Dell® Lifecycle Controller Overview

A Dell Technical White Paper

Remote Services Capabilities

By Jon Hass, Andy Butcher and Raja Tamilarasan

Dell Product Group

December 2009

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Table of Contents

EXECUTIVE SUMMARY

What is Lifecycle Controller?

The **Lifecycle Controller** is the engine for advanced embedded system management and is delivered as part of iDRAC Express in the new generation Dell servers. It includes a 1GB managed and persisted storage that embeds systems management features in addition to the iDRAC features. It eliminates the media based system management tools and utilities for managing Dell systems. Users can further upgrade to iDRAC Enterprise and vFlash for other iDRAC features. vFlash enables hosting of customized and bootable service images using vFlash media, an optional add-on to iDRAC Enterprise.

Lifecycle Controller has two interfaces as described below:

1. Unified Server Configurator (USC) - A graphical UI tool for local access of the Lifecycle Controller features in a pre-OS environment.
2. Remote Services – WS-Management web services interfaces for remote server provisioning and management using iDRAC. Consoles and scripts can use these interfaces for remote OS installations, updates and platform configuration.

Lifecycle Controller simplifies end-to-end server lifecycle management as described below:

- Provisioning – Entire pre-OS configuration from a unified interface.
- Deployment – Simplifies OS installation with drivers resident on the Lifecycle Controller.
- Patching/Updates – OS agnostic and minimizes the maintenance downtime with direct access to updates on the Dell support site. It simplifies BIOS and firmware updates by maintaining a working version for rollback purpose.
- Servicing – Availability of diagnostics 24X7 without hard drive dependency . Capability to flash firmware automatically when replacing field replaceable components such as a PowerEdge™ RAID controller, NIC or power supply.
- User customization – Bootable and managed 256MB persistent storage for logs, service images, crash dumps, etc.

Lifecycle Controller features will be enhanced periodically and delivered as firmware updates.

Lifecycle Controller 1.2 Remote Services

Lifecycle Controller 1.2 Remote Services capabilities are focused on enabling automated system platform discovery by management consoles and enhancing remote operating system deployment capabilities. These capabilities are exposed through the web services based hardware management interface provided by the Lifecycle Controller firmware. The Lifecycle Controller 1.2 release feature set for the Dell 11G monolithic and modular blade platforms include the following new capabilities:

- Auto-Discovery and initial security configuration of system service processor
- Remote activation of local exposure of embedded drivers

- Remote acquisition of embedded drivers per selected OS
- Secure boot of provisioning pre-OS environments (alternative to PXE)

Also included in this release are the interface definitions, use guidelines and sample code for using the web services based platform management interfaces. Additionally, the Provisioning Service that facilitates the Auto-Discovery feature is being integrated with a number of system management Console applications.Lifecycle Controller 1.3 Remote Services

The Lifecycle Controller 1.3 adds the following new capabilities and enhancements:

- Custom Factory Install of Auto-Discovery Security Certificates and Provisioning Server Name/Address
- WS-Man Interface for changing Auto-Discovery Certificates and re-initiation of Auto-Discovery
- Pre-OS image staging on vFlash – Boot to a pre-OS image (such as, WinPE) stored on vFlash
- Remote out-of-band instant Firmware Inventory of installed and available firmware images**
- Bare metal out-of-band updates – Remotely initiate offline BIOS, firmware and driver pack update and schedule updates
- Part replacement – Automatic firmware flash for field/customer replaceable components in the system

** Available Images = BIOS, component firmware, Diagnostics, USC and Driver Pack

INTRODUCTION

This whitepaper is intended to provide a high level technical description of new features introduced in the Dell Lifecycle Controller firmware versions 1.2 and 1.3. These features are aimed at simplifying OS deployment, automating the setup and configuration of new server platforms, simplifying server part replacement, firmware inventory and updates. The following information includes a description of the architecture of the Lifecycle Controller and the web service interface for manageability. Also covered are descriptions of remote utilization of embedded OS drivers, booting deployment OS's from network shared ISO images, the automated discovery and initial configuration capabilities, remote configuration of the Part Replacement feature, remote retrieval of firmware inventory and support for OS independent remote firmware updates provided in Lifecycle Controller 1.2 and 1.3.

