More Pressure Than Ever on IT

- Technology Change
- Regulatory Compliance
- Security
- Competition
- Keep Business Up & Running
- Cost Reduction
- End User Productivity
- Customer Connection
- Business Results & New Value

IT Budgets

- 30% New
- 70% Maintenance
Microsoft’s Promises to You
Enabling IT Pros & Development Teams Across the IT Lifecycle

- Advance the Business with IT Solutions
- Amplify the Impact of Your People
- Manage Complexity, Achieve Agility
- Protect Information, Control Access

people ready
A Solid Foundation for People – Ready Software

**Server**
- **Control**
  - Manage your environment
- **Availability**
  - Maximize uptime and productivity
- **Flexibility**
  - For your changing business needs

**Client**
- **Clear**
  - User Experiences
- **Confident**
  - Safe for users, easier for IT
- **Connected**
  - To information, people, devices
Investing in the Fundamentals
A solid foundation for your business

Challenges

- **Patch Management**
  - Applying security patches is time consuming and disruptive

- **Keep System Running**
  - Too much time trying to keep things running and not enough time improving systems and adding business value

- **Security**
  - Protecting critical systems and high-valued data from unauthorized access and malicious code is job #1

Windows Server Longhorn

- **Reliability**
  - Advanced reliability enhancements to reduce loss of access, work, time, data and control

- **Performance and Scalability**
  - Scalability advancements that enable you to deploy even the most demanding infrastructure for your business

- **Security**
  - Delivers a more robust & secure computing experience for PCs and Servers
Key Development Tenets

- Security, Security, Security
- Scenario-focused Integrated innovation
- Compatibility
- Heterogeneous interoperability
- Enabling broad industry ecosystem and volume economics
- Best of breed functionality for all server workloads

Server Functions

- Operational Infrastructure
- Information Worker Infrastructure
- Application Platform
- Management
- Solutions

Workloads

- Networking
- Remote Access
- Security
- Identity Management
- Terminal Server
- Storage (file, portal)
- Print
- Email
- Collaboration
- Application/Web Server
- Unix integration services
- Database
- High Performance Computing
- Software Distribution
- Virtualization
- Operations Management
- General Purpose & Enterprise
- Medium Business
- Small Business
Do we still really need this slide? Perhaps the promises slide will work better here with an emphasis on our tenants

Ward Ralston, 5/7/2006
Security Features
Windows Service Hardening
Defense In Depth – Factoring/Profiling

- Reduce size of high risk layers
- Segment the services
- Increase # of layers

D Kernel Drivers
D User-mode Drivers
## Service Changes in Longhorn Server

<table>
<thead>
<tr>
<th>Windows XP SP2 / Server 2003 R2</th>
<th>Windows Vista / Longhorn Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account</strong></td>
<td><strong>Services</strong></td>
</tr>
<tr>
<td>LocalSystem</td>
<td>Wireless Configuration</td>
</tr>
<tr>
<td></td>
<td>System Event Notification</td>
</tr>
<tr>
<td></td>
<td>Network Connections (netman)</td>
</tr>
<tr>
<td></td>
<td>NLA</td>
</tr>
<tr>
<td></td>
<td>Rasauto</td>
</tr>
<tr>
<td></td>
<td>Shell Hardware</td>
</tr>
<tr>
<td></td>
<td>Detection</td>
</tr>
<tr>
<td></td>
<td>Themes</td>
</tr>
<tr>
<td></td>
<td>Telephony</td>
</tr>
<tr>
<td></td>
<td>Windows Audio</td>
</tr>
<tr>
<td></td>
<td>Error Reporting</td>
</tr>
<tr>
<td></td>
<td>Workstation</td>
</tr>
<tr>
<td></td>
<td>ICS</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Service</td>
<td>DNS Client</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Service</td>
<td>SSDP</td>
</tr>
<tr>
<td></td>
<td>WebClient</td>
</tr>
<tr>
<td></td>
<td>TCP/IP NetBIOS helper</td>
</tr>
<tr>
<td></td>
<td>Remote registry</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Accounts
- **LocalSystem**
  - Wireless Configuration
  - System Event Notification
  - Network Connections (netman)
  - NLA
  - Rasauto
  - Shell Hardware
  - Detection
  - Themes
  - Telephony
  - Windows Audio
  - Error Reporting
  - Workstation
  - ICS

- **Network Service**
  - DNS Client

- **Local Service**
  - SSDP
  - WebClient
  - TCP/IP NetBIOS helper
  - Remote registry

### Services
- **RemoteAccess**
  - W32time
- **TrkWks**
  - Cryptographic Services
  - Removable Storage
  - WMI Perf Adapter
  - Automatic updates
  - WMI
  - App Management
  - Secondary Logon
  - BITS

