Scanmail for Lotus Domino 5.0

Albert Dejbakhsh

US Core Team

Table of contents

1. Product Description:

Trend Micro ScanMail for Lotus Domino (SMLD) provides an integrated defense against multiple threats, data compromises, and vulnerabilities in Lotus Domino systems. It is capable of protecting Domino Server against malware, spyware, spam, phishing, script bomb and other unwanted contents. The ScanMail for Lotus Domino version 5.0 supports 32bit and 64bit Domino 8.5 on Windows 2003 and Windows 2008. SMLD 5.0 for AIX supports Domino 8.X.X on 64-bit.

ScanMail for Lotus Domino 5.0 currently runs on the following platforms:

- **Microsoft™ Windows™**
- **IBM™ AIX™**

ScanMail is fully compatible with Trend Micro Control Manager™, the Trend Micro centralized management console that lets you consolidate your antivirus and content security protection into a cohesive solution.

Administrators can specify which databases are to be scanned, and users are prevented from overwriting a clean document with an infected version. Manual database scanning cleans existing infections.

ScanMail helps administrators enforce company email policies, increase overall server efficiency, and minimize virus outbreaks. Administrators can create rules to block certain file types and block, delay, and prioritize messages. A corporate policy can be implemented to deal with malware incidents in several ways:

- Isolate the infected file for later cleaning or other action.
- Send the infected item to the intended recipient along with a notification that the file is infected and has not been cleaned.
- Delete the infected file.
- Block the infected file and prevent it from being delivered.
- Alert the administrator.

By using a multi-threaded scan engine and memory scanning, ScanMail is able to maximize efficiency and minimize impact on Lotus Domino servers. Administrators can identify servers that don't require scanning, thus eliminating redundant scanning.

To see where ScanMail for Domino fits in a comprehensive approach to protecting your environment, see

http://us.trendmicro.com/us/products/enterprise/scanmail-for-lotus-domino/index.html

2. Architecture

2.1. Installation

2.1.1. Recommended Hardware and Software Requirements

Individual company networks are as unique as the companies themselves. Different networks have different requirements depending on the level of network complexity. This section describes the system requirements for a ScanMail for Domino server. Table 2-1 lists the system requirements for ScanMail.

Hardware/Software Specifications	**Requirements**
Operating system (OS)	**ScanMail for Windows™:** - Microsoft Windows 2003 Server Standard Edition; - Microsoft Windows 2003 Server Enterprise Edition, Service Pack 2 - Microsoft Windows 2003 Server x64 Edition - Microsoft Windows 2008 Standard Edition, Service Pack 2 - Microsoft Windows 2008 Standard Enterprise Edition, Service Pack 2 - Microsoft Windows 2008 Standard X64 Edition, Service Pack 2 - Microsoft Windows 2008 Standard Enterprise X64 Edition, Service Pack 2 **ScanMail for AIX™:** - IBM AIX 5.3 (64-bit Kernel) , minimum patch level of TL7,0815 (5300-07-04-0815); - IBM AIX 6.1 (64-bit Kernel) , Server Pack 4, APAR IZ10223, APAR IZ09961, APAR IZ10284, APAR IZ 08022
Lotus™ Domino™	- Lotus(TM) Domino(TM) R8.0.1, R8.0.2, R8.5 64 bit

Hardware/Software Specifications	**Requirements**
CPU	**ScanMail for Windows:** - Intel PentiumTM 4 processor or higher **ScanMail for AIX:** - Power4 and higher processor
Memory	**ScanMail for Windows:** - 512-MB of memory; 1-GB recommended **ScanMail for AIX:** - 1-GB Memory
Disk space	**ScanMail for Windows:** - 400-MB available disk space for program files; 100-MB available disk space on each partition **ScanMail for AIX:** - 500-MB available disk space for program files, 100-MB available disk space on each partition, 400-MB available disk space for /tmp file system
File system	**ScanMail for Windows:** NT File System (NTFS) partition
Monitor	All Platforms: VGA monitor cap Colors
Component updates	All Platforms: Internet access for component download
Other	**NotesAPI:** 7.0.2 (32-bit) 8.0.1 (64-bit)

2.2. Network Topology

Scanmail for Domino can be installed on any type of Domino server, either the server is acting as a Hub server or a spoke server. The centralized policy based configuration helps the large scale clients to make changes to the SMD configuration at one point and then replicate the configurations down to other servers. Each server will make use of the configurations that belong to its policy.

