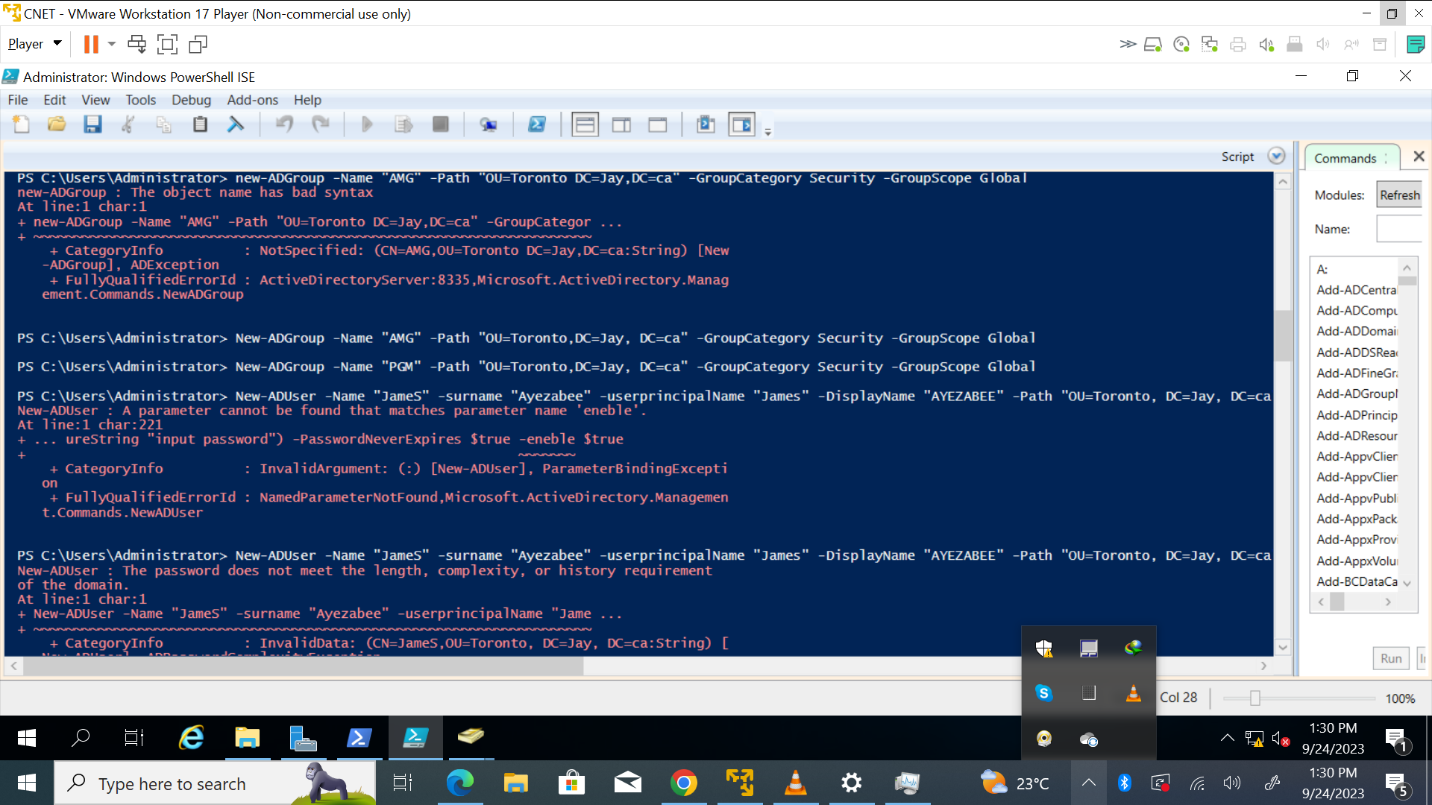
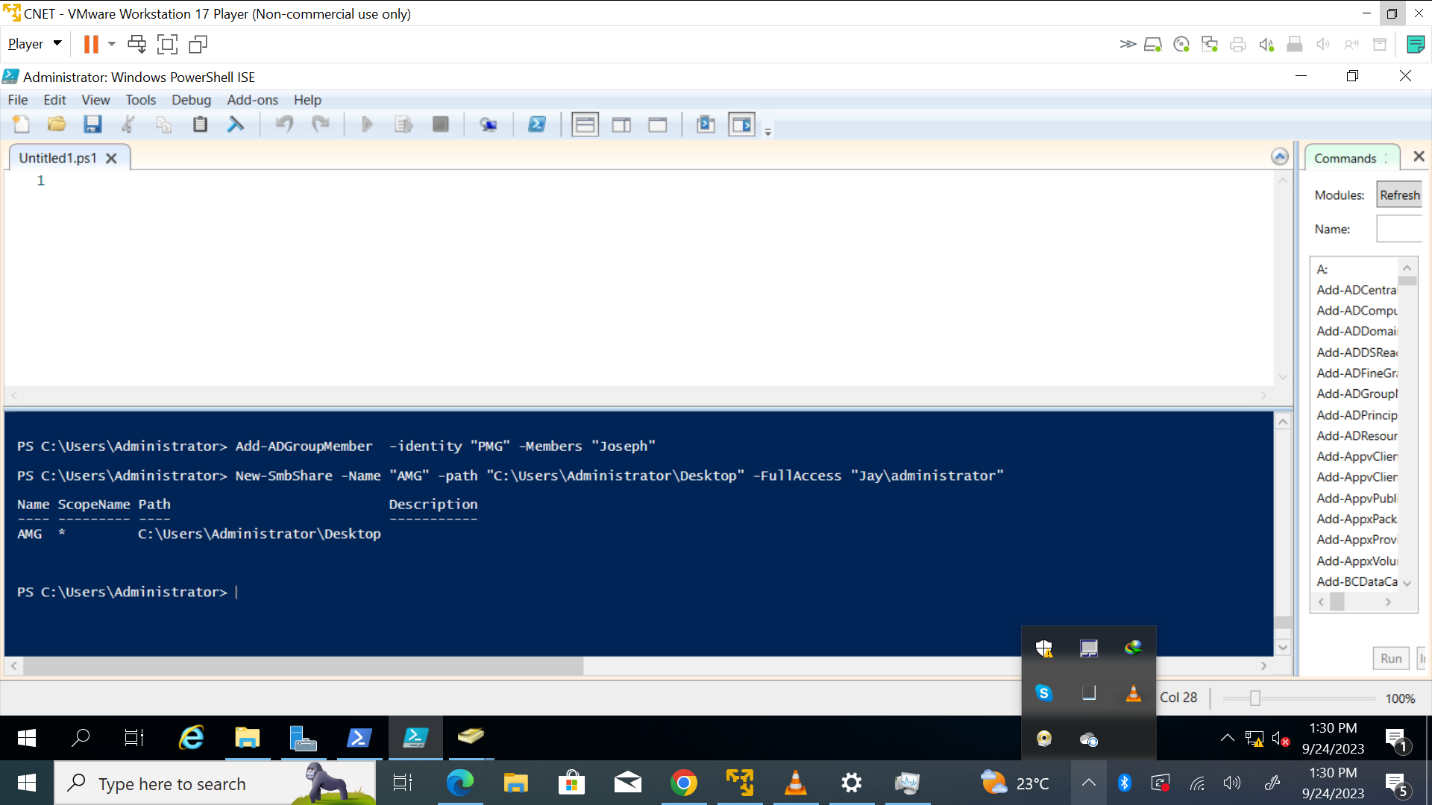
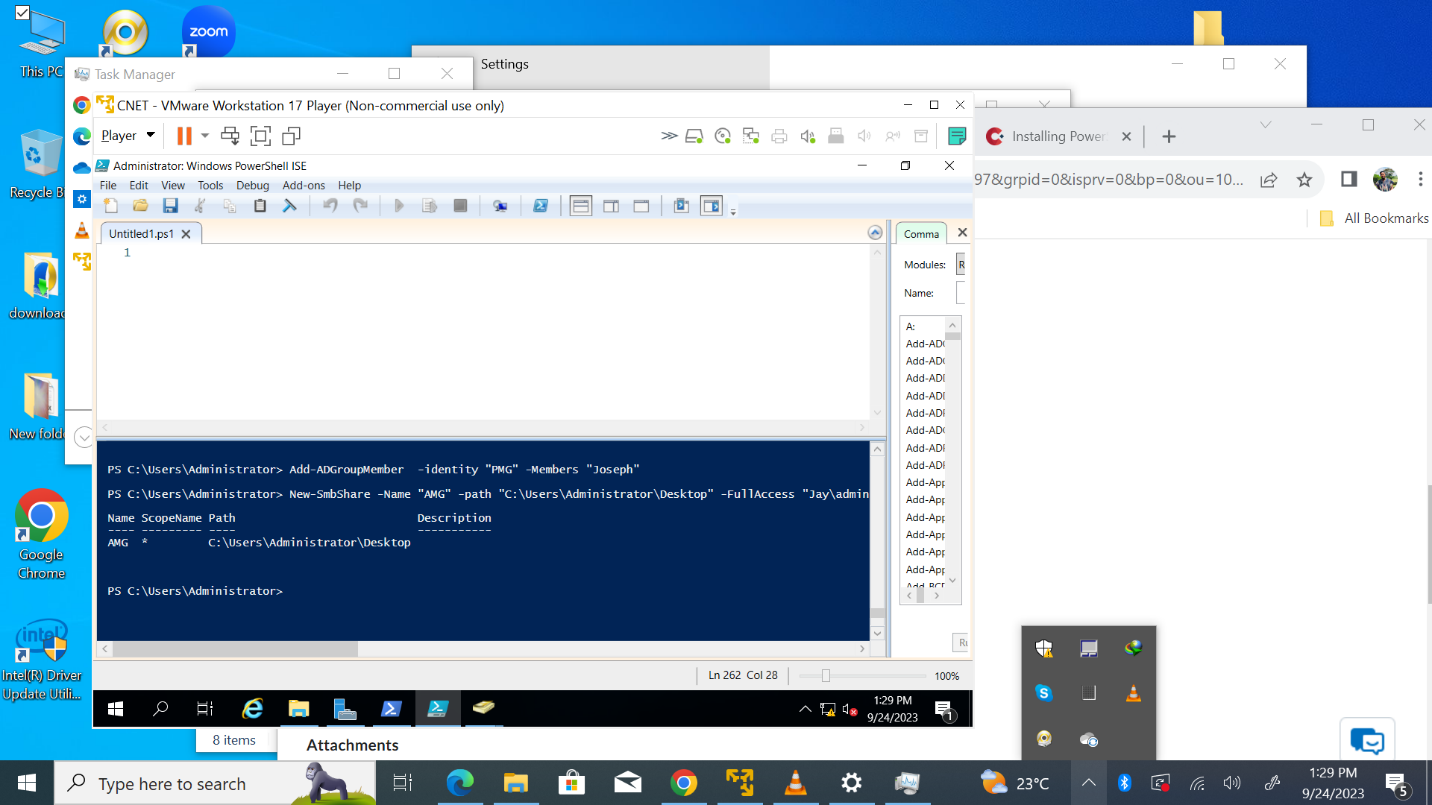
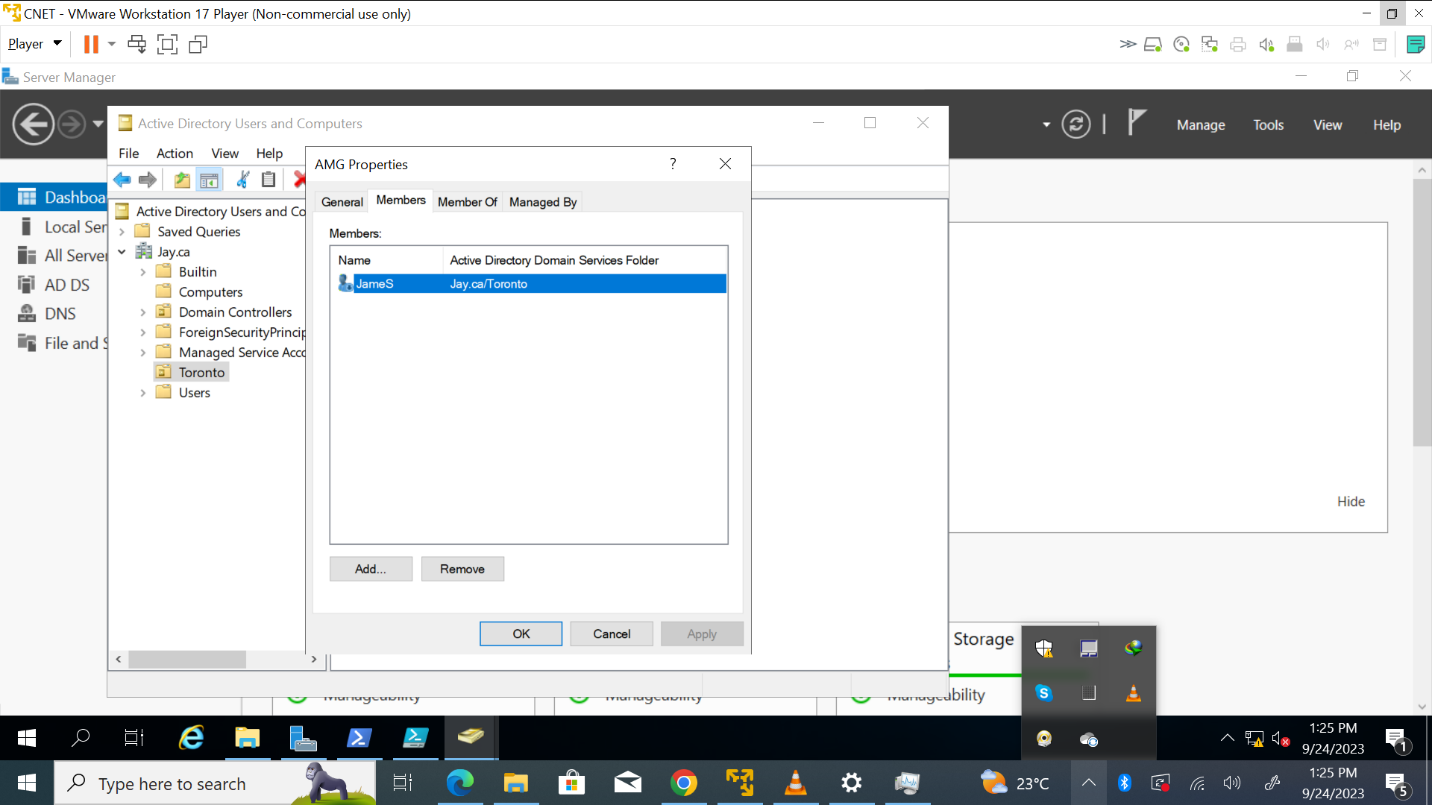
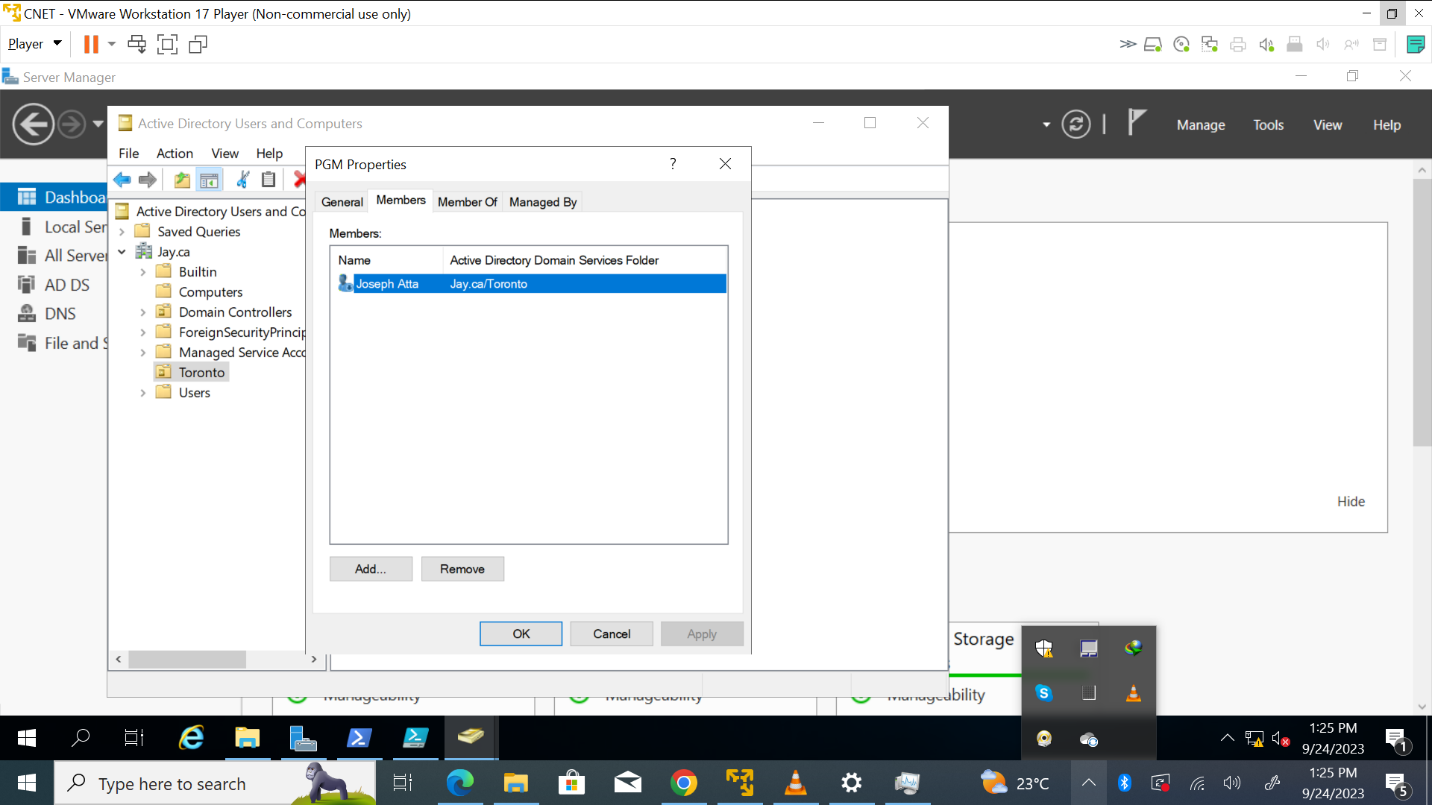
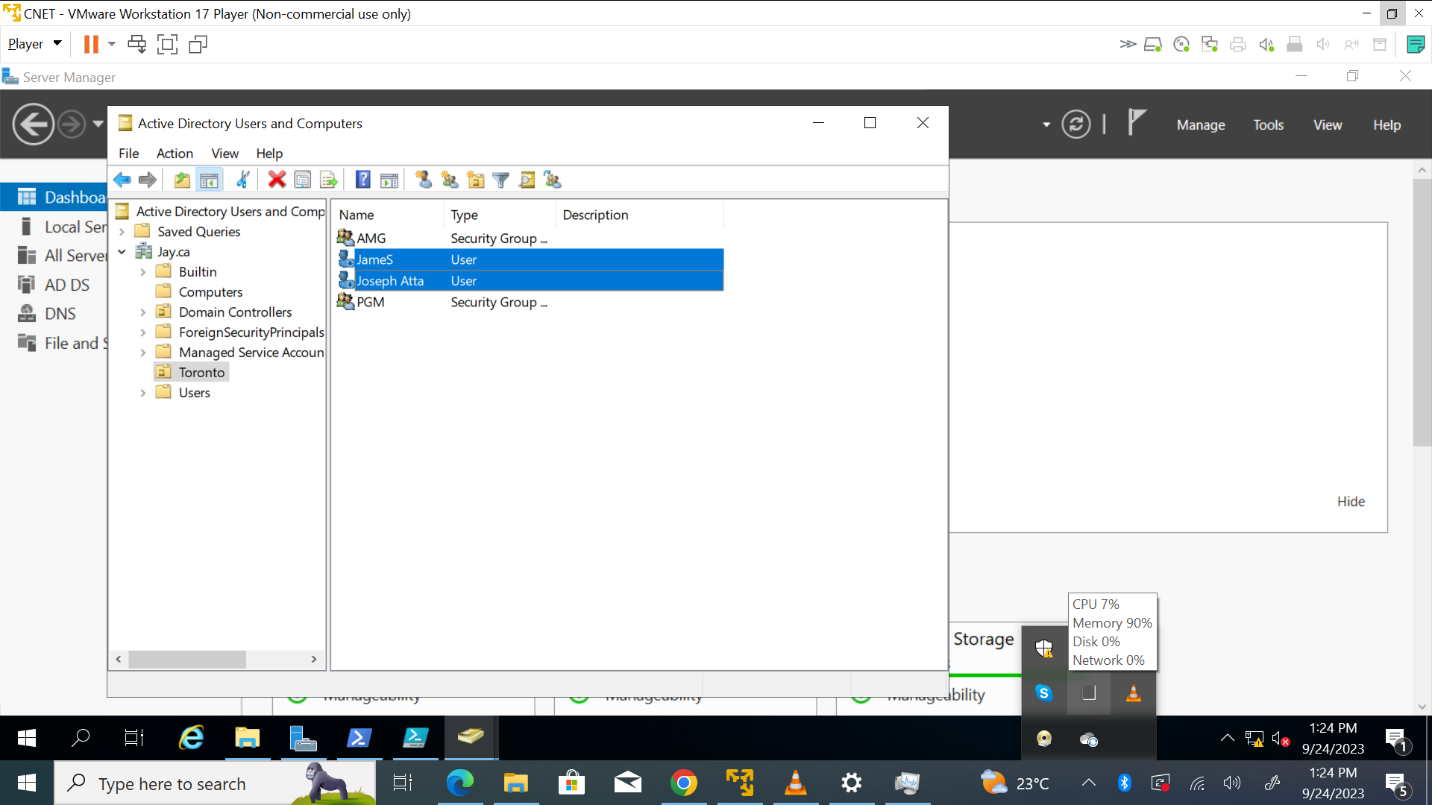
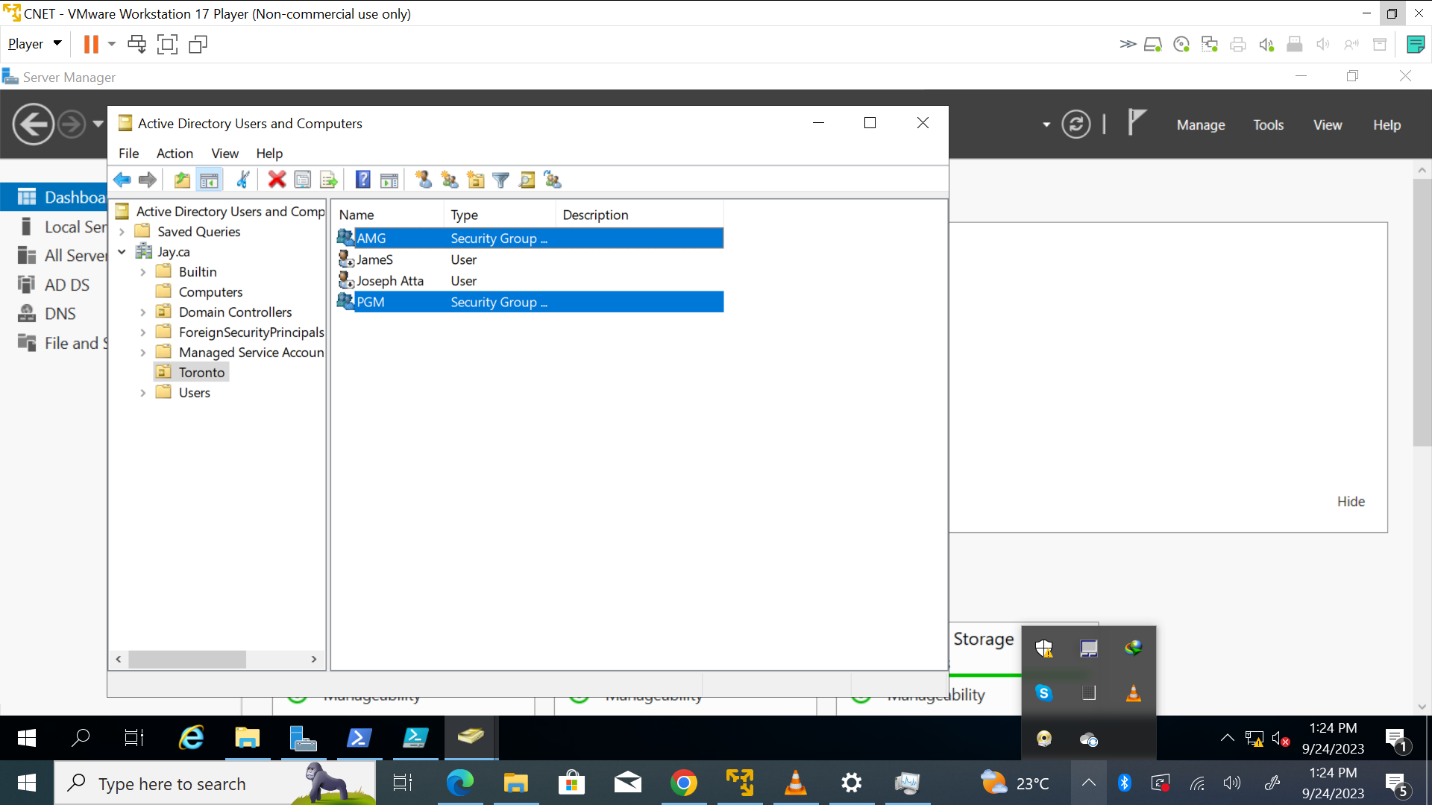
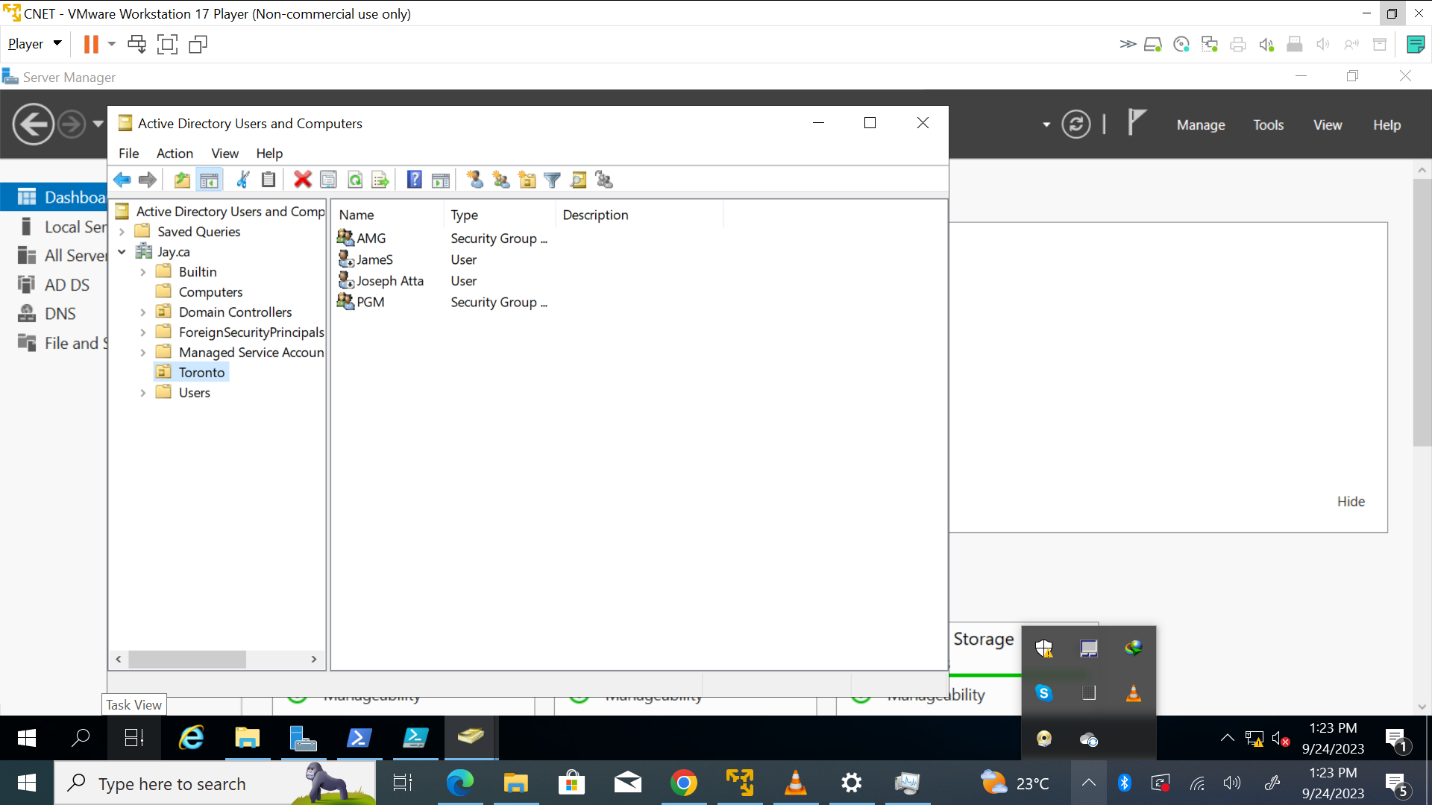
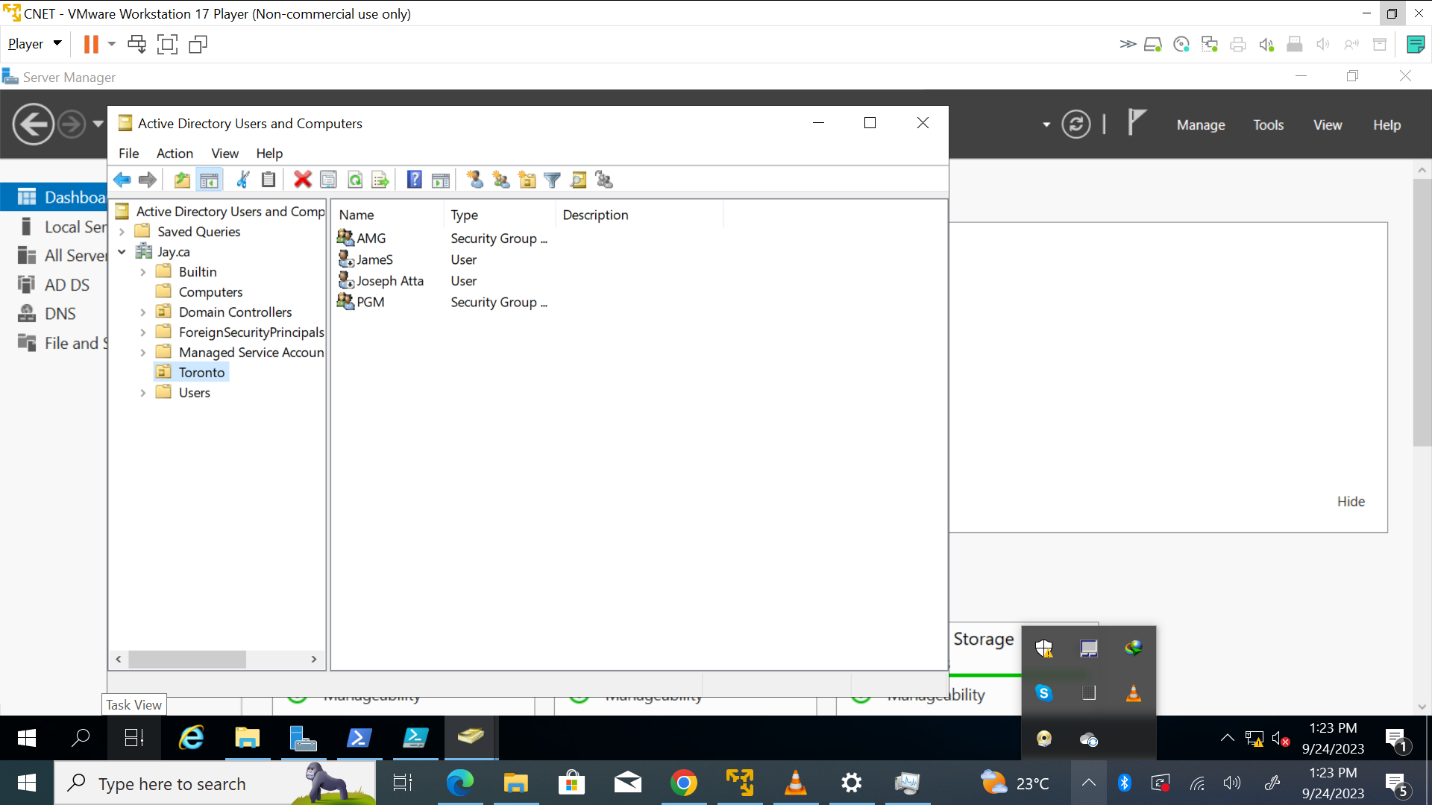
