RSA

GUC
German University in Cairo

# (NETW 1002)

## Systems and Network Security

## Milestone 1

## Deadline: Thursday, 17 April 2025

OWN YOUR IDENTITY.

# Milestone 1:

**This milestone aims to build the foundational infrastructure by configuring a Windows Server as a Domain Controller (DC) and setting up essential network services. It includes enabling DNS resolution for both internal and external hosts and establishing an Active Directory (AD) to host and manage users. Additionally, this milestone involves integrating the Identity Router (IDR) with the Cloud Authentication Service (CAS) and linking CAS to the DC, creating a functional IAM environment in preparation for the next steps.**

1. **Install a Windows Server virtual machine**
    a. Create a new Windows server Virtual Machine (VM) using its ISO image.
    b. Configure the VM's network adapter to connect to VMnet8 **(NAT)** to enable internet access.
    c. Identify the current IP address of the machine and assign it statically to avoid connectivity issues.
    d. Install the **DNS**, **Active Directory domain service (AD DS),** and **DHCP** roles on the Domain Controller (DC).
    e. Add a **DNS forwarder** entry to the DNS server to allow external hostname resolution, this forwarder IP should be the gateway IP address of VMnet8. Kindly follow the following to get the forwarder IP address:
        i. Open VMware Workstation.
        ii. Go to Edit → Virtual Network Editor.
        iii. Select VMnet8 and click NAT Settings.
        **iv.** Note the Gateway IP Address.
    **f.** Promote the Windows Server to a **Domain Controller (DC)** and assign the domain name in the format **rsa<YOUR-GROUP-ID>-local.com** (e.g., **rsa1-local.com**).

2. **Install the RSA Identity router virtual machine**
    a. Log in to the cloud admin console (CAC) and navigate to Platform → Identity Routers and click on **"Obtain IDR template"**.
    b. Open the VMware Workstation and click on File → Open and select the **IDR OVA** file.
    c. Right click on the IDR machine, edit network settings, and delete the second **Network Interface Card (NIC).**
    d. Connect the remaining NIC to VMNET8(NAT) as the domain controller.
    **e.** Power on the machine, login using the default username and password ("idradmin" and "s1mp13"), and fill out the network configurations and complete the quick setup. Change the password to "**RSA_GUCNetw@2025"**
    f. Once the **IDR URL** is displayed in the **CLI**, open a web browser, navigate to the **IDR URL**, and complete the **quick setup** by adding the **Windows Server IP address** as the **DNS** for the IDR and NTP server to be **time.google.com**
    g. In the **Cloud Console**, create an entry for the **IDR** and observe the registration code and the authentication service domain.
    h. Access the **IDR management console** and connect the IDR with the Cloud Authentication service.

3. **Integrate an identity source with Cloud Authentication Service (CAS)**

    a. Create an **identity source** with name <**On-Prem AD**> at the Cloud console and provide the default **domain administrator** username and password as a service account for the establishment of connection.

b. Ensure that the connection is configured to use **LDAP protocol port without TLS/SSL**.
c. Create 5 users with the names of each member of the group in the active directory **and synchronize the identity source** from the Cloud console. (Make sure to assign an email address to all users in the Active directory)
d. **Download and install RSA Authenticator app on your iOS or Android mobile phones.**
e. **Enroll the users to have MFA cloud tokens on their mobile phones.** The administrator should distribute the enrollment URL as well as the enrollment code for each user to self-register the token on their mobile phones.

4. **RSA CAS Reporting:**
   a. Download All users report from CAS > Users > Reports > Generate All Users Report > Download CSV

5. **My Page Configuration – Adding Access Policy & Customization**
   a. Create an **access policy 2.0** to be used for all users trying to access **My Page**. The policy should challenge the users to enter their **password and then approve** the notification on their mobile phone.
   b. After the policy is created, assign it to My Page – My Applications Page
   c. **Customize** My Page with a background image and a title containing the group number. My Page – RSA <YOUR-GROUP-ID> (e.g. **My Page - RSA Group 1)**
   d. Try to access My Page with the users that you created earlier using the MyPage URL found in the cloud console >> Access >> MyPage.

**Reference Links:**

1. Assurance Levels & Configure Assurance Levels
2. Access Policies, Manage Access Policies & Access Policy Examples
3. IDR deployment
4. Authentication registration

## Expected Architecture: