Microsoft

Timothy Warner
Craig Zacker

Egzamin 70-744

Zabezpieczanie systemu Windows Server 2016

Przekład: Krzysztof Kapustka

APN Promise, Warszawa 2017

Egzamin 70-744: Zabezpieczanie systemu Windows Server 2016

Authorized Polish translation of the English language edition entitled: Exam Ref 70-744: Securing Windows Server 2016, by Timothy Warner and Craig Zacker,
ISBN: 978-1-5093-0426-4

APN PROMISE SA, ul. Domaniewska 44a, 02-672 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

ISBN: 978-83-7541-318-2

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

Spis treści

Wprowadzenie

W wielu podręcznikach dotyczących systemu Windows Server stosowane jest podejście, w ramach którego czytelnicy uczą się tego produktu w najdrobniejszych szczegółach. Tego rodzaju książki są zazwyczaj bardzo grube i niewygodne w czytaniu, zaś próba przyswojenia wszystkich podawanych w nich informacji może stanowić ogromne wyzwanie. Z tego powodu podręczniki te nie stanowią zazwyczaj najlepszego wyboru dla osób przygotowujących się do egzaminów certyfikacyjnych, takich jak egzamin 70-744, „Securing Windows Server 2016" (Zabezpieczanie systemu Windows Server 2016). W tej książce skupiam się na przeglądzie tych umiejętności w zakresie obsługi systemu Windows Server, które są niezbędne do zaliczenia egzaminu 70-744. Naszym celem było nie tylko omówienie wszystkich zagadnień, jakie sprawdzane są na egzaminie, ale również przedstawienie zawartych tu informacji w ujęciu praktycznym. Podręcznik ten nie powinien być jedynym materiałem szkoleniowym wykorzystywanym w ramach przygotowań do egzaminu, ale może on być traktowany jako materiał podstawowy. Zalecamy połączenie informacji prezentowanych w tej książce z praktycznymi ćwiczeniami wykonywanymi w środowisku testowym (lub produkcyjnym, w ramach codziennej pracy).

Egzamin 70-744 skierowany jest do profesjonalistów IT, którzy mogą pochwalić się co najmniej trzema latami doświadczenia w pracy z systemem Windows Server. Nie oznacza to, że zdanie tego egzaminu w przypadku nie posiadania tak dużego doświadczenia jest niemożliwe, jednak osiągnięcie tego celu będzie wówczas znacznie trudniejsze. Oczywiście każdy z nas jest inny, więc należy podkreślić, że pozyskanie wiedzy i umiejętności wymaganych do zdania egzaminu 70-744 w czasie krótszym niż trzy lata jest jak najbardziej realne. Uważamy, że zamieszczone w tej książce informacje będą przydatne dla dowolnego czytelnika, bez względu na to, czy będzie to starszy administrator Windows Server, czy też osoba mająca za sobą dopiero kilka lat doświadczenia w pracy z tym systemem.

Podręcznik ten omawia wszystkie główne obszary tematyczne, jakie sprawdzane są na wspomnianym egzaminie, ale nie omawia on wszystkich jego pytań Tylko zespół egzaminacyjny Microsoft ma dostęp do istniejących pytań egzaminu, a że Microsoft regularnie dodaje nowe pytania do istniejącej puli, omówienie konkretnych pytań egzaminacyjnych staje się w praktyce niemożliwe. Podręcznik ten należy więc traktować jako uzupełnienie dla dotychczasowych umiejętności praktycznych oraz innych materiałów szkoleniowych. Jeśli napotkasz w tej książce jakiś temat, w którym nie czujesz się zbyt komfortowo, skorzystaj z dostępnych w tekście odnośników „Dodatkowe materiały". Uzyskasz w ten sposób dostęp do większej ilości informacji, które będziesz

mógł skrupulatnie przestudiować. Wiele cennych informacji można znaleźć nie tylko w witrynach MSDN i TechNet, ale także na blogach oraz forach internetowych.

Organizacja podręcznika

Podręcznik ten zorganizowany został w oparciu o zagadnienia z listy „Sprawdzane umiejętności" opublikowanej dla egzaminu 70-744. Dostęp do listy sprawdzanych umiejętności dla dowolnego egzaminu można uzyskać na stronie Microsoft Learning pod adresem *http://aka.ms/examlist*. Każdy rozdział tej książki odpowiada głównemu obszarowi tematycznemu z tej listy, zaś dostępne w danym obszarze tematycznym zadania techniczne określają organizację danego rozdziału. Jeśli przykładowo egzamin sprawdza umiejętności w sześciu głównych obszarach tematycznych, dedykowany mu podręcznik składać się będzie z sześciu rozdziałów.

Certyfikaty firmy Microsoft

Certyfikaty Microsoft wyróżniają Cię poprzez poświadczenie Twoich umiejętności oraz doświadczenia w pracy z bieżącymi produktami i technologiami firmy Microsoft. Egzaminy i odpowiadające im certyfikaty tworzone są w celu sprawdzenia opanowania przez Ciebie krytycznych kompetencji, które wykorzystywane są podczas projektowania i rozwoju, lub też wdrażania i wspierania rozwiązań z wykorzystaniem produktów i technologii Microsoft – zarówno lokalnie, jak i w chmurze. Certyfikaty przynoszą wiele różnych korzyści nie tylko dla ich posiadaczy, ale także dla pracodawców i organizacji.

Więcej informacji Wszystkie certyfikaty Microsoft

Szczegółowe informacje na temat poszczególnych certyfikatów Microsoft, wliczając w to również ich pełny wykaz, znajdują się na stronie *http://www.microsoft.com/learning*.

Darmowe e-booki od Microsoft Press

Darmowe e-booki wydawnictwa Microsoft Press omawiają szeroki zakres tematów, od ogólnych zagadnień technicznych, aż po szczegółowe informacje na tematy specjalne. Podręczniki te, rozprowadzane w formatach PDF, EPUB oraz Mobi, dostępne są do pobrania na stronie:

http://aka.ms/mspressfree

Zaglądaj tam regularnie, aby sprawdzić dostępne nowości!

Microsoft Virtual Academy

Poszerz swoją wiedzę w zakresie technologii Microsoft za pośrednictwem darmowych i prowadzonych przez ekspertów szkoleń online Microsoft Virtual Academy (MVA). MVA oferuje obszerną bibliotekę filmów, sesji na żywo oraz innych materiałów ułatwiających poznawanie najnowszych technologii oraz przygotowujących do egzaminów certyfikacyjnych. Wszystko, czego potrzebujesz, znajdziesz pod adresem:

http://mva.microsoft.com

Szybki dostęp do zasobów online

W ramach treści tej książki zamieściłem liczne adresy prowadzące do stron internetowych zawierających dodatkowe informacje. Jako że niektóre z tych adresów mogą okazać się niewygodne do ręcznego wprowadzenia w przeglądarce internetowej, zgromadziłem je wszystkie na jednej liście, tak aby czytelnicy wersji drukowanej tego podręcznika mogli łatwo się do nich odnosić podczas czytania.

https://aka.ms/examref744/downloads

Adresy URL pogrupowane są według rozdziałów i nagłówków tej książki. Aby przejść bezpośrednio na stronę dostępną pod adresem napotkanym w treści podręcznika, wyszukaj odpowiadające mu hiperłącze na wspomnianej liście.

Errata, aktualizacje i wsparcie dla książki

Dołożyliśmy wszelkich starań, aby książka ta, jak również towarzysząca jej zawartość, pozbawione były jakichkolwiek wad. Aktualizacje dla tego podręcznika – w formie listy nadesłanych błędów i poprawek – dostępne są pod adresem:

https://aka.ms/examref744/errata

Jeśli znalazłeś błąd, który nie jest widoczny na tej liście, prosimy o przysłanie go nam przy użyciu formularza dostępnego na tej samej stronie.

Jeśli potrzebujesz dodatkowego wsparcia, skontaktuj się z zespołem Microsoft Press Book Support pod adresem mspinput@microsoft.com.

Proszę zwrócić uwagę, że wsparcie dla oprogramowania i sprzętu firmy Microsoft nie jest świadczone w ramach powyższych adresów. W celu uzyskania pomocy w zakresie oprogramowania lub sprzętu Microsoft udaj się na stronę *http://support.microsoft.com*.

Czekamy na Twój odzew

W Microsoft Press Twoja satysfakcja jest naszym najwyższym priorytetem, a Twoja opinia naszym najcenniejszym nabytkiem. Podziel się z nami swoją opinią na temat tej książki na stronie:

http://aka.ms/tellpress

Wiemy, że jesteś zajęty, dlatego skróciliśmy naszą ankietę do zaledwie kilku pytań Twoje odpowiedzi kierowane są bezpośrednio do redaktorów w Microsoft Press (nie pozyskujemy żadnych informacji osobowych). Z góry dziękujemy za wszelkie uwagi!

Pozostańmy w kontakcie

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

Podziękowania

Chciałbym podziękować mojemu przyjacielowi i koledze z Microsoft Press, Orinowi Thomasowi, za przedstawienie mojej osoby, co w efekcie przełożyło się na moją pracę nad tą książką. Dziękuję Karen Shall i Trinie Macdonald za ich profesjonalną pomoc redaktorską. Dziękuję Troy'owi Mottowi za jego wspaniałe umiejętności zarządzania projektem. Jak zawsze, dziękuję swojej rodzinie (Susan, Zoey i „zwierzakom") za ich miłość i wsparcie.

Timothy Warner

Ważne: Jak używać tej książki podczas przygotowania do egzaminu

Egzaminy certyfikacyjne weryfikują Twoją wiedzę praktyczną i znajomość produktu. Ten podręcznik pomoże ci się przekonać, czy jesteś gotów do przystąpienia do egzaminu, sprawdzając Twoją znajomość zagadnień wchodzących w jego skład. Dzięki niemu możesz określić, które tematy znasz doskonale, a które obszary wymagają dodatkowej pracy. Aby ułatwić odświeżenie umiejętności z określonych dziedzin, dołączyliśmy też wskazówki „Dodatkowe materiały", kierujące do dodatkowych, zewnętrznych źródeł informacji.

