Hướng dẫn sử dụng

HP Sure Recover

Ấn bản lần đầu: Tháng 2 năm 2020

Mã Bộ phận Tài liệu: L93434-EP1

Mã cú pháp do người dùng nhập

Văn bản bạn phải nhập vào giao diện người dùng được chỉ dẫn theo `phông chữ có chiều rộng cố định`.

Bảng -1 Mã cú pháp do người dùng nhập

Mục	Mô tả
`Văn bản không có dấu ngoặc hoặc dấu ngoặc nhọn`	Mục bạn phải nhập đúng như minh họa
`<Văn bản bên trong dấu ngoặc nhọn>`	Chỗ dành sẵn cho giá trị bạn phải cung cấp; bỏ qua dấu ngoặc
`[Văn bản bên trong dấu ngoặc vuông]`	Mục tùy chọn; bỏ qua dấu ngoặc
`{Văn bản bên trong dấu ngoặc nhọn}`	Một nhóm các mục để bạn chỉ chọn ra một; bỏ qua dấu ngoặc nhọn
`|`	Một dấu tách cho các mục để bạn chỉ chọn ra một; bỏ qua thanh dọc
`...`	Các mục có thể hoặc phải lặp lại; bỏ qua dấu chấm lửng

Mục lục

1 Bắt đầu

HP Sure Recover giúp bạn cài đặt hệ điều hành một cách an toàn từ mạng với sự tương tác tối thiểu của người dùng. Các hệ thống được cài đặt HP Sure Recover có tính năng Embedded Reimaging (Tạo lại ảnh Tích hợp) cũng hỗ trợ cài đặt từ một thiết bị lưu trữ cục bộ.

QUAN TRỌNG: Sao lưu dữ liệu của bạn trước khi sử dụng HP Sure Recover. Vì quá trình tạo ảnh sẽ định dạng lại ổ đĩa nên sẽ bị mất dữ liệu.

Ảnh phục hồi do HP cung cấp bao gồm cả trình cài đặt Windows 10® cơ bản. Cách khác, HP Sure Recover có thể cài đặt các trình điều khiển được tối ưu hóa cho thiết bị của HP. Ảnh phục hồi của HP chỉ chứa các tác nhân phục hồi dữ liệu được trang bị cùng Windows 10, chẳng hạn như OneDrive. Doanh nghiệp có thể tự tạo ảnh tùy chỉnh để thêm thiết đặt, ứng dụng, trình điều khiển và tác nhân phục hồi dữ liệu của riêng doanh nghiệp.

Tác nhân phục hồi hệ điều hành (HĐH) thực hiện các bước cần thiết để cài đặt ảnh phục hồi. Tác nhân phục hồi do HP cung cấp thực hiện các bước thông thường như phân vùng, định dạng và trích xuất ảnh phục hồi sang thiết bị đích. Do tác nhân phục hồi HP có trên địa chỉ hp.com nên bạn cần có truy cập Internet để truy xuất, trừ khi hệ thống được tích hợp sẵn tính năng tạo lại ảnh. Doanh nghiệp cũng có thể lưu trữ tác nhân phục hồi HP bên trong tường lửa của mình hoặc tạo các tác nhân phục hồi tùy chỉnh cho các môi trường phục hồi phức tạp hơn.

Bạn có thể khởi chạy HP Sure Recover khi không tìm thấy hệ điều hành nào. Bạn cũng có thể chạy HP Sure Recover định kỳ để đảm bảo loại bỏ phần mềm độc hại. Thực hiện cấu hình các thiết đặt này thông qua Trình quản lý Bảo mật Máy khách HP (CSM), Bộ công cụ Tích hợp Khả năng quản lý (MIK) hoặc Thư viện Script Quản lý Máy khách HP.

Thực hiện phục hồi mạng

GHI CHÚ: Để thực hiện phục hồi mạng, bạn phải sử dụng kết nối có dây. HP khuyến cáo nên sao lưu tập tin, dữ liệu, ảnh, video, v.v. trước khi sử dụng HP Sure Recover để tránh bị mất dữ liệu.

