

Administración de servidores de aplicaciones (Despliegue de aplicaciones web)

Arquitectura y configuración básica del servidor de aplicaciones

Una aplicación Web es proporcionada por un servidor Web y utilizada por usuarios que se conectan desde cualquier punto vía clientes Web (browsers o navegadores).

Los componentes de una aplicación web son:

- **Lógica de negocio:** es la parte más importante de la aplicación que define los procesos y operaciones que se involucran en la aplicación.
- **Administración de los datos:** trata sobre la manipulación de las bases de datos y los archivos.
- **Interfaz:** los usuarios interactúan con la aplicación mediante sus dispositivos y a través de sus navegadores.

Las aplicaciones web se modelan mediante lo que se conoce como modelo de capas, una capa representa un elemento que procesa o trata información. Los tipos son:

- **Modelo de dos capas:** la información atraviesa dos capas entre la interfaz y la administración de los datos.
 - **Modelo de n-capas:** la información atraviesa varias capas, el más habitual es el modelo de tres capas.
-

Más información

- <https://www.jesusninoc.com/01/13/curso-de-aplicaciones-y-servicios-web-con-powershell/>
-

Administrar aplicaciones Web

Es fundamental administrar la parte de servidores y bases de datos que son los elementos que utilizan las aplicaciones Web.

Más información

- <https://www.jesusninoc.com/web-service/>
-

Autenticación de usuarios. Dominios de seguridad para la autenticación

Autenticación HTTP con PHP

Es posible usar la función `header()` para enviar un mensaje «Authentication Required» al navegador del cliente causando que se abra una ventana para ingresar usuario y password. Una vez se ha llenado el usuario y password, la URL contenida dentro del script PHP será llamada nuevamente con las variables predefinidas `PHP_AUTH_USER`, `PHP_AUTH_PW`, y `AUTH_TYPE` puestas por el nombre del usuario, password y el tipo de autenticación respectivamente. Esas variables predefinidas son encontradas en los arrays `$_SERVER` y `$HTTP_SERVER_VARS`. Ambos métodos de autenticación «Basic» y «Digest» (desde PHP 5.1.0) son soportados.

Autenticación HTTP Basic

En el contexto de una transacción HTTP, la autenticación de acceso básica es un método diseñado para permitir a un navegador web, u otro programa cliente, proveer credenciales en la forma de usuario y contraseña cuando se le solicita una página al servidor.

Autenticación HTTP Digest

Digest access authentication o Autenticación de acceso con resumen es uno de los métodos usados en servidores web para negociar credenciales, tales como nombre de usuario y contraseña, desde el navegador web. El segundo mecanismo es Autenticación de acceso básica. El método «Digest access authentication» es usado para confirmar la identidad de un usuario antes de servir información sensible, como el historial de transacciones de un banco. Se aplica una función hash a la contraseña antes de ser enviada sobre la red, lo que resulta más seguro que enviarla en texto plano como en la autenticación básica.

Autenticación de usuario

Se puede realizar una autenticación de usuario para entrar en una determinada página del siguiente modo utilizando sesiones.

Administración de sesiones. Sesiones persistentes

Una sesión es un periodo de tiempo durante el cual una persona determinada ve un número de diferentes páginas Web de un determinado dominio.

La sesiones y las variables de sesión permiten pasar datos entre páginas sin necesidad de utilizar formularios y es la

mejor forma para ocultar datos comprometidos.

Más información

- <https://www.jesusninoc.com/02/26/utilizar-sesiones-de-las-aplicaciones-web-en-powershell/>
-

Archivos de registro de acceso y filtro de solicitudes

Con las funciones de registro se pueden enviar mensajes directamente a otras máquinas, a un e-mail, al registro del sistema, etc., por lo que puede registrar y monitorizar selectivamente las partes más importantes de sus aplicaciones y sitios web.

Configurar el servidor de aplicaciones para cooperar con servidores Web

Existe una estrecha relación entre los servidores Web y las aplicaciones Web.

Despliegue de aplicaciones en el servidor de aplicaciones

Cuando finaliza el desarrollo de una aplicación web hay que desplegarla a los servidores de aplicaciones y verificar que se ha realizado correctamente, antes de poner la aplicación en un servidor de producción es conveniente probarla en un

servidor de pruebas.

Seguridad en el servidor de aplicaciones. Configurar el servidor de aplicaciones con soporte SSL/T

Los datos que circulan a través de la red entre aplicaciones son accesibles por terceras personas ajenas a la comunicación, es necesario evitarlo a toda costa mediante el uso de protocolos seguros.

También si importante asegurarse de que los datos no se modifiquen durante el transporte. Los protocolos que aseguran la información a nivel de capa de transporte son SSL y TLS.

El protocolo SSL

Originalmente diseñado por Netscape para establecer comunicaciones seguras con protocolos como HTTP o FTP. Permite negociar qué algoritmos se van a emplear, intercambiar las claves de encriptación y la autenticación de clientes y servidores.

Existen tres versiones del protocolo, la cuarta es una mejora del SSLv3 y se conoce con el nombre de TLS.

El protocolo TLS (Transport Layer Security)

Es una evolución del protocolo SSL (Secure Sockets Layer). La última propuesta de estándar está documentada en la referencia [RFC_2246].