0.1. Testowana funkcjonalność

Gotowy system poddany został testom akceptacyjnym mającym za zadanie sprawdzić poprawne działanie oraz spełnienie wymagań przedstawionych w rozdziałach **??** oraz **??**. W opisie testów jako standardowe uruchomienie systemu rozumiemy procedurę opisaną w sekcji **??**.

Wykonane zostały następujące scenariusze akceptacyjne:

0.1.1. Brak komunikacji z nadzorcą

Przy starcie samodzielnego serwera wirtualizacji i wykryciu braku komunikacji z jakimkolwiek nadzorcą (poprzez brokera wiadomości) serwer powinien poinformować o błędzie i zakończyć działanie.

Kroki:

1. Włącz wewnętrznego brokera wiadomości oraz serwer wirtualizacji.
2. Wyświetl błąd i zakończ działanie.

0.1.2. Utrata komunikacji z nadzorcą

Po poprawnym starcie systemu z pojedynczym nadzorcą oraz serwerem wirtualizacji, serwer powinien zakończyć pracę po wyłączeniu się ostatniego (jedynego) nadzorcy.

Kroki:

1. Uruchom system standardową procedurą.
2. Poczekaj na prawidłowy start systemu.
3. Wyłącz nadzorcę lub brokery wiadomości.
4. Poczekaj na wykrycie braku nadzorców (brak otrzymanych wiadomości).
5. Wyświetl błąd i zakończ działanie.

0.1.3. Standardowe użycie systemu przez użytkownika

Użytkownik podłącza się do systemu złożonego z pojedynczego nadzorcy oraz serwera wirtualizacji, gdzie działa przynajmniej jedna wolna maszyna. Użytkownik powinien prawidłowo otrzymać sesję, a po odłączeniu się od maszyny, powinna ona zostać wyłączona po 15 minutach (czas konfigurowalny).

Kroki:

1. Uruchom system standardową procedurą.
2. Poczekaj na uruchomienie przynajmniej jednej maszyny wirtualnej.
3. Poproś o sesję poprzez aplikację kliencką.
4. Podłącz się poprzez RDP do uzyskanej maszyny.
5. Zakończ sesję z poziomu aplikacji.
6. Po określonym czasie maszyna powinna się wyłączyć.

0.1.4. Standardowe użycie systemu przez użytkownika przy awarii nadzorcy

Użytkownik podłącza się do systemu złożonego z dwóch nadzorców oraz jednego serwera wirtualizacji, gdzie działa przynajmniej jedna wolna maszyna. Użytkownik uzyskuje sesję, a w trakcie jej użytkowania następuje awaria nadzorcy. Po odłączeniu się od sesji i ponownej prośbie o sesję, w czasie krótszym niż czas wyłączenia maszyny, użytkownik powinien otrzymać ponownie tą samą maszynę.

Kroki:

1. Uruchom system standardową procedurą z dwoma nadzorcami.
2. Poczekaj na uruchomienie przynajmniej jednej maszyny wirtualnej.
3. Poproś o sesję poprzez aplikację kliencką.
4. Podłącz się poprzez RDP do uzyskanej maszyny.
5. Wyłącz tego nadzorcę, z którym klient się komunikował.
6. Zakończ sesję z poziomu aplikacji.
7. Poproś ponownie o sesję poprzez aplikację kliencką (powinien uzyskać tą sama maszynę).
8. Podłącz się poprzez RDP do uzyskanej maszyny.

0.1.5. Podłączenie nowego serwera wirtualizacji

W trakcie działania systemu nowy serwer wirtualizacji powinien zostać włączony do modelu nadzorców oraz wyświetlony w panelu administratora.

Kroki:

1. Uruchom system standardową procedurą.

2. Poczekaj na prawidłowy start systemu.

3. Włącz kolejną instancję serwera wirtualizacji.

4. Poczekaj na aktualizację modelu.

5. Sprawdź w panelu administratora, czy dwa serwery sa w modelu.

0.1.6. Podłączenie nowego nadzorcy

W trakcie działania systemu nowy nadzorca powinien posiadać taki sam model, jak aktualnie działający

Kroki:

1. Uruchom system standardową procedurą.

2. Poczekaj na prawidłowy start systemu.

3. Włącz kolejną instancję nadzorcy.

4. Poczekaj na aktualizację modelu.

5. Sprawdź model na pierwszym nadzorcy poprzez panel administratora.

6. Sprawdź model na drugim nadzorcy poprzez panel administratora.

0.1.7. Odnotowanie utraty serwera wirtualizacji

W trakcie działania systemu, przy utracie serwera wirtualizacji, nadzorcy powinni usunąć go z modelu.

Kroki:

1. Uruchom system standardową procedurą.

2. Poczekaj na prawidłowy start systemu.

3. Wyłącz serwer wirtualizacji.

4. Poczekaj na odnotowanie straty.

5. Sprawdź model poprzez panel administratora.

0.1.8. Utrata komunikacji przy działającej sesji

W trakcie działania systemu, przy utracie ostatniego nadzorcy, serwer wirtualizacji powinien zakończyć działanie. Jeżeli serwer posiada działające sesje, przed zakończeniem pracy, musi poczekać na ich zakończenie.

