Integrating Management and Security at Microsoft – Forefront Endpoint Protection 2010 Deployment Case Study at Microsoft

Shitanshu Verma
Lead–Operations Engineering
Microsoft Corporation

Partha Chandran
Senior Service Engineer
Microsoft Corporation
Session Objectives and Takeaways

- Forefront Endpoint Protection Solution at Microsoft IT
  - Components
  - Architecture
  - Deployment strategy
- Configuration Manager After FEP
- Benefits of Forefront Endpoint Protection Integration
- Best Practices
Who is MPSD?

280,000  Clients Managed at Microsoft
7,800  Clients Managed at Energizer
5,300  Clients Managed at XL
2,500  Clients Managed through Windows Intune at Doosan
600+  Clients in the Microsoft Store

296,200  Clients Managed
Solution Overview @ Microsoft IT

Business Challenge
- Limited monitoring
- No consolidated reporting
- Laborious manual process

Solution
- Chose FEP 2010 as new antimalware management solution
- Deployed to existing ConfigMgr 2007 R2 and R3 servers & Clients

Results/Benefits
- Faster response to infections
- Better type of malware knowledge
- Improved SLA for policy deployment
- Only added 1 server for FEP SQL data warehouse
- Minimal impact to network performance
FEP 2010 Deployment and Management Lifecycle

- **Phase 1**: Implementation Planning: Infrastructure & FEP Policies
- **Phase 2**: FEP Server and Client Deployment
- **Phase 3**: Ongoing Policy and Update Management
- **Phase 4**: Monitoring Alerting and Reporting
FEP 2010 Overview
ConfigMgr 2007 and FEP 2010 Integration

1. FEP Service Extensions
2. Databases
   - FEP DB
   - FEP Reporting Data warehouse DB
3. FEP Reporting
4. FEP Console Extensions
5. FEP 2010 Clients
FEP 2010 Overview

FEP Objects in Console
Configuration Manager Architecture at Microsoft IT

Microsoft IT ConfigMgr 07 Central Site
220,000 Clients Managed

Redmond Campus
~80k Clients
6 SUP | 6 MP | 16 DP

North & South America
~35k Clients
10 SS | 2 SUP | 2 MP | 89 DP

Limited Services
~4k Clients
1 SUP | 1 MP | 2 DP

Europe, Middle east & Africa
~35k Clients
14 SS | 2 SUP | 2 MP | 62 DP

Fareast & South Pacific
~65k Clients
7 SS | 2 SUP | 3 MP | 25 DP
FEP Management Models

- Centralized
  - Management done at Central Site
  - Central Reporting for all clients

- Decentralized
  - Managed autonomously at each Child Site
  - Reporting scope limited to Child Sites only

- Decentralized with Central Reporting
  - Managed autonomously at each Child Site
  - Central Reporting for all clients
FEP Deployment Options

- Basic
  - All Components installed on same server
  - Typical for small environments (< 5000 clients)

- Basic with Remote Reporting Database
  - Current Site DB Server not enough for scale
  - Current Site DB Server doesn’t meet software requirements

- Advanced
  - Granular control of FEP role placement
FEP Deployment Solution at Microsoft IT

- Redmond Campus ~80k Clients
- North & South America ~35k Clients
- Limited Services ~4k Clients
- Europe, Middle east & Africa ~35k Clients
- Far East & South Pacific ~65k Clients

- ConfigMgr 07 Central Site 220,000 Clients Managed
- FEP Server + Console Extensions
- FEP SQL DB
- FEP SQL Data Warehouse & Reporting

- FEP Management Model: Centralized
- FEP Deployment Option: Basic with Remote Reporting
FEP 2010 Policy Deployment
FEP 2010 Policy Deployment

- Policy Creation
- Policy Assignment
FEP 2010 Policy Management

- What is FEP Policy?
  - Antimalware, Windows Firewall Settings
  - Definition Update Source Configuration

- What can you do?
  - Copy, Edit, Assign, Import & Export Policy
  - Use Templates, Set Precedence

