

Eviden

# **Guide de l'utilisateur de SafeKit**

Logiciel de haute disponibilité  
pour applications critiques



## Vue générale

<b>Sujet</b>	Ce document couvre toutes les phases de mise en œuvre de SafeKit : architecture, installation, tests, administration, résolution de problèmes, support, interface ligne de commande	
<b>Public visé</b>	<b>Architectures</b>	<a href="#">Aperçu technique</a>
	<b>Installation</b>	<a href="#">Installation</a>
	<b>Console</b>	<a href="#">La console web de SafeKit</a> <a href="#">Sécurisation du service web de SafeKit</a>
	<b>Configuration avancée</b>	<a href="#">Cluster.xml pour la configuration du cluster SafeKit</a> <a href="#">Userconfig.xml pour la configuration du module applicatif</a> <a href="#">Scripts du module pour la configuration du module applicatif</a> <a href="#">Exemples de configurations de module applicatif</a>
	<b>Administration</b>	<a href="#">Administration d'un module miroir</a> <a href="#">Administration d'un module ferme</a> <a href="#">Interface ligne de commande</a> <a href="#">Administration avancée</a>
	<b>Support</b>	<a href="#">Tests</a> <a href="#">Résolution de problèmes</a> <a href="#">Support SafeKit</a> <a href="#">Index des messages du log</a>
	<b>Autres</b>	<a href="#">Table des matières</a> <a href="#">Logiciels tiers</a>
<b>Version</b>	SafeKit 8.2	
<b>OS supportés</b>	Windows et Linux ; pour une liste détaillée des OS supportés, voir <a href="#">ici</a>	
<b>Sites web</b>	<a href="#">Site marketing</a> <a href="#">Portail support</a>	
<b>Ref</b>	39 F2 38MC 07	

Copyright © Eviden, 2026

Eviden reconnaît les droits des propriétaires des marques mentionnées dans ce document.

Il est interdit de reproduire, d'enregistrer sur système de recherche documentaire ou de transmettre sous quelque forme et par quelque moyen que ce soit, électronique, mécanique ou autre, tout ou partie de cette publication sans le consentement préalable par écrit de l'éditeur.







Eviden décline toute garantie implicite de qualité marchande ou d'utilisation dans un but particulier et ne fait aucune garantie, à l'exception de celles effectuées dans le cadre d'un accord écrit avec et pour ses clients. Eviden ne pourra en aucun cas être tenu responsable par qui que ce soit de tout dommage direct, indirect ou spécial.














Les informations et caractéristiques techniques contenues dans ce document sont susceptibles d'être modifiées sans préavis. Pour tout renseignement sur la disponibilité des produits ou services, veuillez consulter un représentant commercial d'Eviden.

# Table des matières

<b>Vue générale .....</b>	<b>3</b>
<b>Table des matières .....</b>	<b>5</b>
<b>1. Aperçu technique.....</b>	<b>17</b>
1.1 Généralités, solutions, architectures.....	17
1.1.1 Introduction à SafeKit .....	17
1.1.2 Solutions SafeKit .....	18
1.1.3 Architectures SafeKit .....	18
1.1.4 Définition du cluster SafeKit.....	19
1.1.5 Définition du module applicatif SafeKit .....	19
1.1.6 Limites de SafeKit .....	20
1.2 Le cluster miroir de SafeKit .....	20
1.2.1 Réplication de fichiers en temps réel et basculement .....	20
1.2.2 Étape 1. Fonctionnement normal .....	21
1.2.3 Étape 2. Basculement .....	21
1.2.4 Étape 3. Réintégration et resynchronisation .....	22
1.2.5 Étape 4. Retour au fonctionnement normal .....	22
1.2.6 Réplication synchrone et réplication asynchrone .....	22
1.2.7 Comportement en cas d'isolation réseau.....	23
1.2.8 Réplication à 3 nœuds.....	23
1.2.9 SafeKit sur un seul nœud pour résister aux pannes logicielles .....	24
1.3 Le cluster ferme de SafeKit .....	24
1.3.1 Équilibrage de charge réseau et basculement d'application .....	24
1.3.2 Principe d'une adresse IP virtuelle avec équilibrage de charge réseau .....	24
1.3.3 Équilibrage de charge pour les services Web avec ou sans état .....	25
1.3.4 Solution de haute disponibilité en chaîne dans une ferme .....	25
1.4 Clusters exécutant plusieurs modules .....	26
1.4.1 Le cluster ferme+miroir de SafeKit .....	26
1.4.2 Le cluster actif/actif avec réplication de SafeKit.....	26
1.4.3 Le cluster N-1 de SafeKit.....	27
1.5 Le cluster Hyper-V ou KVM de SafeKit .....	27
1.5.1 Équilibrage de charge, réplication, basculement de machines virtuelles complètes .....	27
1.6 Clusters SafeKit dans le cloud .....	28
1.6.1 Cluster miroir dans Azure, AWS et GCP .....	28
1.6.2 Cluster ferme dans Azure, AWS et GCP .....	30
<b>2. Installation.....</b>	<b>31</b>
2.1 Installation de SafeKit .....	31
2.1.1 Télécharger le package .....	31
2.1.2 Répertoires d'installation et espace disque.....	32
2.1.3 Procédure d'installation de SafeKit.....	32

2.1.4	Utilisation de la console web et de la ligne de commande SafeKit .....	36
2.1.5	Clés de licence SafeKit .....	37
2.1.6	Caractéristiques spécifiques à chaque OS .....	37
2.2	Recommandation pour une installation d'un module miroir.....	38
2.2.1	Prérequis matériel et système.....	38
2.2.2	Prérequis réseau .....	38
2.2.3	Prérequis application.....	38
2.2.4	Prérequis réplication de fichiers.....	39
2.3	Recommandation pour une installation d'un module ferme.....	39
2.3.1	Prérequis matériel et système.....	39
2.3.2	Prérequis réseau .....	39
2.3.3	Prérequis application.....	39
2.4	Upgrade de SafeKit .....	39
2.4.1	Préparer l'upgrade.....	40
2.4.2	Procédure de désinstallation .....	40
2.4.3	Procédure de réinstallation et post-installation pour l'upgrade .....	40
2.5	Désinstallation complète de SafeKit.....	42
2.5.1	Désinstallation sur Windows.....	42
2.5.2	Désinstallation sur Linux .....	44
2.6	Documentations SafeKit .....	44
<b>3.</b>	<b>La console web de SafeKit .....</b>	<b>47</b>
3.1	Démarrer la console web .....	47
3.1.1	Lancer un navigateur web .....	47
3.1.2	Connecter la console à un nœud SafeKit.....	47
3.1.3	Liste des nœuds de connexion.....	49
3.1.4	Utiliser l'application web (SafeKit Web App).....	49
3.1.5	Mettre à jour la console web .....	51
3.2	Configurer un cluster SafeKit.....	51
3.2.1	L'assistant de configuration du cluster.....	52
3.2.2	Page d'accueil de la configuration du cluster .....	55
3.3	Configurer un module applicatif .....	56
3.3.1	Sélectionner le nouveau module à configurer .....	57
3.3.2	L'assistant de configuration du module.....	58
3.3.3	Page d'accueil de la configuration des modules.....	63
3.3.4	Éditer localement la configuration du module puis l'appliquer .....	65
3.4	Superviser un module applicatif.....	66
3.4.1	Page d'accueil de la supervision.....	66
3.4.2	État du module .....	67
3.4.3	Menus de contrôle d'un module.....	69
3.4.4	Détails du module.....	72
3.4.5	Chronologie des états du module.....	78

3.5	Snapshots et journaux du module applicatif pour le débogage et support.....	78
3.6	Sécuriser la console web.....	79
<b>4.</b>	<b>Tests.....</b>	<b>81</b>
4.1	Installation et tests après boot .....	81
4.1.1	Test installation package .....	81
4.1.2	Test licence et version.....	82
4.1.3	Test des services et modules SafeKit après boot.....	82
4.1.4	Test démarrage de la console web.....	84
4.2	Tests d'un module miroir .....	85
4.2.1	Test du premier start d'un module miroir sur 2 serveurs  STOP (NotReady) .....	85
4.2.2	Test start d'un module miroir sur 2 serveurs  STOP (NotReady) .....	85
4.2.3	Test stop d'un module miroir sur le serveur  PRIM (Ready) .....	85
4.2.4	Test start du module miroir dans l'état  STOP (NotReady) .....	86
4.2.5	Test restart du module miroir dans l'état  PRIM (Ready) .....	86
4.2.6	Test adresse IP virtuelle d'un module miroir.....	86
4.2.7	Test réplication de fichiers d'un module miroir.....	87
4.2.8	Test shutdown du serveur  PRIM (Ready) .....	88
4.2.9	Test power-off du serveur  PRIM (Ready) .....	89
4.2.10	Test split-brain avec un module miroir .....	89
4.2.11	Continuer les tests de votre module miroir avec les checkers .....	91
4.3	Tests d'un module ferme .....	91
4.3.1	Test start d'un module ferme sur les serveurs  STOP (NotReady) .....	91
4.3.2	Test stop d'un module ferme sur un serveur  UP (Ready) .....	91
4.3.3	Test restart d'un module ferme sur un serveur  UP (Ready) .....	91
4.3.4	Test adresse IP virtuelle d'un module ferme.....	91
4.3.5	Test load balancing TCP sur une adresse virtuelle .....	93
4.3.6	Test split-brain avec un module ferme .....	94
4.3.7	Test de la compatibilité du réseau avec l'adresse MAC invisible (vmac_invisible) .....	95
4.3.8	Test shutdown d'un serveur  UP (Ready) .....	96
4.3.9	Test power-off d'un serveur  UP (Ready) .....	97
4.3.10	Continuer les tests du module ferme avec les checkers .....	97
4.4	Tests des checkers communs à un miroir et une ferme.....	97
4.4.1	Test <errd> checker avec action restart ou stopstart.....	97
4.4.2	Test <tcp> checker avec action restart ou stopstart .....	98
4.4.3	Test <tcp> checker avec action wait.....	99
4.4.4	Test <interface check="on"> avec action wait .....	100
4.4.5	Test <ping> checker avec action wait .....	101
4.4.6	Test <module> checker avec action wait.....	102
4.4.7	Test <custom> checker avec action wait.....	103

4.4.8	Test <custom> checker avec action restart ou stopstart .....	104
<b>5.</b>	<b>Administration d'un module miroir .....</b>	<b>107</b>
5.1	Mode de fonctionnement d'un module miroir .....	107
5.2	Automate d'état d'un module miroir (STOP, WAIT, ALONE, PRIM, SECOND - NotReady, Transient, Ready) .....	109
5.3	Premier démarrage d'un module miroir (commande prim) .....	109
5.4	Différents cas de réintégration (utilisation des bitmaps).....	110
5.5	Démarrage d'un module miroir avec les données à jour  STOP (NotReady) -  WAIT (NotReady) .....	112
5.6	Mode de réplication dégradé (  ALONE (Ready) dégradé) .....	113
5.7	Reprise automatique ou manuelle .....	114
5.8	Serveur primaire par défaut (swap automatique après réintégration) .....	115
5.9	La commande prim échoue : pourquoi ? (commande primforce) .....	116
<b>6.</b>	<b>Administration d'un module ferme .....</b>	<b>119</b>
6.1	Mode de fonctionnement d'un module ferme .....	119
6.2	Automate d'état d'un module ferme (STOP, WAIT, UP - NotReady, Transient, Ready).....	120
6.3	Démarrage d'un module ferme .....	120
<b>7.</b>	<b>Résolution de problèmes .....</b>	<b>123</b>
7.1	Problème de connexion avec la console web.....	123
7.1.1	Contrôler le navigateur.....	124
7.1.2	Supprimer l'état du navigateur.....	124
7.1.3	Contrôler les serveurs .....	124
7.2	Problème de connexion HTTPS avec la console web.....	125
7.2.1	Contrôler les certificats serveurs.....	125
7.2.2	Contrôler les certificats installés dans SafeKit.....	126
7.2.3	Revenir à la configuration HTTP.....	127
7.3	Vérification globale de l'environnement (script healthcheck) .....	127
7.4	Comment lire les journaux et les ressources du module applicatif ?.....	127
7.5	Comment lire le journal de commandes du serveur ? .....	128
7.6	Module stable  (Ready) et  (Ready) .....	128
7.7	Module dégradé  (Ready) et  (NotReady) .....	129
7.8	Module hors service  (NotReady) et  (NotReady) .....	129
7.9	Module  STOP (NotReady) : redémarrer le module.....	129
7.10	Module  WAIT (NotReady) : réparer la ressource="down" .....	130
7.11	Module oscillant de  (Ready) à  (Transient) .....	131
7.12	Message sur stop après maxloop .....	132

7.13	Module ✓ (Ready) mais application non opérationnelle .....	132
7.14	Module mirror ✓ <sub>ALONE</sub> (Ready) / ○ <sub>WAIT</sub> ou ✗ <sub>STOP</sub> (NotReady) .....	133
7.15	Module ferme ✓ <sub>UP</sub> (Ready) mais problème de load balancing .....	134
7.15.1	Non cohérence des parts de la charge réseau.....	134
7.15.2	L'adresse IP virtuelle ne répond pas correctement .....	134
7.16	Problème avec l'adresse IP virtuelle après le basculement.....	134
7.17	Problème après boot .....	136
7.18	Analyse à partir des snapshots du module applicatif .....	136
7.18.1	Fichiers de configuration du module.....	137
7.18.2	Fichiers de dump du module .....	137
7.19	Problème avec la taille des bases de données de SafeKit .....	140
7.20	Problème pour récupérer le certificat de l'autorité de certification depuis une PKI externe .....	141
7.20.1	Exporter les certificats CA depuis des certificats publics.....	141
7.21	Problème d'envoi de courriel par l'agent de notification SafeKit.....	144
7.21.1	Failed to read or parse the configuration file .....	144
7.21.2	Blocage lors du test d'envoi de courriel .....	145
7.21.3	Erreurs curl .....	145
7.22	Problème avec les antivirus.....	146
7.23	Problèmes liés aux modules noyau SafeKit.....	147
7.23.1	Module miroir avec le filtre <code>rfs</code> en Windows.....	147
7.23.2	Module ferme avec le module <code>vip</code> en Linux.....	147
7.24	Dépannage de résolution VIP ↔ MAC.....	147
7.24.1	Vérifier les entrées du cache .....	147
7.24.2	Forcer une nouvelle résolution .....	148
7.24.3	Observer les requêtes de résolution .....	148
7.25	Problème persistant .....	149
<b>8.</b>	<b>Support SafeKit .....</b>	<b>151</b>
<b>9.</b>	<b>Interface ligne de commande .....</b>	<b>153</b>
9.1	Commandes de contrôle et setup de SafeKit .....	153
9.1.1	Service <code>safeadmin</code> .....	153
9.1.2	Service <code>safewebserver</code> .....	154
9.1.3	Agent de notification par courriel.....	155
9.1.4	Service SNMP.....	156
9.1.5	Service web <code>safecaserv</code> .....	156
9.2	Commandes de configuration et surveillance du cluster .....	156
9.3	Commandes de contrôle des modules applicatifs.....	158
9.4	Commandes de surveillance des modules applicatifs .....	160
9.5	Commandes de configuration des modules applicatifs.....	161

9.6	Commandes de support.....	163
9.6.1	Journal du module applicatif .....	163
9.6.2	Snapshot d'un module applicatif.....	164
9.6.3	Autres commandes.....	166
9.7	Commandes lors de la maintenance de l'application du module .....	167
9.7.1	Contrôle du module lors de la maintenance.....	167
9.7.2	Exécution de l'application sans le module .....	168
9.8	Commandes distribuées sur plusieurs serveurs SafeKit.....	169
9.9	Exemples.....	171
9.9.1	Commande locale et distribuée .....	171
9.9.2	Configuration globale du cluster en ligne de commande .....	171
9.9.3	Configuration globale d'un module applicatif en ligne de commande .....	171
9.9.4	Snapshot d'un module applicatif en ligne de commande .....	172
<b>10.</b>	<b>Administration et configuration avancées .....</b>	<b>175</b>
10.1	Variables d'environnement et répertoires SafeKit.....	175
10.1.1	Global.....	175
10.1.2	Module applicatif .....	175
10.2	Services/démons SafeKit et communications .....	178
10.2.1	Services SafeKit .....	178
10.2.2	Démons SafeKit par module applicatif .....	179
10.3	Paramétrage du pare-feu .....	183
10.3.1	Paramétrage du pare-feu en Linux.....	184
10.3.2	Paramétrage du pare-feu en Windows.....	184
10.4	Configuration au boot et au shutdown en Windows .....	185
10.4.1	Procédure automatique .....	185
10.4.2	Procédure manuelle .....	185
10.5	Paramétrage de Secure Boot en Linux pour les modules kernel SafeKit.....	186
10.6	Paramétrage des antivirus .....	187
10.7	Cryptage des communications du module applicatif.....	188
10.7.1	Configuration avec la console web de SafeKit.....	188
10.7.2	Configuration en ligne de commandes.....	188
10.7.3	Configuration avancée.....	189
10.8	Cryptage des fichiers sensibles dans SafeKit .....	190
10.9	Configuration du service web de SafeKit .....	191
10.9.1	Serveur Apache HTTP .....	192
10.9.2	Fichiers de configuration.....	193
10.9.3	Configuration des ports de connexion.....	195
10.9.4	Configuration de HTTP/HTTPS et de l'authentification utilisateur .....	195
10.9.5	API SafeKit .....	196
10.10	Agent SafeKit de notification par courriel .....	198

---

10.10.1	Configuration de l'agent de notification SafeKit.....	199
10.10.2	Configuration des identifiants du client SMTP pour l'authentification.....	200
10.10.3	Test d'envoi de courriel.....	201
10.10.4	Activation de l'agent de notification SafeKit.....	201
10.11	Supervision SNMP.....	202
10.11.1	Supervision SNMP en Windows.....	202
10.11.2	Supervision SNMP en Linux.....	202
10.11.3	La MIB SafeKit.....	203
10.12	Journal des commandes du serveur SafeKit.....	204
10.13	Messages SafeKit dans le journal système.....	204
<b>11.</b>	<b>Sécurisation du service web de SafeKit.....</b>	<b>207</b>
11.1	Vue générale.....	207
11.1.1	Configuration par défaut.....	208
11.1.2	Configurations prédéfinies.....	208
11.2	Configuration HTTP.....	209
11.2.1	Configuration par défaut.....	209
11.2.2	Configuration non sécurisée basée sur un rôle identique pour tous.....	211
11.3	Configuration HTTPS.....	212
11.3.1	Configuration HTTPS avec la PKI SafeKit.....	213
11.3.2	Configuration HTTPS avec une PKI externe.....	222
11.4	Configuration de l'authentification utilisateur.....	226
11.4.1	Configuration l'authentification à base de fichier.....	226
11.4.2	Configuration de l'authentification à base de serveur LDAP/AD.....	228
11.4.3	Configuration de l'authentification à base de serveur OpenID Connect.....	231
<b>12.</b>	<b>Cluster.xml pour la configuration du cluster SafeKit.....</b>	<b>235</b>
12.1	Le fichier <code>cluster.xml</code> .....	235
12.1.1	Cluster.xml exemple.....	235
12.1.2	Cluster.xml syntaxe.....	236
12.1.3	<code>&lt;langs&gt;</code> , <code>&lt;lan&gt;</code> , <code>&lt;node&gt;</code> attributs.....	236
12.2	Configuration du cluster SafeKit.....	238
12.2.1	Configuration avec la console web de SafeKit.....	238
12.2.2	Configuration en ligne de commande.....	239
12.2.3	Changements de configuration.....	239
<b>13.</b>	<b>Userconfig.xml pour la configuration du module applicatif.....</b>	<b>241</b>
13.1	Attributs temporels.....	242
13.1.1	Exemple d'attributs temporels.....	242
13.1.2	Syntaxe des attributs temporels.....	242
13.2	Macros - <code>&lt;macro&gt;</code> .....	243
13.2.1	<code>&lt;macro&gt;</code> Exemple.....	243
13.2.2	<code>&lt;macro&gt;</code> Syntaxe.....	243

13.2.3	<macro> Attributs .....	243
13.3	Module ferme ou miroir - <service> .....	244
13.3.1	<service> Exemple.....	244
13.3.2	<service> Syntaxe .....	244
13.3.3	<service> Attributs .....	245
13.4	Heartbeats - <heart>, <heartbeat > .....	247
13.4.1	<heart> Exemple .....	248
13.4.2	<heart> Syntaxe.....	248
13.4.3	<heart>, <heartbeat> Attributs .....	248
13.5	Topologie d'une ferme - <farm>, <lan> .....	250
13.5.1	<farm> Exemple.....	250
13.5.2	<farm> Syntaxe .....	250
13.5.3	<farm>, <lan> Attributs.....	251
13.6	Adresse IP virtuelle - <vip> .....	252
13.6.1	<vip> Exemple dans un module miroir.....	252
13.6.2	<vip> Exemple dans un module ferme.....	252
13.6.3	Alternative à <vip> .....	253
13.6.4	<vip> Syntaxe.....	254
13.6.5	<interface_list>, <interface>, <virtual_interface>, <real_interface>, <virtual_addr> Attributs .....	255
13.6.6	<loadbalancing_list>, <group>, <cluster>, <host> Attributs .....	258
13.6.7	<vip> Description .....	260
13.7	Réplication de fichiers - <rfs>, <replicated> .....	261
13.7.1	<rfs> Exemple.....	262
13.7.2	<rfs> Syntaxe .....	262
13.7.3	<rfs>, <replicated> Attributs .....	263
13.7.4	<rfs>Description .....	272
13.8	Scripts du module - <user>, <var> .....	281
13.8.1	<user> Exemple .....	281
13.8.2	<user> Syntaxe.....	281
13.8.3	<user>, <var> Attributs .....	282
13.9	Hostname virtuel - <vhost>, <virtualhostname> .....	282
13.9.1	<vhost> Exemple.....	282
13.9.2	<vhost> Syntaxe .....	283
13.9.3	<vhost>, <virtualhostname> Attributs .....	283
13.9.4	<vhost> Description .....	283
13.10	Surveillance de processus ou services - <errd>, <proc> .....	284
13.10.1	<errd> Exemple.....	284
13.10.2	<errd> Syntaxe .....	286
13.10.3	<errd>, <proc> Attributs .....	286
13.10.4	<errd> Commandes .....	290

---

13.11 Checkers - <check> .....	292
13.11.1 <check> Exemple .....	292
13.11.2 <check> Syntaxe .....	292
13.11.3 <checker> Description .....	293
13.12 TCP checker - <tcp> .....	296
13.12.1 <tcp> Exemple .....	296
13.12.2 <tcp> Syntaxe .....	296
13.12.3 <tcp> Attributs .....	297
13.13 Ping checker - <ping> .....	298
13.13.1 <ping> Exemple .....	299
13.13.2 <ping> Syntaxe .....	299
13.13.3 <ping> Attributs .....	299
13.14 Interface checker - <intf> .....	301
13.14.1 <intf> Exemple .....	301
13.14.2 <intf> Syntaxe .....	301
13.14.3 <intf> Attributs .....	302
13.15 IP checker - <ip> .....	302
13.15.1 <ip> Exemple .....	302
13.15.2 <ip> Syntaxe .....	303
13.15.3 <ip> Attributs .....	303
13.16 Custom checker - <custom> .....	304
13.16.1 <custom> Exemple .....	304
13.16.2 <custom> Syntaxe .....	305
13.16.3 <custom> Attributs .....	305
13.17 Module checker - <module> .....	306
13.17.1 <module> Exemple .....	307
13.17.2 <module> Syntaxe .....	307
13.17.3 <module> Attributs .....	307
13.18 Splitbrain checker - <splitbrain> .....	308
13.18.1 <splitbrain> Exemple .....	309
13.18.2 <splitbrain> Syntaxe .....	309
13.18.3 <splitbrain> Attributs .....	310
13.19 Failover machine - <failover> .....	310
13.19.1 <failover> Exemple .....	311
13.19.2 <failover> Syntaxe .....	312
13.19.3 <failover> Attributs .....	312
13.19.4 <failover> Description .....	312
<b>14. Scripts du module pour la configuration du module applicatif .....</b>	<b>317</b>
14.1 Liste des scripts .....	317
14.1.1 Scripts de démarrage/arrêt .....	317
14.1.2 Autres scripts .....	319

14.2	Variables d'environnement et arguments passés aux scripts.....	319
14.3	Sortie des scripts .....	320
14.3.1	Sortie dans le journal du script.....	320
14.3.2	Sortie dans le journal du module.....	320
14.4	Automate d'exécution des scripts.....	321
14.5	Commandes spéciales SafeKit pour les scripts .....	322
14.5.1	Commandes pour Windows.....	323
14.5.2	Commandes pour Linux.....	323
14.5.3	Commandes pour Windows et Linux.....	324
<b>15.</b>	<b>Exemples de configurations de module applicatif .....</b>	<b>327</b>
15.1	Exemple de module miroir avec <code>mirror.safe</code> .....	328
15.1.1	Configuration du cluster avec deux réseaux .....	328
15.1.2	Configurations du module miroir.....	329
15.1.3	Scripts du module miroir .....	331
15.2	Exemple de module ferme avec <code>farm.safe</code> .....	333
15.2.1	Configuration du cluster avec trois nœuds .....	333
15.2.2	Configurations du module ferme.....	334
15.2.3	Scripts du module ferme .....	342
15.3	Exemple d'utilisation de macros et variables de script avec <code>hyperv.safe</code> .....	345
15.3.1	Configuration du module avec macro et var .....	345
15.3.2	Accès des variables par les scripts du module .....	346
15.4	Exemple de surveillance de processus avec <code>softerrd.safe</code> .....	347
15.4.1	Configuration du module avec surveillance de processus .....	347
15.4.2	Configuration avancée des scripts du module.....	348
15.5	Exemple de TCP checker.....	350
15.6	Exemple de ping checker .....	351
15.7	Exemple de custom checker avec <code>customchecker.safe</code> .....	353
15.7.1	Configuration du module avec un custom checker.....	353
15.7.2	Configuration avancée du script du module checker.....	355
15.8	Exemple de splitbrain checker .....	356
15.9	Exemples de module checker .....	357
15.9.1	Exemple d'un module ferme dépendant d'un module miroir .....	357
15.9.2	Exemple avec <code>leader.safe</code> et <code>follower.safe</code> .....	359
15.10	Exemple de checker d'interface réseau .....	359
15.11	Exemple d'IP checker .....	360
15.12	Exemple d'hostname virtuel avec <code>vhost.safe</code> .....	361
15.12.1	Configuration du module avec un hostname virtuel.....	361
15.12.2	Scripts du module avec un hostname virtuel .....	362
<b>16.</b>	<b>Cluster SafeKit dans le cloud .....</b>	<b>365</b>

16.1	Cluster SafeKit dans Amazon AWS .....	365
16.1.1	Cluster miroir dans AWS.....	366
16.1.2	Cluster ferme dans AWS.....	367
16.2	Cluster SafeKit dans Microsoft Azure .....	369
16.2.1	Cluster miroir dans Azure .....	370
16.2.2	Cluster ferme dans Azure .....	371
16.3	Cluster SafeKit dans Google GCP .....	372
16.3.1	Cluster miroir dans GCP .....	373
16.3.2	Cluster ferme dans GCP .....	375
<b>17.</b>	<b>Logiciels tiers .....</b>	<b>377</b>
	<b>Index des messages du journal du module.....</b>	<b>381</b>
	<b>Index.....</b>	<b>385</b>



# 1. Aperçu technique

- ⇒ [Section 1.1](#) « Généralités, solutions, architectures »
- ⇒ [Section 1.2](#) « Le cluster miroir de SafeKit »
- ⇒ [Section 1.3](#) « Le cluster ferme de SafeKit »
- ⇒ [Section 1.4](#) « Clusters exécutant plusieurs modules »
- ⇒ [Section 1.5](#) « Le cluster Hyper-V ou KVM de SafeKit »
- ⇒ [Section 1.6](#) « Clusters SafeKit dans le cloud »

## 1.1 Généralités, solutions, architectures

### 1.1.1 Introduction à SafeKit

SafeKit, développé par Eviden, est une solution logicielle de haute disponibilité conçue pour garantir une disponibilité 24/7 des applications critiques pour les entreprises. Il prend en charge les plateformes Windows et Linux et élimine le besoin de disques partagés, d'éditions entreprises de bases de données ou de compétences techniques avancées, ce qui en fait une alternative rentable aux solutions de clustering traditionnelles.

Caractéristiques clés :

- Réplication synchrone en temps réel : Réplication continue des données entre les nœuds pour éviter toute perte de données.
- Basculement et retour automatiques : Basculement transparent vers un système secondaire en cas de panne et retour au système d'origine une fois opérationnel.
- Répartition de charge : Optimise l'utilisation des ressources en répartissant les charges de travail sur plusieurs serveurs.
- Indépendant de la plateforme : Compatible avec les machines physiques, les machines virtuelles et les infrastructures de cloud public.

Avantages clés :

- Aucune compétence spécifique : Aucune compétence informatique spécialisée requise pour le déploiement.
- Aucun surcoût matériel : Pas besoin de matériel spécifique comme des disques partagés ou des répartiteurs de charge.
- Aucun surcoût logiciel : Fonctionne avec les éditions standard de Windows et Linux.

Solutions clés :

- Niveau application : Haute disponibilité avec des scripts de redémarrage par application.
- Niveau hyperviseur : Haute disponibilité sans scripts de redémarrage par application.
- Niveau conteneur ou pod : Haute disponibilité sans scripts de redémarrage par application.

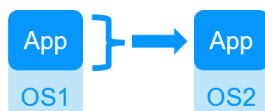
SafeKit est idéal pour les éditeurs de logiciels, les revendeurs et les distributeurs souhaitant améliorer leurs produits avec des fonctionnalités de haute disponibilité. Il offre également une opportunité OEM pour les partenaires d'intégrer SafeKit dans leurs propres applications.

### 1.1.2 Solutions SafeKit

[Cliquez ici pour une liste des solutions SafeKit.](#)

#### HA au niveau de l'application

Dans ce type de solution, seules les données applicatives sont répliquées. Et seule l'application est redémarrée en cas de panne.



Des tâches d'intégration doivent être mises en œuvre, comprenant la définition de la liste des services à redémarrer en cas de basculement, la spécification des dossiers de données pour la réplication, la configuration des vérificateurs logiciels et la mise en place d'une adresse IP virtuelle.

Cette solution est indépendante de la plate-forme et fonctionne avec des applications à l'intérieur de machines physiques, de machines virtuelles et dans le cloud. Tous les hyperviseurs sont pris en charge (par exemple, VMware, Hyper-V, etc.).

Note : Les applications exécutées dans des conteneurs ou des pods n'ont pas besoin non plus de scripts de redémarrage dédiés. SafeKit fournit des redémarrages génériques et une réplication en temps réel des données persistantes pour ces environnements ([voir la liste des solutions SafeKit](#)).

### 1.1.3 Architectures SafeKit

SafeKit propose deux clusters de haute disponibilité de base pour Windows et Linux :

- le **cluster miroir**, avec réplication de fichiers en temps réel et basculement, construit en déployant un module miroir sur 2 serveurs,
- Le **cluster ferme**, avec équilibrage de charge réseau et basculement, construit en déployant un module ferme sur 2 serveurs ou plus.

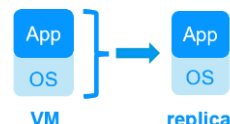
Plusieurs modules peuvent être déployés sur un même cluster. Ainsi, des architectures de clustering avancées peuvent être mises en œuvre :

- le **cluster ferme+miroir** construit en déployant un module ferme et un module miroir sur le même cluster,
- le **cluster actif/actif** construit en déployant plusieurs modules miroirs sur 2 serveurs,
- le **cluster N-1** construit en déployant N modules miroirs sur N+1 serveurs.

Des clusters spécifiques sont également intéressants à prendre en compte avec SafeKit :

#### HA au niveau de la machine virtuelle

Dans ce type de solution, l'intégralité de la machine virtuelle (VM) est répliquée, y compris l'application et le système d'exploitation. La machine virtuelle complète est redémarrée en cas de panne.



L'avantage est qu'il n'est pas nécessaire d'avoir une connaissance approfondie de l'application (services à redémarrer, localisation des données applicatives à répliquer), et aucune adresse IP virtuelle n'a besoin d'être configurée. Si vous ne savez pas comment fonctionne une application, c'est la solution la plus simple.

Cette solution fonctionne avec Windows/Hyper-V et Linux/KVM, mais pas avec VMware. Il s'agit d'une solution active/active avec plusieurs machines virtuelles répliquées et redémarrées entre les deux nœuds.

- le [cluster Hyper-V ou KVM](#) avec réplication en temps réel et basculement de machines virtuelles entières entre 2 hyperviseurs actifs,
- [des clusters ferme ou miroir dans le Cloud](#).

#### **1.1.4 Définition du cluster SafeKit**

Un cluster SafeKit est un ensemble de serveurs sur lesquels SafeKit est installé et en cours d'exécution.

Tous les serveurs d'un cluster SafeKit donné partagent la même configuration de cluster, qui inclut la liste des serveurs et des réseaux utilisés. Ces serveurs communiquent entre eux pour maintenir une vue globale des configurations des [modules SafeKit](#). Un serveur ne peut pas appartenir à plusieurs clusters SafeKit simultanément.

La configuration du cluster est une condition préalable à l'installation et à la configuration des modules SafeKit. Cela peut être fait à l'aide de la console Web de SafeKit ou de commandes en ligne.

#### **1.1.5 Définition du module applicatif SafeKit**

Un module applicatif est une personnalisation de SafeKit pour une application ou un hyperviseur spécifique. [Cliquez ici pour une liste des modules et leurs guides d'installation rapide](#).

##### **Types de modules**

- Modules génériques ferme et miroir pour de nouvelles applications,
- Modules d'application préconfigurés pour des bases de données, des serveurs web...,
- Modules hyperviseurs (hyperv.safe, kvm.safe) pour la réplication en temps réel et le redémarrage de machines virtuelles complètes.

