LACNIC 46 / LACNOG 2026

Después del rollover de la KSK raíz

Lecciones, señales y verificación operativa

KSK ACTIVA

38696

0x9728 · KSK-2024

Carlos Martínez
LACNIC

Nicolás Antoniello
ICANN

Mendoza · octubre de 2026

El cambio ocurrió. La verificación continúa.

El rollover se ejecutó

KSK-2024 ya firma el conjunto DNSKEY de la raíz. El proceso aún tiene hitos pendientes.

La señal no es el impacto

Las IP que anuncian anclas de confianza no equivalen a resolvers averiados ni a usuarios afectados.

Cada instancia cuenta

Comprobar 38696, el estado persistente y la validación real, incluso si el servicio parece normal.

“Completado” no significa “todos los sistemas verificados”.

Del contexto a la acción

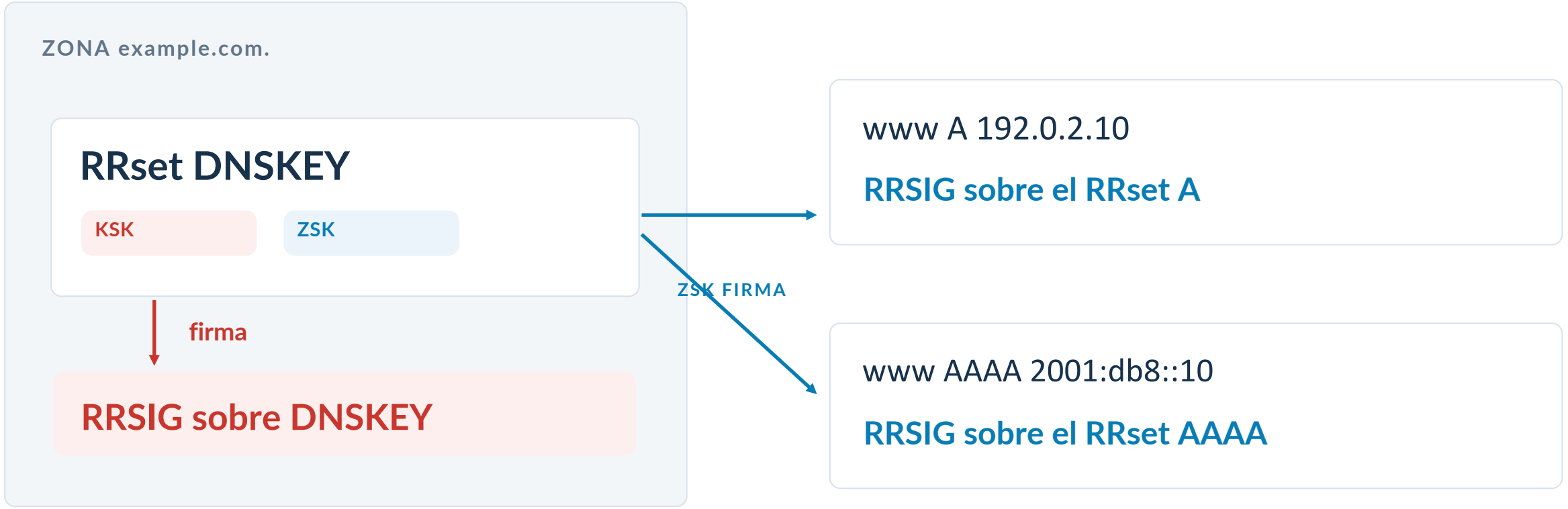
01 **DNSSEC en dos diagramas**
El mínimo contexto para interpretar el cambio.

02 **Lo que nos dejó 2018**
Por qué medir no es lo mismo que entender el impacto.

03 **Qué ocurrió en octubre de 2026**
Anuncio, señales y límites de la evidencia disponible.

04 **Qué revisar hoy**
BIND, Unbound, sentinel y persistencia del estado.

La KSK firma las claves; la ZSK, los demás datos



El rollover de la KSK cambia quién firma el conjunto de claves.

La confianza se construye desde la raíz

Resolver validador

Ancla de confianza

Punto de partida local para autenticar las claves de la raíz.



La raíz no tiene una zona padre que publique su DS.

