Instrukcja obsługi

HP Sure Recover

Wydanie pierwsze: luty 2020

Numer katalogowy dokumentu: L93434-241

Objaśnienie składni poleceń wprowadzanych przez użytkownika

Tekst, który trzeba wprowadzić do interfejsu użytkownika, jest oznaczony `czcionką o stałej szerokości`.

Tabela -1 Objaśnienie składni poleceń wprowadzanych przez użytkownika

Element	Opis
`Tekst bez nawiasów`	Elementy, które trzeba wprowadzić dokładnie tak, jak są pokazane
`<Tekst wewnątrz nawiasów kątowych>`	Miejsce zarezerwowane na wartość do wprowadzenia; pomiń nawiasy
`[Tekst wewnątrz nawiasów kwadratowych]`	Elementy opcjonalne; pomiń nawiasy
`{Tekst wewnątrz nawiasów klamrowych}`	Zbiór elementów, z których trzeba wybrać tylko jeden; pomiń nawiasy
`|`	Separator elementów, z których trzeba wybrać tylko jeden; pomiń kreskę pionową
`...`	Elementy, które można lub trzeba powtórzyć; pomiń wielokropek

Spis treści

1 Rozpoczęcie pracy

Oprogramowanie HP Sure Recover pomaga bezpiecznie zainstalować system operacyjny z sieci przy minimalnym udziale użytkownika. Systemy z oprogramowaniem HP Sure Recover z funkcją Embedded Reimaging obsługują również instalację z lokalnego urządzenia pamięci masowej.

WAŻNE: Przed skorzystaniem z oprogramowania HP Sure Recover należy wykonać kopię zapasową danych. Proces przetwarzania obrazu sformatuje dysk, co spowoduje utratę danych.

Obrazy odzyskiwania dostarczane przez firmę HP zawierają podstawowy instalator systemu Windows 10®. Opcjonalnie oprogramowanie HP Sure Recover może zainstalować zoptymalizowane sterowniki do urządzeń HP. Obrazy odzyskiwania HP zawierają tylko agenty odzyskiwania danych dostarczane z systemem Windows 10, takie jak usługa OneDrive. Korporacje mogą tworzyć własne niestandardowe obrazy w celu dodania ustawień firmowych, aplikacji, sterowników i agentów odzyskiwania danych.

Agent odzyskiwania systemu operacyjnego wykonuje czynności niezbędne do zainstalowania obrazu odzyskiwania. Agent odzyskiwania dostarczony przez firmę HP wykonuje typowe czynności, takie jak partycjonowanie, formatowanie i wyodrębnianie obrazu odzyskiwania do urządzenia docelowego. Ze względu na to, że agent odzyskiwania HP jest dostępny w witrynie hp.com, potrzebny jest dostęp do Internetu, chyba że system jest wyposażony w wbudowaną funkcję tworzenia obrazów. Korporacje mogą również udostępniać agenta odzyskiwania HP wewnątrz zapory lub tworzyć niestandardowe agenty odzyskiwania w przypadku bardziej skomplikowanych środowisk odzyskiwania.

Oprogramowanie HP Sure Recover można uruchomić w przypadku braku systemu operacyjnego. Oprogramowanie HP Sure Recover można również uruchamiać zgodnie z harmonogramem, na przykład w celu upewnienia się, że złośliwe oprogramowanie zostało usunięte. Te ustawienia można konfigurować przy użyciu narzędzia HP Client Security Manager (CSM), zestawu Manageability Integration Kit (MIK) lub biblioteki HP Client Management Script Library.

Wykonywanie odzyskiwania sieciowego

UWAGA: W celu wykonania odzyskiwania sieciowego należy użyć połączenia przewodowego. Firma HP zaleca utworzenie kopii zapasowej ważnych plików, danych, zdjęć, filmów itd. przed skorzystaniem z oprogramowania HP Sure Recover, aby zapobiec utracie danych.

1. Komputer kliencki należy podłączyć do sieci, w której dostępny jest punkt dystrybucji HTTP lub FTP.
2. Uruchom ponownie komputer kliencki, a gdy zostanie wyświetlone logo HP, naciśnij klawisz f11.
3. Wybierz opcję **Restore from network** (Odzyskaj z sieci).

Wykonywanie odzyskiwania z dysku lokalnego

Jeśli komputer kliencki obsługuje wbudowane tworzenie obrazów, a w zastosowanych zasadach włączono opcję pobierania obrazu zgodnie z harmonogramem, obraz zostanie pobrany do komputera klienckiego o zaplanowanej godzinie. Po pobraniu obrazu do komputera klienckiego uruchom go ponownie, aby skopiować obraz do urządzenia pamięci masowej funkcji Embedded Reimaging.

Aby wykonać odzyskiwanie lokalne za pomocą obrazu na urządzeniu pamięci masowej funkcji Embedded Reimaging:

1. Uruchom ponownie komputer kliencki, a gdy zostanie wyświetlone logo HP, naciśnij klawisz f11.
2. Wybierz opcję **Restore from local drive** (Przywróć z dysku lokalnego).

