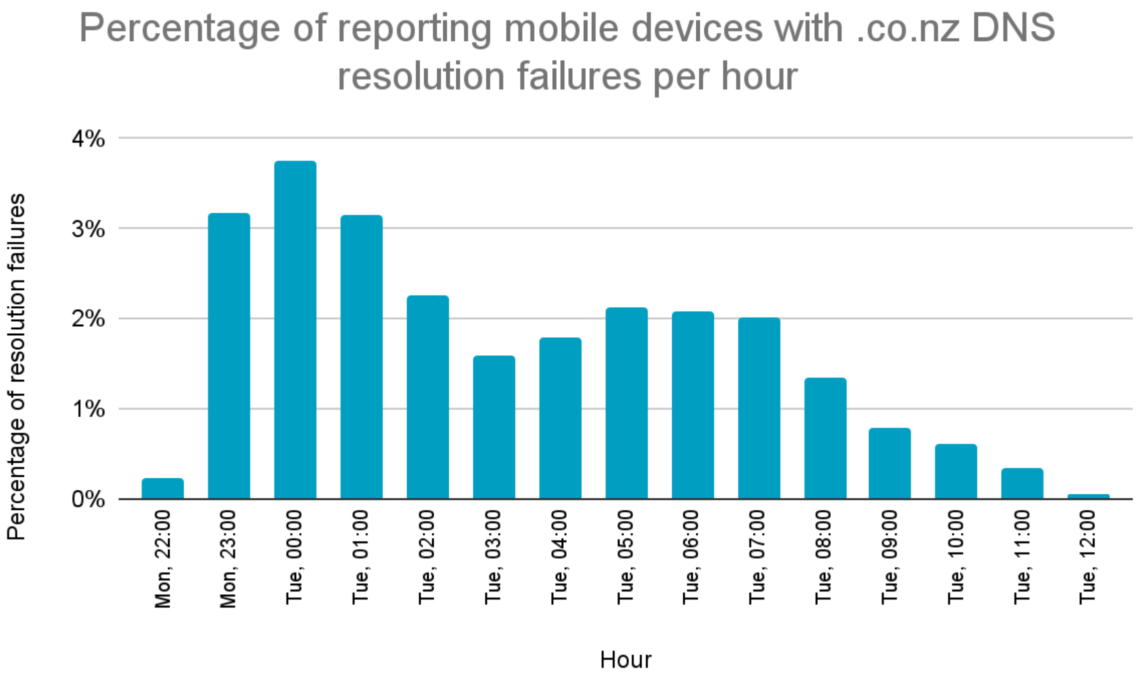
Technical incident report

Incident summary

On Monday, 29 May 2023, during a routine DNSSEC key rollover, we triggered a series of events that led to a subset of end users being unable to access domains at .ac.nz, .nz, .co.nz, .geek.nz, .gen.nz, .kiwi.nz, .maori.nz, .net.nz, .org.nz, .school.nz, .cri.nz, govt.nz, .health.nz, .iwi.nz, .mil.nz and .parliament.nz.

Issues for the domains under .ac.nz began following the zone push at 13:00 NZST. For domains under other registration levels, these issues will have begun following the zone push at 22:45 NZST.

Based on the information provided by third-party organisations, the majority of affected users were experiencing issues for approximately 13 hours between Monday, 29 May at 22:45 NZST to Tuesday, 30 May at 11:45 NZST. Our best estimation is that the incident affected an average of less than 2% of users across this timespan, with a short peak of around 5% at midnight.



Background

Domain Name System Security Extensions (DNSSEC) is a technology that provides an additional layer of trust on top of the Domain Name System (DNS) by verifying the authenticity of its responses. It uses cryptographic keys to sign DNS data — think of this as a seal of authenticity. In .nz, we completed our DNSSEC implementation in 2012.

The Key Signing Key (KSK) is one of these cryptographic keys and is used to sign the keys used to sign the DNS data.

A DNSSEC KSK rollover replaces an old KSK key with a new one. This is done annually in our systems to maintain the security of the DNSSEC system, as using one key for a long time can increase the risk of an attacker compromising that key.

When a KSK rollover happens, we need to ensure that:

1. Sufficient time has passed to ensure all systems expect the new key before switching to it.
2. After switching to the new key, we must retain the old key long enough to ensure no old (cached) records still reference it before removing it.

The latter of those two is where the issue occurred. The DNSSEC signing system removed the old key too early, triggering problems in third-party systems that believed their cached DNS data was untrusted because an unrecognised key signed it.

During a KSK rollover, the appropriate timing values differ depending on factors including:

- Rollover method — the chosen approach to rolling the key.
- DNS record Time To Live (TTL) configuration — how long the DNSKEY and Delegation Signer record (DS records) are valid in caches.
- Propagation time — how long the distribution of the new KSK takes across DNS servers.

In this case, the relevant factor is the DS record TTL — a KSK must be kept in retired state for at least twice the DS TTL:

- When we initially deployed DNSSEC, we used a 1-day DS TTL value, the documented value in our DNSSEC practice statement.
- In 2014, to reduce the impact on users of DNSSEC who suffered the loss of a KSK, we reduced the DS TTL to 1 hour.
- In 2018, we adjusted our DNSSEC configuration policy to reflect this reduced TTL, reducing the overall duration of the KSK rollover.
- On 1 November 2022, the InternetNZ Registry System (IRS) went live. Unlike our legacy zone-build process, this could not set an explicit

TTL on DS records, meaning DS records inherited the default zone TTL of 1-day.