Por qué cambiar la KSK raíz es distinto

En una zona delegada

La coordinación incluye actualizar el DS en la zona padre y mantener una cadena de confianza válida.

En la raíz

Hay que distribuir la nueva ancla a los validadores. No existe un inventario completo de todas esas instancias.

Sin un ancla utilizable, pueden fallar la validación y la resolución.

Tres claves para leer toda la historia

KSK-2010

19036

0x4a5c

RETIRADA

Revocada y retirada en 2019.

KSK-2017

20326

0x4f66

POSPUBLICACIÓN

Ya no firma. Aún no está revocada.

KSK-2024

38696

0x9728

ACTIVA

Firma desde el 11 de octubre de 2026.

RFC 5011 necesita tiempo y estado persistente

AddPend

Clave observada

La nueva DNSKEY está autenticada por una clave ya confiable.

→

30 días

Espera de aceptación

Período de 30 días de observación válida.

→

Valid

Ancla aceptada

La nueva clave puede utilizarse como punto de confianza.

Perder el estado puede hacer que el aprendizaje deba comenzar otra vez.

2017–2018: se postergó para entender la señal

27 sep 2017

Postergación

La telemetría mostraba más sistemas sin la nueva ancla de lo esperado.

11 oct 2017

Fecha original

El cambio de firma no se ejecutó en la fecha inicialmente prevista.

11 oct 2018

Cambio de firma

KSK-2017 pasó a firmar el conjunto de claves de la raíz.

La lección: una señal de riesgo exige contexto, no una lectura literal.

La señal no medía exactamente lo que parecía

1 **Un reenviador puede ocultar al origen**

La IP que llega al servidor raíz puede representar consultas generadas por otros sistemas.

2 **Señalizar no prueba que se esté validando**

Algunas implementaciones enviaban la señal aun sin validar.

3 **Pocos reportes no demuestran ausencia de fallas**

La revisión de 2018 tampoco pudo atribuir todos los reportes al rollover.

La nueva KSK tuvo 21 meses de prepublicación



Tiempo disponible no equivale a estado aprendido y conservado.

Qué cambió a las 14:00 UTC

Antes del cambio

KSK-2017 (20326) firmaba el conjunto DNSKEY.

KSK-2024 ya estaba publicada para que los validadores la aceptaran.

Después del cambio

KSK-2024 (38696) firma el conjunto DNSKEY.

KSK-2017 permanece publicada, pero ya no firma ese conjunto.

La caché puede retrasar la aparición de fallas de validación.

Completado según lo previsto; seguimiento abierto

01

El cambio se ejecutó

La transición de firma tuvo lugar el 11 de octubre.

02

Hay reportes limitados

ICANN evalúa su posible relación con el rollover.

03

El monitoreo sigue

Quedan hitos operativos, incluida la revocación de la KSK anterior.

No afirmar “cero incidentes” ni atribuir todos los reportes al rollover.

El cambio de firma no cierra todo el proceso



Cambio de firma

REALIZADO

Revocación de KSK-2017

PREVISTO

Retiro de KSK-2017

PREVISTO

Seguir los hitos y comprobar cómo evoluciona el estado de las anclas.

Tres preguntas distintas, tres evidencias distintas

¿Qué se publicó?

Datos y firmas de la zona raíz

Confirma el cambio en el lado autoritativo.

¿Qué anclas se anuncian?

Telemetría RFC 8145

Observa señales, con cobertura y ambigüedades.

¿Qué valida mi servicio?

Estado local + pruebas funcionales

Comprueba el comportamiento de una instancia.

RFC 8145: el resolver anuncia qué anclas conoce




```
_ta-4f66-9728. IN NULL
```

20326 + 38696, expresados como 4f66 + 9728

La consulta deja una señal; la respuesta no certifica el estado del resolver.

Cómo leer las cuatro series del gráfico

ETIQUETA OBSERVADA	CONJUNTO ANUNCIADO	KSK-2024
_ta-4f66	KSK-2017	No anuncia 9728
_ta-4f66-9728	KSK-2017 + KSK-2024	Anuncia 9728
_ta-4a5c-4f66	KSK-2010 + KSK-2017	No anuncia 9728
_ta-4a5c-4f66-9728	Las tres claves	Anuncia 9728

La diferencia clave para este rollover: anunciar o no 9728.