Kroki:

1. Uruchom system standardową procedurą.
2. Poczekaj na prawidłowy start systemu.
3. Poproś o sesję poprzez aplikację kliencką.
4. Podłącz się poprzez RDP do uzyskanej maszyny.
5. Wyłącz nadzorcę lub brokery wiadomości.
6. Poczekaj na wykrycie braku nadzorców (brak otrzymanych wiadomości).
7. Wyświetl błąd, ale kontynuuj działanie.
8. Poczekaj na zakończenie sesji.
9. Zakończ działanie.

0.1.9. Odzyskanie komunikacji przy działającej sesji

W trakcie działania systemu, przy utracie ostatniego nadzorcy, serwer wirtualizacji powinien zakończyć działanie. Jeżeli serwer posiada działające sesje, przed zakończeniem pracy, musi poczekać na ich zakończenie. Jeżeli przed zakończeniem ostatniej sesji nastąpi przywrócenie komunikacji, serwer powinien kontynuować działanie po zakończeniu sesji.

Kroki:

1. Uruchom system standardową procedurą.
2. Poczekaj na prawidłowy start systemu.
3. Poproś o sesję poprzez aplikację kliencką.
4. Podłącz się poprzez RDP do uzyskanej maszyny.
5. Wyłącz nadzorcę lub brokery wiadomości.
6. Poczekaj na wykrycie braku nadzorców (brak otrzymanych wiadomości).

7. Wyświetl błąd, ale kontynuuj działanie.
8. Włącz wyłączony wcześniej moduł.
9. Poczekaj na zakończenie sesji.
10. Kontynuuj działanie.

0.2. Środowisko testowe

Testy przeprowadzaliśmy na dwóch komputerach podłączonych do wspólnej sieci lokalnej. Usługa OpenLDAP była uruchomiona na innym komputerze oraz udostępniała testową bazę użytkowników. Każdy z nich pracował pod kontrolą systemu operacyjnego Arch Linux w wersji ze stycznia 2022 roku. Oba posiadały 8 GB pamięci operacyjnej oraz 4 rdzeniowy procesor o 8 wątkach (Intel i7-2600K oraz i7-4790). Do testów skonfigurowaliśmy serwery wirtualizacji, aby miały do dyspozycji 6 wątków oraz 4096 MB pamięci operacyjnej.

Niestety taka platforma uniemożliwiła przetestowanie funkcjonalności PCI Passthrough (patrz wymagania sprzętowe serwera wirtualizacji, rozdział **??**). Budowa ich płyt głównych nie pozwalała na całkowita izolację urządzeń podłączonych do złączy PCI Express. Skorzystaliśmy z innego komputera, który posiadał inną konstrukcję płyty głównej i każde z urządzeń zostało prawidłowo odizolowane dzięki przydzieleniu innych adresów pamięci. Pracował on pod kontrola systemu operacyjnego Arch Linux ze stycznia 2022 roku. Posiadał on 48GB pamięci operacyjnej oraz 12 rdzeniowy procesor o 24 wątkach (AMD Threadripper 1920X). Uruchamiany na nim serwer wirtualizacji miał do dyspozycji 20 wątków oraz 43008 MB pamięci operacyjnej.

Na każdym z tych komputerów można było uruchomić aplikację serwera wirtualizacji, panelu administracyjnego oraz nadzorcy.

0.3. Wykonane testy

W trakcie rozwoju projektu zaprogramowaliśmy wiele testów automatycznych, które sprawdzały podstawową logikę wydzielonych części kodu. W przypadku modułów korzystających z zewnętrznych narzędzi (np. libvirt) stworzyliśmy proste testy integracyjne. Sprawdzają czy wszystkie wykorzystywane funkcjonalności tych narzędzi zostały prawidłowo zintegrowane.

Po zakończeniu rozwoju funkcjonalności systemu przystąpiliśmy do próby wdrożenia systemu w środowiskach testowych. Wykonaliśmy wtedy ręcznie podstawowe scenariusze uruchomienia

systemu w postaci kontenerów dockerowych. Gdy już system pracował stabilnie przystąpiliśmy do ręcznego wykonywania scenariuszy akceptacyjnych

0.4. Wyniki testów

Testy automatyczne często kończyły się błędem po zmianie w kodzie. Był to dla nas znak aby sprawdzić co się dzieje i wprowadzić odpowiednie poprawki.

Próby wdrożenia systemu w środowisku testowych przyniosły odkrycie wielu błędów logicznych w naszych wstępnych pomysłach jak i samej implementacji. Dodatkowo pomogło nam to też lepiej zrozumieć wymagania sprzętowe jak i zależności naszego systemu.

Przy wykonywaniu testów akceptacyjnych mieliśmy szansę dopracować stabilność oraz ponownie skonfrontować wstępne pomysły z rzeczywistością. Po poprawkach błędów i upewnieniu się, że wszystkie scenariusze akceptacyjne są już spełnione system był już wystarczająco stabilny aby można było z niego korzystać. Zrozumieliśmy wtedy lepiej jakie rozwiązania nie są wygodne i wymagają poprawek albo nawet przeprojektowania. Nasze przemyślenia o nieudanych elementach systemu można znaleźć w podsumowaniu (rozdział **??**).