Lifecycle Controller Manageability Architecture

The Dell Lifecycle Controller provides of a comprehensive set of platform management capabilities that are accessible locally and remotely. At the heart of the architecture are the iDRAC (integrated Dell Remote Access Controller) service processor and the UEFI (Unified Extensible Firmware Infrastructure) system firmware. The iDRAC relies on auxiliary power and, therefore, is running and available to manage the platform from the time the system in plugged into AC power. The iDRAC works in concert with the UEFI firmware to access and manage every aspect of the platform hardware, including component and subsystem management that is beyond the domain of traditional server BMC (Baseboard Management Controller) capabilities. Remote management using the network for programmatic web services, command line (CLI) and graphical user (GUI) interfaces is provided by the iDRAC service processor in an OS independent and system power state independent fashion. The UEFI environment provides the local console interface and the infrastructure for locally and remotely managing system components such as RAID storage, NIC and BIOS configuration.

Web Services Platform Management Interface

The remote management interface for the Lifecycle Controller is a web service based on the Web Services for Management (WS-Man) transport protocol and DMTF Common Information Model (CIM) payloads. The Dell embedded server platform management interfaces are organized into Profiles where each Profile defines the specific interfaces for dealing with a particular management domain or area of functionality. Dell Lifecycle Controller provides implementation of many platform management Profiles defined by the Distributed Management Task Force (DMTF) System Management Architecture for System Hardware (SMASH) 2.0 specification. Additionally, Dell has defined a number of Profile extensions that provide interfaces for capabilities that are unique to the Lifecycle Controller.

The Lifecycle Controller WS-Man implementation uses SSL for transport security and supports basic and digest authentication. Additionally the iDRAC supports validating WS-Man credentials against cached credentials and 3rd Party authentication services such as Microsoft® Active Directory®. The credentials provided must be iDRAC Administrators or have Server Command Execution privileges. Web services interfaces can be used by leveraging client infrastructure such as Windows WinRM™ and Powershell™ command line interfaces, open source utilities like WSMANCLI, and application programming environments like Microsoft .NET™. See the Dell TechCenter wiki (www.DellTechCenter.com) in the OpenManage Systems Management - Lifecycle Controller area for more information about using web services from command line and scripting environments.

Automated Discovery and Provisioning

One of the more time consuming and error prone tasks is the initial setup and integration of a new server with a management console. The Auto-Discovery feature of Lifecycle Controller 1.2 was developed to aid the process of setting up a new server and registering it with a console. The advantages of using this capability includes removing the need to do cumbersome manual local configuration of the new server and enabling an automated way for a console to discover a new server that has been connected to the network and plugged into power. When a new server with the Auto-Discovery feature enabled is plugged in to AC power and connected to the network, the LC will attempt to find a deployment console that has been integration with the Dell Provisioning Server, announce itself, and configure iDRAC access credentials that can be used by the console for further setup and deployment.

Auto-Discovery Security Considerations

Auto-Discovery consists of a discovery process and a handshake process. The discovery process relies on DHCP scope option being configured to contain the hostname and IP address of the Provisioning Server or the DNS being configured to resolve the default Provisioning Service hostname. After the Lifecycle Controller has acquired or resolved the Provisioning Server IP address, a SOAP over HTTPS handshake is performed to acquire initial temporary username/password credentials. These initial credentials are then used for subsequent WS-Management protocol web services requests to provision the iDRAC. A best practice would involve initial web services requests to set up more permanent username/password credentials or Active Directory client configuration and deleting the initial temporary credentials.

Lifecycle Controller uses two certificates for establishing a mutually authenticated encrypted SSL connection between the Lifecycle Controller and the Provisioning Server. The iDRAC handshake client certificate is signed with a Dell certificate authority root certificate for which the public key is made available by Dell to console software partners that incorporate an Auto-Discovery Provisioning Server. The handshake client certificate is generated during the factory build of the server and is unique to every system. The default hostname (Common Name) embedded in the handshake client certificate will be the service tag of the server. The console software can optionally check that the certificate hostname (Common Name) provided matches the service tag provided in the initial handshake request payload.

A private certificate signed by the Dell certificate authority for the Provisioning Server in the console software is provided by Dell to console software partners. During the initial handshake connection, the iDRAC handshake client will verify that the certificate provided by the Provisioning Server during the initial SSL exchange is properly signed by the Dell certificate authority.

Ordering Auto-Discovery Enabled Systems

This Auto-Discovery feature is not enabled by default. It is off unless it is explicitly requested when the server is ordered or can be configured manually via CTRL-E during boot. If the option is ordered, the machine comes with DHCP enabled on the iDRAC with all of its admin accounts disabled. Therefore, it is not necessary to configure a static IP address for the iDRAC; it will get one from a DHCP server on the network. To make use of this feature, a DHCP server or a DNS server (or both as described below) will need to be configured to support the discovery process.

