presented by

Microsoft

Windows

BitLocker Network Unlock
&
BitLocker support for Encrypted Drives

UEFI Winter Plugfest – February 21-23, 2011

Presented by Narendra Acharya (Microsoft)

Agenda

- BitLocker Network Unlock
- Windows Requirements for Network Unlock
- Validating Network Unlock

- BitLocker & Encrypted Drives
- Windows Requirements for Encrypted Drives
- Validating Encrypted Drives

- Questions

BitLocker Network Unlock

BitLocker Network Unlock

- Windows 7 BitLocker Unlock experience
  - TPM + PIN key protector which provides a high level of protection
  - Significant deployment problem for servers, which need to be serviced and restarted with no human interaction
  - Power management calls for shutting down or hibernating machine in order to save electricity, especially at night
  - Causes problems by preventing Wake-On-LAN

- Windows 8 improves BitLocker Unlock experience
  - No user prompting
  - Uses Wired network, Windows Deployment Server (WDS) & DHCP
  - BitLocker (at pre-boot) discovers its Network Unlock provider on WDS
  - Retrieves a secret from WDS
  - Automatically unlocks the OS volume using the secret & the TPM
  - Systems without wired network use TPM + PIN

Requirements for Network Unlock

- Systems with wired LAN ports and TPMs must support BitLocker Network Unlock
  - Requires full DHCP support for wired LAN during pre-boot through a UEFI DHCP driver
  - Includes support for EFI_DHCP4 and DHCP6 protocols defined in UEFI 2.3.1
    - EFI_DHCP4_PROTOCOL
    - EFI_DHCP4_SERVICE_BINDING_PROTOCOL
    - EFI_DHCP6_PROTOCOL
    - EFI_DHCP6_SERVICE_BINDING_PROTOCOL
- If implemented for Server
  - Support for both IPv4 and IPv6 required
- System.Fundamentals.Firmware.UEFIBitLocker

Validating Network Unlock

- Download the ‘Network Key Protector Test Suite’ from Microsoft Connect & Refer Instructions
- Use 3 Machines & a regular Network Switch
- Setup DHCP server - Windows Server 2008 R2 or Windows 8 Server
- Setup WDS Server - Windows 8 Server only
  - Install WDS role and BitLocker Network Unlock feature
  - Initialize WDS server – Type from Administrator CMD prompt: ‘wdsutil /Verbose /initialize-server /reminst:"c:\RemoteInstall" /standalone’
  - Add Network Unlock private certificate: Run ‘server-applycert.cmd’
  - Restart WDS Server: Run ‘net stop wdsserver’ & Run ‘net start wdsserver’
- Setup UEFI Client – Windows 8 Client
  - Setup Group Policy: Run ‘client-gp-usepin.cmd’
  - Add Network Unlock public key: Run ‘reg import RSA2048NKP_FVE_NKP.reg’
  - Turn on BitLocker with TPM+PIN (1234) & Save the Recovery Password
  - Verify ‘manage-bde –status’ output protector lists has “Network (Certificate based)”
  - Restart the machine
- If OS boots directly to Windows Logon → Network Unlock works
- If prompted for BitLocker PIN, IPv6 and IPv4 Network Unlock failed

BitLocker support for Encrypted Drives

BitLocker & Encrypted Drives

- Windows 7 BitLocker performance implications and storage support
  - Overhead during encryption, run-time, startup, etc.
  - Performance implications exacerbated on low-power PCs and Slates
  - Hardware Encrypted Drives not supported on Windows 7

- Windows 8 improves BitLocker performance and supports Encrypted Drives
  - Encrypted Drives offload processing to hardware
  - Specialized hardware reduces power use and increases battery life
  - Initial encryption time of volumes eliminated. Run time improved
  - BitLocker manages keys
  - Systems without Hardware Encrypted Drives use software based encryption

Requirements for Encrypted Drives

- Systems with Encrypted Drive must support BitLocker
  - Requires support for EFI_STORAGE_SECURITY_COMMAND_PROTOCOL defined in UEFI 2.3.1
    - IEEE 1667 TCG Silo
    - TCG OPAL v2.0
    - Single User Mode
  - Support Programmatic Tper Reset
- System.Fundamentals.Firmware.UEFIEncryptedHDD

Validating Encrypted Drives

- Correctly provision & partition using Windows 8 in-box tools like Setup / Diskmgmt.msc / Diskpart.exe
- Ensure TPM is enabled & activated (Use TPM.msc)
- “Turn on BitLocker” on the OS volume & Ensure to select “Run BitLocker system check” option on the final UI page
- Restart the machine & Type the following from an Administrator CMD prompt: ‘manage-bde -status’
- You are done if it says ‘Encryption Method: Hardware Encryption’
- If error message specifying BitLocker can’t be enabled appears after you login, then:
  - Capture the error information
  - Export the events from: Applications & Services Logs→Microsoft→Windows→BitLocker-API

Questions?

- Contact
  - BitLocker Network Unlock: dereka@microsoft.com
  - BitLocker & Encrypted Drives: ram.valliyappan@microsoft.com

Thanks for attending the UEFI Winter Plugfest 2012

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

Microsoft

Windows