Používateľská príručka

HP Sure Recover

Prvé vydanie: február 2020

Katalógové číslo dokumentu: L93434-231

Štýl syntaxe zadávanej používateľom

Text, ktorý musíte zadať v používateľskom rozhraní, je označený `neproporcionálnym písmom`.

Tabuľka -1 Štýl syntaxe zadávanej používateľom

Položka	Popis
`Text bez lomených, hranatých alebo zložených zátvoriek`	Položky, ktoré musíte zadať presne tak, ako sú zobrazené.
`<Text v lomených zátvorkách>`	Zástupný symbol hodnoty, ktorú musíte zadať. Zátvorky vynechajte.
`[Text v hranatých zátvorkách]`	Voliteľné položky. Zátvorky vynechajte.
`{Text v zložených zátvorkách}`	Skupina položiek, z ktorých musíte vybrať len jednu. Zložené zátvorky vynechajte.
`|`	Oddeľovač položiek, z ktorých musíte vybrať len jednu. Zvislú čiaru vynechajte.
`...`	Položky, ktoré sa môžu alebo musia opakovať. Tri bodky vynechajte.

Obsah

1 Úvodné informácie

Program HP Sure Recover vám pomôže bezpečne nainštalovať operačný systém zo siete s minimálnou interakciou používateľa. Systémy s konfiguráciou HP Sure Recover with Embedded Reimaging podporujú aj inštaláciu z lokálneho ukladacieho zariadenia.

DÔLEŽITÉ: Pred použitím programu HP Sure Recover zálohujte údaje. Keďže sa pri vytváraní obrazu preformátuje jednotka, dôjde k strate údajov.

Obnovovacie obrazy, ktoré poskytuje spoločnosť HP, zahŕňajú základný inštalátor systému Windows 10®. Voliteľne môže program HP Sure Recover nainštalovať optimalizované ovládače pre zariadenia HP. Obnovovacie obrazy od spoločnosti HP obsahujú len agentov na obnovenie údajov, ktorí sú súčasťou systému Windows 10, napríklad OneDrive. Firmy môžu vytvárať vlastné obrazy na pridanie firemných nastavení, aplikácií, ovládačov a agentov na obnovu údajov.

Agent na obnovu operačného systému (OS) vykonáva kroky potrebné na inštaláciu obrazu na obnovenie. Agent na obnovu poskytovaný spoločnosťou HP vykonáva bežné kroky, ako je delenie, formátovanie a extrakcia obrazu na obnovenie do cieľového zariadenia. Keďže sa agent na obnovu od spoločnosti HP nachádza na lokalite hp.com, na jeho načítanie budete potrebovať prístup na internet (ak systém neobsahuje integrovanú tvorbu obrazov). Firmy tiež môžu hostiť agenta na obnovu od spoločnosti HP za bránou firewall alebo vytvoriť vlastných agentov na obnovu pre zložitejšie obnovovacie prostredia.

Ak sa nenájde žiadny operačný systém, môžete iniciovať program HP Sure Recover. Program HP Sure Recover môžete spustiť aj plánovane, napríklad na zabezpečenie odstránenia malvéru. Konfiguráciu týchto nastavení vykonajte prostredníctvom aplikácie HP Client Security Manager (CSM), Manageability Integration Kit (MIK) alebo HP Client Management Script Library.

Vykonanie sieťovej obnovy

POZNÁMKA: Ak chcete vykonať sieťovú obnovu, musíte použiť káblové pripojenie. Spoločnosť HP odporúča pred použitím programu HP Sure Recover zálohovať dôležité súbory, údaje, fotografie, videá a ďalší obsah, aby nedošlo k strate údajov.

1. Zapojte klientsky systém do siete, v ktorej možno získať prístup k distribučnému bodu HTTP alebo FTP.
2. Reštartujte klientsky systém a po zobrazení loga spoločnosti HP stlačte kláves f11.
3. Vyberte položku **Restore from network** (Obnoviť zo siete).

Vykonanie obnovy lokálnej jednotky

Ak klientsky systém podporuje integrovanú tvorbu obrazov a v použitej politike je povolená možnosť prevzatia obrazu, v plánovanom čase sa obraz prevezme do klientskeho systému. Po prevzatí obrazu do klientskeho systému ho reštartujte, aby sa obraz skopíroval do ukladacieho zariadenia na integrovanú tvorbu obrazov.

