Uživatelská příručka

HP Sure Recover

První vydání: únor 2020

Číslo dokumentu: L93434-221

Formátování uživatelských vstupů

Text, který musíte zadat do uživatelského rozhraní, je označen `neproporcionálním písmem`.

Tabulka -1 Formátování uživatelských vstupů

Položka	Popis
`Text bez závorek`	Položky musíte zadávat tak, jak jsou zobrazeny
`<Text uvnitř ostrých závorek>`	Zástupný objekt pro hodnotu, kterou musíte zadat; vynechte závorky
`[Text uvnitř hranatých závorek]`	Volitelné položky; vynechte závorky
`{Text uvnitř složených závorek}`	Sada položek, ze které si musíte vybrat jen jednu; vynechte závorky
`|`	Oddělovač položek, ze kterých si musíte vybrat jen jednu; vynechte svislou čáru
`...`	Položky, které se mohou nebo musí opakovat; vynechte výpustku

Obsah

1 Začínáme

Software HP Sure Recover vám pomůže bezpečně nainstalovat operační systém ze sítě s minimálním zásahem uživatele. Systémy s technologií HP Sure Recover s technologií Embedded Reimaging také podporují instalaci z místního paměťového zařízení.

DŮLEŽITÉ: Než použijete nástroj HP Sure Recover, zálohujte data. Vzhledem k tomu, že proces obnovení z bitové kopie disku přeformátuje jednotku, dojde ke ztrátě dat.

Bitové kopie pro obnovení, které společnost HP poskytuje, obsahují základní instalační soubor systému Windows 10®. V případě potřeby může nástroj HP Sure Recover nainstalovat optimalizované ovladače pro zařízení HP. Bitové kopie nástroje HP Recovery obsahují pouze agenty obnovování dat, které jsou součástí systému Windows 10, jako je OneDrive. Korporace mohou vytvářet své vlastní bitové kopie, které slouží k přidání korporátních nastavení, aplikací, ovladačů a agentů obnovování dat.

Agent obnovování operačního systému (OS) provádí kroky nezbytné k instalaci bitové kopie pro zotavení. Agent obnovování poskytovaný společností HP provádí běžné kroky, jako je vytváření oddílů, formátování a extrahování bitové kopie pro zotavení na cílové zařízení. Vzhledem k tomu, že agent obnovování HP je umístěn na webové stránce hp.com, budete k jeho získání potřebovat přístup k internetu, pokud systém nezahrnuje technologii Embedded Reimaging. Společnosti mohou také hostovat agenta obnovování HP v rámci jejich brány firewall nebo vytvořit vlastní agenty obnovování pro složitější prostředí obnovení.

Pokud není nalezen žádný operační systém, můžete aktivovat nástroj HP Sure Recover. Můžete také spustit nástroj HP Sure Recover podle plánu, např. abyste se ujistili, že došlo k odstranění malwaru. Proveďte konfiguraci těchto nastavení prostřednictvím nástroje HP Client Security Manager (CSM), Management Integration Kit (MIK) nebo knihovny HP Client Management Script Library.

Obnovení ze sítě

POZNÁMKA: Chcete-li provést obnovení ze sítě, musíte použít kabelové připojení. Společnost HP doporučuje před použitím nástroje HP Sure Recover zálohovat důležité soubory, data, fotografie, videa a tak dále, aby nedošlo ke ztrátě dat.

1. Připojte klientský systém k síti, ve které je přístup k distribučnímu bodu HTTP nebo FTP.
2. Restartujte systém klienta a jakmile se zobrazí logo HP, stiskněte klávesu f11.
3. Vyberte položku **Obnovení ze sítě**.

Obnovení z místní jednotky

Pokud systém klienta podporuje funkci Embedded Reimaging a naplánovaná bitová kopie je povolena v použitých zásadách, pak se bitová kopie stáhne do klientského systému v naplánovaném čase. Po stažení bitové kopie do klientského systému jej restartujte, aby se obraz zkopíroval do paměťového zařízení s funkcí Embedded Reimaging.

Chcete-li provést místní obnovení pomocí bitové kopie na paměťovém zařízení s funkcí Embedded Reimaging, postupujte takto:

1. Restartujte systém klienta a jakmile se zobrazí logo HP, stiskněte klávesu f11.
2. Vyberte položku **Obnovení z místní jednotky**.

