



MAILWATCHER Filter Engine

MODULE : MWADVT



Lotus Notes Version : 5.x, 6.x, 7.x, 8.x
Engine Version : 4.1.1.126+



Introduction

Le moteur de filtre de MailWatcher, connu sous l'acronyme MWADVT (**Mail**Watcher **AD**vanced **T**ask) permet de mettre en œuvre une série d'actions sur les messages en transit au niveau des serveurs de messagerie.

Cette mécanique est conçue de manière à ce que vous puissiez implémenter vos propres politiques de gestion des flux.

Elle s'appuie sur un système d'interprétation de règles.

Les règles comportent à la fois le contexte d'exécution et les actions à entreprendre. Elles ont un niveau de priorité. Le cas échéant plusieurs règles peuvent être appliquées à un même message.

Les serveurs de messagerie étant très sollicités, principalement au niveau des accès disque, le moteur de filtre utilise et gère son propre cache en mémoire. Ce cache se met à jour automatiquement et de manière périodique.

Certaines actions sont sécurisées, c'est notamment le cas des fonctions de copie qui verrouillent les accès en lecture et vérifie la bonne exécution du processus.

Le moteur de filtre fait partie de la suite des modules MailWatcher, il est au cœur des décisions, pour cela il s'appuie sur des modules opérant sur les messages avant et après lui.

Les modules amont ont des fonctions d'analyse de contenu, ou bien de traitement antivirus. Ils donnent des verdicts. Ces informations deviennent des critères qui seront pris en compte par le moteur de filtre.

Les modules qui se trouvent en aval réalisent des actions relativement complexes, telles que la compression ou des opérations de nettoyage antivirales.

Enfin, si vous le souhaitez, le moteur de filtre est capable d'enregistrer toutes ces opérations dans des bases statistiques.



Définition du contexte d'une règle

Avant de définir les actions, vous devez définir le contexte, autrement dit, les émetteurs et/ou les destinataires qui seront concernés par les actions d'une règle.

Un mail peut être défini comme suit :

- 1 : Émetteur (From)
- 1,N : Destinataire(s) (To)
- N : Attributs, Champs TEXT, TEXTLIST, DATE, NUMBER,...
- 0,N : Pièces jointes

Le contexte est d'abord une combinaison : FROM et TO.

MailWatcher va analyser chaque combinaison en formant des couples

- (Émetteur * Destinataire [i=1,N])

Un mail émis vers 10 personnes sera traité comme un ensemble de 10 messages différents.

Par exemple le couple (FROM * TO(5)) activera une règle de non routage, ce qui n'empêchera pas (forcément) les 9 autres destinataires de recevoir le message.

Au contexte {FROM et TO} vous pouvez ajouter d'autres conditions préalables à l'application d'une règle. En fait le contexte réel est formé par trois fonctions booléennes qui devront toutes être vérifiées (vraie) pour continuer et donc appliquer les actions de la règle.

Contexte réel = { FROM et TO(i) et Formula }

Formula = fonction programmable basée sur l'interpréteur Lotus Macro Formula.

Si aucune Formula n'est donnée, le code en utilise une par défaut : @TRUE, qui renvoie toujours « vrai »



Le typage des adresses

Le contexte est défini comme étant la combinaison de { FROM et TO et Formula }, cela dit FROM et TO peuvent avoir des formes différentes { User, Group, Meta, Meta Group }, on référence avec des paramètres ces adresses comme étant potentiellement d'un type particulier.

Soit l'adresse est un utilisateur, ou elle est membre d'un groupe, ou encore elle est conforme à une chaîne de caractères formant une expression régulière, ou bien elle est membre d'un groupe dont les entrées peuvent être définies avec des expressions régulières.

La clause FROM et la clause TO doivent être vérifiées. Le type de paramètre permet de modifier le mode de validation. Dans les définitions suivantes, les types pour - FROM Émetteur - s'appliquent de la même manière à TO - Destinataire -.

