Admins - Anomalie #1369

niveau de sécurité https

30/09/2013 22:28 - Loïc Dachary

Statut:	Fermé	**Début:**	30/09/2013
Priorité:	Normale	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:	Task	**Temps estimé:**	0.00 heure
Version cible:	Backlog	**Temps passé:**	0.00 heure
Difficulté:	4 Fastidieux		

Description

Thread "Niveau de sécurité de notre https"

L'un de mes apprentissages de la conférence de Benjamin sur SSL/TLS est l'outil en ligne ssllabs qui teste la robustesse des configurations https. Je me suis donc amusé à faire le test sur celui de l'april. Je vous livre ici le résultat de cet "audit" :

https://ssllabs.com/ssltest/analyze.html?d=https%3A%2F%2Fapril.org

Historique

#1 - 06/10/2013 14:38 - Nicolas Vinot

- Difficulté changé de 2 Facile à 4 Fastidieux

J'ai essayé de faire les corrections nécessaires pour augmenter notre protection SSL.
Les versions de OpenSSL et de Nginx sont trop anciennes pour comprendre TLSv1.1 et TLSv2.

```
Starting nginx: [warn]: invalid value "TLSv1.1" in /etc/nginx/sites-enabled/01_www.april.org:43
```

```
ii  nginx                          0.7.67-3+squeeze3           small, but very powerful and efficient web se
rver and mail proxy
ii  openssl                        0.9.8o-4squeeze13           Secure Socket Layer (SSL) binary and related
cryptographic tools
```

Les versions à jour seraient nginx 1.2.1-2.2 et openssl 1.0.1e-2.

Il faudrait donc commencer par mettre à jour les machines et les sortir de wheezy.

```
Les paquets suivants seront ENLEVÉS :
  libept1
Les NOUVEAUX paquets suivants seront installés :
  aptitude-common cpio debconf-utils dmidecode gcc-4.7-base git-man krb5-locales
  libapt-inst1.5 libapt-pkg4.12 libasprintf0c2 libbind9-80
  libboost-iostreams1.49.0 libclass-isa-perl libdb5.1 libdns88 libept1.4.12
  libffi5 libfreetype6 libgd2-noxpm libisc84 libisccc80 libisccfg82 libjpeg8
  liblockfile-bin liblwres80 liblzma5 libmount1 libp11-kit0 libpam-modules-bin
  libpipeline1 libpng12-0 libprocps0 librtmp0 libruby1.9.1 libsemanage-common
  libsemanage1 libssl1.0.0 libswitch-perl libsystemd-login0 libtinfo5
  libustr-1.0-1 libxslt1.1 libyaml-0-2 multiarch-support nginx-common nginx-full
  python2.7 python2.7-minimal ruby-json ruby-shadow ruby1.9.1
Les paquets suivants seront mis à jour :
  adduser apt apt-utils apt-xapian-index aptitude augeas-lenses augeas-tools
  base-files base-passwd bash bash-completion bind9-host bsdmainutils bsdutils
  bzip2 ca-certificates coreutils cron cron-apt curl dash dbus dctrl-tools debconf
  debconf-i18n debian-archive-keyring debian-goodies debianutils deborphan dialog
  diffutils dmsetup dnsutils dpkg e2fslibs e2fsprogs emacs23-bin-common
  emacs23-common emacs23-nox emacsen-common etckeeper facter file findutils
  gcc-4.4-base geoip-database gettext-base git git-core gnupg gnupg-curl gpgv grep
  groff-base gzip heirloom-mailx hostname ifupdown info initscripts insserv
  install-info iproute iputils-ping iso-codes less libacl1 libasound2 libattr1
  libaugeas-ruby1.8 libaugeas0 libblkid1 libbsd0 libbz2-1.0 libc-bin libc6 libcap2
  libcomerr2 libcurl3 libcurl3-gnutls libcwidget3 libdbus-1-3 libdevmapper1.02.1
  libedit2 libexpat1 libgcc1 libgcrypt11 libgdbm3 libgeoip1 libgnutls26
  libgpg-error0 libgpm2 libgssapi-krb5-2 libidn11 libk5crypto3 libkeyutils1
```

```
  libkrb5-3 libkrb5support0 libldap-2.4-2 liblocale-gettext-perl liblockfile1
  libmagic1 libncurses5 libncursesw5 libnewt0.52 libpam-modules libpam-runtime
  libpam0g libpci3 libpcre3 libpopt0 libreadline5 libreadline6 libruby libruby1.8
  libsasl2-2 libsasl2-modules libselinux1 libsepol1 libshadow-ruby1.8
  libsigc++-2.0-0c2a libslang2 libsqlite3-0 libss2 libssh2-1 libstdc++6 libtasn1-3
  libtext-charwidth-perl libtext-iconv-perl libudev0 libusb-0.1-4 libuuid1
  libwrap0 libx11-6 libx11-data libxapian22 libxau6 libxcb1 libxdmcp6 libxext6
  libxml2 libxmuu1 locales lockfile-progs login logrotate lsb-base lsb-release
  lsof lzma man-db manpages mawk mime-support mktemp molly-guard mount
  ncurses-base ncurses-bin net-tools netbase netcat netcat-traditional nginx
  openssh-blacklist openssh-blacklist-extra openssh-client openssl passwd patch
  pciutils perl perl-base perl-modules postfix procps puppet puppet-common python
  python-apt python-apt-common python-central python-chardet python-debian
  python-minimal python-support python-xapian python2.6 python2.6-minimal
  readline-common rsync rsyslog ruby ruby1.8 screen sed sensible-utils sgml-base
  ssl-cert sysv-rc sysvinit sysvinit-utils tar tcpd tig tzdata update-inetd
  util-linux vim vim-common vim-runtime wget whiptail xauth xml-core xz-utils
  zlib1g
217 mis à jour, 51 nouvellement installés, 1 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 146 Mo dans les archives.
Après cette opération, 26,7 Mo d'espace disque supplémentaires seront utilisés.
```

