Uporabniški vodnik

HP Sure Recover

Prva izdaja: februar 2020

Št. dela dokumenta: L93434-BA1

Ključ za skladnjo uporabniških vnosov

Za besedilo, ki ga morate vnesti v uporabniški vmesnik, je uporabljena `pisava fiksne širine`.

Tabela -1 Ključ za skladnjo uporabniških vnosov

Element	Opis
`Besedilo brez oglatih ali zavitih oklepajev`	Elementi, ki jih morate vnesti natančno tako, kot so prikazani
`<Besedilo znotraj kotnih oklepajev>`	Označba mesta za vrednost, ki jo morate vnesti; izpustite oklepaje
`[Besedilo znotraj oglatih oklepajev]`	Dodatni elementi; izpustite oklepaje
`{Besedilo znotraj zavitih oklepajev}`	Niz elementov, med katerimi morate izbrati enega; izpustite oklepaje
`|`	Ločilo elementov, med katerimi morate izbrati enega; izpustite navpičnico
`. . .`	Elementi, ki se lahko ali se morajo ponoviti; izpustite tri pike

Kazalo

1 Uvod

Rešitev HP Sure Recover vam pomaga pri varni namestitvi operacijskega sistema prek omrežja z minimalnim posegom uporabnika. Sistemi, ki uporabljajo rešitev HP Sure Recover s funkcijo vdelane preslikave, podpirajo tudi namestitev iz lokalne shranjevalne naprave.

POMEMBNO: Preden uporabite rešitev HP Sure Recover, izdelajte varnostno kopijo podatkov. Ker postopek zajema slike znova formatira pogon, pride do izgube podatkov.

Slike za obnovitev, ki jih zagotovi HP, vključujejo osnovni namestitveni program Windows 10®. Če želite, lahko rešitev HP Sure Recover namesti optimizirane gonilnike za HP-jeve naprave. HP-jeve slike za obnovitev vključujejo samo posrednike za obnovitev podatkov, ki so vključeni s sistemom Windows 10, na primer OneDrive. Podjetja lahko ustvarijo svoje slike po meri, da dodajo nastavitve, aplikacije, gonilnike in posrednike za obnovitev podatkov podjetja.

Posrednik za obnovitev operacijskega sistema izvede korake, potrebne za namestitev slike za obnovitev. Posrednik za obnovitev, ki ga zagotavlja HP, izvede splošne korake, na primer particioniranje, formatiranje in ekstrahiranje slike za obnovitev v ciljno napravo. Ker je HP-jev posrednik za obnovitev na naslovu hp.com, za njegovo pridobitev potrebujete dostop do interneta, razen če sistem vključuje funkcijo vdelane preslikave. Podjetja lahko gostijo HP-jevega posrednika za obnovitev tudi znotraj svojega požarnega zidu ali ustvarijo posrednike za obnovitev po meri, ki jih uporabijo za kompleksnejša obnovitvena okolja.

Rešitev HP Sure Recover lahko zaženete, če operacijski sistem ni najden. Lahko jo izvajate tudi po urniku, da poskrbite za odstranitev zlonamerne programske opreme. Konfiguracijo teh nastavitev izvedite prek pripomočkov HP Client Security Manager (CSM), Manageability Integration Kit (MIK) ali HP Client Management Script Library.

Izvedba obnovitve prek omrežja

OPOMBA: Če želite izvesti obnovitev prek omrežja, morate uporabiti žično povezavo. HP priporoča, da pred uporabo rešitve HP Sure Recover izdelate varnostno kopijo pomembnih datotek, podatkov, fotografij, videoposnetkov in drugih vsebin, da preprečite njihovo izgubo.

1. Odjemalski sistem povežite z omrežjem, kjer je mogoče dostopiti do distribucijske točke HTTP ali FTP.
2. Znova zaženite odjemalski sistem; ko se prikaže logotip HP, pritisnite f11.
3. Izberite **Obnovi prek omrežja**.