Podręcznik ten nie może zastąpić doświadczenia praktycznego. Książka ta nie ma na celu uczenia nowych umiejętności, ale utrwalenie i uporządkowanie już posiadanej wiedzy.

Zalecamy, aby w trakcie przygotowań do egzaminu korzystać z wielu dostępnych materiałów szkoleniowych. Więcej informacji na temat dostępnych szkoleń można znaleźć pod adresem https://www.microsoft.com/learning. Dla wielu egzaminów dostępne są Microsoft Official Practice Tests – ich spis można znaleźć pod adresem https://aka.ms/practicetests. Dostępne są również darmowe szkolenia online i wykłady na żywo w Microsoft Virtual Academy, pod adresem https://www.microsoftvirtualacademy.com.

Książka ta została uporządkowana według listy mierzonych umiejętności (Skills measured) dla tego egzaminu. Lista taka dla każdego egzaminu jest dostępna w witrynie Microsoft Learning: https://aka.ms/examlist.

Warto odnotować, że niniejsza książka opiera się na publicznie dostępnych informacjach na temat egzaminów oraz doświadczeniach autorów. W celu zachowania pełnej poufności autorzy nie mieli dostępu do treści rzeczywistych egzaminów.

ROZDZIAŁ 1

Wdrażanie rozwiązań ograniczających podatność serwerów

Ograniczanie podatności serwera (ang. *server hardening*) jest procesem polegającym na usprawnianiu konfiguracji zabezpieczeń serwera. Serwer z systemem Windows może stać się łatwym celem dla atakujących, jeśli:

- pliki systemu operacyjnego zostaną zainstalowane z niezaufanego źródła,
- w systemie nie zainstalowano najnowszych poprawek i aktualizacji bezpieczeństwa,
- do kont administratorów przypisane zostały słabe hasła,
- zamiast systemu NTFS stosowane są inne, niezaszyfrowane systemy plików.

Oczywiście powyższa lista nie jest kompletna i ma na celu jedynie nakreślenie właściwego sposobu myślenia. W tym rozdziale przyjrzymy się kilku różnym technikom, których celem jest podniesienie poziomu bezpieczeństwa naszych komputerów infrastruktury Windows Server 2016.

Zagadnienia egzaminacyjne omawiane w tym rozdziale:

Zagadnienie 1.1: Konfiguracja szyfrowania dysków i plików

Omawianie umiejętności sprawdzanych na egzaminie 70-744 rozpoczniemy od dostępnej w systemie Windows Server 2016 funkcji szyfrowania dysków i plików. Koncepcja pełnego szyfrowania dysku jest bardzo prosta – chcemy zakodować całą zawartość dysku na poziomie jego sektorów, tak aby dane mogły z niego odczytać wyłącznie osoby do tego uprawnione.

Aby funkcja szyfrowania BitLocker Drive Encryption działała w sposób efektywny, musi ona zostać wdrożona wraz z zasadą najmniejszego uprzywilejowania (ang. principle of least privilege), będącą jedną z podstawowych zasad bezpieczeństwa IT. Oznacza to, że operatorzy serwerów powinni mieć dostęp wyłącznie do tych zasobów, które są im niezbędne do realizacji przydzielonych im zadań. To zrozumiałe, w końcu lokalny administrator mógłby w łatwy sposób wyłączyć funkcję BitLocker, a co za tym idzie ominąć zapewnianą przez nią ochronę.

W ramach tego zagadnienia omówione zostaną następujące zadania:

- Określanie wymagań sprzętu i oprogramowania sprzętowego dla kluczowych funkcji szyfrowania oraz funkcji bezpiecznego rozruchu Secure Boot
- Włączanie funkcji BitLocker w celu wykorzystania funkcji Secure Boot na potrzeby weryfikacji integralności platformy i danych konfiguracji rozruchu BCD
- Wdrażanie funkcji BitLocker Drive Encryption ze wsparciem i z pominięciem modułu TPM
- Konfiguracja ustawień zasad grupy BitLocker
- Konfiguracja funkcji odblokowywania przez sieć Network Unlock
- Konfiguracja funkcji BitLocker na współdzielonych woluminach klastrów oraz w sieciach magazynowania SAN
- Wdrażanie procesu odzyskiwania funkcji BitLocker za pomocą rozwiązań samodzielnego odzyskiwania i odzyskiwania haseł
- Konfiguracja funkcji BitLocker dla maszyn wirtualnych Hyper-V
- Ustalanie scenariuszy wykorzystania systemu szyfrowania plików EFS
- Konfiguracja agenta odzyskiwania danych EFS
- Zarządzanie certyfikatami systemu EFS i funkcji BitLocker, w tym tworzenie kopii zapasowych i ich przywracanie

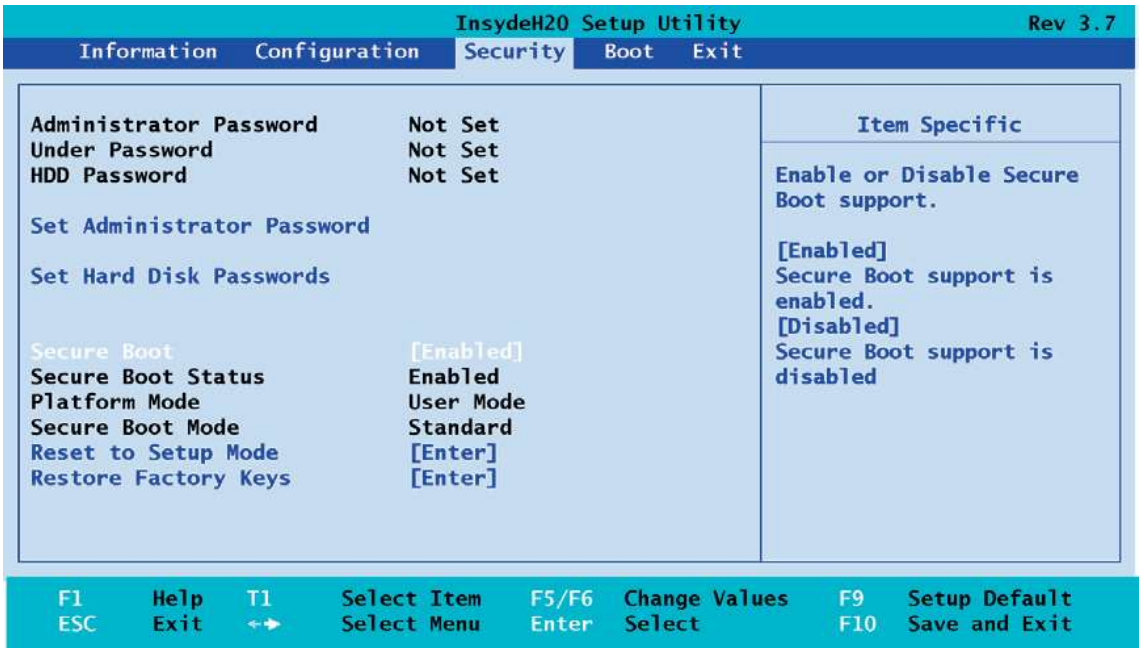
Określanie wymagań sprzętu i oprogramowania sprzętowego dla kluczowych funkcji szyfrowania oraz funkcji bezpiecznego rozruchu Secure Boot

W tej części zajmiemy się kilkoma funkcjami bezpieczeństwa sprzętowego, które nie są wyłącznie domeną systemów operacyjnych Windows Server, lecz są przez te systemy w pełni wspierane. Omówimy sobie interfejs UEFI, funkcję szyfrowania BitLocker Drive Encryption z opcjonalnym wsparciem modułu TPM, sposób działania funkcji odblokowywania przez sieć Network Unlock oraz sposób konfigurowania funkcji BitLocker Drive Encryption z wykorzystaniem zasad grupy.

UEFI

Interfejs Unified Extensible Firmware Interface (UEFI) jest następcą starszego interfejsu sprzętowego Basic Input Output System (BIOS), z którym mieliśmy do czynienia od czasów pierwszych komputerów PC. Dzisiaj każdy nowo zakupiony przez nas serwer będzie już wykorzystywał interfejs UEFI. Windows Server 2016 w pełni obsługuje wszystkie funkcje UEFI, w tym również funkcję Secure Boot.

Sposób uruchamiania na serwerze oprogramowania konfiguracyjnego UEFI uzależniony jest w całości od jego dostawcy OEM. Aby dowiedzieć się, który klawisz lub kombinacja klawiszy aktywuje to oprogramowanie, należy zapoznać się z dołączoną do sprzętu dokumentacją lub odwiedzić stronę internetową konkretnego dostawcy. Rysunek 1-1 pokazuje przykładowy ekran konfiguracji UEFI dostępny na laptopie firmy Lenovo.



Rysunek 1-1 Konfiguracji funkcji Secure Boot oraz haseł uruchamiania dokonuje się z poziomu ekranu konfiguracji UEFI

Secure Boot

Funkcja bezpiecznego rozruchu Secure Boot jest funkcją interfejsu UEFI, której zadaniem jest ochrona środowiska startowego serwera. Oprogramowanie sprzętowe UEFI przechowuje bazę danych zaufanego sprzętu, sterowników, systemów operacyjnych oraz opcjonalnych pamięci ROM, przy czym struktura tej bazy definiowana jest przez producenta OEM danego serwera. Krótko mówiąc, po włączeniu tej funkcji serwer uruchomi się tylko wtedy, gdy pliki programu rozruchowego systemu operacyjnego i sterowniki urządzeń będą podpisane cyfrowo, a baza danych funkcji Secure Boot będzie mieć do nich zaufanie.

