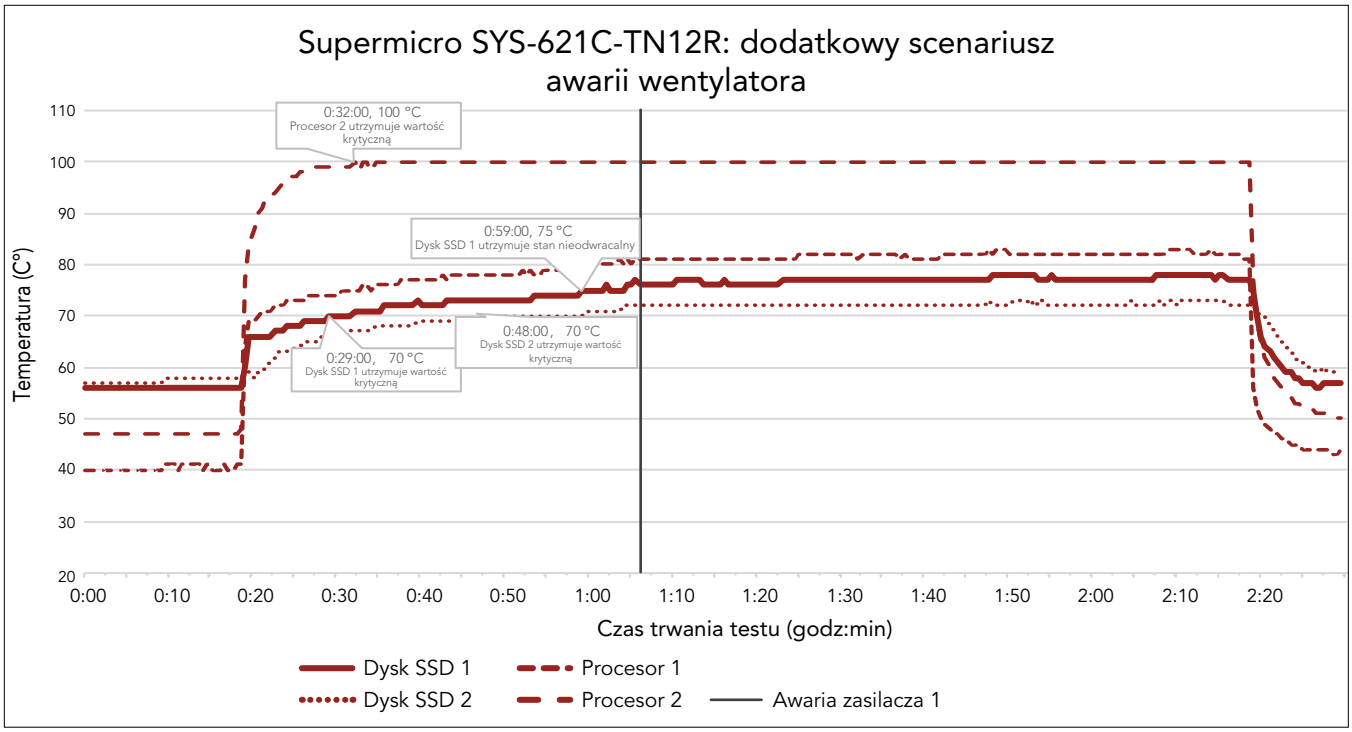
Tło naukowe raportu

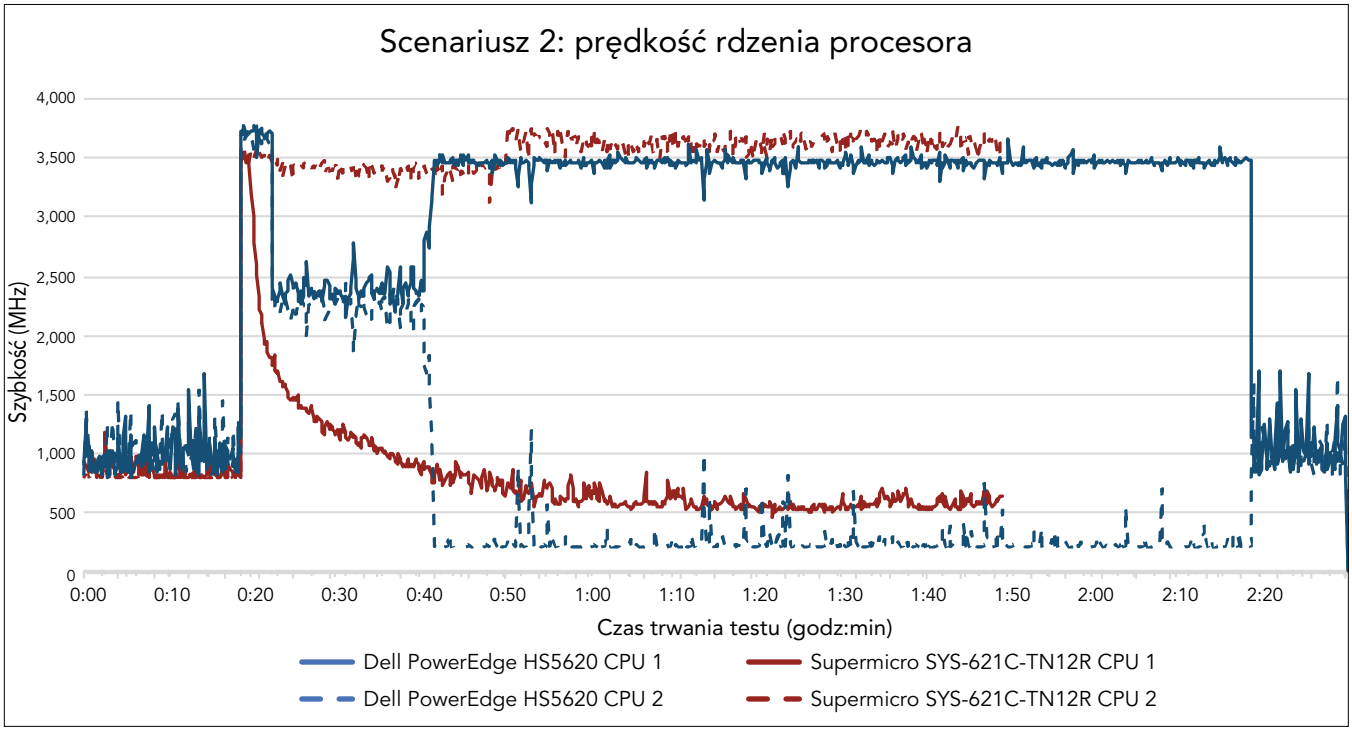
W tej sekcji podajemy nasze pełne wyniki i opisujemy rozwiązania, na których testowaliśmy oraz nasze metodologie testowe.

Testy praktyczne zakończyliśmy 9 kwietnia 2024 r. Podczas testów określiliśmy odpowiednie konfiguracje sprzętu i oprogramowania oraz zastosowaliśmy aktualizacje, gdy tylko stały się dostępne. Wyniki w tym raporcie odzwierciedlają konfiguracje, które sfinalizowaliśmy 11 marca 2024 r. lub wcześniej. W momencie pojawienia się niniejszego raportu te konfiguracje mogą nie reprezentować najnowszych dostępnych wersji.