- Where are they?
  - FEP Node - Policies
  - All Policies -> Programs in one FEP Policy Package
  - All Assignments -> Advertisement of FEP Policy programs
FEP Policy at Microsoft

- **Antimalware Settings**
  - Real time Protection – Both ways
  - Weekly Quick scan
  - Allow Users to:
    - Change Schedule
    - Add Exclusions
    - Processor % Usage

- **No Firewall Setting**

- **Definition Update Source Order**
  - ConfigMgr/WSUS
  - Microsoft Update
## Definition Update Source

- **Update Source Order Configuration**
  - **WSUS** – Set Auto Approval Rules for FEP Definitions
  - **UNC**
    - File Shares - < 500 clients
    - DFS-R – Large Orgs
- **Default order without FEP Policy** – WSUS, MU
- **Definition Size**

<table>
<thead>
<tr>
<th>Source</th>
<th>Delta</th>
<th>Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSUS</td>
<td>~150KB – 1 MB</td>
<td>~13 MB</td>
</tr>
<tr>
<td>UNC</td>
<td>~3MB</td>
<td>~55MB</td>
</tr>
</tbody>
</table>
FEP 2010 Client Deployment

- Configure and Target FEP Policy
- ConfigMgr based Deployment
  - Client Installation Package Available in ConfigMgr
  - Add Distribution Points
  - Target Package to Collections
- Use Dashboard & ConfigMgr Reports for Tracking Deployment
- Uninstalls Existing Antimalware Products before installation

Client Deployment at Microsoft

- Phases of Deployment
  - LAB: Server & < 10 Clients
  - Pre-Production: Server & Clients in Phases: 100, 500, 1000..8500
  - Production: Server & Clients in Phases 1000, 4000 & higher

- Deployment Experience
  - ~1-3% Deployment Failures – Remediate & Re-Target Install
    - Mostly Environmental – Disk space, Other MSI Installs
    - Conflicting Products – Microsoft Security Essentials, Intune, OneCare
Client Deployment at Microsoft

- Windows Filtering Platform (WFP) Hotfix (KB981889) Requirement for Network Inspection System (NIS)
  - Pre-RC – Hotfix Installed ahead of FEP Install
    - Rebooted during Security Updates Cycle
  - RTM – Hotfix is Installed during FEP Client Installation
    - Client Functional before Reboot, except NIS

- Windows 7 SP1 – No Requirement of WFP Hotfix
FEP 2010 Dashboard and Reporting
FEP 2010 Reporting

- FEP Dashboard
- FEP Reports
ConfigMgr After FEP
Security Events – Data Flow

1. Malware Infects Client
2. FEP Client Cleans malware
   - Security Event Raised
   - DCM Evaluation Triggered
3. DCM State Message Sent
4. Infection Data replicated
   to Data Warehouse Server
5. Infection Data available in Reports
ConfigMgr After FEP Deployment

- Client to Server Traffic
  - New Client Installation
  - Malware Infection on client

- Site Server Performance After FEP
  - During FEP Client Deployments
  - During Patch deployments
## Traffic Analysis After FEP Deployment

### FEP/ConfigMgr Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Type</th>
<th>No.</th>
<th>Size (KB)</th>
<th>Total Size (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEP 2010 Client Installation</td>
<td>Status Message</td>
<td>~6</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Delta Hardware Inventory</td>
<td>Inventory File</td>
<td>1</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>FEP Default Policy Applied</td>
<td>Status Message</td>
<td>~6</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>4 DCM Baseline Policies &amp; Results</td>
<td>State Message</td>
<td>1</td>
<td>78</td>
<td>78</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>101 KB</strong></td>
</tr>
</tbody>
</table>

### Malware Detected Event

<table>
<thead>
<tr>
<th>Event</th>
<th>Type</th>
<th>No.</th>
<th>Size (KB)</th>
<th>Total Size (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 DCM Baseline Evaluation &amp; Results</td>
<td>State Message</td>
<td>1</td>
<td>49</td>
<td>49</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>49 KB</strong></td>
</tr>
</tbody>
</table>
## ConfigMgr SQL Database Growth After FEP Deployment