Systémy s funkcí Embedded Reimaging musí konfigurovat plán stahování a používat agenta stahování ke kontrole aktualizací. Agent stahování je obsažen v doplňku HP Sure Recover pro nástroj HP Client Security Manager a může být také konfigurován v MIK. Pokyny k použití MIK naleznete v části https://www.hp.com/go/clientmanagement.

Můžete také vytvořit naplánovanou úlohu, která bude kopírovat agenta do oddílu SR_AED a bitové kopie do oddílu SR_IMAGE. Poté můžete použít nástroj HP Client Management Library a odeslat servisní událost informující systém BIOS, že by měl ověřit obsah a zkopírovat jej na paměťové zařízení s technologií Embedded Reimaging při příštím restartu.

2 Vytvoření korporátní bitové kopie

Většina společností používá nástroje Microsoft Deployment, Windows 10 Assessment and Deployment Kit nebo obojí k výrobě souborů obsahujících bitovou kopii v archivu formátu souborů WIM (Windows Imaging).

Požadavky

- Nejnovější verze Windows 10 Assessment and Deployment Kit (Windows ADK)
- PowerShell
- OpenSSL (nebo jiné řešení pro generování páru soukromého/veřejného klíče RSA)

  Slouží ke generování páru klíčů RSA, který se používá k zajištění integrity korporátní bitové kopie, kterou vytváříte a hostujete.
- Server hostující řešení (například Microsoft Internet Information Services [IIS])

Vytvoření bitové kopie

Před zahájením procesu vytváření bitové kopie nastavte pracovní systém nebo systém sestavení, kde jste nainstalovali požadované nástroje, abyste se připravili na zpracování bitové kopie, jak je znázorněno v následujících krocích:

1. Jako správce otevřete příkazový řádek nástroje `Deployment and Imaging` (nainstalován s nástroji pro nasazení systému Windows ADK).
2. Vytvořte pracovní oblast pro bitovou kopii pomocí následujícího příkazu:

   ```
   mkdir C:\staging
   ```
3. Vytvořte bitovou kopii pomocí jednoho z následujících příkladů:

   Příklad 1: Vytvoření bitové kopie založené na bitové kopii instalace systému Microsoft Windows na stránce 3

   Příklad 2: Vytvoření bitové kopie založené na referenčním systému na stránce 5

Příklad 1: Vytvoření bitové kopie založené na bitové kopii instalace systému Microsoft Windows

1. Vložte nebo otevřete bitovou kopii instalace systému Microsoft Windows (z aplikace Microsoft ISO nebo z aplikace HP OSDVD).
2. Z vložené bitové kopie instalace systému Windows zkopírujte soubor install.wim do pracovní oblasti pomocí následujícího příkazu:

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

   POZNÁMKA: `< M: >` odkazuje na vloženou jednotku. Nahraďte správným písmenem jednotky.
3. Přejmenujte soubor install. wim na název souboru bitové kopie („My-Image“ pro tento příklad) pomocí následujícího příkazu:

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

(Volitelné) Software HP Sure Recover obsahuje funkci pro obnovení konkrétní edice z bitové kopie s více indexy, která je založena na edici Windows původně licencované pro cílový systém HP u výrobce. Tento mechanismus funguje, pokud jsou indexy správně pojmenovány. Pokud vaše bitová kopie instalace systému Windows pochází z bitové kopie HP OSDVD, budete pravděpodobně mít bitovou kopii s více edicemi. Pokud si to nepřejete a chcete zajistit, aby byla jedna konkrétní edice použita pro všechny cílové systémy, musíte mít jistotu, že bitová kopie instalace bude mít pouze jeden index.

4. Zkontrolujte obsah bitové kopie instalace pomocí následujícího příkazu:

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

   Následující příklad zobrazuje ukázkový výstup z bitové kopie instalace, která podporuje pět edic (bude odpovídat podle systému BIOS každého cílového systému):

   Podrobnosti o bitové kopii: `my-image.wim`

   Index: `1`

   Název: `CoreSingleLanguage`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Home Single Language`

   Velikost: `19 512 500 682 bajtů`

   Index: `2`

   Název: `Core`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Home`

   Velikost: `19 512 500 682 bajtů`

   Index: `3`

   Název: `Professional`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Professional`

   Velikost: `19 758 019 520 bajtů`

   Index: `4`

   Název: `ProfessionalEducation`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Professional Education`

   Velikost: `19 758 019 480 bajtů`

   Index: `5`

   Název: `ProfessionalWorkstation`

   Popis: `Aktualizace Windows 10, květen 2019 – edice Professional Workstation`

   Velikost: `19 758 023 576 bajtů`

POZNÁMKA: Je-li k dispozici pouze jeden index, bitová kopie bude použita pro obnovení bez ohledu na název. Velikost souboru bitové kopie může být větší než před odstraněním.

