# Providing Recovery Solutions using Windows Recovery Environment (Windows RE)

Mikael Nyström – TrueSec
MVP Windows Server – Setup/Deployment

# Agenda

- Background
- Windows Recovery Environment (Windows RE) Overview
- Deployment Overview
- Backup and Restore

# Background

- Unbootable systems are difficult to diagnose and repair
  - Users require extensive guidance from support
  - Support professionals often resort to trial-and-error due to limited diagnostic information available
    - Sometimes they further corrupt the system
  - Re-install is commonly suggested as remedy
    - Re-install often leads to multiple follow-up support calls
    - Users may not have the recovery media
- OEM custom recovery platforms can be difficult and costly to maintain and support

# Recovery Today

- Recovery Console
  - Not easily discoverable
  - User interface not suitable for normal users
  - Limited diagnostic and repair functionalities
  - Requires installation media in most cases
- SafeMode
  - Primarily used for systems with malfunctioning drivers, services, and configurations
  - Not guaranteed to boot if the OS itself is unbootable
  - Limited repair functionalities
- Users often choose the wrong tools to diagnose and repair due to the lack of guidance

# Windows RE Goals

- Provide automatic diagnosis and recovery for unbootable systems
  - Empower end users with the ability to automatically recover from ≥ 80% of known causes for unbootable systems
  - Minimize end-user impact when fixing unbootable systems
    - Minimal data loss, minimal downtime
  - Drive down OEM and enterprise support costs
    - Reduce number of support calls for unbootable systems
    - Provide support orgs with diagnostic results to reduce call times
- Provide a centralized platform for manual system recovery
  - A common launch point for various system recovery tools
  - Allow OEMs and enterprises to add custom diagnostic and recovery apps

# Problems Not Repaired by Startup Repair
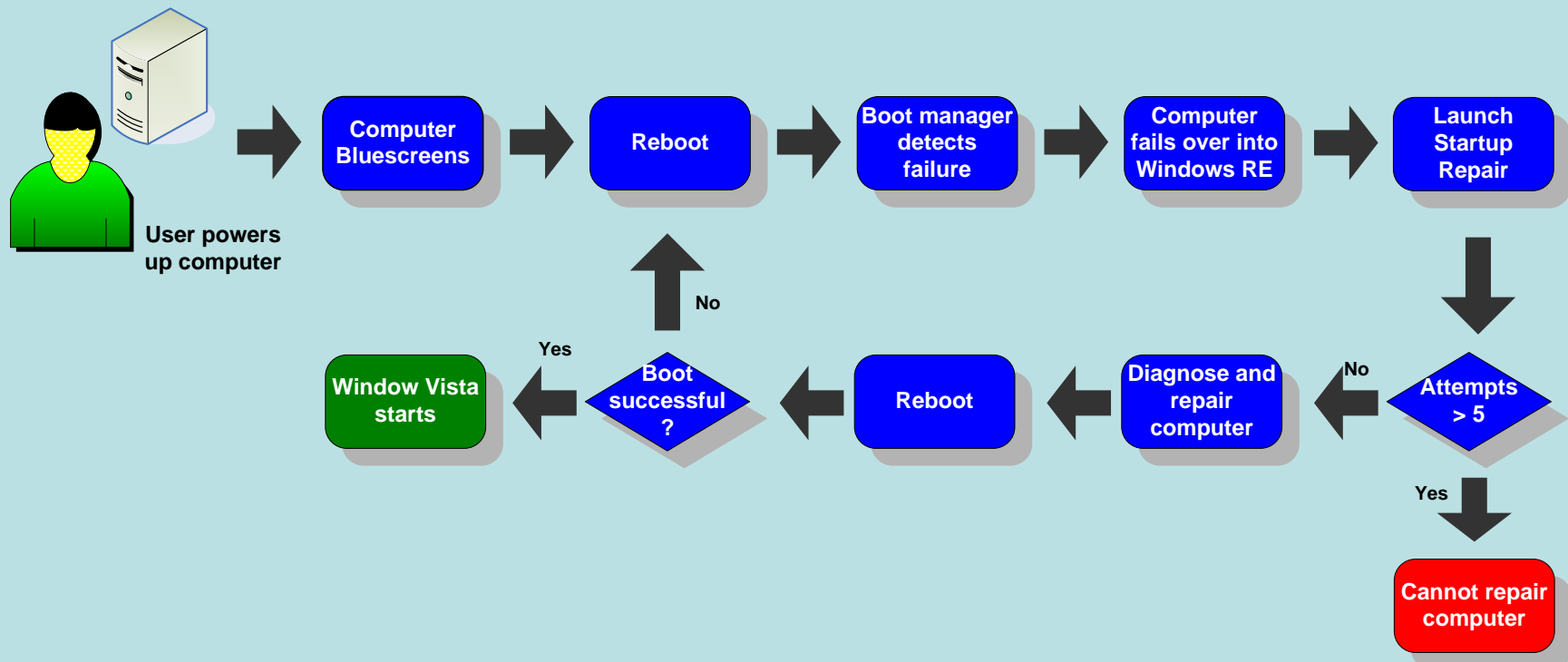
- Startup Repair will not recover unbootable systems caused by:
    - Hardware failures (e.g. firmware)
        - Can diagnose some hardware issues, but cannot repair them
    - Clean install and all OS upgrade (e.g. Windows XP to Windows Vista) related issues
    - Logon related issues
- Will recover systems but not address root cause for viruses and malicious software