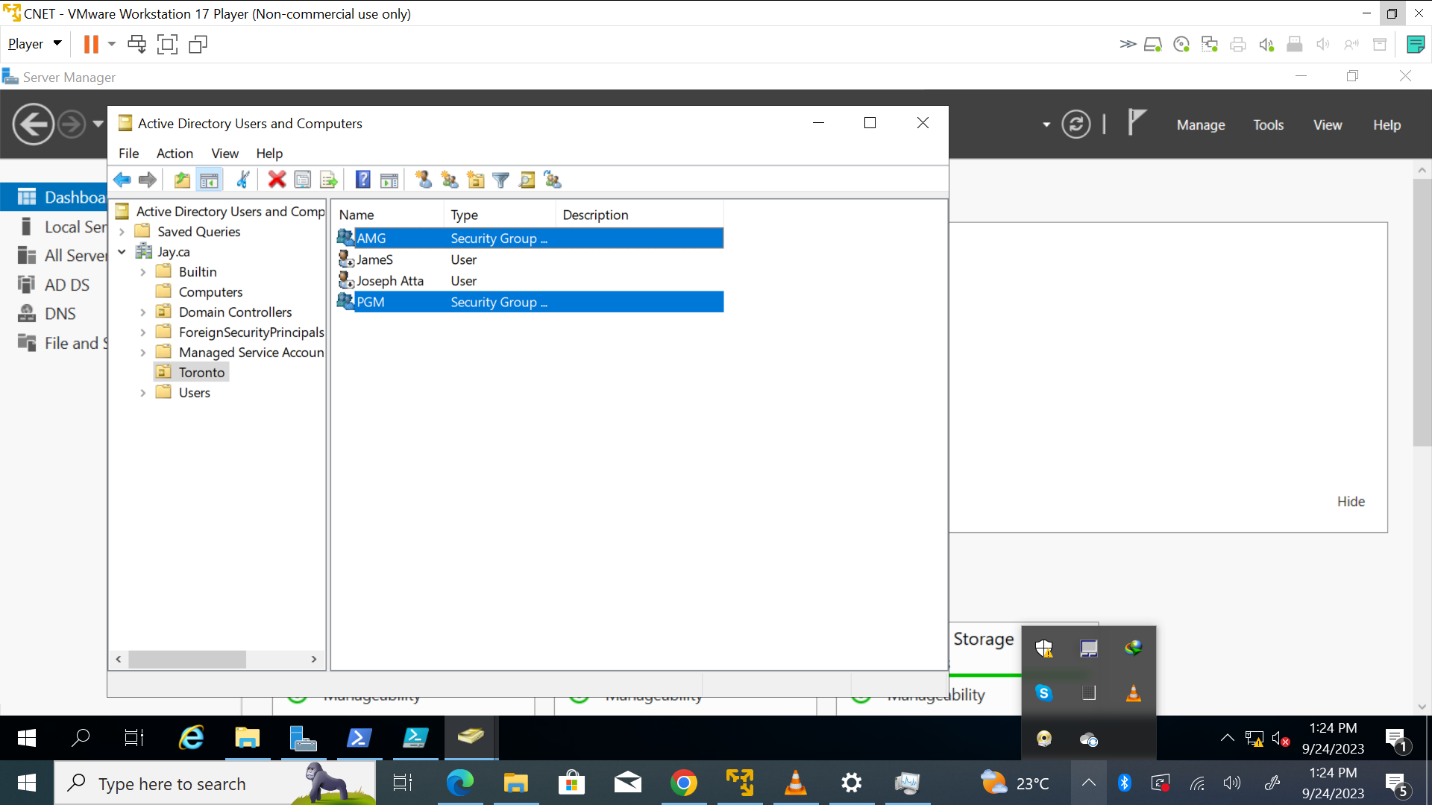
**23F---SCRIPTING AND SYSTEM ADMIN**

**LAB 2**

****

**THEORY**

**Principle of least privilege**

This principle states that no one user is granted the ultimate permission in performing their roles. Therefore, by minimizing and limiting the harm and danger that can be done to a system either by an inside