Na komputerach z funkcją Embedded Reimaging należy skonfigurować harmonogram pobierania i użyć agenta pobierania w celu sprawdzania aktualizacji. Agent pobierania jest dostarczany z dodatkiem HP Sure Recover Plug-in do narzędzia HP Client Security Manager i można go również skonfigurować w zestawie MIK. Instrukcje dotyczące korzystania z zestawu MIK można znaleźć na stronie https://www.hp.com/go/clientmanagement.

Można również utworzyć zaplanowane zadanie, aby skopiować agenta do partycji SR_AED i obraz do partycji SR_IMAGE. Następnie przy użyciu biblioteki HP Client Management Script Library można wysłać zdarzenie usługi informujące system BIOS o konieczności weryfikacji zawartości i wykonania kopii na urządzeniu pamięci masowej funkcji Embedded Reimaging podczas kolejnego ponownego uruchomienia.

2 Tworzenie obrazu firmowego

Większość firm używa narzędzia Microsoft Deployment Tools , zestawu Windows 10 Assessment and Deployment lub obu tych rozwiązań w celu tworzenia plików zawierających obraz w formacie pliku archiwum Windows Imaging (WIM).

Wymagania

- Najnowsza wersja zestawu Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (lub inne rozwiązanie do tworzenia pary kluczy prywatnych/publicznych RSA)

  Służy do generowania pary kluczy RSA używanej do zabezpieczenia integralności tworzonego i udostępnianego obrazu firmowego.
- Serwerowe rozwiązanie hostingowe (takie jak Microsoft Internet Information Services [IIS])

Tworzenie obrazu

Przed rozpoczęciem procesu tworzenia obrazu skonfiguruj działający system lub zbuduj system z zainstalowanymi wymaganymi narzędziami do przetwarzania obrazu, zgodnie z poniższymi instrukcjami:

1. Jako Administrator otwórz wiersz polecenia środowiska `Deployment and Imaging Tools Environment` (zainstalowanego z narzędziami do wdrażania z zestawu ADK dla systemu Windows).
2. Utwórz obszar tymczasowy dla obrazu przy użyciu następującego polecenia:

   ```
   mkdir C:\staging
   ```
3. Utwórz obraz przy użyciu jednego z następujących przykładów:

   Przykład 1: Tworzenie obrazu w oparciu o obraz instalacyjny systemu Microsoft Windows na stronie 3

   Przykład 2: Tworzenie obrazu na podstawie systemu odniesienia na stronie 5

Przykład 1: Tworzenie obrazu w oparciu o obraz instalacyjny systemu Microsoft Windows

1. Zamontuj lub otwórz obraz instalacyjny systemu Microsoft Windows (z pliku ISO firmy Microsoft lub HP OSDVD).
2. Z zamontowanego obrazu instalacyjnego systemu Windows skopiuj plik install.wim do obszaru tymczasowego przy użyciu następującego polecenia:

   ```
   robocopy <M:>\sources C:\staging install.wim
   ```

   UWAGA: Litera `<M:>` oznacza zamontowany napęd. Zastąp ją prawidłową literą napędu.
3. Zmień nazwę pliku install.wim na nazwę pliku obrazu („my-image” w tym przykładzie) przy użyciu następującego polecenia:

   ```
   ren C:\staging\install.wim <my-image>.wim
   ```

(Opcjonalnie) Oprogramowanie HP Sure Recover obejmuje funkcję odzyskiwania określonej wersji z obrazu wieloindeksowego opartego na wersji systemu Windows, dla której pierwotnie uzyskano licencję dla systemu docelowego HP w fabryce. Ten mechanizm działa, jeśli indeksy są nazwane prawidłowo. Jeśli obraz instalacji systemu Windows pochodzi z obrazu HP OSDVD, prawdopodobnie masz obraz zawierający wiele wersji. Jeśli to zachowanie jest niepożądane i chcesz mieć pewność, że jedna konkretna wersja jest używana we wszystkich systemach docelowych, upewnij się, że obraz instalacyjny zawiera tylko jeden indeks.

