netwrix

DNS Server Auditing

This quick reference guide shows how to enable logging of important changes on DNS server in event log.

Audit Policy Settings

- Run **GPMC.msc** (url2open.com/gpmc) > create a new policy and link this GPO to an organizational unit (OU) that contains DNS server in which you'd like to track changes. Once the GPO is created you must go into 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 4gb.*
  - *Retention method to Overwrite events as needed.*

DNS Zone Auditing Settings

- Run **ADSI edit** *(url2open.com/adsi)* 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*

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.

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

Corporate Headquarters:
300 Spectrum Center Drive, Suite 1100,
Irvine, CA 92618

Toll-free: 888-638-9749

Int'l: 1-949-407-5125
EMEA: 44 (0) 203-318-0261

netwrix.com/social