# CURA-DNS

CURA-DNS software es un sistema que provee de servicios críticos de red en servidores de uso general sobre GNU/Linux con características de seguridad reforzadas, entre los servicios provistos se encuentran DNS, DNSSEC, DHCP, HTTP, FTP, TFTP, NTP, VPN.

Su función principal es la administración de zonas de dominios y la resolución de grandes cantidades de consultas de protocolo DNS. La configuración de las zonas se mantiene almacenada en una base de datos interna de rápido acceso, y las demás configuraciones de otros servicios en archivos de texto. Algunas funcionalidades de los servicios integrados son:

- (DNS) Resolución de nombres de dominio
- (FTP) Servidor de transferencia de archivos
- (TFTP) Servidor de transferencia de archivos asíncrono
- (NTP) Servicio de sincronización de tiempo
- (SYSLOG) Servicio de recepción de Eventos
- (DHCP) Servicio de asignación de direcciones IP dinámico
- (SSH) Servicio de transferencia de archivos por canal seguro
- (PHPIP) Servicio de administración de Direcciones IP
- HTTP Servicio de publicación de archivos vía Web

## Características de los equipos

El sistema CURA-DNS puede funcionar en equipos de propósito general de diferentes capacidades, la siguiente tabla precisa las características de servidores para CURA-DNS de diversas dimensiones.

| Desempeño | CPU | RAM | H.D. | Interfaces | Peticiones/Seg | Fuentes |
|---|---|---|---|---|---|---|
| Básico | 2 Core | 2 GB | 160 GB | 1 cobre | 1000 | 1 (2 opcional) |
| Medio | 2 Core | 4 GB | 250 GB | 2 cobre | 2000 | 1 (2 opcional) |
| Alto | 4 Core | 8 GB | 320 GB | 4 cobre | 3000 | 2 |

## Características del modulo de DNS

El sistema CURA-DNS al tener como principal elemento el software de DNS más usado en el mundo Bind 9.8 del Internet System Consortium (ISC), provee una plataforma robusta y estable, compatible con estándares de DNS. Entre muchas de las características del servicio de DNS, se encuentran las siguientes:

Provee soporte completo del estándar DNSSEC (Domain Name System Security Extensions), para probar que los datos no han sido modificados y vienen de la fuente original en las consultas de DNS.

Creación de vistas para la configuración de resolución de dominios con IP's públicas y privadas basadas en los equipos o redes que hacen las peticiones.
Cuenta con una base de datos Berkeley centralizada y administrada por el mismo servicio de Bind para almacenar datos de las zonas.
Soporte para GSSAPI: Permite la integración con servidores GNU/Linux y Windows utilizando el protocolo SMB/NetBIOS.
TSIG — Abreviación para Transaction SIGnatures, esta característica permite una transferencia desde el maestro al esclavo sólo después de verificar que una llave secreta compartida existe en ambos servidores maestro y en el esclavo.
GeoIP: Capacidad de resolver con diferentes nombres dependiendo de la ubicación geográfica donde se genere la consulta, bajo las siguientes fuentes:

- Ciudad
- Región
- ISP
- Organización
- Número de AS
- Velocidad de enlace
- Dominio
- Ipv6

Registros de DNS: Algunos de los registros de DNS soportados se encuentran listados en la siguiente tabla:

| Registro | RFC | Descripción |
|---|---|---|
| A | RFC 1035 | Registros de direcciones Ipv4. Una dirección IPv4 para un equipo |
| AAAA | RFC 3596 | Registro para direcciones Ipv6. Una dirección IPv6 para un equipo |
| CNAME | RFC 1035 | Nombre canónico. Un nombre alias para un equipo |
| DNSKEY | RFC 4034 | DNSSEC.bis. llave publica de DNS. |
| HINFO | RFC 1035 | Información de un equipo - texto opcional con datos de un equipo |

| Registro | RFC | Descripción |
|---|---|---|
| KEY | RFC 2535 | Llave pública asociada con un nombre de DNS |
| MX | RFC 1035 | Intercambiador de correo. Un valor de preferencia y el nombre del host para un servidor o intercambiador de correo que servirá esta zona. El RFC 974 define los nombres validos |
| NS | RFC 1035 | Servidor de Nombre. Define el nombre del servidor(es) autoritativo para el dominio (definido por el registro SOA) o el subdominio |
| PTR | RFC 1035 | Dirección IP (Ipv4 o Ipv6) para un equipo |
| SOA | RFC 1035 | Inicio de autoridad. Define el nombre de la zona, un correo de contacto y varios tiempos y valores de actualización aplicables a la zona. |
| SPF | RFC 4408 | Estructura de política de remitente v1. Define los servidores que están autorizados para enviar correo de un dominio. Su función primaria es prevenir la identificación de robo de identidad por spammers |
| SRV | RFC 2872 | Define los servicios permitidos en la zona, por ejemplo, LDAP, HTTP, etc. |
| TXT | RFC 1035 | Información en texto asociada con el nombre. El registro de SPF debe de ser definido usando un registro TXT |
| SPF RR. DKIM | RFC 4871 | Autenticación de correo. |

