Azure Site Recovery dla Hyper-V bez VMM: replikacja, test, przełączenie i powrót

Poziom: zaawansowany

Dotyczy: Azure Site Recovery (scenariusz Hyper-V do Azure bez System Center VMM), Recovery Services vault, dostawca Azure Site Recovery i agent MARS na hv01 i hv02 (Windows Server 2022), moduł Az.RecoveryServices, Veeam Backup & Replication 13, AWS Elastic Disaster Recovery

Czas: ~90 min

Azure Site Recovery kopiuje dyski maszyn z klastra `hv01` i `hv02` do Azure na bieżąco i pozwala w kilkanaście minut uruchomić z nich maszyny w sieci DR. Ta strona prowadzi przez rejestrację hostów, politykę replikacji, test w izolowanej sieci, prawdziwe przełączenie i powrót do Pamiątkowa, także na nowy sprzęt. Na końcu porównujemy dwie drogi zastępcze: odtworzenie z Veeam do Azure i AWS Elastic Disaster Recovery.

ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu chronimy maszyny klastra `hvclu01` (`hv01` i `hv02`, Windows Server 2022, bez System Center VMM): `sql01` bez dysków bazy, `pg01`, `docker01`, `fs01` bez dysku migawek, `app01` oraz `dc02` tylko do testów. Magazyn `rsv-dr-pl` stoi w `polandcentral` w grupie `rg-dr`, sieć docelowa to `vnet-dr`, a testowa `vnet-dr-test`, tak jak na stronie Azure jako zapasowa serwerownia Zielonej: architektura, co replikujemy, a co odtwarzamy. Replikacja idzie przez internet z publicznego adresu `fw01` (203.0.113.10) po HTTPS, nie przez tunel. Wdrożenie planujemy po zakazie zmian, od 7 stycznia 2027.

Skróty użyte na tej stronie (17)

Skrót	Co znaczy

AWS	Amazon Web Services: chmura Amazonu
DR	Disaster Recovery: plan przywrócenia działania po poważnej awarii
DRS	Device Registration Service: usługa Entra ID, z którą komputer rejestruje się przy dołączaniu, jej testy pokazuje dsregcmd /status
FSMO	Flexible Single Master Operations: pięć zadań w Active Directory, które z założenia wykonuje tylko jeden kontroler domeny naraz
GB	Gigabyte: miliard bajtów, jednostka pojemności pamięci i plików, tu najczęściej rozmiar modelu albo pamięci karty graficznej
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
MARS	Microsoft Azure Recovery Services: agent kopii zapasowej instalowany na serwerach Windows, wysyłający pliki i foldery do magazynu Recovery Services
RPO	Recovery Point Objective: ile danych wolno stracić przy awarii
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
SQL	Structured Query Language: język zapytań do relacyjnych baz danych
USD	dolar amerykański, waluta cenników AWS
VM	Virtual Machine: maszyna wirtualna
VMM	System Center Virtual Machine Manager: konsola Microsoftu do zarządzania wieloma hostami i klastrami Hyper-V; Azure Site Recovery działa z nią albo bez niej
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
VSS	Volume Shadow Copy Service: mechanizm Windows do tworzenia spójnych migawek danych mimo działających w tle usług, wykorzystywany też przy kopiach zapasowych kontrolera domeny
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Polecenia PowerShell z modułem Az wykonujemy na stacji administratora zalogowanej do subskrypcji (`Connect-AzAccount`), kontem z rolą Site Recovery Contributor albo wyższą. Polecenia instalatora i `Set-OBMachineSetting` wykonujemy na każdym hoście Hyper-V jako administrator lokalny.

> **□□ ZMIENIA SYSTEM**

Ustawienie magazynu jako kontekstu: Set-AzRecoveryServicesAsrVaultContext

```
$magazyn = Get-AzRecoveryServicesVault -Name NazwaMagazynu -ResourceGroupName NazwaGrupyZasobow
Set-AzRecoveryServicesAsrVaultContext -Vault $magazyn
```

Każde kolejne polecenie `*-AzRecoveryServicesAsr*` działa na tym magazynie. Bez kontekstu polecenia zwracają błąd albo pusty wynik.

□□ ZMIENIA SYSTEM

Utworzenie witryny Hyper-V: New-AzRecoveryServicesAsrFabric

```
New-AzRecoveryServicesAsrFabric -Type HyperVSite -Name NazwaWitryny
```

Witryna (Hyper-V site) to grupa hostów, które rejestrujemy w magazynie. Wszystkie węzły klastra muszą być w tej samej witrynie, u nas `hvclu01-site` z `hv01` i `hv02`.

□□ TYLKO ODCZYT

Pobranie pliku rejestracji hosta: Get-AzRecoveryServicesVaultSettingsFile

```
$id = Get-AzRecoveryServicesAsrFabric -Name NazwaWitryny | Select-Object -ExpandProperty SiteIdentifier
Get-AzRecoveryServicesVaultSettingsFile -Vault $magazyn -SiteIdentifier $id -SiteFriendlyName NazwaWitryny
```

Plik z kluczem rejestracji jest ważny pięć dni. Kopiujemy go na każdy host i usuwamy po rejestracji, bo pozwala dopisać obcy serwer do naszego magazynu.

