



MAILWATCHER Filter Engine

MODULE : MWADVT



Lotus Notes Version : 5.x, 6.x, 7.x, 8.x



Introduction

Le moteur de filtre de MailWatcher, connu sous l'acronyme MWADVT (**M**ail**W**atcher **A**Dvanced **T**ask) permet de mettre en oeuvre 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 s'appuie sur un cache 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 de l'action.

Le moteur de filtre fait partie de la suite des modules MailWatcher, il est au coeur des décisions, certains modules travaillant en amont, tel que l'analyse de contenu, les scanners anti-virus, ces modules donnent des verdicts et deviennent des critères de filtrage. Les modules aval intègrent des actions relativement complexes, telles que la compression ou les fonctions de nettoyage de virus.

Définition du contexte d'une règle

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

Un mail peut être défini comme suit :

- 1 : Emetteur (From)
- 1,N : Destinataire(s) (To)
- Un corps (sujet, corps, champs divers)
- 0,N : Pièces jointes

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

MailWatcher va analyser chaque combinaison Emetteur * Destinataire (i , i=1,n).

Ainsi un mail émis vers 10 personnes sera vu comme 10 messages différents. Par exemple le couple {FROM * TO(5) } active une règle de non routage, cela n'empêchera pas (forcément) les 9 autres destinataires de recevoir le message.

Tous les messages émis par FROM vers TO ne sont pas identiques. Vous pouvez ajouter une d'autres conditions à l'application d'une règle. En fait le contexte est formé par trois fonctions booléennes qui devront être vraies pour continuer l'interprétation de la règle.

Contexte = FROM & TO(i) & Formula

Formula = fonction programmable basée sur l'interpréteur de fonctions de Lotus Notes (Lotus Macro Formula).

From: ☒ User ☐ Group ☐ Meta ☐ Meta Gp (?)

To: ☒ User ☐ Group ☐ Meta ☐ Meta Gp

Place the formula in (...) to be able to associate it with others in a OR sequence.
(From & To match) condition AND formula **returns TRUE** is required to apply the Black / Red List rule actions.

Except From: ☒ User ☐ Group ☐ Meta ☐ Meta Gp

Except To: ☒ User ☐ Group ☐ Meta ☐ Meta Gp



Le typage des adresses

Le contexte est défini comme étant la combinaison de { FROM*TO*Formula }, cela dit FROM et TO peuvent avoir des formes différentes { User, Group, Meta, Meta Group }.

La clause FROM (identique pour TO) doit être vérifiée, le type permet de modifier le mode de validation.

User : L'émetteur du mail – FROM – doit figurer dans la liste des alias possibles, cela inclus également l'adresse Internet et le ForwardEmailAddress.

Group : L'émetteur – vu comme [User] doit être membre du groupe déclaré dans la paramètre FROM.

Meta : L'émetteur – la valeur contenu dans la chaîne de caractère est évaluée par rapport au « modèle, pattern, expression régulière » défini par le paramètre.

Meta Group : L'émetteur doit être membre du groupe défini par le paramètre, l'évaluation utilise un algorithme de type Meta.

Les exceptions

Les exceptions sont évaluées une fois que les clauses { FROM * TO * Formula } sont toutes vraies.

Les exceptions peuvent être posées sur FROM et TO; respectivement Except_From, Except_TO.

La règle ne s'applique pas si l'une des Exceptions est vraie, autrement dit Pas d'application si 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 tout en préservant une version intacte pour l'application ou non d'autres règles qui auront une influence sur la distribution etc...

Actions de copie

Cette action est faite en amont de toute modification. Elle intervient sur un message avant toutes modifications que pourraient effectuer le router natif Domino.

Les fonctions de copie ajoutent des champs de type READERS. Cela nécessite d'avoir le rôle [Admin] pour y accéder bien entendu si l'utilisateur ne figure pas déjà dans les champs FROM ou Destinataire. La base Lotus Notes de copie peut être également protégée par son ACL.

