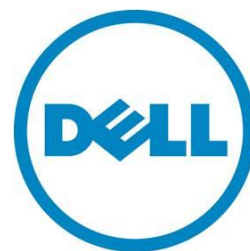

Server Profile Import and Export

Securing a known coherent state for system firmware and configurations

Weijia Zhang

Bill Edwards

Vance Corn



This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2012 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Windows is a registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

February 2012| Rev 1.0

Contents

Executive summary.....	4
Introduction	4
System and setup requirements.....	4
Setup	4
Export system profile	5
Workflow	5
Using WSMAN methods	6
Using Python sample scripts	7
Import system profile	8
Workflow	8
Using WSMAN methods	9
Using Python sample scripts	10
Best practices	11
Conclusion	11

Figures

Figure 1. Export system profile process.....	6
Figure 2. Import system profile process	9

Executive summary

Server profile import and export is a cutting-edge feature of Lifecycle Controller that allows users and field technicians to fully capture and restore BIOS and firmware in any system state—including bare metal or system down. This capability provides an automatic one-touch solution for hardware or firmware problems in use scenarios such as motherboard replacement.

Introduction

Import and Export Server Profile put systems back to its original coherent state in minutes. No more manual firmware update and reconfiguration needed.

Dell introduces the export server profile and import server profile features in Lifecycle Controller which allows IT administrators to backup and restore configurations and firmware for a PowerEdge server. The export and import server profile features are controlled by two interfaces:

1. Unified Server Configurator (USC)—A graphical UI tool for local access of the Lifecycle Controller features in a pre-OS environment. An export and import can be started in the USC interface (refer to the *User's Guide* for more information).
2. Remote Services—WS-Management (WSMAN) web services interfaces. The import and export profile interfaces are defined in the Lifecycle Controller (LC) Management Profile 1.2. This interface allows the scheduling of an import or export.

The export profile feature produces a file that contains the configuration and the currently installed firmware packages for the Lifecycle Controller supported devices including iDRAC, BIOS, PERC RAID controllers, and NICs. The import profile feature updates the firmware of the devices and sets the configuration of devices to that which is saved in the server profile.

The new export feature runs in the background and does not interfere with the host processing.

The new import allows for the easy return of firmware and configuration to the previous server profile backup level. This covers hardware replacement scenarios as well as rollback to a previous level of configuration and firmware.

System and setup requirements

- Dell PowerEdge 11th Generation
- iDRAC Enterprise with Lifecycle Controller revision 1.5 or higher
- Dell vFlash with Enterprise License
- Dell PowerEdge 12th Generation or Custom system based on the 12th Generation
- iDRAC Enterprise with Lifecycle Controller 2 revision 1.0 or higher
- Enterprise License
- SD Card required for USC based usage

Setup

1. For 12G, ensure your Enterprise License level iDRAC is set up according to the user documentation for the iDRAC with Lifecycle Controller. Collect System Inventory On System Restart (CSIOR) must be enabled. Restart at least once after CSIOR is enabled.
2. If the export destination is vFlash:
 - a. Make sure supported vFlash media is inserted in the maintenance port.
3. If the export destination is a network share:
 - a. Select the network connection for iDRAC to use.
 - b. Establish network parameters.
 - c. Make sure the physical network connection is present and active.

The import and export server profile features are now available for use.

