White Paper

Server Configuration Profiles: Reference Guide

An end-to-end guide for DellEMC’s Server Configuration Profiles (SCP).

Abstract

The Server Configuration Profiles: Reference Guide covers all aspects of SCP’s template-based server configuration, updates and operating system deployment operations, along with a multitude of examples and tutorials.

December 2021

Revisions

Date	Description
December 2020	Initial release

Acknowledgements

This paper was produced by the following:

Author: Charles ‘Danny’ Stracener

Support: Texas Roemer, Doug Iler

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Table of contents

Revisions....2
Acknowledgements....2
Table of contents 3
Executive summary....7
1 Getting Started 8
1.1 What are Server Configuration Profiles? 8
1.2 Important Terms and Acronyms 8
1.3 CSIOR 8
1.4 SCP Export....8
1.5 SCP Import 9
1.6 SCP Import Preview 9
1.7 Jobs 9
1.8 iDRAC Lifecycle Logs....9
1.9 SCP Import / Preview Configuration Results....10
1.10 Available Interfaces 11
2 Template....12
2.1 Structure 12
2.1.1 SystemConfiguration 12
2.1.2 Components 12
2.1.3 Attributes....12
2.2 XML Layout....13
2.3 JSON Layout 13
3 SCP Export....15
3.1 Selective Export....15
3.2 Read Only Attributes 15
3.3 Include Password Hashes 16
3.3.1 iDRAC User Passwords 16
3.3.2 BIOS Password SHAs 16
3.4 Export Type - Clone and Replace 17
3.4.1 Clone and Replace with passwords 17
3.4.2 Clone and Replace with storage devices 17
3.5 Include Custom Telemetry....18
3.6 Available Interfaces 19
3.6.1 iDRAC GUI 19

3.6.2 racadm 19
3.6.3 Redfish..19
4 SCP Import 21
4.1 Host Reboot..22
4.2 Shutdown Type..23
4.2.1 Shutdown Type: Graceful 23
4.2.2 Shutdown Type: Forced 23
4.2.3 Shutdown Type: NoReboot 23
4.3 End Host Power State 24
4.4 Dependencies..24
4.5 Backwards Compatibility 24
4.6 Selective Import..24
4.7 Available Interfaces 25
4.7.1 iDRAC GUI 25
4.7.2 racadm..25
4.7.3 Redfish..25
5 SCP Import Preview 27
5.1 Available Interfaces 27
5.1.1 iDRAC GUI 27
5.1.2 racadm..27
5.1.3 Redfish..27
6 iDRAC Configuration 28
6.1 Template Example..28
6.2 Creating and configuring an iDRAC User..28
6.3 Clearing an iDRAC User..29
6.4 SSHPublicKey 29
6.5 Certificates..29
6.6 Password Settings..31
6.7 AutoUpdate..31
7 LifecycleController..33
8 EventFilters..34
9 RAID / Storage Configuration and Operations..35
9.1 Create and initialize a virtual disk..35
9.2 RAIDresetConfig..36
9.3 RAIDdedicatedSpare..36
10 BIOS Configuration 38

10.1 Workload profiles 38
10.2 F1 / F2 Error Prompt 38
10.3 Changing the Boot Order 38
10.4 Enable or disable a boot order entry 39
10.5 System and setup passwords 39
10.6 PXE (Preboot Execution Environment) 40
11 NIC / FiberChannel / InfiniBand Configuration 41
11.1 LegacyBootProto and PXE 41
11.2 VirtualizationMode 41
11.3 InfiniBand modes 42
12 SupportAssist Operations 44
12.1 Registration 44
12.2 Configuration 45
13 RepositoryUpdates 47
13.1 Workflow 47
14 iDRAC Direct (SCP via USB) 50
14.1 Setup 50
14.2 Execution 51
15 OS Deployment 52
15.1 Attributes 52
15.2 Example 52
15.3 OS Deployment via USB 53
16 Telemetry Operations 54
16.1 Example 54
16.2 Custom Metric Report Definitions 54
16.3 Troubleshooting 55
16.3.1 Missing License 55
16.3.2 Telemetry Not Enabled 56
16.3.3 Schema Validation Error 56
17 Secure Enterprise Key Management Operations 57
17.1 Prerequisites 57
17.2 Example XML 57
17.3 Enabling SEKM settings on the iDRAC 58
17.4 Enable SEKM on a PERC device with a locked RAID volume 60
18 Auto Config – DHCP Provisioning 62
19 Troubleshooting 63

19.1 Configuration results and LCL 63
19.2 Known Limitations....63
19.3 Common Issues....63
19.3.1 SYS041 – Schema validation error....63
19.3.2 SYS051 – Unable to shut down in time....64
19.3.3 SYS055 – Completed with Errors 64
19.3.4 SYS072 – Time Out 65
20 Additional Resources 67
20.1 White Papers 67
20.1.1 Using Server Configuration Profiles to Deploy Operating Systems to Dell EMC PowerEdge Servers: 67
20.1.2 Server cloning by using Server Configuration Profiles on PowerEdge servers: 67
20.2 Default, Clone & Replace Tables 67

Executive summary

Managing all the various aspects of a server's configuration can be complex. Making changes to a server's configuration, firmware versions, or even repurposing the server with a new operating system usually requires multiple individual operations to reach the desired end state. Dell EMC's Server Configuration Profiles (SCP) simplifies these operations by providing a single XML or JSON template that can be used to make changes to configuration, firmware and redeploy the operating system with a single command. This single template can be reused to apply the same deployment across many servers.

The goal of this document is to cover all aspects of SCP's verbose feature set, and how utilizing this tool will help streamline any system's management workflow.

1 Getting Started

1.1 What are Server Configuration Profiles?

Server Configuration Profiles (SCP) are XML or JSON templates that contains configuration settings for an individual server. Each configurable setting is a simplified name-value pair. In addition to configuration settings, the SCP template is equipped with attributes that can trigger specific workflows like firmware updates and operating system deployment. The biggest benefit of SCP templates is that all these settings and options are available in a single, easily readable, and editable template that can be reapplied to any number of setups.

1.2 Important Terms and Acronyms

- iDRAC – Integrated Dell Remote Access Controller
- SCP – Server Configuration Profiles
- Template – The XML or JSON file generated by SCP Export and consumed by SCP Import, SCP Import Preview.
- Interface – In the context of this document, this will mean the iDRAC GUI, racadm, WS-Man or Redfish.
- Golden Template – The fully prepared singular template used when configuring many servers.
- JID – Job Identifier
- FQDD – Fully Qualified Device Descriptor
- OSD – Operating System Deployment
- LCL – Lifecycle Controller Log
- CSIOR – Collect System Inventory on Restart
- CLI – Command Line Interface; In the context of this document, it will commonly be shorthand for racadm, WS-Man or Redfish.

1.3 CSIOR

Collect System Inventory on Restart (CSIOR) is the device inventory collection process that occurs just before the host has finished booting. CSIOR is enabled by default. To ensure that the SCP template has the latest configuration data, it is recommended to keep CSIOR enabled.

```
racadm>>get LifecycleController.LCAttributes.LifecycleControllerState
Enabled
```

1.4 SCP Export

SCP Export is the process in which the XML or JSON template is generated. This template can be exported locally or to a network share.

More information on the template format can be found in Template.

More information on SCP Export and all available options can be found in SCP Export.

1.5 SCP Import

SCP Import is the process in which the XML or JSON template is applied to the server. Any configuration settings available in the template will be applied. Any workflows (OSD and firmware update) triggered by the template will also be performed during this operation. SCP Import may restart the host system multiple times to apply all requests but will only restart the host if required. Results and any potential errors can be found in either exporting the Lifecycle Controller Log (LCL) or configuration results for the SCP import job ID using CLI interface.

More information about configuration results can be found in SCP Import / Preview Configuration Results.

More information on SCP Import workflows and all available options can be found in SCP Import.

1.6 SCP Import Preview

SCP Import Preview allows validation of the XML or JSON template against the host server without applying settings, firmware, or other workflows. Any errors detected during this operation will be logged to the LCL. SCP Import Preview is useful for identifying issues with a template without needing to run a full SCP Import operation or shutting down the host.

More information on SCP Import Preview can be found in SCP Import Preview.

1.7 Jobs

SCP operations create a 'Job' for tracking purpose that will contain useful information about the current status of the operation. The job is identified by a JID (Job Identifier) that will be returned when the SCP operation is created.

All iDRAC jobs can be found in the iDRAC GUI under Maintenance > Job Queue or through any iDRAC interface. See the racadm example below.

```
racadm jobqueue view -i JID_952589510966
---------------------------- JOB -------------------------
[Job ID=JID_952589510966]
Job Name=Configure: Import Server Configuration Profile
Status=Completed
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Mon, 20 Jul 2020 10:29:11]
Actual Completion Time=[Mon, 20 Jul 2020 10:29:13]
Message=[SYS053: Successfully imported and applied Server Configuration Profile.]
Percent Complete=[100]
----------------------------------------------------------
```

Note: Only one SCP operation can be run at a time.

1.8 iDRAC Lifecycle Logs

The Lifecycle Logs contain a sequence of XML events posted by various iDRAC and host operations. SCP operations will log all critical information to the LCL. SCP job start, progress, and completion states can be reviewed in the LCL.

The LCL can be viewed or exported under Maintenance > Lifecycle Log in the iDRAC GUI. iDRAC CLI's also provide methods for exporting the LCL. Please refer to the iDRAC User's Guide for full details.

1.9 SCP Import / Preview Configuration Results

SCP Import will generate LCL events as it progresses through the operation. When a configuration attribute is applied or failed to apply, an LCL event will be logged with details under a configuration results node. These ConfigResult entries will include critical information about settings that were applied or reasons why a setting might have failed to apply. If an SCP Import operation ends with a status of Failed or Completed with Errors, the configuration results will be the best place to start help identify a solution.

Configuration results can be viewed via most interfaces or by exporting the LCL. See the racadm example below.

```
racadm lclog viewconfigresult -j JID_952589510966
SeqNumber        = 20585
FQDD             = iDRAC.Embedded.1
Job Name         = Import Configuration
Operation Name   = CHANGE
DisplayValue     = Web Server Idle Timeout
Name             = WebServer.1#Timeout
OldValue         = 1805
NewValue         = 1801
Status           = Success
ErrCode          = 0
```

The example below is using an intentionally incorrect value to show an error condition.

```
racadm lclog viewconfigresult -j JID_033107879045
SeqNumber        = 5933
FQDD             = iDRAC.Embedded.1
Job Name         = Import Configuration
Operation Name   = CHANGE
DisplayValue     = Web Server Idle Timeout
Name             = WebServer.1#Timeout
OldValue         = 1800
NewValue         = badvalue
MessageID        = RAC015
Status           = Failure
ErrCode          = 9240
```

The RAC015 error message according to the Event and Error Message Reference Guide translates to "Unable to run the method because the input value is not one of the possible values for AttributeName Webserver.1#Timeout ." The value is expecting an integer but received a string, so the failure is expected.

SCP Import Preview will only log ConfigResult entries for any errors detected in its evaluation of the template. These errors will commonly be dependency issues, invalid settings, differences in setup, etc. The errors logged by SCP Import Preview will trigger an error in SCP Import.

1.10 Available Interfaces

Server Configuration Profiles are available through multiple iDRAC interfaces. This document will provide examples for the iDRAC GUI, racadm, and Redfish. Refer to the user interface's guide for all available options.

Server Configuration Profiles can be located under the iDRAC GUI via Configuration > Server Configuration Profiles.

The racadm 'get' and 'set' commands using the type (-t) of 'xml' or 'json' will invoke the Server Configuration Profile workflows.

Redfish operations will be detailed in each of the individual sections.

2 Template

The template is the XML or JSON file generated by an SCP Export. This section will cover the difference between the two formats, as well as the overall structure of the template.

2.1 Structure

At a high level, both formats follow a similar structure.

```
SystemConfiguration
 -   Components
 -   -   Attributes
```

2.1.1 SystemConfiguration

SystemConfiguration is the root node in both formats. It contains properties like Model, ServiceTag, and Timestamp which are populated based on the system information where the template was generated.

The template can also be generated with informational comment data that provides more details about how the template was generated.

2.1.2 Components

Components will be children of SystemConfiguration and will be uniquely identified by a Fully Qualified Device Descriptor (FQDD). The FQDD format is- iDRAC.Embedded.1, BIOS.Setup.1-1, etc. There can be numerous components per template, but each component is unique.

Example: `<Component FQDD="NIC.Slot.4-1-1">`

The FQDD helps describe the device and in some cases the physical location of the device in the target server. When applying a template to many servers, it’s critical that the slot devices are located in the same slot position in the target server. If the template’s FQDD points to slot 3, but the target device is present in slot 4 then the configuration will not be applied. See Golden Template for more recommendations.

NOTE: In the case of storage devices, components can also be nested within components.

2.1.3 Attributes

Attributes will be children of Components and are name-value pairs used to identify and set specific component configuration settings.

Example: `<Attribute Name="BlnkLeds">0</Attribute>`

The behavior of all attributes is driven by the Attribute Registry. This registry contains attribute information like description, possible values, read-only status, dependency data, and much more.

The latest version of the Attribute Registry can be located at the link below:

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

If issues are encountered with a specific attribute, then the Integrated Dell Remote Access Controller 9 Attribute Registry is the best place to start.

2.2 XML Layout

XML is the default mode for SCP Export.

The content between the Attribute nodes can be edited and applied via SCP Import. In the example below, changing the VirtMacAddr from F4:02:70:B4:13:AB to F4:02:70:B4:13:DB will trigger a set operation on NIC.Embedded.2-1-1 during an SCP Import.

```
<SystemConfiguration Model="PowerEdge R740" ServiceTag="G123456" TimeStamp="Tue Jul 21
13:56:41 2020">
  <Component FQDD="NIC.Embedded.2-1-1">
    <Attribute Name="VirtMacAddr">F4:02:70:B4:13:DB</Attribute>
```

Some attributes will be commented out by default in XML mode. The example below shows the VirtMacAddr attribute surrounded by XML comments represented by the <!-- --> markup. Commented attributes will be ignored during SCP Import. If a commented setting needs to be applied, then simply remove the comment markup before calling SCP Import.

```
    <!-- <Attribute Name="VirtMacAddr">F4:02:70:B4:13:DB</Attribute> -->
```

There are additional options available which simplify which attributes will be commented and uncommented when generating the template. These modes will be covered in the Clone and Replace sections below.

2.3 JSON Layout

JSON is an optional format that can be requested when generating a template. The overall template structure is like XML but there are some key differences. The most important of which is the layout of the individual attributes.

```
   { "Name": "IPMILan.1#Enable",
     "Value": "Enabled",
     "Set On Import": "True",
     "Comment": "Read and Write" },
```

In XML, sets are determined by whether or not an attribute was commented out. The JSON data format does have a concept of comments. Attributes include a 'Set On Import' item, that when set to 'True' will apply the setting during an SCP Import.

