Οδηγός χρήσης

HP Sure Recover

Πρώτη έκδοση: Φεβρουάριος 2020

Αριθμός εγγράφου: L93434-151

Υπόμνημα σύνταξης δεδομένων εισόδου χρήστη

Το κείμενο που πρέπει να εισαγάγετε σε ένα περιβάλλον εργασίας υποδεικνύεται με `γραμματοσειρά σταθερού πλάτους`.

Πίνακας -1 Υπόμνημα σύνταξης δεδομένων εισόδου χρήστη

Αριθμός	Περιγραφή
`Κείμενο χωρίς αγκύλες ή άγκιστρα`	Στοιχεία που πρέπει να πληκτρολογήσετε ακριβώς όπως εμφανίζονται
`<Κείμενο μέσα σε γωνιώδεις αγκύλες>`	Κείμενο κράτησης θέσης για μια τιμή που πρέπει να καταχωρήσετε. Παραλείψτε τις αγκύλες.
`[Κείμενο μέσα σε ορθογώνιες αγκύλες`	Προαιρετικά στοιχεία. Παραλείψτε τις αγκύλες.
`{Κείμενο μέσα σε άγκιστρα}`	Ένα σύνολο στοιχείων από τα οποία πρέπει να επιλέξετε μόνο ένα. Παραλείψτε τα άγκιστρα.
`|`	Διαχωριστικό για στοιχεία από τα οποία πρέπει να επιλέξετε μόνο ένα. Παραλείψτε την κάθετη γραμμή.
`...`	Στοιχεία που μπορούν ή πρέπει να επαναληφθούν. Παραλείψτε τα αποσιωπητικά.

Πίνακας περιεχομένων

1 Έναρξη χρήσης

Το HP Sure Recover βοηθάει στην ασφαλή εγκατάσταση του λειτουργικού συστήματος από το δίκτυο με ελάχιστη αλληλεπίδραση από τον χρήστη. Τα συστήματα που διαθέτουν HP Sure Recover με Embedded Reimaging υποστηρίζουν επίσης την εγκατάσταση από τοπική συσκευή αποθήκευσης.

ΣΗΜΑΝΤΙΚΟ: Πριν χρησιμοποιήσετε το HP Sure Recover, δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας. Επειδή η διαδικασία απεικόνισης διαμορφώνει εκ νέου τη μονάδα δίσκου, θα υπάρξει απώλεια δεδομένων.

Οι εικόνες αποκατάστασης που παρέχει η HP περιλαμβάνουν το βασικό πρόγραμμα εγκατάστασης των Windows 10®. Προαιρετικά, το HP Sure Recover μπορεί να εγκαταστήσει βελτιστοποιημένα προγράμματα οδήγησης για συσκευές HP. Οι εικόνες αποκατάστασης HP περιλαμβάνουν μόνο παράγοντες αποκατάστασης δεδομένων που περιλαμβάνονται στα Windows 10, όπως το OneDrive. Οι εταιρείες μπορούν να δημιουργήσουν τα δικά τους προσαρμοσμένα είδωλα για να προσθέσουν εταιρικές ρυθμίσεις, εφαρμογές, προγράμματα οδήγησης και παράγοντες αποκατάστασης δεδομένων.

Ο παράγοντας αποκατάστασης λειτουργικού συστήματος εκτελεί τα βήματα που είναι απαραίτητα για την εγκατάσταση του ειδώλου αποκατάστασης. Ο παράγοντας αποκατάστασης που παρέχεται από την HP εκτελεί συνηθισμένα βήματα όπως η δημιουργία διαμερισμάτων, η διαμόρφωση και η εξαγωγή του ειδώλου αποκατάστασης στη συσκευή προορισμού. Επειδή ο παράγοντας αποκατάστασης της HP διατίθεται μέσω της τοποθεσίας hp.com, θα πρέπει να έχετε πρόσβαση στο Internet για να τον ανακτήσετε, εκτός εάν το σύστημά σας διαθέτει δυνατότητα Embedded Reimaging. Οι εταιρείες μπορούν επίσης να φιλοξενήσουν τον παράγοντα αποκατάστασης HP εντός του τείχους προστασίας τους ή να δημιουργήσουν προσαρμοσμένους παράγοντες αποκατάστασης για πιο περίπλοκα περιβάλλοντα αποκατάστασης.

Μπορείτε να εκκινήσετε το HP Sure Recover όταν δεν εντοπίζεται κανένα λειτουργικό σύστημα. Μπορείτε, επίσης, να εκτελείτε το HP Sure Recover βάσει χρονοδιαγράμματος, π.χ. για να διασφαλίσετε την απομάκρυνση τυχόν κακόβουλου λογισμικού. Διαμορφώστε αυτές τις ρυθμίσεις μέσω του HP Client Security Manager (CSM), του Manageability Integration Kit (MIK) ή του HP Client Management Script Library.

Αποκατάσταση μέσω δικτύου

ΣΗΜΕΙΩΣΗ: Για να πραγματοποιήσετε αποκατάσταση μέσω δικτύου, πρέπει να χρησιμοποιήσετε ενσύρματη σύνδεση. Η HP συνιστά να δημιουργήσετε αντίγραφα ασφαλείας των σημαντικών αρχείων, δεδομένων, φωτογραφιών, βίντεο κ.λπ. πριν από τη χρήση του HP Sure Recover για να αποφύγετε τον κίνδυνο απώλειας δεδομένων.