- **Network Service**
  - Network Connections
  - Shell Hardware Detection

- **Local Service**
  - System Event Notification
  - Network Connections
  - Workstation

- **PolicyAgent**
  - Nlasvc

- **6to4**
  - Task scheduler
  - RemoteAccess
  - Rasauto
  - WMI

- **Event Log**
  - WebClient
  - SSDP

- **App Management**
  - WMI Perf Adapter
  - Automatic updates
  - Secondary Logon

- **Bits**
  - Themes
  - Rasman
  - TrkWks
  - Error Reporting

- **Network Service**
  - DNS Client
  - ICS
  - DHCP Client

- **Local Service**
  - System Event Notification
  - Network Connections
  - Shell Hardware Detection

- **COM+ Event System**
  - Event Log
  - Workstation
  - Remote registry

- **Error Reporting**
  - Workstation

- **PolicyAgent**
  - Nlasvc

- **App Management**
  - WMI Perf Adapter
  - Automatic updates
  - Secondary Logon

- **Local Service**
  - TCP/IP NetBIOS helper

- **Event Log**
  - WebClient
  - SSDP
To me - this is a great slide to introduce why upgrades to Win2K are a security risk and we are not supporting....

Ward Ralston, 5/7/2006
BitLocker™ Drive Encryption

- Designed specifically to help prevent a thief who boots another Operating System or runs a hacking tool from breaking Windows file and system protections
- Secure Startup - Helps provides data protection on your Windows systems, even when the system is in unauthorized hands
- Uses a v1.2 TPM or USB flash drive for key storage
BitLocker™ Features Overview

- **Ensures Boot Process Integrity**
  - Protects the system from offline software based attacks.

- **Protects data while the system is offline**
  - Encrypts entire Windows volume including both user data and system files, the hibernation file, the page file and temporary files.

- **Force Recovery**
  - Sys-admin ONLY tool to securely speed-up PC re-deployment

- **Eases Equipment Recycling**

- **Single MS TPM driver**
  - Improved stability and security

- **TPM Base Services (TBS)**
  - Windows and 3rd party SW access to TPM

- **Scenarios:**
  - Lost or stolen laptop
  - Branch-office Server
  - Server Integrity
Code Integrity: OS File Protection

- Validates the integrity of the boot process
  - Checks kernel, HAL and boot-start drivers
  - If validation fails, image won’t load

 Validates the integrity of each binary image

- Implemented as a file system filter driver
- Checks hashes for every page as it’s loaded
- Checks any image loading to a protected process
- Hashes stored in system catalog or in X.509 certificate embedded in file
Controlling Device Installation

- Ability to block all new device installs
  - Can deploy a machine and allow no new devices to be installed
- Set exceptions based on device class or device ID
  - Allow keyboards and mice to be added, but nothing else
  - Allow specific device IDs
  - Configurable via Group Policy
  - Set at the computer level
Motivation and Focus
- Provide more efficient, scalable, high-speed, more secure and manageable networking
- Integrate new capabilities and functionality to meet customer needs
- Reduce cost of ownership
- Improve reliability and servicing

Benefits
- Improved security without need to change the user experience
- Greater reliability for a more resilient, easy to use and manage networking experience
- Better scalability to meet growing connectivity demands and maximize server resources in a cost effective manner

Next Generation TCP/IP

Security
- Reduce the risk of network security threats
- Safeguard sensitive data and intellectual property
- Full-featured, enterprise functionality

Performance
- Automatically adjusts for maximum efficiency
- Optimized performance without loss
- Cost-effectively scale networking up and out
- Adopt hardware acceleration and offloading
Complete Redesign of TCP/IP

- Dual-IP layer architecture for native IPv4 and IPv6 support
- Seamless security through expanded IPsec integration
- Improved performance via hardware acceleration
- Network auto-tuning and optimization algorithms
- Greater extensibility and reliability through rich APIs
## A Short List of New Features

<table>
<thead>
<tr>
<th>Technologies</th>
<th>Security</th>
<th>Experience</th>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Routing Compartments</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Filtering Platform (WFP)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Secure Sockets API</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TCP Chimney</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TCP-A (I/OAT)</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Receive Side Scaling (RSS)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Receive Window Auto-Tuning</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Compound-TCP (CTCP) – Congestion Control</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Wireless Reliability</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Black-Hole Router Detection (BHRD)</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Dead Gateway Detection</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Network Diagnostics Framework/Extended TCP Statistics</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy-based Quality of Service (eQoS)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Windows Firewall with Advanced Security

