Zestaw do backupu i przywracania UniFi

Od sprawdzonej kopii do potwierdzonego odzyskania usług



Ostoja

Wybierz ścieżkę i odpowiedzialność

Ostoja • Plan działania

Anna, 36 lat, administruje biurem rachunkowym w Łodzi. Właściciel zatwierdza przerwę, Anna wykonuje działania, drugi administrator sprawdza wynik.



Anna
36 lat, administruje biurem rachunkowym w Łodzi.



Właściciel
zatwierdza przerwę.



Drugi administrator
sprawdza wynik.

START

Planowana zmiana
strony 3–9.



Najpierw ustal zakres, wybierz kopię, przygotuj dostęp i warunek zatrzymania.

Próba bez wpływu na biuro
strona 10.



Odtwórz konfigurację w fizycznie odizolowanym laboratorium.

Awaria Cloud Gateway
strona 11.



Migracja zarządzania
strona 12.



Urządzenia offline po zmianie hosta
strona 13.



Po odtworzeniu
strony 14–15.



Sprawdź usługi i ograniczenia; następnie zamknij próbę lub wycofaj zmianę według strony 16.



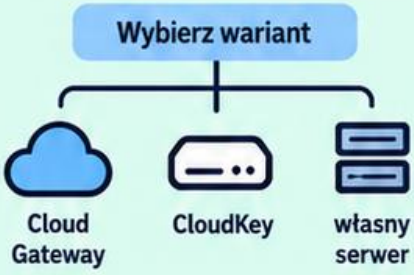
STOP
zatrzymuje niebezpieczną czynność.



POWRÓT
wskazuje bezpieczny stan po przerwaniu.



Przed działaniem wpisz godzinę, host, objaw i właściciela decyzji. Zaznacz wariant: Cloud Gateway, CloudKey albo własny serwer.





Nie łącz kroków różnych wariantów. Formularz incydentu ma prowadzić do pliku i dowodów, nigdy do jawnych haseł lub kluczy.

START oznacza spełnione wymagania. **TEST** określa dowód. **STOP** zatrzymuje niebezpieczną czynność. **POWRÓT** wskazuje bezpieczny stan po przerwaniu.

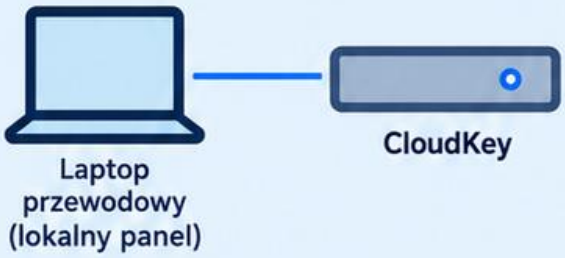
Źródła: [1], [7].

Ostoja • Procedura 01

Ustal granicę awarii oraz RPO i RTO

Zarządzanie (CloudKey)

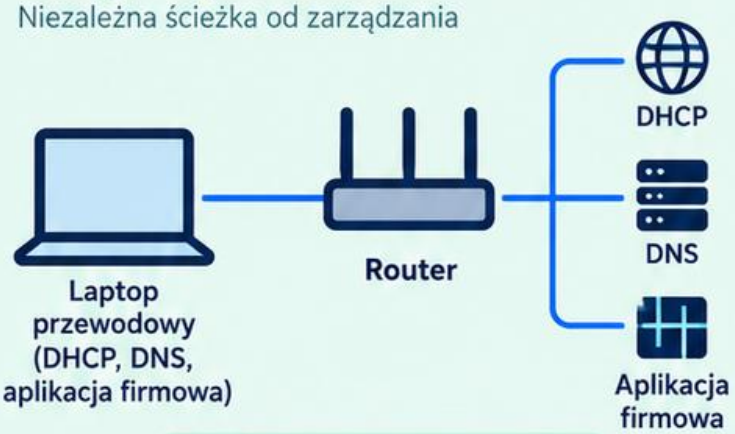
Niezależna ścieżka od usług użytkowników



Wynik zarządzania zapisz osobno.

Usługi użytkowników

Niezależna ścieżka od zarządzania



Wynik usług użytkowników zapisz osobno.

1. **START:** zanotuj godzinę zgłoszenia i wskaż host. W tym przykładzie biuro korzysta z CloudKey oraz osobnego routera.

2. **1.** Sprawdź z laptopa przewodowego lokalny panel, DHCP, DNS i aplikację firmową. Zapisz osobno wynik zarządzania oraz usług użytkowników.

3. **2.** Jeśli działa router, lecz nie CloudKey, nie resetuj routera. Ustal zakres usterki przed odtwarzaniem konfiguracji.

4. **3.** Zapisz datę ostatniej sprawdzonej kopii i zmiany wykonane później. RPO określa dopuszczalną utratę zmian, RTO — czas odzyskania usługi.

Przykład celu firmy: RPO 24 godziny, RTO 2 godziny. To założenia organizacyjne, nie obietnica czasu działania UniFi.

Oś czasu incydentu

- **Godzina zgłoszenia**
  Zanotuj godzinę i wskaż host. .....
- **Ostatnia sprawdzona kopia**
  Zapisz datę. .....
- **Zmiany po kopii**
  Wymień wykonane zmiany. .....
  .....
- **Rozpoczęcie działań**
  Zanotuj godzinę. .....
- **Akceptacja usługi**
  Właściciel potwierdza, że usługa została odzyskana. .....

RPO	RTO
(dopuszczalna utrata zmian)	(czas odzyskania usługi)
.....	.....