1. Συνδέστε το σύστημα-πελάτη στο δίκτυο μέσω του οποίου μπορείτε να αποκτήσετε πρόσβαση στο σημείο διανομής HTTP ή FTP.
2. Επανεκκινήστε το σύστημα-πελάτη και, όταν εμφανιστεί το λογότυπο της HP, πατήστε το πλήκτρο F11.
3. Επιλέξτε **Επαναφορά από δίκτυο**.

Αποκατάσταση μέσω τοπικής μονάδας δίσκου

Αν ένα σύστημα-πελάτης διαθέτει Embedded Reimaging και η επιλογή προγραμματισμένης λήψης ειδώλου είναι ενεργοποιημένη στην εφαρμοσμένη πολιτική, το είδωλο θα μεταφορτωθεί στο σύστημα-πελάτη την προγραμματισμένη ώρα. Μετά τη λήψη του ειδώλου, επανεκκινήστε το σύστημα-πελάτη για να αντιγράψετε το είδωλο στη συσκευή αποθήκευσης Embedded Reimaging.

Για να πραγματοποιήσετε τοπική αποκατάσταση χρησιμοποιώντας το είδωλο στη συσκευή αποθήκευσης Embedded Reimaging:

1. Επανεκκινήστε το σύστημα-πελάτη και, όταν εμφανιστεί το λογότυπο της HP, πατήστε το πλήκτρο F11.
2. Επιλέξτε **Επαναφορά από τοπική μονάδα δίσκου**.

Στα συστήματα με Embedded Reimaging πρέπει να διαμορφωθεί ένα χρονοδιάγραμμα λήψης και να χρησιμοποιείται ο παράγοντας λήψης για την αναζήτηση ενημερώσεων. Ο παράγοντας λήψης περιλαμβάνεται στο πρόσθετο HP Sure Recover για το HP Client Security Manager και μπορεί επίσης να διαμορφωθεί στο MIK. Για τις οδηγίες χρήσης του MIK, ανατρέξτε στη διεύθυνση https://www.hp.com/go/clientmanagement.

Μπορείτε επίσης να δημιουργήσετε μια προγραμματισμένη εργασία για την αντιγραφή του παράγοντα στο διαμέρισμα SR_AED και του ειδώλου στο διαμέρισμα SR_IMAGE. Στη συνέχεια, μπορείτε να χρησιμοποιήσετε το HP Client Management Script Library για να στείλετε ένα συμβάν υπηρεσίας που θα ενημερώνει το BIOS ότι θα πρέπει να επικυρώσει τα περιεχόμενα και να κάνει αντιγραφή στη συσκευή αποθήκευσης Embedded Reimaging κατά την επόμενη επανεκκίνηση.

2 Δημιουργία εταιρικού ειδώλου

Οι περισσότερες εταιρείες χρησιμοποιούν τα Εργαλεία ανάπτυξης της Microsoft, το Κιτ αξιολόγησης και ανάπτυξης των Windows 10 ή και τα δύο για την παραγωγή αρχείων που περιέχουν ένα είδωλο σε μια αρχειοθήκη Windows Imaging (WIM).

Απαιτήσεις

- Η πιο πρόσφατη έκδοση του Κιτ αξιολόγησης και ανάπτυξης των Windows 10 (Windows ADK)
- PowerShell
- OpenSSL (ή άλλη λύση για τη δημιουργία ζευγών ιδιωτικών/δημόσιων κλειδιών RSA)

  Χρησιμοποιείται για τη δημιουργία του ζεύγους κλειδιών RSA που χρησιμοποιείται για την προστασία της ακεραιότητας του εταιρικού ειδώλου που δημιουργείτε και φιλοξενείτε.
- Μια λύση φιλοξενίας διακομιστή (όπως οι υπηρεσίες Microsoft Internet Information Services [IIS])

Δημιουργία ειδώλου

Πριν ξεκινήσετε τη διαδικασία δημιουργίας του ειδώλου, ρυθμίστε το λειτουργικό σύστημα ή το σύστημα δόμησης όπου έχετε εγκαταστήσει τα απαιτούμενα εργαλεία ώστε να είναι έτοιμο για την επεξεργασία του ειδώλου, όπως υποδεικνύεται στα παρακάτω βήματα:

1. Ως διαχειριστής, ανοίξτε τη γραμμή εντολών του `Deployment and Imaging Tools Environment` (εγκαταστάθηκε με τα Εργαλεία ανάπτυξης του Windows ADK).
2. Δημιουργήστε μια περιοχή προεργασίας του ειδώλου, χρησιμοποιώντας την ακόλουθη εντολή:

   ```
   mkdir C:\staging
   ```
3. Δημιουργήστε το είδωλο ακολουθώντας ένα από τα παρακάτω παραδείγματα:

   Παράδειγμα 1: Δημιουργία ειδώλου με βάση το είδωλο εγκατάστασης των Microsoft Windows στη σελίδα 3

   Παράδειγμα 2: Δημιουργία ειδώλου βάσει συστήματος αναφοράς στη σελίδα 6

Παράδειγμα 1: Δημιουργία ειδώλου με βάση το είδωλο εγκατάστασης των Microsoft Windows

1. Μοντάρετε ή ανοίξτε το είδωλο εγκατάστασης των Microsoft Windows (από Microsoft ISO ή HP OSDVD).
2. Αντιγράψτε το αρχείο install.wim από το μονταρισμένο είδωλο εγκατάστασης των Windows στην περιοχή προεργασίας, χρησιμοποιώντας την ακόλουθη εντολή:

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

   ΣΗΜΕΙΩΣΗ: Το `<M:>` αναφέρεται στη μονταρισμένη μονάδα δίσκου. Αντικαταστήστε το με το σωστό γράμμα μονάδας δίσκου.