5. Pokud nechcete více edic, odstraňte každý index, který nechcete.

   Jak je znázorněno v následujícím příkladu, pokud chcete pouze edici Professional (za předpokladu, že jsou všechny cílové systémy licencovány), odstraňte index 5, 4, 2 a 1. Pokaždé, když odstraníte index, budou čísla indexu znovu přiřazena. Proto byste měli odstraňovat indexy od nejvyššího po nejnižší číslo. Po každém odstranění spusťte příkaz `Get-ImageInfo`, abyste vizuálně potvrdili, který index budete dále odstraňovat.

   ```
   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
   ```

   Zvolte pouze jeden index edice (například Professional). Je-li k dispozici pouze jeden index, bitová kopie bude použita pro obnovení bez ohledu na název. Uvědomte si, že velikost souboru bitové kopie může být větší než před odstraněním kvůli způsobu, jakým se provádějí změny metadat WIM a normalizace obsahu.

6. (Volitelné) Chcete-li zahrnout ovladače do korporátní bitové kopie pro obnovení, postupujte následovně:

   a. Bitovou kopii vložte do prázdné složky pomocí následujících příkazů:

   ```
   mkdir C:\staging\mount

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

   b. Vložte příslušný disk DVD s ovladači HP Windows 10 (DRDVD) pro podporovaný cílový systém. Z vložených médií ovladače zkopírujte podsložky ovladače do své pracovní oblasti pomocí následujícího příkazu:

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

   POZNÁMKA: `< M: >` odkazuje na vloženou jednotku. Nahraďte správným písmenem jednotky.

   Do složky C:\staging\mount\SWSETUP\DRV můžete umístit další ovladače typu .inf. Chcete-li získat vysvětlení o tom, jak je tento obsah zpracován nástrojem HP Sure Recover pomocí funkce `dism /Add-Driver /Recurse`, přečtěte si část „Přidání a odebrání ovladačů do offline bitové kopie systému Windows" v následujícím tématu: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Tato funkce nepodporuje ovladače typu .exe, které vyžadují spuštění aplikace.

   c. Uložte změny a odpojte bitovou kopii pomocí následujícího příkazu:

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

   Výsledný soubor bitové kopie je: C:\staging\my-image.wim.

   d. Přejděte na Rozdělení bitové kopie na stránce 6.

Příklad 2: Vytvoření bitové kopie založené na referenčním systému

1. Vytvořte spustitelné médium USB WinPE.

POZNÁMKA: Další metody snímání bitové kopie naleznete v dokumentaci ADK.

Ujistěte se, zda je na jednotce USB dostatek volného místa pro uložení vytvořené bitové kopie z referenčního systému.

2. Vytvoření bitové kopie z referenčního systému
3. Bitovou kopii vytvořte spuštěním referenčního systému s médiem USB WinPE a poté použijte nástroj DISM.

POZNÁMKA: `< U: >` odkazuje na jednotku USB. Nahraďte správným písmenem jednotky.

Podle potřeby upravte část názvu souboru „my-image" a popis `<my-image>`.

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

4. Zkopírujte bitovou kopii z paměťového zařízení USB do pracovní oblasti vašeho pracovního systému pomocí následujícího příkazu:

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

   Měli byste mít následující soubor bitové kopie: C:\staging\my-image.wim.

5. Přejděte na Rozdělení bitové kopie na stránce 6.

Rozdělení bitové kopie

Společnost HP doporučuje, abyste pomocí následujícího příkazu rozdělili bitovou kopii na menší soubory a zlepšili tak spolehlivost stahování ze sítě:

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

POZNÁMKA: Velikost souboru je uvedena v megabajtech. Podle potřeby upravte.

POZNÁMKA: Vzhledem k povaze algoritmu rozdělování DISM může být velikost generovaných souborů SWM menší nebo větší než uvedená velikost souboru.

Vytvoření manifestu

Zformátujte soubory manifestu jako UTF-8 bez značky pořadí bajtů (BOM).

Můžete změnit název souboru manifestu (custom.mft), který se používá v následujících postupech, ale nesmíte měnit přípony .mft a .sig a název souboru části manifestu a podpisu se musí shodovat. Můžete například změnit pár (custom.mft, custom.sig) na (myimage.mft, myimage.sig).

`mft_version` se používá k určení formátu souboru bitové kopie a musí být aktuálně nastaven na hodnotu 1.

`image_version` se používá k určení, zda je k dispozici novější verze bitové kopie a k zabránění instalace starších verzí.

Obě hodnoty musí být 16bitová celá čísla bez znaménka a oddělovač řádků v manifestu musí být `'\r\n'` `(CR + LF)`.

Generování manifestu

Vzhledem k tomu, že součástí rozdělené bitové kopie může být několik souborů, vygenerujte manifest pomocí skriptu PowerShell.

U všech zbývajících kroků musíte být ve složce C:\staging.

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

1. Vytvořte skript PowerShell pomocí editoru, který může vytvořit textový soubor ve formátu UTF-8 bez BOM, a to pomocí následujícího příkazu: `notepad C:\staging\generate-manifest.ps1`

   Vytvořte následující skript:

```
$mftFilename = "custom.mft"

$imageVersion = 1907 (Poznámka: Může to být libovolné 16bitové celé číslo)


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

Out-File -Encoding UTF8 -FilePath $mftFilename -InputObject $header

$swmFiles = Get-ChildItem "." -Filter "*.swm"

$ToNatural = { [regex]::Replace($_, '\d*\....$',
{ $args[0].Value.PadLeft(50) }) }


$pathToManifest = (Resolve-Path ".").Path


$total = $swmFiles.count

$current = 1


$swmFiles | Sort-Object $ToNatural | ForEach-Object {

    Write-Progress

        -Activity "Generating manifest" `

        -Status "$current of $total ($_)" `

        -PercentComplete ($current / $total * 100)


    $hashObject = Get-FileHash -Algorithm SHA256 -Path $_.FullName

    $fileHash = $hashObject.Hash.ToLower()

    $filePath = $hashObject.Path.Replace($pathToManifest + '\', '')

    $fileSize = (Get-Item $_.FullName).length

    $manifestContent = "$fileHash $filePath $fileSize"


    Out-File -Encoding utf8 -FilePath $mftFilename -InputObject
$manifestContent -Append
```

```
    $current = $current + 1
}
```

POZNÁMKA: Manifesty pro nástroj HP Sure Recover nemohou obsahovat BOM, takže následující příkazy přepisují soubor jako UTF8 bez BOM.

```
$content = Get-Content $mftFilename

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

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

2. Uložte skript.
3. Spusťte skript.

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

Generování podpisu manifestu

Nástroj Sure Recovery ověřuje agenta a bitovou kopii pomocí kryptografických podpisů. Následující příklady používají pár soukromých/veřejných klíčů ve formátu X.509 PEM (přípona.PEM). Podle potřeby upravte příkazy pro použití binárních certifikátů DER (přípony .CER nebo.CRT), kódovaných certifikátů BASE-64 PEM (přípony .CER nebo. CRT), nebo souborů PKCS1 PEM (přípona. PEM). Příklad také používá OpenSSL, který generuje podpisy ve formátu big-endian. K podepisování manifestů můžete použít libovolný nástroj, ale některé verze systému BIOS podporují pouze podpisy ve formátu little endian.

1. Pomocí následujícího příkazu vygenerujte soukromý klíč RSA 2048 bajtů. Máte-li ve formátu .pem pár soukromých/veřejných klíčů 2048 bajtů RSA, zkopírujte jej do C:\staging a poté přejděte ke kroku 3.

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

2. Vygenerujte veřejný klíč z vašeho soukromého klíče (pokud máte veřejný klíč odpovídající vašemu soukromému klíči ve formátu PEM, zkopírujte jej do C:\staging) pomocí následujícího příkazu:

   ```
   OpenSSL RSA-in my-Recovery-Private. pem-pubout-out my-Recovery-Public.
   pem
   ```

3. Vytvořte soubor s podpisem (pomocí hash algoritmu SHA256) na základě soukromého klíče RSA 2048 bajtů z kroku 1 pomocí následujícího příkazu:

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

4. Ověřte soubor s podpisem pomocí veřejného klíče z předchozího kroku pomocí následujícího příkazu:

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

POZNÁMKA:

- Pokud potřebujete vytvořit pouze soubor s podpisem, jsou požadované kroky 1 a 3.
- Pro nástroj HP Sure Recover jsou minimální požadované kroky 1, 2 a 3. Pro zajištění cílového systému budete potřebovat veřejný klíč z kroku 2.
- Krok 4 je volitelný, ale doporučuje se, aby soubor s podpisem a soubor manifestu správně ověřovaly.