##### **Contenu du module**

En pratique, un module applicatif est un fichier « .safe » (type zip) qui comprend :

- Le fichier de configuration userconfig.xml, qui contient :
  - L'adresse IP virtuelle (non nécessaire pour un module hyperviseur),
  - Répertoires de fichiers à répliquer en temps réel (pour un module miroir),
  - Critères d'équilibrage de charge réseau (pour un module ferme),
  - Configuration des détecteurs de pannes logicielles et matérielles,
- Les scripts permettant de démarrer et d'arrêter une application ou une machine virtuelle.

##### **Étapes de déploiement**

Une fois qu'un module applicatif est configuré et testé, le déploiement ne nécessite aucune compétence informatique spécifique :

- Installer l'application ou l'hyperviseur sur 2 serveurs standards,
- Installez le logiciel SafeKit sur les deux serveurs,
- Installez le module sur les deux serveurs.

La configuration, le déploiement et la surveillance des modules applicatifs peuvent être effectués à l'aide de la console Web de SafeKit ou de commandes en ligne.

## 1.1.6 Limites de SafeKit

<b>Utilisation typique avec SafeKit</b>			
Réplication de quelques téraoctets	Réplication < 1 millions de fichiers	Réplication <= 32 machines virtuelles	LAN 1 ou 10 G/s ou LAN étendu
<b>Limitation</b>			
<p>La <a href="#">resynchronisation après une défaillance</a> prend trop de temps.</p> <p>Sur un réseau de 1 Gbit/s, 3 heures pour 1 téraoctets.</p> <p>Sur un réseau 10 Gbit/s, 1 heure ou moins pour 1 téraoctets (dépend des performances d'E/S du disque en écriture).</p>	<p>La resynchronisation après une défaillance prend trop de temps.</p> <p>Temps de vérifier chaque fichier entre les deux nœuds.</p>	<p>En mode réplication complète de machines virtuelles, et avec une machine virtuelle dans un module miroir, la limite est de 32 modules par cluster.</p>	<p><a href="#">Le basculement de l'adresse IP virtuelle</a> est intégré lorsqu'on est dans le même sous-réseau.</p> <p>Un LAN fournit une bande passante adéquate pour la resynchronisation.</p> <p>Un LAN offre une latence adéquate (généralement un aller-retour de moins de 2 ms) pour la réplication synchrone.</p>
<b>Alternative</b>			
Utilisez un stockage partagé.	Mettez les fichiers dans un disque dur virtuel répliqué par SafeKit.	Utilisez une autre solution de HA avec stockage partagé.	Utilisez des solutions de backup avec réplication asynchrone.

## 1.2 Le cluster miroir de SafeKit

### 1.2.1 Réplication de fichiers en temps réel et basculement d'application

Le cluster miroir est une solution de haute disponibilité active-passive, créée en déployant un module miroir au sein d'un cluster à deux nœuds. L'application s'exécute sur un serveur primaire et est redémarrée automatiquement sur un serveur secondaire en cas de défaillance du serveur principal.

Avec sa fonction de réplication de fichiers temps réel, cette architecture est particulièrement adaptée pour fournir une haute disponibilité aux applications backend avec des données critiques à protéger contre les pannes.

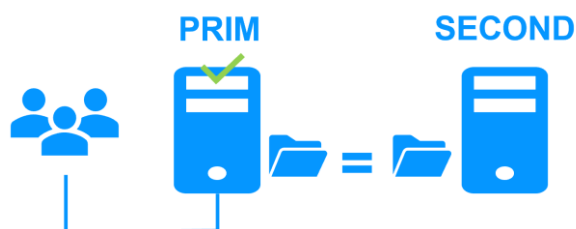
Les solutions Microsoft SQL Server, PostgreSQL, MariaDB, Oracle, Milestone, Nedap, Docker, Podman, Hyper-V et KVM sont des exemples de modules miroirs. Vous pouvez

créer votre propre module miroir pour votre application sur la base du module générique mirror.safe. [Voir ici une liste des modules applicatifs.](#)

Notez que les modules miroirs Hyper-V et KVM répliquent des machines virtuelles entières, y compris les applications et les systèmes d'exploitation. Ils ne nécessitent pas d'adresse IP virtuelle, car le redémarrage de la machine virtuelle gère le basculement de l'adresse IP physique de la VM.

Le cluster miroir fonctionne comme suit.

### 1.2.2 Étape 1. Fonctionnement normal



Le serveur 1 (PRIM) exécute l'application.

SafeKit réplique les fichiers ouverts par l'application. Seules les modifications apportées par l'application dans les fichiers sont répliquées en temps réel sur le réseau, limitant ainsi le trafic.

Pour la réplication, seuls les noms des répertoires de fichiers à répliquer sont configurés dans SafeKit. Il n'y a pas de conditions préalables à l'organisation des disques pour les deux serveurs. Les répertoires à répliquer peuvent se trouver sur le disque système.

### 1.2.3 Étape 2. Basculement



Lorsque le serveur 1 tombe en panne, le serveur 2 prend le relais. SafeKit bascule l'adresse IP virtuelle et redémarre automatiquement l'application sur le serveur 2. L'application retrouve les fichiers répliqués par SafeKit à jour sur le serveur 2, grâce à la réplication synchrone entre le serveur 1 et le serveur 2. L'application continue de s'exécuter sur le serveur 2 en modifiant localement ses fichiers qui ne sont plus répliqués sur le serveur 1.

Le temps de basculement est égal au temps de détection des pannes (défini à 30 secondes par défaut) plus le temps de démarrage de l'application. Contrairement aux solutions de réplication de disque, il n'y a pas de délai pour le remontage des systèmes de fichiers et l'exécution des procédures de récupération.

### 1.2.4 Étape 3. Réintégration et resynchronisation



La réintégration consiste à redémarrer le serveur 1 après avoir résolu le problème qui l'a mis en panne. SafeKit resynchronise automatiquement les fichiers, en ne mettant à jour que les fichiers modifiés sur le serveur 2 lorsque le serveur 1 a été arrêté.

Cette réintégration automatique s'effectue sans arrêter l'application, qui peut continuer à s'exécuter sur le serveur 2. Il s'agit d'une caractéristique majeure qui différencie SafeKit des autres solutions, qui nécessitent des opérations manuelles pour réintégrer le serveur 1 dans le cluster.

### 1.2.5 Étape 4. Retour au fonctionnement normal



Après la réintégration, les fichiers sont à nouveau en mode miroir, comme à l'étape 1. Le système est de nouveau en mode haute disponibilité, l'application s'exécutant sur le serveur 2 et SafeKit répliquant les mises à jour des fichiers sur le serveur 1.

Si les administrateurs souhaitent que l'application s'exécute sur le serveur 1, ils peuvent exécuter une commande « Stop / Start » sur le serveur PRIM soit à travers la console au moment opportun, soit automatiquement via la configuration d'un serveur primaire par défaut.

### 1.2.6 Réplication synchrone et réplication asynchrone

Il existe une différence significative entre la réplication synchrone, telle qu'elle est proposée par la solution miroir de SafeKit, et la réplication asynchrone traditionnellement proposée par d'autres solutions de réplication de fichiers.

Avec la réplication synchrone, lorsqu'une E/S disque est effectuée par l'application sur le serveur primaire à l'intérieur d'un fichier répliqué, SafeKit attend l'accusé de réception d'E/S du disque local et du serveur secondaire, avant d'envoyer l'accusé de réception d'E/S à l'application. Ce mécanisme est essentiel pour la récupération des applications transactionnelles.

La latence d'un LAN (généralement un aller-retour de moins de 2 ms) entre les serveurs est nécessaire pour mettre en œuvre la réplication synchrone des données, éventuellement avec un LAN étendu dans deux salles informatiques géographiquement éloignées.

Avec la réplication asynchrone implémentée par d'autres solutions, les E/S sont placées dans un journal sur le serveur primaire, mais le serveur primaire n'attend pas les accusés de réception d'E/S du serveur secondaire. Ainsi, toutes les données qui n'ont pas été

copiées à travers le réseau sur le deuxième serveur sont perdues en cas de défaillance du premier serveur.

En particulier, une application transactionnelle peut perdre des données validées en cas de défaillance. La réplication asynchrone peut être utilisée pour la réplication de données sur un WAN à faible vitesse afin de sauvegarder des données à distance (backup), mais elle n'est pas adaptée à la haute disponibilité avec basculement automatique.

SafeKit fournit une solution semi-synchrone, mettant en œuvre l'asynchronisme non pas sur le serveur primaire mais sur le secondaire. Dans cette solution, SafeKit attend toujours l'accusé de réception des deux serveurs avant d'envoyer l'accusé de réception à l'application. Mais sur le secondaire, il y a 2 options asynchrone ou synchrone. Dans le cas asynchrone, le secondaire envoie l'accusé de réception au primaire à la réception de l'E/S et écrit sur le disque par la suite. Dans le cas synchrone, le secondaire écrit l'E/S sur le disque, puis envoie l'accusé de réception au primaire. Le mode synchrone est nécessaire si l'on considère une double panne de courant simultanée de deux serveurs, avec l'impossibilité de redémarrer l'ancien serveur primaire et la nécessité de redémarrer sur le serveur secondaire.

### 1.2.7 Comportement en cas d'isolation réseau

Un **heartbeat** est un mécanisme permettant de synchroniser deux serveurs et de détecter les défaillances en échangeant des données sur un réseau partagé. Si un serveur perd tous les heartbeats, il suppose que l'autre est en panne et exécute l'application seul (état ALONE).

SafeKit supporte plusieurs heartbeats sur plusieurs réseaux partagés. Un réseau dédié avec un deuxième heartbeat peut éviter l'isolation réseau et être également utilisé comme réseau de réplication.

#### **Isolation réseau :**

- Sur perte de tous les heartbeats, les deux serveurs passent à l'état ALONE, exécutant l'application indépendamment.
- Après l'isolation, un serveur s'arrête et resynchronise les données à partir de l'autre serveur.
- Le cluster revient à l'état PRIM-SECOND.

#### **Checker splitbrain :**

- Utilise une adresse IP témoin (généralement un routeur) pour éviter la double exécution pendant l'isolation réseau.
- Seul le serveur avec un accès au témoin passe ALONE ; l'autre attend (WAIT).
- Après l'isolation, le serveur WAIT se resynchronise et devient SECOND.

### 1.2.8 Réplication à 3 nœuds

SafeKit ne supporte la réplication qu'entre deux nœuds. Cependant, il est possible de mettre en œuvre une réplication à 3 nœuds en combinant SafeKit avec une solution de sauvegarde.

Une application est rendue hautement disponible entre 2 nœuds grâce à SafeKit avec sa réplication synchrone en temps réel (sans perte de données) et son basculement automatique. De plus, une solution de sauvegarde est mise en œuvre pour la réplication asynchrone vers un troisième nœud dans un site de reprise après sinistre. Étant donné qu'il y a une perte de données avec une solution de sauvegarde asynchrone, le basculement vers le troisième nœud est manuel et décidé par un administrateur.

Notez que la réplication en temps réel de SafeKit n'élimine pas la nécessité d'une solution de sauvegarde. Par exemple, une attaque par ransomware chiffrant les données répliquées sur le serveur primaire chiffrera également les données sur le serveur secondaire en temps réel avec SafeKit. Seule une solution de sauvegarde avec une politique de rétention peut résoudre une attaque par ransomware. L'administrateur doit restaurer la sauvegarde d'avant l'attaque par ransomware.

### 1.2.9 SafeKit sur un seul nœud pour résister aux pannes logicielles

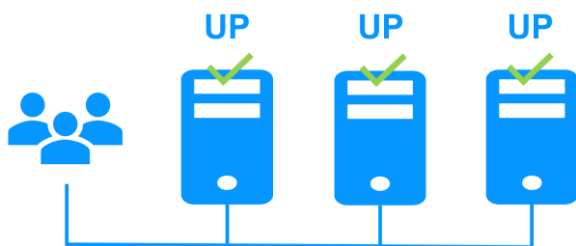
Vous pouvez configurer un module applicatif en mode "light", ce qui correspond à un module fonctionnant sur un seul nœud sans se synchroniser avec d'autres nœuds (contrairement aux modules miroir ou ferme). Un module "light" inclut le démarrage et l'arrêt d'une application, ainsi que les vérificateurs SafeKit qui détectent les erreurs logicielles et effectuent des redémarrages automatiques sur un seul nœud.

Le module "light" s'interface avec la console SafeKit, permettant à un administrateur de visualiser l'état du module et de déclencher manuellement des redémarrages de l'application via une interface clic-bouton.

Il n'est pas nécessaire de définir une adresse IP virtuelle ou des répertoires à répliquer dans un module "light". Notez que cela peut servir également de première étape avant de passer à un module miroir ou à un module ferme

## 1.3 Le cluster ferme de SafeKit

### 1.3.1 Équilibrage de charge réseau et basculement d'application



Le cluster ferme est une solution de haute disponibilité active-active, créée en déployant un module ferme au sein d'un cluster de deux nœuds ou plus. Le cluster ferme fournit à la fois l'équilibrage de la charge réseau, grâce à une distribution transparente du trafic réseau, et le basculement logiciel et matériel. Cette architecture offre une solution simple pour supporter l'augmentation de la charge du système.

La même application s'exécute sur chaque serveur, et la charge est équilibrée par la répartition de l'activité réseau sur les différents serveurs de la ferme.

Les clusters fermes sont adaptés aux applications frontales telles que les services Web.

Les solutions Apache, Microsoft IIS, NGINX sont des exemples de modules ferme. Vous pouvez écrire votre propre module ferme pour votre application, basé sur le module générique farm.safe. [Voir ici pour une liste des modules applicatifs.](#)

### 1.3.2 Principe d'une adresse IP virtuelle avec équilibrage de charge réseau

L'adresse IP virtuelle est configurée localement sur chaque serveur de la ferme. Le trafic en entrée pour cette adresse est réparti entre tous les serveurs par un filtre au sein du noyau de chaque serveur.

L'algorithme d'équilibrage de charge à l'intérieur du filtre est basé sur l'identité des paquets clients (adresse IP du client, port TCP du client). En fonction de l'identité du

paquet client, un seul filtre sur un serveur accepte le paquet. Une fois qu'un paquet est accepté par le filtre sur un serveur, seuls le processeur et la mémoire de ce serveur sont utilisés par l'application répondant à la demande du client. Les messages de sortie sont envoyés directement du serveur d'application au client.

En cas de défaillance d'un serveur, le protocole de heartbeat de SafeKit dans une ferme reconfigure les filtres pour rééquilibrer le trafic entre les serveurs disponibles restants.

### 1.3.3 Équilibrage de charge pour les services Web avec ou sans état

Avec un serveur à état, l'affinité de session est requise. Le même client doit se connecter au même serveur sur plusieurs sessions TCP pour récupérer son contexte. Dans ce scénario, la règle d'équilibrage de charge dans SafeKit est configurée sur l'adresse IP du client. Cela garantit que le même client se connecte toujours au même serveur sur plusieurs sessions TCP, tandis que différents clients sont répartis sur différents serveurs de la ferme. Cette configuration est nécessaire lorsqu'il y a affinité de session.

Avec un serveur sans état, il n'y a pas d'affinité de session. Le même client peut se connecter à différents serveurs de la ferme sur plusieurs sessions TCP, car aucun contexte n'est stocké localement sur un serveur d'une session à l'autre. Dans ce cas, la règle d'équilibrage de charge dans SafeKit est configurée sur l'identité de session du client TCP. Cette configuration est optimale pour la distribution des sessions entre les serveurs, mais nécessite un service TCP sans affinité de session.

### 1.3.4 Solution de haute disponibilité en chaîne dans une ferme

Qu'est-ce qu'une solution de haute disponibilité en chaîne (également connue sous le nom de solution de haute disponibilité en cascade) ?

- Plusieurs serveurs sont liés en séquence : Si un serveur tombe en panne, le suivant dans la chaîne prend le relais.
- Gestion basée sur la priorité : Un seul serveur gère toutes les requêtes des clients, celui ayant la plus haute priorité dans la chaîne et qui est disponible.
- Processus de basculement : Si le serveur ayant la plus haute priorité tombe en panne, le prochain serveur disponible avec la plus haute priorité prend le relais.
- Réintégration : Lorsqu'un serveur revient en ligne et qu'il a la plus haute priorité, il reprend la gestion de toutes les requêtes des clients.
- Temps de récupération rapide : Cette solution a un temps de récupération rapide, car l'application est pré-démarrée sur tous les serveurs. Le temps de récupération est essentiellement le temps nécessaire pour reconfigurer les priorités entre les serveurs de la ferme (quelques secondes).
- Limitations de la réplication : Cette solution ne prend pas en charge la réplication en temps réel, qui est limitée à l'architecture miroir. Cependant, une [architecture combinée ferme+miroir](#) est disponible.

Pour mettre en œuvre une solution de haute disponibilité en chaîne, SafeKit offre une variable "power" dans les règles d'équilibrage de charge : elle se définit au niveau de chaque serveur du cluster. La variable power vous permet d'allouer plus ou moins de trafic à un serveur. Lorsque la variable power est définie comme un multiple de 64 entre les serveurs (par exemple, 1, 64, 64\*64, 64\*64\*64, ...), la solution de haute disponibilité en chaîne est mise en œuvre

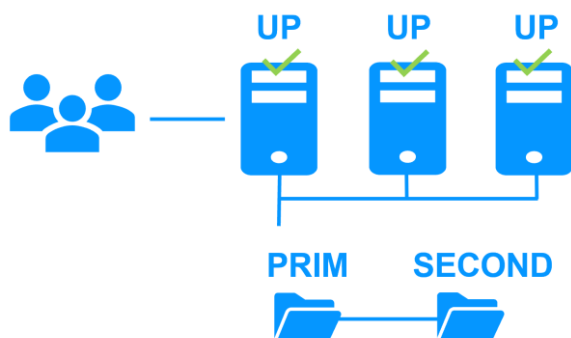
## 1.4 Clusters exécutant plusieurs modules

### 1.4.1 Le cluster ferme+miroir de SafeKit

#### Équilibrage de charge réseau, réplication de fichiers et basculement d'applications

Vous pouvez mélanger des modules ferme et miroir sur le même cluster.

Cette option vous permet d'implémenter une architecture d'application multiniveau, telle que `apache_farm.safe` (architecture ferme avec équilibrage de charge et basculement) et `postgresql.safe` (architecture miroir avec réplication de fichiers et basculement) sur les mêmes serveurs.

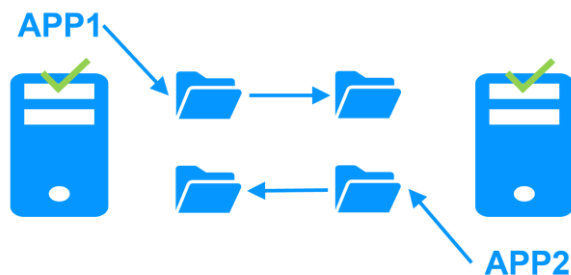


Par conséquent, l'équilibrage de charge, la réplication de fichiers et le basculement sont gérés de manière cohérente sur les mêmes serveurs.

### 1.4.2 Le cluster actif/actif avec réplication de SafeKit

#### Réplication croisée et basculement mutuel

Dans un cluster actif/actif avec réplication, il y a deux serveurs et deux modules miroirs en basculement mutuel (`appli1.safe` et `appli2.safe`). Chaque serveur d'application est une sauvegarde de l'autre serveur.



En cas de défaillance d'un serveur d'application, les deux applications s'exécutent sur le même serveur physique. Une fois le serveur défaillant redémarré, son application revient à son serveur primaire par défaut.

Un cluster de basculement mutuel est plus rentable que deux clusters miroirs distincts, car il élimine le besoin de serveurs de sauvegarde qui restent inactifs la plupart du temps, en attendant qu'un serveur principal tombe en panne. Toutefois, en cas de défaillance d'un serveur, le serveur restant doit être capable de gérer la charge de travail combinée des deux applications.

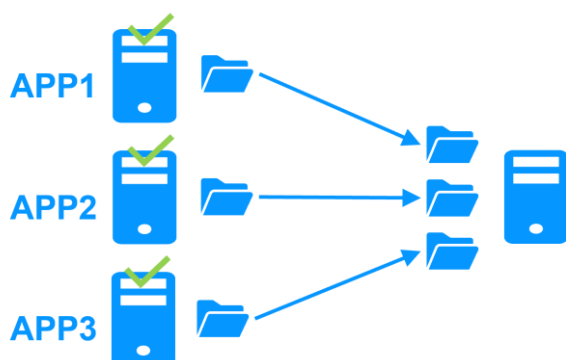
Notez que :

- Les deux applications, Appli1 et Appli2, doivent être installées sur chaque serveur pour permettre le basculement des applications.
- Cette architecture n'est pas limitée à deux applications ; N modules applicatifs peuvent être déployés sur les deux serveurs.
- Chaque module miroir aura sa propre adresse IP virtuelle, ses propres répertoires de fichiers répliqués et ses propres scripts de reprise.

### 1.4.3 Le cluster N-1 de SafeKit

#### Réplication et basculement d'applications de N serveurs vers 1

Dans un cluster N-1, N modules applicatifs miroirs sont déployés sur N serveurs principaux et un seul serveur de sauvegarde.



En cas de panne, contrairement à un cluster actif/actif, le serveur de sauvegarde n'a pas besoin de gérer une double charge de travail en cas de défaillance d'un serveur principal. Cela suppose qu'une seule défaillance se produit à la fois. Bien que la solution puisse prendre en charge plusieurs pannes de serveur principal simultanément, dans ce cas, le serveur de sauvegarde unique devra gérer la charge de travail combinée de tous les serveurs défaillants. Dans un cluster N-1, N modules applicatifs miroirs sont installés entre N serveurs principaux et un serveur de sauvegarde.

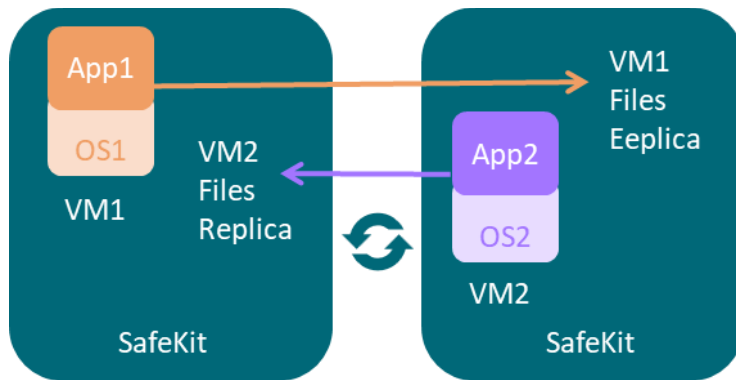
Notez que :

- Toutes les applications (Appli1, Appli2, Appli3) doivent être installées sur le serveur de sauvegarde unique pour permettre le basculement des applications.
- Chaque module miroir aura sa propre adresse IP virtuelle, ses propres répertoires de fichiers répliqués et ses propres scripts de reprise.

## 1.5 Le cluster Hyper-V ou KVM de SafeKit

### 1.5.1 Équilibrage de charge, réplication, basculement de machines virtuelles complètes

Le cluster Hyper-V ou KVM est un exemple de cluster actif-actif. Plusieurs applications peuvent être hébergées dans diverses machines virtuelles, qui sont répliquées et redémarrées par SafeKit. Chaque machine virtuelle est gérée par SafeKit au sein de son propre module miroir.



La solution présente les caractéristiques suivantes :

- Réplication synchrone en temps réel de machines virtuelles entières avec des capacités de basculement.
- Une console SafeKit centralisée et conviviale pour la gestion de toutes les machines virtuelles, y compris la possibilité de migrer des machines virtuelles entre les serveurs afin d'optimiser la répartition de la charge.
- Un checker pour chaque machine virtuelle afin de détecter si elle s'est verrouillée, s'est bloquée ou a cessé de fonctionner, et de redémarrer la machine virtuelle si nécessaire.
- Une solution attrayante qui ne nécessite aucune intégration d'application.
- Une architecture robuste adaptée aux solutions à haute disponibilité qui ne peuvent pas être intégrées au niveau applicatif.

[Une version d'essai gratuite du cluster Hyper-V avec SafeKit est disponible ici.](#)

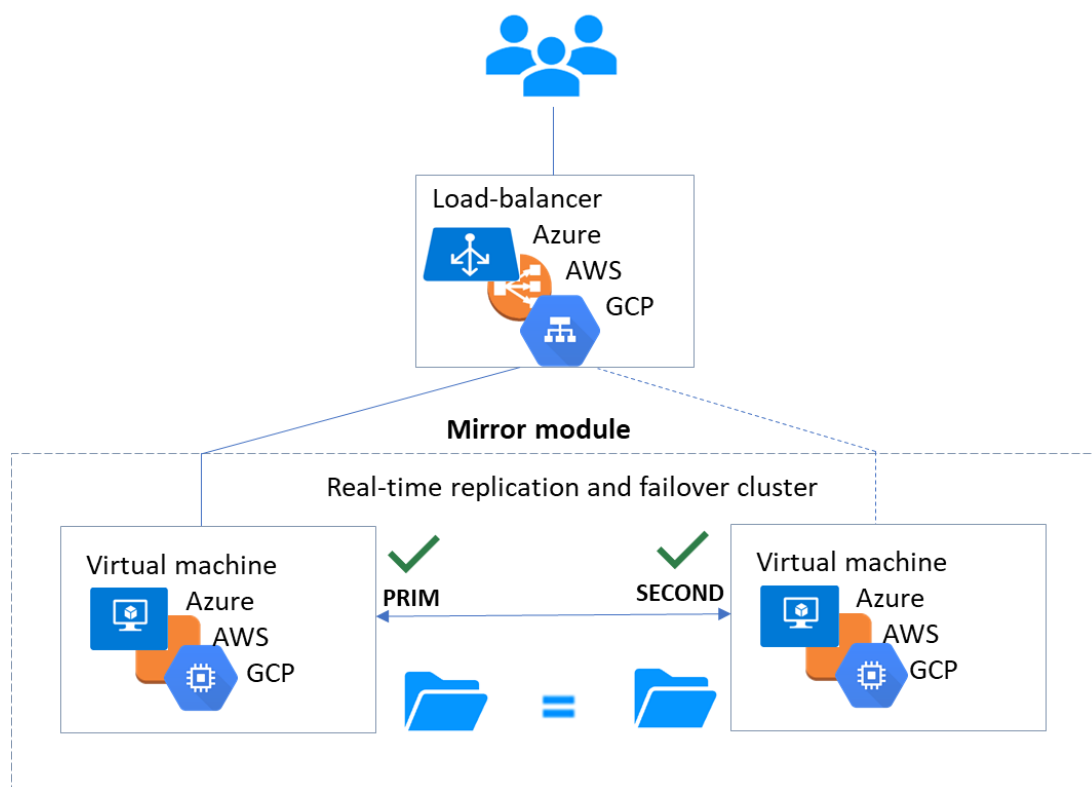
[Une version d'essai gratuite du cluster KVM avec SafeKit est disponible ici.](#)

## 1.6 Clusters SafeKit dans le cloud

Pour une description complète, voir la [section 16](#).

### 1.6.1 Cluster miroir dans Azure, AWS et GCP

SafeKit fournit des clusters de haute disponibilité avec réplication en temps réel et basculement dans Azure, AWS et GCP grâce au déploiement d'un module miroir.



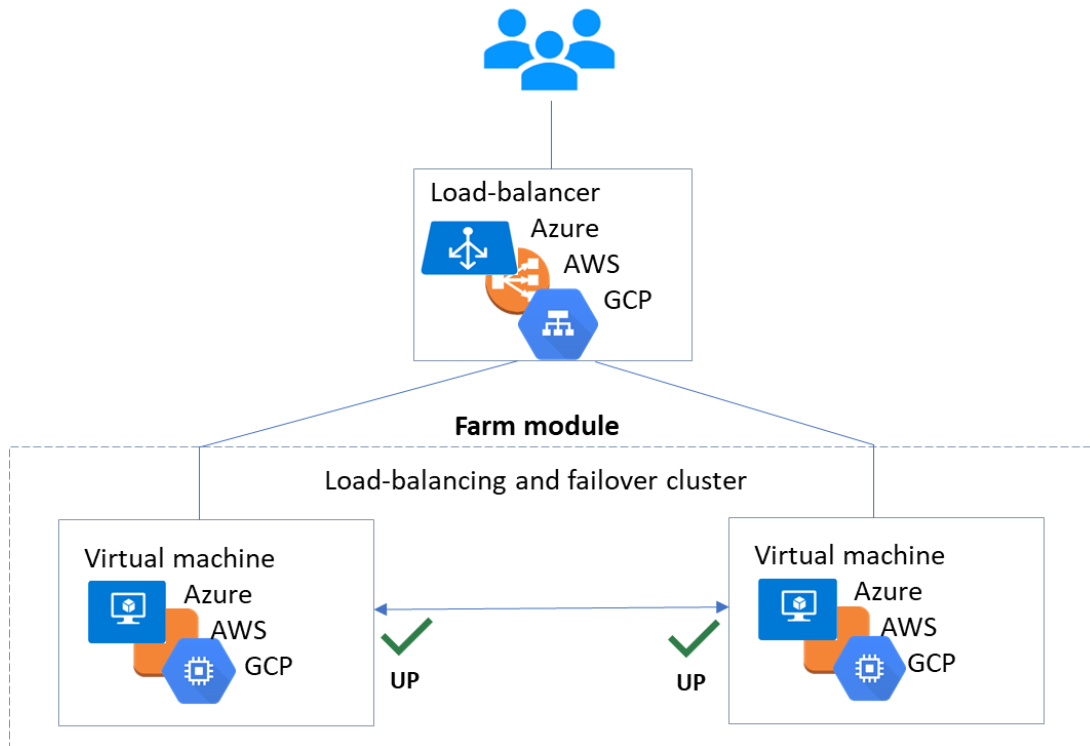
La solution miroir dans le cloud est similaire à celle sur site, mais l'adresse IP virtuelle doit être configurée au niveau de l'équilibreur de charge :

- Les machines virtuelles sont placées dans différentes zones de disponibilité, qui se trouvent dans des sous-réseaux différents.
- L'application critique s'exécute sur le serveur primaire.
- Les utilisateurs se connectent à une adresse IP virtuelle primaire/secondaire gérée par l'équilibreur de charge du cloud.
- SafeKit fournit un « health check » configuré dans l'équilibreur de charge. Sur le serveur primaire, le « health check » renvoie OK à l'équilibreur de charge, tandis qu'il ne renvoie rien sur le serveur secondaire. Ainsi, toutes les requêtes adressées à l'adresse IP virtuelle sont acheminées vers le serveur primaire.
- Si le serveur primaire tombe en panne ou est arrêté, le serveur secondaire devient automatiquement le serveur primaire et renvoie OK au « health check ». Ainsi, toutes les requêtes adressées à l'adresse IP virtuelle sont redirigées vers le nouveau serveur primaire.
- SafeKit surveille l'application critique sur le serveur primaire à l'aide des checkers de SafeKit.
- SafeKit redémarre automatiquement l'application critique en cas de défaillance logicielle ou matérielle, grâce à des scripts de redémarrage.
- SafeKit effectue une réplication synchrone en temps réel des fichiers contenant les données critiques.

Pour plus d'informations, consultez [le cluster miroir dans Azure](#), [le cluster miroir dans AWS](#) ou [le cluster miroir dans GCP](#).

### 1.6.2 Cluster ferme dans Azure, AWS et GCP

SafeKit fournit des clusters à haute disponibilité avec équilibrage de charge réseau et basculement dans Azure, AWS et GCP grâce au déploiement d'un module ferme.



La solution ferme dans le cloud est similaire à celle sur site, mais l'adresse IP virtuelle doit être configurée au niveau de l'équilibreur de charge :

- Les machines virtuelles sont placées dans différentes zones de disponibilité, qui se trouvent dans des sous-réseaux différents.
- L'application critique s'exécute sur tous les serveurs.
- Les utilisateurs sont connectés à une adresse IP virtuelle gérée par l'équilibreur de charge du cloud.
- SafeKit fournit un « health check » configuré dans l'équilibreur de charge. Le « health check » renvoie OK sur tous les serveurs exécutant l'application.
- En cas de défaillance ou d'arrêt d'un serveur, le « health check » ne renvoie rien à l'équilibreur de charge, qui arrête alors d'acheminer les requêtes vers ce serveur.
- SafeKit surveille l'application critique sur tous les serveurs à l'aide des checkers de SafeKit.
- SafeKit redémarre automatiquement l'application critique sur un serveur en cas de défaillance logicielle, grâce à des scripts de redémarrage.