1. Kết nối hệ thống máy khách với mạng cho phép truy cập điểm phân phối HTTP hoặc FTP.
2. Khởi động lại hệ thống máy khách và khi logo HP xuất hiện, nhấn f11.
3. Chọn **Restore from network** (Phục hồi từ mạng).

Thực hiện phục hồi ổ đĩa cục bộ

Nếu hệ thống máy khách có hỗ trợ tạo lại ảnh tích hợp và đã bật tùy chọn tải xuống ảnh theo lịch đã lập trên chính sách áp dụng, ảnh được tải xuống hệ thống máy khách theo thời gian đã lên lịch. Sau khi ảnh được tải xuống hệ thống máy khách, khởi động lại hệ thống để sao chép ảnh sang thiết bị lưu trữ Embedded Reimaging (Tạo lại ảnh Tích hợp).

Để thực hiện phục hồi cục bộ bằng ảnh trên thiết bị lưu trữ Embedded Reimaging (Tạo lại ảnh Tích hợp):

1. Khởi động lại hệ thống máy khách và khi logo HP xuất hiện, nhấn f11.
2. Chọn **Restore from local drive** (Phục hồi từ ổ đĩa cục bộ).

Các hệ thống có tính năng Embedded Reimaging (Tạo lại ảnh Tích hợp) phải cấu hình lịch tải xuống và sử dụng tác nhân tải xuống để kiểm tra xem có cập nhật không. Tác nhân tải xuống được tích hợp sẵn trong Trình cắm HP Sure Recover cho Trình quản lý Bảo mật Máy khách HP và cũng có thể được cấu hình trong MIK. Xem https://www.hp.com/go/clientmanagement để biết hướng dẫn cách sử dụng MIK.

Bạn cũng có thể tạo một tác vụ được lên lịch để sao chép tác nhân này sang phân vùng SR_AED và ảnh sang phân vùng SR_IMAGE. Sau đó bạn có thể sử dụng Thư viện Script Quản lý Máy khách HP để gửi sự kiện dịch vụ báo cho BIOS biết rằng nó cần xác thực nội dung và sao chép sang thiết bị lưu trữ tạo lại ảnh tích hợp ở lần khởi động lại tiếp theo.

2 Tạo ảnh cho doanh nghiệp

Phần lớn các doanh nghiệp sử dụng các Công cụ Triển khai của Microsoft, bộ công cụ Đánh giá và Triển khai dành cho Windows 10 hoặc cả hai để tạo các tập tin chứa ảnh trên kho lưu trữ định dạng tập tin Windows Imaging (WIM).

Yêu cầu

- Phiên bản mới nhất của Bộ công cụ Đánh giá và Triển khai dành cho Windows 10 (Windows ADK)
- PowerShell
- OpenSSL (hoặc giải pháp khác để tạo cặp khóa riêng/chung RSA)

  Sử dụng để tạo cặp khóa RSA dùng để bảo vệ tính toàn vẹn của ảnh cho doanh nghiệp do bạn tạo ra và lưu trữ.
- Giải pháp lưu trữ máy chủ (chẳng hạn như Dịch vụ Thông tin Internet Microsoft [IIS])

Tạo ảnh

Trước khi bắt đầu quá trình tạo ảnh, cài đặt hệ thống làm việc hoặc xây dựng hệ thống để bạn cài đặt các công cụ cần thiết để chuẩn bị xử lý ảnh, như trình bày ở các bước sau:

1. Là Quản trị viên, mở dấu nhắc lệnh `Deployment and Imaging Tools Environment` (Môi trường Công cụ Triển khai và Tạo ảnh) (được cài đặt cùng với các Công cụ Triển khai của Windows ADK).
2. Tạo một khu vực tách chuyển cho ảnh của bạn bằng lệnh sau:

   ```
   mkdir C:\staging
   ```
3. Tạo ảnh bằng cách sử dụng một trong các ví dụ sau:

   Ví dụ 1: Tạo ảnh dựa trên ảnh bản cài đặt Microsoft Windows thuộc trang 3

   Ví dụ 2: Tạo ảnh dựa trên một hệ thống tham chiếu thuộc trang 5

Ví dụ 1: Tạo ảnh dựa trên ảnh bản cài đặt Microsoft Windows

1. Gắn hoặc mở ảnh bản cài đặt Microsoft Windows (từ một Microsoft ISO hoặc từ một HP OSDVD).
2. Từ ảnh bản cài đặt Windows đã gắn, sao chép tập tin install.wim vào khu vực tách chuyển bằng lệnh sau:

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

   GHI CHÚ: `<M:>` là ổ đĩa đã gắn. Thay thế bằng ký tự ổ đĩa phù hợp.
3. Đặt lại tên install.wim thành tên tập tin ảnh ("my-image" cho ví dụ này), bằng lệnh sau:

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

(Tùy chọn) HP Sure Recover có tính năng phục hồi một phiên bản đặc biệt từ một ảnh đa chỉ mục, dựa trên phiên bản Windows được cấp phép ban đầu cho hệ thống đích của HP tại nhà máy. Cơ chế này hoạt động khi các chỉ mục được đặt tên chính xác. Nếu ảnh bản cài đặt Windows của bạn lấy từ ảnh HP OSDVD, bạn nhiều khả năng sẽ có một ảnh đa phiên bản. Nếu bạn không muốn có hoạt động này và muốn đảm bảo sẽ sử dụng một phiên bản cụ thể cho tất cả các hệ thống đích của bạn, bạn cần đảm bảo rằng chỉ có một chỉ mục trong ảnh bản cài đặt.

4. Kiểm tra nội dung của ảnh bản cài đặt bằng cách sử dụng lệnh sau:

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

   Phần dưới đây trình bày mẫu kết quả của một ảnh bản cài đặt có hỗ trợ năm phiên bản (sẽ được khớp dựa trên BIOS của từng hệ thống đích):

   Chi tiết về ảnh: `my-image.wim`

   Chỉ mục: `1`

   Tên: `CoreSingleLanguage`

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

   Kích thước: `19.512.500.682 byte`

   Chỉ mục: `2`

   Tên: `Core`

   Mô tả: `Windows 10 May 2019 Update - Home edition`

   Kích thước: `19.512.500.682 byte`

   Chỉ mục: `3`

   Tên: `Professional`

   Mô tả: `Windows 10 May 2019 Update- Professional Update`

   Kích thước: `19.758.019.520 byte`

   Chỉ mục: `4`

   Tên: `ProfessionalEducation`

   Mô tả: `Windows 10 May 2019 Update - Professional Education edition`

   Kích thước: `19.758.019.480 byte`

   Chỉ mục: `5`

   Tên: `ProfessionalWorkstation`

   Mô tả: `Windows 10 May 2019 Update - Professional Workstation edition`

   Kích thước: `19.758.023.576 byte`

GHI CHÚ: Khi chỉ có một chỉ mục, ảnh được sử dụng để phục hồi, bất kể tên là gì. Kích thước tập tin ảnh của bạn có thể lớn hơn so với trước khi xóa.

5. Nếu bạn không muốn có hoạt động đa phiên bản, xóa từng chỉ mục mà bạn không muốn có đi.

   Như trình bày ở ví dụ dưới đây, nếu bạn chỉ muốn phiên bản Professional (giả định tất cả các hệ thống đích đều được cấp phép), xóa chỉ mục 5, 4, 2 và 1. Mỗi lần bạn xóa một chỉ mục, số chỉ mục sẽ được gán lại. Do đó, bạn cần xóa từ số chỉ mục cao nhất đến thấp nhất. Chạy `Get-ImageInfo` sau mỗi lần xóa để xác nhận trực quan chỉ mục nào bạn sẽ xóa tiếp theo.

   ```
   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
   ```

   Chỉ chọn một chỉ mục của phiên bản (trong ví dụ này, Professional). Khi chỉ có một chỉ mục, ảnh được sử dụng để phục hồi, bất kể tên là gì. Lưu ý rằng kích thước của tập tin ảnh có thể lớn hơn trước khi xóa do cách thức hoạt động của quá trình điều chỉnh siêu dữ liệu WIM và chuẩn hóa nội dung.