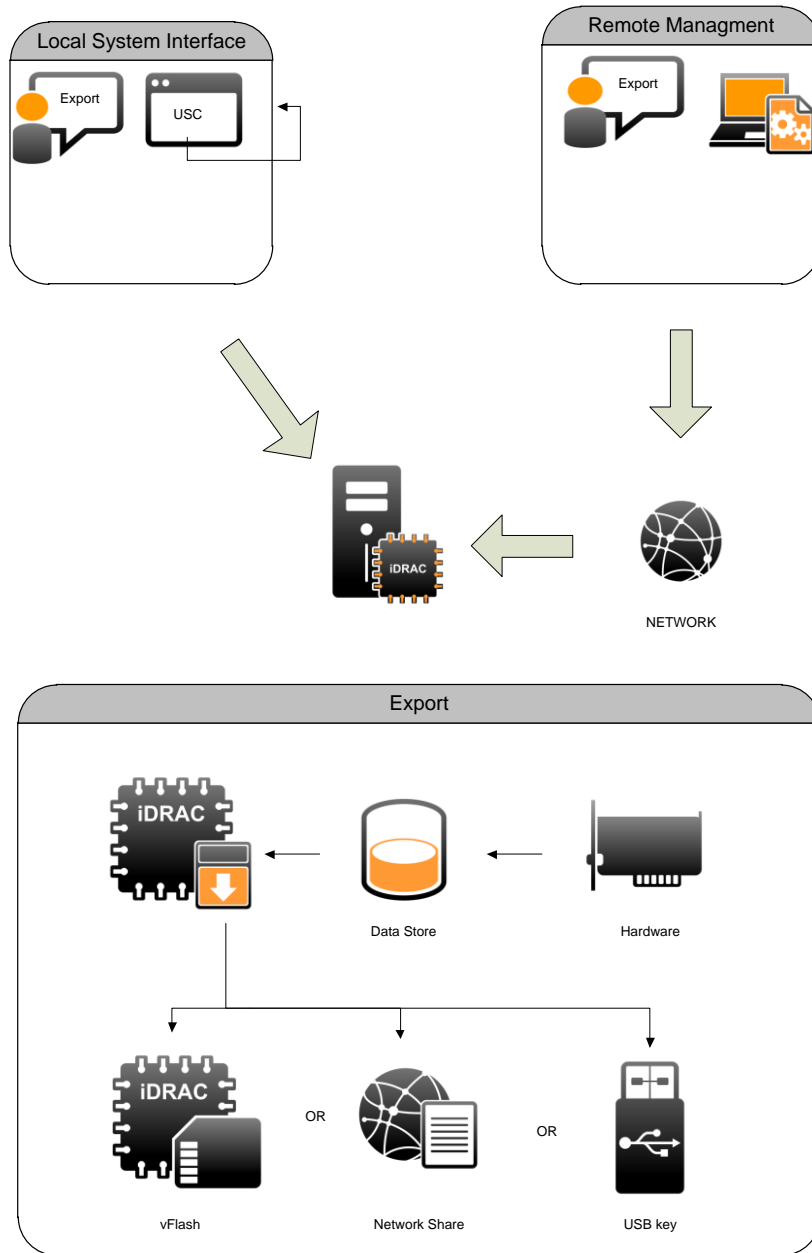
Export system profile

Export system profile is a process of extracting BIOS and firmware information and save them into an image file for later restoration as shown in Figure 1. When the user starts the export system process, the viewable data such as servicetag, system type, firmware versions, are collected. These data are in plain text to allow users to read it without decryption or decompression. When a chunk of data is saved, its hash value is calculated and saved to a portion of the image file to prevent tampering. The process then starts reading the specific storage location for firmware and configuration. Each category of the firmware is saved to a specific section. For example, the USC, Firmwares, iDRAC firmware are saved to different portions of the backup image file. For categories such as configuration information that contain user-sensitive data, the bits are encrypted with a password to ensure that data is safe in the image file.

Workflow

After all categories of the system profile are saved to the image file, the hash value of the content is recalculated and saved to the system. The final image is then made tamper-proof with optional passphrase protection.

Figure 1. Export system profile process



Using WSMAN methods

The method for exporting system would take in target and storage profile location, transport protocol and access credential for backup the image. The method is provided by Lifecycle Controller provider.

Method name: BackupImage

Parameters:

Import and Export of Secure Server Profiles

- Storage Location
- Transport Protocol
- Access credential (Username and Password)
- Passphrase for the image

Once a backup method is called, it will validate input parameters and create a backup job if valid parameters have been collected. If there is a missing or error parameter, the provider will return an error and a modified request would need to be sent. Once the request is validated, the system would stage the export request information and send a job id back to the system. User can then use job id to schedule the operation or track the export status.

A WSMAN command can be sent either through OpenWSMAN client in Linux or through winrm in Windows. The syntax of an export WSMAN request can be found in the Web Services Interface Guide.

Once a job starts, you can query the status and progress of the job by using JobControl provider's job status method. The response would include the job message and progress information. Refer to Job Control provider to see how to query job status.

Using Python sample scripts

To help system administrators simplify and automate management tasks, a set of sample scripts have been provided and are downloadable from DellTechCenter (see More Information section for details).

