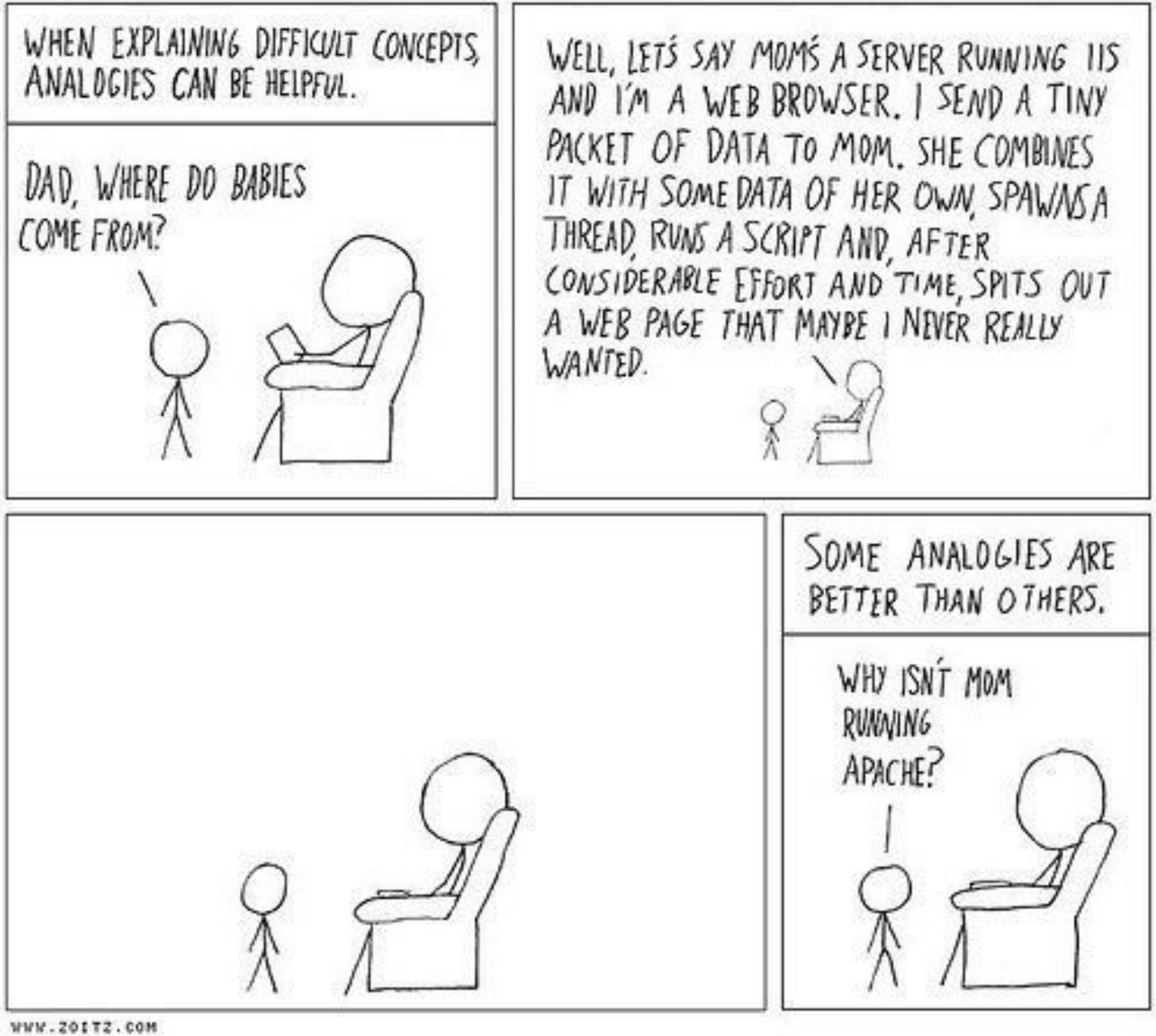
4.5.1 Web Server IIS

Have fun!!!