TEST: właściciel potwierdza, która usługa ma wrócić pierwsza i kiedy uzna ją za odzyskaną. Sam panel nie wystarcza.

STOP: nieznany zakres lub brak dostępu do kopii. Zabezpiecz dowody i wybierz właściwy wariant ze strony 2.

POWRÓT: pozostaw sprawne usługi; usuń wyłącznie wykonane ustawienia testowe laptopa. Kontynuuj diagnozę bez resetowania działającej infrastruktury.

Źródła: [1], [7].

Ostoja • Procedura 02

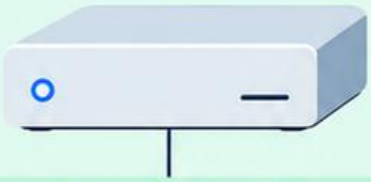
Dobierz rodzaj kopii do hosta

START: odczytaj typ hosta i zapisz, co zamierzasz odzyskać.
Kopia konfiguracji nie jest obrazem całego dysku każdego urządzenia.



Jaki host?

1. Cloud Gateway lub zgodna konsola: wybierz System Config Backup.
Obejmuje konfiguracje systemu UniFi OS, aplikacji i urządzeń.



System Config Backup

- UniFi OS
- aplikacji
- urządzeń

2. Własny Network Server lub odpowiednia starsza instalacja: wybierz Network-only.
Ta kopia obejmuje ustawienia Network i konfiguracje zarządzanych urządzeń.



Network-only

- ustawienia Network
- konfiguracje zarządzanych urządzeń

System operacyjny hosta Windows/Linux jest poza zakresem kopii Network-only.



Windows/Linux (bez kopii)

3. Zanotuj aplikację źródłową, wersję, datę i docelowy host.
Nie kieruj pliku Network do przypadkowej funkcji odzyskiwania systemu.

Przykład: Anna wymienia serwer Windows obsługujący Network. Potrzebuje kopii Network, a nie założenia, że plik zawiera również Windows.

TEST: zakres pliku odpowiada zadaniu, a docelowa funkcja obsługuje wybrany typ.
Przy migracji sprawdź zgodność na stronie 5.

STOP: nieznany typ lub brak wymaganej aplikacji.
Najpierw ustal zakres w dokumentacji, zamiast próbować kolejnych plików na produkcji.

POWRÓT: pozostaw host źródłowy bez zmian.
Skoryguj plan i przygotuj właściwą kopię przed kolejną próbą.

Źródła: [1], [3].

Sprawdź zgodność celu przed odtworzeniem

START: przygotuj dane kopii oraz modele źródła i celu.
Cel testowy pozostaje odłączony od produkcyjnych VLAN-ów.

Źródło

Wersja Network: _____
Wersja UniFi OS: _____
Data kopii: _____
Wymagane aplikacje: _____

Kopia zapasowa

- Wersja Network
- Wersja UniFi OS
- Data kopii
- Wymagane aplikacje

Cel (testowy)

Wersja Network: _____
Wersja UniFi OS: _____
Data kopii: _____
Wymagane aplikacje: _____

1. Zapisz wersję Network, UniFi OS, datę kopii i wymagane aplikacje. Porównaj dostępność funkcji na docelowym modelu.

2. Przy migracji między różnymi modelami konsol dokumentacja wymaga UniFi OS co najmniej 3.1. Sam numer nie gwarantuje każdej kombinacji.

3. Dla migracji Network przygotuj aktualną aplikację docelową. Informacje o wydaniu sprawdź przed aktualizacją, a nie podczas awaryjnego importu.

Sprawdź zgodność

TEST: cel spełnia wymagania, a próbny import nie zgłasza niezgodności. Potwierdź także odzyskane ustawienia według strony 10.

STOP: komunikat o niezgodnej wersji lub zakresie. Nie modyfikuj ręcznie pliku i nie traktuj downgrade jako pewnego rozwiązania.



Przykład: zapasowa konsola ma starsze oprogramowanie. Anna przygotowuje ją osobno, zanim podejmie próbę przywrócenia właściwego zakresu.

POWRÓT: odłącz cel próbny, zachowaj komunikat oraz oryginalną kopię. Wybierz zgodny wariant i ponów próbę po przygotowaniu.

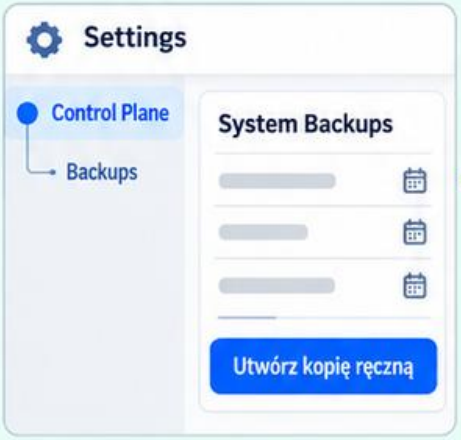
Źródła: [1], [2].

Przygotuj kopię systemową konsoli

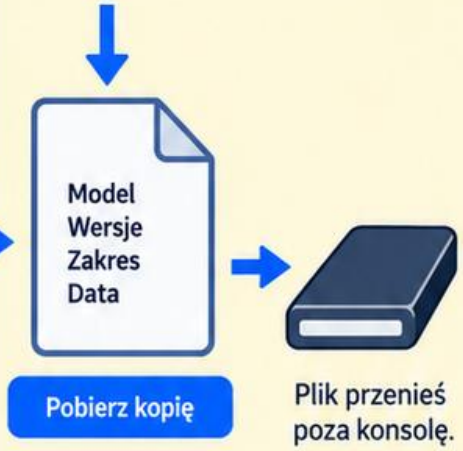
Ostoja • Procedura 04

START: działający Cloud Gateway, uprawniony właściciel konta i bezpieczne miejsce na plik. **W** tym wariancie tworzysz kopię systemową.

