



# IDF2010

INTEL DEVELOPER FORUM

## Zero-Touch Platform Manageability with UEFI

Mark Doran, Senior Principal Engineer, Intel  
Anand Joshi, Senior Software Engineer, Dell  
Brian Richardson, Senior Technical Marketing Engineer, AMI

EFIS004

Sponsors of Tomorrow. 

# Agenda

- **UEFI Innovation and Value**
- **Platform Manageability through UEFI**
- **Using UEFI solutions to simplify configuration management, migration and replication**



# Agenda

- *UEFI Innovation and Value*
- Platform Manageability through UEFI
- Using UEFI solutions to simplify configuration management, migration and replication

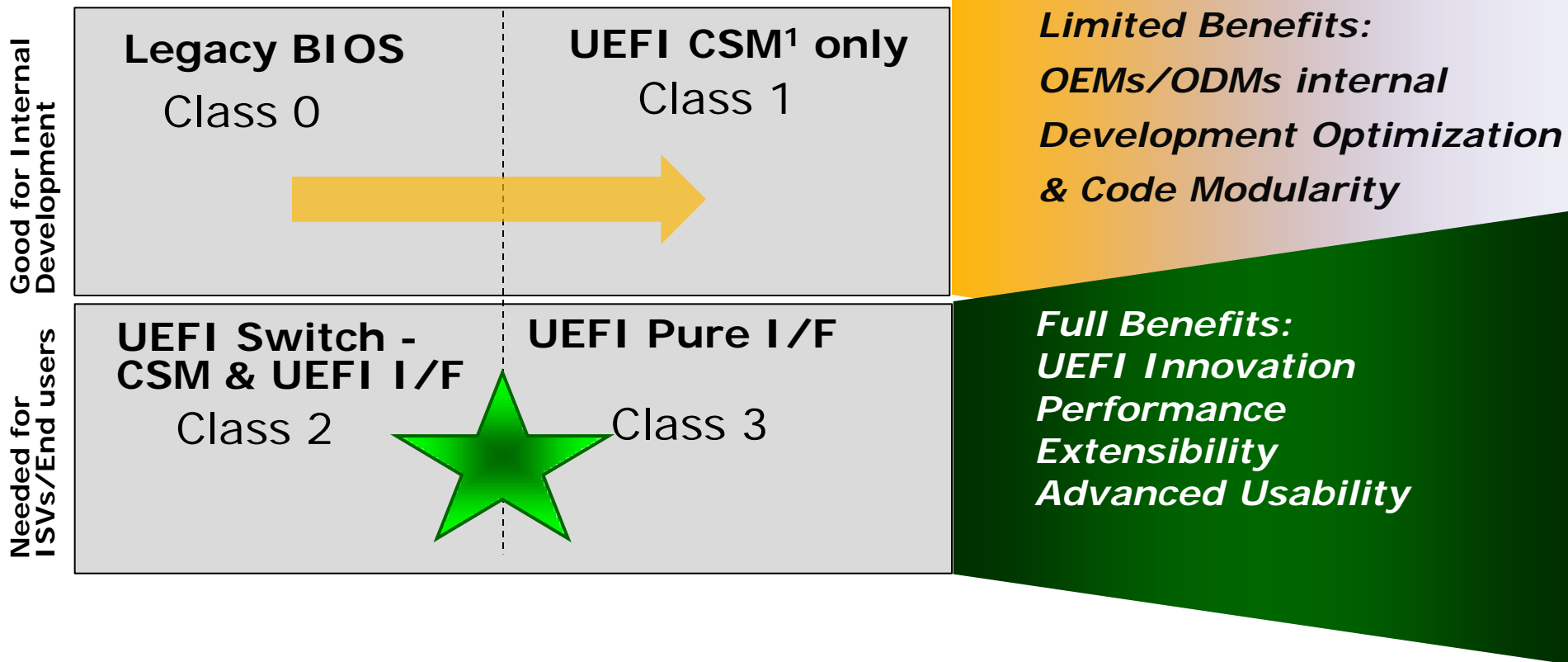




# Intel® UDK2010 enables a common firmware development foundation across the compute continuum



# Utilize UEFI Full Potential



***Build UEFI Class 2/3 UEFI Systems!***

<sup>1</sup> Compatibility Support Module – Legacy BIOS interface on top of UEFI

# Areas of Industry UEFI-based Value-add & Innovation



## Pre-OS Security & Rich Networking

- IPV6/IPSec; Authenticode signature for firmware modules; Secure updates; TPM & CRTM



## Manageability

- Enhanced Diagnostics; Intelligent & efficient platform updates; Flexible OS deployment; Consistent look & feel; Improved UI, usability and OOB mgmt capabilities



## Power Management

- Power metering, power capping, power saving



## Optimized Boot & Modern Look

- Fast boot and resume response; High resolution graphics; System boot from large drives >2.2 TB