Type 'User' : L'adresse de l'émetteur du mail - FROM - doit figurer dans la liste des alias possibles de l'utilisateur, cela inclus également l'adresse Internet et l'adresse de renvoi vers Internet 'ForwardEmailAddress'.

Type 'Group' : L'adresse de l'émetteur doit être membre du groupe déclaré. Sont ajoutés virtuellement aux membres du groupe l'ensemble des alias possibles, ce qui donne une liste de membre de type 'User'

Type 'Meta' : L'adresse de l'émetteur est comparée au «modèle ou pattern ou expression régulière» définie.

Type 'Meta Group' : L'adresse de l'émetteur doit être membre du groupe défini, l'évaluation se fait comme pour le type 'Meta'.

Les exceptions

Les exceptions sont évaluées si les clauses { FROM et TO et Formula } sont toutes vraies.

Les exceptions peuvent concerner FROM et/ou TO. Respectivement Except_FROM et Except_TO.

La règle ne s'applique pas si l'une des Exceptions est vraie, autrement dit, si la condition {Except_FROM ou Except_TO} est vraie.



Les actions d'une règle

Les actions sont combinables, certaines auront même la capacité de modifier le mail, le moteur de filtre maintient toujours une version intacte pour l'application ou non d'autres règles. La non application de règle signifie que le message est distribué normalement.

Actions de copie

Cette action est faite en amont de toute modification. Elle intervient sur une version intact du message d'origine.

Les fonctions de copie ajoutent des champs de type READERS aux messages déposés dans les bases Lotus prévues. Cela nécessite d'avoir le rôle [Admin] au sein de ces bases pour accéder au contenu, sauf si l'utilisateur est lui même l'émetteur ou l'un des destinataires.

En cas d'échec de journalisation les messages sont maintenus en attente 'Hold' dans les mail.box. Le moteur de filtre tentera régulièrement de retraiter ces messages sans intervention extérieure.

Zone de configuration des actions dans la masque 'Filter Rules' :

[- Automatic copy, kill and/or reprocess -]		[- Comments / Warning, additional parameters -]	
Copy email to :	<input type="text"/>	Include Doc Link :	<input type="text"/>
Move To Folder :	<input type="text"/>	Keep ReturnReceipt :	<input checked="" type="radio"/> Yes <input type="radio"/> No
Journal into Mail-in Db :	<input type="text"/>	Default view :	<input type="text"/>

Au moment de la copie il est possible de classer les messages dans des dossiers. Ces dossiers seront créés s'ils n'existent pas. Pour définir une hiérarchie de dossier vous devez utiliser la syntaxe suivante :

- A\B\C

Avec C un sous dossier de B lui même un sous dossier de A

Keep ReturnReceipt : Y/N pour supprimer ou conserver les accusés réception des messages au moment de leur copie.



Actions de suppression & sauvegarde

Les opérations de suppression n'impactent que le message pour un couple (FROM * TO(i)). Une copie intégrale est toujours préservée pour les autres couples (FROM * TO).

Le masque propose une série d'options permettant de faire des retraits, soit de pièces jointes soit de champs. Le retrait de pièces jointes peut – éventuellement - s'appuyer sur les traces laissées par les modules AntiVirus MWKAVSCAN ou par les modules de détection des « vrais » type de fichier MWGFILE (modules amont). Vous pouvez aussi donner des champs de manière explicite, par exemple : ReturnReceipt.

Delete email	: <input type="radio"/> Yes <input checked="" type="radio"/> No		
Detach attachments	: <input checked="" type="radio"/> Yes <input type="radio"/> No	Detach directory Include host file link	: <input type="text"/> - Extension : <input type="text"/>
Remove attachments	: <input checked="" type="radio"/> Yes <input type="radio"/> No	Extension to remove (or) Field as List of file	: <input type="text"/>
Remove Fields	: <input type="text"/>		

Il est possible de sauvegarder les pièces jointes sur disque (detach) dans un répertoire, cela en définissant éventuellement les pièces jointes concernées par leurs extensions. Ce paramétrage est également disponible dans les cas de suppression.

