

Introduction to our authoritative DNS infrastructure

Yifan Bian

Aug 2024

Northwest A&F University

Table of Contents

Evolution

History

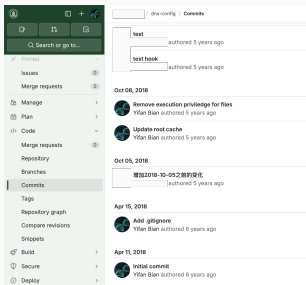
Modern Age

Incident Retrospect

- BIND9 on two servers (*ncs1* and *ncs2*)
- All changes happen directly on servers
 1. Make changes on *ncs1*
 2. *rndc reload* on *ncs1*
 3. *rsync* changes from *ncs1* to *ncs2*
 4. *rndc reload* on *ncs2*

Bronze Age

- On-premise GitLab CE `?.nwafu.edu.cn`
- DNS config (w/ zone files) being hosted on `?.nwafu.edu.cn/c**/dns-config`



- `git pull` on servers after commit

Start using web hook to do *git pull* and *rndc reload*

The screenshot displays the Iron Age web interface. On the left is a dark green sidebar with navigation icons and labels: Merge requests (0), Manage, Plan, Code, Build, Secure, and Deploy. The main content area has a breadcrumb trail: dns-config / Webhook Settings. A light blue banner below the breadcrumb states: "This is an archived project. Repository and other project resources are read-only." Below this is a search bar labeled "Search page". The section is titled "Webhooks" and includes a descriptive paragraph: "Webhooks enable you to send notifications to web applications in response to events in a group or project. We recommend using an integration in preference to a webhook." Under the heading "Project Hooks 4", there is a table of two webhooks. Each row shows a URL (http://61...:30000/git_hook and http://210...:30000/git_hook), "Push events", and "SSL Verification: disabled". To the right of each row are buttons for "Test", "Edit", and "Delete". An "Add new webhook" button is located at the top right of the table.

dns-config / Webhook Settings

This is an archived project. Repository and other project resources are read-only.

Search page

Webhooks

Webhooks enable you to send notifications to web applications in response to events in a group or project. We recommend using an [integration](#) in preference to a webhook.

Project Hooks 4 Add new webhook

http://61...:30000/git_hook	Push events	SSL Verification: disabled	Test	Edit	Delete
http://210...:30000/git_hook	Push events	SSL Verification: disabled	Test	Edit	Delete

A little summary

- Version control for config and zone data with *git*
Easy to trace or revert changes
- All servers pull config from *git*
Git repo is the source of truth
No *AXFR* or *IXFR* in picture
- Web hook to automatically deploy changes

- DNSSEC
- Pipelines
- Pull Requests and Validations

- Key life cycle management
- Sign zones
- Distribute signed zones to servers

Separating repositories

- `?.nwafu.edu.cn/nic/dnssec-keys`
- `?.nwafu.edu.cn/nic/dns-zones`
- `?.nwafu.edu.cn/nic/dns-config`

Pipelines

- *dnssec-keys* Manage key life cycle and rotation
A bunch of bash scripts
- *dns-zones* Sign zones, push signed files to servers, and trigger pipeline in *dns-config*
Triggered daily to keep signatures valid, even without a change
- *dns-config* Update servers with *git pull* and *rndc reload*

Prevent human errors in changes

- Protect *master* branch to prohibit direct push
- Require Pull Request to make changes
- Validate PR with *named-checkzone* and pipelines

Retrospective

- Allow more people to make changes to DNS zones, **c**** just need to review PRs, significantly made his life easier
- No way for bad commits in ***dns-zones*** to take down the service
dns-config is rarely changed and only managed by **c****, so not well protected yet. Consider adding some in future.
- Changes are automatically deployed to servers
- DNSSEC signed

Evolution

Incident Retrospect

Sep 2023: Automatic KSK rotation without DS updates

Mar 2024: Manual operation on servers broke the pipeline

Common mistakes in both incidents

Automatic Key Life Cycle Management

- 231 lines of bash scripts
 - Create new keys after "new key period"
 - Delete keys after "lifetime"
 - Send notification to GitLab Issues once new KSK is created
Contact CERNET to update DS record

Key type	Create new key after	Delete key after	Grace period
Key signing key	660 days	720 days	60 days
Zone signing key	90 days	100 days	10 days

Is it working?