Ak chcete vykonať lokálnu obnovu pomocou obrazu na ukladacom zariadení na integrovanú tvorbu obrazov:

1. Reštartujte klientsky systém a po zobrazení loga spoločnosti HP stlačte kláves f11.
2. Vyberte položku **Restore from local drive** (Obnoviť z lokálnej jednotky).

Systémy s integrovanou tvorbou obrazov musia nakonfigurovať plán preberania a pomocou agenta preberania vyhľadať aktualizácie. Agent preberania je súčasťou doplnku HP Sure Recover Plug-in pre aplikáciu HP Client Security Manager a možno ho tiež nakonfigurovať v aplikácii MIK. Pokyny na používanie aplikácie MIK nájdete na lokalite https://www.hp.com/go/clientmanagement.

Môžete tiež vytvoriť plánovanú úlohu na skopírovanie agenta do oblasti SR_AED a obrazu do oblasti SR_IMAGE. Potom môžete použiť knižnicu HP Client Management Script Library na odoslanie servisnej udalosti, ktorá informuje systém BIOS, že pri nasledujúcom reštartovaní treba overiť obsah a vykonať kopírovanie do ukladacieho zariadenia na integrovanú tvorbu obrazov.

2 Vytvorenie firemného obrazu

Väčšina spoločností používa aplikáciu Microsoft Deployment Tools, súpravu Windows 10 Assessment and Deployment Kit alebo oboje na vytvorenie súborov obsahujúcich obraz v archíve s formátom súboru Windows Imaging (WIM).

Požiadavky

- Najnovšia verzia súpravy Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (alebo iné riešenie na generovanie dvojice súkromného/verejného kľúča RSA)

  Použite na generovanie dvojice kľúčov RSA, ktorá sa používa na zabezpečenie integrity vytváraného a hosteného firemného obrazu.
- Riešenie na hosťovanie servera (napríklad Microsoft Internet Information Services [IIS])

Vytvorenie obrazu

Pred spustením procesu tvorby obrazu nastavte pracovný systém alebo systém zostavy, v ktorom ste nainštalovali potrebné nástroje na prípravu na spracovanie obrazu, ako je uvedené v nasledujúcich krokoch:

1. Ako správca otvorte príkazový riadok `Deployment and Imaging Tools Environment` (nainštalovaný s nástrojmi nasadenia súpravy Windows ADK).
2. Vytvorte pracovnú oblasť pre obraz pomocou nasledujúceho príkazu:

   ```
   mkdir C:\staging
   ```
3. Vytvorte obraz pomocou jedného z nasledujúcich príkladov:

   Príklad 1: Vytvorenie obrazu na základe inštalačného obrazu systému Microsoft Windows na strane 3

   Príklad 2: Vytvorenie obrazu na základe referenčného systému na strane 5

Príklad 1: Vytvorenie obrazu na základe inštalačného obrazu systému Microsoft Windows

1. Pripojte alebo otvorte inštalačný obraz systému Microsoft Windows (zo súboru ISO od spoločnosti Microsoft alebo z disku HP OSDVD).
2. Z pripojeného inštalačného obrazu systému Windows skopírujte súbor install.wim do pracovnej oblasti pomocou nasledujúceho príkazu:

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

   POZNÁMKA: Písmeno `<M:>` označuje pripojenú jednotku. Nahraďte ho správnym písmenom jednotky.
3. Premenujte súbor install.wim na názov súboru obrazu (v tomto príklade „my-image“) pomocou nasledujúceho príkazu:

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

(Voliteľné) Program HP Sure Recover obsahuje funkciu na obnovu konkrétneho vydania z obrazu s viacerými indexmi, a to na základe vydania systému Windows pôvodne licencovaného pre cieľový systém HP od výrobcu. Tento mechanizmus funguje, ak sú indexy pomenované správne. Ak inštalačný obraz systému Windows pochádza z obrazu HP OSDVD, pravdepodobne máte obraz s viacerými vydaniami. Ak si neželáte toto správanie a chcete zabezpečiť používanie jedného konkrétneho vydania pre všetky cieľové systémy, musíte sa uistiť, že v inštalačnom obraze je len jeden index.

