УДК 681.12

В. О. Уманець

ВІДМОВОСТІЙКА FREEIPA СИСТЕМА

Вінницький національний технічний університет

Анотація

Розглянуто спосіб реалізації відмовостійкої централізованої системи з управління ідентифікацією користувачів - FreeIPA

Ключові слова: відмовостійка система, FreeIPA, DNS, SSSD, реплікація, dnsdist, Bind9, LDAP, fail2ban, Open Source, Linux.

Abstract

The method of implementation of a fail tolerant centralized system for managing user identification - FreeIPA.

Keywords: fault tolerant system, FreeIPA, DNS, SSSD, replication, dnsdist, Bind9, LDAP, fail2ban, Open Source, Linux.

Вступ

Висока доступність - це здатність системи уникати втрати сервісу, мінімізуючи час простою. Це виражається в термінах безперебійності роботи системи, як відсоток від загального часу роботи. Система FreeIPA оснащена власними функціями відмови, балансування навантаження та високою доступністю [1].

FreeIPA дозволяє реплікувати сервери в географічно розсіяних центрах обробки даних, щоб скоротити шлях між клієнтами та найближчим доступним сервером. Реплікація серверів дозволяє поширювати навантаження та масштабувати систему для більшої кількості клієнтів.

SSSD (System Security Services Daemon) отримує сервісні (SRV) записи ресурсів з серверів DNS, які клієнт автоматично виявляє. На основі записів SRV, SSSD підтримує список доступних серверів FreeIPA. Якщо один сервер FreeIPA переходить у режим офлайн або перевантажений, SSSD вже знає, з яким іншим сервером спілкуватися.

Опис системи

На рис. 1 продемонстрована відмовостійка та високодоступна система для клієнтської частини FreeIPA. При тестуванні було використано KVM для створення 2 віртуальних нод в одному кластері. На кожній ноді знаходиться 3 віртуальні машини: dnsdist, FreeIPA, Bind9.

Dnsdist - високоефективний балансувальник навантаження на DNS, задача якого - направляти трафік на найкращий сервер, забезпечуючи максимальну ефективність законним користувачам. IP адреси серверів dnsdist вказані як NS записи у Domain реєстратора. Сервери dnsdist балансують між собою навантаження по схемі “roundrobin” [2]. Краще мати як мінімум 2 таких рекурсори, які будуть перенаправляти запити зони example.com до серверів FreeIPA, а в разі їх недоступності - Bind9.

DNS Сервер Bind9 робить бекап DNS зон FreeIPA по протоколу IXFR (Incremental zone transfer) так часто, як вказано у SOA (Start of Authority) записі FreeIPA сервера [3]. Звичайно не потрібно забувати про DDOS атаки та поставити fail2ban для блокування IP адрес, які надсилають занадто багато запитів або налаштувати для цього dnsdist [4].

Якщо у налаштуваннях клієнта вказаний IP DNS рекурсора, але запит надходить не до зони example.com, то dnsdist перенаправляє запит до Google DNS.