Hostování souborů

Na serveru hostujte následující soubory ze složky C:\staging:

- *.swm
- custom.mft (nebo název souboru, který jste zvolili pro soubor manifestu)
- custom.sig (nebo odpovídající název souboru, který jste zvolili pro soubor signatury)

POZNÁMKA: Pokud používáte službu IIS jako své hostitelské řešení, musíte nakonfigurovat položky MIME tak, aby obsahovaly následující přípony, které jsou všechny konfigurovány jako „aplikace/octet-stream:“

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

Zřízení cílových systémů

Své cílové systémy můžete zřídit pomocí nástrojů HP Client Management Script Library, HP Client Security Manager (CSM)/Sure Recover nebo Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Pro toto zřízení uveďte následující informace:

1. Adresa URL souboru manifestu hostovaného v předchozí části (http://your_server.domain/path/custom.mft)
2. Veřejný klíč použitý k ověření dříve vytvořeného souboru s podpisem (například C:\staging\my-recovery-public.pem).

Odstraňování potíží

Pokud se zobrazí zpráva o procesu vlastního obnovení, který selhal při ověřování zabezpečení, zkontrolujte následující:

1. Manifest musí být UTF-8 bez BOM.
2. Zkontrolujte hash soubory.
3. Zkontrolujte, zda byl systém zřízen s veřejným klíčem odpovídajícím soukromému klíči používanému k podepsání manifestu.
4. Typy MIME serveru služby IIS musí být `application/octet-stream`.
5. Cesty k souborům v rámci manifestu musí obsahovat úplnou cestu k vrchnímu adresáři s bitovou kopií, jak je vidět ze systému klienta. Tato cesta nepředstavuje úplnou cestu, kde se soubory ukládají v distribučním bodě.

3 Použití nástroje HP Sure Recover Agent v rámci korporátního firewallu

Nástroj HP Sure Recover Agent může být hostován v korporátní síti intranet. Po instalaci HP Sure Recover SoftPaq zkopírujte soubory agenta z adresáře HP Sure Recover Agent z umístění instalace do distribučního bodu HTTP nebo FTP. Poté zřiďte systém klienta s adresou URL distribučního bodu a veřejným klíčem HP nazvaným `hpsr_agent_public_key. pem`, který je distribuován s agentem HP Sure Recover SoftPaq.

Instalace agenta HP Sure Recover

1. Stáhněte si agenta HP Sure Recover a rozbalte soubory do distribučního bodu HTTP nebo FTP.
2. Nastavte odpovídající oprávnění pro soubory na distribučním bodu.
3. Pokud používáte internetovou informační službu (IIS), vytvořte typy application/octet-stream pro následující formáty souborů:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   DŮLEŽITÉ: Následující kroky popisují zajištění nástroje Sure Recover pomocí SCCM. Příklady zajištění nástroje Sure Recover pomocí nástroje HP Client Management Script Library naleznete v části Práce s nástrojem HP Client Management Script Library (CMSL) na stránce 12.
4. Spusťte nástroj SCCM, přejděte na položku **HP Client Security Suite** a poté vyberte stránku HP Sure Recover.

   POZNÁMKA: Adresa URL distribučního bodu obsahuje jako protokol přenosu buď ftp nebo http. Obsahuje také úplnou cestu k vrchnímu adresáři, který obsahuje manifest pro agenta HP Sure Recover, jak je vidět z klientského systému. Tato cesta nepředstavuje úplnou cestu k umístění souborů v distribučním bodu.
5. V části **Platform Image** (Platforma bitové kopie) vyberte možnost **Corporate** (Korporátní), která obnoví bitovou kopii operačního systému z korporátního distribučního bodu. Zadejte adresu URL poskytnutou správcem IT do pole **Image Location URL** (Adresa URL umístění bitové kopie). Do pole **Image Verification** (Ověření bitové kopie) zadejte veřejný klíč `hpsr_agent_public_key. pem`.