3. Sizing Summary

Trend Micro Technical Sales Solutions (TSS) conducted a series of performance tests to understand the impact of installing Trend Micro™ ScanMail™ 5.0 (SMLD 5.0) on supported Lotus Domino R8.0.1, R8.0.2 and R8.5 servers. Trend Micro designed SMLD 5.0 for customers running 32- and 64-bit versions of Microsoft Windows Server 2003 and 64-bit AIX.

Trend Micro measured the impact of ScanMail 5.0 for Lotus Domino while scanning real-time mail transfers and while performing manual and scheduled scanning of specific databases for malware. The installation of SMLD 5.0 results in a low increase in CPU and memory utilization during real-time scanning. Tests indicate SMLD 5.0 is modestly better performing than the previous version of the product (SMLD 3.0) on a 32-bit Windows platform, but it does require more disk space and memory (more memory and a faster CPU yield better performance).

3.1. SMLD 5.0 Effect on Resources: Examples

This section presents two sizing examples. The first example estimates the effect real-time scanning has on system resources. The second provides a method of estimating the time necessary to complete a manual scan. When used together, these examples can help customers better understand the impact

Trend Micro ScanMail 5.0 for Lotus Domino has on Lotus Domino server performance.

Note: TSS obtained the performance results using a specific type of common hardware. Customers should not consider these results applicable to all hardware types. TSS intends that customers should use these results only as a guideline. The customer’s actual results may differ—perhaps substantially—depending on how different their hardware is from that we used in our tests.

Real-time Scanning Example

The impact of real-time scanning on system performancewill depend highly on existing traffic, type of traffic, scanning policies, and hardware.

Note: New or existing customers that need to understand the consequences of ScanMail 5.0 for Lotus Domino real-time scanning on their Lotus Domino installation should refer to Table 3.

You can help customers achieve the best possible real-time scanning performance, by having them take the following high-level steps:

- Ensure that customer has patched their Lotus Domino environment properly and that they have tuned it optimally for the use to which they will be putting it.
- Gather all available performance metrics (CPU, memory, I/O) for the Lotus Domino server on which they will install SMLD 5.0.
- Make sure that the customer has gathered performance data during peak loads – this is a critical step for properly sizing the server. Peak loads may occur at different times of the day, week, or even time of year.
- Refer to Table 3 to understand the general impact of installing SMLD 5.0.
- Customers may wish to consider adding hardware if the existing equipment does not meet minimum requirements, or if they are not satisfied with the forecasted results of adding SMLD 5.0.

Manual Scanning Example (On tested 32-bit hardware)

It is important that customers estimate the scanning times for manual and scheduled scans. Customerscan apply the following observations to any installed hardware type for rough estimates.

- Manual scanning can be resource intensive. The impact of manual scanning on CPU and memory can be difficult to measure due to the number of variables unique to each environment.
- During our tests, we saw memory utilization increase by 9% to 31% and the CPU utilization increase by 52% to 93%. Different environments will have different results. “Your mileage may vary.”
- If the customer knows the total size of the database present in a specific directory, they can estimate the time required for a manual scan of that directory by using the following simple formula:

ScanTime = 468*MessageStore – 363

Where:

- ScanTime = total scanning time (in seconds)

Please see the SMD Sizing Guide for more information.