1 **Otwórz Settings > Control Plane > Backups.** Sprawdź System Backups oraz datę dostępnej kopii; wykonaj aktualną kopię ręczną.



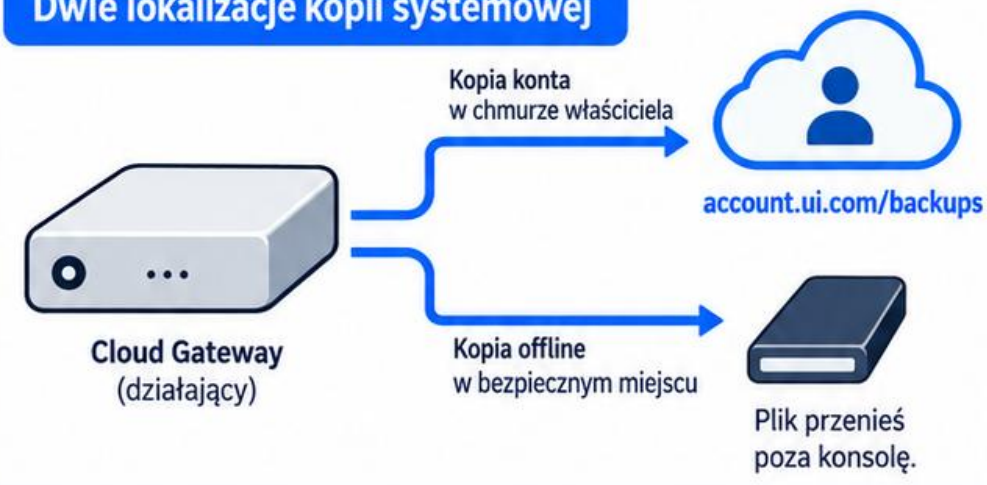
2 **Pobierz kopię offline** z tej sekcji. Zapisz model, wersje, zakres i datę; plik przenieś poza konsolę.



3 Właściciel sprawdza dostęp do kopii konta na **account.ui.com/backups.** Sama sesja administratora nie dowodzi uprawnień do wszystkich kopii.



Dwie lokalizacje kopii systemowej



Przykład:
Anna przygotowuje zmianę VLAN-u. Zachowuje osobny plik sprzed zmiany, zamiast polegać wyłącznie na wcześniejszej kopii automatycznej.

TEST: plik ma niezerowy rozmiar, oczekiwaną datę i jest dostępny z drugiego stanowiska zgodnie z uprawnieniami. Odtworzenie sprawdzisz osobno.

STOP: nieudany zapis lub brak dostępu właściciela. Nie rozpoczynaj planowanej zmiany, dopóki nie przygotujesz skutecznej drogi odzyskania.

POWRÓT: pozostaw konfigurację produkcyjną bez zmian; popraw zapis lub dostęp i ponów przygotowanie kopii.

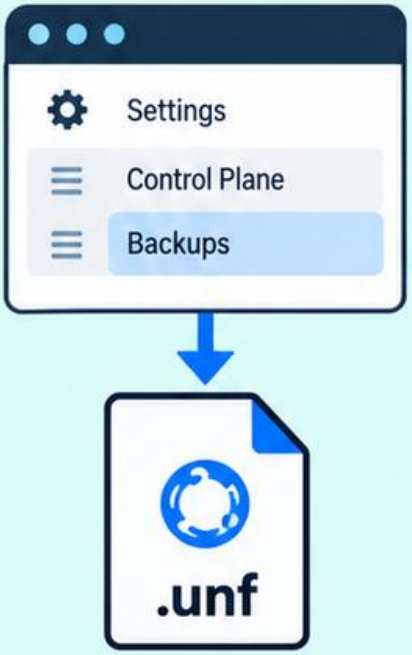
Źródła: [1].

Przygotuj kopię Network-only

Ostoja • Procedura 05

START: własny UniFi Network Server, dostęp administratora i uzgodnione okno prac. Ten wariant nie tworzy kopii całego systemu operacyjnego.

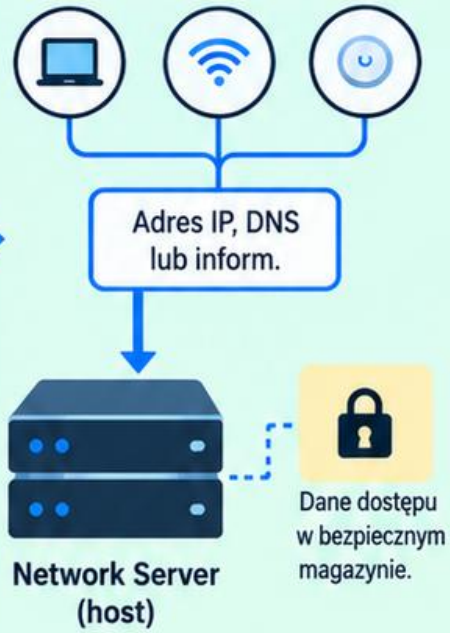
1 W źródłowej aplikacji otwórz Settings > Control Plane > Backups i pobierz kopię Network w pliku .unf.



2 Zapisz nazwę instalacji, wersję Network, datę i lokalizację pliku. Sprawdź, czy wybrano właściwy host, a nie nową, pustą instancję.



3 Zanotuj sposób dotarcia urządzeń do hosta: adres IP, DNS lub inform. Potrzebne dane dostępu zachowaj w bezpiecznym magazynie.