Funkcję Secure Boot można wyłączyć z poziomu ekranu konfiguracji UEFI/BIOS. Krok ten może okazać się konieczny, gdy któryś z komponentów serwera nie jest rozpoznawany przez interfejs UEFI. Istnieje również możliwość przełączenia UEFI w tryb zgodności Compatibility Support Module (CSM) umożliwiający rozruch serwera przy użyciu starego trybu BIOS, jednak stosowanie go pozbawia nas możliwości korzystania z funkcji zabezpieczeń UEFI, a tym samym podważa sens ich istnienia.

UWAGA Ochrona przed nieautoryzowanymi zmianami UEFI

Atakujący, który posiada fizyczny dostęp do Twojego serwera, jakąkolwiek programową ochronę czyni znacznie mniej efektywną. Upewnij się, że rozmieściłeś swoje serwery w obszarach zabezpieczonych przed nieuprawnionym dostępem, a najlepiej takich, które monitorowane są przy użyciu kamer. Program konfiguracyjny UEFI serwera powinien umożliwić Ci zdefiniowanie jednego lub więcej haseł, które ochronią ten system przed nieautoryzowanym rozruchem. Ponieważ ustawienia sprzętowe UEFI/BIOS podtrzymywane są przez zasilanie z baterii na płycie głównej, powinieneś także założyć fizyczną blokadę na obudowę serwera.

TPM

Moduł Trusted Platform Module (TPM) jest mikroukładem, który instalowany jest na płytach głównych serwerów i komputerów stacjonarnych bieżącej generacji. Głównym zadaniem modułu TPM jest ochrona danych związanych z bezpieczeństwem, a w szczególności kluczy szyfrujących i deszyfrujących.

Najważniejszą zaletą modułu TPM jest ścisłe powiązanie jego funkcjonalności z konkretnym sprzętem. Oznacza to, że bezpieczeństwo „wędruje" razem ze sprzętem hosta, przez co rozwiązanie to jest znacznie trudniejsze w obejściu niż jakakolwiek kontrola programowa.

Windows Server 2016 obsługuje zarówno oryginalną specyfikację TPM 1.0, jak i bieżącą generację układu TPM w wersji 1.2. Związek modułu TPM z funkcją Secure Boot może nie być dla wszystkich zrozumiały. Należy więc podkreślić, że choć z technicznego punktu widzenia moduł TPM jest w stanie zaoferować taką samą ochronę

w czasie rozruchu, jaką oferuję funkcja Secure Boot w UEFI, to jednak obydwa te systemy działają oddzielnie i bazują na oddzielnych magazynach zaufania.

WSKAZÓWKA EGZAMINACYJNA

Powinieneś zawsze pamiętać o tym, dlaczego włączane i w jakim celu wykorzystywane są funkcje zabezpieczające Secure Boot i TPM. Głównym powodem ich stosowania jest chęć zabezpieczenia się przed możliwością wstrzyknięcia nieautoryzowanego kodu rozruchowego, który może naruszyć bezpieczeństwo Twojego serwera. Choć egzaminy certyfikacyjne Microsoft wydają się kłaść większy nacisk na zrozumienie tego „dlaczego" dane funkcje są stosowane, zamiast tego „jak" one działają, to jednak na potrzeby egzaminu 70-744 musisz potrafić te funkcje skonfigurować.

Włączanie funkcji BitLocker w celu wykorzystania funkcji Secure Boot na potrzeby weryfikacji integralności platformy i danych konfiguracji rozruchu BCD

Funkcja BitLocker Drive Encryption jest podstawowym rozwiązaniem szyfrowania zawartości dysków twardych przechowujących system operacyjny lub dane. BitLocker, wraz z bazą danych konfiguracji rozruchu Boot Configuration Database (BCD), został po raz pierwszy wprowadzony w systemie Windows Vista.

BCD jest bazą danych niezależną od oprogramowania sprzętowego, która przechowuje dane konfiguracji rozruchu systemu Windows. W systemie Windows Server 2016 baza BCD zlokalizowana jest na zarezerwowanej partycji systemowej dysku rozruchowego. Partycja ta ma rozmiar 500 MB i nie jest oznaczona żadną literą.

Aby przygotować rozwiązanie BitLocker do korzystania z funkcji Secure Boot na potrzeby zweryfikowania integralności platformy i bazy danych BCD, należy włączyć ustawienie Allow Secure Boot For Integrity Validation (Zezwalaj na bezpieczny rozruch w celu zweryfikowania integralności), dostępne w ramach zasad grupy na ścieżce: Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.

Skonfigurowanie serwerów Windows Server 2016 w celu korzystania z funkcji Secure Boot na potrzeby zweryfikowania bazy danych BCD może przynieść nam zwiększoną wydajność i niezawodność, jako że niewielkie zmiany w bazie BCD mogą czasem wyzwolić funkcję odzyskiwania BitLocker Recovery, o czym powiemy sobie w dalszej części tego rozdziału.

Wdrażanie funkcji BitLocker Drive Encryption

Cztery wymienione przez nas do tej pory komponenty: (a) bezpieczeństwo fizyczne, (b) zasada najmniejszego uprzywilejowania, (c) funkcja Secure Boot oraz (d) moduł TPM składają się razem na podstawowe elementy każdego nowoczesnego serwera infrastruktury Windows Server 2016.

Teraz skupimy się na sposobie wdrażania funkcji szyfrowania dysku BitLocker Drive Encryption. Schemat wdrażania tej funkcji na komputerach serwerowych i klienckich jest bardzo podobny, jednak my, kierując się zagadnieniami egzaminu 70-744, zajmiemy się wyłącznie ochroną serwerów działających pod kontrolą systemu Windows Server 2016.

Pierwszym krokiem będzie zainstalowanie funkcji BitLocker Drive Encryption. W tym celu należy uruchomić konsolę Windows PowerShell z uprawnieniami administratora, a następnie wykonać poniższe polecenie:

```
Install-WindowsFeature -Name BitLocker -IncludeAllSubFeature
-IncludeManagementTools -Restart
```

Uwaga Inne sposoby instalacji funkcji Bitlocker

Jeśli preferujesz zarządzanie serwerami z poziomu graficznego interfejsu użytkownika, możesz również zainstalować funkcję BitLocker na komputerze lokalnym lub zdalnym z wykorzystaniem konsoli Server Manager. Jeśli natomiast w swojej pracy wykorzystujesz narzędzie wiersza poleceń Deployment Image Servicing and Management (DISM), możesz nadal z niego korzystać w ramach polecenia Enable-WindowsOptionalFeature. Jego składnia dla instalacji funkcji BitLocker jest następująca:

```
Enable-WindowsOptionalFeature -Online -FeatureName BitLocker,BitLocker-
Utilities -All
```

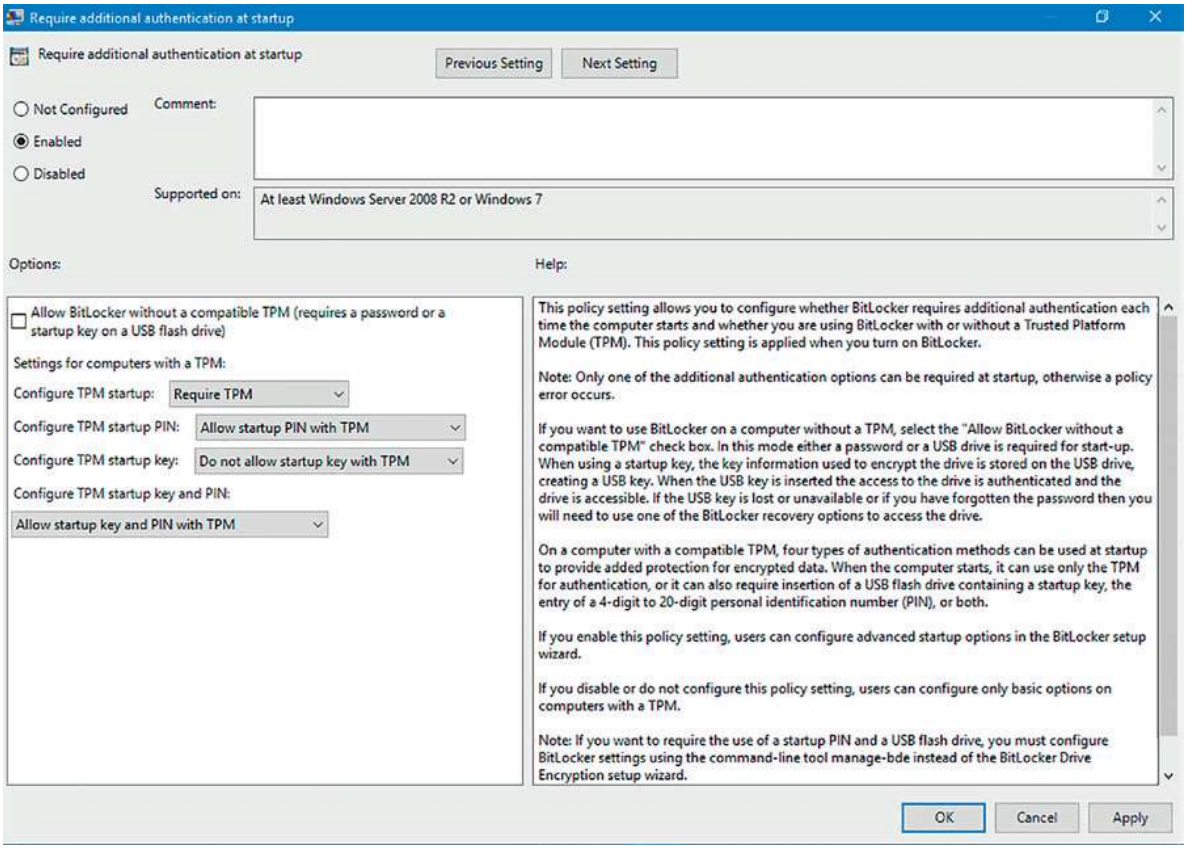
Konfiguracja funkcji BitLocker ze wsparciem i z pominięciem modułu TPM

Funkcja BitLocker Drive Encryption może zostać skonfigurowana w celu wykorzystania różnych metod uwierzytelniania nazywanych funkcjami ochrony (ang. protectors). Tabela 1-1 zawiera wykaz dostępnych opcji wraz z wyjaśnieniem ich zachowania przy uruchamianiu.