6. (Tùy chọn) Nếu bạn muốn tích hợp các trình điều khiển vào ảnh phục hồi doanh nghiệp, làm theo các bước sau:

   a. Gắn ảnh của bạn vào một thư mục trống bằng các lệnh sau:

      ```
      mkdir C:\staging\mount

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

   b. Gắn đĩa DVD (DRDVD) chứa Trình điều khiển Windows 10 của HP thích hợp cho hệ thống đích được hỗ trợ. Từ phương tiện chứa trình điều khiển đã gắn, sao chép thư mục con của trình điều khiển vào khu vực tách chuyển bằng lệnh sau:

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

      GHI CHÚ: `<M:>` là ổ đĩa đã gắn. Thay thế bằng ký tự ổ đĩa phù hợp.

      Bạn có thể tích hợp thêm các trình điều khiển .inf-style bằng cách đưa chúng vào thư mục C:\staging\mount\SWSETUP\DRV. Để xem giải thích về cách HP Sure Recover xử lý nội dung này bằng cách sử dụng chức năng `dism /Add-Driver /Recurse`, xem “Add and Remove Drivers to an Offline Windows image” (Thêm và Gỡ Trình điều khiển cho một Ảnh Windows Ngoại tuyến) trong chủ đề sau: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

      Tính năng này không hỗ trợ các trình điều khiển .exe-style yêu cầu phải chạy một ứng dụng.

   c. Lưu thay đổi và hủy gắn ảnh của bạn bằng lệnh sau:

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

      Tập tin ảnh thu được có dạng như sau: C:\staging\my-image.wim.

   d. Truy cập Tách ảnh thuộc trang 6.

Ví dụ 2: Tạo ảnh dựa trên một hệ thống tham chiếu

1. Tạo USB khởi động bằng phương tiện/ổ đĩa chứa WinPE.

GHI CHÚ: Bạn có thể tham khảo các phương pháp tạo ảnh khác trong tài liệu ADK.

Đảm bảo ổ đĩa USB có đủ dung lượng trống để chứa ảnh tạo ra từ hệ thống tham chiếu.

2. Tạo ảnh trên một hệ thống tham chiếu.
3. Tạo ảnh bằng cách khởi động hệ thống tham chiếu bằng phương tiện chứa WinPE của USB và sau đó sử dụng DISM.

GHI CHÚ: <U:> là ổ đĩa USB. Thay thế bằng ký tự ổ đĩa phù hợp.

Chỉnh sửa phần “my-image” của tên tập tin và mô tả <my-image>, nếu cần.

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

4. Sao chép ảnh từ USB sang khu vực tách chuyển trên hệ thống làm việc của bạn bằng lệnh sau:

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

Bạn cần có tập tin ảnh sau: C:\staging\my-image.wim.

5. Truy cập Tách ảnh thuộc trang 6.

Tách ảnh

HP khuyến cáo rằng bạn nên tách ảnh thành các tập tin nhỏ hơn để cải thiện độ tin cậy của nội dung tải xuống qua mạng bằng lệnh sau:

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

GHI CHÚ: FileSize (Kích thước tập tin) được hiển thị theo megabyte. Chỉnh sửa nếu cần.

GHI CHÚ: Do bản chất của thuật toán tách của DISM, kích thước của các tập tin SWM được tạo ra có thể nhỏ hơn hoặc lớn hơn kích thước tập tin mô tả.

Tạo tập tin kê khai

Định dạng tập tin kê khai theo định dạng UTF-8 và không có Dấu Thứ tự Byte (BOM).

Bạn có thể thay đổi tên tệp tin kê khai (custom.mft) được sử dụng trong các quy trình sau, tuy nhiên bạn không được thay đổi phần mở rộng .mft và .sig và phần tên tệp tin của tệp tin kê khai và chữ ký phải trùng khớp nhau. Ví dụ, bạn có thể thay đổi cặp (custom.mft, custom.sig) thành (myimage.mft, myimage.sig).

`mft_version` được sử dụng để xác định định dạng của tệp tin ảnh và hiện phải được đặt về 1.

`image_version` được sử dụng để xác định xem có phiên bản ảnh mới hơn không và để tránh cài đặt phiên bản cũ hơn.