## New Usages – UEFI Applications

- Access Outlook data in seconds when notebook is off; Pre-boot video advertisement

# Agenda

- **UEFI Innovation and Value**
- **Platform Manageability through UEFI**
- **Using UEFI solutions to simplify configuration management, migration and replication**



---

# Zero Touch Solution from

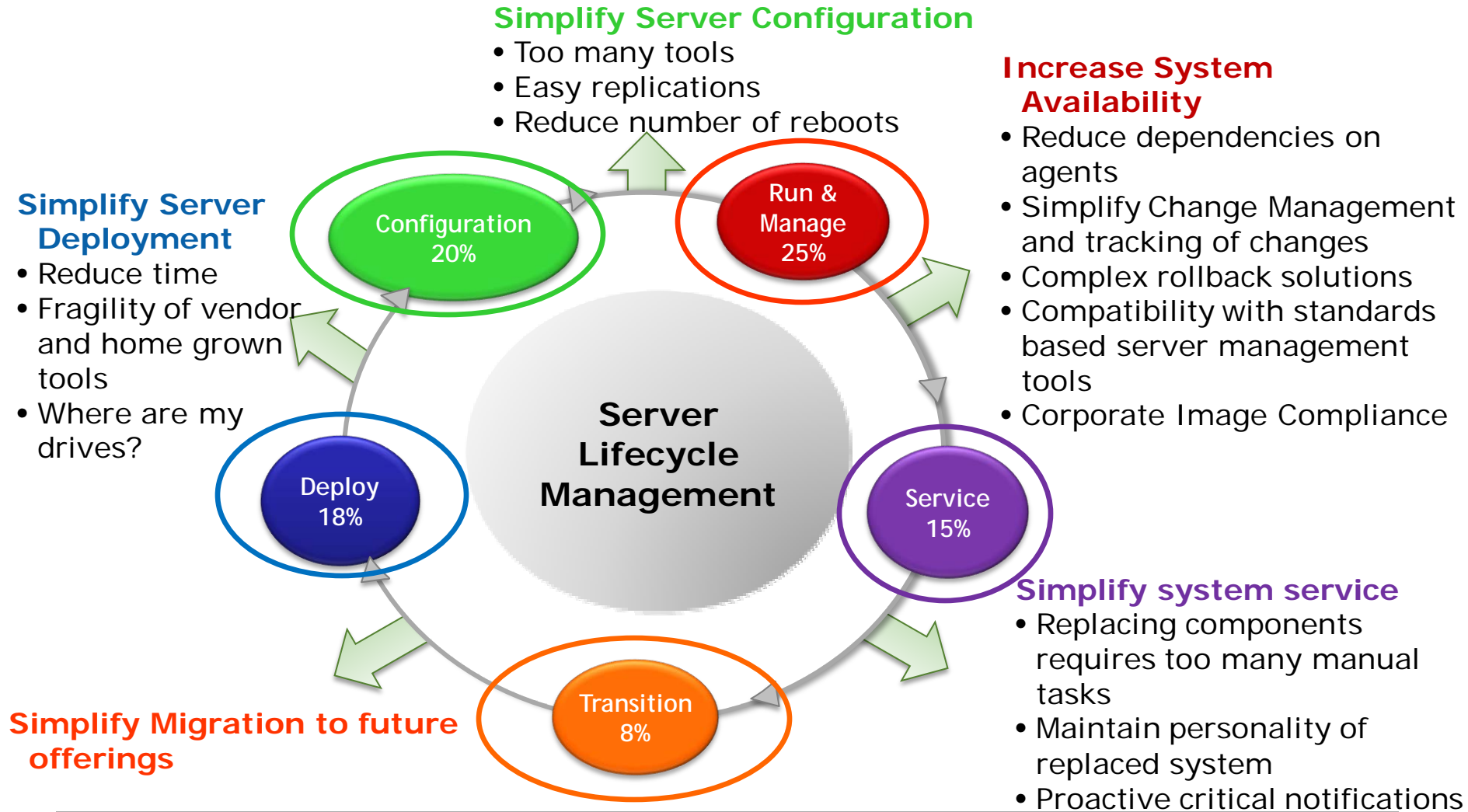
Anand Joshi  
Dell Inc.

