Configurando o impulso SCP do correio entra o ESA

Índice

Introdução

Este documento descreve como setup e configurar o impulso da cópia segura (SCP) de logs do correio (ou de outro tipos do log) de uma ferramenta de segurança do email de Cisco (ESA) a um servidor syslog externo.

Informações de Apoio

Um administrador pode receber notificações de erro que indica que os logs não podem ser empurrados usando o SCP, ou pode haver uns log de erros que indicam a incompatibilidade de chave.

Pré-requisitos

No servidor de SYSLOG que o ESA arquivos de registro SCP a:

1. Assegure que o diretório a ser usado está disponível.
2. Reveja “/etc/ssh/sshd_config” para os ajustes de AuthorizedKeysFile. Isto diz o SSH para aceitar authorized_keys e para olhar no diretório home do usuário para a picada do key_name escrita em .ssh/authorized_keys arquive: `AuthorizedKeysFile %h/.ssh/authorized_keys`
3. Verifique as permissões do diretório ser usado. Você pode precisar de fazer mudanças das permissões: As permissões no “$HOME” são ajustadas a 755.As permissões em “$HOME/.ssh” são ajustadas a 755.As permissões em “$HOME/.ssh/authorized_keys” são ajustadas a 600.

Limitações niveladas e permissões do arquivo em UNIX/Linux

Há três tipos de restrições de acesso:

```
Permission Action chmod option=====================================read (view) r or 4write (edit) w or 2execute (execute) x or 1
```

Há igualmente três tipos de limitações do usuário:

```
User ls output==================owner -rwx------group ----rwx---other -------rwx
```

Dobrador/permissões de diretório:

```
Permission Action chmod option=================================================read (view contents: i.e., ls command) r or 4write (create or remove files from dir) w or 2execute (cd into directory) x or 1
```

Notação numérica:

Um outro método para representar permissões de Linux é uma notação octal como mostrado pelo `stat - c %a`. Esta notação consiste pelo menos em três dígitos. Cada um dos três dígitos rightmost representa um componente diferente das permissões: proprietário, grupo, e outro.

Cada um destes dígitos é a soma de seus bit componentes no sistema numeral binário:

```
Symbolic Notation Octal Notation English=================================================================---------- 0000 no permissions---x--x--x 0111 execute--w--w--w- 0222 write--wx-wx-wx 0333 write & execute-r--r--r-- 0444 read-r-xr-xr-x 0555 read & execute-rw-rw-rw- 0666 read & write-rwxrwxrwx 0777 read. write & execute
```

Para a etapa #3, a recomendação ajustar o diretório $HOME a 755 seria: 7=rwx `5=r-x 5=r-x`

Isto significa que o diretório tem as permissões padrão `- rwxr-XR-x` (representado na notação octal como 0755).

Configurando o impulso SCP do correio entra o ESA

1. Execute o **logconfig do** comando CLI.
2. Selecione a opção **nova**.
3. Escolha o tipo de arquivo de registro para esta assinatura, este será outros "1" para logs do correio de texto de IronPort, ou qualquer tipos de arquivo de registro de sua escolha.
4. Dê entrada com o nome para o arquivo de registro.
5. Selecione o nível apropriado do log. Tipicamente você precisaria de selecionar "3" para log informativo, ou todo o outro em nível de sua escolha.
6. Quando alertado “escolha o método recuperar os logs, selecione "3" para o **impulso SCP**.
7. Entre no endereço IP de Um ou Mais Servidores Cisco ICM NT ou no nome de host DNS para entregar os logs a.
8. Entre na porta para conectar no host remoto.
9. Incorpore o diretório no host remoto para colocar logs.
10. Entre em um nome de arquivo para usar-se para arquivos de registro.
11. Configurar, se necessário, identificadores exclusivos por análise de sistemas como *$hostname*, *$serialnumber* adicionar ao nome de arquivo do log.
12. Ajuste o máximo filesize antes de transferir.

13. Configurar o derrubamento com base no período dos arquivos de registro, se aplicável.
14. Quando pedido “faça você querem permitir a verificação da chave Host? ”, incorpore “Y”.
15. Você é apresentado então “coloca por favor as seguintes chaves SSH em seu arquivo dos authorized_keys de modo que os arquivos de registro possam ser transferidos arquivos pela rede.”
16. Copie essa chave, porque você precisará de pôr a chave SSH em seu arquivo dos “authorized_keys” sobre o servidor de SYSLOG. Cole a chave dada do logconfig ao arquivo $HOME/.ssh/authorized_keys no servidor de SYSLOG.
17. Do ESA, execute o comando CLI **comprometem** para salvar e comprometer alterações de configuração.

