Ghid pentru utilizator

HP Sure Recover

Prima ediţie: februarie 2020

Cod document: L93434-271

Explicarea sintaxei pentru intrările utilizatorului

Textul pe care trebuie să îl introduceţi într-o interfaţă de utilizator este indicat de `fontul cu lățime fixă`.

Tabelul -1 Explicarea sintaxei pentru intrările utilizatorului

Număr	Descriere
`Text fără paranteze sau acolade`	Elemente pe care trebuie să le tastaţi exact aşa cum sunt prezentate
`<Text în interiorul parantezelor unghiulare>`	Un substituent pentru o valoare pe care trebuie să o furnizaţi; omiteţi parantezele
`[Text în interiorul parantezelor drepte]`	Elemente opţionale; omiteţi parantezele
`{Text în interiorul acoladelor}`	Un set de elemente din care trebuie să alegeţi unul singur; omiteţi acoladele
`|`	Un separator pentru elementele din care trebuie să alegeţi unul singur; omiteţi bara verticală
`...`	Elemente care pot sau trebuie să se repete; omiteţi punctele de suspensie

Cuprins

1 Noţiuni introductive

Cu ajutorul HP Sure Recover, puteţi să instalaţi în siguranţă sistemul de operare din reţea, cu o interacţiune minimă cu utilizatorul. Sistemele cu HP Sure Recover cu funcţie integrată de restaurare a imaginii acceptă şi instalarea de pe un dispozitiv de stocare local.

IMPORTANT: Efectuaţi copii de rezervă ale datelor înainte de a utiliza HP Sure Recover. Deoarece procesul de imagistică reformatează unitatea, se vor pierde date.

Imaginile de recuperare pe care le oferă HP includ programul de instalare standard pentru Windows 10®. Opţional, HP Sure Recover poate instala drivere optimizate pentru dispozitivele HP. Imaginile de recuperare HP includ numai agenţi de recuperare a datelor care sunt incluşi în Windows 10, precum OneDrive. Firmele îşi pot crea propriile imagini particularizate pentru a adăuga setări, aplicaţii, drivere şi agenţi de recuperare a datelor pentru firmă.

Un agent de recuperare a sistemului de operare (SO) parcurge paşii necesari pentru a instala imaginea de recuperare. Agentul de recuperare oferit de HP parcurge paşi obişnuiţi, precum partiţionarea, formatarea şi extragerea imaginii de recuperare pe dispozitivul ţintă. Întrucât agentul de recuperare HP se găseşte la hp.com, aveţi nevoie de acces la internet pentru a-l recupera, cu excepţia cazului în care sistemul are integrată funcţia de restaurare a imaginii. Firmele pot să găzduiască agentul de recuperare HP în firewall sau să creeze agenţi de recuperare personalizaţi pentru mediile de recuperare mai complexe.

Puteţi iniţia HP Sure Recover în cazul în care nu este detectat niciun sistem de operare. De asemenea, puteţi să rulaţi HP Sure Recover conform unui program, de exemplu, pentru a vă asigura că programele malware sunt şterse. Configuraţi setările respective folosind HP Client Security Manager (CSM), Kitul de integrare şi maniabilitate (MIK) sau Biblioteca de scripturi HP Client Management.

Efectuarea unei recuperări bazate pe reţea

NOTĂ: Pentru a efectua o recuperare bazată pe reţea, trebuie să utilizaţi o conexiune prin cablu. HP recomandă efectuarea copiilor de rezervă ale fişierelor, datelor, fotografiilor, videoclipurilor şi elementelor importante înainte de a utiliza HP Sure Recover, pentru a evita pierderile de date.

1. Conectaţi sistemul de client la reţeaua din care poate fi accesat punctul de distribuire HTTP sau FTP.
2. Reporniţi sistemul de client şi, când apare sigla HP, apăsaţi pe f11.
3. Selectaţi **Restore from network** (Restabilire din reţea).