---





# Customer Problem: Increase System and IT Efficiency



*Deployment constitutes 10% of Data center cost.*

*%cost estimates per Dell marketing survey*



# UEFI: Making it simple, making it standard

## Easier to configure and deploy

- Richer configuration (allows for more adapters)
- Graphic User Interface in Pre-boot environment
- Remote upgrade capability of specific firmware components
- Solves out of-the-box configuration & provisioning issues

## Makes Computers more manageable

- Creates a common infrastructure for managing all machines
- Enable secure automated management – lower risks of “Rogue” servers or clients on the network

## Network Scalable and Secure Firmware

- Enhanced networking APIs in the pre-boot network stack
- Richer network authentication (log-on)
- UEFI Certificate Authority for interoperable trust

## Breaks through BIOS barriers

- Free from architectural limitation - scales technology across all platforms (Server, Desktop, Mobile, and Handheld)
- Access to disk range beyond 2TB – utilization of resources
- Option Rom Decongestion

# Lifecycle Controller: Zero Touch Solution

Lifecycle Controller **powered by UEFI** simplifies the management of deploying, and updating Dell servers by embedding and automating management for increased efficiency of Dell servers and IT personnel.

Bringing the intelligence to the server by **reducing touch points** and unique OS dependent tools, increases uptime, and reduces IT costs.



# Lifecycle Controller: How UEFI helps Dell?

- **Abstraction for the Operation System**
  - Well defined API/interface between platform firmware
- **Abstraction for devices and related code**
  - Well defined driver model
  - Protocol based abstraction for range of underlying hardware devices
- **Scalable environment**
  - Protocol definition for contemporary platforms
  - Active standards body
- **Rich Pre-Boot environment**
  - Boot services and protocols through UEFI driver (device / service)
  - file system capabilities
  - Provide enhanced platform capabilities
    - › firmware update, platform configuration, diagnostics and deployment service
- **Open source**





# OS Deployment

- Makes use of pre-Boot power of UEFI
  - UEFI based GUI
  - Mouse support
  - Ability to hot plug USB
- Allows user to select the OS
- Extracts drivers from managed store and exposed as an USB key to installer
  - No need for Drivers CD