Tabela 1-1 Funkcje ochrony i ich zachowanie w trakcie uruchamiania

Konfiguracja funkcji ochrony	Zachowanie przy uruchamianiu
Brak TPM	Wymaga hasła BitLocker lub klucza uruchomienia na dysku przenośnym USB
TPM + PIN uruchomienia	Wymaga obecności modułu TPM oraz numeru PIN
TPM + klucz uruchomienia	Wymaga modułu TPM oraz klucza uruchomienia na dysku USB
TPM + pin i klucz uruchomienia	Wymaga modułu TPM, PIN-u oraz klucz uruchomienia

Jak nietrudno się domyślić, do skonfigurowania zasady szyfrowania dysku naszego serwera wykorzystujemy zasady grupy. Rozważana tu zasada nosi nazwę Require Additional Authentication At Startup (Wymagaj dodatkowego uwierzytelniania przy uruchamianiu) i zlokalizowana jest na tej samej ścieżce GPO, z której korzystaliśmy wcześniej: Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives. Zasada ta została przedstawiona na rysunku 1-2.



RYSUNEK 1-2 Konfigurowanie zasady BitLocker Drive Encryption w systemie Windows Server 2016

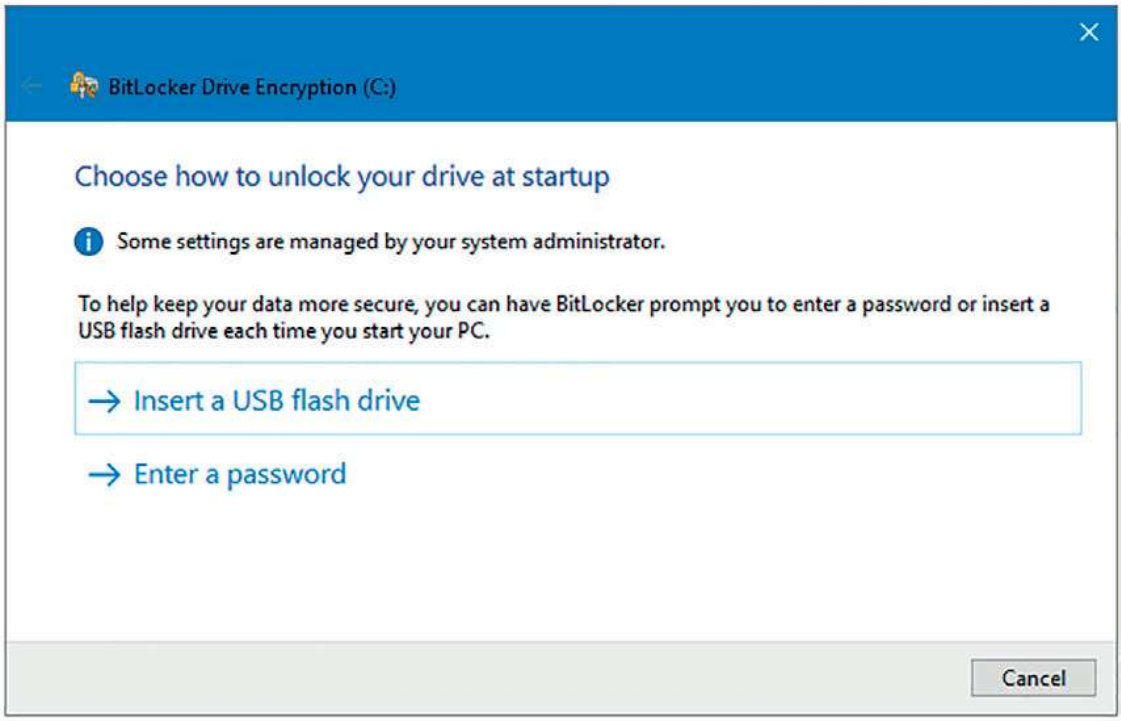
UWAGA Samodzielne działanie modułu TPM

Możliwe jest korzystanie z zabezpieczeń modułu TPM i funkcji BitLocker Drive Encryption bez żadnych dodatkowych funkcji ochrony. W takim przypadku serwer uruchamia się normalnie i na pierwszy rzut oka wydaje się nie przynosić administratorowi żadnych korzyści bezpieczeństwa. Wiesz jużjednak, że moduł TPM chroni serwer przed atakami offline poprzez weryfikowanie środowiska uruchomieniowego, o czym mówiłem wcześniej.

Choć nie jest to zalecane, system Windows Server 2016 możemy skonfigurować do korzystania z funkcji BitLocker bez ochrony oferowanej przez moduł TPM poprzez wykorzystanie ustawienia zasad grupy o nazwie Allow BitLocker Without A Compatible TPM (Requires A Password Or A Startup Key On A USB Flash Drive) (Zezwalaj na używanie funkcji BitLocker bez zgodnego modułu TPM (wymaga hasła lub klucza uruchomienia na dysku flash USB)).

Po zastosowaniu naszych ustawień zasad grupy możemy już zaszyfrować wolumin systemu operacyjnego serwera. Aby to zrobić, wykonaj poniższe kroki:

1. Otwórz Panel sterowania i uruchom element BitLocker Drive Encryption (Szyfrowanie dysków funkcją BitLocker).
2. W ramach interfejsu funkcji BitLocker Drive Encryption przejdź do części Operating System Drive (Dysk systemu operacyjnego), po czym kliknij opcję Turn On BitLocker (Włącz funkcję BitLocker).
3. W zależności od tego, w jaki sposób skonfigurowałeś zasadę funkcji BitLocker w swojej domenie, możesz mieć do dyspozycji różne opcje. Jak widać na rysunku 1-3, nasz serwer testowy oferuje nam możliwość wykorzystania klucza uruchomienia na dysku flash USB lub hasła. Wybierz opcję Enter A Password (Wprowadź hasło).



Rysunek 1-3 Wybieranie funkcji ochrony uwierzytelniania BitLocker

4. W oknie dialogowym Create A Password To Unlock This Drive (Utwórz hasło do odblokowania tego dysku) wprowadź dwukrotnie silne hasło, a następnie kliknij przycisk Next (Dalej). Silne hasło składa się z co najmniej ośmiu znaków, może

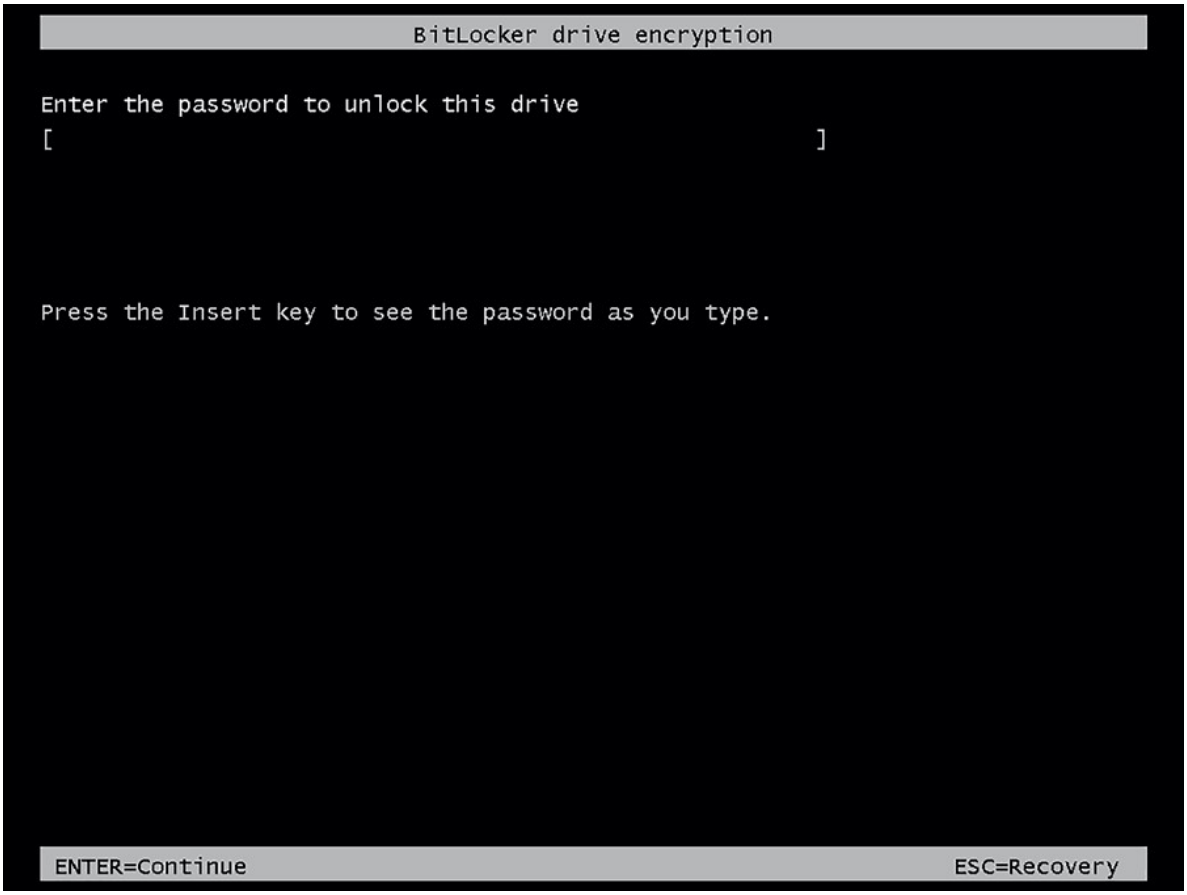
stanowić kombinację (a) małych lub dużych liter alfabetu, (b) znaków niealfanumerycznych oraz (c) cyfr, a przy tym nie występuje w żadnym słowniku żadnego języka.