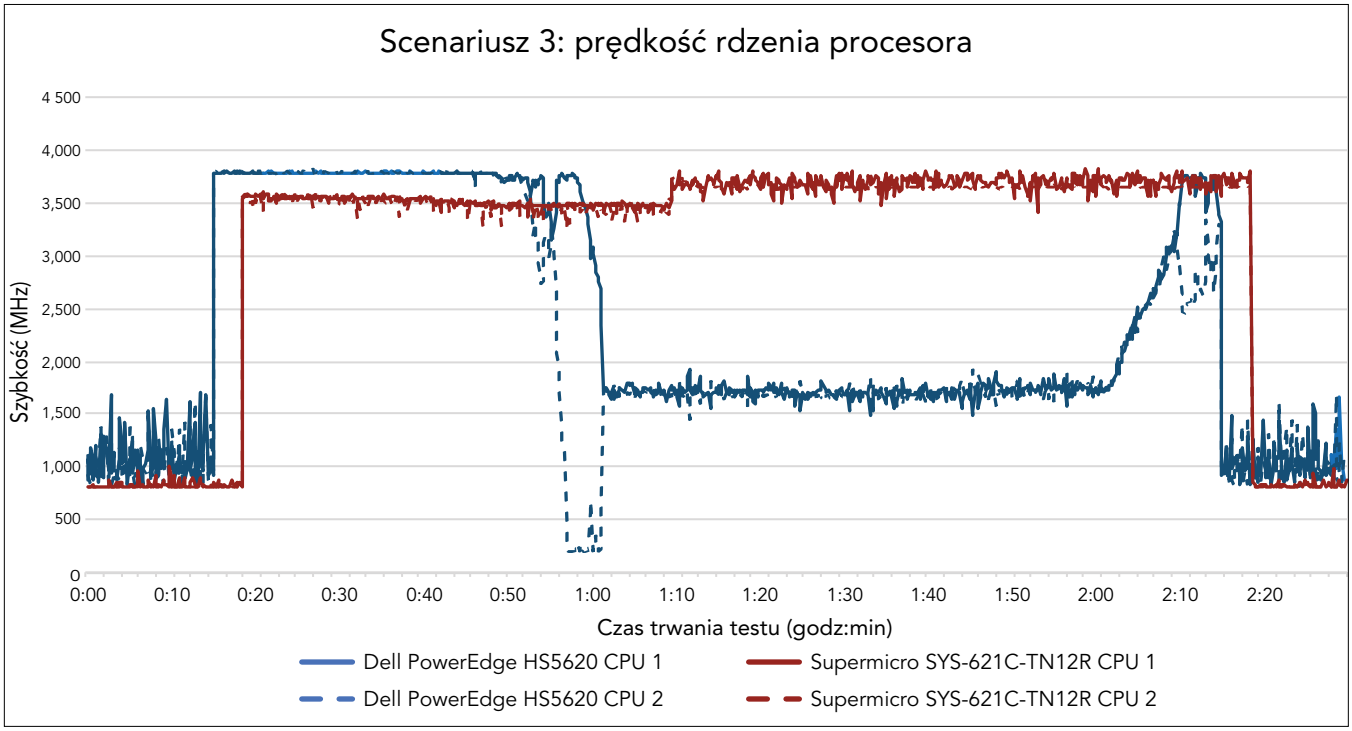
Wykresy



Rysunek 1. Temperatura dysku SSD i procesora w urządzeniu Supermicro® SYS-621C-TN12 podczas dodatkowego scenariusza awarii wentylatora, w którym serwer uruchamiał obciążenie zmiennoprzecinkowe przy wyłączonym wentylatorze 3. Obciążenie robocze rozpoczęło się o 0:15 i zakończyło o 2:15. Dysk SSD 1 uruchomił system operacyjny, podczas gdy dysk SSD 2 był bezczynny. Źródło: Principled Technologies.



Rysunek 2. Prędkość rdzeni procesorów Dell™ PowerEdge™ HS5620 i Supermicro SYS-621C-TN12 podczas pierwszego scenariusza awarii wentylatora. Obciążenie zmiennoprzecinkowe rozpoczęło się o 0:15 i zakończyło o 2:15. Źródło: Principled Technologies.



Rysunek 3. Prędkość rdzeni procesorów Dell PowerEdge HS5620 i Supermicro SYS-621C-TN12 podczas scenariusza nieprawidłowego działania systemu ogrzewania, wentylacji i klimatyzacji. Obciążenie zmiennoprzecinkowe rozpoczęło się o 0:15 i zakończyło o 2:15. Źródło: Principled Technologies.

Informacje o konfiguracji systemu

Tabela 1. Szczegółowe informacje o przetestowanych przez nas systemach.

