Naudotojo vadovas

HP Sure Recover

Pirmasis leidimas: 2020 m. vasario mėn.

Dokumento numeris: L93434-E21

Naudotojo įvesties sintaksės klavišas

`Fiksuoto pločio šriftas` nurodo tekstą, kurį turite įvesti į naudotojo sąsają.

-1 lentelė Naudotojo įvesties sintaksės klavišas

Nr.	Aprašymas
`Tekstas be skliaustų`	Elementai turi būti įvesti tiksliai taip, kaip parodyta
`<Tekstas kampiniuose skliaustuose>`	Vietos rezervavimo ženklas vertei, kurią turite nurodyti; praleisti skliaustus
`[Tekstas laužtiniuose skliaustuose]`	Pasirinktiniai elementai; praleisti skliaustus
`{Tekstas riestiniuose skliaustuose}`	Tam tikrų elementų rinkinys, iš kurio turite pasirinkti tik vieną; praleisti riestinius skliaustus
`|`	Elementų, iš kurių turite pasirinkti tik vieną, skyriklis; praleisti vertikalią juostą
`. . .`	Elementai, kurie gali arba privalo kartotis; praleisti daugtaškį

Turinys

1 Darbo pradžia

Minimaliais naudotojo veiksmais „HP Sure Recover“ padeda saugiai įdiegti operacinę sistemą iš tinklo. Sistemos su „HP Sure Recover“ ir įdėtu atvaizdavimu taip pat palaiko diegimą iš vietinio atminties įrenginio.

SVARBU: prieš naudodami „HP Sure Recover“, sukurkite atsarginę duomenų kopiją. Kadangi atvaizdavimo procesas performatuoja diską, duomenys bus prarasti.

HP pateikiami atkurti vaizdai apima pagrindinę „Windows 10®“ diegimo programą. „HP Sure Recover“ gali įdiegti optimizuotas HP įrenginių tvarkykles. HP atkurti vaizdai apima tik duomenų atkūrimo agentus, kurie yra įtraukti į „Windows 10“, pvz., „OneDrive“. Įmonės gali susikurti savo tinkintus vaizdus ir pridėti įmonės nustatymus, programas, tvarkykles ir duomenų atkūrimo agentus.

Operacinės sistemos (OS) atkūrimo agentas atlieka būtinus veiksmus, kad būtų įdiegtas atkūrimo vaizdas. HP pateiktas atkūrimo agentas atlieka bendruosius veiksmus, tokius kaip skaidymas, formatavimas ir atkūrimo vaizdo ištraukimas į tikslinį įrenginį. HP atkūrimo agentas yra svetainėje hp.com, todėl jam pasiekti yra reikalingas interneto ryšys, nebent sistemoje būtų įdėtas atvaizdavimas. Įmonės gali priglobti HP atkūrimo agentą užkardoje arba sukurti tinkintus atkūrimo agentus sudėtingesnėms atkūrimo aplinkoms.

„HP Sure Recover“ galima inicijuoti, kai nepavyksta rasti operacinės sistemos. „HP Sure Recover“ galima paleisti ir pagal tvarkaraštį, kad būtų užtikrintas kenkimo programinės įrangos pašalinimas. Šių nustatymų konfigūraciją atlikite naudodamiesi „HP Client Security Manager“ (CSM), „Manageability Integration Kit“ (MIK) arba „HP Client Management Script Library“.

Tinklo atkūrimas

PASTABA: jei norite atkurti tinklą, turite naudoti laidinį ryšį. Kad neprarastumėte duomenų, prieš naudojant „HP Sure Recover“ HP rekomenduoja sukurti atsargines svarbių failų, duomenų, nuotraukų, vaizdo įrašų ir kt. kopijas.

1. Prijunkite kliento sistemą prie tinklo, kur galima pasiekti HTTP arba FTP paskirstymo vietą.
2. Paleiskite kliento sistemą iš naujo ir, kai bus parodytas HP logotipas, paspauskite f11.
3. Pasirinkite **Atkurti iš tinklo**.

Vietinio disko atkūrimas

Jei kliento sistema palaiko įdėtą atvaizdavimą ir suplanuoto vaizdo atsisiuntimo parinktis įjungta taikomoje politikoje, tada vaizdas atsisiunčiamas į kliento sistemą suplanuotu laiku. Po to, kai vaizdas atsisiunčiamasį kliento sistemą, paleiskite ją iš naujo, kad vaizdas būtų nukopijuotas į įdėto atvaizdavimo atminties įrenginį.