Efectuarea unei recuperări de pe unitatea locală

Dacă un sistem de client acceptă funcţia integrată de restaurare a imaginii şi opţiunea de descărcare programată a imaginii este activată în politica aplicată, imaginea este descărcată pe sistemul de client la ora programată. După descărcarea imaginii pe sistemul de client, reporniţi sistemul pentru a copia imaginea pe dispozitivul de stocare cu funcţie integrată de restaurare a imaginii.

Pentru a efectua recuperarea locală utilizând imaginea de pe dispozitivul de stocare cu funcţie integrată de restaurare a imaginii:

1. Reporniţi sistemul de client şi, când apare sigla HP, apăsaţi pe f11.
2. Selectaţi **Restore from local drive** (Restabilire de pe unitate locală).

Sistemele cu funcţie integrată de restaurare a imaginii trebuie să configureze un program de descărcare şi să utilizeze agentul de descărcare pentru a căuta actualizări. Agentul de descărcare este inclus în pluginul HP Sure Recover pentru HP Client Security Manager şi poate fi configurat şi în MIK. Consultaţi https://www.hp.com/go/clientmanagement pentru instrucţiunile de utilizare pentru MIK.

De asemenea, puteţi să creaţi o activitate programată pentru a copia agentul pe partiţia SR_AED şi imaginea pe partiţia SR_IMAGE. Apoi puteţi să utilizaţi Biblioteca de scripturi HP Client Management pentru a trimite un eveniment de serviciu care să informeze BIOS-ul că trebuie să valideze conţinutul şi să îl copieze pe dispozitivul de stocare cu funcţie integrată de restaurare a imaginii la următoarea repornire.

2 Crearea unei imagini a firmei

Majoritatea companiilor utilizează Instrumentele de implementare Microsoft, Kitul de evaluare şi implementare Windows 10 sau pe ambele pentru a crea fişiere care conţin o imagine într-o arhivă de formate de fişiere Windows Imaging (WIM).

Cerinţe

- Cea mai recentă versiune a Kitului de evaluare şi implementare Windows 10 (Windows ADK)
- PowerShell
- OpenSSL (sau altă soluţie pentru generarea unei perechi de chei RSA privată/publică)

  Utilizaţi soluţia pentru a genera perechea de chei RSA folosită pentru a asigura integritatea imaginii firmei pe care o creaţi şi găzduiţi.
- O soluţie de găzduire pe server (precum Microsoft Internet Information Services [IIS])

Crearea imaginii

Înainte de a începe procesul de creare a imaginii, configuraţi sistemul de lucru sau sistemul de dezvoltare pe care aţi instalat instrumentele necesare pentru a vă pregăti pentru prelucrarea imaginii, după cum se arată în paşii următori:

1. Ca Administrator, deschideţi linia de comandă pentru `Mediul instrumentelor de implementare și imagistică` (instalat cu ajutorul Instrumentele de implementare din Windows ADK).
2. Creaţi o zonă de tranziţie pentru imagine, utilizând următoarea comandă:

   ```
   mkdir C:\staging
   ```
3. Creaţi imaginea folosind unul dintre următoarele exemple:

   Exemplul 1: Crearea unei imagini pe baza imaginii de instalare Microsoft Windows, la pagina 3

   Exemplul 2: Crearea unei imagini pe baza unui sistem de referinţă, la pagina 5

Exemplul 1: Crearea unei imagini pe baza imaginii de instalare Microsoft Windows

1. Montaţi sau deschideţi imaginea de instalare Microsoft Windows (dintr-un fişier ISO Microsoft sau de pe un DVD cu sistemul de operare de la HP).
2. Din imaginea de instalare Windows montată, copiaţi fişierul install.wim în zona de tranziţie, utilizând următoarea comandă:

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

   NOTĂ: `<M:>` se referă la unitatea montată. Înlocuiţi cu litera unităţii corecte.
3. Redenumiţi install.wim folosind un nume de fişier imagine („my-image” pentru acest exemplu), utilizând următoarea comandă:

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

(Opţional) HP Sure Recover include o caracteristică de recuperare a unei anumite ediţii dintr-o imagine cu mai multe indexuri, bazată pe ediţia Windows licenţiată iniţial din fabrică pentru sistemul HP vizat. Acest mecanism funcţionează dacă indexurile sunt denumite corespunzător. Dacă imaginea de instalare Windows provine dintr-o imagine de pe un DVD cu sistemul de operare de la HP, este posibil să aveţi o imagine pentru mai multe ediţii. Dacă vreţi să utilizaţi o anumită ediţie pentru toate sistemele vizate, trebuie să vă asiguraţi că imaginea de instalare conţine un singur index.