There's also an informational item 'Comment' which will either be 'Read and Write' or 'Read Only'.

2.4 Golden Template (One to Many)

Throughout this document the term 'golden template' is used frequently to describe a single template used to apply a unified configuration across many servers. The SCP Export section below will go over many of the details required for generating a template, but here are some general guidelines that should be followed.

2.4.1 Recommendations

1. Generate a template from a fully configured server.
    a. Selective Export to include only desired components.
    b. Clone or Replace is generally recommended.

    c. Include Password Hash is recommended in mirroring iDRAC user / BIOS password settings.

2. Remove unwanted attributes or components from the template.
3. Confirm that target servers have a similar physical device location setup.
4. If not using RepositoryUpdate, confirm that the target servers have similar iDRAC and device firmware levels.

2.4.2 Active Directory Example

Configuring Active Directory on many iDRACs is a great example of how a golden template can be utilized. There are a significant number of Active Directory settings and configuring them directly from the XML/JSON template could prove to be difficult.

Instead, configure a single iDRAC's Active Directory settings from the iDRAC GUI and confirm that the settings are working as intended. Once confirmed, generate a template using SCP Export with the Clone option. The template will contain populated values for Active Directory. The template can be adjusted if needed, and then applied to an unlimited number of iDRACs to setup Active Directory on these systems.

That's the true strength and flexibility of SCP. It enables the transfer of configuration settings to many setups with a single template.

2.5 General Compatibility

There are a few things to consider regarding the compatibility of the template. Server Configuration Profiles were originally introduced with iDRAC7 and this document is being released alongside iDRAC9 version 4.40. Over the lifespan of SCP, new features have been added that may not be compatible with older versions of iDRAC.

Additionally, feature sets for individual devices can change over their lifetime. The possible values for attributes might be added or removed, or entire attributes might have been added or removed depending on the firmware version of a device.

The factors like server model, platform capabilities, and license level can impact the presence of attributes in a generated template or result in potential errors when applying a conflicting template.

SCP was designed to take all these factors into consideration. The template itself is backwards compatible throughout all generations of iDRAC. The schema has remained unchanged from release until iDRAC9 version 4.40. See Include Custom Telemetry.

SCP Import is also a 'continue on error' operation, which means if a setting fails to apply the remainder of the settings will still be attempted. Any errors encountered will be clearly communicated in the configuration results of the job.

It is recommended, but not necessary, to generate a template from a server that has a similar configuration to the target server(s). This will help reduce the chances of errors during SCP Import.

3 SCP Export

Server Configuration Profile Export will generate an XML or JSON template either locally or to a network share. The export operation will create a new job which can be monitored in the job queue. The template will be made available once the job has been marked as Completed.

The available options used to customize the template generation are detailed in the following sections.

3.1 Selective Export

By default, SCP Export will generate a template that includes most configurable devices on the host system. This includes, iDRAC, Lifecyle Controller, System, EventFilters, BIOS, NIC, FiberChannel, InfiniBand, and RAID / Storage devices. All available interfaces offer the option to selectively export only requested devices or device types.

Example:
```
racadm get -t xml -f export.xml -u username -p password -l //ip/share/ -c
iDRAC,NIC.Integrated.1-1-1
```

racadm provides the '-c' option for selective export. In the example above, export.xml will be exported to a network share and will contain the iDRAC.Embedded.1 component and the NIC.Integrated.1-1-1 component.

Most interfaces allow for both full FQDD or a shorthand version to export all components of a given type. The shorthand 'NIC' would export NIC.Integrated.1-1-1, NIC.Integrated.2-1-1, etc, but full FQDD 'NIC.Integrated.1-1-1' would only provide the component for that specific device.

NOTE: Shorthand values can be used for SCP Export or SCP Import.

Table 1 Available shorthand options

Shorthand	FQDD
iDRAC	iDRAC.Embedded.1
EventFilters	EventFilters.*.1
LifecycleController	LifecycleController.Embedded.1
System	System.Embedded.1
NonRAID	NonRAID.*
RAID	*** Exports/Imports all storage devices ***
AHCI	AHCI.*
PCIeExtender	PCIeExtender.*
PCIeSSD	PCIeSSD.*
Disk	Disk.*
BIOS	BIOS.Setup.1-1
NIC	NIC.*
FC	FC.*
InfiniBand	InfiniBand.*
SupportAssist	SupportAssist.Embedded.1

3.2 Read Only Attributes

Certain device attributes are ReadOnly and by default are not included in the template. These attributes can be requested by using the 'Include ReadOnly' flag provided by the interface.

The example below shows the iDRAC Firmware Version under Info.1#Version.

In the XML format these attributes are marked with ReadOnly in the comment section of the node.

```
<!-- ReadOnly <Attribute Name="Info.1#Version">4.40.00.00</Attribute> -->
```

In the JSON format the Comment item will be set to 'Always Read Only'.

```
    { "Name": "Info.1#Version",
      "Value": "4.40.00.00",
      "Set On Import": "False",
      "Comment": "Always Read Only" },
```

These attributes cannot be set during an SCP Import and are only available for informational purposes.

3.3 Include Password Hashes

Password attributes fields are included in the template. However, they are commented out and obfuscated with '******'. These fields can be manually supplied with a plaintext password, which can be set during SCP Import.

```
<!-- <Attribute Name="Users.2#Password">******</Attribute> -->
```

SCP Export also has the optional parameter 'Include Password Hashes'.

3.3.1 iDRAC User Passwords

This setting will modify the template to include new fields per iDRAC User, which allow the transfer of existing iDRAC user passwords between multiple hosts.

```
<!-- <Attribute Name="Users.2#SHA256Password">
C91B36713D93B1555B6FEB8274A65BA2746446770AA227B6E11979EB24F18221</Attribute> -->
<!-- <Attribute Name="Users.2#SHA1v3Key">
0105AC0DCD4F022A89DCA47E9A56D340E85B7F38</Attribute> -->
<!-- <Attribute Name="Users.2#MD5v3Key">
C9D52210AC9C127F517156A626F69FDE</Attribute> -->
 <!-- <Attribute Name="Users.2#SHA256PasswordSalt">
6D5F9E1B410917BEB0788E230DFCDCCE</Attribute> -->
 <!-- <Attribute Name="Users.2#IPMIKey">
D722C920F0E78CB5161F01AEE7C6559005AA5A5A9E947ED38788031A43DCC99E</Attribute> -->
```

When wanting to transfer existing iDRAC user settings between systems, it is recommended to use the 'Include Password Hash' option when generating the template.

3.3.2 BIOS Password SHAs

The BIOS System and Setup passwords can also be applied via the SHA/Salt attributes that are made available with the "Include Password Hash" optional parameter. These attributes will be empty by default.

```
<Attribute Name="SHA256SystemPassword"></Attribute>
<Attribute Name="SHA256SystemPasswordSalt"></Attribute>
<Attribute Name="SHA256SetupPassword"></Attribute>
<Attribute Name="SHA256SetupPasswordSalt"></Attribute>
```

3.4 Export Type - Clone and Replace

SCP Export offers two optional modes that will alter the template generation by adjusting the number of commented items and changing some values.

The default Normal export type will leave some attributes commented out and require the user to uncomment (or change Set On Import to True) them before they can be applied during an SCP Import.

The Clone export type will generate a template that's better suited to cloning a 'golden' configuration from one server to one/many servers. Compared to a Normal export type, more attributes will be uncommented, and some storage settings will be adjusted to aid in the cloning process.

The Replace export type will generate a template that's better suited for retiring or replacing the complete configuration for a server. Compared to a Clone export type, most attributes will be uncommented, and some storage settings will be adjusted to aid in the replace process.

Refer to the Default, Clone & Replace Tables at the end of this document for a list of settings and their commented state per mode.

Key points of Clone & Replace have been included below. For more information refer to the Server Cloning with Server Configuration Profiles whitepaper.

3.4.1 Clone and Replace with passwords

When the Clone or Replace mode is selected with SCP Export and the Include Password Hashes option is not provided, the iDRAC user passwords will be generated in the template as either 'calvin' or 'Calvin#SCP#CloneReplace1'.

In all versions of iDRAC before iDRAC9 4.40.00.00 the iDRAC user passwords will be generated as 'calvin'.

Starting in iDRAC9 4.40.00.00 the iDRAC user passwords will be generated as 'Calvin#SCP#CloneReplace1'. This was done to accommodate the new optional iDRAC password minimum security requirements.

NOTE: If existing passwords need to be transferred between servers, then it's recommended to use the 'Include Password Hashes' option.

Normal export type example without 'Include Password Hashes':

```
<Attribute Name="Users.2#UserName">root</Attribute>
<!-- <Attribute Name="Users.2#Password">******</Attribute> -->
```

Clone export type example without 'Include Password Hashes':

```
<Attribute Name="Users.2#UserName">root</Attribute>
<Attribute Name="Users.2#Password">Calvin#SCP#CloneReplace1</Attribute>
```

3.4.2 Clone and Replace with storage devices

Clone and Replace will both alter the generated template and automatically populate some storage attributes.

RAIDresetConfig will be set to True and RAIDforeignConfig will be set to Clear.

```
    <Attribute Name="RAIDresetConfig">True</Attribute>
    <Attribute Name="RAIDforeignConfig">Clear</Attribute>
```

Virtual Disk RAIDaction will be set to Create instead of Update, and all attributes needed for the create operation will be uncommented.

```
   <Component FQDD="Disk.Virtual.0:RAID.Integrated.1-1">
     <Attribute Name="RAIDaction">Create</Attribute>
     <Attribute Name="LockStatus">Unlocked</Attribute>
     <Attribute Name="BootVD">True</Attribute>
     <Attribute Name="RAIDinitOperation">None</Attribute>
     <Attribute Name="DiskCachePolicy">Default</Attribute>
     <Attribute Name="RAIDdefaultWritePolicy">WriteBack</Attribute>
     <Attribute Name="RAIDdefaultReadPolicy">ReadAhead</Attribute>
     <Attribute Name="Name">Virtual Disk 0</Attribute>
     <Attribute Name="Size">1199638052864</Attribute>
     <Attribute Name="StripeSize">128</Attribute>
     <Attribute Name="SpanDepth">1</Attribute>
     <Attribute Name="SpanLength">2</Attribute>
     <Attribute Name="RAIDTypes">RAID 1</Attribute>
     <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.0:Enclosure.Internal.0-
1:RAID.Integrated.1-1</Attribute>
     <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.1:Enclosure.Internal.0-
1:RAID.Integrated.1-1</Attribute>
</Component>
```

NOTE: If the template is generated from a system that does not have a virtual disk created, then the template will not contain the Disk.Virtual component. It can be manually added to the template and imported to create the virtual disk.

Disk attributes will be uncommented.

```
<Component FQDD="Disk.Direct.1-1:AHCI.Slot.2-1">
  <Attribute Name="RAIDHotSpareStatus">No</Attribute>
  <Attribute Name="RAIDPDState">Ready</Attribute>
</Component>
```

3.5 Include Custom Telemetry

Starting in iDRAC9 4.40.00.00, the standard format of the SCP template has been expanded to include the Telemetry Custom Report Metric Definitions. The format of this dataset is unique to Telemetry and therefore does not adhere to the same rules covered in Template.

This dataset is not included in the template by default but can be requested by using the ‘Include Custom Telemetry’ optional parameter during SCP Export. Any template generated using this new parameter is not backwards compatible to older version of iDRAC during an SCP Import.

3.6 Available Interfaces

3.6.1 iDRAC GUI

SCP Export can be located on the iDRAC GUI under Configuration > Server Configuration Profiles > Export. All the available options detailed above can be found on this page.

3.6.2 racadm

The racadm 'get' command using the '-t xml' or '-t json' parameters will invoke an SCP Export operation. The following options are also available:

Racadm example:

```
C:\>racadm -r 192.168.0.120 -u root -p calvin get -f R740_scp_file.xml -t xml -l
192.168.0.130:/nfs
```

Available options:

```
-c : FQDD or shorthand for selective Export.
-t : “xml” or “json” to select your format.
--clone : Export type of Clone.
--replace : Export type of Replace.
--includero : Include read only attributes in the template.
--includeph : Include iDRAC user password hashes in the template.
--includeCustomTelemetry : Include the Telemetry Custom Report Metric Definitions.
```

Refer to the racadm help text or the RACADM User's Guide for additional options and details on network settings.

```
>>racadm help get
```

The latest version of the Integrated Dell Remote Access Controller 9 RACADM CLI Guide can be found here:

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

3.6.3 Redfish

Redfish POST example:

```
URI:
/redfish/v1/Managers/iDRAC.Embedded.1/Actions/Oem/EID_674_Manager.ExportSystemConfiguration
Header: content-type application/json
Body: {'ExportFormat': 'XML', 'ShareParameters': {'ShareType': 'NFS',
'ShareName': '/nfs', 'IPAddress': '192.168.0.130', 'Target': 'ALL',
'FileName': 'R740_scp_file.xml'}}
```

Clone can be selected by adding the 'ExportUse' : '1' optional parameter and Replace can be selected by adding 'ExportUse' : '2'. Refer to the Redfish documentation for all available optional parameters.

For more details on the action, supported parameters and values, refer to schema “redfish/v1/Schemas/OemManager_v1.xml”.

The latest version of the Redfish API Guide can be found here:

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

Examples for Redfish scripting using Python and Powershell can be found here:

https://github.com/dell/iDRAC-Redfish-Scripting

4 SCP Import

SCP Import is a streamlined configuration, firmware, and OS deployment workflow that consumes the template generated by the SCP Export process. Import will validate the template and compare the current configuration to the requests made by the template. If changes are detected between the template and the current configuration, then the SCP Import operation will apply the new settings.

NOTE: After executing an Import operation, a job ID will be returned which can be queried to check the status and validate whether the process is completed or failed. If failed, check the iDRAC Lifecycle Logs for more details. For more information on how to check the job status, refer to the workflow section of this document.

Job ID example from the iDRAC shell:

```
racadm>>set -t xml -f default.xml -u user -p password -l //ip/share/ -c iDRAC
RAC977: Import configuration XML file operation initiated.
Use the "racadm jobqueue view -i JID_898317921404" command to view the status
of the operation.
```

The final job status for an SCP Import operation will always be Completed, Completed with Errors, No Change or Failed.

- **Completed** means the operation successfully applied requested changes and performed all requested actions successfully.
- **Completed with Errors** means the operation was partially successful.
- **No Change** means that the operation was unable to detect any differences between the template and the current configuration.
- **Failed** means that all detected changes were unable to be applied.

Regardless of the end status of the operation, it's recommended to review the LCL and confirm that the desired actions were performed.

Viewing the job status example:

```
racadm>>jobqueue view -i JID_898317921404
---------------------------- JOB -------------------------
[Job ID=JID_898317921404]
Job Name=Configure: Import Server Configuration Profile
Status=Completed
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Mon, 14 May 2001 04:16:32]
Actual Completion Time=[Mon, 14 May 2001 04:16:35]
Message=[SYS053: Successfully imported and applied Server Configuration Profile.]
Percent Complete=[100]
----------------------------------------------------------
```

All changes applied are logged to the LCL with configuration results entries. If any change is attempted and fails to apply, then a configuration results event is logged to the LCL with an error message stating the reason for the failure.