What is Web Server IIS?

- IIS = Internet Information Services
- Runs on Microsoft (possible to run on Linux, but unstable)
- Web server = process for hosting web applications; cannot have Internet without web servers
  - *Pretty sure you guys interact with the Internet daily… XD*


WHEN EXPLAINING DIFFICULT CONCEPTS, ANALOGIES CAN BE HELPFUL.
DAD, WHERE DO BABIES COME FROM?
WELL, LET'S SAY MOM'S A SERVER RUNNING IIS AND I'M A WEB BROWSER. I SEND A TINY PACKET OF DATA TO MOM. SHE COMBINES IT WITH SOME DATA OF HER OWN, SPAWNS A THREAD, RUNS A SCRIPT AND, AFTER CONSIDERABLE EFFORT AND TIME, SPITS OUT A WEB PAGE THAT MAYBE I NEVER REALLY WANTED.
SOME ANALOGIES ARE BETTER THAN OTHERS.
WHY ISN'T MOM RUNNING APACHE?
WWW.ZOITZ.COM

Web comic

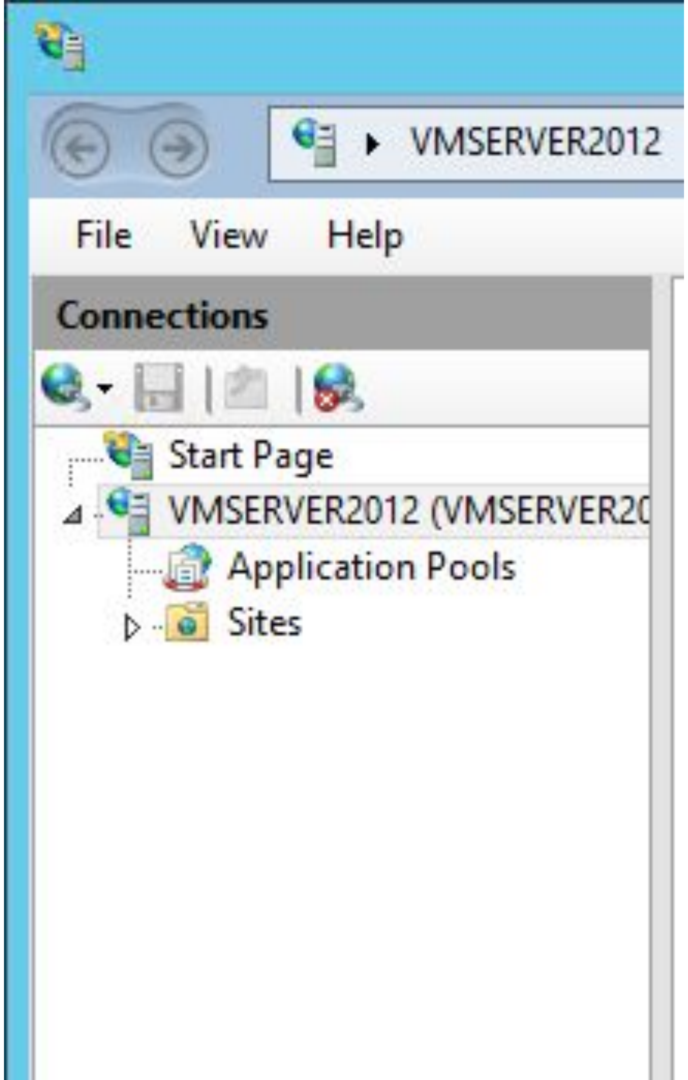
More On Web Server IIS

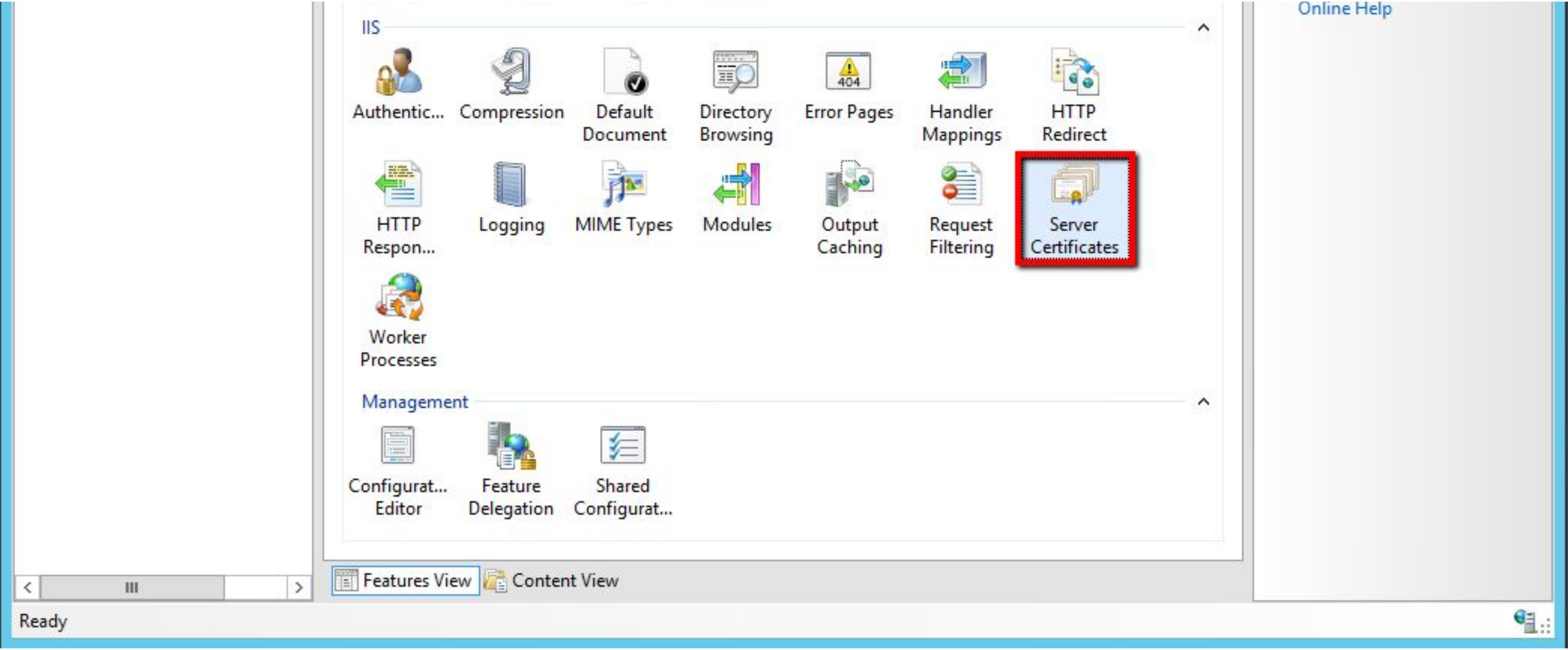
- Commonly used to host ASP.NET web applications & static websites
- Can also be used as an FTP server, host WCF services, also extended to host web applications
- Built-in authentication: Basic, Windows Auth, etc
- Built-in security: TLS, binding for HTTPS and SFTP
- Key feature: application pool
    - Segregates multiple applications from each other

—

Connections

Here you can view your websites (they can be FTP sites or actual HTTP sites)