Incident details

The specific events related to the incident for .ac.nz began on 29 May 2023 at 09:18 NZST when the new KSK became active and the old KSK moved to retired state.

Following existing policies, the old .ac.nz key transitioned into dead state at 12:55 NZST. This time was well beyond the known safety margin for our original one-hour DS TTL (approximately 11:33 NZST) but well short of the safety margin required for a new one-day DS TTL (approximately 9:33 NZST on Wednesday, 31 May). The changes were pushed to the zone at 13:00 NZST, triggering issues for some users of the .ac.nz domain.

For all other zones, the new keys became active between 12:55 NZST and 14:37 NZST based on their standard key lifecycles, and the older keys moved to retired state. Problems started after an automated lifecycle transitioned old keys into dead state at 22:45 NZST.

Due to the nature of the issue and the fact it occurred downstream in copies of data held in recursive nameservers, we were not immediately aware of the origin of the problem. Both internal and external monitoring and troubleshooting tools did not show any issues. It wasn't until an internal recursive system encountered the problem that we could get a cache dump to understand it fully.

Root cause

The technical root cause of this incident was a misalignment between the existing DNSSEC signing configuration policies and the resulting DS record TTL from the IRS zone build process. The legacy zone build process had an explicit TTL for DS records of one hour, while the IRS zone build process inherited the zone default TTL of one day.

This misalignment resulted in us prematurely removing the old DNSSEC KSK, causing problems for resolvers with cached records.

Known contributing factors

1. The new IRS zone generation process does not allow for setting a distinct TTL on DS records, preventing us from completely eliminating timing changes.
2. We were not aware that the DS TTL changes needed to be backported into our existing signing infrastructure and configuration policies.
3. Our automated testing for zone build results did not include comparing TTL, and our validation scenarios did not fully consider recursive servers.
4. The issue was not immediately apparent to our team since it occurred downstream in recursive nameservers, and no standard monitoring tools could detect it.

Lessons learned and next steps

Moving forward, we must carefully consider all changes and updates to our system and their potential impact on our operations.

1. The InternetNZ Council is commissioning an independent review to examine the events leading up to the incident, the response to the incident, and to make recommendations to prevent similar failures in the future. These outcomes will be made public.
2. Our DNSSEC signing configuration policies must be updated to reflect any changes to our zone build process.
3. Our testing methods for future changes will be revised to include a comparison of TTL for all record types, and validation scenarios should be extended to consider recursive servers.
4. We should revise our incident detection and monitoring systems for better visibility of potential issues.

We are taking this incident very seriously and working to make the necessary changes to prevent a similar occurrence.