4. Skontrolujte obsah inštalačného obrazu pomocou nasledujúceho príkazu:

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

Nasleduje vzorový výstup z inštalačného obrazu, ktorý podporuje päť vydaní (na porovnanie podľa systému BIOS jednotlivých cieľových systémov):

Podrobné informácie o obraze: `my-image.wim`

Index: `1`

Názov: `CoreSingleLanguage`

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

Veľkosť: `19,512,500,682 bytes`

Index: `2`

Názov: `Core`

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

Veľkosť: `19,512,500,682 bytes`

Index: `3`

Názov: `Professional`

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

Veľkosť: `19.758,019,520 bytes`

Index: `4`

Názov: `ProfessionalEducation`

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

Veľkosť: `19,758,019,480 bytes`

Index: `5`

Názov: `ProfessionalWorkstation`

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

Veľkosť: `19,758,023,576 bytes`

POZNÁMKA: Ak je k dispozícii len jeden index, obraz sa použije na obnovu bez ohľadu na názov. Veľkosť súboru obrazu môže byť väčšia ako pred odstráneniami.

5. Ak nechcete správanie s viacerými vydaniami, odstráňte všetky neželané indexy.

   Ako je uvedené v nasledujúcom príklade, ak chcete len vydanie Professional (za predpokladu, že všetky cieľové systémy majú licenciu), odstráňte indexy 5, 4, 2 a 1. Pri každom odstránení indexu sa čísla indexov priradia znova. Preto by ste mali odstraňovať od najväčšieho po najmenšie číslo indexu. Po každom odstránení spustite príkaz `Get-ImageInfo` na vizuálne potvrdenie indexu, ktorý budete odstraňovať ako ďalší.

   ```
   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
   ```

   Vyberte len jeden index vydania (v tomto príklade Professional). Ak je k dispozícii len jeden index, obraz sa použije na obnovu bez ohľadu na názov. Veľkosť súboru obrazu môže byť väčšia ako pred odstráneniami v dôsledku spôsobu fungovania úprav metadát a štandardizácie obsahu WIM.

6. (Voliteľné) Ak chcete do firemného obnovovacieho obrazu zahrnúť ovládače, postupujte podľa týchto krokov:

   a. Obraz pripojte k prázdnemu priečinku pomocou nasledujúcich príkazov:

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

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

   b. Pripojte príslušný disk HP Windows 10 Driver DVD (DRDVD) pre podporovaný cieľový systém. Z pripojeného média s ovládačmi skopírujte podpriečinky s ovládačmi do pracovnej oblasti pomocou nasledujúceho príkazu:

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

   POZNÁMKA: Písmeno `<M:>` označuje pripojenú jednotku. Nahraďte ho správnym písmenom jednotky.

   Ďalšie ovládače vo formáte .inf môžete zahrnúť ich umiestnením do priečinka C:\staging\mount \SWSETUP\DRV. Vysvetlenie spôsobu spracovania tohto obsahu programom HP Sure Recover pomocou funkcie `dism /Add-Driver /Recurse` nájdete v časti „Pridanie a odstránenie ovládačov z obrazu systému Windows v režime offline“ v nasledujúcej téme: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Táto funkcia nepodporuje ovládače vo formáte .exe, ktoré vyžadujú spustenie aplikácie.

   c. Uložte zmeny a odpojte obraz pomocou nasledujúceho príkazu:

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

   Výsledný súbor obrazu je: C:\staging\my-image.wim.

   d. Prejdite na lokalitu Rozdelenie obrazu na strane 6.

Príklad 2: Vytvorenie obrazu na základe referenčného systému

1. Vytvorte spustiteľné médium USB WinPE.

POZNÁMKA: Ďalšie spôsoby zachytenia obrazu možno nájsť v dokumentácii súpravy ADK.

Uistite sa, že jednotka USB má dostatok voľného miesta na uloženie zachyteného obrazu z referenčného systému.

2. Vytvorte obraz v referenčnom systéme.
3. Zachyťte obraz spustením referenčného systému pomocou média USB WinPE a potom použite príkaz DISM.