Viewing the results example:

```
racadm>>lclog viewconfigresult -j JID_898317921404
SeqNumber       = 5008
FQDD            = iDRAC.Embedded.1
Job Name        = Import Configuration
Operation Name  = CHANGE
DisplayValue    = SSH Idle Timeout
Name            = SSH.1#Timeout
OldValue        = 1800
NewValue        = 1805
Status          = Success
ErrCode         = 0
```

Refer to the Event and Error Message Reference Guide to locate the Recommended Response Action to a specific error code.

Error code lookup can also be performed using this tool:

https://qrl.dell.com/LCDError/Lookup?q=ErrorCode

4.1 Host Reboot

The SCP Import operation may automatically restart the host to apply all settings, but only if the template contains settings that require a host reboot. As an example, if an SCP Import was performed and only iDRAC settings changes were detected then the host reboot would not be performed.

NOTE: The SCP Import operation may reboot multiple times to apply all configuration settings and firmware.

4.1.1 What will trigger a reboot?

The following components will trigger a reboot.

- BIOS.Setup.1-1
- All network (NIC, FC, InfiniBand) components.
- All storage components.

The following components will not trigger a reboot.

- iDRAC.Embedded.1
- System.Embedded.1
- LifecycleController.Embedded.1 excluding BIOSRequestRTD.
- EventFilters
- SupportAssist

The SCP Import Preview operation will indicate if a template requires a host reboot in the configuration results without applying settings or triggering a reboot.

```
racadm>> lclog viewconfigresult -j JID_040778842537
SeqNumber       = 10365
Job Name        = Preview Configuration
Message ID      = SYS087
Message          = A system reboot is required to apply configuration changes.
SeqNumber        = 10364
Job Name         = Preview Configuration
FQDD             = BIOS.Setup.1-1
```

4.2 Shutdown Type

If a host shutdown is required, then SCP Import will issue a graceful shutdown request to the host operating system. The operating system could reject the graceful shutdown request which would result in the SCP Import operation failing with SYS051 – "The system could not be shut down within the specified time."

SCP Import provides options to help control this workflow in the way of 3 shutdown options; Graceful, Forced and NoReboot.

4.2.1 Shutdown Type: Graceful

Graceful Shutdown is the default selection for Shutdown Type of SCP Import. It also has an additional optional parameter called 'Time to Wait', which is the amount of time SCP Import will wait for the host to shut down before timing out. The default is 5 minutes and the maximum in 1 hour.

NOTE: The operating system can potentially deny or ignore the graceful shutdown request.

If the SCP Import operation times out with an error stating that it was unable to shut down the host in time, then consider the following options:

- Increase the optional 'Time to Wait' parameter.
- Use the Forced shutdown option.
- Power down the host manually.

4.2.2 Shutdown Type: Forced

The forced shutdown type is an alternative to graceful shutdown. The host server will be powered off immediately regardless of the state of the host. This is only recommended when it's safe to power down the host.

4.2.3 Shutdown Type: NoReboot

The NoReboot shutdown type will tell the SCP Import operation to ignore all automatic power control that's typically performed by SCP. The system will not be powered down (gracefully or forced) automatically, and instead will wait for the user to reset the host or perform a power on. Once either of these actions has occurred, then the SCP Import operation will begin applying settings.

This workflow impacts all settings, even those that don't necessarily require a reboot. As an example, a template that contains iDRAC only attributes will still wait for a host reboot if the shutdown type of NoReboot is provided.

Important: When the NoReboot shutdown type is provided, a typical SCP Import job will be created but the job will stop at 20% with a message of "Paused, Waiting for Reboot." This is the operation signaling that it's done staging and will only apply settings after the host has been rebooted or powered on.

SCP Import is a blocking operation that will prevent most other set configuration activities from being performed. This also applies to the NoReboot shutdown type. Since there are pending configuration changes gated behind a power cycle, no other configuration operations are permitted. Only once the host has been rebooted and the SCP operation completes will other configuration operations be permitted.

4.3 End Host Power State

The ‘End Host Power State’ optional flag can tell the host to power down after the SCP Import operation has completed. The default power state will be On.

NOTE: This flag is forced to On when SCP Import contains an OS Deployment operation that boots to a networked ISO.

4.4 Dependencies

Some device settings are dependent on one another and cannot be set until their dependency has been resolved. SCP Import will automatically attempt to resolve all dependencies detected within the template.

If a dependency is unable to be resolved, then an event will be logged to the LCL. The associated configuration results entry for the failing attribute will contain a message indicating the reason for the failure. A common example would be that most iDRAC user settings cannot be set unless both a username and password have been set and the user is enabled. If the template addresses all those criteria, then all settings will be applied, and no errors will be seen.

Dependency data for individual attributes can be located in the Attribute Registry.

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

4.5 Backwards Compatibility

The SCP schema has been expanded in iDRAC9 version 4.40.00.00 to add support for Telemetry Custom Metric Report definitions. This was covered previously in the SCP Export section and will be detailed further later in the document. It’s important to note that if this optional flag was used to generate the template, then the template will not be compatible on older versions of the iDRAC.

In all other scenarios, the SCP template will be compatible across all supported versions of the iDRAC. However, differences in configurations between iDRAC or component versions may result in errors being logged during the Import. SCP Import is a ‘continue on error’ operation so it will attempt to apply all settings even if failures are detected along the way. It’s recommended to review the LCL or configuration results if a SCP Import job completes with Completed with Errors or Failed.

4.6 Selective Import

By default, all components contained within the SCP template will be processed and all detected changes will be applied. SCP Import offers the option to ‘selectively import’ only the desired components from a full template. The same options detailed in the Selective Export section is also available for Import.

Example:
```
racadm set -t xml -f export.xml -u username -p password -l //ip/share/ -c
iDRAC,NIC.Integrated.1-1-1
```

racadm provides the ‘-c’ option for selective import. In the example above, export.xml will be imported from a network share and only process the iDRAC.Embedded.1 and NIC.Integrated.1-1-1 components.

Most interfaces allow for both the full FQDD or a shorthand version to import all components of a given type. The shorthand ‘NIC’ would import NIC.Integrated.1-1-1, NIC.Integrated.2-1-1, etc, but the full FQDD ‘NIC.Integrated.1-1-1’ would only process the component for that specific device.

Shorthand values can be used for both SCP Export and SCP Import. Please refer to the Available shorthand options table in the Selective Export section.

4.7 Available Interfaces

4.7.1 iDRAC GUI

SCP Import can be located on the iDRAC GUI under Configuration > Server Configuration Profiles > Import. All the available options detailed above can be found on this page.

4.7.2 racadm

The racadm ‘set’ command using the ‘-t xml’ or ‘-t json’ parameters will invoke an SCP Import operation.

Racadm example:

```
C:\>racadm -r 192.168.0.120 -u root -p calvin set -f R740_scp_file.xml -t xml -l
192.168.0.130:/nfs
```

Available options:

```
-c : FQDD or shorthand for selective Import.
-t : “xml” or “json” to select your format.
-b : Shutdown type; Graceful, forced or NoReboot.
-w : Time to Wait; Maximum wait time for graceful shutdown.
-s : Set the host power to On or Off after Import completes.
```

Refer to the racadm help text or the RACADM User’s Guide for additional options and details on network settings.

```
>>racadm help set
```

The latest version of the Integrated Dell Remote Access Controller 9 RACADM CLI Guide can be found here:

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

4.7.3 Redfish

To import SCP profile using Redfish, execute a POST call on OEM action *EID_674_Manager*.

Redfish POST example:

```
URI: /redfish/v1/Managers/iDRAC.Embedded.1/Actions/Oem/EID_674_Manager.
ImportSystemConfiguration
Header: content-type application/json
Body: Body: { 'ShareParameters': {'ShareType': 'NFS', 'ShareName': '/nfs', 'IPAddress':
'192.168.0.130', 'Target': 'ALL', 'FileName': 'R740_scp_file.xml'}}
```

For more details on the action, supported parameters and values, refer to schema “redfish/v1/Schemas/OemManager_v1.xml”.

The latest version of the Redfish API Guide can be found here:

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

Examples for Redfish scripting using Python and Powershell can be found here:

https://github.com/dell/iDRAC-Redfish-Scripting

5 SCP Import Preview

SCP Import Preview will execute the validation portion of the SCP Import operation but will not apply any settings. Any errors detected during the validation process will be logged to the LCL as configuration results. The preview operation will not reboot the host.

Before importing the SCP file, it is not required, but is recommended, that an Import Preview operation is executed. By executing this operation first, any potential format issues or invalid attribute settings can be identified without impacting the state of the server.

NOTE: After executing an Import Preview operation, a job ID is returned which can be queried to check the status and validate if the process completed or failed. If failed, check the iDRAC Lifecycle Logs for more details. For more details on checking the job status, refer to the Jobs section in this document.

Unlike Export and Import, the Import Preview operation does not have the option to select individual components for validation. The entire template will be validated.

5.1 Available Interfaces

5.1.1 iDRAC GUI

SCP Import Preview can be located on the iDRAC GUI under Configuration > Server Configuration Profiles > Import and click Preview. The options available to Import do not apply to Import Preview.

5.1.2 racadm

The racadm 'set' command has an additional '--preview' flag that will convert a SCP Import into a SCP Import Preview operation.

5.1.3 Redfish

To import preview a SCP profile using Redfish, execute a POST call on OEM action *EID_674_Manager.ImportSystemConfigurationPreview*.

Redfish POST example:

```
URI: /redfish/v1/Managers/iDRAC.Embedded.1/Actions/Oem/EID_674_Manager.
ImportSystemConfigurationPreview
Header: content-type application/json
Body: Body: {'ShareParameters': {'ShareType': 'NFS', 'ShareName': '/nfs',
'IPAddress': '192.168.0.130', 'FileName': 'R740_scp_file.xml'}}
```

6 iDRAC Configuration

This section of the guide will focus exclusively on the attributes found under the iDRAC.Embedded.1 component within the template. There are too many iDRAC attributes to cover in this document, so it’s recommended that the iDRAC User’s Guide is reviewed for any features that might not be covered here.

6.1 Template Example

The example below is of a snapshot of the iDRAC.Embedded.1 component generated by an SCP Export using the Include Password Hashes option.

```
<Component FQDD="iDRAC.Embedded.1">
 <Attribute Name="Users.2#UserName">root</Attribute>
 <!-- <Attribute Name="Users.2#Password">******</Attribute> -->
 <Attribute Name="Users.2#Privilege">511</Attribute>
 <Attribute Name="Users.2#IpmiLanPrivilege">Administrator</Attribute>
 <Attribute Name="Users.2#IpmiSerialPrivilege">Administrator</Attribute>
 <Attribute Name="Users.2#Enable">Enabled</Attribute>
 <Attribute Name="Users.2#SolEnable">Enabled</Attribute>
 <Attribute Name="Users.2#ProtocolEnable">Disabled</Attribute>
 <Attribute Name="Users.2#AuthenticationProtocol">SHA</Attribute>
 <Attribute Name="Users.2#PrivacyProtocol">AES</Attribute>
 <!-- <Attribute
Name="Users.2#SHA256Password">5522A153BF9E4AB5CE02DC51290A5A48E603B48FA3B611C67C675ACF4A183D6
F</Attribute> -->
 <!-- <Attribute
Name="Users.2#SHA1v3Key">CB915933B669F8B8BE6D8C2F4395FF686AB05718</Attribute> -->
 <!-- <Attribute Name="Users.2#MD5v3Key">947F1A44E14757AF0712D5B51511365D</Attribute> -->
 <!-- <Attribute
Name="Users.2#SHA256PasswordSalt">594B1509A26F10BEF69B5B0A97D01895</Attribute> -->
 <!-- <Attribute
Name="Users.2#IPMIKey">EA4F150A02AE1970552D551AB73E43815514C57F9D9CEECEFFA20165DB18482C</Attr
ibute> -->
 <!-- <Attribute Name="Users.2#SSHPublicKey1"></Attribute> -->
 <!-- <Attribute Name="Users.2#SSHPublicKey2"></Attribute> -->
 <!-- <Attribute Name="Users.2#SSHPublicKey3"></Attribute> -->
 <!-- <Attribute Name="Users.2#SSHPublicKey4"></Attribute> -->
```

6.2 Creating and configuring an iDRAC User

iDRAC has 2-16 users available for configuration. The attributes above show an example of user 2 and all users are grouped in a similar manner; Users.2, Users.3, Users4, etc.

When creating a new user, the user must be set to Enabled and a username and password must be supplied.

NOTE: Passwords in SCP templates will always be commented out by default and populated with ‘****’ as their value.**

```
    { "Name": "Users.3#UserName",
      "Value": "guest",
      "Set On Import": "True",
      "Comment": "Read and Write" },
    { "Name": "Users.3#Password",
      "Value": "password123",
      "Set On Import": "True",
      "Comment": "Read and Write" },
    { "Name": "Users.3#Enable",
      "Value": "Enabled",
      "Set On Import": "True",
      "Comment": "Read and Write" },
```

Additional settings for the user can be applied via the same template. The example above uses a ‘plaintext’ password to configure the user instead of the password hashes. The password must either be plaintext or hashes but cannot contain both.

NOTE: Commented attributes are ignored during SCP Import.

6.3 Clearing an iDRAC User

To remove a user and clear its settings, set the UserName to an empty value and set Enable to Disabled.

```
<Attribute Name="Users.3#UserName"></Attribute>
<Attribute Name="Users.3#Enable">Disabled</Attribute>
```

This will remove the user and clear all associated settings. All other attributes for this user will be ignored if a reset was requested.

6.4 SSHPublicKey

Available on iDRAC9 version 4.00.00.00 and above.

An iDRAC user’s public SSH key can be set using SCP Import.

```
  <Attribute Name="Users.4#SSHPublicKey1"></Attribute>
  <Attribute Name="Users.4#SSHPublicKey2">ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEA32CnKmqW5nHswuLrczixMxzaevolKbMsy/bNlZNvnAEQPWhYFK80ln+0U44h0Hqns
F/cVQo3RLAfehFj/Xf7AcBwNXy38oB+IbkURQVdB/t0k/74IB5RAgwa3R0svu9VW8qinBS+Yi5bzKi/TvPZrOoWaA/RLn
crI+cEI8EdSD5s+aoLic336eTltTEnAwP157GNz0IjSRWNYGL8kKAmDfjgrFOUOTfbC02VODHxN/FYRTNAJj8N+OCI/fS
uR0TLoRXhZhtyP9TL+5Nmz80wM6l+MemR+GaJSUZolTFw3opmhnHdn1WNotoR7NprCcJZBwQgK8e8Ewo62mxDFMTfAQ==
rsa-key-20190211</Attribute>
  <Attribute Name="Users.4#SSHPublicKey3"></Attribute>
  <!-- <Attribute Name="Users.4#SSHPublicKey4"></Attribute> -->
```

To remove the public SSH key from an iDRAC user leave the attribute’s value empty and run an SCP Import operation.