# Windows RE Overview
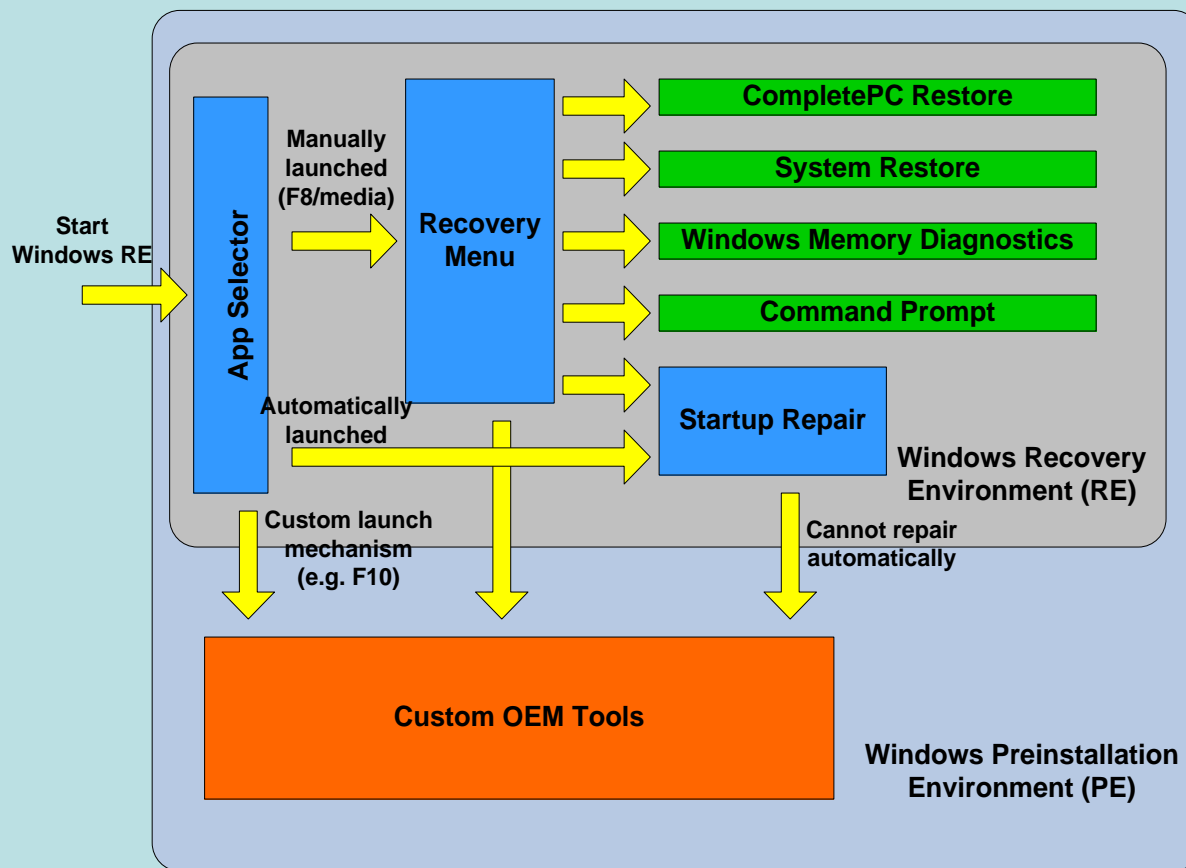


- Automatic diagnosis and recovery using Startup Repair
- Manual recovery tools available for advanced users
- Extendable with custom recovery and support tools
- Replacement for the Recovery Console