Vykdykite šiuos nurodymus, jei norite atlikti vietinį atkūrimą naudodami vaizdą iš įdėto atvaizdavimo atminties įrenginio.

1. Paleiskite kliento sistemą iš naujo ir, kai bus parodytas HP logotipas, paspauskite f11.
2. Pasirinkite **Atkurti iš vietinio disko**.

Sistemos su įdėtu atvaizdavimu turi sukonfigūruoti atsisiuntimų tvarkaraštį ir tikrinti naujinius naudojant atsisiuntimų agentą. Atsisiuntimų agentas yra įtrauktas į „HP Sure Recover“ įskiepį skirtą „HP Client Security Manager“ ir gali būti konfigūruojamas MIK. MIK naudojimo instrukcijas žr. https://www.hp.com/go/clientmanagement.

Taip pat galite sukurti suplanuotą užduotį, kad nukopijuotumėte agentą į SR_AED skaidinį ir vaizdą į SR_IMAGE skaidinį. Tada galite pasinaudoti „HP Client Management Script Library“, kad išsiųstumėte techninės priežiūros įvykį informuojantį BIOS patvirtinti turinį ir nukopijuoti į įdėto atvaizdavimo atminties įrenginį, kai kitą kartą operacinė sistema bus įkelta iš naujo.

2 Įmonės vaizdo kūrimas

Dauguma įmonių naudoja „Microsoft“ diegimo įrankius, „Windows 10“ įvertinimo ir diegimo rinkinį, ar abu, kad sukurtu failus su vaizdu „Windows Imaging“ (WIM) failo formato archyve.

Reikalavimai

- Naujausia „Windows 10“ įvertinimo ir diegimo rinkinio versija („Windows ADK“)
- PowerShell
- OpenSSL (arba kitas sprendimas, kuriuo galima sugeneruoti RSA privačiųjų/viešųjų raktų porą)

  Naudokite, jei norite sugeneruoti RSA raktų porą, kuri naudojama apsaugant sukurto ir priglobto įmonės vaizdo vientisumą.
- Serverio prieglobos sprendimas (pvz., „Microsoft Internet Information Services“ [IIS])

Vaizdo kūrimas

Prieš pradėdami vaizdo kūrimo procesą nustatykite darbinę sistemą arba sukurkite sistemą ten, kur įdiegėte reikiamus įrankius vaizdui apdoroti, kaip tai nurodyta toliau pateikiamuose veiksmuose.

1. Administratoriaus teisėmis atidarykite `Deployment and Imaging Tools Environment` komandinę eilutę (įdegtą su su „Windows ADK“ diegimo įrankiais).
2. Sukurkite savo atvaizdo kūrimo sritį naudodami toliau nurodytą komandą:

   ```
   mkdir C:\staging
   ```
3. Sukurkite vaizdą naudodami vieną iš toliau nurodytų pavyzdžių

   1 pavyzdys. Vaizdo kūrimas pagal „Microsoft Windows“ diegimo vaizdą 3 puslapyje

   2 pavyzdys. Vaizdo kūrimas pagal nuorodų sistemą 5 puslapyje

1 pavyzdys. Vaizdo kūrimas pagal „Microsoft Windows“ diegimo vaizdą

1. Įdėkite arba atidarykite „Microsoft Windows“ diegimo vaizdą (iš „Microsoft ISO“ arba iš HP OSDVD).
2. Iš įdėto „Windows“ diegimo vaizdo nukopijuokite install.wim failą į atvaizdo kūrimo sritį naudodami toliau nurodytą komandą.

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

   PASTABA: `<M:>` žymi integruotą diską. Pakeiskite teisinga disko raide.
3. Pervadinkite install.wim vaizdo failo pavadinimu (šiame pavyzdyje tai „my-image“) naudodami toliau nurodytą komandą.

