted Root Certification Authorities" folder.
* Right-click on "Certificates" and choose "All Tasks" > "Import."
* Follow the prompts to locate and import the exported certificate.
* Repeat the same process for the "Personal" folder in the Certificate Manager.

e. Add a CNAME record for Autodiscover in DNS Forward Lookup:

* Access your DNS management console or DNS service provider.
* Locate the zone for "[DomainName] " in the Forward Lookup Zone.
* Right-click on the zone and select "Add CNAME" or "New Alias."
* Enter "Autodiscover" as the Alias name.
* Provide the FQDN for the target host as "<Exchange-Server.[DomainName] >."
* Save or apply the changes to add the CNAME record.

## **Install Analysis VM**

To configure Outlook for the email account [DesignatedEmail@[DomainName]](mailto:OCRAnalyst@monguardians.com)  and set up Outlook Anywhere, follow these steps:

1. Install Outlook:
   * Download and install Microsoft Outlook on your Windows 10 Pro computer.
2. Set up the email account in Outlook:
   * Open Outlook and click on "File" in the top menu.
   * Click on "Add Account" to start the email account setup wizard.
   * Enter the email address [DesignatedEmail@[DomainName]](mailto:OCRAnalyst@monguardians.com)  and follow the prompts to set up the account.
   * Provide the necessary login credentials and account settings when prompted.
3. Configure Outlook Anywhere using PowerShell:
   * Open PowerShell as an administrator.
   * Run the following command to set the Outlook Anywhere configuration:
   * Get-OutlookAnywhere -Server Exchange-Server | Set-OutlookAnywhere -ExternalHostname mymail.[DomainName] -InternalHostname mymail.[DomainName] -ExternalClientsRequireSsl $true -InternalClientsRequireSsl $true -DefaultAuthenticationMethod NTLM
4. Verify the Outlook Anywhere configuration:
   * Run the following command to retrieve the Outlook Anywhere configuration:
   * Get-OutlookAnywhere -Server Exchange-Server | Format-List ExternalHostname, InternalHostname
   * Check the output to ensure that the "ExternalHostname" and "InternalHostname" values are set to "mymail.[DomainName] ."

By following these steps, you will have installed and configured Outlook on your Windows 10 Pro computer for the email account [DesignatedEmail@[DomainName]](mailto:OCRAnalyst@monguardians.com) . Additionally, you will have set up Outlook Anywhere with the specified hostnames and authentication method.

### **Install Exchange Management Tool**

<https://learn.microsoft.com/en-us/Exchange/plan-and-deploy/post-installation-tasks/install-management-tools?view=exchserver-2016>

Prerequisites:

* Visual C++ Redistributable Package for Visual Studio 2012
* IIS6 Management Compatibility Feature installation

To install the IIS6 Management Compatibility Feature, open the Command Prompt (CMD) and run the following command:

dism /online /Enable-Feature /FeatureName:IIS=IIS6ManagementCompatibility /all

Download Exchange Server Cumulative Update 19.

During the Exchange Server installation, make sure to select the option for installing the Exchange Management Tools.

## **Setup a designated account to analyze image attachments**

To create a mail forwarding rule in the Exchange Control Panel (ECP) for redirecting emails with image attachments to the DesignatedEmail inbox, follow these steps:

1. Access the Exchange Control Panel (ECP) and navigate to "Mail Flow" and then "Rules."
2. Click on "New rule" to create a new rule.
3. Provide a name for the rule, such as "Image Analysis."
4. Click on "More options" to access additional rule conditions.
5. Under "Apply this rule if...," select "Any attachment" and choose "File extension includes these words."
6. Click on the "+" sign to add file extensions. Add the following file extensions: "jpg," "jpeg," "png," "gif."
7. Add a condition under "Apply this rule if..." by selecting "The sender..." and choose "is external/intenet."
8. Select the sender location as "outside the organization."
9. Under "Do the following...," choose "Redirect the message to..." and add the DesignatedEmail account as the recipient.
10. Choose a mode for this rule. Select "Enforce" to ensure the rule is applied.
11. Click "Save" to save the mail forwarding rule.

