Dell™ Lifecycle Controller
Remote Services Overview

A Dell Technical White Paper

By Jon Hass and Andy Butcher
Dell Product Group
August 2009
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>What Is Lifecycle Controller?</td>
<td>4</td>
</tr>
<tr>
<td>Lifecycle Controller 1.2 Remote Services</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Lifecycle Controller Manageability Architecture</td>
<td>5</td>
</tr>
<tr>
<td>Web Services Platform Management Interface</td>
<td>5</td>
</tr>
<tr>
<td>Using Embedded OS Drivers</td>
<td>6</td>
</tr>
<tr>
<td>Exposing Drivers via Local Media</td>
<td>6</td>
</tr>
<tr>
<td>Uploading Drivers to Deployment Console Repositories</td>
<td>6</td>
</tr>
<tr>
<td>Boot ISO Images from Network Shares</td>
<td>6</td>
</tr>
<tr>
<td>Automated Discovery and Provisioning</td>
<td>7</td>
</tr>
<tr>
<td>Ordering Auto-Discovery Enabled Systems</td>
<td>7</td>
</tr>
<tr>
<td>Leveraging DHCP and DNS Infrastructure</td>
<td>8</td>
</tr>
<tr>
<td>Security Considerations and Integration with Deployment Consoles</td>
<td>8</td>
</tr>
<tr>
<td>Summary</td>
<td>9</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

What is Lifecycle Controller?

The Lifecycle Controller is the engine for advanced embedded management and is delivered as part of iDRAC (Integrated Dell Remote Access Controller) Express in the newest generation Dell servers. It eliminates the media-based system management tools/utilities for managing Dell systems. Users can further upgrade to iDRAC Enterprise and vFlash for other iDRAC features. vFlash allows hosting of customized and/or bootable service images via Secure Digital (SD) Card 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 pre-OS environment.
2. Remote Services – WS-Management web services interfaces for remote server provisioning and management via iDRAC. Consoles and scripts can use these interfaces for remote OS install, 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 install with drivers resident on the Lifecycle Controller.
- **FW Updates** – OS agnostic and minimizes the maintenance downtime with direct access to updates on 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.
- **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 functionality is provided by a combination of USC-Lifecycle Controller, iDRAC, and BIOS firmware.

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 using the Web services-based hardware management interface provided by the Lifecycle Controller firmware in concert with the iDRAC 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 the system service processor
- Remote activation of local exposure of embedded drivers
- Remote acquisition of embedded drivers for a selected OS
- Network-share based boot of provisioning pre-OS environments (alternative to PXE)
Also included in this release are the interface definitions, scripting guidelines and examples 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.

INTRODUCTION

This whitepaper is intended to provide a high level technical description of the new remote services features introduced in Dell Lifecycle Controller 1.2. These features are aimed at simplifying OS deployment and automating the setup and configuration of new server platforms. The following information includes a Lifecycle Controller architecture and manageability Web-service interface description. Also covered are descriptions of the remote utilization of embedded OS drivers, booting deployment OS’s from network-shared ISO images, and the automated discovery and initial configuration capabilities provided in Lifecycle Controller 1.2.

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. iDRAC relies on auxiliary power and therefore is running and available to manage the platform from the time the system is 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 the traditional server BMC (Baseboard Management Controller) capabilities. Remote management using the network for programmatic Web services, RACADM 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 (in concert with the iDRAC) managing system components such as BIOS, RAID storage, NIC and HBA 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 an implementation of many of the 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 Active Directory®. Credentials provided must be iDRAC Administrators or have Server Command Execution privileges. Web services interfaces can be utilized 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.
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 using the local Unified Server Configurator console. Having the drivers embedded on the system, and exposing the drivers locally builds the foundation to remove the need for traditional driver maintenance done manually, both locally and at one-to-many deployment consoles. Lifecycle Controller 1.2 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, and at the right time, to feed to 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 need for complicated and time consuming driver maintenance. With drivers appropriate for the system being embedded on the system, the worry about driver conflicts or having to group drivers to work around conflict situations is eliminated.

Exposing the appropriate drivers as local media is done by invoking a Web services request that causes the Lifecycle Controller to expose the drivers for a specified OS version as a local USB device of a specified type, for example floppy, CDROM, or flash drive. The request includes specifying how long the drivers should be 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 an OS deployment console and application repositories. Having the correct drivers for all the OS’s and components supported by the platform, already collected and available from the platform, is a first step in simplifying repository maintenance. The Lifecycle Controller 1.2 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 network-share. It also adds a Web services request for a list of all OS and OS versions for which there are embedded drivers available.

Boot ISO Images from Network Shares

Platform provisioning involves configuring the platform hardware in preparation for installing an 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. Most data centers do not allow it PXE booting, forcing an administrator to create separate staging environments 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, but 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 an alternative way to boot a to pre-OS or deployment OS image from CIFS and NFS network shares, 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 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 using 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, like Microsoft® Powershell, or integrated with deployment applications and consoles using the WS-Man protocol.

**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 in 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 manual local configuration of iDRAC remote access credentials, and enabling an automated methodology for a console to discover a new server that has been connected to the network and plugged into AC power. When a new server with the Auto-Discovery feature enabled is plugged in to AC power and connected to the network, the iDRAC will attempt to find a deployment console that has been integrated with the Dell Provisioning Service, announce itself, and configure iDRAC access credentials that can be used by the console for further setup and deployment.

**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 using 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 enabled 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. This manual process for enabling Auto-Discovery is available for server with iDRAC Express and USC firmware versions 1.2 or greater.

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 handshake process that follows the discovery process is for the Provisioning Service to create an admin account with a username and password provided to the Provisioning Service 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 using the WS-Man Web services protocol, 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 Service. There are four different ways to set this up that have subtle differences (see the Dell Auto-Discovery Network Setup Specification at the Dell TechCenter wiki [www.DellTechCenter.com](http://www.DellTechCenter.com) in the OpenManage Systems Management - Lifecycle Controller for step by step setup instructions):

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 identifier by sending a vendor specific option (option 43) for incoming DHCP requests that contain this identifier. The format for the vendor specific option content is hostname(ipaddress):port. It is also possible to specify multiple Provisioning Service host names or IP addresses in the vendor specific option, and they will be tried in order by the iDRAC. If option 43 is not found by iDRAC, it will attempt to find the deployment console Provisioning Service by using the DNS server.

Security Considerations and Integration with Deployment Consoles

After the iDRAC determines the IP address of the deployment console Provisioning Service, it is ready to perform the handshake step in the Auto-Discovery process. It will make a Web service call using SOAP (simple object access protocol) to the Provisioning Service. This call is made over a secure connection using TLS (Transport Layer Security). By using TLS, it is possible for the deployment console Provisioning Service 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 Service to the deployment console where the input parameter is the server service tag and the output parameters, returned to the iDRAC by the Provisioning Service, are an iDRAC admin username and password credentials. These iDRAC admin credentials are used for subsequent remote access and configuration using WS-Man Web service requests or remote IPMI, CLI, and iDRAC 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.

In Lifecycle Controller 1.2, two certificates are utilized for the mutually authenticated encrypted TLS (Transport Layer Security) connection between the Lifecycle Controller and the Provisioning Service. The iDRAC handshake client encryption 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 Service. The handshake client encryption 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 encryption certificate will be the service tag of the server.

A private certificate signed by the Dell certificate authority for the Provisioning Service in the deployment 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 TLS exchange is properly signed by the Dell certificate authority.

**SUMMARY**

Lifecycle Controller 1.2 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 version 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, and the remotely controlled acquisition of and local exposure of OS drivers that come embedded on the platform.