4. Verificaţi conţinutul imaginii de instalare utilizând următoarea comandă:

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

Mai jos este prezentat un exemplu de rezultat bazat pe o imagine de instalare care acceptă cinci ediţii (care se potrivesc cu BIOS-ul fiecărui sistem vizat):

Detalii pentru imagine: `my-image.wim`

Index: `1`

Denumire: `CoreSingleLanguage`

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

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

Index: `2`

Denumire: `Core`

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

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

Index: `3`

Denumire: `Professional`

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

Dimensiune: `19.758,019,520 bytes`

Index: `4`

Denumire: `ProfessionalEducation`

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

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

Index: `5`

Denumire: `ProfessionalWorkstation`

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

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

NOTĂ: Atunci când există un singur index, imaginea este utilizată pentru recuperare, indiferent de nume. Dimensiunea fişierului imagine poate fi mai mare decât înainte de ştergere.

5. Dacă nu doriţi comportamentul pentru mai multe ediţii, ştergeţi fiecare index pe care nu îl doriţi.

   După cum se arată în exemplul de mai jos, dacă doriţi numai ediţia Professional (presupunând că toate sistemele vizate sunt licenţiate), ştergeţi indexurile 5, 4, 2 şi 1. De fiecare dată când ştergeţi un index, numerele de index sunt realocate. Prin urmare, trebuie să ştergeţi începând de la cel mai mare număr de index la cel mai mic. Executaţi `Get-ImageInfo` după fiecare ştergere pentru a confirma vizual indexul pe care îl veţi şterge în continuare.

   ```
   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
   ```

   Alegeţi un singur index al ediţiei (în acest exemplu, Professional). Atunci când există un singur index, imaginea este utilizată pentru recuperare, indiferent de nume. Reţineţi că dimensiunea fişierului imagine poate fi mai mare decât înainte de ştergere, datorită modului de funcţionare a modificărilor metadatelor WIM şi a normalizării conţinutului.

6. (Opţional) Dacă doriţi să includeţi drivere în imaginea de recuperare a firmei, parcurgeţi aceşti paşi:

   a. Montaţi imaginea într-un folder gol, utilizând următoarele comenzi:

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

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

   b. Introduceţi DVD-ul cu driverul Windows 10 (DRDVD) de la HP corespunzător sistemului vizat. De pe suportul cu drivere introdus, copiaţi subfolderele driverului în zona de tranziţie, utilizând următoarea comandă:

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

   NOTĂ: `<M:>` se referă la unitatea montată. Înlocuiţi cu litera unităţii corecte.

   Puteţi include drivere .inf-style suplimentare plasând-le în folderul C:\staging\mount\SWSETUP\DRV. Pentru o explicaţie a modului în care acest conţinut este procesat de HP Sure Recover utilizând funcţia `dism /Add-Driver /Recurse`, consultaţi „Adăugarea şi eliminarea driverelor dintr-o imagine Windows offline” din următorul subiect: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Această caracteristică nu acceptă driverele .exe-style care necesită rularea unei aplicaţii.

   c. Salvaţi modificările şi anulaţi montarea imaginii utilizând următoarea comandă:

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

   Fişierul imagine rezultat este: C:\staging\my-image.wim.

   d. Accesaţi Divizarea imaginii, la pagina 6.

Exemplul 2: Crearea unei imagini pe baza unui sistem de referinţă

1. Creaţi suporturi USB WinPE bootabile.

NOTĂ: Puteţi găsi metode suplimentare de capturare a imaginii în documentaţia ADK.

