netwrix

IIS Configuration Auditing Guide

IIS 7.5-8

What is IIS Configuration Auditing?

- IIS configuration auditing is a feature that would allow you to track changes made to IIS configuration store (ApplicationHost.config). It generates event messages in Operational event logs.

Enable IIS Configuration Auditing

- Open Event Viewer **eventvwr.msc** > Expand Application and Service Log > Microsoft > Windows > IIS-Configuration > Right click Operational > Choose **Properties** > Click **Enable logging** > Set Maximum log size to 299968KB > Select **Overwrite events as needed** > OK
- Repeat same steps for Application and Service Log > Microsoft > Windows > IIS-Configuration > Administrative log

Review Configuration History Settings

- On IIS server run in command shell with administrative privileges:
  - cd %windir%\system32\inetsrv
  - Appcmd list config /section:configHistory /config:*
- By default 10 configuration backups are kept. You can modify settings:
  - Appcmd set config /section:configHistory -maxHistories:15

Review Auditing Events

- Check Operational and Administrative event logs through Event Viewer. Note: manual changes to the configuration store are not audited. For example if someone modifies ApplicationHost.config with Notepad it won't be recorded to audit logs. Also if someone uses Appcmd to modify IIS configuration you will see auditing entry, but PID won't be a valid one.

What Information is Available through Auditing Logs:

- Process ID (PID)
- Security ID of Account (SID)
- Path to configuration
- Old value
- New value

Will it Affect Server's Performance?

No. IIS configuration auditing uses native Windows subsystem which is capable of handling thousands of events per second without any noticeable CPU overhead

Restore Configuration from Backup Commands:

- **Appcmd list backups**
  shows list of stored backups
- **Appcmd restore backup**
  restores configuration

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