Izvedba obnovitve z lokalnega pogona

Če odjemalski sistem podpira funkcijo vdelane preslikave in je v uporabljenem pravilniku omogočena možnost za načrtovan prenos slike, se slika prenese v odjemalski sistem ob določenem času. Ko se slika prenese v odjemalski sistem, jo znova zaženite, da jo prekopirate v napravo za shranitev s funkcijo vdelane preslikave.

Če želite izvesti lokalno obnovitev s sliko iz naprave za shranitev s funkcijo vdelane preslikave, naredite naslednje:

1. Znova zaženite odjemalski sistem; ko se prikaže logotip HP, pritisnite f11.
2. Izberite **Obnovi z lokalnega pogona**.

Sistemi s funkcijo vdelane preslikave morajo nastaviti urnik za prenos in uporabiti posrednika za prenos, ki preveri, ali so na voljo posodobitve. Posrednik za prenos je vključen v vtičnik HP Sure Recover za HP Client Security Manager, konfigurirate pa ga lahko tudi v pripomočku MIK. Za navodila za uporabo pripomočka MIK pojdite na spletno mesto https://www.hp.com/go/clientmanagement.

Ustvarite lahko tudi načrtovano nalogo za kopiranje posrednika na particijo SR_AED in slike na particijo SR_IMAGE. Nato lahko s pripomočkom HP Client Management Script Library pošljete dogodek storitve, ki obvesti BIOS, naj pri naslednjem vnovičnem zagonu preveri vsebino in jo prekopira v napravo za shranitev s funkcijo vdelane preslikave.

2 Ustvarjanje slike podjetja

Večina podjetij uporablja za ustvarjanje datotek, ki vsebujejo sliko znotraj arhiva z obliko zapisa datoteke WIM (Windows Imaging), Microsoftova orodja za uvedbo, komplet Windows 10 Assessment and Deployment Kit ali oboje.

Zahteve

- Najnovejša različica kompleta Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (ali druga rešitev za ustvarjanje para zasebnega/javnega ključa RSA)

  Uporablja se za ustvarjanje para ključev RSA za zaščito celovitosti slike podjetja, ki jo ustvarite in gostite.
- Rešitev za gostovanje na strežniku (na primer Microsoft Internet Information Services [IIS])

Ustvarjanje slike

Preden začnete postopek ustvarjanja slike, nastavite delovni sistem ali izdelajte sistem, v katerega ste namestili zahtevana orodja, da se pripravite na obdelavo slike, kot je opisano v spodnjih korakih:

1. Kot skrbnik odprite ukazni poziv `Deployment and Imaging Tools Environment` (nameščen z orodji za uvedbo iz kompleta Windows ADK).
2. Z naslednjim ukazom ustvarite izvajalno območje za svojo sliko:

   ```
   mkdir C:\staging
   ```
3. Z enim od naslednjih primerov ustvarite sliko:

   1. primer: ustvarjanje slike, ki temelji na namestitveni sliki Microsoft Windows na strani 3

   2. primer: ustvarjanje slike, ki temelji na referenčnem sistemu na strani 5

1. primer: ustvarjanje slike, ki temelji na namestitveni sliki Microsoft Windows

1. Vpnite ali odprite namestitveno sliko Microsoft Windows (iz datoteke Microsoft ISO ali z nosilca HP OSDVD).
2. Iz vpete namestitvene slike Windows z naslednjim ukazom prekopirajte datoteko install.wim v svoje izvajalno območje:

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

   OPOMBA: `<M:>` se nanaša na vpeti pogon. Vnesite ustrezno črko pogona.
3. Z naslednjim ukazom preimenujte install.wim v ime slikovne datoteke (v tem primeru »my-image«):

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

   (Izbirno) Rešitev HP Sure Recover vključuje funkcijo, ki omogoča obnovitev določene izdaje iz slike z več indeksi, temelječe na izdaji Windows, ki je bila izvirno licencirana za HP-jev ciljni sistem v tovarni. Ta mehanizem deluje, če so indeksi pravilno poimenovani. Če namestitvena slika Windows izhaja iz slike z nosilca HP OSDVD, gre najverjetneje za sliko z več izdajami. Če ne želite uporabiti tega vedenja in želite

zagotoviti, da je za vse ciljne sisteme uporabljena ena specifična izdaja, morate biti prepričani, da namestitvena slika vsebuje samo en indeks.