Ça en devient beaucoup plus sensible que de toucher à 2 fichiers de config… :(

#2 - 06/10/2013 16:43 - Nicolas Vinot

Sur les conseils de vx, j'ai cloné le vserver nginx pour tenter une migration.
L'upgrade en lui-même semble bon, mais pas mal de fichiers sont modifiés entre les 2 versions (cron-apt, logrotate, puppet, nginx)
La non régression devient importante à vérifier.
Je remarque au passage des choses installées qui sont bizarres pour un serveur (debian-goodies, emacs, dbus).
Le nouveau fichier de config de nginx nécessite aussi de migrer les déclarations ssl du nginx.conf vers chaque vhost, sous peine d'un

```
Restarting nginx: nginx: [emerg] no "ssl_certificate" is defined for the "ssl" directive in /etc/nginx/sites-e
nabled/libreassociation.info:23
```

On pourrait envisager d'installer proprement un nginx from scratch dans Openstack au lieu de chercher à upgrader l'ancien aux forceps.
Mais on risque d'avoir plusieurs obstacles : * pas d'inventaire fiable des services * par exemple la présence de lighthttpd sur les nginx est quelque chose d'absolument pas documenté et pourtant est utilisé pour les stats des sites web (awstats) * pas de migration des apache dans Openstack * Est-ce que c'est possible de faire causer un nginx openstack avec un apache vserver ? * Quid de la latence ? * Est-ce qu'on aurait pas un double travail à faire, avec une puppetisation « hard-codée » suivie d'une repuppetisation quand les apache seront à leur tour puppetissés ?

#3 - 04/10/2016 17:03 - François Poulain

- Description mis à jour

- Statut changé de Nouveau à Fermé

Problème corrigé par la nouvelle infra et un peu d'amour.

#4 - 26/12/2020 00:20 - Christian P. Momon

- Assigné à mis à François Poulain