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

   (Pasirenkama) „HP Sure Recover“ turi funkciją, kuria galima atkurti konkretų leidimą iš kelių rodyklių vaizdo pagal „Windows“ leidimą, kuris gamykliškai buvo licencijuotas HP tikslinei sistemai. Šis mechanizmas veikia, jei rodyklės yra pavadintos tinkamai. Jei „Windows“ diegimo vaizdas yra iš HP OSDVD vaizdo, jūs tikriausiai turite kelių leidimų vaizdą. Jei tokio veikimo nepageidaujate ir norite

naudoti vieną konkretų leidimą visoms tikslinėms sistemoms, tada turite būti tikri, kad diegimo vaizde būtų tik viena rodyklė.

4. Patikrinkite diegimo vaizdo turinį naudodami toliau nurodytą komandą.

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

Toliau pateikiamas diegimo atvaizdo išvesties pavyzdys, kuris palaiko penkis leidimus (pritaikomas pagal kiekvienos tikslinės sistemos BIOS):

Vaizdo informacija: `my-image.wim`

Rodyklė: `1`

Pavadinimas: `CoreSingleLanguage`

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

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

Rodyklė: `2`

Pavadinimas: `Core`

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

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

Rodyklė: `3`

Pavadinimas: `Professional`

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

Dydis: `19.758,019,520 bytes`

Rodyklė: `4`

Pavadinimas: `ProfessionalEducation`

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

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

Rodyklė: `5`

Pavadinimas: `ProfessionalWorkstation`

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

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

PASTABA: jei yra tik viena rodyklė, vaizdas naudojamas atkūrimui neatsižvelgiant į pavadinimą. Jūsų vaizdo failo dydis gali būti didesnis nei prieš ištrynimus.

5. Jei nenorite kelių leidimų veikimo, ištrinkite kiekvieną nepageidaujamą rodyklę.

Kaip parodyta toliau pateiktame pavyzdyje, jei norite naudoti tik „Professional“ leidimą (jei yra licencijuotos visos tikslinės sistemos), ištrinkite 5, 4, 2 ir 1 rodyklę. Kiekvieną kartą, kai ištrinate rodyklę,

rodyklės numeriai priskiriami iš naujo. Todėl reikia trinti nuo didžiausių iki mažiausių rodyklės numerių. Po kiekvieno trynimo paleiskite `Get-ImageInfo` ir vizualiai patvirtinkite, kurią kitą rodyklę trinsite.

```
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
```

Pasirinkite tik vieną leidimo rodyklę (šiame pavyzdyje tai „Professional“). Jei yra tik viena rodyklė, vaizdas naudojamas atkūrimui neatsižvelgiant į pavadinimą. Atkreipkite dėmesį, kad jūsų vaizdo failo dydis gali būti didesnis nei prieš trynimus, nes veikia WIM metaduomenų modifikavimas ir turinio normalizavimas.

6. (Pasirenkama) Jei norite įtraukti tvarkykles į bendrą atkūrimo vaizdą, atlikite toliau nurodytus veiksmus.

   a. Įdėkite vaizdą į tuščią aplanką naudodami toliau nurodytas komandas.

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

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

   b. Įdėkite atitinkamą HP „Windows 10“ tvarkyklės DVD (DRDVD) palaikomai tikslinei sistemai. Iš įdėtos tvarkyklės medijos nukopijuokite tvarkyklės poaplankius į atvaizdo kūrimo sritį naudodami toliau nurodytą komandą.

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

   PASTABA: `<M:>` žymi integruotą diską. Pakeiskite teisinga disko raide.

   Taip pat galite įtraukti papildomų .inf stiliaus tvarkyklių įkeldami jas į aplanką C:\staging\mount \SWSETUP\DRV. Jei reikia paaiškinimo, kaip šį turinį apdoroja „HP Sure Recover“ naudojant `dism /Add-Driver /Recurse` funkciją, žr. „Pridėti ir pašalinti tvarkykles „Windows“ vaizde neprisijungus“ toliau pateikiamoje svetainėje: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Ši priemonė nepalaiko .exe stiliaus tvarkyklių, kurioms reikia paleisti programą.

   c. Įrašykite pakeitimus ir išimkite vaizdą naudodami toliau nurodytą komandą.

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

   Gautas vaizdo failas yra: C:\staging\my-image.wim.

   d. Eikite į Vaizdo skaidymas 6 puslapyje.

2 pavyzdys. Vaizdo kūrimas pagal nuorodų sistemą

1. Sukurkite užkraunamą USB „WinPE“ mediją.

   PASTABA: papildomus vaizdo fiksavimo metodus rasite ADK dokumentacijoje.

