

Grep ESA, SMA, et WSA avec l'expression régulière pour rechercher des logs

Contenu

[Introduction](#)

[Conditions préalables](#)

[Grep avec l'expression régulière](#)

[Scénario 1 : Trouvez un site Web particulier dans les logs d'Access](#)

[Scénario 2 : Tentative de trouver une extension de fichier ou un domaine de haut niveau particulière](#)

[Scénario 3 : Tentative de trouver un bloc particulier pour un site Web](#)

[Scénario 4 : Trouvez un nom d'ordinateur dans les logs d'Access](#)

[Scénario 5 : Trouvez une période spécifique dans les logs d'Access](#)

[Scénario 6 : Recherchez les messages essentiels ou d'avertissement](#)

Introduction

Ce document décrit comment employer des expressions régulières (expression régulière) avec la commande de **grep** afin de rechercher des logs.

Conditions préalables

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité Web de Cisco (WSA)
- Appliance de sécurité du courrier électronique de Cisco (ESA)
- Appliance de Gestion de sécurité Cisco (SMA)

Grep avec l'expression régulière

L'expression régulière peut être un outil puissant une fois utilisée avec la commande de **grep** de rechercher par des logs disponibles sur l'appliance, telle qu'Access se connecte, des logs de proxy, et d'autres. Vous pouvez rechercher les logs basés sur le site Web, ou n'importe quelle partie de l'URL, et de noms d'utilisateur avec la commande CLI de **grep**.

Voici quelques scénarios communs où vous pouvez employer l'expression régulière avec la commande de **grep** afin d'assister le dépannage.

Scénario 1 : Trouvez un site Web particulier dans les logs d'Access

Le scénario le plus commun est quand vous tentez de trouver les demandes qui sont faites à un site Web dans les logs d'accès du WSA.

Voici un exemple :

Connectez à l'appliance par l'intermédiaire du Protocole Secure Shell (SSH). Une fois que vous avez la demande, sélectionnez la commande de **grep** afin de répertorier les logs disponibles.

```
CLI> grep
```

Introduisez le nombre du log que vous souhaitez au **grep**.

```
[ ]> 1 (Choose the # for access logs here)
```

Écrivez l'expression régulière au **grep**.

```
[ ]> website\.com
```

Scénario 2 : Tentative de trouver une extension de fichier ou un domaine de haut niveau particulière

Vous pouvez employer la commande de **grep** afin de trouver une extension de fichier particulière (.doc, .pptx) dans un URL ou un domaine de haut niveau (.com, .org).

Voici un exemple :

Afin de trouver tout l'URLs qui finissent avec .crl, utilisez cette expression régulière :

```
[ ]> website\.com
```

Afin de trouver tout l'URLs qui contiennent l'extension de fichier .pptx, utilisez cette expression régulière :

```
[ ]> website\.com
```

Scénario 3 : Tentative de trouver un bloc particulier pour un site Web

Quand vous recherchez un site Web particulier, vous pourriez également rechercher une réponse de HTTP particulière.

Voici un exemple :

Si vous voulez rechercher tous les messages TCP_DENIED/403 pour domain.com, utilisez cette expression régulière :

```
[ ]> website\.com
```

Scénario 4 : Trouvez un nom d'ordinateur dans les logs d'Access

Quand vous utilisez le modèle d'authentification NTLMSSP, vous pourriez rencontrer un exemple où un agent d'utilisateur (Microsoft NCSI est le plus commun) envoie inexactement des qualifications d'ordinateur au lieu des identifiants utilisateurs quand il authentifie. Afin de dépister l'agent URL/User qui entraîne cette question, employez l'expression régulière avec le **grep** afin d'isoler la requête effectuée quand l'authentification s'est produite.

Si vous n'avez pas le nom d'ordinateur qui a été utilisé, utilisez le **grep** et trouvez tous les noms d'ordinateur qui ont été utilisés comme noms d'utilisateur en authentifiant avec cette expression régulière :

```
[ ]> website\.com
```

Une fois que vous avez la ligne où ceci se produit, **grep** pour le nom d'ordinateur spécifique qui a été utilisé avec cette expression régulière :

```
[ ]> website\.com
```

La première entrée qui apparaît devrait être la demande qui a été faite quand l'utilisateur authentifié avec le nom d'ordinateur au lieu du nom d'utilisateur.

Scénario 5 : Trouvez une période spécifique dans les logs d'Access

Par défaut, les abonnements de log d'accès n'incluent pas le champ qui affiche le date/heure lisible pour l'homme. Si vous voulez vérifier l'accès se connecte pendant un délai prévu particulier, se terminent ces étapes :

1. Consultation l'horodateur UNIX d'un site tel que la [conversion en ligne](#).
2. Une fois que vous avez l'horodateur, recherchez une heure précise dans les logs d'Access.

Voici un exemple :

Un horodateur d'Unix de **1325419200** est équivalent à **01/01/2012 12:00:00**.

Vous pouvez employer cette entrée d'expression régulière afin de rechercher les logs d'accès de près de 12:00 le 1er janvier, 2012 :

```
13254192
```

Scénario 6 : Recherchez les messages essentiels ou d'avertissement

Vous pouvez rechercher les messages essentiels ou d'avertissement dans tous les logs disponibles, tels que des logs de proxy ou des logs système, avec des expressions régulières.

Voici un exemple :

Afin de rechercher les messages d'avertissement dans les logs de proxy, entrez dans cette expression régulière :

CLI> **grep**

Introduisez le nombre du log que vous souhaitez au **grep**.

[]> 17 (Choose the # for proxy logs here)

Écrivez l'expression régulière au **grep**.

[]> **warning**