Additional instance of SMDReal

The first modification to increase performance on a ScanMail server is to invoke a second instance of the SMDReal task. This can be performed by adding a new entry for SMDReal on the ServerTasks line in the notes.ini file

Adding a second instance of SMDReal can offer a boost in performance on a ScanMail server when compared to ScanMail performance with a single instance running. The drawback to enabling a second instance of SMDReal is that processor utilization increases by approximately 15 percent.

An important consideration to understand before invoking a new instance of SMDReal is the number of dedicated threads and dedicated memory. By default, SMDReal is allocated 13 threads.

Thread Purpose	# Threads
Real-Time Mail Scan	5
Real-Time Database Scan	5
Thread Generation	1
Thread Management	1
Communication	1

When a new instance of SMDReal is invoked, a certain amount of memory is pre-allocated for the task. By default approximately 45 MB is utilized to run the additional SMDReal task, with another amount used on demand. The amount of on-demand memory used by the SMDReal threads is specified by the ScanMail administrator in the Server Settings document of smconf.nsf. By default this amount is a maximum of 5MB per thread. Care should be taken when setting the Memory Size for Scanning values in the Server Document. These values should not exceed the maximum attachment size limitations specified by the ScanMail administrator.

Adding Threads to SMDReal

An alternative method of increasing performance of ScanMail is to increase the number of threads used by SMDReal for scanning. By default, SMDReal utilizes 13 threads. ScanMail administrators can modify the number of threads used by ScanMail for scanning of messages and databases. The maximum number of scan threads that can be allocated to SMDReal is 20. This does not include the three control threads.
Each new thread added to SMDReal equates to one more document that can be scanned simultaneously.

4. Product

4.1. Configuration

4.1.1. GUI

SETTINGS	COMMENTS
Configurations	
Policies	Client can create different policies targeted towards different servers
Mail Scan Rules **Scan Options (Virus Scan)**	
Files to Scan	'All files' is recommended as it’s a safer approach. If 'Selected Files' option is chosen and the files are not chosen with care then there is a chance for the malware to go through.
Advanced Options	
Clean Compressed Files	This option is disabled by default. If enabled, it becomes resource extensive as the system will have to uncompress and then clean the files inside the archive and then compress them back again.
Macros in Microsoft Office files	This option applies to ALL the Macros in the Microsoft Office Files and NOT just the infected macros. So if the action is 'Strip' then all the macros will be stripped from the Microsoft Office Files. The infected macros are taken care of, according to the malware type and the action for that malware configured in the virus actions.
Scan Options (Scan Restrictions)	
Maximum extracted file size	10 MB can be used as default. Which means any email that has an attachment whose size after extraction exceeds 10MB will trigger the associated action. Clients are recommended to adjust this number according to their environment, if required.
Maximum compression level	3 Can be used as default. Any attachment that has the number of compression layers more than 4 will trigger the associated action. Clients are encouraged to adjust this number according to their environment. Please keep in mind that choosing a higher number will result in CPU extensive scanning if the attachments have the higher number of compression layers.

Scan Options (Attachment Filter)	
Using "True file type(s)" Vs "Extension name(s)"	Using "True file types" means that SMLD will look inside the file to find out the true type of the file, instead of just relying on the extension name. So if some one renames an .exe to .txt then using "Extension names" blocking to block .exe will not be able to catch it. But using "True file type(s)" blocking to block 'Executable' will still catch that .txt file.
Scan Options (Content Filter) Create new content filter	
Create new expression	It is more efficient to create multiple expressions under the same rule instead of creating multiple rules for the same category of expressions. For example, if you would like to create the expressions to catch the racial words then a rule can be created as 'Racial' and then all different expressions could be added within that rule, as compared to creating different rule for each racial expression. Rules are there to help the users to separate different category of the expressions used to perform content filtering.
Database Scan	
Scan Options (Virus Scan)	Same as discussed above in the "Mail Scan Rules->Scan Options (Virus Scan)
Scan Options (Scan Restrictions)	Same as discussed above in the "Mail Scan Rules->Scan Options (Scan Restrictions)
Scheduled Scan	
Scan Options (Virus Scan)	Same as discussed above in the "Mail Scan Rules->Scan Options (Virus Scan)
Scan Options (Scan Restrictions)	Same as discussed above in the "Mail Scan Rules->Scan Options (Scan Restrictions)
Scheduled Update	At least a Daily scheduled download is recommended for the pattern components. The Scan engine, Anti-spam engine and the Scanmail for Domino application components are not recommended to be enabled by default.

