

Timothy Warner  
Craig Zacker

## **Egzamin 70-744**

# Zabezpieczanie systemu Windows Server 2016

Przekład: Krzysztof Kapustka

APN Promise, Warszawa 2017

# Spis treści

<i>Wprowadzenie</i> .....	ix
<i>Ważne: Jak używać tej książki podczas przygotowania do egzaminu</i> .....	xiii
<b>1 Wdrażanie rozwiązań ograniczających podatność serwerów</b> .....	1
<b>Zagadnienie 1.1: Konfiguracja szyfrowania dysków i plików</b> .....	2
Określanie wymagań sprzętu i oprogramowania sprzętowego dla kluczowych funkcji szyfrowania oraz funkcji bezpiecznego rozruchu Secure Boot .....	3
Wdrażanie funkcji BitLocker Drive Encryption .....	5
Konfiguracja funkcji odblokowywania przez sieć Network Unlock .....	12
Wdrażanie procesu odzyskiwania funkcji BitLocker .....	13
Zarządzanie systemem plików EFS .....	18
<b>Zagadnienie 1.2: Wdrażanie rozwiązań do instalowania poprawek i aktualizowania serwerów</b> .....	20
Instalacja i konfiguracja usług WSUS .....	21
Tworzenie grup komputerów i konfigurowanie aktualizacji automatycznych ..	24
Zarządzanie aktualizacjami z wykorzystaniem usługi WSUS .....	27
Konfigurowanie raportowania WSUS .....	28
Rozwiązywanie problemów z konfiguracją i wdrożeniem WSUS .....	30
<b>Zagadnienie 1.3: Wdrażanie ochrony przed złośliwym oprogramowaniem</b> ....	32
Wdrażanie rozwiązania chroniącego przed złośliwym oprogramowaniem z użyciem programu Windows Defender .....	32
Integrowanie programu Windows Defender z usługami WSUS i Windows Update .....	36
Implementacja reguł funkcji AppLocker .....	37
Implementacja funkcji Control Flow Guard .....	42
Implementacja zasad funkcji Device Guard .....	44
<b>Zagadnienie 1.4: Ochrona poświadczeń</b> .....	49
Określanie wymagań funkcji Credential Guard .....	50
Konfiguracja funkcji Credential Guard .....	51
Wdrażanie blokowania NTLM .....	55
<b>Zagadnienie 1.5: Tworzenie linii bazowych zabezpieczeń</b> .....	56
Instalacja i konfiguracja programu Security Compliance Manager .....	57

Tworzenie i importowanie linii bazowych zabezpieczeń . . . . .	61
Wdrażanie konfiguracji do serwerów przyłączonych i nieprzyłączonych do domeny. . . . .	63
Podsumowanie rozdziału . . . . .	66
Eksperyment myślowy. . . . .	69
Odpowiedzi do eksperymentu myślowego. . . . .	69
<b>2 Ochrona infrastruktury wirtualizacji . . . . .</b>	<b>71</b>
<b>Zagadnienie 2.1: Wdrażanie rozwiązania Guarded Fabric . . . . .</b>	<b>72</b>
Instalacja i konfiguracja usługi Host Guardian Service . . . . .	73
Konfiguracja zaświadczenia przez zaufanego administratora lub zaufany moduł TPM . . . . .	75
Konfiguracja usługi Key Protection Service z użyciem ochrony HGS . . . . .	81
Konfiguracja chronionego hosta . . . . .	81
Migracja chronionych maszyn wirtualnych do innych chronionych hostów . . . . .	83
Rozwiązywanie problemów z chronionymi hostami . . . . .	88
<b>Zagadnienie 2.2: Wdrażanie maszyn wirtualnych chronionych     i wspieranych przez szyfrowanie . . . . .</b>	<b>90</b>
Określanie scenariuszy i wymagań wdrażania chronionych maszyn wirtualnych. . . . .	90
Tworzenie chronionych maszyn wirtualnych za pośrednictwem środowiska Hyper-V . . . . .	92
Włączanie i konfiguracja modułu vTPM. . . . .	97
Określanie wymagań i scenariuszy wdrażania maszyn wirtualnym wspieranych przez szyfrowanie. . . . .	100
Odzyskiwanie chronionej maszyny wirtualnej. . . . .	101
Podsumowanie rozdziału . . . . .	104
Eksperyment myślowy. . . . .	105
Odpowiedzi do eksperymentu myślowego. . . . .	105
<b>3 Ochrona infrastruktury sieciowej . . . . .</b>	<b>107</b>
<b>Zagadnienie 3.1: Konfiguracja zapory systemu Windows . . . . .</b>	<b>108</b>
Konfiguracja zapory systemu Windows z zabezpieczeniami zaawansowanymi . . . . .	108
Konfiguracja profili lokalizacji sieciowej oraz wdrażanie reguł profilów przy użyciu zasad grupy. . . . .	117
Konfiguracja reguł zabezpieczeń połączeń przy użyciu zasad grupy, konsoli z graficznym interfejsem użytkownika lub programu Windows PowerShell. . . . .	119

