**What is Active Directory and how does it work?**

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources.

Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer. Objects are normally defined as either resources, such as printers or computers, or security principals, such as users or groups.

Active Directory categorizes directory objects by name and attributes.

The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain.

AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource, as well as group policies.

The server that hosts AD DS is the **domain controller.**

### Active Directory services

* **Lightweight Directory Services** has the same codebase as AD DS, sharing similar functionalities, such as the application program interface. AD LDS, however, can run in multiple instances on one server and holds directory data in a data store using Lightweight Directory Access Protocol.
* **Lightweight Directory Access Protocol**is an application protocol used to access and maintain directory services over a network. LDAP stores objects, such as usernames and passwords, in directory services, such as Active Directory, and shares that object data across the network.
* **Certificate Services** generates, manages and shares certificates. A certificate uses encryption to enable a user to exchange information over the internet securely with a public key.
* **Active Directory Federation Services** authenticates user access to multiple applications -- even on different networks -- using single sign-on. As the name indicates, SSO only requires the user to sign on once, rather than use multiple dedicated authentication keys for each service.
* **Rights Management Services** control information rights and management. AD RMS encrypts content, such as email or Microsoft Word documents, on a server to limit access

Active Directory Domain Services uses a tiered layout structure consisting of domains, trees and forests to coordinate networked elements.

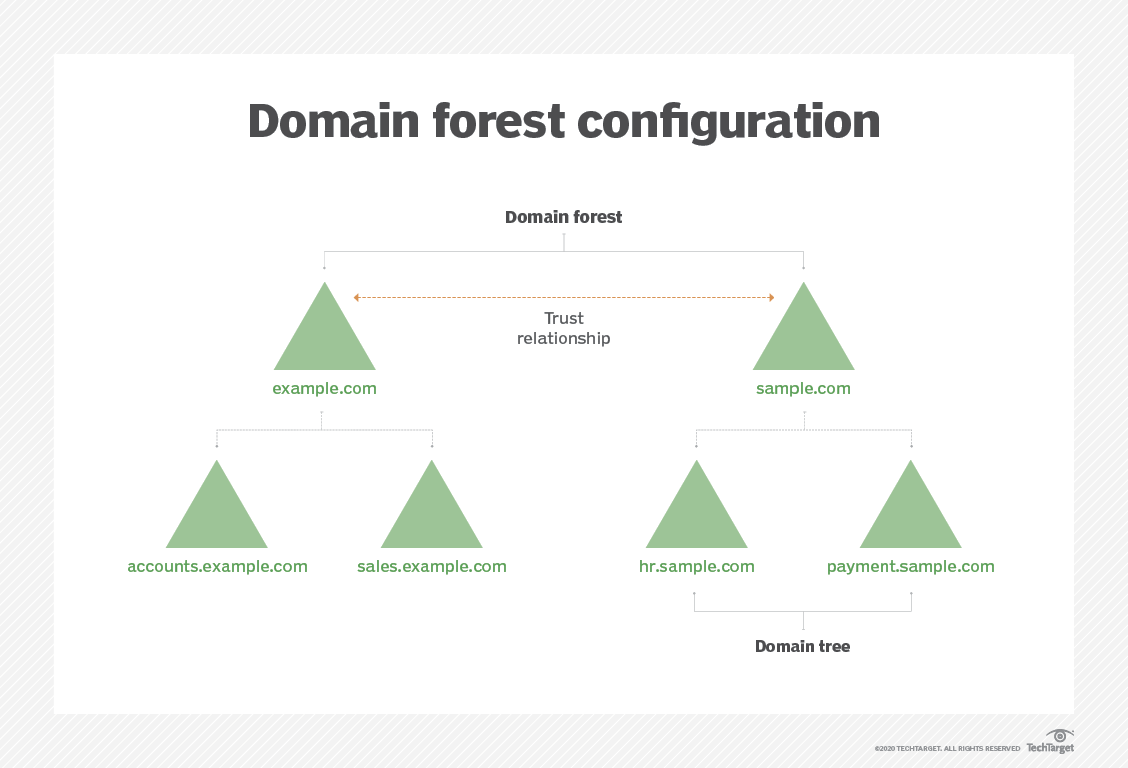
**Domains** are the smallest of the main tiers, while forests are the largest. Different objects, such as users and devices, that share the same AD database will be on the same domain. Domains have a domain name system

**A tree** is one or more domains grouped together with hierarchical trust relationships.The tree structure uses a contiguous namespace to gather the collection of domains in a logical hierarchy. Trees can be viewed as trust relationships where a secure connection, or trust, is shared between two domains. Because of the hierarchical nature of this setup, the first domain can implicitly trust the third domain without needing explicit trust.

**A forest** is a group of multiple trees. A forest consists of shared catalogs, directory [schemas](https://searchsqlserver.techtarget.com/definition/schema), application information and domain configurations. The schema defines an object's class and attributes in a forest. In addition, global catalog servers provide a listing of all the objects in a forest. According to Microsoft, the forest is Active Directory's security boundary.

**Organizational Units**(OUs) organize users, groups and devices. Each domain can contain its own OU. However, OUs cannot have separate namespaces, as each user or object in a domain must be unique. For example, a user account with the same username cannot be created.

**Containers**are similar to OUs, but Group Policy Objects cannot be applied or linked to container objects.



### Trusting terminology

Active Directory relies on trusts to moderate the access rights of resources between domains. There are several different types of trusts:

* A **one-way trust** is when a first domain allows access privileges to users on a second domain. However, the second domain does not allow access to users on the first domain.
* A **two-way trust** is when there are two domains and each domain enables access to users of the other domain.
* A **trusted domain**is a single domain that enables user access to another domain, which is called the **trusting domain**.
* A **transitive trust** can extend beyond two domains and allow access to other trusted domains within a forest.
* An **intransitive trust** is a one-way trust that is limited to two domains.
* An **explicit trust** is a one-way, nontransitive trust that is created by a network admin.
* A **cross-link trust** is a type of explicit trust. Cross-link trusts take place between domains within 1) the same tree, with no child-parent relationship between the two domains, or 2) different trees.
* A **forest trust** applies to domains within the entire forest and can be one-way, two-way or transitive.
* A **shortcut** joins two domains that belong to separate trees. Shortcuts can be one-way, two-way or transitive.
* A **realm** is a trust that is transitive, intransitive, one-way or two-way.
* An **external trust** is a trust that links domains [across separate forests](https://www.techtarget.com/searchwindowsserver/tip/How-to-create-a-cross-forest-trust-in-Active-Directory) or domains that are non-AD. External trusts can be nontransitive, one-way or two-way.

Group Policy is a feature of Windows that facilitates a wide variety of advanced settings that network administrators can use to control the working environment of users and computer accounts in Active Directory.

Group Policy is a feature of Windows that facilitates a wide variety of advanced settings that network administrators can use to control the working environment of users and computer accounts in Active Directory.

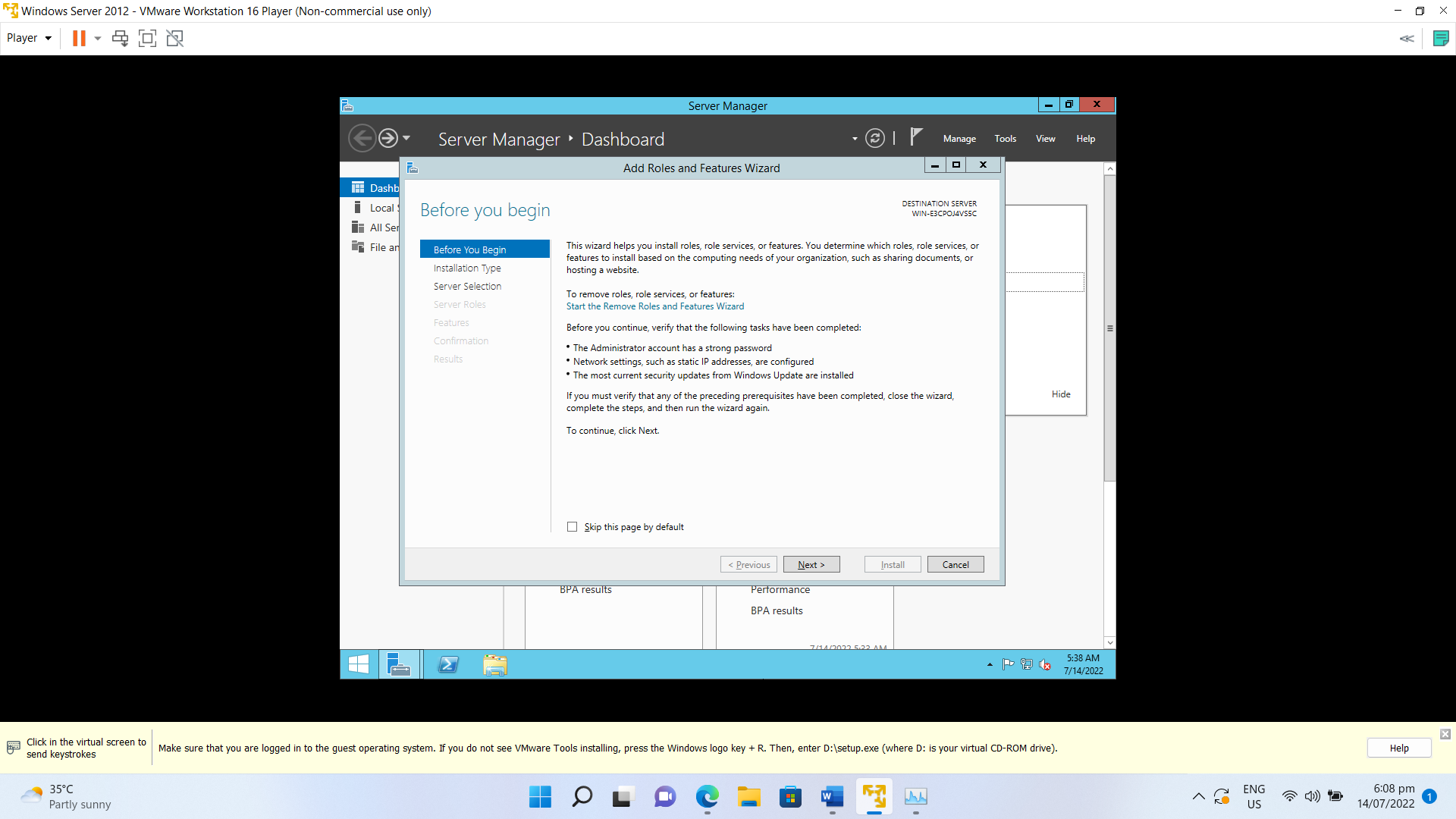
A Group Policy Object (GPO) is a group of settings that are created using the Microsoft Management Console (MMC) Group Policy Editor.