5. Sporządź kopię zapasową swojego klucza odzyskiwania poprzez zapisanie go w jednej z poniższych lokalizacji:
   - **Dysk flash USB** Zwróć uwagę, że nie jest to ten sam nośnik USB, którego użyłbyś jako klucza uruchomienia.
   - **Plik** Pamiętaj o usunięciu tego pliku z systemu plików lokalnego serwera!
   - **Wydruk** Raz jeszcze, przechowuj wydrukowany klucz w bezpiecznym miejscu, z dala od powiązanego z nim serwera.
6. Zdecyduj, jaką część dysku systemu operacyjnego chcesz zaszyfrować. Co więcej, możesz (i w zasadzie powinieneś) zaszyfrować na swoim serwerze również pozostałe dyski przechowujące dane – my jednak dla uproszczenia zajmiemy się wyłącznie szyfrowaniem dysku systemu operacyjnego. Możesz zaszyfrować tylko zajęte miejsce na dysku lub też całą jego zawartość. Dla istniejącego serwera wybierz tę drugą opcję, a następnie kliknij Next.
7. Wybierz algorytm (tryb) szyfrowania, z którego chcesz skorzystać. Windows Server 2016 obsługuje następujące cztery algorytmy:
   - **AES-128** Jest to domyślny algorytm o standardowej długości szyfru.
   - **AES-256** Algorytm AES-128, ale o podwójnej długości szyfru.
   - **XTS-AES-128** Oferuje zgodność ze standardem Federal Information Processing Standard (FIPS) oraz pewne dodatkowe funkcje, jednak nie jest kompatybilny ze starszymi wersjami systemu Windows Server.
   - **XTS-AES-256** Algorytm XTS-AES-128 o podwójnej długości szyfru.

   Zwróć uwagę, że siła szyfrowania algorytmów szyfrujących jest odwrotnie proporcjonalna do wydajności tych algorytmów.

   W ramach interfejsu funkcji BitLocker Drive Encryption w Panelu sterowania musisz wybrać pomiędzy trybem New Encryption mode (Nowy tryb szyfrowania; wykorzystuje algorytm XTS-AES-128) lub trybem Compatible mode (Tryb zgodności; wykorzystuje algorytm AES-128).
8. Upewnij się, że opcja Run BitLocker system check (Uruchom test systemowy funkcji BitLocker) jest zaznaczona, po czym kliknij przycisk Continue (Kontynuuj). Po ponownym uruchomieniu systemu funkcja BitLocker Drive Encryption rozpocznie proces szyfrowania woluminu systemu operacyjnego.

Na rysunku 1-4 przedstawiono komunikat z prośbą o podanie hasła dla funkcji BitLocker Drive Encryption.



Rysunek 1-4 Przykładowy zrzut ekranu

Uwaga Inne metody szyfrowania woluminu systemu operacyjnego za pomocą funkcji BITLOCKER

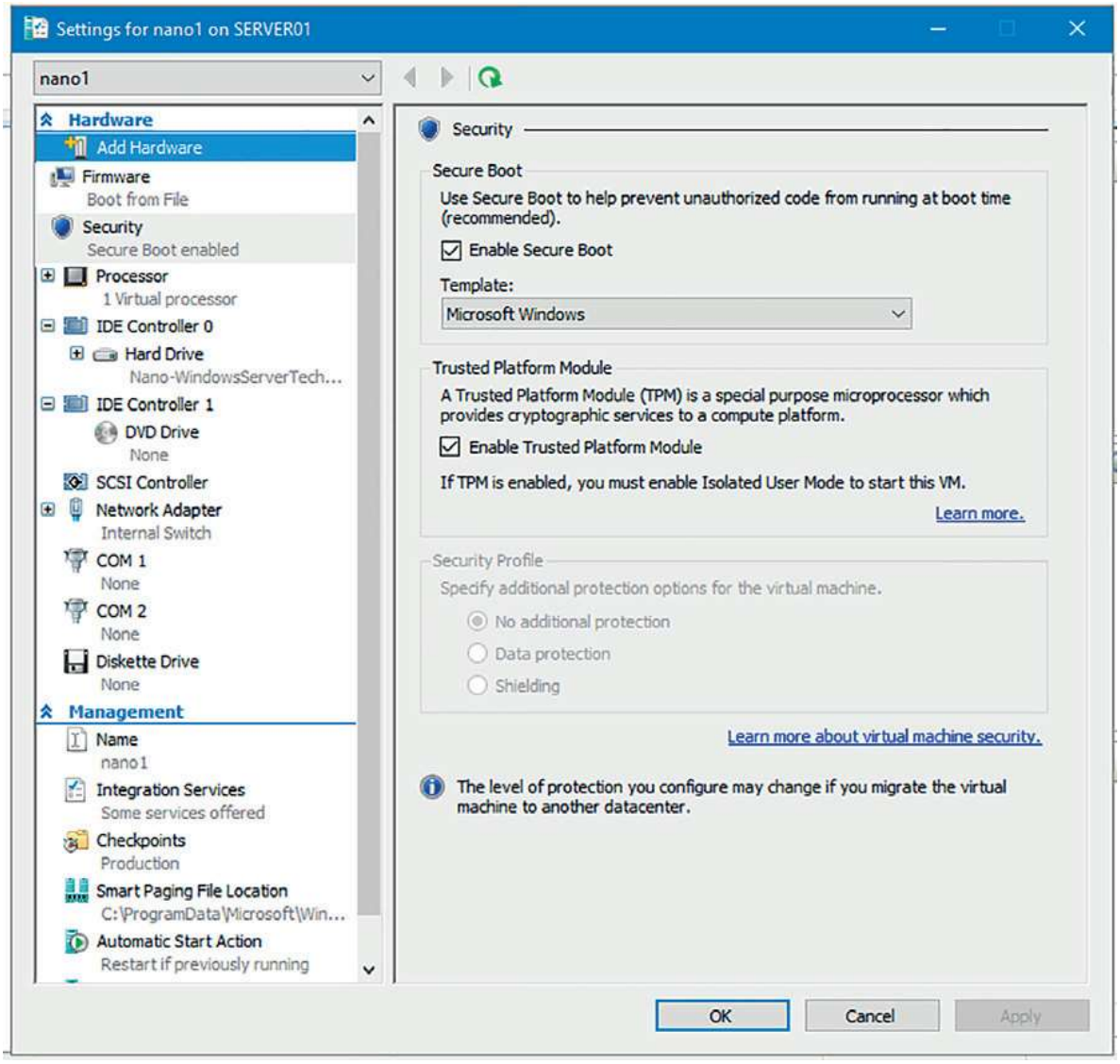
Podczas instalowania funkcji BitLocker Drive Encryption system Windows Server 2016 załaduje dla niej polecenia powłoki Windows PowerShell. Oznacza to, że od tej pory dyski lokalne i zdalne możesz szyfrować z poziomu konsoli PowerShell za pomocą polecenia Enable-BitLocker. Poniższy przykład spowoduje zaszyfrowanie dysku C z wykorzystaniem funkcji ochrony modułu TPM i PIN-u:

```
$SecureString = ConvertTo-SecureString ‘$tr0ngP@$$w0rd!!’ -AsPlainText
-Force
Enable-BitLocker -MountPoint ‘C:’ -EncryptionMethod Aes256 –UsedSpaceOnly
-Pin $SecureString -TPMandPinProtector
```

Aby zaszyfrować, zarządzać lub odszyfrować wolumin systemu operacyjnego lub danych, możesz również posłużyć się starym narzędziem wiersza poleceńo nazwie Manage-BDE.

Wdrażanie funkcji BitLocker na maszynach wirtualnych Hyper-V

Hyper-V w systemie Windows Server 2016 zezwala na korzystanie w maszynach wirtualnych zarówno z funkcji Secure Boot, jak i zwirtualizowanego modułu (vTPM). Jak widać na rysunku 1-5, możliwości te są teraz dostępne w oknie dialogowym właściwości maszyny wirtualnej Hyper-V.



Rysunek 1-5 Włączanie funkcji Secure Boot i modułu vTPM w maszynie wirtualnej Hyper-V

To oczywiście oznacza, że funkcję BitLocker Drive Encryption w lokalnych maszynach wirtualnych możemy wdrażać dokładnie tak samo, jak robimy to na sprzęcie hosta, wliczając w to również wymaganie co do modułu TPM!

Konfiguracja funkcji BitLocker na współdzielonych woluminach klastrów oraz w sieciach magazynowania SAN

Windows Server 2012 zapoczątkował możliwość stosowania funkcji BitLocker Drive Encryption na współdzielonych woluminach klastrów (ang. cluster shared volumes, CSV) bazujących na wspólnym magazynie w sieci magazynowania Storage Area Network (SAN). Funkcjonalność ta znana jest jako CSV v2. Woluminy te mogą zostać zaszyfrowane albo przed ich dodaniem do klastra, albo już po dokonaniu tej operacji. Aby wykonać to zadanie, możemy posłużyć się powłoką Windows PowerShell lub skorzystać z narzędzia Manage-BDE.

Konfiguracja funkcji odblokowywania przez sieć Network Unlock

Windows Server 2016 obsługuje wprowadzoną w systemie Windows Server 2012 funkcję odblokowywania przez sieć BitLocker Network Unlock. Funkcja Network Unlock umożliwia automatyczny dostęp do kluczy deszyfrujących BitLocker, co oznacza, że nasze serwery możemy uruchamiać, restartować, a także zdalnie nimi zarządzać (chociażby w ramach funkcji Wake on LAN) z pominięciem dodatkowych czynności wymaganych przez funkcję ochrony PIN.