□□ **id** = pokaż użytkownika, jego numer UID oraz grupy, do których należy

□□ TYLKO ODCZYT

Instalacja dostawcy na hoście bez pulpitu: setupdr.exe /i

```
AzureSiteRecoveryProvider.exe /x:. /q
.\setupdr.exe /i
"C:\Program Files\Microsoft Azure Site Recovery Provider\DRConfigurator.exe" /r
/Friendlyname "NazwaHosta" /Credentials "SciezkaDoPlikuRejestracji"
```

Pierwsze polecenie rozpakowuje instalator, drugie instaluje dostawcę razem z agentem MARS, trzecie rejestruje host w magazynie. Na hoście z pulpitem to samo robi kreator. Log instalacji leży w `%Programdata%\ASRLogs\DRASetupWizard.log`, a host pojawia się w portalu po czas do 30 minut.

MARS = Microsoft Azure Recovery Services: agent kopii zapasowej instalowany na serwerach Windows, wysyłający pliki i foldery do magazynu Recovery Services

ZMIENIA SYSTEM

Utworzenie polityki replikacji: New-AzRecoveryServicesAsrPolicy

```
New-AzRecoveryServicesAsrPolicy -Name NazwaPolityki -ReplicationProvider
HyperVReplicaAzure -ReplicationFrequencyInSeconds 300 -NumberOfRecoveryPointsToRetain 24
-ApplicationConsistentSnapshotFrequencyInHours 1 -RecoveryAzureStorageAccountId
IdKontaMagazynu
```

> (gdzie `ReplicationFrequencyInSeconds` przyjmuje według dokumentacji polecenia wartości 30, 300 i 900; liczbę punktów i jej górną granicę dla Hyper-V sprawdzamy w portalu przy tworzeniu polityki, a `IdKontaMagazynu` dotyczy wariantu z kontem magazynu: przy dyskach zarządzanych ustawiamy je przy włączaniu ochrony maszyny)

Polityka mówi, jak często wysyłamy zmiany, ile punktów odtworzenia trzymamy i jak często robimy punkt spójny aplikacyjnie. Jedna polityka wystarcza dla całej witryny.

TYLKO ODCZYT

Sprawdzenie stanu chronionych maszyn: Get-AzRecoveryServicesAsrReplicationProtectedItem

```
$kontener = Get-AzRecoveryServicesAsrFabric -Name NazwaWitryny | Get-
AzRecoveryServicesAsrProtectionContainer
```

```
Get-AzRecoveryServicesAsrReplicationProtectedItem -ProtectionContainer $kontener |
Select-Object FriendlyName, ProtectionState, ReplicationHealth
```

Codzienna kontrola: każda maszyna powinna mieć stan ochrony „Protected” i zdrowie „Normal”. Ostrzeżenie zdrowia zwykle znaczy, że RPO rośnie, bo łącze nie nadąża.

RPO = Recovery Point Objective: ile danych wolno stracić przy awarii

ZMIENIA SYSTEM

Ograniczenie pasma replikacji w godzinach pracy: Set-OBMachineSetting

```
Set-OBMachineSetting -WorkDay ([System.DayOfWeek]::Monday),
([System.DayOfWeek]::Tuesday), ([System.DayOfWeek]::Wednesday),
([System.DayOfWeek]::Thursday), ([System.DayOfWeek]::Friday) -StartWorkHour "6:00:00" -
EndWorkHour "18:00:00" -WorkHourBandwidth (5120*1024) -NonWorkHourBandwidth (20480*1024)
```

> (wartości pasma podajemy tak jak w przykładzie Microsoftu, jako iloczyn z 1024; jednostkę potwierdzamy w dokumentacji, zanim policzymy, ile to megabitów)

Wykonujemy na każdym hoście, bo limit dotyczy agenta MARS na danym hoście. W godzinach pracy replikacja nie może zabrać łącza, którym idą Optima przez VPN handlowców i poczta.

MARS = Microsoft Azure Recovery Services: agent kopii zapasowej instalowany na serwerach Windows, wysyłający pliki i foldery do magazynu Recovery Services · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej

TYLKO ODCZYT

Sprawdzenie sterowników Hyper-V w obrazie startowym Linuksa: lsinitrd

```
sudo lsinitrd | grep -E "hv_(vmbus|storvsc|netvsc)"
```

Wykonujemy na `docker01`, `pg01` i `app01` przed włączeniem ochrony. Maszyna w Azure startuje na tych samych sterownikach co w Hyper-V, więc brak `hv_storvsc` w obrazie

startowym kończy się systemem, który nie widzi dysku.

lsinitrd = list initramfs: wypisuje zawartość obrazu startowego Linuksa, na przykład czy są w nim sterowniki Hyper-V

ZMIENIA SYSTEM

Test przełączenia w izolowanej sieci: Start-AzRecoveryServicesAsrTestFailoverJob

```
$siecTestowa = Get-AzVirtualNetwork -Name NazwaSieciTestowej -ResourceGroupName NazwaGrupyZasobow
$element = Get-AzRecoveryServicesAsrReplicationProtectedItem -ProtectionContainer $kontener -FriendlyName NazwaMaszyny
Start-AzRecoveryServicesAsrTestFailoverJob -ReplicationProtectedItem $element -Direction PrimaryToRecovery -AzureVMNetworkId $siecTestowa.Id
```

Tworzy kopię maszyny w sieci testowej z wybranego punktu, a replikacja z Pamiątkowa trwa dalej. Produkcja nic nie zauważa, płacimy tylko za czas działania maszyny testowej.