Pour plus d'informations, consultez [le cluster ferme dans Azure](#), [le cluster ferme dans AWS](#) ou [le cluster ferme dans GCP](#)

## 2. Installation

- ⇒ [Section 2.1](#) « Installation de SafeKit »
- ⇒ [Section 2.2](#) « Recommandation pour une installation d'un module miroir »
- ⇒ [Section 2.3](#) « Recommandation pour une installation d'un module ferme »
- ⇒ [Section 2.4](#) « Upgrade de SafeKit »
- ⇒ [Section 2.5](#) « Désinstallation complète de SafeKit »
- ⇒ [Section 2.6](#) « Documentations SafeKit »

### 2.1 Installation de SafeKit

#### 2.1.1 Télécharger le package

1. Se connecter à [SafeKit product download area](#)
2. Aller dans <SafeKit 8.2>/Platforms/<Your platform>/Current versions
3. Télécharger le package

Windows	<p>Deux packages d'installation sont disponibles :</p> <ul style="list-style-type: none"><li>• <code>safekit_windows_x86_64_8_2_x_y.msi</code> Un package d'installation Windows (.msi). Ce package nécessite que le runtime C de Visual Studio 2022 soit préinstallé sur le système.</li><li>• <code>safekit_windows_x86_64_8_2_x_y.exe</code> Un exécutable autonome (.exe). Il inclut à la fois le package SafeKit et le runtime C de Visual Studio 2022, ce qui le rend adapté aux systèmes où ce runtime n'est pas encore installé.</li></ul> <p>Choisir l'un ou l'autre package suivant que le runtime C VS2022 est installé ou non.</p>
Linux	<p>Deux fichiers sont fournis, ainsi qu'une Key Id :</p> <ul style="list-style-type: none"><li>• <code>safekitlinux_x86_64_8_2_x_y.bin</code> Un fichier auto-extractible contenant, entre autres, les packages Linux et le script d'installation associé.</li><li>• <code>safekitlinux_x86_64_8_2_x_y.sha256</code> Un fichier contenant la somme de contrôle SHA-256 utilisée pour vérifier l'intégrité du fichier .bin.</li></ul> <p>Vous pouvez vérifier l'intégrité du .bin avec la commande :</p> <pre>sha256sum -c safekitlinux_x86_64_8_2_x_y.sha256</pre> <ul style="list-style-type: none"><li>• Key Id (e.g. 779244d710b22ada) L'identifiant, au format long, de la clé publique GPG utilisée pour signer les paquets RPM de SafeKit à partir de la version 8.2.5</li></ul>

	<p>pour Red Hat. Cette signature garantit à l'utilisateur l'installation d'un paquet vérifié, non altéré, provenant d'Eviden.</p> <p>Vous pouvez vérifier que le RPM est bien signé avec la clé SafeKit avec la commande ci-dessous. Celle-ci affiche l'identifiant (Key Id) de la clé de signature.</p> <pre>rpm -qi SafeKit-8.2.5-x.el9.x86_64.rpm</pre> <pre>... Signature: RSA/SHA256, ..., Key ID 779244d710b22ada ...</pre>
--	---

### 2.1.2 Répertoires d'installation et espace disque

SafeKit est installé dans :

SAFE	<ul style="list-style-type: none"> <li>sur Windows SAFE=C:\safekit si %SYSTEMDRIVE%=C:</li> <li>sur Linux SAFE=/opt/safekit</li> </ul>	Espace disque libre au minimum : 97MB
SAFEVAR	<ul style="list-style-type: none"> <li>sur Windows SAFEVAR= C:\safekit\var si %SYSTEMDRIVE%=C:</li> <li>sur Linux SAFEVAR=/var/safekit</li> </ul>	Espace disque libre minimum : 20MB + au moins 20MB (jusqu'à 3 GB) par module pour les dumps

### 2.1.3 Procédure d'installation de SafeKit

#### 2.1.3.1 Installation sur Windows en tant qu'Administrateur

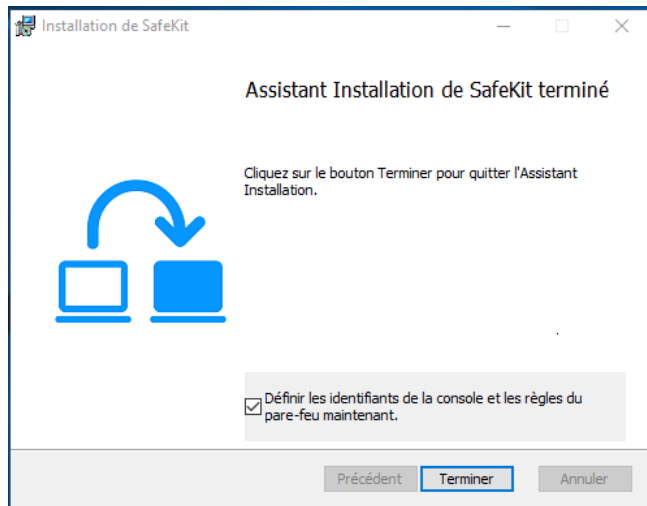
Les journaux d'installation de SafeKit se trouvent dans le répertoire SAFEVAR.

##### 2.1.3.1.1 Installation du package SafeKit

1. Se loguer en tant qu'administrateur sur le serveur Windows
2. Localiser le fichier téléchargé safekit\_windows\_x86\_64\_8\_2\_x\_y.msi (ou safekit\_windows\_x86\_64\_8\_2\_x\_y.exe)
3. Installer en mode interactif en double-cliquant dessus puis dérouler l'assistant d'installation.

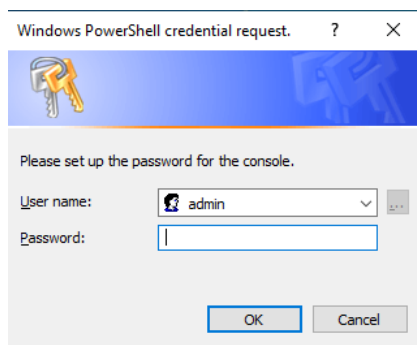
Avant SafeKit 8.2.3, après l'installation, vous devez exécuter les scripts de configuration du pare-feu (voir la [section 10.3](#)) et d'initialisation du service web SafeKit (voir la [section 11.2.1.2](#)).

Depuis SafeKit 8.2.3, à la fin de l'installation, il vous est demandé de cocher ou décocher « Définir les identifiants de la console et les règles du pare-feu maintenant. ».



Si la case reste cochée, lorsque le bouton « Terminer » est cliqué :

- Le pare-feu Microsoft est configuré pour SafeKit. Pour plus de détails ou d'autres pare-feu, voir la [section 10.3](#).
- Une fenêtre est ouverte pour entrer le mot de passe de l'utilisateur `admin` de la console web de SafeKit.



Cette étape est obligatoire pour initialiser la configuration par défaut du service web qui nécessite de s'authentifier. Elle est initialisée avec l'utilisateur `admin` et le mot de passe saisi, par exemple `pwd`. Cela permet ensuite d'accéder à toutes les fonctionnalités de la console web, en se connectant avec `admin/pwd`, et d'exécuter des commandes distribuées. Pour plus de détails, voir la [section 11.2.1](#).



Le mot de passe doit être identique sur tous les nœuds qui appartiennent au même cluster SafeKit. Sinon, la console web et les commandes distribuées échoueront avec des erreurs d'authentification.

Ou

3. Installer le `.msi` en mode non interactif en exécutant dans un terminal PowerShell en tant qu'administrateur :

```
msiexec /qn /i safekitwindows_8_2_x_y.msi
```

Une fois installé, la configuration du pare-feu et l'initialisation du service web SafeKit doivent être effectués manuellement.

### 2.1.3.1.2 Paramétrage du pare-feu

Cette étape est obligatoire pour permettre les communications entre les nœuds du cluster SafeKit, et avec la console web.

Aucune action supplémentaire n'est requise lorsque la configuration automatique du pare-feu a été appliquée pendant l'installation du package  $\geq 8.2.3$ . Sinon, voir la [section 10.3](#).

### 2.1.3.1.3 Initialisation du service web SafeKit

Cette initialisation est nécessaire pour la console web et les commandes distribuées.

Aucune action requise si l'initialisation a été faite pendant l'installation du package  $\geq 8.2.3$ . Sinon, voir la [section 11.2.1.2](#).

### 2.1.3.1.4 Paramétrage des antivirus

Cette étape est nécessaire en cas d'interférence de l'antivirus du serveur sur le fonctionnement de SafeKit. Comme ce problème (décrit dans la [section 7.22](#)) peut survenir de manière sporadique mais non systématique avec Windows Defender, il est recommandé de le configurer afin d'éviter tout dysfonctionnement.

Voir la [section 10.6](#) pour la liste des répertoires et processus légitimes de SafeKit qui ne doivent pas être impactés par l'antivirus.

## 2.1.3.2 Installation sur Linux en tant que root

Depuis SafeKit 8.2.6, les journaux d'installation de SafeKit sont générés dans le répertoire `/tmp/safekit`.

### 2.1.3.2.1 Installation du package SafeKit

1. Se loguer en tant que root sur le serveur Linux
2. Localiser le fichier téléchargé `safekitlinux_x86_64_8_2_x_y.bin`
3. Exécuter `chmod +x safekitlinux_x86_64_8_2_x_y.bin`
4. Exécuter `./safekitlinux_x86_64_8_2_x_y.bin`

Cela extrait le package SafeKit et le script `safekitinstall`

5. Installer en mode interactif en exécutant `./safekitinstall`

Pendant l'installation :

- Depuis SafeKit 8.2.5 sur Red Hat, répondre à "Do you accept to import this public key (yes|no)?"

Les packages RPM de SafeKit sont désormais signés avec une clé GPG. En répondant `yes`, le script importe automatiquement la clé publique GPG de SafeKit et poursuit le processus d'installation. Si vous répondez `no`, l'installation sera interrompue.



Le script affiche l'identifiant de la clé (Key ID) utilisée pour signer le paquet RPM. Vous pouvez vérifier cette valeur en la comparant avec celle publiée officiellement dans [SafeKit product download area](#).

La clé publique GPG utilisée pour signer le paquet RPM est extraite en même temps que le paquet, dans le fichier nommé `RPM-GPG-KEY-SafeKit`. Vous pouvez récupérer la Key ID avec la commande suivante :



```
gpg --show-keys --no-options RPM-GPG-KEY-SafeKit
```

(Key ID correspond aux 16 derniers caractères de la ligne pub)

- Répondre à "Do you accept that SafeKit automatically configure the local firewall to open these ports (yes|no)?"

Si vous répondez `yes`, le pare-feu Linux `firewalld` ou `iptables` est configuré pour SafeKit. Pour plus de détails ou d'autres pare-feu, voir la [section 10.3](#).

- Répondre à "Please enter a password or "no" if you want to set it later".

La saisie d'un mot de passe est obligatoire pour initialiser la configuration par défaut du service web. Celui-ci nécessite en effet de s'authentifier pour y accéder.

Si vous répondez `pwd` par exemple, cette valeur est utilisée comme mot de passe pour l'utilisateur `admin`. Cela permet ensuite d'accéder à toutes les fonctionnalités de la console web, en se connectant avec `admin/pwd`, et d'exécuter des commandes distribuées. Pour plus de détails, voir la [section 11.2.1](#).



Le mot de passe doit être identique sur tous les nœuds qui appartiennent au même cluster SafeKit. Sinon, la console web et les commandes distribuées échoueront avec des erreurs d'authentification.

## Ou

5. Installer en mode non interactif en exécutant :

```
./safekitinstall -q
```

Ajouter l'option `-passwd pwd` pour initialiser l'authentification, requise par le service web (`pwd` est le mot de passe affecté à l'utilisateur `admin`).

Une fois installé, la configuration du pare-feu être effectuée manuellement.



À partir de la version 8.2.5 de SafeKit sur Red Hat, les paquets RPM sont signés avec une clé GPG. Ainsi, la clé publique GPG de SafeKit est automatiquement importée pour permettre la poursuite de l'installation.

### 2.1.3.2.2 Paramétrage du pare-feu

Cette étape est obligatoire pour permettre les communications entre les nœuds du cluster SafeKit et avec la console web.

Aucune action supplémentaire n'est requise lorsque la configuration automatique du pare-feu a été appliquée pendant l'installation interactive du package. Sinon, voir la [section 10.3](#).

### 2.1.3.2.3 Initialisation du service web SafeKit

Cette initialisation est nécessaire pour la console web et les commandes distribuées.

Aucune action requise si l'initialisation a été faite pendant l'installation du package. Sinon, voir la [section 11.2.1.2](#).

### 2.1.3.2.4 Paramétrage des antivirus

Cette étape est nécessaire uniquement en cas d'interférence de l'antivirus du serveur sur le fonctionnement de SafeKit. Voir la [section 10.6](#) pour la liste des répertoires et processus légitimes de SafeKit qui ne doivent pas être impactés par l'antivirus.

### 2.1.4 Utilisation de la console web et de la ligne de commande SafeKit

Une fois installé, le cluster SafeKit doit être défini. Ensuite, les modules applicatifs peuvent être installés, configurés et administrés. Toutes ces actions peuvent être effectuées avec la console ou l'interface en ligne de commande.

#### 2.1.4.1 La console web SafeKit

1. Démarrer un navigateur web (Microsoft Edge, Firefox ou Chrome)
2. Le connecter à l'URL `http://host:9010` (où `host` est l'adresse IP ou le nom d'un nœud SafeKit)
3. Dans la section de login, s'identifier avec `admin` comme nom d'utilisateur et le mot de passe que vous avez donné pendant l'initialisation juste au-dessus (par exemple, `pwd`)
4. Une fois la console chargée, l'utilisateur `admin` a accès à la  « Supervision » et à la  « Configuration » dans la barre latérale de navigation, car il a le rôle `Admin` par défaut

Pour une description complète, voir la [section 3](#).

#### 2.1.4.2 La ligne de commande SafeKit

Elle repose sur la commande unique `safekit` située à la racine du répertoire d'installation de SafeKit. Presque toutes les commandes `safekit` peuvent être appliquées localement ou sur une liste de nœuds du cluster SafeKit. C'est ce qui est appelé commande globale ou distribuée.

Pour une description complète de la commande, voir la [section 9](#).

Pour utiliser la commande `safekit` :

Windows	<ol style="list-style-type: none"><li>1. Ouvrir une console PowerShell en tant qu'administrateur</li><li>2. Aller à la racine du répertoire d'installation de SafeKit <code>SAFE</code> (par défaut <code>SAFE=C:\safekit</code> si <code>%SYSTEMDRIVE%=C:</code>) <code>cd c:\safekit</code></li><li>3. Exécuter <code>.\safekit.exe &lt;arguments&gt;</code> pour la commande locale</li><li>4. Exécuter <code>.\safekit.exe -H "&lt;hosts&gt;" &lt;arguments&gt;</code> pour la commande distribuée sur plusieurs nœuds</li></ol>
Linux	<ol style="list-style-type: none"><li>1. Ouvrir une console Shell en tant que root</li><li>2. Aller à la racine du répertoire d'installation de SafeKit <code>SAFE</code> (par défaut <code>SAFE=/opt/safekit</code>) <code>cd /opt/safekit</code></li><li>3. Exécuter <code>./safekit &lt;arguments&gt;</code> pour la commande locale</li></ol>

- 
- |  |   |
|--|---|
|  | 4. Exécuter <code>./safekit -H "&lt;hosts&gt;" &lt;arguments&gt;</code> pour la commande distribuée sur plusieurs nœuds |
|--|---|
- 

Par exemple, pour afficher la version (SafeKit, OS...) :

- pour le nœud local

```
safekit level
```

- pour tous les nœuds configurés dans le cluster SafeKit

```
safekit -H "*" level
```

## 2.1.5 Clés de licence SafeKit

Les clés de licence sont déterminées et vérifiées en fonction du système d'exploitation (Windows ou Linux) et des noms d'hôtes des machines (pas le FQDN), comme renvoyé par la commande `hostname` dans une invite de commandes Windows ou un shell Linux. Elles sont livrées dans un fichier texte. Une fois le fichier de clé de licence installé, il n'est plus nécessaire d'être connecté à un serveur de licence.

- Si vous n'installez pas de fichier de clé de licence, le produit cessera de fonctionner tous les 3 jours. Cependant, il peut être redémarré pour 3 jours supplémentaires.
- Vous pouvez [télécharger un fichier de clé d'essai ici](#).
- Lorsque la clé de licence expire ou est incorrecte (par exemple, système d'exploitation ou nom d'hôte erroné), le système entre dans le comportement de 3 jours.
- Après avoir passé une commande d'achat, vous obtenez un fichier de clé permanent. Le fichier de clé permanent peut être installé sans réinstaller ou arrêter le produit.
- Le fichier de clé peut contenir des clés pour plusieurs noms d'hôtes. SafeKit détectera la licence appropriée pour le bon système d'exploitation/nouveau d'hôte sur chaque serveur.
- Enregistrez le fichier de clé dans le fichier `SAFE/conf/license.txt` (ou tout autre fichier dans `SAFE/conf`) sur chaque serveur.
- Si les fichiers dans `SAFE/conf` contiennent plus d'un fichier de clé, la clé la plus favorable sera choisie.
- Vérifiez la conformité de la clé sur chaque serveur avec la commande `SAFE/safekit level` ou avec la console web SafeKit.

## 2.1.6 Caractéristiques spécifiques à chaque OS

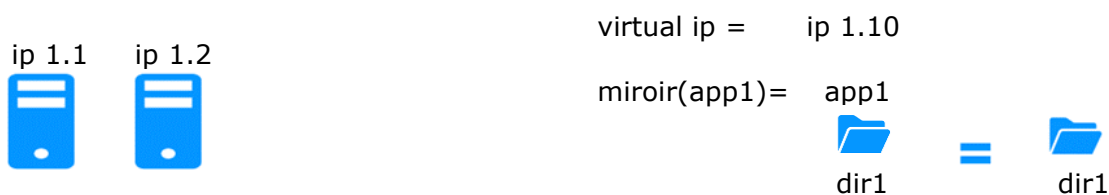
### 2.1.6.1 Windows

- Il faut appliquer une procédure spéciale pour arrêter proprement les modules applicatifs au shutdown d'une machine et démarrer le service `safeadmin` au boot (voir la [section 10.4](#))
- En cas d'interfaces réseau en teaming avec du load balancing SafeKit, il est nécessaire de décocher "Vip" sur les interfaces réseau physiques de teaming et de le conserver coché seulement sur l'interface virtuelle de teaming

### 2.1.6.2 Linux

- En Linux, le package SafeKit dépend d'autres packages système. La plupart sont installés automatiquement, excepté ceux spécifiques à la mise en œuvre du load balancing dans une ferme et de la réplication de fichiers dans un miroir.
- Pour la liste à jour des packages nécessaires, voir le [SafeKit Release Notes](#).
- L'utilisateur `safekit` et un groupe `safekit` sont créés : tous les utilisateurs appartenant au groupe `safekit` et l'utilisateur `root` peuvent exécuter des commandes SafeKit.
- Dans une ferme avec load balancing, le module kernel `vip` est compilé au moment de la configuration du module applicatif. Pour réussir la compilation, des packages Linux doivent être installés. Voir le [SafeKit Release Notes](#) pour une liste des packages à jour.
- En ferme avec load balancing sur une interface de bonding, pas d'ARP dans la configuration de bonding. Sinon l'association <adresse IP virtuelle, adresse MAC virtuelle invisible> est cassée dans les caches ARP des clients avec l'adresse MAC physique de la carte de bonding.
- Lorsque Secure Boot est activé et que vous utilisez un module ferme, suivez la procédure décrite à la [section 10.5](#) pour signer et enregistrer les modules kernel SafeKit qui implémentent le load balancing.

## 2.2 Recommandation pour une installation d'un module miroir



### 2.2.1 Prérequis matériel et système

- au moins 2 serveurs avec le même système d'exploitation
- [OS supportés](#)
- Contrôleur disque avec cache write-back recommandé pour la performance des IO

### 2.2.2 Prérequis réseau

- 1 adresse IP physique par serveur (ip 1.1 et ip 1.2)
- Si vous devez définir une adresse IP virtuelle (ip 1.10), les deux serveurs doivent appartenir au même réseau IP avec la configuration standard de SafeKit (LAN ou LAN étendu entre deux salles informatiques distantes). Dans le cas contraire, voir une alternative dans la [section 13.6.3](#).

### 2.2.3 Prérequis application

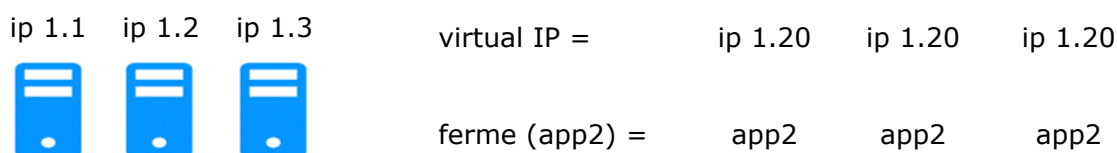
- L'application est installée et démarre sur les 2 serveurs
- L'application fournit des commandes en ligne pour démarrer et s'arrêter
- Sur Linux, commandes du style : `service "service" start|stop` ou `su -user "appli-cmd"`

- Sur Windows, commandes du style : `net start|stop "service"`
- Si nécessaire, définir une procédure de reprise suite à un crash serveur
- Retirer le démarrage automatique au boot de l'application et le remplacer par la configuration du démarrage au boot du module applicatif

### 2.2.4 Prérequis réplication de fichiers

- Les répertoires de fichiers qui seront répliqués sont créés sur les 2 serveurs
- Ils se situent au même endroit sur les 2 serveurs dans l'arborescence fichier
- Il vaut mieux synchroniser les horloges des 2 serveurs pour la réplication de fichiers (protocole NTP)
- Sous Linux, aligner les valeurs des uids/gids sur les 2 serveurs pour les propriétaires des répertoires et fichiers à répliquer
- Voir aussi la [section 2.1.6](#)

## 2.3 Recommandation pour une installation d'un module ferme



### 2.3.1 Prérequis matériel et système

- au moins 2 serveurs avec le même système d'exploitation
- [OS supportés](#)
- Linux : outils de compilation du kernel installés pour le module kernel vip

### 2.3.2 Prérequis réseau

- 1 adresse IP physique par serveur (ip 1.1, ip 1.2, ip 1.3)
- Si vous devez définir une adresse IP virtuelle (ip 1.20), les serveurs doivent appartenir au même réseau IP avec la configuration standard de SafeKit (LAN ou LAN étendu entre les salles informatiques distantes). Dans le cas contraire, voir une alternative décrite dans la [section 13.6.3](#)
- Voir aussi la [section 2.1.6](#)

### 2.3.3 Prérequis application

Les mêmes prérequis que pour un module miroir décrits en [section 2.2.3](#).

## 2.4 Upgrade de SafeKit

Si vous rencontrez un problème avec SafeKit, consulter le [Software Release Bulletin](#) pour consulter la liste des fixes produits.

Si vous souhaitez profiter de nouvelles fonctionnalités, consulter le [SafeKit Release Notes](#). Ce document vous indiquera également si vous êtes dans le cas d'un upgrade

majeur (ex. 7.5 vers 8.2) qui nécessite d'effectuer une procédure différente de celle présentée ici.

La procédure d'upgrade consiste à désinstaller l'ancien package puis à réinstaller le nouveau package. Tous les nœuds du même cluster doivent être upgradé.

### 2.4.1 Préparer l'upgrade

1. Noter l'état "on" ou "off" des services et modules applicatifs de SafeKit démarrés automatiquement au boot

`safekit boot webstatus ; safekit boot status -m AM` (où *AM* est le nom du module) et en Windows : `safekit boot snmpstatus`



Le démarrage au boot du module applicatif peut être défini dans son fichier de configuration. Si c'est le cas, l'usage de la commande `safekit boot` devient inutile.

2. Pour un module miroir

Noter le serveur qui est dans l'état `ALONE` ou `PRIM` afin de connaître le serveur avec les fichiers répliqués à jour

3. Prise de snapshots, facultative

La désinstallation/réinstallation va réinitialiser les logs SafeKit et effacer les dumps de chaque module. Si vous souhaitez conserver ces informations, exécuter la commande `safekit snapshot -m AM /chemin/snapshot_xx.zip` pour chaque module (où *AM* est le nom du module)

### 2.4.2 Procédure de désinstallation

Sur Windows en tant qu'administrateur et sur Linux en tant que root :

1. Arrêter tous les modules applicatifs avec la commande `safekit shutdown`

Pour un module miroir dans l'état `PRIM-SECOND`, commencer par l'arrêt du serveur `SECOND` afin d'éviter un basculement inutile

2. Fermer tous les éditeurs, explorateur de fichiers, shells ou terminaux sous `SAFE` et `SAFEVAR`
3. Désinstaller le package SafeKit

Windows	Désinstaller via Control Panel-Add/Remove Programs applet
Linux	Utiliser la commande <code>safekit uninstall</code>



4. Défaire les modifications manuelles effectuées sur le pare-feu




Voir la [section 10.3](#)


La désinstallation de SafeKit inclut la création d'un backup des modules installés dans `SAFE/Application_Modules/backup`, puis leur déconfiguration.

### 2.4.3 Procédure de réinstallation et post-installation pour l'upgrade

1. Installer le nouveau package comme décrit dans la [section 2.1](#)
2. Vérifier avec la commande `safekit level` la version SafeKit installée et la validité de la licence qui n'a pas été désinstallée

3. Si vous avez un problème avec le nouveau package et l'ancienne clé, prendre une licence temporaire (voir [section 2.1.5](#))
4. Si la console web est utilisée, vider le cache du navigateur web et forcer l'actualisation des pages HTML
5. Depuis SafeKit 8.2.1, les modules précédemment configurés sont automatiquement reconfigurés sur upgrade.  
Cependant, vous pouvez avoir à reconfigurer quand même le module pour appliquer d'éventuelles évolutions de configuration apportées par la nouvelle version (consulter le [SafeKit Release Notes](#)). Reconfigurer le module soit avec :
  - o la console web en naviguant sur  « Configuration/Configuration des modules/ Configurer le module/ »
  - o la console web en entrant directement l'URL <http://host:9010/console/fr/configuration/modules/AM/config/>
  - o la commande `safekit config -m AM`
  - o où *AM* est le nom du module
6. Reconfigurer le démarrage automatique du module au boot si nécessaire
7. Le démarrage du module au boot peut être défini dans son fichier de configuration. Si c'est le cas, passer cette étape. Si non, exécuter la commande `safekit boot -m AM on` (où *AM* est le nom du module)
8. Redémarrer les modules

Module miroir	<p>Le module doit être démarré en primaire sur le nœud ayant les fichiers répliqués à jour (ancien <code>PRIM</code> ou <code>ALONE</code>) :</p> <ul style="list-style-type: none"> <li>• Avec la console web en naviguant sur  « Supervision/... du nœud/Forcer le démarrage/En primaire »</li> <li>• Avec la commande <code>safekit prim -m AM</code> (remplacer <i>AM</i> par le nom du module)</li> </ul> <p>Vérifier que l'application fonctionne correctement une fois le module dans l'état <code>ALONE</code> avant de démarrer l'autre nœud.</p> <p>Sur l'autre nœud (ancien <code>SECOND</code>), le module doit être démarré en secondaire :</p> <ul style="list-style-type: none"> <li>• Avec la console web en naviguant sur  « Supervision/... du nœud/Forcer le démarrage/En secondaire »</li> <li>• Avec la commande <code>safekit second -m AM</code> (remplacer <i>AM</i> par le nom du module)</li> </ul> <p>Une fois ce premier démarrage réalisé en sélectionnant les nœuds primaire et secondaire, les démarrages suivants peuvent être effectués avec :</p> <ul style="list-style-type: none"> <li>• Avec la console web en naviguant sur  « Supervision/... du nœud/▶ Démarrer/ »</li> <li>• Avec la commande <code>safekit start -m AM</code> (remplacer <i>AM</i> par le nom du module)</li> </ul>
---------------	---

Module ferme	<p>Démarrer le module soit avec :</p> <ul style="list-style-type: none"><li>• Avec la console web en naviguant sur  « Supervision/ ... du nœud/ ▶ Démarrer/ »</li><li>• Avec la commande <code>safekit start -m AM</code> (remplacer <code>AM</code> par le nom du module)</li></ul>
-----------------	--

De plus, dans les cas exceptionnels où vous aviez modifié la configuration par défaut du service web SafeKit ou de la surveillance SNMP.

### 1. Le service web de SafeKit `safewebserver`

- Si son démarrage automatique avait été désactivé, désactivez-le à nouveau avec la commande `safekit boot weboff`
- Si vous aviez modifié des fichiers de configuration et que ceux-ci ont évolué dans la nouvelle version, vos modifications ont été sauvegardées dans `SAFE/web/conf` avant d'être écrasées par la nouvelle version. Le report de votre ancienne configuration dans la nouvelle version peut nécessiter quelques adaptations. Pour plus de détails sur la configuration par défaut et toutes les configurations prédéfinies, voir la [section 11](#).

Pour les configurations HTTPS et login/mot de passe, les certificats et les fichiers `user.conf/group.conf` générés pour la version précédente devraient être compatibles.

### 2. L'agent SafeKit de notification par courriel

Depuis SafeKit 8.2.4, SafeKit propose un agent de notification pour envoyer des courriels lors des événements majeurs sur les modules. Pour plus de détails, consultez la [section 10.10](#).

Si vous l'avez activé, il restera activé après la mise à jour de SafeKit. Cependant, vous devrez peut-être reconfigurer l'agent de notification SafeKit, comme décrit dans la [section 10.10.1](#), si son fichier de configuration a évolué entre les deux versions.

### 3. La surveillance SNMP de SafeKit

- En Windows, si son démarrage automatique avait été activé, réactivez-le à nouveau avec la commande `safekit boot snmpon`
- Si vous aviez modifié des fichiers de configuration et que ceux-ci ont évolué dans la nouvelle version, vos modifications ont été sauvegardées dans `SAFE/snmp/conf` avant d'être écrasées par la nouvelle version. Le report de votre ancienne configuration dans la nouvelle version peut nécessiter quelques adaptations. Pour plus de détails, voir la [section 10.11](#).

## 2.5 Désinstallation complète de SafeKit

Suivre la procédure décrite ci-dessous pour désinstaller complètement SafeKit.

### 2.5.1 Désinstallation sur Windows

1. Se loguer en tant qu'administrateur sur le serveur Windows
2. Arrêter tous les modules à l'aide de la commande `safekit shutdown`

3. Fermer tous les éditeurs, explorateur de fichiers, ou terminaux sous SAFE et SAFEVAR (SAFE=C:\safekit si %SYSTEMDRIVE%=C: ; SAFEVAR=C:\safekit\var si %SYSTEMDRIVE%=C:)
4. Désinstaller le package SafeKit via Control Panel-Add/Remove Programs
5. Redémarrer le serveur
6. Détruire le répertoire SAFE qui correspond à l'installation précédente de SafeKit
7. Défaire les modifications effectuées pour configurer le démarrage au boot/l'arrêt au shutdown de SafeKit (voir la [section 10.4](#))
8. Défaire les modifications manuelles effectuées sur le pare-feu (voir la [section 10.3](#))
9. Désinstallez l'application Web SafeKit si elle est installée (voir [section 3.1.4.2](#))
10. Depuis SafeKit 8.2.5, les pilotes SafeKit suivants sont désinstallés mais ne sont plus automatiquement supprimés de Windows Driver Store :
  - viplwf (Virtual IP load balancer)
  - ndis6pckt (ARP rerouter)
  - rfsfilter (File replication filter)

Si vous souhaitez les supprimer du Driver Store, suivez la procédure ci-dessous :

- a. Assurer que tous les services liés aux pilotes sont arrêtés en exécutant les commandes suivantes :

```
net stop rfsfilter
net stop viplwf
net stop ndis6pckt
```

- b. Lister tous les paquets de pilotes tiers installés dans le Windows Driver Store avec la commande :

```
pnputil /enum-drivers
```

Exemple de sortie :

```
...
Published Name:  oem4.inf
Original Name:   ndis6pckt.inf
Provider Name:   Evidian
Class Name:      Network Protocol
...
Published Name:  oem18.inf
Original Name:   saferfs.inf
Provider Name:   Evidian
Class Name:      FS Replication filters
...
Published Name:  oem5.inf
Original Name:   viplwf.inf
Provider Name:   Evidian
Class Name:      Network Service
...
```

- c. Identifier le 'Published name' (oemxx.inf) correspondant aux pilotes SafeKit  
Rechercher les entrées dont 'Original Name' correspond à : viplwf.inf, ndis6pckt.inf, et saferfs.inf.

- d. Supprimer chaque pilote SafeKit en utilisant la commande :

```
pnputil /delete-driver oemxx.inf /uninstall
```

Remplacer `oemxx.inf` par le nom exact identifié à l'étape c.

### 2.5.2 Désinstallation sur Linux

1. Se loguer en tant que root sur le serveur Linux
2. Arrêter tous les modules à l'aide de la commande `safekit shutdown`
3. Fermer tous les éditeurs, explorateur de fichiers, ou terminaux sous `SAFE` et `SAFEVAR` (`SAFE=/opt/safekit` ; `SAFEVAR=/var/safekit`)
4. Désinstaller SafeKit avec la commande `safekit uninstall -all` et répondre `yes` lorsque cela est demandé pour confirmer la destruction de tous les répertoires créés lors de la précédente installation
5. Redémarrer le serveur
6. Défaire les modifications effectuées pour paramétrer les règles de pare-feu (voir la [section 10.3](#))
7. Supprimer, l'utilisateur/groupe créés par l'installation précédente (par défaut `safekit/safekit`) avec les commandes :

```
userdel safekit
groupdel safekit
```
8. Désinstallez l'application Web SafeKit si elle est installée (voir [section 3.1.4.2](#))

## 2.6 Documentations SafeKit

<a href="#">SafeKit Solution</a>	La solution SafeKit y est entièrement détaillée.
<a href="#">Formation SafeKit</a>	Reportez-vous à cette formation en ligne pour un démarrage rapide de l'utilisation de SafeKit.
<a href="#">SafeKit Release Notes</a>	Il contient : <ul style="list-style-type: none"><li>• Dernières instructions d'installation</li><li>• Changements majeurs</li><li>• Restrictions et problèmes connus</li><li>• Instructions de migration</li></ul>
<a href="#">Software Release Bulletin</a>	Bulletin listant les packages SafeKit 8.2 avec la description des changements et des problèmes corrigés.
<a href="#">SafeKit Knowledge Base</a>	Liste des problèmes et restrictions connus de SafeKit. D'autres KB sont accessibles sur le <a href="#">portail du support</a> , mais sont accessibles uniquement aux utilisateurs enregistrés.
<a href="#">Guide de l'utilisateur SafeKit</a>	Il s'agit de ce guide. Veillez à consulter le guide correspondant à votre numéro de version SafeKit. Celui-ci est installé avec le package SafeKit et

accessible via la console web sous [🔗](#) Guide de l'utilisateur.

Le lien ci-contre renvoie à la dernière version de ce guide.

---



## 3. La console web de SafeKit

- ⇒ [Section 3.1](#) « Démarrer la console web »
- ⇒ [Section 3.2](#) « Configurer un cluster SafeKit »
- ⇒ [Section 3.3](#) « Configurer un module applicatif »
- ⇒ [Section 3.4](#) « Superviser un module applicatif »
- ⇒ [Section 3.5](#) « Snapshots et journaux du module applicatif pour le débogage et support »
- ⇒ [Section 3.6](#) « Sécuriser la console web »

La console web et l'API SafeKit ont évolué en SafeKit 8 par rapport aux versions précédentes. Par conséquent, la console livrée avec SafeKit 8 n'est capable d'administrer que des serveurs avec SafeKit 8 ; de plus, ceux-ci ne peuvent être administrés avec une ancienne console.

### 3.1 Démarrer la console web

La console web de SafeKit offre la possibilité d'administrer un cluster SafeKit. Un cluster SafeKit est un groupe de serveurs sur lesquels SafeKit est installé et fonctionnel. Tous les serveurs appartenant à un cluster donné partagent la même configuration de cluster (liste des serveurs et réseaux utilisés) et communiquent entre eux afin d'avoir une vue globale des configurations des modules installés. Un même serveur ne peut appartenir à plusieurs clusters.

