ProTech

protechtraining.com

"Charting the Course ...

... to Your Success!"

Windows 2008 R2 Internals Part 2 (Custom for Wells Fargo)

Course Summary

Description

This class is a combination of lecture and hands-on exercises designed to increase the skills and understanding of experienced Windows 2008R2 Support and Admin specialists. It includes a variety of topics that should be selected by the client for maximum benefit.

Topics

- I/O System
- Memory Management
- Cache Manager
- File Systems
- Crash Dump Analysis

Audience

This course is intended for IT Professional technical specialists who work in the complex computing environment of a medium to large company and are responsible for the underlying Microsoft technologies that support a business application infrastructure in Windows Server 2008 and Windows Server 2008 R2.

Prerequisites

Up to one year of experience managing Windows Server 2008 and/or Windows Server 2008 R2 in a medium-to-large networking environment of multiple physical locations. At least two years of experience configuring and managing Windows Vista or Windows 7 clients Experience managing applications and network technologies in an enterprise environment, which may include network services and resources such as messaging, databases, file and print, a firewall, Internet access, an intranet, Public Key Infrastructure, remote access, remote desktop, virtualization, and client computer management.

Duration

20 – 40 hours depending upon client topic selections

ProTech

protechtraining.com

"Charting the Course ...

... to Your Success!"

Windows 2008 R2 Internals Part 2 (Custom for Wells Fargo)

Course Outline

I. I/O System

A. I/O System Components
   1. The I/O Manager
   2. Typical I/O Processing

B. Device Drivers
   1. Types of Device Drivers
   2. Structure of a Driver
   3. Driver Objects and Device Objects
   4. Opening Devices

C. I/O Processing
   1. Types of I/O
   2. I/O Request to a Single-Layered Driver
   3. I/O Requests to Layered Drivers
   4. I/O Cancellation
   5. I/O Completion Ports
   6. I/O Prioritization
   7. Container Notifications
   8. Driver Verifier

D. Kernel-Mode Driver Framework (KMDF)
   1. Structure and Operation of a KMDF Driver
   2. KMDF Data Model
   3. KMDF I/O Model

E. User-Mode Driver Framework (UMDF)

F. The Plug and Play (PnP) Manger
   1. Level of Plug and Play Support
   2. Driver Support for Plug and Play
   3. Driver Loading, Initialization, and Installation
   4. Driver Installation

G. The Power Manager
   1. Power manager Operation
   2. Driver Power Operation
   3. Driver and Application Control of Device Power
   4. Power Availability Requests
   5. Processor Power Management (PPM)

H. Conclusion

II. Storage Management

A. Storage Terminology

B. Disk Drivers
   1. Rotating Magnetic Disks
   2. Solid State Disks

C. Volume Management
   1. Winload
   2. Disk Class, Port, and Miniport Drivers
   3. Disk Device Objects
   4. Partition Manager

D. Volume Management
   1. Basic disks
   2. Dynamic Disks
   3. Multipartition Volume Management
   4. The volume Namespace
   5. Volume I/O Operation
   6. Virtual Disk Service

E. Virtual hard Disk Support
   1. Attaching VHDs
   2. Nested File Systems

F. BitLocker Drive Encryption
   1. Encryption keys
   2. Trusted Platform Module (TPM)
   3. Bitlocker Boot Process
   4. Bitlocker Key Recovery
   5. Full-Volume Encryption Driver
   6. BitLocker Management
   7. BitLocker to Go

G. Volume Shadow Copy Service
   1. Shadow Copies
   2. VSS Architecture
   3. VSS Operation
   4. Uses in Windows

H. Conclusion

III. Memory Management

A. Introduction to the Memory Manager
   1. Memory Manager Components
   2. Internal Synchronization
   3. Examining Memory Usage

B. Services the memory Manager Provides
   1. Large and Small Pages
   2. Reserving and Committing Pages
   3. Commit Limit
   4. Locking Memory Allocation Granularity
   5. Shared Memory and Mapped Files
   6. Protecting memory
   7. No Execute Page Protection
   8. Copy on Write
   9. Address Windowing Extensions

C. Kernel-Mode Heaps (System Memory Pools)
   1. Pool Sizes
   2. Monitoring Pool Usage
   3. Look Aside Lists

D. Heap Manager
   1. Types of Heaps
   2. Heap Manager Structure
   3. Heap Synchronization
   4. The Low Fragmentation heap
   5. Heap Security Features
   6. Heap Debugging Features
   7. Pageheap
   8. Fault tolerant Heap

Windows 2008 R2 Internals Part 2 (Custom for Wells Fargo)

Course Outline (cont'd)

E. Virtual Address Space Layouts
   1. x86 Address Space Layouts
   2. x86 System Address Space Layout
   3. x86 Session Space
   4. System Page Table Entries
   5. 64-Bit Address Space layouts
   6. x64 Virtual Addressing Limitations
   7. Dynamic System Virtual Address Space Management
   8. System Virtual Address Space Quotas
   9. User Address Space Layout

F. Address Translation
   1. X86 Virtual Address Translation
   2. Translation Look-Aside Buffer
   3. Physical Address Extension (PAE)
   4. X64 Virtual Address Translation
   5. IA64 Virtual Address Translation

