Lietotāja rokasgrāmata

HP Sure Recover

Pirmais izdevums: 2020. gada februāris

Dokumenta daļas numurs: L93434-E11

Lietotāja ievades sintakses taustiņš

Teksts, kas jums ir jāievada lietotāja saskarnē, ir norādīts ar `fiksēta platuma fontu`.

-1. tabula. Lietotāja ievades sintakses taustiņš

Vienums	Apraksts
`Teksts bez iekavām vai figūriekavām`	Vienumi, kas jāievada tieši tā, kā parādīts
`<Teksts leņķiekavās>`	Vietturis vērtībai, kas jums ir jānorāda; izlaidiet iekavas
`[Teksts kvadrātiekavās]`	Papildu vienumi; izlaidiet iekavas
`{Teksts figūriekavās}`	Vienumu kopa, no kuras jāizvēlas tikai viens vienums; izlaidiet figūriekavas
`|`	Vienumu, no kuriem jāizvēlas tikai viens vienums, atdalītājs; izlaidiet vertikālo joslu
`...`	Vienumi, kurus var vai ir jāatkārto; izlaidiet daudzpunkti

Saturs

1 Darba sākšana

HP Sure Recover palīdz jums droši instalēt operētājsistēmu no tīkla ar minimālu lietotāja mijiedarbību. Sistēmas ar HP Sure Recover ar iegultu atkārtotu attēlveidošanu atbalsta arī instalāciju no lokālas atmiņas ierīces.

SVARĪGI! Pirms HP Sure Recover izmantošanas dublējiet datus. Tā kā attēlu apstrādes process pārformatē disku, radīsies datu zudumi.

HP nodrošinātie atkopšanas attēli ietver operētājsistēmas Windows 10® pamata instalētāju. HP Sure Recover var papildus uzstādīt optimizētus draiverus HP ierīcēm. HP atkopšanas attēlos ir iekļauti tikai tādi datu atkopšanas aģenti, kas ietverti Windows 10, piemēram, OneDrive. Korporācijas var izveidot savus pielāgotos attēlus, lai pievienotu uzņēmuma iestatījumus, lietojumprogrammas, draiverus un datu atkopšanas aģentus.

Operētājsistēmas (OS) atkopšanas aģents veic nepieciešamās darbības, lai instalētu atkopšanas attēlu. HP nodrošinātais atkopšanas aģents veic bieži veicamās darbības, piemēram, sadalīšanu, formatēšanu un atkopšanas attēla izvilkšanu mērķa ierīcē. Tā kā HP Recovery aģents atrodas hp.com, ir nepieciešama piekļuve internetam, lai to izgūtu, ja vien sistēmā nav ietverta iegulta atkārtotā attēlveidošana. Korporācijas var arī viesot HP atkopšanas aģentu savā ugunsmūrī vai izveidot pielāgotus atkopšanas aģentus sarežģītākām atkopšanas vidēm.

Jūs varat aktivizēt HP Sure Recover, kad nav atrasta operētājsistēma. Varat arī palaist HP Sure Recover pēc grafika, piemēram, lai nodrošinātu ļaunprogrammatūras dzēšanu. Veiciet šo iestatījumu konfigurāciju, izmantojot HP Client Security Manager (CSM), pārvaldāmības integrēšanas komplektu (MIK) vai HP Client Management Script Library.

Tīkla atkopšanas veikšana

PIEZĪME. Lai veiktu tīkla atkopšanu, ir jāizmanto vadu savienojums. Lai izvairītos no datu zuduma, HP iesaka pirms HP Sure Recover izmantošanas veikt svarīgo failu, datu, fotoattēlu, video un citas informācijas dublēšanu.

1. Pievienojiet klienta sistēmu tīklam, kurā var piekļūt HTTP vai FTP izplatīšanas punktam.
2. Restartējiet klienta sistēmu un, kad tiek parādīts HP logotips, nospiediet taustiņu f11.
3. Atlasiet **Atjaunot no tīkla**.

Lokālā diska atkopšanas veikšana

Ja klienta sistēma atbalsta iegultu atkārtoto attēlveidošanu un plānotā attēla lejupielādes opcija ir iespējota piemērotajā politikā, attēls plānotajā laikā tiek lejupielādēts klienta sistēmā. Kad attēls ir lejupielādēts klienta sistēmā, restartējiet to, lai kopētu attēlu iegultās atkārtotās attēlveidošanas atmiņas ierīcē.

