

J. C. Mackin
Orin Thomas

Egzamin 70-412

Konfigurowanie zaawansowanych usług Windows Server® 2012 R2

Przekład: Krzysztof Kapustka

APN Promise, Warszawa 2014

Egzamin 70-412: Konfigurowanie zaawansowanych usług Windows Server® 2012 R2
© 2014 APN PROMISE SA

Authorized Polish translation of the English edition Exam Ref 70-412: Configuring
Advanced Windows Server 2012 R2 Services, ISBN: 978-0-7356-7361-8
Copyright © 2014 J.C. Mackin (Content); Orin Thomas (Content)

This translation is published and sold by permission of O'Reilly Media, Inc., which owns
or controls all rights to publish and sell the same.

APN PROMISE SA, biuro: ul. Kryniczna 2, 03-934 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana
ani rozpowszechniana w jakiegokolwiek formie i w jakikolwiek sposób (elektroniczny,
mechaniczny), włącznie z fotokopiowaniem, nagrywaniem na taśmy lub przy użyciu
innych systemów bez pisemnej zgody wydawcy.

Książka ta przedstawia poglądy i opinie autorów. Przykłady firm, produktów, osób
i wydarzeń opisane w niniejszej książce są fikcyjne i nie odnoszą się do żadnych
konkretnych firm, produktów, osób i wydarzeń, chyba że zostanie jednoznacznie
stwierdzone, że jest inaczej. Ewentualne podobieństwo do jakiegokolwiek rzeczywistej
firmy, organizacji, produktu, nazwy domeny, adresu poczty elektronicznej, logo, osoby,
miejsca lub zdarzenia jest przypadkowe i niezamierzone.

Nazwa Microsoft oraz znaki towarowe wymienione na stronie <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> są zastrzeżonymi znakami
towarowymi grupy Microsoft. Wszystkie inne znaki towarowe są własnością ich
odnośnych właścicieli.

APN PROMISE SA dołożyła wszelkich starań, aby zapewnić najwyższą jakość tej
publikacji. Jednakże nikomu nie udziela się rękojmi ani gwarancji.
APN PROMISE SA nie jest w żadnym wypadku odpowiedzialna za jakiegokolwiek szkody
będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet
jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-113-3

Przekład: Krzysztof Kapustka
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

<i>Wprowadzenie</i>	ix
---------------------------	----

1 Konfiguracja i zarządzanie wysoką dostępnością	1
---	---

Zagadnienie 1.1: Konfigurowanie równoważenia obciążenia sieciowego	2
---	---

Podstawy równoważenia obciążenia sieciowego	2
Tworzenie i konfigurowanie klastra NLB	3
Konfigurowanie reguł portów	9
Uaktualnianie klastra NLB	15
Podsumowanie zagadnienia	17
Pytania kontrolne	18

Zagadnienie 1.2: Konfigurowanie klastra pracy awaryjnej	19
--	----

Podstawy klastrów pracy awaryjnej	19
Tworzenie klastra pracy awaryjnej	22
Konfigurowanie sieci klastra	25
Klastry odłączone od Active Directory	26
Konfigurowanie magazynu danych klastra	27
Konfigurowanie kworum	34
Implementowanie aktualizacji typu Cluster-Aware	36
Migrowanie klastra pracy awaryjnej	40
Podsumowanie zagadnienia	42
Pytania kontrolne	43

Zagadnienie 1.3: Zarządzanie rolami klastra pracy awaryjnej	45
--	----

Konfigurowanie ról	45
Przypisywanie priorytetów uruchamiania roli	50
Opróżnianie węzła	51
Monitorowanie usług na klastrowanych maszynach wirtualnych	52
Podsumowanie zagadnienia	57
Pytania kontrolne	58

Zagadnienie 1.4: Zarządzanie ruchem maszyny wirtualnej	60
---	----

Wykonywanie migracji na żywo	60
Dodatkowe rozważania dotyczące migracji	70
Korzystanie z migracji magazynu	74
Konfigurowanie ochrony kondycji sieci maszyny wirtualnej	76
Konfigurowanie opróżniania przy zamykaniu	77
Podsumowanie zagadnienia	78
Pytania kontrolne	78

Odpowiedzi	81
Zagadnienie 1.1: Eksperyment myślowy	81
Zagadnienie 1.1: Pytania kontrolne	81
Zagadnienie 1.2: Eksperyment myślowy	83
Zagadnienie 1.2: Pytania kontrolne	83
Zagadnienie 1.3: Eksperyment myślowy	84
Zagadnienie 1.3: Pytania kontrolne	84
Zagadnienie 1.4: Eksperyment myślowy	86
Zagadnienie 1.4: Pytania kontrolne	86
2 Konfiguracja rozwiązań plików i magazynu	89
Zagadnienie 2.1: Konfigurowanie zaawansowanych usług plików	90
Czym jest BranchCache?	90
Konfigurowanie funkcji BranchCache	94
Korzystanie z menedżera File Server Resource Manager	100
Implementowanie inspekcji dostępu do plików	104
Instalowanie komponentu serwera systemu plików NFS	105
Podsumowanie zagadnienia	107
Pytania kontrolne	108
Zagadnienie 2.2: Implementowanie dynamicznej kontroli dostępu	110
Wprowadzenie do kontroli DAC	110
Konfigurowanie uwierzytelniania opartego na oświadczeniach	112
Konfigurowanie klasyfikacji plików	116
Konfigurowanie zasad dostępu	126
Podsumowanie zagadnienia	132
Pytania kontrolne	133
Zagadnienie 2.3: Konfigurowanie i optymalizowanie magazynu	135
Magazyn iSCSI	135
Korzystanie z funkcji na żądanie	146
Instalowanie komponentu Data Deduplication	149
Korzystanie z magazynów warstwowych	152
Podsumowanie zagadnienia	154
Pytania kontrolne	155
Odpowiedzi	156
Zagadnienie 2.1: Eksperyment myślowy	156
Zagadnienie 2.1: Pytania kontrolne	156
Zagadnienie 2.2: Eksperyment myślowy	157
Zagadnienie 2.2: Pytania kontrolne	157
Zagadnienie 2.3: Eksperyment myślowy	158
Zagadnienie 2.3: Pytania kontrolne	159

3	Implementacja ciągłości biznesowej i odzyskiwania awaryjnego	161
	Zagadnienie 3.1: Konfigurowanie i zarządzanie kopiami zapasowymi	162
	Korzystanie z funkcji Windows Server Backup	162
	Korzystanie z operatorów kopii zapasowych	172
	Korzystanie z funkcji Shadow Copies (Previous Versions)	173
	Konfigurowanie usługi Windows Azure Backup	174
	Podsumowanie zagadnienia	182
	Pytania kontrolne	183
	Zagadnienie 3.2: Odzyskiwanie serwerów	186
	Korzystanie z zaawansowanych opcji rozruchu	186
	Odzyskiwanie serwerów z poziomu nośnika instalacyjnego Windows	190
	Podsumowanie zagadnienia	196
	Pytania kontrolne	197
	Zagadnienie 3.3: Konfigurowanie odporności na uszkodzenia na poziomie lokacji	199
	Konfigurowanie serwerów fizycznego hosta Hyper-V	199
	Konfigurowanie maszyn wirtualnych	204
	Hyper-V Replica w pracy awaryjnej	212
	Funkcja Hyper-V Replica w klastrze pracy awaryjnej	216
	Konfigurowanie rozszerzonej replikacji Hyper-V Replica	220
	Korzystanie z menedżera Global Update Manager	220
	Odzyskiwanie wielolokacyjnych klastrów pracy awaryjnej	221
	Podsumowanie zagadnienia	222
	Pytania kontrolne	223
	Odpowiedzi	225
	Zagadnienie 3.1: Eksperyment myślowy	225
	Zagadnienie 3.1: Pytania kontrolne	225
	Zagadnienie 3.2: Eksperyment myślowy	227
	Zagadnienie 3.2: Pytania kontrolne	227
	Zagadnienie 3.3: Eksperyment myślowy	228
	Zagadnienie 3.3: Pytania kontrolne	229
4	Konfiguracja usług sieciowych	231
	Zagadnienie 4.1: Implementowanie zaawansowanego rozwiązania DHCP	232
	Tworzenie i konfigurowanie superzakresów oraz zakresów multitemisji	232
	Implementowanie DHCPv6	235
	Konfigurowanie wysokiej dostępności dla DHCP	239
	Konfigurowanie rejestracji DNS	240
	Konfigurowanie ochrony nazw DHCP	242
	Podsumowanie zagadnienia	245
	Pytania kontrolne	245

Zagadnienie 4.2: Implementowanie zaawansowanego rozwiązania DNS.	247
Implementowanie DNSSEC.	247
Konfigurowanie puli gniazd DNS	248
Konfigurowanie blokowania pamięci DNS.	249
Konfigurowanie rejestrowania DNS.	250
Konfigurowanie administracji delegowanej.	251
Konfigurowanie rekursji DNS	252
Konfigurowanie porządkowania maski sieci	253
Konfigurowanie strefy GlobalNames.	254
Analizowanie statystyk na poziomie strefy	254
Podsumowanie zagadnienia.	256
Pytania kontrolne.	257
Zagadnienie 4.3: Wdrażanie i zarządzanie funkcją IPAM.	258
Wprowadzenie do IPAM	258
Instalowanie i konfigurowanie IPAM.	259
Zarządzanie przestrzenią adresów	269
Konfigurowanie magazynu bazy danych IPAM.	278
Podsumowanie zagadnienia.	279
Pytania kontrolne.	280
Odpowiedzi	282
Zagadnienie 4.1: Eksperyment myślowy	282
Zagadnienie 4.1: Pytania kontrolne.	282
Zagadnienie 4.2: Eksperyment myślowy	283
Zagadnienie 4.2: Pytania kontrolne.	283
Zagadnienie 4.3: Eksperyment myślowy	285
Zagadnienie 4.3: Pytania kontrolne.	285
5 Konfiguracja infrastruktury Active Directory.	287
Zagadnienie 5.1: Konfigurowanie lasu lub domeny.	288
Implementowanie wielodomenowych środowisk Active Directory.	288
Implementowanie wielolasowych środowisk Active Directory.	290
Konfigurowanie współdziałania z wcześniejszymi wersjami Active Directory .	291
Uaktualnianie istniejących domen i lasów	292
Konfigurowanie sufiksów nazw UPN.	293
Podsumowanie zagadnienia.	295
Pytania kontrolne.	296
Zagadnienie 5.2: Konfigurowanie zaufania	297
Podstawowe pojęcia dotyczące zaufania.	297
Konfigurowanie zaufania zewnętrznego i zaufania obszaru.	298
Konfigurowanie zaufania lasu	299
Konfigurowanie zaufania skrótów	300
Konfigurowanie uwierzytelniania zaufania	301
Konfigurowanie filtrowania Security Identifier (SID).	301

Konfigurowanie trasowania sufiksów nazw	302
Podsumowanie zagadnienia.....	303
Pytania kontrolne.....	304
Zagadnienie 5.3: Konfigurowanie lokacji.....	306
Konfigurowanie lokacji i podsieci	306
Tworzenie i konfigurowanie łączy lokacji.....	309
Zarządzanie rejestracją rekordów SRV	311
Przenoszenie kontrolerów domeny pomiędzy lokacjami	313
Podsumowanie zagadnienia.....	314
Pytania kontrolne.....	314
Zagadnienie 5.4: Zarządzanie Active Directory i replikacją SYSVOL	316
Konfigurowanie replikacji do kontrolerów domeny tylko do odczytu (RODC)	316
Monitorowanie i zarządzanie replikacją	320
Uaktualnianie replikacji SYSVOL do rozproszonego systemu plików replikacji	322
Podsumowanie zagadnienia.....	323
Pytania kontrolne.....	324
Odpowiedzi.....	325
Zagadnienie 5.1: Eksperyment myślowy	325
Zagadnienie 5.1: Pytania kontrolne.....	325
Zagadnienie 5.2: Eksperyment myślowy	326
Zagadnienie 5.2: Pytania kontrolne.....	327
Zagadnienie 5.3: Eksperyment myślowy	328
Zagadnienie 5.3: Pytania kontrolne.....	328
Zagadnienie 5.4: Eksperyment myślowy	329
Zagadnienie 5.4: Pytania kontrolne.....	330
6 Konfiguracja rozwiązań dostępu i ochrony informacji	331
Zagadnienie 6.1: Wdrażanie usług Active Directory Federation Services (AD FS)	332
Instalowanie usług AD FS	332
Implementowanie uwierzytelniania opartego na oświadczeniach	333
Konfigurowanie zasad uwierzytelniania	335
Konfigurowanie funkcji Workplace Join	337
Konfigurowanie uwierzytelniania wieloczynnikowego.....	338
Podsumowanie zagadnienia.....	340
Pytania kontrolne.....	341
Zagadnienie 6.2: Instalowanie i konfigurowanie usług Active Directory Certificate Services (AD CS)	342
Instalowanie urzędów certyfikacji przedsiębiorstwa	343
Konfigurowanie punktów dystrybucji list CRL (CDP)	347
Instalowanie i konfigurowanie obiektów odpowiadających w trybie online	349
Implementowanie separacji roli administracyjnej.....	349
Konfigurowanie kopii zapasowej i odzyskiwania urzędu certyfikacji	351