3. Μετονομάστε το install.wim σε ένα όνομα αρχείου ειδώλου ("my-image" σε αυτό το παράδειγμα) χρησιμοποιώντας την ακόλουθη εντολή:

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

(Προαιρετικό) Το HP Sure Recover περιλαμβάνει μια λειτουργία για την αποκατάσταση μιας συγκεκριμένης έκδοσης από ένα είδωλο πολλών ευρετηρίων, με βάση την έκδοση των Windows που είχε αδειοδοτηθεί αρχικά για το σύστημα προορισμού HP από το εργοστάσιο. Ο μηχανισμός αυτός λειτουργεί εάν τα ευρετήρια έχουν ονομαστεί σωστά. Αν το είδωλο εγκατάστασης των Windows προέρχεται από είδωλο HP OSDVD, κατά πάσα πιθανότητα έχετε ένα είδωλο πολλών εκδόσεων. Αν δεν θέλετε αυτή τη συμπεριφορά και θέλετε να διασφαλίσετε ότι θα χρησιμοποιείται μια συγκεκριμένη έκδοση για όλα τα συστήματα προορισμού, θα πρέπει να διασφαλίσετε ότι υπάρχει μόνο ένα ευρετήριο στο είδωλο εγκατάστασης.

4. Ελέγξτε τα περιεχόμενα του ειδώλου εγκατάστασης χρησιμοποιώντας την παρακάτω εντολή:

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

Παρακάτω μπορείτε να δείτε ένα δείγμα αποτελέσματος από είδωλο εγκατάστασης που υποστηρίζει πέντε εκδόσεις (οι οποίες αντιστοιχούνται με βάση το BIOS κάθε συστήματος προορισμού):

Λεπτομέρειες για το είδωλο: `my-image.wim`

Ευρετήριο: `1`

Όνομα: `CoreSingleLanguage`

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

Μέγεθος: `19.512.500.682 bytes`

Ευρετήριο: `2`

Όνομα: `Core`

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

Μέγεθος: `19.512.500.682 bytes`

Ευρετήριο: `3`

Όνομα: `Professional`

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

Μέγεθος: `19.758.019.520 bytes`

Ευρετήριο: `4`

Όνομα: `ProfessionalEducation`

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

Μέγεθος: `19.758.019.480 bytes`

Ευρετήριο: `5`

Όνομα: `ProfessionalWorkstation`

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

Μέγεθος: `19.758.023.576 bytes`

ΣΗΜΕΙΩΣΗ: Όταν υπάρχει μόνο ένα ευρετήριο, το είδωλο χρησιμοποιείται για την αποκατάσταση ανεξάρτητα από το όνομά του. Το μέγεθος του αρχείου ειδώλου μπορεί να είναι μεγαλύτερο απ' ό,τι ήταν πριν από τις διαγραφές.

5. Αν δεν θέλετε να υπάρχουν πολλές εκδόσεις, διαγράψτε τα ευρετήρια που δεν θέλετε.

   Όπως φαίνεται στο παρακάτω παράδειγμα, αν θέλετε μόνο την έκδοση Professional (με την προϋπόθεση ότι διαθέτουν την απαιτούμενη άδεια χρήσης όλα τα συστήματα προορισμού), διαγράψτε τα ευρετήρια 5, 4, 2 και 1. Κάθε φορά που διαγράφετε ένα ευρετήριο, αλλάζει και η αρίθμηση των ευρετηρίων. Κατά συνέπεια, η διαγραφή θα πρέπει να γίνεται από το ευρετήριο με τον μεγαλύτερο αριθμό. Εκτελέστε την εντολή `Get-ImageInfo` μετά από κάθε διαγραφή για να επιβεβαιώνετε οπτικά το επόμενο ευρετήριο προς διαγραφή.

   ```
   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
   ```

   Επιλέξτε μόνο ένα ευρετήριο της έκδοσης (σε αυτό το παράδειγμα χρησιμοποιείται η έκδοση Professional). Όταν υπάρχει μόνο ένα ευρετήριο, το είδωλο χρησιμοποιείται για την αποκατάσταση ανεξάρτητα από το όνομά του. Σημειώστε ότι το μέγεθος του αρχείου ειδώλου μπορεί να είναι μεγαλύτερο απ' ό,τι ήταν πριν από τις διαγραφές εξαιτίας του τρόπου με τον οποίο λειτουργούν οι τροποποιήσεις των μεταδεδομένων και η κανονικοποίηση του περιεχομένου του WIM.

6. (Προαιρετικό) Αν θέλετε να συμπεριλάβετε προγράμματα οδήγησης στο εταιρικό είδωλο αποκατάστασης, ακολουθήστε τα παρακάτω βήματα:

   α. Μοντάρετε το είδωλο σε έναν άδειο φάκελο χρησιμοποιώντας τις παρακάτω εντολές:

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

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

   β. Μοντάρετε το κατάλληλο DVD προγραμμάτων οδήγησης της HP για τα Windows 10 (DRDVD) για το υποστηριζόμενο σύστημα προορισμού. Αντιγράψτε τους υποφακέλους με τα προγράμματα οδήγησης από το μονταρισμένο μέσο προγραμμάτων οδήγησης στην περιοχή προεργασίας, χρησιμοποιώντας την ακόλουθη εντολή:

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

   ΣΗΜΕΙΩΣΗ: Το `< M:>` αναφέρεται στη μονταρισμένη μονάδα δίσκου. Αντικαταστήστε το με το σωστό γράμμα μονάδας δίσκου.