ZMIENIA SYSTEM

Sprzątanie po teście: Start-AzRecoveryServicesAsrTestFailoverCleanupJob

```
Start-AzRecoveryServicesAsrTestFailoverCleanupJob -ReplicationProtectedItem $element -Comment "Test DR zaliczony, protokol w GLPI"
```

Usuwa maszynę testową i jej dyski. Dopóki test nie jest posprzątany, kolejnego testu tej maszyny nie uruchomimy.

DR = Disaster Recovery: plan przywrócenia działania po poważnej awarii · **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

ZMIENIA SYSTEM

Przełączenie awaryjne: Start-AzRecoveryServicesAsrUnplannedFailoverJob

```
Start-AzRecoveryServicesAsrUnplannedFailoverJob -ReplicationProtectedItem $element -
Direction PrimaryToRecovery
```

Uruchamia maszynę w `vnet-dr` z ostatniego dostępnego punktu albo punktu, który wskażemy. Używamy go tylko po decyzji o przełączeniu z planu ciągłości, nigdy „na próbę”.

ZMIENIA SYSTEM

Zatwierdzenie przełączenia: Start-AzRecoveryServicesAsrCommitFailoverJob

```
Start-AzRecoveryServicesAsrCommitFailoverJob -ReplicationProtectedItem $element
```

Po zatwierdzeniu nie da się już wybrać innego punktu odtworzenia. Zatwierdzamy dopiero wtedy, gdy właściciel usługi potwierdzi, że dane są dobre.

OSTROŻNIE · NIEODWRACALNE

Zmiana rekordu DNS maszyny linuksowej po przełączeniu: Add-DnsServerResourceRecordA

```
Remove-DnsServerResourceRecord -ZoneName NazwaStrefy -Name NazwaHosta -RRType A -Force
Add-DnsServerResourceRecordA -ZoneName NazwaStrefy -Name NazwaHosta -IPv4Address
NowyAdres
```

Wykonujemy na `dc-az01`. Maszyny Windows rejestrują nowy adres same, linuksy w Zielonej mają rekordy statyczne, więc zmieniamy je ręcznie według karty odtworzenia.

Przykład (poglądowy, `docker01` po przełączeniu):

```
HostName  RecordType Timestamp TimeToLive RecordData
--------  ---------- --------- ---------- ----------
docker01  A          0         00:05:00   10.31.10.42
```

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

KLIKAMY W INTERFEJSIE

Ścieżka w portalu do testu przełączenia

```
Portal Azure → Recovery Services vaults → rsv-dr-pl → Replicated items → docker01 → Test failover
```

Ten sam ekran ma przyciski Failover, Commit, Planned failover i Reverse replicate, potrzebne przy przełączeniu i powrocie.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Replicated items w magazynie `rsv-dr-pl` po pierwszej replikacji, widoczne wiersze `sql01`, `pg01`, `docker01`, `fs01`, `app01` i `dc02` ze stanem Protected i kolumną RPO, zaznaczona kolumna Replication health.

◫ **RPO** = Recovery Point Objective: ile danych wolno stracić przy awarii

Z życia wzięte

◫ Z ŻYCIA WZIĘTE

Wtorek, 2 lutego 2027, 17:20, pierwszy test DR. Tomek uruchamia test przełączenia `pg01` i `docker01` w `vnet-dr-test`, a po kwadransie Gitea w teście odpowiada, tylko bez logowania. Okazuje się, że Gitea pyta Active Directory, a w sieci testowej nie ma kontrolera, bo kopię `dc02` zaplanowaliśmy na następny tydzień. Wniosek trafia do protokołu: w teście najpierw `dc02`, przejęcie ról FSMO na kopii, dopiero potem aplikacje, dokładnie w tej kolejności, którą zaleca Microsoft.

