

WINDOWS 2012 NOTES

1. Change Root Password

- Ctrl+Alt+Delete
- Click Change Password

2. Change User Account Control Settings

- Put it to the highest setting.
- Check Firewalls and enable them if needed.
- Look for commands and pid, running services

3. Disable ports SSH, Telnet, and any other ports

To disable a port in Windows Server 2012, follow these steps:

1. Log in to the server as an administrator.
2. Click on the Start button and select Control Panel.
3. In the Control Panel window, click on the System and Security option.
4. In the System and Security window, click on the Windows Firewall option.
5. In the Windows Firewall window, click on the Advanced Settings option.
6. In the Windows Firewall with Advanced Security window, click on the Inbound Rules option in the left pane.
7. In the Inbound Rules section, locate the port you want to disable and right-click on it.
8. From the context menu, select Disable Rule.
9. Repeat the steps for the Outbound Rules section if you want to disable the same port for outbound traffic.
10. Close the Windows Firewall with Advanced Security window.

Note: Disabling a port may prevent certain applications from functioning properly. It is recommended to be careful when disabling ports and only do so for specific security reasons.

4.

To set important files as immutable in Windows Server 2012, you can use the built-in File Server Resource Manager (FSRM) tool. Follow these steps:

1. Log in to the server as an administrator.
2. Click on the Start button and select Server Manager.
3. In the Server Manager window, click on Tools and select File Server Resource Manager.
4. In the File Server Resource Manager window, click on File Management Task.
5. In the File Management Task window, click on the Create File Screen link.

6. In the Create File Screen wizard, give the new file screen a name and select the folder where the important files are stored.
7. In the next step, select the Block action and click on the Next button.
8. In the next step, select the criteria for the files you want to make immutable. For example, you can select the "Read-only" attribute and click on the Next button.
9. In the final step, you can choose to send an email notification when a file is blocked, or create a report of all blocked files.
10. Click on the Finish button to complete the wizard.
11. Repeat the steps for each folder or set of files you want to make immutable.

Once the file screen is set, any changes made to the files will be blocked, making them immutable. This helps to ensure the integrity of the important files and prevent unauthorized modifications.

5. Check for updates (don't upgrade though)

To check for updates in Windows Server 2012, follow these steps:

1. Click the "Start" button and select "Control Panel."
2. In the "Control Panel," select "System and Security."
3. Click "Windows Update."
4. In the Windows Update window, click "Check for updates."
5. Windows will check for any available updates and display a list of any updates found.

6. Enable Microsoft Defender Antivirus

- Microsoft Defender Antivirus is included in Windows Server 2012, but it is not enabled by default.
- To enable Microsoft Defender Antivirus, follow these steps:
 1. Click the "Start" button and select "Server Manager."
 2. In the "Server Manager," select "Local Server."
 3. In the Properties section, scroll down and find the "Antivirus" row.
 4. Click "Microsoft Defender Antivirus" to open the settings.
 5. Turn on "Real-time protection."
 6. Click "Save changes."

7. Disable Root Login in Windows Server 2012

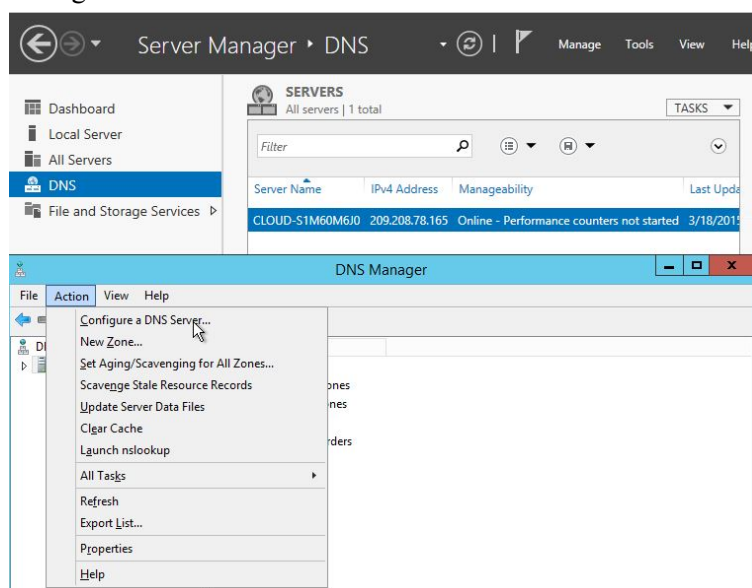
To disable root login in Windows Server 2012, you need to follow these steps:

1. Click the "Start" button and select "Server Manager."
2. In the "Server Manager," select "Local Server."
3. In the Properties section, scroll down and find the "Remote Management" row.
4. Click "Configure Remote Management" to open the settings.
5. Under the "Basic" settings, turn off "Enable Remote Management of this server."
6. Click "Save changes."

