

Webinar Question/Answer

Webinar: Upgrading to Websense Web Security v7.6

Date: April 13/2011

Q1: Are there any issues with using virtualized servers - Hyper V?

Although there are no known issues with running virtualized, Websense's official policy has been that we do not test or certify our software on virtualized platforms. Instead, we provide "best effort" support for Hyper V and VMWare. If the problem resides in the Websense software, we'll fix it, but if it is specific to the virtualized deployment, we can't guarantee that it will be resolved.

See <http://www.websense.com/support/article/t-kbarticle/VMware-support> for more details.

Q2: Best Practice suggests two 64bit servers, however I have 500 users, a small install, can the system run effectively on 1 box? (..plus the sql server of course)

Depending on what components you install and how much traffic your average user generates, for 500 users, you can probably get away with a single, modern 64-bit server. The installation guide will make this clearer for each specific requirement.

Q3: Is the patch installation on v7.6 better (no more manual manipulation to copy, backup etc)?

On the appliances, yes the patch installation is improved. The RPMs can be downloaded directly from the Appliance Manager interface. It is always best practice to confirm a recent backup before patching.

Q4: We are running Triton 7.5. Why should we upgrade to 7.6?

7.6 is a major upgrade to the 7.x products. This includes new features, better compatibility with new operating systems and network directories, better performance and stability. See the v7.6 Release Notes for specific details.

Q5: Is DSS still going to have the bundled oracle? And does that mean that the DSS management server still needs to be on a separate machine?

DSS no longer uses Oracle. That database engine has switched to MSSQL. The DSS management server should typically be on the same machine as TRITON.

Q6: Are you moving away from Postgres for the management database?

No. Postgres remains the database engine for policies and certain configuration options.

Q 7: How about Linux deployments?

Many components can be deployed on Linux, but the complete TRITON interface with management plug-ins is not supported on Linux, and reporting still requires use of an MSSQL reporting database.

Q 8: Is the Content Gateway also updated during this release? Does it now log SSL traffic when running in tunnel mode?

Yes - WCG is comprehensively updated for 7.6. "SSL Decryption Bypass" (Available in the TRITON Web Security -> Settings -> Scanning section) should be used to tunnel traffic, and HTTPS traffic is logged when used in that manner.

Q 9: We have two V10000 G2 Appliances. Can 7.6 be deployed to these appliances?

Yes - See the release notes for more specifics, or tune in next month for a Webinar that addresses the appliances specifically.

Q 10: You say Hyper-V is supported. Does that include support for Network Agent?

Double-check with Microsoft on this, but it does not appear that promiscuous NICs are supported on Hyper-V at this time. That may have changed, or there may be a trick to get it working. Microsoft would be your best source of information on that.

Q 11: Can we use the 64bit version of 2003?

The information currently available is that the 64-bit versions of Windows 2003 are not certified, but when the product is released, the installation guide will have the official details.

Q 12: When doing the upgrade, we will most likely rebuild the box 64bit. How can I verify that the internet will fail open instead of closed? I am integrating this with Cisco Firewall.

The Cisco install supplement has the details on page 18. Set the "allow" parameter in your "filter" line(s) to fail open.

<http://www.websense.com/support/article/documentation/Cisco-Installation-Supplement>

Q 12: When will the install/updates be available via .exe package versus manually copying files/stopping/starting services?

The install and major updates are done with an executable. Hotfixes are usually not scripted because we prefer to get them to the customers sooner rather than having to QA an installer in a variety of different deployments.

Additionally, while the multiple Websense components inherently increase security and stability, they also allow for installation across multiple servers. Applying a single hotfix for a single Websense component may require changes on multiple servers, so it becomes important to read the associated ReadMe file for any hotfix. As a policy, hotfixes do not need to be applied unless you discover an issue affecting your Websense server; however, as a technician I like to be proactive and install hotfixes when they become available. If a serious problem is discovered, that requires applying a hotfix, then you will receive an email alert (if you are signed up for Websense Alerts).

Q 13: Triton Mgt Server - can this be our own server hardware or does this have to be your server/appliance?

In most all installations, the TRITON Management Server will be on your server. In fact, it's only available in a limited form on the appliance itself. This limited management was added to demonstrate the appliance and should not be used in a production environment.

Q 14: Are virtual servers supported for management and log servers? If they are supported, are they recommended?