4. Vsebino namestitvene slike lahko preverite z naslednjim ukazom:

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

Spodaj so prikazani vzorčni izhodni podatki iz namestitvene slike, ki podpira pet izdaj (ki se uporabijo glede na BIOS posameznega ciljnega sistema):

Podrobnosti slike: `my-image.wim`

Indeks: `1`

Ime: `CoreSingleLanguage`

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

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

Indeks: `2`

Ime: `Core`

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

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

Indeks: `3`

Ime: `Professional`

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

Velikost: `19.758,019,520 bytes`

Indeks: `4`

Ime: `ProfessionalEducation`

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

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

Indeks: `5`

Ime: `ProfessionalWorkstation`

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

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

OPOMBA: Če obstaja samo en indeks, se slika uporabi za obnovitev ne glede na ime. Velikost slikovne datoteke je lahko večja kot pred brisanji.

5. Če ne želite uporabiti vedenja z več izdajami, izbrišite vse neželene indekse.

Če želite na primer uporabiti samo »Professional edition« (če so licencirani vsi ciljni sistemi), izbrišite indekse 5, 4, 2 in 1, kot prikazuje spodnji primer. Vsakič, ko izbrišete indeks, se številke indeksov znova

dodelijo. Zato brišite od najvišje do najnižje številka indeksa. Po vsakem brisanju zaženite `Get-ImageInfo`, da vizualno preverite, kateri indeks boste izbrisali kot naslednjega.

```
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
```

Izberite samo en indeks izdaje (v tem primeru »Professional«). Če obstaja samo en indeks, se slika uporabi za obnovitev ne glede na ime. Upoštevajte, da je lahko velikost slikovne datoteke zaradi načina, na katerega delujejo spremembe metapodatkov WIM in normalizacija vsebine, večja kot pred brisanji.

6. (Izbirno) Če želite v sliko za obnovitev podjetja vključiti gonilnike, upoštevajte spodnje korake:

   a. Z naslednjimi ukazi vpnite sliko v prazno mapo:

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

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

   b. Vpnite ustrezen HP-jev DVD z gonilnikom za Windows 10 (DRDVD) za podprt ciljni sistem. Z vpetega nosilca z gonilnikom z naslednjim ukazom prekopirajte mape gonilnika v svoje izvajalno območje:

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

   OPOMBA: `<M:>` se nanaša na vpeti pogon. Vnesite ustrezno črko pogona.

   Vključite lahko dodatne gonilnike v slogu .inf, tako da jih premaknete v mapo C:\staging\mount\SWSETUP\DRV. Če želite prebrati, kako to vsebino obdela rešitev HP Sure Recover s funkcijo `dism /Add-Driver /Recurse`, glejte »Dodajanje gonilnikov v namestitveno sliko Windows brez povezave in odstranjevanje iz nje« v naslednji temi: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Ta funkcija ne podpira gonilnikov v slogu .exe, ki zahtevajo zagon aplikacije.

   c. Shranite spremembe in z naslednjim ukazom izpnite sliko:

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

   Nastala slikovna datoteka je: C:\staging\my-image.wim.

   d. Glejte Razdelitev slike na strani 6.

2. primer: ustvarjanje slike, ki temelji na referenčnem sistemu

1. Ustvarite zagonski medij USB WinPE.

   OPOMBA: Dodatne načine za zajem slike lahko najdete v dokumentaciji za ADK.

   Prepričajte se, da je na pogonu USB dovolj prostora za shranitev zajete slike iz referenčnega sistema.