Podsumowanie zagadnienia.....	353
Pytania kontrolne.....	354
Zagadnienie 6.3: Zarządzanie certyfikatami	355
Zarządzanie szablonami certyfikatów.....	355
Implementowanie i zarządzanie walidacją i odwoływaniem certyfikatów....	357
Zarządzanie rejestracją certyfikatów.....	358
Zarządzanie odnawianiem certyfikatów.....	359
Konfigurowanie i zarządzanie archiwizacją i odzyskiwaniem kluczy.....	360
Implementowanie i zarządzanie wdrożeniem certyfikatu.....	361
Podsumowanie zagadnienia.....	363
Pytania kontrolne.....	363
Zagadnienie 6.4: Instalowanie i konfigurowanie usług AD RMS	365
Instalowanie serwera licencji lub certyfikatów AD RMS	365
Zarządzanie punktem połączenia usługi AD RMS	366
Zarządzanie szablonami RMS.....	367
Konfigurowanie zasad wykluczania.....	369
Tworzenie kopii zapasowych i przywracanie AD RMS.....	370
Podsumowanie zagadnienia.....	371
Pytania kontrolne.....	372
Odpowiedzi.....	373
Zagadnienie 6.1: Eksperyment myślowy	373
Zagadnienie 6.1: Pytania kontrolne.....	373
Zagadnienie 6.2: Eksperyment myślowy	374
Zagadnienie 6.2: Pytania kontrolne.....	374
Zagadnienie 6.3: Eksperyment myślowy	375
Zagadnienie 6.3: Pytania kontrolne.....	376
Zagadnienie 6.4: Eksperyment myślowy	377
Zagadnienie 6.4: Pytania kontrolne.....	377
Indeks.....	379
O autorach.....	404

Wprowadzenie

W przeciwieństwie do innych egzaminów ze ścieżki MCSA, egzamin certyfikacyjny 70-412 obejmuje zaawansowane zagadnienia, takie jak usługi Active Directory Rights Management Services czy usługi Active Directory Federation Services. Na egzamin ten w większości składają się tematy, które nawet doświadczeni administratorzy systemów napotykać rzadziej niż podstawowe technologie infrastruktury, takie jak usługi Active Directory Domain Services czy usługi Windows Deployment Services.

Kandydatami do tego egzaminu są profesjonaliści branży IT, którzy chcą potwierdzić swoją wiedzę i umiejętności w zakresie zaawansowanej konfiguracji systemu operacyjnego Windows Server 2012 R2. Aby zdać ten egzamin, kandydaci muszą być w stanie skonfigurować i zarządzać w systemie Windows Server 2012 R2 wysoką dostępnością, rozwiązaniami zarządzania plikami i magazynowania danych, a także rozwiązaniami w zakresie odzyskiwania po awarii, usług sieciowych, infrastruktury Active Directory oraz dostępu i ochrony informacji. Od kandydatów wymagane jest również posiadanie ugruntowanej wiedzy teoretycznej oraz dużego doświadczenia praktycznego w zakresie implementacji wykorzystywanych technologii. W przypadku braku takiego doświadczenia, warto rozważyć pozycję uzupełniającą „*Training Guide: Configuring Advanced Windows Server 2012 R2 Services*”, która zawiera obszerną liczbę praktycznych ćwiczeń laboratoryjnych.

Niniejszy podręcznik porusza wszystkie zagadnienia egzaminacyjne, jednak nie pokrywa wszystkich pytań egzaminu 70-412. Tylko zespół egzaminacyjny Microsoft ma dostęp do pytań tego egzaminu, a że jest on regularnie wzbogacany o nowe pytania, odniesienie się do konkretnych pytań egzaminacyjnych nie jest możliwe. Książkę tę należy więc traktować jako uzupełnienie praktycznego doświadczenia, bądź też jako dodatek do innych materiałów szkoleniowych. W przypadku napotkania w tej książce na temat, w którym nie czujemy się zbyt pewnie, warto skorzystać z podanych w tekście odnośników odsyłających do materiałów dodatkowych i poświęcić odpowiednią ilość czasu na jego opanowanie. Wartościowe informacje możemy znaleźć również w witrynie TechNet, a także na blogach zespołów produktów oraz forach internetowych.

Certyfikaty Microsoft

Certyfikaty firmy Microsoft wyróżniają nas, udowadniając posiadanie przez nas szerokiego zestawu umiejętności i doświadczenia związanych z aktualnymi produktami i technologiami firmy. Egzaminy i odpowiadające im certyfikaty są opracowane tak, aby sprawdzić naszą biegłość w zakresie kompetencji decydujących przy projektowaniu i tworzeniu lub implementacji i obsłudze rozwiązań związanych z produktami i technologiami firmy Microsoft na miejscu w firmie i w chmurze. Certyfikaty dają wiele korzyści zarówno poszczególnym osobom, jak i pracodawcom i organizacjom.

DODATKOWE INFORMACJE Wszystkie certyfikaty Microsoft

Więcej informacji odnośnie certyfikatów Microsoft, w tym ich pełny wykaz, można znaleźć pod adresem <http://www.microsoft.com/learning/en/us/certification/cert-default.aspx>.

Errata i wsparcie dla książki

Zrobiliśmy wszystko, co w naszej mocy, aby książce tej, jak również wspomagającym ją materiałom, zapewnić jak najlepszą dokładność. Lista wszystkich błędów zgłoszonych od czasu wydania tej książki dostępna jest pod adresem:

<https://www.microsoftpressstore.com/store/exam-ref-70-412-configuring-advanced-windows-server-9780735673618>

W przypadku odkrycia błędu, który nie został uwzględniony na tej liście, prosimy o jego zgłoszenie przy użyciu powyższej witryny*.

Jeśli potrzebna będzie dodatkowa pomoc, prosimy o email do Microsoft Press Book Support, na adres mspinput@microsoft.com.

Zwracamy uwagę, że pod tym adresem nie jest oferowana pomoc związana z działaniem oprogramowania firmy Microsoft.

Czekamy na uwagi

Najwyższym priorytetem wydawnictwa Microsoft Press jest zadowolenie Czytelników, a ich opinie są dla nas niezwykle cenne. Prosimy o przekazywanie uwag na witrynie:

<http://aka.ms/tellpress>

Ankieta jest krótka, a my czytamy wszystkie przysłane do nas spostrzeżenia i pomysły. Z góry dziękujemy za wszystkie wpisy!

* Strona erraty dotyczy angielskiego wydania książki. Błędy zgłoszone tam w czasie przygotowywania polskiego wydania zostały już uwzględnione. Ewentualne nowe błędy odkryte w polskim wydaniu prosimy zgłaszać na adres mspress@promise.pl (przyp. red.).

Pozostańmy w kontakcie

Niech dyskusja trwa! Jesteśmy na Twitterze: <http://twitter.com/MicrosoftPress>.

Przygotowanie do egzaminu

Egzaminy certyfikacyjne Microsoft są wspaniałym sposobem na rozbudowanie Twojego CV i pokazanie światu poziomu Twoich umiejętności. Egzaminy te potwierdzają Twoje doświadczenie i wiedzę na temat danego produktu. Choć nic nie jest w stanie zastąpić doświadczenia zdobytego w codziennej pracy, przygotowywanie się w oparciu o samodzielną naukę i wykonywanie ćwiczeń praktycznych pomoże Ci przygotować się do egzaminu. Zalecamy Ci, byś uzupełnił swój plan nauki o kombinację dostępnych materiałów szkoleniowych i kursów. Możesz przykładowo przygotowywać się z pomocą podręcznika Training Guide i innego podręcznika do samodzielnej nauki „w domu”, jak również odbyć kurs Microsoft Official Curriculum w sali szkoleniowej. Wybierz kombinację, która Twoim zdaniem będzie dla Ciebie najlepsza.

ROZDZIAŁ 1

Konfiguracja i zarządzanie wysoką dostępnością

Obszar zagadnień omawiany w tym rozdziale odnosi się do wieloserwerowych funkcji, których zadaniem jest zapewnienie klientom stałej dostępności wybranych usług i aplikacji. Do funkcji tych należą równoważenie obciążenia sieciowego, tworzenie klastrów pracy awaryjnej oraz migracja na żywo maszyn wirtualnych. Zrozumienie powyższych zagadnień wymaga solidnej znajomości nowych technologii, z których z pewnością nie wszystkie mieliśmy okazję zaimplementować w naszym własnym środowisku. Dlatego informacje zamieszczone w tym rozdziale warto uzupełnić ćwiczeniami praktycznymi, co pomoże nam rozwinąć umiejętność zarówno wykorzystywania tych technologii w rzeczywistych scenariuszach, jak i rozwiązywania problemów w zaawansowanych środowiskach serwerowych.

Zagadnienia egzaminacyjne omawiane w tym rozdziale:

- **Zagadnienie 1.1: Konfigurowanie równoważenia obciążenia sieciowego** 2
- **Zagadnienie 1.2: Konfigurowanie klastra pracy awaryjnej** 19
- **Zagadnienie 1.3: Zarządzanie rolami klastra pracy awaryjnej** 45
- **Zagadnienie 1.4: Zarządzanie ruchem maszyny wirtualnej** 60
- **Odpowiedzi** 81

Zagadnienie 1.1: Konfigurowanie równoważenia obciążenia sieciowego

Równoważenie obciążenia sieciowego (Network Load Balancing, NLB) jest funkcją systemu Windows Server, która sprawia, że dla klientów zewnętrznych określona grupa serwerów widoczna jest jako pojedynczy serwer. Taka grupa serwerów połączonych poprzez NLB nosi nazwę *klastra NLB* lub *farmy serwerów*, zaś każdy serwer będący jej członkiem jest zazwyczaj nazywany *hostem* lub *węzłem*. Celem równoważenia obciążenia sieciowego jest zwiększenie zarówno dostępności, jak i skalowalności usługi hostowanej na wszystkich indywidualnych węzłach.

W przypadku korzystania z ustawień domyślnych, funkcja równoważenia obciążenia sieciowego jest zaskakująco łatwa w konfiguracji. Na potrzeby egzaminu 70-412 musimy jednak znać nieco więcej niż tylko podstawy funkcji NLB. Upewnijmy się, że dobrze znamy również dostępne dla niej opcje konfiguracji, takie jak ustawienia priorytetów oraz wszystkie ustawienia reguł portów.

Niniejsze zagadnienie obejmuje następującą tematykę:

- Instalowanie węzłów równoważenia obciążenia sieciowego
- Konfigurowanie wymagań wstępnych równoważenia obciążenia sieciowego
- Konfigurowanie koligacji
- Konfigurowanie reguł portów
- Konfigurowanie trybu działania klastra
- Uaktualnianie klastra równoważenia obciążenia sieciowego

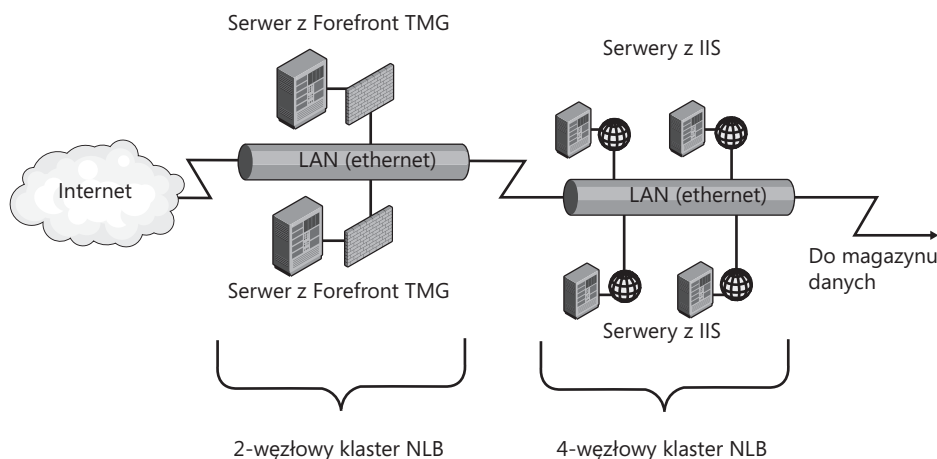
Podstawy równoważenia obciążenia sieciowego

Funkcja równoważenia obciążenia sieciowego zwiększa zarówno dostępność, jak i skalowalność usługi poprzez dystrybucję wszystkich otrzymanych od klientów żądań do dwóch lub więcej serwerów. Dla każdego z klientów NLB wygląda jak pojedynczy serwer, do którego przypisano jedną nazwę i jeden adres.