   Įsitikinkite, kad USB atmintinėje užtenka laisvos vietos, kad tilptų užfiksuotas vaizdas iš nuorodų sistemos.

2. Sukurkite vaizdą nuorodų sistemoje.

3. Užfiksuokite vaizdą įkraudami nuorodų sistemą su USB „WinPE“ medija, tada naudokite DISM.

PASTABA: `<U:>` nurodo USB atmintinę. Pakeiskite teisinga disko raide.

Redaguokite „my-image“ failo pavadinimo dalį ir `<my-image>` aprašymą.

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

4. Nukopijuokite vaizdą iš USB į atvaizdo kūrimo sritį darbinėje sistemoje naudodami toliau nurodytą komandą:

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

   Jūsų vaizdo failas turėtų būti: C:\staging\my-image.wim.

5. Eikite į Vaizdo skaidymas 6 puslapyje.

Vaizdo skaidymas

HP rekomenduoja suskaidyti vaizdą į mažesnius failus ir pagerinti tinklo atsisiuntimų patikimumą naudojant toliau nurodytą komandą:

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

PASTABA: failo dydis rodomas megabaitais. Redaguokite pagal poreikį.

PASTABA: dėl DISM skaidymo algoritmo pobūdžio, sukurtų SWM failų dydžiai gali būti mažesni arba didesni, nei nurodytas failų dydis.

Deklaracijos kūrimas

Formatuokite deklaracijos failus kaip UTF-8 be baitų eiliškumo žymos (BOM).

Galite pakeisti deklaracijos failo pavadinimą (custom.mft), kuris naudojamas šiose procedūrose, tačiau negalima keisti plėtinių .mtf ir .sig, o deklaracijos ir parašo failų pavadinimų dalis turi sutapti. Pavyzdžiui, galite pakeisti porą (custom.mft, custom.sig) į (myimage.mft, myimage.sig).

`mft_version` naudojama nustatant vaizdo failo formatą ir turi būti nustatyta kaip 1.

`image_version` naudojama nustatant, ar yra naujesnių vaizdo versijų ir siekiant apsisaugoti nuo senesnių versijų įdiegimo.

Abi reikšmės turi būti 16 bitų sveikasis skaičius be ženklo, o deklaracijos eilučių skyriklis turi būti `'\r\n'` `(CR + LF)`.

Deklaracijos generavimas

Kadangi su suskaidytu vaizdu gali būti susiję keli failai, deklaracijai generuoti naudokite „PowerShell“ scenarijų.

Atlikdami likusius veiksmus turite būti C:\staging aplanke.

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

1. Sukurkite „PowerShell“ scenarijų rengykle, kuri gali sukurti tekstinį failą UTF-8 formatu be BOM, naudojant toliau nurodytą komandą: `notepad C:\staging\generate-manifest.ps1`

   Sukurkite tokį scenarijų:

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

```
$imageVersion = 1907
```
(Pastaba. Tai gali būti bet kuris 16 bitų sveikasis skaičius)

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

PASTABA: „HP Sure Recover“ skirtose deklaracijose negali būti BOM, todėl šios komandos perrašo failą kaip UTF8 be BOM.

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

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

2. Išsaugokite scenarijų.
3. Vykdykite scenarijų.

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

Deklaracijos parašo generavimas

„Sure Recover“ patvirtina agentą ir vaizdą naudojant kriptografinius parašus. Toliau pateikti pavyzdžiai naudoja privačių / viešų raktų porą X.509 PEM formatu (.PEM plėtinys). Koreguokite komandas, kad galėtumėte naudoti DER dvejetainius sertifikatus (.CER arba .CRT plėtinys), BASE-64 užkoduotus PEM sertifikatus (.CER arba .CRT plėtinys), arba PKCS1 PEM failus (.PEM plėtinys). Pavyzdyje taip pat naudojamas „OpenSSL“, kuris generuoja parašus mažėjančių baitų formatu. Deklaracijų pasirašymui galite naudoti bet kokias priemones, tačiau kai kurios BIOS versijos palaiko tik parašus didėjančių baitų formatu.

1. Sugeneruokite 2048 bitų RSA privatų raktą naudodami toliau nurodytą komandą. Jei turite 2048 bitų RSA privačių/viešų raktų porą pem formatu, nukopijuokite juos į C:\staging ir pereikite prie 3 žingsnio.