2. Ustvarite sliko v referenčnem sistemu.

3. Sliko zajemite tako, da zaženete referenčni sistem z nosilcem USB WinPE, nato pa uporabite DISM.

   OPOMBA: `<U:>` se nanaša na pogon USB. Vnesite ustrezno črko pogona.

   Po potrebi spremenite del imena datoteke »my-image« in opis `<my-image>`.

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

4. Sliko z naslednjim ukazom prekopirajte s pogona USB v izvajalno okolje v svojem delovnem sistemu:

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

   Imeti morate naslednjo slikovno datoteko: C:\staging\my-image.wim.

5. Glejte Razdelitev slike na strani 6.

Razdelitev slike

HP priporoča, da z naslednjim ukazom razdelite sliko v manjše datoteke, s čimer izboljšate zanesljivost prenosov prek omrežja:

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

OPOMBA: Velikost datoteke (FileSize) je prikazana v megabajtih. Naredite ustrezne spremembe.

OPOMBA: Zaradi narave algoritma razdeljevanja DISM so lahko velikosti ustvarjenih datotek SWM manjše ali večje od navedene velikosti datoteke.

Ustvarjanje manifesta

Datoteke manifesta formatirajte kot UTF-8 brez oznake za vrstni red bajtov (BOM).

Ime datoteke manifesta (custom.mft), uporabljeno v spodnjih postopkih, lahko spremenite, ne smete pa spremeniti pripon .mft in .sig, poskrbeti pa morate tudi, da se del z imenom datoteke v datotekah manifesta in podpisa ujema. Par (custom.mft, custom.sig) lahko na primer spremenite v (myimage.mft, myimage.sig).

`mft_version` se uporablja za določitev oblike zapisa datoteke in mora biti trenutno nastavljen na 1.

`image_version` se uporablja za določitev, ali je na voljo novejša različica slike, in za preprečevanje namestitve starejših različic.

Obe vrednosti morata biti nepodpisani 16-bitni celi števili, ločilo vrstic, uporabljeno v manifestu, pa mora biti `'\r\n' (CR + LF)`.

Generiranje manifesta

Ker je lahko v razdeljeno sliko vključenih več datotek, za generiranje manifesta uporabite skript PowerShell.

V vseh preostalih korakih morate biti v mapi C:\staging.

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

1. Z naslednjim ukazom ustvarite skript PowerShell z urejevalnikom, ki lahko ustvari besedilno datoteko z obliko zapisa UTF-8 brez oznake BOM: `notepad C:\staging\generate-manifest.ps1`

   Ustvarite naslednji skript:

   `$mftFilename = "custom.mft"`

   `$imageVersion = 1907` (opomba: to je lahko poljubno 16-bitno celo število)

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

}
```

OPOMBA: Manifesti za HP Sure Recover ne smejo vključevati oznake BOM, zato naslednji ukazi datoteko na novo napišejo kot UTF8 brez oznake BOM.

```
$content = Get-Content $mftFilename

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

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

2. Shranite skript.
3. Izvršite skript.

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

Generiranje podpisa manifesta

Sure Recover preveri posrednika in sliko s kriptografskimi podpisi. Spodnji primeri uporabljajo par zasebnega/javnega ključa z obliko zapisa X.509 PEM (s pripono .PEM). Ukaze po potrebi prilagodite tako, da bodo uporabljali dvojiška potrdila DER (s pripono .CER ali .CRT), potrdila PEM, kodirana z BASE-64 (s pripono .CER ali .CRT) ali datoteke PKCS1 PEM (s pripono .PEM). Primer uporablja tudi OpenSSL, ki generira podpise z obliko zapisa big-endian. Za podpisovanje manifestov lahko uporabite kateri koli pripomoček, toda nekatere različice BIOS-a podpirajo samo podpise z obliko zapisa little-endian.

1. Z naslednjim ukazom generirajte 2048-bitni zasebni ključ RSA. Če imate par 2048-bitnega javnega/zasebnega ključa RSA z obliko zapisa PEM, ga prekopirajte v mapo C:\staging, nato pa pojdite na 3. korak.