W najbardziej typowym scenariuszu równoważenie obciążenia sieciowego służy do tworzenia *farmy sieci Web*, czyli grupy komputerów działających pod kontrolą systemu Windows Server, wspierających witrynę lub aplikację sieci Web. NLB możemy również wykorzystać do tworzenia farm serwerów innego typu, np. farm serwerów Remote Desktop Server, farm serwerów VPN czy farm serwerów proxy/zapory sieciowej. Rysunek 1-1 pokazuje wdrożenie klastra NLB składającego się z serwerów z uruchomionymi usługami Internet Information Services (IIS). Klaster ten umiejscowiony jest za innym klastrem NLB, na którego serwerach uruchomiono produkt Forefront Threat Management Gateway (TMG).

Po pierwsze, NLB zwiększa dostępność usługi przechwytyjąc awarie indywidualnych serwerów i ukrywając te awarie przed klientami. NLB automatycznie wykrywa serwery, które nie odpowiadają lub zostały od farmy odłączone, a następnie redystrybuuje nowe żądania klientów pomiędzy pozostałe aktywne hosty. Po drugie, NLB wspiera skalowalność, jako że grupa serwerów może obsłużyć więcej żądań klientów niż pojedynczy serwer. Gdy tylko zapotrzebowanie na usługę (np. w postaci witryny) wzrasta, możemy dodać do farmy dodatkowe serwery, przez co będzie ona w stanie obsłużyć jeszcze większe obciążenia robocze.

Musimy pamiętać, że każdy indywidualny klient kierowany jest do dokładnie jednego serwera w klastrze NLB. Oznacza to, że klient otrzymuje zasoby pamięci, magazynu i procesora należące tylko i wyłącznie do tego jednego hosta. Każdy węzeł w klastrze NLB pracuje niezależnie i bez żadnego dostępu do zasobów innych serwerów, zaś zmiany wprowadzane na jednym serwerze nie są kopiowane do pozostałych węzłów w farmie. NLB wykorzystujemy do wsparcia *aplikacji bezstanowych* (stateless applications). NLB nie powinniśmy stosować w przypadku korzystania z *aplikacji stanowych* (stateful applications), takich jak serwery baz danych, zezwalające indywidualnym klientom na aktualizowanie danych, ponieważ może to skutkować niespójnością doświadczeń poszczególnych klientów.



RYSUNEK 1-1 Prosty schemat dla dwóch połączonych klastrów NLB

Tworzenie i konfigurowanie klastra NLB

Rozpoczynamy od zainstalowania na serwerach funkcji Network Load Balancing. Instalacji tej możemy dokonać korzystając z kreatora Add Roles and Features Wizard (Kreator dodawania ról i funkcji), dostępnego z poziomu konsoli Server Manager. Egzamin 70-412 prawdopodobnie będzie wymagał od nas umiejętności przeprowadzenia instalacji tej funkcji również z poziomu powłoki Windows PowerShell. Aby

tego dokonać, w oknie powłoki Windows PowerShell z podniesionymi uprawnieniami należy wpisać:

```
Install-WindowsFeature NLB -IncludeManagementTools
```

UWAGA Aliasy

Add-WindowsFeature jest aliasem dla Install-WindowsFeature, natomiast Remove-WindowsFeature to alias dla Uninstall-WindowsFeature.

Po zainstalowaniu funkcji NLB wraz z dedykowanymi jej narzędziami zarządzania, możemy przystąpić do konfiguracji klastra NLB, wykorzystując do tego powłokę Windows PowerShell lub graficzną konsolę Network Load Balancing Manager. Dostęp do niej uzyskamy z poziomu menu Tools (Narzędzia) konsoli Server Manager. Konsolę Network Load Balancing Manager możemy również otworzyć wpisując w oknie wiersza poleceń Nlbmgr.



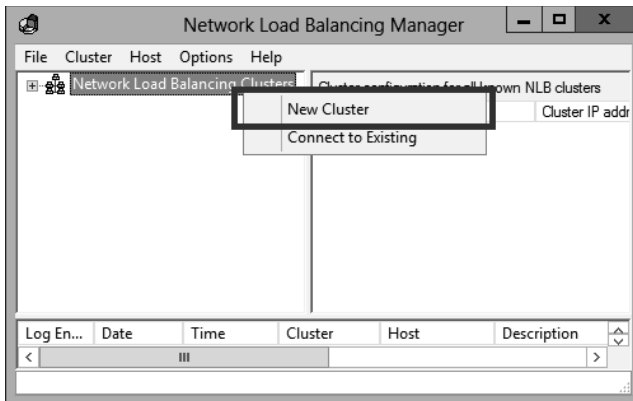
WSKAZÓWKĄ EGZAMINACYJNA

W Windows Server 2012 R2 narzędzia zarządzania *nie* zawsze instalowane są wraz z powiązanymi rolami i funkcjami, jak to miało miejsce w poprzednich wersjach systemu Windows Server. Narzędzia zarządzania domyślnie instalowane są tylko wtedy, gdy powiązane role i funkcje instalujemy z poziomu kreatora Add Roles and Features Wizard. Jeśli do instalacji roli lub funkcji wykorzystamy polecenie Install-WindowsFeature, wówczas narzędzia zarządzania nie zostaną automatycznie zainstalowane. Aby zainstalować narzędzia zarządzania wraz z konkretną rolą lub funkcją, należy skorzystać z opcji -IncludeManagementTools. Przy zarządzaniu wieloma serwerami z poziomu jednego, pojedynczego serwera (co nazywane jest również administracją rozdysponowaną), na serwerze lokalnym, czy też na wykorzystywanym do codziennej administracji stacjonarnym kliencie Windows 8.1, zechcemy prawdopodobnie zainstalować narzędzia zarządzania dla zdalnych ról i funkcji.

Aby uruchomić kreator New Cluster Wizard (Kreator nowego klastra), w drzewie konsoli Network Load Balancing Manager klikamy prawym przyciskiem Network Load Balancing Clusters (Klasytry równoważenia obciążenia sieciowego), a następnie New Cluster (Nowy klaster), jak pokazano na rysunku 1-2. Zauważmy, że choć interfejs użytkownika odnosi się do klastra NLB prostym terminem „cluster” (klaster), to egzamin 70-412 będzie często określał taki klaster terminami „NLB cluster” (klaster NLB) lub „farm” (farma).

Pierwszą stroną kreatora New Cluster Wizard jest strona New Cluster: Connect, widoczna na rysunku 1-3. Wymaga ona od nas połączenia się z serwerem, na którym zainstalowano funkcję Network Load Balancing. Po pomyślnym połączeniu wybieramy interfejs tego serwera dla ruchu NLB. W środowisku testowym fakt, że serwer, który

chcemy dodać do klastra NLB, ma tylko jeden interfejs sieciowy nie ma znaczenia, gdyż interfejs ten będzie wówczas współdzielony pomiędzy NLB i zwykłą komunikacją sieciową. Jednak w środowisku produkcyjnym na każdym z hostów będziemy chcieli zarezerwować dla NLB osobną kartę sieciową, a następnie przypisać te interfejsy do jednego wydzielonego segmentu sieci z własnym połączeniem do lokalnego routera. Bez względu na to, czy rezerwujemy dedykowany interfejs dla NLB, czy też nie, przypisywanemu interfejsowi musimy nadać statyczny adres IP. W późniejszym czasie nadamy mu drugi adres IP, który będzie współdzielony pomiędzy wszystkimi węzłami w klastrze NLB.

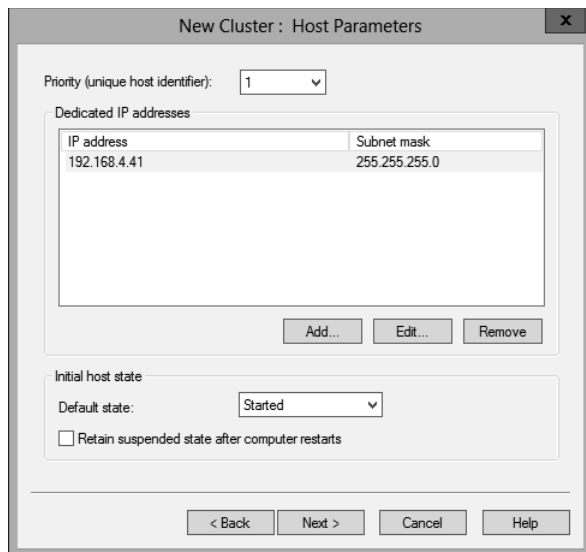


RYSUNEK 1-2 Tworzenie nowego klastra NLB



RYSUNEK 1-3 Określanie interfejsu zarezerwowanego dla ruchu klastra NLB

Drugą stroną kreatora jest strona New Cluster: Host Parameters, pokazana na rysunku 1-4. Dostępne na niej ustawienia mają zastosowanie tylko i wyłącznie do lokalnego hosta (węzła), nie zaś do całego klastra NLB.



IP address	Subnet mask
192.168.4.41	255.255.255.0

RYСУNEK 1-4 Druga strona kreatora New Cluster Wizard

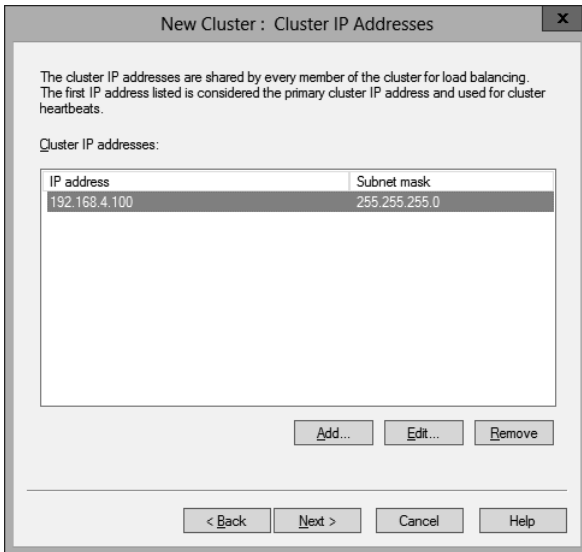
Na stronie tej widnieją trzy obszary konfiguracji: Priority (Unique Host Identifier), Dedicated IP Addresses oraz Initial Host State.

- **Priority (Unique Host Identifier)** Ustawienie Priority jest wartością z przedziału od 1 do 21, unikalną dla każdego hosta w klastrze NLB. Wartość 1 nadawana jest hostowi o najwyższym priorytecie. Wartość tego priorytetu określa, który z węzłów klastra NLB będzie obsługiwał ruch sieciowy, który *nie jest* równoważony (innymi słowy, *nie jest* objęty regułami portów, tworzonymi w dalszej części kreatora). Jeśli host o najwyższym priorytecie nie jest dostępny, wówczas kolejny host o najwyższym priorytecie będzie obsługiwał ten nierównoważony ruch. Ustawienie to znane jest również jako ustawienie **Host Priority** (Priorytet hosta).
- **Dedicated IP Addresses** W tym miejscu możemy zmodyfikować lokalny adres IP lub też zbiór adresów IP, które host łączy z klastrem NLB. Zazwyczaj domyślny adres IP dostosowujemy tu tylko wtedy, gdy do dedykowanego dla NLB interfejsu przypisaliśmy więcej niż jeden adres IP. Pamiętajmy, że omawiane na tej stronie adresy nie są przypisywane do klastra jako całości, lecz odnoszą się one tylko i wyłącznie do lokalnego hosta. Te dedykowane, przypisywane do indywidualnych hostów w klastrze NLB adresy IP muszą znajdować się w tej samej logicznej podsieci i zależnie od potrzeb muszą być osiągalne z zewnątrz poprzez działającą ścieżkę trasowania lub z poziomu lokalnego segmentu sieciowego.

- **Initial Host State** W tym miejscu możemy ustawić domyślny stan lokalnego węzła w obrębie klastra NLB. Dostępne opcje to Started (Uruchomiony, opcja domyślna), Suspended (Wstrzymany) lub Stopped (Zatrzymany). Jak widać na rysunku 1-4, możemy również włączyć opcję zachowania stanu wstrzymania po ponownym uruchomieniu komputera.

Teraz wybieramy wirtualny adres (lub adresy) IP, który zostanie przypisany do farmy serwerów jako całości. Wirtualny adres klastra lub wybrane przez nas adresy muszą znajdować się w tej samej podsieci logicznej co dedykowany adres (lub adresy) IP hosta, który wybraliśmy na poprzedniej stronie.

Strona New Cluster: Cluster IP Addresses widoczna jest na rysunku 1-5.



New Cluster : Cluster IP Addresses

The cluster IP addresses are shared by every member of the cluster for load balancing. The first IP address listed is considered the primary cluster IP address and used for cluster heartbeats.