If Auto-Discovery is not enabling during order entry, the factory programming process that occurs when the option is ordered can be duplicated by performing the following steps using the iDRAC setup screen that is initiated on the server by pressing ctrl-E during boot.

1. Enable the NIC (blade servers)
2. Enable Auto-Discovery
3. Enable DHCP
4. Disable the admin accounts
5. Enable “Get DNS server address from DHCP”
6. Enable “Get DNS domain name from DHCP”

Note that the discovery process will not run if the admin accounts are enabled. The final step in the handshake process that follows the discovery process is for the Provisioning Server to create an admin account with a username and password provided to the Provisioning Server by a deployment console that supports the Auto-Discovery feature. This newly provisioning admin account can be used for further setup and deployment from the console via WS-MAN (web services for management), via the iDRAC RACADM command line utility or via the iDRAC web graphical user interface.

Leveraging DHCP and DNS infrastructure

The Auto-Discovery feature leverages typical DHCP and/or DNS services in customer networks to locate the Provisioning Server. There are four different ways to set this up that have subtle differences:

1. The scope options on the DHCP server can specify an IP address for the deployment console. In this case, a DNS server is not needed.

2. The DNS server can specify an IP address for the default hostname. In this case, the DHCP server is needed but does not need to be configured to provide the vendor specific scope option.

3. The DHCP server can specify a hostname in the vendor specific scope options. In this case, the DNS server must resolve the specified hostname to an address.

4. The DNS must specify a service option _dellprov that specifies a hostname that can be resolved.

The iDRAC will send its vendor class identifier (DCIM.iDRAC) to the DHCP server. The DHCP server can react to this by sending a vendor specific option (option 43) for incoming DHCP REQUESTs that contain this option. The format for its content is hostname(ipaddress):port. It is also possible to specify multiple Provisioning Server in the vendor specific option, and they will be tried in order by the iDRAC. If option 43 is not found by the iDRAC, it will attempt to find the deployment console Provisioning Server by using the DNS server.

Provisioning Server integration with Deployment Consoles

After the iDRAC determines the IP address of the deployment console Provisioning Server, it is ready to perform the final handshake step in the Auto-Discovery process. It will make a web service call using SOAP (simple object access protocol) to the Provisioning Server. This call is made over a secure connection using TLS (Transport Layer Security). By using TLS, it is possible for the deployment console Provisioning Server to authenticate the iDRAC and for the iDRAC to authenticate the Provisioning Service.

Following the successful TLS connection, a web service call is made from the Provisioning Server to the deployment console where the input parameter is the server service tag and the output parameters which are returned to the iDRAC are the username and password that the iDRAC will configure for subsequent remote access via web services or existing remote IPMI, CLI, and HTML GUI interfaces. The deployment console can optionally check the service tag against a pre-approved list of service tags that are authorized to be provisioned. At this point in the process, the deployment console knows which service tags have come online.

Factory Customization available for Auto-Discovery

Auto-discovery provides a secure mechanism for zero touch provisioning of a server when it is connected to a customer network on power up. Dell servers can be ordered with the Auto-Discovery feature enabled from the factory. With Lifecycle Controller 1.3, the Custom Factory Install (CFI) process can be used to install customer provided encryption certificates for the Auto-Discovery feature. Both the Auto-Discovery client private certificate and the Provisioning Server public certificate can be custom installed at the factory. Additionally, one or more Names and/or IP Addresses of the customer Provisioning Server can be specified using the CFI process and configured when the server is built. Prespecifying the Provisioing Server(s) in the factory can eliminate the need to utilize DHCP or DNS services for Auto-Discovery in networks where IP addresses are statically assigned.

OS Deployment using Lifecycle Controller

Using Embedded OS Drivers

The Lifecycle Controller 1.0 release introduced the feature of having all platform related drivers for all supported OS's embedded in the platform and accessible via the local Unified Server Configurator console. Having the drivers embedded on the system and exposing of the drivers locally builds the foundation for removing the need for traditional driver maintenance done manually, both locally and at 1 to many deployment consoles. Lifecycle Controller remote services introduces the ability to remotely select and expose embedded drivers needed for OS deployment.

Exposing Drivers via Local Media

Traditionally drivers are collected, stored and managed at the console so that the drivers can be downloaded to the system in just the right format, at the right time, to feed the right tool to do an OS deployment. Drivers that are embedded on the system and web services interfaces providing the logic to expose the drivers as needed removes the complicated and time consuming driver maintenance. With drivers appropriate for the system being embedded on the system, worry about driver conflicts or having to group drivers to work around conflict situations is eliminated.