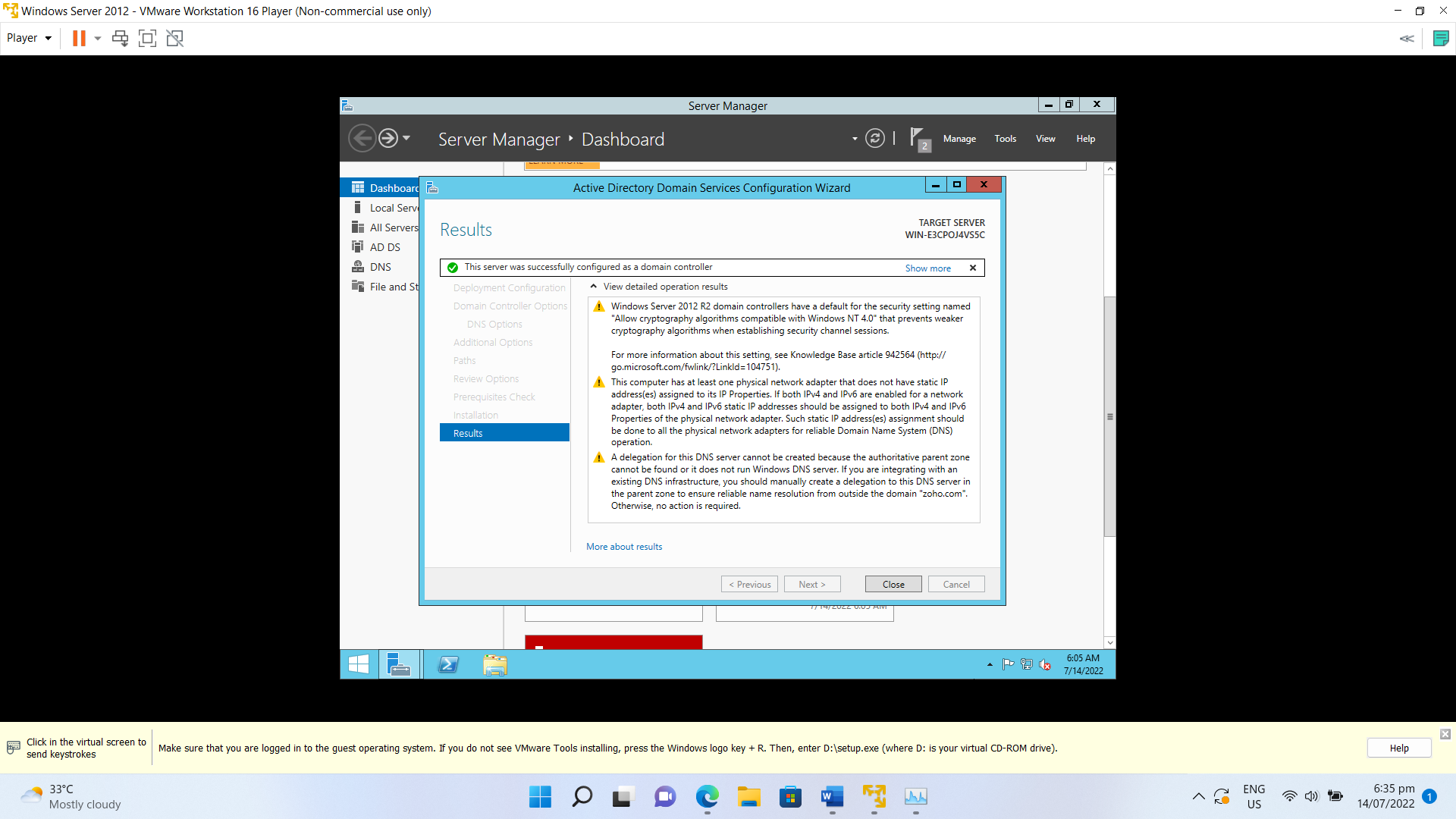
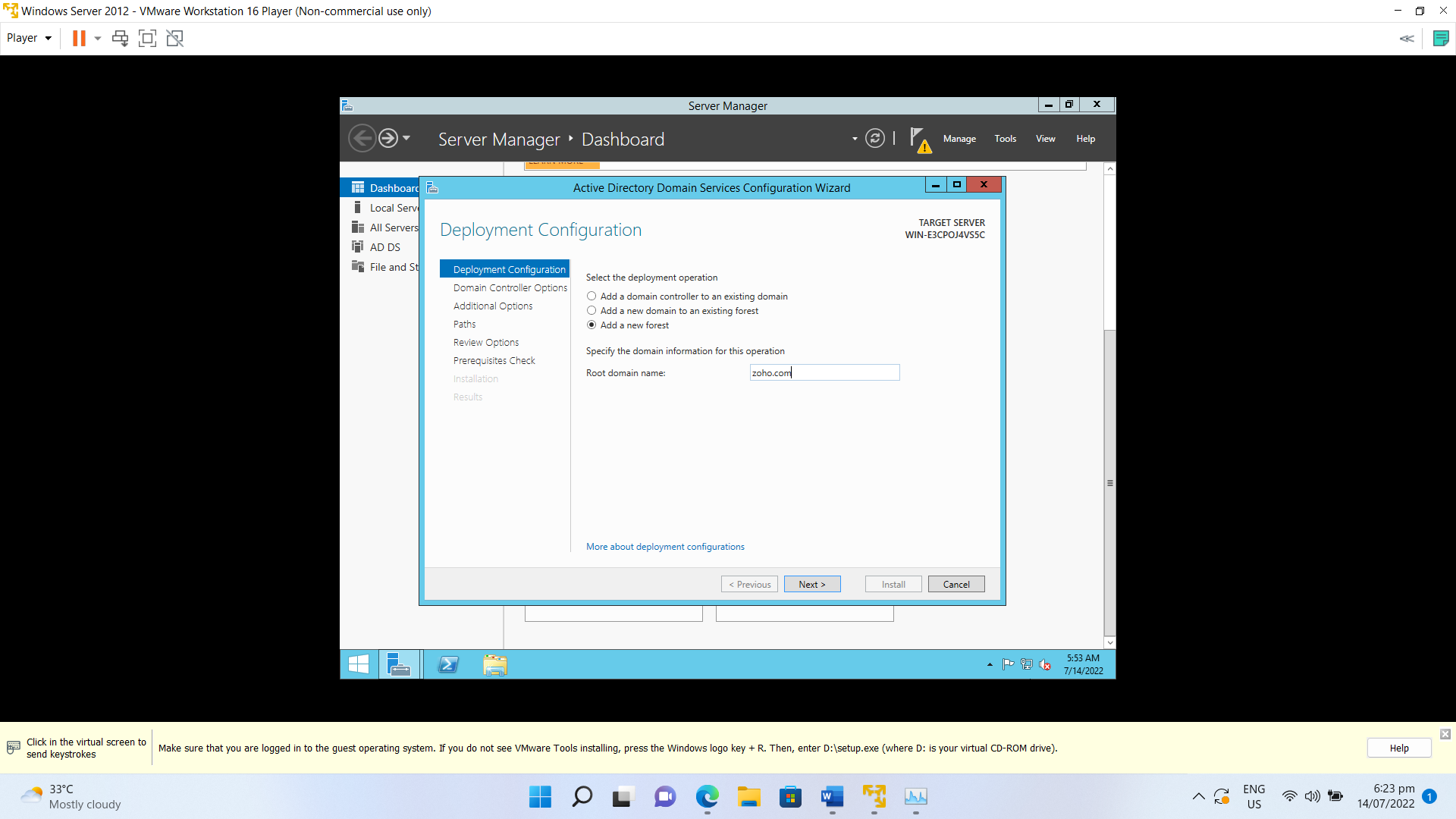
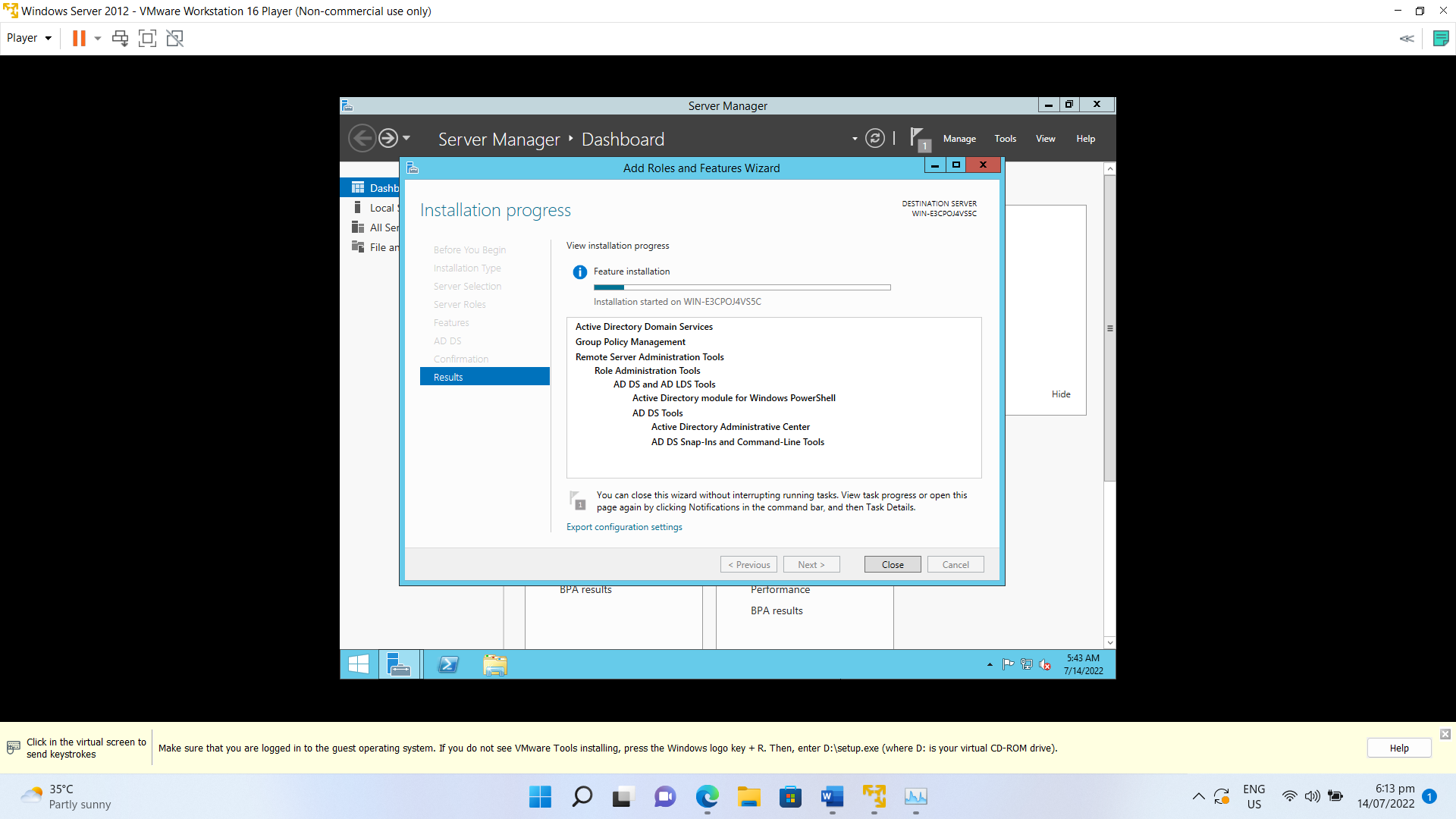
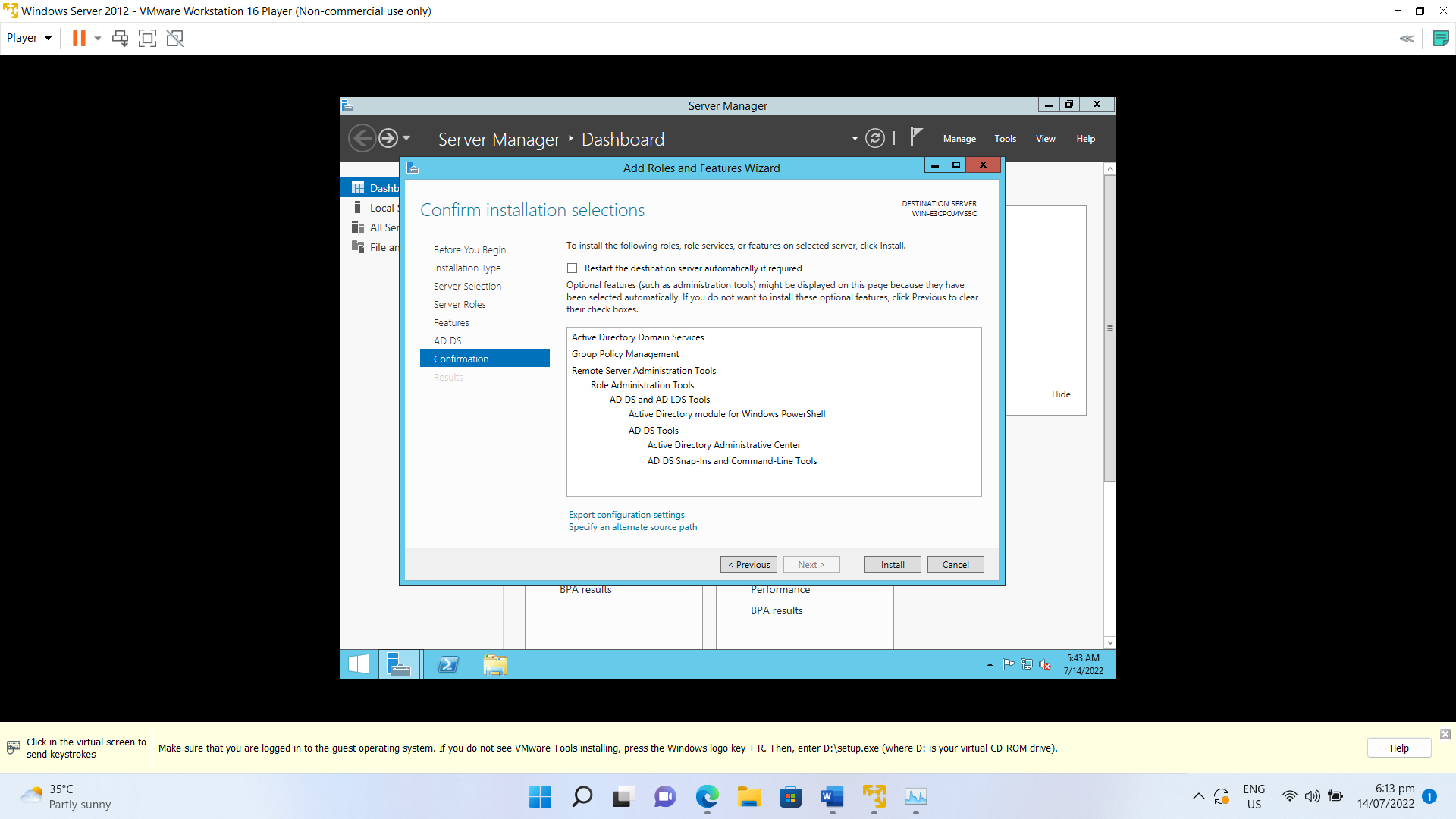
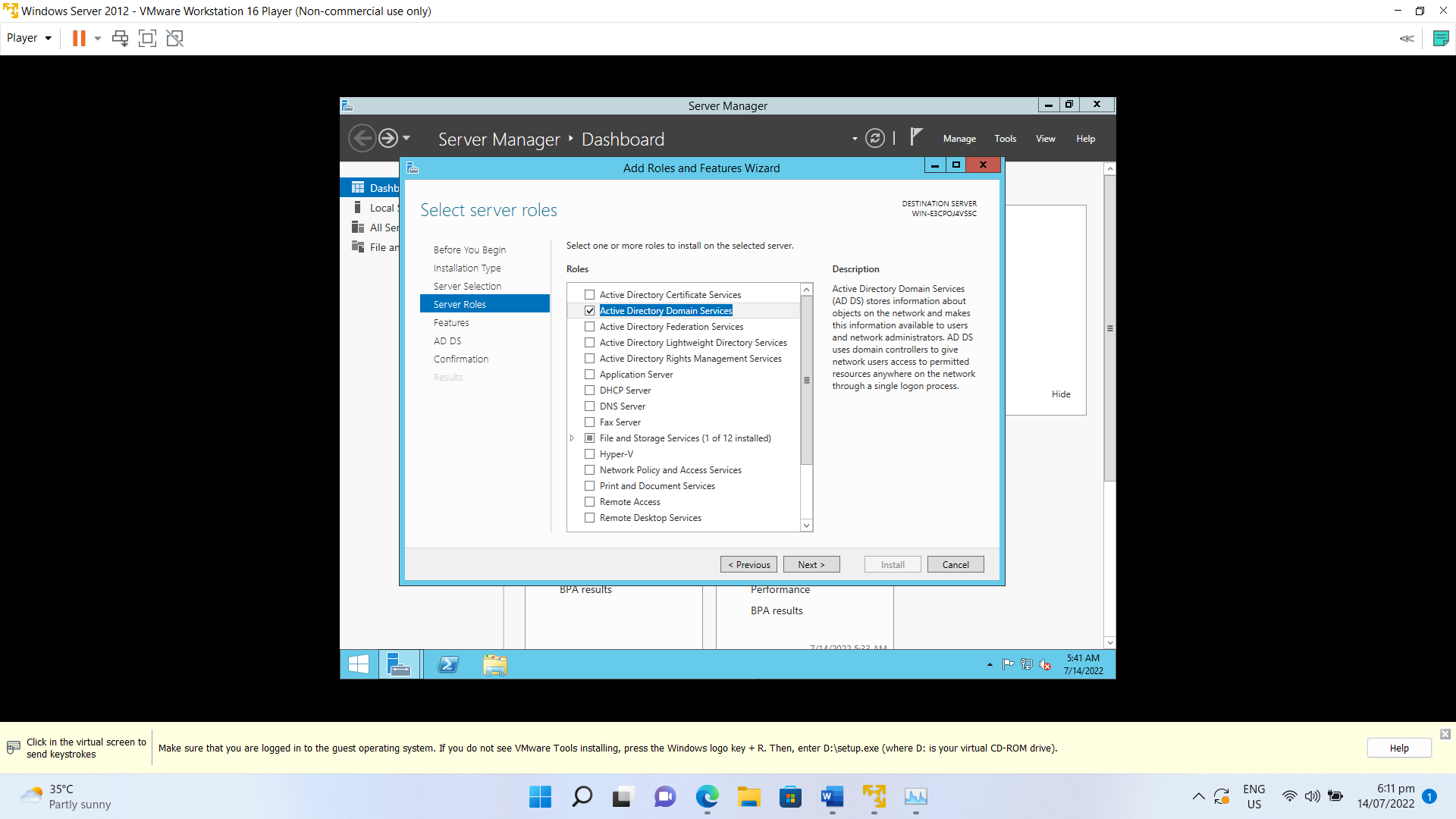