Cluster IP addresses:

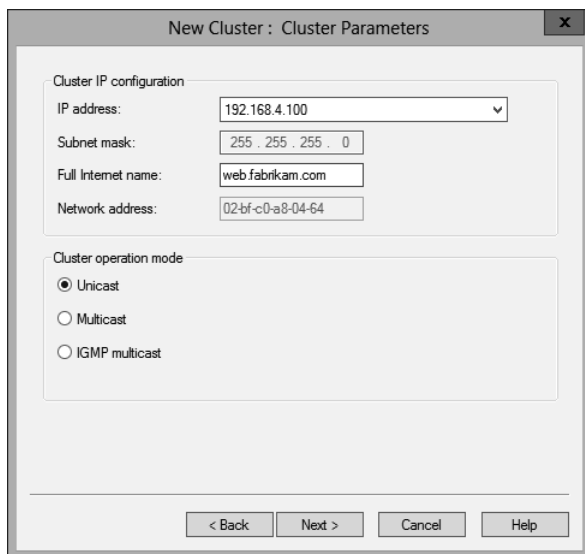
IP address	Subnet mask
192.168.4.100	255.255.255.0

Add... Edit... Remove

< Back Next > Cancel Help

RYSUNEK 1-5 Przypisywanie do klastra NLB wirtualnego adresu IP

W czasie instalacji, na stronie New Cluster: Cluster Parameters, widocznej na rysunku 1-6, konfigurujemy adres IP klastra, maskę podsieci, pełną nazwę w Internecie, adres sieciowy oraz tryb działania klastra. Ustawienia te możemy również zmodyfikować już po utworzeniu klastra.



The screenshot shows a window titled "New Cluster : Cluster Parameters". It contains two main sections: "Cluster IP configuration" and "Cluster operation mode".

Cluster IP configuration:

- IP address: 192.168.4.100
- Subnet mask: 255 . 255 . 255 . 0
- Full Internet name: web.fabrikam.com
- Network address: 02-bf-c0-a8-04-64

Cluster operation mode:

- ☒ Unicast
- ☐ Multicast
- ☐ IGMP multicast

At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

RYSUNEK 1-6 Czwarta strona kreatora New Cluster Wizard

Strona ta zawiera obszary Cluster IP Configuration (Konfiguracja IP klastra) oraz Cluster Operation Mode (Tryb działania klastra).

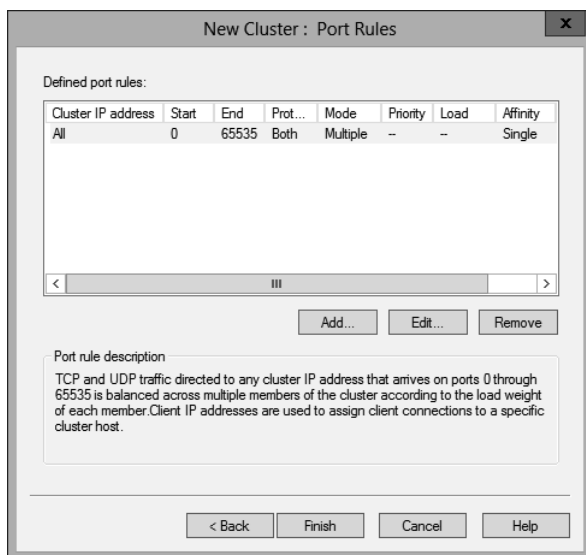
- **Cluster IP Configuration** Te ustawienia są dość intuicyjne. Weryfikujemy tu po prostu wirtualny adres IP i w polu tekstowym Internet Name wpisujemy w pełni kwalifikowaną nazwę domeny (Fully Qualified Domain Name, FQDN) dla całego klastra NLB. Należy jeszcze zwrócić uwagę na wartość Network Address (Adres sieciowy). Jest to wirtualny adres MAC przypisany do wszystkich kart sieciowych, które dedykowaliśmy klastrowi NLB.
- **Cluster Operation Mode** Znaczenie tego ustawienia może nie być dla wszystkich oczywiste. Z jego pomocą ustawiamy jeden z trzech dostępnych trybów operacji klastra NLB: Unicast (Emisja pojedyncza), Multicast (Multiemisja) lub IGMP Multicast (Multiemisja IGMP). Przyjrzyjmy się znaczeniu tych opcji:
 - **Unicast** (opcja domyślna) Tryb ten pozwala zastąpić adres MAC karty sieciowej na każdym z hostów adresem MAC karty sieciowej klastra NLB. Z technicznego punktu widzenia jest to wydajne rozwiązanie, jednak w wybranych środowiskach wirtualnych może być ono niezgodne z niektórymi kartami sieciowymi.
 - **Multicast** W tym trybie każdy host zatrzymuje swój oryginalny adres MAC. Dokładniej mówiąc, adres MAC klastra NLB wykorzystywany jest jako adres multiemisji, który następnie każdy host tłumaczy na właściwy mu, oryginalny adres MAC.
 - **IGMP Multicast** Ta opcja konfiguruje multiemisję na poziomie adresu IP. Zaletą takiego rozwiązania jest zapobieganie zalewania przełączników,

wykorzystując w tym celu ograniczanie ruchu równoważenia obciążenia sieciowego tylko i wyłącznie do portów NLB. Z kolei wadą tej opcji jest to, że nie wszystkie przełączniki obsługują IGMP Multicast.

Konfigurowanie reguł portów

Reguły portów są najważniejszą częścią konfiguracji klastra NLB. Reguły te definiują, który ruch będzie równoważony w klastrze oraz w jaki sposób. Każda reguła portów dopasowuje ruch przychodzący na podstawie zakresu zdefiniowanych portów TCP lub UDP oraz (opcjonalnie) docelowego adresu IP. Nie jest możliwe utworzenie dwóch reguł pasujących do tego samego ruchu przychodzącego, zatem nigdy nie będziemy mieć problemów z konfliktami pomiędzy regułami, jak również ich priorytetem oraz kolejnością. Do przychodzącego pakietu ma zatem zastosowanie tylko jedna reguła portów.

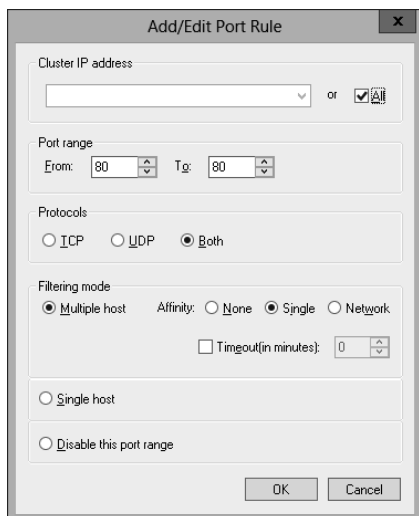
Jedna reguła portów jest predefiniowana. Jest ona widoczna na rysunku 1-7. Reguła ta dopasowuje cały ruch TCP/IP (mówiąc dokładniej, cały ruch TCP i UDP wysłany na portach od 0 do 65535). O ile z reguły tej możemy chcieć korzystać w praktyce, o tyle w ramach naszego przygotowywania się do egzaminu 70-412 nie będzie ona zbyt użyteczna.



RYСУNEK 1-7 Piąta strona kreatora New Cluster Wizard

W czasie egzaminu 70-412 należy przyjąć, że w każdym zaprezentowanym nam scenariuszu równoważenia obciążenia sieciowego predefiniowana reguła portów została usunięta, zaś wszystkie obecne reguły portów są skonfigurowane niestandardowo. Aby więc dobrze przygotować się do egzaminu, musimy znać wszystkie opcje konfiguracji

dostępne w oknie dialogowym Add/Edit Port Rule (Dodawanie/edytowanie reguły portów), widocznym na rysunku 1-8. Musimy również znać dwie dodatkowe opcje, które będą dostępne w tym oknie, gdy będziemy później edytować istniejącą regułę portów. Będziemy tego dokonywać z poziomu właściwości konkretnego *hosta* (a nie klastra) w konsoli Network Load Balancing Manager.



RYСУNEK 1-8 Dodawanie lub edytowanie reguły portów równoważenia obciążenia sieciowego

W oknie Add/Edit Port Rule możemy edytować następujące opcje:

- **Cluster IP Address** Obszar ten pozwala nam zdefiniować kryteria dopasowania dla nowej reguły portów, tak by dopasowywała ona ruch przychodzący kierowany tylko do jednego z adresów klastra. Domyślnie nowa reguła portów dopasowuje wszystkie adresy klastra NLB.
- **Port Range and Protocols** Sekcje te pozwalają nam zdefiniować kryteria dopasowania dla nowej reguły portów, tak by dopasowywała ona ruch przychodzący kierowany do ciągłego zakresu jednego lub więcej portów TCP, portów UDP lub też obu tych rodzajów portów na raz. Zdefiniowany przez nas zakres nie może pokrywać się z zakresem zdefiniowanym w innej regule portów.
- **Filtering Mode** Ta sekcja pozwala nam określić, w jaki sposób żądania są dystrybuowane. Dostępne ustawienia to Multiple Host, Single Host oraz Disable This Port Range.

Tryb filtrowania Multiple Host (Wiele hostów) jest ustawieniem domyślnym. Dla wszystkich przychodzących i dopasowanych do reguły portów żądań tryb *Multiple Host* dostarcza zarówno funkcji równoważenia obciążenia, jak i odporności na uszkodzenia.

Dopasowane do reguły portów żądania klientów dystrybuowane są pomiędzy aktywne węzły farmy. Korzystając z trybu filtrowania Multiple Host musimy wybrać jedną z opcji koligacji, określając tym samym sposób, w jaki oddziaływujący z klastrem w czasie trwania sesji klient będzie odpowiadać. Dostępne opcje to None (Brak), Single (Pojedyncza) oraz Network (Sieć). Ich działanie przedstawia się następująco:

- **None** Z tym ustawieniem ruch każdego klienta kierowany jest do dowolnego węzła w klastrze, w zależności od aktualnego obciążenia. Również każdy kolejny ruch pochodzący od danego klienta będzie kierowany do dowolnego węzła w klastrze, w zależności od aktualnego obciążenia.
- **Single** W przypadku tego ustawienia, jeśli klient o nazwie Client1 przy pierwszym połączeniu do klastra NLB połączy się z węzłem o nazwie Host1, wówczas klient Client1 będzie nadal łączył się z hostem Host1 w przyszłości. Jeśli klient o nazwie Client2 połączy się do węzła NLB o nazwie Host2, wówczas klient ten będzie łączył się z hostem Host2 także w przyszłości, itd. Zaletą tego ustawienia jest możliwość zachowania danych stanu użytkownika pomiędzy jedną a drugą sesją, jeśli tylko dane te zapisywane są na lokalnym węźle. Jest to domyślne ustawienie koligacji.
- **Network** Ta opcja powoduje, że każdy węzeł w klastrze NLB jest odpowiedzialny za wszystkie połączenia pasujące do podanego adresu sieciowego /24 IPv4. Na przykład, jeśli klient o nazwie Client1 połączy się najpierw z klastrem NLB przez serwer proxy o nazwie Proxy1 i adresie 207.46.130.101, a następnie połączy się z klastrem NLB poprzez inny serwer proxy o nazwie Proxy 2 i adresie 207.46.130.102, wówczas połączenie zostanie skierowane do tego samego węzła, ponieważ oba serwery proxy mają przypisany ten sam adres sieciowy (207.46.130.z).

Musimy być jednak świadomi tego, że nasz wybór pomiędzy trzema powyższymi ustawieniami koligacji może zostać ograniczony przez hostowaną w klastrze NLB aplikację, bowiem nie wszystkie aplikacje wspierają przykładowo ustawienie Affinity-None (Koligacja – Brak).

Tryb filtrowania *Single Host* (Pojedynczy host) cały dopasowany ruch kieruje do hosta o najwyższej wartości priorytetu. Jeśli host ulegnie awarii, wówczas ruch kierowany jest do hosta z najwyższą wartością priorytetu w obrębie pozostałych hostów. Jak pamiętamy, taka sama usługa dostępna jest dla ruchu, który nie został dopasowany do żadnej z reguł portów. Po co więc zawracać sobie głowę tworzeniem reguły portów w trybie Single Host? Otóż zaletą konfiguracji reguły portów w trybie Single Host jest to, że korzystając z ustawienia *Handling Priority*, dostępnego w konsoli Network Load Balancing Manager, możemy później zdefiniować dla dopasowywanego ruchu niestandardowy priorytet serwera.



WSKAZÓWKA EGZAMINACYJNA

Egzamin 70-412 wymaga znajomości ustawień koligacji Affinity-None, Affinity-Single oraz Affinity-Network.

Ustawienie Timeout (Limit czasu), poprzez odpowiednie zmiany w konfiguracji klastra NLB, rozszerza koligację do określonej liczby minut. Jeśli przykładowo klastr NLB jest wykorzystywany w celu wsparcia witryny sklepu internetowego, klient może doświadczyć korzyści ze stosowania ustawienia Timeout w formie możliwości zachowania produktów w koszyku przez podaną liczbę minut. Bez rozszerzania koligacji przy użyciu ustawienia Timeout, produkty w koszyku mogłyby teoretycznie zniknąć, jeśli po zmianie konfiguracji farmy serwerów połączenie klienta zostałoby przekierowane do innego hosta. Ustawienie Disable This Port Range (Wyłącz ten zakres portu) pozwala nam na to, by klastr NLB porzucił cały ruch na podanym porcie.

Ustawienia Load Weight (Obciążenie) oraz Handling Priority (Priorytet obsługi) są dostępne tylko w przypadku edytowania istniejącej reguły portów z poziomu właściwości hosta w konsoli Network Load Balancing Manager. Podczas edytowania istniejącej reguły portów otworzy się specjalna wersja okna dialogowego Add/Edit Port Rule, widoczna na rysunku 1-9.