Actions de routage

Le fait de mettre « No » à 'Deliver Email To' provoque le retrait de l'adresse TO(i) de la liste des destinataires – Recipients.

NB : Les champs d'affichage des adresses SendTo, CopyTo, BlindCopyTo ne sont pas modifiés.

[-- Check addresses / add new recipients --]		[-- New routing conditions --]	
Deliver email to > (To)	: <input type="radio"/> Yes <input checked="" type="radio"/> No	Deliver email to > (To) vote	: [<input type="text"/> Majority <input type="text"/>]
Return email to > (From)	: <input type="radio"/> Yes <input checked="" type="radio"/> No	Route thru Domain	: <input type="text"/>
Forward email to >	: <input type="text"/>	Switch Importance To Low	: <input type="radio"/> Yes <input checked="" type="radio"/> No

'Forward Email to' permet d'ajouter de manière « invisible » un destinataire (ou un groupe)

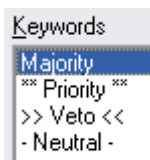
'Route thru Domain' permet de modifier à la volée le domaine de routage, ainsi les adresses prennent la forme suivante : abc@NouveauDomain.

Cette fonctionnalité est très utile pour forcer le passage d'un message par un serveur particulier.



Notion de vote

Sachant que plusieurs règles peuvent donner des avis – éventuellement contradictoires – on part du principe qu'un mail émis est a priori distribué vers les destinataires. Chaque règle vote avec un poids (Majority par défaut).



- Majority = 1
- Priority = $N (\text{Max} - \text{Rang})$
- Veto = Max
- Neutral = 0

La valeur de 'Max' est le nombre de règle active

Rang est la position de la règle dans une liste triée par priorité.

Exemple de 'Priority' pour la règle au rang 2 sur 10(max) = $10 - 2 = 8$.

Si la règle vote POUR (' Deliver Email to' = Yes) alors la valeur du vote est positive : 8

Si la règle vote CONTRE ('Deliver Email To' = No) la valeur est négative : -8

À la fin du processus quand toutes les règles applicables l'ont été, un destinataire est retiré de la liste si le total des votes est négatif.

Ces utilisateurs dits « BlackListés », sont conservés dans des zones spéciales permettant de mettre en œuvre une forme de notification automatique (activation sous contrôle).

Actions de modification de l'aspect



Les fonctions de modifications supportent l'adjonction de données de type TEXT RICH et de type TEXT composable à partir des éléments du message d'origine. Vous pouvez désactiver le paramétrage sans avoir à supprimer les valeurs saisies, pour cela il suffit de mettre 'No' au paramètre : 'Append at the End of the Body'.

Append at the end of Body : ☒ Yes ☐ No

[--Append content (Rich Text) --]
If not possible use attachment:

Subject prefix :

Append to original mail 'Body' :
- MailWatcher Disclaimer -



Keep
your mail
ready
for business

À la suite du champ TEXT RICH vous pouvez ajouter des informations via un autre champ TEXT qui est composé -éventuellement- à partir de données issues du document d'origine.

Pour cela il suffit de placer le nom des champs concernés entre accolades. Il existe une valeur spéciale: {MW_TO} qui est le TO(i) courant, celui de la liste des couples (FROM* TO(i))

Append at the end of Body : ☒ Yes ☐ No

Subject prefix :

Append RICH TEXT to original mail 'Body' :

Append TEXT supporting macro {FIELD} to original mail 'Body' :

test modification du body pour signaler à {FROM} que son mail {Subject} pour le destinataire {MW_TO}
a bien été reçu le {PostedDate}... voilà
saut de ligne

fin du message ici ->

Les champs supportés : TEXT, TEXT LIST, NUMBER, DATE.