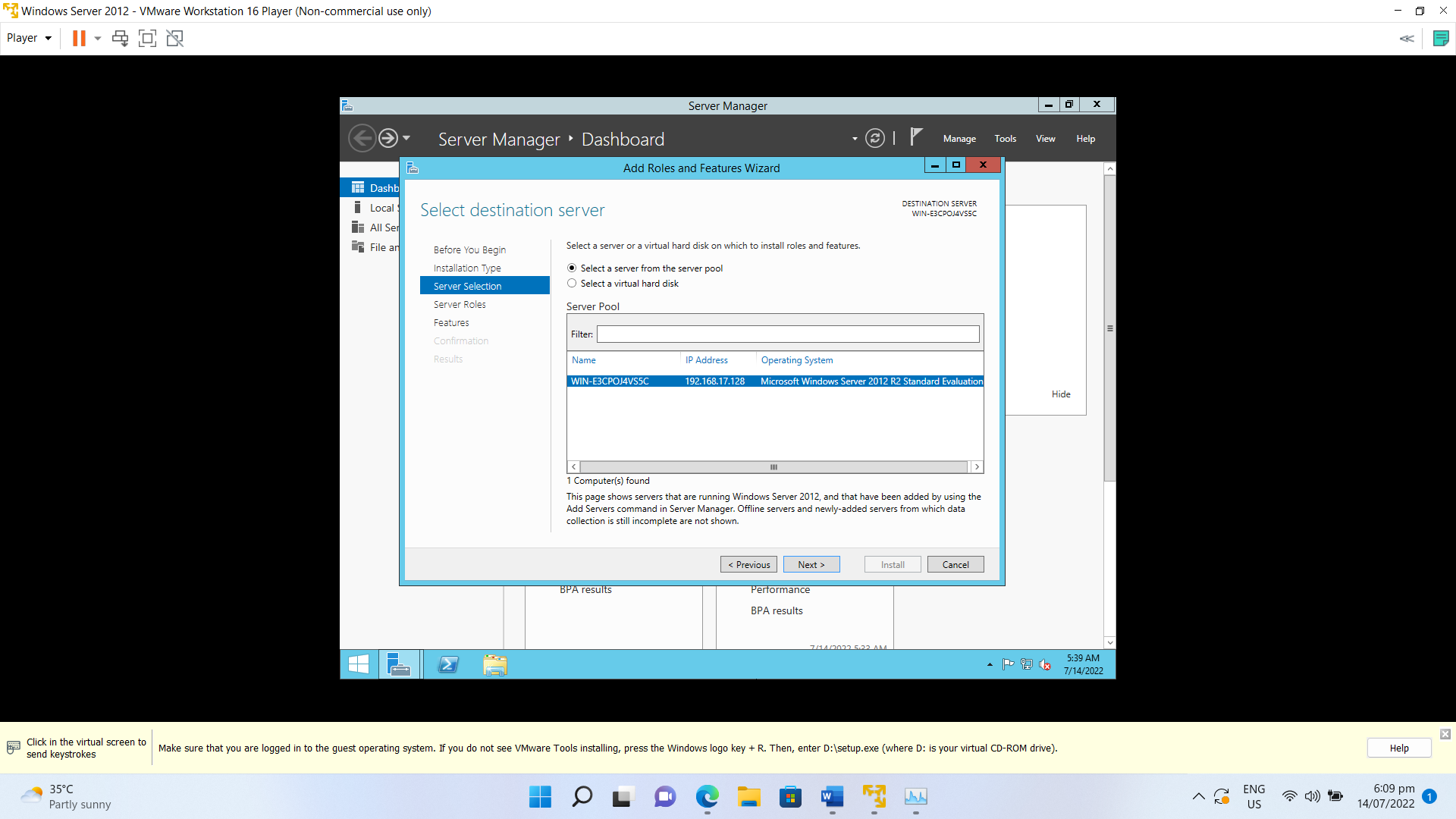
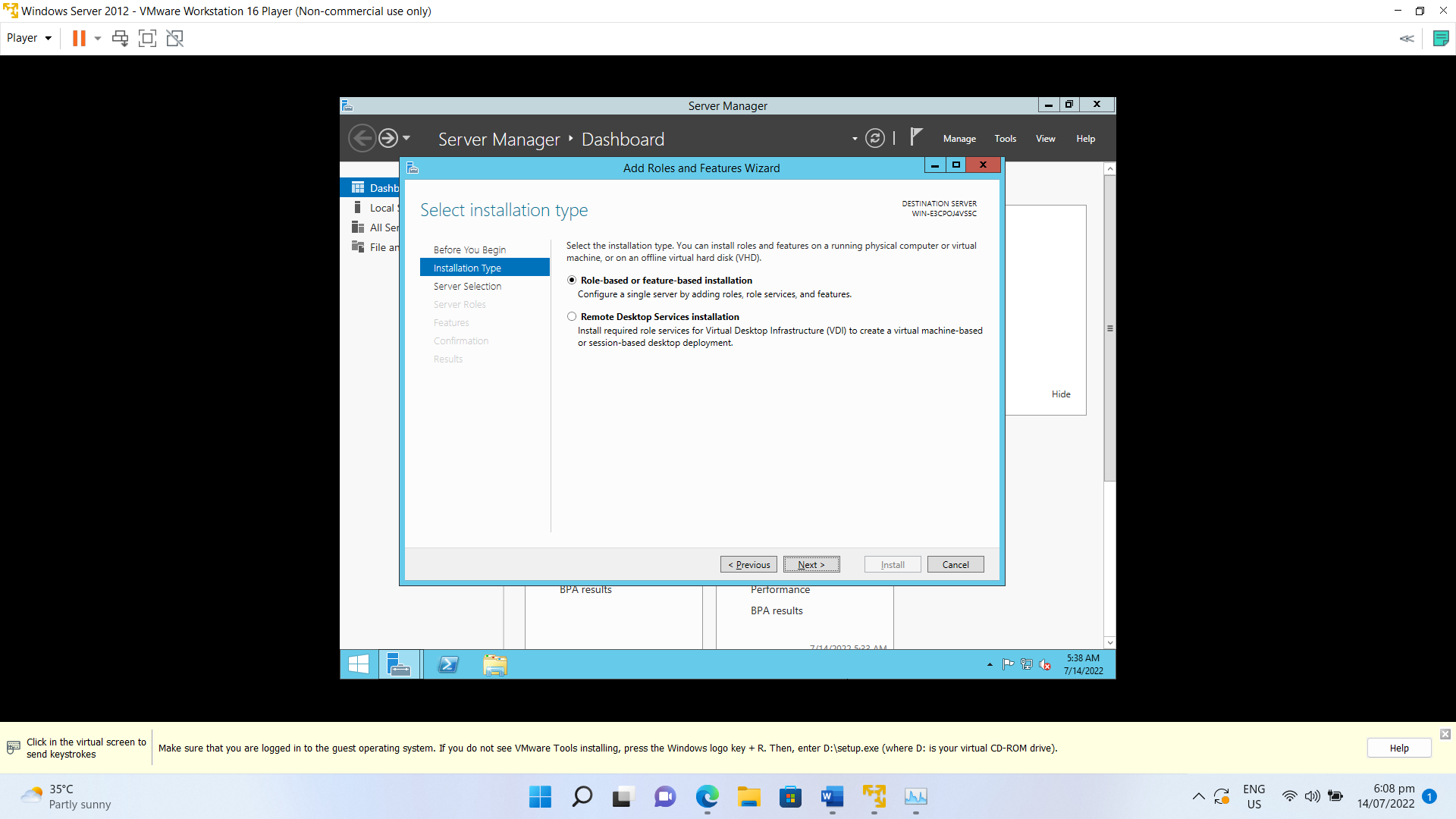
 The MMC allows users to create GPOs that define registry-based policies, security options, software installation and much more.