### FEP related Status Messages

<table>
<thead>
<tr>
<th>Key Tables Changed</th>
<th>Rows Added</th>
<th>Size Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEP related Status Messages</td>
<td>121</td>
<td>35.05 KB</td>
</tr>
<tr>
<td>Compliance Detail</td>
<td>4</td>
<td>16 KB</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>121</strong></td>
<td><strong>51.05 KB</strong></td>
</tr>
</tbody>
</table>

**Projected Growth for 220k clients:** 10.71 GB

### Malware Incident Key Tables Changed

<table>
<thead>
<tr>
<th>Key Tables Changed</th>
<th>Rows Added</th>
<th>Size Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Status, Compliance Details, Compliance History</td>
<td>4</td>
<td>17 KB</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>4</strong></td>
<td><strong>17 KB</strong></td>
</tr>
</tbody>
</table>

**Projected Growth for 220k clients:** 3.56 GB
Server Performance After FEP Deployment

- **Less than 25% spike**
- **Greater than 25% and less than 50% spike**
- **Greater than 50% spike**

<table>
<thead>
<tr>
<th>Role</th>
<th>Processor % Variance</th>
<th>Memory Available Variance</th>
<th>Network – Kilobytes/sec Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Server</td>
<td>-24%</td>
<td>0%</td>
<td>21%</td>
</tr>
<tr>
<td>MP's</td>
<td>20%</td>
<td>0%</td>
<td>-29%</td>
</tr>
<tr>
<td>SUP</td>
<td>-2%</td>
<td>0.5%</td>
<td>-71</td>
</tr>
</tbody>
</table>
## Server Performance After FEP Deployment

<table>
<thead>
<tr>
<th>Role</th>
<th>State Message Files Processing Variance</th>
<th>State Message Records Processing Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Site</td>
<td>3%</td>
<td>✅</td>
</tr>
<tr>
<td>Primary Site</td>
<td>-10%</td>
<td>✅</td>
</tr>
</tbody>
</table>
Benefits and Best Practices from Microsoft IT
Best Practices

- **Implementation**
  - Deploy in phases to reduce potential for negative impact to the environment
  - Allow an opt-out option
  - Re-deploy the client to failed machines
- **Security**
  - Use multiple sources for definitions updates
  - Determine the best times for scanning
- **Monitoring and Reporting**
  - Consider installing the reporting database on a dedicated server
Benefits

- Simplified implementation of large-scale endpoint protection with centralized administration

- Faster response to infections and better knowledge of the type of malware

- Improved SLA for antimalware policy deployment from more than a day to four hours

- Use of existing infrastructure with only 1 additional server and minimal impact to network performance
Summary and Key Takeaways

- Use Microsoft IT FEP 2010 Deployment and Management Lifecycle
  - Planning, Deployment, Management & Reporting

- Evaluate potential ConfigMgr changes After FEP Deployment

- Leverage Best Practices from Microsoft IT

- Maximize the benefit by integrating management and security
More Information

- **Forefront Endpoint Protection (FEP)**
  - FEP Server Policy Templates - [http://go.microsoft.com/fwlink/?LinkId=207730](http://go.microsoft.com/fwlink/?LinkId=207730)

- **System Center Configuration Manager (ConfigMgr)**


- **Configuration Manager News from Microsoft IT -**
  - [http://twitter.com/ConfigMgr_MSIT](http://twitter.com/ConfigMgr_MSIT)
Please Complete an Evaluation Form

Your feedback is important!

Be eligible to win great daily prizes!

For more information please refer to your Conference Guide

- Two ways to access online evaluation forms:
- CommNet stations located throughout the Mandalay Bay Convention Center
- From any wired or wireless connection to www.mms-2011.com
Questions?

Shitanshu Verma – shverma@microsoft.com
Partha Chandran- partha.chandran@microsoft.com
Microsoft Management Summit 2011

March 21-25, 2011

You. Empowered.
2011