Setup of Microsoft DNSSEC-validating Resolver in Windows Server Virtual Machine

1. Install Windows Server virtual machine

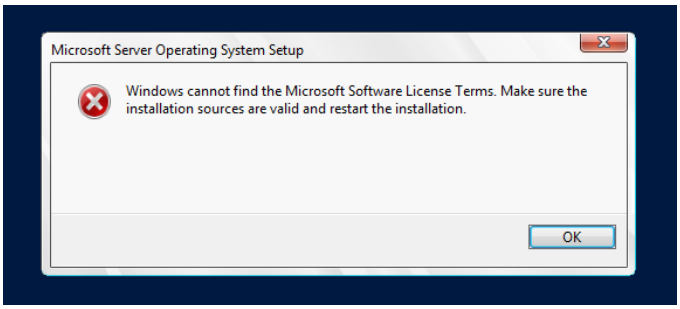
Before installing the virtual machine, make sure that there is a virtual machine tool (e.g., VMware Workstation) on your local device.

Download the ISO for Windows Server 2022 from Microsoft Evaluation Center. Please note that the freely-downloadable ISO is primarily intended for function evaluation, where the Windows OS may only be available for a 180-day trial period.

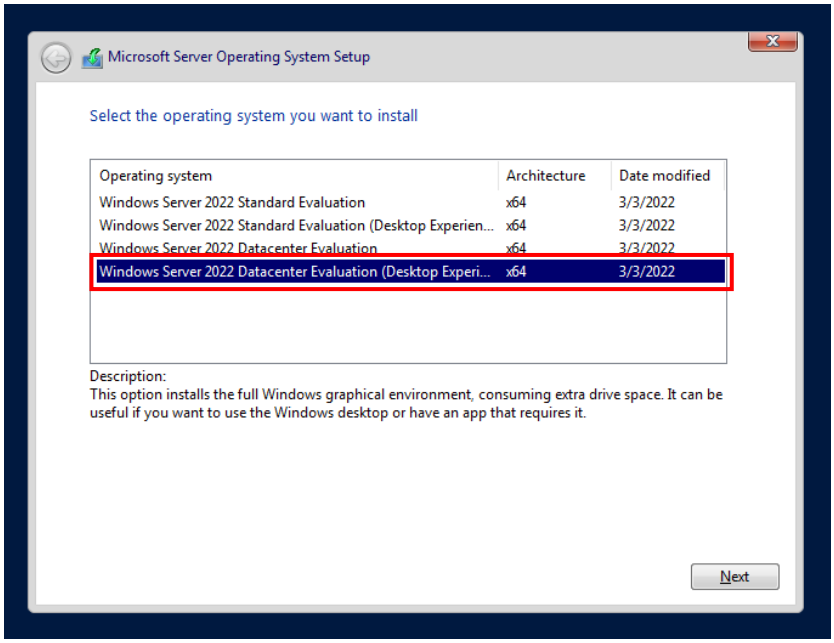
Create a new virtual machine via the ISO. Recommended configuration:

Version	# CPU core	RAM	Storage	Boot mode
Windows Server 2022 Datacenter	⩾4	⩾4GB	⩾20GB	BIOS

Note: There is no need to enter the license key when creating the virtual machine. If you encounter the following error when starting the machine, please remove Floppy in the Virtual Machine Settings menu, and restart the machine.