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

2. Z naslednjim ukazom generirajte javni ključ iz zasebnega ključa (če imate javni ključ, ki ustreza zasebnemu ključu z obliko zapisa PEM, ga prekopirajte v mapo C:\staging):

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

3. Z naslednjim ukazom ustvarite datoteko s podpisom (z uporabo zgoščevalnega algoritma, temelječega na sha256), ki temelji na 2048-bitnem zasebnem ključu RSA iz 1. koraka:

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

4. Z naslednjim ukazom preverite datoteko s podpisom z uporabo javnega ključa iz prejšnjega koraka:

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

OPOMBA:

- Če morate ustvariti samo datoteko s podpisom, morate izvesti 1. in 3. korak.
- Za HP Sure Recover je treba izvesti vsaj 1., 2. in 3. korak. Za omogočenje ciljnega sistema potrebujete javni ključ iz 2. koraka.
- 4. korak je izbiren, vendar je priporočen, da sta datoteka s podpisom in datoteka manifesta pravilno preverjeni.

Gostovanje datotek

Na strežniku gostite naslednje datoteke iz mape C:\staging:

- *.swm;
- custom.mft (ali ime datoteke, ki ga izberete za datoteko manifesta);
- custom.sig (ali ustrezno ime datoteke, ki ga izberete za datoteko s podpisom).

OPOMBA: Če kot rešitev za gostovanje uporabljate IIS, morate vnose MIME konfigurirati tako, da vključujejo naslednje pripone, ki so konfigurirane kot »application/octet-stream«:

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

Omogočanje ciljnih sistemov

Za omogočenje ciljnih sistemov lahko uporabite pripomočke HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover ali Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Za to omogočenje vnesite naslednje informacije:

1. Naslov URL datoteke z manifestom, ki ste jo gostili v prejšnjem razdelku (http://your_server.domain/path/custom.mft).
2. Javni ključ, uporabljen za preverjanje predhodno ustvarjene datoteke s podpisom (na primer C:\staging\my-recovery-public.pem).

Odpravljanje težav

Če prejmete sporočilo, ki vas obvesti, da postopek obnovitve po meri ni opravil varnostnega preverjanja, preverite naslednje:

1. Manifest mora uporabljati obliko zapisa UTF-8 brez oznake BOM.
2. Preverite zgoščevalne algoritme datoteke.
3. Prepričajte se, da je bil sistem omogočen z javnim ključem, ki ustreza zasebnemu ključu, uporabljenemu za podpis manifesta.
4. Tipi mime za strežnik IIS morajo biti `application/octet-stream`.
5. Poti do datotek znotraj manifesta morajo vključevati celotno pot do najvišjega imenika, ki vsebuje sliko, kot je ta videna v odjemalskem sistemu. To ni celotna pot, na kateri so shranjene datoteke na distribucijski točki.

3 Uporaba posrednika HP Sure Recover znotraj požarnega zidu podjetja

Posrednik HP Sure Recover lahko gostuje v intranetu podjetja. Ko namestite SoftPaq za HP Sure Recover, prekopirajte datoteke posrednika iz imenika posrednika HP Sure Recover z namestitvenega mesta na distribucijsko točko HTTP ali FTP. Nato omogočite odjemalski sistem z URL-jem distribucijske točke in HP-jevim javnim ključem, imenovanim `hpsr_agent_public_key.pem`, ki je poslan skupaj s paketom SoftPaq posrednika HP Sure Recover.

Nameščanje posrednika HP Sure Recover

1. Prenesite posrednika HP Sure Recover in ekstrahirajte datoteke na distribucijsko točko HTTP ali FTP.
2. Nastavite ustrezna datotečna dovoljenja za distribucijsko točko.
3. Če uporabljate ISS (Internet Information Services), ustvarite tipe MIME application/octet-stream za naslednje oblike zapisa datotek:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   POMEMBNO: Naslednji koraki opisujejo omogočanje rešitve Sure Recover z upravljalnikom SCCM. Primeri, ki navajajo, kako omogočiti rešitev Sure Recover s pripomočkom HP Client Management Script Library, so opisani v poglavju Delo s pripomočkom HP Client Management Script Library (CMSL) na strani 12.
4. Zaženite SCCM, odprite **HP Client Security Suite** in izberite stran HP Sure Recover.