Informacje o konfiguracji systemu	Dell PowerEdge HS5620	Supermicro SYS-621C-TN12R
Nazwa i wersja systemu BIOS	Dell 2.1.3	Supermicro 2.1
Inne niż domyślne ustawienia systemu BIOS	Performance Per Watt (OS)	Nie dotyczy
Nazwa systemu operacyjnego i numer wersji/ kompilacji	Ubuntu 22.04.3	Ubuntu 22.04.3
Data ostatnich zastosowanych aktualizacji/ poprawek systemu operacyjnego	11.03.2024	28.01.2024
Zasady zarządzania energią	Performance Per Watt (OS)	Zrównoważona wydajność
Procesor		
Liczba procesorów	2	2
Dostawca i model	Intel® Xeon® Gold 6444Y	Intel Xeon Gold 6444Y
Liczba rdzeni (na procesor)	16	16
Częstotliwość rdzenia (GHz)	3,60 (4,0 turbo)	3,60 (4,0 turbo)
Stopień zaawansowania jądra procesora (stepping)	8	8
Moduły pamięci		
Łączna ilość pamięci w systemie (GB)	1024	1024
Liczba modułów pamięci	16	16
Dostawca i model	Hynix® HMCG94AEBRA109N	SK Hynix HMCG94MEBRA123N
Pojemność (GB)	64	64
Typ	DDR5 DIMM	DDR5
Szybkość (MHz)	4 800	4 800
Szybkość działania w serwerze (MHz)	4 800	4 800
Kontroler pamięci masowej (przednia pamięć masowa)		
Dostawca i model	Dell HBA355i Adp	Supermicro MegaRAID AOC-S3916L-H16iR-32DD-P
Rozmiar pamięci podręcznej (GB)	0	8
Wersja oprogramowania układowego	24.15.14.00	5.240.02-3768
Wersja sterownika	Nie dotyczy	52.24.0-4766
Kontroler pamięci masowej (NVMe® M.2)		
Dostawca i model	Dell BOSS-N1 Monolithic	Nie dotyczy
Rozmiar pamięci podręcznej (GB)	0	Nie dotyczy
Wersja oprogramowania układowego	2.1.13.2025	Nie dotyczy
Lokalna pamięć masowa (system operacyjny)		
Liczba napędów	2	2
Dostawca i model dysku	Dell NVMe PE8010 RI M.2 960 GB	Micron® 7450 MTFDKBA960TFR

Informacje o konfiguracji systemu	Dell PowerEdge HS5620	Supermicro SYS-621C-TN12R
Rozmiar dysku (GB)	960	960
Informacje o dysku (prędkość, interfejs, typ)	Dysk SSD M.2 8 GT/s	PCIe® M.2 NVMe
Lokalna pamięć masowa (dane)		
Liczba napędów	12	12
Dostawca i model dysku	HGST HUH721212AL5200	WDC WUH721814ALE6L4
Rozmiar dysku (GB)	120 000	1400
Informacje o dysku (prędkość, interfejs, typ)	Dysk twardy SAS 3,5" 12 Gb/s	Dysk twardy SATA 3,5" 6 Gb
Karta sieciowa A		
Dostawca i model	4x Intel 25G 2P E810-XXV	3x Intel E810-XXVAM2 (AOC-S25GC-i2S)
Liczba i typ portów	2x 25 Gb	2x 25 Gb
Wersja sterownika	22.5.7	4.20 (0x800177B4)
Karta sieciowa B		
Dostawca i model	1x Broadcom® NetXtreme Gigabit Ethernet (BCM5720)	1x Intel E810-XXVAM2 (AOC-A25G-i2SM)
Liczba i typ portów	2x 1 Gb	2x 25 Gb
Wersja sterownika	22.71.3	4.30 (0x800177B4)
Wentylatory chłodzące		
Liczba, dostawca, model	1x Dell HPR Gold 5x Dell HPR Silver	3 środkowe wentylatory Supermicro FAN-0206L4
Zasilacze		
Dostawca i model	Dell 05222NA00	Supermicro PWS-1K23A-1R
Liczba zasilaczy	2	2
Moc jednego urządzenia (W)	1 800	1 200