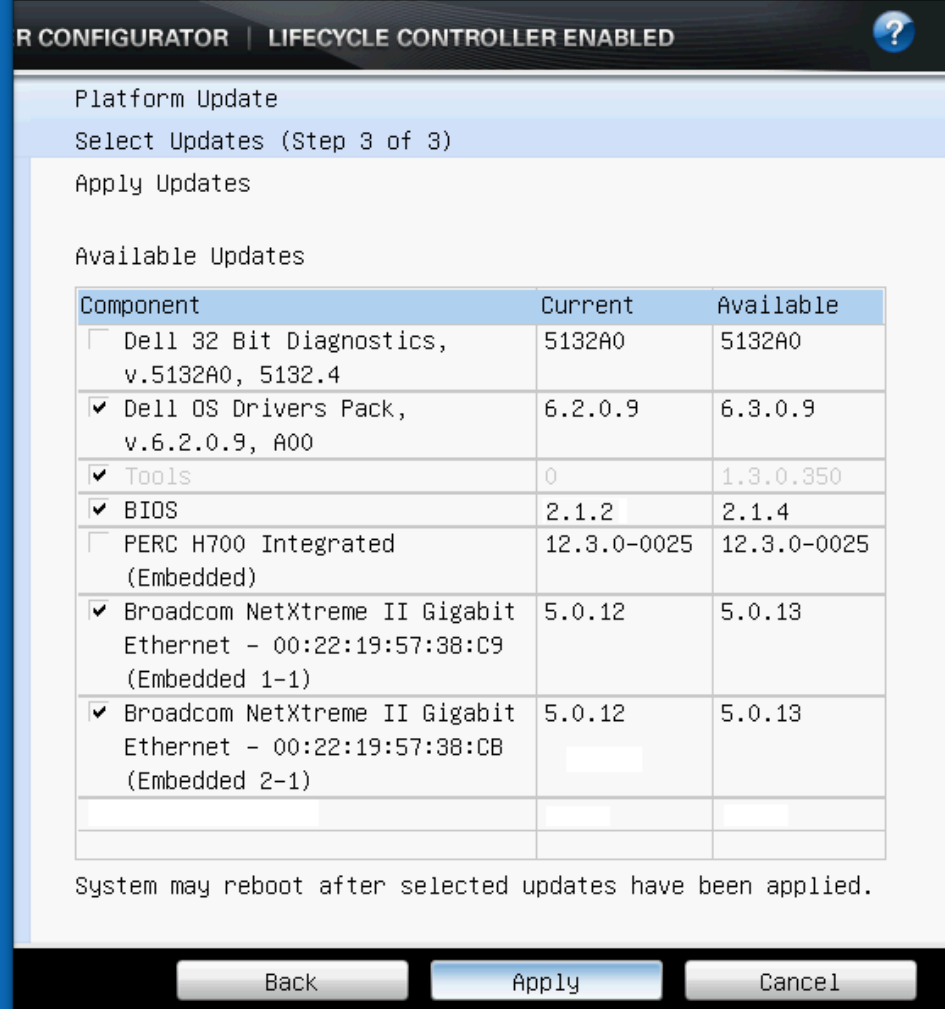
# Configuration



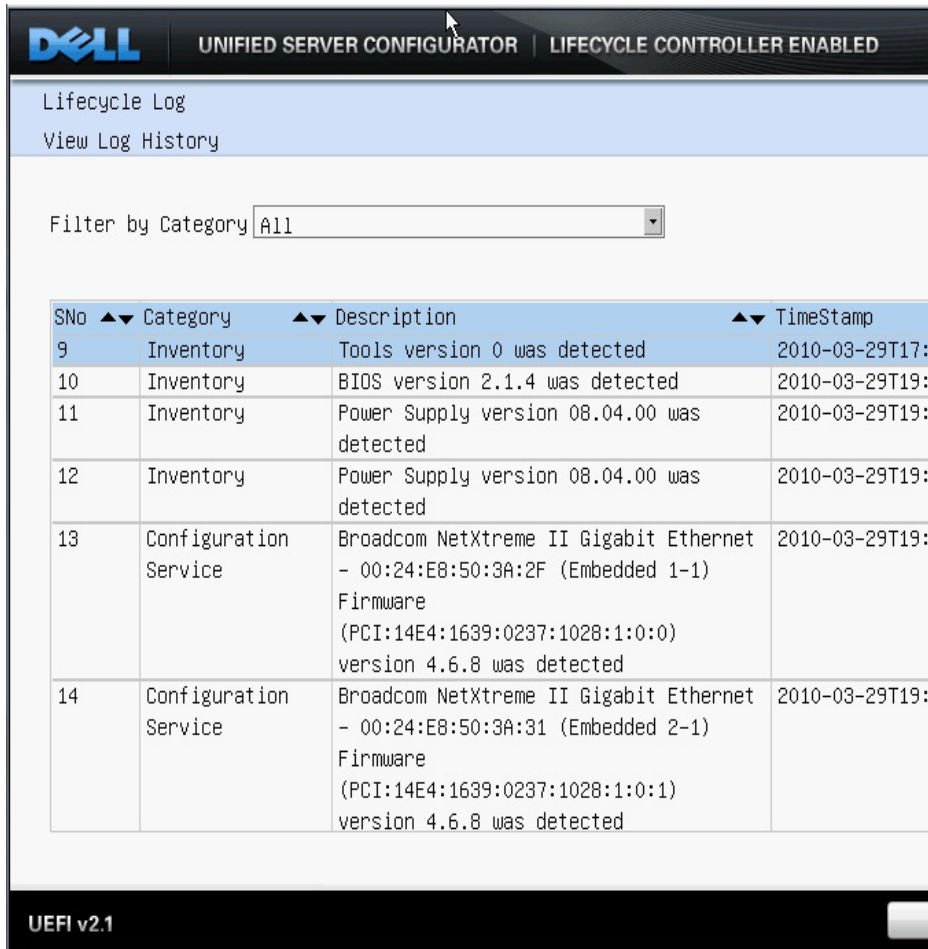
- Displays complete system configuration in single window
  - HII based configuration
  - Localization support
- Provides a unified look and feel for system configuration
  - System BIOS, NIC, Storage etc.
  - No separate configuration utilities
  - Configure all at once, reduce reboots

# Run & Manage: Firmware update

- Based on UEFI Firmware Management protocol (FMP)
- OS agnostic way of updating system firmware
  - BIOS, network and storage adaptors etc.
- Get current info using FMP
- Access the catalog over rich UEFI based network stack



# Run & Manage: System Inventory log



**DELL** UNIFIED SERVER CONFIGURATOR | LIFECYCLE CONTROLLER ENABLED

Lifecycle Log  
View Log History

Filter by Category

SNo	Category	Description	TimeStamp
9	Inventory	Tools version 0 was detected	2010-03-29T17:0
10	Inventory	BIOS version 2.1.4 was detected	2010-03-29T19:4
11	Inventory	Power Supply version 08.04.00 was detected	2010-03-29T19:4
12	Inventory	Power Supply version 08.04.00 was detected	2010-03-29T19:4
13	Configuration Service	Broadcom NetXtreme II Gigabit Ethernet - 00:24:E8:50:3A:2F (Embedded 1-1) Firmware (PCI:14E4:1639:0237:1028:1:0:0) version 4.6.8 was detected	2010-03-29T19:4
14	Configuration Service	Broadcom NetXtreme II Gigabit Ethernet - 00:24:E8:50:3A:31 (Embedded 2-1) Firmware (PCI:14E4:1639:0237:1028:1:0:1) version 4.6.8 was detected	2010-03-29T19:4