RYСУNEK 1-9 Okno dialogowe Add/Edit Port Rule dla określonego hosta

W czasie edytowania istniejącej reguły portów możemy skonfigurować następujące opcje:

- **Load Weight** Edytując właściwości danego hosta, ustawienie to pozwala nam na przypisanie do niego dysproporcjonalnej wartości obciążenia. Domyślnie wybraną wartością jest Equal (Równomierne), co przypisuje hostowi średnioważoną lub proporcjonalną dystrybucję obciążenia sieciowego. Jeśli odznaczmy ustawienie Equal (jak na rysunku 1-9), będziemy mogli przypisać do hosta większy lub mniejszy udział kierowanego do farmy ruchu sieciowego. W takim wypadku otrzymana proporcja ustalana jest jako wartość lokalnego obciążenia, podzielona przez całkowite obciążenie w obrębie klastra NLB. Domyślną wartością jest 50.
- **Handling Priority** Ustawienie to dostępne jest tylko wtedy, gdy dla reguły włączyliśmy tryb filtrowania Single Host. W trybie filtrowania Single Host ruch określony w regule portów zawsze otrzymuje serwer z najwyższym priorytetem. Zaletą tworzenia dla konkretnego ruchu reguły portów z włączonym trybem filtrowania Single Mode (w przeciwieństwie do braku takiej reguły), jest to, że w zdefiniowanej regule portów możemy ustawić niestandardowy priorytet serwera dla tego ruchu. Priorytet ten ustawiany jest przy użyciu opcji Handling Priority. Jeśli opcja ta nie jest ustawiona, wówczas wartością priorytetu przypisaną do lokalnego hosta jest wartość ustawiona dla całego klastra, dostępna w oknie dialogowym Host Parameters.

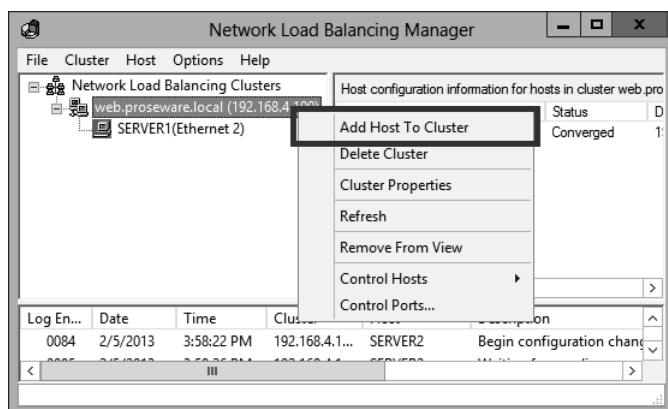
WSKAZÓWKA EGZAMINACYJNA

Należy pamiętać o różnicy pomiędzy priorytetami Host Priority i Handling Priority. *Host Priority* określa, który serwer w klastrze otrzymuje ruch nie objęty regułą portów. *Handling Priority* jest natomiast niestandardową wartością priorytetu serwera, wykorzystywaną dla ruchu objętego regułą portów, ale z przypisanym trybem filtrowania Single Host.



Dodawanie hostów do klastra NLB

Aby dodać hosty do istniejącego już klastra NLB, w drzewie konsoli Network Load Balancing Manager klikamy klawiszem prawym przyciskiem, po czym wybieramy opcję Add Host To Cluster (Dodaj hosta do klastra), jak rysunku 1-10. Spowoduje to uruchomienie kreatora Add Host To Cluster Wizard. Do klastra NLB możemy dodać maksymalnie 16 hostów.



RYSUNEK 1-10 Instalowanie hostów w klastrze NLB po jego utworzeniu

Wykaz poleceń cmdlet dla równoważenia obciążenia sieciowego

Aby zobaczyć wszystkie dostępne polecenia cmdlet dedykowane równoważeniu obciążenia sieciowego, w oknie powłoki Windows PowerShell wpisujemy `Get-Command *nlb*` lub `Get-Command -Module NetworkLoadBalancingClusters`.

TABELA 1-1 Polecenia cmdlet dla równoważenia obciążenia sieciowego w Windows Server 2012 i Windows Server 2012 R2

Polecenie cmdlet	Opis
<code>Add-NlbClusterNode</code>	Dodaje do klastra NLB nowy węzeł
<code>Add-NlbClusterNodeDip</code>	Dodaje do klastra NLB dedykowany adres IP
<code>Add-NlbClusterPortRule</code>	Dodaje do klastra NLB nową regułę portów
<code>Add-NlbClusterVip</code>	Dodaje do klastra NLB wirtualny (wspólny dla klastra) adres IP
<code>Disable-NlbClusterPortRule</code>	Wyłącza regułę portów w klastrze NLB lub należącym do niego hoście
<code>Enable-NlbClusterPortRule</code>	Włącza regułę portów w klastrze NLB lub należącym do niego hoście
<code>Get-NlbCluster</code>	Pozyskuje informacje o klastrze NLB
<code>Get-NlbClusterNode</code>	Pozyskuje informacje o węźle klastra NLB
<code>Get-NlbClusterNodeDip</code>	Pozyskuje dedykowany adres IP
<code>Get-NlbClusterNodeNetworkInterface</code>	Pozyskuje informacje o interfejsach na hoście klastra NLB
<code>Get-NlbClusterPortRule</code>	Pozyskuje obiekty reguły portów
<code>Get-NlbClusterVip</code>	Pozyskuje wirtualne adresy IP

TABELA 1-1 Polecenia cmdlet dla równoważenia obciążenia sieciowego w Windows Server 2012 i Windows Server 2012 R2

Polecenie cmdlet	Opis
New-NlbCluster	Tworzy klaster NLB na konkretnym interfejsie, zdefiniowany przez nazwę węzła i karty sieciowej
Remove-NlbCluster	Usuwa klaster NLB
Remove-NlbClusterNode	Usuwa węzeł z klastra NLB
Remove-NlbClusterNodeDip	Usuwa z klastra NLB dedykowany adres IP
Remove-NlbClusterPortRule	Usuwa z klastra NLB regułę portów
Remove-NlbClusterVip	Usuwa wirtualny adres IP klastra NLB
Resume-NlbCluster	Wznawia wszystkie węzły klastra NLB
Resume-NlbClusterNode	Wznawia wstrzymany węzeł klastra NLB
Set-NlbCluster	Edytuje konfigurację klastra NLB
Set-NlbClusterNode	Edytuje ustawienia węzła klastra NLB
Set-NlbClusterNodeDip	Edytuje dedykowany adres IP klastra NLB
Set-NlbClusterPortRule	Edytuje reguły portów klastra NLB
Set-NlbClusterPortRuleNodeHandlingPriority	Ustawia priorytet hosta reguły portów dla konkretnego węzła NLB
Set-NlbClusterPortRuleNodeWeight	Ustawia wartość obciążenia reguły portów dla konkretnego węzła NLB
Set-NlbClusterVip	Edytuje wirtualny adres IP klastra NLB
Start-NlbCluster	Uruchamia wszystkie węzły w klastrze NLB
Start-NlbClusterNode	Uruchamia klaster NLB
Stop-NlbCluster	Zatrzymuje wszystkie węzły w klastrze NLB
Stop-NlbClusterNode	Zatrzymuje węzeł w klastrze NLB
Suspend-NlbCluster	Wstrzymuje wszystkie węzły klastra NLB
Suspend-NlbClusterNode	Wstrzymuje konkretny węzeł w klastrze NLB

Uaktualnianie klastra NLB

Aby uaktualnić istniejący klaster NLB do Windows Server 2012 lub Windows Server 2012 R2, możemy go po prostu wyłączyć, zaktualizować wszystkie hosty, a następnie wznowić jego pracę. Wadą takiego rozwiązania jest to, że klaster – na czas jego odłączenia – nie będzie w stanie obsługiwać żądań klientów.

Na szczęście wiele hostowanych w klastrze NLB aplikacji i usług wspiera dużo lepszą opcję uaktualniania – tzw. *uaktualnianie stopniowe* (rolling upgrade). Uaktualnianie

stopniowe pozwala nam na przeprowadzenie procesu uaktualnienia bez konieczności wyłączenia klastra NLB. Krótko mówiąc, wyłączamy pojedynczy węzeł klastra, aktualizujemy go, a następnie włączamy z powrotem. Postępujemy tak z każdym z węzłów klastra z osobna. Aby upewnić się, że przy wyłączaniu hosta istniejące już, nawiązane z nim połączenia zostaną bezpiecznie zakończone, korzystamy z funkcji Drainstop (Opróżnij i zatrzymaj, dostępnej w konsoli Network Load Balancing Manager w podmenu Control Host menu kontekstowego, wywoływanego prawym kliknięciem na danym hoście w drzewie). Funkcja Drainstop sprawia, że węzeł przestaje przyjmować nowe połączenia. Od tej pory wszystkie żądania klientów będą po prostu kierowane do pozostałych węzłów, które znajdują się w stanie aktywnym. Po dokonaniu uaktualnienia, każdy z hostów możemy przywrócić z powrotem do pracy korzystając z opcji Start, dostępnej z poziomu wspomnianego podmenu kontroli hosta. Kontynuujemy ten proces uaktualniając każdy z hostów z osobna, do momentu uaktualnienia całego klastra.



Eksperyment myślowy

Konfigurowanie równoważenia obciążenia sieciowego w Tailspin Toys

Opierając się na zamieszczonym poniżej scenariuszu i stosując wiedzę pozyskaną na temat tego zagadnienia, spróbuj przewidzieć kroki, jakie należałoby podjąć, by zrealizować podane cele. Odpowiedzi do poniższych pytań znajdziesz w dziale „Odpowiedzi”, zamieszczonym na końcu tego rozdziału.

Jesteś administratorem w Tailspin Toys, odpowiedzialnym za zarządzanie infrastrukturą serwerów hostujących firmową witrynę. Ruch do witryny Tailspin Toys stopniowo wzrasta. Obecnie na projekt witryny składają się hostujący ją pojedynczy serwer Windows Server 2012 R2 z IIS w roli frontonu oraz pojedynczy serwer Windows Server 2012 R2 hostujący instancję serwera SQL Server 2012, przechowującego dane konsumentów. Zwiększony ruch na stronie spowodował wydłużenie jej czasu odpowiedzi. Dodatkowo w ubiegłym miesiącu, w czasie dokonywania aktualizacji oprogramowania, witryna była niedostępna. W przeszłości kierownictwo godziło się na to, jednak teraz zapadły decyzje, by witryna była dostępna dla klientów również w czasie aktualizowania oprogramowania.

Zrealizuj następujące cele:

- Serwery IIS i SQL Server uczynić wysoko dostępnymi.
- Upewnij się, że gdy dowolny pojedynczy serwer zostanie uruchomiony ponownie w celu zaktualizowania oprogramowania, witryna nadal będzie dostępna.

- Klienci przeglądający witrynę Tailspin Toys na czas trwania sesji powinni nawiązywać kontakt zawsze z tym samym serwerem IIS, z innym zaś tylko wtedy, gdy serwer, do którego byli początkowo podłączeni, ulegnie awarii.
- Upewnij się, że klienci, którzy podłączeni są do serwera IIS, zostaną poprawnie rozłączeni, zanim serwer rozpocznie proces aktualizacji oprogramowania. Mając na uwadze powyższe informacje, odpowiedz na następujące pytania:
 1. Które z należących do Tailspin Toys serwerów możesz uczynić wysoko dostępnymi wdrażając równoważenie obciążenia sieciowego?
 2. Po zaimplementowaniu równoważenia obciążenia sieciowego, której funkcji użyjesz, by upewnić się, że jakiegokolwiek połączenia do wysoko dostępnych serwerów zakańczane są prawidłowo?
 3. Których trybów filtrowania oraz jakiego rodzaju koligacji i opcji użyjesz, by upewnić się, że klienci zawsze nawiązują kontakt z tym samym serwerem IIS w czasie trwania sesji?

Podsumowanie zagadnienia

- Równoważenie obciążenia sieciowego pozwala nam na odpowiednie skonfigurowanie grupy serwerów, dzięki czemu dla klientów zewnętrznych będą one widoczne jako jeden serwer. Otrzymane przez klaster NLB żądania klientów rozkładane są pomiędzy wszystkie hosty klastra (zwane również węzłami), jeśli tylko zostaną one dopasowane do skonfigurowanych reguł portów.
- Chcąc dobrze przygotować się do egzaminu 70-412 z tematyki równoważenia obciążenia sieciowego, musimy znać wszystkie ustawienia konfiguracji dostępne na pięciu stronach kreatora New Cluster Wizard oraz wszystkie ustawienia reguł portów.
- Jeśli żadna reguła portów nie pasuje do żądania klienta, wówczas żądanie kierowane jest do węzła o najwyższym priorytecie hosta.
- Ustawienie Affinity określa, czy konkretny klient w kolejnych wizytach będzie konsekwentnie kierowany do tego samego hosta w klastrze NLB. Opcja Single Affinity dla każdego z klientów określa koligację klient-host. Opcja Network Affinity do jednego hosta przypisuje wszystkich klientów z tym samym adresem sieciowym /24.
- Dla ruchu, który nie będzie podlegał równoważeniu obciążenia pomiędzy wszystkimi węzłami klastra NLB możemy nadpisać domyślną wartość priorytetu hosta. Aby ustawić niestandardowy priorytet hosta, musimy najpierw utworzyć regułę portów dopasowaną do pożądanego ruchu, z włączonym trybem filtrowania Single Host. Następnie, z poziomu właściwości węzła, któremu chcemy nadać

niestandardowy priorytet, edytujemy regułę portów i modyfikujemy parametr Handling Priority.