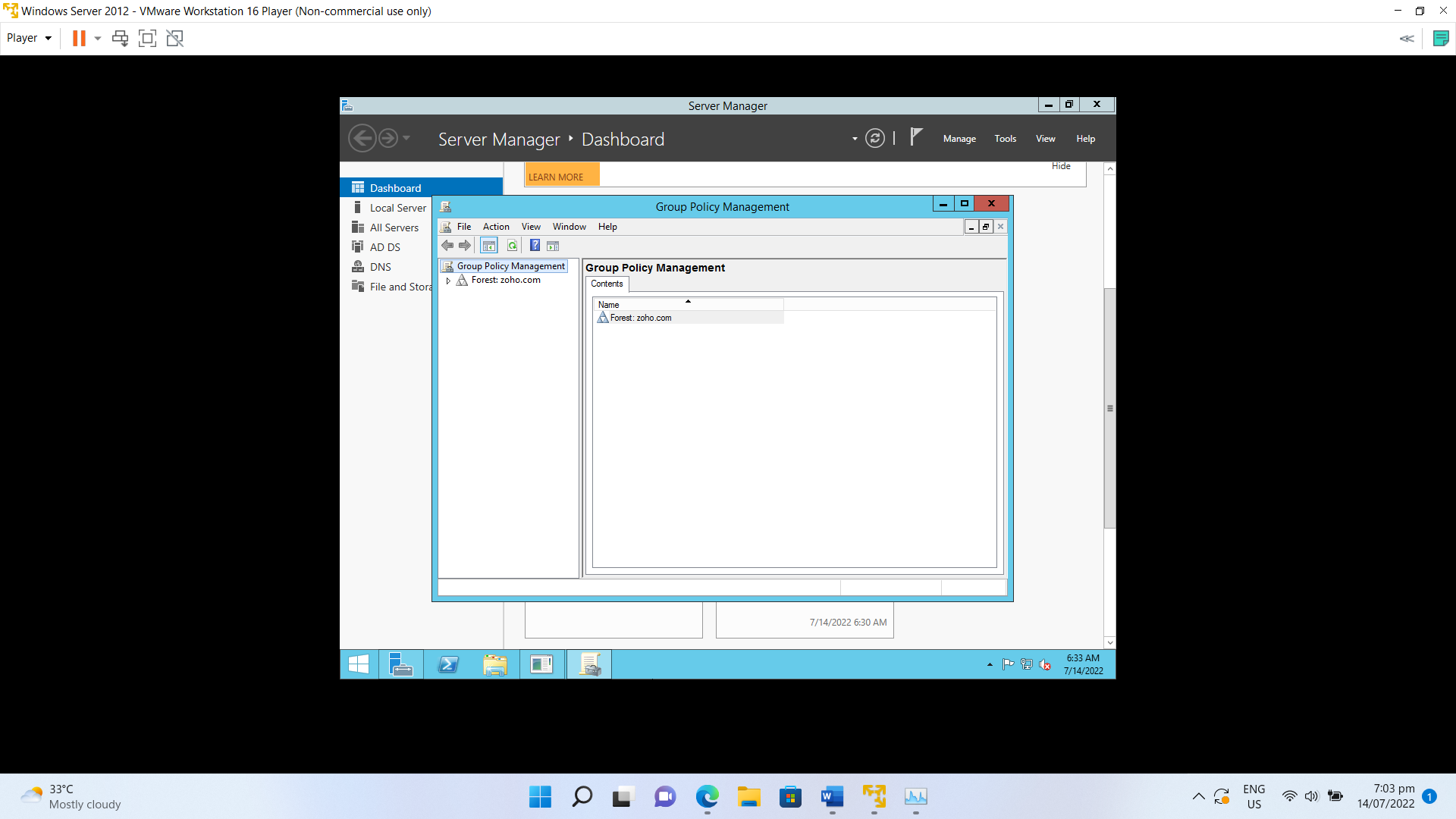
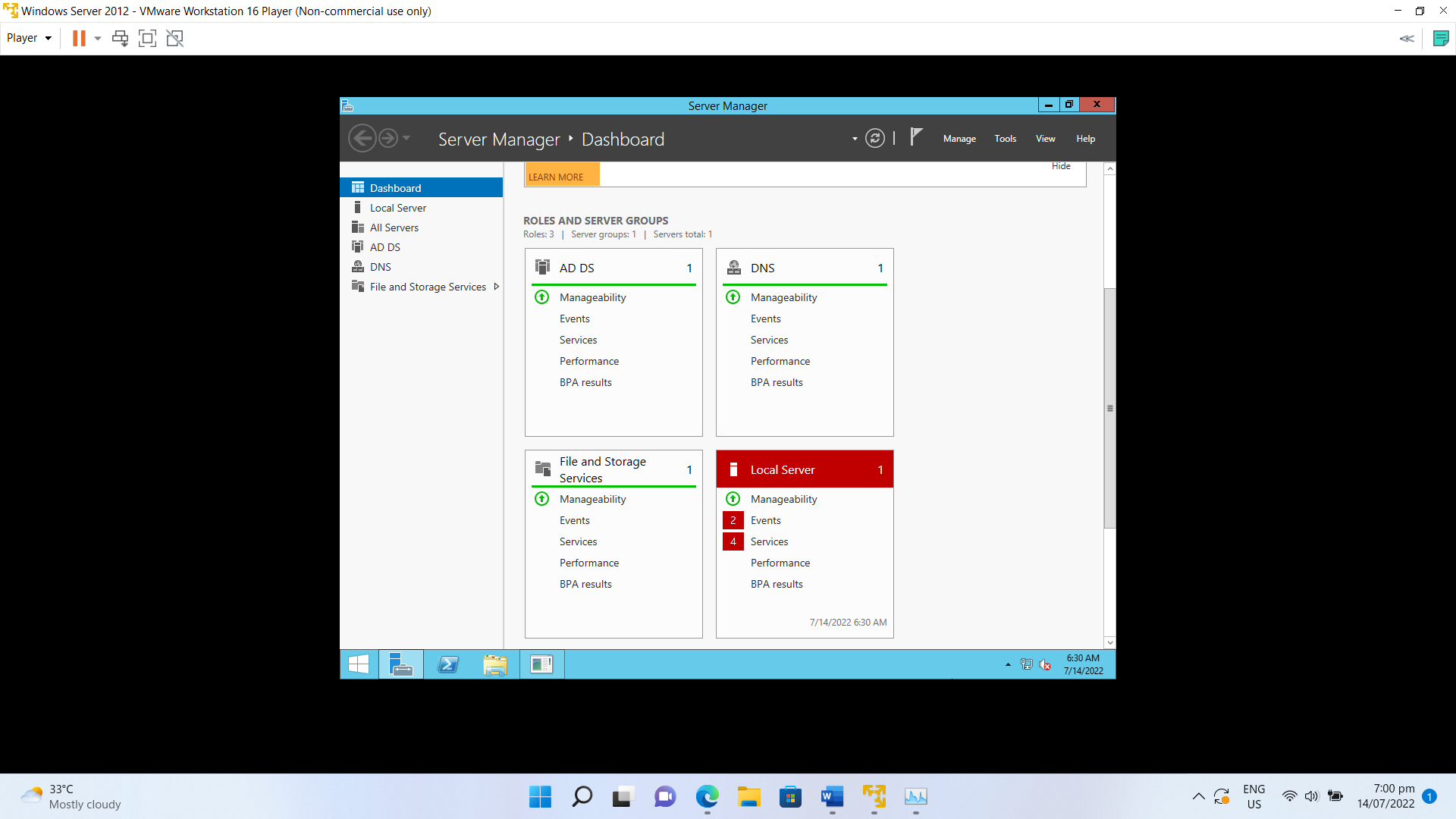
The order at which GPOs are processed affects what settings are applied to the computer and user. The order that GPOs are processed is known as LSDOU, which stands for local, site, domain, organizational unit.