Przykład: plik LDZ-Network-przed-migracja.unf opisuje konfigurację biura. Instalator systemu i wymagania nowego hosta są przygotowywane oddzielnie.

TEST: plik jest czytelny i dostępny poza serwerem; jego zakres pasuje do planu ze strony 12. Sprawdzenie rozmiaru nie zastępuje odtworzenia.

STOP: nieznana instancja lub błąd pobierania. Nie wyłączaj źródła i nie resetuj urządzeń w celu zdobycia kopii.

POWRÓT: pozostaw działający Network Server; popraw wybór instancji i ponów pobranie przed migracją.

Źródła: [1], [3].

Ostoja • Procedura 06

Zabezpiecz kopię poza urządzeniem

START: pobrany plik i zatwierdzone zasady przechowywania. Kopię traktuj jako wrażliwe dane, nie załącznik do publicznego zgłoszenia.



1. Umieść plik w chronionym magazynie poza konsolą. Przygotuj drugą kontrolowaną kopię, dostępną również podczas awarii podstawowego stanowiska.



2. Zapisz identyfikator, model źródła, wersję, datę, zakres i właściciela. W karcie podaj lokalizację, nie hasło do magazynu.

Karta kopii (przykład B-02)	
Identyfikator	B-02
Model źródła	
Wersja	
Data	
Zakres	
Właściciel	
Lokalizacja	kopia biura i zastępca Anny

3. Porównaj rozmiar i sumę kontrolną po przeniesieniu. Zgodna suma potwierdza identyczność plików, nie poprawność odzyskania konfiguracji.



Zgodna suma potwierdza identyczność plików, nie poprawność odzyskania konfiguracji.

Przykład: wpis B-02 wskazuje kopię biura i zastępcę Anny. Uprawniona osoba uzyskuje dostęp według procedury, bez publikowania sekretów.



TEST: zastępca odnajduje właściwy plik i odczytuje go z innego stanowiska. Zapisz czas oraz wynik próby dostępu.



STOP: plik jest uszkodzony lub dostępny publicznie. Zabezpiecz magazyn; odtwórz kopię z zaufanego źródła i ponów kontrolę.

POWRÓT: zachowaj poprzednią sprawdzoną wersję. Nie kasuj jedynej dobrej kopii przed odbiorem nowej.

Źródła: [1].

Ostoja • Procedura 07

Zamknij punkt kontrolny przed zmianą

START: działająca instalacja, właściciel zmiany i sprawdzona kopia.
Zarezerwuj czas na testy oraz bezpieczne wycofanie, nie tylko zapis ustawień.

1. Zapisz wartości początkowe, datę kopii i dokładny zakres.
Wstrzymaj równoległe zmiany, które unieważniłyby punkt odniesienia.



- wartości początkowe
- data kopii
- zakres

2. Z laptopa przewodowego potwierdź lokalne logowanie.
Zanotuj port i adres; tej ścieżki nie przebudowuj równocześnie ze zmienianym uplinkiem.

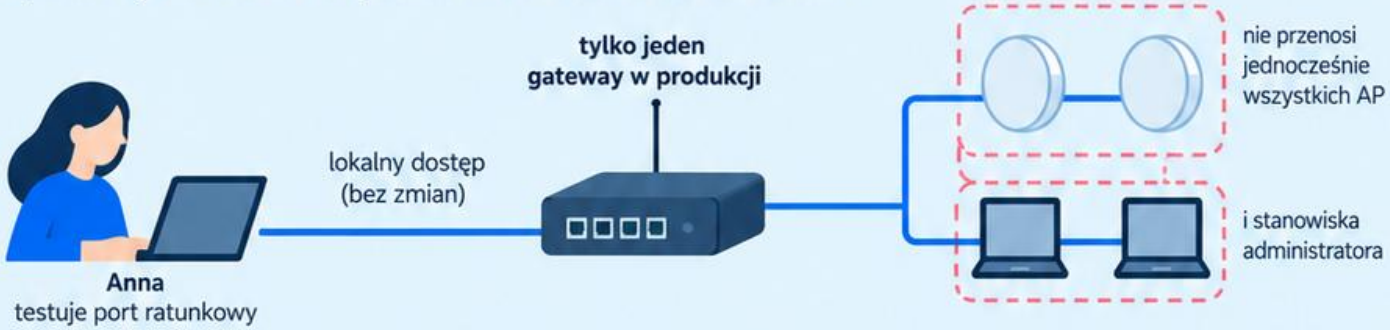


3. Przygotuj próbę pozytywną, próbę zabronionego dostępu i warunek STOP.
Aktualizacje planuj według informacji o wydaniu, etapami.



- próba pozytywna
- próba zabronionego dostępu
- warunek STOP
- informacje o wydaniu

Przykład: przed zmianą sieci zarządzania Anna testuje port ratunkowy.
Nie przenosi jednocześnie wszystkich AP i stanowiska administratora.



TEST: drugi administrator potrafi wskazać plik, poprzednią wartość i sposób odzyskania dostępu. Dopiero wtedy właściciel potwierdza rozpoczęcie.



- plik
- poprzednia wartość
- sposób odzyskania dostępu

STOP: brak kopii, lokalnego dostępu lub jednoznacznego powrotu. Przesuń zmianę, zamiast improwizować podczas utraty zarządzania.



- brak kopii
- brak lokalnego dostępu
- brak jednoznacznego powrotu

POWRÓT: zakończ przygotowanie bez zmiany produkcji. Jeśli zmiana już ruszyła, przywróć ostatnią wartość przez zachowaną ścieżkę.