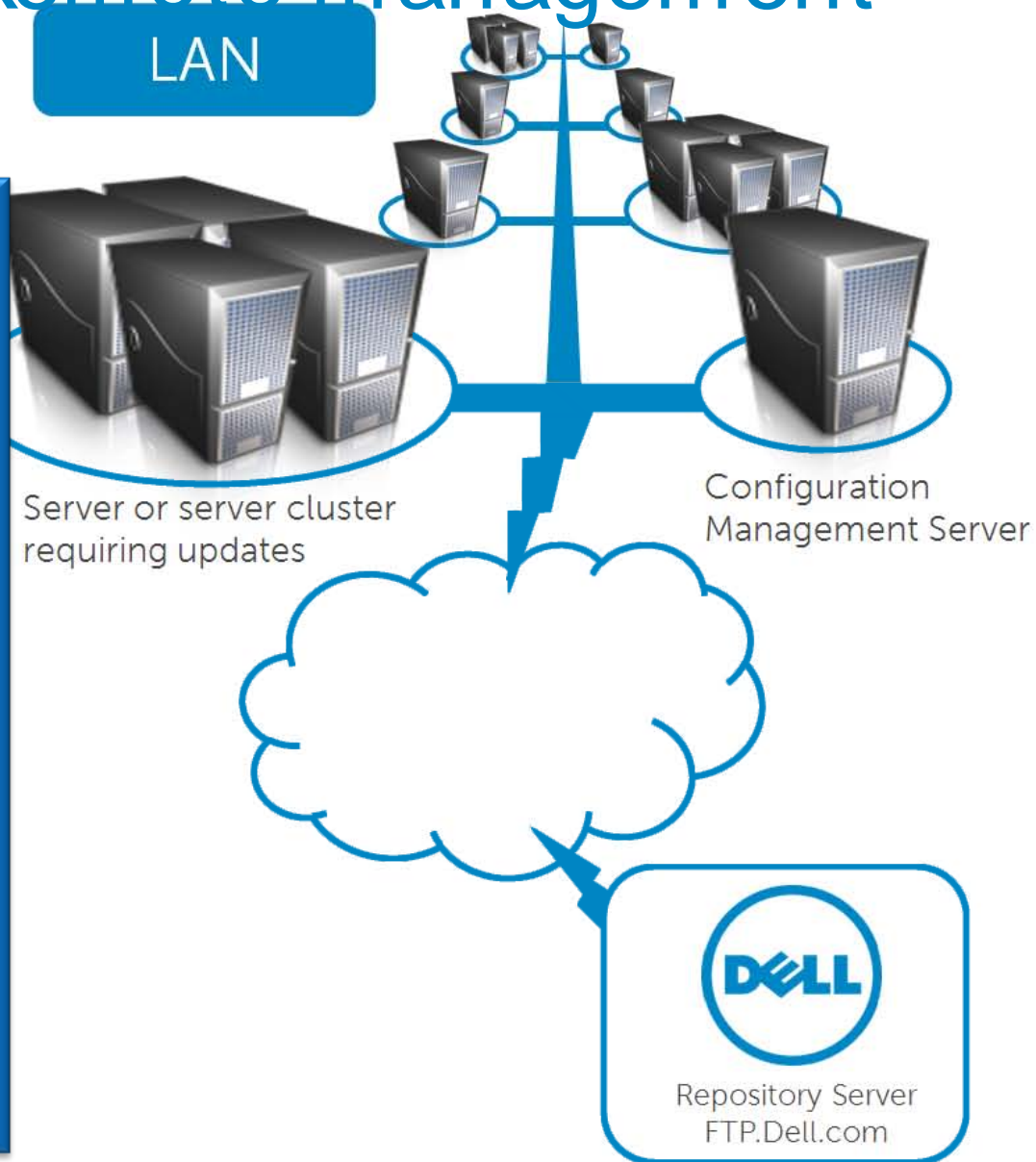
UEFI v2.1

- Collects system inventory every boot
  - Hardware
    - › Memory, PCI devices, Disks, Fan, PSU etc.
  - Firmware
    - › Firmware versions using UEFI FMP
  - Configuration
    - › HII based configuration is offlined
- Collected Inventory is logged in the managed store