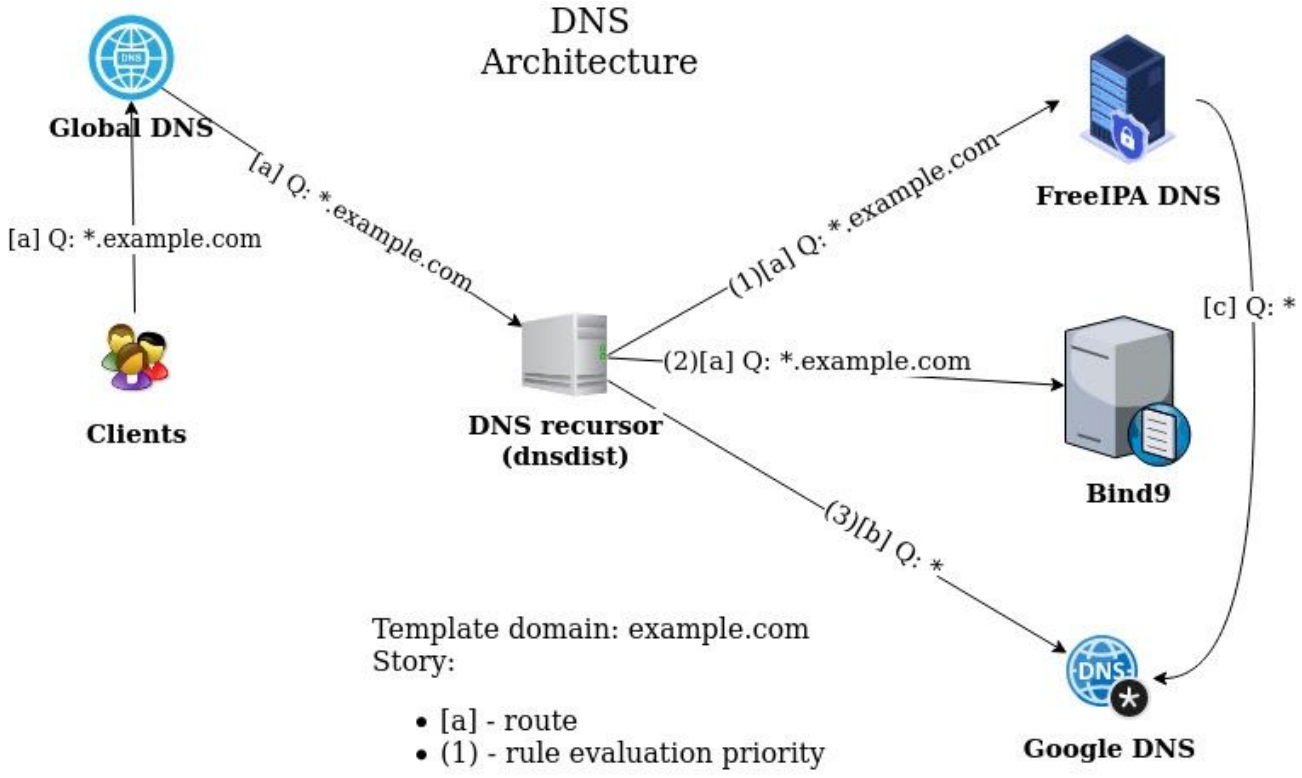

рис. 1 - Структура відмовостійкої клієнтської частини FreeIPA

Можливі маршрути запитів:

[a] - Клієнт має деякий глобальний сервер DNS у налаштуваннях і надсилає запит на сервер / сервіс * .examplet.com.

- Запит надсилається до глобальної системи DNS.

- Глобальний DNS пересилає запит на DNS рекурсор.
- DNS рекурсор запитує один із його бекендів FreeIPA або Bind9 на основі правил.
- Відповідь передається клієнтові вхідним ланцюжком.

[b] - Клієнт має DNS рекурсор у налаштуваннях і надсилає запит на сервер / сервіс не в зону example.com.

- Запит надсилається до DNS рекусора.
- DNS рекурсор пересилає запит на глобальний DNS.
- Відповідь передається клієнтові назал.

[c] - FreeIPA надсилає запит на що-небудь інше, ніж сервер / сервіс * .example.com.

- FreeIPA надсилає запит в Google DNS.
- Відповідь передається FreeIPA.

Висновки

FreeIPA повинна бути відмовостійка, так як це важлива система, що відповідає за авторизацію користувачів по LDAP для систем Linux/UNIX та містить вбудований DNS. Сервер FreeIPA зберігає дані про користувача, групи, хости та інші об’єкти, необхідні для управління аспектами безпеки мережі хостів. У даній публікації вказаний лише один з варіантів забезпечення відмовостійкості [5].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Високодоступніть ті відмовостійкість FreeIPA [Електронний ресурс] – Режим доступу: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/load-balancing
2. DNS recursor - dnsdist [Електронний ресурс] – Режим доступу: https://dnsdist.org
3. DNS сервер - Bind9 [Електронний ресурс] – Режим доступу: https://wiki.debian.org/Bind9
4. Програмне забезпечення для запобігання вторгнень - fail2ban [Електронний ресурс] – Режим доступу: http://www.fail2ban.org/wiki/index.php/Main_Page
5. Централізована система управління користувачами - FreeIPA [Електронний ресурс] – Режим доступу: https://www.freeipa.org/page/About

Уманець Владислав Олександрович — студент групи 1АКІТ-19м, факультет комп’ютерних систем та автоматики, Вінницький національний технічний університет, Вінниця, e-mail: umanets.vladyslav@gmail.com

Науковий керівник: ***Паламарчук Євген Анатолійович*** — кандидат технічних наук, доцент кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця

Umanets Vladyslav A. — Department of Computer Systems and Automatic, Vinnytsia National Technical University, Vinnytsia, e-mail : umanets.vladyslav@gmail.com

Supervisor: ***Palamarchuk Yevhen A.*** — PhD, Docent of Automatics and Informatics and Measurement Techniques Department, Vinnytsya National Technical University, Vinnytsia, email : p@vntu.edu.ua