Cả hai giá trị phải là số nguyên 16-bit không dấu và dấu tách dòng trong tệp tin kê khai phải là `'\r \n' (CR + LF)`.

Tạo tệp tin kê khai

Do một số tệp tin có thể liên quan đến ảnh được tách của bạn, sử dụng powershell script để tạo tệp tin kê khai.

Trong tất cả các bước còn lại, bạn phải ở thư mục C:\staging.

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

1. Tạo powershell script bằng cách sử dụng một trình soạn thảo có thể tạo tệp tin văn bản theo định dạng UTF-8 và không có BOM, bằng lệnh sau: `notepad C:\staging\generate-manifest.ps1`

   Tạo script sau:

```
$mftFilename = "custom.mft"
$imageVersion = 1907 (Lưu ý: Số này có thể là bất kỳ số nguyên 16-bit nào)


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

GHI CHÚ: Tệp tin kê khai cho HP Sure Recover không được chứa BOM, do đó các lệnh sau ghi lại tệp tin thành UTF8 và không có BOM.

```
$content = Get-Content $mftFilename

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

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

2. Lưu script.
3. Thực thi script.

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

Tạo chữ ký tệp tin kê khai

Sure Recover xác thực tác nhân và ảnh bằng cách sử dụng chữ ký mật mã. Các ví dụ sau sử dụng một cặp khóa riêng/chung theo định dạng X.509 PEM (phần mở rộng .PEM). Điều chỉnh lệnh sao cho thích hợp để sử dụng chứng nhận nhị phân DER (phần mở rộng .CER hoặc .CRT), chứng nhận PEM mã hóa theo BASE-64 (phần mở rộng .CER hoặc .CRT) hoặc tệp tin PKCS1 PEM (phần mở rộng .PEM). Ví dụ này cũng sử dụng OpenSSL để tạo chữ ký theo định dạng big-endian. Bạn có thể sử dụng bất kỳ tiện ích nào để ký tệp tin kê khai, tuy nhiên một số phiên bản BIOS chỉ hỗ trợ chữ ký theo định dạng little-endian.

1. Tạo khóa riêng 2048 bit RSA bằng lệnh sau. Nếu bạn có cặp khóa riêng/chung 2048 bit RSA theo định dạng pem, sao chép chúng sang C:\staging và sau đó đến bước 3.

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

2. Tạo khóa chung từ khóa riêng của bạn (nếu bạn có khóa chung tương đương với khóa riêng của bạn theo định dạng PEM, sao chép nó sang C:\staging) bằng lệnh sau:

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

3. Tạo tệp tin chữ ký (bằng hàm băm dựa trên sha256) dựa trên khóa riêng 2048 bit RSA của bạn tạo ra từ bước 1, bằng lệnh sau:

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

4. Xác minh tệp tin chữ ký bằng cách sử dụng khóa chung của bạn được tạo ra từ bước trước, bằng lệnh sau:

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

GHI CHÚ:

- Nếu bạn chỉ cần tạo tệp tin chữ ký, các bước cần thực hiện gồm bước 1 và 3.
- Đối với HP Sure Recover, các bước tối thiểu cần thực hiện gồm bước 1, 2 và 3. Bạn cần khóa chung được tạo ra từ bước 2 để dự phòng hệ thống đích của bạn.
- Bước 4 là bước tùy chọn nhưng khuyến cáo nên thực hiện để xác thực chính xác tệp tin chữ ký và tệp tin kê khai của bạn.

Lưu trữ tệp tin

Lưu trữ các tệp tin sau trên máy chủ của bạn từ thư mục C:\staging:

- *.swm
- custom.mft (hoặc tên tệp tin mà bạn chọn cho tệp tin kê khai)
- custom.sig (hoặc tên tệp tin trùng khớp mà bạn chọn cho tệp tin chữ ký)

GHI CHÚ: Nếu bạn sử dụng IIS làm giải pháp lưu trữ, bạn phải cấu hình các dữ liệu nhập vào MIME để bao gồm các phần mở rộng sau, tất cả được cấu hình thành "application/octet-stream:"

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

Dự phòng các hệ thống đích của bạn

Bạn có thể dự phòng các hệ thống đích bằng cách sử dụng Thư viện Script Quản lý Máy khách HP, Trình quản lý Bảo mật Máy khách HP (CSM)/Sure Recover hoặc Bộ công cụ Tích hợp Khả năng Quản lý (MIK) (https://www.hp.com/go/clientmanagement).