La unidad es IP de origen única por intervalo

Una IP cuenta una vez

por serie y por intervalo de observación.

En esta captura

Intervalo: 1 minuto
Escala: logarítmica
Tiempo: UTC

No es volumen

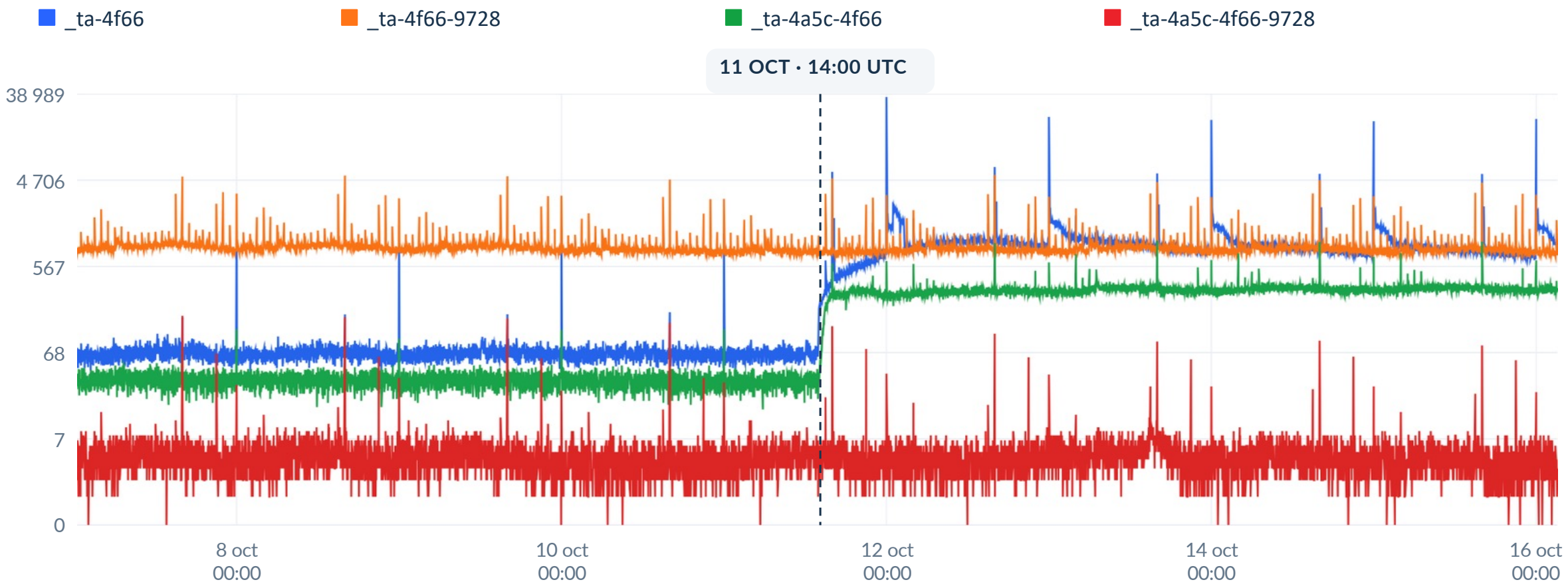
Más consultas de una misma IP no multiplican su conteo dentro del intervalo.