Sposób testowania

Aby stworzyć środowisko, w którym mogliśmy kontrolować i mierzyć temperaturę, zbudowaliśmy niestandardową obudowę wokół całkowicie załadowanej szafy serwerowej 42U. Przetestowaliśmy systemy Dell i Supermicro w tym samym miejscu w szafie serwerowej i sprawdziliśmy temperaturę wewnętrzną serwerów w trzech typach scenariuszy. Przeprowadziliśmy test porównawczy stress-ng na serwerach w szafie serwerowej w czterech falach, w odstępie 1 minuty i 10 sekund. Testowane przez nas systemy Dell i Supermicro uruchomiły obciążenie robocze w czwartej fali, zaczynając 3 minuty i 30 sekund po uruchomieniu obciążenia roboczego przez pierwsze serwery. Poniżej przedstawiamy kroki, które podjęliśmy, aby skonfigurować i przeprowadzić testy.

Instalowanie i konfigurowanie systemu Ubuntu 22.04.3

1. Przeprowadź rozruch z nośnika Ubuntu 22.04.3.
2. Wybierz opcję Try or Install Ubuntu Server.
3. W menu języka pozostaw wartości domyślne i wybierz opcję Done.
4. Wybierz opcję Update to the new installer.
5. W konfiguracji klawiatury pozostaw wartości domyślne i wybierz opcję Done.
6. W typie instalacji pozostaw wartości domyślne i kliknij przycisk Done.
7. W menu połączeń sieciowych pozostaw wartości domyślne i wybierz opcję Done.
8. Na ekranie konfiguracji proxy pozostaw wartości domyślne i wybierz opcję Done.
9. Na ekranie konfiguracji kopii lustrzanej archiwum Ubuntu poczekaj na zakończenie testu, a następnie wybierz opcję Done.
10. Na ekranie konfiguracji pamięci masowej pozostaw wartości domyślne i wybierz opcję Done.
11. Na ekranie podsumowania konfiguracji pamięci masowej pozostaw wartości domyślne i wybierz opcję Done.
12. Aby potwierdzić destrukcyjne działanie, wybierz opcję Continue.
13. Na ekranie konfiguracji profilu, w obszarze Your name and Username, wprowadź `ptuser`. W obszarze Your servers name wprowadź nazwę i potwierdź hasło.
14. Wybierz opcję Done.
15. Na ekranie uaktualnienia do systemu Ubuntu Pro pozostaw wartości domyślne i wybierz opcję Continue.
16. Na ekranie konfiguracji SSH wybierz opcję Install OpenSSH server i wybierz opcję Done.
17. Na ekranie obsługiwanych snapów serwerowych pozostaw wartości domyślne i wybierz opcję Done.
18. Po zakończeniu instalacji wybierz opcję Reboot now.
19. Zaloguj się do systemu Ubuntu przy użyciu powyższych poświadczeń.
20. Aktualizacje procesów:

```
sudo apt update
sudo apt upgrade
```

21. Zainstaluj narzędzia CIFS i zmapuj udział PT:

```
sudo apt install cifs-utils
sudo mkdir /mnt/pt-data01
sudo mount -t cifs //10.41.1.21/pt /mnt/pt-data01/ -o “rw,user=<konto_użytkownika>,pass=<hasło>”
```

22. Skonfiguruj sieć:

```
sudo cp /etc/netplan/*.yaml /etc/netplan/00-installer-config.yaml.bak
sudo nano /etc/netplan/*.yaml
```

23. Zidentyfikuj żądaną kartę sieciową i dokonaj następujących zmian:

```
addresses:
  - <adres_IP>/<CIDR>
routes:
  - to: default
    via: <brama_domyślna>
nameservers:
    search: [<serwer_nazw1>, <serwer_nazw2>]
    addresses: [<DNS_IP1>, <DNS_IP2>, <DNS_IP3>]
```