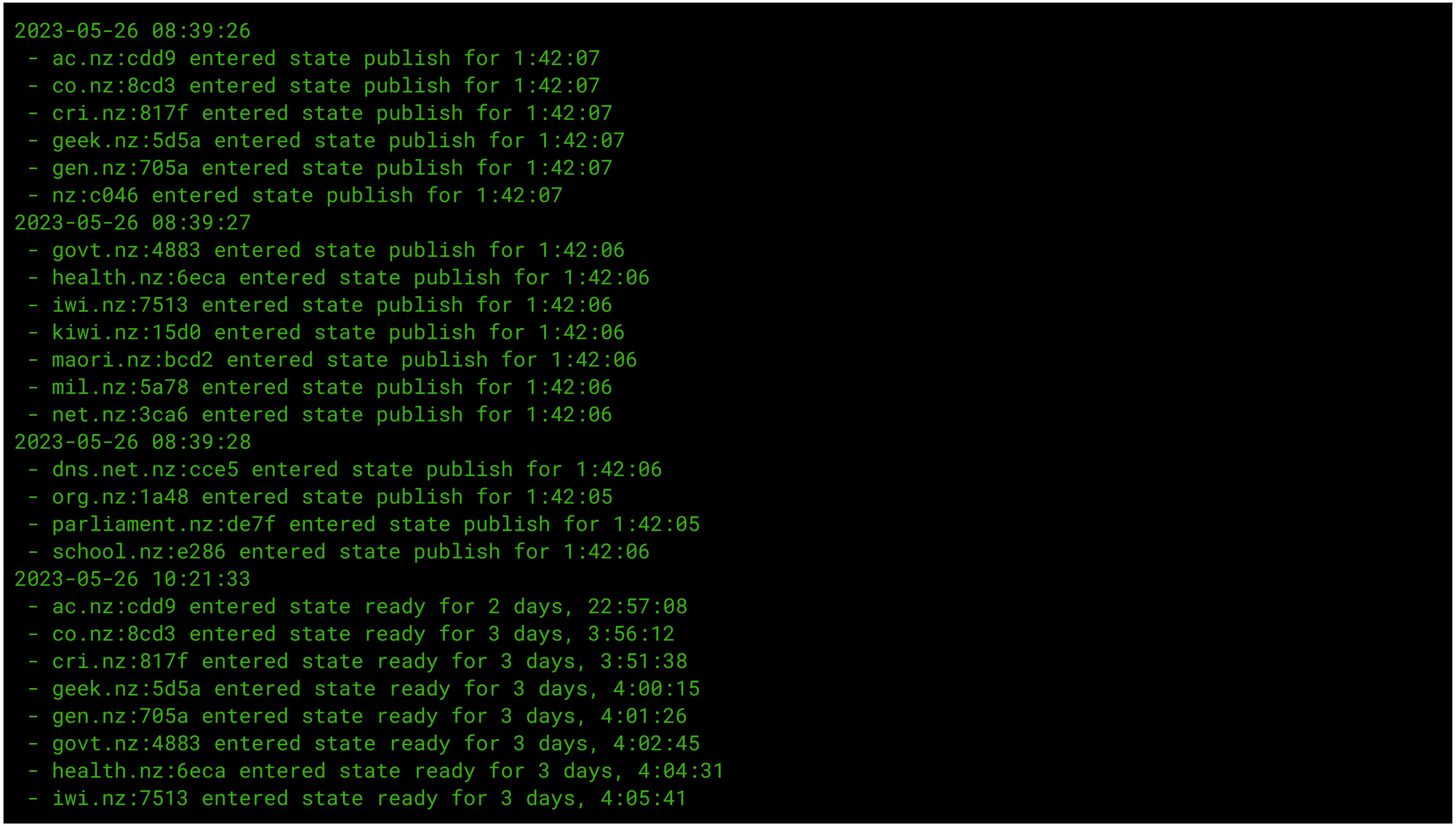
Glossary of terms

1. **DNSSEC (Domain Name System Security Extensions):** A set of protocols that add a layer of security to the DNS system, validating information with digital signatures to prevent attacks such as DNS spoofing.
2. **KSK (Key Signing Key):** A cryptographic key pair used in the DNSSEC protocol to sign the Zone Signing Key (ZSK) and its associated DNS records.

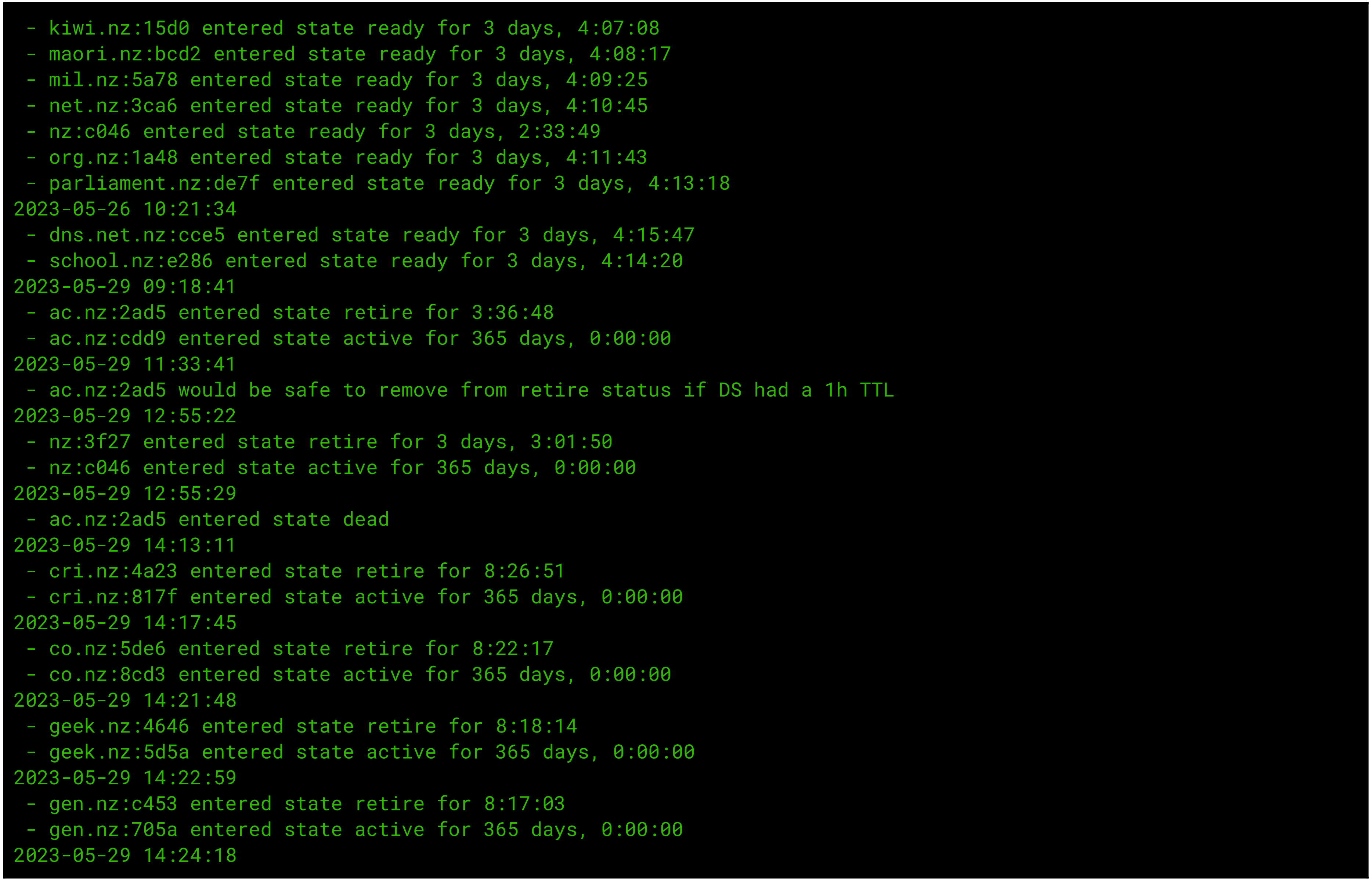
3. **Rollover:** The process of changing keys, in this case, the KSK.
4. **Zone push:** Updating the domain's zone file in DNS servers. This is when changes to the DNS records take effect. In .nz, this occurs every 15 minutes.
5. **NZST (New Zealand Standard Time):** The time zone for New Zealand outside of daylight savings: UTC+12:00.
6. **TTL (Time To Live):** A value in a DNS record that tells the resolver how long it may keep a copy of the record locally.
7. **DNSKEY:** A type of DNS record that holds a public key used to authenticate DNS responses in DNSSEC protocol. It can be one of two types: Zone Signing Keys (ZSK) and Key Signing Keys (KSK), each with specific signing responsibilities.
8. **DS record (Delegation Signer record):** A type of DNS record used in DNSSEC. It is placed in the parent zone to authenticate the DNSKEY record in the child zone.
9. **Cache:** A hardware or software component that stores data so that future requests for that data can be served faster.
10. **Key lifecycle:** The process a DNS key goes through from creation to use and retirement. In our case, we follow OpenDNSSEC's key life cycle of:
    a. **Generate**: This is the initial state of the key. OpenDNSSEC generates the cryptographic key pair (private and public keys).
    b. **Publish**: Once the keys are generated, they are published in the DNSKEY RRset, which is a part of the zone. At this stage, the keys are not yet used to sign anything. The purpose of the "publish" phase is to ensure that the key is propagated throughout the DNS infrastructure and cached before it is used for signing.
    c. **Ready**: The key enters the "ready" phase once it's been in the "published" phase for a period equivalent to the Pre-Publication interval defined in the policy. It means the key is ready to be used for signing.
    d. **Active**: In the "active" phase, the key is used for signing DNS records. The transition from "ready" to "active" is a smooth process, without any specific triggering event.
    e. **Retire**: The key enters the "retire" phase after being in the "active" phase for a period equivalent to the key's lifetime. The key is still published and used for signing, but a replacement key is generated and published in the zone (going through the "generate", "publish", and "ready" phases).
    f. **Dead**: After the new key is "active" and the old key has been in the "retire" phase for a period equivalent to the Retire Safety interval defined in the policy, the old key enters the "dead" phase. It is no longer used for signing and is not included in the zone.
11. **IRS:** The InternetNZ Registry System, the updated registry platform deployed on 1 November 2022 to replace the original .nz Shared Registry System (SRS) platform. IRS is based on the Canadian Internet Registration Authority (CIRA) Registry Platform.