Exposing appropriate drivers as local media is done by invoking a web services request that causes the Lifecycle Controller to expose drivers for a specified OS version as a local USB device of a specified type (e.g. floppy, CDROM, or flash drive). The request includes specifying how long the drivers are made available to the local system (default is 5 hours, maximum of 17 hours) and another request is available to stop the driver exposure when the deployment is done.

Uploading Drivers to Deployment Console Repositories

Another task that can be time consuming and tricky to accomplish is the acquiring, preparing and inserting of appropriate drivers into OS deployment console and application repositories. Having the correct drivers for all the OS's and components supported for the platform, already collected and available from the platform is a first step in simplifying repository maintenance. The 1.2 Lifecycle Controller firmware adds a web services interface that supports a request to upload drivers for a specified OS and OS version to a specified NFS or CIFS share. It also adds a web services request for a list of all OS and OS versions for which there are embedded drivers available.

Securely Booting ISO Images From Network Shares

Platform provisioning involves configuring the platform hardware in preparation for installing and OS and then performing the OS install. Traditionally, one of the more pervasive ways of provisioning a platform remotely is by using PXE (Pre Execution Environment)protocols and booting into a pre OS (a deployment OS that contains hardware configuration utilities and scripts and the initiation of a production OS install) to initiate and carryout the deployment process. PXE is considered by many to be a non secure protocol/environment and most data centers do not allow it, thus forcing the administrator to create a separate staging environment for utilizing PXE. This staging environment is used to bring a new system in to boot PXE and cause the deployment OS to install a production OS. Sometimes the installed OS is not the final production OS, it is an intermediate step allowing the system to be moved into the production environment so it can be managed securely and then installed with its final production OS.

By providing more secure way to boot a to pre OS or deployment OS image, Lifecycle Controller allows the administrator to put the system directly into the datacenter, bypassing the temporary staging environment all together and enabling a reduction in time, money and resources. The following methodology for secure pre OS image boot is supported in Lifecycle Controller 1.2:

- The administrator will create or select an ISO image of a pre OS/deployment OS to be booted on the platform
- A hash using currently available hashing technologies can be computed for the ISO image
- The administrator will share the ISO image via a network sharing technology such as NFS or CIFS
- A web services request to boot to an ISO image is sent to the Lifecycle Controller specifying the network location or URI for the ISO image, any credentials needed to access the share, the ISO hash and hash type

The boot from network ISO web services request can be invoked by scripting from an OS CLI or integrated with deployment applications and consoles via WS-Management protocol.

Deploying ISO Images using vFlash

The Dell vFlash SD card can be used to locally stage and boot to an ISO image. The OS Deployment using vFlash feature available in Lifecycle Controller 1.3 can be performed using the WS-Man interface. Previous versions of Lifecycle Controller only used images stored in a network share for OS Deployment activities. This new feature supports the downloading and staging of bootable ISO images onto the local vFlash SD card OS Deployment partition.

The downloaded ISO image size can be up to the available space in the vFlash SD card. Security enhancements are in place to validate the ISO image by generating a hash on the ISO image and providing the hash and hash type when requesting the download of the ISO image from a network share.

Once downloaded the ISO image can be used to boot the system to the ISO once or the system can be configured to boot to the vFlash ISO permanently. The ISO image on the vFlash SD card can be explicitly deleted or overwritten with another ISO image using WS-Man. The vFlash SD Card can be enabled and initialized using the iDRAC6 web GUI.

vFlash Licensing

Several Lifecycle Controller features are enabled using a licensing mechanism that requires the presence of the Dell vFlash SD Card in the iDRAC6 Enterprise SD Card slot. The Dell vFlash SD card can be ordered along with Dell servers or separately. The licensed features include:

- Part Replacement – Available through USC and WS-MAN
- OS Deployment using vFlash – Available through WS-MAN only
- Choice of different vFlash based Virtual Flash Partition sizes – Available through iDRAC web GUI only

In Lifecycle Controller 1.3, vFlash supports two partitions, one as the Virtual Flash Partition available for use as a local USB device through a host operating system and the other as the OS Deployment partition used for staging a bootable ISO image.

Remote Firmware Inventory and Updates

The Lifecycle Controller 1.3 release features instant firmware inventory of installed BIOS, firmware, drivers, and related embedded software. Instant firmware inventory can be requested independent of the power state of the system. Traditionally system inventory was performed by downloading an Inventory Collector tool to an OS and then executing it locally or remotely and gathering the results. The new Lifecycle Controller Instant FW Inventory feature enables remote collection of FW inventory from the target platform regardless of whether the target platform is running an operating system or not. The inventory is represented by a Dell extension of the industry standard Software Inventory Profile available at the Dell TechCenter wiki. (http://www.delltechcenter.com/page/DCIM.Library)

The inventory includes information about both the installed and available firmware versions. The available versions are present in the Lifecycle Controller and can be used to update or rollback the firmware currently installed on the target component.