POZNÁMKA: Písmeno `<U:>` označuje jednotku USB. Nahraďte ho správnym písmenom jednotky.

V prípade potreby upravte časť názvu súboru „my-image“ a popis `<my-image>`.

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

4. Skopírujte obraz z jednotky USB do pracovnej oblasti v pracovnom systéme pomocou nasledujúceho príkazu:

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

Mali by ste mať nasledujúci súbor s obrazom: C:\staging\my-image.wim.

5. Prejdite na lokalitu Rozdelenie obrazu na strane 6.

Rozdelenie obrazu

Spoločnosť HP odporúča rozdeliť obraz na menšie súbory, aby sa zlepšila spoľahlivosť preberania v sieti. Použite nasledujúci príkaz:

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

POZNÁMKA: Parameter FileSize sa zobrazuje v megabajtoch. Upravte ho podľa potreby.

POZNÁMKA: Vzhľadom na povahu algoritmu rozdelenia DISM je možné, že veľkosti generovaných súborov SWM budú menšie alebo väčšie ako uvedená veľkosť súboru.

Vytvorenie manifestu

Formátujte súbory manifestu vo formáte UTF-8 bez značky poradia bajtov (BOM).

Môžete zmeniť názov súboru manifestu (custom.mft), ktorý sa používa v nasledujúcich postupoch. Nesmiete však zmeniť prípony .mft a .sig a časť názvu súboru manifestu sa musí zhodovať so súbormi podpisu. Môžete napríklad zmeniť dvojicu (custom.mft, custom.sig) na (myimage.mft, myimage.sig).

`mft_version` sa používa na určenie formátu súboru obrazu a aktuálne musí byť nastavený na 1.

`image_version` sa používa na určenie, či je k dispozícii novšia verzia obrazu, a na zabránenie v inštalácii starších verzií.

Obe hodnoty musia byť nepodpísané 16-bitové celé čísla a ako oddeľovač riadkov sa musí v manifeste používať `\r\n (CR + LF)`.

Generovanie manifestu

Rozdelený obraz sa môže týkať niekoľkých súborov, a preto pomocou skriptu PowerShell vygenerujte manifest.

Vo všetkých zostávajúcich krokoch musíte byť v priečinku C:\staging.

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

1. Vytvorte skript PowerShell pomocou editora, ktorý dokáže vytvoriť textový súbor vo formáte UTF-8 bez značky BOM. Použite nasledujúci príkaz: `notepad C:\staging\generate-manifest.ps1`

   Vytvorte nasledujúci skript:

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

   `$imageVersion = 1907` (Poznámka: Môže ísť o ľubovoľné 16-bitové celé číslo.)

   ```
   $header = "mft_version=1, image_version=$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
   }
   ```