To start a backup image process, simply invoke script:

```
backup_image.py
```

You can get help option with `-h`.

One example of the backup is shown with the following syntax:

```
backup_image.py -i TargetIP -u UserName -p Password -f  
backup_setting.txt
```

Where **TargetIP** is the IP address of the target system, and **UserName** and **Password** are the login credentials for the iDRAC.

`Backup_setting.txt` is the backup operation settings. A sample backup setting is shown below:

```
# Sample input file for backup image  
#  
# ShareType - 0:NFS, 2:CIFS, 4:VFlash  
# Examples:  
# NFS - ImageName,IPAddress,ShareName are required  
#  
ShareType=0
```

Import and Export of Secure Server Profiles

```
ImageName=bk_20111130.img
IPAddress=192.168.0.77
ShareName=/nfsshare
# Start time for job to start
# In datetime format:yyyymmddhhmmss
# The string "TIME_NOW" means immediate.
ScheduledStartTime=TIME_NOW
#ScheduledStartTime=20120707000000
```

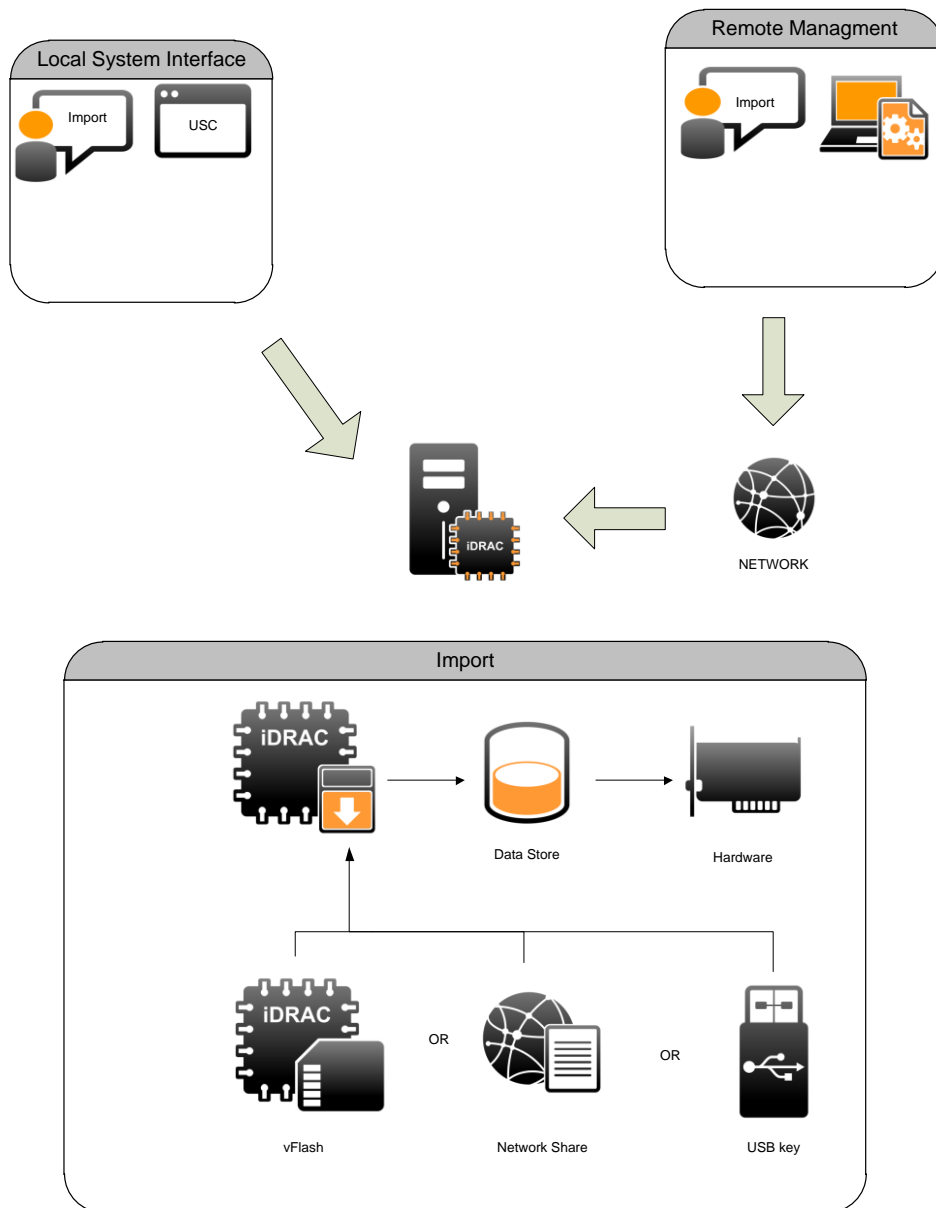
In the above sample setting, the storage type (ShareType), backup image name, storage location and share name are specified. Once the script is executed with the correct parameters, it will output a JobID which identifies this backup job. The status of this job can be queried via jobget.py script. The jobget.py with a JobID as input parameter will return job status, percentage completed, and messages.

