eole-common - Tâche #11977

Scénario # 11155 (Terminé (Sprint)): Renforcer la configuration SSH en accord avec les préconisations de l'ANSSI

Renforcer la configuration SSH en accord avec les préconisations de l'ANSSI

06/15/2015 10:04 AM - Scrum Master

Status:	Fermé	**Start date:**	06/01/2015
Priority:	Normal	**Due date:**	
Assigned To:	Emmanuel GARETTE	**% Done:**	100%
Target version:	Sprint_2015_23-25 - Équipe MENESR	**Estimated time:**	4.00 hours
		Spent time:	3.00 hours

Description

Related issues:

Related to Amon - Demande #16651: Tunnel SSH via Amon 2.5	**Classée sans suite**	**06/28/2016**
Related to eole-common - Demande #15846: Ajouter dans variables dans sshd_config	**Classée sans suite**	**04/13/2016**
Related to Distribution EOLE - Demande #16177: il n'est plus possible de fair...	**Classée sans suite**	**05/25/2016**
Related to Distribution EOLE - Tâche #18105: Améliorer la définition de la va...	**Fermé**	**11/28/2016**

Associated revisions

Revision 7e9ee905 - 06/17/2015 03:56 PM - Emmanuel GARETTE

mise à jour du template SSH (ref #11977 @2h)

Revision 7d826e02 - 06/22/2015 01:52 PM - Daniel Dehennin

Supporter les connexions SSH en provenance de 2.3

Les serveurs 2.3 doivent pouvoir se connecter à Zéphir.

- tmpl/sshd_config: Suppression du paramètre « KexAlgorithms »

Ref: #11977

History

#1 - 06/15/2015 10:07 AM - Scrum Master

- Estimated time set to 4.00 h

- Remaining (hours) set to 4.0

#2 - 06/15/2015 03:38 PM - Daniel Dehennin

- File sshd_config.txt added

Un fichier de configuration basé sur les recomendations de l'ANSSI, à intégrer au template EOLE.

#3 - 06/16/2015 09:56 AM - Scrum Master

- Status changed from Nouveau to En cours

#4 - 06/16/2015 04:35 PM - Emmanuel GARETTE

En vrac :

variables identiques :

Port 22
Protocol 2
PubkeyAuthentication yes
UsePrivilegeSeparation yes
StrictModes yes
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_rsa_key
LogLevel INFO
SyslogFacility AUTH
Subsystem sftp /usr/lib/sftp-server
PrintMotd no
HostbasedAuthentication no
IgnoreRhosts yes
AuthorizedKeysFile %h/.ssh/authorized_keys

variables existantes avec valeurs différentes :

ANSSI | EOLE
HostKey /etc/ssh/ssh_host_ed25519_key => /etc/ssh/ssh_host_dsa_key
TCPKeepAlive no => yes
AcceptEnv LANG LC_* => LANG LANGUAGE LC_* EDITOR
X11forwarding no => yes
LoginGraceTime 30 => 600
PermitRootLogin no => (forcé à yes dans le cas de la haute dispo)

variables uniquement ANSSI

GSSAPIAuthentication yes
GSSAPIKeyExchange yes
GSSAPICleanupCredentials yes
PasswordAuthentication no
Ciphers chacha20-poly1305@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-sha1-etm@openssh.com
,hmac-sha2-512,hmac-sha2-256,hmac-sha1-96,hmac-sha1
KexAlgorithms curve25519-sha256@libssh.org
IgnoreUserKnownHosts yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
PermitUserEnvironment no
AllowTcpForwarding no
Banner none
PrintLastLog yes
Compression delayed
ClientAliveInterval 30
ClientAliveCountMax 10
MaxStartups 5:30:10

variables uniquement EOLE

KeyRegenerationInterval 3600
ServerKeyBits 2048
UseDNS no
UsePAM yes
X11DisplayOffset 10
RSAAuthentication yes
RhostsRSAAuthentication no
AllowGroups xxxxxxxxxxxx

#5 - 06/16/2015 04:36 PM - Emmanuel GARETTE

- Assigned To set to Emmanuel GARETTE

#6 - 06/22/2015 02:14 PM - Daniel Dehennin

- Status changed from En cours to Fermé

- % Done changed from 0 to 100

- Remaining (hours) changed from 4.0 to 0.0

Toutes les recommandations ne sont pas faites car certaines requierent des développements (ref: #12123).

#7 - 11/29/2016 10:52 AM - Joël Cuissinat

- Related to Tâche #18105: Améliorer la définition de la variable "ssh_maxstartups" dans le dictionnaire added

Files

sshd_config.txt	3.08 KB	06/15/2015	Daniel Dehennin