A configuração do log pode igualmente ser realizada do GUI: **Assinaturas da administração do sistema > do log**

> Nota: Reveja por favor o capítulo de registro do Guia do Usuário ESA para detalhes e a informação adicional completos.

Confirmação

Hostkeyconfig

Execute o **logconfig** > o **hostkeyconfig do** comando. Você deve ver uma entrada para o servidor de SYSLOG configurado alistado como o “SSH-dss” com um similar chave abreviado à chave fornecida durante a configuração.

```
myesa.local > logconfig
...
[]> hostkeyconfig

Currently installed host keys:
1. 172.16.1.100 ssh-dss AAAAB3NzaC1kc3MAAACBAMUqUBGztO0T...OutUns+DY=
```

Log de sistema

Os log de sistema gravam o seguinte: carreg a informação, alertas virtuais da expiração da licença do dispositivo, informação de status DNS, e comente os usuários datilografados usando o comando commit. Os log de sistema são úteis para pesquisar defeitos o estado básico do dispositivo.

Executar os **system_logs do** comando tail do CLI fornecer-lhe-á um olhar vivo ao status de sistema.

Você pode igualmente escolher o **rollovernow do** comando CLI e selecionar o número associado ao arquivo de registro. Você verá este o arquivo de registro SCP a seu servidor de SYSLOG nos system_logs:

```
myesa.local > tail system_logs

Press Ctrl-C to stop.
Thu Jan 5 11:26:02 2017 Info: Push success for subscription mail_logs: Log
mail_logs.myesa.local.@20170105T112502.s pushed via SCP to remote host 172.16.1.100:22
```

Troubleshooting Avançado

Se há umas edições continuadas com Conectividade ao servidor de SYSLOG, do host local e ssh da utilização, execute o “ssh testuser@hostname - v” para testar o acesso de usuário no modo eloquente. Isto pode Troubleshooting do assistente mostrar onde a conexão do ssh não está sucedendo.

```
$ ssh testuser@172.16.1.100 -v
OpenSSH_7.3p1, LibreSSL 2.4.1
debug1: Reading configuration data /Users/testuser/.ssh/config
debug1: /Users/testuser/.ssh/config line 16: Applying options for *
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 20: Applying options for *
debug1: Connecting to 172.16.1.100 [172.16.1.100] port 22.
debug1: Connection established.
debug1: identity file /Users/testuser/.ssh/id_rsa type 1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_rsa-cert type -1
debug1: identity file /Users/testuser/.ssh/id_dsa type 2
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_dsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ecdsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ecdsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ed25519 type -1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/testuser/.ssh/id_ed25519-cert type -1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_7.3
debug1: Remote protocol version 2.0, remote software version OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
debug1: match: OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8 pat OpenSSH_6.6.1* compat 0x04000000
debug1: Authenticating to 172.16.1.100:22 as 'testuser'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256@libssh.org
debug1: kex: host key algorithm: ssh-dss
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression:
zlib@openssh.com
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression:
zlib@openssh.com
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ssh-dss SHA256:c+YpkZsQyUwi3tkIVJFXHAstwlkdewO1G0s7P2khV7U
debug1: Host '172.16.1.100' is known and matches the DSA host key.
debug1: Found key in /Users/testuser/.ssh/known_hosts:5
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS received
debug1: Skipping ssh-dss key /Users/testuser/.ssh/id_dsa - not in PubkeyAcceptedKeyTypes
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Offering RSA public key: /Users/testuser/.ssh/id_rsa
debug1: Authentications that can continue: publickey,password
debug1: Trying private key: /Users/testuser/.ssh/id_ecdsa
debug1: Trying private key: /Users/testuser/.ssh/id_ed25519
debug1: Next authentication method: password
testuser@172.16.1.100's password: <<< ENTER USER PASSWORD TO LOG-IN >>>
debug1: Enabling compression at level 6.
```

```
debug1: Authentication succeeded (password).
Authenticated to 172.16.1.100 ([172.16.1.100]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: pledge: exec
debug1: No xauth program.
Warning: untrusted X11 forwarding setup failed: xauth key data not generated
debug1: Requesting authentication agent forwarding.
debug1: Sending environment.
debug1: Sending env LANG = en_US.UTF-8
debug1: Sending env LC_CTYPE = en_US.UTF-8
```