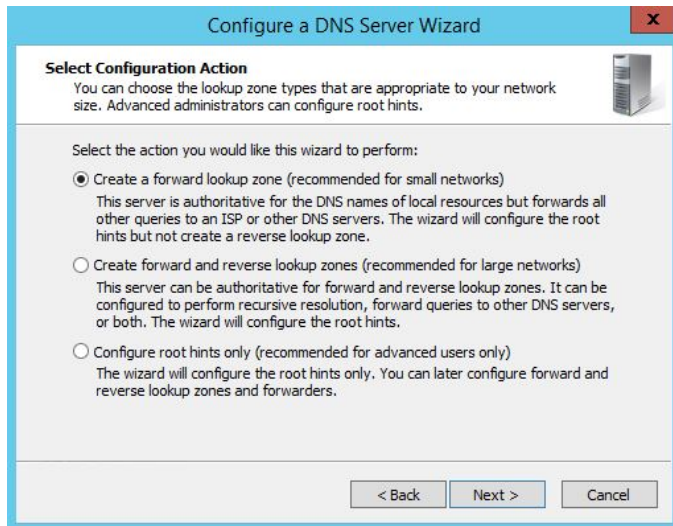
Note: Disabling root login in Windows Server 2012 does not actually disable the root user account. However, by disabling remote management, you are effectively preventing unauthorized users from logging in as the root user remotely. It is recommended to create a separate non-root user account for daily use and perform administrative tasks using the Run as administrator option.

8. Configuring DNS Windows Server 2012

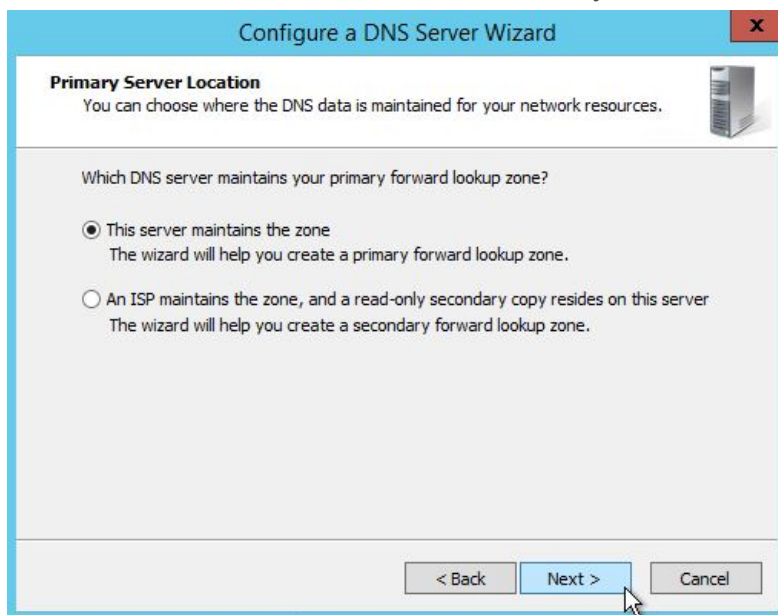
- Click on DNS/ Right Click your server / select DNS Manager / Click the Action Tab / Select Configure a DNS server.



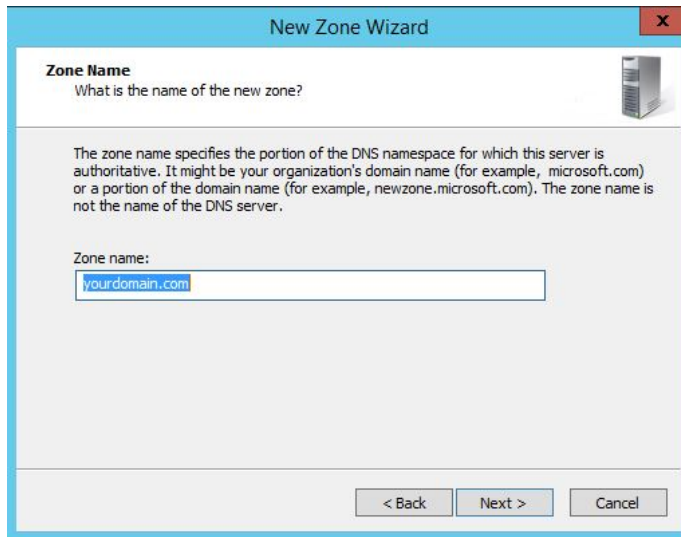
- The Configure DNS Server Wizard will come up. Click Next to continue and select one of the following actions:
- – Create a forward lookup zone
- A forward lookup zone is a DNS function that takes a domain name and resolves it to an IP address.
- – Create forward and reverse lookup zones
- A reverse lookup zone is a DNS function that takes an IP address and resolves it to a domain name.
- – Configure root hints only
- Root hints only Will have the IP addresses of DNS servers where records can be acquired.