#### 3.1.1 Lancer un navigateur web

Les prérequis pour lancer la console sont les suivants :

- L'appareil (station de travail, serveur, mobile) a un accès réseau au(x) serveur(s) SafeKit et l'autorisation d'accès
- Les réseaux, pare-feu et proxy sont configurés de manière à permettre l'accès à tous les serveurs SafeKit
- Les navigateurs supportés sont Microsoft Edge, Firefox et Chrome

À partir de la version 5 de la console, celle-ci est également disponible en tant qu'application Web progressive (PWA) sur les ordinateurs et mobiles (voir [section 3.1.4](#)).



La console dispose d'un système de versionnage distinct de celui du package SafeKit.

#### 3.1.2 Connecter la console à un nœud SafeKit

Par défaut, l'accès à la console web nécessite que l'utilisateur s'authentifie avec un nom et mot de passe. A l'installation de SafeKit, vous avez dû l'initialiser avec l'utilisateur `admin` et lui affecter un mot de passe. Ce nom `admin`, et ce mot de passe sont suffisants pour accéder à toutes les fonctionnalités de la console. Pour plus de détails sur cette configuration, voir la [section 11.2.1](#).

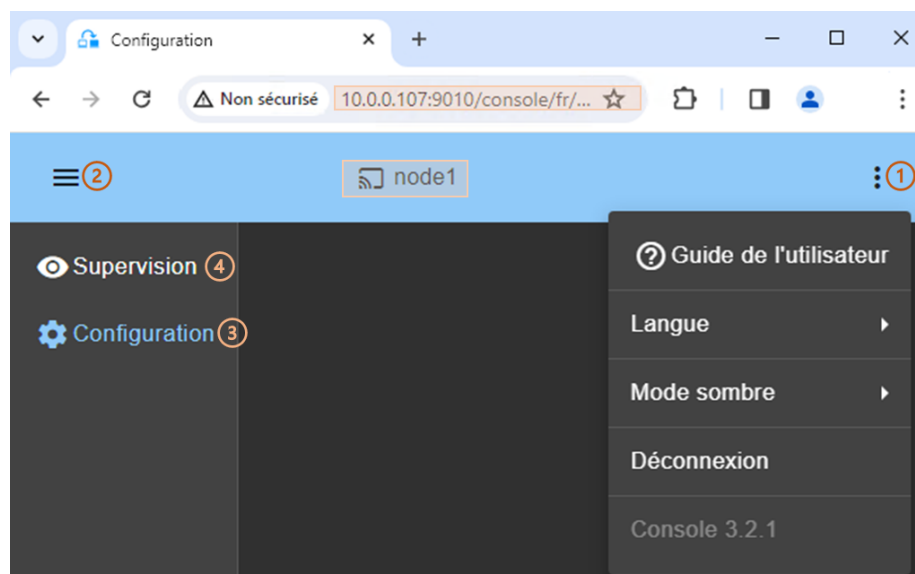
1. Lancer un navigateur web (Microsoft Edge, Firefox, or Chrome)

2. Le connecter à l'URL `http://host:9010` (`host` est le nom ou l'adresse IP d'un des serveur SafeKit). Si HTTPS est configuré, il y a une redirection automatique sur `https://host:9453`.
3. Le serveur SafeKit sur laquelle la console est connectée (`host` dans l'URL) est nommé nœud de connexion. Ce nœud agit en tant que proxy pour communiquer au compte de la console avec tous les autres serveurs SafeKit.





Vous pouvez vous connecter à n'importe quel nœud du cluster puisque la console offre une vue et des actions globales. En cas d'erreur de connexion avec un nœud, connectez-vous à un autre nœud.

4. Dans la page de login, s'identifier avec `admin` comme nom d'utilisateur et le mot de passe que vous avez donné pendant l'initialisation (par exemple, `pwd`).
5. La console web de SafeKit est chargée

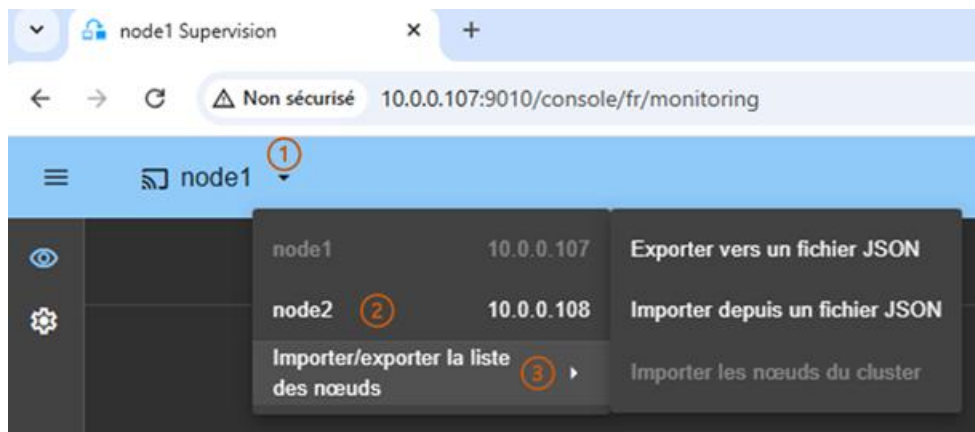


- Quand la console est connectée à un serveur SafeKit sur lequel le cluster est configuré, le nom du nœud correspond au serveur (tel que défini dans la configuration du cluster) est affiché dans l'entête. Il s'agit **du nœud de connexion** (`node1` dans l'exemple).  
Si le cluster n'est pas encore configuré, aucun nom n'est affiché.
- (1) Cliquer sur pour ouvrir le menu afin d'accéder au Guide de l'utilisateur SafeKit, sélectionner la langue, activer/désactiver le mode sombre et se déconnecter.
- (2) Cliquer sur pour réduire ou développer la barre latérale de navigation.
- (3) Cliquer sur « Configuration » pour configurer le cluster et les modules. La configuration n'est autorisée qu'aux utilisateurs ayant le rôle Admin. Par défaut, l'utilisateur `admin` a le rôle Admin.
- (4) Cliquer sur « Supervision » pour superviser et contrôler les modules configurés. La supervision est autorisée aux utilisateurs qui ont les rôles Admin, Control et Monitor. Avec le rôle Monitor, les actions sur les modules (démarrage, arrêt...) sont interdites

 La console web offre des aides contextuelles en cliquant sur l'icône .

### 3.1.3 Liste des nœuds de connexion

La console offre la possibilité de changer aisément de nœud de connexion même si ce nœud appartient à un cluster différent.



- (1) Cliquer sur ▼ pour afficher la liste des nœuds de connexion.  
Par défaut, si le cluster est configuré, il liste tous les nœuds appartenant au cluster. Sinon, ce menu n'est pas disponible.
- (2) Par exemple, cliquez sur node2 pour connecter la console web à ce nœud. La console web est chargée depuis ce nœud, qui devient le nœud de connexion.
- (3) Cliquer sur ▶ pour ouvrir le sous-menu qui permet de :
  - Exporter la liste des nœuds de connexion dans un fichier JSON sur votre station de travail.  
Il contient les noms et les adresses des nœuds de la liste.
  - Importer la liste des nœuds de connexion depuis un fichier JSON sur votre station de travail.  
Utilisez le fichier JSON exporté comme modèle et définissez votre propre liste de nœuds de connexion. Cela peut être utilisé si vous souhaitez gérer des nœuds appartenant à différents clusters SafeKit. Vous pouvez également définir un nom de cluster auquel les nœuds appartiennent.
  - Importer les nœuds du cluster  
Utilisez cette option pour réinitialiser une liste importée et restaurer la liste par défaut qui contient uniquement les nœuds définis dans le cluster du nœud sur lequel la console est connectée.

### 3.1.4 Utiliser l'application web (SafeKit Web App)

À partir de la version 5 de la console SafeKit, celle-ci est également disponible en tant qu'application Web progressive (PWA) sur les ordinateurs et mobiles. L'utilisation de l'application web SafeKit offre plusieurs avantages :

- Expérience utilisateur

La console peut être lancée directement depuis l'écran d'accueil, le menu de démarrage... Cela offre une expérience utilisateur similaire à celle d'une application native, en particulier sur mobile.

- **Notifications en temps réel**

Lorsqu'elles sont activées, les notifications permettent aux utilisateurs de recevoir immédiatement des informations sur les changements d'état des modules.

- Sur mobile, les notifications sont disponibles uniquement via l'application Web SafeKit. De plus, HTTPS est requis.
- Sur ordinateur, les notifications fonctionnent dans l'application Web et le navigateur. Cependant, à distance, HTTPS est requis ; HTTP n'est autorisé que sur localhost.

- **Sécurité renforcée**

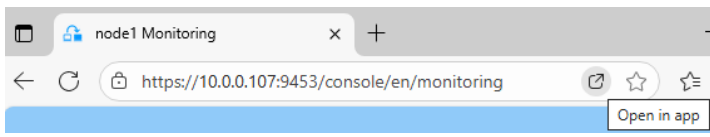
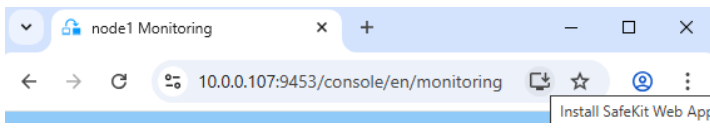
L'application Web bénéficie d'une isolation par rapport aux onglets du navigateur, et utilise le protocole HTTPS ainsi que des service workers pour une meilleure protection.

Pour installer l'application web SafeKit, la plate-forme et le navigateur utilisés doivent supporter PWA. C'est notamment le cas des navigateurs Chrome, Microsoft Edge et Firefox. Une fois installée, l'application devient autonome et a sa propre procédure de désinstallation.

### 3.1.4.1 Installer l'application Web

#### Sur ordinateur

1. Charger la console web SafeKit dans le navigateur web via l'URL `https://<host>:9453`
2. Repérer l'icône d'installation dans la barre d'adresse du navigateur :

Microsoft Edge	<p>Une petite icône est affichée à côté de l'URL</p>  <p>Ou aller dans le menu Apps</p>
Chrome	<p>Une petite icône est affichée à côté de l'URL</p> 

3. Cliquer pour installer et confirmer

La console SafeKit apparaîtra alors comme une application autonome, avec sa propre icône dans le menu de démarrage, le bureau...

#### Sur mobile

1. Charger la console web SafeKit dans votre navigateur via l'URL `https://<host>:9453`
2. Si votre mobile et navigateur supportent le PWA, repérer l'action « Ajouter »

Chrome	Dans le menu (:) en haut à droite
--------	-----------------------------------

3. Sélectionner « Ajouter à l'écran d'accueil » et confirmer

La console SafeKit sera accessible depuis l'écran d'accueil, comme une application native.

### 3.1.4.2 Désinstaller l'application web

Sur la plupart des plateformes, la désinstallation de l'application web se fait de la même manière que celle des autres applications.

Sur certains systèmes d'exploitation de bureau, la désinstallation de l'application peut se faire directement depuis l'application ouverte, en accédant au menu situé dans le coin supérieur droit.

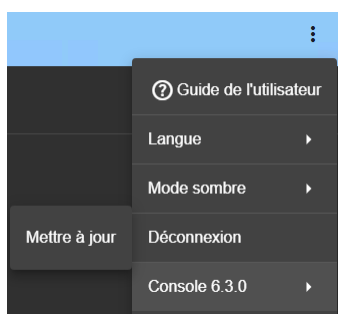
### 3.1.5 Mettre à jour la console web

Chaque mise à jour du package SafeKit peut éventuellement inclure une nouvelle version de la console web. Pour recharger cette nouvelle version, il peut être nécessaire de vider le cache du navigateur. Pour cela, vous pouvez utiliser un raccourci clavier :

1. Ouvrir le navigateur sur n'importe quelle page web, et presser en même temps les touches `Ctrl`, `Shift` et `Suppr`
2. Cela ouvre une fenêtre de dialogue : cocher tous les items puis cliquer le bouton `Nettoyer maintenant` ou `Supprimer`.
3. Fermer le navigateur, arrêter tous les processus du navigateur qui continueraient à tourner en tâche de fond et le relancer pour la charger la console web

À partir de la version 5 de la console SafeKit, celle-ci amène la fonctionnalité d'application Web progressive (PWA). Cette évolution amène des capacités de mise à jour automatique. Toutefois, si la mise à jour automatique ne se déclenche pas, vous pouvez la forcer :

- Soit en vidant le cache du navigateur comme décrit ci-dessus
- Soit en cliquant sur le bouton « Mettre à jour » accessible depuis le menu situé dans le coin supérieur droit. Si une nouvelle version est disponible, la console sera mise à jour ainsi que sa version.



## 3.2 Configurer un cluster SafeKit

Le cluster SafeKit doit être défini avant d'installer, de configurer ou de démarrer un module SafeKit.

Le cluster est défini par un ensemble de réseaux et les adresses, sur ces réseaux, d'un groupe de serveurs SafeKit, appelés nœuds. Ces nœuds mettent en œuvre un ou

plusieurs modules. Un serveur n'est pas obligatoirement connecté à tous les réseaux du cluster, mais tous les serveurs sont connectés à au moins un.

La configuration du cluster est sauvegardée du côté des serveurs dans le fichier `cluster.xml` (voir [section 12](#)). Pour que le fonctionnement soit correct, il est impératif que la configuration du cluster soit identique sur tous les nœuds.



Il est préférable de définir complètement tous les nœuds du cluster avant de configurer les modules. En effet, la modification de la configuration du cluster peut impacter la configuration et l'exécution des modules déjà installés.

La page d'accueil de la configuration du cluster est accessible :

- Directement via l'URL <http://host:9010/console/fr/configuration/cluster>

Ou

- En naviguant dans la console via  « Configuration/Configuration du cluster »

Si le cluster n'est pas encore configuré, l'assistant de configuration du cluster s'ouvre automatiquement au chargement de la console web.

### 3.2.1 L'assistant de configuration du cluster

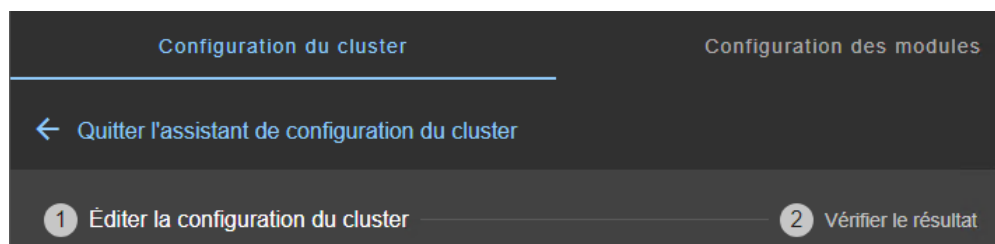
Ouvrir l'assistant de configuration :

- Directement via l'URL <http://host:9010/console/fr/configuration/cluster/config>

Ou

- En naviguant dans la console via  « Configuration/Configuration du cluster/  
 Configurer le cluster »

L'assistant de configuration du cluster est un formulaire à étapes :



1. « Éditer la configuration du cluster » décrit en [section 3.2.1.1](#)
2. « Vérifier le résultat » décrit en [section 3.2.1.2](#)
3. ← pour « Quitter l'assistant de configuration du cluster »

#### 3.2.1.1 Éditer la configuration du cluster

L'assistant de configuration du cluster est un formulaire guidé étape par étape.

Configuration du cluster

← Quitter l'assistant de configuration du cluster

1 Éditer la configuration du cluster 2 Vérifier le résultat

3 Configuration avancée Aide

Lan et nœuds 1

Nom du lan\*  
default

Adresse du nœud\* 10.0.0.107 2 ✓ Nom du nœud\* node1

Adresse du nœud\* 10.0.0.108 ✓ Nom du nœud\* node2

Lan et nœuds

Nom du lan\*  
private

Adresse du nœud\* 10.1.0.107 ✓ Nom du nœud\* node1

Adresse du nœud\* 10.1.0.108 ✓ Nom du nœud\* node2

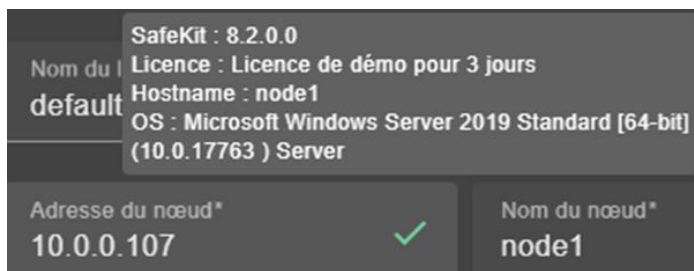
Recharger Sauvegarder et appliquer 4

- (1) Remplir le formulaire pour affecter d'abord le nom convivial pour le réseau. Ce nom est utilisé plus tard pour configurer les réseaux de surveillance utilisés par un module.

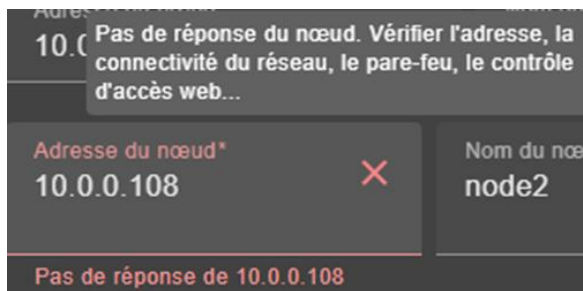
Cliquer sur **+** pour ajouter un nouveau nœud /lan ou sur **☒** pour supprimer un nœud/lan du cluster.

**!** Quand un nœud/lan est supprimé du cluster, tous les modules l'utilisant dans sa configuration peuvent devenir inutilisables.


- (2) Saisir l'adresse IP du nœud, puis appuyer sur la touche tabulation pour vérifier la disponibilité du serveur et l'insertion automatique de son nom.  
L'icône à côté de l'adresse reflète l'accessibilité du nœud.





✓ signifie que le serveur SafeKit est disponible. L'infobulle donne des informations sur le serveur.



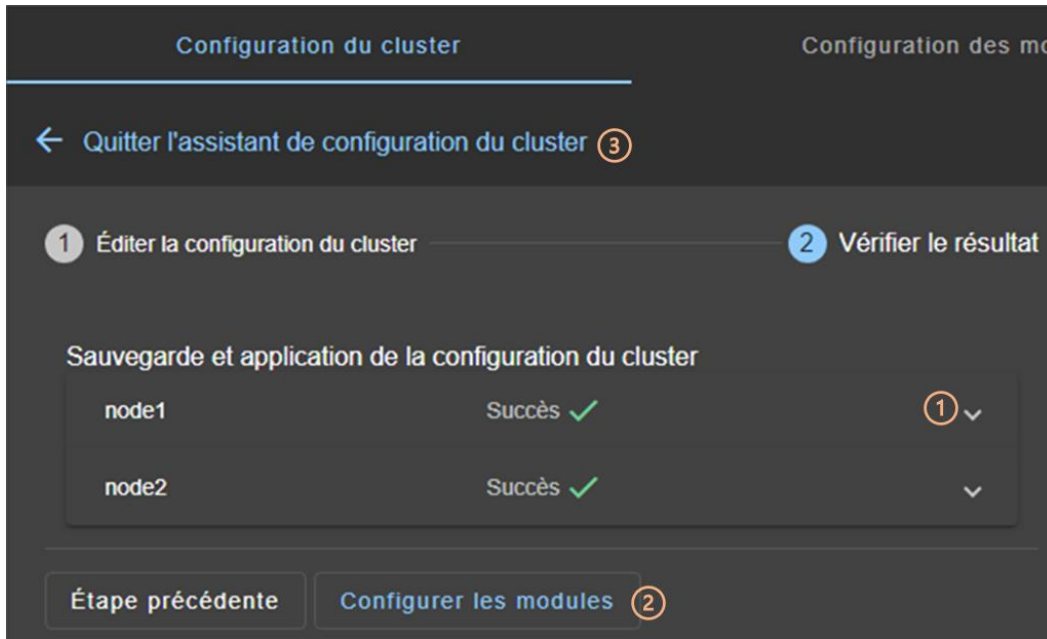
✗ signifie que le serveur n'a pas répondu dans le délai imparti. Résoudre le problème, afin de pouvoir administrer ce nœud. Cela peut être dû à une mauvaise adresse, une défaillance du réseau ou du serveur, une mauvaise configuration du navigateur web ou du pare-feu, l'arrêt du service web SafeKit sur le nœud. Pour investiguer le problème, voir la [section 7.1](#).

- Modifier le nom du nœud si besoin. Ce nom est celui qui sera utilisé par le service d'administration de SafeKit pour identifier de manière unique chaque nœud du cluster. C'est également le nom affiché dans la console web.
- (3) Si besoin, cliquer sur « Configuration avancée » pour basculer sur l'édition du cluster au format XML.  
Cliquez sur  pour ouvrir le Guide de l'utilisateur SafeKit sur la description de la configuration dans le fichier `cluster.xml`.
- Cliquer sur « Recharger » pour abandonner vos modifications en cours et recharger la configuration d'origine.
- (4) Une fois l'édition terminée, cliquez sur « Sauvegarder et appliquer » pour enregistrer et appliquer la configuration à tous les nœuds du cluster.

 Si besoin, vous pouvez réappliquer la configuration du cluster sur tous les nœuds sans la modifier.

 Pour des exemples de configuration du cluster avec deux réseaux voir la [section 15.1.1](#); avec trois nœuds voir la [section 15.2.1](#).

### 3.2.1.2 Vérifier le résultat



- (1) Lire le résultat de la configuration sur chaque nœud :
  - « Succès » ✓ signifie que la configuration a réussi.
  - « Échec » ✗, signifie que la configuration a échoué. Cliquer sur ∨ pour lire la sortie des commandes exécutées sur le nœud et rechercher l'erreur. Vous pouvez avoir à modifier les paramètres saisis ou à vous connecter au serveur afin de corriger le problème. Une fois l'erreur corrigée, Sauvegarder et appliquer à nouveau.
- (2) Cliquer sur « Configurer les modules » pour quitter l'assistant de configuration du cluster et naviguer vers la configuration des modules.

Ou

- (3) Cliquer sur ← pour « Quitter l'assistant de configuration du cluster » et aller sur la page d'accueil de configuration du cluster.

### 3.2.2 Page d'accueil de la configuration du cluster

Lorsque le cluster est configuré, la page d'accueil de la configuration du cluster est accessible.

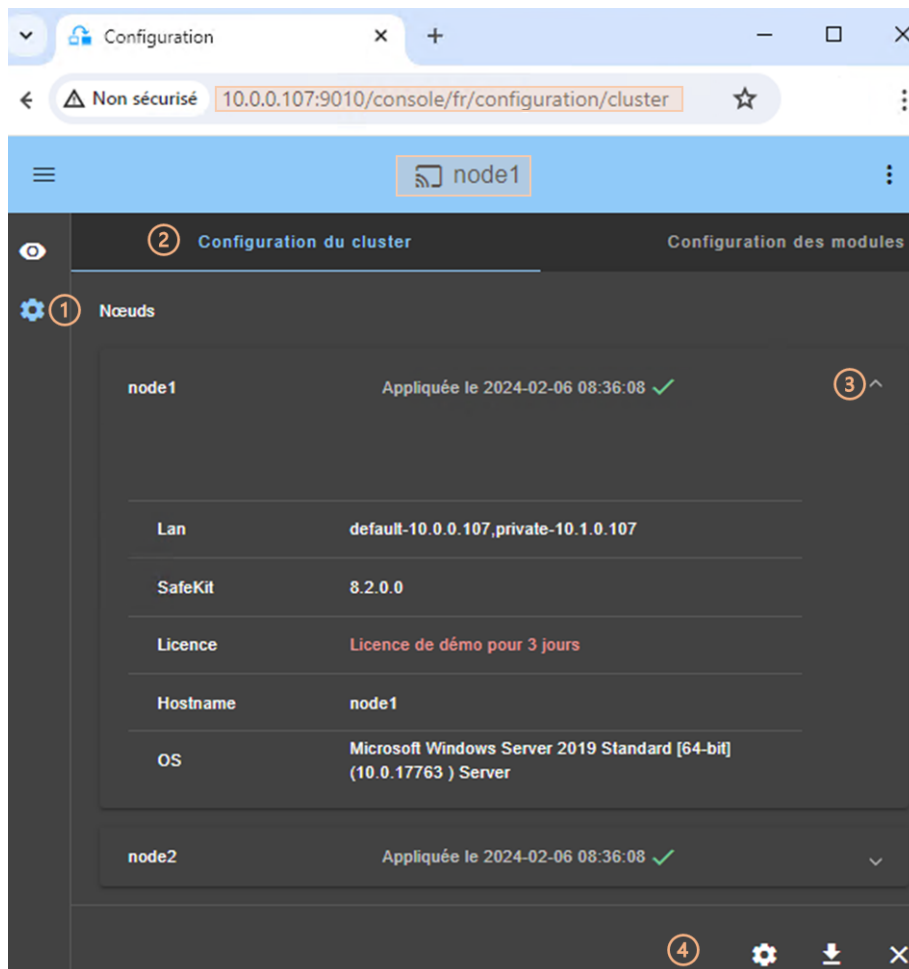
L'ouvrir :






- Directement avec <http://host:9010/console/fr/configuration/cluster>

Ou

- En naviguant dans la console sur ⚙️ « Configuration/Configuration du cluster »

Dans cet exemple, la console est chargée depuis 10.0.0.107 qui correspond au nœud node1 dans le cluster existant. Il s'agit du nœud de connexion.



- (1) Cliquer sur  « Configuration » dans la barre de navigation latérale
- (2) Cliquer sur l'onglet « Configuration du cluster »  
Les nœuds configurés dans le cluster sont listés avec leur date de configuration
- (3) Cliquer sur  pour afficher des détails sur le nœud.  
Il s'agit du nom des lans et adresses définies dans la configuration du cluster, version et licence SafeKit, hostname et OS.
- (4) Cliquer sur l'un des boutons :
  -  pour modifier la configuration du cluster ou réappliquer la configuration courante. Cela ouvre l'assistant de configuration du cluster et charge la configuration courante depuis le nœud de connexion.
  -  pour télécharger la configuration du cluster au format XML depuis le nœud de connexion.
  -  pour déconfigurer le cluster sur un ou plusieurs nœuds.

### 3.3 Configurer un module applicatif

Une fois le cluster configuré, il est possible de configurer un nouveau module sur le cluster. La page d'accueil de la configuration des modules est accessible :

- Directement via l'URL <http://host:9010/console/fr/configuration/modules>

Ou

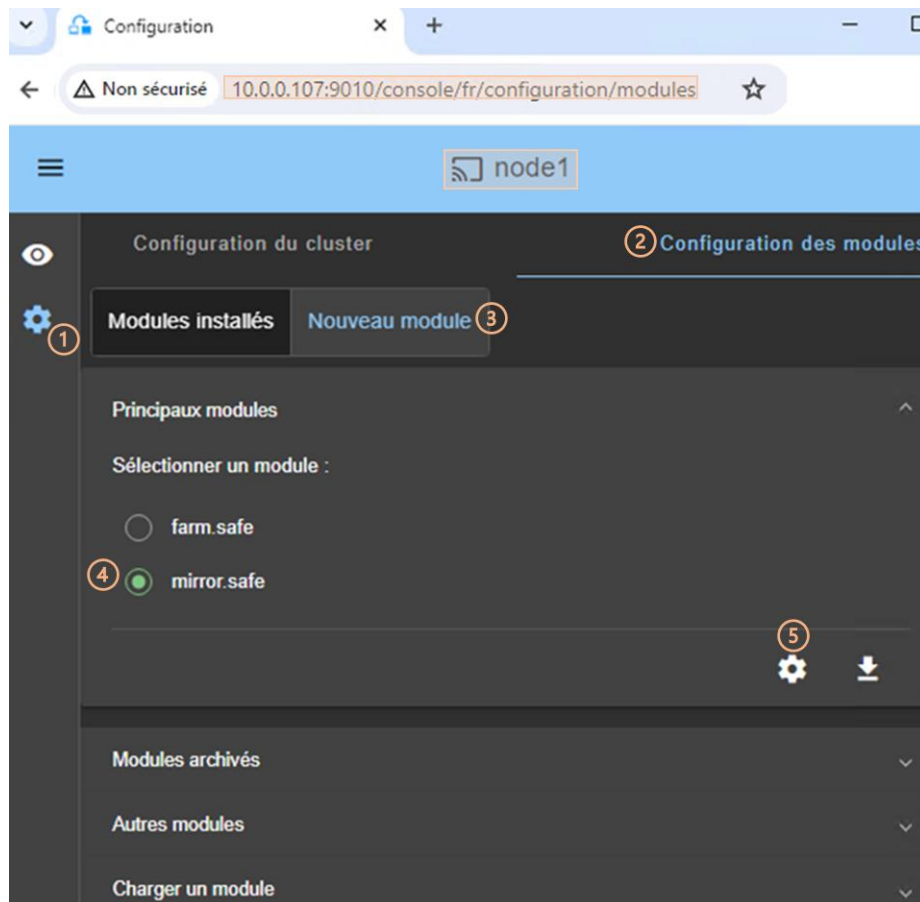
- En naviguant dans la console via  « Configuration/Configuration des modules »



S'il n'y a aucun module configuré, la console présente automatiquement la page pour configurer un « Nouveau Module ».

Pour des exemples de configuration de modules voir la [section 15](#).

### 3.3.1 Sélectionner le nouveau module à configurer

Dans cet exemple, la console est chargée depuis 10.0.0.107 qui correspond au nœud `node1` dans le cluster existant. Il s'agit du nœud de connexion.



- Cliquer sur  « Configuration » dans la barre de navigation latérale
- (2) Cliquer sur l'onglet « Configuration des modules »
- (3) Cliquer sur « Nouveau module »
- La page propose de sélectionner un nouveau module parmi plusieurs propositions visibles en cliquant sur  :
  - Les « Principaux modules », notamment les modules génériques `mirror.safe` (voir la [section 15.1.2](#)) et `farm.safe` (voir la [section 15.2.2](#)) à utiliser pour l'intégration d'une nouvelle application dans une architecture miroir ou ferme.

Sont présentés les modules stockés sur le nœud de connexion, `node1`, sous `SAFE/Application_Modules/generic`, `SAFE/Application_Modules/demo` et `SAFE/Application_Modules/published`.

- Les « Modules archivés » sur le nœud de connexion qui sont sauvegardés lorsqu'un module est désinstallé sur ce nœud.


Ils sont récupérés depuis `node1` sous `SAFE/Application_Modules/backup`.

- D'« Autres modules » qui sont des exemples d'utilisation de fonctionnalités de SafeKit dans des modules fournis en vue de tests uniquement. Voir la [section 15](#) pour la description de certains d'entre eux.

Ils sont récupérés depuis `node1` sous `SAFE/Application_Modules/other`.

- Un module stocké localement accessible depuis « Charger un module ».

Cette fonctionnalité peut être utilisée pour configurer un module, pour une application donnée (par exemple, Microsoft SQL Server, PostgreSQL...), téléchargé depuis l'un des [guides d'installation rapide de SafeKit](#).

- (4) Sélectionner un module à configurer parmi les propositions listées ci-dessus. Dans l'exemple, `mirror.safe`.
- (5) Cliquer sur le bouton  « Configurer le nouveau module ».
- Un dialogue s'ouvre pour saisir le nom du nouveau module

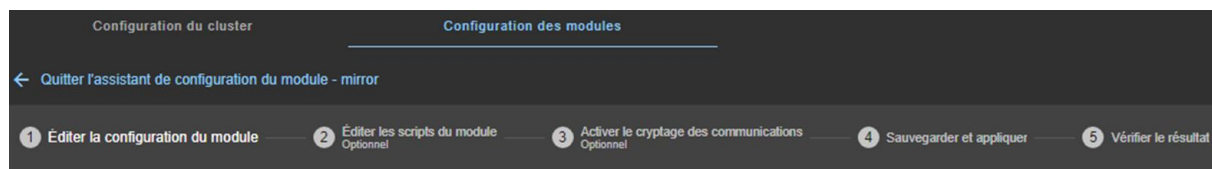


- (6) Entrer le nom du nouveau module
- (7) Cliquer sur « Confirmer »

L'assistant de configuration du module est ouvert. Celui-ci est décrit ci-dessous.

### 3.3.2 L'assistant de configuration du module


L'assistant de configuration du module est un formulaire à étapes :



1. « Éditer la configuration du module » décrit en [section 3.3.2.1](#)
2. « Éditer les scripts du module (Optionnel) » décrit en [section 3.3.2.2](#)
3. « Activer le cryptage des communications (Optionnel) » décrit en [section 3.3.2.3](#)
4. « Sauvegarder et appliquer » décrit en [section 3.3.2.4](#)
5. « Vérifier le résultat » décrit en [section 3.3.2.5](#)


6. ← pour « Quitter l'assistant de configuration du module »

Notez que la reconfiguration d'un module ne peut être appliquée qu'aux nœuds sur lesquels le module en question n'est pas démarré. Il convient donc d'arrêter le module avant de lancer l'assistant de configuration.


 Si besoin, vous pouvez réappliquer la configuration du module sur tous les nœuds sans la modifier.

### 3.3.2.1 Éditer la configuration du module


Ci-dessous l'exemple de l'édition de la configuration du module miroir `mirror.safe`.

- (1) Remplir le formulaire pour affecter les valeurs aux différents composants, en ajouter ou en supprimer. Cliquer sur  pour ouvrir le panneau détaillé pour chaque composant.

Ce formulaire permet de saisir uniquement les principaux paramètres de configuration du module.

 Le nom des « Réseaux de heartbeat » proposés sont les noms des lans saisis lors de la configuration du cluster.

- (2) Pour une configuration avancée du module, exhaustive par rapport au formulaire, cliquer sur « Configuration avancée ». Cela bascule sur l'édition du fichier de configuration du module au format XML, `userconfig.xml`.

Cliquer sur  pour ouvrir le Guide de l'utilisateur SafeKit sur la description de la configuration des différents composants dans le fichier `userconfig.xml`.