# Automated Recovery using Startup Repair

**User powers up computer**

Computer Bluescreens → Reboot → Boot manager detects failure → Computer fails over into Windows RE → Launch Startup Repair

Window Vista starts ← Boot successful? ← Reboot ← Diagnose and repair computer ← Attempts > 5

**Yes** (from Boot successful? to Reboot above)
**No** (from Boot successful? upward to Reboot)
**No** (from Attempts > 5 to Diagnose and repair computer)
**Yes** (from Attempts > 5 down to Cannot repair computer)

Cannot repair computer

- Automatically repairs at least 80% of unbootable systems due to known root causes

- Diagnoses boot failures using system instrumentation
  - New Windows Vista and Windows Longhorn Server instrumentation for driver and patch installations and boot status

- Diagnostic and repair logs available to system administrators and support professionals

# Problems Addressed by Windows RE

- Prioritized top causes for boot failures based on MS support call statistics

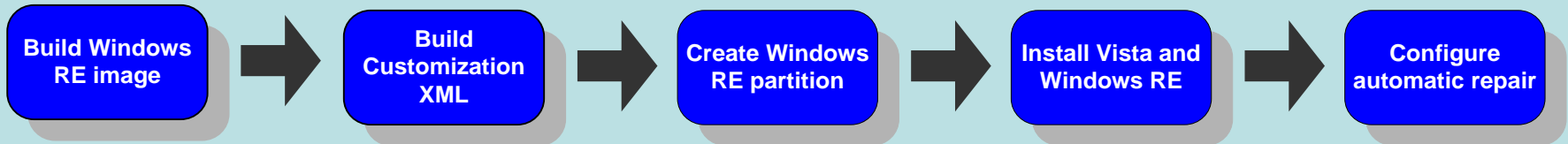| Problem | Repair Action | *Automated | Manual |
|---|---|:---:|:---:|
| Registry Corruption | • System Restore | ✓ | ✓ |
| | • Repair using backup registry | ✓ | ✓ |
| Missing or Damaged System and Driver Files | • Repair using system file cache | ✓ | ✓ |
| | • Repair using driver store | ✓ | ✓ |
| **Corrupt Disk Metadata | • Disk metadata repair | | |
| |    • MBR fix-up | ✓ | ✓ |
| |    • Partition table fix-up | ✓ | ✓ |
| |    • Boot sector fix-up | ✓ | ✓ |
| Corrupt File System Metadata | • ChkDsk | ✓ | ✓ |
| Bluescreen caused by Buggy or Incompatible Driver | • System Restore | ✓ | ✓ |
| | • Remove incompatible drivers | ✓ | ✗ |
| Incompatible Hotfix/SP Installation | • System Restore | ✓ | ✓ |
| Bad Memory Hardware | • ***Windows Memory Diagnostics | ✓ | ✓ |
| Bad Hard Drive Hardware | • ***Windows Disk Diagnostics | ✓ | ✗ |
| | • CompletePC restore | ✗ | ✓ |
| **Missing or Damaged Boot Configuration Data | • Rebuild boot configuration data | ✓ | ✓ |
| Irreparable System | • CompletePC restore | ✗ | ✓ |

*Automated repair available only in Windows Vista client SKUs through Startup Repair
**These scenarios require bootable recovery media
***Detection only; cannot repair hardware problems

# Deployment Overview

- Windows RE is deployed using OPK tools

| Build Windows RE image | → | Build Customization XML | → | Create Windows RE partition | → | Install Vista and Windows RE | → | Configure automatic repair |
|---|---|---|---|---|---|---|---|---|

- Windows PE image customizations can be used for Windows RE

- Recovery partition required for Windows RE

  - NTFS partition > 300 MB

  - If configured as a hidden partition (recommended)