4. Sprawdź zawartość obrazu instalacyjnego za pomocą następującego polecenia:

```
dism /Get-ImageInfo /ImageFile:C:\staging\<my-image>.wim
```

Poniżej przedstawiono przykładowe dane wyjściowe z obrazu instalacyjnego obsługującego pięć wersji (do dopasowania na podstawie systemu BIOS poszczególnych systemów docelowych):

Szczegóły obrazu: `my-image.wim`

Indeks: `1`

Nazwa: `CoreSingleLanguage`

Opis: `Windows 10 May 2019 Update - Home Single Language Edition`

Rozmiar: `19,512,500,682 bytes`

Indeks: `2`

Nazwa: `Core`

Opis: `Windows 10 May 2019 Update - Home edition`

Rozmiar: `19,512,500,682 bytes`

Indeks: `3`

Nazwa: `Professional`

Opis: `Windows 10 May 2019 Update- Professional Update`

Rozmiar: `19.758,019,520 bytes`

Indeks: `4`

Nazwa: `ProfessionalEducation`

Opis: `Windows 10 May 2019 Update - Professional Education edition`

Rozmiar: `19,758,019,480 bytes`

Indeks: `5`

Nazwa: `ProfessionalWorkstation`

Opis: `Windows 10 May 2019 Update - Professional Workstation edition`

Rozmiar: `19,758,023,576 bytes`

UWAGA: Jeśli istnieje tylko jeden indeks, obraz jest używany do odzyskiwania niezależnie od jego nazwy. Rozmiar pliku obrazu może być większy niż przed usunięciem.

5. Jeśli zachowanie związane z dostępnością wielu wersji jest niepożądane, usuń poszczególne niepotrzebne indeksy.

   Jak pokazano na poniższym przykładzie, jeśli potrzebna jest tylko wersja Professional (przy założeniu posiadania licencji dla wszystkich systemów docelowych), usuń indeksy 5, 4, 2 i 1. Za każdym razem, gdy usuwany jest indeks, numery indeksu są ponownie przypisywane. Dlatego należy usuwać numery indeksu w kolejności od najwyższego do najniższego. Uruchom polecenie `Get-ImageInfo` po każdym usunięciu, aby wizualnie potwierdzić, który indeks ma zostać usunięty w następnej kolejności.

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:5
   ```

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:4
   ```

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:2
   ```

   ```
   dism /Delete-Image /ImageFile:C:\staging\my-image.wim /Index:1
   ```

   Wybierz tylko jeden indeks wersji (na przykład Professional). Jeśli istnieje tylko jeden indeks, obraz jest używany do odzyskiwania niezależnie od jego nazwy. Należy pamiętać, że rozmiar pliku obrazu może być większy niż przed usunięciem, ze względu na sposób modyfikacji metadanych WIM i normalizacji zawartości.

6. (Opcjonalnie) Aby dołączyć sterowniki do firmowego obrazu odzyskiwania, wykonaj następujące czynności:

   a. Zamontuj obraz w pustym folderze przy użyciu następujących poleceń:

   ```
   mkdir C:\staging\mount
   ```

   ```
   dism /Mount-Wim /WimFile:C:\staging\my-image.wim /MountDir:C:
   \staging\mount /Index:1
   ```

   b. Zamontuj odpowiedni obraz HP Windows 10 Driver DVD (DRDVD) dla obsługiwanego systemu docelowego. Z zamontowanego nośnika ze sterownikami skopiuj podfoldery sterowników do obszaru tymczasowego za pomocą następującego polecenia:

   ```
   robocopy /E <M:>\SWSETUP\DRV C:\staging\mount\SWSETUP\DRV
   ```

   UWAGA: Litera `<M:>` oznacza zamontowany napęd. Zastąp ją prawidłową literą napędu.

   Możesz dołączyć dodatkowe sterowniki w plikach .inf, umieszczając je w folderze C:\staging\mount \SWSETUP\DRV. Aby dowiedzieć się, w jaki sposób ta zawartość jest przetwarzana przez oprogramowanie HP Sure Recover przy użyciu funkcji `dism /Add-Driver /Recurse`, zobacz punkt „Dodawanie sterowników do obrazu offline systemu Windows i usuwanie ich” w następującym temacie: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Ta funkcja nie obsługuje sterowników w plikach .exe, które wymagają uruchomienia aplikacji.

   c. Zapisz zmiany i odmontuj obraz przy użyciu następującego polecenia:

   ```
   dism /Unmount-Wim /MountDir:C:\staging\mount /Commit
   ```

   Wynikowy plik obrazu to: C:\staging\my-image.wim.

   d. Przejdź na stronę Dzielenie obrazu na stronie 6.

Przykład 2: Tworzenie obrazu na podstawie systemu odniesienia

1. Utwórz rozruchowy nośnik USB środowiska WinPE.

UWAGA: Informacje na temat dodatkowych sposobów przechwytywania obrazu zawiera dokumentacja zestawu ADK.

Upewnij się, że na urządzeniu USB jest wystarczająca ilość wolnego miejsca do zapisania przechwyconego obrazu systemu odniesienia.

2. Utwórz obraz w systemie odniesienia.
3. Przechwyć obraz, uruchamiając system odniesienia przy użyciu nośnika USB środowiska WinPE, a następnie użyj narzędzia DISM.

UWAGA: Litera `<U:>` oznacza napęd USB. Zastąp ją prawidłową literą napędu.

Edytuj część nazwy pliku „my-image” i opis `<my-image>` zależnie od potrzeb.

