Upgrading to Websense Web Security v7.7

Websense Support Webinar August 2012
Title:
- Support Specialist

Accomplishments:
- 10 years supporting Websense products

Qualifications:
- Technical Support Mentor
- Product Trainer

Greg Didier
Goals and Objectives

• Review version 7.7 system requirements
• Determine your upgrade path
• Is your system ready for upgrading
• Backing up policies
• Best practice tips
• What to expect during the upgrade
• Migrating your settings to a new server
Upgrade Scenarios

- Upgrade existing servers
  - Direct upgrade
  - Intermediate upgrade

- Migrate to new physical servers
  - Install 7.7 on a new server and either; manually input or import policies

- Migrate from a single to multiple servers
  - Suggested recommendation
    - Two 64-bit servers with SQL Server located off-box

- Relocate databases to an off-box SQL Server

- Virtualization
  - Follow directions for upgrading physical servers
Determine Your Upgrade Path

Web Filter & Web Security software-only deployments

• Direct upgrade
  – 7.5.x or 7.6.0 - 7.6.5, may directly upgrade to version 7.7

• Intermediate upgrade
  – 7.0 (Web Filter, software-only) > 7.5 > 7.7
  – 7.1.1 (Web Security Gateway) > 7.6 > 7.7
    • Content Gateway deployments must upgrade to 7.6.x before upgrading to version 7.7

• Migration
  – Install 7.7 on a new server and import your policies
    – You can import policies from versions 7.5.x or 7.6.x using the *PgSetup* command
System Requirements

• TRITON Management Server
  – TRITON - Web Security hardware and operating system
    • Windows Server 2008 R2 (Standard and Enterprise) 64-bit
      – Suggested implementation
      – Allows installing multiple Web Security modules
    • Windows Server 2008 (Standard and Enterprise) 32-bit
      – Supports only the Web Security module
  • With local SQL reporting database
    – 4 CPU cores (2.5 GHz), 4 GB RAM, 100 GB Disk Space
  • With remote SQL reporting database
    – 4 CPU cores (2.5 GHz), 4 GB RAM, 7 GB Disk Space

• TRITON - Web Security console browser support
  • Mozilla Firefox 4.x through 13.x
  • Google Chrome 13 and later
  • Microsoft Internet Explorer 8 and 9
    – Do not use compatibility mode with Internet Explorer 8
System Requirements

• Web Security software components
  – Not supported on domain controllers
  – Operating systems:
    • Windows Server 2008 (32-bit) and 2008 R2 (64-bit)
    • Red Hat Enterprise Linux 5 and 6
  – Windows-only components:
    • Linking Service
    • Log Server
    • DC Agent
    • Real-Time Monitor
  – Websense Content Gateway is Linux only:
    • Red Hat Enterprise Linux 5 and 6
System Requirements

• Web Security software components (continued)
  – Logon application, Remote Filtering Client, and Web Endpoint client are supported on
    • Windows XP with Service Pack 2 or higher (32-bit and 64-bit)
    • Windows Vista with Service Pack 1 or higher (32-bit and 64-bit)
    • Windows 7 (32-bit and 64-bit)
    • Windows Server 2003
    • Windows Server 2008 and 2008 R2
  – The Web Endpoint client fully supports the following Web browsers on both 32-bit and 64-bit operating systems
    • Documentation states:
      – Internet Explorer 7, 8, and 9 and Firefox 3.x, 4.x, 5, 6, and 7
    • Note: Actually, Firefox 13 and 14 and all Google Chrome versions are supported
System Requirements

- Web Security supported database engines
  - SQL Server 2005 SP4
    - Except Web, Express, and Compact; 32/64-bit, but not IA64
  - SQL Server 2008
    - Except Web, Express, and Compact; all service packs, 32/64-bit, but not IA64
  - SQL Server 2008 R2 Express
    - Installed via the Websense installer only
  - SQL Server 2008 R2
    - Except Web and Compact; all service packs, 32/64-bit, but not IA64

- Virtualization systems
  - Hyper-V over Windows Server 2008 R2
  - VMware over Windows Server 2008 R2
Intermediate Upgrades

If you currently run version 7.5 or earlier, you need to be aware of the new TRITON Management Server

• 7.6 introduced a new management infrastructure
  – Unified interface for all Websense consoles

• For information on the new TRITON Management Server, see prior webinars
  – Upgrading to Web Security v7.6
  – Migrating your custom settings to version 7.6
Intermediate Upgrades