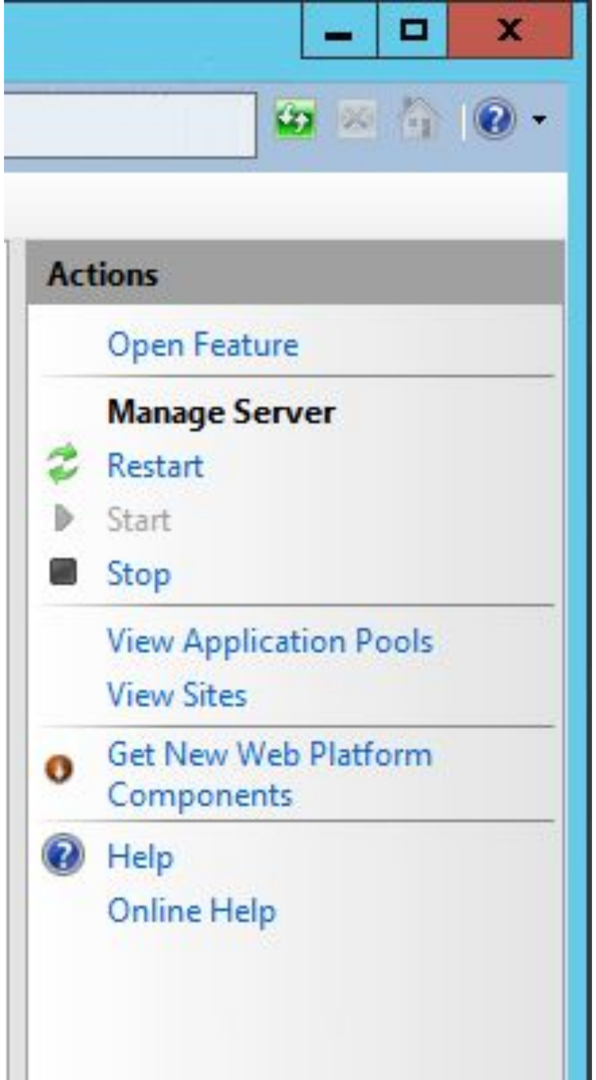




IIS options. You can also add certificates to turn your HTTP server into HTTPS

Server Actions

- Options to restart, start, and stop server
  - Restarts might be needed after security changes are made
- View Application Pools
- View Sites



What's an Application Pool?

All IIS websites run under the w3wp.exe process

You can have multiple instances of w3wp.exe running, where each process hosts a different set of websites

Some application pools of w3wp may have higher access rights than other pools

Application Pool Functions

Allows you to

- run different websites under different users
- run different websites under different frameworks (.Net Framework 2.0 or 4.0, etc)
- run different websites under different bit versions (32 and 64)

Multiple pools will take more memory, however

More on “More on Web Server IIS”

- Kernel Mode → complete access to connected hardware
    - Can execute any command
    - Used for trusted processes
- User Mode → execute commands short of accessing hardware or reference memory
    - Delegates APIs to interact with

Microsoft IIS is kernel mode, so it is faster and has access to non-paged memory, CPU time-slices

How to Install and Configure IIS

- Control Panel → Add or Remove Programs → Add/Remove Windows Components → Check “Internet Information Services (IIS)” → “Next” → “Finish”
- On Server: Server Manager → Add Roles and Features → follow the steps in the window, under roles expand IIS and choose the specific role you want → finish through the installation

Where to Manage?