Lai veiktu lokālu atkopšanu, izmantojot iegultās atkārtotās attēlveidošanas atmiņas ierīcē esošo attēlu, veiciet tālāk norādītās darbības.

1. Restartējiet klienta sistēmu un, kad tiek parādīts HP logotips, nospiediet taustiņu f11.
2. Atlasiet **Atjaunot no lokālā diska**.

Sistēmās ar iegultu atkārtotu attēlveidošanu ir jākonfigurē lejupielādes grafiks un jāizmanto lejupielādes aģents, lai pārbaudītu, vai nav atjauninājumu. Lejupielādes aģents ir iekļauts HP Sure Recover Plug-in for HP

Client Security Manager, un to var konfigurēt arī MIK. Lietošanas norādījumus attiecībā uz MIK skatiet vietnē https://www.hp.com/go/clientmanagement.

Varat arī izveidot ieplānotu uzdevumu, lai kopētu aģentu uz SR_AED nodalījumu, bet attēlu — uz SR_IMAGE nodalījumu. Pēc tam varat izmantot HP Client Management Script Library, lai nosūtītu servisa notikumu, kas informē BIOS, ka tam nākamajā atsāknēšanas reizē jāvalidē un jākopē saturs uz iegultās atkārtotās attēlveidošanas atmiņas ierīcē.

2 Uzņēmuma attēla izveide

Vairums uzņēmumu izmanto Microsoft izvietošanas rīkus, Windows 10 novērtējuma un izvietošanas komplektu vai tos abus, lai izveidotu failus, kas satur attēlu Windows Imaging (WIM) failu formāta arhīvā.

Prasības

- Windows 10 novērtējuma un izvietošanas komplekta (Windows ADK) jaunākā versija
- PowerShell
- OpenSSL (vai cits risinājums, lai ģenerētu RSA privāto/publisko kodu pāri)

  Izmantojiet, lai ģenerētu RSA kodu pāri, kas tiek izmantots, lai nodrošinātu izveidotā un viesotā uzņēmuma attēla integritāti.
- Servera viesošanas risinājums (piemēram, Microsoft interneta informācijas pakalpojumi [IIS])

Attēla izveide

Pirms sākat attēla izveides procesu, iestatiet darba sistēmu vai izstrādājiet sistēmu, kurā ir instalēti nepieciešamie rīki attēla apstrādei, kā norādīts tālākajās darbībās.

1. Kā administrators atveriet komandu uzvedni `Izvietošanas un attēlveidošanas rīku vide` (instalēta ar Windows ADK izvietošanas rīkiem).
2. Izveidojiet sava attēla izstādīšanas apgabalu, izmantojot tālāk norādīto komandu.

   ```
   mkdir C:\staging
   ```
3. Izveidojiet attēlu, izmantojot kādu no tālāk norādītajiem piemēriem.

   1. piemērs. Attēla izveide, pamatojoties uz Microsoft Windows instalācijas attēlu 3. lpp.

   2. piemērs. Attēla izveide, pamatojoties uz atsauces sistēmu 5. lpp.

1. piemērs. Attēla izveide, pamatojoties uz Microsoft Windows instalācijas attēlu

1. Montējiet vai atveriet Microsoft Windows instalācijas attēlu (no Microsoft ISO vai HP OSDVD).
2. No montētā Windows instalācijas attēla kopējiet failu install.wim failu uz izstādīšanas apgabalu, izmantojot tālāk norādīto komandu.

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

   PIEZĪME. `< M: >` attiecas uz montēto disku. Aizstājiet to ar pareizo diska burtu.
3. Pārdēvējiet install.wim par attēla faila nosaukumu (šajā piemērā “my-image”), izmantojot tālāk norādīto komandu.

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

   (Papildus) HP Sure Recover ietver funkciju, lai atkoptu noteiktu izdevumu no vairāku indeksu attēla, pamatojoties uz Windows izlaiduma sākotnēji licencēto HP mērķa sistēmu rūpnīcā. Šis mehānisms darbojas, ja indeksiem ir piešķirti pareizi nosaukumi. Ja jūsu Windows instalācijas attēls ir iegūts no HP OSDVD attēla, jums, iespējams, ir vairākizdevumu attēls. Ja jūs nevēlaties šādu uzvedību un vēlaties

nodrošināt, ka viens konkrēts izdevums tiek izmantots visām jūsu mērķa sistēmām, jums ir jāpārliecinās, ka instalācijas attēlā atrodas tikai viens indekss.