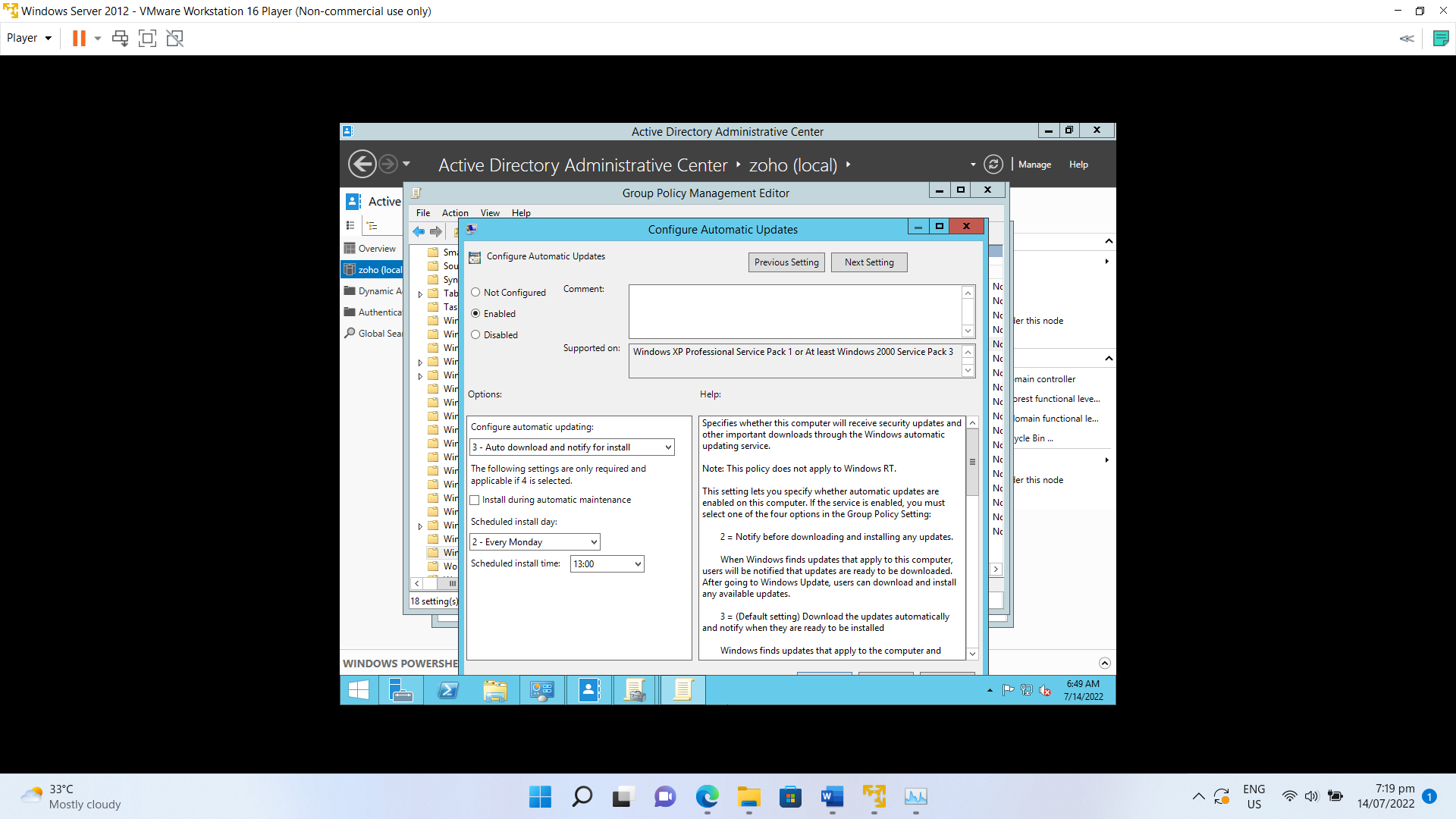
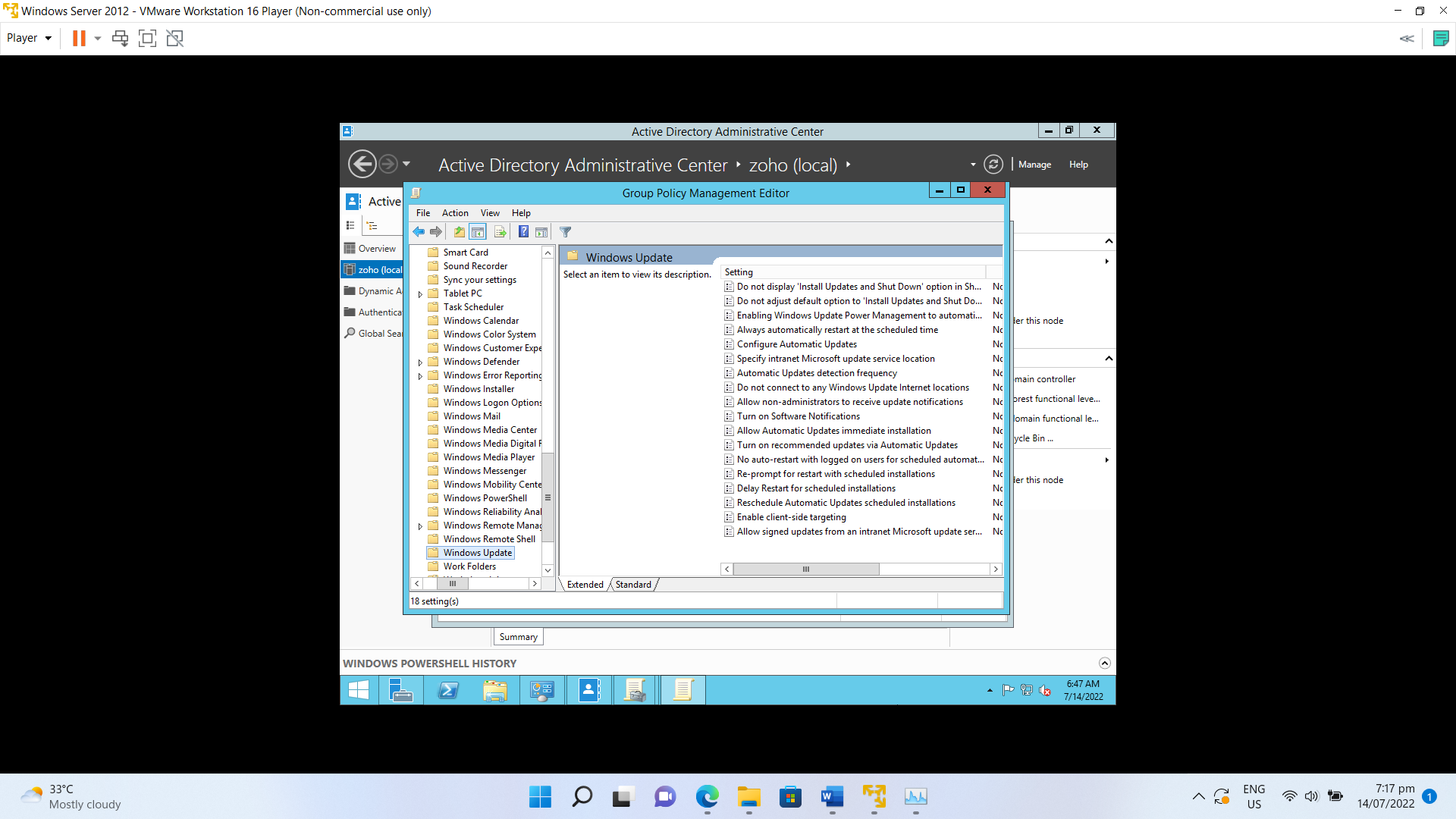
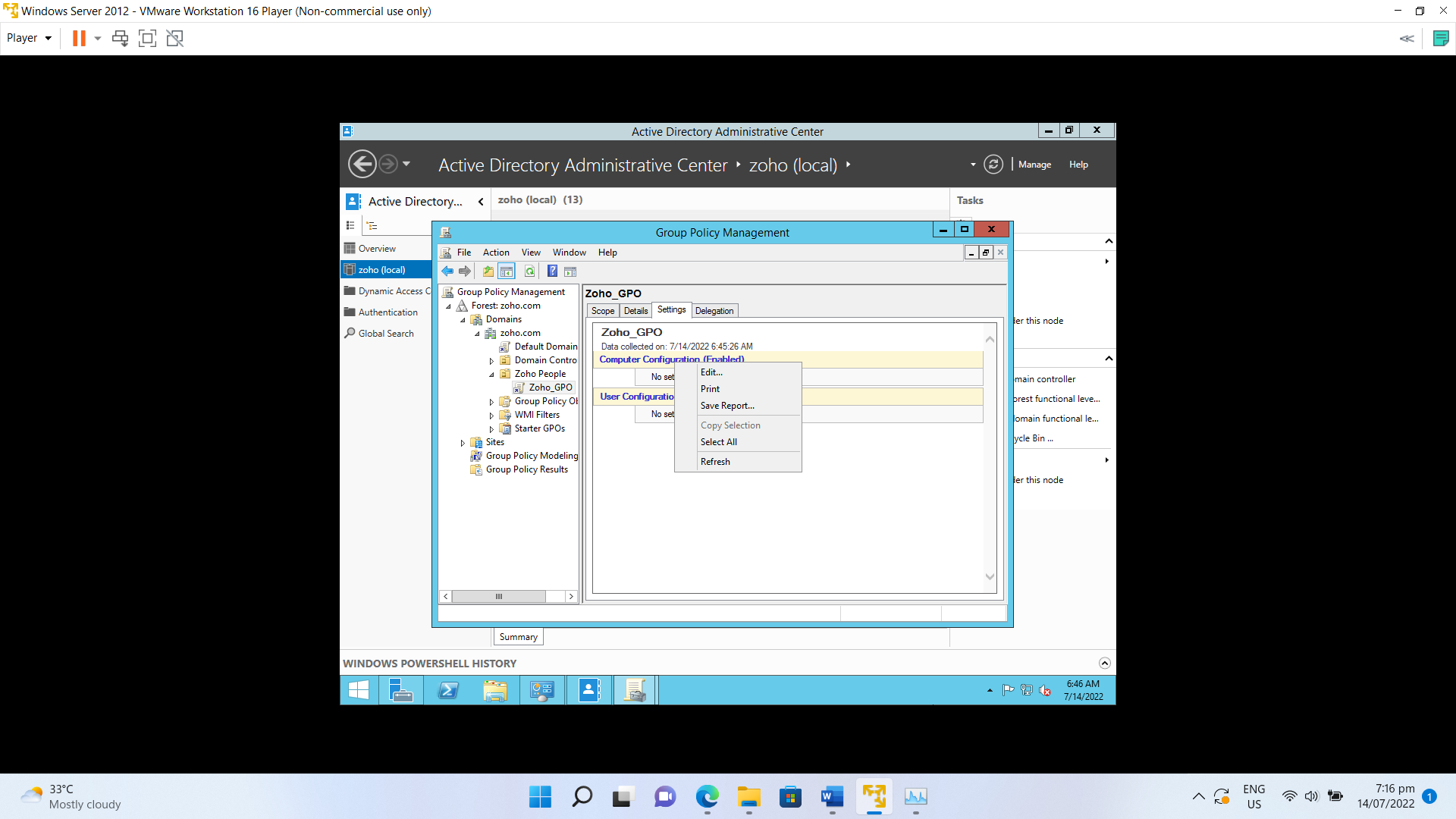
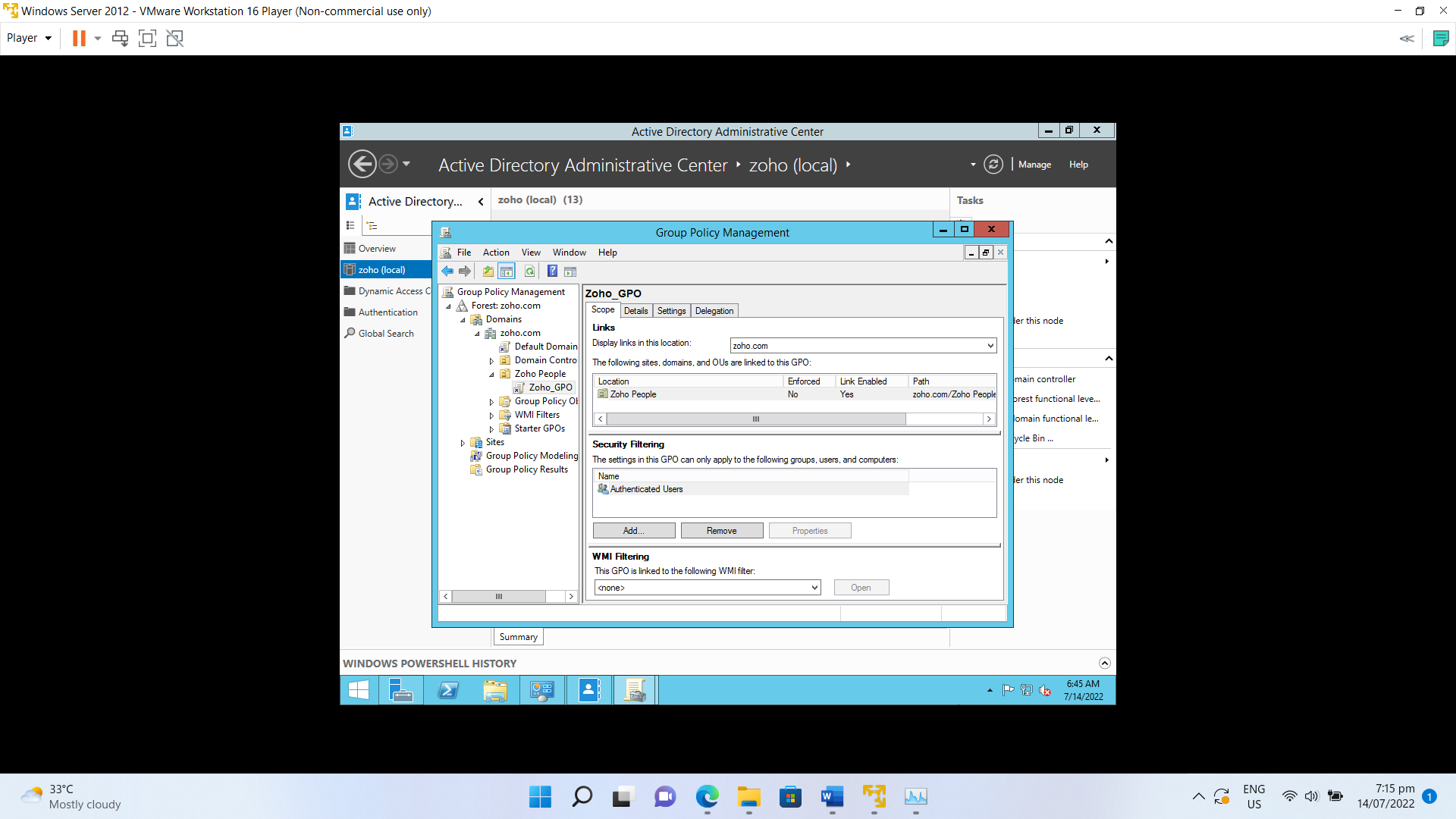