   OPOMBA: URL distribucijske točke vključuje kot transportni protokol ftp ali http. Vključuje tudi celotno pot do najvišjega imenika, ki vsebuje manifest za posrednika HP Sure Recover, kot je viden v odjemalskem sistemu. To ni celotna pot do mesta, na katerem so shranjene datoteke na distribucijski točki.
5. V razdelku **Slika platforme** izberite možnost **Podjetje**, da obnovite prilagojeno sliko operacijskega sistema z distribucijske točke podjetja. V vnosno polje **URL mesta slike** vnesite URL, ki ga dobite pri skrbniku za informacijsko tehnologijo. V polje **Preverjanje slike** vnesite javni ključ `hpsr_agent_public_key.pem`.

   OPOMBA: URL slike po meri mora vključevati ime datoteke manifesta slike.
6. V razdelku **Posrednik za obnovitev** izberite možnost **Podjetje**, da uporabite posrednika za obnovitev po meri ali HP-jevega posrednika za obnovitev z distribucijske točke podjetja. V vnosno polje **URL mesta**

posrednika vnesite URL, ki ga dobite pri skrbniku za informacijsko tehnologijo. V polje **Ključ za preverjanje posrednika** vnesite javni ključ `hpsr_agent_public_key.pem`.

OPOMBA: V URL ne vključite imena datoteke za manifest posrednika, ker BIOS zahteva, da se imenuje recovery.mft.

7. Ko za odjemalski sistem uveljavite pravilnik, ga znova zaženite.
8. Med začetnim omogočanjem se prikaže poziv za vnos štirimestne varnostne kode, s katero dokončate aktiviranje rešitve HP Sure Recover. Za dodatne podrobnosti pojdite na spletno mesto hp.com in poiščite informativni dokument HP Manageability Integration Kit (MIK) za Microsoft System Center Manager.

Po uspešnem aktiviranju rešitve HP Sure Recover je URL po meri, ki ga uporabi rešitev, prikazan v meniju z nastavitvami za BIOS HP Sure Recover.

Za potrditev uspešne aktivacije znova zaženite računalnik; ko se prikaže logotip HP, pritisnite f10. Izberite **Napredno**, izberite **HP Sure Recover**, nato pa **Posrednik za obnovitev** in **URL**.

4 Delo s pripomočkom HP Client Management Script Library (CMSL)

Pripomoček HP Client Management Script Library omogoča upravljanje nastavitev za rešitev HP Sure Recover z lupino PowerShell. Spodnji vzorčni skript prikazuje, kako omogočiti rešitev HP Sure Recover, določiti njeno stanje, spremeniti konfiguracijo in jo onemogočiti.

OPOMBA: Več ukazov presega dolžino vrstice tega vodnika, vendar jih je treba vnesti v eni vrstici.

```
$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
}
```

Generiranje vzorčnega ključa s kompletom OpenSSL

Zasebne ključe shranite na varnem mestu. Javni ključi bodo uporabljeni za preverjanje in jih je treba zagotoviti med omogočanjem. Dolžina teh ključev mora biti 2048 bitov in morajo uporabljati eksponent 0x10001. Zadevo v primerih zamenjajte s podatki o svoji organizaciji.

Preden nadaljujete, nastavite naslednjo spremenljivko okolja:

```
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:
```

S tem ukazom lahko podpišete manifest slike:

```
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:
```

S tem ukazom lahko podpišete manifest posrednika:

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

OpenSSL generira datoteke s podpisom v obliki zapisa big-endian, ki ni združljiv z nekaterimi različicami BIOS-a, zato bo pred uvedbo morda treba zamenjati vrstni red bajtov datoteke s podpisom posrednika. Različice BIOS-a, ki podpirajo vrstni red bajtov, podpirajo tudi vrstni red bajtov little-endian.