4. Pārbaudiet instalācijas attēla saturu, izmantojot tālāk norādīto komandu.

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

Tālāk parādīta parauga izvade no instalācijas attēla, kas atbalsta piecus izdevumus (jāsaskaņo, pamatojoties uz katras mērķa sistēmas BIOS).

Detalizēta informācija par attēlu: `my-image.wim`

Indekss: `1`

Nosaukums: `CoreSingleLanguage`

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

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

Indekss: `2`

Nosaukums: `Core`

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

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

Indekss: `3`

Nosaukums: `Professional`

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

Lielums: `19.758,019,520 bytes`

Indekss: `4`

Nosaukums: `ProfessionalEducation`

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

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

Indekss: `5`

Nosaukums: `ProfessionalWorkstation`

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

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

PIEZĪME. Ja ir tikai viens indekss, attēlu izmanto atkopšanai neatkarīgi no nosaukuma. Jūsu attēla faila lielums var būt lielāks nekā pirms dzēšanas.

5. Ja nevēlaties vairākizdevumu uzvedību, izdzēsiet visus nevajadzīgos indeksus.

Kā redzams tālāk sniegtajā piemērā, ja vēlaties tikai Professional izdevumu (pieņemot, ka visas mērķa sistēmas ir licencētas), izdzēsiet indeksus 5, 4, 2 un 1. Katru reizi, dzēšot indeksu, indeksa numuri tiek

piešķirti atkārtoti. Tāpēc jums vajadzētu izdzēst no augstākā līdz zemākajam indeksa numuram. Pēc katras dzēšanas palaidiet `Get-ImageInfo`, lai vizuāli apstiprinātu, kurš indekss tiks dzēsts nākamais.

```
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
```

Izvēlieties tikai vienu izdevuma indeksu (šajā piemērā — Professional). Ja ir tikai viens indekss, attēlu izmanto atkopšanai neatkarīgi no nosaukuma. Ņemiet vērā, ka jūsu attēla faila lielums var būt lielāks nekā pirms dzēšanas, jo to ietekmē veids, kā darbojas WIM metadatu modifikācijas un satura normalizēšana.

6. (Papildus) Ja vēlaties iekļaut draiverus savā uzņēmuma atkopšanas attēlā, veiciet tālāk norādītās darbības.

   a. Montējiet savu attēlu tukšā mapē, izmantojot tālāk norādītās komandas.

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

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

   b. Montējiet atbilstošo HP Windows 10 draivera DVD disku (DRDVD) atbalstītajai mērķa sistēmai. No montētā draivera datu nesēja kopējiet draivera apakšmapes izstādīšanas apgabalā, izmantojot tālāk norādīto komandu.

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

   PIEZĪME. `< M: >` attiecas uz montēto disku. Aizstājiet to ar pareizo diska burtu.

   Jūs varat iekļaut papildu .inf stila draiverus, novietojot tos zem mapes C:\staging\mount\SWSETUP\DRV. Lai iegūtu izskaidrojumu, kā šo saturu apstrādā HP Sure Recover, izmantojot funkciju `dism /Add-Driver /Recurse`, skatiet sadaļu “Draiveru pievienošana un noņemšana bezsaistes Windows attēlam” šādā tematā: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Šī funkcija neatbalsta .exe stila draiverus, kuriem ir nepieciešams palaist lietojumprogrammu.

   c. Saglabājiet izmaiņas un demontējiet attēlu, izmantojot tālāk norādīto komandu.

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

   Rezultātā iegūtais attēla fails: C:\staging\my-image.wim.

   d. Skatiet sadaļu Attēla sadalīšana 6. lpp.

2. piemērs. Attēla izveide, pamatojoties uz atsauces sistēmu

1. Izveidojiet sāknējamu USB WinPE datu nesēju.

   PIEZĪME. Papildu metodes attēla tveršanai ir atrodamas ADK dokumentācijā.

   Pārliecinieties, vai USB diskā ir pietiekami daudz brīvas vietas, lai saglabātu no atsauču sistēmas tverto attēlu.