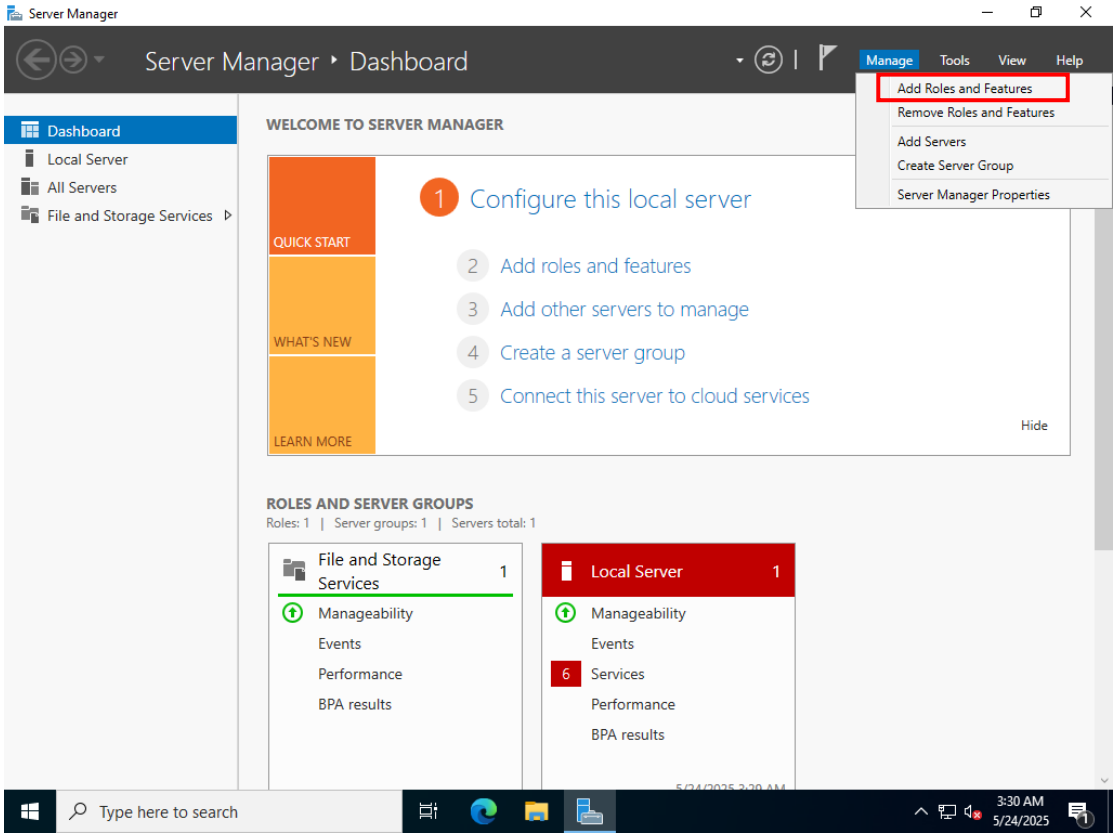
Select the OS with Desktop UI to install, and pick Custom installation:



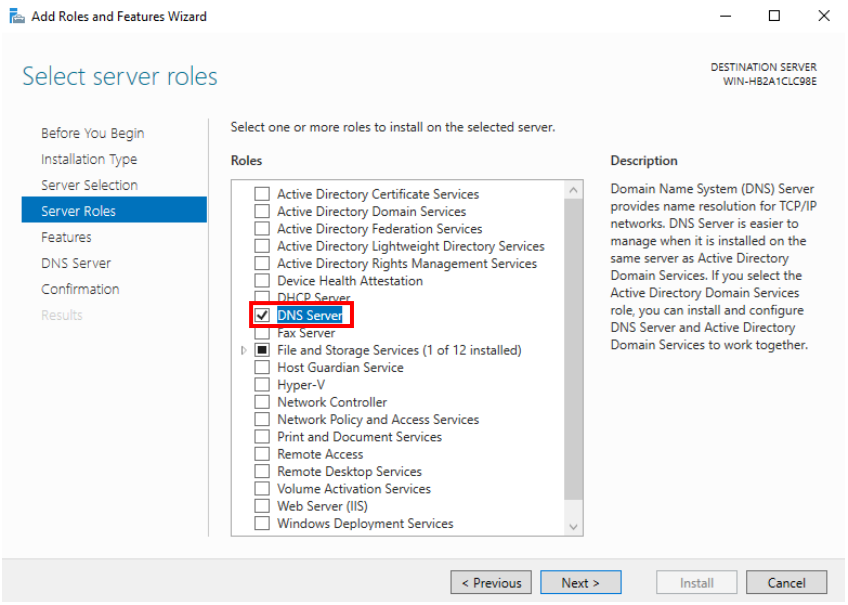
Then set the password and log in. Now the Windows Server virtual machine is ready.