No es un censo

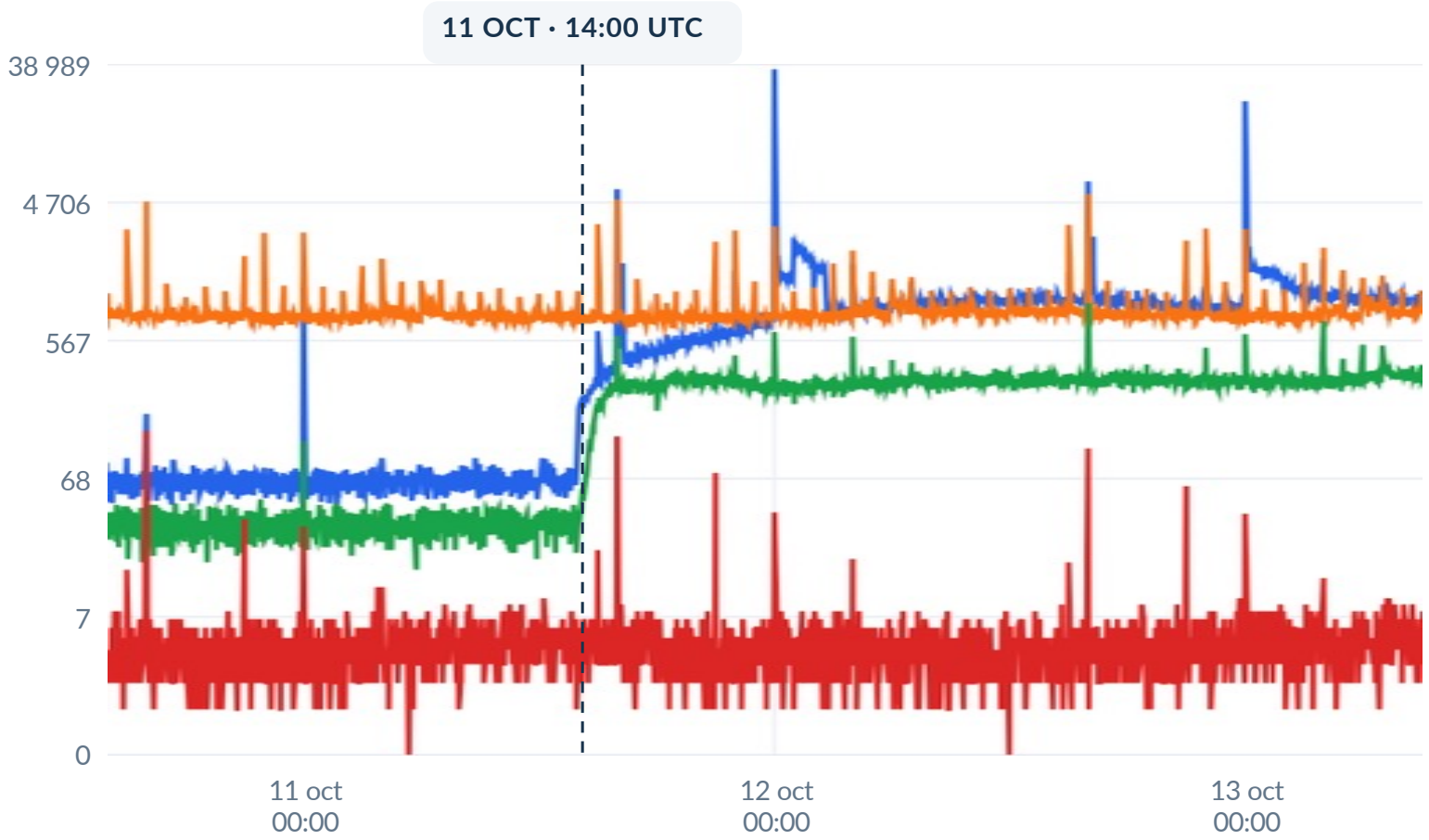
Una IP no identifica necesariamente una instancia ni una cantidad de usuarios.

La señal antes y después del rollover

IP de origen únicas por intervalo · 1 minuto · escala logarítmica · UTC



Un cambio visible no explica por sí solo la causa



Lo visible

Las series azul y verde suben de nivel.

Lo que no sabemos

Cuántas instancias o usuarios tuvieron fallas.

Lo que falta

Cruzar la señal con validación y registros.

Sin 9728: una señal de riesgo, no un censo de fallas

No anuncia 9728

Podría no tener el ancla necesaria para validar después del cambio.

No confirma una falla por sí solo.

Anuncia 9728

La señal incluye la etiqueta de la nueva clave.

No prueba la validación de extremo a extremo.

No aparece en la captura

Puede no señalizar o no estar visible para ese punto de observación.

No implica que no valide DNSSEC.

Comparar dos semanas, sin inventar el resultado

VENTANA DESCRITA EN LA EXPLICACIÓN



1 Deduplicar y definir la población

No sumar los conteos de cada minuto como si fueran fuentes distintas.

No asumir. Verificar cada resolver.

Que resuelva hoy no demuestra que arranque bien mañana.

01 **Ancla aceptada**

38696 en el estado efectivo.

02 **Estado persistente**

Sobrevive al ciclo de vida del servicio.

03 **Validación comprobada**

Controles positivos y negativos.