Cluster Trusting	Cluster trusting is the feature that helps SMLD to create a trust relationship among the nodes of the cluster. If server A of the cluster trusts Server B of the cluster then Server A will not scan any database events that originate from Server B. Cluster trusting is recommended to be used to reduce the overhead of re-scanning the events from other servers in the same cluster. Of course the assumption over here is that all the servers in the cluster have SMD installed and doing real time scan of their own events. Please note that this trusting is only limited to the database events like replication and more. This does not include the emails coming from that server. For that purpose another configuration setting is used to trust such traffic. That configuration is called ‘Trusted Antivirus Servers” and is found in the ‘Server Settings”. It is discussed in the sections ahead.
Server Settings	
Scan Memory	By default this amount is a maximum of 5MB per thread. Care should be taken when setting the Memory Size for Scanning values in the Server Document. These values should not exceed the maximum attachment size limitations specified by the ScanMail administrator. This value should be set to the average size of the attachments that passes through the Domino server. For example, if the maximum number of emails that are handled by that Domino server contain the attachment size around 10 MB then change this value to 10 MB.
Miscilenious Multi-threaded scanning	
Number of threads	The default number of threads is 5. Set the value per thread to be between 1 and 20, inclusive. The sum of both the real-time mail and real-time database scanning threads cannot exceed 20. Please refer to the "Sizing Summary" section to read the discussion on changing the number of threads versus the number of SMDReal tasks.

Trusted Antivirus servers	Over here you can choose the Domino servers or enter the SMTP servers that will be trusted. So the emails coming from those servers will be trusted as clean. Verify that trusted servers have antivirus and content security protection to prevent viruses and other malware from spreading to other Domino servers. NOTE: This setting is only to trust the email traffic and not the database events generated from the other domino servers, for example the events generated from the nodes in the clustered domino servers. For the clustered domino servers use the 'Cluster trusting' option as mentioned above.
Mail Routing	
Do not deliver mails when the Mail scan task is not running.	If enabled then it means if the SMDReal is not loaded, the emails will sit in the mail.box and will not be routed out. The default/recommended value is enabled. If it is disabled/unchecked then please note that the emails will be routed out to the recipients unscanned, if SMDReal is not loaded.
Exclude tasks	Recommended value is compact, fixup, updall, update. This will make sure that the events generated from these tasks will not be scanned.

4.1.2. INI

SETTINGS	COMMENTS
SMDSkipTaskList	This parameter is added in Notes.ini. The default/recommended value is SMDSkipTaskList=COMPACT,FIXUP,UPDALL,UPDATE Which means that the database events originated from these tasks, will not be scanned.
ServerTasks	This is an existing parameter in Notes.ini. This will have some already added values in it. We recommend to add the following tasks: SMDReal SMDMon SMDSch SMDEmf SMDCM (e.g. ServerTasks=Update,Replica,Router,AMgr,AdminP,CalConn, Sched,SMDemf,SMDreal,SMDsch,SMDmon) These tasks will be loaded by itself when the Domino server starts.SMD tasks are added by default to ServerTasks by the install program of SMD.
EXTMGR_ADDINS	In this Notes.ini parameter you will find the names of the modules that hook into the Extension Manager of Domino server. By default SMD install program will add SMDExt (e.g. EXTMGR_ADDINS=SMDExt) to the EXTMGR_ADDINS parameter. It is very important to keep it in there as if there is no SMDExt found in EXTMGR_ADDINS then there will be no scanning taking place.
SMDAutoReleaseMail	To enable "mail.box" scanning while the real-time scanner loads, add this parameter in "notes.ini". To disable this feature, delete the parameter or use the value "0". If this feature is disabled then if there are any mails sitting in mail.box(s) with the status 'HOLD', and SMDReal is loaded up, those mails will not be scanned by SMDReal. They will keep sitting in the mail.box(s) until a manual scan is run on the mail.box(s). If this parameter =1 then SMDReal will scan the mail.box(s) to release those mails, right after loading up. Trend recommends the value 1.