    - Must be located in front of all OS and user partitions

    - Must be of type 0x27 (Cannot be marked active)

| 1 OEM (optional) | 2 Windows RE | 3 OS/Boot (active) |
|---|---|---|

- Windows RE user experience can be customized using a configuration XML file

# Windows RE Image Customization

- Add mass storage drivers
  - PEImg.exe and Drvload.exe enable injecting drivers offline into Windows PE (and Windows RE) and are available in the OPK/WAIK
  - Windows RE UI also allows users to manually add drivers
- Add language packs
  - OEMs can add language packs to Windows PE and the Windows RE optional component using PEImg.exe
  - Windows RE uses the language specified in the boot configuration data (BCD) by default
    - If not specified, user is prompted to choose a language
- Install patches
  - OEMs can install patches to the Windows RE image using PEImg.exe during the manufacturing stage

# Customization:
# OEM Front-end and Imaging/Diagnostic Tools

- OEMs can configure a custom front-end UI to launch when Windows RE is started using a custom mechanism (e.g. physical button or function key)
- Windows PE installation can be shared between Windows RE and OEM recovery tools
- OEMs can create a support or extended diagnostic tool that can be launched when Startup Repair is unable to fix the computer
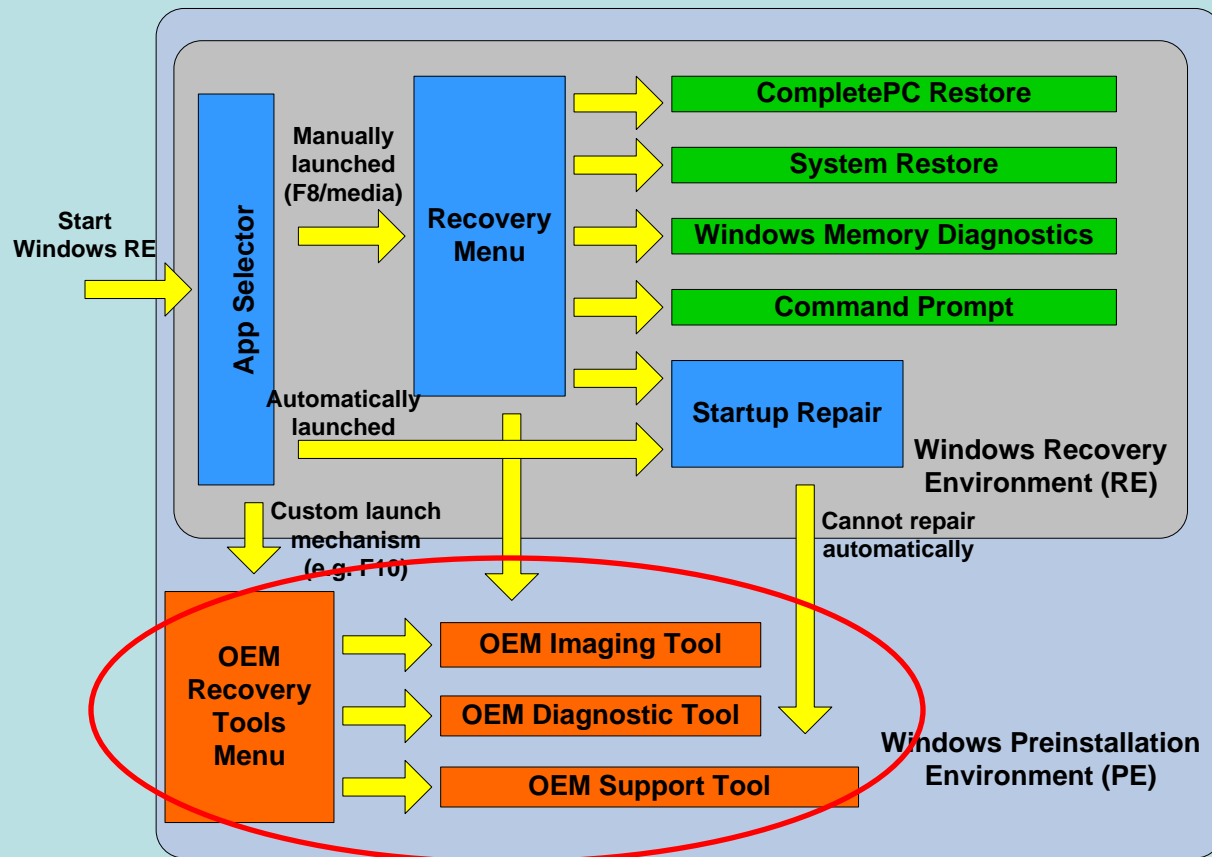
# Example: End-to-end Recovery
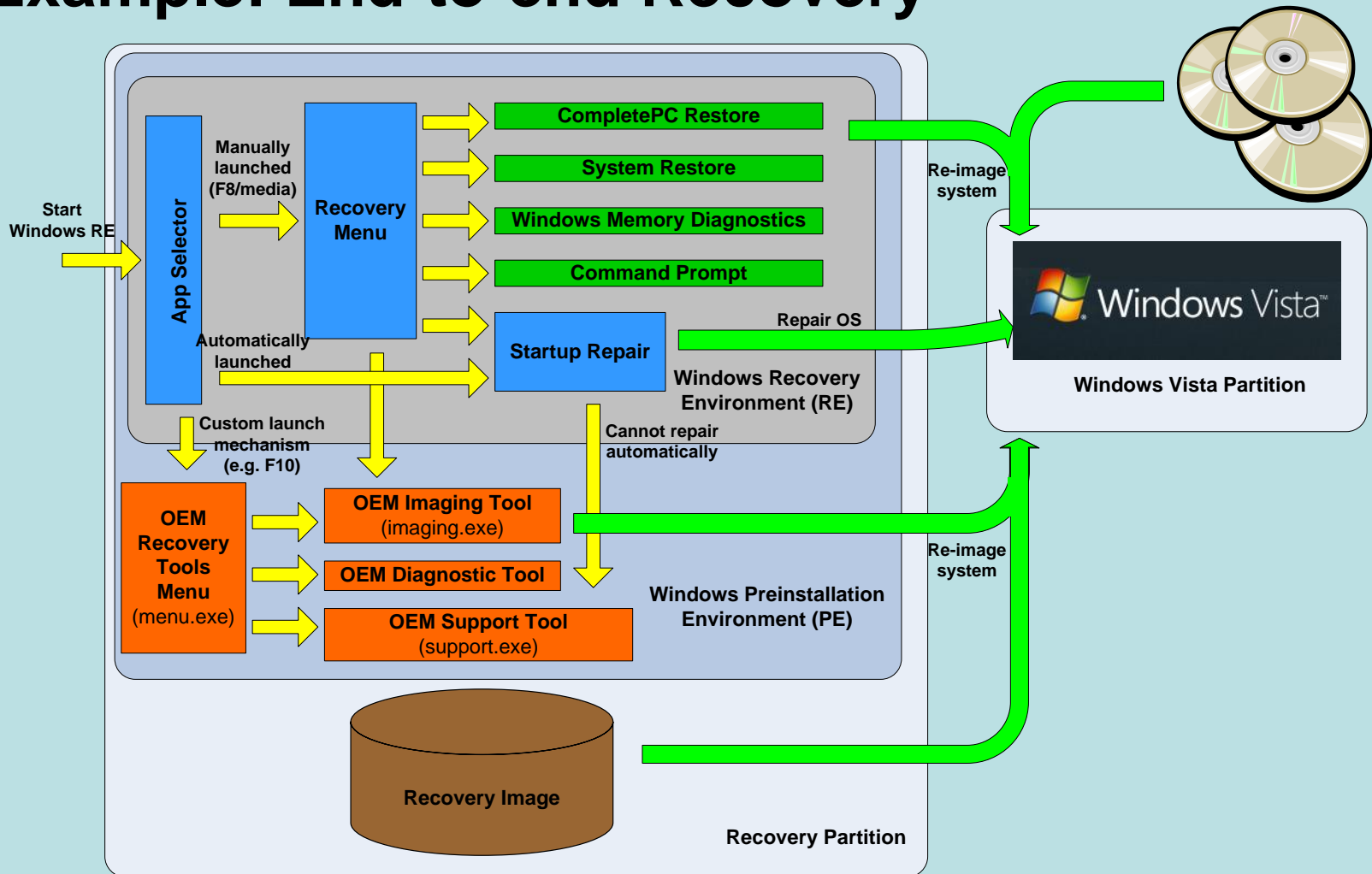


- F10 button sets Windows RE partition as active
  - App Selector (part of Windows RE) launches the OEM Recovery Tools Menu
  - Requires BIOS support and custom MBR
- Recovery image is stored on the Windows RE partition