2. Izveidojiet attēlu atsauču sistēmā.

3. Uzņemiet attēlu, veicot atsauču sistēmas sāknēšanu ar USB WinPE datu nesēju, un pēc tam izmantojiet DISM.

PIEZĪME. `<U:>` attiecas uz USB disku. Aizstājiet to ar pareizo diska burtu.

Rediģējiet faila nosaukuma daļu “my-image” un pēc nepieciešamības — `<my-image>` aprakstu.

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

4. Kopējiet attēlu no USB uz izstādīšanas apgabalu darba sistēmā, izmantojot tālāk norādīto komandu.

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

   Jums ir nepieciešams šāds attēla fails: C:\staging\my-image.wim.

5. Skatiet sadaļu Attēla sadalīšana 6. lpp.

Attēla sadalīšana

HP iesaka sadalīt attēlu mazākos failos, lai uzlabotu tīkla lejupielādes uzticamību, izmantojot tālāk norādīto komandu.

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

PIEZĪME. FileSize tiek parādīts megabaitos. Rediģējiet pēc nepieciešamības.

PIEZĪME. Ņemot vērā DISM sadalīšanas algoritma specifiku, ģenerēto SWM failu lielums var būt mazāks vai lielāks par norādīto faila lielumu.

Manifesta izveide

Formatējiet manifesta failus kā UTF-8 bez baitu secības atzīmes (BOM).

Varat mainīt manifesta faila nosaukumu (custom.mft), ko izmanto tālāk norādītajās procedūrās, taču jūs nedrīkstat mainīt paplašinājumus .mft un .sig, un manifesta un paraksta failu nosaukuma daļai ir jāsakrīt. Piemēram, jūs varat mainīt pāri (custom.mft, custom.sig) uz (myimage.mft, myimage.sig).

`mft_version` izmanto, lai noteiktu attēla faila formātu, un pašlaik tas ir jāiestata uz 1.

`image_version` izmanto, lai noteiktu, vai ir pieejama jaunāka attēla versija, un novērstu vecāku versiju instalēšanu.

Abām vērtībām jābūt 16 bitu veseliem skaitļiem bez zīmes, un līnijas atdalītājam manifestā jābūt `'\r\n'` `(CR + LF)`.

Manifesta ģenerēšana

Tā kā sadalītais attēls var būt saistīts ar vairākiem failiem, izmantojiet powershell skriptu, lai ģenerētu manifestu.

Veicot visas pārējās darbības, jums ir jāatrodas mapē C:\staging.

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

1. Izveidojiet powershell skriptu, izmantojot redaktoru, kas var izveidot teksta failu formātā UTF-8 bez BOM, izmantojot tālāk norādīto komandu. `notepad C:\staging\generate-manifest.ps1`

   Izveidojiet tālāk norādīto skriptu.

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

```
$imageVersion = 1907
```
(Piezīme. Tas var būt jebkurš 16 bitu vesels skaitlis.)

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

PIEZĪME. HP Sure Recover manifesti nevar ietvert BOM, tāpēc tālāk norādītās komandas pārraksta failu kā UTF8 bez BOM.

```
$content = Get-Content $mftFilename
$encoding = New-Object System.Text.UTF8Encoding $False
```

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

2. Saglabājiet skriptu.
3. Izpildiet skriptu.

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

Manifesta paraksta ģenerēšana

Sure Recover validē aģentu un attēlu, izmantojot kriptogrāfiskus parakstus. Tālāk norādītajos piemēros izmantots privāto/publisko kodu pāris X.509 PEM formātā (.PEM paplašinājums). Pēc nepieciešamības pielāgojiet komandas, lai izmantotu DER bināros sertifikātus (.CER vai.CRT paplašinājums), BASE-64 kodētos PEM sertifikātus (.CER vai .CRT paplašinājums) vai PKCS1 PEM failus (.PEM paplašinājums). Piemērā tiek izmantots arī OpenSSL, kas ģenerē parakstus big-endian formātā. Manifestu parakstīšanai varat izmantot jebkuru utilītu, taču dažas BIOS versijas atbalsta tikai parakstus little-endian formātā.

1. Ģenerējiet 2048 bitu RSA privāto kodu, izmantojot tālāk norādīto komandu. Ja jums ir 2048 bitu RSA privāto/publisko kodu pāris pem formātā, kopējiet tos C:\staging un pēc tam veiciet 3. darbību.

