Understanding Server Hardware

Module 5: Hardware Maintenance

Glenn Berry
Glenn@SQLskills.com

pluralsight
hardcore developer training

Introduction

- **The importance of hardware maintenance**
  - System vendors frequently release firmware updates
- **Knowing what has to be maintained**
  - Main BIOS, NIC firmware, RAID controller firmware, etc.
- **When are hardware-related updates needed?**
  - When they are released or when you have issues?
- **Planning and testing hardware updates**
  - Testing on identical hardware, planning maintenance windows
- **When are operating system updates needed?**
  - Released on Microsoft Patch Tuesday
- **Planning and testing operating system updates**
  - Regression testing on test servers, planning maintenance windows
- **Using rolling maintenance techniques**
  - Using server farms and other HA technologies to apply updates

The Importance of Hardware Maintenance

- **Hardware system vendors have frequent system BIOS updates**
  - Important fixes and enhancements are included in these updates
  - Staying current can help you avoid problems in the future
  - If you ever have a hardware support call with the system vendor, they will want you to be on a current version of the system BIOS
- **Hardware system vendors have frequent firmware updates**
  - RAID controllers, HBAs, NICs, and other components are updated
  - Important fixes and enhancements are included in these updates
  - Staying current can help you avoid problems in the future
  - If you ever have a hardware support call with the system vendor, they will want you to be on a current version of the firmware
- **Hardware system vendors have frequent driver updates**
  - Updated drivers will often correct problems that you have experienced

Knowing What Has to be Maintained

- **This depends on the make and model of your server**
  - It also depends on what components are installed in the server
  - Examples:
    - Main system BIOS
    - RAID controller firmware
      - Embedded RAID controller
      - PCI-E card RAID controller
    - Embedded server management firmware
    - Network interface card (NIC) firmware
      - Embedded NIC firmware
      - PCI-E card NIC firmware
    - Host bus adapter (HBA) firmware
    - PCI-E storage card firmware

When Are Hardware-Related Updates Needed?

- **This depends on the importance of the update**
  - Also depends on what issues were fixed with the update
    - Have you experienced these issues?
    - Does it seem likely that you will experience them in the future?
    - How far out of date is your firmware or drivers?
- **This also depends on your SLA for system uptime**
  - Do you have any high-availability solution in place?
    - This may let you install firmware and driver updates with less downtime
  - Do you have a stand-alone server?
    - How long does a reboot take versus how much downtime is allowed?
    - For example: Five 9s availability is just over five minutes per year

Planning and Testing Hardware Updates

- **Ideally, you have an identical test server to install all firmware and driver updates on before you do it in production**
- **If this is not possible, then another alternative is to use part of your high-availability solution for testing**
  - Examples:
    - Installing on one node of a cluster
    - Installing on one server in a server farm behind a load balancer
- **In reality, many organizations do not have a test environment**
  - This is a dangerous situation, for many reasons
  - Firmware updates are normally reliable, but there is always a risk
  - Try a scheduled maintenance window on Friday night
    - This gives you all weekend to recover from a problem

When are Operating System Updates Needed?

- **Microsoft releases important updates on Patch Tuesday**
  - Second Tuesday of the month, since October 2003
  - Security updates and other important updates are released
- **Windows Update is for the operating system only**
  - Microsoft Update also patches other applications, such as MS Office
- **For servers, you do not want automatic installation!**
  - Change to download only or notify only setting
  - It is important to test Windows Updates
    - You also want to install them during a scheduled maintenance window
- **It is a best practice to use Windows Server Update Services**
  - WSUS allows you to manage the distribution of updates
  - It also limits the download bandwidth usage for updates

Planning and Testing Operating System Updates

- **Ideally, you have a robust test environment for OS updates**
  - You also have an automated regression test suite
    - This gives you a higher degree of confidence that the OS update did not cause any issues for your applications or the servers themselves
- **In reality, many organizations have limited test environments**
  - They also may have limited testing resources
    - May be limited to “smoke-testing” and limited functional testing
    - This means more risk of breaking applications with OS updates
- **It is also common to wait a while before installing OS updates**
  - This allows other organizations to encounter problems first
  - It also gives a false sense of confidence to your organization
  - It also increases the chance that unpatched servers are vulnerable

Using Rolling Maintenance Techniques

- **This requires an HA solution or a server farm to implement**
  - This can be very effective for reducing downtime
  - This is also effective for reducing the risk of an update
- **Server farm technique:**
  - Remove one server from the farm
  - Install the desired hardware and software updates
  - Test the patched server and then add it back to the farm
  - Go to the next server in the farm and repeat
- **High availability technique:**
  - Patch one node in a cluster or one portion of the HA solution
  - Failover the node or portion of the HA solution
  - Continue until everything is patched
  - This can dramatically reduce your downtime for scheduled maintenance

Summary

- **Servers have many components that must be maintained**
  - This includes firmware and driver updates
    - Main system BIOS, ESM, RAID controllers, NICs, etc.
- **The operating system must be maintained**
  - This includes Service Packs and monthly OS updates
- **Failing to maintain your servers increases your risks of problems**
  - You are more likely to have problems with poorly-maintained servers
  - You may have vendor support issues with poorly-maintained servers
  - There is also a risk whenever you make a change to a server
- **Proper planning and testing can reduce your risks**
  - Rolling maintenance techniques can reduce your downtime
  - Regular server maintenance can force you to exercise your HA solution

What is Next?

- **Module 6 will cover servers in the real world**
  - How to justify the purchase of a new server
  - Knowing what hardware tradeoffs to make
  - Choosing hardware to minimize software license costs
  - Server consolidation
  - Hardware virtualization