

J-EOLE

17-18 Octobre 2013

Évolutions Amon - Sphynx 2.3

Fabrice Barconnière
Émmanuel Garette

Évolutions Amon - Sphynx 2.3

Proxy et postes hors domaine

- Problème d'authentification NTLM pour les postes hors domaine
- CNTLM force une fenêtre d'authentification
- CNTLM est un service sur le port 3127
- Les flux passent par le proxy Amon

Évolutions Amon - Sphynx 2.3

Proxy et postes hors domaine

- Installé par défaut à partir Amon 2.3.11 (paquet eole-cntlm)
- Désactivé par défaut
- Activable dans l'onglet « Proxy authentifié » si le type d'authentification est « NTLM/SMB » ou « NTLM/KERBEROS »

Évolutions Amon - Sphynx 2.3

Proxy et postes hors domaine

Type d'authentification	NTLM/SMB	
Valeur 1 ✕	Valeur 2 ✕	+
Nom du contrôleur de domaine SMB	scribe	
Nom du domaine SMB	mondomaine	
Adresse IP du contrôleur de domaine SMB	10.121.11.5	
Activer le proxy NTLM	oui	

Évolutions Amon - Sphynx 2.3

Proxy et postes hors domaine

- Proxy CNTLM à déclarer dans le navigateur
- La configuration de WPAD renseigne le port CNTLM

Évolutions Amon - Sphynx 2.3

Évolutions DNS

- Nouveau programme « h2n »
- Les vues DNS

Évolutions Amon - Sphynx 2.3

Évolutions DNS

- Vues DNS VPN AGRIATES
- Sur chaque interface, autorisé par défaut sur eth1
- Alias
- VLAN
- Routes statiques, autorisé par défaut
- Possibilité d'interdire l'utilisation du DNS

Évolutions Amon - Sphynx 2.3

Évolutions DNS

- Vues DNS zones forward
- Sur chaque interface, autorisé par défaut sur eth1
- Alias
- VLAN
- Routes statiques, autorisé par défaut

Évolutions Amon - Sphynx 2.3

Paquet eole-vpn commun Amon/Sphynx
(à partir de la release EOLE 2.3.10)

- Installe strongSwan (Version actuelle 5.0.1)
- Dictionnaire de personnalisation de strongSwan
- Templates des fichiers configuration
- Scripts de mise en place du VPN :
Même script active_rvp pour Amon et Sphynx

Évolutions Amon - Sphynx 2.3

Le dictionnaire (à partir de la release EOLE 2.3.10)

- Mode fichier plat

Paramètres strongSwan	
Configuration des tunnels en mode database (sw_database_mode)	non
Nombre d'essais de retransmission avant Dead Peer Detection (sw_retransmit_tries)	11

Évolutions Amon - Sphynx 2.3

Le dictionnaire

- Gestion des routes

Gestion des Routes VPN	
Gestion des routes par strongSwan (sw_install_vpn_route)	<input type="text" value="oui"/>
Forcer l'adresse IP source de l'interface (sw_force_ip_src)	<input type="text" value="non"/>

Évolutions Amon - Sphynx 2.3

Le dictionnaire
(à partir de la release EOLE 2.3.11)

- Gestion des threads

Gestion des threads	
Nombre de threads disponibles pour strongSwan (<code>sw_threads</code>)	32
Nombre de threads à réserver pour les jobs HIGH priority (<code>sw_high_priority_threads</code>)	2
Nombre de threads à réserver pour les jobs MEDIUM priority (<code>sw_medium_priority_threads</code>)	4

Évolutions Amon - Sphynx 2.3

Le dictionnaire

- Agent Zéphir 'rvp'

Paramètres agent Zéphir rvp et diagnose

Agent rvp Zéphir en mode 'No action'
(zephir_client_noaction)

non

Valeur 1 ✖ +

Adresses IP à tester dans test-rvp
(ip_test_rvp)

Évolutions Amon - Sphynx 2.3

Le dictionnaire

- Paramétrage d'ipsec

Paramètres ipsec	
Contrôle du status des certificats dans le CRL (sw_crl_check)	<input type="text" value="oui"/>
Forcer l'encapsulation (Détection NAT) (sw_forceencap)	<input type="text" value="non"/>
Autoriser le changement d'adresse IP d'une extrémité de connexion (sw_mobike)	<input type="text" value="non"/>

Évolutions Amon - Sphynx 2.3

L'agent Zéphir rvp (à partir de la release EOLE 2.3.11)