Incluye réplicas, contenedores, equipos de reserva y rutas de reenvío.

Validar lo correcto y rechazar lo incorrecto

SUSTITUIR LA DIRECCIÓN DE EJEMPLO POR LA DE CADA INSTANCIA

```
RESOLVER=192.0.2.53

dig @"$RESOLVER" . SOA +dnssec
dig @"$RESOLVER" dnssec-failed.org A +dnssec
dig @"$RESOLVER" dnssec-failed.org A +dnssec +cdflag
```

Control positivo

Raíz: respuesta válida y bit AD.

Control negativo

Dominio de falla: SERVFAIL.

Solo diagnóstico

+cdflag afecta esa consulta, no la configuración.

Buscar 38696 en las anclas del proceso

CONSULTA DEL ESTADO

```
sudo rndc managed-keys status

sudo rndc secroots -
```

managed-keys status

Estado de la gestión automática RFC 5011.

Qué buscar

38696 aceptada como ancla, no solo pendiente de inicialización.

Revisar todas las vistas relevantes.

Consultar secroots también ayuda a revisar anclas configuradas estáticamente.

Automático y estático no son lo mismo

EJEMPLO DE CONFIGURACIÓN

```
options {
    dnssec-validation auto;
};
```

Activa la validación y la gestión automática del ancla raíz.

initial-key / initial-ds

Punto de partida para la gestión RFC 5011.

static-key / static-ds

Anclas fijas: requieren mantenimiento explícito.

No deducir el mecanismo de actualización solo de dnssec-validation yes.

El archivo inicial no es todo el estado aprendido

Ancla de arranque

El archivo incluido por el paquete o bind.keys inicia la confianza.

Estado administrado

managed-keys.bind, archivos .mkeys y sus diarios conservan el aprendizaje.

```
sudo rndc managed-keys sync
sudo rndc managed-keys status
```

Revisar el directorio efectivo, los permisos y el almacenamiento persistente.

La actualización necesita un archivo escribible

RUTA DE EJEMPLO: USAR LA CONFIGURADA EN CADA INSTANCIA

```
server:
    auto-trust-anchor-file: "/var/lib/unbound/root.key"
```

Archivo

El usuario de Unbound debe poder actualizarlo.

Directorio

También necesita permiso de escritura para archivos temporales.

Volumen

La ruta debe persistir y ser accesible dentro del chroot, si se usa.

Consultar las anclas conocidas por Unbound

CONSULTA DIRECTA A UNA INSTANCIA IDENTIFICADA

```
RESOLVER=192.0.2.53
dig @"$RESOLVER" trustanchor.unbound CH TXT \
    +noall +nocomments +answer
```

SALIDA ILUSTRATIVA (NO EJECUTADA)

```
trustanchor.unbound. 0 CH TXT ". 20326 38696"
```

Buscar 38696. Una respuesta REFUSED no demuestra que falte la clave.

No basta encontrar el número dentro de un archivo

USAR EL ARCHIVO EFECTIVO DE LA INSTANCIA

```
ROOT_KEY=/var/lib/unbound/root.key
grep -E 'id = (20326|38696)' "$ROOT_KEY"
ls -ld "$(dirname "$ROOT_KEY")" "$ROOT_KEY"
```

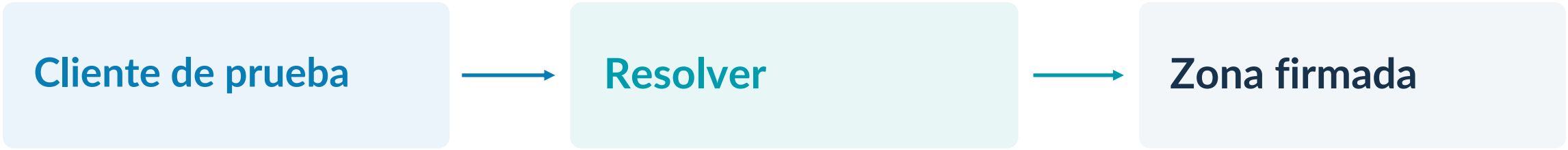
1. **Leer el estado, no solo la etiqueta**

   Comprobar que 38696 esté aceptada, no pendiente o revocada.

2. **Correlacionar archivo y proceso**

   Comparar lo guardado con la respuesta de la instancia en ejecución.