   Μπορείτε να συμπεριλάβετε και πρόσθετα προγράμματα οδήγησης .inf-style τοποθετώντας τα στον φάκελο C:\staging\mount\SWSETUP\DRV. Για να δείτε μια επεξήγηση του τρόπου επεξεργασίας αυτού του περιεχομένου από το HP Sure Recover μέσω της λειτουργίας `dism /Add-Driver /Recurse`, ανατρέξτε στην ενότητα "Προσθήκη και κατάργηση προγραμμάτων οδήγησης σε είδωλο των Windows χωρίς σύνδεση" στο παρακάτω άρθρο: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-and-remove-drivers-to-an-offline-windows-image.

   Αυτή η λειτουργία δεν υποστηρίζει τα προγράμματα οδήγησης .exe που απαιτούν την εκτέλεση εφαρμογής.

γ. Αποθηκεύστε τις αλλαγές και καταργήστε το μοντάρισμα του ειδώλου χρησιμοποιώντας την παρακάτω εντολή:

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

Το αρχείο ειδώλου που θα προκύψει θα είναι το εξής: C:\staging\my-image.wim.

δ. Μεταβείτε στην ενότητα Διαίρεση ειδώλου στη σελίδα 6.

Παράδειγμα 2: Δημιουργία ειδώλου βάσει συστήματος αναφοράς

1. Δημιουργήστε ένα μέσο USB WinPE με δυνατότητα εκκίνησης.

ΣΗΜΕΙΩΣΗ: Μπορείτε να βρείτε πρόσθετες μεθόδους για την καταγραφή του ειδώλου στην τεκμηρίωση του ADK.

Βεβαιωθείτε ότι η μονάδα USB έχει αρκετό ελεύθερο χώρο για την αποθήκευση του ειδώλου που θα καταγραφεί από το σύστημα αναφοράς.

2. Δημιουργήστε ένα είδωλο στο σύστημα αναφοράς.
3. Καταγράψτε το είδωλο εκκινώντας το σύστημα αναφοράς με το μέσο USB WinPE και, στη συνέχεια, χρησιμοποιήστε το DISM.

ΣΗΜΕΙΩΣΗ: Το `<U:>` αναφέρεται στη μονάδα USB. Αντικαταστήστε το με το σωστό γράμμα μονάδας δίσκου.

Επεξεργαστείτε το τμήμα "my-image" του ονόματος αρχείου και την περιγραφή `<my-image>` όπως απαιτείται.

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

4. Αντιγράψτε το είδωλο από τη μονάδα USB στην περιοχή προεργασίας του συστήματος εργασίας χρησιμοποιώντας την ακόλουθη εντολή:

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

Θα πρέπει να έχετε το παρακάτω αρχείο ειδώλου: C:\staging\my-image.wim.

5. Μεταβείτε στην ενότητα Διαίρεση ειδώλου στη σελίδα 6.

Διαίρεση ειδώλου

Η HP συνιστά να διαιρείτε το είδωλο σε μικρότερα αρχεία για τη βελτίωση της αξιοπιστίας των δικτυακών λήψεων χρησιμοποιώντας την ακόλουθη εντολή:

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

ΣΗΜΕΙΩΣΗ: Το μέγεθος του αρχείου εμφανίζεται σε megabyte. Κάντε τις απαιτούμενες αλλαγές.

ΣΗΜΕΙΩΣΗ: Εξαιτίας της φύσης του αλγόριθμου διαίρεσης του DISM, τα μεγέθη των αρχείων SWM που θα δημιουργηθούν μπορεί να είναι μικρότερα ή μεγαλύτερα από το δηλωμένο μέγεθος αρχείου.

Δημιουργία διακήρυξης

Αποθηκεύστε τα αρχεία της διακήρυξης σε μορφή UTF-8 χωρίς σήμανση σειράς byte (BOM).

Μπορείτε να αλλάξετε το όνομα του αρχείου διακήρυξης (custom.mft) που χρησιμοποιείται στις παρακάτω διαδικασίες, αλλά δεν πρέπει να αλλάξετε τις επεκτάσεις .mft και .sig. Επίσης, τα ονόματα των αρχείων διακήρυξης και υπογραφής θα πρέπει να είναι ίδια. Για παράδειγμα, μπορείτε να αλλάξετε το ζεύγος (custom.mft, custom.sig) σε (myimage.mft, myimage.sig).

Το `mft_version` χρησιμοποιείται για τον προσδιορισμό της μορφής του αρχείου ειδώλου και πρέπει να έχει οριστεί σε 1.

Το `image_version` χρησιμοποιείται για να προσδιοριστεί αν υπάρχει νεότερη έκδοση του ειδώλου και να αποτραπεί η εγκατάσταση παλιότερων εκδόσεων.

Και οι δύο τιμές πρέπει να είναι ακέραιοι αριθμοί 16 bit χωρίς πρόσημο και το διαχωριστικό γραμμής στη διακήρυξη πρέπει να είναι `'\r\n' (CR + LF)`.