Cung cấp các thông tin sau cho việc dự phòng này:

1. Địa chỉ URL của tệp tin kê khai được lưu trữ ở phần trước (http://your_server.domain/path/custom.mft)
2. Khóa chung được sử dụng để xác minh tệp tin chữ ký đã được tạo ra trước đó (ví dụ: C:\staging\my-recovery-public.pem).

Xử lý sự cố

Nếu bạn nhận được thông báo về việc xác thực bảo mật cho quá trình phục hồi tùy chỉnh gặp thất bại, tiến hành kiểm tra như sau:

1. Tệp tin kê khai phải có định dạng UTF-8 và không có BOM.
2. Kiểm tra hàm băm của tệp tin.
3. Đảm bảo rằng hệ thống được dự phòng bằng khóa chung tương ứng với khóa riêng được sử dụng để ký tệp tin kê khai.
4. Kiểu loại mime máy chủ IIS phải là `application/octet-stream`.
5. Đường dẫn tệp tin trong tệp tin kê khai phải chứa đường dẫn đầy đủ dẫn đến thư mục trên cùng, có chứa ảnh như được nhìn thấy từ hệ thống máy khách. Đường dẫn này không phải là đường dẫn đầy đủ dẫn đến nơi tệp tin được lưu tại điểm phân phối.

3 Sử dụng Tác nhân HP Sure Recover Bên trong Tường lửa của Doanh nghiệp

Có thể lưu trữ tác nhân HP Sure Recover trên mạng nội bộ của doanh nghiệp. Sau khi bạn cài đặt HP Sure Recover SoftPaq, sao chép tệp tin tác nhân từ thư mục tác nhân HP Sure Recover từ vị trí cài đặt sang điểm phân phối HTTP hoặc FTP. Sau đó dự phòng hệ thống máy khách bằng URL của điểm phân phối và khóa chung HP có tên là `hpsr_agent_public_key.pem`, khóa này được phân phối cùng tác nhân SoftPaq của HP Sure Recover.

Cài đặt tác nhân HP Sure Recover

1. Tải xuống tác nhân HP Sure Recover và trích xuất tệp tin vào điểm phân phối HTTP hoặc FTP của bạn.
2. Đặt quyền tệp tin sao cho phù hợp trên điểm phân phối.
3. Nếu bạn sử dụng Dịch vụ Thông tin Internet (IIS), tạo các kiểu loại application/octet-stream MIME cho các định dạng tệp tin sau:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   QUAN TRỌNG: Các bước sau mô tả việc dự phòng Sure Recover bằng SCCM. Để biết ví dụ về cách dự phòng Sure Recover bằng Thư viện Script Quản lý Máy khách HP, xem Làm việc với Thư viện Script Quản lý Máy khách HP (CMSL) thuộc trang 12.
4. Bắt đầu SCCM, điều hướng đến **HP Client Security Suite** (Gói Bảo mật Máy khách HP) và sau đó chọn trang HP Sure Recover.

   GHI CHÚ: URL điểm phân phối có chứa ftp hoặc http với tư cách là giao thức vận chuyển. Nó cũng chứa đường dẫn đầy đủ dẫn đến thư mục trên cùng, có chứa tệp tin kê khai dành cho tác nhân HP Sure Recover như được nhìn thấy từ hệ thống máy khách. Đường dẫn này không phải là đường dẫn đầy đủ dẫn đến nơi tệp tin được lưu tại điểm phân phối.
5. Trong mục **Platform Image** (Ảnh Nền tảng), chọn tùy chọn **Corporation** (Doanh nghiệp) để phục hồi ảnh HĐH tùy chỉnh từ điểm phân phối doanh nghiệp. Nhập URL do quản trị viên CNTT cung cấp vào hộp nhập liệu **Image Location URL** (URL Vị trí Ảnh). Nhập khóa chung `hpsr_agent_public_key.pem` vào trường **Image Verification** (Xác minh Ảnh).