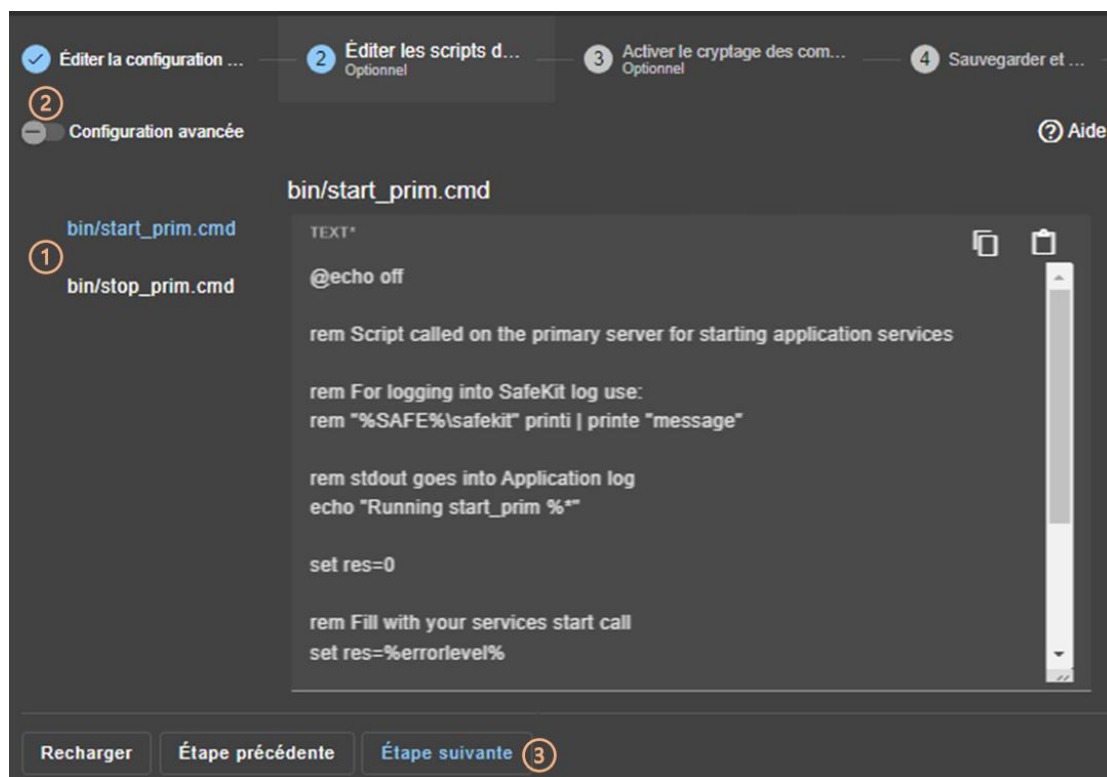
- Si besoin, cliquer sur « Recharger » pour abandonner vos modifications et recharger la configuration complète d'origine (y compris les scripts si ceux-ci avaient été modifiés dans l'étape suivante).
- (3) Une fois l'édition de la configuration du module achevée, cliquer sur « Étape suivante ».







Pour des exemples de configuration d'un module miroir voir la [section 15.1.2](#) ; d'un module ferme voir la [section 15.2.2](#).

### 3.3.2.2 Éditer les scripts du module

Ci-dessous l'exemple de l'édition des scripts du module miroir `mirror.safe`.

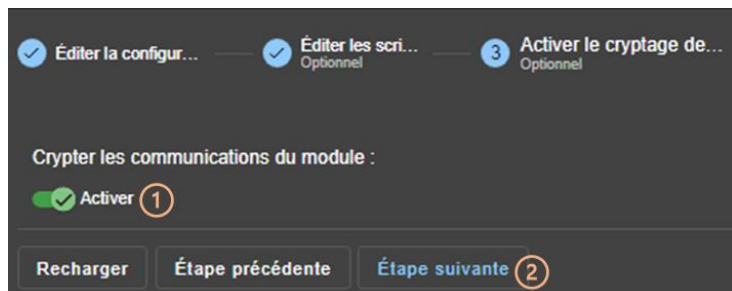


- (1) Cliquer sur « start\_prim » ou « stop\_prim » pour l'éditer et y insérer le démarrage/arrêt de votre application.  
Cliquez sur  pour copier le contenu du script et l'éditer avec votre éditeur syntaxique favori. Une fois fait, copier le contenu mis à jour dans le champ d'input avec .
- (2) Si besoin, cliquer sur « Configuration Avancée » pour lister les autres scripts du module et les éditer (`prestart`, `poststop`, scripts pour les checkers...).  
Cliquez sur  pour ouvrir le Guide de l'utilisateur SafeKit sur la description des scripts du module.
- Si besoin, cliquer sur « Recharger » pour abandonner vos modifications et recharger la configuration complète d'origine (y compris la configuration du module si celle-ci avait été modifiée dans l'étape précédente).
- (3) Une fois l'édition des scripts du module achevée, cliquer sur « Étape suivante ».


 Pour des exemples de scripts d'un module miroir voir la [section 15.1.3](#) ; d'un module ferme voir la [section 15.2.3](#).

### 3.3.2.3 Activer le cryptage des communications

Le cryptage des communications internes du module entre les nœuds du cluster, est activé par défaut. Pour plus de détails, voir la [section 10.7](#).



- (1) Cliquer **Activer** pour activer ou désactiver le cryptage des communications du module.

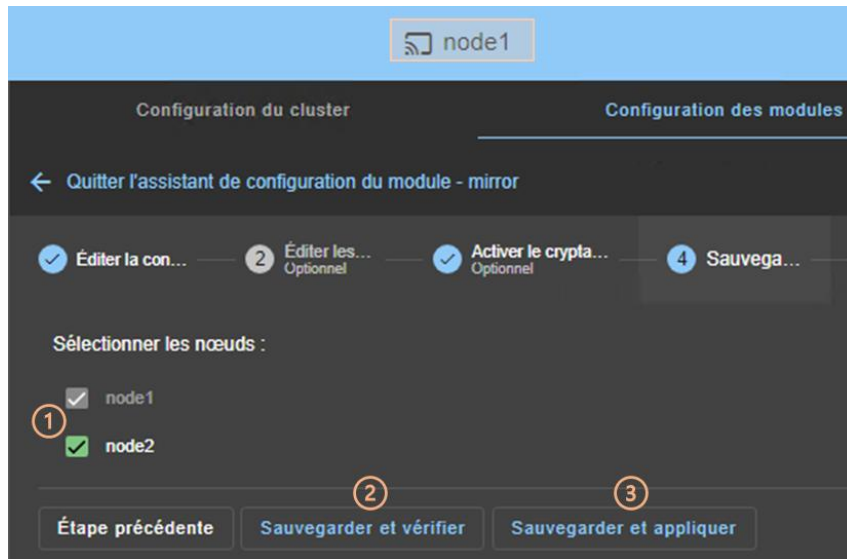
 Lorsque la clé de cryptage du module n'est pas identique sur tous les nœuds, la communication interne est impossible. Il faut réappliquer la configuration sur tous les nœuds pour propager la même clé.

Pour générer de nouvelles clés de cryptage, il faut :

1. Désactiver le cryptage, puis « Sauvegarder et appliquer » la configuration sur tous les nœuds
  2. Activer le cryptage, puis « Sauvegarder et appliquer » la configuration sur tous les nœuds
- Si besoin, cliquer sur « Recharger » pour abandonner vos modifications et recharger la configuration complète d'origine (y compris la configuration du module et les scripts si ceux-ci avaient été modifiés dans les étapes précédentes).
  - (2) Une fois cette étape achevée, cliquer sur « Étape suivante ».

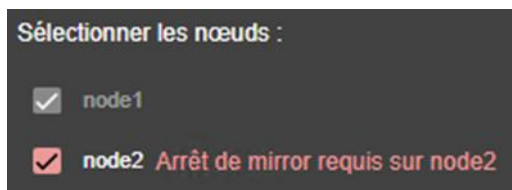
### 3.3.2.4 Sauvegarder et appliquer

Étape de sélection des nœuds concernés par la configuration.

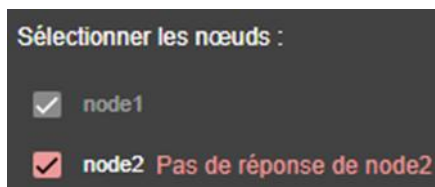


- (1) Cochez/décochez pour sélectionner/désélectionner les nœuds. Veuillez noter que le nœud de connexion (`node1` dans l'exemple) est obligatoire.

Il y a 2 cas où « Sauvegarder et appliquer » est désactivé :



Le module sur le nœud sélectionné est démarré et dans un état différent de  $\times$ STOP (NotReady).



Le nœud sélectionné n'a pas répondu dans le délai imparti. Cela peut être dû à une mauvaise adresse, une défaillance du réseau ou du serveur, une mauvaise configuration du navigateur web ou du pare-feu, l'arrêt du service web SafeKit sur le nœud. Pour investiguer le problème, voir la [section 7.1](#).

Dans les deux cas, décocher le nœud ou cliquer sur « Sauvegarder et vérifier » pour l'appliquer plus tard, après avoir arrêté le module ou résolu le problème de communication.

- (2) Cliquer sur « Sauvegarder et vérifier » pour sauvegarder la configuration modifiée sur le nœud de connexion et vérifier sa cohérence. Il passe ensuite à l'étape suivante pour afficher le résultat de cette opération.

Une fois cette opération terminée, toutes les modifications sont enregistrées sur le nœud de connexion. L'assistant de configuration peut être quitté et relancé ultérieurement pour appliquer la configuration sauvegardée. Tant que la configuration sauvegardée n'est pas appliquée, la dernière configuration appliquée reste active.

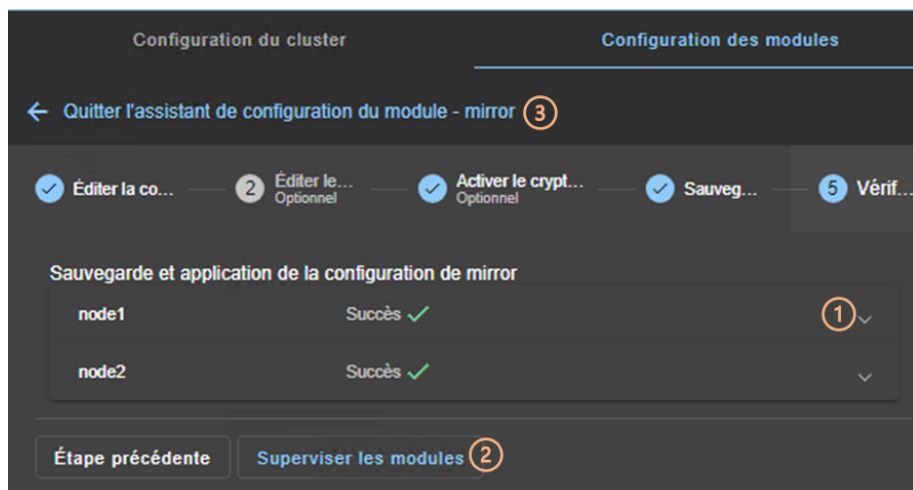
- (3) Cliquer sur « Sauvegarder et appliquer » pour sauvegarder et appliquer la configuration modifiée aux nœuds sélectionnés. Il passe ensuite à l'étape suivante pour afficher le résultat de cette opération.

Si l'opération est réussie, la configuration appliquée devient la configuration active du module.

La configuration du module est sauvegardée du côté serveur sous `SAFE/modules/AM` (où `AM` est le nom du module). Lors de la reconfiguration du module, ce répertoire est détruit et écrasé à partir des modifications faites dans la console. Du côté serveur, fermer tous les éditeurs, explorateur de fichiers, shells ou cmd sous `SAFE/modules/AM` (au risque sinon que la configuration se passe mal).

### 3.3.2.5 Vérifier le résultat

L'exemple ci-dessous montre le résultat de l'opération « Sauvegarder et appliquer ». La présentation pour « Sauvegarder et vérifier » est similaire.



- (1) Lire le résultat de l'opération sur chaque nœud :
  - o « Succès » ✓ signifie que l'opération a réussi
  - o « Échec » ✗, signifie que l'opération a échoué.

Cliquer sur ∨ pour lire la sortie des commandes exécutées sur le nœud et rechercher l'erreur. Vous pouvez avoir à modifier les paramètres saisis ou à vous connecter au serveur afin de corriger le problème. Une fois l'erreur corrigée, répéter l'opération depuis l'étape précédente.
- (2) Ou cliquer sur « Superviser les modules » pour quitter l'assistant de configuration du module et naviguer vers la supervision des modules.

Ou

- (3) Cliquer sur ← pour « Quitter l'assistant de configuration du module » et aller sur la page d'accueil de configuration des modules.

### 3.3.3 Page d'accueil de la configuration des modules

Lorsqu'un premier module est configuré, la page d'accueil de la configuration des modules est accessible. Elle permet de visualiser les modules installés sur le cluster et d'accéder à la configuration d'un nouveau module.

L'ouvrir :

- Directement avec <http://host:9010/console/fr/configuration/modules>

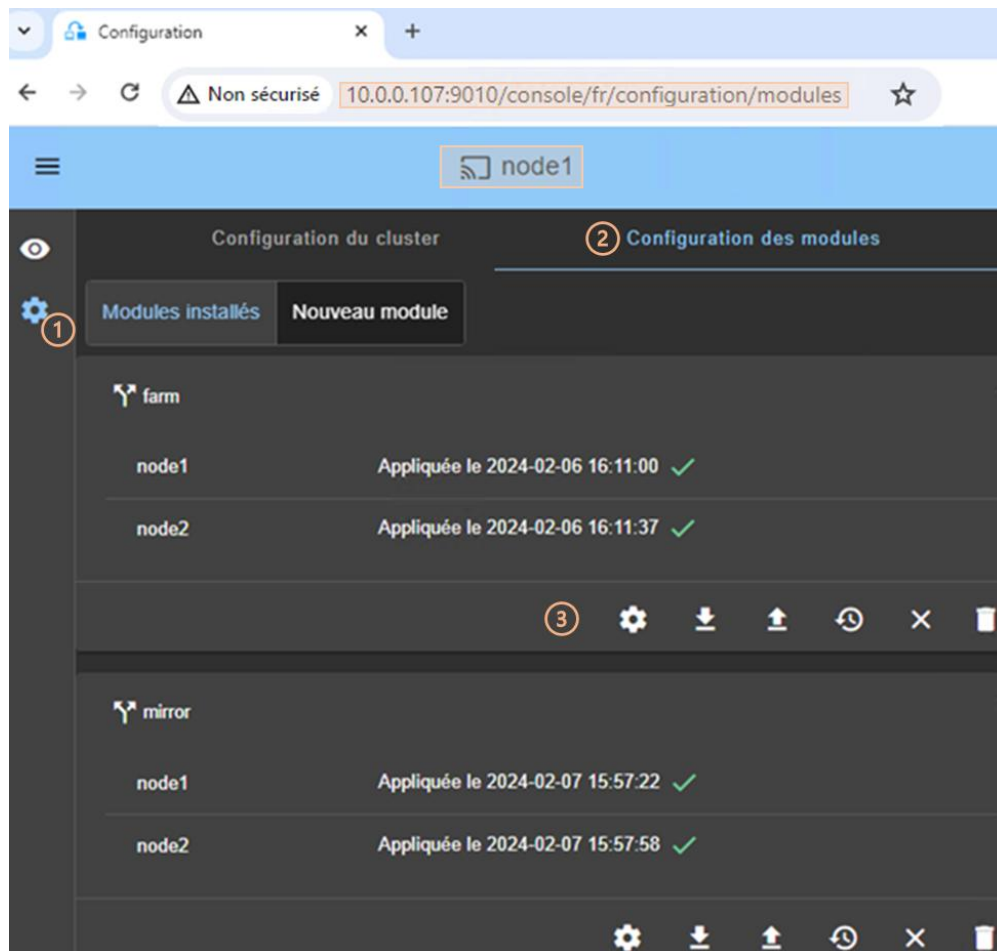
Ou

- En naviguant dans la console sur ⚙️ « Configuration/Configuration des modules »








Avant chaque reconfiguration, déconfiguration et désinstallation, sur chaque nœud, fermer tous les éditeurs, explorateur de fichiers, shells ou cmd sous `SAFE/modules/AM` (au risque sinon que l'opération échoue).

Dans l'exemple suivant, la console est chargée depuis `10.0.0.107` qui correspond au nœud `node1` dans le cluster existant. Il s'agit du nœud de connexion.



- (1) Cliquer sur ⚙️ « Configuration » dans la barre de navigation latérale.
- (2) Cliquer sur l'onglet « Configuration des modules ».
- Les modules installés dans le cluster sont listés avec la date d'application de la configuration et éventuellement la date de sauvegarde d'une configuration qui n'a pas été encore appliquée.
- (3) Cliquer sur l'un des boutons associés au module :
  - ⚙️ pour modifier sa configuration ou réappliquer sa configuration courante. Cela ouvre l'assistant de configuration du module et charge sa configuration courante depuis le nœud de connexion.

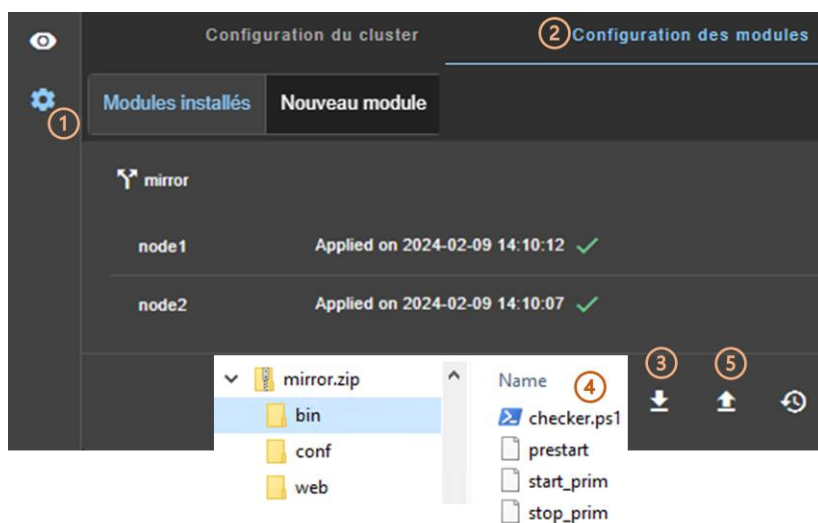
- o  pour télécharger le `.safe`, composé de tous les fichiers du module (`userconfig.xml`, `scripts`) depuis le nœud de connexion.
  - o  pour reconfigurer le module depuis le contenu d'un `.safe` stocké localement.
  - o  pour restaurer une ancienne configuration du module.
- SafeKit conserve une copie des trois dernières configurations réussies (stockées sous `SAFE/modules/lastconfig` du côté serveur). L'ensemble des fichiers de configuration du module sont empaquetés dans un fichier `.safe`, dont le nom est du type `AM_<date>_<heure>` (où `AM` est le nom du module).
- o  pour déconfigurer le module sur un ou plusieurs nœuds, sans le désinstaller. Ses fichiers de configuration sont conservés pour être éventuellement réappliquer plus tard.
  - o  pour désinstaller complètement le module sur un ou plusieurs nœuds.
- À la désinstallation du module, l'ensemble de ses fichiers sont empaquetés dans un fichier `.safe` qui est archivé du côté serveur sous `SAFE/Application_Modules/backup`.




- Pour configurer un nouveau module, cliquer sur « Nouveau module ».

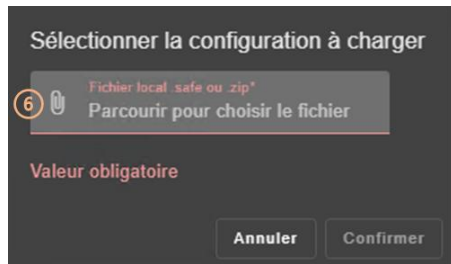
### 3.3.4 Éditer localement la configuration du module puis l'appliquer


Vous préférerez peut-être utiliser votre éditeur favori sur votre station de travail pour éditer la configuration du module et/ou ajouter des scripts, tels qu'un custom checker.

Suivez la procédure suivante pour éditer la configuration du module sur votre station de travail puis l'appliquer.



- (1) Cliquer sur  « Configuration » dans la barre de navigation latérale.
- (2) Cliquer sur l'onglet « Configuration des modules ».
- (3) Cliquer sur  pour télécharger le `mirror.safe` sur votre station de travail
- (4) Extraire le contenu de `mirror.safe` (qui est un fichier zip) pour éditer `conf/userconfig.xml`, éditer/ajouter/détruire des scripts sous `bin` (un custom checker par exemple).
- (5) Compresser le répertoire modifié dans un fichier `xx.safe` (ou `xx.zip`), puis le charger avec  (`.safe` et `.zip` acceptés).



- (6) Cliquer sur  pour sélectionner le fichier à charger, puis « Confirmer ».

L'assistant de configuration du module est lancé avec le nouveau contenu de ce fichier. Passez à l'étape 4 pour « Sauvegarder et appliquer » cette nouvelle configuration

### 3.4 Superviser un module applicatif

Une fois un module configuré, vous pouvez superviser son état et exécuter des actions dessus (start, stop...).

La page d'accueil de supervision des modules est accessible :

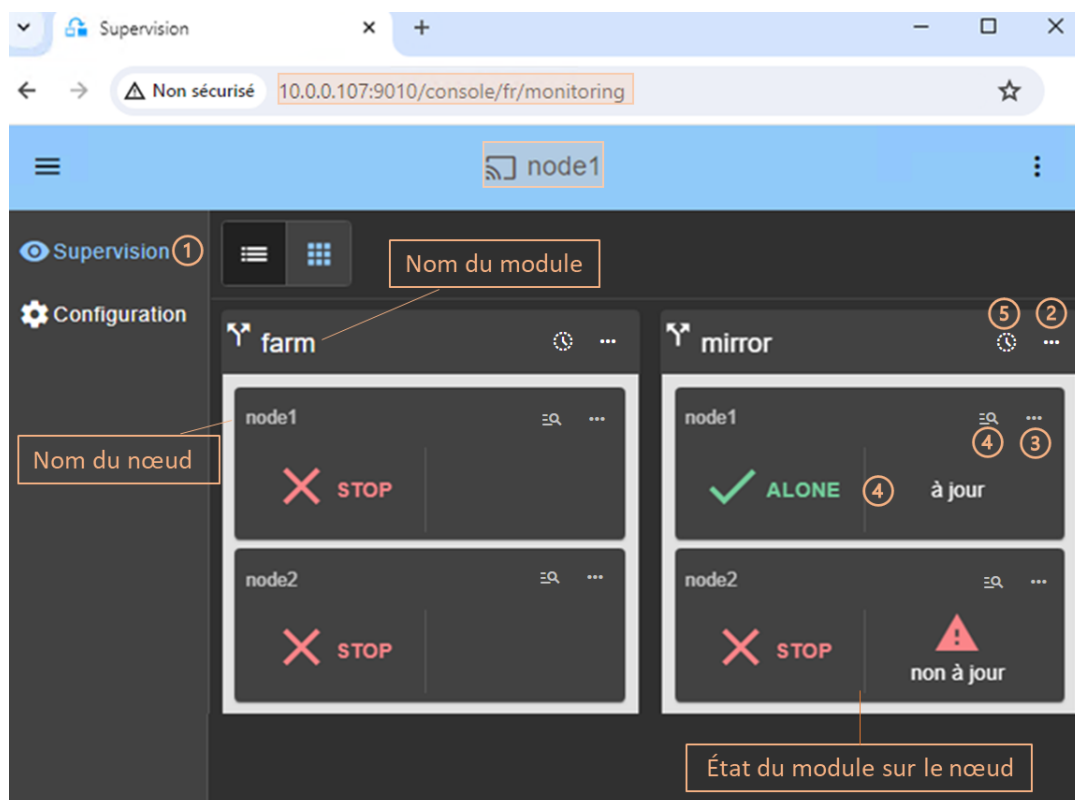
- Directement avec <http://host:9010/console/fr/monitoring>






Ou

- En naviguant dans la console sur  « Supervision »

#### 3.4.1 Page d'accueil de la supervision

Dans cet exemple, la console est chargée à partir de 10.0.0.107, qui correspond à `node1` dans le cluster. Il s'agit du nœud de connexion. Deux modules sont configurés : `farm` et `mirror`.









- (1) Cliquer sur  « Supervision » dans la barre de navigation latérale
- Pour chaque module installé, sont affichés :
  - le nom du module et des nœuds sur lesquels il est installé
  - l'état du module sur chaque nœud (voir [section 3.4.2](#))
  - une notification pour chaque changement d'état, si l'utilisateur a accordé la permission et l'URL est https, ou http://localhost
- (2) Cliquer sur  pour ouvrir le menu d'actions (start, stop...) globales sur le module, qui s'appliquent à tous les nœuds (node1, node2 dans l'exemple).  
Pour sa description, voir [section 3.4.3.1](#).
- (3) Cliquer sur  pour ouvrir le menu d'actions (start, stop...) locales sur le module, qui s'appliquent uniquement au nœud (node1 dans l'exemple).  
Pour sa description, voir [section 3.4.3.2](#).
- (4) Cliquer sur le panneau du nœud (mirror>node1 dans l'exemple) pour ouvrir les détails du module sur ce nœud (journaux, ressources...). Depuis SafeKit 8.2.2, cliquer plutôt sur  pour ouvrir/fermer les détails.  
Pour sa description, voir [section 3.4.4](#).
- (5) Cliquer sur  pour ouvrir/fermer la chronologie des états du module sur tous les nœuds où il est installé.  
Pour sa description, voir [section 3.4.5](#).







## 3.4.2 État du module

Le module est représenté par son état synthétique dans la partie gauche et par son état détaillé dans la partie droite.

### 3.4.2.1 État synthétique

La console affiche l'un des états synthétiques suivants pour le module sur le nœud.

 STOP (NotReady) (rouge)	Module arrêté (prêt à démarrer)
 WAIT (Transient) (orange)	État transitoire du module
 ALONE (Transient) (orange)	État transitoire du module miroir primaire sans secondaire
 ALONE (Ready) (vert)	État stable du module miroir primaire sans secondaire
 PRIM (Transient) (orange)	État transitoire du module miroir primaire avec secondaire
 PRIM (Ready) (vert)	État stable du module miroir primaire avec secondaire

 SECOND (Transient) (orange)	État transitoire du module miroir secondaire avec primaire, pendant la phase de resynchronisation des répertoires répliqués
 SECOND (Ready) (vert)	État stable du module miroir, secondaire avec primaire
 UP (Transient) (orange)	État transitoire du module ferme
 UP (Ready) (vert)	État stable du module ferme
 WAIT (NotReady) (rouge)	État bloqué du module en attente d'une ou plusieurs ressources
NOT CONFIGURED (gris)	Module installé mais non configuré
 ERROR (rouge)	Pas de réponse du nœud dans le délai imparti

Cela peut être dû à une mauvaise adresse, une défaillance du réseau ou du serveur, une mauvaise configuration du navigateur web ou du pare-feu, l'arrêt du service web SafeKit sur le nœud (voir [section 7.1](#)).




Cela peut également être dû à l'indisponibilité temporaire du nœud de connexion. Dans ce cas, rechargez la console à partir d'un autre nœud du cluster.


Pour la description des changements d'état d'un module miroir voir la [section 5.2](#).


Pour la description des changements d'état d'un module ferme voir la [section 6.2](#).

### 3.4.2.2 État détaillé

Il s'agit de l'état des principales ressources et règles de failover.

à jour	Les répertoires répliqués du module miroir sont à jour
 non à jour	Les répertoires répliqués du module miroir ne sont pas à jour
 dégradé	Le module miroir est en mode dégradé décrit en <a href="#">section 7.7</a>
50%, 100%	La part de partage de charge du module ferme (par exemple 50% ou 100% pour 2 nœuds)
 0%	Aucune charge prise par le module ferme

 Le module a appliqué la règle de failover (par exemple, la règle nommée `c_checkfile`) qui entraîne l'action `restart`, `stop`, `stopstart` ou `wait` sur le module en raison d'une ressource passé à `down`. Voir la [section 13.19.4.2](#) pour des détails sur les règles de failover. Pour analyser le problème, lisez les journaux et les états des ressources comme décrit plus loin

**HTTP** Avec le module dans l'état  **ERREUR** (rouge)  
 erreur Pas de réponse du nœud dans le délai imparti  
 de connexion

### 3.4.3 Menus de contrôle d'un module

#### 3.4.3.1 Menu global

Les actions du menu global s'appliquent à tous les nœuds sur lesquels le module est configuré.

Dans cet exemple, les actions s'appliquent au module `mirror` sur `node1` et `node2`.



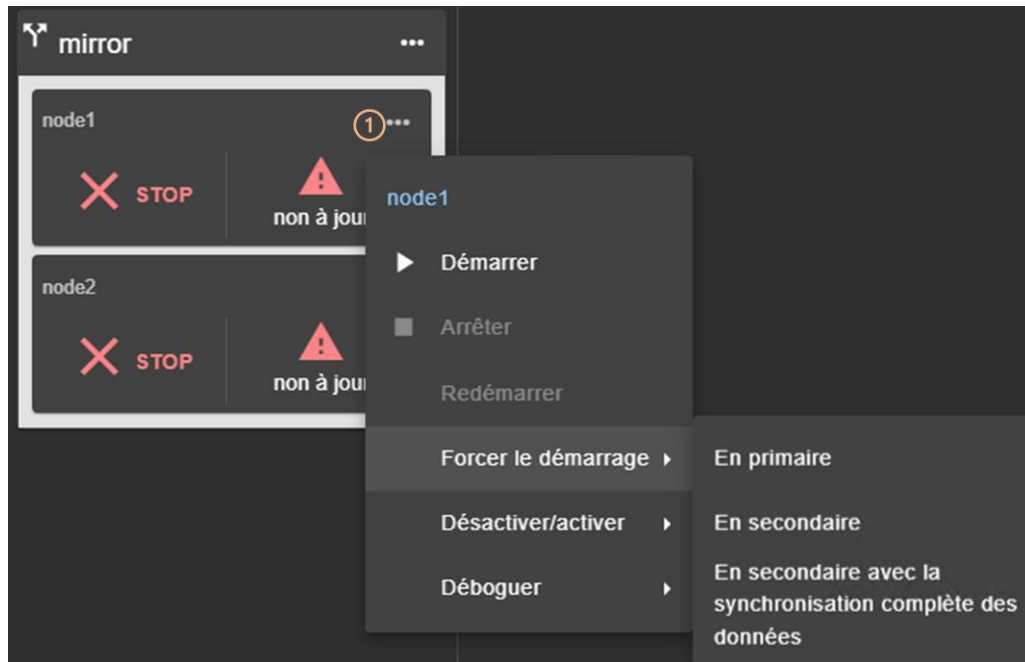
- (1) Cliquer sur `...` pour ouvrir le menu d'actions globales.
- Cliquer sur « Démarrer » pour démarrer le module sur tous les nœuds.  
 Pour un module miroir, un nœud est démarré automatiquement en tant que primaire s'il a les données à jour ; sinon, il démarre en tant que secondaire.
- Cliquer sur « Arrêter » pour arrêter le module sur tous les nœuds.  
 Pour un module miroir, le nœud qui est secondaire est arrêté en premier pour éviter un basculement inutile.
- Cliquer sur « Déboguer » pour le débogage et support comme décrit en [section 3.5](#).

#### 3.4.3.2 Menu local

Les actions du menu local s'appliquent uniquement au nœud sélectionné.

##### 3.4.3.2.1 Contrôler un module miroir

Dans cet exemple, les actions s'appliquent au module `mirror` sur `node1` uniquement.

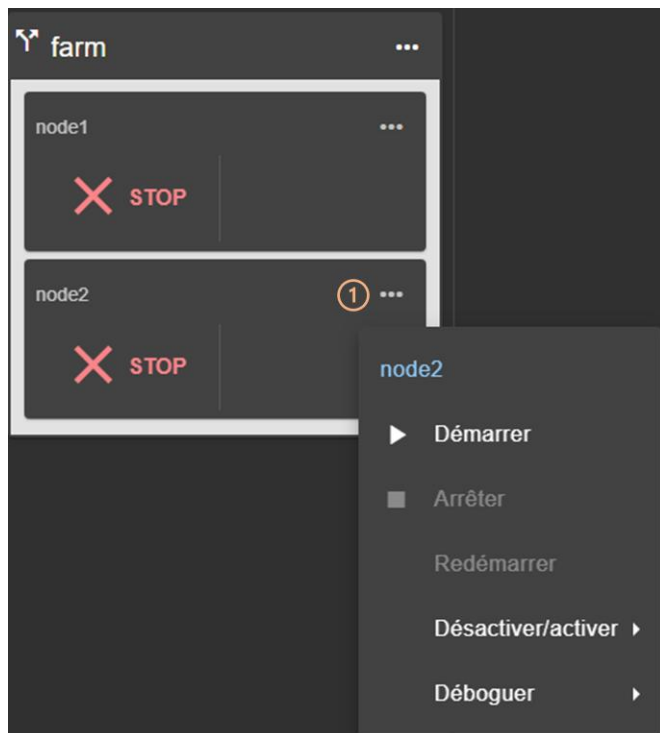


- (1) Cliquer sur **...** pour ouvrir le menu d'actions locales sur le nœud désiré (e.g. `node1`).
- Cliquer sur « Démarrer » pour démarrer le module sur le nœud.  
Pour un module miroir, un nœud est démarré automatiquement en tant que primaire s'il a les données à jour ; sinon, il démarre en tant que secondaire. Voir la [section 5.5](#).
- Cliquer sur « Arrêter » pour arrêter le module sur le nœud.
- Cliquer sur « Redémarrer » pour redémarrer le module sur le nœud.  
Il exécute uniquement les scripts d'arrêt puis de démarrage pour redémarrer l'application localement sans entraîner de basculement
- Utiliser le sous-menu « Forcer le démarrage » lorsque vous devez décider quel nœud doit démarrer en primaire ou secondaire.
  - Sélectionner « En primaire » pour forcer le nœud à démarrer en tant que primaire.  
Par exemple, au 1er démarrage d'un module miroir tel que décrit en [section 5.3](#), vous devez « Forcer le démarrage En primaire » le nœud qui a les répertoires répliqués à jour.
  - Sélectionner « En secondaire » pour forcer le nœud à démarrer en tant que secondaire.
  - La synchronisation des données peut être optimisée ou non en fonction du dernier état interne du module.
  - Sélectionner « En secondaire avec la synchronisation complète des données » pour forcer le nœud à démarrer en tant que secondaire après recopie complète des données répliquées.
- Cliquer sur « Désactiver/activer » pour contrôler la détection d'erreur telle que décrite dans la [section 3.4.3.2.3](#).
- Cliquer sur « Déboguer » pour télécharger le journal ou snapshot du module depuis le nœud plutôt que depuis tous les nœuds tels que décrit dans la [section 3.5](#).