Δημιουργία διακήρυξης

Επειδή στη διαίρεση του ειδώλου μπορεί να εμπλέκονται διάφορα αρχεία, χρησιμοποιήστε μια δέσμη ενεργειών powershell για να δημιουργήσετε μια διακήρυξη.

Σε όλα τα υπόλοιπα βήματα, πρέπει να βρίσκεστε στον φάκελο C:\staging.

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

1. Δημιουργήστε μια δέσμη ενεργειών powershell χρησιμοποιώντας ένα πρόγραμμα επεξεργασίας που μπορεί να δημιουργήσει αρχεία κειμένου σε μορφή UTF-8 χωρίς BOM, χρησιμοποιώντας την ακόλουθη εντολή: `notepad C:\staging\generate-manifest.ps1`

   Δημιουργήστε την ακόλουθη δέσμη ενεργειών:

   ```
   $mftFilename = "Custom. MFT"
   ```

   `$imageVersion = 1907` (Σημείωση: Μπορεί να είναι οποιοσδήποτε αριθμός 16 bit)

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

ΣΗΜΕΙΩΣΗ: Οι διακηρύξεις για το HP Sure Recover δεν μπορούν να περιλαμβάνουν σήμανση σειράς byte (BOM). Κατά συνέπεια, οι παρακάτω εντολές επανεγγράφουν το αρχείο ως UTF8 χωρίς BOM.

```
$content = Get-Content $mftFilename
$encoding = New-Object System.Text.UTF8Encoding $False
[System.IO.File]::WriteAllLines($pathToManifest + '\' + $mftFilename,
$content, $encoding)
```

2. Αποθηκεύστε τη δέσμη ενεργειών.
3. Εκτελέστε τη δέσμη ενεργειών.

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

Δημιουργία υπογραφής διακήρυξης

Το Sure Recover επικυρώνει τον παράγοντα και το είδωλο με τη χρήση κρυπτογραφικών υπογραφών. Τα παρακάτω παραδείγματα χρησιμοποιούν ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού σε μορφή X.509 PEM (επέκταση .PEM). Προσαρμόστε τις εντολές όπως απαιτείται για τη χρήση δυαδικών πιστοποιητικών DER (επέκταση .CER ή .CRT), πιστοποιητικών PEM με κωδικοποίηση BASE-64 (επέκταση .CER ή .CRT) ή αρχείων PEM PKCS1 (επέκταση .PEM). Το παράδειγμα χρησιμοποιεί επίσης το OpenSSL, το οποίο δημιουργεί υπογραφές σε μορφή big endian. Μπορείτε να χρησιμοποιήσετε οποιοδήποτε βοηθητικό πρόγραμμα για την υπογραφή των διακηρύξεων, αλλά ορισμένες εκδόσεις BIOS υποστηρίζουν μόνο τις υπογραφές μορφής little endian.

1. Δημιουργήστε ένα ιδιωτικό κλειδί RSA 2048 bit χρησιμοποιώντας την ακόλουθη εντολή. Αν έχετε ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού RSA 2048 bit σε μορφή PEM, αντιγράψτε τα κλειδιά αυτά στον φάκελο C:\staging και προχωρήστε στο βήμα 3.

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

2. Δημιουργήστε το δημόσιο κλειδί από το ιδιωτικό (αν έχετε δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό σας κλειδί σε μορφή PEM, αντιγράψτε το στον φάκελο C:\staging) χρησιμοποιώντας την ακόλουθη εντολή:

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

3. Δημιουργήστε ένα αρχείο υπογραφής (χρησιμοποιώντας κατακερματισμό βάσει sha256) με βάση το ιδιωτικό κλειδί RSA 2048 bit που δημιουργήσατε στο βήμα 1, χρησιμοποιώντας την ακόλουθη εντολή:

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

4. Επαληθεύστε το αρχείο υπογραφής με το δημόσιο κλειδί από το προηγούμενο βήμα, χρησιμοποιώντας την ακόλουθη εντολή:

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

ΣΗΜΕΙΩΣΗ:

- Αν θέλετε να δημιουργήσετε μόνο ένα αρχείο υπογραφής, τα απαιτούμενα βήματα είναι τα βήματα 1 και 3.
- Για το HP Sure Recover, τα ελάχιστα απαιτούμενα βήματα είναι τα βήματα 1, 2 και 3. Για την υλοποίηση της λύσης στο σύστημα προορισμού θα χρειαστείτε το δημόσιο κλειδί από το βήμα 2.
- Το βήμα 4 είναι προαιρετικό αλλά συνιστάται να το ακολουθήσετε για να διασφαλίσετε τη σωστή επικύρωση των αρχείων υπογραφής και διακήρυξης.

Φιλοξενία αρχείων

Φιλοξενήστε τα παρακάτω αρχεία από τον φάκελο C:\staging στον διακομιστή σας:

- *.swm
- custom.mft (ή το όνομα αρχείου που επιλέξατε για το αρχείο διακήρυξης)
- custom.sig (ή το αντίστοιχο όνομα αρχείου που επιλέξατε για το αρχείο υπογραφής)

ΣΗΜΕΙΩΣΗ: Αν χρησιμοποιείτε τις υπηρεσίες IIS ως λύση φιλοξενίας, πρέπει να διαμορφώσετε τις καταχωρήσεις MIME ώστε να περιλαμβάνουν τις παρακάτω επεκτάσεις ως "application/octet-stream":

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

Υλοποίηση της λύσης στα συστήματα προορισμού

Μπορείτε να υλοποιήσετε τη λύση στα συστήματα προορισμού χρησιμοποιώντας το HP Client Management Script Library, το HP Client Security Manager (CSM)/Sure Recover ή το Manageability Integration Kit (MIK) (https://www.hp.com/go/clientmanagement).