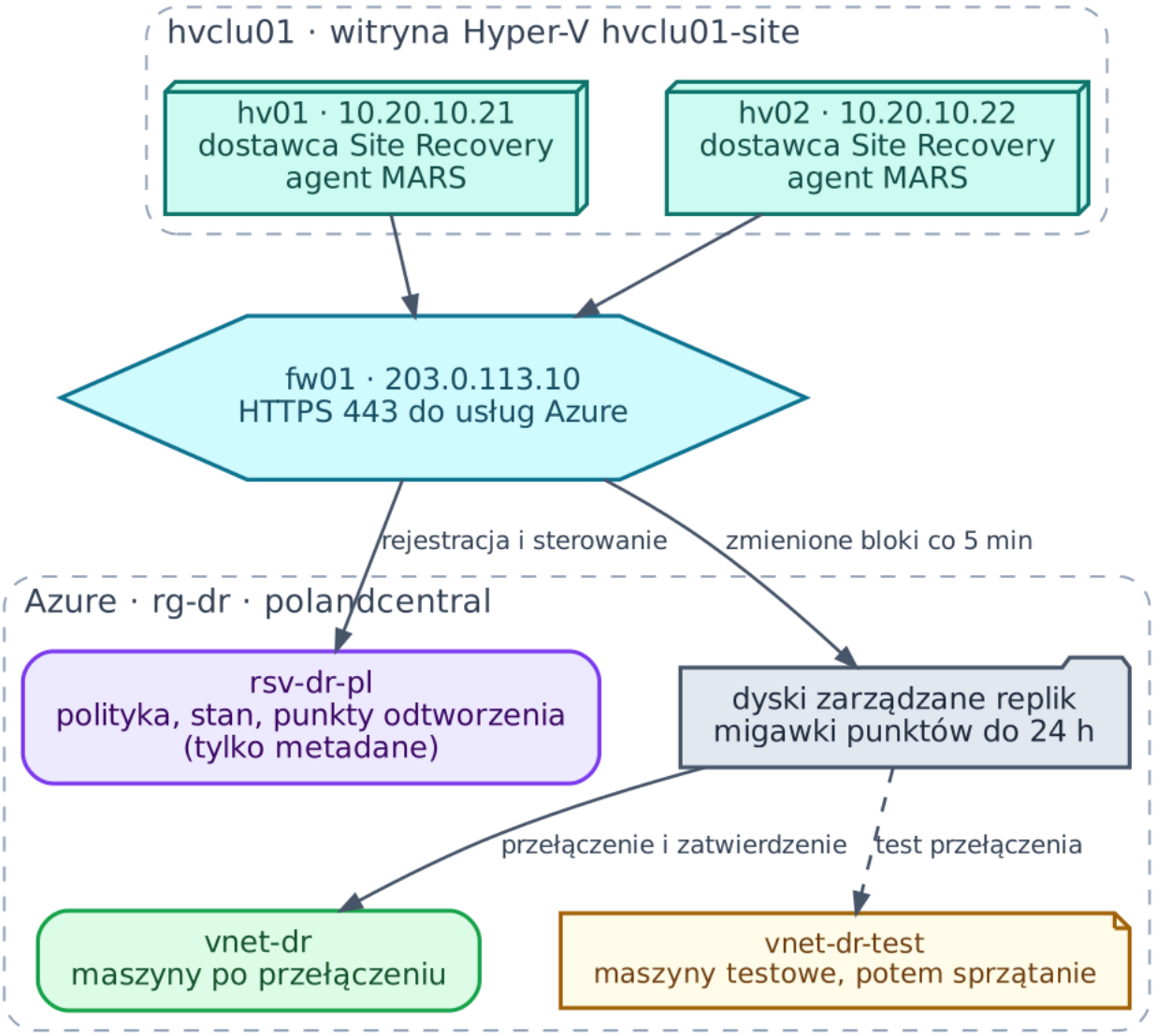
Jak to działa

◫ Rozwiń: jak to działa pod spodem

Składniki

Na każdym hoście klastra instalujemy dostawcę Azure Site Recovery i agenta Recovery Services (MARS), który instaluje się razem z dostawcą. Host korzysta z mechanizmu replikacji

Hyper-V i wysyła zmienione bloki dysków przez HTTPS do Azure, gdzie lądują w dyskach zarządzanych repliki. Magazyn `rsv-dr-pl` trzyma politykę, stan i punkty odtworzenia, a do usługi Site Recovery trafiają tylko metadane, nie dane maszyn.



Rysunek 1. Składniki Azure Site Recovery dla Hyper-V bez VMM: na hv01 i hv02 dostawca i agent MARS wysyłają zmiany przez HTTPS z fw01 do dysków zarządzanych w Azure, magazyn rsv-dr-pl trzyma politykę i punkty odtworzenia, a z replik powstają maszyny w vnet-dr przy przełączeniu albo w vnet-dr-test przy teście (kliknięcie otwiera pełny rozmiar)

Pojęcie: punkt odtworzenia. Stan dysków maszyny z konkretnej chwili, z którego Site Recovery może utworzyć maszynę. Punkt spójny awaryjnie odpowiada nagłemu wyłączeniu prądu, a punkt spójny aplikacyjnie powstaje po krótkim zamrożeniu zapisu przez aplikacje (VSS w Windows), więc bazy w środku są w porządku.

Pojęcie: przełączenie awaryjne (failover) i powrót (failback). Przełączenie uruchamia usługę w miejscu zapasowym z repliki. Powrót to planowane przełączenie w drugą stronę, z Azure do serwerowni, po usunięciu przyczyny awarii.

Co mówi dokumentacja (stan z 1 listopada 2026)

Pytanie	Odpowiedź	Źródło
Hosty bez VMM	Windows Server 2025, 2022, 2019, 2016 i 2012 R2 z aktualizacjami, także Server Core	macierz obsługi [1]
Klaster	obsługiwany, wszystkie węzły w jednym magazynie i jednej witrynie Hyper-V	często zadawane pytania [2]
Częstotliwość wysyłania	co 30 sekund (poza dyskami premium) albo co 5 minut; polecenie PowerShell przyjmuje też 900 sekund	[2], [4]
Retencja punktów	dla Hyper-V do Azure do 24 godzin według podręcznika AZ-801 (stan z dnia wydania); ogólne pytania Site Recovery podają 15 dni dla dysków zarządzanych w innych scenariuszach	[6], [3]
Punkt spójny aplikacyjnie	co najmniej co godzinę	[6]
Dyski	do 64 dysków na maszynę, dysk danych do 32 767 GiB, wykluczanie dysków obsługiwane, 4Kn nie	[1]
Generacja 2	obsługiwana, gdy rozmiar maszyny w Azure obsługuje generację 2; UEFI tak, Secure Boot nie; starsze pytania mówią o zamianie na generację 1 przy przełączeniu, co sprawdzamy w teście	[1], [2]