-
- Select where the DNS data will be maintained for your network resources, and then click Next



-
- Enter your new zone name, in this case, your domain, and click Next.



New Zone Wizard

Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:
yourdomain.com

< Back Next > Cancel

-
- Create a new zone file or use an existing one from a different DNS server



New Zone Wizard

Zone File
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:
yourdomain.com.dns

☐ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back Next > Cancel

-
- Next, you select how your server will respond to Dynamic Updates.



New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

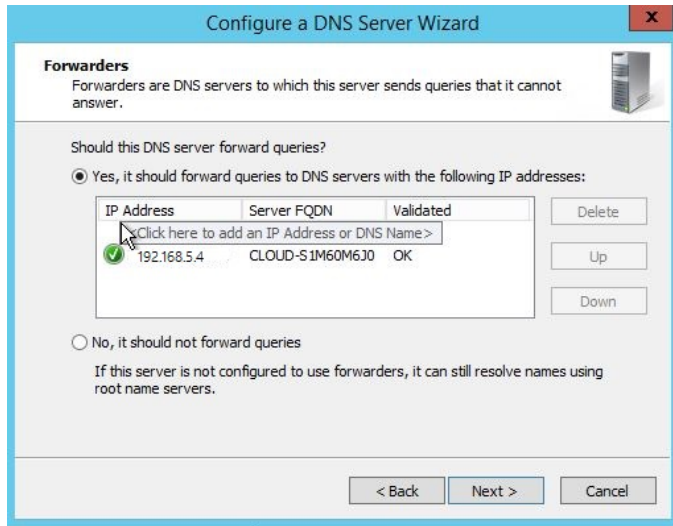
☐ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☒ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

-
- Select whether your DNS server should forward queries or not. If you choose YES, type the IP of the server and click Next. If NO, select No. It should not forward queries and Click Next.



- Click Finish, and you're all set.
- <https://www.quad9.net/service/service-addresses-and-features/#dnscrypt>

- Click the "Start" button and select "Control Panel."
- In the "Control Panel," select "Network and Sharing Center."
- Click "Change adapter settings."
- Right-click on the network adapter that you want to configure and select "Properties."
- Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties."
- In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select "Use the following DNS server addresses."
- Enter "9.9.9.9" as the Preferred DNS server and "149.112.112.112" as the Alternate DNS server.
- Click "OK" to save the changes.

Note: Quad9 is a secure, privacy-focused public DNS resolver that provides protection against malicious domains, phishing attacks, and other security threats. By configuring Windows Server 2012 to use Quad9 as the DNS resolver, you can improve the security and privacy of your network.

To secure Active Directory (AD) in Windows Server 2012, you can follow these steps:

1. Enable strong authentication:
 - Require multi-factor authentication (MFA) for privileged accounts and enforce password policies to ensure that users choose strong passwords.
 - Consider implementing smart cards, biometrics, or other forms of MFA.
 - Enable Kerberos event logging and monitor log files for signs of unauthorized access.
2. Control access to AD:
 - Use Group Policy Objects (GPOs) to control access to sensitive data.
 - Restrict the number of privileged accounts that have administrative permissions.
 - Regularly review and audit the permissions of all users and groups.
3. Secure the AD environment:

- Regularly update Windows Server 2012 and the underlying hardware to ensure that the latest security patches are installed.
 - Use firewalls and other security technologies, such as VPNs and intrusion detection systems, to secure the network perimeter.
 - Regularly back up AD data to prevent data loss or corruption in case of a disaster.
4. Monitor AD activity:
- Monitor AD logs and events to detect suspicious activity, such as unexpected changes to the AD database or unauthorized access attempts.
 - Use auditing and reporting tools to detect and respond to security incidents.
 - Regularly run security scans and penetration tests to identify and remediate vulnerabilities.

By following these steps, you can help ensure that your Active Directory environment is secure and protected against unauthorized access and other security threats.

To enable strong authentication in Windows Server 2012, you can follow these steps:

1. Open the "Server Manager" from the Start menu.
2. Click "Tools," then "Active Directory Administrative Center."
3. In the left-hand navigation pane, click on the domain for which you want to enable strong authentication.
4. Click on "Authentication Policies" in the center pane.
5. Click "Create a Custom Authentication Policy" in the Tasks menu.
6. Enter a name for the custom policy, then select the options for multi-factor authentication (MFA) requirements.
 - For example, you may require users to provide a password and a smart card, or a password and a one-time code sent to their phone.
7. Click "Create."

Note: The specific options available for MFA will depend on the security technologies that you have implemented in your environment, such as smart cards, biometrics, or authentication apps.

Once you have created a custom authentication policy, you can apply it to individual users or groups of users. To do this, you will need to modify the user account properties in the Active Directory Users and Computers tool, or use Group Policy Objects (GPOs) to enforce the policy for multiple users.