Για τη διαδικασία αυτή θα πρέπει να καταχωρήσετε τις ακόλουθες πληροφορίες:

1. Τη διεύθυνση URL του φιλοξενούμενου αρχείου διακήρυξης (βλ. προηγούμενη ενότητα) (http://your_server.domain/path/custom.mft)
2. Το δημόσιο κλειδί που χρησιμοποιήθηκε για την επαλήθευση του αρχείου υπογραφής που δημιουργήθηκε προηγουμένως (π.χ. C:\staging\my-recovery-public.pem).

Αντιμετώπιση προβλημάτων

Αν εμφανιστεί κάποιο μήνυμα που σας ενημερώνει για την αποτυχία της επικύρωσης ασφαλείας της διαδικασίας προσαρμοσμένης αποκατάστασης, ελέγξτε τα παρακάτω:

1. Το αρχείο διακήρυξης πρέπει να είναι σε μορφή UTF-8 χωρίς σήμανση σειράς byte (BOM).
2. Ελέγξτε τον κατακερματισμό των αρχείων.
3. Βεβαιωθείτε ότι το σύστημα διαθέτει το δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό κλειδί που χρησιμοποιήθηκε για την υπογραφή της διακήρυξης.
4. Οι τύποι MIME του διακομιστή IIS πρέπει να είναι `application/octet-stream`.
5. Οι διαδρομές αρχείων που υπάρχουν στη διακήρυξη θα πρέπει να περιλαμβάνουν την πλήρη διαδρομή προς τον ανώτερο κατάλογο που περιέχει το είδωλο, όπως φαίνεται στο σύστημα-πελάτη. Αυτή η διαδρομή δεν είναι η πλήρης διαδρομή για τη θέση αποθήκευσης των αρχείων στο σημείο διανομής.

3 Χρήση του παράγοντα HP Sure Recover εντός εταιρικού τείχους προστασίας

Ο παράγοντας HP Sure Recover μπορεί να φιλοξενηθεί σε εταιρικά τοπικά δίκτυα. Μετά την εγκατάσταση του HP Sure Recover SoftPaq, αντιγράψτε τα αρχεία του καταλόγου του παράγοντα HP Sure Recover από τη θέση εγκατάστασης σε ένα σημείο διανομής HTTP ή FTP. Στη συνέχεια, καταχωρήστε στο σύστημα-πελάτη τη διεύθυνση URL του σημείου διανομής και το δημόσιο κλειδί HP με την ονομασία `hpsr_agent_public_key.pem`, το οποίο διανέμεται με το HP Sure Recover SoftPaq.

Εγκατάσταση του παράγοντα HP Sure Recover

1. Κατεβάστε τον παράγοντα HP Sure Recover και εξαγάγετε τα αρχεία στο σημείο διανομής HTTP ή FTP.
2. Ορίστε τα κατάλληλα δικαιώματα για τα αρχεία στο σημείο διανομής.
3. Αν χρησιμοποιείτε τις υπηρεσίες Internet Information Services (IIS), δημιουργήστε τύπους MIME application/octet-stream για τις παρακάτω μορφές αρχείων:
   - .
   - .wim
   - .swm
   - .mft
   - .sig
   - .efi
   - .sdi

   ΣΗΜΑΝΤΙΚΟ: Τα παρακάτω βήματα περιγράφουν την υλοποίηση του Sure Recover μέσω του SCCM. Για να δείτε παραδείγματα για την υλοποίηση του Sure Recover μέσω του HP Client Management Script Library, ανατρέξτε στην ενότητα Χρήση του HP Client Management Script Library (CMSL) στη σελίδα 13.
4. Ανοίξτε το SCCM, μεταβείτε στο **HP Client Security Suite** και επιλέξτε τη σελίδα του HP Sure Recover.

   ΣΗΜΕΙΩΣΗ: Η διεύθυνση URL του σημείου διανομής περιλαμβάνει είτε το ftp είτε το http ως πρωτόκολλο μεταφοράς. Περιλαμβάνει επίσης την πλήρη διαδρομή προς τον ανώτερο κατάλογο που περιέχει τη διακήρυξη για τον παράγοντα HP Sure Recover, όπως αυτή εμφανίζεται στο σύστημα-πελάτη. Αυτή η διαδρομή δεν είναι η πλήρης διαδρομή για τη θέση αποθήκευσης των αρχείων στο σημείο διανομής.
5. Στην ενότητα **Είδωλο πλατφόρμας**, επιλέξτε τη ρύθμιση **Εταιρεία** για να κάνετε επαναφορά ενός προσαρμοσμένου ειδώλου λειτουργικού συστήματος από ένα εταιρικό σημείο διανομής. Εισαγάγετε τη διεύθυνση URL που σας έχει δοθεί από τον διαχειριστή IT στο πλαίσιο **Διεύθυνση URL θέσης ειδώλου**. Εισαγάγετε το δημόσιο κλειδί `hpsr_agent_public_key.pem` στο πεδίο **Επαλήθευση ειδώλου**.

   ΣΗΜΕΙΩΣΗ: Η διεύθυνση URL του προσαρμοσμένου ειδώλου πρέπει να περιλαμβάνει το όνομα του αρχείου διακήρυξης του ειδώλου.