Asiguraţi-vă că pe unitatea USB există suficient spaţiu liber pentru a stoca imaginea capturată din sistemul de referinţă.

2. Creaţi o imagine pe un sistem de referinţă.
3. Capturaţi imaginea prin iniţializare sistemului de referinţă folosind suportul USB WinPE, apoi utilizaţi DISM.

NOTĂ: `<U:>` se referă la unitatea USB. Înlocuiţi cu litera unităţii corecte.

Editaţi secţiunea „my-image” a numelui de fişier şi descrierea `<my-image>`, după cum este necesar.

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

4. Copiaţi imaginea de pe USB în zona de tranziţie de pe sistemul de lucru utilizând următoarea comandă:

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

Trebuie să obţineţi următorul fişier imagine: C:\staging\my-image.wim.

5. Accesaţi Divizarea imaginii, la pagina 6.

Divizarea imaginii

HP vă recomandă să divizaţi imaginea în fişiere mai mici pentru a îmbunătăţi fiabilitatea descărcărilor din reţea, utilizând următoarea comandă:

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

NOTĂ: Dimensiunea fişierului este exprimată în megabiţi. Editaţi după cum este necesar.

NOTĂ: Datorită naturii algoritmului de divizare DISM, dimensiunile fişierelor SWM generate pot fi mai mici sau mai mari decât dimensiunea de fişier indicată.

Crearea unui manifest

Formataţi fişierele manifest în format UTF-8, fără marcator pentru ordinea octeţilor (BOM).

Puteţi să modificaţi numele fişierului manifest (custom.mft) utilizat în următoarele proceduri, dar nu puteţi să modificaţi extensiile .mft şi .sig, iar secţiunea cu numele fişierului din fişierele manifest şi de semnătură trebuie să corespundă. De exemplu, puteţi să schimbaţi perechea (custom.mft, custom.sig) în (myimage.mft, myimage.sig).

Valoarea `mft_version` se utilizează pentru a stabili formatul fişierului imagine şi trebuie setată la 1.

`image_version` se utilizează pentru a stabili dacă este disponibilă o versiune mai nouă a imaginii şi pentru a împiedica instalarea versiunilor mai vechi.

Ambele valori trebuie să fie numere întregi fără semn, pe 16 biţi, iar separatorul de linie din manifest trebuie să fie „`\r\n” (CR + LF)`.

Generarea unui manifest

Deoarece imaginea divizată poate fi împărţită în mai multe fişiere, utilizaţi un script powershell pentru a genera un manifest.

Pentru ceilalţi paşi, accesaţi folderul C:\staging.

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

1. Creaţi un script powershell utilizând un editor care poate crea un fişier text în format UTF-8 fără BOM, utilizând următoarea comandă: `notepad C:\staging\generate-manifest.ps1`

   Creaţi următorul script:

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

   `$imageVersion = 1907` (Notă: acesta poate fi orice număr întreg pe 16 biţi)