G. Page Fault Handling
   1. Invalid PTEs
   2. Prototype PTEs
   3. In-paging I/O
   4. Collided page Faults
   5. Clustered Page Faults
   6. Page Files
   7. Commit charge and the System Commit Limit
   8. Commie charge and Page File Size

H. Stacks
   1. User Stacks
   2. Kernel Stacks
   3. DPC Stack

I. Virtual Address Descriptors
   1. Process VADs
   2. Rotate VAADs

J. NUMA

K. Section Objects

L. Driver Verifier

M. Page Frame Number Database
   1. Page List Dynamics
   2. Page Priority
   3. Modified Page Writer
   4. PFN Data Structures

N. Physical Memory Limits
   1. Windows Client Memory Limits

O. Working Sets
   1. Demand Paging
   2. Logical Prefetcher
   3. Placement policy
   4. Working Set Management
   5. Balance Set manager and Swapper
   6. System Working Sets
   7. Memory Notification Events

P. Proactive memory Management (SuperFetch)
   1. Components
   2. Tracing and Logging
   3. Scenarios
   4. Page Priority and Rebalancing
   5. Robust Performance
   6. ReadyBoost
   7. ReadyDrive
   8. Unified Caching
   9. Process Reflection

Q. Conclusion

IV. Cache Manager

A. Key Features of the Cache Manager
   1. Single, Centralized System Cache
   2. The Memory Manager
   3. Cache Coherency
   4. Virtual Block Caching
   5. Steam-Based Caching
   6. Recoverable File System Support

B. Cache Virtual Memory Management

C. Cache Size
   1. Cache Virtual Size
   2. Cache Working Set Size
   3. Cache Physical Size

D. Cache Data Structures
   1. Systemwide Cache Data Structures
   2. Pre-File Cache Data Structures

E. File System Interfaces
   1. Copying to and from the Cache
   2. Caching with the mapping and Pinning Interfaces
   3. Caching with the Direct memory Access Interfaces

F. Fast I/O

G. Read Ahead and Write Behind
   1. Intelligent Read-Ahead
   2. Write-Back Caching andLazy Writing
   3. Write Throttling
   4. System Threads

H. Conclusion

V. File Systems

A. Windows File System Formats
   1. CDFS
   2. UDF
   3. FAT12, FAT16, and FAT32
   4. ExFAT
   5. NTFS

Windows 2008 R2 Internals Part 2 (Custom for Wells Fargo)

Course Outline (cont'd)

B. File System Driver Architecture
   1. Local FSDs
   2. Remote FSDs
   3. File System Operation
   4. File System Filter Drivers
C. Troubleshooting File System Problems
   1. Process Monitor Basic vs. Advanced Modes
   2. Process Monitor Troubleshooting Techniques
D. Common Log File Systems
E. NTFS Design Goals and Features
   1. High-end file System Requirements
   2. Advanced Features of NTFS
F. NTFS File System Driver
G. NTFS On-Disk Structure
   1. Volumes
   2. Clusters
   3. Master File Table
   4. File Record Nmbers
   5. File Records
   6. File Names
H. Resident and Nonresident Attributes
I. Data Compression and Sparse Files
J. The Change Journal File
   1. Indexing
   2. Object Ids
   3. Quota Tracking
   4. Consolitated Security
   5. Reparse Points
   6. Transaction Support
K. NTFS Recovery Support
   1. Design
   2. Metadata Logging
   3. Recovery
   4. NTFS Bad-cluster Recovery
   5. Self-Healing
L. Encrypting File System Security
   1. Encrypting a File for the First Time
   2. The Decryption Process
   3. Backing Up Encrypted Files
   4. Copying encrypted Files
M. Conclusion

VI. Startup and Shutdown
A. Boot Process
   1. BIOS Preboot
   2. The BIOS Boot Sector and Bootmgr
   3. The UEFI Boot Process
   4. Booting from iSCSI
   5. Initializing the Kernel and Executive Subsystems
   6. Smss, Csrss, and Wininit
   7. ReadyBoot
   8. Images That Start Automatically
B. Troubleshooting boot and Startup Problems
   1. Last Known Good
   2. Safe Mode
   3. Windows Recovery Environment (WinRE)
   4. Solving Common Boot Problems
C. Shutdown
D. Conclusion

VII. Crash Dump Analysis
A. Why Does Windows Crash?
B. The Blue Screen
   1. Causes of Windows Crashes
C. Troubleshooting Crashes
D. Crash Dump Files
   1. Crash Dump Generation
E. Windows Error Reporting
F. Online Crash Analysis
G. Basic Crash Dump Analysis
   1. Notmyfault
   2. Basic Crash Dump Analysis
   3. Verbose Analysis
H. Using Crash Troubleshooting Tools
   1. Buffer Overruns, Memory Corruption, and Special Pool
   2. Code Overwrite and System Code Write Protection
I. Advanced Crash Dump Analysis
   1. Stack Trashes
   2. Hung or Unresponsive Systems
   3. When There is No Crash Dump
J. Analysis of Common Stop Codes
   1. 0xD1- DRIVER_IRQL_NOT_LESS_OR_EQUAL
   2. OX8E_- KERNEL_MODE_EXCEPTION_NOT_HANDLED
   3. OX7F- UNEXPECTED_KERNEL_MODE_TRAP
   4. OXC5- DRIVER_CORRUPTED_EXPOOL
   5. Hardware Malfunctions
K. Conclusion