6. Στην ενότητα **Παράγοντας αποκατάστασης**, επιλέξτε τη ρύθμιση **Εταιρεία** για να χρησιμοποιήσετε έναν προσαρμοσμένο παράγοντα αποκατάστασης ή τον παράγοντα αποκατάστασης της HP από ένα εταιρικό σημείο διανομής. Εισαγάγετε τη διεύθυνση URL που σας έχει δοθεί από τον διαχειριστή IT στο πλαίσιο **Διεύθυνση URL θέσης παράγοντα**. Εισαγάγετε το δημόσιο κλειδί `hpsr_agent_public_key.pem` στο πεδίο **Κλειδί επαλήθευσης παράγοντα**.

   ΣΗΜΕΙΩΣΗ: Μην συμπεριλάβετε το όνομα αρχείου της διακήρυξης για τον παράγοντα στη διεύθυνση URL, επειδή το BIOS απαιτεί τη χρήση του ονόματος recovery.mft.

7. Αφού εφαρμοστεί η πολιτική, επανεκκινήστε το σύστημα-πελάτη.

8. Την πρώτη φορά που θα εκτελέσετε τη διαδικασία υλοποίησης, θα εμφανιστεί ένα μήνυμα που θα σας ζητάει να καταχωρήσετε έναν τετραψήφιο κωδικό ασφαλείας για να ολοκληρωθεί η ενεργοποίηση του HP Sure Recover. Για περισσότερες λεπτομέρειες, μεταβείτε στην τοποθεσία hp.com και πραγματοποιήστε αναζήτηση για το έγγραφο "HP Manageability Integration Kit (MIK) for Microsoft System Center Manager".

Αφού ολοκληρωθεί επιτυχώς η ενεργοποίηση του HP Sure Recover, η προσαρμοσμένη διεύθυνση URL που εφαρμόστηκε από την πολιτική θα εμφανίζεται στο μενού ρυθμίσεων BIOS του HP Sure Recover.

Για να επιβεβαιώσετε την επιτυχία της ενεργοποίησης, επανεκκινήστε τον υπολογιστή και, όταν εμφανιστεί το λογότυπο της HP, πατήστε το πλήκτρο F10. Επιλέξτε **Advanced** (Για προχωρημένους), **HP Sure Recover**, **Recovery Agent** (Παράγοντας αποκατάστασης) και έπειτα **URL**.

4 Χρήση του HP Client Management Script Library (CMSL)

Το HP Client Management Script Library σας δίνει τη δυνατότητα να διαχειρίζεστε τις ρυθμίσεις του HP Sure Recover μέσω PowerShell. Το παρακάτω παράδειγμα δέσμης ενεργειών δείχνει πώς μπορείτε να υλοποιήσετε το HP Sure Recover, να προσδιορίσετε την κατάστασή του, να αλλάξετε τη διαμόρφωσή του και να καταργήσετε την υλοποίησή του.

ΣΗΜΕΙΩΣΗ: Πολλές από τις εντολές υπερβαίνουν το μήκος γραμμής αυτού του οδηγού. Ωστόσο, στην πράξη, πρέπει να εισάγονται σε μία γραμμή.

```
$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
}
```

Δείγμα δημιουργίας κλειδιών με χρήση του OpenSSL

Αποθηκεύστε τα ιδιωτικά κλειδιά σε ασφαλή τοποθεσία. Τα δημόσια κλειδιά θα χρησιμοποιηθούν για την επικύρωση και θα πρέπει να καταχωρηθούν στο πλαίσιο της διαδικασίας υλοποίησης. Αυτά τα κλειδιά πρέπει να έχουν μήκος 2048 bit και να χρησιμοποιούν εκθέτη 0x10001. Αντικαταστήστε το θέμα των παραδειγμάτων με πληροφορίες σχετικά με τον οργανισμό σας.

Πριν προχωρήσετε, ορίστε την ακόλουθη μεταβλητή περιβάλλοντος:

```
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:
```

Μπορείτε να υπογράψετε τη διακήρυξη του ειδώλου με αυτή την εντολή:

```
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:
```

Μπορείτε να υπογράψετε τη διακήρυξη του παράγοντα με αυτή την εντολή:

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

Το OpenSSL δημιουργεί αρχεία υπογραφής σε μορφή big endian, η οποία δεν είναι συμβατή με ορισμένες εκδόσεις BIOS. Κατά συνέπεια, μπορεί να χρειαστεί να αντιστρέψετε τη σειρά των byte του αρχείου

υπογραφής του παράγοντα πριν προχωρήσετε στην υλοποίησή του. Οι εκδόσεις BIOS που υποστηρίζουν τη σειρά byte big endian υποστηρίζουν και τη σειρά byte little endian.

