Como eu crio e para configurar entra uma ferramenta de segurança do email de Cisco (ESA)?

Índice

Pergunta

Como eu crio e para configurar entra a ferramenta de segurança do email de Cisco (ESA)?

Resposta

Uma característica importante dentro da ferramenta de segurança do email de Cisco (ESA) é suas potencialidades de registro. AsyncOS no ESA pode gerar muitos tipos de logs, gravando tipos de variação de informação. Os arquivos de registro contêm os registros de operações e de exceções regulares dos vários componentes do sistema. Esta informação pode ser valiosa ao monitorar Cisco ESA assim como durante o Troubleshooting de uma edição ou ao verificar o desempenho.

Os logs podem ser configurados e criado do CLI usando o comando do "**logconfig**" ou através do GUI sob a **"administração do sistema"** > do **"assinaturas log"** > **"adicionar a assinatura do log..."**

Está abaixo um exemplo de criar um LDAP debuga a assinatura do log usando o CLI:.

```
CLI> logconfig

Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
4. "brightmail" Type: "Symantec Brightmail Anti-Spam Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
```

```
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>  NEW

Choose the log file type for this subscription:
...
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. System Logs
9. CLI Audit Logs
10. FTP Server Logs
11. HTTP Logs
12. NTP logs
13. Mailflow Report Logs
14. Symantec Brightmail Anti-Spam Logs
15. Symantec Brightmail Anti-Spam Archive
16. Anti-Virus Logs
17. Anti-Virus Archive
18. LDAP Debug Logs
[1]>  18

Please enter the name for the log:
[]>  ldap_debug

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> <Press Enter>

Filename to use for log files:
[ldap.log]> <Press Enter>

Please enter the maximum file size:
[10485760]> <Press Enter>

Please enter the maximum number of files:
[10]> <Press Enter>

Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll

....

7. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
8. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
9. "ldap_debug" Type: "LDAP Debug Logs" Retrieval: FTP Poll

.....

CLI> commit
```

Está abaixo um exemplo para editar um log existente.

```
CLI> logconfig
```

```
Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
4. "brightmail" Type: "Symantec Brightmail Anti-Spam Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
.....


Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> EDIT

Enter the number of the log you wish to edit.

[]> 9

Please enter the name for the log:
[ldap_debug]>

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]>

Please enter the filename for the log:
[ldap.log]>  <Press Enter>

Please enter the maximum file size:


[10485760]> 52422880

Please enter the maximum number of files:
[10]> 100

Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
4. "brightmail" Type: "Symantec Brightmail Anti-Spam Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
....


CLI > commit
```