



DNS Server Auditing

How to audit DNS records changes on Windows Server 2008/2012

Audit Policy Settings

- Run **GPMC.msc** (url2open.com/gpmc) > edit "Default Domain Policy" > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy > Audit directory service access > Define > Success.
- Computer Configuration > Policies > Windows Settings > Security Settings > Event Log > Define:
 - Maximum security log size to 1gb.
 - Retention method to Overwrite events as needed.

DNS Zone Auditing Settings

- Run **ADSI edit** (url2open.com/adsis) on Domain Controller with DNS role > Connect to Default naming context > Expand DomainDNS object with the name of your domain > System > Right click MicrosoftDNS > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and all descendant objects" > Permissions > Select the following check boxes: Write all properties, Delete, Delete subtree > Click "OK".

DNS Manager Auditing Settings

- Open **DNS Manager** > Expand your servername > Forward Lookup Zone > Right click the zone you want to audit > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Add Principal "Everyone" > Type "Success" > Applies to "This object and all descendant objects" > Permissions > Select the following check boxes: Write all properties, Delete, Delete Subtree > Click "OK".

Review Auditing Events

- Look for Event ID **4662** with Object Type: dnsNode in the Security Event log on DC whenever DNS record is created, modified or deleted.

For Detailed Windows Server Auditing, Try Netwrix Auditor - netwrix.com/go/trial-ws

- **Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

DNS Record Deletion Methods:

- Scavenging
- Manual deletion
- When it gets a valid TTL update with TTL=0
- An LDAP delete command using interfaces such as ADSI edit or LDP

Event ID 4662 Log Content:

- Security ID
- Account Name (**Who**)
- Account Domain
- Object Name (**What**)
- Date and Time (**When**)
- Accesses (**Action Taken**)

Enable Directory Service Access Auditing in CMD

- `Auditpol /set /category:"DS Access" / Success:Enable`
- `Auditpol /set /category:"DS Access" / Failure:Enable`

netwrix
#1 for change auditing

Try Windows Server
Auditing For Free:

netwrix.com/go/trial-ws