A Αντιμετώπιση προβλημάτων

Αποτυχία δημιουργίας διαμερισμάτων στη μονάδα

Η δημιουργία διαμερισμάτων στη μονάδα μπορεί να αποτύχει, αν το διαμέρισμα SR_AED ή SR_IMAGE έχει κρυπτογραφηθεί με το Bitlocker. Τα διαμερίσματα αυτά δημιουργούνται συνήθως με ένα χαρακτηριστικό gpt που εμποδίζει την κρυπτογράφησή τους από το Bitlocker. Ωστόσο, αν ο χρήστης διαγράψει και δημιουργήσει εκ νέου τα διαμερίσματα, ή τα δημιουργήσει με μη αυτόματο τρόπο σε μια μονάδα ολικής αποκατάστασης λειτουργικού συστήματος, τότε ο παράγοντας Sure Recover δεν μπορεί να τα διαγράψει με αποτέλεσμα να τερματίζεται η λειτουργία του και να εμφανίζεται ένα σφάλμα κατά τη διαδικασία δημιουργίας νέων διαμερισμάτων στη μονάδα. Ο χρήστης θα πρέπει να διαγράψει τα διαμερίσματα με μη αυτόματο τρόπο εκτελώντας το DiskPart, επιλέγοντας τον τόμο και δίνοντας την εντολή παράκαμψης `del vol` ή άλλη παρόμοια εντολή.

Αρχείο καταγραφής ελέγχου υλικολογισμικού

Οι πληροφορίες για τις μεταβλητές EFI είναι οι εξής:

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

Τα Windows παρέχουν API για την ανάγνωση των μεταβλητών EFI. Εναλλακτικά, μπορείτε να αποτυπώσετε το περιεχόμενο των μεταβλητών σε ένα αρχείο χρησιμοποιώντας το βοηθητικό πρόγραμμα UEFI Shell dmpstore.

Μπορείτε να αποτυπώσετε το αρχείο καταγραφής ελέγχου χρησιμοποιώντας την εντολή `Get-HPFirmwareAuditLog` που παρέχει το HP Client Management Script Library.

Αρχείο καταγραφής συμβάντων των Windows

Τα συμβάντα εκκίνησης και διακοπής του Sure Recover αποστέλλονται στο αρχείο καταγραφής ελέγχου του BIOS. Μπορείτε να δείτε αυτά τα συμβάντα στο αρχείο καταγραφής του Sure Start μέσα από το Πρόγραμμα προβολής συμβάντων των Windows, εφόσον έχετε εγκαταστήσει το HP Notifications. Αυτά τα συμβάντα περιλαμβάνουν την ημερομηνία και την ώρα, το αναγνωριστικό προέλευσης, το αναγνωριστικό συμβάντος και έναν συγκεκριμένο κωδικό συμβάντος. Για παράδειγμα, η εγγραφή `[fe 00 40 26 02 27 06 18 84 2a 02 01 00 30 f2 c3]` υποδηλώνει ότι η αποκατάσταση απέτυχε επειδή δεν ήταν δυνατή η επικύρωση της διακήρυξης με τον κωδικό συμβάντος c3f 23000, το οποίο καταγράφηκε στις 2:26:40 στις 27/6/18.

ΣΗΜΕΙΩΣΗ: Αυτά τα αρχεία καταγραφής χρησιμοποιούν την αμερικανική μορφή ημερομηνίας: μήνας/ημέρα/έτος.

HP Secure Platform Management (κωδικός προέλευσης = 84h)

Πίνακας A-1 HP Secure Platform Management

Αναγνωριστικό συμβάντος	Αριθμός συσκευών (Όλες/DaaS)	Αριθμός συμβάντων (Όλα/DaaS)	Περιγραφή	Σημειώσεις
40	256/178	943/552	Η διαδικασία αποκατάστασης του λειτουργικού συστήματος της πλατφόρμας εκκινήθηκε από το υλικολογισμικό.	Έναρξη αποκατάστασης πλατφόρμας
41	221/147	588/332	Η διαδικασία αποκατάστασης του λειτουργικού συστήματος της πλατφόρμας ολοκληρώθηκε επιτυχώς.	Ολοκλήρωση αποκατάστασης πλατφόρμας
42	54/42	252/156	Η διαδικασία αποκατάστασης του λειτουργικού συστήματος της πλατφόρμας απέτυχε.	Αποτυχία αποκατάστασης πλατφόρμας

Μπορείτε να ανακτήσετε το αρχείο καταγραφής ελέγχου υλικολογισμικού χρησιμοποιώντας την εντολή Get-HPFirmwareAuditLog στο HP Client Management Script Library, το οποίο διατίθεται στη διεύθυνση http://www.hp.com/go/clientmanagement. Τα αναγνωριστικά συμβάντων 40, 41 και 42 του HP Secure Platform Management επιστρέφουν συγκεκριμένους κωδικούς συμβάντων που υποδεικνύουν το αποτέλεσμα των λειτουργιών του Sure Recover. Για παράδειγμα, η ακόλουθη καταχώρηση του αρχείου καταγραφής υποδεικνύει ότι το Sure Recover δεν μπόρεσε να κατεβάσει το αρχείο διακήρυξης ή υπογραφής με το σφάλμα event_id 42 και data: 00:30:f1:c3, το οποίο πρέπει να ερμηνευτεί ως η τιμή 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
```

Η επιτυχής αποκατάσταση εμφανίζεται ως event_id = 41 και data: 00:00:00:00. Για παράδειγμα:

```
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
```

Το HP Sure Recover χρησιμοποιεί τους παρακάτω κωδικούς συμβάντων.

Πίνακας A-2 Κωδικοί συμβάντων

Περιγραφή συμβάντος	Κωδικός συμβάντος
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

Πίνακας A-2 Κωδικοί συμβάντων (συνέχεια)

Περιγραφή συμβάντος	Κωδικός συμβάντος
SureRecoverJsonParsingFailed	0xC3FF2000
RebootRequestFailed	0xC3FF3000
UnableToReadConfigFile	0xC3FF4000
FailedToDetectWindowsPE	0xC3FF5000