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

2. Iš savo privataus rakto sugeneruokite viešąjį raktą (jei turite viešąjį raktą, kuris atitinka jūsų privatųjį raktą PEM formatu, nukopijuokite jį į C:\staging), naudodami toliau nurodytą komandą:

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

3. Sukurkite parašo failą (naudodami sha256 pagrįstą maišą) pagal savo 2048 bitų RSA privatų raktą iš 1 žingsnio, naudodami toliau nurodytą komandą:

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

4. Patvirtinkite parašo failą viešuoju raktu iš ankstesnio žingsnio, naudodami toliau nurodytą komandą:

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

PASTABA:

- Jei reikia sukurti tik parašo failą, būtini tik 1 ir 3 žingsniai.
- „HP Sure Recover“ būtini žingsniai yra 1, 2 ir 3. Jums reikalingas viešais raktas iš 2 žingsnio, kad galėtumėte konfigūruoti tikslinę sistemą.
- 4 žingsnis yra pasirenkamas ir rekomenduojamas, kad jūsų parašo failas ir deklaracijos failas būtų tinkamai patvirtintas.

Failų priegloba

Serveryje priglobkite šiuos failus iš C:\staging aplanko:

- *.swm
- custom.mft (arba failo pavadinimas, kurį pasirinkote deklaracijos failui)
- custom.sig (arba atitinkamas failo pavadinimas, kurį pasirinkote parašo failui)

PASTABA: jei kaip prieglobos sprendimą naudojate IIS, turite konfigūruoti MIME įrašus, kad juose būtų šie plėtiniai, sukonfigūruoti kaip „application/octet-stream:“

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

Tikslinių sistemų konfigūravimas

Tikslines sistemas galite konfigūruoti naudodami „HP Client Management Script Library“, „HP Client Security Manager“ (CSM) / „Sure Recover“ arba „Manageability Integration Kit“ (MIK) (https://www.hp.com/go/clientmanagement).

Konfigūracijai pateikite šią informaciją:

1. Ankstesniame skyriuje priglobto deklaracijos failo URL adresą (http://your_server.domain/path/custom.mft)
2. Viešąjį raktą, kurį naudojote patvirtindami anksčiau sukurtą parašo failą (pvz., C:\staging\my-recovery-public.pem).

Trikčių šalinimas

Jei gavote pranešimą, kad pasirinktinio atkūrimo procesui nepavyko patvirtinti saugos, patikrinkite šiuos dalykus:

1. Deklaracija turi būti UTF-8 be BOM.
2. Patikrinkite failų maišas.
3. Įsitikinkite, kad sistemai buvo pateiktas deklaracijos pasirašymui naudotą privatų raktą atitinkantis viešasis raktas.
4. IIS serverio MIME tipas turi būti `application/octet-stream`.
5. Deklaracijos failų keliuose turi būti visas kelias į svarbiausią katalogą, kuriame yra vaizdas matomas iš kliento sistemos. Šis kelias nėra visas kelias į paskirstymo vietą, kur saugomi failai.

3 „HP Sure Recover“ agento naudojimas įmonės užkardoje

„HP Sure Recover“ agentas gali būti priglobtas įmonės intranete. Įdiegę „HP Sure Recover“ naudojamą „SoftPaq“, nukopijuokite agento failus iš „HP Sure Recover“ agento katalogo diegimo vietoje į HTTP arba FTP paskirstymo vietą. Tada kliento sistemai pateikite paskirstymo vietos URL ir HP viešąjį raktą `hpsr_agent_public_key.pem`, kuris yra platinamas kartu su „HP Sure Recover“ agento „SoftPaq“.

„HP Sure Recover“ agento įdiegimas

1. Atsisiųskite „HP Sure Recover“ agentą ir išskleisite failus HTTP arba FTP paskirstymo vietoje.
2. Paskirstymo vietoje nustatykite atitinkamus failų leidimus.
3. Jei naudojate informacines interneto paslaugas „Internet Information Services“ (IIS), sukurkite application/octet-stream MIME tipus šiems failų formatams:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   SVARBU: toliau nurodytuose žingsniuose aprašomas „Sure Recover“ konfigūravimas su SCCM. Pavyzdžius, kaip konfigūruoti „Sure Recover“ su „HP Client Management Script Library“, žr. „Darbas su „HP Client Management Script Library“ (CMSL)“ 12 puslapyje.