Network Center / DNSSEC Keys / Commits / 419e92e7

Commit 419e92e7 authored 6 months ago by Yifan Bian

Browse files Options

Fix script and template file reference

parent db519894

Branches > Branches containing commit

No related merge requests found

Changes 2

Showing 2 changed files with 2 additions and 2 deletions

Hide whitespace changes Inline Side-by-side

View file @ 419e92e7

gitlab/keys-rotation.sh

```
@@ -66,7 +66,7 @@ function rotate_one_zone {
    create_time "${current_yshas}"
    #!
    if [ ! -z "${GITLAB_ACCESS_TOKEN}" ]; then
-       ./gitlab/create-gitlab-issue.py \
+       $SCRIPT_DIR/create-gitlab-issue.py \
        --project-id $CI_PROJECT_ID \
        --assignee-id $ISSUE_ASSIGNEE_ID \
        --token $GITLAB_ACCESS_TOKEN \
```

View file @ 419e92e7

gitlab/teams-cards/ksk-update.json

```
@@ -21,7 +21,7 @@
    },
    {
        "name": "密钥创建时间",
-       "value": "${creation_time}"
+       "value": "${creat_time}"
    }
}
```

Is anyone watching?

- Once every two years, who can remember?
- Don't delete if DS still points to the old key

The screenshot shows the Network Center interface for DNSSEC Keys. The left sidebar contains navigation links: Project, DNSSEC Keys, Pinned, Issues, Merge requests, Manage, Plan, Code, Merge requests, Repository, Branches, Commits, Tags, Repository graph, Compare revisions, Build, Secure, Deploy, Operate, Monitor, and Help.

The main content area displays the 'parent 29e2dect1' view. It shows a status bar indicating 'Pipeline #6112 passed with stage In 12 minutes and 4 seconds'. Below this, the 'Changes' section shows '2 changed files' with '12 additions and 1 deletion'. The diff view for the file 'glib/keys-rotation.sh' is shown, with line numbers 15 to 34. The script content is as follows:

```
15 15 16 16 17 17 18 18 19 19 20 20 21 21 22 22 23 23 24 24 25 25 26 26 27 27 28 28 29 29 30 30 31 31 32 32 33 33 34 34
```

```
@@ -15,11 +15,22 @@ function rotate_one_zone {  
    ZONE=$1  
    cd $ZONE_KEY_DIR/$ZONE  
    echo "> Rotating keys for $ZONE"  
  
    # DS records are managed in parent zones  
    # If a key is used as trust anchor, revoking it could cause outage  
    # So don't revoke a key specified in DS records  
    keys_in_ds=$(dig $ZONE DS +short | cut -d ' ' -f 1)  
  
    keys=$(ls *.key | sed 's/./key/')  
    # Check if keys are expired and revoke the expired ones  
    for x in $keys; do  
        key_expired $x.key  
        if [[ $? -eq 0 ]]; then  
            key_id=$(echo $x | cut -d -f3)  
            if printf '%s\n' "${keys_in_ds[@]}" | grep -Pass -- "$key_id"; then  
                echo "> $x has expired but still in DS record, cannot revoke this key. Please update DS records as soon  
                as possible."  
            else  
                continue  
            fi  
            echo "> $x has expired, discarding this key"
```

RRSIG Expired

```
# [redacted] in ~ [11:03:07]
$ dig @8.8.8.8 mx nwafu.edu.cn

; <<>> DiG 9.11.36-RedHat-9.11.36-11.0.1.an8 <<>> @8.8.8.8 mx nwafu.edu.cn
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 59830
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: ud: 512
; EDE: 7 (Signature Expired): (Expired RRSIG found for nwafu.edu.cn/mx (keytag=4, 82))
;; QUESTION SECTION:
;nwafu.edu.cn.                IN      MX

;; Query time: 110 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Apr 02 11:03:14 CST 2024
;; MSG SIZE rcvd: 100
```

But... Signing pipeline is running fine?





Q Search or go to...

Project

D DNS Zones

Pinned

Issues 0

Merge requests 0

Manage

Plan

Code

Build

Pipelines

Jobs

Pipeline editor

Pipeline schedules

Artifacts

Deploy

Monitor

Analyze

Settings

 Help

Network Center / DNS Zones / Pipelines

Passed 00:06:45 1 week ago	#6919 677 27e44c7a latest merge request		
Passed 00:00:29 1 week ago	Update hosts #6913 master 9886a68e scheduled		
Passed 00:00:27 1 week ago	Update hosts #6907 master 9886a68e		
Passed 00:00:03 1 week ago	Update hosts #6906 676 ad6dcec6 latest merge request		
Passed 00:00:27 1 week ago	Update hosts #6894 master 75119289		
Passed 00:00:05 1 week ago	Update hosts #6893 675 e8ad16e7 latest merge request		
Failed 00:00:41 1 week ago	#6889 master e292867b scheduled		
Passed 00:00:39 2 weeks ago	#6886 master e292867b scheduled		
Passed 00:00:40 2 weeks ago	#6883 master e292867b scheduled		

What went wrong?