In support, we typically don't actively recommend virtualization because there are additional considerations with regard to networking and resource bottlenecks which can increase the complexity of troubleshooting intermittent or performance-related issues. If something like that becomes a concern and we cannot identify the problem based on normal troubleshooting procedures, we may ask you to take steps to confirm the virtualization is not causing the problem.

Specifically answering your question concerning Log Server, this component is very file intensive. It does a lot of writing to the hard disk, which in a virtualized environment can quickly become a problem. Typically, I suggest not installing Log Server on a virtual server. If you do install it, then you will want to monitor your disks for performance issues.

Q 16: Does v7.6 include Real Time Analyzer?

Yes. It does include an improved Real Time Analyzer feature called, 'Real Time Monitor.'

Q 17: In regards to this statement: "Install SQL Server Client Tools on the server where websense log server will be located." Does that mean on "Server Two" in your best practice scenario, or the standalone SQL server?

Referencing Slide 13 on the Webinar, yes the SQL Client Tools would be installed on server two. More generally, they should be installed on the server where Websense Log Server resides.

Q 18: What is the current best practice for monitoring terminal services environments? We are currently on 6.3 installed on top of ISA 2006 only because we need to identify terminal services users.

You can continue to use ISA, or upgrade to Websense Security Gateway (7.0+), which includes Websense Content Gateway (a proxy server capable of uniquely identifying terminal server users).

Q 19: Will the new version support Kerberos?

Yes. When integrated Windows Authentication, Websense now uses Kerberos for authentication of users.

Q20: Will the Citrix plugin support 64bit servers?

Yes. There is a 64-bit plugin for Citrix in 7.6.

Q21: How does this process apply to V10000 G2 appliance users?

Much of it applies directly, as your off-box components will need to be updated to 7.6 - using the procedures discussed here - when you patch the appliance to 7.6. If you are using V-Series appliance, then it is most likely that this is where you have your central Websense policies services running. In this case, your V-Series appliance requires upgrading first (to v7.6) before upgrading your remote Websense components. Additional information, more specific to appliance deployments, will be the subject of next month's webinar.

Q 22: What differences are there for the appliances?

The TRITON management infrastructure is designed to run on a Windows server, so most of what you're seeing here indirectly applies to an appliance-based environment. The next webinar deals with the appliances more directly.

Q 23: Does the new version come with the remote filtering upgrade and does it available for windows 64 bit client?

Yes - The 7.6 Remote Filtering Client has a true 64-bit version for compatibility with 64-bit clients.

Q 24: We have the Control Service and Filtering Service on the V10k not the stand alone server. Anything unique for this setup that we need to be aware of?

We've tried to make it as intuitive as we can, and have tested 7.6 extensively in appliance-based deployments, but for the specifics of all the best practices and upgrade procedures, you may want to tune into the next webinar. And always review the release documentation and installation guide carefully to confirm your infrastructure for off-box components is compatible.

Q 25: I have Web Filter only version 6.3.3 on a P4 3 GHz system running server 2003 for 75 users. Client would like to upgrade to Web Security 7.6. Will this hardware work?

It will probably work for just Web Filtering, but that CPU is not certified, so we can't guarantee it will run properly. We know that businesses don't always have money to invest on new servers, so my recommendation would be to take a full backup, upgrade and test it. This may help you hold off from purchasing a new server for a year or so, that would be great. If not, you will need to reinstall at your current version and restore Websense policies.

Q 26: Do you support Oracle as database?

No, Oracle along with MSDE is not supported. Only Microsoft SQL is supported. See the v7.6 Deployment for specific details.

Q 27: I understand Microsoft doesn't provide a new MSDE. Will the old one still work? I don't understand what you mean by "we mirror it".

Use SQL 2008 Express R2. It's included with the installer, free, and provides a larger database size limit. Additionally, it's certified on recent operating systems and tested to work with current Websense reporting software.

Before upgrading, a supported SQL server must be available in your network.

Q 28: We currently run Blue Coat with Websense on-box URL database. We do use Websense reporting extensively. Besides the 64bit upgrade which should give us a huge performance increase, what other benefits could we expect for Websense Reporting in 7.6?

The reporting benefits are evolutionary. In other words, it should be more stable and refined, but don't expect a ton of new features in that deployment environment.

Q 29: Since we are looking at an OS upgrade/overhaul would it be better to do a new installation or try upgrading all of the components?

With any software, you'll generally have better results with a fresh installation, particularly if you'll be upgrading the OS. This also allows for continued filtering while building and testing your new v7.6 Websense server.