24. Przetestuj i zastosuj zmieniony plik:

```
sudo netplan try
sudo netplan apply
```

25. Ustaw nazwę hosta:

```
sudo hostnamectl set-hostname <nowa_nazwa_hosta>
```

26. Uruchom ponownie hosta:

```
sudo shutdown -r now
```

Wdrażanie sudo bez hasła

Wdrażanie po stronie klienta

1. Edytuj plik sudoers:

```
sudo visudo /etc/sudoers
```

2. Dodaj poniższe na samym końcu pliku:

```
ptuser ALL=(ALL:ALL) NOPASSWD: ALL
```

Wdrażanie po stronie kontrolera

1. Wygeneruj parę kluczy SSH:

```
ssh-keygen -t rsa -b 4096 -N "" -f "$HOME/.ssh/id_rsa.pub"
```

2. Skopiuj klucz publiczny SSH do każdego serwera zdalnego:

```
ssh-copy-id ptuser@<adres_IP_serwera_zdalnego>
```

Implementacja stosu TIG-P do zbierania danych

Konfigurowanie programu Docker

1. Zaloguj się do rejestratora jako ptuser.
2. Przygotowanie do instalacji programu Docker:

```
sudo apt update
sudo apt install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
```

3. Dodaj repozytorium do źródeł Apt i zainstaluj:

```
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.
```

```
docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

Konfiguracja stosu TIG Huntabyte

1. W rejestratorze sklonuj repozytorium tig-stack:

```
git clone https://github.com/huntabyte/tig-stack.git
```

2. Edytuj plik .env do wdrożenia:

```
sudo nano tig-stack/.env
```

3. W przypadku FluxDB wypełnij nazwę użytkownika, hasło, organizację, zasobnik i okres przechowywania w następujący sposób:

```
DOCKER_INFLUXDB_INIT_USERNAME: admin
DOCKER_INFLUXDB_INIT_Password: <hasło>
DOCKER_INFLUXDB_INIT_ORG: PT
DOCKER_INFLUXDB_INIT_BUCKET: <nazwa_zasobnika>
DOCKER_INFLUXDB_INIT_RETENTION: 52w
```

4. Wygeneruj losowy 32-znakowy ciąg szesnastkowy za pomocą poniższego polecenia i wprowadź wynik tokenu administratora w pliku .env:

```
openssl rand -hex 32
```

5. Zapisz i wyjdź.
6. Edytuj plik telegraf.conf:

```
sudo nano tig-stack/telegraf/telegraf.conf
```

7. Ustaw następujące wartości:

```
services:
  influxdb:
    image: influxdb
  telegraf:
    image: gibletron/telegraf-ipmitool
  grafana:
    image: grafana/grafana-oss
    links:
      - prometheus
```

8. Zapisz i wyjdź.
9. Uruchom Docker compose (headless/detached):

```
sudo docker-compose up -d
```

10. Na każdym serwerze, który chcesz monitorować, uruchom następujące polecenie:

```
sudo apt install telegraf
```

11. Aby otworzyć interfejs zarządzania InfluxDB, przejdź do adresu IP hosta InfluxDB z portem 8086.

12. W razie potrzeby utwórz tokeny interfejsu API, zapisując je przed zamknięciem okna.
13. W obszarze Load Data kliknij pozycję API Tokens, a następnie Generate API Token.
14. Na każdym serwerze, który chcesz monitorować, edytuj plik /etc/telegraf/telegraf.conf w następujący sposób:

```
[[outputs.influxdb_v2]]
  urls = ["<adres_IP_influxDB>:8086"]
  token = "<token_API>"
  organization = "PT"
  bucket = "<nazwa_zasobnika>"
```

15. W każdym testowanym systemie dodaj poniższe:

```
[[inputs.intel_powerstat]]
  cpu_metrics = ["cpu_frequency"]
```

16. Zapisz i wyjdź.
17. Uruchom ponownie Telegraf:

```
sudo systemctl restart telegraf
```

Konfigurowanie rozwiązania Prometheus

1. Dodaj poniższe do /home/ptuser/tig-stack/docker-compose.yml:

```
prometheus:
  image: prom/prometheus:latest
  volumes:
    - ${PROM_CFG_PATH}:/etc/prometheus/prometheus.yml
    - prom-storage:/prometheus
  ports:
    - 9090:9090
volumes:
  prom-storage:
```

2. Zapisz i wyjdź.
3. Edytuj plik .env i dodaj poniższe:

```
PROM_CFG_PATH=./prometheus/prometheus.yml
```

4. Zapisz i wyjdź.
5. Na każdym serwerze, który chcesz monitorować, uruchom następujące polecenie:

```
sudo apt install dbus prometheus-node-exporter prometheus-node-exporter-collectors -y
```

6. W każdym testowanym systemie uruchom następujące polecenie:

```
sudo apt install prometheus -y
```

7. Aby utworzyć zadanie monitorowania w Prometheus, dodaj następujące elementy do /home/ptuser/tig-stack/prometheus/prometheus.yml:

```
- job_name: "<własna_nazwa>"
  static_configs:
    - targets: ["<adres_IP_komputera_docelowego:9090>"]
```

8. Dodaj dodatkowe zadania i/lub cele, tworząc dodatkowe wpisy podobne do kroku 7. Można dodać inne obiekty docelowe dla tego samego zadania jako inny wiersz celu.
9. Zapisz i wyjdź.

Testowanie za pomocą stress-ng

W każdym scenariuszu testowym wykonaliśmy następujące kroki, aby uruchomić obciążenie zmiennoprzecinkowe stress-ng.

1. Na każdym serwerze uruchom następujące polecenie:

```
sudo apt install stress-ng linux-tools-generic -y
```

2. Na każdym testowanym serwerze uruchom następujące polecenia:

```
sudo modprobe rapl
sudo modprobe intel_rapl_common
sudo modprobe intel_rapl_msr
sudo modprobe msr
sudo modprobe intel-uncore-frequency
sudo setcap cap_sys_rawio,cap_dac_read_search,cap_sys_admin+ep /usr/bin/telegraf
sudo chmod -R a+rx /sys/devices/virtual/powercap/intel-rapl/
```

3. Na każdym testowanym serwerze przejdź na stronę *https://github.com/andikleen/pmu-tools/blob/master/event_download.py*, pobierz plik raw i uruchom go:

```
sudo chmod +x event_download.py
./event_download.py
```

4. Na kontrolerze zainstaluj PSSH:

```
sudo apt install pssh -y
```

5. Na kontrolerze utwórz pliki, które zostaną wykorzystane podczas wykonywania stress-ng:

```
sudo touch ~/.pssh_hosts_file
sudo touch ~/.pssh_hosts_file_wave1
sudo touch ~/.pssh_hosts_file_wave2
sudo touch ~/.pssh_hosts_file_wave3
sudo touch ~/.pssh_hosts_file_wave4
```

6. Edytuj plik ~/.pssh_hosts_file i wprowadź wszystkie adresy IP serwera po jednym w każdym wierszu.
7. Edytuj pliki od ~/.pssh_hosts_file_wave1 do ~/.pssh_hosts_file_wave4 i wprowadź odpowiednio jedną czwartą adresów IP w każdym pliku.
8. Sprawdź, czy wszystkie serwery są w trybie online i reagują na polecenia zdalne:

```
sudo pssh -i -h ~/.pssh_hosts_file uptime
```

9. Na kontrolerze utwórz folder dziennika dla testu stress-ng:

```
sudo mkdir /var/log/stress-ng
sudo chmod 777 /var/log/stress-ng
```

10. Wykonaj test za pomocą poniższych poleceń, edytując „wave1" z odpowiednim numerem fali.

```
pssh -i -h ~/.pssh_hosts_file_wave1 sudo stress-ng --cpu 4 --matrix 0 --cpu-method matrixprod --mq
4 --hdd 6 --tz --metrics --perf --times --aggressive -t 2h --log-file /var/log/stress-ng/$(date
+'%Y%m%d_%H%M%S').log
```

Zobacz oryginalną, angielską wersję tego raportu na stronie *https://facts.pt/gPS09my*

Projekt ten został zlecony przez Dell Technologies.

Principled Technologies®

Facts matter.®