- Combined firewall and IPsec management
  - New management tools – Windows Firewall with Advanced Security MMC snap-in
  - Reduces conflicts and coordination overhead between technologies
- Firewall rules become more intelligent
  - Specify security requirements such as authentication and encryption
  - Specify Active Directory computer or user groups
- Outbound filtering
  - Enterprise management feature – not for consumers
- Simplified protection policy reduces management overhead
Windows Server 2003
Installing, securing, and managing server roles fragmented across multiple tools

- Windows Server 2003 Setup
- Post-Setup Security Updates
- Manage Your Server
- Configure Your Server Wizard
- Add/Remove Windows Components
- Computer Management
- Security Configuration Wizard
Longhorn Server Setup Phases

OS Setup

Initial Configuration Tasks

Server Manager
Server Manager
Provides a great, out-of-the-box experience for adding, configuring, and managing server roles

1. Out of box experience (OOBE)
   - Walks the user through the tasks necessary to complete setup and operationalize the server

2. Single experience for configuring LH Server
   - Steps the user through adding and removing server roles and features securely

3. Portal for ongoing management
   - Display server status, expose key management tasks, and guide the user to advanced management tools
Network Access Protection
How it works

1. Client requests access to network and presents current health state
2. DHCP, VPN or Switch/Router relays health status to Microsoft Network Policy Server (RADIUS)
3. Network Policy Server (NPS) validates against IT-defined health policy
   If not policy compliant, client is put in a restricted VLAN and given access to fix up resources to download patches, configurations, signatures (Repeat 1 - 4)
4. If policy compliant, client is granted full access to corporate network
## NAP - Enforcement Options

<table>
<thead>
<tr>
<th>Enforcement</th>
<th>Healthy Client</th>
<th>Unhealthy Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Full IP address given, full access</td>
<td>Restricted set of routes</td>
</tr>
<tr>
<td>VPN (MS and 3rd Party)</td>
<td>Full access</td>
<td>Restricted VLAN</td>
</tr>
<tr>
<td>802.1X</td>
<td>Full access</td>
<td>Restricted VLAN</td>
</tr>
<tr>
<td>IPsec</td>
<td>Can communicate with any trusted peer</td>
<td>Healthy peers reject connection requests from unhealthy systems</td>
</tr>
<tr>
<td></td>
<td>• Complements layer 2 protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Works with existing servers and infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Flexible isolation</td>
<td></td>
</tr>
</tbody>
</table>
## NAP Benefits

<table>
<thead>
<tr>
<th>Support</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in client</td>
<td>• No need to deploy/license 3&lt;sup&gt;rd&lt;/sup&gt; party client</td>
</tr>
<tr>
<td></td>
<td>• Updates via WUS / WSUS / SMS</td>
</tr>
<tr>
<td>Flexible enforcement</td>
<td>• Works with today’s &amp; tomorrow’s networks</td>
</tr>
<tr>
<td></td>
<td>• Enables risk-benefit trade offs</td>
</tr>
<tr>
<td>3&lt;sup&gt;rd&lt;/sup&gt; party enforcement</td>
<td>Customers can use any network or security infrastructure vendor</td>
</tr>
<tr>
<td>Health assessment</td>
<td>• Seamless integration with Windows infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Works with any AV, patch or endpoint security solution</td>
</tr>
<tr>
<td>User experience</td>
<td>Polished look and feel tailored for the customer environment</td>
</tr>
<tr>
<td>Management</td>
<td>Complete policy based administration and operation</td>
</tr>
</tbody>
</table>

- Support: Windows Vista, XP
- Flexible enforcement: DHCP, VPN, 802.1x, Terminal Services, Server and Domain isolation
- 3<sup>rd</sup> party enforcement: All major switch / router / firewall / VPN
- Health assessment: SMS, WUS, SecurityCenter, 3<sup>rd</sup> party
Demo

Role: Win2k3 DC, CA issuing Health Certs
Host name: Microsoft-9emzvu.napdemo.com
IP: 10.0.0.1
Subnet Mask: 255.0.0.0

Legend
- IPSec Policy
- Filter List: Secure Policy
- Filter: Vy IP <= 10.0.0.13 (mirrored)
- Description: ESP/NULL between NAP client and Secure Server
- Filter Action: *IPSEC - Secure Required Mode
- Security Method Preference Order: ESP-nullSHA1
- DONT Accept unsecured communications
- DONT Allow unsecured communication with non-IPsec-aware hosts
- Authentication: Certificate
- Tunnel: No.
- Connection Type: ALL

Role: Vista NAP Client (5270)
Host name: VistaCTP5270.napdemo.com
IP: 10.0.0.111
Subnet mask: 255.0.0.0