SETTINGS	COMMENTS
SMDEMDEBUG	To enable the debug log for the Extension Manager and EMFilter add 'SMDEMDEBUG=1" to notes.ini. The debug logs for the Extension Manager and EMFilter are created in the smdtemp folder as smdext.dbg and smdemf.dbg. Please Note: this operation requires domino restart. Also some operations of the EMFilter also generates a file called nSMDemf_YYYYMMDD.dbg.
eManagerDebugEnable	Add this entry in notes.ini: eManagerDebugEnabled=1 to enable the eManager debug debug file SMD_eMgrYYYYMMDD.dbg
TMUFEDebug	Add this entry in notes.ini: TMUFEDebug=X to enable TMUFE debug. where X: = "1-5" with higher number more details debug log file is nSMDreal_YYYYMMDD.dbg NOTE: To trigger TMUFE debugging, nSMDreal must be loaded with the –debug option
DisableSecureupdate	By default SMLD uses secure update. It download and verify the.sig files for components. To disable this add DisableSecureUpdate=1 to notes.ini.
SMDSkipScanBySize_MB	This entry will determine the maximum size to be skip.
SMDBackupInfected	Add SMDBackupinfected=1 in the notes.ini to copy blocked messages to qurantiane database.

5. Backup and Disaster Recovery

5.1. Scanmail Databases

The following databases can be backed up for the purpose of disaster recovery. Please not that these databases are found in the <Domino Data Directory>\smd path.

Database Name	File Name	Function
Configuration	smconf.nsf	Policy, server and Outbreak Prevention Policy settings
Quarantine	smquar.nsf	Stores messages quarantined by a scan action
Log	smvlog.nsf	ScanMail logs
Delay	smtime.nsf	Stores messages until a specified routing time
Approved	smdapproved.nsf	Stores messages that must be approved by an administrator before delivery

5.2. Scanmail Parameters in Notes.ini

In addition to the databases above Trend also recommends to backup the values of the SMD related parameters in Notes.ini. Such as:

SMDAutoReleaseMail

SMDSkipTaskList

Other parameters like ServerTasks, SMStopMail, EXTMGR_ADDINS, SMDSkipDBEvent and ScanMailCMAgentInstallPath, do not need to be backed up as those are created by the install of SMD.

6. Miscellaneous

6.1. Recommended Scan-Exclusion List

The following folders should be excluded

<Domino Data Directory>\smd

<Domino Data Directory>\smdtemp

\Program Files\Trend Micro\Scanmail for Domino\

The temp folders by default are located at:

Mail Scan -	<Domino Data Directory>\smd\smtemp\mailtemp\
Manual Database Scan -	<Domino Data Directory>\smd\smtemp\dbtemp\
Real-time Database Scan -	<Domino Data Directory>\smd\smtemp\reptemp\
Scheduled Database Scan -	<Domino Data Directory>\smd\smtemp\ptemp\

By excluding the “<Domino Data Directory>\smd” folder above, will take care of these exclusion also. But if the client has customized these locations then those paths also need to be excluded from the local AV software running on the SMD server.

To find out these paths on the server go to the “Configurations->Server Settings” in smconf.nsf.