Import and Export of Server Profiles

How to Secure Systems Firmware and Configuration to a Known Coherent State

Weijia Zhang, Bill Edwards, and 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. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or 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

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

Executive summary

Server profile import and export is a cutting-edge feature of Lifecycle Controller that lets users and field technicians 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

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

- Unified Server Configurator (USC) - A graphical UI tool for local access of the Lifecycle Controller features in a pre-OS environment. Start an export and import in the USC interface.
- Remote Services – WS-Management 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 those saved in the server profile.

The new export feature runs in the background and does 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 previous level of configuration and firmware.

System and setup requirements

Dell PowerEdge 11th Generation servers

- iDRAC Enterprise with Lifecycle Controller revision 1.5 or higher
- Dell vFlash with enterprise license

Dell PowerEdge 12th Generation servers or Custom system based on the 12th Generation

- iDRAC Enterprise with Lifecycle Controller 2 revision 1.0 or higher

- Enterprise license
- Dell vFlash required for USC based usage

Setting up the Import and Export Server profile features:

1. Install the enterprise license as instructed in the user documentation for the iDRAC with Lifecycle Controller.
2. Enable Collect System Inventory on system restart (CSIOR).
3. Enable the collection of system inventory.
4. If the export destination is vFlash:
    a. Make sure supported vFlash media is inserted in the maintenance port.
5. 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.

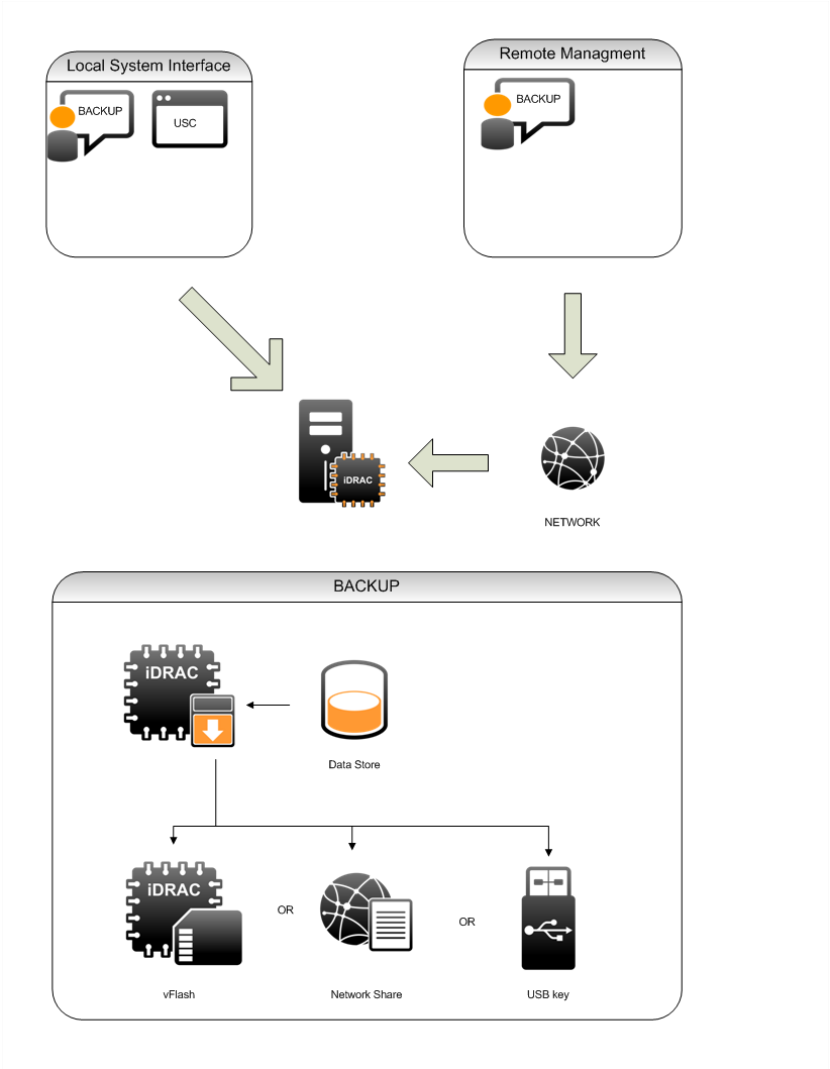
Export system profile

The Export system profile is a process of extracting BIOS and firmware information and saving them into an image file for later restoration as shown in Figure 1. When users start the export system process, the viewable data such as servicetag, system type, and firmware versions are collected. The data is in plain text to let users read it without decryption or decompression. When a chuck 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 specific storage location for firmware and configuration. Each category of the firmware is saved to a specific section. For example, the USC, Firmwares, and iDRAC firmware are saved to different portions of the backup image file. For categories such as configuration information that contains user sensitive data, the bits are password encrypted to make sure 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 re-calculated and saved to the system. The final image is then tamper-proof with optional passphrase protection.

Figure 1. Exporting a system profile.



Methods

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

Method name: BackupImage

Parameters:

Storage Location

Transport Protocol

Access credential (Username and Password)

Passphrase for the image (alphanumerical with min 6 chars and max 20 characters Look like Raid profile LKM passphrase)

Once a backup method is called, it validates input parameters and creates a backup job if valid parameters have been collected. If there is a missing or error parameter, the provider returns an error and a modified request is sent. Once the request is validated, the system stages the export request information and sends a job id back to the system. Users can then use a job id to schedule the operation or tract 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 is shown below:

```
winrm i BackupImage http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_LCService?SystemCreationClassName=DCIM
_ComputerSystem+CreationClassName=DCIM_LCService+SystemName=DC
IM:ComputerSystem+Name=DCIM:LCService -u:[idrac-username] -
p:[idrac-password] -r:https://[TarggetIPAddress]/wsman -
SkipCNCheck -SkipCACheck -encoding:utf-8 -a:basic
@{IPAddress=[IPAddress];ShareName="/tmp";ShareType=[ShareType]
;Username="root";Password="[Passphrase]";ImageName=[BackupImag
eName];ScheduledStartTime=[StartTime]}
```

Here BackupImage is the method name for exporting system profile. The [TargetIPAddress] is the IP of the target system. IPAddress attribute is for the IP address of the storage. Sharename is the name of the share in which the image file is stored.