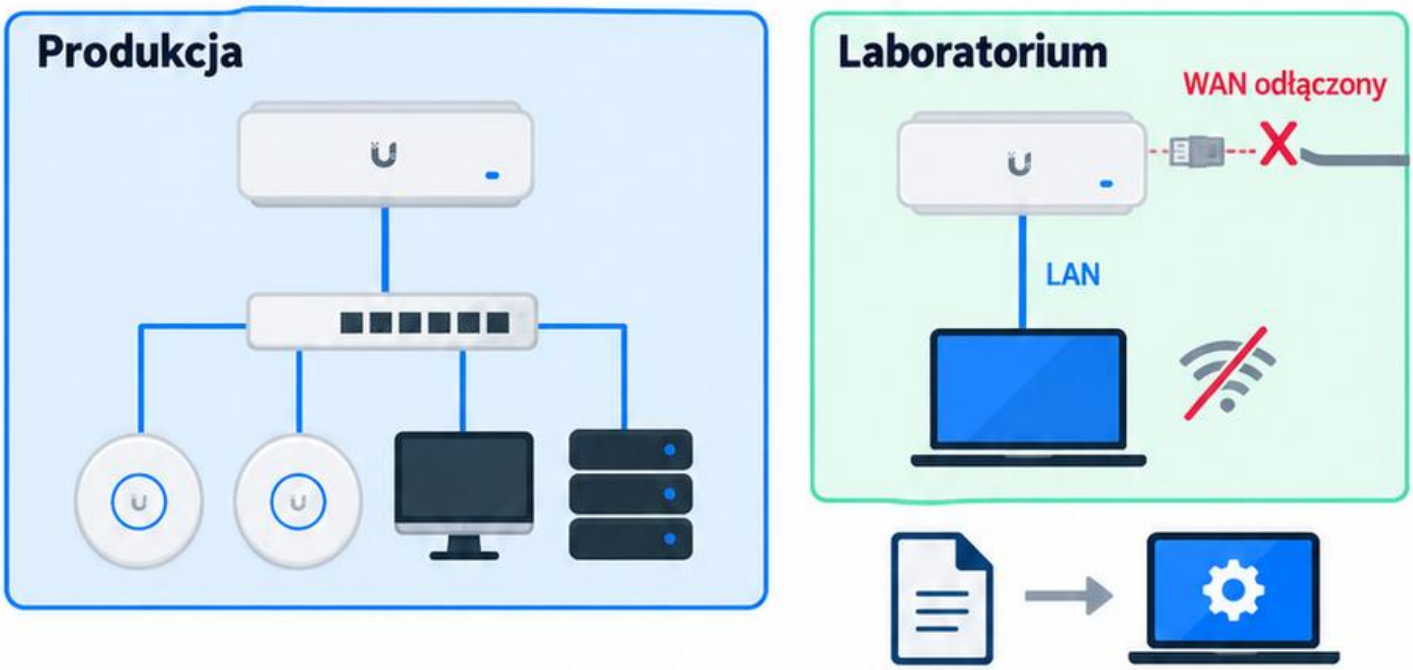


przywróć ostatnią wartość przez zachowaną ścieżkę

Źródła: [1], [2], [7].

Ostoja • Procedura 08

Odtwórz kopię w odizolowanym laboratorium



START: zgodny, przygotowany Cloud Gateway, właściwa kopia systemowa i sprawdzone logowanie lokalne. Wykonujesz próbę odtworzenia.

Przykład: Anna testuje kopię biura w Łodzi, zawierającą produkcyjny adres bramy i konfigurację DHCP.

1. Odłącz konsolę próbną od produkcji. WAN pozostaw odłączony; żadnych wspólnych VLAN-ów ani produkcyjnych urządzeń.
2. Podłącz laptop tylko do LAN konsoli próbnej, Wyłącz Wi-Fi, VPN i mostkowanie.
3. Zaloguj się lokalnie. Otwórz Settings > Control Plane > Backups > Restore i wgraj właściwy plik System Config Backup.
4. Pozostaw Restore All Applications and Settings dla próby całego systemu. Potwierdź zakres; poczekaj na zakończenie.

TEST: zaloguj się lokalnie; porównaj sieci, polityki i konta. Zapisz czas. Próba nie potwierdza działania produkcyjnych AP ani WAN.

STOP: połączenie z produkcją lub niezgodna kopia. Przerwij próbę; nie uruchamiaj drugiego DHCP ani hosta zarządzającego w produkcji.

POWRÓT: odłącz laboratorium, zachowaj protokół. Produkcja pozostaje na dotychczasowym hoście.

Źródła: [1], [3], [4].

Zastąp konsolę po potwierdzonej awarii

Ostoja • Procedura 09

START: uszkodzony Cloud Gateway, zgodny zamiennik i sprawdzona kopia systemowa. Właściciel zatwierdził przerwę; lokalny laptop jest gotowy.

1. Sprawdź zasilanie i dostęp lokalny.

Jeśli urządzenie działa, najpierw ustal usterkę; nie odtwarzaj całej instalacji z powodu pojedynczej aplikacji.



2. Oznacz i odłącz starą bramę od WAN oraz LAN.

Nie pozwól, by wróciła do tej samej sieci po odzyskaniu zasilania.



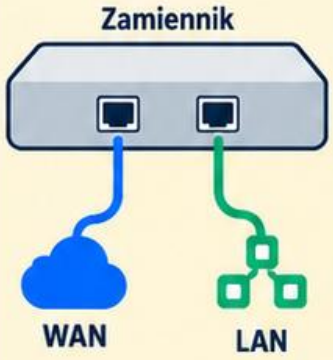
3. Przygotuj zamiennik zgodnie ze stroną 5.