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

2. Ģenerējiet publisko kodu no sava privātā koda (ja jums ir publiskais kods, kas atbilst jūsu privātajam kodam PEM formātā, kopējiet to C:\staging), izmantojot tālāk norādīto komandu.

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

3. Izveidojiet paraksta failu (izmantojot uz sha256 balstītu jaukšanu), pamatojoties uz 2048 bitu RSA privāto kodu no 1. darbības, izmantojot tālāk norādīto komandu.

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

4. Pārbaudiet paraksta failu, izmantojot savu publisko kodu no iepriekšējās darbības, izmantojot tālāk norādīto komandu.

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

PIEZĪME.

- Ja nepieciešams izveidot tikai paraksta failu, jāveic 1. un 3. darbība.
- HP Sure Recover obligāti jāveic 1., 2. un 3. darbība. Lai nodrošinātu savu mērķa sistēmu, ir nepieciešams publiskais kods no 2. darbības.
- 4. darbība ir papildu darbība, taču tā ir ieteicama, lai jūsu paraksta fails un manifesta fails būtu pareizi validēts.

Failu viesošana

Viesojiet serverī šādus failus no mapes C:\staging:

- *.swm;
- custom.mft (vai ar faila nosaukumu, kuru izvēlējāties manifesta failam);
- custom.sig (vai ar atbilstošo faila nosaukumu, kuru izvēlējāties paraksta failam).

PIEZĪME. Ja kā viesošanas risinājumu izmantojat IIS, jums ir jākonfigurē MIME ieraksti, iekļaujot šādus paplašinājumus, kas ir konfigurēti kā "application/octet-stream":

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

Mērķa sistēmu nodrošināšana

Jūs varat nodrošināt savas mērķa sistēmas, izmantojot HP Client Management Script Library, HP Client Security Manager (CSM) / Sure Recover vai pārvaldības integrēšanas komplektu (MIK) (https://www.hp.com/go/clientmanagement).

Sniedziet tālāk norādīto informāciju par šo nodrošinājumu.

1. Iepriekšējā sadaļā viesotā manifesta faila vietrāža URL adrese (http://your_server.domain/path/custom.mft)
2. Publiskais kods, ko izmanto, lai pārbaudītu iepriekš izveidoto paraksta failu (piemēram, C:\staging\my-recovery-public.pem).

Problēmu novēršana

Ja saņemat ziņojumu, ka pielāgotajam atkopšanas procesam neizdevās veikt drošības validāciju, veiciet tālāk norādītās darbības.

1. Manifestam ir jābūt UTF-8 formātā bez BOM.
2. Pārbaudiet failu jaukšanu.
3. Nodrošiniet, lai sistēma būtu nodrošināta ar publisko kodu, kas atbilst privātajam kodam, ko izmanto manifesta parakstīšanai.
4. IIS servera mime tipiem ir jābūt `application/octet-stream`.
5. Failu ceļiem manifestā jāiekļauj pilnais ceļš uz augšējo direktoriju, kas satur klienta sistēmā redzamo attēlu. Šis ceļš nav pilnais ceļš, kur faili tiek saglabāti izplatīšanas punktā.

3 HP Sure Recover Agent izmantošana uzņēmuma ugunsmūrī

HP Sure Recover aģentu var viesot uzņēmuma iekštīklā. Kad esat instalējis HP Sure Recover SoftPaq, kopējiet aģenta failus no HP Sure Recover aģentu direktorija no instalācijas atrašanās vietas uz HTTP vai FTP izplatīšanas punktu. Pēc tam nodrošiniet klienta sistēmai izplatīšanas punkta vietrādi URL un HP publisko kodu ar nosaukumu `hpsr_agent_public_key.pem`, kas tiek izplatīts ar HP Sure Recover aģentu SoftPaq.

HP Sure Recover aģenta instalēšana

1. Lejupielādējiet HP Sure Recover aģentu un izvelciet failus jūsu HTTP vai FTP izplatīšanas punktā.
2. Iestatiet atbilstošas failu atļaujas izplatīšanas punktā.
3. Ja izmantojat interneta informācijas pakalpojumus (IIS), izveidojiet application/octet-stream MIME tipus šādiem failu formātiem:
   - .
   - .wim;
   - .swm;
   - .mft;
   - .sig;
   - .efi;
   - .sdi.