- Ustawienia Load Weight używamy do modyfikacji wartości względnej obciążenia klienta, przypisanej do konkretnego węzła w klastrze.

Pytania kontrolne

Aby sprawdzić swoją wiedzę w zakresie tego zagadnienia, odpowiedz na poniższe pytania. Odpowiedzi na nie, wraz z wyjaśnieniem, dlaczego dana odpowiedź jest poprawna lub niepoprawna, znajdziesz w dziale „Odpowiedzi” na końcu tego rozdziału.

1. Skonfigurowałeś klaster NLB złożony z 10 serwerów sieci Web działających pod kontrolą systemu Windows Server 2012 R2 z IIS. Spostrzegasz, że ruch sieciowy kierowany do klastra NLB nie jest rozkładany równomiernie pomiędzy indywidualnymi członkami klastra NLB. Ustawienia reguł portów dla każdego z węzłów nie były modyfikowane i przyjmują wartości domyślne.

Chcesz się upewnić, że żądania sieci Web od klientów rozkładane są pomiędzy wszystkimi 10-cioma węzłami klastra NLB tak równomiernie, jak to tylko możliwe. Które z poniższych ustawień powinieneś włączyć?

- A. Affinity-None
- B. Affinity-Single
- C. Affinity-Network
- D. Load Weight

2. Twoja sieć zawiera klaster NLB wspierający witrynę e-commerce. Wykorzystanie witryny wzrasta. Za każdym razem, gdy dodajesz do klastra NLB nowy węzeł, Twoi klienci skarżą się, że produkty znikają z ich koszyków zakupowych. Chcesz zmniejszyć prawdopodobieństwo wystąpienia tego problemu w przyszłości.

Co powinieneś zrobić?

- A. Zmodyfikować ustawienia Load Weight
- B. Włączyć tryb filtrowania Single Host
- C. Włączyć tryb filtrowania Multiple Host
- D. Zmodyfikować ustawienia Timeout

3. Skonfigurowałeś klaster NLB. Jeden z należących do niego serwerów chcesz wyznaczyć do obsługi całego ruchu, który nie jest wylapywany przez żadną z reguł portów. Co powinieneś zrobić?

- A. Zmodyfikować ustawienie Load Weight
- B. Włączyć tryb filtrowania Single Host
- C. Skonfigurować ustawienie Host Priority
- D. Skonfigurować ustawienie Handling Priority

Zagadnienie 1.2: Konfigurowanie klastra pracy awaryjnej

Zadaniem *klastrów pracy awaryjnej* (Failover Clustering) jest zapewnienie trwałej dostępności wybranych usług lub aplikacji, nawet gdy hostujący je serwer ulegnie awarii. W przeciwieństwie do równoważenia obciążenia sieciowego, klastry pracy awaryjnej są zazwyczaj wykorzystywane do zapewnienia wysokiej dostępności danym, które mogą być często uaktualniane przez klientów. Standardowymi usługami hostowanymi w klastrach pracy awaryjnej są serwery baz danych, serwery poczty elektronicznej, serwery wydruku, maszyny wirtualne wdrożone na Hyper-V (często hostujące krytyczne aplikacje) oraz serwery plików.

Klastry pracy awaryjnej są jednym z najbardziej zaawansowanych zagadnień poruszanych na egzaminie 70-412. Aby je dobrze zrozumieć, musimy najpierw zapoznać się z podstawowymi informacjami na ich temat. Najpierw dowiemy się do czego służą, jak działają oraz jakich wymagają składników. Następnie omówimy zagadnienia wymagane do poprawnej konfiguracji składników klastrów pracy awaryjnej, wliczając w to ustawienia quorum, sieci klastrów oraz magazyny klastrów.

Niniejsze zagadnienie obejmuje następującą tematykę:

- Konfigurowanie quorum
- Konfigurowanie sieci klastrów
- Przywracanie pojedynczych węzłów lub konfiguracji klastra
- Konfigurowanie magazynu klastra
- Implementowanie aktualizacji typu Cluster Aware
- Aktualizowanie klastra
- Konfigurowanie i optymalizowanie współdzielonych woluminów klastra
- Konfigurowanie klastrów bez nazw sieciowych
- Konfigurowanie funkcji Storage Spaces

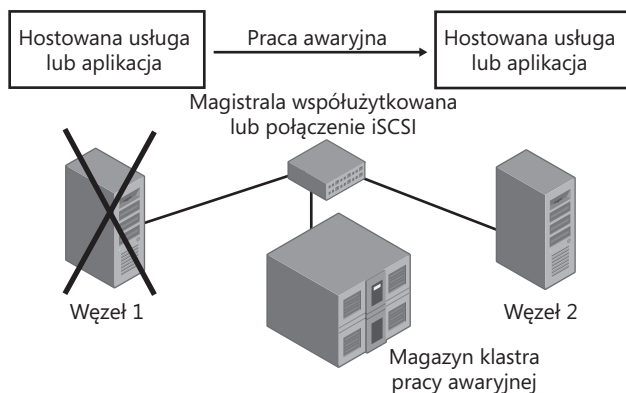
Podstawy klastrów pracy awaryjnej

Klaster pracy awaryjnej jest grupą odpowiednio skonfigurowanych serwerów, zapewniającą ochronę wybranym usługom lub aplikacjom przed awarią. Usługi i aplikacje skonfigurowane w klastrze w celu zapewnienia ochrony znane są również jako *role*, *role klastrowane*, *klastrowane usługi i aplikacje*, *wysoko dostępne usługi i aplikacje*, lub też jako *usługi i aplikacje skonfigurowane pod kątem wysokiej dostępności*. Należące do klastra pracy awaryjnej serwery nazywane są węzłami. Jeśli któryś z węzłów klastra ulegnie awarii, wówczas każda z hostowanych na nim ról natychmiast rozpocznie pracę na innym, wyznaczonym dla danej roli hoście. Jeśli awarii ulegnie jedynie rola, a nie cały węzeł, wtedy podejmowana jest próba jej ponownego uruchomienia,

z ewentualnym przeniesieniem na inny węzeł, jeśli będzie to konieczne. Proces zmiany węzła jest dla użytkowników mało lub praktycznie w ogóle niezauważalny.

Pomiędzy klastrami NLB i klastrami pracy awaryjnej istnieją zasadnicze różnice. Przede wszystkim, w klastrze pracy awaryjnej w danym momencie tylko jeden serwer hostuje klastrowaną usługę. Ponadto węzły klastra pracy awaryjnej, zamiast odczytywać i zapisywać do własnego, lokalnego dysku, przechowują dane roli tylko i wyłącznie w woluminach ulokowanych na *magazynach współużytkowanych*, takich jak np. numery jednostki logicznej (Logical Unit Number, LUN) ulokowane w sieciach magazynowania iSCSI lub Fibre Channel SAN albo na macierzach dyskowych Serial SCSI (SAS). Jako że dla ról w klastrze pracy awaryjnej istnieje tylko jedno źródło danych, klienci nie doświadczają niespójności danych zawartych w klastrowanych usługach. W rezultacie klastry pracy awaryjnej są szczególnie przydatne w zapewnianiu dostępności usługom, w których klienci mogą dokonywać aktualizacji danych. Do typowych usług hostowanych jako role w klastrach pracy awaryjnej zaliczyć można serwery plików, serwery baz danych, serwery wydruku i poczty elektronicznej, a nawet maszyny wirtualne.

Rysunek 1-11 ilustruje proces przenoszenia ról w prostym, dwuwęzłowym klastrze pracy awaryjnej.



RYСУNEK 1-11 W klastrze pracy awaryjnej, gdy jeden serwer ulegnie awarii, kolejny przejmuje jego pracę, wykorzystując dotychczasowy magazyn.

Komponenty sprzętowe klastra pracy awaryjnej

Wymagania sprzętowe dla klastrów pracy awaryjnej dotyczą również serwerów i magazynu. Wszystkie komponenty muszą spełniać określone, niezbędne do uzyskania logo Certified for Windows Server 2012 lub Certified for Windows Server 2012 R2 standardy.

- **Wymagania serwera** Kłaster pracy awaryjnej wymaga co najmniej dwóch fizycznych serwerów z dostępem do sieci. Inaczej mówiąc, wymaga się jednego fizycznego serwera na każdy węzeł w klastrze (maksymalnie do 64 węzłów).

UWAGA Konfigurowanie maszyn wirtualnych do testów

W celach testowych można skonfigurować kłaster jednowęzłowy. Jeśli dysponujemy tylko jednym fizycznym serwerem, jeszcze lepszą opcją do testów i nauki będzie skonfigurowanie dwóch lub więcej maszyn wirtualnych, pełniących funkcje węzłów klastra. Oczywiście opcja ta nie zapewni żadnej ochrony przed awarią fizycznego serwera. Dodatkowo, jako że węzły te będą już wtedy zwirtualizowane, w roli klastrowanych usług nie będzie można wykorzystać już maszyn wirtualnych.

- **Wymagania magazynu** Działanie klastrow pracy awaryjnej opiera się na magazynach współużytkowanych w postaci magazynów sieciowych SAN (iSCSI lub Fibre Channel) lub też macierzy dyskowych Serial-attached SCSI (SAS). Jeśli klastrowaną rolę jest maszyna wirtualna hostowana w Hyper-V, możemy skorzystać z dodatkowej opcji przechowywania plików tej maszyny w udziale sieciowym Windows Server 2012 lub Windows Server 2012 R2.

UWAGA Więcej o sieciach SAN

Mówiąc ogólnie, sieć SAN jest specjalnym typem sieci o wysokiej wydajności, dedykowanej łączeniu serwerów do jednej lub więcej macierzy danych. Macierze dyskowe w sieci SAN są w stanie symulować na podłączonych do sieci SAN komputerach magazyny przyłączone lokalnie. Wybrane i przygotowane przez użytkownika dyski logiczne macierzy (często nazywane *numerami jednostki logicznej*) dla systemu operacyjnego są wówczas widoczne jako dyski lokalne. Jeśli Czytelnik nie jest zbyt obeznany w tematyce sieci SAN, warto, by choć w podstawowym stopniu zapoznać się z tą technologią w Internecie, aby czuć się w tym temacie bardziej pewnie. Jako że zagadnienie 2.3 egzaminu 70-412 dedykowane jest funkcjom Windows Server 2012 R2 związanym z technologią iSCSI, kolejny rozdział tej książki szczegółowo omawia sieci iSCSI SAN.

- **Zalecenia dotyczące sprzętu** Zalecenia pojawiają się na egzaminach firmy Microsoft zdecydowanie rzadziej niż wymagania. Jednak by łatwiej nam było zrozumieć, w jaki sposób klastry pracy awaryjnej Windows Server 2012 lub Windows Server 2012 R2 wdrażane są w środowisku produkcyjnym, powinniśmy zapoznać się z poniższymi wytycznymi:
 - Dla każdego węzła wykorzystujemy identyczne lub mocno zbliżone serwery.
 - Jeśli korzystamy z iSCSI lub Fibre Channel over Ethernet (FCoE), każda karta sieciowa powinna być dedykowana albo sieci LAN, albo sieci SAN, ale nie obu tym sieciom jednocześnie.

- ❑ W celu zapewnienia odporności na uszkodzenia należy upewnić się, że każdemu połączeniu przypisaliśmy zespół kart sieciowych. W idealnym przypadku powinniśmy również skonfigurować nadmierne przełączniki, routery oraz ścieżki sieciowe do klastra.

Wymagania programowe klastrów pracy awaryjnej

Klasytry pracy awaryjnej Windows Server 2012 i Windows Server 2012 R2 wymagają wersji Standard lub Datacenter tych systemów. Klasytry pracy awaryjnej wymagają również, aby wszystkie węzły przyłączone były do tej samej domeny Active Directory Domain Services (AD DS). Dodatkowo na wszystkich węzłach musi zostać zainstalowana funkcja Failover Clustering.

Tworzenie klastra pracy awaryjnej

Na egzaminie 70-412 zadawane w obrębie zagadnienia 1.2 pytania będą raczej dotyczyły ustawień i konfiguracji istniejącego już klastra pracy awaryjnej. Pytania dotyczące poszczególnych kroków tworzenia nowego klastra pracy awaryjnej pojawiają się na egzaminie dużo rzadziej. Aby jednak dobrze się przygotować do tego egzaminu, powinniśmy utworzyć w naszej sieci testowej własny klaster pracy awaryjnej, bowiem najłatwiej przyjdzie nam zrozumieć te klasytry, jeśli zobaczymy je w akcji. Możemy rozpocząć od utworzenia „nagiego” klastra pracy awaryjnej z jedną pustą rolą, a dopiero potem skonfigurować wszystkie wymagane komponenty.