6.5 Certificates

Available on iDRAC9 version 4.00.00.00 and above.

Import of certificates is enabled via the CertType and CertData attributes under the iDRAC component. The header and footer tags are required for import.

```
<Attribute Name="SecurityCertificate.1#CertData">-----BEGIN CERTIFICATE-----
  MIIDazCCAlOgAwIBAgIQd3Kt+V8JUYdGdoqfwI4pJDANBgkqhkiG9w0BAQsFADBI
  MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRla21zMRkw
  FwYDVQQDExBla21zLUVLTVMtUkNBLUNBMB4XDTE5MDMxMzE2NDAwNFoXDTI0MDMx
  MzE2NTAwNFowSDEVMBMGCgmSJomT8ixkARkWBWxvY2FsMRQwEgYKCZImiZPyLGQB
  GRYEZWttczEZMBcGA1UEAxMQZWttcy1FS01TLVJDQS1DQTCCASIwDQYJKoZIhvcN
  AQEBBQADggEPADCCAQoCggEBAKVcwkh6Iz8FIXBQXHK931SB0abutzsBjB/zdwoP
  zoYZUmsBUl16oNsD31/pLHi1rR9K4+VRLizkPmcdipc/u04VxrOeDTX8/1XlWc2V
  r4F9vngLKz6Uo0+BYaCKu3A0gCdfT9/sJYDv1T+PE64h2CnQqnspsRPvtbNgpOQG
  NnQy5wQuDYK/6Ri4h6xBF7VSwUsY/qiO/zBqRXlCLrPO1GtrHqG8aNzQpBjPAb13
  tTwFrua9FgRL6xtr6ZpSaPMxGhkceAfT4s299915ehyrLvyRfYM05TPkgYkGlEif
  8yvXVaoO2tEUkCAomFdpdXAraW1CuaosfMUfOk5Z49jr/LUCAwEAAaNRME8wCwYD
  VR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFFdRsjlhMKU7cz0E
  I89BTtLtaPGOMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBCwUAA4IBAQBn
  dzOBezSW0P01loC6S82sIIkT4Ls87Pp6VhTjVPc01ybTNVpYS6yKlWVbi7CCuh9j
  O7bZbvs45mpvCBmCCsRl4opUmwMJi57qCPjRRdOWqZCrHDh80LJDSR5EM2175fd2
  yRarDwDsSUp4DDfYJFWWMqv3TiRQPGAizoidJokjXFjO6Y5ZKFSl9ps0+uiQPo3G
  ytUTam6xjBHO+eH2hpZiNMU4FR/c4pB4cnXYY+s28JTvBAhKtYmJhs1IPsz+s4iu
  N3m41Or+6qmIvsFl2FnQa8NEOqXO18H+Npp9gZwT1NNDn/ZhH3JAZm0Wi3QtKLhJ
  dvYaLy2hqa1PcWvQmS5G
  -----END CERTIFICATE-----</Attribute>
<Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
```

In the example above, the CertType indicates that this is a Key Management System (KMS) Server Certificate Authority (CA). The CertData field contains the actual data for the certificate. The iDRAC uses the CertType attribute to determine how to interpret the data.

The available CertTypes are:

- KMS_SERVER_CA
- SEKM_SSL_CERT
- RSYSLOG_1
- RSYSLOG_2
- DEL_AUTH_HTTPS_1
- DEL_AUTH_HTTPS_2

Types ending with _1 or _2 refer to the instance of the certificate. There can be 2 instances of RSys Log and Delegated Authorization HTTPs certificates.

The successful installation of certificates via SCP can be confirmed via configuration results.

```
racadm>>lclog viewconfigresult -j JID_581182121065
SeqNumber = 5963
FQDD = iDRAC.Embedded.1
Job Name = Import Configuration
DisplayValue = Certificate Data
Name = SecurityCertificate.1#CertData
```

```
OldValue = ******
NewValue = ******
Status = Success
ErrCode = 0
DisplayValue = Certificate Type
Name = SecurityCertificate.1#CertType
OldValue = ""
NewValue = KMS_SERVER_CA
Status = Success
ErrCode = 0
```

6.6 Password Settings

With iDRAC9 version 4.40.00.00, new iDRAC user password security options are now available.

The following settings can be Enabled or Disabled.

```
<Attribute Name="Security.1#PasswordRequireUpperCase">Enabled</Attribute>
<Attribute Name="Security.1#PasswordRequireNumbers">Enabled</Attribute>
<Attribute Name="Security.1#PasswordRequireSymbols">Enabled</Attribute>
```

A minimum password length can be set with PasswordMinimumLength.

```
<Attribute Name="Security.1#PasswordMinimumLength">10</Attribute>
```

A password score can be enforced with either Weak, Moderate, Strong or No Protection.

```
<Attribute Name="Security.1#MinimumPasswordScore">Strong Protection</Attribute>
```

A regular expression can also be enforced on iDRAC user passwords.

```
<Attribute Name="Security.1#PasswordRequireRegex"/>
```

6.7 AutoUpdate

The iDRAC can be configured to automatically perform firmware updates via repository update using the AutoUpdate attributes. The iDRAC will run a repository update at the recurrence specified by the imported template. In the scenario below, it will check the network share at 4:00am daily for Catalog.xml and compare it against the existing server applying any new firmware updates.

```
<Component FQDD="iDRAC.Embedded.1">
  <Attribute Name="AutoUpdate.1#IPAddress">192.168.0.20</Attribute>
  <Attribute Name="AutoUpdate.1#Domain">Home</Attribute>
  <Attribute Name="AutoUpdate.1#ShareName">Share</Attribute>
  <Attribute Name="AutoUpdate.1#ShareType">cifs</Attribute>
  <Attribute Name="AutoUpdate.1#Username">user1</Attribute>
  <Attribute Name="AutoUpdate.1#Password">******</Attribute>
  <Attribute Name="AutoUpdate.1#ApplyReboot">0</Attribute>
  <Attribute Name="AutoUpdate.1#Repeat">1</Attribute>
  <Attribute Name="AutoUpdate.1#CatalogName">Catalog.xml</Attribute>
  <Attribute Name="AutoUpdate.1#Time">4:00</Attribute>
  <Attribute Name="AutoUpdate.1#DayofMonth">*</Attribute>
  <Attribute Name="AutoUpdate.1#WeekofMonth">*</Attribute>
  <Attribute Name="AutoUpdate.1#DayOfWeek">*</Attribute>
</Component>
```

The AutoUpdate functionality must be enabled under the LifecycleController component to activate these settings. This feature can be enabled, and all associated settings applied in a single SCP Import operation.

```
<Component FQDD="LifecycleController.Embedded.1">
  <Attribute Name="LCAttributes.1#AutoUpdate">Enabled</Attribute>
</Component>
```

7 LifecycleController

The LifecycleController component contains a variety of LifecycleController settings and the attribute template for OS deployment operations. The OS deployment operations are covered in more detail below. This section will focus on the LifecycleController specific settings.

```
<Component FQDD="LifecycleController.Embedded.1">
  <Attribute Name="LCAttributes.1#CollectSystemInventoryOnRestart">Enabled</Attribute>
  <Attribute Name="LCAttributes.1#PartConfigurationUpdate">Apply Always</Attribute>
  <Attribute Name="LCAttributes.1#PartFirmwareUpdate">Match firmware of replaced 
part</Attribute>
  <Attribute Name="LCAttributes.1#BIOSRTDRequested">False</Attribute>
  <Attribute Name="LCAttributes.1#AutoUpdate">Disabled</Attribute>
</Component>
```

CollectSystemInventoryOnRestart – This is the inventory collection process that was cover in the CSIOR section above. It's recommended to keep this feature Enabled so that the inventory data stored on the iDRAC is up to date.

PartConfigurationUpdate – The Part Replacement feature can automatically restore the last known configuration of a device if it's replaced with a similar device. The available options for this setting are:

- Disabled
- Apply Always
- Apply only if Firmware Match.

PartFirmwareUpdate – The Part Replacement feature can automatically update to the last installed firmware if a device is replaced with a similar device. The available options for this setting are:

- Disable
- Allow version upgrade only
- Match firmware of replaced part

BIOSRTDRequested – This BIOS Reset to Defaults attribute will trigger a full reset to default settings for the BIOS. Any attributes configured in the BIOS.Setup.1-1 component will be applied after the reset to defaults has occurred. This is the only LifecycleController attribute that will require a host reboot to apply. This value does not persist and will reset to False after the host has been rebooted.

AutoUpdate – The AutoUpdate feature can be enabled or disabled under the LifecycleController component. The associated scheduling attributes are located at the end of the iDRAC component. This feature is detailed in the AutoUpdate section of this document.

8 EventFilters

EventFilter settings can be configured using SCP Import and are found under these six components:

```
<Component FQDD="EventFilters.SystemHealth.1">
<Component FQDD="EventFilters.Storage.1">
<Component FQDD="EventFilters.Updates.1">
<Component FQDD="EventFilters.Audit.1">
<Component FQDD="EventFilters.Configuration.1">
<Component FQDD="EventFilters.WorkNotes.1"/>
```

The SCP template will contain many event filters. To help navigate this large array of settings, they are broken down into categories. The three major categories of each setting are Critical (1), Warning (2) and Informational (3). The settings available under each category will vary depending on the event filter.

Below is an example of a power event filter under the Informational (3) category. Each grouping will start with a commented out DisplayName attribute stating the category. This attribute cannot be set and is just used to assist in navigating the settings.

```
<!-- <Attribute Name="PWR_5_3#DisplayName">PWR_5_3 (Informational)</Attribute> -->
 <Attribute Name="PWR_5_3#Alert#Email">Disabled</Attribute>
 <Attribute Name="PWR_5_3#Alert#SNMP">Disabled</Attribute>
 <Attribute Name="PWR_5_3#Alert#IPMI">Disabled</Attribute>
 <Attribute Name="PWR_5_3#Alert#SysLog">Disabled</Attribute>
 <Attribute Name="PWR_5_3#Alert#WSEventing">Disabled</Attribute>
 <Attribute Name="PWR_5_3#Alert#OSLog">Disabled</Attribute>
 <Attribute Name="PWR_5_3#Alert#RedfishEventing">Enabled</Attribute>
 <Attribute Name="PWR_5_3#Action">No Action</Attribute>
```

Each of the event filters settings can be toggled, and an action can be set to perform when one of these events is triggered. The available Action settings are:

- `No Action`
- `Reboot`
- `PowerOff`
- `PowerCycle`

Not all action options may be applicable to an event filter. Refer to the iDRAC User’s Guide for more information on event filters.

9 RAID / Storage Configuration and Operations

SCP can be used to perform a variety of RAID and storage operations. A few common activities have been included below and additional details can be found in the Creating and Managing XML Configuration Files by Using WS-Man whitepaper.

NOTE: HBA controllers are not supported for SCP export or import.
NOTE: Storage Component elements can be nested inside of their parent Components. This is done to show the hierarchy of these devices. In the first example below, Disk.Virtual.0 is a subcomponent of RAID.Slot.2-1. This is also reflected in the Disk.Virtual.0:RAID.Slot.2-1 FQDD.

9.1 Create and initialize a virtual disk

SCP can be used to create and initialize a virtual disk. The XML example below illustrates how this can be accomplished with a template. The Virtual Disk will be a part of RAID.Slot.2-1 using disk 0 and 9. The RAIDaction attribute specifies the Create activity, and the RAIDinitOperation attribute specifies how the VD will be initialized.

```
<Component FQDD="RAID.Slot.2-1">
  <Component FQDD="Disk.Virtual.0:RAID.Slot.2-1">
    <Attribute Name="IncludedPhysicalDiskID">
      Disk.Bay.0:Enclosure.External.0-0:RAID.Slot.2-1
    </Attribute>
    <Attribute Name="IncludedPhysicalDiskID">
      Disk.Bay.9:Enclosure.External.0-0:RAID.Slot.2-1
    </Attribute>
    <Attribute Name="RAIDaction">Create</Attribute>
    <Attribute Name="RAIDinitOperation">Fast</Attribute>
    <Attribute Name="DiskCachePolicy">Default</Attribute>
    <Attribute Name="RAIDdefaultWritePolicy">WriteBack</Attribute>
    <Attribute Name="RAIDdefaultReadPolicy">Adaptive</Attribute>
    <Attribute Name="Name">xmlconfig</Attribute>
    <Attribute Name="Size">146163105792</Attribute>
    <Attribute Name="StripeSize">128</Attribute>
    <Attribute Name="SpanDepth">1</Attribute>
    <Attribute Name="SpanLength">2</Attribute>
    <Attribute Name="RAIDTypes">RAID 1</Attribute>
  </Component>
</Component>
```

This action can also be performed without specifying the physical disks. If no physical disks are included in the VD creation, they will be chosen automatically.

```
<Component FQDD="RAID.Slot.2-1">
  <Component FQDD="Disk.Virtual.0:RAID.Slot.2-1">
    <Attribute Name="RAIDaction">CreateAuto</Attribute>
    <Attribute Name="RAIDinitOperation">Fast</Attribute>
    <Attribute Name="Name">xmlconfig</Attribute>
    <Attribute Name="Size">0</Attribute>
    <Attribute Name="RAIDTypes">RAID 1</Attribute>
  </Component>
</Component>
```

NOTE: Because physical disk drives included in the VDs are selected automatically based on size and RAIDTypes, span parameters such as SpanLength and SpanDepth are also determined automatically. Hence, they also must not be specified in the input configuration XML file.

When Size value is specified as “0”, the VD will be created with minimum number of disks required for the RAIDTypes.

9.2 RAIDresetConfig

SCP Export will include the RAIDresetConfig attribute in the template but will be marked as False. If the attribute is changed to True and imported, then the configuration for the associated RAID device will be reset. This includes the removal of an VDs.

NOTE: Setting RAIDresetConfig to True is destructive and will erase all virtual disks on the controller. Only perform this action if you intend to destroy all virtual disks on the controller.

This action will always take place before all other requested operations, so it can be stacked with create VD and initialization.

```
  { "FQDD": "RAID.Slot.6-1",
    "Attributes": [
    { "Name": "RAIDresetConfig",
      "Value": "True",
      "Set On Import": "True",
      "Comment": "Read and Write" },
```

RAIDresetConfig will automatically be set to True when exported with Clone or Replace mode.