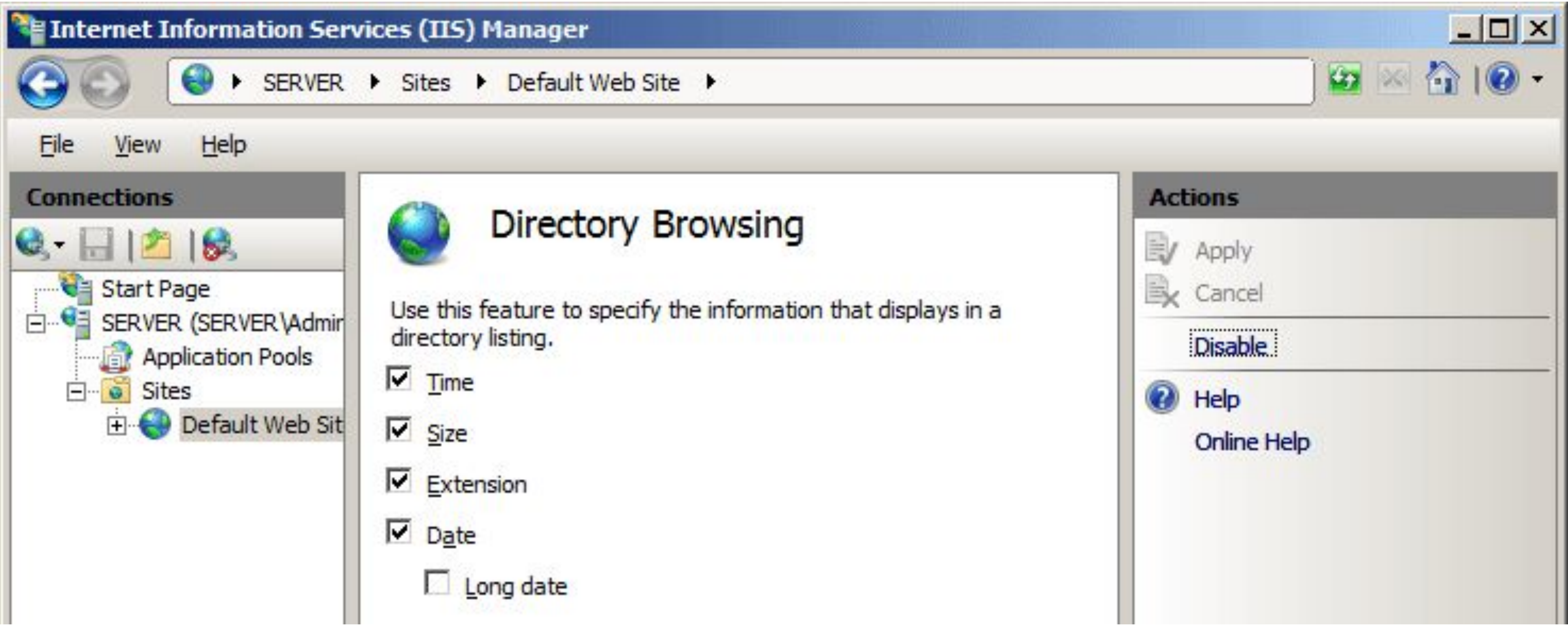
- IIS Manager = GUI
  - The better manager (no SMTP)
  - Can add FTP sites or websites, manage site logs, configure security settings, etc…
- IIS Manager 6.0
  - IIS Manager w SMTP
- Win + R: inetmgr
- Search IIS Manager and click to open :D

Configuration/Security Settings

- Make sure only authorized users can access UNLESS site is meant to be anonymously accessible
    - Control Panel → Programs and Features → Turn Windows features on or off → IIS Services (expand) → World Wide Web Services (expand) → expand Security → select URL Authentication
    - In IIS Manager, go to Authentication and Disable Anonymous Authentication

Configuration/Security Settings

- Users should not have ability to directory browse, but only specific path
    - Open IIS Manager → navigate to level you want to manage → Features View → Directory Browsing → Actions Pane → Disable
- Enable logging
    - ServerName → expand Web Sites or FTP Sites → right-click either where you want to enable logging → click Properties → Click Web Site or FTP Site Tab → select Enable logging
    - Alternatively IIS Manager → Logging → Turn logging on
- Open ports for service
    - Firewall will block unspecified ports by default. Enable the ports required by your server



Directory Browsing

Use this feature to specify the information that displays in a directory listing.