Konfiguracja zapory systemu Windows w celu zablokowania lub odblokowania aplikacji. ....	126
Konfiguracja uwierzytelnionych wyjątków zapory systemu Windows .....	128
<b>Zagadnienie 3.2: Wdrażanie sterowanej programowo rozproszonej zapory sieciowej</b> .....	130
Określanie scenariuszy i wymagań wdrażania rozproszonej zapory sieciowej za pomocą sieci sterowanych programowo .....	131
Określanie scenariuszy wykorzystania dla zasad rozproszonych zapór sieciowych oraz grup zabezpieczeń sieciowych .....	134
<b>Zagadnienie 3.3: Ochrona ruchu sieciowego</b> .....	138
Określanie scenariuszy i implementacji zabezpieczeń protokołu SMB 3.1.1 ..	138
Włączanie szyfrowania SMB w udziałach SMB .....	140
Konfiguracja podpisywania SMB i wyłączanie SMB 1.0. ....	142
Zabezpieczanie ruchu DNS przy użyciu zasad DNSSEC i DNS. ....	143
Instalacja i konfiguracja narzędzia Microsoft Message Analyzer w celu analizy ruchu sieciowego .....	149
Podsumowanie rozdziału .....	152
Eksperyment myślowy. ....	153
Odpowiedzi do eksperymentu myślowego. ....	154
<b>4 Zarządzanie tożsamościami uprzywilejowanymi</b> .....	157
<b>Zagadnienie 4.1: Wdrażanie podejścia do projektowania lasu administracyjnego ESAE</b> .....	158
Określanie scenariuszy i wymagań wdrażania architektury projektowania lasów ESAE w celu utworzenia dedykowanego lasu administracyjnego. ....	158
Określanie scenariuszy i wymagań wdrażania zasad czystego źródła w architekturze Active Directory .....	162
<b>Zagadnienie 4.2: Wdrażanie funkcjonalności Just-in-Time Administration.</b> ...	166
Tworzenie nowego lasu ufortyfikowanego w istniejącym środowisku Active Directory za pomocą programu Microsoft Identity Manager (MIM). ....	167
Konfiguracja zaufania pomiędzy lasem produkcyjnym a lasem ufortyfikowanym .....	168
Tworzenie podmiotów zabezpieczeń w tle w obrębie lasu ufortyfikowanego	171
Konfiguracja portalu sieci Web programu MIM .....	172
Żądanie dostępu uprzywilejowanego za pomocą portalu sieci Web programu MIM .....	173
Określanie wymagań i scenariuszy użycia dla rozwiązań PAM. ....	174
Tworzenie i wdrażanie zasad programu MIM. ....	176