NB : Les dates sont affichées en texte avec le format YYYY/MM/DD, ce format est précisé à l'affichage.



Exemple avec le paramètre ci-dessus

NB : les valeurs sont mises en gras pour faciliter la lecture de la documentation uniquement.

test modification du body pour signaler à **CN=admin notes_853_x64/O=mwatcher** que son mail **test sujet R22** pour le destinataire **CN=user test2/O=mwatcher@mwatcher** a bien été reçu le (YYYY/MM/DD) : **2012/12/14**... voilà
saut de ligne

fin du message ici->

NB : pour sauter des lignes dans ce paramètre TEXT, ajoutez des espaces vides avant le retour chariot.

Actions de notifications

C'est l'une des fonctions les plus riches du moteur, elle permet de re-générer un message en s'appuyant sur le message d'origine puis de le distribuer, soit à l'émetteur, soit au destinataire To(i) soit à des tiers, et/ou à des adresses figurant dans des champs du message d'origine.

[..... Compose a new message]	
Send this notification/email : <input checked="" type="radio"/> Yes <input type="radio"/> No	
From address : <input type="text" value="Mail/Watcher"/>	Subject prefix : <input type="text" value="Courrier non autorisé"/>
Forward email to > : <input type="text" value=""/>	Append the original mail 'Body' : <input type="radio"/> No <input checked="" type="radio"/> Bottom <input type="radio"/> Top
Deliver email to (From) : <input type="text" value=""/>	Remove attachments : <input checked="" type="radio"/> Yes <input type="radio"/> No
Deliver email to (To) : <input type="radio"/> Yes <input checked="" type="radio"/> No	
Message : <i>Votre message n'a pas été distribué.</i> <i>Vous n'êtes pas autorisé à utiliser cette liste de diffusion.</i> <i>Pour toute information prière de vous adresser à votre hiérarchie.</i>	

NB : Par défaut la notification est à destination de l'émetteur : 'Deliver email to' (From), ce qui se configure en laissant cette zone vide.

La zone de texte 'Message' peut être placée au dessus ou en dessous du Body d'origine.

- Append the original mail Body 'No', Bottom, Top.

NB : Le masque de saisie comporte de nombreux messages d'assistance, placez le curseur sur les zones de texte des paramètres pour les afficher.



Comme pour le champ BODY, les paramètres FROM, TO de la notification peuvent être des valeurs explicites ou dynamiques.

Les données dynamiques sont définies entre accolades {abc} et proviennent des champs du document d'origine. Ces valeurs peuvent être multiples, utilisez la virgule comme séparateur, attention les blancs laissés entre les valeurs seront conservés, donc saisissez, sans espace, comme ceci : {abc},{efg} le cas échéant.

Exemple de règle avec adresses dynamiques et champs d'information

Send this notification/email : <input checked="" type="radio"/> Yes <input type="radio"/> No		[----- Compose a new message -----]	
From address :	MailWatcher	Subject prefix :	Delivery failure
Forward email to > :	NOHEADER	Append the original mail 'Body' :	<input type="radio"/> No <input checked="" type="radio"/> Bottom <input type="radio"/> Top
Deliver email to (From) :	{ReplyTo},{from}	Remove attachments :	<input checked="" type="radio"/> Yes <input type="radio"/> No
Deliver email to (To) :	<input type="radio"/> Yes <input checked="" type="radio"/> No	Field (values) appended as info :	UpdatedBy: From
Append Field Info :	<input checked="" type="radio"/> Yes <input type="radio"/> No	Field (Titles) appended as info :	----- Ceux qui ont fait des modifications -----; Sender

TEST MESSAGE NOTIFICATION
RICH TEXT

- Forward Email To : {champ},{champ},ValeurDirect
- Deliver email to (FROM) : ce champ laisser vide prendra la valeur de FROM, mais si voulez utiliser {ReplyTo} vous devez le préciser.