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

NOTĂ: fişierele manifest pentru HP Sure Recover nu pot include un BOM, prin urmare următoarele comenzi rescriu fişierul în format UTF8 fără BOM.

```
$content = Get-Content $mftFilename

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

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

2. Salvaţi scriptul.
3. Executaţi scriptul.

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

Generarea semnăturii pentru manifest

Sure Cover validează agentul şi imaginea utilizând semnături criptografice. Următoarele exemple utilizează o pereche de chei privată/publică în format X.509 PEM (extensia .PEM). Ajustaţi comenzile după cum este necesar pentru a utiliza certificate în format DER (extensia .CER sau .CRT), certificate PEM codate cu BASE-64 (extensia .CER sau .CRT) sau fişiere PEM PKCS1 (extensia .PEM). Exemplul utilizează şi OpenSSL, care generează semnături în format big-endian. Puteţi să folosiţi orice utilitar pentru a semna fişiere manifest, dar unele versiuni de BIOS acceptă numai semnături în format little-endian.

1. Generaţi o cheie privată RSA pe 2048 de biţi utilizând următoarea comandă. Dacă aveţi o pereche de chei RSA privată/publică pe 2048 de biţi în format PEM, copiaţi-le în C:\staging, apoi treceţi la pasul 3.

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

2. Generaţi cheia publică pe baza cheii private (dacă aveţi o cheie publică ce corespunde cheii private în format PEM, copiaţi-o în C:\staging), utilizând următoarea comandă:

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

3. Creaţi un fişier de semnătură (folosind cod hash SHA256) pe baza cheii private RSA pe 2048 biţi de la pasul 1, utilizând următoarea comandă:

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

4. Verificaţi fişierul de semnătură folosind cheia publică de la pasul anterior, utilizând următoarea comandă:

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

NOTĂ:

- Dacă vreţi să creaţi numai un fişier de semnătură, paşii necesari sunt 1 şi 3.
- Pentru HP Sure Recover, paşii necesari sunt 1, 2 şi 3. Aveţi nevoie de cheia publică de la pasul 2 pentru a asigura accesul la sistemul vizat.
- Pasul 4 este opţional, dar este recomandat pentru ca fişierul de semnătură şi fişierul manifest să fie validate corect.

Găzduirea fişierelor

Găzduiţi următoarele fişiere pe serverul dvs. din folderul C:\staging:

- *.swm
- custom.mft (sau numele de fişier pe care l-aţi ales pentru fişierul manifest)
- custom.sig (sau numele de fişier corespunzător pe care l-aţi ales pentru fişierul de semnătură)

NOTĂ: Dacă utilizaţi IIS ca soluţie de găzduire, trebuie să configuraţi intrările MIME pentru a include următoarele extensii, toate configurate ca „application/octet-stream:”

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

Asigurarea accesului la sistemele vizate

Puteţi să acordaţi acces la sistemele vizate utilizând Biblioteca de scripturi HP Client Management, HP Client Security Manager (CSM)/Sure Recover sau Kitul de integrare şi maniabilitate (MIK) (https://www.hp.com/go/clientmanagement).

Introduceţi următoarele informaţii pentru asigurarea accesului:

1. Adresa URL a fişierului manifest găzduită în secţiunea anterioară (http://your_server.domain/path/custom.mft)
2. Cheia publică utilizată pentru a verifica fişierul de semnătură creat anterior (de exemplu, C:\staging\my-recovery-public.pem).

Depanare

Dacă primiţi un mesaj cu privire la validarea nereuşită a securităţii pentru procesul de recuperare particularizat, verificaţi următoarele lucruri:

1. Fişierul manifest trebuie să fie în format UTF-8 fără BOM.
2. Verificaţi codurile hash ale fişierelor.
3. Asiguraţi-vă că sistemul are acces la cheia publică asociată cheii private utilizate pentru semnarea manifestului.
4. Tipurile MIME de pe serverul IIS trebuie să fie `application/octet-stream`.
5. Căile fişierelor din manifest trebuie să includă calea completă către directorul cel mai de sus care conţine imaginea, vizibil pe sistemul de client. Această cale nu este calea completă unde sunt salvate fişierele în punctul de distribuire.