Q Search or go to...

Project

DNS Config

Pinned

Issues 0

Merge requests 0

Manage

Plan

Code

Build

Pipelines

Jobs

Pipeline editor

Pipeline schedules

Artifacts

Secure

Deploy

Operate

Monitor

Analyze

Settings

Help

Network Center / DNS Config / Jobs / #14050

This job is archived. Only the complete pipeline can be retried.

Search job log

```
40 core/2.15/reference_appendices/interpreter_discovery.html for more information.
41 [WARNING]: Platform linux on host 210[REDACTED] is using the discovered Python
42 interpreter at /usr/bin/python3.6, but future installation of another Python
43 interpreter could change the meaning of that path. See
44 https://docs.ansible.com/ansible-
45 core/2.15/reference_appendices/interpreter_discovery.html for more information.
46 fatal: [61[REDACTED]]: FAILED! => {"ansible_facts": {"discovered_interpreter_python": "/usr/bin/python
3.6"}, "changed": true, "cmd": ["/usr/local/bin/git", "pull"], "delta": "0:00:00.003091", "end": "202
4-03-12 01:04:10.529534", "msg": "non-zero return code", "rc": 128, "start": "2024-03-12 01:04:10.526
443", "stderr": "fatal: detected dubious ownership in repository at '/chnamed/etc'\nTo add an excepti
on for this directory, call:\n\n\tgit config --global --add safe.directory /chnamed/etc", "stderr_lin
es": ["fatal: detected dubious ownership in repository at '/chnamed/etc'", "To add an exception for t
his directory, call:", "", "\tgit config --global --add safe.directory /chnamed/etc"], "stdout": "",
"stdout_lines": []}]
47 fatal: [210[REDACTED]]: FAILED! => {"ansible_facts": {"discovered_interpreter_python": "/usr/bin/python
3.6"}, "changed": true, "cmd": ["/usr/local/bin/git", "pull"], "delta": "0:00:00.002729", "end": "202
4-03-12 01:04:10.536097", "msg": "non-zero return code", "rc": 128, "start": "2024-03-12 01:04:10.533
368", "stderr": "fatal: detected dubious ownership in repository at '/chnamed/etc'\nTo add an excepti
on for this directory, call:\n\n\tgit config --global --add safe.directory /chnamed/etc", "stderr_lin
es": ["fatal: detected dubious ownership in repository at '/chnamed/etc'", "To add an exception for t
his directory, call:", "", "\tgit config --global --add safe.directory /chnamed/etc"], "stdout": "",
"stdout_lines": []}]
48 changed: [210[REDACTED]]
49 TASK [Update submodules] *****
50 changed: [210[REDACTED]]
51 TASK [Restart named] *****
52 changed: [210[REDACTED]]
53 PLAY RECAP *****
54 210[REDACTED] : ok=3 changed=3 unreachable=0 failed=0 skipped=0 rescued=0
ign[REDACTED]
55 210[REDACTED] : ok=0 changed=0 unreachable=0 failed=1 skipped=0 rescued=0
ign[REDACTED]
56 61[REDACTED] : ok=0 changed=0 unreachable=0 failed=1 skipped=0 rescued=0
ignored=0
57 Cleaning up project directory and file based variables
58 ERROR: Job failed: exit code 1
```

00:00

What went wrong?

最近一次成功在 3月10号，回忆一下那天是不是手动上去做了啥？

应该是升级 git 了。

Common mistakes in both incidents

- No offsite monitor to validate DNS functionality
- No alert to maintainers
- Relies on user report to trigger investigation

Takeaways

- Murphy's Law: Anything that can go wrong will go wrong
 - Never rely only on people
 - Robust testing + Continuous monitor
- Offsite backup and monitor
- Alerting and tracking system

Future improvements

- Server setup and updates are still manual
Automate with *cloud-init*?
- Combine *dns-config* and *dns-zone* repos
- Remove *git* on servers
Use web hook (or *ansible*) and download artifacts from
GitLab
- Rewrite DNSSEC Key management tool with Rust