

Monitorowanie komputerów w pracowni

Czas: 2 × 45 min

praca w parach

Cel: Zbudowanie prostego systemu monitorowania dostępności komputerów i usług, przetestowanie powiadomień na symulowanej awarii i opracowanie procedury reakcji na awarię.

Po zajęciach potrafisz:

- konfiguruje monitory typu ping, port TCP i HTTP w Uptime Kuma
- tworzy stronę stanu usług i konfiguruje powiadomienie
- symuluje awarię usługi, mierzy czas wykrycia i przywraca działanie
- odczytuje bieżące obciążenie serwera w Glances
- opracowuje procedurę reakcji na awarię

Sprzęt i materiały

- komputer stacjonarny z VM Ubuntu Server (z zadań 10–12 i 27; tryb mostkowany)
- maszyna wirtualna Windows 11 lub komputer partnera jako monitorowane urządzenie
- telefon (opcjonalnie — odbiór powiadomień)

Oprogramowanie

- **Uptime Kuma** — kontener z zadania 27, panel `http://<IP VM>:3001`
github.com/louislam/uptime-kuma
- **Glances** — `sudo apt install glances`;
tryb WWW: `glances -w`
github.com/nicolargo/glances
- **ntfy** — **opcjonalnie** — powiadomienia na telefon; aplikacja Android/iOS, bez zakładania konta
ntfy.sh
- **Netdata** — **opcjonalnie** — rozbudowane wykresy wydajności; dla chętnych
netdata.cloud

Przygotowanie przed zajęciami

- Sprawdź, że w VM Ubuntu Server działa kontener Uptime Kuma (`docker compose ps` w `~/kuma`) oraz usługi `ssh`, `smbd` i Jellyfin (jeśli instalowałeś go w zadaniu 12).
- Zapisz adresy IP: VM Ubuntu Server, VM Windows lub komputera partnera.

Bezpieczeństwo

- Monitoruj tylko własne maszyny wirtualne i komputer partnera za jego zgodą — skanowanie i odpytywanie cudzych urządzeń w sieci szkolnej jest zabronione.
- Regułę zapory zezwalającą na ping włączaj tylko w maszynie wirtualnej.
- W ntfy publiczny temat może odczytać każdy, kto zna jego nazwę — wybierz trudną do odgadnięcia nazwę i nie wysyłaj w powiadomieniach haseł ani adresów spoza pracowni.
- Awarię symuluj tylko zatrzymaniem usługi w swojej VM — nie wyłączaj sprzętu sieciowego ani serwera szkolnego.

Przebieg zadania

1 Monitory w Uptime Kuma

1. W VM Windows włącz odpowiedź na ping: w PowerShell (administrator) `Enable-NetFirewallRule -Name FPS-ICMP4-ERQ-In`.
2. Dodaj monitor „Ping” dla VM Windows (lub komputera partnera) z interwałem 20 s.
3. Dodaj monitory „Port TCP”: SSH (22) i Samba (445) na VM Ubuntu Server, oraz monitor HTTP Jellyfin `http://<IP VM>:8096` (jeśli działa).
4. Dla każdego monitora ustaw liczbę ponowień przed zgłoszeniem awarii na 1. Zanotuj konfigurację w tabeli.

2 Strona stanu i powiadomienia

1. Utwórz stronę stanu (Strony statusu → Nowa) o nazwie „Pracownia — stanowisko <nr>” i dodaj do niej wszystkie monitory.
2. Skonfiguruj powiadomienie: ntfy (temat o trudnej nazwie, aplikacja na telefonie) albo kanał wskazany przez nauczyciela. Przypisz je do wszystkich monitorów.
3. Wyślij powiadomienie testowe przyciskiem „Test” i zrób zrzut odebranej wiadomości.
4. Wstrzymaj na chwilę jeden monitor (Pauza) i sprawdź, jak zmienia się strona stanu; wznów monitor.

3 Symulacja awarii

Partner zatrzymuje usługę, a Ty wykrywasz awarię tylko na podstawie monitoringu.

1. Partner zapisuje godzinę i zatrzymuje jedną usługę, np. `sudo systemctl stop smbd`, nie mówiąc której.
2. Zapisz godzinę powiadomienia i oblicz czas wykrycia. Na podstawie panelu ustal, która usługa nie działa.
3. Zaloguj się przez SSH, sprawdź `systemctl status smbd` i `journalctl -u smbd --since "10 min ago"`, uruchom usługę i potwierdź powrót do stanu „Up”.
4. Powtórz scenariusz z zamianą ról: wyłączenie VM Windows lub odłączenie jej karty sieciowej (Urządzenia → Sieć).

4 Zasoby serwera i procedura

1. Zainstaluj Glances (`sudo apt install glances`) i uruchom go w terminalu. Odczytaj obciążenie CPU, RAM, dysku i najbardziej obciążający proces.
2. Opcjonalnie uruchom tryb WWW `glances -w` i otwórz `http://<IP VM>:61208`. Zakończ go klawiszami Ctrl+C.
3. Napisz procedurę reakcji na awarię (wykrycie → ocena → powiadomienie → diagnoza → naprawa → weryfikacja → wpis do dziennika) dla jednej z monitorowanych usług.

W sprawozdaniu umieść

- ☐ tabela monitorów z typem, adresem, portem i interwałem
- ☐ zrzuty: strona stanu, powiadomienie testowe, monitor w stanie „Down” i ponownie „Up”
- ☐ przebieg dwóch symulacji awarii z czasem wykrycia
- ☐ procedura reakcji na awarię
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego udany ping do serwera nie oznacza, że działa udział Samba lub serwer Jellyfin?
2. Od czego zależy czas wykrycia awarii i dlaczego zbyt krótki interwał i brak ponowień mogą dawać fałszywe alarmy?

3. Co się stanie z monitoringiem, gdy awarii ulegnie sam serwer z Uptime Kuma? Jak temu zaradzić?
4. Jakie informacje powinien zawierać wpis w dzienniku awarii?

Kryteria oceny

Kryterium	Punkty
Poprawnie skonfigurowane monitory (min. 4, trzy typy)	5
Strona stanu i działające powiadomienie	3
Dwie symulacje awarii z diagnozą i czasem wykrycia	5
Procedura reakcji na awarię	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).