Les fonctions de Journalisation, sauvegardent les champ FROM et BlindCopyTo dans JRN_FROM et JRN_BlindCopyTo.

NB : En cas d'échec de journalisation les messages seront 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 : 		Include Doc Link :  No 	Default view : 
Move To Folder : 		Keep ReturnReceipt :  Yes  No	
Journal into Mail-in Db : 			



Actions de suppression

Les opérations de suppression n'impactent que le message dans son contexte FROM * TO(i).
Une copie intégrale est 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 s'appuyer sur les traces laissées par les modules AntiVirus ou les modules de détection des « vrais » type de fichier (modules amont).

Delete email	: <input type="radio"/> Yes <input checked="" type="radio"/> No		
Detach attachments	: <input checked="" type="radio"/> Yes <input type="radio"/> No	Detach directory	: <input type="text"/> Extension : <input type="text"/>
		Include host file link	: <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"/>		

Actions de routage

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

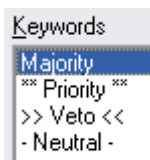
'Route thru Domain' permet de modifier à la volée le domaine de routage, ainsi les adresses prennent la forme suivante : abc@NouveauDomain.

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 (Max – Rang)

Veto = Max

Neutral = 0.

Max = Nombre de règle active

Exemple de 'Priority' pour la règle au rang 2 sur 10 = 8.

Si la règle vote POUR = ' Deliver Email to' = Yes alors la valeur du vote est positif

Si la règle vote CONTRE = 'Deliver Email To' = No » la valeur est négative.

À la fin du processus quand toutes les règles applicables l'ont été, un destinataire est retiré de la liste si le vote < 0.

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



Actions de modification de l'aspect

Les fonctions de modifications supportent l'adjonction de Text Rich.

Vous pouvez désactiver le paramétrage sans avoir à supprimer les valeurs saisies.

-- Append content (Rich Text) --


Append at the end of Body : ☒ Yes ☐ No


If not possible use attachment:

Subject prefix :

Append to original mail 'Body' :

- MailWatcher Disclaimer -


MAILWATCHER
EMAIL ARCHITECTS



Keep
your mail
ready
for business

pour cela il suffit de mettre 'No' comme paramètre à : 'Append at the End of the Body'.



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 les valeurs d'origines.

[..... Compose a new message]			
Send this notification/email : <input checked="" type="radio"/> Yes <input type="radio"/> No			
From address	: <input type="text" value="MailWatcher"/>	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), 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.

Placez le curseur sur les zones de texte pour obtenir des informations supplémentaires.

Subject prefix		: <input type="text" value="Courrier non autorisé"/>
The subject header will be appended in front of the original subject. Ex : Delivery Failure => Delivery Failure : Original Subject..		<input checked="" type="radio"/> Bottom <input type="radio"/> Top <input type="radio"/> No

Actions combinées (Copie & notification)

Le fait d'avoir activer la fonction de 'Copie avec 'DocLink' vous permettra d'intégrer automatiquement ce lien dans la partie supérieure du texte saisie.

[-- Comments / Warning, additional parameters --]		
Include Doc Link	: <input type="text" value="Yes (DocLink Only)"/>	Default view : <input type="text" value="\$All"/>
Keep ReturnReceipt	: <input checked="" type="radio"/> Yes <input type="radio"/> No	



Les performances

Le moteur de filtre utilise un cache mémoire. Il stocke le contexte des règles :

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

À chaque rafraîchissement du cache, MWADVT laisse une trace du contenu des groupes.

Cf : fichier texte 'DumpBlackList.txt' dans le répertoire programme du serveur.

Format du fichier

[Adresse]

Gr1, Gr2.....

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

Pour provoquer la prise en compte immédiate d'une nouvelle règle ou d'un changement de contexte tapez la commande suivante à la console serveur :

> TELL MWADVT quit

> LOAD MWADVT.