   SVARĪGI! Tālāk norādītās darbības raksturo Sure Recover nodrošināšanu ar SCCM. Lai iegūtu informāciju par to, kā nodrošināt Sure Recover ar HP Client Management Script Library, skatiet sadaļu Darbs ar HP Client Management Script Library (CMSL) 12. lpp..
4. Palaidiet SCCM, atveriet **HP Client Security Suite** un pēc tam atlasiet HP Sure Recover lapu.

   PIEZĪME. Izplatīšanas punkta vietrādis URL kā transporta protokolu ietver gan ftp, gan http. Tajā ir ietverts arī pilnais ceļš uz augstāko direktoriju, kas ietver manifestu HP Sure Recover aģentam, kas redzams klienta sistēmā. Šis ceļš nav pilnais ceļš uz vietu, kur faili tiek saglabāti izplatīšanas punktā.
5. Sadaļā **Platformas attēls** atlasiet opciju **Korporācija**, lai atjaunotu pielāgotu OS attēlu no uzņēmuma izplatīšanas punkta. Ievadiet IT administratora nodrošināto vietrādi URL ievades lodziņā **Attēla atrašanās vietas vietrādis URL**. Ievadiet publisko kodu `hpsr_agent_public_key.pem` laukā **Attēla verifikācija**.

   PIEZĪME. Pielāgotajā attēla vietrādī URL jābūt iekļautam attēla manifesta faila nosaukumam.
6. Sadaļā **Atkopšanas aģents** atlasiet opciju **Korporācija**, lai izmantotu pielāgotu atkopšanas aģentu vai HP Recovery aģentu no uzņēmuma izplatīšanas punkta. Ievadiet IT administratora norādīto vietrādi URL ievades lodziņā **Aģenta atrašanās vietas vietrādis URL**. Ievadiet publisko kodu `hpsr_agent_public_key.pem` ievades laukā **Aģenta verifikācijas kods**.

PIEZĪME. Neiekļaujiet aģenta manifesta faila nosaukumu vietrādī URL, jo BIOS pieprasa, lai tā nosaukums būtu recovery.mft.

7. Kad politika ir piemērota klienta sistēmai, restartējiet to.
8. Sākotnējā nodrošinājuma laikā tiek parādīta uzvedne ar aicinājumu ievadīt četrciparu drošības kodu, lai pabeigtu HP Sure Recover aktivizāciju. Lai iegūtu papildinformāciju, atveriet vietni hp.com un meklējiet HP pārvaldības integrēšanas komplektu (MIK), kas paredzēts Microsoft System Center Manager tehniskajam dokumentam.

Kad HP Sure Recover aktivizācija ir veiksmīgi pabeigta, politikas lietotais pielāgotais vietrādis URL tiek parādīts HP Sure Recover BIOS iestatījumu izvēlnē.

Lai pārliecinātos, ka aktivizācija ir veiksmīga, restartējiet datoru un, kad parādās HP logotips, nospiediet taustiņu f10. Atlasiet **Papildu**, atlasiet **HP Sure Recover**, atlasiet **Atkopšanas aģents** un pēc tam atlasiet **Vietrādis URL**.

4 Darbs ar HP Client Management Script Library (CMSL)

HP Client Management Script Library nodrošina iespēju pārvaldīt HP Sure Recover iestatījumus ar PowerShell. Tālāk redzamajā skripta piemērā ir parādīts, kā nodrošināt HP Sure Recover, noteikt tā statusu, mainīt konfigurāciju un pārtraukt nodrošināšanu.

PIEZĪME. Vairākas komandas pārsniedz šīs rokasgrāmatas rindas garumu, bet tās ir jāievada kā viena rinda.

```
$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
}
```

Parauga kodu ģenerēšana, izmantojot OpenSSL

Glabājiet privātos kodus drošā vietā. Publiskie kodi tiks izmantoti validācijai, un tiem jābūt pieejamiem nodrošinājuma laikā. Šiem kodiem ir jābūt 2048 bitus gariem un jāizmanto 0x10001 eksponents. Nomainiet piemēros norādīto tematu ar informāciju par savu organizāciju.

Pirms turpināt, iestatiet tālāk norādīto vides mainīgo.