Przywróć System Config Backup podczas konfiguracji albo przez Settings > Control Plane > Backups > Restore.



4. Podłącz opisane przewody do właściwych ról portów zamiennika.

Przy innym modelu sprawdź mapowanie; nie kopiuj samych numerów.



Przykład: stara konsola pozostaje odłączona, a nowa przejmuje jedyną rolę bramy i DHCP.



TEST: wykonaj odbiór ze stron 14–15.

Recovery Mode rozważ dopiero według instrukcji konkretnego modelu.

STOP: niezgodność lub utrata krytycznej usługi.

POWRÓT: odłącz zamiennik; przywróć stary tylko wtedy, gdy jest sprawny. W przeciwnym razie kontynuuj zatwierdzone odzyskiwanie.

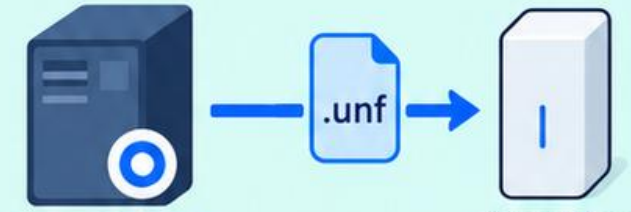
Źródła: [1], [6], [7].

Przenieś zarządzanie Network na nowy host

Ostoja • Procedura 10

START: wybierz jeden wariant.
A: Network Server do CloudKey, jedna witryna.
B: Network Server do UniFi OS Server na tym samym komputerze Windows.

A Network Server do CloudKey, jedna witryna.



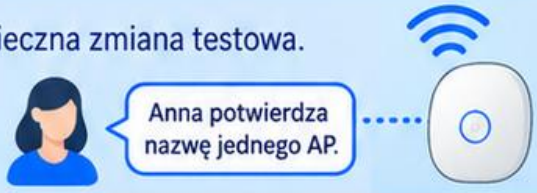
1. **1.** Pobierz kopię .unf ze źródła według strony 7. Zapisz adres hosta i metodę inform; przygotuj możliwość powrotu.
2. **A:** skonfiguruj CloudKey i aktualną aplikację Network. W Settings > Control Plane > Backups przywróć plik Network, nie kopię systemową innego hosta.
3. **A:** sprawdź kierowanie urządzeń według strony 13. Gdy są online na celu, wyłącz starą instancję; nie pozostawiaj konkurencyjnego zarządzania.

B Network Server do UniFi OS Server na tym samym komputerze Windows.



1. **B:** zamknij Network Server przed instalacją UniFi OS Server. Instalator Windows może wykryć domyślną instalację i zaproponować migrację.
2. **B:** jeśli nie proponuje migracji, zatrzymaj ten wariant i sprawdź oficjalną procedurę ręczną; nie uruchamiaj drugiej instancji na próbę.

TEST: właściwa witryna, urządzenia online i bezpieczna zmiana testowa.
Przykład: Anna potwierdza nazwę jednego AP.



STOP: niezgodność lub niewłaściwa witryna.
POWRÓT: zatrzymaj cel przed ponownym uruchomieniem źródła; przywróć poprzedni inform, jeżeli został zmieniony.

Źródła: [1], [3], [4].

Przywróć połączenie urządzeń z Network

Ostoja • Procedura 11

START: docelowy Network działa, kopia jest przywrócona, lecz AP pozostaje offline.
Nie zakładaj, że działające Wi-Fi potwierdza zarządzanie.

Ścieżka danych AP

Ruch klientów Wi-Fi jest niezależny od zarządzania.

Ścieżka zarządzania

Urządzenie łączy się z Network przez sieć zarządzania, routing i TCP 8080.



Metody informowania o adresie Network (wybierz jedną)

Ustal używaną metodę i popraw właściwy wpis; nie zmieniaj jednocześnie wszystkich metod.

Adres inform
Ustaw osiągalny adres nowego hosta.

DNS unifi
Popraw wpis DNS na adres nowego hosta.

DHCP Option 43
Popraw wpis DHCP Option 43 na adres nowego hosta.

1. **Sprawdź** adres hosta, routing z sieci zarządzania i TCP 8080 między urządzeniem a Network. Nie udostępniaj panelu ani SSH na WAN.
2. **Ustal używaną metodę:** adres inform, DNS unifi albo DHCP Option 43. Popraw właściwy wpis; nie zmieniaj jednocześnie wszystkich metod.
3. **Przy migracji ze źródłowego** Network sprawdź Override Inform Host zgodnie z instrukcją migracji. Wskaż osiągalny adres nowego hosta.
4. **W uzasadnionej gałęzi SSH** użyj znanych danych urządzenia. Przykład lokalny: `set-inform http://192.168.99.5:8080/inform`, wyłącznie dla właściwego hosta.

TEST: urządzenie jest online na celu i przyjmuje bezpieczną zmianę nazwy. Sprawdź, czy nie wraca do poprzedniej instancji.

STOP: brak uprawnień lub nieznana własność urządzenia.
Reset fabryczny pozostaje ostatnią, świadomą gałęzią, nie pierwszą próbą.

POWRÓT: przywróć poprzedni inform lub wpis DNS zgodnie z planem migracji; nie uruchamiaj równoległego zarządzania.

Źródła: [1], [4], [5].

Odbierz WAN, DHCP, DNS i sieci lokalne

START: odtworzona brama lub host jest właściwą instancją produkcyjną.
Zachowaj lokalną sesję administratora oraz punkt odniesienia sprzed awarii.