9.3 RAIDdedicatedSpare

A dedicated hot spare can be defined using the RAIDdedicatedSpare attribute found under the VD component element. A specific disk can be defined by using the FQDD for the disk.

```
  <Component FQDD="Disk.Virtual.0:RAID.Slot.2-1">
    <Attribute Name="RAIDdedicatedSpare">
      Disk.Bay.5:Enclosure.External.0-0:RAID.Slot.2-1
    </Attribute>
```

The value ‘AutoSelect’ can be provided to automatically assign a dedicated hot spare.

```
<Component FQDD="Disk.Virtual.0:RAID.Slot.2-1">
    <Attribute Name="RAIDdedicatedSpare">AutoSelect</Attribute>
```

9.4 Cryptographic Erase

A cryptographic erase of PCIe SSD devices either controlled by bridge card or CPU can be performed by setting the PCIeSSDsecureErase attribute to True.

```
<Component FQDD="Disk.Bay.16:Enclosure.Internal.0-1:PCIeExtender.Slot.4">
    <Attribute Name="PCIeSSDsecureErase">True</Attribute>
</Component>
```

A cryptographic erase of NVMe or SAS / SATA drives attached to a PERC can be performed by setting the 'Cryptographic Erase' attribute to True.

```
<Component FQDD="Disk.Bay.5:Enclosure.Internal.0-1:RAID.Slot.1-1">
  <Attribute Name="Cryptographic Erase">True</Attribute>
</Component>
```

10 BIOS Configuration

SCP can be used to apply any BIOS setting. A few common activities have been included below and additional details can be found in the Creating and Managing XML Configuration Files by Using WS-Man whitepaper.

10.1 Workload profiles

Workload profiles are collections of BIOS settings. When workload profiles are combined with SCP Imports, the workload profile will be applied first and then the remaining attributes in the template will be applied.

```
{ "FQDD": "BIOS.Setup.1-1",
  "Attributes": [
  { "Name": "WorkloadProfile",
    "Value": "NotAvailable",
    "Set On Import": "True",
    "Comment": "Read and Write" },
```

The 'WorkloadProfile' attribute will always be exported as NotAvailable regardless of what was recently applied. This attribute is not persistent and only serves to trigger a workload profile swap.

NOTE: Depending on the server's installed processor, certain possible values might not be available for this attribute.

10.2 F1 / F2 Error Prompt

The BIOS 'F1 / F2 Error Prompt' setting is enabled by default. If BIOS detects an error during POST while this setting is Enabled, then the POST boot process will be stopped at a 'Press F1/F2 to continue' prompt.

This setting can be disabled in F2 during POST or via SCP with this attribute:

```
{ "Name": "ErrPrompt",
  "Value": "Disabled",
  "Set On Import": "True",
  "Comment": "Read and Write" },
```

This error prompt can disrupt LifecycleController operations including Server Configuration Profile Imports. If a SCP Import operation appears to be stuck at 20% 'Applying configuration changes.' then check the host to see if it's waiting at this error prompt.

10.3 Changing the Boot Order

SCP offers a few different options for updating the boot order and hard disk order for the host.

Set the order by putting a single FQDD into each of SetBootOrderFqdd numbered attributes.

```
<Attribute Name="SetBootOrderFqdd1">NIC.Integrated.1-1-1</Attribute>
<Attribute Name="SetBootOrderFqdd2">HardDisk.List.1-1</Attribute>
…
<Attribute Name="SetBootOrderFqdd16"></Attribute>
```

The same can be done for the hard disk order.

```
<Attribute Name="SetLegacyHddOrderFqdd1">RAID.Integrated.1-1</Attribute>
<Attribute Name="SetLegacyHddOrderFqdd2">RAID.Slot.2-1</Attribute>
…
<Attribute Name="SetLegacyHddOrderFqdd16"></Attribute>
```

Alternatively, the BiosBootSeq and UefiBootSeq attributes offer a comma delimited option. BiosBootSeq will be available when in legacy boot mode. UefiBootSeq will be available when in UEFI boot mode.

```
<Attribute Name="BiosBootSeq">HardDisk.List.1-1,NIC</Attribute>
```

Hard drive disk can also be declared as a comma delimited FQDD list.

```
<Attribute Name="HddSeq">RAID.Integrated.1-1, RAID.Slot.2-1</Attribute>
```

One-time boot options are also available and will only persist through a single boot.

```
<Attribute Name="OneTimeBiosBootSeq"></Attribute>
<Attribute Name="OneTimeUefiBootSeq"></Attribute>
<Attribute Name="OneTimeHddSeq"></Attribute>
```

10.4 Enable or disable a boot order entry

A boot device can be enabled in the boot order by using the SetBootOrderEn attribute. Any FQDD in the comma delimited list will be enabled in the boot order.

```
<Attribute Name="SetBootOrderEn">HardDisk.List.1-1,NIC.Integrated.1-1-1</Attribute>
```

Likewise, a boot device can be disabled in the boot order by using the SetBootOrderDis attribute in a similar manner.

```
<Attribute Name="SetBootOrderDis">HardDisk.List.1-1</Attribute>
```

10.5 System and setup passwords

BIOS system and setup passwords can be applied with the following attributes.

```
    { "Name": "OldSysPassword",
      "Value": "oldpassword",
      "Set On Import": "True",
      "Comment": "Read and Write" },
    { "Name": "NewSysPassword",
      "Value": "newpassword",
      "Set On Import": "True",
      "Comment": "Read and Write" },
    { "Name": "OldSetupPassword",
      "Value": "oldpassword",
      "Set On Import": "True",
      "Comment": "Read and Write" },
    { "Name": "NewSetupPassword",
      "Value": "newpassword",
      "Set On Import": "True",
      "Comment": "Read and Write" },
```

Each password requires that the old password be provided along with the new password. The old password will be validated and if successful then the new password will be applied.

NOTE: Passwords in SCP templates will always be commented out by default and populated with ‘****’ as their value.**

10.6 PXE (Preboot Execution Environment)

PXE attributes are available under the BIOS component while the BIOS is in Uefi BootMode.

When one of the PxeDevXEnDis (1,2,3,4) attributes is Enabled, a new associated PXE device will appear under the UefiBootSeq. The PxeDevXInterface attribute will need to be mapped to the desired bootable network device.

In the example below, PxeDev1EnDis is set to Enabled and PxeDev1Interface is assigned to NIC.Embedded.1-1-1.

```
<Component FQDD="BIOS.Setup.1-1">
  <Attribute Name="PxeDev1EnDis">Enabled</Attribute>
  <Attribute Name="PxeDev1Interface">NIC.Integrated.1-1-1</Attribute>
  <Attribute Name="PxeDev1Protocol">IPv4</Attribute>
  <Attribute Name="PxeDev1VlanEnDis">Disabled</Attribute>
  <Attribute Name="PxeDev1VlanId">1</Attribute>
  <Attribute Name="PxeDev1VlanPriority">0</Attribute>
  <Attribute Name="UefiBootSeq">NIC.PxeDevice.1-1</Attribute>
</Component>
```

If PxeDev1EnDis is Disabled, then this device (NIC.Embedded.1-1-1 or NIC.PxeDevice.1-1) would not appear as a bootable device.

Some PXE options are available in legacy (Bios) BootMode and are covered under the LegacyBootProto and PXE section below.

11 NIC / FiberChannel / InfiniBand Configuration

SCP supports a variety of network devices. The focus of this section will be on the unique behaviors available in SCP for these devices.

The full feature set for these devices is outside the scope of this document. It’s recommended to review the network device’s documentation for all available features.

11.1 LegacyBootProto and PXE

While the BIOS is in legacy (Bios) BootMode and a network device’s LegacyBootProto attribute is set to PXE, then that component will appear under the BiosBootSeq (BIOS.Setup.1-1). If the LegacyBootProto is changed to PXE in a template for import, the associated FQDD of the network device can be added to the BiosBootSeq in the desired position. Otherwise it will be appended to the end of the boot sequence.

```
 { "FQDD": "NIC.Integrated.1-1-1",
    "Attributes": [
   { "Name": "LegacyBootProto",
     "Value": "PXE",
     "Set On Import": "True",
     "Comment": "Read and Write" },

{ "FQDD": "BIOS.Setup.1-1",
    "Attributes": [
   { "Name": "BiosBootSeq",
     "Value": "HardDisk.List.1-1, NIC.Integrated.1-1-1",
     "Set On Import": "True",
     "Comment": "Read and Write" },
```

NOTE: This setting does not impact the boot settings for the BIOS while in Uefi BootMode. See the above PXE section for Uefi BootMode PXE operations.

11.2 VirtualizationMode

If a network device supports a VirtualizationMode of NPAR or NPAR+SRIOV then enabling this functionality will cause new FQDDs to appear on the next host reboot.

```
<Component FQDD="NIC.Slot.2-1-1">
  <Attribute Name="VirtualizationMode">NPAR</Attribute>
```

By enabling NPAR settings, new networked partitions will appear as new FQDDs / Components after the next CSIOR operation.

```
<Component FQDD="NIC.Slot.2-1-2">
<Component FQDD="NIC.Slot.2-1-3">
<Component FQDD="NIC.Slot.2-1-4">
```

If a template is generated on a server with NPAR enabled and applied to a system with NPAR disabled, then SCP Import will automatically resolve these dependencies. The settings will be applied in a single SCP Import operation. Confirm that all desired settings were applied by reviewing the configuration results and/or LCL.

11.3 InfiniBand modes

InfiniBand network devices can transition between 'Ethernet' mode and 'IB (InfiniBand)' mode using the NetworkLinkType attribute. While in 'Ethernet' mode, the network device will present with an FQDD starting with NIC (e.g. NIC.Slot.4-1-1). While in 'IB' mode, the network device will present with an FQDD starting with InfiniBand (e.g. InfiniBand.Slot.4-1-1).

Example of a device in 'Ethernet' mode:

```
<Component FQDD="NIC.Slot.4-1-1">
  <Attribute Name="NetworkLinkType">Ethernet</Attribute>
```

Example of a device in 'IB' mode:

```
<Component FQDD="InfiniBand.Slot.4-1">
  <Attribute Name="NetworkLinkType">IB</Attribute>
```

When using SCP Import to transition between modes, two Part Replacement messages will appear in the LCL like the example below.

```
2020-10-22 09:29:58     PR8    Device not detected: Mellanox ConnectX-6 Single Port VPI HDR
QSFP Adapter - 98:03:9B:9F:51:42(NIC in Slot 4 Port 1 Partition 1)
2020-10-22 09:29:58     PR7    New device detected: Mellanox ConnectX-6 Single Port VPI HDR
QSFP Adapter - 98:03:9B:9F:51:42(InfiniBand Controller in Slot 4)
```

These messages are expected because of the FQDD change in the device.

The configuration results for a NetworkLinkType change will use the FQDD of the original mode. In this example the device is in Ethernet mode and switched to IB mode.

```
Racadm>>lclog viewconfigresult -j JID_033767124177
SeqNumber       = 2316
FQDD            = NIC.Slot.4-1-1
Operation Name  = CHANGE
DisplayValue    = BlnkLeds
Name            = BlnkLeds
OldValue        = 15
NewValue        = 0
Status          = Success
Operation Name  = CHANGE
DisplayValue    = NetworkLinkType
Name            = NetworkLinkType
OldValue        = Ethernet
NewValue        = IB
Status          = Success
```

Despite having different FQDDs, these devices are the same. The set of attributes available to these devices will be different depending on the mode. The feature sets available to these devices are outside of the scope of this document. Please review the network devices user manual for full details.

NOTE: Switching modes and applying attributes on the new mode will require two separate SCP Import operations to complete.

12 SupportAssist Operations

Available on later versions of iDRAC7, iDRAC8 and iDRAC9.

DellEMC's SupportAssist feature can be registered and configured via SCP.

More information about SupportAssist can be found in the SupportAssist on Dell EMC's 14th generation of PowerEdge servers whitepaper.

12.1 Registration

An SCP Export will generate empty attributes under the SupportAssist component for easier registration. These attributes are only used for the registration process and will never export personal information.

```
<Component FQDD="SupportAssist.Embedded.1">
  <!-- <Attribute Name="SupportAssist.1#SupportAssistEULAAccepted"></Attribute> -->
  <!--<Attribute Name="SupportAssist.1#SupportAssistEULAAcceptedByiDRACUser"></Attribute>-->
  <!-- <Attribute Name="SupportAssist.1#PrimaryContactFirstName"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#PrimaryContactLastName"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#PrimaryContactPhoneNumber"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#PrimaryContactAlternatePhoneNumber"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#PrimaryContactEmail"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#SecondaryContactFirstName"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#SecondaryContactLastName"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#SecondaryContactPhoneNumber"></Attribute> -->
  <!--<Attribute Name="SupportAssist.1#SecondaryContactAlternatePhoneNumber"></Attribute>-->
  <!-- <Attribute Name="SupportAssist.1#SecondaryContactEmail"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoCompanyName"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoStreet1"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoStreet2"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoCity"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoState"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoCountry"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#ShippingInfoZip"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#HostOSProxyConfigured"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#HostOSProxyAddress"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#HostOSProxyPort"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#HostOSProxyUserName"></Attribute> -->
  <!-- <Attribute Name="SupportAssist.1#HostOSProxyPassword"></Attribute> -->
</Component>
```

To register SupportAssist, edit the SCP template, provide the Registration information and then import the template.

NOTE: The mandatory fields that are required for registering SupportAssist are Primary First Name, Primary Last Name, Primary Phone Number, Primary Email, Company Name, and Service Address fields (Street1, City, State, Country, Zip).

The following is an example of the attributes for SupportAssist registration using an SCP XML template.

```
<Component FQDD="SupportAssist.Embedded.1">
```

```
  <Attribute Name="SupportAssist.1#SupportAssistEULAAccepted">True</Attribute>
  <Attribute Name="SupportAssist.1#SupportAssistEULAAcceptedByiDRACUser">root</Attribute>
  <Attribute Name="SupportAssist.1#PrimaryContactFirstName">John</Attribute>
  <Attribute Name="SupportAssist.1#PrimaryContactLastName">Doe</Attribute>
  <Attribute Name="SupportAssist.1#PrimaryContactPhoneNumber">123-456-7890</Attribute>
  <Attribute Name="SupportAssist.1#PrimaryContactAlternatePhoneNumber"></Attribute>
  <Attribute Name="SupportAssist.1#PrimaryContactEmail">John_Doe@Dell.com</Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoCompanyName">Dell Inc.</Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoStreet1">200 Dell Way</Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoStreet2"></Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoCity">Round Rock</Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoState">Tx</Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoCountry">USA</Attribute>
  <Attribute Name="SupportAssist.1#ShippingInfoZip">78684</Attribute>
</Component>
```

Additional options for registration are covered in the white paper linked above.