Pour comprendre et vérifier le bon fonctionnement d'un module miroir, voir la [section 5](#).  
Pour le tester, voir la [section 4](#).

### 3.4.3.2.2 Contrôler un module ferme

Dans cet exemple, les actions s'appliquent au module `farm` sur `node2` uniquement.



- (1) Cliquer sur `...` pour ouvrir le menu d'actions locales sur le nœud désiré (e.g. `node2`).
- Cliquer sur « Démarrer » pour démarrer le module sur le nœud.
- Cliquer sur « Arrêter » pour arrêter le module sur le nœud.
- Cliquer sur « Redémarrer » pour redémarrer le module sur le nœud.  
Il exécute uniquement les scripts d'arrêt puis de démarrage pour redémarrer l'application localement sans entraîner de basculement
- Cliquer sur « Désactiver/activer » pour contrôler la détection d'erreur telle que décrite dans la [section 3.4.3.2.3](#).
- Cliquer sur « Déboguer » pour télécharger le journal ou snapshot du module depuis le nœud plutôt que depuis tous les nœuds tels que décrit dans la [section 3.5](#).

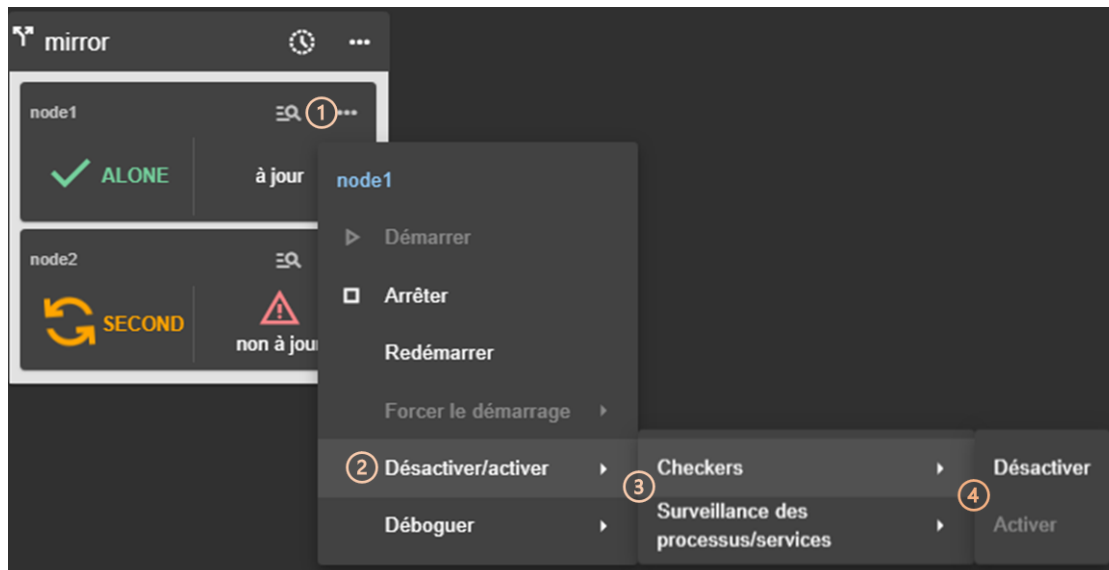
Pour comprendre et vérifier le bon fonctionnement d'un module ferme, voir la [section 6](#).  
Pour le tester, voir la [section 4](#).

### 3.4.3.2.3 Contrôler les checkers ou la surveillance des processus/services

Pour éviter une détection d'erreur infondée et un basculement automatique lors de la maintenance de l'application, vous pouvez désactiver les checkers configurés (TCP, ping, custom, etc.) ou la surveillance des processus/services. Une fois la maintenance terminée, ils peuvent être réactivés en toute sécurité. Ces actions peuvent être

effectuées lorsque le module est démarré/arrêté et ne sont pas réinitialisées lorsque le module redémarre.

Dans l'exemple ci-dessous, les actions s'appliquent au `mirror` sur `node1`.



- (1) Cliquer sur `...` pour ouvrir le menu d'actions locales sur le nœud désiré (e.g. `node1`).
- (2) Cliquer sur « Désactiver/activer » pour ouvrir le sous-menu.
- (3) Cliquer sur « Checkers » ou « Surveillance des processus/services » pour ouvrir le sous-menu.
- (4) Cliquer sur « Désactiver » pour désactiver la détection d'erreur.  
Cela désactive tous les checkers (TCP, ping, custom, etc.) ou la surveillance des processus/services configurés dans le module.
- (4) Cliquer sur « Activer » pour réactiver la détection d'erreur.  
Cela réactive tous les checkers (TCP, ping, custom, etc.) ou la surveillance des processus/services configurés dans le module.

### 3.4.4 Détails du module

Vous pouvez afficher les détails d'un module sur un nœud :

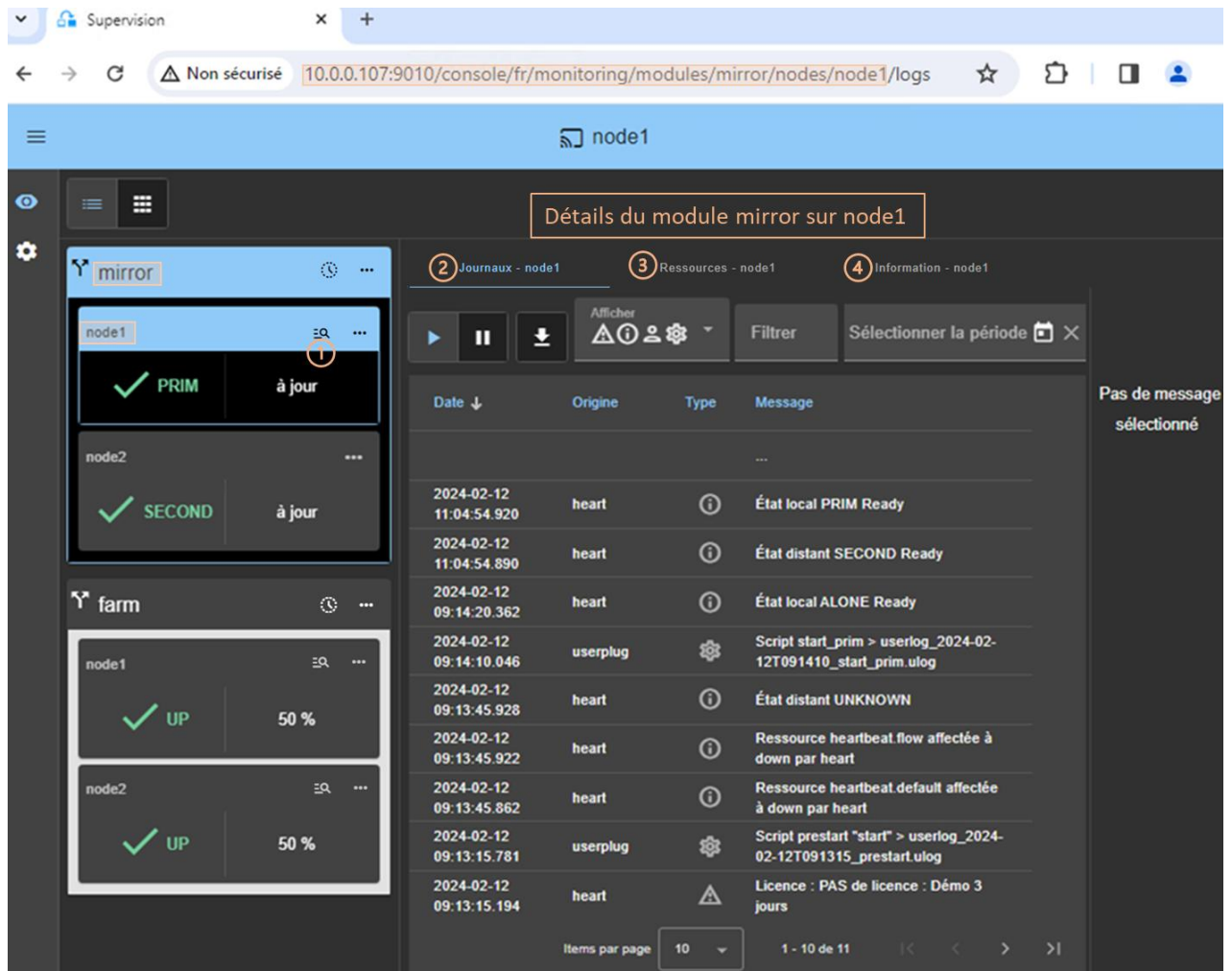
- Directement via l'URL  
<http://host:9010/console/fr/monitoring/modules/AM/nodes/node> (remplacer `AM` par le nom du module et `node` par le nom du nœud)

Ou

- En naviguant dans la console sur `👁 « Supervision/Cliquer sur module>nœud »`

Le module>nœud sélectionné est mis en évidence par une couleur bleue.

Dans l'exemple suivant, les détails du module `mirror` sur le `node1` sont affichés.



- (1) Cliquer sur pour ouvrir/fermer les détails du module sur ce nœud (logs, ressources...).
- (2) Cliquer sur l'onglet « Journaux » pour visualiser les journaux du module.
- (3) Cliquer sur l'onglet « Ressources » pour visualiser les ressources du module.
- (4) Cliquer sur l'onglet « Information » pour visualiser les informations sur le nœud.

Il s'agit du nom des lans et adresses définies dans la configuration du cluster, version et licence SafeKit, hostname et OS.

### 3.4.4.1 Journaux du module

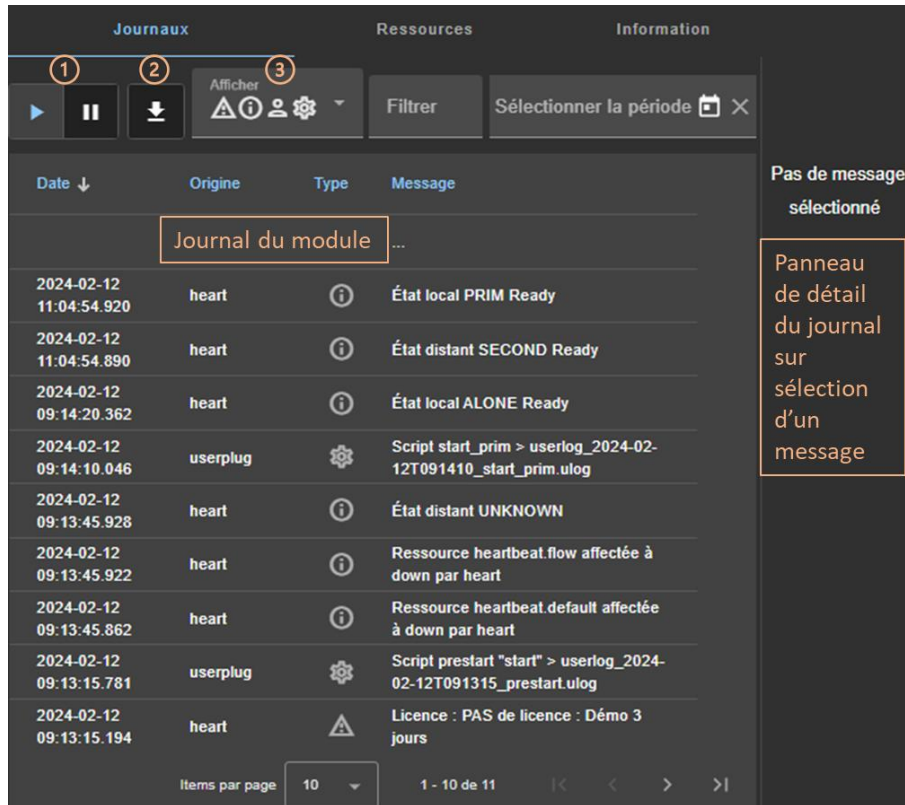
Vous pouvez afficher les journaux d'un module sur un nœud :

- Directement via l'URL <http://host:9010/console/fr/monitoring/modules/AM/nodes/node/logs> (remplacer *node* par le nom du nœud et *AM* par le nom du module)

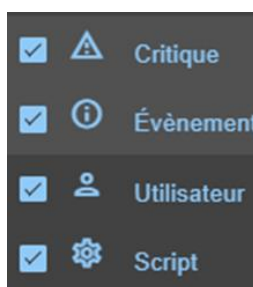
Ou

- En naviguant dans la console sur « Supervision/Cliquer sur module>nœud/Onglet Journaux »

Le panneau de gauche affiche en temps réel le journal non verbeux du module>nœud sélectionné.



- Cliquer sur ▶|| pour reprendre/suspendre la visualisation en temps réel du journal du module.  
Voir la [section 7](#), pour une explication des principaux messages.
- (2) Cliquer sur ↓ pour télécharger le journal du module (non verbeux ou verbeux).
- (3) Sélectionner le type de messages à afficher :



- C(ritique) messages tels que des détections d'erreurs
  - E(vènement) messages tels que l'état local et distant
  - U(ser) messages lorsque l'utilisateur exécute une action sur le module
  - S(cript) messages quand les scripts du module sont exécutés
- Cliquer sur un message pour afficher le journal verbeux du module ou le journal des scripts (sortie des scripts) dans le détail du journal dans le panneau de droite.

### 3.4.4.1.1 Journal du script

Pour afficher le journal du script du module, cliquer sur le message ⚙️S(cript) dont vous souhaitez visualiser l'output.

Date ↓	Origine	Type	Message	Journal du script
			...	----- 2024-02-12T09:14:10 start_prim
2024-02-12 11:04:54.920	heart		État local PRIM Ready	"Running start_prim WAIT ALONE"
2024-02-12 11:04:54.890	heart		État distant SECOND Ready	"Running start_prim WAIT ALONE"
2024-02-12 09:14:20.362	heart		État local ALONE Ready	[SC] ChangeServiceConfig SUCCESS
2024-02-12 09:14:10.046	userplug	1	Script start_prim > userlog_2024-02-12T091410_start_prim.ulog	The World Wide Web Publishing Service service is starting.
2024-02-12 09:13:45.928	heart		État distant UNKNOWN	The World Wide Web Publishing Service service was started successful
2024-02-12 09:13:45.922	heart		Ressource heartbeat.flow affectée à down par heart	The SQL Server (MSSQLSERVER) service is starting..
2024-02-12 09:13:45.862	heart		Ressource heartbeat.default affectée à down par heart	The SQL Server (MSSQLSERVER) service was started successfully.
2024-02-12 09:13:15.781	userplug		Script prestart "start" > userlog_2024-02-12T091315_prestart.ulog	The Milestone XProtect Management Server service is starting.
2024-02-12 09:13:15.194	heart		Licence : PAS de licence : Démo 3 jours	The Milestone XProtect Management Server service was started success

- (1) Cliquer sur le message S(cript) qui consiste en :
  - o la date et l'heure d'exécution du script
  - o le nom du script exécuté
  - o le nom du fichier userlog correspond

Le contenu du fichier userlog est affiché dans le panneau de droite. Dans l'exemple, il s'agit du contenu du fichier SAFEVAR/modules/AM/userlog\_2024-02-12T091410\_start\_prim.ulog (où AM est le nom du module).

### 3.4.4.1.2 Journal verbeux

Pour afficher le journal verbeux du module, cliquer sur un message autre que S(cript).

Date ↓	Origin	Type	Message	Date	Origin	Type	Message
			...	2024-02-12 11:04:54.920	heart		Local state PRIM Ready
2024-02-12 11:04:54.920	heart	1	Local state PRIM Ready	2024-02-12 11:04:54.918	heart	W	Local internal state ALONE_TO_PRI_2
2024-02-12 11:04:54.890	heart		Remote state SECOND Ready	2024-02-12 11:04:54.918	heart	W	Action alone_to_pri_2a terminated (-> CMD_OK)
2024-02-12 09:14:20.362	heart		Local state ALONE Ready	2024-02-12 11:04:54.900	rfsplug	W	Resource rfs.rfssync set to up by set_rfssync
2024-02-12 09:14:10.046	userplug		Script start_prim > userlog_2024-02-12T091410_start_prim.ulog	2024-02-12 11:04:54.890	heart		Remote state SECOND Ready
2024-02-12 09:13:45.928	heart		Remote state UNKNOWN	Items per page 10 1 - 5 of 5			
2024-02-12 09:13:45.922	heart		Resource heartbeat.flow set to down by heart				
2024-02-12 09:13:45.862	heart		Resource heartbeat.default set to down by heart				
2024-02-12 09:13:15.781	userplug		Script prestart "start" > userlog_2024-02-12T091315_prestart.ulog				
2024-02-12 09:13:15.194	heart		License : NO license : Demo 3 days				

- (1) Cliquer sur le message qui consiste en :
  - la date et l'heure de l'évènement
  - le message du module
- Tous les messages verbeux entre le message sélectionné et le précédent dans la table, sont affichés dans le panneau de droite.

### 3.4.4.2 Ressources du module

Vous pouvez afficher les ressources d'un module sur un nœud :

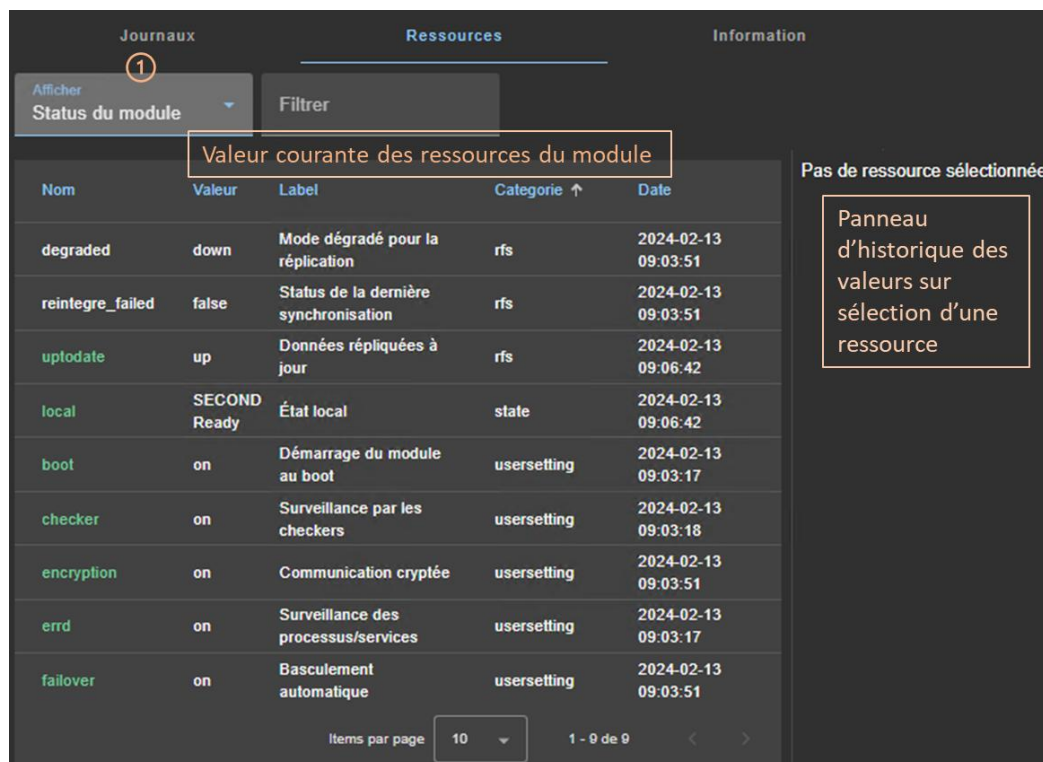
- Directement via l'URL  
<http://host:9010/console/fr/monitoring/modules/AM/nodes/node/ressources>  
(remplacer *AM* par le nom du module et *node* par le nom du nœud)

Ou

- En naviguant dans la console sur  « Supervision/Cliquer sur module>nœud/Onglet Ressources »

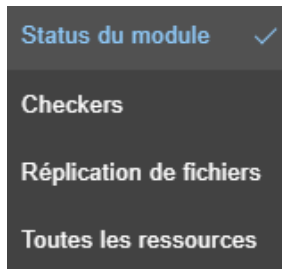
#### 3.4.4.2.1 État courant des ressources

Le panneau de gauche affiche en temps réel l'état courant des ressources du module>nœud sélectionné.



Nom	Valeur	Label	Categorie ↑	Date
degraded	down	Mode dégradé pour la réplication	rfs	2024-02-13 09:03:51
reintegre_failed	false	Status de la dernière synchronisation	rfs	2024-02-13 09:03:51
uptodate	up	Données répliquées à jour	rfs	2024-02-13 09:06:42
local	SECOND Ready	État local	state	2024-02-13 09:06:42
boot	on	Démarrage du module au boot	usersetting	2024-02-13 09:03:17
checker	on	Surveillance par les checkers	usersetting	2024-02-13 09:03:18
encryption	on	Communication cryptée	usersetting	2024-02-13 09:03:51
errd	on	Surveillance des processus/services	usersetting	2024-02-13 09:03:17
failover	on	Basculement automatique	usersetting	2024-02-13 09:03:51

- (1) Sélectionner le groupe de ressources à afficher



- Status du module  
Ressources principales, notamment de la réplication de fichiers pour un module miroir
  - Checkers  
Ressources affectées par des checkers
  - Réplication de fichiers  
Ressources spécifiques à la réplication de fichiers qui démontrent la progression de la synchronisation
  - Toutes les ressources
- Cliquer sur une ressource pour afficher la valeur de la ressource dans le temps dans le panneau de droite. Cet historique peut être vide pour certaines ressources (non affecté ou nettoyé).

L'état courant des ressources du module est contrôlé par la failover machine pour provoquer des actions sur le module en cas de défaillance (voir [section 13.19](#)).

### 3.4.4.2 Historique des valeurs d'une ressource

Pour afficher l'historique des valeurs d'une ressource, cliquer sur la ressource qui vous intéresse.

Nom	Valeur	Label	Categorie ↑	Date
checkfile	up	Custom checker	custom	2024-02-13 09:05:32
maxloop	false	Arrêt sur maxloop	heart	2024-02-13 09:03:51
default	up	Lien de surveillance	heartbeat	2024-02-13 09:03:52
flow	up	Lien de surveillance	heartbeat	2024-02-13 09:03:52
default	up	Interface de surveillance	heartbeatlocal addr	2024-02-13 09:03:51
flow	up	Interface de surveillance	heartbeatlocal addr	2024-02-13 09:03:51
10.0.0.0	up	Interface checker	intf	2024-02-13 09:44:47
10.0.0.228	inactif	IP checker	ip	
arpreroute.exe	up	Surveillance de processus/service	proc	2024-02-13 09:03:53
heart.exe	up	Surveillance de processus/service	proc	2024-02-13 09:03:51



Nom	Valeur	Date ↓
checkfile	up	2024-02-13 09:05:32
checkfile	down	2024-02-13 09:04:07

- (1) Cliquer sur la ligne qui consiste en :
  - la dernière date à laquelle la ressource a été affectée
  - le nom et la catégorie de la ressource. Le nom complet de la ressource est de la forme *catégorie.nom* (*custom.checkfile* dans l'exemple).

L'historique des valeurs de la ressource est affiché dans le panneau de droite. Dans l'exemple, il s'agit de la ressource `custom.checkfile` correspondant à une ressource affectée par un custom checker.

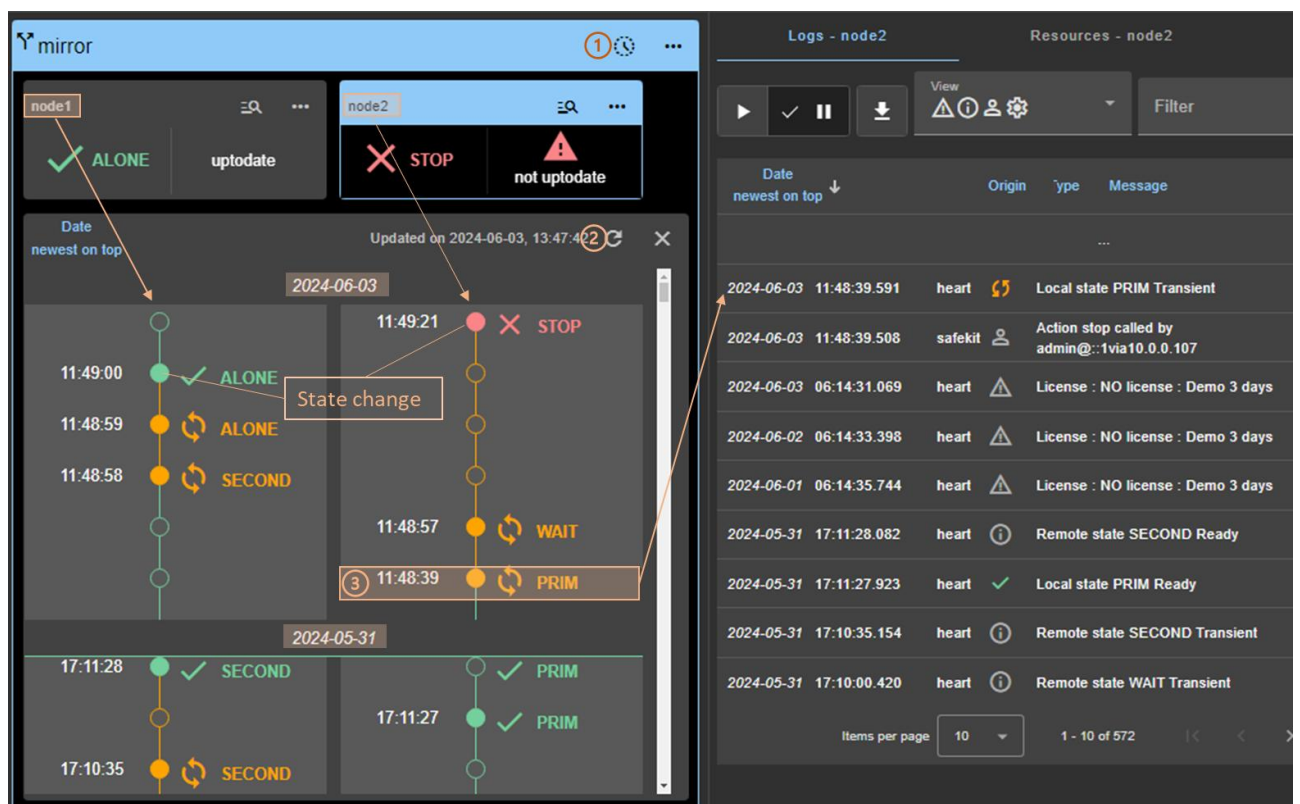
### 3.4.5 Chronologie des états du module

Depuis SafeKit 8.2.2, vous pouvez afficher la chronologie des états d'un module :

- En naviguant dans la console sur  « Supervision/Cliquer sur  pour le module »

Cela permet d'avoir une vue globale de l'état du module sur le cluster. Notez que :

- les horloges des deux nœuds doivent être synchronisées pour que la mise en correspondance des changements d'état soit significative.
- la chronologie affichée est inversée : les états du module sur tous les nœuds au fil du temps, en commençant par la date la plus récente.





The screenshot displays the 'mirror' interface for monitoring a module. The left pane shows a state history timeline for two nodes, 'node1' and 'node2'. The right pane shows the logs for 'node2'.

**State History Timeline (Left Pane):**

Date	Node	State	Icon
2024-06-03 11:49:21	node2	STOP	Red X
2024-06-03 11:48:59	node1	ALONE	Green checkmark
2024-06-03 11:48:58	node1	ALONE	Yellow refresh
2024-06-03 11:48:58	node1	SECOND	Yellow refresh
2024-06-03 11:48:57	node2	WAIT	Yellow refresh
2024-06-03 11:48:39	node2	PRIM	Yellow refresh
2024-05-31 17:11:28	node1	SECOND	Green checkmark
2024-05-31 17:11:27	node2	PRIM	Green checkmark
2024-05-31 17:10:35	node1	SECOND	Yellow refresh
2024-05-31 17:10:00	node2	PRIM	Green checkmark

**Logs for node2 (Right Pane):**

Date	Time	Origin	Type	Message
2024-06-03	11:48:39.591	heart	🔔	Local state PRIM Transient
2024-06-03	11:48:39.508	safekit	👤	Action stop called by admin@:1 via 10.0.0.107
2024-06-03	06:14:31.069	heart	⚠️	License : NO license : Demo 3 days
2024-06-02	06:14:33.398	heart	⚠️	License : NO license : Demo 3 days
2024-06-01	06:14:35.744	heart	⚠️	License : NO license : Demo 3 days
2024-05-31	17:11:28.082	heart	🔔	Remote state SECOND Ready
2024-05-31	17:11:27.923	heart	✅	Local state PRIM Ready
2024-05-31	17:10:35.154	heart	🔔	Remote state SECOND Transient
2024-05-31	17:10:00.420	heart	🔔	Remote state WAIT Transient

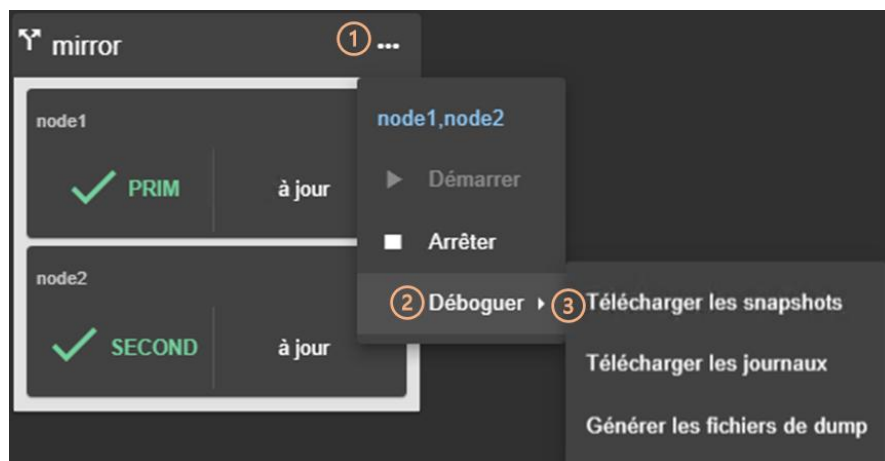
- (1) Cliquer sur  pour ouvrir/fermer la chronologie. La chronologie affichée est celle disponible au moment du chargement.
- (2) Cliquer sur  pour rafraîchir la chronologie avec les derniers changements d'état.
- (3) Cliquer sur un événement de changement d'état pour afficher le journal du module pour le nœud à partir de cette date.

### 3.5 Snapshots et journaux du module applicatif pour le débogage et support

Lorsque le problème n'est pas facilement identifiable, il est recommandé de prendre un snapshot du module sur tous les nœuds, comme décrit ci-dessous. Les snapshots permettent une analyse hors ligne et approfondie de l'état du module et du nœud, tel

que décrit dans la [section 7.18](#). Si cette analyse échoue, envoyez les snapshots au support via le [portail du support](#).

Dans l'exemple suivant, le module `mirror` est configuré sur `node1` et `node2`. Notez qu'un snapshot peut être téléchargé dans n'importe quel état du module.



- (1) Cliquer sur `...` pour ouvrir le menu global sur le module.
- (2) Cliquer sur « Déboguer » pour ouvrir le sous-menu de débogage.
- (3) Cliquer sur « Télécharger les snapshots » pour créer et télécharger le snapshot du module pour chaque nœud.

La console web s'appuie sur les paramètres de téléchargement du navigateur web pour sauvegarder les snapshots sur la station de travail. Certains navigateurs peuvent demander une confirmation pour télécharger plusieurs fichiers et des `.zip`.

La commande de génération du snapshot génère un nouveau dump et crée un fichier `.zip` qui contient les 3 derniers dumps et les 3 dernières configurations du module.

Dans cet exemple, 2 snapshots sont téléchargés : `snapshot_node1_mirror.zip` et `snapshot_node2_mirror.zip`.

- Cliquer sur « Télécharger les journaux » pour télécharger le journal du module (verbeux ou non) pour chaque nœud.
- En cas de problèmes de réplication de fichiers, il peut être nécessaire de « Générer les fichiers de dump » au moment où le problème se produit.









Le dump contient les journaux du module et des informations sur l'état du système et de SafeKit au moment du dump. Il est généré du côté serveur sous `SAFEVAR/snapshot/modules/mirror/dump_AAAA_MM_DD_hh_mm_ss`.



Depuis SafeKit 8.2.4, les zips générés pour les snapshots sont protégés par le mot de passe `safekit`. Ceci permet de réceptionner le snapshot dans sa totalité lorsqu'il est envoyé dans un courriel.

### 3.6 Sécuriser la console web

SafeKit propose différentes politiques de sécurité pour la console web mises en œuvre en modifiant la configuration du service web SafeKit. Ces configurations offrent aussi une gestion de rôles :

Rôle Admin  	Ce rôle accorde tous les droits d'administration en autorisant l'accès à la  Configuration et  Supervision dans la barre de navigation latérale
Rôle Control 	Ce rôle accorde tous les droits de supervision et contrôle en autorisant l'accès à la  Supervision
Rôle Monitor 	Ce rôle n'accorde que des droits de supervision, interdisant les actions sur les modules (démarrage, arrêt...) sous  Supervision

SafeKit fournit différentes configurations pour le service web afin de renforcer la sécurité de la console. Les configurations prédéfinies sont listées ci-dessous de la moins sécurisée à la plus sécurisée :

- HTTP. Rôle identique pour tous les utilisateurs sans authentification  
Cette solution ne peut être mise en œuvre qu'en HTTP et est incompatible avec les méthodes d'authentification des utilisateurs.
- HTTP/HTTPS avec authentification à base de fichiers et gestion de rôles facultative  
Elle repose sur le fichier Apache `user.conf` pour authentifier les utilisateurs et, optionnellement, restreindre leurs accès en fonction des rôles avec le fichier `group.conf`. La connexion à la console nécessite la saisie du nom et du mot de passe de l'utilisateur tels qu'ils ont été configurés avec les mécanismes d'Apache.  
Il s'agit de la configuration par défaut, en HTTP et initialisée avec un seul utilisateur `admin` ayant le rôle Admin. Cette configuration peut être étendue pour rajouter des utilisateurs ou passer en HTTPS.
- HTTP/HTTPS avec authentification à base de serveur LDAP/AD. Gestion de rôles facultative  
Elle repose sur le serveur LDAP/AD pour authentifier les utilisateurs et, optionnellement, restreindre leurs accès en fonction des rôles. La connexion à la console nécessite la saisie de l'identifiant et du mot de passe de l'utilisateur tels qu'ils ont été configurés dans le serveur LDAP/AD. Elle peut être appliquée en HTTP ou HTTPS.
- HTTPS avec authentification à base de serveur d'OpenId Connect. Gestion de rôles facultative  
Elle repose sur le serveur OpenID Identity Provider pour authentifier les utilisateurs et, optionnellement, restreindre leurs accès en fonction des rôles. La connexion à la console nécessite la saisie de l'identifiant et du mot de passe de l'utilisateur tels qu'ils ont été configurés dans le serveur OpenID. Depuis SafeKit 8.2.3, l'authentification OpenId ne peut être utilisée qu'avec HTTPS.