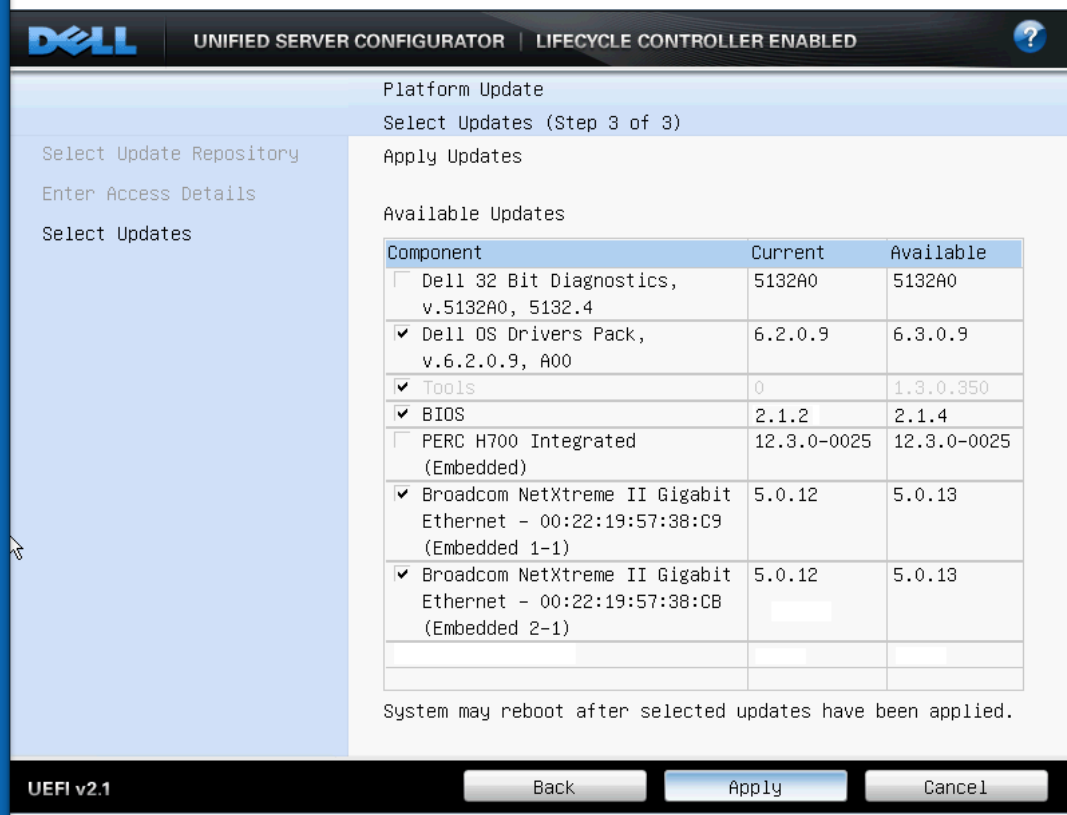
# Run & Manage: Remote management

- UEFI pre-boot drivers log Inventory and offline HII data on the managed store
- Access Lifecycle Controller through WSMAN interface provided by iDRAC
  - WSMAN Profiles
    - › SW Inventory and update
    - › BIOS configuration
- Dell Management Console use WSMAN to interact with Lifecycle Controller
- Management operations (Update, Configuration) are staged remotely and executed in UEFI pre-boot
  - OSagnostic, No OSagents
  - No need for custom tools
  - Reduce downtime, maintenance window



# Service: Part replacement

- UEFI pre-boot collects and logs inventory
  - Hardware, Firmware, Configuration
- If Inventory collector detects that a part has been replaced
  - PERC, NIC, PSU etc.
- New part gets updated to previous firmware and/or settings from Lifecycle Controller



# Summary

- UEFI enables Dell to reduce touch points in system management
- UEFI simplifies and standardizes management of deploying, and updating Dell servers
- All shipping Dell PowerEdge servers support UEFI
- More information on Lifecycle Controller  
<http://www.dell.com/embeddedservermanagement>



# Agenda

- UEFI Innovation and Value
- Platform Manageability through UEFI
- *Using UEFI solutions to simplify configuration management, migration and replication*



# Pre-Boot Solutions in UEFI

- UEFI offers the building blocks for a new generation of platform management tools
- Now to look at solutions based on UEFI ...
  - What extensions can be added to UEFI to manage the platform more effectively?
  - How can UEFI be leveraged for diagnostics?
  - What management problems can be solved across different types of platforms using UEFI?
  - How are UEFI pre-boot solutions used to solve problems on today's platforms?
- Can these solutions have parity with OS apps?
  - EDK and UEFI Shell are good starting points
  - UEFI can be further extended for developers
  - Graphic libraries for pre-boot, networking, parsing, ...

# AMI's PreBoot Extensions for UEFI

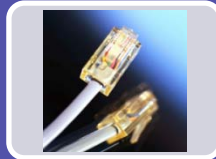
- Look at AMI's Graphical Execution Environment (GEE) as an example
- AMI GEE is a set of libraries for rapid development of UEFI pre-boot apps
  - C/C++ libraries built on UEFI specifications
  - Goes beyond UEFI shell interfaces



Graphics Driver and Menu Rendering Engine



Multi-Language Support



Networking Support



Security Infrastructure with Digital Signature Support



HII & XML Parsing Support

***UEFI applications extend and complement OS-based management tools***

# Pre-Boot Application Examples

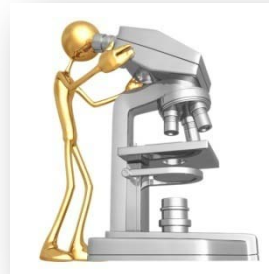
**OS-Independent  
Platform Management**