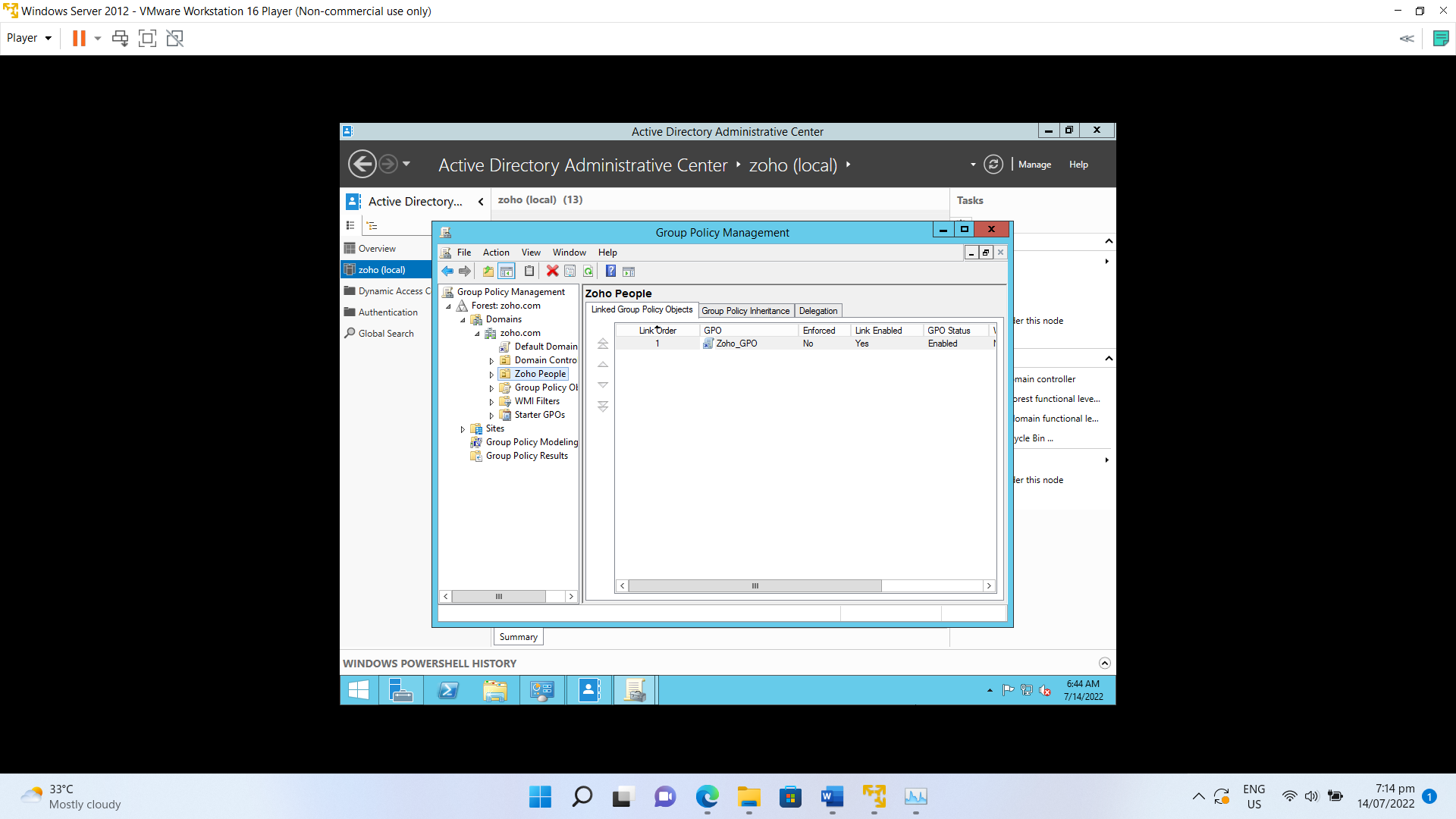
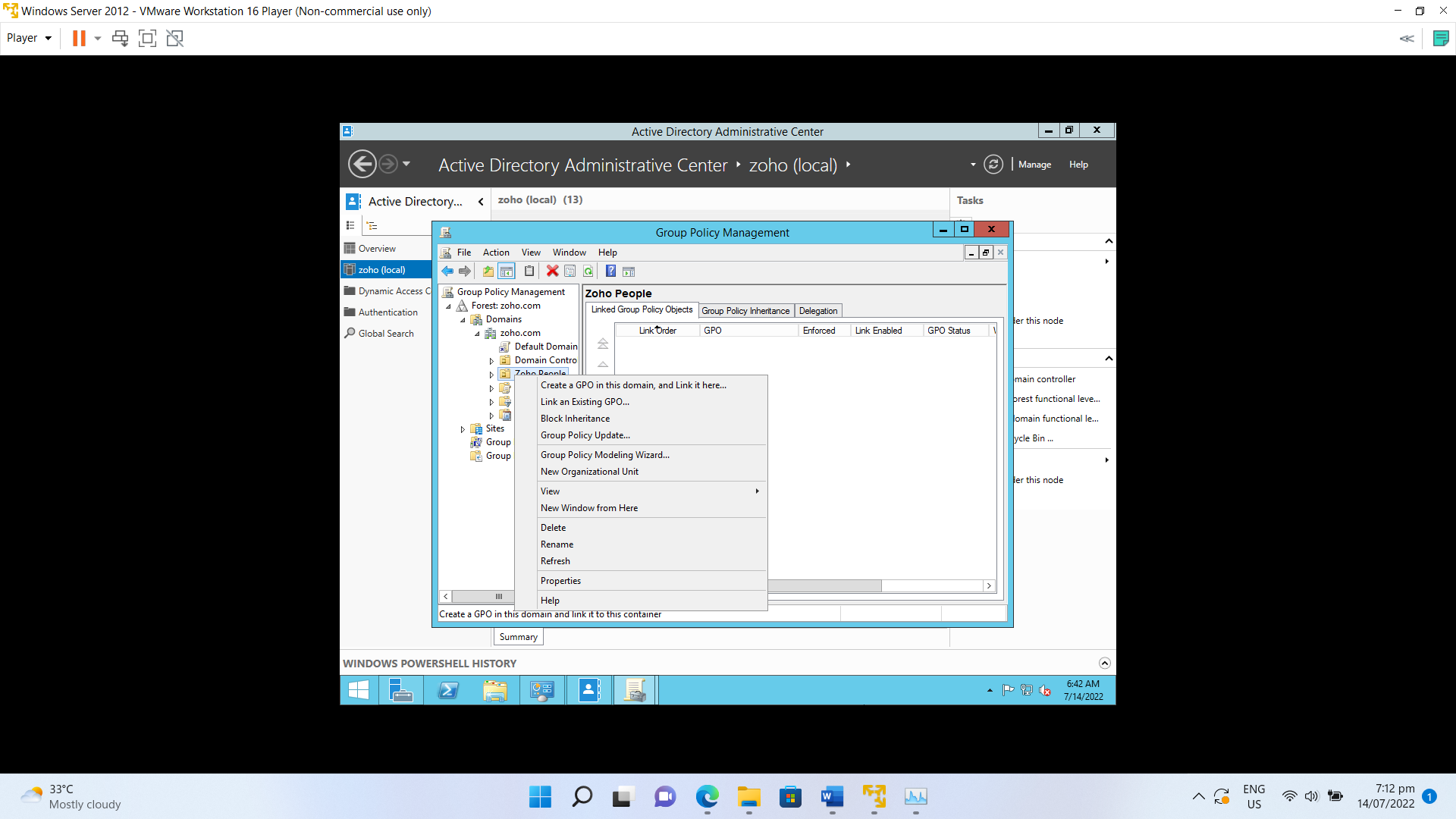
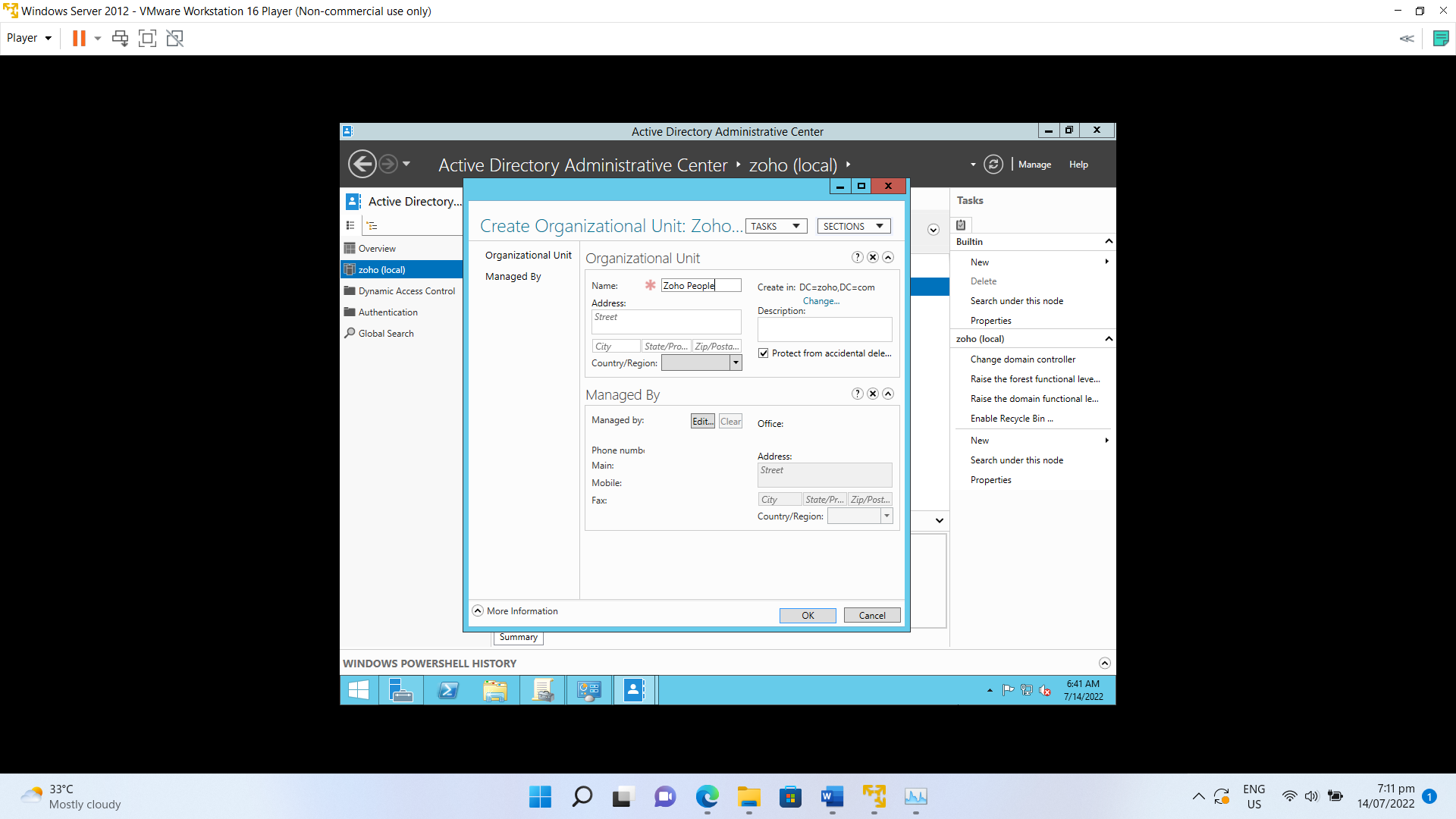
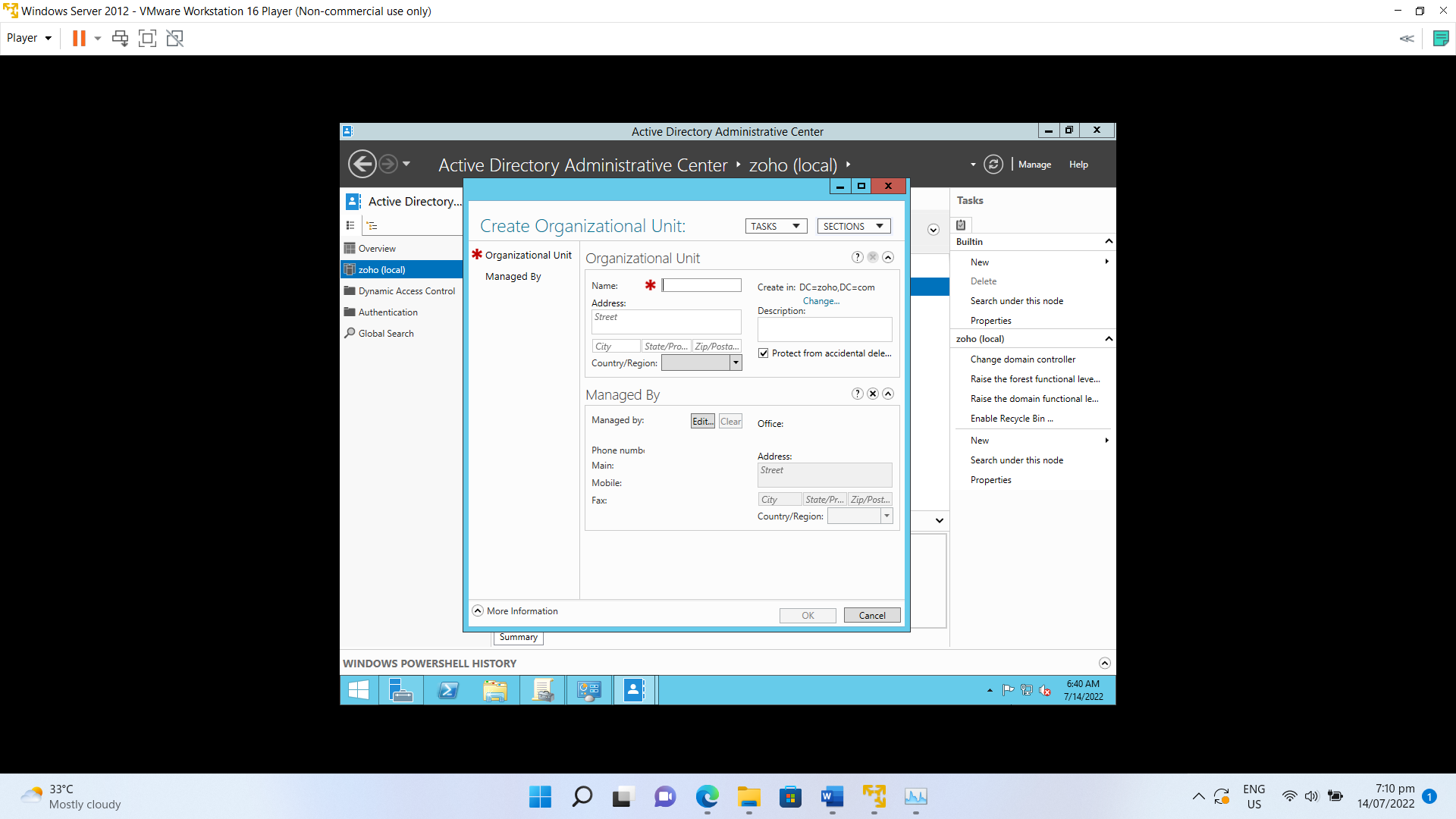