Pour les mettre en œuvre, se référer à la [section 11](#).

## 4. Tests

- ⇒ [Section 4.1](#) « Installation et tests après boot »
- ⇒ [Section 4.2](#) « Tests d'un module miroir »
- ⇒ [Section 4.3](#) « Tests d'un module ferme »
- ⇒ [Section 4.4](#) « Tests des checkers communs à un miroir et une ferme »

Les tests suivants permettent de mieux comprendre le fonctionnement de SafeKit et de s'assurer que la solution déployée retourne bien les résultats attendus. Ils peuvent être utilisés comme base de cahier de recette chez un client.

Dans la suite, l'analyse des résultats des tests peut nécessiter de consulter le journal du module, le journal des scripts (qui contient l'output des scripts du modules) ou l'état des ressources du module. Pour cela, voir la [section 7.4](#).

### 4.1 Installation et tests après boot

#### 4.1.1 Test installation package

Dans la suite, remplacer `node1` par le nom du nœud et `AM` par le nom du module.

- `safekit -p` exécuté sur un nœud retourne, entre autres valeurs, la valeur de `SAFE`, le chemin d'installation racine de SafeKit, et `SAFEVAR`, le répertoire de travail de SafeKit :
  - o sous Windows

```
SAFE=C:\safekit si SystemDrive=C:
SAFEVAR=C:\safekit\var
```
  - o sous Linux

```
SAFE="/opt/safekit"
SAFEVAR="/var/safekit"
```

Pour plus d'informations, voir la [section 10.1](#).

- L'édition de `userconfig.xml` d'un module miroir (/ferme) et de ses scripts `start_prim/start_both`, `stop_prim/stop_both` est réalisée avec :
- La console web avec l'URI [/console/fr/configuration/modules/AM/config](#)
- Sous le répertoire `SAFE/modules/AM` sur `node1`
- Le journal du module et le journal des scripts (qui contient output des scripts du module) peuvent être consultés avec :
  - o la console web avec l'URI [/console/fr/monitoring/modules/AM/nodes/node1/logs](#)
  - o la commande `safekit logview -m AM` exécutée sur `node1`, pour le journal du module
  - o sur `node1`, dans les fichiers `SAFEVAR/modules/AM/userlog_<year>_<month>_<day>T<time>_<script name>.u.log`, pour le journal des scripts

### 4.1.2 Test licence et version

`safekit level` retourne

```
Host : <hostname>
OS : <OS version>
SafeKit : <SafeKit version>
License : Demo (No license)| Invalid Product | Invalid Host | ... Expiration... | <license id> for
<hostname>...
or License : Expired license
```

- "No license"  
signifie qu'il n'y a pas de fichier `SAFE/conf/license.txt` : le produit s'arrête tous les 3 jours
- "Invalid Product"  
signifie que la licence a expiré dans `SAFE/conf/license.txt`
- "Invalid Host"  
signifie que le hostname est invalide dans `SAFE/conf/license.txt`
- " ...Expiration..."  
indique une clé temporaire
- "<license id> for <hostname>"  
indique une clé permanente

Cliquer [ici](#) pour obtenir une clé temporaire d'un mois pour n'importe quel hostname/OS.

Cliquer [ici](#) pour obtenir une clé permanente basée sur le hostname et l'OS.

### 4.1.3 Test des services et modules SafeKit après boot

Pour Windows, voir aussi la [section 10.4](#).

#### Test du service `safeadmin`

Le service `safeadmin` doit être démarré automatiquement au boot. Pour vérifier son état :

Windows	<ol style="list-style-type: none"><li>1. Ouvrir une console PowerShell en tant qu'administrateur</li><li>2. Exécuter <code>Get-Service -name safeadmin</code> <pre>Status Name      DisplayName ----- Running safeadmin  safeadmin</pre></li></ol>
Linux	<ol style="list-style-type: none"><li>1. Ouvrir une console Shell en tant que root</li><li>2. Exécuter <code>systemctl status safeadmin</code> <pre>Redirecting to /bin/systemctl status safeadmin.service ● safeadmin.service - The SafeKit Administration Daemon    Loaded: loaded (/usr/lib/systemd/system/safeadmin.service; enabled; vendor preset: disabled)    Active: active (running) since Tue 2024-11-12 17:30:56 CET; 20h ago    ...</pre></li></ol>

Lorsque le service `safeadmin` n'est pas actif, toutes les commandes `safekit` échouent et retournent par exemple :

```
safekit level
```

```
Waiting for safeadmin .....
Error: safeadmin administrator daemon not running
```

Voir la [section 9.1.1](#) pour démarrer le service `safeadmin`.

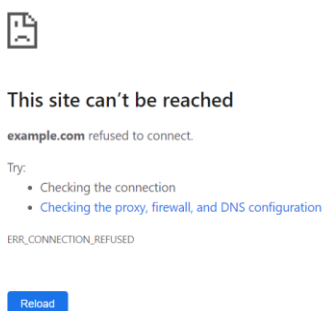
### Test du service `safewebserver`

Par défaut, le service `safewebserver` est démarré automatiquement au boot. Pour vérifier son état :

Windows	<ol style="list-style-type: none"> <li>Ouvrir une console PowerShell en tant qu'administrateur</li> <li>Exécuter Run <code>Get-Service -name safewebserver</code></li> </ol> <pre>Status Name          DisplayName ----- ----          - Running safewebserver safewebserver</pre>
Linux	<ol style="list-style-type: none"> <li>Ouvrir une console Shell en tant que root</li> <li>Exécuter <code>systemctl status safewebserver</code></li> </ol> <pre>systemctl status safewebserver Redirecting to /bin/systemctl status safewebserver.service safewebserver.service - SafeKit Apache Server    Loaded: loaded (/usr/lib/systemd/system/safewebserver.service; enabled;    vendor preset: disabled)    Active: active (running) since Wed 2024-11-13 11:01:31 CET; 2h 58min ago    ...</pre>

Lorsque le service `safewebserver` n'est pas actif, les fonctionnalités suivantes ne sont pas opérationnelles :

- La console web SafeKit qui affiche :



- Le module checker
- La commande distribuée qui retourne par exemple :

```
safekit -H "*" level
----- Server=https://10.0.0.107:9453 -----
```

```
curl: (7) Failed to connect to 10.0.0.107 port 9453 after 1022 ms: Couldn't connect to server
----- Server=https://10.0.0.108:9453 -----
curl: (28) Failed to connect to 10.0.0.108 port 9453 after 21024 ms: Couldn't connect to server
```

Voir la [section 9.1.2](#) pour démarrer le service `safewebserver`.

### Test du service SNMP

Par défaut, la surveillance SNMP n'est pas activée. Voir la [section 10.11](#) pour l'activer.

En Windows, elle est fournie par le service `Net-SNMP Agent`. En Linux, elle repose sur le service standard `snmpd`. Pour vérifier son état :

Windows	<ol style="list-style-type: none"><li>Ouvrir une console PowerShell en tant qu'administrateur</li><li>Exécuter <code>Run Get-Service -name "Net-SNMP Agent"</code></li></ol> <pre>Status Name          DisplayName ----- ----          - Running Net-SNMP Agent  Net-SNMP Agent</pre>
Linux	<ol style="list-style-type: none"><li>Ouvrir une console Shell en tant que root</li><li>Exécuter <code>systemctl status snmpd</code></li></ol> <pre>systemctl status snmpd Redirecting to /bin/systemctl status snmpd.service snmpd.service - ... Active: active (running) since Wed 2024-11-13 11:01:31 CET; 2h 58min ago ...</pre>

Lorsque le service n'est pas actif, la surveillance SNMP n'est pas opérationnelle.

Voir la [section 9.1.4](#) pour démarrer le service.

### Test des modules

- `safekit boot status` retourne le démarrage ("on") ou non ("off") des modules au boot
- `safekit state` retourne l'état de tous les modules configurés : `STOP` (miroir ou ferme), `WAIT` (miroir ou ferme), `ALONE` (miroir), `PRIM` (miroir), `SECOND` (miroir), `UP` (ferme)
- vérifier les processus d'un module (voir [section 10.2](#))  
Pour lister les processus du module `AM`, exécuter :  

```
safekit -r processtree list all AM
```

  
Cette commande retourne tous les processus ayant `AM` en argument.
- `safekit module listid` retourne le nom des modules installés et leurs ids : l'id d'un module doit être le même sur tous les serveurs

#### 4.1.4 Test démarrage de la console web

- Connecter un navigateur web à `http://<server IP>:9010`
- La page d'accueil de la console web apparaît

## 4.2 Tests d'un module miroir

### 4.2.1 Test du premier start d'un module miroir sur 2 serveurs **X**STOP (NotReady)

Au premier démarrage du module après sa configuration :

- Message dans les journaux du module sur les 2 serveurs (pour lire les journaux, voir la [section 7.4](#))

```
"Action start called by admin@<IP>/SYSTEM/root"
```

- Le module va dans l'état **O** WAIT (NotReady) and **O** WAIT (NotReady) sur les 2 serveurs et le journal contient les messages

```
"Action wait from failover rule rfs_notuptodate_server"
>Data may be not uptodate for replicated directories (wait for the start of the remote server)"
>If you are sure that this server has valid data, run safekit stop, then safekit prim to force start as primary"
```

Pour le premier démarrage d'un module miroir avec de la réplication de fichiers, l'utilisateur doit forcer le démarrage en primaire du serveur ayant les données répliquées à jour. Voir la [section 5.3](#).

### 4.2.2 Test start d'un module miroir sur 2 serveurs **X**STOP (NotReady)

Pour les démarrages suivants :

- Message dans les journaux du module sur les 2 serveurs (pour lire les journaux, voir la [section 7.4](#))

```
"Action start called by admin@<IP>/SYSTEM/root"
```

- Le module va dans l'état stable **✓** PRIM (Ready) et **✓** SECOND (Ready) sur les 2 nœuds avec dans le 1<sup>er</sup> journal

```
"Remote state SECOND Ready"
"Local state PRIM Ready"
```

- Et dans le 2<sup>nd</sup> journal

```
"Local state SECOND Ready"
"Remote state PRIM Ready"
```

- L'application est démarrée dans le script `start_prim` du module PRIM avec le message dans son log

```
"Script start_prim"
```

### 4.2.3 Test stop d'un module miroir sur le serveur **✓**PRIM (Ready)

Sur le serveur qui s'arrête :

- Message dans le journal du module (pour lire les journaux voir la [section 7.4](#))

```
"Action stop called by admin@<IP>/SYSTEM/root"
```

- Le module qui s'arrête exécute le script `stop_prim` pour arrêter l'application sur le serveur avec le message dans son journal :

```
"Script stop_prim"
```

- Le module arrêté devient **X**STOP (NotReady) avec les messages dans son journal :

```
"Local state STOP NotReady"
```

Sur l'autre serveur :

- Le module exécute un basculement avec le message dans son journal :  
"Action alone called by heart : remote stop"
- L'application est démarrée avec le script `start_prim` script du module :  
"Script start\_prim"
- Le serveur de reprise devient ALONE (Ready) avec le message dans son journal :  
"Local state ALONE Ready "

### 4.2.4 Test start du module miroir dans l'état STOP (NotReady)

Démarrage du module alors que le module est dans l'état ALONE (Ready) sur l'autre serveur :

- Message dans le journal du module redémarré (pour lire les journaux voir la [section 7.4](#))  
"Action start called by admin@<IP>/SYSTEM/root"
- Le module STOP (NotReady) devient SECOND (Ready)
- Le module sur l'autre serveur passe de ALONE (Ready) à PRIM (Ready) et continue à exécuter l'application

### 4.2.5 Test restart du module miroir dans l'état PRIM (Ready)

- Message dans le journal du module redémarré (pour lire les journaux voir la [section 7.4](#))

```
"Action restart called by admin@<IP>/SYSTEM/root"
```

- Le module PRIM devient PRIM (magenta) puis PRIM (Ready)
- Les scripts du module `stop_prim/start_prim` sont exécutés sur le module PRIM et redémarre localement l'application avec les messages dans son journal :

```
"Script stop_prim"  
"Script start_prim"
```

- L'autre serveur reste SECOND (Ready)

### 4.2.6 Test adresse IP virtuelle d'un module miroir

Le test ci-dessus utilise la commande `arp` spécifique à IPv4. Pour une VIP de type IPv6 ou des problèmes de résolution VIP ↔ MAC, voir la [section 7.24](#).

Module miroir dans l'état PRIM (Ready) sur le serveur node1 et SECOND (Ready) sur le serveur node2.

userconfig.xml :

```
<vip>  
  <interface_list>  
    <interface check="on">  
      <real_interface>  
        <virtual_addr addr="virtip"  
          where="one_side_alias"  
          check="on"/>  
      </real_interface>  
    </interface>  
  </interface_list>  
</vip>
```

1. Sur le serveur node1, `ipconfig /all` (Windows) ou `ip addr show` (Linux) retourne `virtip` en alias sur l'interface réseau.

Sur la station externe (ou le serveur), les 3 pings répondent

Sur la station externe (ou le serveur) dans le même LAN, `virtip` est mappé sur l'adresse MAC de node1

<pre>&lt;/real_interface&gt; &lt;/interface&gt; &lt;/interface_list&gt; &lt;/vip&gt;</pre> <ol style="list-style-type: none"> <li>Sur une station de travail externe (ou un serveur) dans le même LAN, ping des 2 adresses IP physiques + adresse IP virtuelle : <pre>ping adresse_ip_node2 ping adresse_ip_node1 ping virtip arp -a</pre> </li> <li>safeKIT stopstart -m AM (où AM est le nom du module) sur le serveur primaire</li> <li>Sur la station de travail externe (ou le serveur) dans le même LAN, <pre>ping adresse_ip_node2 ping adresse_ip_node1 ping virtip arp -a</pre> <p>Note: refaire le ping vers virtip avant de regarder la table ARP car l'entrée peut être marquée obsolète et est rafraîchie après le ping</p> </li> </ol>	<pre>arp -a adresse_ip_node1    00-0c-29-0a-5c-fc adresse_ip_node2    00-0c-29-26-44-93 virtip              00-0c-29-0a-5c-fc</pre> <ol style="list-style-type: none"> <li>Après le stopstart avec  SECOND (Ready) sur serveur node1 et  PRIM (Ready) sur serveur node2 <p>Dans le journal verbeux du nouveau PRIM, message :</p> <pre>"Virtual IP &lt;virtip of mirror&gt; set"</pre> </li> <li>Sur le serveur node2, ipconfig /all (Windows) ou ip addr show (Linux) retourne virtip en tant qu'alias sur l'interface réseau <p>Sur la station externe (ou le serveur), les 3 pings répondent</p> <p>Sur la station externe (ou le serveur), virtip est mappé sur l'adresse MAC de ip1.2</p> <pre>arp -a adresse_ip_node1    00-0c-29-0a-5c-fc adresse_ip_node2    00-0c-29-26-44-93 virtip              00-0c-29-26-44-93</pre> </li> </ol>
--	--

#### 4.2.7 Test réplification de fichiers d'un module miroir

<p>Module miroir dans l'état  PRIM (Ready) sur serveur node1 et  SECOND (Ready) sur serveur node2.</p> <p>userconfig.xml en Windows :</p> <pre>&lt;rfs&gt;   &lt;replicated dir="c:\replicated" mode="read_only" /&gt; &lt;/rfs&gt;</pre> <p>userconfig.xml en Linux :</p> <pre>&lt;rfs&gt;   &lt;replicated dir="/replicated" mode="read_only" /&gt; &lt;/rfs&gt;</pre> <p>En Windows, le répertoire répliqué est c:\replicated ; en Linux, /replicated.</p> <ol style="list-style-type: none"> <li>Sur le serveur  PRIM (Ready), aller dans le répertoire répliqué et créer 1 fichier file1.txt</li> </ol>	<ol style="list-style-type: none"> <li>Le fichier file1.txt a été créé sur le serveur  SECOND (Ready) dans le répertoire répliqué</li> <li>Échec car le répertoire répliqué /replicated est en lecture seule sur le serveur  SECOND (Ready)</li> <li>Le fichier file2.txt n'est pas répliqué dans le répertoire sur le serveur  STOP (NotReady)</li> <li>Le fichier file2.txt est réintégré sur le serveur redémarré. Pendant la phase de réintégration, le serveur est  SECOND (Transient)</li> </ol> <p>Dans le journal du serveur Linux réintégré, message</p> <pre>"Updating directory tree from /replicated_For_SafeKit_Replication "</pre>
--	--

<ol style="list-style-type: none"><li>2. Sur le serveur  SECOND (Ready), aller dans le répertoire répliqué et essayer de détruire <code>file1.txt</code></li><li>3. Arrêter le serveur  PRIM (Ready) et attendre qu'il soit  STOP (NotReady). Puis aller sur l'autre serveur devenu  ALONE (Ready) et créer un nouveau fichier <code>file2.txt</code></li><li>4. Redémarrer le serveur  STOP (NotReady) et attendre qu'il soit  SECOND (Ready).</li></ol>	<p>Dans le journal du serveur Windows réintégré, message</p> <pre>"Updating directory tree from c:\replicated"</pre> <p>Et à la fin de la réintégration du répertoire, lorsqu'au moins 1 fichier avec des données modifiées a été réintégré de la machine primaire vers la machine secondaire, message</p> <pre>"Copied &lt;reintegration statistics&gt;" "Reintegration ended (synchronize)"</pre> <p>Ce message donne les statistiques de réintégration du répertoire : taille réintégré, nombre de fichiers, temps, débit sur le réseau de réplication en KB/sec.</p> <p>Note : réintégrer un fichier de plus de 100 MB pour avoir des statistiques fiables</p> <p>A la fin de la réintégration, le serveur est  SECOND (Ready)</p>
---	--

### 4.2.8 Test shutdown du serveur PRIM (Ready)

- Sur Windows, vérifier que la procédure spéciale d'arrêt des modules au shutdown a été réalisée (voir [section 10.4](#))
- Effectuer un shutdown du serveur PRIM (Ready)
- Vérifier dans le journal du serveur SECOND (Ready) le message

```
"Action alone called by heart : no heartbeat"
```
- Le serveur SECOND (Ready) devient ALONE (Ready). L'application dans le script `start_prim` du module est démarrée sur le serveur ALONE avec le message dans le log

```
"Script start_prim"
```
- Sur timeout dans la console web, l'ancien serveur PRIM (Ready) devient ERROR (connection error)
- Après reboot du serveur arrêté, vérifier que le shutdown de l'OS a réellement été appelé avec un shutdown

```
"Action shutdown called by SYSTEM/root"
```
- Vérifier que le script `stop_prim` de l'application a été exécuté avec le message

```
"Script stop_prim"
```
- Vérifier que le module a été complètement arrêté avant le shutdown du serveur avec le dernier message

```
"Local state STOP NotReady"
```

- Après reboot du serveur arrêté, si le module est automatiquement démarré au boot (`safekit boot status`), message dans le log

"Action start called at boot time"

- Après démarrage du module sur le serveur arrêté, le module devient SECOND (Ready) sur ce serveur et PRIM (Ready) sur l'autre serveur

#### 4.2.9 Test power-off du serveur PRIM (Ready)

En cas de panne de courant, le module n'est pas correctement arrêté comme il le serait lors d'un shutdown du serveur. Le basculement est déclenché par la perte des heartbeats, plutôt que par la détection de l'arrêt du module.

userconfig.xml avec 2 heartbeats :

```
<heart>
  <heartbeat name="default" />
  <heartbeat name="private"
    ident="flow" />
</heart>
```

Note : si vous voulez faire un test de double panne électrique simultanée sur les deux serveurs, vérifiez que `<rfs async="none">` est positionné dans `userconfig.xml`. Pour plus d'information, voir la [section 13.7.3](#).

- Dans le journal du nœud SECOND (Ready), message
 



```
"Resource heartbeat.default set to down by heart"
"Resource heartbeat.flow set to down by heart"
"Remote state UNKNOWN"
"Action alone called by heart : no heartbeat"
```
- Les messages apparaissent après 30 secondes à la suite du power-off (si aucun timeout configuré dans la section `<heart>` de `userconfig.xml`)
- Le serveur SECOND (Ready) devient ALONE (Ready) ; l'application dans le script `start_prim` du module est démarrée sur le serveur avec le message dans son log
 

```
"Script start_prim"
```
- Sur timeout de la console web, l'ancien serveur PRIM (Ready) devient ERROR (connection error)
- Après reboot du serveur arrêté, si le module est démarré automatiquement au boot (`safekit boot status`), message dans le log
 

```
"Action start called at boot time"
```
- Après redémarrage du module sur le serveur arrêté, le module devient SECOND (Ready) sur ce serveur et PRIM (Ready) sur l'autre serveur

#### 4.2.10 Test split-brain avec un module miroir

Le split-brain se produit en situation d'isolation réseau entre les deux serveurs SafeKit. Chaque serveur devient primaire ALONE et tourne l'application. Au retour du split-brain, un sacrifice doit être réalisé en arrêtant l'application sur un seul des deux serveurs.

Module miroir dans l'état  PRIM (Ready) et  SECOND (Ready)

userconfig.xml :

```
<heart>
  <heartbeat name="default" />
  <heartbeat name="repli" ident="flow" />
</heart>
```

+

sur Windows pour gérer le conflit sur l'adresse IP virtuelle virtip


```
<vip>
  <interface_list>
    <interface check="off">
      <real_interface>
        <virtual_addr addr="virtip"
          where="one_side_alias"
          check="on"/>
      </real_interface>
    </interface>
  </interface_list>
</vip>
```

Pour obtenir le split-brain, vérifier qu'il n'y a pas de checkers dans userconfig.xml qui peuvent détecter l'isolation : pas de `<interface check="on">` ou de `<ping>` checker

1. Déconnecter en même temps les réseaux default et repli
2. Reconnecter les réseaux

1. Après isolation réseau des deux serveurs, tous les heartbeats sont perdus. Dans les logs des 2 serveurs,

```
"Resource heartbeat.default set to down by heart"
"Resource heartbeat.flow set to down by heart"
"Remote state UNKNOWN"
"Local state ALONE Ready"
```

Cas de split-brain : les 2 serveurs sont  ALONE (Ready) et l'application est démarrée

2. Lorsque les réseaux sont reconnectés, sacrifice d'un des 2 serveurs ALONE : l'ancien serveur SECOND

Journal de l'ancien PRIM non sacrifié :



```
"Remote state ALONE Ready"
"Split brain recovery: staying alone"
```

Journal de l'ancien SECOND sacrifié :

```
"Remote state ALONE Ready"
"Split brain recovery: exiting alone"
"Script stop_prim"
```

Le serveur réalise un stopstart : arrêt de l'application avec stop\_prim puis réintégration des fichiers répliqués à partir de l'autre serveur.

En Windows, sur reconnexion, il peut se produire un conflit sur l'adresse IP virtuelle, entraînant le stopstart du module.

3. Retour à l'état  PRIM (Ready) et  SECOND (Ready) sur les 2 serveurs tel qu'ils étaient avant split-brain

Note : la situation de split-brain dans un module miroir avec réplication est malsaine. En effet, le sacrifice de l'ex secondaire provoque la réintégration des données sur ce serveur à partir de la primaire et la perte des données enregistrées sur la secondaire pendant la situation de split-brain.


Pour cette raison, 2 voies de heartbeat sur 2 réseaux physiquement distincts sont conseillées. Typiquement, un câble entre les deux serveurs va permettre (1) d'éviter le split-brain avec un réseau supplémentaire de heartbeat et (2) de faire passer le flux de réplication.

### 4.2.11 Continuer les tests de votre module miroir avec les checkers

Voir les tests décrits en [section 4.4](#).

## 4.3 Tests d'un module ferme

### 4.3.1 Test start d'un module ferme sur les serveurs STOP (NotReady)


- Message dans les logs de tous les nœuds (pour lire les journaux, voir la [section 7.4](#))  
"Action start called by admin@<IP>/SYSTEM/root"
- Le module va dans l'état  UP (Ready) sur tous les serveurs
- L'application est démarrée dans le script `start_both` du module sur tous les serveurs avec le message dans les logs

"Script start\_both"



### 4.3.2 Test stop d'un module ferme sur un serveur UP (Ready)

- Message dans le journal du nœud arrêté (pour lire les journaux, voir la [section 7.4](#))  
"Action stop called by admin@<IP>/SYSTEM/root"
- Le nœud qui s'arrête exécute le script `stop_both` pour stopper l'application localement avec le message dans le log

"Script stop\_both"

- Le module sur le serveur arrêté devient  STOP (NotReady) avec les messages dans son journal :



"Local state STOP NotReady"

- L'autre serveur reste  UP (Ready) et continue à exécuter l'application
- Redémarrer le serveur  STOP (NotReady) avec la commande `start`

### 4.3.3 Test restart d'un module ferme sur un serveur UP (Ready)

- Message dans le journal du module où la commande `restart` est servée (pour lire les journaux, voir la [section 7.4](#))

"Action restart called by admin@<IP>/SYSTEM/root"

- Le module redémarré devient  UP (Transient) puis devient  UP (Ready)
- Les scripts du module `stop_both/start_both` sont exécutés sur le serveur pour redémarrer localement l'application avec les messages dans le log

"Script stop\_both"  
"Script start\_both"

### 4.3.4 Test adresse IP virtuelle d'un module ferme

Les tests ci-dessus utilisent la commande `arp` spécifique à IPv4. Pour une VIP de type IPv6 ou des problèmes de résolution VIP ↔ MAC, voir la [section 7.24](#).

#### 4.3.4.1 Configuration avec `vmac_directed`

Module ferme dans l'état  UP (Ready) sur les 3 serveurs `ip1.1`, `ip1.2`

- Dans le journal verbeux de tous les serveurs :

userconfig.xml avec load balancing sur le service safewebserver (port TCP 9010) :

```
<farm>
<lan name="default" />
</farm>

<vip>
  <interface_list>
    <interface check="on">
      <virtual_interface type="vmac_directed" >
        <virtual_addr addr="virtip"
where="alias" check="on"/>
      </virtual_interface>
    </interface>
  </interface_list>

  <loadbalancing_list>
    <group name="FarmProto">
      <rule port="9010" proto="tcp"
filter="on_port"/>
    </group>
  </loadbalancing_list>
</vip>
```

Sur un poste (ou un serveur) externe dans le même LAN, ping des 2 IP physiques + IP virtuelle + arp -a

"Virtual IP <virtip of farm> set"

- Sur les 2 serveurs, ipconfig /all (Windows) ou ip addr show (Linux) retourne virtip en alias sur l'interface réseau.
- Sur une station de travail (ou un serveur) du même LAN, les pings répondent et virtip est mappée sur l'adresse MAC de l'un des deux serveurs :

```
ping node1_ip_address
ping node2_ip_address
ping virtip
```

```
arp -a
node1_ip_address      00-0c-29-0a-5c-fc
node2_ip_address      00-0c-29-26-44-93
virtip                00-0c-29-26-44-93
```

#### 4.3.4.2 Configuration avec vmac\_invisible

Module ferme dans l'état  UP (Ready) sur les 3 serveurs ip1.1, ip1.2

userconfig.xml avec load balancing sur le service safewebserver (port TCP 9010) :

```
<farm>
<lan name="default" />
</farm>

<vip>
  <interface_list>
    <interface check="on">
      <virtual_interface type="vmac_invisible" >
        <virtual_addr addr="virtip"
where="alias" check="on"/>
      </virtual_interface>
    </interface>
  </interface_list>

  <loadbalancing_list>
    <group name="FarmProto">
      <rule port="9010" proto="tcp"
filter="on_port"/>
    </group>
  </loadbalancing_list>
</vip>
```

- Dans le journal verbeux de tous les serveurs :

"Virtual IP <virtip of farm> set"

- Sur les 2 serveurs, ipconfig /all (Windows) ou ip addr show (Linux) retourne virtip en alias sur l'interface réseau.
- Sur une station de travail (ou un serveur) du même LAN, les pings répondent et virtip est mappée sur l'adresse MAC virtuelle :

```
ping node1_ip_address
ping node2_ip_address
ping virtip
```

```
arp -a
node1_ip_address      00-0c-29-0a-5c-fc
node2_ip_address      00-0c-29-26-44-93
virtip                5a-fe-c0-a8-38-14
```

```
</loadbalancing_list>
</vip>
```

Sur un poste (ou un serveur) externe dans le même LAN, ping des 2 IP physiques + IP virtuelle + arp -a

- Note : par défaut, l'adresse MAC virtuelle est une adresse Ethernet unicast construite avec 5A:FE (SAFE) et l'adresse IP virtuelle en hexadécimale

### 4.3.5 Test load balancing TCP sur une adresse virtuelle

Le module ferme est dans l'état **✓UP** (Ready) sur les 2 serveurs node1, node2.

Même configuration de load balancing dans `userconfig.xml` que le test précédent.

Sur une station distante :

- Se connecter à l'URL <http://virtip:9010/safekit/mosaic.html>, puis cliquer sur Mosaic Test. node1, node2 répondent



- stop du module sur node2. Rechargement de l'URL. Seul node1 répond



Commande spéciale pour vérifier la bitmap de load balancing sur le port 9010 et sur chaque nœud

**✓UP** (Ready) :

```
safekit -r vip_if_ctrl -l
```

Une entrée de la bitmap de 256 bits doit être à 1 sur un seul serveur

De plus, les 256 bits sont distribués de manière équitable dans les bitmaps de tous les serveurs **✓UP** (Ready) (si pas de définition de l'attribut `power` dans `userconfig.xml`)

- ✓UP** (Ready) sur les 2 serveurs : load balancing des sessions TCP entre node1, node2 en chargeant l'URL

- Dans les ressources du module, pour node1 et node2 : `FarmProto_0 50%`

- Journal verbeux de node1 et node2

```
"farm membership: node1 node2 (group FarmProto_0)"
"farm load: 128/256 (group FarmProto_0)"
```

128/256 : 128 bits sur 256 sont gérés par chacun des serveurs

- `safekit -r vip_if_ctrl -l` sur node1 et node2

Avec `type="vmac_directed"`

```
Bitmap node1:
01010101:01010101:01010101:01010101:ffffffff:fff
ffff:ffffffff:ffffffff
Bitmap node2:
ffffffff:ffffffff:ffffffff:ffffffff:02020202:02020202:02020202:02020202
```

01 and 02 correspondent au numéro des nœuds qui répondent.

Avec `type="vmac_invisible"`

```
Bitmap node1:
00000000:00000000:00000000:00000000:ffffffff:fff
ffff:ffffffff:ffffffff
Bitmap node2:
ffffffff:ffffffff:ffffffff:ffffffff:00000000:00000000:00000000:00000000
```

Les bits sont équitablement répartis entre les 2 nœuds.

- ✗STOP** (NotReady) sur node2 : les sessions TCP sont servies par node1 lorsqu'on charge l'URL

- Dans les ressources du module, pour node1 : `FarmProto_0 100%`

- Dans le journal verbeux de node1 :

	<pre>"farm membership: node1 (group FarmProto_0)" "farm load: 256/256 (group FarmProto_0)"  256/256 : tous les bits sont gérés par node1  o safekit -r vip_if_ctrl -l sur node1:  Bitmap : ffffffff.ffffffff.ffffffff.ffffffff.ffffffff.ffffffff.ffffffff</pre>
--	---

### 4.3.6 Test split-brain avec un module ferme

Le split-brain se produit en situation d'isolation réseau entre les serveurs SafeKit.

Le module ferme est UP (Ready) UP (Ready) sur node1 et node2.

Même configuration de load balancing dans userconfig.xml que les tests précédents. Pour obtenir le split-brain, vérifier qu'il n'y a pas de checker pouvant détecter l'isolation : pas de `<interface check="on">` ou de checker `<ping>`.

Sur la station externe :

1. Se connecter à <http://virtip:9010/safekit/mosaic.html>, puis cliquer sur Mosaic Test. node1 and node2 répondent



2. Déconnecter le réseau default entre node1 et node2. Suivant l'endroit où se trouve la station externe, node 1 ou node 2 répond



ou



1. Avant split-brain, état UP (Ready) sur node1 et node2.

- o Dans les ressources pour node1 et node2 : FarmProto\_0 50%

- o Dans les logs verbeux de node1 et node2 :

```
"farm membership: node1 node2 (group FarmProto_0)"
"farm load: 128/256 (group FarmProto_0)"
```

128/256 : 128 bits sur 256 sont gérés par chacun des serveurs

- o safekit -r vip\_if\_ctrl -l sur node1 et node2 :

Avec type="vmac\_directed"

```
Bitmap node1:
01010101:01010101:01010101:01010101:ffffffff.ffffffff:fff
ffff:ffffffff
Bitmap node2:
ffffffff.ffffffff:ffffffff.ffffffff:02020202:02020202:02020202:0
2020202
```

01 and 02 correspondent au numéro des nœuds qui répondent.