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


# Izveidojiet pašparakstītu saknes CA sertifikātu testēšanai
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"


# Izveidojiet koda apstiprinājuma sertifikātu
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:


# Izveidojiet komandas parakstīšanas kodu

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:


# Izveidojiet attēla parakstīšanas kodu

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:
```

Varat parakstīt attēla manifestu ar tālāk norādīto komandu.

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


# Izveidojiet aģenta parakstīšanas kodu

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:
```

Varat parakstīt aģenta manifestu ar tālāk norādīto komandu.

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

OpenSSL ģenerē paraksta failus big-endian formātā, kas nav saderīgs ar dažām BIOS versijām, tāpēc aģenta paraksta faila baitu secība, iespējams, ir jāapgriež pirms izvietošanas. BIOS versijas, kas atbalsta big-endian baitu secību, atbalsta arī little-endian baitu secību.

A Problēmu novēršana

Diska nodalījumu izveide neizdevās

Diska nodalījumu izveide var neizdoties, ja SR_AED vai SR_IMAGE nodalījums ir šifrēts ar Bitlocker. Šie nodalījumi parasti tiek izveidoti ar gpt atribūtu, kas neļauj Bitlocker tos šifrēt, bet, ja lietotājs izdzēš un atkārtoti izveido nodalījumus vai izveido tos manuāli tukšā metāla diskā, tad HP Sure Recover aģents nevar tos izdzēst un iziet, parādot kļūdu, kad tiek veikta diska nodalījumu atkārtota izveide. Lietotājam tie ir manuāli jāizdzēš, palaižot diskpart, atlasot skaļumu un izmantojot `del vol` pārlabošanas komandu vai līdzīgu komandu.

Programmaparatūras audita žurnāls

EFI mainīgā informācija ir tāda, kā norādīts tālāk.

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

API ir pieejami Windows, lai nolasītu EFI mainīgos, vai varat izmest mainīgo saturu failā, izmantojot UEFI Shell dmpstore utilītu.

Jūs varat izmest audita žurnālu, izmantojot komandu `Get-HPFirmwareAuditLog`, ko nodrošina HP Client Management Script Library.

Windows notikumu žurnāls

Sure Recover sākuma un beigu notikumi tiek nosūtīti BIOS audita žurnālam, ko var skatīt Windows notikumu skatītājā Sure Start žurnālā, ja ir instalēta programma HP Notifications. Šie notikumi ietver datumu un laiku, avota ID, notikuma ID un īpašo notikuma kodu. Piemēram, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` norāda, ka neizdevās veikt atkopšanu, jo manifestu nevar autentificēt ar īpašo notikuma kodu c3f 23000, kas tika reģistrēts vietnē 2:26:40 šajā datumā: 6/27/18.

PIEZĪME. Šie žurnāli izmanto ASV datuma formātu: mēnesis/datums/gads.

HP Secure Platform Management (avota ID = 84h)

A-1. tabula. HP Secure Platform Management

Notikuma ID	Ierīču skaits (visas/DaaS)	Notikumu skaits (visi/DaaS)	Apraksts	Piezīmes
40	256/178	943/552	Platformas OS atkopšanas procesu uzsāka programmaparatūra.	Platformas atkopšana uzsākta
41	221/147	588/332	Platformas OS atkopšanas process ir veiksmīgi pabeigts.	Platformas atkopšana pabeigta
42	54/42	252/156	Platformas OS atkopšanas procesu neizdevās veiksmīgi pabeigt.	Platformas atkopšana neizdevās

Varat izgūt programmaparatūras audita žurnālu, izmantojot Get-HPFirmwareAuditLog HP Client Management Script Library, kas pieejama vietnē http://www.hp.com/go/clientmanagement. HP Secure Platform Management notikumu ID 40, 41 un 42 datu laukā atgriež īpašos notikumu kodus, kas norāda Sure Recover darbību rezultātu. Piemēram, šis žurnāla ieraksts norāda, ka Sure Recover neizdevās lejupielādēt manifestu vai paraksta failu ar kļūdu event_id 42 un datiem 00:30:f1:c3, kas jāinterpretē kā DWORD vērtība 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
```

Veiksmīga atkopšana ir redzama kā event_id = 41 un dati 00:00:00:00, piemēram:

```
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 izmanto tālāk norādītos īpašos notikumu kodus.

A-2. tabula. Event Specific Codes

Notikuma apraksts	Notikuma kods
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000

A-2. tabula. Event Specific Codes (turpinājums)

Notikuma apraksts	Notikuma kods
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