Pytanie	Odpowiedź	Źródło
Niewspierane w maszynie	BitLocker, dyski współdzielone, Storage Spaces wewnątrz maszyny, Trusted Launch	[1]
Szybkość zmian	do 54 MB/s na maszynę	[1]
Powrót	przy dyskach zarządzanych, agent MARS od wersji 2.0.9214, także na inny host	[5], [7]

> ⚠ Autor w swojej praktyce zakładał retencję punktów odtworzenia 12 miesięcy. Site Recovery tego nie daje: punkty żyją godziny (Hyper-V) albo najwyżej dni, bo usługa służy do szybkiego uruchomienia maszyn, a nie do cofania się o miesiące. Dwanaście miesięcy wstecz zapewniają w Zielonej kopie: restic i Veeam z niezmiennością według kp1-01 oraz kopie baz w Azure Blob. Usługą replikacji z długą retencją jest AWS Elastic Disaster Recovery (do 365 dni, tabela niżej).

Polityka dla Zielonej

Ustawienie	Wartość	Dlaczego
Częstotliwość wysyłania	5 minut	30 sekund nie poprawi RPO po pożarze w sposób, który zauważy właściciel, a obciąży łącze; 15 minut tylko, gdy łącze nie nadąża
Retencja punktów	najwyższa dostępna w portalu (do 24 godzin)	pozwala cofnąć się przed zaszyfrowanie zauważone rano, o ile atak trwał krócej niż doba
Punkt spójny aplikacyjnie	co godzinę	`fs01` i bazy w kontenerach na `docker01` dostają co godzinę stan po zamrożeniu zapisu
Pierwsza replikacja	wieczorem w dzień roboczy, maszyny po kolei	3,4 TB przydzielonych dysków przy 150 Mb/s to około 51 godzin (rachunek na stronie o wymiarowaniu), więc nie wszystko naraz
Dyski docelowe	dyski zarządzane SSD Standard dla systemów, HDD Standard dla `D:` na `fs01`	koszt kontra czas startu, decyzja po teście

Kolejność w planie odzyskiwania

> **Pojęcie: plan odzyskiwania (recovery plan).** Lista maszyn w Site Recovery podzielona na grupy, które przełączają się po kolei, z możliwością dołożenia kroków ręcznych i skryptów między grupami. Zamienia kilkanaście kliknięć w jedno przełączenie z przewidywalną kolejnością.

Grupa	Maszyny	Krok przed grupą	Krok po grupie
0 (poza planem)	`dc-az01` działa stale	przejęcie ról FSMO na `dc-az01`, gdy Pamiątkowo nie wróci szybko	sprawdzenie `repadmin /replsummary`
1	`pg01`, `sql01`	decyzja o przełączeniu, zapis godziny zero	odtworzenie `CDN_Zielona` z kopii w Blob, zmiana rekordu `pg01`
2	`ora-dr01` (start maszyny przygotowanej, poza Site Recovery)	pobranie kopii RMAN	odtworzenie `WMSPRD`, rekord WMS, test skanera w Swarzędzu
3	`docker01`, `app01`, `fs01`	brak	rekordy A linuksów, zmiana celu poczty na `edge-az01`, test logowania przez Traefik