• Best practice for version 7.5 and earlier
  – Remove TRITON manager before upgrading
  – Consider installing 7.7 fresh and migrate in your settings
  – MSDE was last supported in 7.5
    – You must be integrated with a supported SQL Server during the upgrade process
    – Or, uninstall Log Server before upgrading
  – Your directory service must include an email address for each Websense delegated administrator
  – admin replaces the WebsenseAdministrator account
## Intermediate Upgrades

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Current Platform</th>
<th>Upgrade Path</th>
</tr>
</thead>
</table>
| v7.0.x          | Windows 2003         | 1. Upgrade to v7.5.x in place.  
                  |                      | 3. Upgrade to v7.7.x on the new platform. |
| v7.0.x          | Red Hat Enterprise Linux 3 | 1. Migrate to Red Hat Enterprise Linux 5.  
                  |                      | 2. Upgrade to v7.5.x on the new platform.  
                  |                      | 3. Upgrade to v7.7.x. |
                  |                      | 2. Upgrade to v7.5.x on the new platform.  
                  |                      | 3. Upgrade to v7.7.x. |
| v7.1.x          | Red Hat Enterprise Linux 4 | 1. Migrate to Red Hat Enterprise Linux 5.  
                  |                      | 2. Upgrade to v7.5.x or v7.6.x on the new platform.  
                  |                      | 3. Upgrade to v7.7.x. |
                  |                      | 2. Upgrade to v7.7.x. |
| v7.5.x, v7.6.x  | Red Hat Enterprise Linux 4 | 1. Migrate to Red Hat Enterprise Linux 5.  
                  |                      | 2. Upgrade to v7.7.x on the new platform. |
                  |                      | 2. Upgrade to v7.7.x. |
### Is Your Integration Supported?

- Websense Web Security 7.7 may be integrated with the following products

<table>
<thead>
<tr>
<th>Product</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Forefront TMG</td>
<td>2008 or later</td>
</tr>
<tr>
<td>Cisco PIX Firewall</td>
<td>v5.3 or later</td>
</tr>
<tr>
<td>Cisco ASA</td>
<td>PIX v7.0 or later</td>
</tr>
<tr>
<td>Cisco Content Engine</td>
<td>ACNS v5.5 or 5.6</td>
</tr>
<tr>
<td>Cisco Router</td>
<td>IOS v12.3 or later</td>
</tr>
<tr>
<td>Check Point</td>
<td>Firewall-1 NGX, NGX 65, UTM-1 (VPN-1) Edge</td>
</tr>
<tr>
<td>Citrix XenApp</td>
<td>5.0 or 6.0</td>
</tr>
</tbody>
</table>
Back up TRITON Management Server (Best practice!)
  - In Task Scheduler, run: TRITON Backup
    • Document: Backing up TRITON infrastructure settings

Full backup (Best practice!)
  - On all Websense servers, run: wsbackup.exe
    • Document: Backing up Web Security configuration
    • Document: How do I back up and restore Web Security software?

Policy settings backup (For migrations)
  - On Policy Broker machine, run: PgSetup.exe
    • Article: How to back up and restore the v7.x policy database

Content Gateway Backup (Best practice!)
  - Via Content Gateway Manager
    • Doc: How do I back up and restore Websense Content Gateway?
    • Doc: Back up Content Gateway v7.7 using WCGbackup

Demonstration
Identify Upgrade Order

• If Websense components reside on multiple servers, you must identify which server to upgrade first

• Component upgrade order
  – Policy Broker
  – Policy Server
  – Filtering Service and User Service
  – Log Server
  – TRITON Unified Security Center (management server)
  – Network Agent and Content Gateway
  – Remaining server components
  – Remaining off-server components
    • Logon Agent, Remote Filtering Client, Endpoint clients
Restart Websense Components

• Intermediate upgrades, virtual servers upgrades, and Linux OS component upgrades require server reboot

• If Websense has been running for months, restart

• Restart order
  – Article: Stopping and starting Websense services

• Best practice
  – Reboot server
    • For multiple Websense servers, the installed components determine the order in which servers are stopped and started
    • Stop in reverse order of the component list show on prior slide
    • Rule of thumb: Policy Broker and Policy Server services must be running prior to all other services

• If installer hangs stopping a service, manually stop it
• If moving to a new SQL Server and **NOT** retaining the existing reporting database
  – Update the TRITION Infrastructure SQL Server settings
    • Launch Websense installer and select Modify
  – Uninstall Websense Log Server
  – Upgrade
  – Reinstall Log Server
    • A new 7.7 reporting database is generated
• If moving to new SQL Server and retaining the database
  – Update the TRITION Infrastructure SQL Server settings
    • Launch Websense installer and select Modify
  – Detach, move, and then reattach databases to new SQL Server
  – Connect Log Server to the databases on the new SQL Server
    • Article: [How to update the ODBC and the Log Server connections](#)
  – Upgrade
    • The existing reporting database is upgraded to version 7.7
Logging and Database