   GHI CHÚ: URL ảnh tùy chỉnh phải chứa tên tệp tin kê khai ảnh.

6. Trong mục **Recovery Agent** (Tác nhân Phục hồi), chọn tùy chọn **Corporation** (Doanh nghiệp) để sử dụng tác nhân phục hồi tùy chỉnh hoặc tác nhân phục hồi HP từ điểm phân phối doanh nghiệp. Nhập URL do quản trị viên CNTT cung cấp vào hộp nhập liệu **Agent Location URL** (URL Vị trí Tác nhân). Nhập khóa chung `hpsr_agent_public_key.pem` vào trường nhập liệu **Agent Verification Key** (Khóa Xác minh Tác nhân).

GHI CHÚ: Không được bao gồm tên tệp tin cho tệp tin kê khai tác nhân trong URL vì BIOS yêu cầu phải đặt tên nó là recovery.mft.

7. Sau khi áp dụng chính sách cho hệ thống máy khách, khởi động lại hệ thống máy khách.

8. Trong quá trình dự phòng ban đầu, dấu nhắc sẽ xuất hiện để bạn nhập mã bảo mật gồm 4 chữ số để hoàn tất quá trình kích hoạt HP Sure Recover. Để biết thêm chi tiết, truy cập hp.com và tìm sách trắng HP Manageability Integration Kit (MIK) for Microsoft System Center Manager (Bộ công cụ Tích hợp Khả năng Quản lý HP (MIK) cho Trình quản lý Trung tâm Hệ thống Microsoft).

Sau khi quá trình kích hoạt HP Sure Recover hoàn tất thành công, URL tùy chỉnh được áp dụng bởi chính sách sẽ được hiển thị trong menu thiết đặt BIOS của HP Sure Recover.

Để xác nhận đã kích hoạt thành công, khởi động lại máy tính và khi logo HP xuất hiện, nhấn f10. Chọn **Advanced** (Nâng cao), chọn **HP Sure Recover**, chọn **Recovery Agent** (Tác nhân Phục hồi) và sau đó chọn **URL**.

4 Làm việc với Thư viện Script Quản lý Máy khách HP (CMSL)

Thư viện Script Quản lý Máy khách HP cho phép bạn quản lý thiết đặt HP Sure Recover bằng PowerShell. Script ví dụ dưới đây trình diễn cách dự phòng, xác định trạng thái, thay đổi cấu hình và hủy dự phòng HP Sure Recover.

GHI CHÚ: Một số lệnh vượt quá giới hạn độ dài dòng trong hướng dẫn này, nhưng phải được nhập thành một dòng.

```
$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
}
```

Tạo mẫu khóa bằng cách sử dụng OpenSSL

Lưu khóa riêng ở một nơi an toàn. Khóa chung sẽ được sử dụng để xác thực và phải được cung cấp trong quá trình dự phòng. Các khóa này phải có độ dài 2048 bit và sử dụng số mũ 0x10001. Thay thế chủ đề trong các ví dụ bằng thông tin về tổ chức của bạn.

Đặt biến số môi trường sau trước khi tiếp tục:

```
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:
```

Bạn có thể ký tệp tin kê khai ảnh bằng lệnh sau:

```
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:
```

Bạn có thể ký tệp tin kê khai tác nhân bằng lệnh sau:

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

OpenSSL tạo tệp tin chữ ký theo định dạng big-endian, định dạng này không tương thích với một số phiên bản BIOS, do đó có thể cần phải đảo thứ tự byte của tệp tin chữ ký tác nhân trước khi sử dụng. Các phiên bản BIOS hỗ trợ thứ tự byte big-endian cũng hỗ trợ cả thứ tự byte little-endian.