IPsec ESP/NULL Traffic

Server Isolation Zone

Role: Win2k3 Secure Web Server
Host name: SecureServer.napdemo.com
IP: 10.0.0.13
Subnet Mask: 255.0.0.0

IPsec ESP/NULL Traffic

Role: LH RADIUS and HRA Server (5270)
Host name: RADIUS55270.napdemo.com
IP: 10.0.0.6
Subnet Mask: 255.0.0.0

Boundary Zone

NAP Demo VLAN
Investing in the Fundamentals

Security
- Threat modeling, tools, testing and code review
- Secure startup with BitLocker drive encryption
- Service hardening and user access control

Reliability
- Hot-pluggable subsystems and self-healing file system
- Server core and composite roles require fewer reboots
- Restart manager and restartable Active Directory

Performance
- Redesigned TCP/IP stack for better bandwidth use
- Optimized virtualization platform
- Support for 64x64-bit cores and 1TB RAM
Goals
- Common Services
- Common Experiences
- Integrated Innovations

3 Step Process
- Gather requirements, prioritize and create specifications
- Review products at three milestones – product definition, beta, and RTM
  - Product release - Go/No Go Decision
- Publish report for reviewed products at public beta

External Publication of Report
- Transparency
- Predictability
Read-only DC value proposition

- Attack surface has been reduced for DCs in physically unsecured locations
  - Impact of stolen DC to the Active Directory reduced
    - By default, no users\computers passwords stored on RODC
  - Attack surface to the Active Directory for a compromised DC has been reduced
    - Read-only state
    - Unidirectional replication for AD and FRS\DFSR
    - Each RODC has its own KDC KrbTGT account
    - Very limited rights to write in Directory
    - RODCs are workstation accounts, no EDC or DDC group membership

- Easier management and configuration of DCs in branch offices
  - Most AD branch office guide recommendations enabled by default
Read-only DC

Demo: How RODC mitigates “stolen DC”

Attacker perspective

Hub Admin perspective
RODC deployment prerequisites

Summary: Works in existing environments!!!

- No patching to down-level DCs or clients needed
  - No domain restructuring
    - May be able to consolidate bridgehead servers
- Incremental Requirements
  - Must be in Win2003 Forest Functional Mode
    - Linked value replication reduces lost updates
    - RODCs require constrained delegation
  - PDC FSMO must be running Longhorn
    - To ensure uniqueness of RODC Kerberos TGT accounts
    - PDC FSMO understands RODC accounts for secure channel
  - Recommend multiple LH DCs per domain
    - To load balance RODC replication
  - 1 RODC per domain per site supported
    - Writeable LH DC and RODC can coexist
    - RODCs from different domains can coexist
Admin Role Separation:

Overview

Problem:
- Customers have too many Domain Admins
  - Most of these DAs are really server admins (patch management, etc)

Solution:
- Provides a new “local administrator” level of access per RODC
  - Also includes all Builtin groups (Backup Operators, etc)
- Prevents accidental AD modifications by machine administrators
- Does not prevent “local administrator” from maliciously modifying the local DB
What is Server Core?

- Part of the “Windows Server” SKU, available as an install option
- Delivers the core set of server OS functionality
- Can boot and operate stand-alone in headless/embedded scenarios
- Part of an overall Windows/LH Server infrastructure solution
Tying it all together

- Server Core + Restartable AD
  - Reduced reboots for servicing

- Server Core + RODC + Admin Role
  - The ultimate secure appliance domain controller
  - Separation
Authentication Enhancements

- **New logon architecture**
  - GINA (the old Windows logon model) is gone.
  - Third parties can add biometrics, one-time password tokens, and other authentication methods to Windows with much less coding.

- **Easier Smart Card Deployments**
  - Drivers and Certificate Service Provider (CSP) included in Windows Vista and Windows Update.
  - Login and credential prompts for User Account Control all support Smart Cards.
Credential Providers

Technology Introduction

- Credential Providers replace GINA
- Credential Providers plug in to Logon UI
  - Logon UI can interact simultaneously with multiple credential providers
  - Credential Providers can be user selected and/or event driven
- Inbox Credential Providers
  - Password
  - Smart Card
- What Credential Providers cannot do
  - Replace the UI for the logon screen
Credential Providers

Value Proposition

- Easier to write a Credential Provider than it was to write a GINA
  - LogonUI and CredUI provide all UI
  - Winlogon handles LSALogonUser and Terminal Services support
  - Credential providers simply define credentials and use LogonUI to gather the data
  - Uses COM to interact with LogonUI and CredUI
Other Security Features
Revised/Improved

- ADFS
- PKI Improvements
- Indigo-Common Development Platform
- Claims aware applications
- Web SSO
- RMS 2.0
- Group Policy