12.2 Configuration

Configuration options for SupportAssist are found under the iDRAC.Embedded.1.

```
<Component FQDD="iDRAC.Embedded.1">
  <Attribute Name="SupportAssist.1#SupportAssistEnableState">Enabled</Attribute>
  <Attribute Name="SupportAssist.1#EventBasedAutoCollection">Enabled</Attribute>
  <Attribute Name="SupportAssist.1#ProSupportPlusRecommendationsReport">Disabled</Attribute>
  <Attribute Name="SupportAssist.1#FilterAutoCollections">Yes</Attribute>
  <Attribute Name="SupportAssist.1#DefaultProtocol">CIFS</Attribute>
  <Attribute Name="SupportAssist.1#DefaultIPAddress"/>
  <Attribute Name="SupportAssist.1#DefaultShareName"/>
  <Attribute Name="SupportAssist.1#DefaultWorkgroupName"/>
  <Attribute Name="SupportAssist.1#DefaultUserName"/>
  <!-- <Attribute Name="SupportAssist.1#DefaultPassword">******</Attribute> -->
  <Attribute Name="SupportAssist.1#EmailOptIn">Yes</Attribute>
  <Attribute Name="SupportAssist.1#PreferredLanguage">English</Attribute>
  <Attribute Name="SupportAssist.1#DefaultProtocolPort">0</Attribute>
  <Attribute Name="SupportAssist.1#RequestTechnicianForPartsDispatch">No</Attribute>
</Component>
```

SupportAssist.1#EmailOptIn - The EmailOptIn attribute should be set to Yes to receive email notifications from Dell on case creation and collection upload.

SupportAssist.1#PreferredLanguage – Possible values are English, German, French, Japanese, Spanish, Simplified Chinese

SupportAssist.1#FilterAutoCollections - The FilterAutoCollections attribute should be set to Yes if to filter the auto generated collections for identification information

SupportAssist.1#ProSupportPlusRecommendationsReport - The ProSupportPlusRecommendationReport attribute must be set to Enabled to receive recommendations for the server in the ProSupport Plus Recommendations Report.

SupportAssist.1#EventBasedAutoCollection - The EventBasedAutoCollection attribute should be set to Enabled for SupportAssist to receive critical events and request collections from the server.

SupportAssist.1#SupportAssistEnableState - The SupportAssistEnableState attribute indicates whether the SupportAssist auto collection features are enabled on the server.

13 RepositoryUpdates

Available on later versions of iDRAC7, iDRAC8 and iDRAC9.

SCP Import can also perform firmware updates via Dell's Repository Update feature using the SCP.1#RepositoryUpdate attribute.

Dell Repository Manager can be used to construct an update repository. The tool set and more information about the feature is provided in the link below.

https://www.dell.com/support/article/en-us/sln283183/support-for-dell-emc-repository-manager-drm

NOTE: This feature requires network connectivity and cannot be performed via SCP over USB.

The RepositoryUpdate value should point to a Catalog.xml file in a path relative to the location of the SCP template on a network share. The exact name of the Catalog.xml file may vary on new repository generation, so it's recommended to check the repository for the correct name.

```
<Component FQDD="System.Embedded.1">
  <Attribute Name="SCP.1#RepositoryUpdate">repo/Catalog.xml</Attribute>
</Component>
```

Example share layout:

```
network_share/template.xml            <- The SCP template.
network_share/repo/Catalog.xml        <- The Catalog.xml describing the updates repository.
network_share/repo/<repository files> <- The repository files needed for updates.
```

Older versions of iDRAC may generate the attribute as just 'RepositoryUpdate' instead of 'SCP.1#RepositoryUpdate'. The older format is supported on all versions of iDRAC.

13.1 Workflow

The RepositoryUpdates workflow is a little different from a traditional SCP Import. If the RepositoryUpdates attribute is populated with a valid path to a repository, then the updates workflow will attempt to detect any devices that need to be updated when compared against the catalog. Any detected updates will generate a new job (with JID) for that device. The Job Queue will contain a standard SCP Import job, Repository Update job and potentially multiple device specific update jobs.

```
racadm>>jobqueue view
-------------------------JOB QUEUE------------------------
[Job ID=JID_033096641979]
Job Name=Configure: Import Server Configuration Profile
Status=Downloading
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Wed, 21 Oct 2020 14:47:44]
Actual Completion Time=[Not Applicable]
Message=[SYS191: Importing Server Configuration Profile.]
Percent Complete=[5]
----------------------------------------------------------
[Job ID=JID_033096656685]
```

```
Job Name=Repository Update
Status=New
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Not Applicable]
Actual Completion Time=[Not Applicable]
Message=[JCP000: New]
Percent Complete=[NA]
----------------------------------------------------------
```

The first stage of the update operation will be to download the DUP (Dell Update Packages) to the iDRAC and prepare for updates. Once the downloads have completed, the SCP Import operation will continue as normal.

If any of the updates or configuration require a host reboot, then the host will reboot and begin applying all updates and settings. The update jobs will be marked as Completed as they finish applying. The SCP operation will continue as normal.

Once all firmware and configuration settings have been applied, the host will reboot and run through a single CSIOR operation to collect inventory. If an iDRAC update was detected, then the SCP operation will be marked as Completed and restart the iDRAC. If no iDRAC update was detected, then the SCP operation will be marked as Completed.

In the example below, the repository only contained NIC packages.

```
racadm>>jobqueue view
-------------------------JOB QUEUE------------------------
[Job ID=JID_033097888997]
Job Name=Configure: Import Server Configuration Profile
Status=Completed
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Wed, 21 Oct 2020 14:49:48]
Actual Completion Time=[Wed, 21 Oct 2020 15:10:14]
Message=[SYS053: Successfully imported and applied Server Configuration Profile.]
Percent Complete=[100]
----------------------------------------------------------
[Job ID=JID_033097907795]
Job Name=Repository Update
Status=Completed
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Not Applicable]
Actual Completion Time=[Not Applicable]
Message=[RED001: Job completed successfully.]
Percent Complete=[100]
----------------------------------------------------------
[Job ID=JID_408320785833]
Job Name=Firmware Update: NIC
Status=Completed
Start Time=[Next Reboot]
Expiration Time=[Not Applicable]
Message=[PR19: Job completed successfully.]
```

```
Percent Complete=[NA]
----------------------------------------------------------
```

The SCP Import job status will be a combination of all update jobs and configuration settings. A job status of ‘Completed with Errors’ or ‘Failed’ requires review of the configuration results or LCL for next steps.

SCP Import with RepositoryUpdates can also be paired with SCP OS deployment operations to create a full end-to-end updates, configuration, and deployment solution all from a single template.

NOTE: Local SCP support (non-networked) via Redfish and Racadm, and SCP via USB does not support RepositoryUpdates.

14 iDRAC Direct (SCP via USB)

On the 14th generation servers, a dedicated micro USB port is available to configure iDRAC. A server can be configured by using a SCP template stored on a USB drive.

14.1 Setup

Create a directory in root of the USB device called System_Configuration_XML that contains both the SCP template and control files:

- The SCP template must follow the following naming convention; <servicetag>-config.xml, <servicetag>-config.json, <modelnumber>-config.xml, <modelnumber>-config.json,config.xml or config.json.
- Control file (control.xml) – Includes parameters to control the SCP Import operation. The control file contains three parameters:
    - ShutdownType – Graceful, Forced, No Reboot.
    - TimeToWait (in secs) – 300 minimum and 3600 maximum.
    - EndHostPowerState – on/off.

Example control.xml:

```
<InstructionTable>
  <InstructionRow>
    <InstructionType>Configuration XML import Host control Instruction</InstructionType>
    <Instruction>ShutdownType</Instruction>
    <Value>NoReboot</Value>
    <ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
    <InstructionType>Configuration XML import Host control Instruction</InstructionType>
    <Instruction>TimeToWait</Instruction>
    <Value>300</Value>
    <ValuePossibilities>Minimum value is 300 -Maximum value is 3600
seconds.</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
    <InstructionType>XML import Host control Instruction</InstructionType>
    <Instruction>EndHostPowerState</Instruction>
    <Value>On</Value>
    <ValuePossibilities>On,Off</ValuePossibilities>
  </InstructionRow>
</InstructionTable>
```

NOTE: The Server Control privilege is required to perform this operation.

14.2 Execution

To import the server configuration profile from the USB device to iDRAC:

1. Configure the USB management port:

    a. Set USB Management Port Mode to Automatic or iDRAC.

    b. Set iDRAC Managed: USB XML Configuration to Enabled with default credentials or Enabled.

2. Insert the USB key (that has the **configuration.xml** and the **control.xml** file) to the iDRAC USB port.

3. The server configuration profile is discovered on the USB device in the **System_Configuration_XML** sub-directory under the USB device root directory. It is discovered in the following sequence:

    a. <servicetag>-config.xml / <servicetag>-config.json

    b. <modelnum>-config.xml / <modelnum>-config.json

    c. config.xml / config.json

4. A server configuration profile import job starts. If the profile is not discovered, then the operation stops. If **iDRAC Managed: USB XML Configuration** was set to **Enabled with default credentials** and the BIOS setup password is not null or if one of the iDRAC user accounts have been modified, an error message is displayed, and the operation stops.

5. LCD panel and LED, if present, display the status that an import job has started.

6. If there is a configuration that needs to be staged and the **Shutdown Type** is specified as **No Reboot** is specified in the control file, the server must be manually rebooted for the settings to be applied. Else, the server is rebooted, and the configuration will be applied. Only when the server was already powered down, then the staged configuration is applied even if the **No Reboot** option is specified.

7. After the import job is complete, the LCD/LED indicates that the job is complete. If a reboot is required, LCD displays the job status as “Paused waiting on reboot”.

8. If the USB device is left inserted on the server, the result of the import operation is recorded in the **results.xml** file in the USB device.

NOTE: More information about this workflow, logs, results and error codes can be found in the iDRAC User’s Guide.

15 OS Deployment

OS deployment support was added to SCP in iDRAC9 version 4.00.00.00. When paired with RepositoryUpdate and configuration, this enables an SCP Import operation to perform a full deployment using a single template.

The benefits of utilizing SCP for OS deployment and all available workflows are covered in great detail in the ‘Using Server Configuration Profiles to Deploy Operating Systems to Dell EMC PowerEdge Servers’ whitepaper.

The OS deployment with SCP workflows are already well covered by the whitepaper above. To expand on the whitepaper, this section includes steps to perform an OS deployment operation via SCP over USB.

15.1 Attributes

SCP Export will automatically generate empty attributes for OS deployment in a template under the LifeycleController.Embedded.1 component.

The SupportedOSList attribute will contain a list of supported operating system drivers. This is a read only attribute but is included by default for informational purposes. Providing one of these operating systems to the OSName attribute will trigger the DriverPack attach operation.

NOTE: If the SupportedOSList attribute is empty, then install the DriverPack DUP from the iDRAC user interface. This can occur after a System Erase has been performed on the server.

The ExposeDuration attribute determines how long the DriverPack partition will be exposed to the host OS (in seconds). The default is 65535 seconds or 18 hours.

The remainder of the attributes pertain to the BootToNetworkISO operation detailed in the whitepaper.

15.2 Example

```
<Component FQDD="LifecycleController.Embedded.1">
  <!-- <Attribute Name="OSD.1#SupportedOSList">Microsoft Windows Server 2016, Microsoft
Windows Server 2012 R2, Red Hat Enterprise Linux 6.9 x64, Red Hat Enterprise Linux 7.5 x64,
SuSE Enterprise Linux 12 SP3 x64</Attribute> -->
  <Attribute Name="OSD.1#OSName"></Attribute>
  <Attribute Name="OSD.1#OSMediaShareIP"></Attribute>
  <Attribute Name="OSD.1#OSMediaShareName"></Attribute>
  <Attribute Name="OSD.1#OSMediaShareUsername"></Attribute>
  <Attribute Name="OSD.1#OSMediaSharePassword">******</Attribute>
  <Attribute Name="OSD.1#OSMediaShareDomainName"></Attribute>
  <Attribute Name="OSD.1#OSMediaShareType"></Attribute>
  <Attribute Name="OSD.1#OSMediaName"></Attribute>
  <Attribute Name="OSD.1#AnswerFileName"></Attribute>
  <Attribute Name="OSD.1#ExposeDuration"></Attribute>
  <Attribute Name="OSD.1#OSMediaHashType"></Attribute>
  <Attribute Name="OSD.1#OSMediaHashValue"></Attribute>
</Component>
```

15.3 OS Deployment via USB

OS Deployment operations can be performed via the iDRAC Direct / SCP via USB workflow assuming the iDRAC can access the network share containing the ISO.

In the template file located on the USB key configure the following attributes to point to the networked ISO.

Example:

```
<SystemConfiguration>
  <Component FQDD="LifecycleController.Embedded.1">
    <!-- <Attribute Name="OSD.1#SupportedOSList">Microsoft Windows Server 2016, Microsoft 
Windows Server 2012 R2, Microsoft Windows Server 2019, Red Hat Enterprise Linux 8.0 x64, Red 
Hat Enterprise Linux 7.6 x64, SuSE Enterprise Linux 15 x64</Attribute> -->
    <Attribute Name="OSD.1#OSName">Microsoft Windows Server 2019</Attribute>
    <Attribute Name="OSD.1#OSMediaShareIP">100.65.84.72</Attribute>
    <Attribute Name="OSD.1#OSMediaShareName">cifs_share_vm</Attribute>
    <Attribute Name="OSD.1#OSMediaShareUsername">administrator</Attribute>
    <Attribute Name="OSD.1#OSMediaSharePassword">P@ssw0rd</Attribute>
    <Attribute Name="OSD.1#OSMediaShareType">CIFS</Attribute>
    <Attribute Name="OSD.1#OSMediaName">WindowsSvrs2019EnglishStd.iso</Attribute>
  </Component>
</SystemConfiguration>
```

Once the template is configured, follow the steps detailed in the iDRAC Direct (SCP via USB) section to trigger an SCP Import operation with OS deployment.

NOTE: An OSMediaShareType value of ‘local’ is not supported in this workflow.

16 Telemetry Operations

With iDRAC9 v4.0, Dell EMC introduced the Telemetry Streaming solution for PowerEdge servers. The feature enables IT managers to integrate advanced server hardware operation telemetry into their existing analytics solutions.

More information about the Telemetry Streaming solution can be found in the Telemetry Streaming with iDRAC9—What you Need to Get Started white paper.

Additional Telemetry information can be found on the Support for Integrated Dell Remote Access Controller 9 (iDRAC9) webpage under the Telemetry tab.

The Telemetry Streaming solution requires the Datacenter license. Most options are viewable in the template regardless of license but can only be enabled and configured via SCP Import with the Datacenter license.

16.1 Example

Telemetry attributes are in the template under the iDRAC.Embedded.1 component.

```
<Component FQDD="iDRAC.Embedded.1">
  <Attribute Name="Telemetry.1#EnableTelemetry">Enabled</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer1">10.35.xxx.xxx</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer1Port">xxxx</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer2">10.35.xxx.xxx</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer2Port">xxxx</Attribute>
  <Attribute Name="TelemetryCPUSensor.1#EnableTelemetry">Enabled</Attribute>
  <Attribute Name="TelemetryCPUSensor.1#ReportInterval">600</Attribute>
  <Attribute Name="TelemetryCPUSensor.1#RsyslogTarget">TRUE</Attribute>
  <Attribute Name="TelemetryCPUSensor.1#ReportTriggers">TMPCpuCriticalTrigger</Attribute>
</Component>
```

On a successful SCP Import, the configuration results will contain an entry for each successfully applied attribute. The example below simply enables the Telemetry feature.

```
racadm>>lclog viewconfigresult -j JID_034846688291
SeqNumber        = 8008
FQDD             = iDRAC.Embedded.1
Job Name         = Import Configuration
Operation Name   = CHANGE
DisplayValue     = Enable Telemetry
Name             = Telemetry.1#EnableTelemetry
OldValue         = Disabled
NewValue         = Enabled
Status           = Success
ErrCode          = 0
```

16.2 Custom Metric Report Definitions

As a part of the iDRAC9 4.40.00.00 release, SCP now includes the ability to configure Telemetry's custom Metric Report Definitions via the 'Include Custom Telemetry' flag in SCP Export. This option is available via all interfaces and a racadm example is shown below.

```
racadm get -t xml -f export.xml -u user -p password -l //ip/share/ --includeCustomTelemetry
```

or

```
racadm get -t json -f export.json -u user -p password -l //ip/share/ --includeCustomTelemetry
```

NOTE: The ‘Include Custom Telemetry’ option can be combined with any other optional parameters.