Wdrażanie podmiotów administracji just-in-time za pomocą zasad opartych o czas .....	177
Żądanie dostępu uprzywilejowanego za pomocą powłoki Windows PowerShell .....	179
<b>Zagadnienie 4.3: Wdrażanie funkcjonalności Just-Enough-Administration</b> ...	181
Włączanie rozwiązania JEA w systemie Windows Server 2016 .....	182
Tworzenie i konfiguracja plików konfiguracyjnych sesji .....	184
Tworzenie i konfiguracja plików możliwości ról .....	186
Tworzenie punktu końcowego JEA .....	190
Łączenie się do punktu końcowego JEA na serwerze w celu administracji ...	191
Przeglądanie dzienników .....	191
Pobieranie programu WMF 5.1 do systemu Windows Server 2008 R2 .....	193
Konfiguracja punktu końcowego JEA na serwerze za pomocą konfiguracji żądanego stanu .....	194
<b>Zagadnienie 4.4: Wdrażanie stacji roboczych z dostępem uprzywilejowanym</b>	196
Wdrażanie rozwiązania PAW .....	196
Konfiguracja zasad grupy dla przypisywania praw użytkownika .....	201
Konfiguracja opcji zabezpieczeń w zasadach grupy .....	206
Włączanie i konfiguracja funkcji Remote Credential Guard w celu uzyskania zdalnego dostępu do komputerów .....	208
<b>Zagadnienie 4.5: Wdrażanie rozwiązania hasła administratora lokalnego (LAPS)</b> .....	210
Instalacja i konfiguracja narzędzia LAPS .....	211
Ochrona haseł administratorów lokalnych za pomocą narzędzia LAPS .....	216
Zarządzanie właściwościami i parametrami haseł za pomocą narzędzia LAPS	218
Podsumowanie rozdziału .....	221
Eksperyment myślowy .....	223
Odpowiedzi do eksperymentu myślowego .....	223
<b>5 Wdrażanie rozwiązań do wykrywania zagrożeń</b> .....	225
<b>Zagadnienie 5.1: Konfiguracja zaawansowanych zasad inspekcji</b> .....	225
Określanie różnic i scenariuszy wykorzystania lokalnych i zaawansowanych zasad inspekcji .....	227
Wdrażanie inspekcji za pomocą zasad grupy i narzędzia Auditpol.exe .....	235
Wdrażanie inspekcji za pomocą programu Windows PowerShell .....	243
Tworzenie zasad inspekcji opartych o wyrażenia .....	245
Konfiguracja zasad inspekcji aktywności PNP .....	246
Konfiguracja zasad inspekcji członkostwa w grupach .....	247
Włączanie i konfiguracja rejestrowania modułu, bloku skryptu i transkrypcji w programie Windows PowerShell .....	248

<b>Zagadnienie 5.2: Instalacja i konfiguracja narzędzia Microsoft Advanced Threat Analytics</b> .....	251
Określanie scenariuszy wykorzystania narzędzia ATA .....	252
Określanie wymagań dla wdrożenia narzędzia ATA .....	254
Instalacja i konfiguracja bramki ATA Gateway na dedykowanym serwerze ..	259
Instalacja i konfiguracja bramki ATA Lightweight Gateway bezpośrednio na kontrolerze domeny .....	263
Konfiguracja alertów w konsoli ATA Center na wypadek wykrycia podejrzanej aktywności .....	264
Przegląd i edycja podejrzanej aktywności na osi czasu ataku .....	267
<b>Zagadnienie 5.3: Wykrywanie zagrożeń za pomocą pakietu Operations Management Suite</b> .....	270
Określanie scenariuszy wdrażania i wykorzystania OMS .....	270
Określanie dostępnych do wykorzystania funkcji zabezpieczeń i inspekcji ..	278
Określanie scenariuszy wykorzystania analizy dzienników .....	281
Podsumowanie rozdziału .....	284
Eksperyment myślowy .....	285
Odpowiedzi do eksperymentu myślowego .....	286
<b>6 Wdrażanie zabezpieczeń odpowiednich dla obciążeń roboczych</b> ..	287
<b>Zagadnienie 6.1: Zabezpieczanie infrastruktury rozwoju aplikacji i obciążeń serwera</b> .....	287
Określanie scenariuszy wykorzystania wspieranych obciążeń roboczych i wymagań dla wdrożeń systemu Nano Server .....	288
Instalacja i konfiguracja systemu Nano Server .....	290
Wdrażanie zasad zabezpieczeń w systemach Nano Server za pomocą funkcji Desired State Configuration .....	304
Określanie scenariuszy i wymagań dla kontenerów Windows Server i Hyper-V .....	307
Instalacja i konfiguracja kontenerów Hyper-V .....	309
<b>Zagadnienie 6.2: Wdrażanie bezpiecznej infrastruktury usług plików dynamiczną kontrolą dostępu</b> .....	311
Instalacja usługi roli File Server Resource Manager .....	312
Konfiguracja limitów przydziałów .....	314
Konfiguracja osłon plików .....	322
Konfiguracja raportów magazynowania .....	324
Konfiguracja zadań zarządzania plikami .....	327
Konfiguracja infrastruktury klasyfikacji plików za pomocą narzędzia FSRM ..	330
Wdrażanie folderów roboczych .....	337
Konfiguracja typów oświadczeń użytkowników i urządzeń .....	341

Tworzenie i konfiguracja właściwości zasobów oraz list właściwości zasobów	344
Tworzenie i konfiguracja centralnych reguł i zasad dostępu	347
Wdrażanie przemieszczania i zmian zasad	353
Konfiguracja inspekcji dostępu do plików	354
Korygowanie problemu odmowy dostępu	356
Podsumowanie rozdziału	360
Eksperyment myślowy	361
Odpowiedzi do eksperymentu myślowego	361
<i>Indeks</i>	363
<i>O autorach</i>	376