Preguntarle al resolver por un ancla concreta




```
root-key-sentinel-is-ta-38696
root-key-sentinel-not-ta-38696
```

El procesamiento especial requiere una respuesta previamente validada.

Consultar las dos variantes, con controles previos

EJEMPLO DE CONSULTA

```
RESOLVER=192.0.2.53
TEST_ZONE=ksk-test.net

dig @"$RESOLVER" \
  "root-key-sentinel-is-ta-38696.$TEST_ZONE" A +dnssec
dig @"$RESOLVER" \
  "root-key-sentinel-not-ta-38696.$TEST_ZONE" A +dnssec
```

Antes de la demo: verificar que la zona y ambos nombres para 38696 sean válidos.

Leer el par de respuestas, no una consulta aislada

is-ta-38696	not-ta-38696	Interpretación
Respuesta	**SERVFAIL**	Confía en la clave 38696.
SERVFAIL	**Respuesta**	No confía en 38696, si el control seguro funciona.
Respuesta	**Respuesta**	No demuestra soporte ni validación correctos.
SERVFAIL	**SERVFAIL**	Inconcluso: investigar validación y zona de prueba.

Tras el rollover, un ancla ausente puede impedir la validación previa y hacer fallar ambas consultas.

Dónde buscar problemas de actualización

Permisos o almacenamiento

El proceso aprende, pero no logra guardar el estado de forma duradera.

Contenedores e imágenes

Cada recreación vuelve al archivo inicial o a una instantánea antigua.

Equipos y software antiguos

Firmware o paquetes que no incorporan un ancla de arranque vigente.

Aprendizaje incompleto o manual

Equipos fuera de línea y anclas fijas sin un procedimiento de mantenimiento.

Obtener el ancla no es lo mismo que autenticarla

CONSULTA DEL REPOSITORIO OFICIAL

```
curl --fail --show-error --location --remote-name \
  https://data.iana.org/root-anchors/root-anchors.xml
```

Origen

IANA publica el conjunto de anclas y su firma.

Vigencia

Confirmar 38696 y los parámetros de la clave correcta.

Carga segura

Seguir el mecanismo autenticado del proveedor o del software.

Corregir la causa, sin apagar DNSSEC

BIND

Revisar paquete y ancla de arranque.

Recuperar la gestión de claves con el procedimiento de la versión instalada.

Unbound

Con copia del estado y servicio detenido, usar la herramienta de anclas con el usuario y la ruta adecuados.

No borrar el estado administrado ni reiniciar a ciegas como receta universal.

```
sudo -u unbound unbound-anchor \
  -a /var/lib/unbound/root.key
```

Después: comprobar ancla, registros y validación antes de devolver tráfico.

Comprobar también el próximo arranque

1. **Reinicio controlado**

   ¿El proceso conserva 38696 y sigue validando?

2. **Recreación de una instancia**

   ¿La imagen y el volumen preservan el estado correcto?

3. **Restauración de un respaldo**

   ¿Se vuelve a un ancla o configuración obsoleta?

Probar sobre una réplica o en una ventana acordada; no reiniciar toda la flota.

Hoy, esta semana y antes de los próximos hitos

Hoy

Inventariar las instancias.

Comprobar 38696.

Probar validación positiva y negativa.

Esta semana

Revisar persistencia e imágenes.

Correlacionar SERVFAIL, registros y reclamos.

Enero–marzo

Seguir los hitos previstos de revocación y retiro.

Repetir verificaciones y documentar resultados.

Posibles incidentes: globalsupport@icann.org · asunto: KSK Rollover

Seis comprobaciones para cerrar el ciclo operativo

Ancla activa

38696 aceptada en cada instancia.

Estado persistente

El aprendizaje sobrevive a reinicios.

Validación funcional

Controles positivos y negativos.

Sentinel con controles

Zona válida, soporte y respuestas coherentes.

Cobertura completa

Vistas, réplicas, contenedores y reserva.

Próximos hitos

Revocación y retiro bajo seguimiento.

Documentar resultados, evidencias y acciones correctivas.

DESPUÉS DEL ROLLOVER

38696.
Estado persistente.
Validación comprobada.

¿Preguntas?

Carlos Martínez · LACNIC
Nicolás Antoniello · ICANN