ShareType is the type of share such as 0 for NFS, 2 for CIFS, and 4 for vflash. [StartTime] is the scheduled start time for the export to start.

For the security credentials, idrac-username and idrac-password are the login credentials for users to get to the iDRAC sub-system. To protect the image, there is also a passphrase that you use to encrypt the export image file.

In addition, you can schedule the export command. The ScheduledStartTime is the time to start the export. If you want to start immediately, use TIME_NOW. Otherwise, specify a detailed time in the ScheduledStartTime.

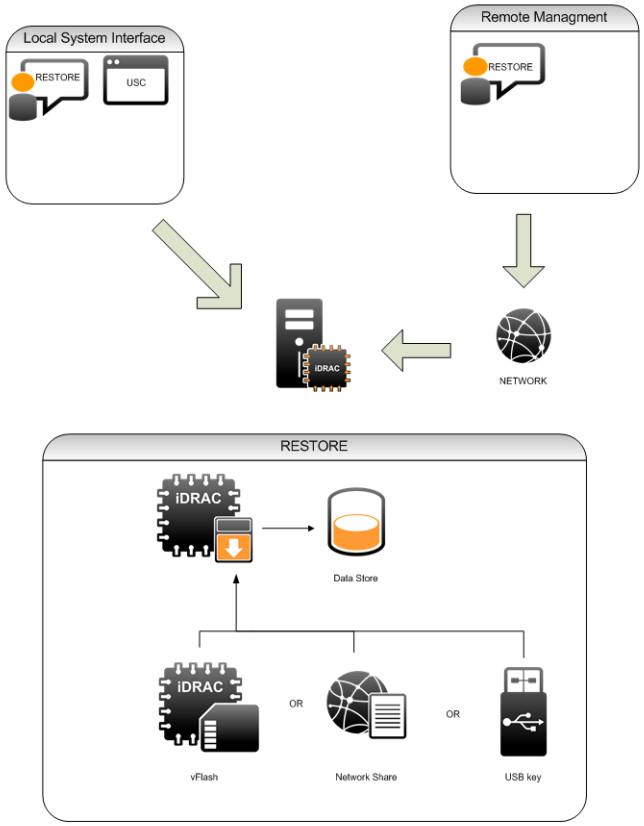
Once a job starts, you can query the status and progress of the job by using JobControl provider's job status method. The response would include the job message and progress information. Refer to Job Control provider to see how to query job status.

Import System Profile

Workflow

The Import system profile is the process of returning the captured image file to the target, refreshing the firmware, and re-configuring the system, as shown in Figure 2. When you start 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 back the firmware and configurations.

Figure 2. The Import System profile process.



Methods

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

Method name: RestoreImage

Parameters:

Storage Location

Transport Protocol

Access credential (Username and Password)

Passphrase for the image (alphanumerical with min 6 chars and max 20 characters Look like Raid profile LKM passphrase)

Once a RestoreImage method is called, it validates input parameters and creates a Restore job if valid parameters were collected. If there is a missing or error parameter, their provider return error and a modified request must be sent. Once the request is validated, the system stages the import request information and sends a job id back to the system. You can then use the job id to schedule the operation or tract the import status.

Send a WSMAN command either through an OpenWSMAN client in Linux or through winrm in Windows. The syntax of an import WSMAN request is shown below:

```
winrm i RestoreImage http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_LCService?SystemCreationClassName=DCIM
_ComputerSystem+CreationClassName=DCIM_LCService+SystemName=DC
IM:ComputerSystem+Name=DCIM:LCService -u:[idrac-username] -
p:[idrac-password] -r:https://[TarggetIPAddress]/wsman -
SkipCNCheck -SkipCACheck -encoding:utf-8 -a:basic
@{IPAddress=[IPAddress];ShareName="/tmp";ShareType=[ShareType]
;Username="root";Password="[Passphrase]";ImageName=[BackupImag
eName];ScheduledStartTime=[StartTime]}
```

Here RestoreImage is the method name for importing system profile. The [TargetIPAddress] is the ip of the target system. IPAddress attribute is for the IP address of the storage. Sharename is the name of the share in which the image file is stored.

ShareType is the type of share such as 0 for NFS, 2 for CIFS, and 4 for vflash. [StartTime] is the scheduled start time for the import to start.

For the security credentials, idrac-username and idrac-password are the login credentials for users to get to the iDRAC sub-system. In addition, to protect the image, there is also a passphrase that you use to encrypt the import image file.

Also, you can schedule the import command. The ScheduledStartTime is the time to start the import. If you want to start immediately, use TIME_NOW. Otherwise, specify a detailed time in the ScheduledStartTime.

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.

Best Practices

Import and Export Server Profile involves multiple components and steps and the following are suggested

- Make sure that the network is connected and the storage is working properly.
- When import or export is in process, do not run operations that might change the system state.
- The import and export process shows what task is running and what stage they are in.
- The import and export process might take up to one hour depending on the configuration.

Conclusion or Summary

To aid in redeployment or system recovery perform the export operation each time there is a configuration change. Configurations changes range from custom user settings to the update of device firmware. This lets you easily return to a known coherent state.