Poza obecnością w serwerach oprogramowania sprzętowego UEFI i zainstalowanego w nich modułu TPM, funkcja Network Unlock do swojego wdrożenia wymaga jeszcze spełnienia kilku dodatkowych wymagań infrastruktury:

- **UEFI DHCP** Ta funkcja UEFI znana była dawniej jako Preboot Execution Environment (PXE). Krótko mówiąc, serwer po uruchomieniu może pozyskać konfigurację TCP/IP z serwera DHCP bezpośrednio od UEFI i zainstalowanej karty sieciowej.
- **Brak CSM** Tryb zgodności w oprogramowaniu UEFI naszych serwerów musi zostać całkowicie wyłączony (brak modułów Compatibility Support Modules, CSM).
- **Oddzielne serwery WDS i DHCP** Będziemy potrzebować osobnych serwerów z rolami serwera Windows Deployment Service (WDS) oraz Dynamic Host Configuration Protocol (DHCP).
- **Infrastruktura PKI** Będziemy potrzebować infrastruktury klucza publicznego (ang. public key infrastructure, PKI) do generowania cyfrowych certyfikatów X.509 wymaganych przez funkcję Network Unlock. Do tego celu w zupełności wystarczą nam usługi Active Directory Certificate Services (AD CS).
- **Ustawienia zasad grupy funkcji Network Unlock** Należy skonfigurować uprzednio wspomniane ustawienia zasad grupy w celu określenia funkcji ochrony TPM+PIN. Aby skonfigurować zasadę certyfikatów dla funkcji Network Unlock,

należy przejść do kontenera Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption Network Unlock Certificate, a następnie dodać docelowy plik certyfikatu odblokowywania przez sieć (plik .cer).

Działanie funkcji Network Unlock

Prześledzimy teraz krok po kroku sposób działania funkcji BitLocker Network Unlock.

1. Po uruchomieniu serwera menedżer rozruchu systemu Windows wykrywa obecność funkcji ochrony rozwiązania Network Unlock. Funkcja ta realizowana jest przez ustawienie zasad grupy Allow Network Unlock At Startup (Zezwalaj na odblokowywanie przez sieć podczas uruchamiania).
2. Serwer wykorzystuje swój sterownik UEFI DHCP do pozyskania poprawnego adresu IPv4 od serwera DHCP.
3. Serwer wysyła rozgłoszenie w postaci specyficznego dla dostawcy żądania DHCP, które zaszyfrowane jest certyfikatem Network Unlock serwera WDS (będącego w posiadaniu serwera lokalnego dzięki konfiguracji zasad grupy).
4. Dostawca usług WDS przetwarza to żądanie i produkuje klucz AES-256, który odblokowuje wolumin systemu operacyjnego lokalnego serwera.
5. Serwer kontynuuje proces rozruchu nie wymagając przy tym od administratora podejmowania żadnych dodatkowych czynności.

Dodatkowe materiały Zapoznanie z funkcją Network Unlock

Egzamin 70-744 wymaga jedynie opanowania podstaw funkcji BitLocker Network Unlock. Aby dowiedzieć się więcej na jej temat, prześledź artykuł „BitLocker: How to Enable Network Unlock", dostępny na stronie TechNet pod adresem *https://technet.microsoft.com/en-us/library/jj574173(v=ws.11).aspx#BKMK_NUnlockCoreReqs*.

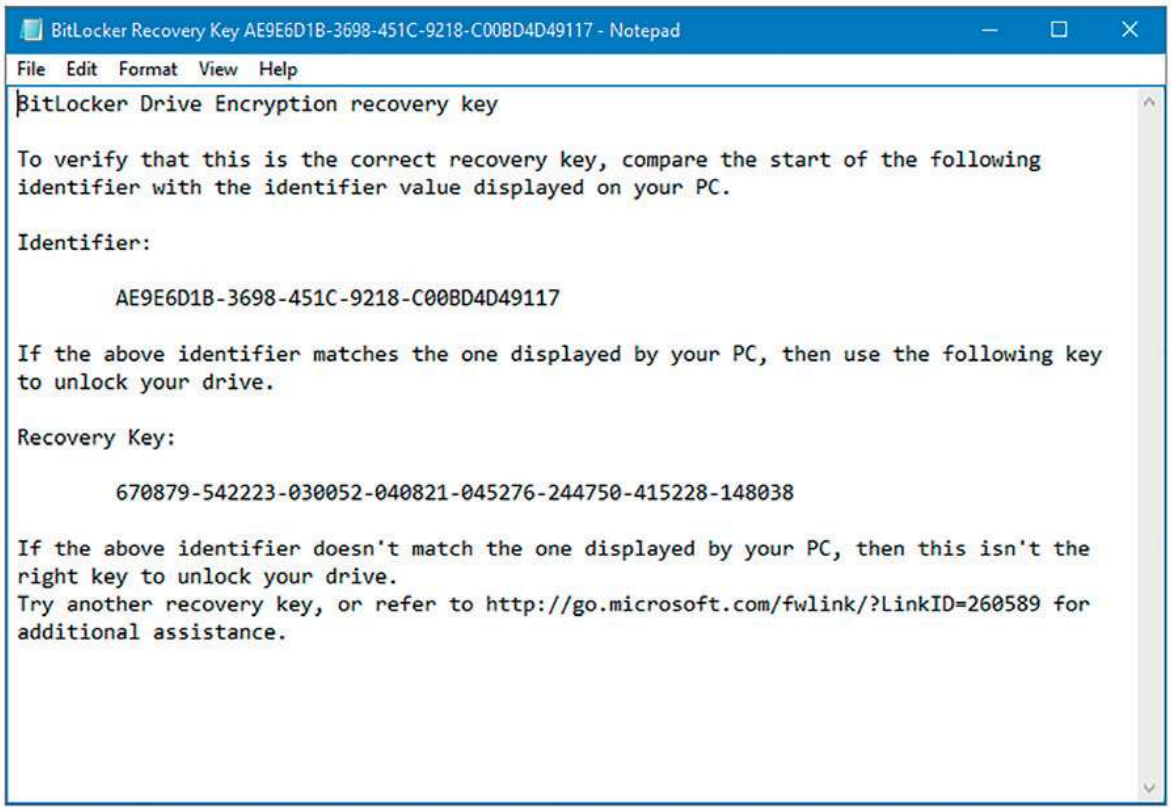
Wdrażanie procesu odzyskiwania funkcji BitLocker

Co zrobić w przypadku, gdy nie jesteśmy w stanie w normalny sposób odblokować dysku systemu operacyjnego chronionego przez funkcję BitLocker? Powodem, dla którego tak się dzieje, może być chociażby zapomnienie przez nas PIN-u lub hasła do odblokowania. Nietrudno o takie roztargnienie, zwłaszcza gdy na co dzień zarządzamy kilkoma serwerami, z których każdy ma swoje własne hasła i PIN-y.

Hasło odzyskiwania

Najbardziej oczywistym sposobem rozwiązania problemu z odblokowaniem funkcji BitLocker jest wprowadzenie 48-bitowego klucza odblokowującego, który został

wygenerowany podczas procesu szyfrowania. Spójrzmy na rysunek 1-6, który pokazuje zawartość testowego pliku klucza odzyskiwania (ang. *recovery key*).

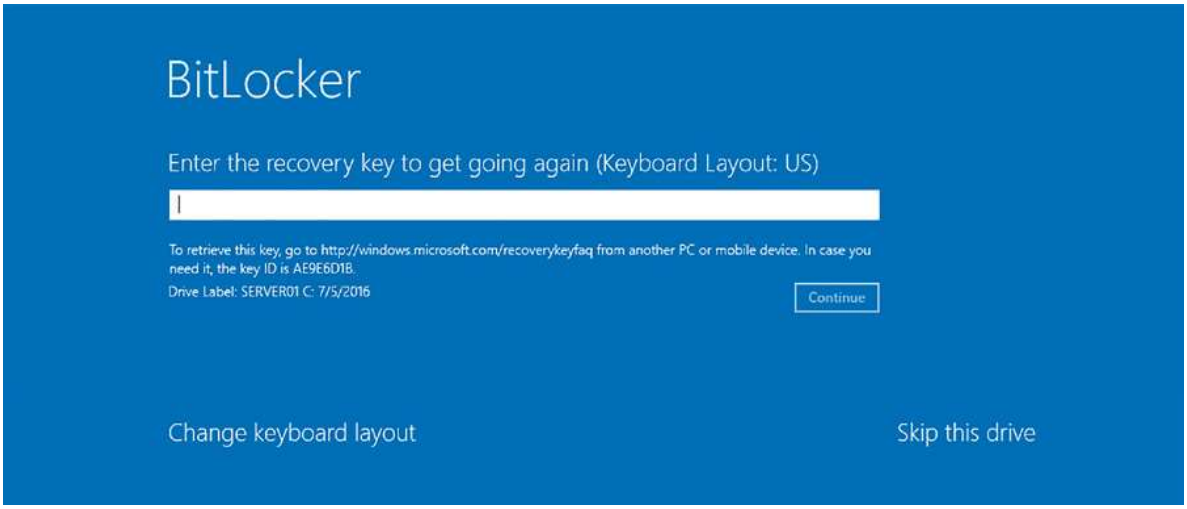


Rysunek 1-6 Przykład pliku klucza odzyskiwania dla funkcji BitLocker

Aby ręcznie przejść do trybu odzyskiwania, należy na ekranie odblokowywania BitLocker Drive Encryption wcisnąć klawisz ESC. Jak pokazano na rysunku 1-7, w tym właśnie miejscu wpisujemy klucz odzyskiwania w celu odblokowania dysku.