12. **Recursive nameservers:** A type of DNS server that handles requests from client machines by providing answers from its own cache or by querying other DNS servers on behalf of the client.
13. **Resolver:** A software component on a device tasked with initiating and orchestrating queries for complete resolution of a sought-after resource, such as converting a domain name into its corresponding IP address.
14. **Backporting:** Taking parts from a newer system or software component and porting them to an older version.
15. **Downstream:** Refers to processes or activities that occur after a particular stage in a system or network.
16. **Zone-build process:** The process of creating or updating a DNS zone file, which includes the collection and formatting of domain information.

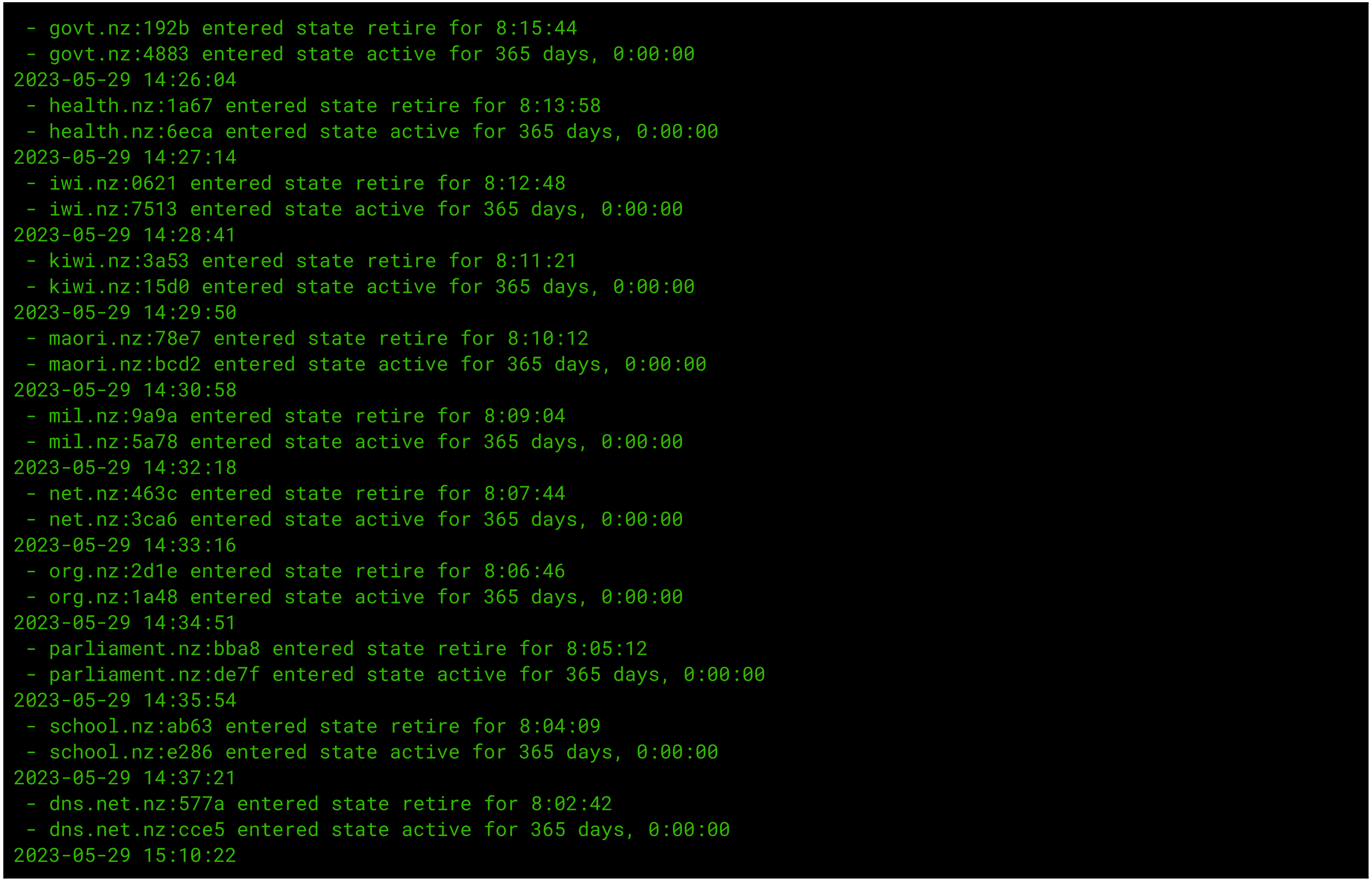
Appendix 1 - Key lifecycle changes during incident



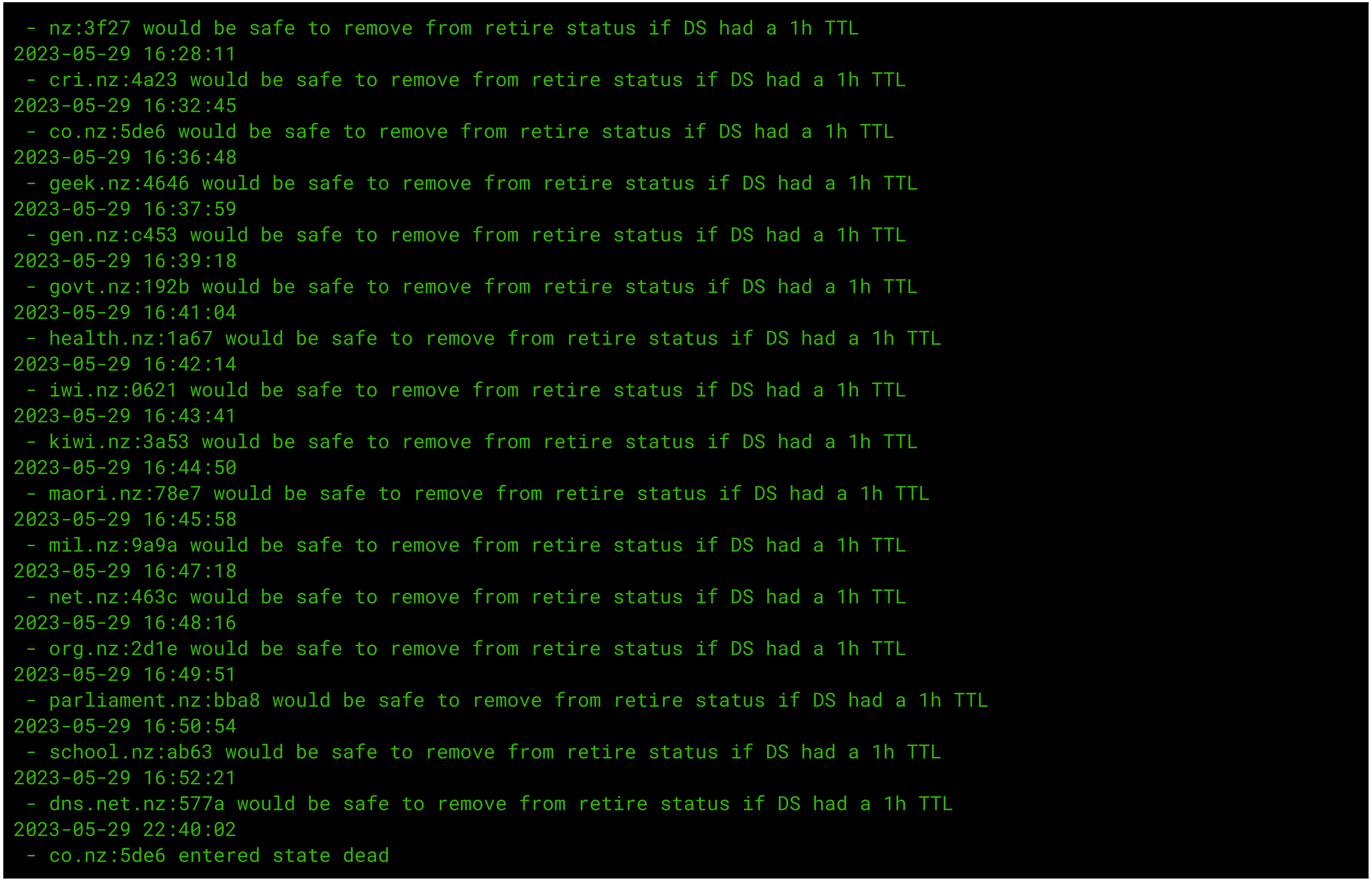
```
2023-05-26 08:39:26
 - ac.nz:cdd9 entered state publish for 1:42:07
 - co.nz:8cd3 entered state publish for 1:42:07
 - cri.nz:817f entered state publish for 1:42:07
 - geek.nz:5d5a entered state publish for 1:42:07