Import system profile

Workflow

Import system profile is a process whereby the captured image file is returned to the target, the firmware is refreshed, and the system reconfigured as shown in Figure 2. When the user starts the import system process, the image file is first validated for any corruption or tampering. The bits are then decrypted and uncompressed if necessary, and copied to the specific location of the system. The system then restarts in the host space and restores the firmware and configurations.

Figure 2. Import system profile process



Using WSMAN methods

The WSMAN method for importing a system profile would take in target and storage location, transport protocol and access credentials for backing up the image. The method is provided by the Lifecycle Controller provider.

Method name: RestoreImage

Parameters:

- Storage Location
- Transport Protocol
- Access credential (Username and Password)
- Passphrase for the image

Once a `RestoreImage` method is called, it will validate input parameters and create a Restore job if valid parameters have been collected. If there are missing or incorrect parameters, the provider will return an error, and a modified request would need to be sent. Once the request is validated, the system would stage the import request information and send a job id back to the system. The user can then use the job id to schedule the operation or track the export status.

A WSMAN command can be sent either through OpenWSMAN client in Linux or through `winrm` in Windows. The syntax of an export WSMAN request can be found in the Web Services Interface Guide.

Once a job starts, the user may query the status and progress of the job using the `JobControl` provider's job status method. The response would include the job message and progress information. Refer to Job Control provider for more information on how to query job status.

Using Python sample scripts

The python sample script for restore is similar to the script used for backup. To start a restore image process, simply invoke the script:

```
restore_image.py
```

You can get a help option using `-h`.

One example of the backup is shown with the following syntax:

```
restore_image.py -i TargetIP -u UserName -p Password -f restore_setting.txt
```

Where **TargetIP** is the IP address of the target system, and **UserName** and **Password** are the login credentials for the iDRAC

`Restore_setting.txt` is the restore operation settings. A sample restore setting is shown below:

```
# Sample input file for restore image
#
# ShareType - 0:NFS, 2:CIFS, 4:VFlash
# Examples:
# NFS - ImageName,IPaddress,ShareName are required
ShareType=0
ImageName=bk_20111130.img
IPAddress=192.168.0.77
```

Import and Export of Secure Server Profiles

```
ShareName=/nfsshare  
  
...  
  
# Start time for job to start  
  
# In datetime format:yyyymmddhhmmss  
  
# The string "TIME_NOW" means immediate.  
  
ScheduledStartTime=TIME_NOW  
  
#ScheduledStartTime=20120707000000
```

In the above sample restore setting, the storage type (ShareType), backup image name, storage location and share name are specified. Once the script is executed with correct parameters, it will output a JobID which identifies this restore job. The status of this job can be queried via jobget.py script. The jobget.py with a JobID as input parameter will return job status, percentage completed, and messages.

Best practices

Import and export server profile involves multiple components and steps, and the following best practices are suggested

- Make sure that the network is connected and the storage device is working properly.
- When import or export procedures are taking place, no operations that might change the system state should be performed.
- The import and export processes will show what task is running and what stage it is in.
- Import and export might take up to one hour depending on the configuration of the system.
- At the end of iDRAC import, the system needs to reboot iDRAC and the server might lose communication for one or two minutes. This is normal.

Conclusion

To aid in redeployment or system recovery, the export operation should be performed each time there is a configuration change. Configuration changes range from changes in custom user settings to the update of device firmware. This will enable the customer to easily restore a known coherent state.

More Information

<http://en.community.dell.com/techcenter/systems-management/w/wiki/1979.lifecycle-controller.aspx>