**Centralized firmware updates,  
system configuration and diagnostics**

**Manage Firmware Updates  
(local and network sources)**



**Diagnostics Operate in UEFI  
(even when OS fails to boot)**



**Graphical HII Browser  
(enhanced BIOS setup)**



**Assist OS Provisioning  
(driver discs & BIOS settings)**



# Simplify IT Management with UEFI

## Factory CD/DVD Replacements

- Always part of the system
- The disc doesn't get lost/misplaced
- Doesn't rely on a DVD drive

## Remote Management Scenarios

- Administrators access the UEFI pre-OS services installed on the remote platform
- Use Intel® vPro™ technology, IPMI BMC or other network-based access methods

## Bare Metal Provisioning

- Full platform configuration prior to OS installation (or if OS needs to be reloaded)
- Include tools to generate OS driver discs and simplify OS deployment

## Reduce Unnecessary Returns

- Launch diagnostics from UEFI even when the OS cannot start (corrupted, hacked)
- Recover or reinstall the OS from the UEFI pre-boot environment



# Using UEFI on Today's Platforms



## Configuration Management



Simplify system configuration in a centralized interface, with no dependencies on the OS (updates, diagnostics, config, ...)



## Configuration Replication



Collect common configuration parameters so the system configuration is easily cloned



## Configuration Migration



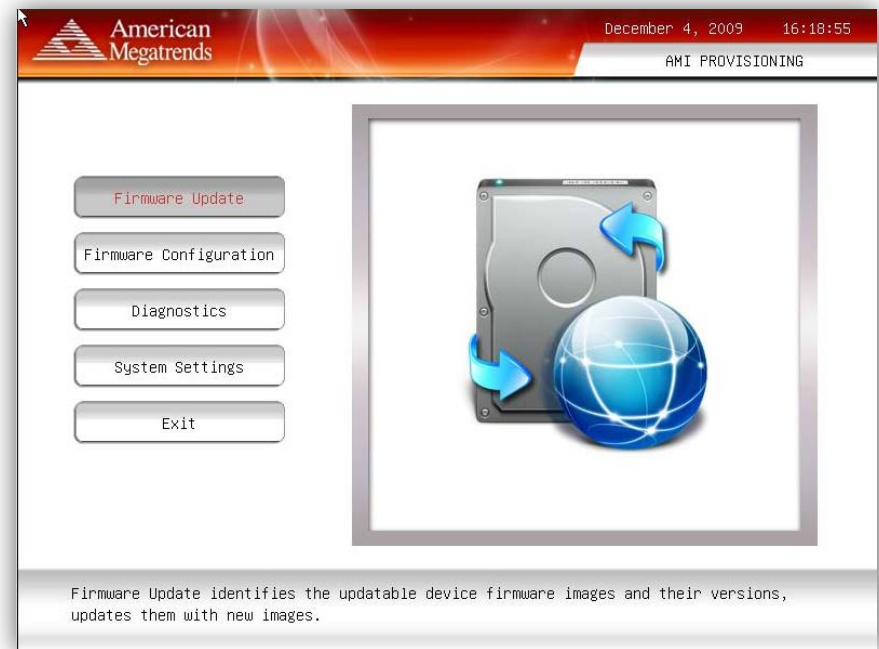
Transfer common configuration parameters across multiple systems with minimal effort

*Full configuration management  
can be performed in pre-boot  
using UEFI*

# Configuration Management

- Replace the “factory DVD” with an *always available UEFI pre-boot solution*
  - Available for local & remote platform management
- Applications like AMI Provisioning™ use AMI GEE to address the following in the pre-OS space ...
  - Platform update
  - Platform configuration
  - Platform diagnostic
  - OS installation & recovery
  - Manufacturing support

***Use UEFI pre-boot for consistent and persistent platform management***



# Replication versus Migration

**Replication:** Duplicate Configuration Across Identical Platforms



**Migration:** Apply Common Configuration To Different Platforms



**Common Goal:** seamless migration of parameters **across platforms**

- Identify and map common parameters across platforms
- Generate platform configuration scripts, load locally or via network
- Apply configuration across systems (in the field or manufacturing)

***UEFI simplifies configuration  
replication and migration***

# Management Across Platforms

- By leveraging UEFI standards, AMI GEE solutions easily scale across different hardware
  - Higher performance Intel® Xeon® servers can integrate UEFI applications with IPMI solutions
  - Desktop & mobile Intel® Core® platforms leverage Intel® vPro™ technology for remote access to UEFI pre-boot applications like AMI Provisioning
  - Embedded platforms based on Intel® Atom™ processor use UEFI pre-boot solutions for server and workstation class management on lower-cost platforms
- Complement existing management solutions using UEFI pre-boot across all product lines
  - Intel technologies add value at different price points