This flag will add a new XML or JSON element to the template that is outside of the legacy schema. As a result, the schema has been updated in iDRAC9 4.40.00.00 to accommodate this new feature. Templates generated with this optional flag are not backwards compatible with older versions of iDRAC.

The custom Metric Report Definitions can be located at the end of the template under the CustomComponents element in XML templates.

```
<SystemConfiguration>
  <Component FQDD="iDRAC.Embedded.1">
    <Attribute Name="Telemetry.1#EnableTelemetry">Enabled</Attribute>
  </Component>
  <CustomComponents>
    <CustomMetricReportDefinitions>
      …
    </CustomMetricReportDefinitions>
  </CustomComponents>
</SystemConfiguration>
```

Likewise, the CustomComponents block can be located towards the end of a JSON template.

```
],
"CustomComponents": {
  "CustomMetricReportDefinitions": [
  {
    "@odata.type": "#MetricReportDefinition.v1_3_0.MetricReportDefinition",
```

Importing Telemetry custom Metric Report Definitions requires that the Datacenter license is installed on the iDRAC and the Telemetry feature is enabled. The Telemetry feature can be enabled, configured, and applied custom Metric Report Definitions in a single SCP Import operation.

16.3 Troubleshooting

Below are examples of possible error scenarios when configuring Telemetry and custom Metric Report Definitions.

16.3.1 Missing License

If the Datacenter license is missing, then the configuration results will show a SYS319 message ID for CustomComponents.

SYS319 - The operation cannot be completed because either the required license is missing or expired.

```
racadm>>lclog viewconfigresult -j JID_034847857859
SeqNumber       = 8049
```

```
FQDD            = iDRAC.Embedded.1
Job Name        = Import Configuration
Operation Name  = CHANGE
DisplayValue    = iDRAC.Embedded.1#CustomComponents
Name            = CustomComponents
OldValue        = ""
NewValue        = ""
Status          = Failure
MessageID       = SYS319
ErrCode         = 12562
```

16.3.2 Telemetry Not Enabled

If the Telemetry feature is not enabled, then the configuration results will show a SYS460 message ID for CustomComponents.

SYS460 - Unable to perform the necessary telemetry operation because the Telemetry feature is disabled.

```
racadm>>lclog viewconfigresult -j JID_034845831354
SeqNumber       = 8002
FQDD            = iDRAC.Embedded.1
Job Name        = Import Configuration
Operation Name  = CHANGE
DisplayValue    = iDRAC.Embedded.1#CustomComponents
Name            = CustomComponents
OldValue        = ""
NewValue        = ""
Status          = Failure
MessageID       = SYS460
ErrCode         = 10376
```

16.3.3 Schema Validation Error

If the CustomComponents element is included in a template imported to any iDRAC before version iDRAC9 v4.40, then the resulting job status will be Failed with a message id of SYS047.

SYS047 - Input file for import configuration is not compliant with configuration schema.

```
racadm>>jobqueue view -i JID_035451979234
---------------------------- JOB -------------------------
[Job ID=JID_035451979234]
Job Name=Configure: Import Server Configuration Profile
Status=Failed
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Sat, 24 Oct 2020 08:13:17]
Actual Completion Time=[Sat, 24 Oct 2020 08:13:18]
Message=[SYS047: Input file for import configuration is not compliant with configuration
schema.]
Percent Complete=[100]
```

17 Secure Enterprise Key Management Operations

Available in iDRAC9 version 4.00.00.00 and above.

Full details on the Secure Enterprise Key Management solution can be found in the Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers documentation. The focus of this document will be on enabling and configuring SEKM via SCP Import.

17.1 Prerequisites

The example workflow below uses Gemalto KeySecure for the Key Management Server. Configuration of SEKM via SCP will require a CSR generated and signed from Gemalto, and a Server CA also from Gemalto.

The contents of both can be imported using the CertType/CertData attributes (Certificates).

17.2 Example XML

```
<Component FQDD="iDRAC.Embedded.1">
  <Attribute Name="SEKM.1#IPAddressInCertificate">Disabled</Attribute>
  <Attribute Name="SEKM.1#SEKMStatus">Enabled</Attribute>
  <Attribute Name="SEKM.1#KeyAlgorithm">AES-256</Attribute>
  <Attribute Name="SEKM.1#Rekey">False</Attribute>
  <Attribute Name="KMS.1#PrimaryServerAddress">100.64.25.206</Attribute>
  <Attribute Name="KMS.1#KMIPPortNumber">5696</Attribute>
  <Attribute Name="KMS.1#Timeout">10</Attribute>
  <Attribute Name="KMS.1#iDRACUserName">idracuserG1FWHQ2</Attribute>
  <Attribute Name="KMS.1#iDRACPassword">P@ssw0rd</Attribute>
  <Attribute Name="KMS.1#RedundantKMIPPortNumber">5696</Attribute>
  <Attribute Name="SEKMCert.1#CommonName">idracuserG1FWHQ2</Attribute>
  <Attribute Name="SEKMCert.1#OrganizationName">Dell EMC</Attribute>
  <Attribute Name="SEKMCert.1#OrganizationUnit">Test</Attribute>
  <Attribute Name="SEKMCert.1#LocalityName">Round Rock</Attribute>
  <Attribute Name="SEKMCert.1#StateName">Texas</Attribute>
  <Attribute Name="SEKMCert.1#CountryCode">US</Attribute>
  <Attribute Name="SEKMCert.1#EmailAddress">tester@dell.com</Attribute>
  <Attribute Name="SEKMCert.1#SubjectAltName"/>
  <Attribute Name="SEKMCert.1#UserId"/>
  <Attribute Name="SecurityCertificate.1#CertData">-----BEGIN CERTIFICATE-----
    MIIEvzCCA6egAwIBAgIBADANBgkqhkiG9w0BAQsFADCBoDELMAkGA1UEBhMCVVMx
    DjAMBgNVBAgTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2NrMREwDwYDVQQKEwhE
    ZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxpZGF0aW9uMRAwDgYD
    VQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19yb2VtZXJAZGVsbC5j
    b20wHhcNMTkwMjE0MjA1NjQ4WhcNMjkwMjEyMjA1NjQ4WjCBoDELMAkGA1UEBhMC
    VVMxDjAMBgNVBAgTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2NrMREwDwYDVQQK
    EwhEZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxpZGF0aW9uMRAw
    DgYDVQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19yb2VtZXJAZGVs
    bC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQChyihz1suLIIzl
    K+XxI9nh59J+yCNXsMpKzneX0CSr1Aiay1Yyd1Uy2lcifJbmuocP2wLQUEWTnR19
    K0zbRKTMNty0fr9NhnwiRFVfUzUPiEGPwTyqR7w2WmHqu5jCnOodC9n+6w8lGnV9
    3LzKLaJYdJ9TPGn63ffVrDeprhQ376EK6QjR1xlrTG7kUH2Hu9D1thwxQCykS2eQ
    50icshUAsy5sCo5quisNLZZmJefREPxlx7ih/NtMGe5lEiZGyHIf91Ucf5L2vP6J
    lYKLZL7AqvJioHSSxD8nvP7naxKmIL3d1zohV8V+8DMc1UabDLhgUek/UX+jqSQ3
    cuCY6LhLAgMBAAGjggEAMIH9MB0GA1UdDgQWBBQEk+OPdA03pnzCGUBnUK5a2Z/v
    hzCBzQYDVR0jBIHFMIHCgBQEk+OPdA03pnzCGUBnUK5a2Z/vh6GBpqSBozCBoDEL
    MAkGA1UEBhMCVVMxDjAMBgNVBAgTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2Nr
    MREwDwYDVQQKEwhEZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxp
    ZGF0aW9uMRAwDgYDVQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19y
    b2VtZXJAZGVsbC5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOC
    AQEAgumRcKE3+dbYgNRNeYbvKH29B1NI0l/PIP2V6he4/rDLYgyBLqNmtvRCUvu9
    DnZczchZoGIdWm0j/1gW21O8nptDM+R3olMEwNGdl+ZQNLUdMKdzKJbji8IaSxun
    B4Y21uLvykGm0Ts+X2/R84RAFHgDrRrentaM2WyJ7GCT470CDdUIg7NApxm8WoSA
    EQrt6RGJYQlRZTFTW12f9+2K7CifHvNnth0zLjaK+vK4bTwhaPhkbM/OO/qE1vaH
    zgwN+ZaVbl+amGabZdMvQbtDRgNoS+hQ7T91kbJjPJfza4frrxDzZyhxEN2H99pt
    zIto472w7hLB56tRjHfA6Vnh4w==
    -----END CERTIFICATE-----</Attribute>
  <Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
  <Attribute Name="SecurityCertificate.2#CertData">-----BEGIN CERTIFICATE-----
    MIID2zCCAsOgAwIBAgIDAmNQMA0GCSqGSIb3DQEBCwUAMIGgMQswCQYDVQQGEwJV
    UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJvdW5kIFJvY2sxETAPBgNVBAoT
    CERlbGwgRU1DMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbGlkYXRpb24xEDAO
    BgNVBAMTB0RlbGwgQ0ExJDAiBgkqhkiG9w0BCQEWFXRleGFzX3JvZW1lckBkZWxs
    LmNvbTAeFw0xOTA1MTYxODMyMzlaFw0yOTAyMTIxODMyMzlaMIGPMQswCQYDVQQG
    EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV
    BAoMCERlbGwgRU1DMQ0wCwYDVQQLDARUZXN0MRkwFwYDVQQDDBBpZHJhY3VzZXJH
    MUZXSFEyMR4wHAYJKoZIhvcNAQkBFg90ZXN0ZXJAZGVsbC5jb20wggEiMA0GCSqG
    SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCl2WXSI3N9OEXmbCxwylhkk2g/OYyvupwg
    nL5uEF4TF8+BKjc3hw1PryzK+vPMPSv7J9fX4Ropy5bjsLXL7ZUdKTYMrhSlZ/13
    v7qdZkBInHJfpHTiXbKQwvaMryPedToLNTWdG0Mr+ni05Ebzx/eG+x3LJQsbkxwX
    f5NQGVZNtZnYzdTCkQnwmfseBRfJSzbxTm8HpoT9KGchVsYZDpPSz54ZIRlbqRmz
    wJBlcyEPq63CjFp4RxfmZW0IPOGbmmcnGy3Rd4YFBmiC75pR3Wx+J1Xzr3inyRJ2
    /XWpgm4XYfGSbyQ2in6Kzwf8CA3hTdsdx20FGJ0j3EUnj1PpOOq1AgMBAAGjLTAr
    MAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgeAMAsGA1UdDwQEAwIF4DANBgkq
    hkiG9w0BAQsFAAOCAQEAVJdEgKMfmhjrRulC/f7SZjy6pDhLSGM5KwJjQm/8fSjm
    lfEyVTbD/eedWo6U6cah2uZrY0jD6SN17CAGMU/J6r4jkhZMrmB/cr3HXiCDQd/x
    ReqmjVWOCJDb/tStOkWAS3VFuRZzXfkO83Kp6Zzak4Ue3mwJywThklOsoyXx1XEs
    esNFxcsAGL9ABcuGUShpdKtYYwWo98og6P1w1aiWRnaZQ6HP4To3tfmnQ9QKUeZ1
    i3QsZ5Q6l86dBZjaaoKSWp5y1fph2ciV//SoOtPhNHXYP5H/3AUQoEqNw7lSX2H/
    w9TJtElsc2htmbp6bHudrVIlB80lehk6IE4UxAEO/w==
    -----END CERTIFICATE-----</Attribute>
  <Attribute Name="SecurityCertificate.2#CertType">SEKM_SSL_CERT</Attribute>
</Component>
```

17.3 Enabling SEKM settings on the iDRAC

The two prerequisites can be found in SecurityCertificate.1#CertType, SecurityCertificate.1#CertData for the Server CA (KMS_SERVER_CA), and SecurityCertificate.2#CertType, SecurityCertificate.2#CertData for the CSR (SEKM_SSL_CERT).

The configuration results for the SCP Import operation will confirm the successful enablement of SEKM via the SKEM.1#SEKMStatus attribute.

```
racadm>>lclog viewconfigresult -j JID_581182121065
SeqNumber = 5966
FQDD = iDRAC.Embedded.1
Job Name = Import Configuration
DisplayValue = SEKM.1#SEKMStatus
Name = SEKM.1#SEKMStatus
OldValue = Disabled
NewValue = Enabled
Status = Success
ErrCode = 0
SeqNumber = 5963
```

The SEKM certificate installation can be confirmed via the same configuration results by checking the CertData and CertType attributes.

```
SeqNumber = 5963
FQDD = iDRAC.Embedded.1
Job Name = Import Configuration
DisplayValue = Certificate Data
Name = SecurityCertificate.1#CertData
OldValue = ******
NewValue = ******
Status = Success
ErrCode = 0
DisplayValue = Certificate Type
Name = SecurityCertificate.1#CertType
OldValue = ""
NewValue = KMS_SERVER_CA
Status = Success
ErrCode = 0
DisplayValue = Certificate Data
Name = SecurityCertificate.2#CertData
OldValue = ******
NewValue = ******
Status = Success
ErrCode = 0
DisplayValue = Certificate Type
Name = SecurityCertificate.2#CertType
OldValue = ""
NewValue = SEKM_SSL_CERT
Status = Success
ErrCode = 0
```

NOTE: iDRAC SEKM attributes must be configured in a separate SCP Import operation (or another interface) before enabling SEKM on a PERC device and creating a locked virtual disk. These operations cannot be combined in a single SCP Import.

