

Que signifie le travail maximal par erreur d'analyse d'expression ?

Contenu

[Introduction](#)

[Informations générales](#)

[Exemples de messages d'erreur « maximum work by expression »](#)

[Journaux de messagerie](#)

[Suivi des messages](#)

[Défaillance de l'application](#)

[Dépannage](#)

[Dictionnaires](#)

[Via l'interface utilisateur graphique](#)

[Via l'interface de ligne de commande](#)

[Filtres de contenu](#)

[Via l'interface utilisateur graphique](#)

[Via l'interface de ligne de commande](#)

[Filtres de messages](#)

[Via l'interface utilisateur graphique](#)

[Via l'interface de ligne de commande](#)

[Informations connexes](#)

Introduction

Ce document décrit la signification du message d'erreur « Problème d'analyse : travail maximum par expression/limite de données dépassée » et comment résoudre les problèmes qui en découlent.

Informations générales

Le message d'erreur « Problème d'analyse : travail maximum par expression/limite de données dépassée » peut être dû à des entrées de dictionnaire, des filtres de contenu ou des filtres de messages qui ont de nombreuses correspondances d'expression régulière (RegEx). Cette erreur peut se produire pour les raisons suivantes :

- Lorsqu'un grand nombre d'entrées sont répertoriées dans un dictionnaire.
- Expressions régulières (RegEx) contenant des correspondances de longueur variable (Exemple : `.*`, `.+` ou `.{5,}`).

Les dictionnaires volumineux et les expressions régulières correspondantes à grande échelle nécessitent des ressources système importantes et doivent être évités.

Exemples de messages d'erreur « maximum work by expression »

Journaux de messagerie

Thu Feb 15 12:01:20 2021 Warning: MID #####,
Message Scanning Problem: maximum work per expression/data limit exceeded

Suivi des messages

Message ##### encountered message scanning error: maximum work per expression/data limit exceeded

Défaillance de l'application

```
An application fault occurred: ('egg/filters.py expand_short_url|1570',  
<type 'exceptions.RuntimeError'>', 'maximum work per expression/data limit exceeded',  
[egg/omh.py queue_worker_thread|3733] [egg/omh.py process_item|4209]  
[egg/omh.py pass_spamcheck|6402] [egg/omh.py update_url_reporting_info|4951]  
[egg/filters.py get_web_info|1810] [egg/filters.py fetch_urlinfo|1480]  
[egg/filters.py get_url_info|1658] [egg/filters.py get_expanded_url_list|1606]  
[egg/filters.py expand_short_url|1570]') MID: #####
```

Dépannage

Dictionnaires

Via l'interface utilisateur graphique

1. Connectez-vous à l'interface utilisateur graphique de votre passerelle de messagerie sécurisée.
2. Passez le curseur sur **les stratégies de messagerie**.
3. Cliquez sur **Dictionnaires**.
4. Consultez les dictionnaires et les entrées.

Via l'interface de ligne de commande

```
> dictionaryconfig
```

```
Currently configured content dictionaries:
```

```
1. Test
```

```
Choose the operation you want to perform:
```

- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
- CLUSTERSET - Set how content dictionaries are configured in a cluster.
- CLUSTERSHOW - Display how content dictionaries are configured in a cluster.

```
[ ]>
```

Consultez les dictionnaires et les entrées.

Filtres de contenu

Via l'interface utilisateur graphique

1. Connectez-vous à l'interface utilisateur graphique de votre passerelle de messagerie sécurisée.
2. Passez le curseur sur **les stratégies de messagerie**.
3. Cliquez sur **Filtres de contenu entrant** ou **Filtres de contenu sortant**.
4. Vérifiez les filtres.

Via l'interface de ligne de commande

```
> policyconfig
```

```
Would you like to configure Incoming Mail Policy or Outgoing Mail Policies or Match Headers Priority?
```

1. Incoming Mail Policies
2. Outgoing Mail Policies
3. Match Headers Priority

```
[1]> 1 <- Enter 1 or 2
```

```
Incoming Mail Policy Configuration
```

```
Name: Anti-Spam: Anti-Virus: Advanced Malware Protection: Graymail: Content Filter:
```

```
Outbreak Filters: Advanced Phishing Protection
```

```
-----  
DEFAULT Off Sophos Off Off Enabled
```

```
Retention Time: N/A
```

```
Virus: 15 minutes
```

```
Choose the operation you want to perform:
```

- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
- CLUSTERSET - Set how Incoming Mail Policies are configured in a cluster
- CLUSTERSHOW - Display how Incoming Mail Policies are configured in a cluster

```
[ ]> filters
```

```
Defined filters:
```

1. example_filter_one
2. example_filter_two

```
Choose the operation you want to perform:
```

- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter

Vérifiez les filtres. Répétez 'l' pour les filtres de contenu sortants si nécessaire.

Filtres de messages

Via l'interface utilisateur graphique

Non disponible.

Via l'interface de ligne de commande

```
> filters
```

Choose the operation you want to perform:

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
- CLUSTERSET - Set how filters are configured in a cluster.
- CLUSTERSHOW - Display how filters are configured in a cluster.

```
[> list
```

```
Num Active Valid Name
```

```
1 Y Y example_message_filter
```

Vérifiez les filtres.

Informations connexes

- [Guides de l'utilisateur final de la passerelle de messagerie sécurisée Cisco](#)
- [Notes de version de Cisco Secure Email Gateway](#)
- [Support et documentation techniques - Cisco Systems](#)