Test przełączenia krok po kroku

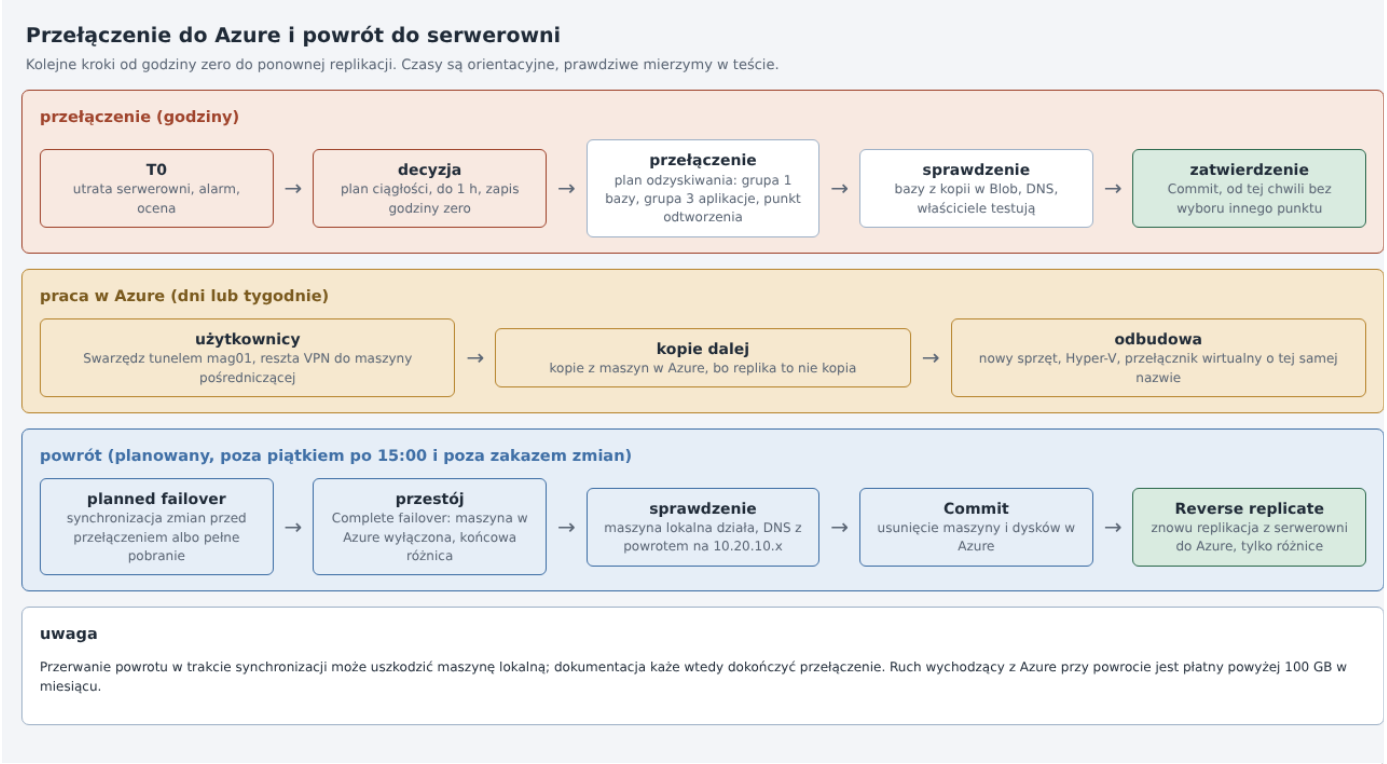
Test robimy co kwartał we wtorkowym oknie 17:00 do 20:00, poza zakazem zmian od 15 listopada do 6 stycznia, z protokołem z macierzy wysokiej dostępności.

1. Sprawdzamy, że `vnet-dr-test` nie ma peeringu ani tunelu (`az network vnet peering list`).
2. Test `dc02`: maszyna startuje w sieci testowej, przejmujemy na niej role FSMO (`Move-ADDirectoryServerOperationMasterRole` z opcją `-Force`), sprawdzamy `dcdiag /v` i udziały `SYSVOL` i `NETLOGON` poleceniem `net share`.
3. Test `pg01` i `sql01`, potem odtworzenie bazy `CDN_Zielona` z kopii w maszynie testowej według strony o bazach.
4. Test `docker01`, `app01` i `fs01`. Logujemy się z maszyny pomocniczej w sieci testowej (osobna maszyna z przeglądarką albo Azure Bastion w `vnet-dr-test`).
5. Właściciele sprawdzają swoje usługi: pani Halina otwiera Optimę, Ola Gitea, Marek raport z WMS (gdy test obejmuje `ora-dr01`).

6. Zapisujemy zmierzone RTO i RPO, sprzątamy test (cleanup) dla każdej maszyny i zamykamy zmianę w GLPI.

Przełączenie i powrót

Przełączenie wykonujemy z planu odzyskiwania albo maszyna po maszynie. Powrót to planowane przełączenie z Azure do serwerowni, z jednym z dwóch sposobów synchronizacji: tylko zmiany przed przełączeniem (maszyna w Azure pracuje, wyłącza się tylko na końcową różnicę) albo pełne pobranie w trakcie przełączenia (szybszy start, dłuższy przestój; Microsoft poleca je, gdy Azure pracował miesiąc lub dłużej albo maszyny lokalnej już nie ma).



Rysunek 2. Oś przełączenia i powrotu: godzina zero, decyzja, przełączenie z wybranego punktu, sprawdzenie i zatwierdzenie, praca w Azure, odbudowa serwerowni, planowane przełączenie z synchronizacją, przestój na końcową różnicę, zatwierdzenie i ponowna replikacja do Azure (kliknięcie otwiera pełny rozmiar)

Po pożarze stary sprzęt nie wraca, więc powrót idzie na nowy host. Dokumentacja opisuje to jako powrót do innej lokalizacji: na nowym serwerze instalujemy Windows Server z rolą Hyper-V, tworzymy przełącznik wirtualny o tej samej nazwie co na starym, a w planowanym przełączeniu zaznaczamy utworzenie maszyny lokalnej, jeśli nie istnieje. Po zatwierdzeniu Site Recovery usuwa maszynę w Azure i jej dyski, a odwrotna replikacja wysyła już tylko zmiany od wyłączenia maszyny w Azure.

> ⚠ Przerwanie powrotu w trakcie synchronizacji może uszkodzić maszynę lokalną tak, że nie wystartuje; dokumentacja każe wtedy uruchomić przełączenie jeszcze raz i dokończyć synchronizację. Powrotu nie planujemy więc na piątek po 15:00.