Aby utworzyć klaster pracy awaryjnej, przyłączamy serwery do odpowiedniej domeny AD DS i łączymy je z magazynem udostępnionym. Na wszystkich węzłach w klastrze musimy również zainstalować funkcję Failover Clustering. Możemy posłużyć się w tym celu konsolą Server Manager lub skorzystać z następującego polecenia Windows PowerShell:

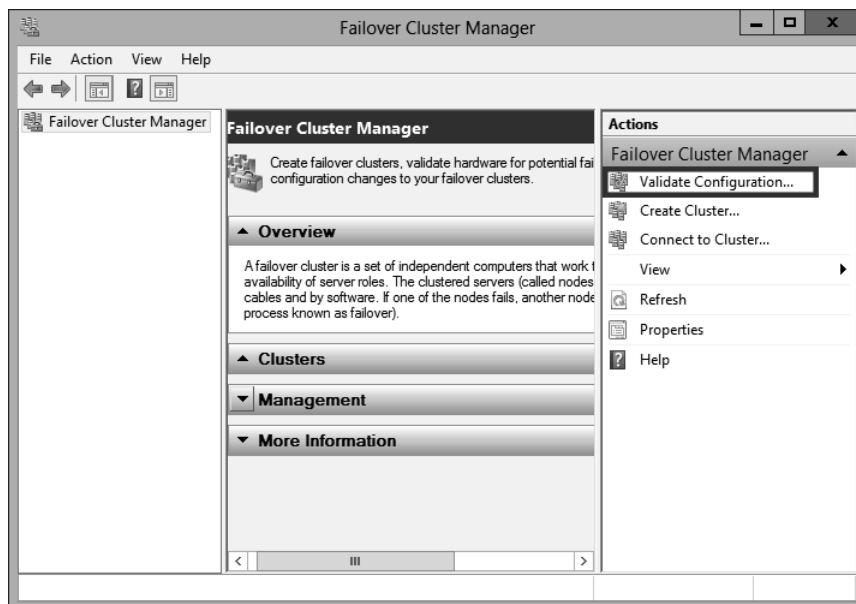
```
Install-WindowsFeature Failover-Clustering -IncludeManagementTools
```

Przed utworzeniem klastra pracy awaryjnej wykonujemy kilka testów weryfikujących, mających na celu sprawdzenie, czy nasz sprzęt i oprogramowanie spełniają określone wymagania. Testy te możemy uruchomić przy pomocy kreatora Validate A Configuration Wizard (klikając Validate Configuration w panelu Actions konsoli Failover Cluster Manager, patrz rysunek 1-12) lub korzystając z polecenia cmdlet Test-Cluster. Jeśli testów tych nie wykonamy ręcznie, zostaną one uruchomione automatycznie z poziomu kreatora Create Cluster Wizard.

Po uruchomieniu testów wybieramy po prostu węzły, które chcemy dodać do klastra. Testy te możemy również uruchomić ponownie także już po jego utworzeniu. Wówczas zamiast konkretnych węzłów podajemy jedynie nazwę utworzonego klastra.

Po zakończeniu pracy kreatora, jeśli to konieczne, dokonujemy odpowiednich zmian w konfiguracji i ponownie uruchamiamy test, powtarzając cały proces

aż do pomyślnego zakończenia weryfikacji. Po zweryfikowaniu konfiguracji, korzystając z kreatora Create Cluster Wizard lub polecenia cmdlet New-Cluster tworzymy nowy klaster. W tym kroku, prócz instalacji podstawy programowej dla klastra, przyłączony magazyn zostanie skonwertowany na dyski klastra, zaś w usłudze Active Directory zostanie utworzone dedykowane klastrowi nowe konto komputera.



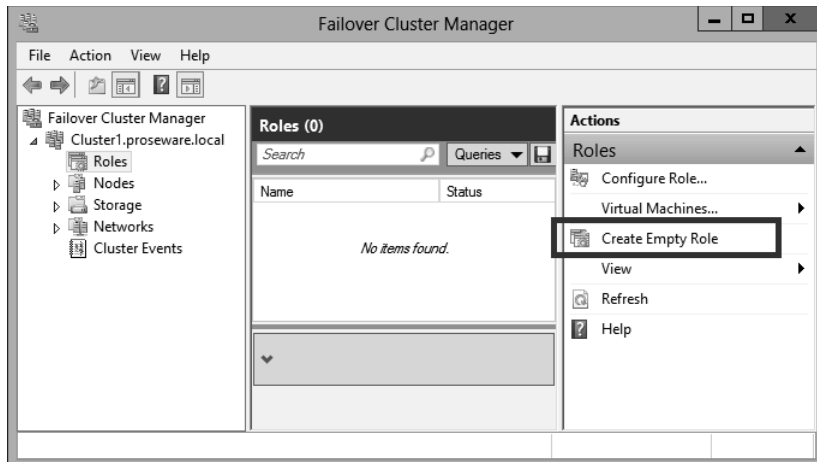
RYСУNEK 1-12 Weryfikowanie wymagań wstępnych serwera pracy awaryjnej

Aby uruchomić kreator Create Cluster Wizard, w panelu Actions konsoli Failover Cluster Manager klikamy Create Cluster (Utwórz klaster). Cała procedura jest dość prosta. Musimy jedynie wiedzieć:

- Które węzły chcemy dodać do klastra.
- Jaką nazwę będzie nosić nowy klaster.
- Jaki adres IP chcemy przypisać do każdej z sieci, do której przyłączone są węzły (możemy również odznaczyć wybrane sieci, jeśli nie chcemy, by klienci łączyli się przez nie do klastra).
- Czy chcemy zachować domyślne ustawienie dodające do klastra cały dostępny magazyn. Zmiana tego zachowania w kreatorze następuje po odznaczeniu opcji Add All Eligible Storage To The Cluster. W powłoce Windows PowerShell, przy poleceniu New-Cluster stosujemy opcję -NoStorage.

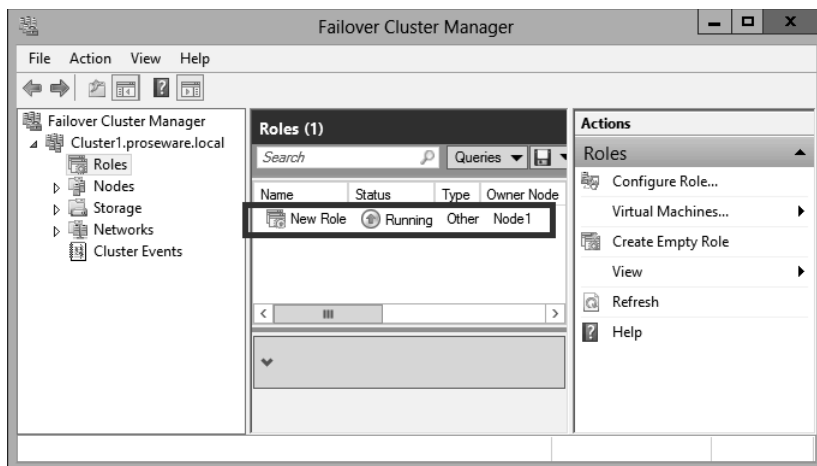
Zanim skonfigurujemy poszczególne komponenty, takie jak sieci, magazyn, kworum czy role, w celu przetestowania podstawowej funkcjonalności klastra pracy awaryjnej możemy posłużyć się rolą pustą. Aby utworzyć pustą rolę w klastrze pracy awaryjnej,

w drzewie konsoli Failover Cluster Manager zaznaczamy węzeł Roles (Role), po czym w panelu Actions klikamy Create Empty Role (Utwórz rolę pustą), jak pokazano na rysunku 1-13.



RYСУNEK 1-13 Tworzenie pustej roli

Po kliknięciu Create Empty Role, przy nadal zaznaczonym węźle Roles nowa rola pojawi się w panelu centralnym, jak na rysunku 1-14.



RYСУNEK 1-14 Pusta rola widoczna w konsoli Failover Cluster Manager

Po utworzeniu podstawowego klastra pracy awaryjnej i zawartej w nim roli pustej, możemy przetestować jego funkcjonalność w konsoli Failover Cluster Manager. W tym celu w środkowym panelu konsoli zaznaczamy tę rolę, następnie w panelu Actions klikamy Move (Przenieś), po czym wybieramy Best Possible Node (Najlepszy możliwy

węzeł), jak na rysunku 1-15. W czasie przenoszenia instancji klastrowanej usługi, w centralnym panelu konsoli możemy zaobserwować zmiany statusu. Jeśli wartość pola Owner Node (Węzeł-właściciel) pomyślnie zmieni się z nazwy jednego węzła na nazwę drugiego, będzie to oznaczać, że funkcja pracy awaryjnej działa w klastrze prawidłowo.



RYСУNEK 1-15 Testowanie klastra pracy awaryjnej poprzez przenoszenie roli na inny węzeł

Aby klasterek pracy awaryjnej uczynić w pełni funkcjonalnym, po jego utworzeniu musimy skonfigurować również pozostałe komponenty. Kolejne podrozdziały stanowią krótki przegląd wymaganych na egzaminie informacji w zakresie konfiguracji sieci, magazynu danych oraz kworum klastrów pracy awaryjnej.

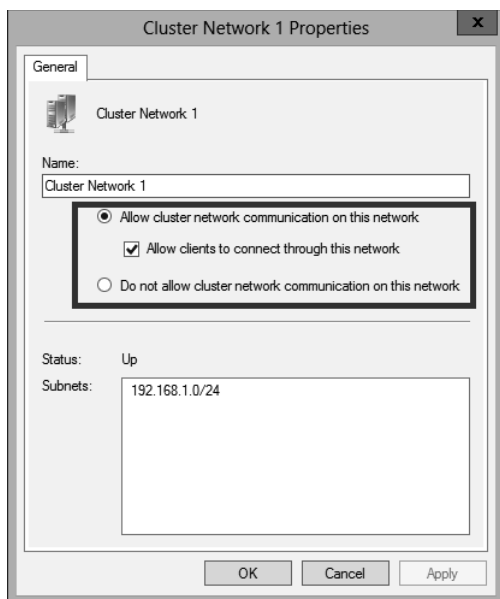
Konfigurowanie sieci klastra

Ustawienia sieci klastra, które musimy znać na potrzeby egzaminu 70-412, znajdziemy w oknie dialogowym właściwości sieci klastra, widocznym na rysunku 1-20. Dostęp do niego uzyskamy klikając prawym przyciskiem konkretną sieć w drzewie konsoli Failover Cluster Manager i wybierając Properties.

Jak pokazano na rysunku 1-16, wykrywane w konsoli Failover Cluster Manager sieci można przypisać do jednej z trzech kategorii:

- Allow Cluster Network Communication On This Network (Zezwól na komunikację sieci klastra w obrębie tej sieci)
- Allow Cluster Network Communication On This Network oraz Allow Clients To Connect Through This Network (Zezwól klientom na łączenie się poprzez tę sieć)
- Do Not Allow Cluster Communication On This Network (Nie zezwalaj na komunikację klastra w obrębie tej sieci)

Jeśli chcemy zarezerwować sieć dla komunikacji wewnątrz klastra lub komunikacji „pulsu” (heartbeat – komunikat określający, czy usługa jest nadal dostępna na danym węźle) oraz uniemożliwić klientom komunikację poprzez tę sieć, musimy odznaczyć opcję Allow Clients To Connect Through This Network. Jeśli rezerwujemy tę sieć dla połączeń węzłów do magazynu danych iSCSI lub jakiejś innej funkcji, zaznaczamy opcję Do Not Allow Cluster Network Communication On This.



RYSUNEK 1-16 Ustawienia sieci klastra

Klastry odłączone od Active Directory

Windows Server 2012 R2 umożliwia nam wdrażanie klastrów pracy awaryjnej niezależnych od usług Active Directory Domain Service (AD DS), dostarczających informacji o nazwach sieciowych. Wdrażając klastery w ten sposób, nazwa sieci klastra lub administracyjny punkt dostępu i nazwy sieciowe klastrowanych ról przechowywane są w obrębie DNS, lecz obiekty nie są tworzone w bazie danych AD DS. Klastry odłączone od Active Directory (Active Directory Detached Clusters) nie wymagają wewnątrz Active Directory obiektów komputera reprezentujących klastry. Kluczem do zrozumienia klastrów odłączonych od Active Directory jest to, że o ile usługa AD DS nie jest dla nazwy sieci klastra wymagana, to tworzące klastery węzły nadal muszą być członkami domeny Active Directory. Korzyścią płynącą z tej funkcji jest możliwość utworzenia klastra pracy awaryjnej bez konieczności posiadania uprawnień wymaganych do tworzenia obiektów komputera wewnątrz AD DS. Microsoft nie zaleca stosowania klastrów odłączonych od Active Directory w przypadku scenariuszy

wymagających użycia uwierzytelniania Kerberos. Ten typ klastra może zostać wdrożony tylko i wyłącznie z poziomu powłoki Windows PowerShell.