• If retaining a database hosted on a full SQL Server
  – Stop Log Server service
  – Disable all Websense SQL Agent jobs
  – After upgrade, re-enable Websense SQL Agent jobs

• If using a Windows trusted account for the SQL connection, perform the upgrade logged on as the same trusted account
Tips

• Ensure your system is functional prior to upgrading
  – Upgrading does not repair a non-functional system

• The Filtering Service and TRITON - Web Security machines must have same locale settings
  – After upgrade, Filtering Service can be restarted with any locale settings

• Reporting database
  – Disable SQL Server Agent jobs prior to upgrading
  – Stop Log Server
  – Consider backing up SQL partitions
  – Your SQL version and service pack must be supported
    • Incompatible versions may result in corrupted databases
• Master Database is removed during upgrade
  – Plan on a large file download when upgrade completes
  – Prior 7.7 Endpoint Clients begin working after Master database download finishes

• Set service recovery option to, “Take no action”
• Upgrade only affects local Websense components
• Perform full backups on all Websense servers
• Log out of TRITON - Web Security console
  – Endpoint clients are exceptions
• New services require opening ports on firewalls
Tips

• Stop antivirus software during upgrade
  – Restart after upgrade completes

• Some Content Gateway settings are not preserved
  – Must restore Integrated Windows Authentication settings
  – See the WCG post-upgrade activities list for full details

• See the Deployment guide for more considerations on upgrading Linux servers
Expectations

• What to expect from the upgrade
  – Users are not filtered during upgrade process
  – Components successfully upgraded cannot be rolled back
  – Policies and most configuration details are preserved across intermediate upgrades
  – Demonstration

• Post-upgrade, enhancements and new features
  – Read the Release Notes
  – Review the Upgrading User Quick Start Tutorial
Issues Seen In Techsupport

• Incompatibility between the Content Gateway 7.7 implementation of WCCP GRE and Cisco ASA firewall products
  – To avoid this problem, do not change the WCCP configuration file (wccp.config) as suggested in the upgrade documentation
  – Article: Content Gateway v7.7.0: WCCP and Cisco ASA
  – Best practice
    • Install a 7.7 Content Gateway test system

• Encountering corrupted reporting databases when upgrading with an unsupported SQL Server
• Running the Websense installer on a Linux server results in incorrect library file errors
  – Specific update packages must be installed prior to running the Websense Content Gateway installer
  – Use YUM to update libraries on the Linux server
  • Article: How to install 'update packages' for Websense Content Gateway v7.7 software installations
  • Document: Installing Web Security components on Linux
If Your Upgrade Does Not Succeed

- **Restore from backup**
  - How To Back Up And Restore v7.x Policy Database
  - How Do I Restore My Websense Filtering Configuration?

- **Migrate policies to fresh 7.7 installation**
  - Document: Moving Web Security policy components to a new machine

- **Best practice**
  - If resources are available, install 7.7 on a new server and either
    - Migrate in your current policies, or
    - Manually enter your policies
      - Allows spring cleaning
      - Affords reviewing current policies, key words, custom URLs, etc.
• Upgrading User Quick Start Tutorial
• Before upgrading Web Security to v7.7
• Upgrading Web Filter or Web Security software-only deployments from v7.5.x
• Backup and Restore FAQ
• Backing up and restoring your Websense data
• How do I back up and restore the TRITON infrastructure?
• How do I back up or restore TRITON Unified Security Center settings?
• How do I back up and restore Web Security software?
• How do I back up and restore Websense Content Gateway?
• How to back up and restore the v7.x policy database
Additional Resources

- How to migrate 7.1 and 7.5 policies to 7.6
- Migrating Web Security to a new operating system
- What tasks should I perform prior to installing or upgrading Websense?
- Installation and upgrade
- How to install 'update packages' for Websense Content Gateway v7.7 software installations
- Content Gateway Pre and post-upgrade activities
- Webinar: Installing Version 7.6: The Latest Tips
Upcoming Webinar

Introduction to Websense Data Security v7.7

Date:
September 19th, 2012

Time:
8:30 A.M. PDT (GMT -8)

How to register:
http://www.websense.com/content/SupportWebinars.aspx
Training

• To find Websense classes offered by Authorized Training Partners in your area, visit:
  http://www.websense.com/findaclass

• Websense Training Partners offer classes online and onsite at your location.

• For more information, please send email to:
  readiness@websense.com