POZNÁMKA: Manifesty pre program HP Sure Recover nemôžu obsahovať značku BOM, takže nasledujúce príkazy prepíšu súbor na formát UTF8 bez značky BOM.

```
$content = Get-Content $mftFilename

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

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

2. Uložte skript.
3. Spustite skript.

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

Vytvorenie podpisu manifestu

Program Sure Recover overuje agenta a obraz pomocou kryptografických podpisov. Nasledujúce príklady používajú dvojicu súkromného/verejného kľúča vo formáte X.509 PEM (prípona .PEM). Podľa potreby upravte príkazy, aby sa mohli používať binárne certifikáty DER (prípona .CER alebo .CRT), certifikáty PEM s kódovaním BASE-64 (prípona .CER alebo .CRT) alebo súbory PKCS1 PEM (prípona .PEM). Príklad používa aj riešenie OpenSSL, ktoré generuje podpisy vo formáte Big Endian. Manifesty môžete podpísať pomocou ľubovoľného nástroja, ale niektoré verzie systému BIOS podporujú len podpisy vo formáte Little Endian.

1. Vygenerujte 2048-bitový súkromný kľúč RSA pomocou nasledujúceho príkazu. Ak máte 2048-bitovú dvojicu súkromného/verejného kľúča RSA vo formáte PEM, skopírujte kľúče do priečinka C:\staging a prejdite na krok 3.

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

2. Vygenerujte verejný kľúč zo súkromného kľúča (ak máte verejný kľúč zodpovedajúci súkromnému kľúču vo formáte PEM, skopírujte ho do priečinka C:\staging) pomocou nasledujúceho príkazu:

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

3. Vytvorte súbor podpisu (pomocou hodnoty hash SHA256) na základe 2048-bitového súkromného kľúča RSA z kroku 1 pomocou nasledujúceho príkazu:

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

4. Overte súbor podpisu pomocou verejného kľúča z predchádzajúceho kroku pomocou nasledujúceho príkazu:

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

POZNÁMKA:

- Ak potrebujete vytvoriť len súbor podpisu, požadujú sa kroky 1 a 3.
- V prípade programu HP Sure Recover sa požadujú minimálne kroky 1, 2 a 3. Na poskytnutie cieľového systému potrebujete verejný kľúč z kroku 2.
- Krok 4 je voliteľný, ale odporúča sa, aby sa súbor podpisu a súbor manifestu správne overili.

Hostenie súborov

Na serveri hostite nasledujúce súbory z priečinka C:\staging:

- *.swm
- custom.mft (alebo názov súboru, ktorý ste vybrali pre súbor manifestu)
- custom.sig (alebo zodpovedajúci názov súboru, ktorý ste vybrali pre súbor podpisu)

POZNÁMKA: Ak ako riešenie na hosťovanie používate server IIS, musíte nakonfigurovať položky MIME tak, aby zahŕňali nasledujúce prípony, ktoré sú všetky nakonfigurované ako „application/octet-stream:“

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

Poskytovanie cieľových systémov

Cieľové systémy môžete poskytovať pomocou knižnice HP Client Management Script Library, programu HP Client Security Manager (CSM)/Sure Recover alebo súpravy Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Pre toto poskytovanie poskytnite nasledujúce informácie:

1. Adresa URL súboru manifestu hosťovaného v predchádzajúcej časti (http://váš_server.doména/cesta/custom.mft)
2. Verejný kľúč používaný na overenie súboru podpisu, ktorý bol vytvorený predtým (napríklad C:\staging\my-recovery-public.pem).

Riešenie problémov

Ak sa zobrazí hlásenie, že zlyhalo overenie zabezpečenia procesu vlastnej obnovy, skontrolujte nasledujúce:

1. Manifest musí byť vo formáte UTF-8 bez BOM.
2. Skontrolujte hodnoty hash súborov.
3. Skontrolujte, či bol systém poskytnutý pomocou verejného kľúča, ktorý zodpovedá súkromnému kľúču použitému na podpis manifestu.
4. Typy MIME servera IIS musia byť `application/octet-stream`.
5. Cesty k súborom v rámci manifestu musia obsahovať úplnú cestu k hlavnému adresáru obsahujúcemu obraz, ako sa zobrazuje z klientskeho systému. Táto cesta nie je úplná cesta k miestu uloženia súborov v distribučnom bode.