Koszty

Cennik Site Recovery liczy opłatę za każdą chronioną maszynę miesięcznie, a każda maszyna ma pierwsze 31 dni bez opłaty za usługę. Strona cennika w dniu odczytu nie pokazywała kwoty bez wybrania regionu i waluty; odpowiedź na Microsoft Q&A z 10 września 2025 roku podaje około 25 USD miesięcznie za maszynę chronioną do Azure, co sprawdzamy w kalkulatorze przed zakupem. Osobno płacimy za dyski replik, migawki punktów odtworzenia, transakcje magazynu, maszyny w teście i w awarii oraz ruch wychodzący przy powrocie (pierwsze 100 GB miesięcznie bez opłaty, potem według cennika transferu). Rachunek dla Zielonej jest na stronie Wymiarowanie i zakup zapasowej serwerowni w Azure: pojemność, koszty i zapytanie do partnera.

Licencje systemów i baz po przełączeniu to osobny temat. Maszyna Windows uruchomiona w Azure płaci za licencję w cenie godziny, chyba że korzystamy z Azure Hybrid Benefit. Dla SQL Server Microsoft opisuje bezpłatną pasywną replikę DR w Azure dla klientów z Software Assurance, ale tekst dotyczy replik, a nie przełączenia z Site Recovery, więc prawo do niej przy naszym układzie potwierdzamy u partnera (do potwierdzenia).

Drogi zastępcze: Veeam do Azure i AWS Elastic Disaster Recovery

	Azure Site Recovery	Veeam: Restore to Microsoft Azure	AWS Elastic Disaster Recovery
Skąd dane	ciągła replikacja z hostów Hyper-V	kopie z repozytoriów `vbr01` (na `bkp01`, `bkp02` albo w chmurze)	ciągła replikacja agentem w każdej maszynie
RPO po katastrofie	minuty	wiek ostatniej kopii (u nas noc)	sekundy do minut; punkty co 10 minut przez godzinę, co godzinę przez dobę
RTO	kilkanaście minut na maszynę po decyzji	godziny: konwersja dysków i wysyłka do Azure w chwili awarii	minuty na serwer według producenta

	Azure Site Recovery	Veeam: Restore to Microsoft Azure	AWS Elastic Disaster Recovery
Retencja wstecz	godziny	tyle, ile retencja kopii (12 miesięcy możliwe)	punkty dzienne od 1 do 365 dni
Koszt stały	licencja za maszynę i dyski replik	licencja Veeam (już planowana w kp2-03) i magazyn kopii	0,028 USD za serwer za godzinę (cennik AWS, odczyt 1.11.2026), dyski przejściowe EBS, migawki i serwery replikacji
Linux	każdy system obsługiwany w Azure	systemy obsługiwane w Azure; dla Linuksa maszyna pomocnicza	lista dystrybucji: Rocky Linux 8 i tylko 9.7 z gałęzi 9
Bez Microsoftu	nie	częściowo (narzędzie niezależne, cel Azure)	tak

Veeam w tej roli jest tańszy na co dzień, ale RTO liczymy w godzinach i dniach, bo dyski powstają w Azure dopiero po awarii. AWS Elastic Disaster Recovery to najbliższy odpowiednik Site Recovery poza Microsoftem i jedyny z tej trójki, który sam trzyma punkty odtworzenia do roku; wymaga jednak agenta w każdej maszynie i własnej sieci w AWS, której Zielona dziś produkcyjnie nie ma.

Częste błędy

Objaw	Przyczyna	Co robimy
Host nie pojawia się w portalu po rejestracji	brak wyjścia HTTPS do usług Azure albo minęło mniej niż 30 minut	sprawdzamy log `DRASetupWizard.log` i reguły `fw01` dla `hv01` i `hv02`
Po migracji maszyny na drugi węzeł replikacja stoi	drugi węzeł nie jest zarejestrowany w tej samej witrynie	rejestrujemy wszystkie węzły klastra w jednej witrynie
Nie da się włączyć ochrony `fs01`	BitLocker albo dysk współdzielony w maszynie	wyłączamy BitLocker w maszynie (szyfrowanie zapewnia magazyn Azure) albo wykluczamy dysk
Zdrowie replikacji „Warning”, RPO rośnie w zamknięciu miesiąca	szybkość zmian przekracza łącze albo limit 54 MB/s na maszynę	limity pasma w nocy wyżej, częstotliwość 15 minut dla tej maszyny, dyski bazy poza replikacją
Linux w teście nie startuje, brak dysku	brak sterowników Hyper-V w obrazie startowym	`lsinitrd`, dopisanie modułów do dracut i odbudowa obrazu przed kolejną replikacją
Kolejny test niemożliwy	poprzedni test nie został posprzątany	`Start-AzRecoveryServicesAsrTestFailoverCleanupJob` dla każdej maszyny

Objaw	Przyczyna	Co robimy
Gitea w teście bez logowania	brak kontrolera w sieci testowej	test `dc02` jako pierwsza grupa, role FSMO przejęte na kopii

Ćwiczenia

1. Właściciel `fs01` pyta, czy po ataku szyfrującym zauważonym po trzech dniach odtworzymy pliki z Site Recovery. Co odpowiadamy?

Odpowiedź

Nie: punkty odtworzenia Hyper-V do Azure żyją do 24 godzin, a zaszyfrowane pliki replikują się do Azure jak każda inna zmiana. Po trzech dniach odtwarzamy z kopii restic z repozytorium `pliki` (poziom retencji według kp1-01), najlepiej z kopii niezmiennej.