The Software Update feature of Lifecycle Controller 1.3 release supports remote installation and update of BIOS, firmware and drivers from a console on to the target platform. Traditional update methodologies involve running an update utility locally on the system and might involve reboots between every update. The Lifecycle Controller software update feature is OS agnostic, that is, does not require an OS to be on the system and multiple updates can be applied in a single reboot request. The update packages for BIOS, firmware, and driver images can be downloaded and installed from common network file sharing technologies such as CIFS, NFS, FTP, TFTP, and HTTP.

The remote software update feature supports update installation from a URI (Uniform Resource Identifier) location or update packages available in the Lifecycle Controller.

- A web services request can be used to perform an update on a target platform using an URI. The URI specifies the location of the update package available on a network share that will be downloaded to the Lifecycle Controller for installation on the target platform.

- The Lifecycle Controller caches current and previously installed versions of BIOS, firmware and driver images. A web services request can be used to perform an update using the update packages that are already cached and available on the Lifecycle Controller.

The Lifecycle Controller 1.3 release also adds the ability to stage and schedule when updates will be performed. Using Lifecycle Controller Job Control updates can be performed immediately or can be scheduled for a later date and time. Single or multiple updates can be scheduled to be performed during maintenance time windows. The following types of system reboots can be scheduled along with the update jobs.

- Power Cycle
- Graceful Shutdown
- Graceful Shutdown with Forced Reboot
- No Reboot (update jobs are executed only if the system is externally rebooted within the maintenance time window)

Part Replacement Feature

Part Replacement is a new feature that is available as a part of Lifecycle Controller 1.3 release and is available on systems with vFlash media attached. This new feature provides the automated firmware flash on a newly replaced component, such as a PowerEdge™ RAID controller, NIC or power supply, to match that of the original part. Part Replacement is disabled by default and can be enabled if desired. . When a component is replaced and the Part Replacement feature is enabled, the actions taken by the Lifecycle Controller are displayed locally on the system monitor.

Managing Part Replacement

The Part Replacement Firmware Update setting can be configured at any time. It can be set to one of the following settings. Automatic firmware flash can be enabled or disabled using Unified Server Configurator Lifecycle Controller enabled

- Disable: The feature is disabled by default. Firmware update on replaced parts will not be performed. Disabling this setting will require manual configuration of replaced parts.
- Allow version upgrade only: Firmware update on replaced parts will only be performed if the firmware version of the new part is lower than the original part.

- Use current firmware version on new part: Firmware on the new part will be updated to the version of the original part.

Collecting System Inventory

The Lifecycle Controller performs an inventory and collects the configuration information for all hardware on every system restart, when the Collect System Inventory On Restart (CSIOR) setting is enabled. Additionally, the system inventory collection capability detects hardware changes and, if Part Replacement Firmware Update Setting is enabled, the Lifecycle Controller has the ability to restore an existing configuration on any newly detected hardware based on the inventory collected during the previous system restart.

The CSIOR setting is disabled by default and can be enabled locally using USC or remotely with WS-Man. It can be set to one of the following settings:

- Enable: Hardware inventory and configuration information is collected on every system restart. Collecting system inventory might affect boot time depending on the hardware present in the system.
- Disable: Hardware inventory and configuration information will not be collected on every system restart. Part replacement might not have the most up to date information when inventory collection on restart is disabled and part replacement accuracy will be impacted.

SUMMARY

Lifecycle Controller 1.2 and 1.3 offers new, unprecedented capabilities for remotely deploying and managing your Dell PowerEdge server platform. Building on Lifecycle Controller version 1.0 and 1.1 capabilities introduced with the 11th Generation PowerEdge Servers, the 1.2 and 1.3 versions leverages the embedded OS drivers and the iDRAC service processor to address several common pain points associated with platform provisioning and deployment. The focus of this release has been the new Auto-Discovery capability, the ability to boot ISO images from network shares, remotely controlled acquisition of and local exposure of OS drivers that come embedded on the platform, remote firmware inventory and updates, simplifying part replacement and innovative staging of OS Deployment images on vFlash SD card.

References

Dell Tech Center Wiki

Lifecycle Controller

Web Services Scripting

Dell CIM Extensions Library