1

Podłącz klienta testowego przewodowo.
Odnów dzierżawę i zapisz IP, prefiks, bramę, DNS oraz VLAN; sprawdź, czy odpowiada planowi.

2

Wykonaj zapytanie do przydzielonego DNS.
Otwórz znaną stronę HTTPS oraz uzgodnioną usługę lokalną; rozdziel wynik nazw od osiągalności.

3

Powtórz próbę w każdym wymaganym VLAN-ie.
Następnie sprawdź SSID, uwierzytelnienie, adresację i aplikację na reprezentatywnym urządzeniu Wi-Fi.

IPv6 (opcjonalnie)

IPv6 sprawdź oddzielnie, jeśli jest używane; brak wdrożenia odnotuj jawnie. Nie zakładaj wyniku na podstawie IPv4.



Wynik:
IP: _____
Prefiks: _____
Brama: _____
DNS: _____
VLAN: _____

Wynik:
Zapytanie DNS: _____
Strona HTTPS: _____
Usługa lokalna: _____

Wynik:
VLAN: _____
SSID: _____
Adresacja: _____
Aplikacja: _____

Wynik:
Używane: _____
Zapytanie: _____
Osiągalność: _____

Przykład: laptop przewodowy działa, telefon nie otrzymuje adresu. Sprawdź przypisanie SSID i drogę VLAN-u, zamiast ponownie odtwarzać całą kopię.

TEST: zanotuj klienta, usługę, czas i wynik. Stara dzierżawa oraz zielona ikona WAN nie zastępują świeżej próby.

STOP: błędna adresacja lub niedziałająca usługa krytyczna.
POWRÓT: zatrzymaj odbiór, zachowaj dowód i wróć do ostatniego sprawdzonego etapu.

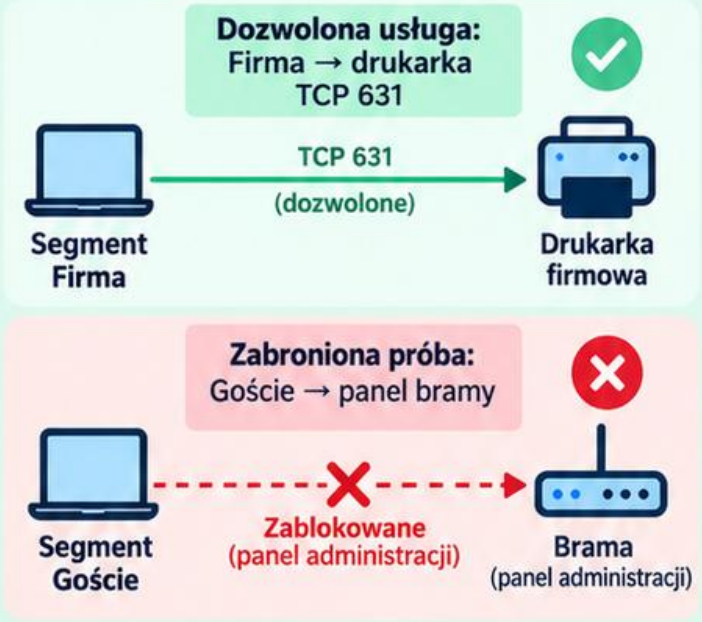
Źródła: [8], [9].

Odbierz segmentację i dostęp VPN

START: podstawowe usługi przeszły test ze strony 14. Przygotuj zatwierdzoną macierz dostępu i własne urządzenia testowe w odpowiednich segmentach.

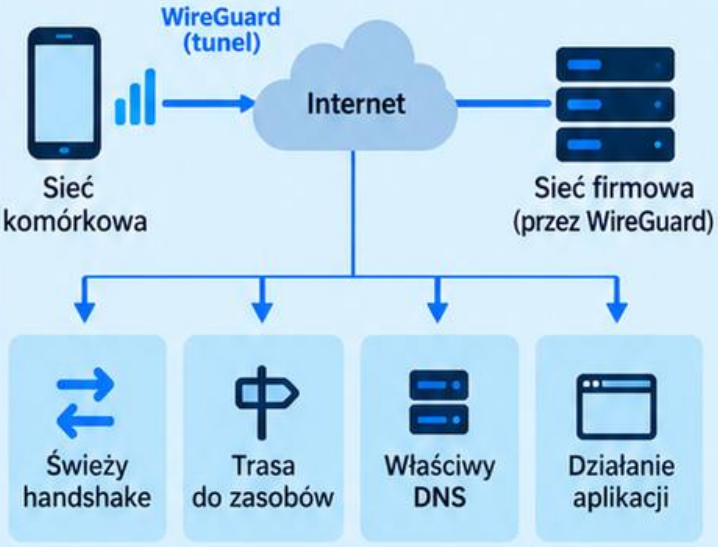
Przykład polityki biura

Firma drukuje przez TCP 631;
Goście nie otwierają panelu bramy.
Użyj rzeczywiście zatwierdzonych adresów.



Zdalny dostęp przez WireGuard

Dla WireGuard uruchom klienta z sieci komórkowej.
Sprawdź świeży handshake, trasę, właściwy DNS
i działanie aplikacji.



1. Sprawdź nową sesję do dozwolonej usługi oraz próbę zabronioną. Testuj konkretny port, nie wyłącznie ping.
2. Przykład polityki biura: Firma drukuje przez TCP 631; Goście nie otwierają panelu bramy. Użyj rzeczywiście zatwierdzonych adresów.
3. Dla WireGuard uruchom klienta z sieci komórkowej. Sprawdź świeży handshake, trasę, właściwy DNS i działanie aplikacji.
4. Sprawdź również zasób spoza uprawnień. Po unieważnieniu dostępu potwierdź brak ponownego połączenia; nie umieszczaj profilu ani klucza w protokole.