4. Paleiskite SCCM, eikite į **HP Client Security Suite** ir pasirinkite „HP Sure Recover“ puslapį.

   PASTABA: paskirstymo vietos URL kaip perdavimo protokolą naudoja ftp arba http. Čia taip pat pateikiamas visas kelias į svarbiausią katalogą, kuriame yra „HP Sure Recover“ agento deklaracija, kokia matoma iš kliento sistemos. Šis kelias nėra visas kelias į paskirstymo vietą, kur saugomi failai.

5. Skyriuje **Platformos vaizdas** pasirinkite parinktį **Įmonė**, kad galėtumėte atkurti tinkintą OS vaizdą iš įmonės paskirstymo vietos. Įveskite IT administratoriaus pateiktą URL laukelyje **Vaizdo vietos URL**. Įveskite viešąjį raktą `hpsr_agent_public_key.pem` laukelyje **Vaizdo patvirtinimas**.

   PASTABA: pasirinktinio vaizdo URL turi apimti vaizdo deklaracijos failo pavadinimą.

6. Skyriuje **Atkūrimo agentas** pasirinkite parinktį **Įmonė**, kad galėtumėte naudoti tinkintą atkūrimo agentą arba HP atkūrimo agentą iš įmonės paskirstymo vietos. Įveskite IT administratoriaus pateiktą URL laukelyje **Agento vietos URL**. Įveskite viešąjį raktą `hpsr_agent_public_key.pem` laukelyje **Agento patvirtinimo raktas**.

PASTABA: neįtraukite į URL agento deklaracijos failo pavadinimo, nes BIOS būtina, kad jis būtų pavadintas recovery.mft.

7. Po to, kai politika pritaikoma kliento sistemai, paleiskite ją iš naujo.
8. Atliekant pirminę konfigūraciją parodomas raginimas įvesti 4 skaitmenų saugos kodą ir užbaigti „HP Sure Recover“ aktyvinimą. Jei reikia daugiau informacijos, apsilankykite hp.com ir ieškokite „HP Manageability Integration Kit“ (MIK) „Microsoft“ sistemos centro konfigūracijos tvarkyklės techninėje dokumentacijoje.

Kai „HP Sure Recover“ aktyvinimas bus sėkmingai baigtas, politikos pritaikytas pasirinktinis URL bus rodomas „HP Sure Recover“ BIOS nustatymų meniu.

Jei norite patvirtinti sėkmingą aktyvinimą, paleiskite kompiuterį iš naujo ir, kai pasirodys HP logotipas, paspauskite f10. Pasirinkite **Išplėstiniai**, pasirinkite **„HP Sure Recover“**, pasirinkite **Atkūrimo agentas**, tada pasirinkite **URL**.

4 Darbas su „HP Client Management Script Library“ (CMSL)

„HP Client Management Script Library“ suteikia galimybę tvarkyti „HP Sure Recover“ nustatymus naudojant „PowerShell“. Toliau pateikiamas scenarijaus pavyzdys rodo, kaip konfigūruoti, nustatyti būseną, keisti konfigūraciją ir nutraukti „HP Sure Recover“.

PASTABA: kelios komandos viršija šio vadovo eilutės ilgį, bet turi būti įvestos kaip viena eilutė.

```
$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
}
```

Pavyzdinis rakto generavimas naudojant OpenSSL

Privačius raktus laikykite saugioje vietoje. Viešieji raktai bus naudojami patvirtinimui ir turi būti pateikti konfigūruojant. Šie raktai turi būti 2048 bitų ilgio ir naudoti 0x10001 laipsnio rodiklį. Pakeiskite subjektą pavyzdžiuose informacija apie savo įmonę.

Prieš tęsdami nustatykite šį aplinkos kintamąjį:

```
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:
```

Vaizdo deklaraciją galite pasirašyti naudodami šią komandą:

```
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:
```

Agento deklaraciją galite pasirašyti naudodami šią komandą:

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

„OpenSSL“ sugeneruoja parašo failus mažėjančių baitų formatu, kuris yra nesuderinamas su kai kuriomis BIOS versijomis, todėl agento parašo failo baitų eiliškumą gali tekti pakeisti prieš įdiegiant. BIOS versijos, kurios palaiko mažėjančių baitų eiliškumą taip pat palaiko ir didėjančių baitų eiliškumą.