```
dism /Capture-Image /ImageFile:<U:><\my-image>.wim /CaptureDir:C:\ /
Name:<My Image>
```

4. Skopiuj obraz z urządzenia USB do obszaru tymczasowego w systemie roboczym przy użyciu następującego polecenia:

```
robocopy <U:>\ C:\staging <my-image>.wim
```

Powinien istnieć następujący plik obrazu: C:\staging\my-image.wim.

5. Przejdź na stronę Dzielenie obrazu na stronie 6.

Dzielenie obrazu

Firma HP zaleca dzielenie obrazu na mniejsze pliki w celu zwiększenia niezawodności pobierania przez sieć przy użyciu następującego polecenia:

```
dism /Split-Image /ImageFile:C:\staging\<my-image>.wim /SwmFile:C:\staging
\<my-image>.swm /FileSize:64
```

UWAGA: Wartość FileSize jest wyświetlana w megabajtach. Edytuj je w razie potrzeby.

UWAGA: Ze względu na sposób działania algorytmu dzielenia narzędzia DISM rozmiary wygenerowanych plików SWM mogą być mniejsze lub większe niż deklarowany rozmiar pliku.

Tworzenie manifestu

Pliki manifestu należy tworzyć w formacie UTF-8 bez BOM (Byte Order Mark).

Można zmienić nazwę pliku manifestu (custom.mft) użytą w poniższych procedurach, ale nie należy zmieniać rozszerzeń .mft i .sig, a nazwy plików manifestu i podpisu muszą być zgodne. Na przykład można zmienić parę (custom.mft, custom.sig) na (myimage.mft, myimage.sig).

Właściwość `mft_version` służy do określania formatu pliku obrazu i obecnie musi mieć wartość 1.

Właściwość `image_version` jest używana w celu określenia, czy dostępna jest nowsza wersja obrazu, oraz w celu zapobiegnięcia instalacji starszych wersji.

Obie wartości muszą być 16-bitowymi liczbami całkowitymi bez podpisu, a separatorem wierszy w manifeście musi być „`\r\n`” `(CR + LF)`.

Generowanie manifestu

Podzielony obraz może obejmować kilka plików, dlatego należy wygenerować manifest za pomocą skryptu programu PowerShell.

Wszystkie pozostałe czynności należy wykonywać w folderze C:\staging.

```
CD /D C:\staging
```

1. Utwórz skrypt programu PowerShell za pomocą edytora, który może wygenerować plik tekstowy w formacie UTF-8 bez BOM, używając następującego polecenia: `notepad C:\staging\generate-manifest.ps1`

   Utwórz następujący skrypt:

   ```
   $mftFilename = "custom.mft"
   ```

   `$imageVersion = 1907` (Uwaga: Może to być 16-bitowa liczba całkowita).

   ```
   $header = "mft_version=1, image_version=$imageVersion"
   Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header
   $swmFiles = Get-ChildItem "." -Filter "*.swm"
   $ToNatural = { [regex]::Replace($_, '\d*\....$',
   { $args[0].Value.PadLeft(50) }) }

   $pathToManifest = (Resolve-Path ".").Path

   $total = $swmFiles.count
   $current = 1

   $swmFiles | Sort-Object $ToNatural | ForEach-Object {
       Write-Progress
           -Activity "Generating manifest" `
           -Status "$current of $total ($_)" `
           -PercentComplete ($current / $total * 100)

       $hashObject = Get-FileHash -Algorithm SHA256 -Path $_.FullName
       $fileHash = $hashObject.Hash.ToLower()
       $filePath = $hashObject.Path.Replace($pathToManifest + '\', '')
       $fileSize = (Get-Item $_.FullName).length
       $manifestContent = "$fileHash $filePath $fileSize"
   ```

```
    Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
$manifestContent -Append

    $current = $current + 1

}
```

UWAGA: Manifesty dla oprogramowania HP Sure Recover nie mogą zawierać BOM, dlatego poniższe polecenia zapisują ponownie plik w formacie UTF8 bez BOM.

```
$content = Get-Content $mftFilename

$encoding = New-Object System.Text.UTF8Encoding $False

[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename,
$content, $encoding)
```

2. Zapisz skrypt.
3. Uruchom skrypt.