Uwaga Inne przyczyny aktywacji trybu odzyskiwania

Zapomnienie PIN-u lub hasła odblokowania jest tylko jednym z powodów, dla których BitLocker może przejść do trybu odzyskiwania. Zmiana kolejności rozruchu na ekranie konfiguracji UEFI/BIOS również może aktywować ten tryb. Aby się przed tym problemem uchronić, Microsoft zaleca ustawienie dysku systemowego jako pierwszego na liście urządzeń rozruchowych. Do pozostałych przyczyn aktywacji trybu odzyskiwania BitLocker należą tworzenie, usuwanie lub zmiana rozmiaru partycji, wyłączenie układu TPM, aktualizacja oprogramowania UEFI, a także instalacja lub usunięcie pewnych urządzeń sprzętowych.



Rysunek 1-7 Tryb odzyskiwania funkcji BitLocker Drive Encryption

Pozyskiwanie hasła odzyskiwania z usług AD DS

Sporządzanie kopii zapasowej hasła odzyskiwania dla funkcji BitLocker Drive Encryption i jej przechowywanie w ramach usług Active Directory Domain Services (AD DS) możliwe jest już od dawna. Na potrzeby egzaminu 70-744 musimy znać podstawy działania tego procesu.

Odpowiednie ustawienie konfiguracji znajduje się w zasadach grupy, a konkretniej na ścieżce Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption. Rozważane przez nas ustawienie zasad grupy nosi nazwę Store BitLocker recovery information in Active Directory Domain Services (Zapisuj informacje umożliwiające odzyskiwanie dla funkcji BitLocker w Usługach domenowych Active Directory).

Zasada ta daje nam wybór pomiędzy przechowywaniem w usługach AD DS samego hasła odzyskiwania BitLocker a przechowywaniem tego hasła razem z powiązanymi kluczami szyfrowania.

Będziemy także musieli aktywować zasadę Choose How BitLocker-Protected Operating System Drives Can Be Recovered (Określ, jak mogą być odzyskiwane dyski z systemem operacyjnym chronione funkcją BitLocker) dostępną w podfolderze Operating System Drives (Dyski z systemem operacyjnym) edytora Group Policy Editor. W szczególności musimy włączyć opcję Save BitLocker Recovery Information To AD DS for operating system drives (Zapisz informacje odzyskiwania funkcji BitLocker w usługach AD DS dla dysków z systemem operacyjnym).

Następnie dla wybranych serwerów należy uruchomić polecenie powłoki PowerShell o nazwie Invoke-GPUpdate. Przykładowo poniższe polecenie wymusza zdalnie aktualizację zasad grupy na każdym serwerze, który uwzględniony został w pliku `servers.txt`:

```
Invoke-GPUpdate -Computer (Get-Content -Path .\servers.txt) -Force
```

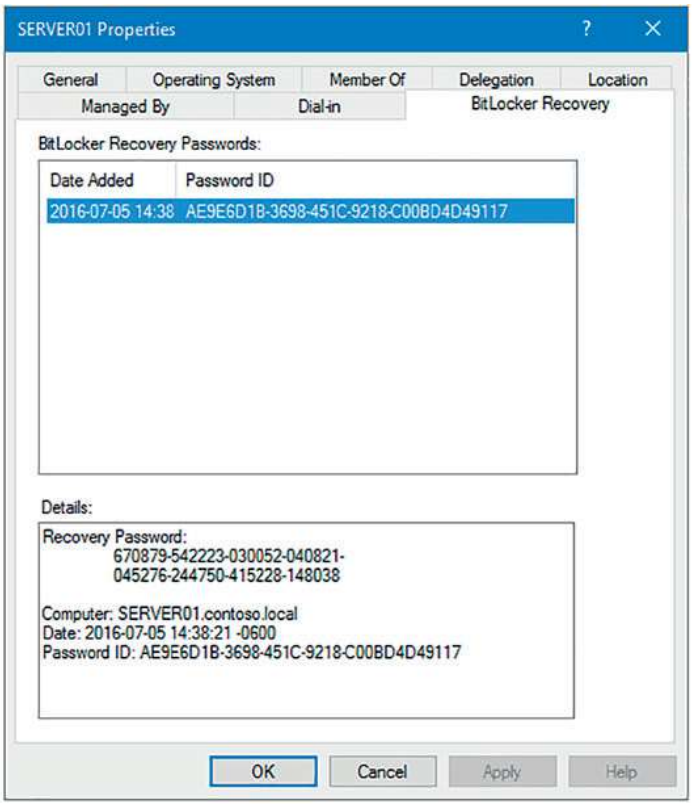
Od tej pory każdy serwer, na którym włączyliśmy funkcję BitLocker, będzie przechowywał swoje hasło odzyskiwania wraz z kluczami szyfrowania w usługach domenowych Active Directory. Jest tylko jeden haczyk: to ustawienie zasad grupy nie będzie miało wpływu na serwery, na których funkcja BitLocker jest już zainstalowana. Na takich maszynach należy najpierw uruchomić polecenie Manage-BDE w celu pozyskania numerycznego identyfikatora hasła naszego systemu:

```
manage-bde -protectors -get c:
```

a następnie wykonać poniższe polecenie wymuszające archiwizację klucza/hasła, podając mu jako argumenty odpowiednią literę dysku oraz pozyskany identyfikator hasła (należy pamiętać o nawiasach klamrowych otaczających ten identyfikator):

```
manage-bde -protectors -adbackup c: -id {password id}
```

Gdy zachodzi potrzeba uzyskania dostępu do hasła odzyskiwania, należy kolejno: otworzyć konsolę Active Directory Users and Computers, zlokalizować serwer docelowy, otworzyć okno jego właściwości, a następnie przejść na kartę BitLocker Recovery. Hasło odzyskiwania widoczne będzie jak w przykładzie na rysunku 1-8. Przy okazji, ta integracja z konsolą Active Directory Users and Computers możliwa jest dzięki narzędziu BitLocker Recovery Password Viewer (Przeglądarka haseł odzyskiwania funkcji BitLocker) dostępnego w ramach funkcji serwera BitLocker Drive Encryption.



Rysunek 1-8 Pozyskiwanie hasła odzyskiwania funkcji BitLocker z konsoli Active Directory Users and Computers

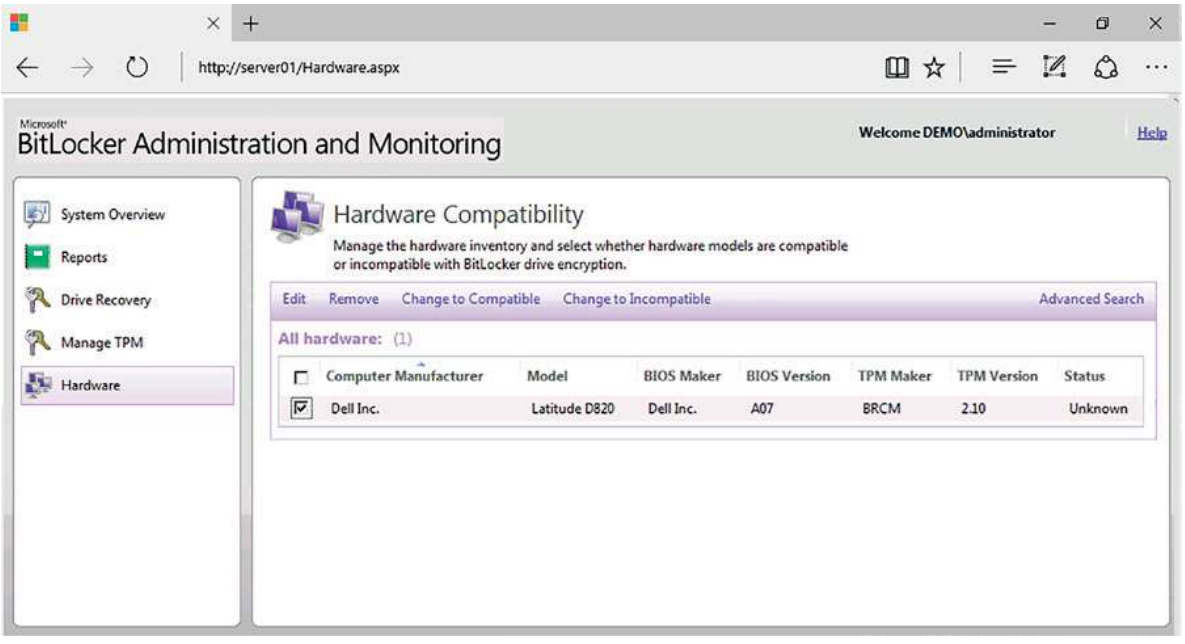
Uwaga Archiwizowanie modułu TPM w usługach AD DS

W podobny sposób Windows Server 2016 pozwala na zarchiwizowanie w usługach domenowych Active Directory Domain Services również danych modułu TPM. Aby tego dokonać, w edytorze zasad grupy należy przejść do Computer Configuration\Policies\Administrative Templates\System\Trusted Platform Module Services, a następnie włączyć zasadę Turn On TPM Backup To Active Directory Domain Services (Włącz tworzenie kopii zapasowej modułu TPM w usługach domenowych Active Directory).

Odzyskiwanie samoobsługowe

Kolejną opcją zarządzania kluczami odzyskiwania BitLocker, szczególnie przydatną w dużych przedsiębiorstwach, jest zestaw narzędzi Microsoft BitLocker Administration and Monitoring (MBAM). Narzędzia MBAM w wersji v2.5 SP1 są częścią pakietu dodatkowego Microsoft Desktop Optimization Pack (MDOP) 2015. Instalacja MBAM jest bardzo złożona, ponieważ jest to rozbudowana aplikacja wielowarstwowa, która może zostać wdrożona zarówno samodzielnie, jak i zintegrowana z programem System Center Configuration Manager 2012 R2.