 - gen.nz:705a entered state publish for 1:42:07
 - nz:c046 entered state publish for 1:42:07
2023-05-26 08:39:27
 - govt.nz:4883 entered state publish for 1:42:06
 - health.nz:6eca entered state publish for 1:42:06
 - iwi.nz:7513 entered state publish for 1:42:06
 - kiwi.nz:15d0 entered state publish for 1:42:06
 - maori.nz:bcd2 entered state publish for 1:42:06
 - mil.nz:5a78 entered state publish for 1:42:06
 - net.nz:3ca6 entered state publish for 1:42:06
2023-05-26 08:39:28
 - dns.net.nz:cce5 entered state publish for 1:42:06
 - org.nz:1a48 entered state publish for 1:42:05
 - parliament.nz:de7f entered state publish for 1:42:05
 - school.nz:e286 entered state publish for 1:42:06
2023-05-26 10:21:33
 - ac.nz:cdd9 entered state ready for 2 days, 22:57:08
 - co.nz:8cd3 entered state ready for 3 days, 3:56:12
 - cri.nz:817f entered state ready for 3 days, 3:51:38
 - geek.nz:5d5a entered state ready for 3 days, 4:00:15
 - gen.nz:705a entered state ready for 3 days, 4:01:26
 - govt.nz:4883 entered state ready for 3 days, 4:02:45
 - health.nz:6eca entered state ready for 3 days, 4:04:31
 - iwi.nz:7513 entered state ready for 3 days, 4:05:41
```