# Demo – Pre-Boot in UEFI



# AMI Provisioning



# Key Points from AMI

- UEFI applications extend and complement OS-based management tools
- Full configuration management can be performed in pre-boot using UEFI
- Use UEFI pre-boot for consistent and persistent platform management
- UEFI simplifies configuration replication and migration
- Use UEFI to present consistent solutions across all price points

*Complement the UEFI and UEFI Shell with robust pre-boot management solutions*

# Summary

- UEFI enables platform innovation for Modern IT  
UEFI simplifies and standardizes management of deploying, and updating Dell servers
- UEFI enables robust pre-boot management and provisioning solutions

# Additional sources of information on this topic:

- Other Sessions – Next Slide
- Demos in the showcase – #160
- Additional info in the SSG community – EFI Booth
- More web based info:
  - *UDK 2010* - <http://www.tianocore.Sourceforge.net>
  - *UEFI Specifications* - <http://www.uefi.org>
  - Lifecycle Controller  
<http://www.delltechcenter.com/page/Lifecycle+Controller>
- Book on topic:
  - Beyond BIOS 2<sup>nd</sup> edition - Intel Press

# IDF 2010 UEFI Fall Sessions

## Sept. 13, 2010 Moscone Room 2006

EFI#	Company	Description	Time
✓ S001	Intel, IBM, HP	Introducing the New Intel® UEFI Development Kit: Industry Foundation for Platform Innovation	11:00 AM
✓ S002	Intel, LSI, Dell, Phoenix	UEFI Advancements for Independent Hardware Vendors	1:05 PM
✓ S003	Intel, WindRiver	Boot Loader Solutions for Intel® Atom™ Processor Based Embedded Devices	2:10 PM
✓ S004	Intel, Dell, AMI	Zero-Touch Platform Manageability with UEFI	3:15 PM
S005	Intel, IBM, Insyde	Beyond DOS: The UEFI Shell – a Modern Pre-boot Application Environment	4:20 PM
Q001	All	UEFI Q & A session with all Speakers	5:25 PM

✓ DONE

# Beyond BIOS 2nd edition promotion



**2nd Edition - *Beyond BIOS* available Q4 2010**

To receive a complementary copy of the book  
Register at  
<http://www.intel.com/intelpress/register.htm>

Enter "Beyond BIOS Offer" plus the serial  
number on the back of this voucher in the  
Book Title field. Your book will be shipped to you.

Offer not valid for Intel employees. Limited time offer.

Vouchers available in session room and  
UEFI Technology Showcase booth #160



# Intel® UDK2010 Available on tianocore.org



[tianocore.org](http://tianocore.org)

Intel® UDK2010  
*Open Source*  
UEFI Development Kit

*Develop. Contribute. Advance.*

<http://www.tianocore.Sourceforge.net>

**IDF2010**  
INTEL DEVELOPER FORUM

# Session Presentations - PDFs

**The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:**

**[intel.com/go/idfsessions](http://intel.com/go/idfsessions)**

**URL is on top of Session Agenda Pages in Pocket Guide**

# **Please Fill out the Session Evaluation Form**

**Give the completed form to  
the room monitors as you  
exit!**

**Thank You for your input, we use it to  
improve future Intel Developer Forum  
events**

# Q&A



**Tweet your questions and comments to  
[@intel\\_uefi](https://twitter.com/intel_uefi)**

# Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.
- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.
- Intel, vPro, Atom, Intel Sponsors of Tomorrow. and Intel Sponsors of Tomorrow. Logo and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: <http://www.intel.com/technology/vpro>
- \*Other names and brands may be claimed as the property of others.
- Copyright ©2010 Intel Corporation.



# Risk Factors

The above statements and any others in this document that refer to plans and expectations for the second quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel's actual results, and variances from Intel's current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation's expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; customer acceptance of Intel's and competitors' products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Additionally, Intel is in the process of transitioning to its next generation of products on 32nm process technology, and there could be execution issues associated with these changes, including product defects and errata along with lower than anticipated manufacturing yields. Revenue and the gross margin percentage are affected by the timing of new Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel's response to such actions; defects or disruptions in the supply of materials or resources; and Intel's ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on changes in revenue levels; product mix and pricing; start-up costs, including costs associated with the new 32nm process technology; variations in inventory valuation, including variations related to the timing of qualifying products for sale; excess or obsolete inventory; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; the timing and execution of the manufacturing ramp and associated costs; and capacity utilization. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The majority of our non-marketable equity investment portfolio balance is concentrated in the flash memory market segment, and declines in this market segment or changes in management's plans with respect to our investment in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel's results could be affected by the timing of closing of acquisitions and divestitures. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting our ability to design our products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel's results is included in Intel's SEC filings, including the report on Form 10-Q for the quarter ended March 27, 2010.

Rev. 5/7/10