2. Add DNS service to Windows Server

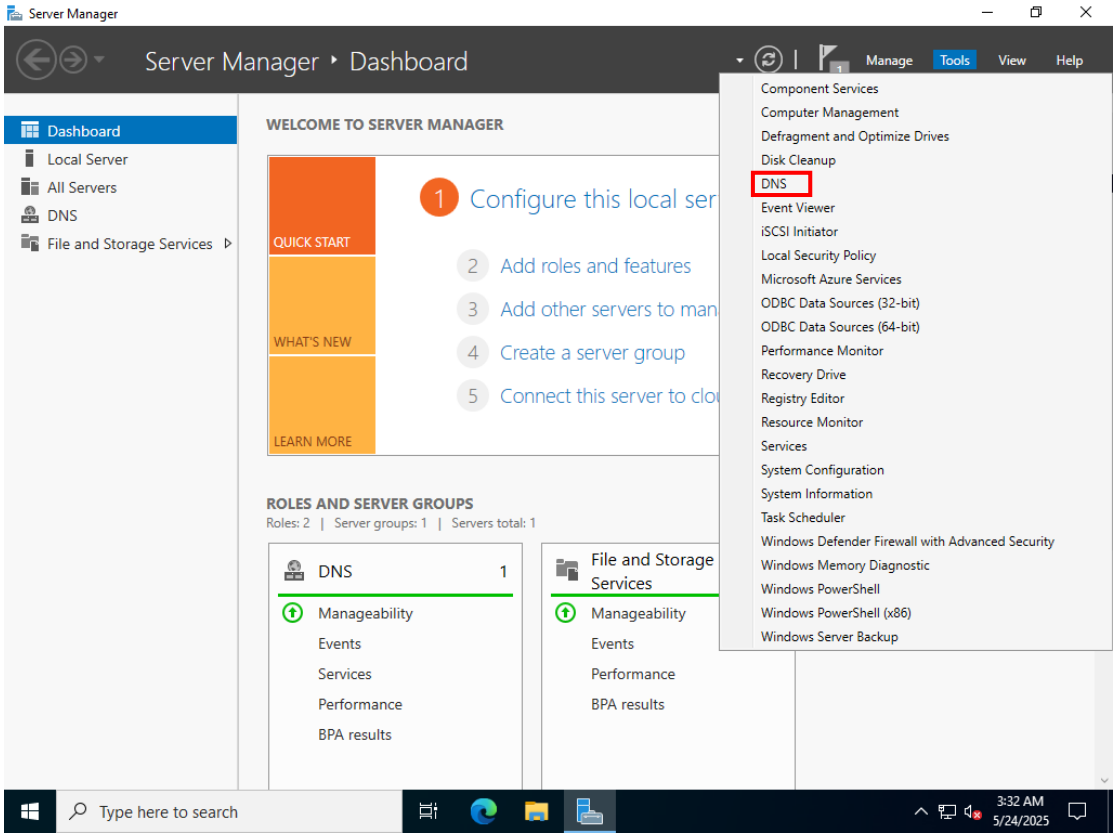
In Server Manager, select Manage -> Add Roles and Features.



Click "Next", until you see the list of server roles. Select "DNS Server" to install the DNS service.

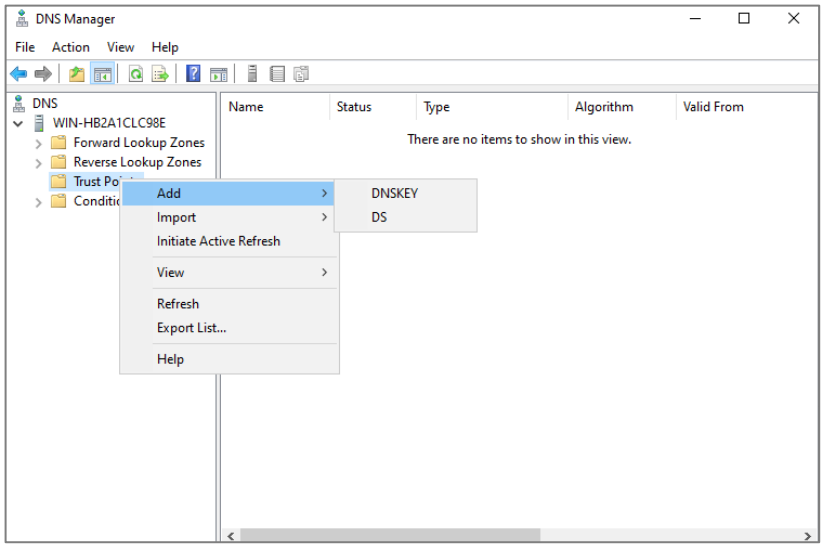


After installation, you can see "DNS" from the Tools menu.