Q 30: For just v7.6 Filtering and Network Agent, what are the most recent versions of Red Hat Enterprise supported?

RHEL 5 update 3 and greater is supported, but not RHEL 6.

Q 31: Websense DSS DLP needs an Oracle server right now. Does that mean I don't need an Oracle server anymore since the Triton Management 7.6 server will support MS SQL? Is that correct?

That is correct. The DSS product now runs on MSSQL server.

Q 32: No support of SQL-2008R2? What about SQL-2008R2 clustered?

SQL 2008 R2 is supported. SQL cluster support is being added as well, but we'll need to verify with the official installation guide once it is released for full details.

Q 33: We use a license for version 7.1, is it possible to update to version 7.6 with this existing license?

Yes - unless you plan to add new Websense products (with different subscription keys) to your deployment, you can always upgrade to our latest software. Since you are running v7.1, you may perform a direct upgrade to v7.6. Before upgrading, check the Deployment Guide to ensure your hardware meets the minimum requirements.

Q 34: Should all existing 7.5 servers be upgraded to 7.6? For example: 1 server is only network agent with 1 policy broker and then another policy server.

Definitely. All Websense components in a deployment must run on the same major version. You must upgrade the central server, with Websense Policy Server and Policy Broker services first.

Q 35: Will Websense 7.6 run on a core installation of 2008 R2?

No. Websense does not test or certify installation on the Windows 2008 Server Core versions.

Q 36: I'm not seeing any notes specific to WCCP or IP spoofing, any known issues on 7.6?

This question is a little beyond the scope of this Webinar, but the major change for IP spoofing is that HTTPS transactions are now spoofed as well as HTTP. WCCP is enhanced with more detailed configuration options, and some compatibility and performance refinements.

Q 37: Can the SQL server be 32bit and the Triton server 64 bit?

Yes - there should be no compatibility issue.

Q 38: What is the suggested OS to run WS 7.6 on? Will the performance be better on Red Hat?

The recommended operating system for management and reporting components is Windows 2008 R2. Depending on what products you are deploying, this may be the only certified operating system. We have not noticed a significant performance difference between properly designed Windows and Linux deployments, but you should be aware there are some components/products that only run on Windows, and some that only run on Linux (or the appliance).

Q 39: How many servers should I use for 800 users? Currently I run one Websense Server integrated with Cisco ASA and then Citrix Integration plugin on all Citrix/Xenapp Servers.

That's a bit of a grey area depending on what exact services you're running on that server, how powerful it is, and how you feel about the performance right now. Ultimately the installation guide is going to be the authority on what is certified to work on typical loads for small, medium, and large businesses.

Q 40: We use appliances; the webinar on this is next month. Does this mean the release date for upgrading our appliances is going to be end of May or early June?

No. The release date for 7.6 will (in all likelihood) be the same date for all 7.6 components - including the appliance patch. The 7.6 appliance webinar will be after the release. You can either wait until that webinar to help plan your upgrade, or carefully review the installation documentation prior to upgrading (that's recommended anyway).

Q 41: When is ESG supposed to be releasing?

Email Security Gateway will be part of the 7.6 appliance images, which will be released with the other 7.6 software installers.

Q 42: Can I run SQL Server 2008 Workgroup Ed. on the same server that is running Websense for an office with only 30 staff? You had a slide that said if it is on the same box it only supports SQL Server Express. Why couldn't I use a full version of SQL?

I don't see why you couldn't run workgroup edition, but it's not something that we've specifically certified. Our recommendation is to stick with the certified platforms (2008 R2 Express will be more than adequate for 30 users), and save yourself a little money. Also, we don't recommend full SQL on the same server because the free version's resource limits line up nicely with the recommended size for a single-server deployment in a small business. In other words, moving to full SQL to deal with a larger load than Express can handle may just starve other services for resources.

Q 43: Can we install Websense Web Security on Windows 2008 R2 x64?

Yes.

Q 44: Where can I find more information on Kerberos? We stopped using Websense due to lack of transparent Kerberos authentication support.

Kerberos is supported in 7.6 as "Integrated Windows Authentication." The details are a bit beyond the scope of this Q&A session, but the basic procedure is that Content Gateway joins the domain and becomes a Service Server for proxy clients.

Q 45: Is Websense v7.6 a 64-bit application?

As of v7.6, you will no longer hear us apologizing that we do not support 64-bit servers. Most Websense applications are still 32-bit, but there are a few 64-bit components for compatibility on operating systems that don't support the emulation layer required to run 32-bit applications. Future releases will provide more true 64-bit components that can take advantage of the increased resources. This is the process how companies migrate applications to 64-bit architecture.