3 Utilizarea agentului HP Sure Recover într-un firewall al firmei

Agentul HP Sure Recover poate fi găzduit într-un intranet al firmei. După ce instalaţi SoftPaqul HP Sure Recover, copiaţi fişierele agentului din directorul agentului HP Sure Recover din locaţia de instalare într-un punct de distribuire HTTP sau FTP. Apoi, asiguraţi accesul sistemului de client prin adresa URL a punctului de distribuire şi cheia publică HP denumită `hpsr_agent_public_key.pem`, care este distribuită prin intermediul SoftPaqului agentului HP Sure Recover.

Instalarea agentului HP Sure Recover

1. Descărcaţi agentul HP Sure Recover şi extrageţi fişierele în punctul de distribuire HTTP sau FTP.
2. Setaţi permisiunile adecvate de fişier în punctul de distribuire.
3. Dacă utilizaţi Internet Information Services (IIS), creaţi tipuri MIME application/octet-stream pentru următoarele formate de fişiere:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   IMPORTANT: Paşii de mai jos descriu modalitatea de asigurare a accesului Sure Recover la SCCM. Pentru exemple privind asigurarea accesului Sure Recover la Biblioteca de scripturi HP Client Management, consultaţi Lucrul cu Biblioteca de scripturi HP Client Management (CMSL), la pagina 12.
4. Porniţi SCCM, navigaţi la **Suita HP Client Security**, apoi selectaţi pagina HP Sure Recover.

   NOTĂ: Adresa URL a punctului de distribuire include protocolul de transport ftp sau http. De asemenea, include calea completă către directorul cel mai de sus care conţine manifestul pentru agentul HP Sure Recover, vizibil de pe sistemul de client. Această cale nu este calea completă unde sunt salvate fişierele în punctul de distribuire.
5. În secţiunea **Imagine platformă**, selectaţi opţiunea **Firmă** pentru a restabili o imagine personalizată a sistemului de operare dintr-un punct de distribuire al firmei. Introduceţi adresa URL oferită de administratorul IT în caseta de intrare **URL locaţie imagine**. Introduceţi cheia publică `hpsr_agent_public_key.pem` în câmpul **Verificare imagine**.

   NOTĂ: Adresa URL a imaginii particularizate trebuie să includă numele fişierului manifest imagine.
6. În secţiunea **Agent de recuperare**, selectaţi opţiunea **Firmă** pentru a utiliza un agent de recuperare particularizat sau agentul de recuperare HP dintr-un punct de distribuire al firmei. Introduceţi adresa

URL oferită de administratorul IT în caseta de intrare **URL locaţie agent**. Introduceţi cheia publică `hpsr_agent_public_key.pem` în câmpul de intrare **Cheie de verificare agent**.

NOTĂ: Nu includeţi numele fişierului manifest al agentului în adresa URL, deoarece BIOS-ul solicită ca acesta să fie denumit recovery.mft.

7. După aplicarea politicii pentru sistemul de client, reporniţi sistemul.
8. În timpul asigurării iniţiale a accesului, apare un mesaj care vă solicită să introduceţi un cod de securitate alcătuit din 4 cifre pentru a finaliza activarea HP Sure Recover. Pentru mai multe detalii, accesaţi hp.com şi căutaţi Kitul de integrare şi maniabilitate (MIK) pentru cartea albă Microsoft System Center Manager.

După finalizarea activării HP Sure Recover, adresa URL particularizată aplicată de politică este afişată în meniul de setări pentru BIOS-ul HP Sure Recover.

Pentru a confirma activarea, reporniţi computerul şi, când apare sigla HP, apăsaţi pe f10. Selectaţi **Avansat**, **HP Sure Recover**, **Agent de recuperare**, apoi **URL**.

4 Lucrul cu Biblioteca de scripturi HP Client Management (CMSL)

Biblioteca de scripturi HP Client Management vă permite să gestionaţi setările HP Sure Recover cu PowerShell. Următorul exemplu de script vă arată cum să asiguraţi accesul, să identificaţi starea, să modificaţi configuraţia şi să anulaţi asigurarea accesului la HP Sure Recover.

NOTĂ: Mai multe dintre comenzi depăşesc lungimea de linie din acest ghid, dar acestea trebuie introduse pe o singură linie.