☑ Time

☑ Size

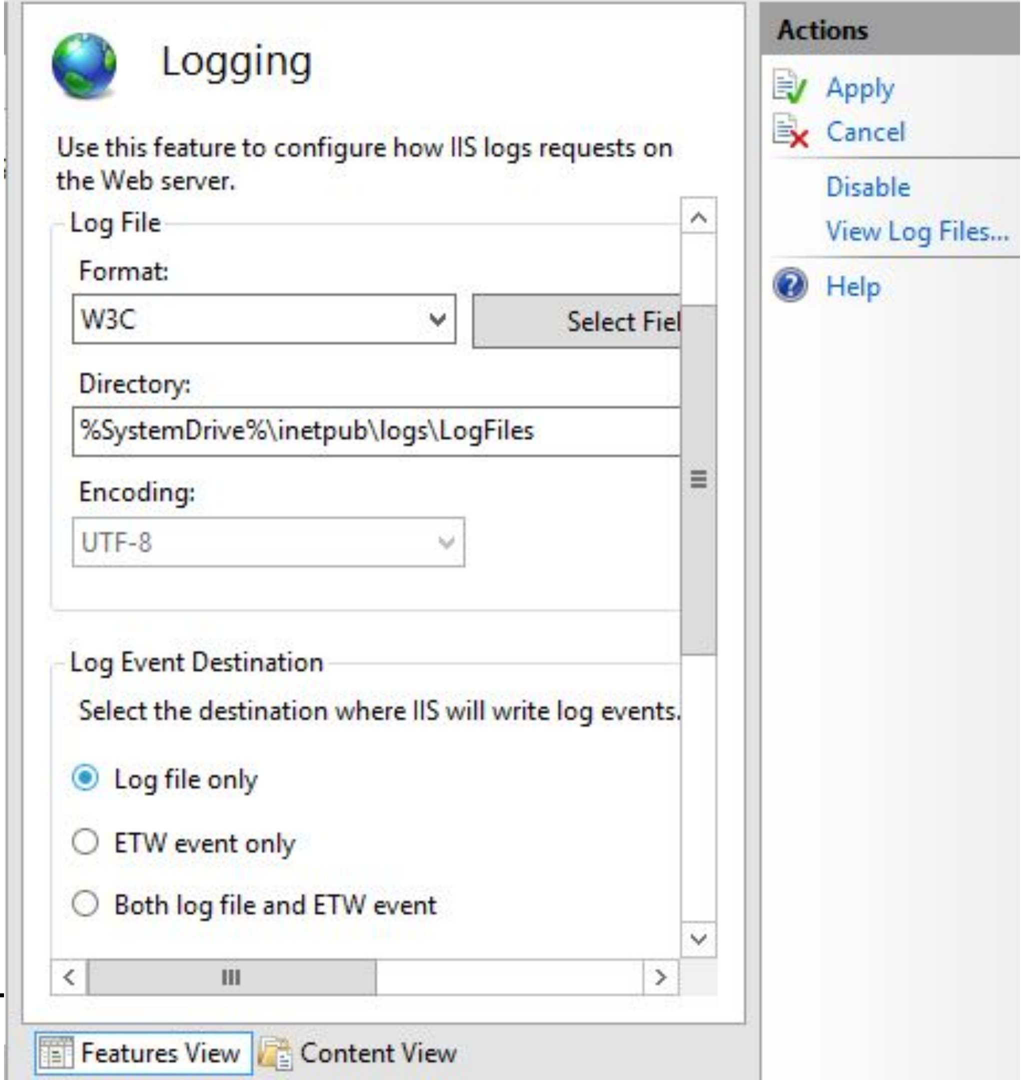
☑ Extension

☑ Date

□ Long date

Click Disable on the right side, and don’t forget to Apply
Might need to restart server for changes to take effect

Enable logging



Logging

Use this feature to configure how IIS logs requests on the Web server.

Log File

Format: W3C

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

○ ETW event only

○ Both log file and ETW event

Want To Know More?

https://www.cisecurity.org/benchmark/microsoft_iis/