person or a compromiser. Under this principle a user, application, entities and devices must be granted the access it requires before it can function or perform its task. For example, most employees do not need administrative access to their own computers to fulfill their roles, so this principle states that they should not have it. Similarly, finance personnel do not need access to HR records or IT systems, so they should not be granted it. Also, an IT administrator may require privileged access to perform some of their job duties. However, they should use a non-privileged account for day-to-day tasks and only use their privileged account when it is necessary for a given task.

**Privilege Creep**

When users or people accumulate or amass rights and permissions for a long period of time so as to grant them access to a particular system or information that is sensitive. Privilege creep is a severe administrative oversight. As people amass unnecessary data access rights, organizations become increasingly exposed to threats. This can lead to unauthorized data access, employee data theft, compliance breaches, and insider threats. The issue is especially prevalent in dynamic, fast-growing organizations with high employee turnover rates or complex technological environments. Privilege creep is a ticking bomb in information security, posing a significant threat to data confidentiality and trust.

**Server Message Block**

**This is a network protocol that allows files to be shared and accessed by multiple computers in diverse locations over a network.** Server Message Block (SMB) enables file sharing, printer sharing, network browsing, and inter-process communication (through named pipes) over a computer network. SMB serves as the basis for Microsoft's Distributed File System implementation. SMB relies on the TCP and IP protocols for transport.Most usage of SMB involves computers running Microsoft Windows, which was called Microsoft Windows Network before the introduction of Active Directory. The corresponding Windows services are the LAN Manager server for server components and the LAN Manager workstation for client components.