Q 46: So there will not be three different apps: web security, data security, email security?

From a technical perspective there will be some components that are dedicated to one of these products. For example, the new email security product must run on the appliance, so you could say the app is installed on the appliance.

From a management interface perspective, the TRITON Security Center interface is integrated, allowing single logon and the sharing configuration setting. The different products are accessed by clicking on the appropriate tab at the top of the TRITON management interface.

Q 47: Does 7.6 resolve authentication issues with the transparent redirect like WCCP using NTLM to authenticate users against 2008 AD?

NTLM support is enhanced including explicit and transparent proxy support, NTLMv2 with session security, and NTLMv1 with session security.

Q 48: Can 7.5 and 7.6 run side-by-side with the same license key? Isolated hardware.

Yes, if these are totally isolated deployments. Just running the same license key between the two deployments will not cause any compatibility issues.

Contractually, you are only allowed to run your subscription on a 'single' Websense installation. Since you download Master URL database updates daily, we know the number and versions of your installations. However, in real life we know you need to upgrade and best practice is to install Websense on a new server—using the same key is convenient. This allows you to preserve current web filtering and test the new v7.6 installation, and fail back to your prior v7.5 install if necessary. So, no one from Websense will bother you unless you continue to run the same subscription key on multiple Websense deployments for several months.

If you decide to retain a complete second Websense deployment sitting in standby mode, in case the primary Websense server fails, then contact Sales for a second subscription key.

Q 49: So it won't cause a meltdown then if my domain controller, active directory and Websense are on one Win Server 2008 machine? Or should I really press for another server with fewer than 500 users?

You should really press for a dedicated Websense server.

Q 50: We just recently installed 7.5. How much longer will it be supported before we have to upgrade to 7.6?

There is no date decided for 7.5 end of life, but typically it is three or more years, after a major release, that prior versions are EOL (End Of Life). Before this becomes an issue, you we'll be given fair warning. For specific details, see the 'Version Support and End of Life Policies' support page.

<http://www.websense.com/content/VersionSupportPolicy.aspx>

Q 51: Can we use workstation names rather than just IP addresses for the clients?

Workstation names are not valid for clients, but this functionality is already being researched for a future release.

Q 52: Will this be backward compatible with 7.1 remote client?

Typically Remote Filtering Clients are certified to work with the same version of Remote Filtering Server (7.6) as well as two major updates prior. So 7.1 and 7.5 Clients should also work with 7.6 Server. Double-check the release notes once they are published for the official details.

Q 53: Will the v7.6 remote desktop client (64-bit) work in conjunction with a v7.0 Websense Web filtering installation?

No. This is not a certified deployment. Older Remote Clients are tested against current (v7.6) Remote Filtering Server installations, but current Remote Clients (v7.6) are not tested for compatibility against older Remote Filtering Server versions.

Q 54: If you are running policy lite on v10 in 4 node cluster can real time monitor pull from all at the same time?

Real Time Monitor only pulls data on a "per Policy Server" basis, so in this configuration (appliances in "Filtering and Directory mode), you'd have to switch to the V10000 you want to view live traffic from.

Q 55: Given the new Real-Time Monitor, does the command line TestLogServer go away or is it still available in 7.6?

TestLogServer is still available and works the same way as in previous versions.

Q 56: We have a single modern server recently install with Windows Standard 2008 32 bit and Web Filter 7.5. What is the best way to upgrade to V7.6, maybe format the server again?

If you anticipate having any desire to check out DLP or Email Security products, it's probably better to get on a 64-bit OS before upgrading. That way you're certified for multiple products. With a 32-bit OS, you can only run Web Filter.

I always suggest clean installs and manually re-entering your settings and policies. This affords you the opportunity to clean up and simplify your custom policies. In your case, if you can afford to not filter your end users for a time, then this route is best.

Q 57: In 7.6, V10k Xen 64 bit or not?

The V-series appliance operating system is modified 32-bit CentOS.

Q 58: For the small environment of 200 users, can we move Websense to Virtual Server (VMWare)?

The best answer I can give is "probably." The two main considerations are network (will you be able to configure a promiscuous NIC to see the necessary network traffic?) and unanticipated performance bottlenecks in the VM host. You can leave your current Websense server running and test by installing v7.6 on VMWare. I typically do not suggest installing the Log Server component on a VM as it is very disk write intensive.