```
$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
}
```

Exemplu de generare a cheilor utilizând OpenSSL

Păstraţi cheile private într-un loc sigur. Cheile publice vor fi utilizate pentru validare şi trebuie introduse în timpul asigurării accesului. Aceste chei trebuie să aibă lungimea de 2048 biţi şi să utilizeze un exponent 0x10001. Înlocuiţi subiectul din exemple cu informaţii despre organizaţie.

Înainte de a continua, setaţi următoarea variabilă de mediu:

```
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:
```

Puteţi să semnaţi manifestul imagine folosind această comandă:

```
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:
```

Puteţi să semnaţi manifestul agentului folosind această comandă:

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

OpenSSL generează fişiere de semnătură în format big-endian, care este incompatibil cu unele versiuni de BIOS, prin urmare este posibil să fie necesară inversarea ordinii octeţilor din fişierul de semnătură al agentului înainte de a fi implementat. Versiunile de BIOS care acceptă ordinea octeţilor în format big-endian acceptă şi ordinea octeţilor în format little-endian.

A Depanare

Partiţionarea unităţii a eşuat

Partiţionarea unităţii poate eşua dacă partiţia SR_AED sau SR_IMAGE este criptată folosind BitLocker. Aceste partiţii sunt create de obicei cu un atribut gpt care împiedică criptarea cu BitLocker, dar dacă un utilizator şterge şi recreează partiţiile sau dacă le creează manual pe o unitate metalică goală, agentul Sure Recover nu poate să le şteargă şi să le închidă afişând o eroare la repartiţionarea unităţii. Utilizatorul trebuie să le şteargă manual rulând diskpart, selectând volumul şi emiţând comanda de ignorare `del vol` sau o comandă similară.

Jurnalul de audit al firmware-ului

Informaţiile variabile EFI sunt după cum urmează:

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

În Windows există API-uri pentru citirea variabilelor EFI sau puteţi să faceţi un dump al conţinutului variabilelor într-un fişier folosind utilitarul UEFI Shell dmpstore.

Puteţi să faceţi un dump al jurnalului de audit utilizând comanda `Get-HPFirmwareAuditLog` din Biblioteca de scripturi HP Client Management.

Jurnalul de evenimente Windows

Evenimentelele de pornire şi de oprire Sure Recover sunt trimise în jurnalul de audit al BIOS-ului, pe care îl puteţi vizualiza în Vizualizatorul de evenimente din Windows din jurnalul Sure Start dacă aţi instalat Notificări HP. Aceste evenimente includ data şi ora, ID-ul sursei, ID-ul evenimentului şi un cod specific evenimentului. De exemplu, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` indică faptul că recuperarea nu a reuşit, deoarece manifestul nu a putut fi autentificat cu codul specific evenimentului c3f 23000, care a fost înregistrat la 2:26:40 pe 27.06.18.

NOTĂ: Aceste jurnale utilizează formatul de dată lună/zi/an folosit în S.U.A.

HP Secure Platform Management (ID-ul sursei = 84h)

Tabelul A-1 HP Secure Platform Management

ID-ul evenimentului	Număr de dispozitive (Toate/DaaS)	Număr de evenimente (Toate/DaaS)	Descriere	Note
40	256/178	943/552	Procesul de recuperare a sistemului de operare al platformei a fost iniţiat de firmware.	Recuperarea platformei a fost iniţializată

Tabelul A-1 HP Secure Platform Management (Continuare)

ID-ul evenimentului	Număr de dispozitive (Toate/DaaS)	Număr de evenimente (Toate/DaaS)	Descriere	Note
41	221/147	588/332	Procesul de recuperare a sistemului de operare al platformei s-a finalizat.	Recuperarea platformei s-a finalizat
42	54/42	252/156	Procesul de recuperare a sistemului de operare al platformei nu s-a finalizat.	Recuperarea platformei nu a reuşit

Puteţi să recuperaţi jurnalul de audit al firmware-ului utilizând comanda Get-HPFirmwareAuditLog din Biblioteca de scripturi HP Client Management, disponibilă la http://www.hp.com/go/clientmanagement. ID-urile de eveniment 40, 41 şi 42 din HP Secure Platform Management returnează coduri specifice evenimentului în câmpul de date, care indică rezultatul operaţiunilor Sure Recover. De exemplu, următoarea intrare în jurnal indică faptul că Sure Recover nu a reuşit să descarce fişierul manifest sau de semnătură, generând eroarea event_id 42 şi datele: 00:30:f1:c3, care trebuie interpretate ca valoare 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
```

O recuperare reuşită este afişată cu event_id = 41 şi datele: 00:00:00:00, de exemplu:

```
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 utilizează următoarele coduri specifice evenimentului.

Tabelul A-2 Codurile specifice evenimentului

Descrierea evenimentului	Codul evenimentului
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