```
powershell .\generate-manifest.ps1
```

Generowanie podpisu manifestu

Oprogramowanie Sure Recover weryfikuje agenta i obraz przy użyciu podpisów kryptograficznych. W poniższych przykładach użyto pary kluczy prywatnego/publicznego w formacie PEM X.509 (rozszerzenie .PEM). Dostosuj odpowiednio polecenia, aby użyć plików binarnych certyfikatów DER (rozszerzenie .CER lub .CRT), certyfikatów PEM z szyfrowaniem BASE-64 (rozszerzenie .CER lub .CRT) lub plików PEM PKCS1 (rozszerzenie .PEM). W tym przykładzie używane jest również narzędzie OpenSSL, które generuje podpisy w formacie big-endian. Do podpisywania manifestów można użyć dowolnego narzędzia, ale niektóre wersje systemu BIOS obsługują tylko podpisy w formacie little-endian.

1. Wygeneruj 2048-bitowy klucz prywatny RSA przy użyciu następującego polecenia. Jeśli masz parę 2048-bitowych kluczy RSA prywatnych/publicznych w formacie pem, skopiuj je do folderu C:\staging, a następnie przejdź do kroku 3.

   ```
   openssl genrsa -out my-recovery-private.pem 2048
   ```

2. Wygeneruj klucz publiczny z klucza prywatnego (jeśli masz klucz publiczny odpowiadający Twojemu kluczowi prywatnemu w formacie PEM, skopiuj go do folderu C:\staging), używając następującego polecenia:

   ```
   openssl rsa -in my-recovery-private.pem -pubout -out my-recovery-
   public.pem
   ```

3. Utwórz plik podpisu (przy użyciu wartości skrótu sha256) w oparciu o 2048-bitowy klucz prywatny RSA z kroku 1 przy użyciu następującego polecenia:

   ```
   openssl dgst -sha256 -sign my-recovery-private.pem -out custom.sig
   custom.mft
   ```

4. Sprawdź plik podpisu, korzystając z klucza publicznego w poprzednim kroku, przy użyciu następującego polecenia:

   ```
   openssl dgst -sha256 -verify my-recovery-public.pem -signature
   custom.sig custom.mft
   ```

UWAGA:

- Jeśli chcesz tylko utworzyć plik podpisu, wymagane są kroki 1 i 3.
- W przypadku oprogramowania HP Sure Recover minimalne wymagane kroki to 1, 2 i 3. Do zainicjowania systemu docelowego potrzebny jest klucz publiczny z kroku 2.
- Krok 4 jest opcjonalny, ale zaleca się, aby plik sygnatury i plik manifestu zostały prawidłowo zweryfikowane.

Hosting plików

Na serwerze należy udostępnić następujące pliki z folderu C:\staging:

- *.swm
- custom.mft (lub nazwa pliku wybrana dla pliku manifestu)
- custom.sig (lub zgodna nazwa pliku wybrana dla pliku podpisu)

UWAGA: Jeśli korzystasz z usług IIS jako rozwiązania hostingu, musisz skonfigurować wpisy MIME, aby zawierały następujące rozszerzenia, z których wszystkie muszą być skonfigurowane jako „application/octet-stream:”

- .mft
- .sig
- .swm
- .wim

Inicjowanie systemów docelowych

Systemy docelowe można zainicjować przy użyciu biblioteki HP Client Management Script Library, narzędzia HP Client Security Manager (CSM)/Sure Recover lub zestawu Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

W tym celu należy podać następujące informacje:

1. Adres URL pliku manifestu udostępnionego w poprzedniej sekcji (http://twoj_serwer.domena/sciezka/custom.mft)
2. Klucz publiczny służący do weryfikacji utworzonego wcześniej pliku podpisu (na przykład C:\staging\my-recovery-public.pem).

Rozwiązywanie problemów

Jeśli pojawi się komunikat dotyczący niepowodzenia weryfikacji zabezpieczeń niestandardowego procesu odzyskiwania, sprawdź następujące elementy:

1. Manifest musi być w formacie UTF-8 bez BOM.
2. Sprawdź skróty plików.
3. Upewnij się, że system został zainicjowany przy użyciu klucza publicznego odpowiadającego kluczowi prywatnemu użytemu do podpisania manifestu.

4. Wymagane typy mime serwera IIS to `application/octet-stream`.
5. Ścieżki plików w manifeście muszą zawierać pełną ścieżkę do katalogu najwyższego poziomu zawierającego obraz widziany z systemu klienckiego. Ta ścieżka nie jest pełną ścieżką, w której zapisane są pliki w punkcie dystrybucji.

3 Korzystanie z narzędzia HP Sure Recover Agent wewnątrz firmowej zapory sieciowej