3 Používanie agenta programu HP Sure Recover za firemnou bránou firewall

Agenta programu HP Sure Recover možno hosťovať na firemnom intranete. Po nainštalovaní balíka HP Sure Recover SoftPaq skopírujte súbory agenta z adresára agenta programu HP Sure Recover v mieste inštalácie do distribučného bodu HTTP alebo FTP. Potom poskytnite klientsky systém pomocou adresy URL distribučného bodu a verejného kľúča spoločnosti HP s názvom `hpsr_agent_public_key.pem`, ktorý sa distribuuje s balíkom SoftPaq agenta programu HP Sure Recover.

Inštalácia agenta programu HP Sure Recover

1. Prevezmite agenta programu HP Sure Recover a extrahujte súbory do distribučného bodu HTTP alebo FTP.
2. Nastavte príslušné povolenia súborov v distribučnom bode.
3. Ak používate server Internet Information Services (IIS), vytvorte typy MIME application/octet-stream pre nasledujúce formáty súborov:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   DÔLEŽITÉ: Nasledujúci postup opisuje poskytovanie programu Sure Recover pomocou aplikácie SCCM. Príklady, ako poskytnúť program Sure Recover pomocou knižnice HP Client Management Script Library, nájdete v časti Práca s knižnicou HP Client Management Script Library (CMSL) na strane 12.
4. Spustite aplikáciu SCCM, prejdite na položku **HP Client Security Suite** a vyberte stránku HP Sure Recover.

   POZNÁMKA: Adresa URL distribučného bodu zahŕňa prenosový protokol ftp alebo http. Zahŕňa aj úplnú cestu k hlavnému adresáru obsahujúcemu manifest pre agenta programu HP Sure Recover, ako sa zobrazuje z klientskeho systému. Táto cesta nie je úplná cesta k miestu uloženia súborov v distribučnom bode.
5. V časti **Platform Image** (Obraz platformy) vyberte možnosť **Corporation** (Firma) na obnovenie prispôsobeného obrazu operačného systému z firemného distribučného bodu. Do vstupného poľa **Image Location URL** (Adresa URL umiestnenia obrazu) zadajte adresu URL, ktorú poskytol správca IT. Do poľa **Image Verification** (Overenie obrazu) zadajte verejný kľúč `hpsr_agent_public_key.pem`.

   POZNÁMKA: Adresa URL vlastného obrazu musí obsahovať názov súboru manifestu obrazu.

6. V časti **Recovery Agent** (Agent na obnovu) vyberte možnosť **Corporation** (Firma) na použitie vlastného agenta na obnovu alebo agenta na obnovu od spoločnosti HP z firemného distribučného bodu. Do vstupného poľa **Agent Location URL** (Adresa URL umiestnenia agenta) zadajte adresu URL, ktorú poskytol správca IT. Do vstupného poľa **Agent Verification Key** (Kľúč overenia agenta) zadajte verejný kľúč `hpsr_agent_public_key.pem`.

POZNÁMKA: Adresa URL nesmie obsahovať názov súboru pre manifest agenta, pretože systém BIOS vyžaduje názov recovery.mft.

7. Po použití politiky na klientsky systém ho reštartujte.

8. Počas úvodného poskytovania sa zobrazí výzva na zadanie 4-ciferného kódu zabezpečenia na dokončenie aktivácie programu HP Sure Recover. Ak chcete získať ďalšie informácie, prejdite na lokalitu hp.com a vyhľadajte technickú dokumentáciu k súprave HP Manageability Integration Kit (MIK) pre Microsoft System Center Manager.

Po úspešnom aktivovaní programu HP Sure Recover sa vlastná adresa URL použitá politikou bude zobrazovať v ponuke nastavení HP Sure Recover systému BIOS.

Ak chcete skontrolovať úspešnú aktiváciu, reštartujte počítač a po zobrazení loga spoločnosti HP stlačte kláves f10. Postupne vyberte položky **Advanced** (Rozšírené), **HP Sure Recover**, **Recovery Agent** (Agent na obnovu) a **URL**.

4 Práca s knižnicou HP Client Management Script Library (CMSL)

Knižnica HP Client Management Script Library umožňuje spravovať nastavenia programu HP Sure Recover v prostredí PowerShell. Nasledujúci vzorový skript ukazuje, ako poskytnúť, určiť stav, zmeniť konfiguráciu a zrušiť poskytnutie programu HP Sure Recover.

POZNÁMKA: Niektoré príkazy prekračujú dĺžku riadka v tejto príručke, ale musia sa zadávať ako jeden riadok.

