INTEGRATING DOMINO WITH AN ICAP SERVER

Marianna Tomasatti - marianna.tomasatti@gttech.it
Roberto Boccadoro - roberto.boccadoro@eldeng.it
WELCOME TO THE YELLOW RESTAURANT!
THE SPECIAL OF TODAY IS....
THE CHEFS

Roberto Boccadoro
Former Lotus / IBMer
Working with Lotus/IBM/HCL
Collaboration since 1994
Many years of experience with Domino, Sametime, Connections, Docs and other HCL products
HCL Ambassador
OpenNTF Director

Marianna Tomasatti
Working with Domino since 1997
Lots of experience as System and Domino Administrator
THE MASTER CHEF WHO HELPED US

Daniel Nashed

If you know him, you don’t need his bio 😊
If you don’t know him, too bad, we will need too many slides to tell you what he does
THE INGREDIENTS

1) HCL Domino
   Minimum version 12.0.2

2) An ICAP server
THE RECIPE

• Run mailscan for the first time to create cscancfg.nsf
• Create a configuration document in cscancfg.nsf
• Create a server document in cscancfg.nsf
• Run mailscan again

Official documentation
https://help.hcltechsw.com/domino/14.0.0/admin/conf_scanningattachmentsforviruses.html?
RIN MAILSCAN THE FIRST TIME

• load mailscan.

• The mailscan task starts up, creates cscancfg.nsf on the administration server, creates a replica on the current server, and shuts down.
CSCANCFG.NSF

• Open it and create a configuration
CONFIGURATION

• In the basic tab type a name for the configuration.

You can’t assign it to any server yet, because you have not created one. It will be done in the next steps.
CONFIGURATION

• In the mail scan tab you define the options
VIRUS DETECTED ACTION

• Choose from the following options to specify what happens to a message when a virus is detected:

  • **Discard message with notification** - This option deletes the original message content. The message is sent with a Subject prefix that contains the text configured in the Subject prefix message discarded field and body text configured in the Body text message discarded field.

  • **Clean message and deliver** - This option deletes viruses from infected attachments. The message is sent with a Subject prefix that contains the text configured in the Subject prefix virus found field and the contents of any infected attachments are replaced with the text configured in the Virus attachment text field.

  • **Silently discard the message** - With this option, the recipient does not receive the message or any notification about a virus.
Domino mail servers might rarely process a MIME message that contains unencoded content. Although such content is not technically an attachment, when the document is opened in Notes it is manifested as an attachment. We refer to such data as an embedded attachment. Starting in Domino 14.0 you can configure virus scanning to scan such attachments by checking Scan embedded attachments.
QUARANTINE ACTION

• Quarantine original message: Original messages with viruses are saved in Domino Content Scan Quarantine (cscanquarantine.nsf).
• Do not quarantine
MESSAGE LOG OPTION

<table>
<thead>
<tr>
<th>Message log option:</th>
<th>Log database:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log attachments with viruses only</td>
<td>Log all attachments</td>
</tr>
</tbody>
</table>

Specify with attachments should be logged.
## Log and Quarantine Options

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log database</td>
<td>cscanlog.nsf</td>
</tr>
<tr>
<td>Quarantine database</td>
<td>cscanquarantine.nsf</td>
</tr>
<tr>
<td>Log retention (days)</td>
<td>40 days</td>
</tr>
<tr>
<td>Quarantine (days)</td>
<td>40 days</td>
</tr>
</tbody>
</table>
### Mail Tag for Notifications

<table>
<thead>
<tr>
<th>Mail Tag for Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject prefix scanned:</td>
</tr>
<tr>
<td>Subject prefix virus found:</td>
</tr>
<tr>
<td>Subject prefix message discarded:</td>
</tr>
<tr>
<td>Virus view icon:</td>
</tr>
<tr>
<td>Virus attachment text:</td>
</tr>
<tr>
<td>Body text message discarded:</td>
</tr>
</tbody>
</table>

- **Subject prefix scanned:** The text to display before the subject in a sent message indicating that the message was scanned for viruses and none were found. For example, "Virus scanned."
- **Subject prefix virus found:** The text to display before the subject in a sent message indicating that a virus was found. For example, "Virus found."
- **Subject prefix message discarded:** Applies when the virus detected action is "Clean message and deliver."
- **Virus view icon:** The text to display before the subject in a sent message indicating that the message was discarded because it contained a virus. For example, "Message blocked due to virus." Applies when the virus detected action is "Discard message with notification."
- **Virus attachment text:** A number representing the icon to use in a mail view to indicate a message had a virus. (Hint, red envelope is 131)
- **Body text message discarded:** The text to display inside an attachment that has been cleaned due to a virus. For example, "Virus found! Attachment text replaced." Applies when the virus detected action is "Clean message and deliver." If unable to double-click the attachment to open it, open it from a text editor to read the message.
- **Body text message discarded:** The text to display in the body of sent message indicating that the message was discarded because it contained a virus. For example, "Virus found! Message discarded." Applies when the virus detected action is "Discard message with notification."
You must know the port the ICAP server uses, default for ICAP is 1344 but it may be different.

You must know the name of the service your vendor uses. E.g. Trend Micro is “interscan”.

The demo server I use is “clamav”.

Now is empty, we have to import the trusted root via Cscan connection.
IMPORTING TRUSTED ROOTS

• This process requires that certstore.nsf is present on the server
IMPORTING TRUSTED ROOTS

• open cerstore.nsf on the same server on which you opened cscancfg.nsf, and open the Trusted Roots view.

• validate the trusted root as follows:
  • Expand the ICAP category. Any new trusted roots added by the preceding steps have been added under that category, in a pending state.

• Open the document for a root certificate that you want to examine. Verify that the Status is Pending Validation and the Certificate status is Valid
• Use the action Mark trusted root validated to validate the trusted root.
CREATE A SERVER

• Open cscancfg.nsf and go in the Servers view

• Click on New Server
NEW SERVER

When you first create a server document, the Health status field displays as Pending validation. It remains that way until the mailscan task runs with a valid configuration and connects to the ICAP server. At that point, the status should be updated to Service Validated.
TEST THE SOLUTION

• Go to the EICAR web site and download the test virus https://www.eicar.org/download-anti-malware-testfile/
• Send an email with the virus

What is the eicar test file?
The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO), to test the response of computer antivirus programs. Instead of using real malware, which could cause real damage, this test file allows people to test anti-virus software without having to use a real computer virus.