



# NIS

Lois Briones Oliveira  
Brais Fernández Reyes  
Fernando Losada Pérez

# ¿Que es NIS?

- **NIS (Network Information Service)** es un sistema cliente-servidor que centraliza la gestión de información de red como usuarios, contraseñas y grupos. Permite que múltiples máquinas compartan esta información de forma consistente.
- **NIS utiliza RPC (Remote Procedure Call)** para la comunicación entre clientes y servidores.
- El daemon `ybind` en el cliente envía solicitudes RPC buscando un servidor NIS.
- Los servidores responden con su dirección y gestionan las peticiones usando `ypserv`.

# ARQUITECTURA NIS

- **NIS Master Server:** almacena la copia principal de los archivos compartidos (ej. /etc/passwd).
- **NIS Slave Server:** mantiene una copia sincronizada para redundancia y balanceo de carga.
- **NIS Clients:** consultan al servidor para autenticación y acceso a datos del sistema.

# NIS DOMAIN

Un **dominio NIS** es un conjunto lógico de máquinas que comparten la misma información de red a través de NIS. Todos los clientes y servidores deben pertenecer al mismo dominio para comunicarse correctamente.

# NIS MAPS

- Son archivos generados desde ficheros de configuración
- Organizan información usando estructuras hash para búsquedas rápidas
- Dependiendo del sistema operativo tienen distintos formatos
- Los mapas generados se guardan en `/var/yp/dominio`
- A veces se le asocia un alias a los mapas que se puede consultar en `/var/yp/nicknames`
- Problemas de seguridad
  - El acceso no requiere autenticación
  - Sin cifrado: cualquier usuario con acceso a la red puede ver los datos

# Comandos basicos

ypcat	Sirve para obtener el contenido de los mapas NIS.
ypinit	Comando que se utiliza para preparar el master, el cliente o el slave, depende el flag
ypmatch	Imprime el valor de las claves de un mapa NIS.
yppoll	Muestra qué versión del mapa NIS está corriendo en el servidor. También devuelve el servidor maestro del mapa.
yppush	Copia la nueva versión del mapa NIS desde el servidor maestro a los esclavos. Se debe ejecutar desde el master server.
ypset	Hace que un proceso de 'ypbind' se vincule a un servidor indicado. No se recomienda su uso habitual por razones de seguridad
ypwhich	Muestra que servidor NIS está usando el cliente para solicitar información.
ypxfr	Extrae un mapa NIS desde un servidor remoto al directorio local '/var/yp/domain', utilizando NIS como medio de transporte. Puede ejecutarse manualmente o desde 'crontab', y también lo llama 'ypserv' para iniciar una transferencia

# NFS

**NFS (Network File System)** es un protocolo que permite a los sistemas acceder a archivos remotos como si fueran locales. Usado para compartir directorios (como /home) a través de la red de forma transparente.

# Seguridad en NIS - NIS + - LDAP

- NIS

- No implementa cifrado ni autenticación robusta.
- Los datos (incluyendo hashes de contraseñas) están expuestos para cualquier cliente del dominio.
- Depende de la seguridad perimetral o física de la red (insuficiente).

- NIS+

- Introduce mejoras usando DES para cifrado y autenticación mutua mediante Secure RPC (AUTH\_DES).
- Permite definir permisos de acceso granulares sobre las “tablas” de NIS+.

- LDAP

- Diseñado con seguridad robusta; soporta SSL/TLS (ej.: LDAPS o StartTLS) para cifrar comunicaciones.
- Admite múltiples esquemas de autenticación (simple, SASL, GSSAPI/Kerberos, etc.).
- Permite control de acceso a nivel de entrada y atributo, ofreciendo políticas precisas de lectura y modificación.



# Escalabilidad en NIS - NIS + - LDAP

- NIS

- Pensado para redes LAN pequeñas a medianas.
- Arquitectura de dominio plano sin jerarquías por lo que requiere dominios separados para organizaciones grandes.
- Utiliza difusión (broadcast) para descubrir servidores.

- NIS+

- Espacio de nombres jerárquico similar al DNS, permitiendo una delegación organizada por regiones.
- Soporta subdominios, con maestros y réplicas, mejorando la distribución de la carga.
- En la práctica, su complejidad limitó su adopción masiva, favoreciendo el traslado a LDAP en grandes entornos.

- LDAP

- Altamente escalable, ideal para despliegues globales (puede manejar millones de entradas).
- Estructura jerárquica (árbol DIT), alineada con el DNS de la organización.
- Soporta replicación multi-maestro, permitiendo la distribución y alta disponibilidad incluso a través de WAN o Internet.
- En términos de rendimiento, es muy eficiente en búsquedas gracias a la indexación de atributos.

# Administración en NIS - NIS + - LDAP

- NIS

- Configuración sencilla basada en archivos planos y mapas simples.
- Adecuado para entornos pequeños donde la rápida puesta en marcha es prioritaria.
- Herramientas básicas como ypwhich y ypcat facilitan su verificación.

- NIS+

- Mayor complejidad administrativa por la necesidad de establecer dominios seguros y gestionar credenciales.
- Requiere comandos y herramientas más complejas.
- La complejidad se asocia a la mejora en seguridad, generando la reputación de “seguro pero difícil”.

- LDAP

- Requiere definir un esquema adecuado, planificar la estructura del DIT y configurar políticas de acceso.
- Integración con otros servicios puede ser compleja inicialmente.
- Existen soluciones modernas (Apache DS) que simplifican la administración mediante interfaces gráficas y automatización de tareas.

# Soporte en NIS - NIS+ - LDAP

- NIS

- Considerado legado.
- Aunque aún está presente en algunas distribuciones Linux por compatibilidad, su uso nuevo es raro.

- NIS+

- Fue soportado oficialmente en Solaris hasta la versión 10, pero discontinuado en Solaris 11 en 2012.
- En Linux nunca tuvo adopción plena y actualmente se recomienda migrar entornos NIS+ a LDAP.
- Es visto como un producto obsoleto de los años 90.

- LDAP

- Es la tecnología vigente y ampliamente soportada.
- Se integra en prácticamente todos los sistemas operativos modernos.
- Continúa evolucionando para incorporar cifrados modernos y mejoras en rendimiento.