УДК 004.77:004.056

А. О. Троян
І. В. Богач

АВТОМАТИЗОВАНА СИСТЕМА ЗБЕРЕЖЕННЯ РЕЗЕРВНИХ КОПІЙ КОНФІГУРАЦІЙ

Вінницький національний технічний університет

Анотація

У цій роботі розглядаються сучасні підходи до автоматизації процесів резервного копіювання налаштувань мережевого обладнання, що є критично важливим для забезпечення безперервності інфраструктурних процесів та підвищення загального рівня відмовостійкості комп'ютерних мереж. Основна увага приділяється розробці архітектури системи автономного збору даних та впровадженню методів версіонування текстових конфігурацій за допомогою систем контролю версій. Досліджуються технології безпечного криптографічного транспорту (SSH), механізми централізованого логування подій за допомогою демона rsyslog, а також алгоритми автоматичної ротації файлів для оптимізації дискового простору сервера.

Ключові слова: автоматизація, резервне копіювання, конфігурація пристроїв, Git-версіонування, SSH-транспорт, rsyslog, відмовостійкість інфраструктури.

Abstract

This paper examines modern approaches to automating backup processes for network equipment configurations, which is critically important for ensuring infrastructure continuity and increasing the overall fault tolerance of computer networks. The main focus is on developing the architecture of an autonomous data collection system and implementing version control methods for textual configurations using version control systems. Technologies of secure cryptographic transport (SSH), centralized event logging mechanisms via rsyslog daemon, and automatic file rotation algorithms to optimize server disk space are investigated.

Keywords: automation, backup, device configuration, Git versioning, SSH transport, rsyslog, infrastructure fault tolerance.

Вступ

Сучасні інформаційно-комунікаційні мережі є не просто важливою, а критичною складовою функціонування будь-якого підприємства, організації чи державної інфраструктури. Умови цифровізації та глобальної взаємодії бізнес-процесів підвищують залежність організацій від безперебійної роботи мережевих сервісів, оскільки будь-який збій може призвести до значних фінансових, репутаційних і операційних втрат. Зростання масштабу, складності та динамічності мережевих інфраструктур супроводжується значним збільшенням ризиків, пов’язаних із апаратними збоями, кібератаками, витоком конфіденційної інформації та помилками людського фактору.

Результати дослідження

Резервне копіювання є одним із ключових механізмів забезпечення надійності та безперервності функціонування інформаційних систем. Його основне призначення полягає у створенні копій даних, необхідних для відновлення працездатності системи після виникнення збоїв, втрати інформації, помилок користувачів, апаратних відмов або кіберінцидентів. Традиційно об'єктами резервного копіювання виступають файлові системи серверів, бази даних, операційні системи, віртуальні машини, прикладне програмне забезпечення та користувацькі дані. Для цього використовуються повні, диференціальні та інкрементні резервні копії, які зберігаються на локальних носіях, мережевих сховищах або в хмарних середовищах.

Класичні системи резервного копіювання орієнтовані переважно на роботу зі значними обсягами інформації, що можуть становити від десятків гігабайт до кількох терабайтів даних.

Відповідно, основна увага приділяється ефективному використанню дискового простору, швидкості передачі даних, стисненню інформації та мінімізації часу відновлення. У більшості випадків резервне копіювання виконується за розкладом із використанням спеціалізованих програмних комплексів, які підтримують централізоване керування процесом створення та зберігання резервних копій.

Разом з тим класичний підхід має низку обмежень під час застосування до мережевої інфраструктури. Насамперед він орієнтований на збереження даних, а не конфігурацій мережевого обладнання. У разі втрати налаштувань маршрутизатора, комутатора або міжмережевого екрана відновлення працездатності мережі може вимагати значного часу навіть за наявності повних резервних копій серверів. Крім того, традиційні системи резервного копіювання часто не забезпечують автоматичного контролю змін конфігурацій мережевих пристроїв, що ускладнює аудит виконаних налаштувань та пошук помилок, внесених адміністраторами.

Ще одним недоліком класичного підходу є недостатня гнучкість щодо роботи з великою кількістю мережевих пристроїв різних виробників. У багатьох випадках резервне копіювання конфігурацій виконується вручну або потребує використання окремих скриптів та утиліт. Це підвищує ймовірність людських помилок, збільшує навантаження на персонал та створює ризик втрати актуальної версії конфігурації. Особливо критичною така проблема стає для розподілених мереж, де кількість мережевих вузлів може становити десятки або сотні пристроїв.

З огляду на це виникає потреба у спеціалізованих механізмах резервного копіювання мережевого обладнання, які враховують особливості зберігання та відновлення конфігурацій, забезпечують автоматичний збір налаштувань, контроль версій та оперативне відновлення роботи мережевої інфраструктури після збоїв.

Висновок

Проведений аналіз підтвердив, що традиційні системи резервного копіювання є неефективними для мережевого обладнання, оскільки вони орієнтовані на великі обсяги даних, а не на специфіку й логіку текстових конфігурацій.Впровадження розробленої автоматизованої системи дозволяє вирішити ці обмеження завдяки таким факторам:Повна автономність: Використання планувальника cron та Bash-скриптів повністю усуває людський фактор і автоматизує збір налаштувань за розкладом.Прозорий аудит змін: Інтеграція системи Git забезпечує чітке версіонування конфігурацій, дозволяючи адміністратору миттєво бачити різницю (дельти) між версіями файлів.Безпека та оптимізація: Криптографічний транспорт SSH захищає дані під час передачі, демон rsyslog централізовано фіксує події, а алгоритми ротації запобігають переповненню диска.Загальний результат: Розроблений підхід мінімізує час відновлення мережі після аварій (RTO) та суттєво підвищує відмовостійкість усієї інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Nazarenko I. Linux Administration Fundamentals / I. Nazarenko. – Kyiv : IT Book Press, 2024.

2.Melnyk V. Network Infrastructure Security and Backup Systems / V. Melnyk. – Lviv : New World Publishing, 2025.

3.Stallings W. Network Security Essentials: Applications and Standards / W. Stallings. – 7th ed. – Boston : Pearson, 2024.

4.Nemeth E. UNIX and Linux System Administration Handbook / E. Nemeth, G. Snyder, T. Hein. – 6th ed. – Boston : Pearson, 2024.

5.Petrenko S. Automation of Network Administration Processes / S. Petrenko. Kharkiv : KhNURE Press, 2025.

6.Tkachenko O. Information Infrastructure Reliability and Disaster Recovery / O. Tkachenko. Kyiv : Polytechnic Publishing, 2024.

Троян Андрій Олександрович – студент групи АКІТ-22бз, кафедра автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: andreytroy@gmail.com

Богач Ілона Віталіївна – к.т.н., доцент, професор кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: ilona.bogach@gmail.com

Troyan Andrii Oleksandrovych – **s**tudent of group AKIT-22bz, Department of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: andreytroy@gmail.com

Bogach Ilona Vitaliivna – PhD, Professor of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: ilona.bogach@gmail.com