## Hardening del sistema

CURA-DNS cuenta con el sistema GNU/Linux que ha sido reforzado desde un nivel de núcleo de sistema hasta el nivel de cada servicio, dicho reforzamiento permite bloquear un gran número de ataques conocidos para los protocolos del sistema, además de registrar estos eventos con fines de auditoría. Entre las múltiples configuraciones de seguridad instaladas se encuentran las siguientes:

- Habilitación de módulos del Kernel solo para el hardware utilizado
- Instalación de sistema operativo de base
- Desactivación de servicios no utilizados
- Actualizaciones automáticas deshabilitadas
- Instalación de servicios en chroot
- Registro de los comandos de una sesión SSH
- chroot en las sesiones de usuarios
- Utilización de sudo para funciones administrativas
- Reglas de Iptables para la detención de ataques por TCP
- Configuración por canal cifrado de SSH y acceso directo negado a la cuenta de super-usuario (root)
- Administración de direcciones IP por HTTPS
- Habilitación de DNSSEC

## Sincronización de configuraciones

La configuración de zonas de dominios esta simplificada al configurar un sistema CURA-DNS como Maestro y otro(s) sistema(s) CURA-DNS como esclavos, ya que la información de nuevas zonas o la actualización de las mismas se propaga entre los equipos que integran el grupo. Esto se lleva a cabo por transferencia de zonas sobre el puerto TCP 53, sin embargo cabe aclarar que estas configuraciones viajan sobre un canal cifrado previamente establecido a través del uso del protocolo SSL por el sistema OpenVPN. En otras palabras los CURA-DNS han sido configurados para comunicarse por un direccionamiento de red provisto por el servicio OpenVPN quien cifrara cada uno de los paquetes que pasen por el túnel cifrado entre equipos. Lo cual evita la falsificación intrusión y manipulación de los datos.

## Administración del direccionamiento IP

CURA-DNS utiliza PHPIP para la administración del inventario de direcciones IP, como su nombre lo especifica está basado en PHP, lo que permite administrar el banco de IP's a través de un servidor Web sobre HTTPS usando como motor PHP y una base de datos MySQL.

PHPIP permite administrar direccionamiento en estándar IPV4 e IPv6, además soporta el uso de CIDR (Classless Inter-Domain Routing) para la especificación de clases de direccionamiento, subredes y direcciones bajo las especificaciones del RFC 1519.

En términos de autenticación soporta comunicación con un Directorio Activo o protocolo LDAP para la autenticación al momento de ingresar a la interface de administración Web.

Por otra parte la herramienta esta construida para agregar usuarios y asignarles permisos a áreas específicas de la administración, esto permite crear usuario para agregar o quitar bloques o direcciones de CIDR, mientras que otros usuarios solo podrán ver la lista de direcciones IP.

## Administración de los servicios

El acceso a la administración del equipo es a través de protocolo SSH, de este modo no solo se permite el acceso a través de un canal cifrado por OpenSSL, sino que se dispone de una consola de comandos para ejecutar tareas de administración. Las cuentas de usuario de consola también pueden ser configuradas bajo ciertos perfiles a fin de permitir el acceso solo lectura a los archivos de configuración o el acceso en lectura y/o escritura.

Las cuentas (a excepción del super-usuario) están configuradas para realizar funciones como la habilitación de red, cambio de contraseña, el inicio, recarga y detención de procesos, la lectura de archivos de configuración y el monitoreo de bitácoras; cualquier otra tarea estará deshabilitada, así como el acceso a otros directorios ajenos al HOME del usuario.

## Importación de configuraciones

La interfaz Web PHPIP dispone de un modulo de importación de configuraciones de DNS y DHCP de otros servidores al servicio BIND en formatos como: BIND 9, BIND 8, BIND 4, y Microsoft DNS. Además soporta importación de datos DHCP en formatos: ISC DHCP, y Microsoft DHCP.

## Automatización de cambios

El sistema CURA-DNS dispone de binarios para el monitoreo de enlaces de red, ya sea por un OID de SNMP o por una prueba de Round Trip. Estos binarios se encargaran de leer un archivo de configuración donde se encuentran las direcciones IP de un registro para cada enlace, al detectar la caída de uno de ellos, automáticamente se cambiaran las direcciones IP de las zonas al enlace que se encuentre disponible. Dicho proceso también podrá ser ejecutado de forma manual, y cualquier cambio de direcciones IP en la zonas podrá hacerse desde el archivo de configuración del binario de monitoreo realizando la recarga de la configuración sin afectar el servicio a través de rndc.

insys
Integral Solutions of IT Security

Lada sin costo: 01-800-3636725
Tel. +52 (55) 5322-5200
Soporte: +52 (55) 5322-5240
5322-5241

www.insys-corp.com.mx