# Backup and Restore

- OEMs can provide a custom WIM-based restore solution using wimgapi APIs
  - Suitable when factory image is also used for recovery
- CompletePC backup and restore provides users the ability to backup and restore their entire computer
  - Available in Business, Enterprise, and Ultimate SKUs
  - Block-level (64K) image of system and boot volumes, stored on hard disk or DVD (or greater)
    - Based on volume snapshot technology
    - Captures ASR information (disk layout)
    - Stored as .vhd files
  - CompletePC backups can be created in three ways
    - OEM scripted backup in factory after sysprep
    - OEM scripted backup launched after OOBE
    - User initiated backup through Windows Backup UI

# Summary

- Windows RE helps reduce support costs through automatic repair of unbootable OS installations

- OEMs can add custom recovery tools to Windows RE

- Windows RE can be used as the platform for image recovery

# Call to Action

- Preinstall Windows RE with all Windows Vista computers
  - Design custom diagnostic/recovery tools to leverage Windows RE as a recovery platform
- Use CompletePC or a WIM-based solution for system image recovery
  - Include recovery image on the Windows RE partition
- Check out Windows RE whitepaper on Microsoft Connect website
- Send feedback and questions to *recovery @microsoft.com*
- Complete your evaluation

# Questions?

Thank you.

# Appendix

# Security

- Networking turned off by default
    - Applications that require networking can turn it on dynamically
    - No inbound connection allowed through Firewall
- Authentication required if manual tools are launched from on-disk Windows RE
    - Users with no local account and guest users do not have access to the tools
    - Users with local accounts have access to GUI tools
    - Built-in administrator can access both GUI and command line tools

# Windows Disk Diagnostics

- Proactively detects impending hard disk failures
  - Uses SMART failure prediction status from the hard disk hardware
- Prompts users to back up their data before the actual failure occurs
- User experience can be configured through group policy settings

# Windows Memory Diagnostics

- In-box tool which runs in the boot environment
  - Available in Windows XP as a web download
- Diagnostic algorithms can detect the following error types
  - Memory addresses fail to retain its assigned values
  - Coupling faults
- Scheduled automatically by Startup Repair
- Windows Vista prompts users to launch the tool when a problem might be caused by failing memory
  - Determined by Microsoft Online Crash Analysis (MOCA)
- Can be launched manually from
  - Windows RE recovery menu
  - Windows Vista Control Panel

# Windows RE Partition for GPT

- For GPT systems, the hidden Windows RE partition should be configured as follows:
  - Partition GUID: {DE94BBA4-06D1-4D40-A16A-BFD50179D6AC}
  - GPT_ATTRIBUTE_PLATFORM_REQUIRED attributes are set

| 1<br>ESP | 2<br>OEM<br>(optional) | 3<br>Windows RE | 4<br>MSR | 5/6…<br>OS/Data |
|---|---|---|---|---|
| | | | | |

# Shadow copies ("snapshots")

- Turned on by default on Vista
  - Shadow copies created with every application or driver install
  - Also created with every backup
  - Otherwise, every 24 hours
- 15% of disk space set aside by default
  - Tunable via VSS APIs, sysprep/unattend
- Basis for all backup/restore functionality
- Snapshot driver is present in Windows RE, so snapshots can be mounted (and copy-on-write works)

# System Restore

- Rolls back system files and settings from a volume shadow copy (does not require backup media)

- Used to remove offending drivers and apps, revert configurations

- Does not touch user data (file/folder rules)

- Creates "restore point" when run from regular Windows

- Can also run from Windows RE to fix unbootable system (both automatic and manual)

# User data backup

- Primary backup feature for Vista

- Collects user data files (from all over the disk)

- Stages in 200 MB chunks (ZIP files) and then stored on hard disk, CD/DVD, or network share

- Intended to be configured once by user, and then runs non-interactively

  - Backup creation must be initiated manually on Home Basic version of Windows Vista

# FAQ

- What are the cases when Windows RE will be launched automatically?
  - When the system detects that the previous boot attempt did not complete, Windows RE will be launched upon reboot
- Does Startup Repair recover systems that successfully boot, but hangs afterwards?
  - No, Startup Repair will only be launched automatically if the system fails to boot, and its repair logic is tailored for boot failures only
  - Users can still launch into Windows RE to access manual recovery tools
- Does Windows RE work with Secure Startup enabled systems?
  - Yes, the user will be prompted to supply the encryption key in order to access the OS volume