A screenshot of a computer

Description automatically generated

By following these steps, you will have created a mail forwarding rule in the ECP that redirects emails with image attachments from external senders to the DesignatedEmail inbox.

## **Image Analysis by Optical Character Recognition (OCR) Application**

**Analyze each email in the Image Analyst inbox using OCR as it arrives.**

To analyze each email in the Image Analyst inbox using OCR as it arrives, follow the steps below:

Ensure the "exchange admin" account has Import Export permission by running the following command:

New-ManagementRoleAssignment -Role "Mailbox Import Export" -User "exchange admin" | Format-Table -AutoSize

Download and install the OCR Module by executing the following command:

Install-Module -Name PsOcr -Scope CurrentUser

Convert the image files to text files using the PSOImageToText module and save them to a file. Iterate through each file in the specified directory using the following code:

foreach ($file in Get-ChildItem "C:\Users\ExchangeAdmin\Desktop\Attachments\Images\")

{

$OCRText = Convert-PsoImageToText -Path (Join-Path 'C:\Users\ExchangeAdmin\Desktop\Attachments\Images\' $file)

Write-Output $OCRText >> "C:\Users\ExchangeAdmin\Desktop\Attachments\Images\ImageToText.txt"

}

Search for and delete email messages. Use the ORC recognition script to find matching emails and delete them using the following command:

Search-Mailbox -Identity "<email address>" -SearchQuery 'Subject:"<subject>"' -DeleteContent -Force

Replace "<email address>", "<subject>", and "<time>" with the appropriate values obtained from the main script.

Create a Content Search to find the message to delete. Use the following commands:

$Search = New-ComplianceSearch -Name "[NewComplianceSearchName]" -ExchangeLocation All -ContentMatchQuery '(Received:4/13/2016..4/14/2016) AND (Subject:"Action required")'

Start-ComplianceSearch -Identity $Search.Identity

Delete the messages found by the search:

New-ComplianceSearchAction -SearchName "[NewComplianceSearchName]" -Purge

For more information and detailed instructions, refer to the following link: Microsoft 365 Compliance - eDiscovery: Search for and delete email messages.

**Create a task scheduler**

The objective is to execute the script whenever an email is received in the DesignatedEmail Quarantine folder.

To create a rule in Outlook that sends a desktop notification when an email arrives, follow these steps:

1. Open Outlook and go to "File" > "Manage Rules & Alerts."
2. In the "Rules and Alerts" window, click on "New Rule."
3. In the "Start from a blank rule" section, select "Apply rule on messages I receive" and click "Next."
4. Skip any conditions by clicking "Next" without selecting any options.
5. Choose the action "Display a Desktop Alert" and click "Next."
6. Skip any exceptions by clicking "Next" without selecting any options.
7. Specify a name for this rule and click "Finish."

To confirm that the desktop notification works, send a test email to your mailbox and check if the Desktop Alert appears.

To find the event ID for the Desktop Alert, you can use PowerShell. Follow these instructions:

1. Open PowerShell and enter the following command:

Get-EventLog -LogName System -Newest 5

This command displays the newest five events logged by the system. You may need to perform additional testing and investigation to identify the specific Event ID associated with the Desktop Alert.

To create a new Task Schedule, follow these steps:

1. Open the Task Scheduler application.
2. Click on "Create Task."
3. Provide a name for the task and select the following options:
   * Security Option: "Run only when the user is logged on"
   * Configure for: Select the version of Windows you are using (e.g., Windows 10)
4. In the "Triggers" tab, configure the trigger as follows:
   * Begin the task: "On an event"
   * Settings: "Basic"
   * Log: "System"
   * Source: "DistributedCOM"
   * Event ID: Enter the Event ID you identified for the Desktop Alert
5. In the "Actions" tab, configure the action as follows:
   * Action: "Start a program"
   * Program/script: "Powershell.exe"
   * Add arguments (optional): "-ExecutionPolicy Bypass [the full path of your script]"
6. Click "OK" to save the task.

By following these steps, you should be able to create a rule in Outlook to display a desktop notification when an email arrives and set up a Task Schedule to execute a script based on the associated event.