Narzędzie HP Sure Recover Agent może być udostępniane w intranecie firmowym. Po zainstalowaniu pakietu HP Sure Recover SoftPaq skopiuj pliki agenta z katalogu agenta HP Sure Recover z lokalizacji instalacji do punktu dystrybucji HTTP lub FTP. Następnie zainicjuj system kliencki przy użyciu adresu URL punktu dystrybucji i klucza publicznego HP o nazwie `hpsr_agent_public_key.pem`, który jest dostarczany z pakietem SoftPaq agenta HP Sure Recover.

Instalowanie agenta HP Sure Recover

1. Pobierz agenta HP Sure Recover i wyodrębnij pliki do punktu dystrybucji HTTP lub FTP.
2. Ustaw odpowiednie uprawnienia do plików w punkcie dystrybucji.
3. W przypadku korzystania z usług IIS (Internet Information Services) utwórz typy MIME application/octet-stream dla następujących formatów plików:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   WAŻNE: Poniższe kroki opisują inicjowanie oprogramowania Sure Recover przy użyciu rozwiązania SCCM. Przykłady inicjowania oprogramowania Sure Recover przy użyciu biblioteki HP Client Management Script Library zawiera Praca z biblioteką HP Client Management Script Library (CMSL) na stronie 13.

4. Uruchom rozwiązanie SCCM, przejdź do obszaru **HP Client Security Suite**, a następnie wybierz stronę HP Sure Recover.

   UWAGA: Adres URL punktu dystrybucji obejmuje protokół FTP lub HTTP jako protokół transmisji. Zawiera również pełną ścieżkę do katalogu najwyższego poziomu z manifestem agenta HP Sure Recover widzianym z systemu klienta. Ta ścieżka nie jest pełną ścieżką do miejsca zapisu plików w punkcie dystrybucji.

5. W sekcji **Platform Image** (Obraz platformy) wybierz opcję **Corporation** (Korporacja), aby odzyskać niestandardowy obraz systemu operacyjnego z firmowego punktu dystrybucji. Wprowadź adres URL podany przez administratora IT w polu wprowadzania **Image Location URL** (Adres URL lokalizacji obrazu). Wprowadź klucz publiczny `hpsr_agent_public_key.pem` w polu **Image Verification** (Weryfikacja obrazu).

   UWAGA: Niestandardowy adres URL obrazu musi zawierać nazwę pliku manifestu obrazu.

6. W sekcji **Recovery Agent** (Agent odzyskiwania) wybierz opcję **Corporation** (Korporacja), aby użyć niestandardowego agenta odzyskiwania lub agenta odzyskiwania HP z firmowego punktu dystrybucji. Wprowadź adres URL podany przez administratora IT w polu wprowadzania **Agent Location URL** (Adres URL lokalizacji agenta). Wprowadź klucz publiczny `hpsr_agent_public_key.pem` w polu wprowadzania **Agent Verification Key** (Klucz weryfikacji agenta).

UWAGA: Nie dodawaj nazwy pliku manifestu agenta do adresu URL, ponieważ system BIOS wymaga, aby był nazwany recovery.mft.

7. Po zastosowaniu zasad do systemu klienckiego uruchom go ponownie.

8. Podczas wstępnego inicjowania wyświetlany jest monit o wprowadzenie 4-cyfrowego kodu zabezpieczającego w celu ukończenia aktywacji oprogramowania HP Sure Recover. Aby uzyskać więcej informacji przejdź do witryny hp.com i wyszukaj opracowanie techniczne dotyczące zestawu HP Manageability Integration Kit (MIK) dla rozwiązania Microsoft System Center Manager.

Po pomyślnym ukończeniu aktywacji oprogramowania HP Sure Recover niestandardowy adres URL zastosowany do zasad jest wyświetlany w menu ustawień oprogramowania HP Sure Recover w systemie BIOS.

Aby potwierdzić powodzenie aktywacji, uruchom ponownie komputer i po wyświetleniu logo HP naciśnij klawisz f10. Wybierz opcję **Advanced** (Zaawansowane), wybierz oprogramowanie **HP Sure Recover** i wybierz opcję **Recovery Agent** (Agent odzyskiwania), a następnie wybierz opcję **URL** (Adres URL).

4 Praca z biblioteką HP Client Management Script Library (CMSL)

Biblioteka HP Client Management Script Library umożliwia zarządzanie ustawieniami oprogramowania HP Sure Recover przy użyciu programu PowerShell. Poniższy przykładowy skrypt prezentuje sposób inicjowania oprogramowania HP Sure Recover, określania jego stanu, zmieniania jego konfiguracji i anulowania jego inicjowania.

UWAGA: Niektóre polecenia przekraczają długość wiersza tego podręcznika, ale muszą być wprowadzane w jednym wierszu.