```
$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
}
```

Generovanie vzorového kľúča pomocou riešenia OpenSSL

Súkromné kľúče ukladajte na bezpečnom mieste. Verejné kľúče sa použijú na overenie a musia sa poskytnúť počas poskytovania. Tieto kľúče musia mať dĺžku 2048 bitov a používať exponent 0x10001. Predmet v príkladoch nahraďte informáciami o svojej organizácii.

Pred pokračovaním nastavte nasledujúcu premennú prostredia:

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

# Create a self-signed root CA certificate for testing
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"

# Create a key endorsement certificate
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:


# Create a command signing key

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:


# Create an image signing key

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:
```

Manifest obrazu môžete podpísať pomocou tohto príkazu:

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


# Create an agent signing key

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:
```

Manifest agenta môžete podpísať pomocou tohto príkazu:

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

OpenSSL generuje súbory podpisu vo formáte Big Endian, ktorý je nekompatibilný s niektorými verziami systému BIOS, takže pred nasadením sa môže požadovať obrátenie poradia bajtov súboru podpisu agenta. Verzie systému BIOS, ktoré podporujú poradie bajtov Big Endian, podporujú aj poradie bajtov Little Endian.

A Riešenie problémov

Nepodarilo sa vytvoriť oddiely na jednotke

Ak je oblasť SR_AED alebo SR_IMAGE zašifrovaná pomocou funkcie BitLocker, vytvorenie oddielov môže zlyhať. Tieto oddiely sa zvyčajne vytvárajú pomocou atribútu GPT, ktorý zabraňuje ich šifrovaniu pomocou nástroja BitLocker. Ak však používateľ odstráni a vytvorí oddiely znova alebo ich vytvorí manuálne na jednotke nevyžadujúcej operačný systém, agent programu Sure Recover ich nedokáže odstrániť a pri zmene oddielov jednotky skončí s chybou. Používateľ ich musí odstrániť manuálne spustením aplikácie diskpart, výberom zväzku a spustením príkazu prepísania `del vol` alebo podobného príkazu.

Denník auditu firmvéru

Informácie o premennej EFI sú nasledujúce:

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

V systéme Windows existujú rozhrania API na čítanie premenných EFI alebo môžete vytvoriť výpis obsahu premenných do súboru pomocou nástroja UEFI Shell dmpstore.

Z denníka auditu môžete vytvoriť výpis pomocou príkazu `Get-HPFirmwareAuditLog`, ktorý je súčasťou knižnice HP Client Management Script Library.

Denník udalostí systému Windows

Udalosti spustenia a zastavenia programu Sure Recover sa odosielajú do denníka auditu systému BIOS, ktorý môžete zobraziť v Zobrazovači udalostí systému Windows v denníku Sure Start, ak je nainštalovaný program HP Notifications. Súčasťou týchto udalostí je dátum a čas, identifikátor zdroja, identifikátor udalosti a špecifický kód udalosti. Kód `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` napríklad označuje, že obnovenie zlyhalo, pretože manifest nebolo možné overiť pomocou špecifického kódu udalosti c3f 23000, ktorý bol prihlásený 27.6.2018 o 2:26:40.

POZNÁMKA: Tieto denníky používajú americký formát mesiac/dátum/rok.

HP Secure Platform Management (identifikátor zdroja = 84h)

Tabuľka A-1 HP Secure Platform Management

Identifikátor udalosti	Počet zariadení (všetky/DaaS)	Počet udalostí (všetky/DaaS)	Popis	Poznámky
40	256/178	943/552	Proces obnovy platformy operačného systému bol spustený firmvérom.	Obnova platformy sa spustila

Tabuľka A-1 HP Secure Platform Management (pokračovanie)

Identifikátor udalosti	Počet zariadení (všetky/DaaS)	Počet udalostí (všetky/DaaS)	Popis	Poznámky
41	221/147	588/332	Proces obnovy platformy operačného systému sa úspešne dokončil.	Obnova platformy sa dokončila
42	54/42	252/156	Proces obnovy platformy operačného systému sa nepodarilo úspešne dokončiť.	Obnova platformy zlyhala

Denník auditu firmvéru môžete načítať pomocou príkazu Get-HPFirmwareAuditLog v knižnici HP Client Management Script Library, ktorá je k dispozícii na lokalite http://www.hp.com/go/clientmanagement. Identifikátory udalostí 40, 41 a 42 v aplikácii HP Secure Platform Management vrátia špecifické kódy udalostí v údajovom poli, ktoré označujú výsledok operácií programu Sure Recover. Napríklad nasledujúca položka denníka označuje, že programu Sure Recover sa nepodarilo prevziať súbor manifestu alebo podpisu s chybou event_id 42 a údajmi: 00:30:f1:c3, ktoré by sa mali interpretovať ako hodnota 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
```

Úspešné obnovenie sa zobrazuje ako event_id = 41 a data: 00:00:00:00, napríklad:

```
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
```

Program HP Sure Recover používa nasledujúce špecifické kódy udalostí.

Tabuľka A-2 Špecifické kódy udalostí

Popis udalosti	Kód udalosti
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