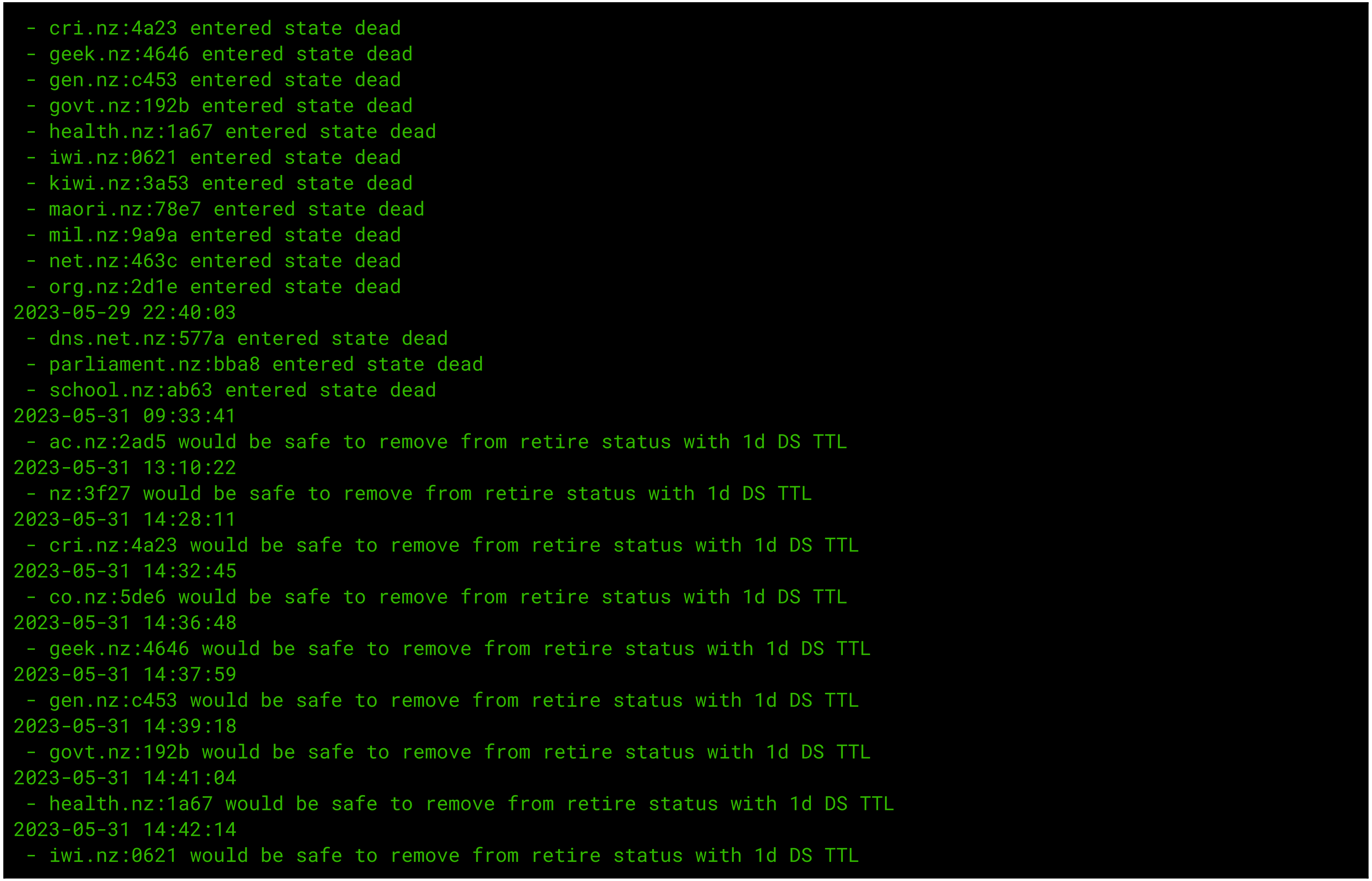
```
 - kiwi.nz:15d0 entered state ready for 3 days, 4:07:08
 - maori.nz:bcd2 entered state ready for 3 days, 4:08:17
 - mil.nz:5a78 entered state ready for 3 days, 4:09:25
 - net.nz:3ca6 entered state ready for 3 days, 4:10:45
 - nz:c046 entered state ready for 3 days, 2:33:49
 - org.nz:1a48 entered state ready for 3 days, 4:11:43
 - parliament.nz:de7f entered state ready for 3 days, 4:13:18
2023-05-26 10:21:34
 - dns.net.nz:cce5 entered state ready for 3 days, 4:15:47
 - school.nz:e286 entered state ready for 3 days, 4:14:20
2023-05-29 09:18:41
 - ac.nz:2ad5 entered state retire for 3:36:48
 - ac.nz:cdd9 entered state active for 365 days, 0:00:00
2023-05-29 11:33:41
 - ac.nz:2ad5 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 12:55:22
 - nz:3f27 entered state retire for 3 days, 3:01:50
 - nz:c046 entered state active for 365 days, 0:00:00
2023-05-29 12:55:29
 - ac.nz:2ad5 entered state dead
2023-05-29 14:13:11
 - cri.nz:4a23 entered state retire for 8:26:51
 - cri.nz:817f entered state active for 365 days, 0:00:00
2023-05-29 14:17:45
 - co.nz:5de6 entered state retire for 8:22:17
 - co.nz:8cd3 entered state active for 365 days, 0:00:00
2023-05-29 14:21:48
 - geek.nz:4646 entered state retire for 8:18:14
 - geek.nz:5d5a entered state active for 365 days, 0:00:00
2023-05-29 14:22:59
 - gen.nz:c453 entered state retire for 8:17:03
 - gen.nz:705a entered state active for 365 days, 0:00:00
2023-05-29 14:24:18
```