DODATKOWE INFORMACJE Klastry odłączone od Active Directory

Więcej informacji na temat klastrów odłączonych od Active Directory można znaleźć na stronie <http://technet.microsoft.com/en-us/library/dn265970.aspx>.

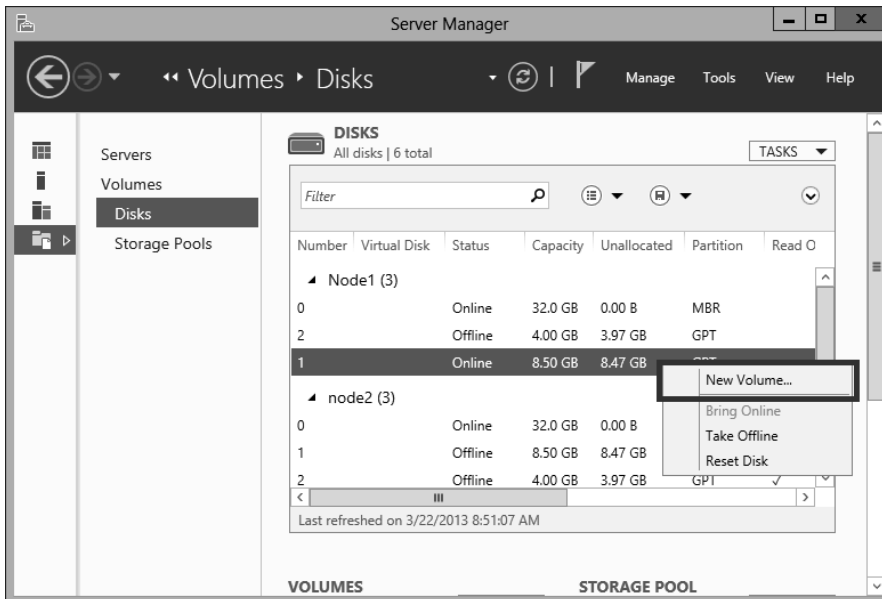
Konfigurowanie magazynu danych klastra

Konfigurowanie magazynu klastra to w praktyce dość skomplikowany temat. Jednak do egzaminu 70-412 wystarczy nam opanowanie tylko kilku zagadnień, takich jak dodawanie dysków do klastra, znajomość i konfiguracja pól magazynu klastra oraz znajomość i umiejętność konfiguracji współdzielonych woluminów klastra.

Dodawanie nowych dysków do klastra

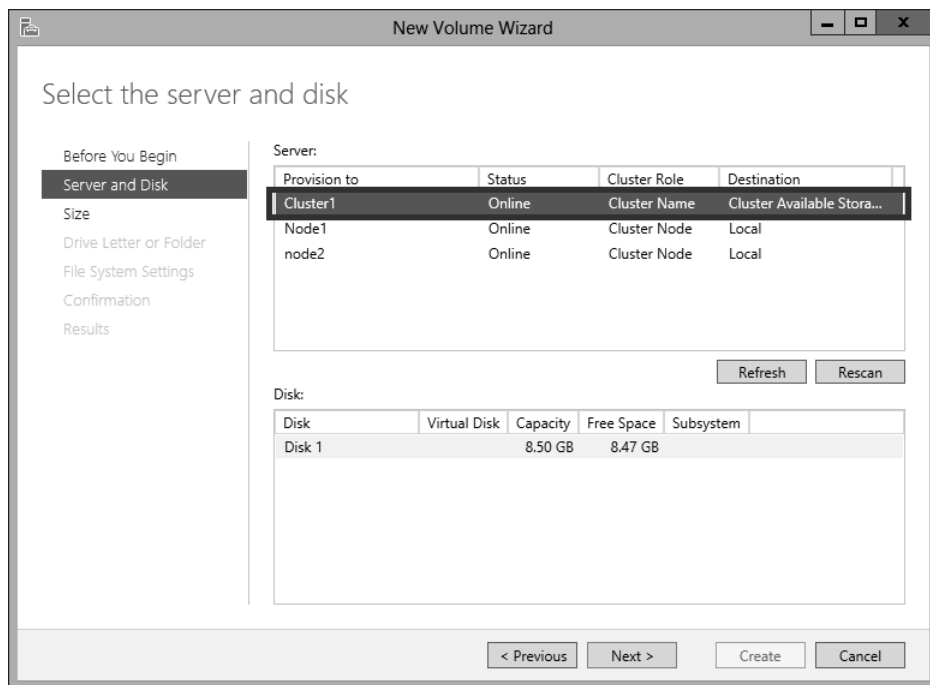
Jeśli do istniejącego klastra pracy awaryjnej chcemy dodać dyski, musimy najpierw przygotować dyski logiczne z magazynu udostępnionego, takiego jak choćby obiekt docelowy iSCSI. Gdy udostępniony dysk pojawi się w konsoli Server Manager, inicjalizujemy go i zmieniamy jego stan na aktywny.

Następnie tworzymy z tego dysku wolumin, jak pokazano na rysunku 1-17.



RYСУNEK 1-17 Tworzenie nowego woluminu w konsoli Server Manager

Przypisujemy nowy wolumin do wybranego klastra pracy awaryjnej, jak na rysunku 1-18 (nazwa klastra widnieje jako nazwa serwera).

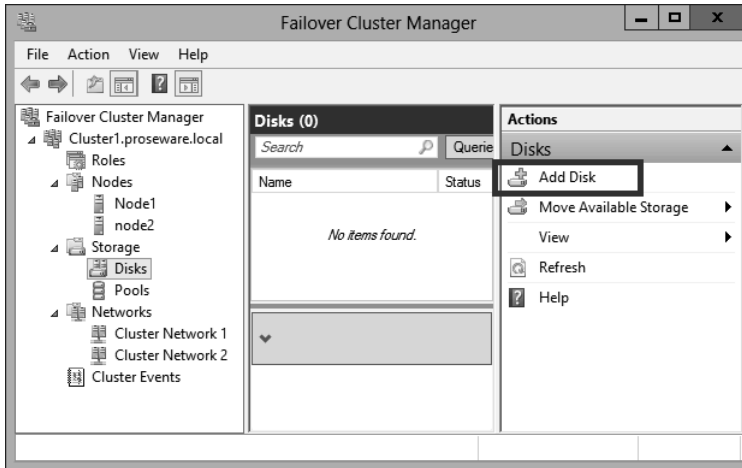


RYСУNEK 1-18 Przypisywanie nowego woluminu do klastra

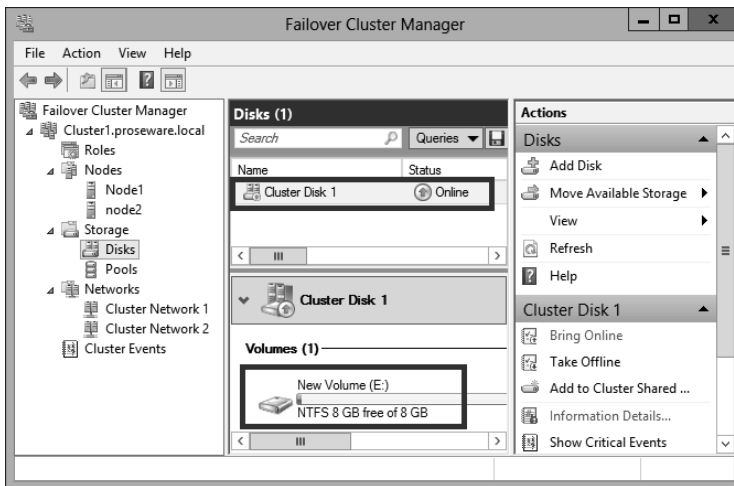
Alternatywnie, dostępny magazyn możemy dodać do klastra z poziomu konsoli Failover Cluster Manager. W tym celu pod sekcją Storage (Magazyn) zaznaczamy w drzewie konsoli węzeł Disk, po czym w panelu Actions klikamy Add Disk (Dodaj dysk, patrz rysunek 1-19). Wybrany przez nas dysk powinien już zawierać jeden lub więcej woluminów, zanim zostanie dodany. Jeśli przygotowaliśmy go przy użyciu narzędzia Disk Management, nie zaś z poziomu konsoli Server Manager, upewnijmy się, że podzieliliśmy go na partycje typu GPT (GUID Partition Table), a nie MBR (Master Boot Record).

Ostatnią opcją jest możliwość dodania dysku do klastra pracy awaryjnej z poziomu powłoki Windows PowerShell. Aby tego dokonać, korzystamy z polecenia Add-ClusterDisk.

Gdy już dodamy dysk do klastra, nowy dysk wraz z jego woluminami będzie widoczny w konsoli Failover Cluster Manager, jak na rysunku 1-20.



RYSUNEK 1-19 Dodawanie nowego dysku do klastra pracy awaryjnej

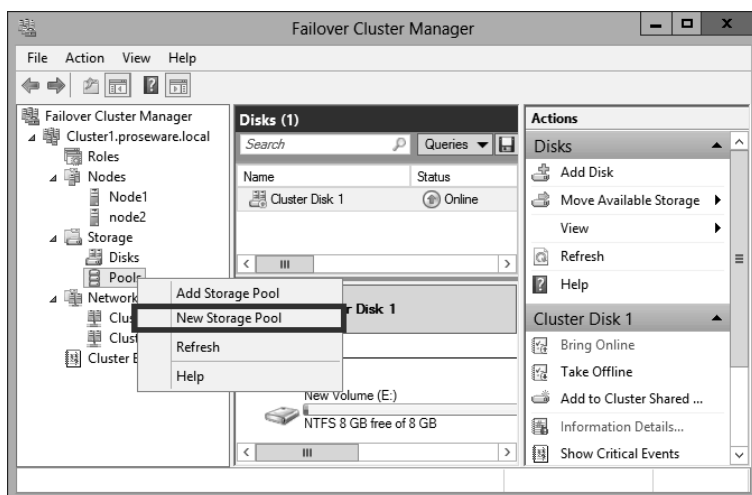


RYSUNEK 1-20 Dysk dodany do klastra pracy awaryjnej

Tworzenie pul magazynu klastra

W systemach Windows Server 2012 i Windows Server 2012 R2 możemy już wykorzystywać magazyny danych w postaci macierzy dyskowych Serial Attached SCSI (SAS) do tworzenia jednej lub więcej pul magazynu dla klastra pracy awaryjnej. Pule te są podobne do tych, które tworzymy dla indywidualnego serwera, korzystając z funkcji Storage Spaces (Miejsca do magazynowania, zagadnienie egzaminu 70-410). Podobnie jak w tej funkcji, pule magazynu możemy wykorzystać w klastrze pracy awaryjnej w formie źródła, z którego możemy następnie utworzyć dyski wirtualne, a ostatecznie woluminy.

Aby utworzyć nową pulę magazynu, w konsoli Failover Cluster Manager przechodzimy do Failover Cluster Manager\[Nazwa klastra]\Storage\Pools, klikamy prawym przyciskiem Pools (Pule), po czym z menu kontekstowego wybieramy New Storage Pool (Nowa pula magazynu), jak na rysunku 1-21. Spowoduje to uruchomienie kreatora New Storage Pool Wizard – tego samego co w przypadku funkcji Storage Spaces (prawdę mówiąc, jeśli dysponujemy udostępnioną macierzą dyskową SAS, możemy posłużyć się konsolą Server Manager do utworzenia puli, a następnie dodać ją do systemu przy pomocy opcji Add Storage Pool). Po utworzeniu puli musimy utworzyć z niej dyski wirtualne, zaś z nowych dysków wirtualne woluminy, zanim będziemy mogli wykorzystać klastrowaną przestrzeń magazynu do hostowania naszych obciążeń roboczych klastra.



RYСУNEK 1-21 Tworzenie nowej puli magazynu dla klastra

DODATKOWE INFORMACJE Konfigurowanie pul magazynu klastra

Więcej informacji dotyczących konfigurowania pul magazynu klastra można znaleźć w artykule „How to Configure a Clustered Storage Space in Windows Server 2012” (Jak skonfigurować klastrowaną funkcję Storage Spaces w Windows Server 2012) dostępnym pod adresem <http://blogs.msdn.com/b/clustering/archive/2012/06/02/10314262.aspx> oraz w artykule „Deploy Clustered Storage Spaces” (Wdrażanie klastrowanej funkcji Storage Spaces) opublikowanym na stronie <http://technet.microsoft.com/en-us/library/jj822937.aspx>.

Dostępność pul magazynu w klastrach pracy awaryjnej niejako implikuje ich obecność na egzaminie 70-412, tym bardziej że ich wymagania i ograniczenia mogą stanowić dobrą podstawę do pytań testowych. Zwróćmy zatem uwagę na następujące wymagania stawiane pulom magazynu w klastrach pracy awaryjnej: