Event Viewer is the built-in Windows utility that collects, organizes, and displays logs generated by the operating system, applications, and security subsystems.

Think of it as the "black box recorder" of Windows Server — everything important that happens (good or bad) gets written to a log.

Why Event Viewer Matters for SysAdmins

- Troubleshooting: Helps pinpoint the root cause of system crashes, application failures, and performance issues.
- Security Monitoring: Records login attempts, group policy changes, and unauthorized access attempts.
- Auditing & Compliance: Provides evidence trails for IT audits (e.g., HIPAA, PCI-DSS, SOX).
- Preventive Maintenance: Early warnings of failing hardware, misconfigured services, or resource bottlenecks.

Without Event Viewer, you’re essentially blind to what’s happening under the hood of your server.

Types of Logs in Event Viewer

1. Windows Logs (most commonly used):
    - Application → Events logged by applications/services. Example: SQL Server failure, Exchange service error.
    - System → Events from Windows components. Example: driver errors, disk failure warnings, service startup/shutdown.
    - Security → Logs login attempts, resource access, privilege use. Example: failed login attempts (Event ID 4625).
    - Setup → Records events during Windows installation and upgrades.
    - Forwarded Events → Collects logs from other servers for centralized monitoring.
2. Applications and Services Logs:
    - More granular logs for specific services (DNS Server, Active Directory, Group Policy, etc.).
3. Custom Logs:
    - Admins can create custom views and filters to focus on relevant events.

Introduction to DNS and Basic Configuration

This topic aims to lay the foundation for understanding Domain Name System (DNS), a critical component of modern networking. It's about demystifying how human-readable domain names (like google.com) are translated into IP addresses (like 172.217.160.142) that computers use to communicate.

· Introduction to DNS: Purpose, Components (Servers, Zones, Records), and Hierarchy.

o Purpose:

§ DNS's primary purpose is to translate domain names into IP addresses and vice-versa. This eliminates the need for users to remember complex numerical IP addresses.

§ Think of it as the internet's phonebook.

o Components:

§ DNS Servers: These are computers that store DNS records. They respond to queries from clients seeking to resolve domain names.

§ Zones: A zone is a portion of the DNS namespace that a DNS server is responsible for. It represents a specific domain or subdomain.

§ Records: These are the core data entries within a zone. They map domain names to IP addresses or other information.

o Hierarchy:

§ DNS has a hierarchical structure, similar to an upside-down tree.

§ The root zone (represented by ".") is at the top, followed by top-level domains (TLDs) like .com, .org, .net, .edu, etc. § Below TLDs are second-level domains (e.g., google in google.com), and further subdomains can exist (e.g., mail.google.com).

§ This heirarchy allows for distributed management of domain names.

· DNS Namespace and Domain Names.

o DNS Namespace: This refers to the overall structure of domain names and their hierarchical organization. It's the complete "tree" of all possible domain names.

o Domain Names: These are human-readable names assigned to network resources. They consist of one or more labels separated by dots (e.g., www.example.com).

§ The rightmost label is the TLD, and the leftmost label is the most specific part of the domain name.

· Types of DNS Records (A, CNAME, MX, NS, PTR, etc.).

o This section introduces the various types of DNS records, each serving a specific purpose.

§ A (Address) Record: Maps a domain name to an IPv4 address.

§ AAAA (Quad-A) Record: Maps a domain name to an IPv6 address.

§ CNAME (Canonical Name) Record: Creates an alias for a domain name.

§ MX (Mail Exchange) Record: Specifies the mail server responsible for accepting email for a domain.

§ NS (Name Server) Record: Delegates a subdomain to a different set of name servers.

§ PTR (Pointer) Record: Maps an IP address to a domain name (used for reverse lookups).

§ There are many other record types, but these are the most common.

· Forward and Reverse Lookup Zones.

o Forward Lookup Zones: These zones are used to resolve domain names to IP addresses. This is the most common type of DNS lookup.

o Reverse Lookup Zones: These zones are used to resolve IP addresses to domain names. This is less frequent but essential for certain applications and security purposes.

§ Reverse lookup zones use the "in-addr.arpa" (for IPv4) or "ip6.arpa" (for IPv6) domain.

o The lecture will explain the differences between these zone types and when each is necessary.