A Xử lý sự cố

Phân vùng ổ đĩa thất bại

Phân vùng ổ đĩa thất bại có thể xảy ra nếu phân vùng SR_AED hoặc SR_IMAGE được mã hóa bằng Bitlocker. Các phần vùng này thường được tạo ra, có thuộc tính gpt, thuộc tính này ngăn không cho Bitlocker mã hóa chúng, tuy nhiên nếu người dùng xóa và tạo lại phân vùng hoặc tạo chúng theo cách thủ công trên một ổ đĩa kim loại trống không, thì tác nhân Sure Recover sẽ không thể xóa chúng được và sẽ thoát kèm theo lỗi khi phân vùng lại ổ đĩa. Người dùng phải xóa chúng theo cách thủ công bằng cách chạy diskpart, chọn ổ đĩa và thực thi lệnh đè `del vol` (xóa ổ đĩa) hoặc lệnh tương tự.

Nhật ký kiểm tra phần mềm điều khiển

Thông tin biến số EFI như sau:

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

Các API tồn tại trên Windows để đọc biến số EFI hoặc bạn có thể kết xuất nội dung biến số sang một tệp tin bằng cách sử dụng tiện ích UEFI Shell dmpstore.

Bạn có thể kết xuất nhật ký kiểm tra bằng cách sử dụng lệnh `Get-HPFirmwareAuditLog` do Thư viện Script Quản lý Máy khách HP cung cấp.

Nhật ký sự kiện Windows

Sure Recover bắt đầu và dừng các sự kiện được gửi đến nhật ký kiểm tra BIOS để bạn có thể xem trong Windows Event Viewer (Trình xem Sự kiện của Windows) trong nhật ký của Sure Start nếu đã cài đặt HP Notifications (Thông báo của HP). Các sự kiện này bao gồm ngày và giờ, ID Nguồn, ID Sự kiện và một mã riêng của sự kiện. Chẳng hạn, `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` chỉ báo rằng phục hồi thất bại do không thể xác thực tệp tin kê khai bằng mã riêng của sự kiện c3f 23000, mã này được ghi nhật ký vào lúc 2:26:40 vào ngày 27 tháng 6 năm 2018.

GHI CHÚ: Các nhật ký này tuân theo định dạng ngày của Hoa Kỳ là tháng/ngày/năm.

HP Secure Platform Management (ID Nguồn = 84 giờ)

Bảng A-1 HP Secure Platform Management

ID Sự kiện	Số lượng thiết bị (Tất cả/DaaS)	Số lượng sự kiện (Tất cả/DaaS)	Mô tả	Lưu ý
40	256/178	943/552	Quá trình phục hồi HĐH nền tảng được bắt đầu bởi phần mềm điều khiển.	Phục hồi nền tảng đã bắt đầu

Bảng A-1 HP Secure Platform Management (còn tiếp)

ID Sự kiện	Số lượng thiết bị (Tất cả/DaaS)	Số lượng sự kiện (Tất cả/ DaaS)	Mô tả	Lưu ý
41	221/147	588/332	Quá trình phục hồi HĐH nền tảng đã hoàn tất thành công.	Phục hồi nền tảng đã hoàn tất
42	54/42	252/156	Quá trình phục hồi HĐH nền tảng không hoàn tất thành công.	Phục hồi nền tảng thất bại

Bạn có thể truy xuất Nhật ký Kiểm tra Phần mềm điều khiển bằng cách sử dụng Get-HPFirmwareAuditLog trong Thư viện Script Quản lý Máy khách HP, có sẵn tại http://www.hp.com/go/clientmanagement. ID Sự kiện 40, 41 và 42 của HP Secure Platform Management trả về các Mã Riêng của Sự kiện trong trường dữ liệu, các mã này chỉ báo kết quả thực hiện các thao tác Sure Recover. Chẳng hạn, mục nhập liệu nhật ký sau đây chỉ báo rằng Sure Recover đã không tải xuống được tệp tin kê khai hoặc chữ ký với id lỗi sự kiện 42 và dữ liệu: 00:30:F1:c3, cần diễn giải mã này là giá trị 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
```

Phục hồi thành công được hiển thị dưới dạng event_id = 41 và dữ liệu: 00:00:00:00, chẳng hạn:

```
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 sử dụng các Mã Riêng của Sự kiện sau.

Bảng A-2 Mã Riêng của Sự kiện

Mô tả sự kiện	Mã sự kiện
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