cPanel (Control Panel)

cPanel (Control Panel) is a **Linux-based web hosting control panel**, designed to automate the processes involved with running a web server. It lets you conveniently manage all services in a single place. cPanel & WHM allows hosting providers and users the ability to automate server management tasks while offering your customers the tools they need to manage their sites.

A few of the core web hosting processes that are automated via the cPanel software are:

- **Server Security**
- **Domains & DNS**
- **Email Handling**
- **File Transfer & Management**
- **Database Handling**
- **Logging**

WHM

WHM, short for WebHost Manager, is a web-based tool which is used for server administration. There are at least two tiers of WHM, often referred to as "root WHM", and non-root WHM.

Root WHM is used by server administrators and non-root WHM (with fewer privileges) is used by others, like entity departments, and resellers to manage hosting accounts often referred to as cPanel accounts on a web server.

WHM is also used to manage SSL certificates (both server self-generated and CA provided SSL certificates), cPanel users, hosting packages, DNS zones, themes, and authentication methods.[12] The default automatic SSL (AutoSSL) provided by cPanel is powered by Sectigo (formerly Comodo CA).[13] Additionally, WHM can also be used to manage FTP, Mail (POP, IMAP, and SMTP) and SSH services on the server.

As well as being accessible by the root administrator, WHM is also accessible to users with reseller privileges. Reseller users of cPanel have a smaller set of features than the root user, generally limited by the server administrator, to features which they determine will affect their customers' accounts rather than the server as a whole.

cPanel Account

- **Login Credentials**: To access your cPanel account, you are provided with a username and password. This information is used to log in to the cPanel control panel.
- **Web Hosting Management**: The cPanel account allows you to manage different aspects of your web hosting, including file management, domain settings, email accounts, databases, and more.
- **User Interface**: The cPanel interface is designed to be user-friendly and provides a graphical way to perform various tasks related to website and server management. It's divided into different sections, each focusing on specific functionalities.
- **Tools and Features**: cPanel provides a variety of tools and features to manage your website. This includes file managers, email configuration, domain management, security settings, backup tools, and software installations.

- **Customization**: Depending on your hosting provider, the appearance and available tools in cPanel may vary. Some hosting providers might customize the cPanel interface or provide additional tools specific to their services.
- **Security Settings**: cPanel allows users to configure security settings for their hosting account, including setting up SSL certificates for secure connections, password protection, and more.
- **Resource Usage**: Users can also view information about resource usage, website statistics, and logs within the cPanel interface.

Hosting providers purchase this software for use on their own servers. They are responsible for managing and administering their own servers. cPanel has no ownership of the server or the accounts within it, even if it uses our software. As a result, all necessary changes to the server must be relayed through the hosting providers themselves.

Resources

In the cPanel interface users are able to see exactly how much of and what kind of resources have been allocated to them. This can impact the potential speed, size, and complexity that sites within the user account can reach.

DNS, or Domain Name System

DNS, or Domain Name System, is a system that translates human-readable domain names into IP addresses, allowing users to access websites and other internet services using easy-to-remember names instead of numerical IP addresses. The DNS acts like a distributed database that maintains a mapping between domain names and IP addresses.

Domain Name: A domain name is a human-readable web address (e.g., www.example.com).

IP Address: An IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions: host or network interface identification and location addressing.

DNS Server: A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames. There are different types of DNS servers, including authoritative DNS servers, recursive DNS servers, and caching DNS servers.

DNS Resolution:

- Recursive DNS Resolution: When you type a domain name into your browser, your computer queries a recursive DNS resolver. This resolver, often provided by your ISP or another service, is responsible for finding the IP address associated with the requested domain.
- Authoritative DNS Resolution: The recursive resolver then queries authoritative DNS servers responsible for the specific domain to obtain the corresponding IP address.

DNS Hosting: DNS hosting services allow you to manage your DNS records and configurations. Many domain registrars and third-party DNS providers offer DNS hosting services.

A resolver, also called a resolving nameserver, is just a server that responds to DNS requests for domain names that it is not authoritative.