   POZNÁMKA: Adresa URL vlastní bitové kopie musí obsahovat název souboru manifestu bitové kopie.
6. V části **Recovery Agent** (Agent obnovování) vyberte možnost **Corporation** (Korporátní), abyste mohli používali vlastního agenta obnovení nebo agenta obnovení HP z podnikového distribučního bodu. Zadejte adresu URL poskytnutou správcem IT do pole **Agent Location URL** (URL adresa umístění

agenta). Zadejte veřejný klíč `hpsr_agent_public_key.pem` do pole **Agent Verification Key** (Klíč k ověření agenta).

POZNÁMKA: Nezahrnujte název souboru manifestu agenta do adresy URL, protože systém BIOS vyžaduje, aby byl pojmenován recovery.mft.

7. Po použití zásady na systém klienta proveďte jeho restart.
8. Během úvodního zajišťování se zobrazí výzva k zadání bezpečnostního kódu se čtyřmi číslicemi, aby bylo možno dokončit aktivaci nástroje HP Sure Recover. Chcete-li získat další informace, přejděte na web hp.com a vyhledejte dokument HP Manageability Integration Kit (MIK) for Microsoft System Center Manager.

Po úspěšném dokončení aktivace nástroje HP Sure Recover se v nabídce nastavení nástroje HP Sure Recover BIOS zobrazí vlastní adresa URL aplikovaná zásadami.

Chcete-li potvrdit úspěšnost aktivace, restartujte počítač a jakmile se zobrazí logo HP, stiskněte klávesu f10. Vyberte položku **Advanced** (Pokročilé), vyberte položku **HP Sure Recover**, vyberte položku **Recovery Agent** (Agent obnovení) a poté vyberte položku **URL**.

4 Práce s nástrojem HP Client Management Script Library (CMSL)

Nástroj HP Client Management Script Library umožňuje spravovat nastavení nástroje HP Sure Recover pomocí skriptu PowerShell. Následující příklad skriptu ukazuje, jak zřizovat, určovat stav, měnit konfiguraci a rušit zajištění nástroje HP Sure Recover.

POZNÁMKA: Několik příkazů překračuje délku řádku této příručky, ale musí být zadáno jako jeden řádek.

```
$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
}
```

Generování ukázkových klíčů pomocí OpenSSL

Soukromé klíče uložte na bezpečném místě. Veřejné klíče budou použity k ověření a musí být poskytnuty během zajišťování. Tyto klíče musí být dlouhé 2048 bajtů a musí používat exponent 0x10001. Nahraďte předmět v příkladech informacemi o vaší organizaci.

Než budete pokračovat, nastavte následující proměnnou prostředí:

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

# Vytvoření certifikátu kořenové certifikační autority podepsaného svým držitelem pro testování
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"

# Vytvoření klíče certifikátu potvrzení
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:


# Vytvoření podpisového klíče příkazu

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:


# Vytvoření podpisového klíče bitové kopie

openssl req -sha256 -nodes -newkey rsa:2048 -keyout os.key -out os.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in os.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out os.crt

openssl pkcs12 -inkey os.key -in os.crt -export -out os.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Manifest bitové kopie můžete podepsat pomocí tohoto příkazu:

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


# Vytvoření podpisového klíče agenta

openssl req -sha256 -nodes -newkey rsa:2048 -keyout re.key -out re.csr -
subj "/C=US/ST=State/L=City/O=Company/OU=Org/CN=www.example.com"

openssl x509 -req -sha256 -in re.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out re.crt