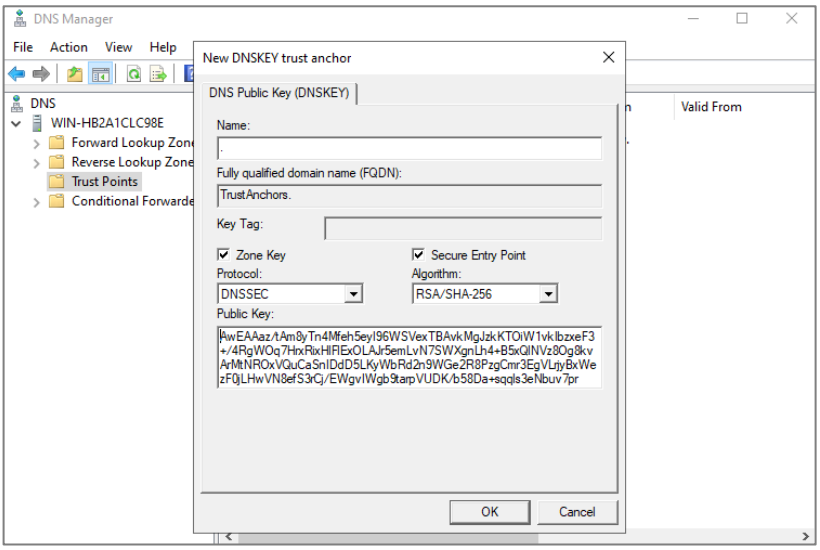


3. Enable DNSSEC validation

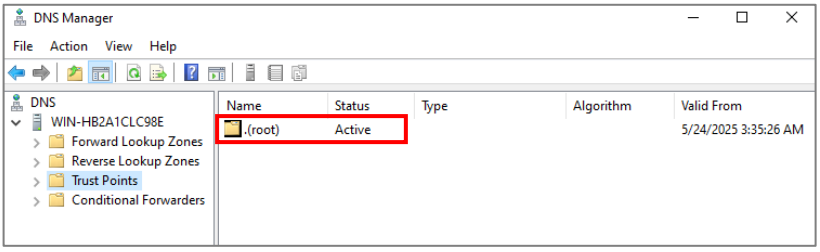
Click "DNS" in the Tools menu of the Server Manager, and you can see the newly-installed DNS server. Right-click "Trust Points", select Add -> DNSKEY.



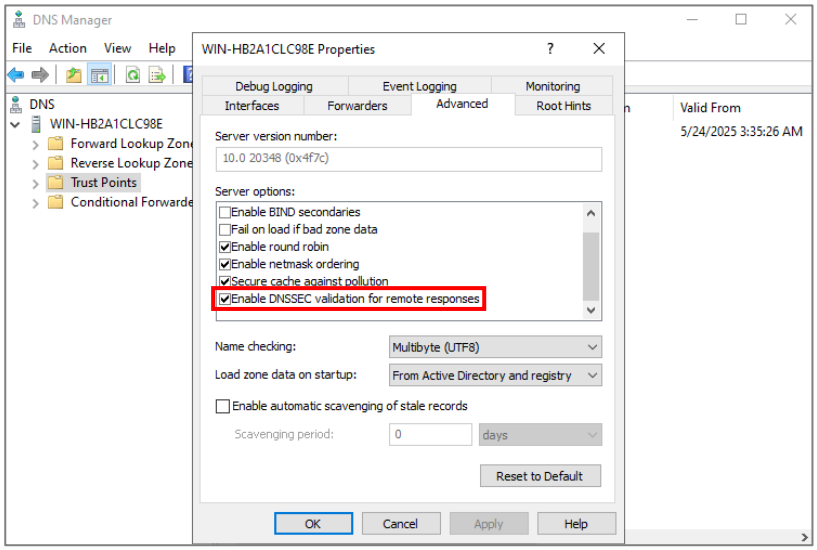
Retrieve the latest DNSSEC trust anchor (i.e., the KSK of the root zone) from IANA root anchor. Copy and paste the KSK with tag 20326 (start with AwEAAaz/tAm8yTn…) into the "Public Key" field. Enter "." (the root zone) in the "Name" field. Then click "OK".



Now the newly-added trust point should be in Active status.



Also please make sure that the DNSSEC validation property has been enabled: right-click the DNS server identifier -> Properties -> Advanced, see if "Enable DNSSEC validation for remote responses" has been checked.



Now the setup of a Microsoft DNSSEC-validating resolver has completed.