A Trikčių šalinimas

Disko išskaidyti nepavyko

Disko išskaidymas gali nepavykti, jei SR_AED arba SR_IMAGE skaidinys yra užšifruotas su „Bitlocker“. Šie skaidiniai paprastai kuriami su gpt atributu, kuris neleidžia „Bitlocker“ jų užšifruoti, bet jei naudotojas ištrina ir iš naujo atkuria skaidinius arba rankiniu būdu sukuria juos tuščiame metaliniame diske, tada „Sure Recover“ agentas negali jų ištrinti ir išsijungia pateikdamas disko išskaidymo klaidą. Naudotojas turi atlikti disko išskaidymą ir ištrinti juos rankiniu būdu, pasirenkant tūrį ir sukuriant `del vol` perrašymo komandą ar pan.

Programinės aparatinės įrangos įrašų žurnalas

EFI kintamojo informacija:

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

„Windows“ sistemoje yra API, kurios nuskaito EFI kintamuosius, arba galite iškelti kintamųjų turinį į failą panaudodami UEFI dmpstore priemonę.

Galite iškelti įrašų žurnalą naudodami `Get-HPFirmwareAuditLog` komandą, kurią pateikia „HP Client Management Script Library“.

„Windows“ įvykių žurnalas

„Sure Recover“ paleidimo ir sustabdymo įvykiai siunčiami į BIOS įrašų žurnalą, kurį galite peržiūrėti „Windows“ įvykių peržiūros programoje „Sure Start“ žurnale, jei yra įdiegti HP pranešimai. Šie įvykiai apima datą ir laiką, šaltinio ID, įvykio ID ir specifinį įvykio kodą. Pvz., `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` rodo, kad atkūrimas nepavyko, nes deklaracijos nepavyko patvirtinti specifiniu įvykio kodu c3f 23000, kuris buvo įrašytas 2:26:40, 6/27/18.

PASTABA: šiuose žurnaluose naudojamas JAV datos formatas – mėn./d./m.

„HP Secure Platform Management“ (šaltinio ID = 84h)

A-1 lentelė HP Secure Platform Management

Įvykio ID	Įrenginių skaičius (Visi/DaaS)	Įvykių skaičius (Visi/DaaS)	Aprašymas	Pastabos
40	256/178	943/552	Platformos OS atkūrimo procesą paleido programinė aparatinė įranga.	Platformos atkūrimas pradėtas
41	221/147	588/332	Platformos OS atkūrimo procesas sėkmingai užbaigtas.	Platformos atkūrimas baigtas
42	54/42	252/156	Platformos OS atkūrimo proceso nepavyko sėkmingai baigti.	Platformos atkūrimas nepavyko

Programinės aparatinės įrangos įrašų žurnalą galite gauti pasinaudodami „Get-HPFirmwareAuditLog“ iš „HP Client Management Script Library“, kurią rasite http://www.hp.com/go/clientmanagement. „HP Secure Platform Management“ įvykio ID 40, 41 ir 42 pateikia specifinius įvykių kodus duomenų lauke, kuris nurodo „Sure Recover“ operacijų rezultatą. Pvz., šis žurnalo įrašas rodo, kad „Sure Recover“ nepavyko atsisiųsti deklaracijos arba parašo failo klaida event_id 42 ir data: 00:30:F1:c3 turi būti interpretuojamas kaip dword reikšmė 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
```

Sėkmingas atkūrimas rodomas kaip event_id = 41 ir duomenys: 00:00:00:00, pavyzdžiui:

```
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: Platformos OS atkūrimo proceso nepavyko sėkmingai baigti.

data: 00:00:00:00
```

„HP Sure Recover“ naudoja šiuos įvykių kodus.

A-2 lentelė Specifiniai įvykių kodai

Įvykio aprašymas	Įvykio kodas
CatalogDownloadFailed	0xC3F11000
SignatureDownloadFailed	0xC3F12000
MftOrSigDownloadFailed	0xC3F13000
FtpHttpDownloadFailed	0xC3F14000

A-2 lentelė Specifiniai įvykių kodai (tęsinys)

Įvykio aprašymas	Įvykio kodas
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