```
$ErrorActionPreference = "Stop"

$path = 'C:\test_keys'
$ekpw = ""
$skpw = ""

Get-HPSecurePlatformState

try {
    Write-host 'Provisioning Endorsement Key'
    $p = New-HPSecurePlatformEndorsementKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$path\kek.pfx"
    $p | Set-HPSecurePLatformPayload

    Start-Sleep -Seconds 3

    Write-host 'Provisioning signing key'
    $p = New-HPSecurePlatformSigningKeyProvisioningPayload `
        -EndorsementKeyPassword $ekpw `
        -EndorsementKeyFile "$path\kek.pfx" `
        -SigningKeyFile "$path\sk.pfx"
    $p | Set-HPSecurePLatformPayload
```

```
    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image OS `
        -ImageKeyFile "$path\os.pfx" `
        -username test -password test `
        -url "http://www.hp.com/custom/image.mft"
    $p | Set-HPSecurePLatformPayload

    $p = New-HPSureRecoverImageConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -Image agent `
        -ImageKeyFile "$path\re.pfx" `
        -username test -password test `
        -url "http://www.hp.com/pub/pcbios/CPR"
    $p | Set-HPSecurePLatformPayload

  $p = New-HPSureRecoverSchedulePayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -DayOfWeek Sunday,EveryWeek -Hour 13 -Minute 27 -WindowSize 30
    $p | Set-HPSecurePlatformPayload

    $p = New-HPSureRecoverConfigurationPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx" `
        -OSImageFlags NetworkBasedRecovery `
        -AgentFlags DRDVD
    $p | Set-HPSecurePlatformPayload

    Get-HPSureRecoverState -all
    Get-HPSecurePlatformState
}
```

```
finally {
    Write-Host 'Deprovisioning Sure Recover'
    Start-Sleep -Seconds 3
    $p = New-HPSureRecoverDeprovisionPayload `
        -SigningKeyPassword $skpw `
        -SigningKeyFile "$path\sk.pfx"
    $p | Set-HPSecurePlatformPayload

    Start-Sleep -Seconds 3
    Write-host 'Deprovisioning P21'

    $p = New-HPSecurePlatformDeprovisioningPayload `
        -verbose `
        -EndorsementKeyPassword $pw `
        -EndorsementKeyFile "$Path\kek.pfx"
    $p | Set-HPSecurePlatformPayload

    Write-Host 'Final secure platform state:'
    Get-HPSecurePlatformState
}
```

Przykład generowania kluczy przy użyciu narzędzia OpenSSL

Klucze prywatne należy przechowywać w bezpiecznym miejscu. Klucze publiczne będą używane do walidacji i muszą zostać podane podczas inicjowania. Te klucze muszą mieć długość 2048 bitów i używać wykładnika 0x10001. Zastąp temat w przykładach informacjami o swojej organizacji.

Ustaw następującą zmienną środowiskową przed kontynuowaniem:

```
set OPENSSL_CONF=<path>\openssl.cnf


# Tworzenie certyfikatu głównego CA z podpisem własnym na potrzeby
testowania
openssl req -sha256 -nodes -x509 -newkey rsa:2048 -keyout ca.key -out
ca.crt -subj
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"


# Tworzenie certyfikatu poręczenia klucza
openssl req -sha256 -nodes -newkey rsa:2048 -keyout kek.key -out kek.csr -
subj
```

```
"/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in kek.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out kek.crt

openssl pkcs12 -inkey kek.key -in kek.crt -export -out kek.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:


# Tworzenie klucza podpisywania poleceń

openssl req -sha256 -nodes -newkey rsa:2048 -keyout sk.key -out sk.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in sk.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out sk.crt

openssl pkcs12 -inkey sk.key -in sk.crt -export -out sk.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:

openssl pkcs12 -in sk.pfx -clcerts -nokeys -out sk_public.pem -passin
pass:


# Tworzenie klucza podpisywania obrazu

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Za pomocą tego polecenia można zarejestrować manifest obrazu:

```
openssl dgst -sha256 –sign os.key -out image.sig image.mft


# Tworzenie klucza podpisywania agenta

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Za pomocą tego polecenia można zarejestrować manifest agenta:

```
openssl dgst -sha256 –sign re.key -out agent.sig agent.mft
```

Narzędzie OpenSSL generuje pliki podpisów w formacie big-endian, który nie jest obsługiwany przez niektóre wersje systemu BIOS, dlatego kolejność bajtów w pliku podpisu agenta może wymagać odwrócenia przed

wdrożeniem. Wersje systemu BIOS obsługujące kolejność bajtów big-endian obsługują również kolejność bajtów little-endian.

A Rozwiązywanie problemów

Niepowodzenie partycjonowania dysku

Niepowodzenie partycjonowania dysku może wystąpić, jeśli partycja SR_AED lub SR_IMAGE jest zaszyfrowana przy użyciu funkcji Bitlocker. Partycje te są zwykle tworzone z atrybutem gpt, który uniemożliwia ich szyfrowanie, ale jeśli użytkownik usunie i ponownie utworzy partycje lub utworzy je ręcznie na napędzie fizycznym, agent Sure Recover nie może ich usunąć, a jego działanie zostaje zakończone z powodu błędu podczas ponownego dzielenia dysku na partycje. Użytkownik musi je ręcznie usunąć, uruchamiając program DiskPart, wybierając wolumin i wydając zastępcze polecenie `del vol` lub podobne.

Dziennik audytu oprogramowania układowego

Informacje o zmiennych interfejsu EFI są następujące:

- GUID: `{0xec8feb88, 0xb1d1, 0x4f0f, {0xab, 0x9f, 0x86, 0xcd, 0xb5, 0x3e, 0xa4, 0x45}}`
- Nazwa: `OsRecoveryInfoLog`

Interfejsy API istnieją w systemie Windows w celu odczytywania zmiennych interfejsu EFI lub umożliwiają zrzucanie zawartości zmiennej do pliku za pomocą narzędzia dmpstore środowiska UEFI Shell.

Dziennik audytu można zrzucić za pomocą polecenia `Get-HPFirmwareAuditLog` dostarczonego przez bibliotekę HP Client Management Script Library.

Dziennik zdarzeń systemu Windows

Zdarzenia uruchomienia i zatrzymania oprogramowania Sure Recover są wysyłane do dziennika audytu systemu BIOS, który można wyświetlić w narzędziu Podgląd zdarzeń systemu Windows w dzienniku Sure Start, jeśli zainstalowane jest oprogramowanie HP Notifications. Informacje o tych zdarzeniach zawierają datę i godzinę, identyfikator źródła, identyfikator zdarzenia oraz kod konkretnego zdarzenia. Na przykład wpis `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` oznacza niepowodzenie odzyskiwania z powodu braku możliwości uwierzytelnienia manifestu o kodzie c3f 23000, które zostało zarejestrowane o godzinie 2:26:40 w dniu 6/27/18.

UWAGA: Dzienniki te są zgodne z amerykańskim formatem daty miesiąc/dzień/rok.

HP Secure Platform Management (identyfikator źródła = 84h)

Tabela A-1 HP Secure Platform Management

Identyfikator zdarzenia:	Liczba urządzeń (wszystkie/ DaaS)	Liczba zdarzeń (wszystkie/ DaaS)	Opis	Uwagi
40	256/178	943/552	Proces odzyskiwania systemu operacyjnego platformy został uruchomiony przez oprogramowanie układowe.	Uruchomiono odzyskiwanie platformy.

Tabela A-1 HP Secure Platform Management (ciąg dalszy)

Identyfikator zdarzenia:	Liczba urządzeń (wszystkie/ DaaS)	Liczba zdarzeń (wszystkie/ DaaS)	Opis	Uwagi
41	221/147	588/332	Proces odzyskiwania systemu operacyjnego platformy został zakończony pomyślnie.	Ukończono odzyskiwanie platformy.
42	54/42	252/156	Proces odzyskiwania systemu operacyjnego platformy nie powiódł się.	Odzyskiwanie platformy nie powiodło się.

Dziennik audytu oprogramowania układowego można pobrać przy użyciu polecenia Get-HPFirmwareAuditLog w bibliotece HP Client Management Script Library dostępnej na stronie http://www.hp.com/go/clientmanagement. Zdarzenia HP Secure Platform Management o identyfikatorach 40, 41 i 42 zwracają w polu danych kody zdarzeń, które oznaczają wynik operacji oprogramowania Sure Recover. Na przykład następujący wpis w dzienniku oznacza, że pobieranie pliku manifestu lub podpisu przez oprogramowanie Sure Recover nie powiodło się z błędem o identyfikatorze błędu event_id 42 i danymi: 00:30:f1:c3, które należy interpretować jako wartość dword 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

timestamp: 5/27/2019 2:44:18 PM

description: The platform OS recovery process failed to complete
successfully.

data: 00:30:f1:c3
```

Pomyślne odzyskiwanie jest wyświetlane jako identyfikator zdarzenia event_id = 41 i dane: 00:00:00:00, na przykład:

```
Event Specific Codes

Success = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

severity: Info

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41

timestamp_is_exact: 1

timestamp: 5/27/2019 2:55:41 PM
```

```
description: The platform OS recovery process failed to complete
successfully.
data: 00:00:00:00
```

Oprogramowanie HP Sure Recover używa następujących kodów zdarzeń.

Tabela A-2 Kody zdarzeń

Opis zdarzenia	Kod zdarzenia
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000
AwsDownloadFailed	0xC3F15000
AwsDownloadUnattendedFailed	0xC3F16000
UnableToConnectToNetwork	0xC3F17000
CatalogNotAuthenticated	0xC3F21000
FtpHttpDownloadHashFailed	0xC3F22000
ManifestDoesNotAuthenticate	0xC3F23000
CatalogVersionMismatch	0xC3F31000
CatalogLoadFailed	0xC3F32000
OsDvdDidNotResolvedToOneComponent	0xC3F33000
DriversDvdDidNotResolvedToOneComponent	0xC3F34000
ManifestFileEmptyOrInvalid	0xC3F41000
ListedFileInManifestNotFound	0xC3F42000
FailedToInstallDrivers	0xC3F51000
FailedToApplyWimImage	0xC3F52000
FailedToRegisterWimCallback	0xC3F53000
FailedToCreateDismProcess	0xC3F54000
BcdbootFailed	0xC3F55000
NoSuitableDiskFound	0xC3F56000
PartitoningFailed	0xC3F57000
DiskLayoutCreationFailed	0xC3F58000
UnexpectedProblemWithConfigJson	0xC3FF1000
SureRecoverJsonParsingFailed	0xC3FF2000
RebootRequestFailed	0xC3FF3000
UnableToReadConfigFile	0xC3FF4000
FailedToDetectWindowsPE	0xC3FF5000