openssl pkcs12 -inkey re.key -in re.crt -export -out re.pfx -CSP
"Microsoft Enhanced RSA and AES Cryptographic Provider" -passout pass:
```

Manifest agenta můžete podepsat pomocí tohoto příkazu:

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

OpenSSL vytváří soubory podpisů ve formátu big-endian, který není kompatibilní s některými verzemi systému BIOS, takže pořadí bajtů souborů podpisů agenta může být nutné před nasazením stornovat. Verze systému BIOS, které podporují pořadí bytů big-endian, také podporují pořadí bytů little-endian.

A Odstraňování potíží

Rozdělování jednotky se nezdařilo

K selhání rozdělování jednotky může dojít v případě, že je oddíl SR_AED nebo SR_IMAGE zašifrován pomocí nástroje BitLocker. Tyto oddíly jsou obvykle vytvářeny s atributem gpt, který zamezuje nástroji BitLocker jejich šifrování, ale v případě, že uživatel odstraní a znovu vytvoří oddíly nebo je vytvoří ručně na holém kovovém disku, agent Sure Recovery při opětovném rozdělování disku nedokáže odstranit a skočí s chybou. Uživatel je musí ručně odstranit spuštěním nástroje diskpart, výběrem svazku a vykonáním příkazu `del vol` nebo podobného.

Protokol auditu firmwaru

Informace o proměnné EFI jsou následující:

- GUID: `{0xec8feb88, 0xb1d1, 0x4f0f, {0xAB, 0x9F, 0x86, 0xCD, 0xB5, 0x3e, 0xa4, 0x45}}`
- Název: `OsRecoveryInfoLog`

Rozhraní API existují v systému Windows pro čtení proměnných EFI, nebo můžete vypsat proměnný obsah do souboru pomocí nástroje UEFI Shell dmpstore.

Protokol auditu můžete vypsat pomocí příkazu `Get-HPFirmwareAuditLog`, který je součástí knihovny skriptů HP Client Management.

Protokolu událostí systému Windows

Události obnovení spuštění a zastavení nástroje Sure Recover jsou odesílány do protokolu auditu systému BIOS, který lze zobrazit v nástroji Prohlížeč událostí systému Windows v protokolu Sure Start, je-li nainstalována aplikace HP Notifications. Mezi tyto události patří datum a čas, ID zdroje, ID události a specifický kód události. Například `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 F2 C3]` označuje, že obnovení se nezdařilo, protože manifest nelze ověřit pomocí specifického kódu c3f 23000, který byl zaznamenán v 2:26:40 dne 6/27/18.

POZNÁMKA: Tyto protokoly se řídí AMERICKÝM formátem data měsíc/den/rok.

HP Secure Platform Management (zdroj ID = 84h)

Tabulka A-1 HP Secure Platform Management

ID události	Počet zařízení (Vše/DaaS)	Počet událostí (Vše/DaaS)	Popis	Poznámky
40	256/178	943/552	Proces obnovení platformy OS byl spuštěn firmwarem.	Spuštění obnovení platformy

Tabulka A-1 HP Secure Platform Management (pokračování)

ID události	Počet zařízení (Vše/DaaS)	Počet událostí (Vše/DaaS)	Popis	Poznámky
41	221/147	588/332	Proces obnovení platformy OS byl úspěšně dokončen.	Obnovení platformy dokončeno
42	54/42	252/156	Proces obnovení operačního systému platformy se nepodařilo úspěšně dokončit.	Obnovení platformy se nezdařilo

Protokol auditu firmwaru můžete načíst pomocí funkce Get-HPFirmwareAuditLog v nástroji HP Client Management Script Library, který je k dispozici na adrese http://www.hp.com/go/clientmanagement. ID události nástroje HP Secure Platform Management 40, 41 a 42 vrací specifické kódy událostí v datovém poli, které označují výsledek operací nástroje Sure Recover. Například následující položka protokolu indikuje, zda nástroj Sure Recover selhal při stažení souboru manifestu nebo podpisu s chybou event_id 42 a daty: 00:30:f1:c3, což by mělo být interpretováno jako hodnota dword 0xC3F13000 = MftOrSigDownloadFailed.

```
message_number: 0

závažnost: Informace

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 42

timestamp_is_exact: 1

časové razítko: 5/27/2019 2:44:18 PM

popis: Proces obnovení operačního systému platformy se nepodařilo úspěšně
dokončit.

data: 00:30:f1:c3
```

Úspěšné obnovení je zobrazeno jako event_id = 41 a daty: 00:00:00:00, například:

```
Specifické kódy událostí

Úspěch = 0x00000000

CatalogDownloadFailed = 0xC3F11000

message_number: 0

závažnost: Informace

system_state_at_event: S0

source_id: HP Secure Platform Management

event_id: 41

timestamp_is_exact: 1

časové razítko: 5/27/2019 2:55:41 PM

popis: Proces obnovení operačního systému platformy se nepodařilo úspěšně
dokončit.

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

Nástroj HP Sure Recover používá následující specifické kódy událostí.

Tabulka A-2 Specifické kódy událostí

Popis události	Kód události
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