En bas de la notification, le corps du message peut recevoir des informations supplémentaires, les champs supportés sont : Text, Text List.

Le formatage des ces informations se fait via les champs suivant :

- Field (Values) appended as info : crée un tableau avec les valeurs des champs
- Field (Titles) Appended as info : Définition des entêtes du tableau

Vous pouvez saisir jusqu'à trois valeurs. Il y a une correspondance entre les deux champs. Dans VALUES vous donnez les champs comportant les valeurs et dans TITLES donnez les titres de la première colonne du tableau.



Exemple de notification avec tableau d'information et texte dynamique

**TEST MESSAGE NOTIFICATION
RICH TEXT**

le corps

les PJ

dcontrlr201203291153.out dcontrlr201203291519.out dcontrlr201203291530.out dcontrlr201203291545.out dcontrlr201204031233.out

Fin

test modification du body pour signaler à CN=admin notes_853_x64/O=mwatcher que son mail test sujet R21 a bien été reçu le (YYYY/MM/DD) : 2012/12/14... voilà
saut de ligne

fin du message ici ->

----- Ceux qui ont fait des modifications -----	
	Sender
!	CP=admin notes_853_x64/O=mwatcher
!	CP=admin notes_853_x64/O=mwatcher

Actions combinées (Copie & notification)

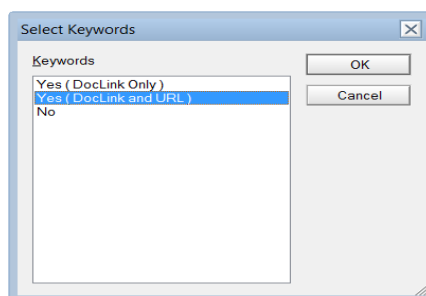
Le fait d'avoir activé la fonction de 'Copie avec 'DocLink' vous permettra d'intégrer automatiquement ce lien dans la partie supérieure du corps de la notification.

[-- Comments / Warning, additional parameters --]

Include Doc Link : ☒ Yes (DocLink Only)  Default view : ☒ \$All 

Keep ReturnReceipt : ☒ Yes ☐ No

NB : Le masque de saisie propose également l'ajout de DocLink sous sa forme native, accompagné de son équivalent en format URL.





Les performances

Le moteur de filtre utilise un cache mémoire pour éviter de faire des requêtes vers le carnet d'adresse public. Cela dit, les groupes peuvent être modifiés et les règles de filtre doivent s'y référer.

Le cache est mis à jour à chaque rechargement ou cycle de rafraîchissement. Il stocke le contexte des règles, mais pas les actions qui peuvent être modifiées à la volée :

- FROM-TO-FORMULA
- Le contenu des groupes figurant dans les clauses FROM, TO, Except_From, Except_To.

À chaque rafraîchissement du cache, MWADVT laisse une trace du contenu des groupes résolus récursivement dans un fichier texte, nommé '**DumpBlackList.txt**'. Ce fichier est stocké dans le répertoire programme du serveur.

Format du fichier de Dump/Cache

[Adresse ou alias (shortname, internet adresse..)]
Groupe1, Groupe2,...

Par défaut les mises à jour du cache se font toutes les 180 minutes. Vous pouvez modifier cette valeur avec la variable suivante dans le notes.ini du serveur :

MWREFRESHVIEWMODE = n (minutes)

ou

MWREFRESHVIEWMODE=never (jamais remis à jour)

Pour provoquer la prise en compte immédiate d'une nouvelle règle ou d'un changement de contexte (FROM,TO,FORMULA,EXCEPT) tapez la commande suivante à la console serveur

```
> TELL MWADVT QUIT  
> LOAD MWADVT
```

Attention Domino gère également un cache mémoire, cela concerne également les groupes, il sera peut être parfois nécessaire de faire :

```
> dbcach flush
```