Przykład: tunel działa, lecz dokumenty po **nazwie** nie. Porównaj próbę po adresie oraz zapytanie do przewidzianego resolvera.

TEST: wyjątki i blokady odpowiadają macierzy. Powtórz odpowiednie próby po IPv6, jeśli jest wdrożone, i zapisz dowody.

STOP: nadmierny dostęp lub utrata administracji.
POWRÓT: wyłącz ostatnią politykę testową przez zachowaną sesję lokalną i ponów kontrolę.

Źródła: [10], [11].

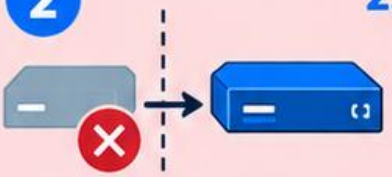
Ostoja • Procedura 14

Wycofaj zmianę i zamknij próbę DR

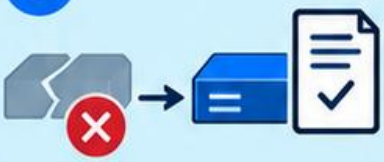
START: niespełnione kryterium odbioru albo zakończone ćwiczenie odzyskiwania. Właściciel podejmuje decyzję na podstawie zapisanych wyników, nie samego statusu online.

1. **Zatrzymaj** kolejne zmiany. Zanotuj objaw, czas, ostatni krok i urządzenia; zachowaj sprawną drogę lokalnego zarządzania.

2. Odłącz niesprawdzony zamiennik przed powrotem starej bramy. Uruchom tylko jedną instancję w danej roli; przywróć właściwe kierowanie inform.



3. Jeśli stary sprzęt jest uszkodzony, nie obiecuj powrotu do niego. Wybierz zgodny cel i ponów zatwierdzoną procedurę odzyskiwania.





Przykład: Anna wycofuje zmianę VLAN-u przez port ratunkowy. Nie otwiera wszystkich segmentów, aby ukryć brak konkretnej usługi.

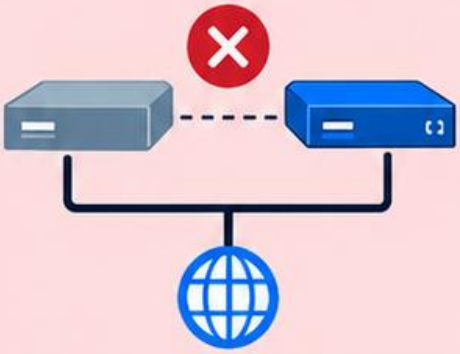


TEST: drugi administrator potwierdza usługi i ograniczenia. Zapisz czas odzyskania oraz przedział zmian nieobjętych odtworzoną kopią; porównaj z RTO i RPO.

STOP: brak pewnej kopii lub zgodnego celu. Zgłoś zależność właścicielowi i zachowaj ostatni sprawdzony stan.

POWRÓT: po odbiorze utwórz nową kopię, uzupełnij instrukcję i odłącz laboratorium. Backup konfiguracji nie gwarantuje cofnięcia firmware.

Nie uruchamiaj jednocześnie dwóch bram w tej samej roli.



Uruchom **tylko jedną instancję** w danej roli.



Porównaj z RTO i RPO.

RTO

RPO

Zamknięcie ćwiczenia DR to co innego niż odzyskiwanie po rzeczywistym incydencie.

Zakończone ćwiczenie odzyskiwania → zamknij próbę DR.

Rzeczywisty incydent → postępuj według procedury odzyskiwania.

Źródła: [1], [2], [3].

Źródła i zgodność • 1/2

Ostoja • Źródła

Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w procedurach.

1 Kopie i migracja UniFi

https://help.ui.com/hc/en-us/articles/360008976393

2 Aktualizacje UniFi

https://help.ui.com/hc/en-us/articles/7605005245975

3 Samodzielne hostowanie UniFi

https://help.ui.com/hc/en-us/articles/34210126298775

4 Adopcja urządzeń

https://help.ui.com/hc/en-us/articles/360012622613

5 Adopcja warstwy trzeciej

https://help.ui.com/hc/en-us/articles/204909754

6 Tryb odzyskiwania UniFi

https://help.ui.com/hc/en-us/articles/360043360253

Źródła i zgodność • 2/2

Ostoja • Źródła

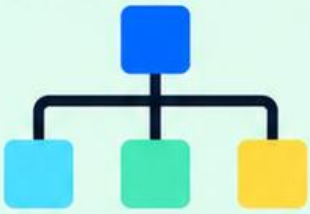
Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w procedurach.

[7] Lokalne zarządzanie UniFi



https://help.ui.com/hc/en-us/articles/28457353760919

[8] Diagnostyka sieci VLAN



https://help.ui.com/hc/en-us/articles/9592924981911

[9] Diagnostyka DNS UniFi



https://help.ui.com/hc/en-us/articles/17484948645015

[10] Serwer WireGuard



https://help.ui.com/hc/en-us/articles/115005445768

[11] Zapora strefowa



https://help.ui.com/hc/en-us/articles/115003173168

RPO, RTO, izolacja laboratorium i zapis dowodów są metodą operacyjną Ostoja. Nie stanowią gwarancji producenta.

Przed działaniem sprawdź model, wersję oraz zakres kopii. Nie mieszaj kopii systemowej z Network-only.