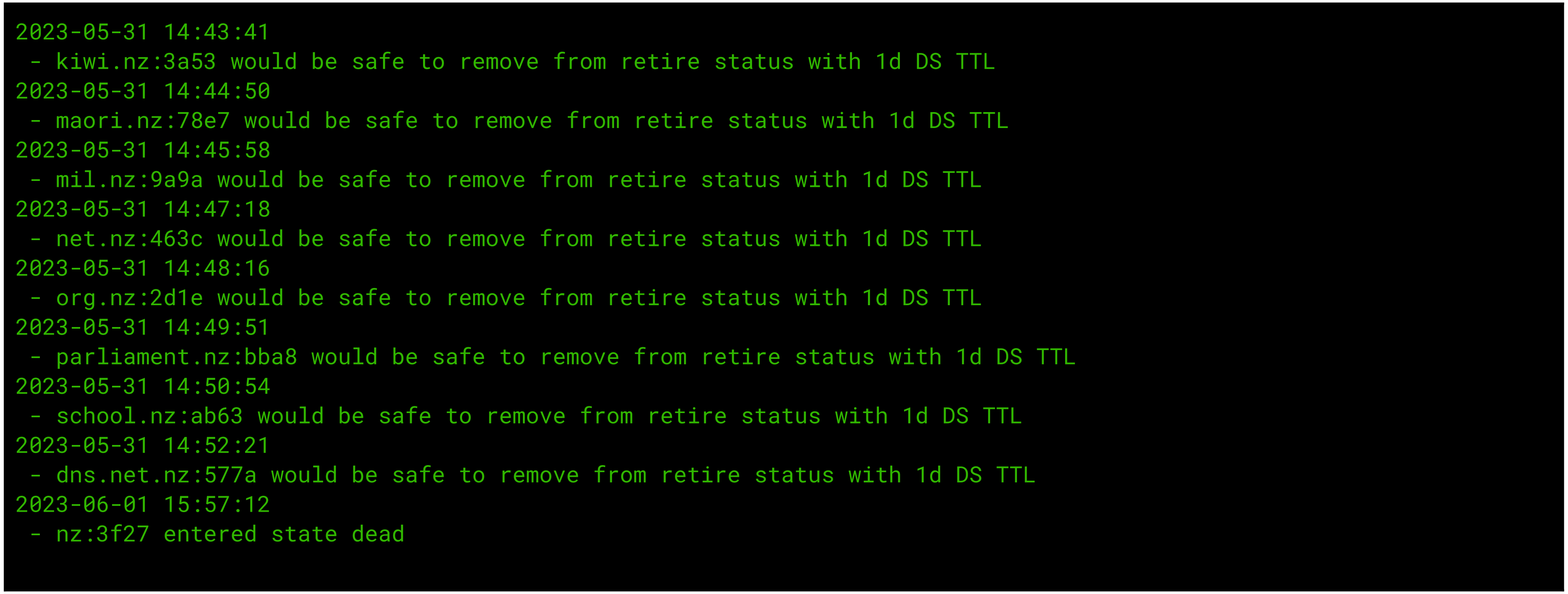
```
 - govt.nz:192b entered state retire for 8:15:44
 - govt.nz:4883 entered state active for 365 days, 0:00:00
2023-05-29 14:26:04
 - health.nz:1a67 entered state retire for 8:13:58
 - health.nz:6eca entered state active for 365 days, 0:00:00
2023-05-29 14:27:14
 - iwi.nz:0621 entered state retire for 8:12:48
 - iwi.nz:7513 entered state active for 365 days, 0:00:00
2023-05-29 14:28:41
 - kiwi.nz:3a53 entered state retire for 8:11:21
 - kiwi.nz:15d0 entered state active for 365 days, 0:00:00
2023-05-29 14:29:50
 - maori.nz:78e7 entered state retire for 8:10:12
 - maori.nz:bcd2 entered state active for 365 days, 0:00:00
2023-05-29 14:30:58
 - mil.nz:9a9a entered state retire for 8:09:04
 - mil.nz:5a78 entered state active for 365 days, 0:00:00
2023-05-29 14:32:18
 - net.nz:463c entered state retire for 8:07:44
 - net.nz:3ca6 entered state active for 365 days, 0:00:00
2023-05-29 14:33:16
 - org.nz:2d1e entered state retire for 8:06:46
 - org.nz:1a48 entered state active for 365 days, 0:00:00
2023-05-29 14:34:51
 - parliament.nz:bba8 entered state retire for 8:05:12
 - parliament.nz:de7f entered state active for 365 days, 0:00:00
2023-05-29 14:35:54
 - school.nz:ab63 entered state retire for 8:04:09
 - school.nz:e286 entered state active for 365 days, 0:00:00
2023-05-29 14:37:21
 - dns.net.nz:577a entered state retire for 8:02:42
 - dns.net.nz:cce5 entered state active for 365 days, 0:00:00
2023-05-29 15:10:22
```



```
 - nz:3f27 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:28:11
 - cri.nz:4a23 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:32:45
 - co.nz:5de6 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:36:48
 - geek.nz:4646 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:37:59
 - gen.nz:c453 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:39:18
 - govt.nz:192b would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:41:04
 - health.nz:1a67 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:42:14
 - iwi.nz:0621 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:43:41
 - kiwi.nz:3a53 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:44:50
 - maori.nz:78e7 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:45:58
 - mil.nz:9a9a would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:47:18
 - net.nz:463c would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:48:16
 - org.nz:2d1e would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:49:51
 - parliament.nz:bba8 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:50:54
 - school.nz:ab63 would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 16:52:21
 - dns.net.nz:577a would be safe to remove from retire status if DS had a 1h TTL
2023-05-29 22:40:02
 - co.nz:5de6 entered state dead
```



```
 - cri.nz:4a23 entered state dead
 - geek.nz:4646 entered state dead
 - gen.nz:c453 entered state dead
 - govt.nz:192b entered state dead
 - health.nz:1a67 entered state dead
 - iwi.nz:0621 entered state dead
 - kiwi.nz:3a53 entered state dead
 - maori.nz:78e7 entered state dead
 - mil.nz:9a9a entered state dead
 - net.nz:463c entered state dead
 - org.nz:2d1e entered state dead
2023-05-29 22:40:03
 - dns.net.nz:577a entered state dead
 - parliament.nz:bba8 entered state dead
 - school.nz:ab63 entered state dead
2023-05-31 09:33:41
 - ac.nz:2ad5 would be safe to remove from retire status with 1d DS TTL
2023-05-31 13:10:22
 - nz:3f27 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:28:11
 - cri.nz:4a23 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:32:45
 - co.nz:5de6 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:36:48
 - geek.nz:4646 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:37:59
 - gen.nz:c453 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:39:18
 - govt.nz:192b would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:41:04
 - health.nz:1a67 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:42:14
 - iwi.nz:0621 would be safe to remove from retire status with 1d DS TTL
```



```
2023-05-31 14:43:41
 - kiwi.nz:3a53 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:44:50
 - maori.nz:78e7 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:45:58
 - mil.nz:9a9a would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:47:18
 - net.nz:463c would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:48:16
 - org.nz:2d1e would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:49:51
 - parliament.nz:bba8 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:50:54
 - school.nz:ab63 would be safe to remove from retire status with 1d DS TTL
2023-05-31 14:52:21
 - dns.net.nz:577a would be safe to remove from retire status with 1d DS TTL
2023-06-01 15:57:12
 - nz:3f27 entered state dead
```