How DNS works

The Domain Name System (DNS) is a hierarchical and distributed naming system for computers, services, or resources connected to the Internet or a private network. DNS translates human-readable domain names into IP addresses, allowing users to access websites and other internet services using easy-to-remember names. Here's a step-by-step overview of how DNS works:

User Input: A user types a domain name into a web browser (e.g., www.example.com).

Local DNS Resolver: The user's device checks its local DNS resolver cache to see if it already has the IP address for the requested domain. If the information is not present or has expired, the resolver proceeds to the next step.

Recursive DNS Server:

- The local DNS resolver queries a recursive DNS server. This server is typically provided by the user's Internet Service Provider (ISP) or another DNS service.
- The recursive DNS server may have the IP address for the requested domain in its cache. If not, it initiates the process of finding the IP address.

Root DNS Server: If the recursive DNS server does not have the IP address, it queries one of the 13 root DNS servers. These servers are distributed worldwide and maintain information about the top-level domain (TLD) servers.

TLD DNS Server:

- The root DNS server responds with a referral to the TLD DNS server responsible for the top-level domain of the requested domain (e.g., ".com" for www.example.com).
- The recursive DNS server then queries the TLD DNS server.

DNS Records:

- The authoritative DNS server responds with the requested DNS records, which may include the IP address (A or AAAA record), mail server information (MX record), or other records such as CNAME or TXT.
- The recursive DNS server stores the obtained information in its cache for a specified period known as the Time To Live (TTL).

Response to User:

The recursive DNS server provides the IP address to the local DNS resolver, which, in turn, provides the IP address to the user's device.

Local Cache Update:

The local DNS resolver caches the obtained information, allowing for faster future lookups for the same domain until the TTL expires.

TLD

TLD stands for top-level domain. That doesn't help much if you're not familiar with DNS, though, so I'll explain. To keep it simple - when you hear people talk about TLDs, they’re usually referring to the last part of a domain: .com, .net, .org, .gov, .ninja, .tv, .anything; these are handled by TLD nameservers, with help from standards organizations to determine who gets to use which TLDs and where. So, if our domain ends in .com, the root nameserver will tell us where to find the TLD nameservers that handle all .com domains.

DNS Records

A DNS record instructs the name to go to an IP Address. The intent is that, when you look for that particular name, you then know the correct IP address to find the content. This might be a full domain name, or it might be part of one. These records are stored on DNS servers and help translate human-readable domain names into IP addresses or perform other functions related to domain management.

Here are some common types of DNS records:

A Record (Address Record): Associates a domain or subdomain with an IPv4 address.

AAAA Record (IPv6 Address Record): Associates a domain or subdomain with an IPv6 address.

CNAME Record (Canonical Name): Creates an alias from one domain or subdomain to another.

MX Record (Mail Exchange): Specifies mail servers responsible for receiving email on behalf of a domain.

PTR Record (Pointer Record): Used in reverse DNS lookups to map an IP address to a domain name.

NS Record (Name Server): Specifies authoritative DNS servers for the domain.

SOA Record (Start of Authority): Contains information about the domain and the zone it's in, including the primary authoritative DNS server and contact information.

TXT Record (Text): Stores arbitrary text data. Often used for domain verification, SPF (Sender Policy Framework), and other purposes.

SRV Record (Service): Specifies information about available services, including the hostname, port, and protocol.

CAA Record (Certification Authority Authorization): Defines which certificate authorities are allowed to issue certificates for a domain.

DNSKEY Record (DNS Key Record): Holds the public key that resolvers can use to verify DNSSEC signatures.

WWW

The World Wide Web (WWW, is an information system that enables content sharing over the Internet through user-friendly ways meant to appeal to users beyond IT specialists and hobbyists. It allows documents and other web resources to be accessed over the Internet according to specific rules of the Hypertext Transfer Protocol (HTTP).

Documents and other media content are made available to the network through web servers and can be accessed by programs such as web browsers.

Servers and resources on the World Wide Web are identified and located through character strings called uniform resource locators (URLs).