- Surveillance des threads

État : OK

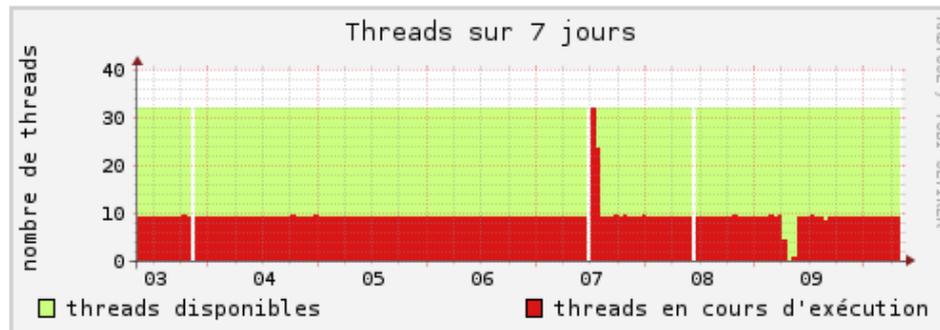
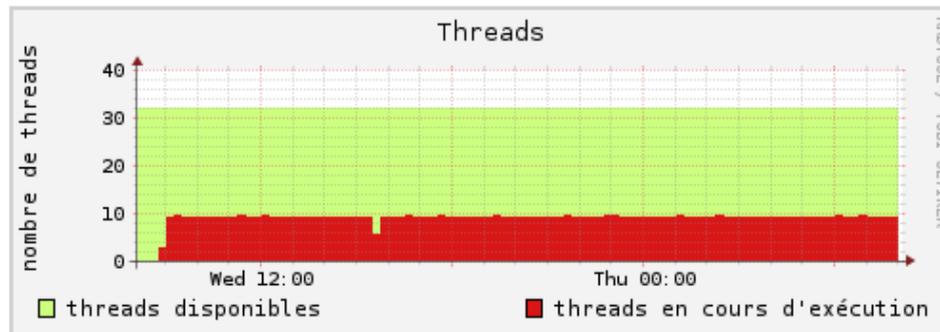
Date de la mesure : 2013-10-10 08:04:14

Dernier problème (**Erreur : Moins de 2 threads strongSwan disponibles**) : 2013-10-07 11:58:06

Intervalle de mesure : 180 s

Systeme

- ☀ [Informations système](#) [OK]
- ☀ [Occupation des disques](#) [OK]
- ☀ [Statistiques réseau](#) [OK]
- ☀ [État des sommes MD5 de paquets](#) [OK]
- ☀ [État des threads strongSwan](#) [OK]



Évolutions Amon - Sphynx 2.3

Nouveautés ARV (à partir de la release EOLE 2.3.10)

- Tri et filtrage des colonnes

Tunnels		Serveurs RVP		Modèles		Certificats	
Serveur RVP 1				Serveur RVP 2			
UAI	▼	Nom		UAI	Nom		
0000000A	A ↓	Tri croissant		0000000A	Amon avé accent		
0000000A	Z ↓	Tri décroissant		0000000A	amon1		
0000000A	A ↓						
		<input checked="" type="checkbox"/> Filters		<input type="checkbox"/>		0000000A	

Évolutions Amon - Sphynx 2.3

Nouveautés ARV

- Détail des tunnels

Tunnels			Serveurs RVP			Modèles			Certificats		
Serveur RVP 1			Serveur RVP 2			Tunnel					
UAI	Nom		UAI	Nom		Nom	IP / Réseau		IP / Réseau		
0000000A	sphynxha1		0000000A	Amon avé accent		RACINE-AGRIATES - 192.168.0.1 ... 192.168.0.3					
0000000A	amon1		0000000A	amon1		adm-eth1	eth1 : 172.30.102.0 / 255.255.255.0		adm : 10.21.11.0 / 255.255.255.0		
0000000A	Amon avé accent					dmz-eth1	eth1 : 172.30.102.0 / 255.255.255.0		dmz : 10.121.11.0 / 255.255.255.224		
						adm_rés172	rez_172 : 172.16.0.0 / 255.240.0.0		adm : 10.21.11.0 / 255.255.255.0		
						vlanpeda	eth1 : 172.30.102.0 / 255.255.255.0		vlan_pedago : 10.21.14.0 10.21.15.0		

Évolutions Amon - Sphynx 2.3

Nouveautés ARV

- Archives VPN
- État des connexions

Tunnels	Serveurs RVP	Modèles	Certificats
UAI	Nom	État	
0000000A	sphynxha1		
0000000A	amon1	Connexion OK - Problème de tunnel(s)	
0000000A	Amon avé accent	Problème de connexion - Problème de tunnel(s)	
 Ajouter  Modifier  Supprimer  Certificat  IP externe  Renvoyer sur Zéphir			
Prêt			Appliquer 

Évolutions Amon - Sphynx 2.3

Nouveautés ARV

- Gestion des certificats

Tunnels	Serveurs RVP	Modèles	Certificats	
Nom	Date d'expiration	Expire dans (j)	CA	
0210026P-01	2010/11/08	-1066	false	^
autoamon	2013/11/01	23	false	≡
AGRIATES-DIJON-...	2015/01/25	473	false	
0890977D-01	2015/02/02	481	false	
0210017E-01	2015/02/02	481	false	
0210066H-15	2015/03/22	529	false	v

 Modifier

Prêt Appliquer 