17.4 Enable SEKM on a PERC device with a locked RAID volume

Virtual disk creation in this workflow is very similar to the steps cover in the Create and initialize a virtual disk section. The two key differences are the EncryptionMode and LockStatus attributes.

```
<Component FQDD="RAID.Slot.3-1">
  <Attribute Name="RAIDresetConfig">True</Attribute>
  <Attribute Name="EncryptionMode">Secure Enterprise Key Manager</Attribute>
  <Component FQDD="Disk.Virtual.0:RAID.Slot.3-1">
    <Attribute Name="RAIDaction">Create</Attribute>
    <Attribute Name="LockStatus">Locked</Attribute>
    <Attribute Name="BootVD">True</Attribute>
    <Attribute Name="RAIDinitOperation">None</Attribute>
    <Attribute Name="DiskCachePolicy">Disabled</Attribute>
    <Attribute Name="RAIDdefaultWritePolicy">WriteBack</Attribute>
    <Attribute Name="RAIDdefaultReadPolicy">ReadAhead</Attribute>
    <Attribute Name="Name">SCP VD</Attribute>
    <Attribute Name="Size">0</Attribute>
    <Attribute Name="StripeSize">512</Attribute>
    <Attribute Name="SpanDepth">1</Attribute>
    <Attribute Name="SpanLength">2</Attribute>
    <Attribute Name="RAIDTypes">RAID 1</Attribute>
    <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.0:Enclosure.Internal.0-1:RAID.Slot.3-
1</Attribute>
    <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.1:Enclosure.Internal.0-1:RAID.Slot.3-
1</Attribute>
  </Component>
</Component>
```

To enable SEKM on the PERC device, change the EncryptionMode on your PERC device to ‘Secure Enterprise Key Manager’. The virtual disk on the device can be locked by updating LockStatus to ‘Locked’. The configuration results for the SCP Import operation will reflect the new settings after the job has completed.

```
racadm>>lclog viewconfigresult -j JID_581203847849
SeqNumber = 6094
FQDD = RAID.Slot.3-1
DisplayValue = PERC H740P Adapter
Name = PERC H740P Adapter
Status = Success
DisplayValue = PERC H740P Adapter
Name = PERC H740P Adapter
Status = Success
DisplayValue = SCP VD
Name = SCP VD
NewValue = RAID 1
NewValue = Physical Disk 0:1:0
NewValue = Physical Disk 0:1:1
NewValue = Virtual Disk Size in Bytes : 899527213056
NewValue = Virtual Disk Stripe Size : 256 Kb
NewValue = Physical Disks per Span : 2
NewValue = VirtualDisk Lock status: Locked
```

```
Status = Success
DisplayValue = RAIDbootVD
Name = RAIDbootVD
OldValue = None
NewValue = Disk.Virtual.0:RAID.Slot.3-1
Status = Success
SeqNumber = 6091
FQDD = RAID.Slot.3-1
DisplayValue = PERC H740P Adapter
Name = PERC H740P Adapter
Status = Success
DisplayValue = PERC H740P Adapter
Name = PERC H740P Adapter
Status = Success
```

For more details on SEKM, refer to the Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers white paper.

18 Auto Config – DHCP Provisioning

Dell offers the ability to deploy SCP templates just by connecting a server to the network via the AutoConfig feature. The 'Zero-Touch, Bare-Metal Server Provisioning Using the Dell EMC iDRAC with Lifecycle Controller AutoConfig' white paper contains more details on this functionality.

From the Executive Summary of the white paper;

The Auto Config feature allows IT administrators to build an environment in which servers can automatically configure all hardware settings as part of the out-of-band network management. This eliminates the necessity of high-touch, manual steps to configure server subsystems such as storage, networking, and BIOS. Administrators can develop configuration profiles for classes of servers and apply those profiles without interacting with individual systems.

19 Troubleshooting

19.1 Configuration results and LCL

The first step in troubleshooting issues with an SCP Import operation is to review the configuration results and/or the LCL. When an attribute fails to apply, the configuration results for the job will provide a message ID which will describe the reason for the error condition. Depending on the interface used, the full error message may be shown as well. The full message, recommended response action and detailed descript for each message can be found in the Event and Error Message Reference Guide.

Configuration results are a consolidated version of the information stored in the LCL. These results are not currently viewable from the iDRAC web interface but are available through all command line interfaces and included in the TSR (Technical Support Report) generated by SupportAssist.

Information on the LCL can be found above in the iDRAC Lifecycle Logs section.

Information on configuration results can be found above in the SCP Import / Preview Configuration Results section.

19.2 Known Limitations

- SupportAssist cannot be deregistered or email-opt-out with an SCP Import operation.
- Creating a new VD and adding it to a specific position in the BIOS.Setup.1-1#HddSeq requires two separate SCP Import operations. If the correct FQDD is selected.
- Creating a SWRAID virtual disk and changing the BIOS attribute EmbSata to RAID mode requires two separate SCP Import operations.
- On InfiniBand network devices, switching between Ethernet and IB NetworkLinkTypes and applying changes to attributes on the new mode requires two separate SCP Import operations.
- iDRAC SEKM settings and RAID VD locking actions require two separate SCP Import operations.
- Enabling a BIOS attribute HD place holder, setting it as the first device in the boot order and creating a RAID volume requires two separate SCP Import operations.

19.3 Common Issues

If issues are detected while running an SCP Import or SCP Import Preview operation, then as a general rule the first step should be to check the job status and the configuration results. Most issues can be resolved by reviewing these two data points.

If the issue is still unclear, then the next recommended step would be to review the iDRAC Lifecycle Logs. The start of the SCP operation can be located in the LCL by searching for the Job ID / JID. Each SCP Import operation will begin with a "SYS191: Importing Server Configuration Profile." message. This can be used as a starting point in the LCL for triaging issues.

19.3.1 SYS041 – Schema validation error

SYS041 - Unable to apply some component configuration values.

If a SCP Import operation fails with a "SYS047: Input file for import configuration is not compliant with configuration schema." message, then the configuration results will typically provide a line number for the failure.

```
racadm>>lclog viewconfigresult -j JID_035451979234
SeqNumber       = 8304
Job Name        = Import Configuration
Message ID      = SYS064
Message         = Input file for import configuration is invalid at line 2911
```

If the line number is unclear, then it's recommended to run the template through an external XML or JSON validator to check for errors.

19.3.2 SYS051 – Unable to shut down in time

SYS051 - The system could not be shut down within the specified time.

The operating system can potentially deny or ignore the graceful shutdown request. If the SCP Import operation times out this error, then consider the following options:

- Increase the optional 'Time to Wait' parameter.
- Use the Forced shutdown option.
- Power down the host manually.

19.3.3 SYS055 – Completed with Errors

SYS055 - Import of Server Configuration Profile operation completed with errors.

SCP Import operations use a 'continue on error' policy. Detected errors will be reported to the LCL but the job will continue to apply all settings. SCP Import has intelligent attribute dependency resolution and multiple layers of retries to resolve all possible conflicts. However, any unresolved errors will be logged to the LCL.

The majority of issues will be reported in the configuration results. This includes schema validation issues and dependency issues SCP Import was unable to resolve.

If the operation Completed with Errors and the reason is unclear from the configuration results, then it's recommended to review the iDRAC Lifecycle Logs for more information.

```
racadm>>jobqueue view -i JID_041519610631
---------------------------- JOB -------------------------
[Job ID=JID_041519610631]
Job Name=Configure: Import Server Configuration Profile
Status=Completed with Errors
Scheduled Start Time=[Not Applicable]
Expiration Time=[Not Applicable]
Actual Start Time=[Sat, 31 Oct 2020 08:46:01]
Actual Completion Time=[Sat, 31 Oct 2020 08:46:04]
Message=[SYS055: Import of Server Configuration Profile operation completed with errors.]
Percent Complete=[100]
----------------------------------------------------------
racadm>>lclog viewconfigresult -j JID_041519610631
SeqNumber       = 10430
FQDD            = LifecycleController.Embedded.1
Job Name        = Import Configuration
Operation Name  = CHANGE
DisplayValue    = BIOS Reset To Defaults Requested
Name            = LCAttributes.1#BIOSRTDRequested
```

```
OldValue        = False
NewValue        = badvalue
MessageID       = RAC015
Status          = Failure
ErrCode         = 9240
Operation Name  = CHANGE
DisplayValue    = Default Ignore Certificate warning
Name            = LCAttributes.1#IgnoreCertWarning
OldValue        = On
NewValue        = Off
Status          = Success
ErrCode         = 0
```

In the example above, the job resulted in Completed with Errors. The BIOSRTDRequested attribute only accepts True or False but the template contained 'badvalue' for this attribute. The error shows RAC015 for the attribute.

The error code lookup for RAC015 shows the message as 'Unable to run the method because the input value is not one of the possible values for AttributeName arg1.'

Error Code Lookup: https://qrl.dell.com/LCDError/Lookup?q=ErrorCode

The Attribute Registry shows that 'badvalue' is not one of the possible values for BIOSRTDRequested.

Attribute Registry: https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

19.3.4 SYS072 – Time Out

SYS072 - Server Configuration Profile import operation timed-out.

SCP Import maintains an internal timer for all operations. This timer will scale based on the size of the configuration changes, firmware updates, and other operations being performed by SCP Import.

In the unlikely event that the SCP Import operation times out, check your host boot status. Confirm that the server was able to complete POST successfully. The F1/F2 Error Prompt detailed above may have been triggered and prevented the SCP Import operation from completing its tasks.

19.3.5 LC in Use

It's recommended to perform a GetRemoteServicesStatus check before performing any SCP operation. This command will provide a quick roll up of the server and LC (LifecycleController) status.

```
racadm getremoteservicesstatus
Server status: Out of POST
LC status    : Ready
RT status    : Ready
Status       : Ready
```

If the 'LC status' is In Use or Reloading, then wait until it shows Ready to perform the operation.

If the 'Server status' shows any error such as 'Server has halted at F1/F2 error prompt because of a POST error' then it's recommended to resolve that error before attempting an SCP operation.

20 Additional Resources

20.1 User's Guides, Release Notes, API Guides

The latest versions of the user's guides referenced throughout this document can be located at the link below:

https://www.dell.com/support/home/en-us/product-support/product/idrac9-lifecycle-controller-v4.x-series/docs

20.2 White Papers

All white papers related to SCP and other features can be found at the link below:

https://www.dell.com/support/article/en-us/sln311300/support-for-integrated-dell-remote-access-controller-9-idrac9?lang=en

20.2.1 Using Server Configuration Profiles to Deploy Operating Systems to Dell EMC PowerEdge Servers:

https://downloads.dell.com/manuals/common/dell-emc-scp-os-deploy-poweredge.pdf

20.2.2 Server cloning by using Server Configuration Profiles on PowerEdge servers:

https://downloads.dell.com/solutions/dell-management-solution-resources/ServerCloning_SCP%20v2_50%28DTC%20copy%29.pdf

20.3 Default, Clone & Replace Tables

This section will cover the expected XML commented state when in Default, Clone or Replace modes during an SCP Export. In the JSON format, this is equivalent to the 'SetOnImport' flag being set to True (uncommented) or False (commented).

NOTE: Attributes that are not impacted by Default, Clone and Replace are not included in these tables.

These values are based on the current implementation in iDRAC9 v4.40.00.00.

X – Commented

Blank - Uncommented

Table 2 iDRAC – Default, Clone & Replace

Attribute	Default	Clone	Replace
Users.X#Password	X		
Users.X#SSHPublicKey1	X		
Users.X#SSHPublicKey2	X		
Users.X#SSHPublicKey3	X		
Users.X#SSHPublicKey4	X		
Users.X#SHA256Password	X		
Users.X#SHA1v3Key	X		
Users.X#MD5v3Key	X		
Users.X#SHA256PasswordSalt	X		

Users.X#IPMIKey	X		
SCEP.1#ChallengePassword	X		
LDAP.1#BindPassword	X		
RemoteHosts.1#SMTPPassword	X		
RFS.1#Password	X		
NIC.1#DNSRacName	X	X	
NICStatic.1#DNSDomainName	X	X	
IPv4Static.1#Address	X		
IPv6Static.1#Address1	X		
NTPConfigGroup.1#NTP1SecurityKey	X		
NTPConfigGroup.1#NTP2SecurityKey	X		
NTPConfigGroup.1#NTP3SecurityKey	X		
IOIDOpt.1#VirtualAddressPersistencePolicyNonAuxPwrd	X	X	
IOIDOpt.1#VirtualAddressPersistencePolicyAuxPwrd	X	X	
IOIDOpt.1#InitiatorPersistencePolicy	X	X	
IOIDOpt.1#StorageTargetPersistencePolicy	X	X	
VNCServer.1#Password	X		
USB.1#ZipPassword	X		
SupportAssist.1#DefaultPassword	X		
RSASecurID2FA.1#RSASecurIDClientID	X		
RSASecurID2FA.1#RSASecurIDAccessKey	X		
KMS.1#iDRACPassword	X		
AutoUpdate.1# - All attributes.	X	X	X

Table 3 BIOS – Default, Clone and Replace

Attribute	Default	Clone	Replace
SHA256SystemPassword	X		
SHA256SystemPasswordSalt	X		
SHA256SetupPassword	X		
SHA256SetupPasswordSalt	X		
BiosBootSeq	X		
UefiBootSeq	X		
HddSeq	X		

Table 4 NIC, InfiniBand – Default, Clone and Replace

Attribute	Default	Clone	Replace
VirtFIPMacAddr	X	X	
VirtIscsiMacAddr	X	X	
VirtWWN / VirtualWWN	X	X	
VirtWWPN / VirtualWWPN	X	X	
VLanId	X	X	
VirtPortGUID	X	X	
VirtNodeGUID	X	X	
IscsiInitiator* - All Attributes	X	X	
ConnectFirstTgt	X	X	
FirstTgt* - All Attributes	X	X	

ConnectSecondTgt	X	X	
SecondTgt	X	X	
SecondaryDeviceMacAddr	X	X	
UseIndTgtPortal	X	X	
UseIndTgtName	X	X	
ConnectFirstFCoETarget	X	X	
FirstFCoEWWPNTarget	X	X	
FirstFCoEBootTargetLUN	X	X	
FirstFCoEFCFVLANID	X	X	

Table 5 FC (FiberChannel) – Default, Clone and Replace

Attribute	Default	Clone	Replace
VirtFIPMacAddr	X	X	
VirtIscsiMacAddr	X	X	
VirtWWN / VirtualWWN	X	X	
VirtWWPN / VirtualWWPN	X	X	
VLanId	X	X	
VirtPortGUID	X	X	
VirtNodeGUID	X	X	
BootScanSelection	X	X	
FirstFCTargetConnect	X	X	
FirstFCTargetWWPN	X	X	
FirstFCTargetLUN	X	X	
SecondFCTargetConnect	X	X	
SecondFCTargetWWPN	X	X	
SecondFCTargetLUN	X	X	

Table 6 Storage – Default, Clone and Replace

Attribute	Default	Clone	Replace
CurrentControllerMode	X		
VD – Name	X		
VD – Size	X		
VD – StripeSize	X		
VD – SpanDepth	X		
VD – SpanLength	X		
VD – RAIDTypes	X		
VD – IncludePhysicalDiskID	X		
VD – DiskCachePolicy	X		
VD – RAIDdefaultWritePolicy	X		
VD – RAIDdefaultReadPolicy	X		
Disk – RAIDHostSpareStatus	X		
Disk – RAIDPDState	X		