Dobrą wiadomością dla administratorów systemu Windows jest to, że MBAM dostarcza pełnej automatyzacji dla funkcji BitLocker, oferując przy tym samoobsługowe pozyskiwanie kluczy, wskazówki dla użytkownika oparte na agencie, itd. Rysunek 1-9 pokazuje zrzut ekranu portalu samoobsługowego MBAM. Zwróćmy uwagę, że portal ten umożliwia nam nie tylko zarządzanie kluczami wraz z ich odzyskiwaniem, ale też monitorowanie bieżącego stanu i dokonywanie inspekcji funkcji BitLocker.



Rysunek 1-9 Samoobsługowy portal MBAM

Uwaga Pozyskiwanie narzędzi MDOP i MBAM

Niestety narzędzia MDOP nie są dostępne dla wszystkich. Można z nich korzystaćw celach rozwojowych w ramach subskrypcji Microsoft Developer Network (MSDN). W środowisku produkcyjnym korzystanie z tego oprogramowania wymaga posiadania licencji grupowej.

Zarządzanie systemem plików EFS

Szyfrowanie BitLocker Drive Encryption funkcjonuje na poziomie woluminów. Prawdą jest, że funkcji BitLocker możemy używać do szyfrowania nośników wymiennych, jednak w większości serwerów produkcyjnych szyfrować będziemy pełne woluminy dysków twardych.

BitLocker umożliwia nam również tworzenie zaszyfrowanych plików kontenera, jednak te traktowane są przez system Windows Server 2016 jako obrazy wirtualnych dysków twardych (ang. virtual hard disk, VHD).

System plików Encrypting File System (EFS) stanowi bardziej szczegółowe rozwiązanie szyfrowania danych, dzięki któremu możemy chronić poszczególne foldery i pliki.

Agenci odzyskiwania danych

Domyślnie EFS generuje certyfikaty z podpisem własnym i przechowuje je w folderach profilów każdego użytkownika lub administratora. W środowisku produkcyjnym nie jest to dobre rozwiązanie, ponieważ

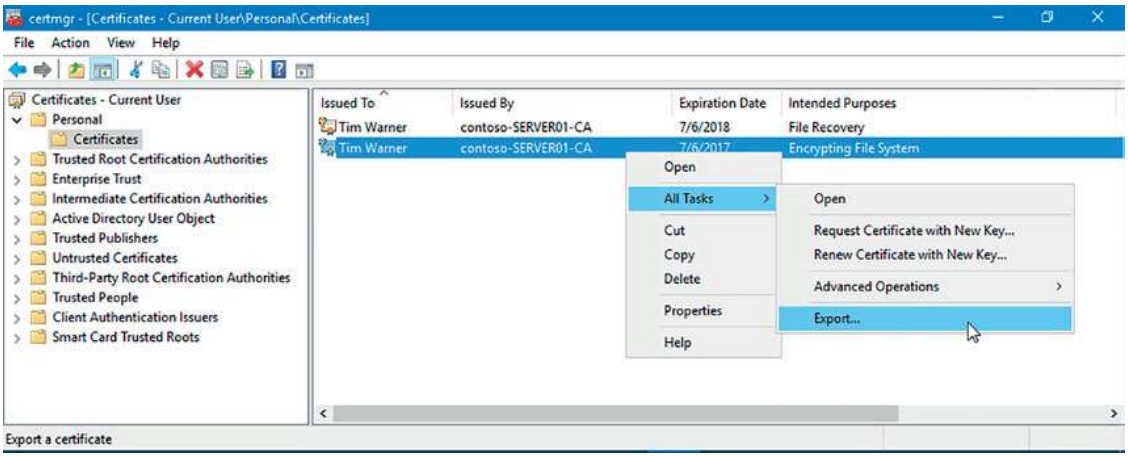
- klucze szyfrujące EFS mogą zostać uszkodzone lub skradzione
- w przypadku certyfikatów z podpisem własnym nie mamy do czynienia z łańcuchem zaufania

Z tego względu, jeśli planujemy wdrożenie systemu plików EFS w naszym przedsiębiorstwie, powinniśmy dysponować prawdziwą infrastrukturą klucza publicznego (PKI), najlepiej opartą na usługach Active Directory Certificate Services (AD CS), dzięki czemu będziemy mogli w pełni zarządzać certyfikatami EFS. W końcu usługi AD CS zawierają już szablony certyfikatów Basic EFS (Podstawowy EFS) i EFS Recovery Agent (Agent odzyskiwania EFS).

Agent odzyskiwania danych (ang. data recovery agent, DRA) jest uprzywilejowanym kontem użytkownika, które może odszyfrowywać certyfikaty EFS innych użytkowników domeny. Domyślnie agentem odzyskiwania danych jest konto Administrator, ale agentem tym możemy bez przeszkód uczynić jakiekolwiek inne konto administratora.

Aby bieżącego administratora uczynić nowym agentem odzyskiwania danych w domenie Active Directory opartej na Windows Server 2016, która zawiera główny urząd certyfikacji, wykonaj poniższe kroki:

1. Zażądaj certyfikatu EFS Recovery Agent od swojego urzędu certyfikacji AD CS. W przystawce Certificates (Certyfikaty) dla konsoli Microsoft Management Console (MMC) można to zrealizować poprzez kliknięcie prawym przyciskiem magazynu certyfikatów Personal (Osobisty) i wybranie opcji All Tasks (Wszystkie zadania) | Request New Certificate (Żądaj nowego certyfikatu).
2. Z poziomu przystawki Certificates można w łatwy sposób wykonać kopię zapasową certyfikatu EFS, BitLocker lub jakiegokolwiek innego certyfikatu cyfrowego. W tym celu należy kliknąć certyfikat prawym przyciskiem i wybrać opcję All Tasks | Export (Eksportuj). Aby przywrócić certyfikat przy użyciu jego kopii zapasowej, należy kliknąć prawym przyciskiem magazyn Personal, a następnie wybrać opcję All Tasks | Import (Importuj). Czynności te zostały przedstawione na rysunku 1-10. Zwróć uwagę, że w przykładzie tym konto użytkownika dysponuje certyfikatami Basic EFS i EFS Recovery Agent. Jest to bardzo ważne.



Rysunek 1-10 Zarządzanie certyfikatami EFS

3. Aby przypisać agenta odzyskiwania danych na poziomie domeny, otwórz odpowiedni obiekt zasad grupy i przejdź do ścieżki Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies. Zobaczysz tam dwa podfoldery: Encryption File System (System szyfrowania plików) oraz BitLocker Drive Encryption (Szyfrowanie dysków funkcją BitLocker). W tym miejscu będziesz mógł nominować agentów odzyskiwania danych dla obu tych technologii.
4. Kliknij prawym przyciskiem folder zasady Encryption File System i wybierz z menu kontekstowego opcję Add Data Recovery Agent (Dodaj agenta odzyskiwania danych). W kreatorze Add Recovery Agent (Kreator dodawania agenta odzyskiwania) będziesz mieć dwie możliwości lokalizowania odpowiednich użytkowników:
   - **Browse Directory (Przeglądaj katalog)** Pozwala zlokalizować użytkownika poprzez wyszukanie go bezpośrednio w katalogu Active Directory. Aby skorzystać z tej opcji, certyfikat musi zostać opublikowany w usłudze Active Directory.

- **Browse Folders (Przeglądaj foldery)** Pozwala zlokalizować wyeksportowany certyfikat EFS Recovery Agent w lokalnym lub zdalnym systemie plików.

5. Po odświeżeniu zasad grupy wskazani przez Ciebie agenci odzyskiwania danych będą mieć nadane przywileje pozwalające im deszyfrować zaszyfrowane pliki wszystkich użytkowników w domenie. Przydaje się to podczas awaryjnego uzyskiwania dostępu do danych w przypadku chociażby uszkodzenia profilu użytkownika, zagubienia certyfikatów, zwolnienia pracownika, itd.

Zagadnienie 1.2: Wdrażanie rozwiązań do instalowania poprawek i aktualizowania serwerów

Kolejnym zagadnieniem na naszej liście jest instalowanie poprawek i aktualizacja serwerów. Jest to temat, który u najbardziej doświadczonych administratorów Windows powoduje zazwyczaj głębokie westchnienie. W końcu komu z nas nie zdarzyło się, że wdrażana na serwer aktualizacja zamiast go wzmocnić tylko upośledziła działające na nim usługi?

Do podstawowych zasad bezpieczeństwa IT należy upewnienie się, że wszystkie serwery infrastruktury są zawsze zaktualizowane pod kątem znanych exploitów i zagrożeń Za pomocą usługi Windows Server Update Services (WSUS) będziemy mogli osiągnąć ten cel z dużo mniejszą ilością błędów.

Na potrzeby egzaminu 70-744 musimy dobrze poznać zasadę działania oraz sposób wykorzystania usług WSUS w celu ochrony naszych serwerów Windows Server 2016, redukując przy tym do minimum prawdopodobieństwo wystąpienia awarii jakiejś usługi po aktualizacji.

W tej części rozdziału omówione zostaną następujące zadania:

- Instalacja i konfiguracja usług WSUS
- Tworzenie grup komputerów i konfigurowanie aktualizacji automatycznych
- Zarządzanie aktualizacjami za pomocą usług WSUS
- Konfiguracja raportowania WSUS
- Rozwiązywanie problemów z konfiguracją i wdrożeniem WSUS

Większość administratorów systemu Windows wie, że Microsoft wydaje poprawki bezpieczeństwa i aktualizacje oprogramowania w drugi wtorek każdego miesiąca. Wydarzenie to znane jest nieformalnie jako „Patch Tuesday". Oczywiście gdy Microsoft adresuje exploity typu zero-day, poprawki te traktowane i wydawane są priorytetowo.