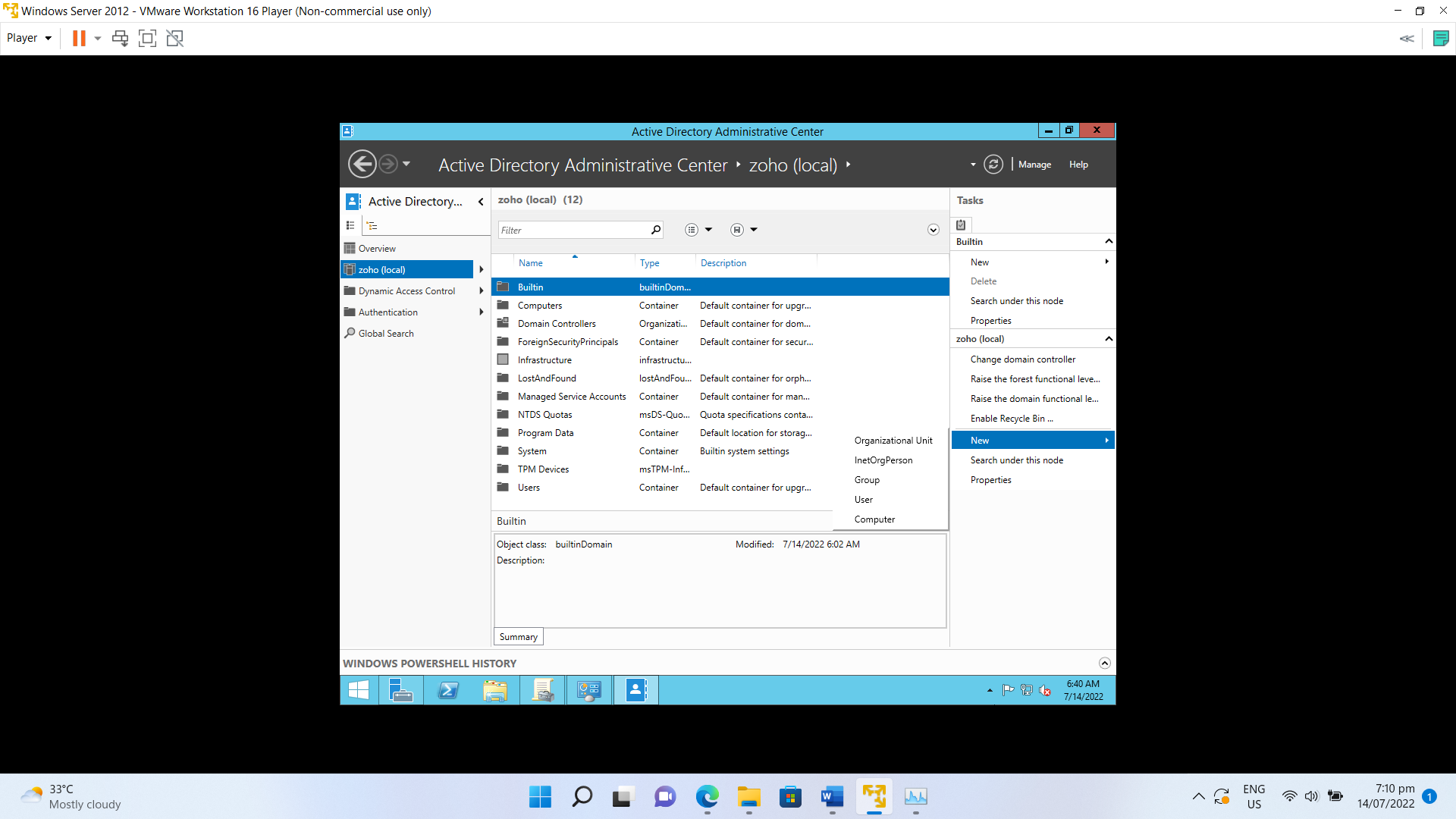
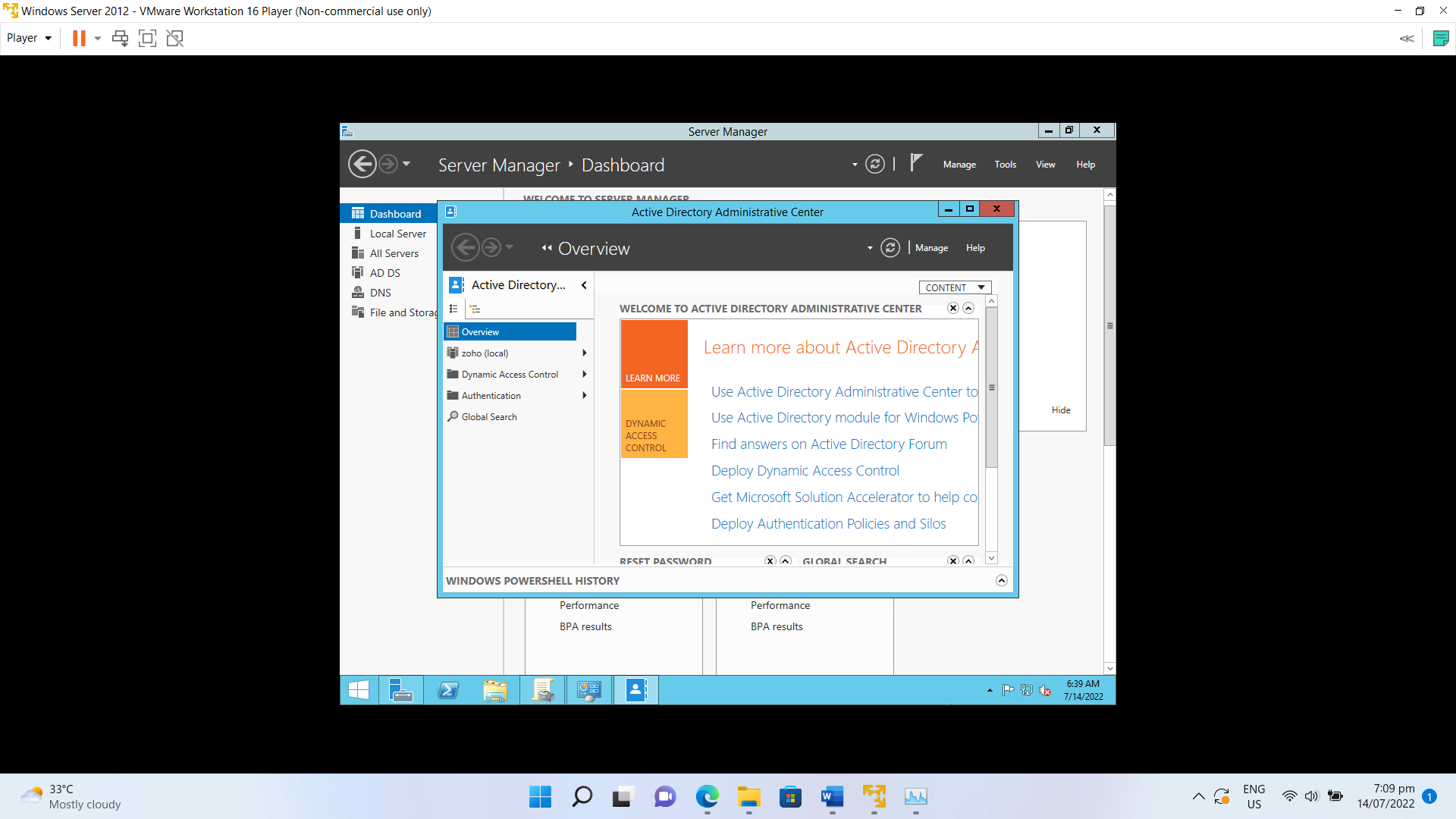
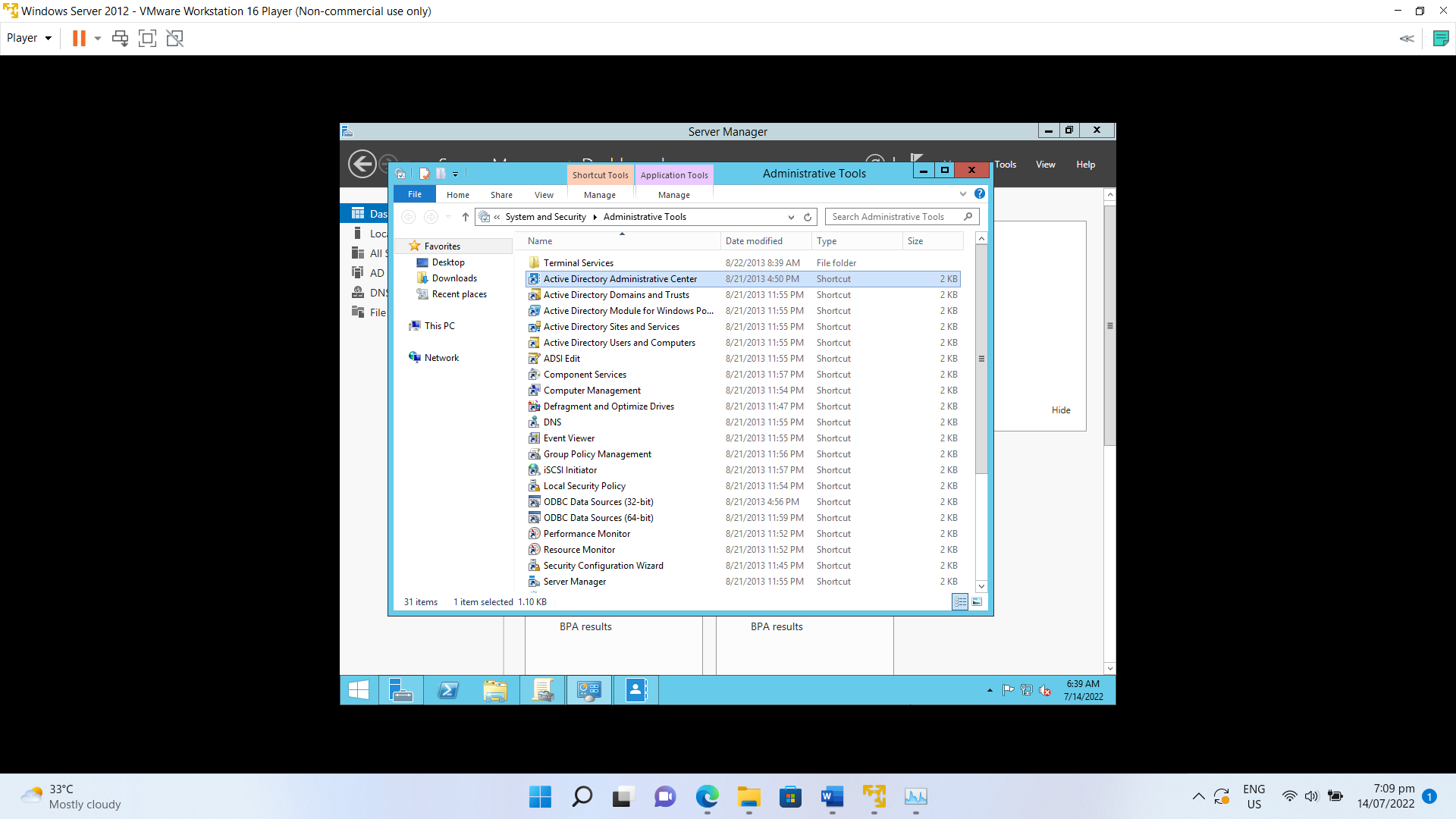
Active Directory set up on

# Windows Server 2012 R2









GPO has been setup . and automatic windows update is scheduled for all computers under the OU(Organizational Unit) on every Monday at 1.00 pm .