1. Pierwsza replikacja `fs01` (2,1 TB) ma się zmieścić w nocach. Jaką kolejność i ustawienia proponujemy?

Odpowiedź

`fs01` jako osobna partia, po mniejszych maszynach, z limitem pasma w dzień (`Set-OBMachineSetting`) i pełnym pasmem w nocy i weekend. Przy 150 Mb/s 2,1 TB to około 31 godzin czystego transferu, więc liczymy kilka nocy i weekend; dysk migawek `E:` wykluczamy z replikacji.

1. Dlaczego w teście przełączenia nie uruchamiamy kopii obu kontrolerów domeny?

Odpowiedź

Microsoft zaleca, żeby w teście nie odtwarzać wszystkich kontrolerów: wystarczy jeden z katalogiem globalnym, na którym przejmujemy potrzebne role FSMO. Mniej kopii kontrolerów to mniej sprzątania metadanych i mniejsze ryzyko pomyłki, a test i tak odbywa się w sieci bez połączenia z produkcją.

1. Serwerownia spłonęła, pracujemy w Azure od trzech tygodni, przyszły nowe serwery. Który sposób synchronizacji wybieramy przy powrocie i dlaczego?

Odpowiedź

Maszyn lokalnych już nie ma, więc powrót idzie do innej lokalizacji z utworzeniem maszyny lokalnej. Dokumentacja dla takiego przypadku poleca synchronizację przed przełączeniem: dane płyną, gdy Azure jeszcze pracuje, a przestój dotyczy tylko końcowej różnicy. Pełne pobranie w trakcie przełączenia ma sens, gdy Azure pracuje miesiąc lub dłużej albo gdy liczy się prostota kosztem dłuższego przestoju.

Powiązane: Azure jako zapasowa serwerownia Zielonej: architektura, co replikujemy, a co odtwarzamy · Bazy w zimnym archiwum Azure: kopie sql01 i ora01, niezmienność i odtworzenie do punktu w czasie · Monitorowanie i kopie: Azure Monitor, KQL, alerty, Backup i Site Recovery · Odporne architektury, część 2: RDS Multi-AZ, Aurora, AWS Backup i strategie DR · Kopie hostów Dockera narzędziami do kopii: Veeam i odpowiedniki · Hyper-V na co dzień: przełącznik, maszyny, punkty kontrolne i migracja

Źródła (odczyt 1 listopada 2026):

1. learn.microsoft.com, „Support for disaster recovery of Hyper-V VMs to Azure with Azure Site Recovery”, aktualizacja 15 października 2026.
2. learn.microsoft.com, „Common questions for Hyper-V disaster recovery with Azure Site Recovery”, aktualizacja 10 sierpnia 2026 (replikacja co 30 s albo 5 min, klaster, powrót z synchronizacją).
3. learn.microsoft.com, „General questions about Azure Site Recovery” (15 dni przy dyskach zarządzanych, 31 dni bez opłaty, koszt testu), aktualizacja 13 czerwca 2025.
4. learn.microsoft.com, polecenie `New-AzRecoveryServicesAsrPolicy` (wartości 30, 300, 900) oraz „Hyper-V VM disaster recovery using Azure Site Recovery and PowerShell” (witryna, plik rejestracji, test i sprzątanie).
5. learn.microsoft.com, „Set up Hyper-V disaster recovery by using Azure Site Recovery” (dostawca z agentem MARS, klucz ważny 5 dni, do 30 minut na pojawienie się hosta, MARS od 2.0.9214 do powrotu), aktualizacja 5 maja 2026.
6. microsoftpressstore.com, rozdział o Azure Site Recovery z podręcznika do egzaminu AZ-801, strony 3 i 4 (częstotliwość od 30 sekund do 5 minut, retencja do 24 godzin, punkt aplikacyjny co najmniej co godzinę).
7. learn.microsoft.com, „Failback of Hyper-V VMs from Azure to on-premises” (dwa sposoby synchronizacji, powrót do innej lokalizacji, ostrzeżenie o przerwaniu).
8. learn.microsoft.com, „How to manage on-premises to Azure protection network bandwidth usage” (`Set-OBMachineSetting`, `UploadThreadsPerVM`).
9. azure.microsoft.com, cennik Site Recovery (opłata za chronioną maszynę, 31 dni) i cennik transferu (ruch przychodzący bez opłaty, 100 GB wychodzących miesięcznie bez opłaty); learn.microsoft.com/answers, odpowiedź z 10 września 2025 (około 25 USD za maszynę do Azure).
10. learn.microsoft.com, „High availability and disaster recovery for SQL Server on Azure VMs” (pasywna replika DR z Software Assurance).

11. aws.amazon.com, cennik AWS Elastic Disaster Recovery (0,028 USD za serwer za godzinę); docs.aws.amazon.com, „Point in time (PIT) policy” (1 do 365 dni) i „AWS DRS supported Linux operating systems” (Rocky Linux 8 i 9.7).
12. helpcenter.veeam.com, „Restore to Microsoft Azure” (Veeam Backup & Replication 13, osobny przebieg dla Windows i Linuksa, maszyna pomocnicza).

Revision #2
Created 2026-11-01 18:02:22 UTC by Tomasz Konieczny
Updated 2026-11-01 18:03:46 UTC by Tomasz Konieczny