A Odpravljanje težav

Pogona ni bilo mogoče particionirati

Do napake pri particioniranju pogona lahko pride, če je particija SR_AED ali SR_IMAGE šifrirana s storitvijo Bitlocker. Te particije so običajno ustvarjene z atributom gpt, ki storitvi Bitlocker preprečuje, da bi jih šifrirala, toda če uporabnik particije izbriše in poustvari ali če jih ustvari ročno na pogonu za popolno obnovo, jih posrednik Sure Recover ne more izbrisati, zato se pri vnovičnem particioniranju pogona zapre in sporoči napako. Uporabnik jih mora ročno izbrisati tako, da izvede diskpart, izbere nosilec in izda preglasitveni ukaz `del vol` ali drug podoben ukaz.

Dnevnik nadzora vdelane programske opreme

Informacije o spremenljivki EFI so:

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

Za branje spremenljivk EFI so v sistemu Windows na voljo API-ji, sicer pa lahko izvozite vsebino spremenljivk v datoteko s pripomočkom UEFI Shell dmpstore.

Dnevnik nadzora lahko izvozite z ukazom `Get-HPFirmwareAuditLog`, ki je vključen v HP Client Management Script Library.

Dnevnik dogodkov Windows

Dogodki zagona in zaustavitve Sure Recover so poslani v dnevnik nadzora BIOS, ki si ga lahko ogledate v pregledovalniku dogodkov Windows v dnevniku Sure Start, če je nameščen pripomoček HP Notifications. Ti dogodki vključujejo datum in čas, ID izvora, ID dogodka in specifično kodo dogodka. `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` na primer kaže, da obnovitev ni uspela, ker manifesta ni bilo mogoče overiti s specifično kodo dogodka c3f 23000, ki je bila zabeležena ob 2.26.40 dne 27. 6. 2018.

OPOMBA: Ti dnevniki upoštevajo ameriški zapis datuma v obliki mesec/dan/leto.

HP Secure Platform Management (ID izvora = 84h)

Tabela A-1 HP Secure Platform Management

ID dogodka	Število naprav (vse/DaaS)	Število dogodkov (vsi/DaaS)	Opis	Opombe
40	256/178	943/552	Vdelana programska oprema je začela postopek obnovitve operacijskega sistema platforme.	Obnovitev platforme se je začela.

Tabela A-1 HP Secure Platform Management (Se nadaljuje)

ID dogodka	Število naprav (vse/DaaS)	Število dogodkov (vsi/DaaS)	Opis	Opombe
41	221/147	588/332	Postopek obnovitve operacijskega sistema platforme se je uspešno končal.	Obnovitev platforme je končana.
42	54/42	252/156	Postopka obnovitve operacijskega sistema platforme ni bilo mogoče uspešno končati.	Obnovitev platforme ni uspela.

Dnevnik nadzora vdelane programske opreme lahko pridobite z ukazom Get-HPFirmwareAuditLog v pripomočku HP Client Management Script Library, ki je na voljo na naslovu http://www.hp.com/go/clientmanagement. ID-ji dogodkov HP Secure Platform Management 40, 41 in 42 vrnejo v podatkovnem polju specifične kode dogodkov, ki kažejo rezultat postopkov Sure Recover. Naslednji vnosi v dnevnik na primer kažejo, da rešitev Sure Recover ni uspela prenesti datoteke z manifestom ali podpisom in je vrnila napako event_id 42 ter podatke 00:30:f1:c3, ki jih je treba razložiti kot vrednost 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
```

Uspešna obnovitev je prikazana kot event_id = 41 podatek 00:00:00:00, na primer:

```
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
```

HP Sure Recover uporablja naslednje specifične kode dogodkov.

Tabela A-2 Specifične kode dogodkov

Opis dogodka	Koda dogodka
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