Avec type="vmac\_invisible"

```
Bitmap node1:
00000000:00000000:00000000:00000000:ffffffff.ffffffff:fff
ffff:ffffffff
Bitmap node2:
ffffffff.ffffffff:ffffffff.ffffffff:00000000:00000000:00000000:0
000000
```

Les bits sont équitablement répartis entre les 2 serveurs

2. Après isolation réseau, split-brain :

- o Dans les ressources, pour node1 et node2 : FarmProto\_0 100%

3. Reconnecter le réseau et se recharger la page



Même commande spéciale que le test précédent pour vérifier la bitmap de load balancing sur le port 9010 sur chaque nœud

✓ UP (Ready)

- o Dans le journal verbeux de node1 :  

```
"farm membership: node1 (group FarmProto_0)"
"farm load: 256/256 (group FarmProto_0)"
```

256/256 : tous les bits sont gérés par node1
- o Dans le journal verbeux de node2 :  

```
"farm membership: node2 (group FarmProto_0)"
"farm load: 256/256 (group FarmProto_0)"
```

256/256 : tous les bits sont gérés par node2
- o `safekit -r vip_if_ctrl -l` sur node1 et node2:  

```
Bitmap:
ffffffff.ffffffff.ffffffff.ffffffff.ffffffff.ffffffff.ffffffff
```

3. Après split-brain lorsque le réseau est reconnecté, les mêmes messages peuvent être trouvés dans le journal et les mêmes bitmaps que ceux avant split-brain

Le comportement par défaut d'une ferme en situation de split-brain est correct. La recommandation est de mettre dans `userconfig.xml` un réseau de surveillance `<lan>` `</lan>`, là où se trouve l'adresse IP virtuelle.

Les messages dans le journal et le résultat de `vip_if_ctrl` sont légèrement différents selon le type `vmac_directed` ou `vmac_invisible`.

### 4.3.7 Test de la compatibilité du réseau avec l'adresse MAC invisible (`vmac_invisible`)

#### Prérequis réseau

Une adresse MAC Ethernet unicast `5a-fe-xx-xx-xx-xx` est associée à l'adresse virtuelle `virtip` d'un module ferme. Elle n'est jamais présentée par les serveurs SafeKit en tant qu'adresse Ethernet source (MAC invisible). Les switches ne peuvent donc pas localiser cette adresse. Lorsqu'ils font suivre un paquet à destination de l'adresse MAC `5a-fe-xx-xx-xx-xx`, ils doivent broadcaster le paquet sur tous les ports du LAN ou VLAN où se situe l'adresse IP virtuelle (flooding). Et tous les serveurs de la ferme reçoivent donc les paquets à

1. Tous les serveurs sont ✓ UP (Ready)
2. Le monitoring réseau est lancé dans chaque serveur en filtrant sur `virtip`
3. Un terminal externe envoie un seul ping vers l'adresse IP virtuelle avec `ping -n (ou -c) 1 virtip`
  - o 1 paquet envoyé et reçu par l'ensemble des serveurs  

```
"ICMP: Echo: From extip To virtip"
```
  - o il doit y avoir autant de paquets  

```
"ICMP: Echo Reply: To extip From virtip"
```

qu'il y a de serveurs ✓ UP (Ready)

Si ce n'est pas le cas, vérifier si des options restreignent le "port flooding" dans les switches

<p>destination de l'adresse MAC virtuelle 5a-fe-xx-xx-xx-xx.</p> <p>Noter que ce prérequis n'existe pas pour un module miroir (voir <a href="#">section 4.2.6</a>).</p> <h3>Prérequis serveur</h3> <p>Les paquets remontent dans les cartes Ethernet mises en mode promiscuous par SafeKit. Et les paquets sont filtrés par le module kernel &lt;vip&gt; suivant la bitmap de load balancing. Pour réaliser le test, il faut un outil de monitoring du réseau.</p> <p>Ex. monitoring réseau sur Linux :</p> <pre>tcpdump host virtip</pre>	<p>et empêche le broadcast de "ICMP: Echo" vers tous les serveurs.</p> <p>Attention : la restriction "port flooding" dans les switches peut avoir lieu après un certain nombre de flooding (temps, nombre de KB floodés) : le test ping est à répéter sur plusieurs heures en créant du flooding sur l'adresse IP virtuelle</p> <p>Note : pour éviter les outils de monitoring réseau, une console externe Linux peut être utilisée. Le ping Linux permet de vérifier les paquets dupliqués revenant des 3 serveurs</p> <p>✓ UP (Ready) :</p> <pre>ping virtip 64 bytes from virtip icmp_seq=1 64 bytes from virtip icmp_seq=1 (DUP!) 64 bytes from virtip icmp_seq=1 (DUP!) 64 bytes from virtip icmp_seq=2 64 bytes from virtip icmp_seq=2 (DUP!) 64 bytes from virtip icmp_seq=2 (DUP!) ...</pre> <p>Ce test peut être réalisé pendant plusieurs minutes en stockant l'output du ping dans un fichier et en vérifiant ensuite qu'il y a eu des (DUP!) tout le temps :</p> <pre>date &gt; /tmp/ping.txt ; ping virtip &gt;&gt; /tmp/ping.txt</pre>
--	--

### 4.3.8 Test shutdown d'un serveur ✓ UP (Ready)

- Sur Windows, vérifier que la procédure spéciale d'arrêt des modules au shutdown a été réalisée : voir [section 10.4](#)
- Effectuer un shutdown d'un serveur ✓ UP (Ready)
- Les autres serveurs restent ✓ UP (Ready) et continuent à exécuter l'application
- Sur timeout dans la console web, l'ancien serveur ✓ UP (Ready) devient **!** ERROR (connection error)
- Après reboot du serveur arrêté, vérifier que le shutdown de l'OS a réellement appelé un shutdown du module avec le message  
"Action shutdown called by SYSTEM"
- Vérifier que le script `stop_both` de l'application a été exécuté avec le message  
"Script stop\_both"
- Vérifier que le module a été complètement arrêté avant le shutdown du serveur avec le dernier message  
"Local state STOP NotReady"
- Après reboot du serveur arrêté, si le module est automatiquement démarré au boot (`safekit boot status`), message dans le log  
"Action start called at boot time"

- Après démarrage du module sur le serveur arrêté, le module devient UP (Ready) sur ce serveur et il exécute le script `start_both` qui redémarre l'application sur le serveur avec le message dans le log

"Script start\_both"

### 4.3.9 Test power-off d'un serveur UP (Ready)

En cas de panne de courant, le module n'est pas correctement arrêté comme il le serait lors d'un shutdown du serveur. Le basculement est déclenché par la perte des heartbeats, plutôt que par la détection de l'arrêt du module

- Les autres serveurs restent UP (Ready) et continuent à exécuter l'appli
- Sur timeout dans la console web, l'ancien serveur UP (Ready) devient ERROR (connection error)
- Après reboot du serveur arrêté, si le module est démarré automatiquement au boot (`safekit boot status`), message dans le log

"Action start called at boot time"

- Après redémarrage du module sur le serveur rebooté, le module devient UP (Ready) et il exécute le script `start_both` qui relance l'appli sur ce serveur avec le message dans le log

"Script start\_both"

### 4.3.10 Continuer les tests du module ferme avec les checkers

Voir les tests décrits en la [section 4.4](#).

## 4.4 Tests des checkers communs à un miroir et une ferme

### 4.4.1 Test <errd> checker avec action restart ou stopstart

Pour la description de la surveillance de processus/service, voir la [section 13.10](#).

Dans `userconfig.xml` :

```
<errd>
  <proc name="appli.exe" atleast="1"
  action="restart" class="prim"/>
</errd>
```

Le checker surveille le processus nommé `appli.exe`.





- `name="appli.exe" atleast="1"`

Au moins un processus `appli.exe` doit s'exécuter

- `class`
    - `class="prim"` pour un module miroir
- Checker démarré/arrêté, sur le serveur dans l'état PRIM ou ALONE (Ready), après/avant






- Tuer le processus `appli.exe` sur le serveur (Ready) ; c'est-à-dire dans l'état PRIM ou ALONE pour un module miroir et l'état UP pour un module ferme.





- Messages dans le journal :
  - "Process appli.exe not running"
  - "Action restart|stopstart called by errd"
- Le module passe dans un état (Transient), respectivement PRIM, ALONE ou UP
- Dans le cas `restart`, le module redevient (Ready), respectivement dans l'état PRIM, ALONE ou UP
- Dans le cas `stopstart`, le module redevient (Ready),

<p>l'application (<code>start_prim /stop_prim</code>)</p> <ul style="list-style-type: none"> <li>o <code>class="both"</code> pour un module ferme</li> </ul> <p>Checker démarré/arrêté, sur tous les serveurs dans l'état  UP (Ready), après/avant l'application (<code>start_both /stop_both</code>)</p> <ul style="list-style-type: none"> <li>• action</li> </ul> <p>Si le processus est absent, le checker met la ressource <code>proc.appli.exe</code> à <code>down</code>. Puis il exécute un <code>restart</code> ou <code>stopstart</code>.</p> <ul style="list-style-type: none"> <li>o <code>action="restart"</code></li> </ul> <p>L'application est redémarrée localement (<code>stop_xx ; start_xx</code>)</p> <ul style="list-style-type: none"> <li>o <code>action="stopstart"</code></li> </ul> <p>Le module est arrêté, ainsi que l'application, puis est démarré automatiquement</p>	<p>respectivement dans l'état <code>SECOND</code>, <code>ALONE</code> ou <code>UP</code></p> <p>Message dans le journal :</p> <p><b>"Action start called automatically"</b></p> <p>Note : un <code>stopstart</code> sur  PRIM (Ready) provoque un basculement</p> <p>2. Reproduire le test sur le même serveur s'il tourne toujours l'application (i.e.  (Ready) <code>ALONE</code>, <code>PRIM</code> ou <code>UP</code>) :</p> <p>Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir <code>maxloop</code> et <code>loop_interval</code> décrits dans la <a href="#">section 13.3.3</a>), le module va dans l'état  <code>STOP</code> (<code>NotReady</code>) .</p> <p>Message dans le journal avant l'arrêt :</p> <p><b>"Action stop called by maxloop"</b></p>
--	--

#### 4.4.2 Test <tcp> checker avec action restart ou stopstart




Pour la description du TCP checker, voir la [section 13.12](#).

<p>Dans <code>userconfig.xml</code> :</p> <pre>&lt;check&gt;   &lt;tcp ident="id" when="prim"   action="restart" &gt;     &lt;to addr="addr" port="port"/&gt;   &lt;/tcp&gt; &lt;/check&gt;</pre> <p>Le checker vérifie que l'application répond aux demandes de connexion.</p> <ul style="list-style-type: none"> <li>• <code>addr="addr", port="port"</code></li> </ul> <p>Connexions TCP testées <code>addr:port</code></p> <ul style="list-style-type: none"> <li>• when</li> </ul> <ul style="list-style-type: none"> <li>o <code>when="prim"</code> pour un module miroir</li> </ul> <p>Checker démarré/arrêté, sur le serveur dans l'état  PRIM ou <code>ALONE</code> (Ready), après/avant l'application (<code>start_prim /stop_prim</code>)</p>	<p>1. Arrêter l'application qui écoute sur <code>addr:port</code> sur le serveur dans un état  (Ready) ; c'est-à-dire dans l'état <code>PRIM</code> ou <code>ALONE</code> pour un module miroir et l'état <code>UP</code> pour un module ferme.</p> <ul style="list-style-type: none"> <li>o Messages dans le journal :</li> </ul> <p><b>"Resource tcp.id set to down by tcpcheck"</b>  <b>"Action restart stopstart from failover rule t_id "</b></p> <ul style="list-style-type: none"> <li>o Le module passe dans un état  (Transient)</li> <li>o Dans le cas <code>restart</code>, le module redevient  (Ready), respectivement dans l'état <code>PRIM</code>, <code>ALONE</code> ou <code>UP</code></li> <li>o dans le cas <code>stopstart</code>, le module redevient  (Ready), respectivement dans l'état <code>SECOND</code>, <code>ALONE</code> ou <code>UP</code></li> </ul>
---	--

<ul style="list-style-type: none"> <li>o when="both" pour un module ferme  <p>Checker démarré/arrêté, sur tous les serveurs dans l'état  UP (Ready), après/avant l'application (start_both /stop_both)</p> </li> <li>• action  <p>Si la connexion échoue, le checker met la ressource tcp.id à down. La règle de failover associée, nommée t_id, exécute un restart ou stopstart.</p> </li> <li>o action="restart"  <p>L'application est redémarrée localement (stop_xx ; start_xx)</p> </li> <li>o action="stopstart"  <p>Le module est arrêté, ainsi que l'application, puis est démarré automatiquement</p> </li> </ul>	<p>Message dans le journal :</p> <p>"Action start called automatically"</p> <p>Note : un stopstart sur  PRIM (Ready) provoque un basculement</p> <p>2. Reproduire le test sur le même serveur s'il tourne toujours l'application (i.e.  (Ready) ALONE ou UP).</p> <p>Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir maxloop et loop_interval décrits dans la <a href="#">section 13.3.3</a>), le module va dans l'état  STOP (NotReady) .</p> <p>Message dans le journal avant l'arrêt :</p> <p>"Action stop called by maxloop"</p>
---	--

### 4.4.3 Test <tcp> checker avec action wait

Pour la description du TCP checker, voir la [section 13.12](#).

<p>Dans userconfig.xml :</p> <pre>&lt;check&gt;   &lt;tcp ident="id" when="pre"   action="wait" &gt;     &lt;to addr="addr" port="port"/&gt;   &lt;/tcp&gt; &lt;/check&gt;</pre> <p>Le checker vérifie qu'une application, externe au module, répond aux demandes de connexion.</p> <ul style="list-style-type: none"> <li>• addr="addr", port="port"  <p>Connexions TCP testées addr:port</p> </li> <li>• when="pre"  <p>Checker démarré avant, arrêté après, l'application intégrée dans le module (dans start_xx /stop_xx)</p> </li> <li>• action="wait"  <p>Si la connexion échoue, le checker met la ressource tcp.id à down. La règle de failover associée, nommée t_id, exécute un wait.</p> <p>Cela arrête le module, et son application, puis l'amène dans l'état</p> </li> </ul>	<p>1. Arrêter l'application externe qui écoute sur addr:port quand le serveur est  (Ready) ; c'est-à-dire dans l'état PRIM, ALONE ou SECOND pour un module miroir et l'état UP pour un module ferme.</p> <ul style="list-style-type: none"> <li>o Messages dans le journal :  <p>"Resource tcp.id set to down by tcpcheck"            "Action wait from failover rule t_id"</p> </li> <li>o Le module devient  WAIT (NotReady) sur tous les nœuds  <p>Note : un wait sur  PRIM (Ready) provoque un basculement</p> </li> </ul> <p>2. Redémarrer l'application externe qui écoute sur addr:port</p> <ul style="list-style-type: none"> <li>o Messages dans le journal verbeux  <p>"Resource tcp.id set to up by tcpcheck"            "Action wakeup from failover rule Implicit_wakeup"</p> </li> <li>o le module redevient  (Ready)</li> </ul> <p>3. Répéter le test.</p>
--	---

<p>WAIT en attente de <code>tcp.id</code> repositionné à <code>up</code> par le checker.</p>	<p>Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir <code>maxloop</code> et <code>loop_interval</code> décrits dans la <a href="#">section 13.3.3</a>), le module va dans l'état <b>✗</b> STOP (NotReady) .</p> <p>Message dans le journal avant l'arrêt :</p> <pre>"Action stop called by maxloop"</pre> <p>Note : ce test permet de tester la connectivité d'un serveur à un service externe. Mais si le service externe est en panne ou s'il est inatteignable sur tous les serveurs, tous les serveurs vont en <b>○</b> WAIT (NotReady) et l'application est indisponible.</p>
--	--

#### 4.4.4 Test <interface check="on"> avec action wait

Pour la description du checker d'interface, voir la [section 13.14](#). Pour sa configuration automatique avec `<interface check="on">`, voir la [section 13.6.5](#).

Dans `userconfig.xml` :

```
<vip>
  <interface_list>
    <interface check="on">
      <real_interface>
        <virtual_addr addr="172.17.0.20"
          where="one_side_alias"
          check="on"/>
      </real_interface>
    </interface>
  </interface_list>
</vip>
```

Le checker vérifie que le câble Ethernet est connecté sur l'interface du réseau où est définie l'adresse IP virtuelle.

- Si une erreur est détectée sur l'interface, le checker met la ressource associée `intf.172.17.0.0` à `down`. Le préfixe est `intf` et le suffixe est le réseau correspondant à l'IP virtuelle.
- La règle de failover par défaut, nommée `interface_failure`, exécute un `wait`.

Cela arrête le module, et son application, puis l'amène dans l'état WAIT en attente de `intf.172.17.0.0` repositionné à `up` par le checker.

Note : ne pas utiliser `check="on"` sur des interfaces de bonding ou teaming car ces

1. Retirer le câble Ethernet de la carte du réseau (sur laquelle est configurée l'IP virtuelle) sur le serveur dans un état **✓** (Ready) ; c'est-à-dire dans l'état PRIM ou ALONE pour un module miroir et l'état UP pour un module ferme :
  - o Messages dans le journal :
 

```
"Resource intf.172.17.0.0 set to down by intfcheck"
"Action wait from failover rule interface_failure"
```
  - o Le module devient **○** WAIT (NotReady)
 

Note : un `wait` sur **✓** PRIM (Ready) provoque un basculement
2. Remettre le câble
  - o Messages dans le journal verbeux
 

```
"Resource intf.172.17.0.0 set to up by intfcheck"
"Action wakeup from failover rule Implicit_wakeup"
```
  - o Le module redevient **✓** (Ready), respectivement dans l'état SECOND, ALONE ou UP
 

Note : un `wait` sur **✓** PRIM (Ready) provoque un basculement

interfaces apportent leurs propres mécanismes de reprise d'interface à interface

3. Reproduire le test sur le même serveur  
Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir `maxloop` et `loop_interval` décrits dans la [section 13.3.3](#)), le module va dans l'état **✗** STOP (NotReady) .

Message dans le journal avant l'arrêt :

```
"Action stop called by maxloop"
```

Note : Désactiver l'interface au lieu de débrancher le câble réseau conduit à l'état **✗** (NotReady) STOP si ce réseau est utilisé comme heartbeat. Dans ce cas, le module ne peut démarrer (ni redémarrer) car l'adresse IP locale, pour le heartbeat, n'est pas définie.

#### 4.4.5 Test <ping> checker avec action wait

Pour la description du ping checker, voir la [section 13.13](#).

Dans `userconfig.xml`:

```
<check>
  <ping ident="id" when="pre"
  action="wait">
    <to addr="extip"/>
  </ping>
</check>
```

Le checker vérifie qu'un composant externe (ex. : un routeur) avec l'adresse `extip` répond au ping.

- `when="pre"`

Checker démarré avant, arrêté après, l'application intégrée dans le module (dans `start_xx/stop_xx`)

- `action="wait"`

Si le ping échoue, le checker met la ressource `ping.id` à down. La règle de failover associée, nommée `p_id`, exécute un `wait`.

Cela arrête le module, et son application, puis l'amène dans l'état WAIT en attente de `ping.id` repositionné à `up` par le checker.

1. Rompre la liaison réseau entre le composant externe testé et un serveur dans un état **✓** (Ready) ; c'est-à-dire dans l'état PRIM, ALONE ou SECOND pour un module miroir et l'état UP pour un module ferme.

- o Messages dans le journal :

```
"Resource ping.id set to down by
pingcheck"
"Action wait from failover rule p_id"
```

- o Le module devient **○** WAIT (NotReady) sur tous les nœuds

Note : un `wait` sur **✓** PRIM (Ready) provoque un basculement

2. Rétablir la liaison réseau

- o Messages dans le journal verbeux

```
"Resource ping.id set to up by
pingcheck"
"Action wakeup from failover rule
Implicit_wakeup"
```

- o le module redevient **✓** (Ready)

3. Répéter le test.

Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir `maxloop` et `loop_interval` décrits dans la [section](#)

13.3.3), le module va dans l'état **×** STOP (NotReady) .

Message dans le journal avant l'arrêt :

"Action stop called by maxloop"

Note : ce test permet de tester la connectivité d'un serveur au réseau. Mais si le composant externe est en panne et si le ping échoue sur tous les serveurs, tous les serveurs vont en **○** WAIT (NotReady) et l'application est indisponible.

#### 4.4.6 Test <module> checker avec action wait

Pour la description du module checker, voir la [section 13.17](#).

Dans userconfig.xml du module AM :

```
<check>
  <module name="othermodule">
    <to addr="ip" port="9010"/>
  </module>
</check>
```

Le checker du module AM, vérifie que le module othermodule, accédé depuis son adresse IP virtuelle ip, est **✓** (Ready) .

- Si le module othermodule n'est pas démarré, le checker met la ressource associée module.othermodule\_ip à down. Le préfixe est module et le suffixe est le nom du module externe suivi de son adresse.
- La règle de failover par défaut, nommée module\_failure, exécute un wait.

Cela arrête le module, et son application, puis l'amène dans l'état WAIT en attente de module.othermodule\_ip repositionné à up par le checker.

Note : si le module AM est un module miroir qui utilise la réplication de fichiers et en raison de la règle notuptodate\_server, vous pouvez rencontrer un comportement incorrect avec le module AM bloqué dans un état WAIT si l'action stopstart arrive pendant la transition SECOND vers ALONE

1. Arrêter le module othermodule. Et démarrer le module AM sur tous ses serveurs.

- o Messages dans le journal

"Resource module.othermodule\_ip set to down by modulecheck  
"Action wait from failover rule module\_failure"

- o Le module devient **○** WAIT (NotReady) sur tous les nœuds

Note : un wait sur **✓** PRIM (Ready) provoque un basculement

2. Démarrer le module othermodule.

- o Messages dans le journal verbeux

"Resource module.othermodule\_ip set to up by modulecheck"  
"Action wakeup from failover rule Implicit\_wakeup"

- o Le module redevient **✓** (Ready) sur tous les nœuds

3. Exécuter un restart du module othermodule.

- o Message dans le journal du module AM :

"stopstart called by modulecheck"

- o Le module AM s'arrête puis démarre automatiquement

## 4. Répéter le test.

Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir `maxloop` et `loop_interval` décrits dans la [section 13.3.3](#)), le module va dans l'état **✗** STOP (NotReady) .

Message dans le journal avant l'arrêt :

```
"Action stop called by maxloop"
```

#### 4.4.7 Test <custom> checker avec action wait

Pour la description du custom checker, voir la [section 13.16](#).

Dans `userconfig.xml` :

```
<check>
  <custom ident="id" when="pre"
  exec="customscript" action="wait" />
</custom>
</check>
```

Le custom checker est une boucle infinie qui effectue un test et affecte la ressource associée à `up` ou `down`, en fonction du résultat du test.

- `when="pre"`

Checker démarré avant, arrêté après, l'application intégrée dans le module (dans `start_xx /stop_xx`)

- `exec="customscript"`

Script localisé sous `AM/bin/`, qui affecte la ressource `custom.id` :

- o Sur échec

```
SAFE/safekit set -r custom.id
-v down -i customscript
```

- o Sur succès

```
SAFE/safekit set -r custom.id
-v up -i customscript
```

- `action="wait"`

Quand la ressource `custom.id` passe à `down`, la règle de failover associée, nommée `c_id`, exécute un `wait`.

Cela arrête le module, et son application, puis l'amène dans l'état

1. Provoquer l'échec du test du custom checker quand le serveur est dans un état **✓** (Ready) ; c'est-à-dire dans l'état `PRIM`, `ALONE` ou `SECOND` pour un module miroir et l'état `UP` pour un module ferme.

- o Messages dans le journal verbeux:

```
"Resource custom.id set to down by
customscript"
"Action wait from failover rule c_id"
```

- o Le module devient **○** `WAIT` (NotReady) sur tous les nœuds

Note : un `wait` sur **✓** `PRIM` (Ready) provoque un basculement

2. Réparer l'erreur testée par le custom checker.

- o Messages dans le journal verbeux

```
"Resource custom.id set to up by
customscript "
"Action wakeup from failover rule
Implicit_wakeup"
```

- o Le module redevient **✓** (Ready)

3. Répéter le test.

Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir `maxloop` et `loop_interval` décrits dans la [section 13.3.3](#)), le module va dans l'état **✗** STOP (NotReady) .

Message dans le journal avant l'arrêt :

```
"Action stop called by maxloop"
```

WAIT en attente de `custom.id` repositionné à `up` par le checker.

L'action associée au custom checker peut-être définie via une règle de failover explicite plutôt que l'attribut `action`, qui vaut dans ce cas `noaction`. L'exemple suivant est équivalent au précédent, excepté pour le nom de la règle de failover qui est `customid_failure` :

```
<check>
  <custom ident="id" when="pre" exec="customscript" action="noaction" />
</custom>
</check>
<failover>
  <![CDATA[
    customid_failure: if (custom.id == down) then wait();
  ]]>
</failover>
```

Cette syntaxe est celle supportée avant SafeKit 8.

### 4.4.8 Test <custom> checker avec action restart ou stopstart



Pour la description du custom checker, voir la [section 13.16](#).





#### 4.4.8.1 Action via une règle de failover




Dans `userconfig.xml` :

```
<check>
  <custom ident="id" when="prim"
  exec="customscript" action="restart"
  />
</custom>
</check>
```

Le custom checker est une boucle infinie qui effectue un test et affecte la ressource associée à `up` ou `down`, en fonction du résultat du test.

- when
  - o when="prim" pour un module miroir  
Checker démarré/arrêté, sur le serveur dans l'état  PRIM ou ALONE (Ready), après/avant l'application (`start_prim` /`stop_prim`)
  - o when="both" pour un module ferme  
Checker démarré/arrêté, sur tous les serveurs dans l'état  UP (Ready), après/avant

1. Provoquer l'échec du test du custom checker le custom checker quand le serveur est dans un état  (Ready) ; c'est-à-dire dans l'état PRIM ou ALONE pour un module miroir et l'état UP pour un module ferme :
    - o Messages dans le journal verbeux :  
`"Resource custom.id set to down by customscript"`  
et  
`"Action restart from failover rule c_id "`  
ou  
`"Action stopstart from failover rule c_id "`
    - o Le module passe dans un état  (Transient) .
    - o Dans le cas `restart`, le module redevient  (Ready), respectivement dans l'état PRIM, ALONE ou UP
    - o Dans le cas `stopstart`, le module redevient  (Ready), respectivement dans l'état SECOND, ALONE ou UP.
- Message dans le journal :
- `"Action start called automatically"`


<p>l'application (<code>start_both /stop_both</code>)</p> <ul style="list-style-type: none"> <li>• <code>exec="customscript"</code> Script localisé sous <code>AM/bin/</code>, qui affecte la ressource <code>custom.id</code> : <ul style="list-style-type: none"> <li>o Sur échec <code>SAFE/safekit set -r custom.id -v down -i customscript</code></li> <li>o Sur succès <code>SAFE/safekit set -r custom.id -v up -i customscript</code></li> </ul> </li> <li>• <code>action</code> Quand la ressource <code>custom.id</code> passe à <code>down</code>, la règle de failover, nommée <code>c_id</code>, exécute un <code>restart</code> ou <code>stopstart</code>. <ul style="list-style-type: none"> <li>o <code>action="restart"</code> L'application est redémarrée localement (<code>stop_xx ; start_xx</code>)</li> <li>o <code>action="stopstart"</code> Le module est arrêté, ainsi que l'application et le checker, puis est démarré automatiquement.</li> </ul> </li> </ul>	<p>Note : un <code>stopstart</code> sur  <code>PRIM (Ready)</code> provoque un basculement</p> <p>2. Reproduire le test sur le même serveur s'il tourne toujours l'application (i.e.  <code>(Ready) ALONE</code> ou <code>UP</code>).</p> <p>Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir <code>maxloop</code> et <code>loop_interval</code> décrits dans la <a href="#">section 13.3.3</a>), le module va dans l'état  <code>STOP (NotReady)</code>.</p> <p>Message dans le journal avant l'arrêt : "Action stop called by maxloop"</p>
--	---

L'action associée au custom checker peut-être définie via une règle de failover explicite plutôt que l'attribut `action`, qui vaut dans ce cas `noaction`. L'exemple suivant est équivalent au précédent, excepté pour le nom de la règle de failover qui est `customid_failure` :

```
<check>
  <custom ident="id" when="pre" exec="customscript" action="noaction" />
</custom>
</check>
<failover>
  <![CDATA[
    customid_failure: if (custom.id == down) then restart();
  ]]>
</failover>
```

Cette syntaxe est celle supportée avant SafeKit 8.


#### 4.4.8.2 Action directe dans le script


<p>Dans <code>userconfig.xml</code> :</p> <pre>&lt;check&gt;</pre>	<p>1. Provoquer l'échec du test du custom checker le custom checker quand le serveur est dans un état  <code>(Ready)</code> ;</p>
--	--

```
<custom ident="id" when="prim"
exec="customscript" action="noacion"
/>
</custom>
</check>
```

Le custom checker est une boucle infinie qui effectue un test et effectue un restart ou stopstart, en fonction du résultat du test.

- when
  - o when="prim" pour un module miroir
 

Checker démarré/arrêté, sur le serveur dans l'état  PRIM ou ALONE (Ready), après/avant l'application (start\_prim /stop\_prim)
  - o when="both" pour un module ferme
 

Checker démarré/arrêté, sur tous les serveurs dans l'état  UP (Ready), après/avant l'application (start\_both /stop\_both)
- action="noaction"
 

Pas de règle de failover générée.
- exec="customscript"
 

Script localisé sous AM/bin/, qui affecte la ressource custom.id :

  - o Sur échec
 

```
SAFE/safekit restart -i
customscript
```

L'application est redémarrée localement (stop\_xx ; start\_xx)
  - Ou
    - o Sur échec
 

```
SAFE/safekit stopstart -i
customscript
```




Le module est arrêté, ainsi que l'application et le checker, puis est démarré automatiquement.

c'est-à-dire dans l'état PRIM ou ALONE pour un module miroir et l'état UP pour un module ferme :

- o Messages dans le journal verbeux :
 

"Action restart called by customscript"


ou


"Action stopstart called by customscript"
- o Le module passe dans un état  (Transient).
- o Dans le cas restart, le module redevient  (Ready), respectivement dans l'état PRIM, ALONE ou UP
- o Dans le cas stopstart, le module redevient  (Ready), respectivement dans l'état SECOND, ALONE ou UP.

Message dans le journal :

"Action start called automatically"

Note : un stopstart sur  PRIM (Ready) provoque un basculement

2. Reproduire le test sur le même serveur s'il tourne toujours l'application (i.e.  (Ready) ALONE ou UP)

Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir maxloop et loop\_interval décrits dans la [section 13.3.3](#)), le module va dans l'état  STOP (NotReady).

Message dans le journal avant l'arrêt :

"Action stop called by maxloop"

Note : sur une action directe dans le custom checker, le compteur maxloop est incrémenté si -i identité est passé à la commande restart ou stopstart. Sans identité, SafeKit considère qu'il s'agit d'une opération d'administration. Le compteur est remis à 0 et il n'y a pas de stop au bout de 4 redémarrages.

## 5. Administration d'un module miroir

- ⇒ [Section 5.1](#) « Mode de fonctionnement d'un module miroir »
- ⇒ [Section 5.2](#) « Automate d'état d'un module miroir (STOP, WAIT, ALONE, PRIM, SECOND - NotReady, Transient, Ready) »
- ⇒ [Section 5.3](#) « Premier démarrage d'un module miroir (commande `prim`) »
- ⇒ [Section 5.4](#) « Différents cas de réintégration (utilisation des bitmaps) »
- ⇒ [Section 5.5](#) « Démarrage d'un module miroir avec les données à jour ~~X~~<sub>STOP</sub> (NotReady) - ○<sub>WAIT</sub> (NotReady) »
- ⇒ [Section 5.6](#) « Mode de réplication dégradé (✓<sub>ALONE</sub> (Ready) dégradé) »
- ⇒ [Section 5.7](#) « Reprise automatique ou manuelle »
- ⇒ [Section 5.8](#) « Serveur primaire par défaut (swap automatique après réintégration) »
- ⇒ [Section 5.9](#) « La commande `prim` échoue : pourquoi ? (commande `primforce`) »

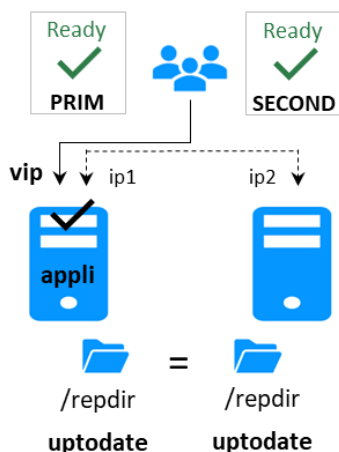
Pour tester un module miroir, voir la [section 4.2](#).

Pour analyser un problème, voir la [section 7](#).

### 5.1 Mode de fonctionnement d'un module miroir

#### 1. Fonctionnement normal

État stable : primaire avec secondaire

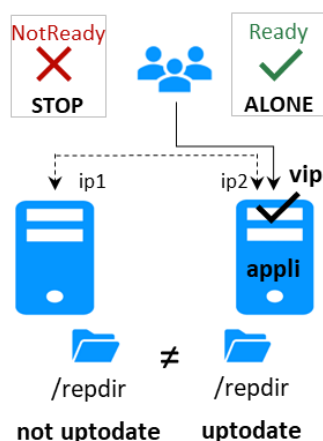


Sur la primaire :

- Réplication de fichiers temps réel
- IP virtuelle définie
- application démarrée

#### 2. Reprise automatique

État stable : primaire sans secondaire

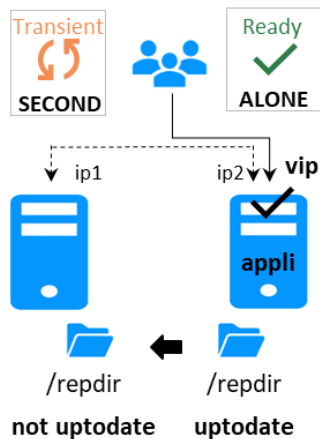


Sur arrêt du primaire, reprise automatique de l'IP virtuelle et de l'application.

La secondaire est prête à effectuer une reprise automatique pour devenir primaire.

### 3. Réintégration après panne

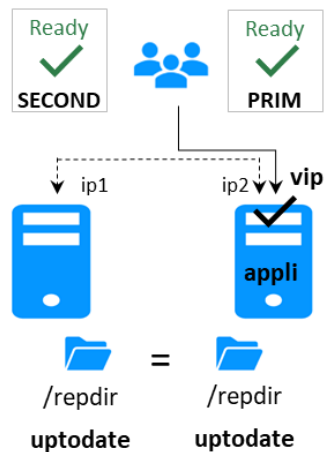
État transitoire : secondaire en cours de réintégration.



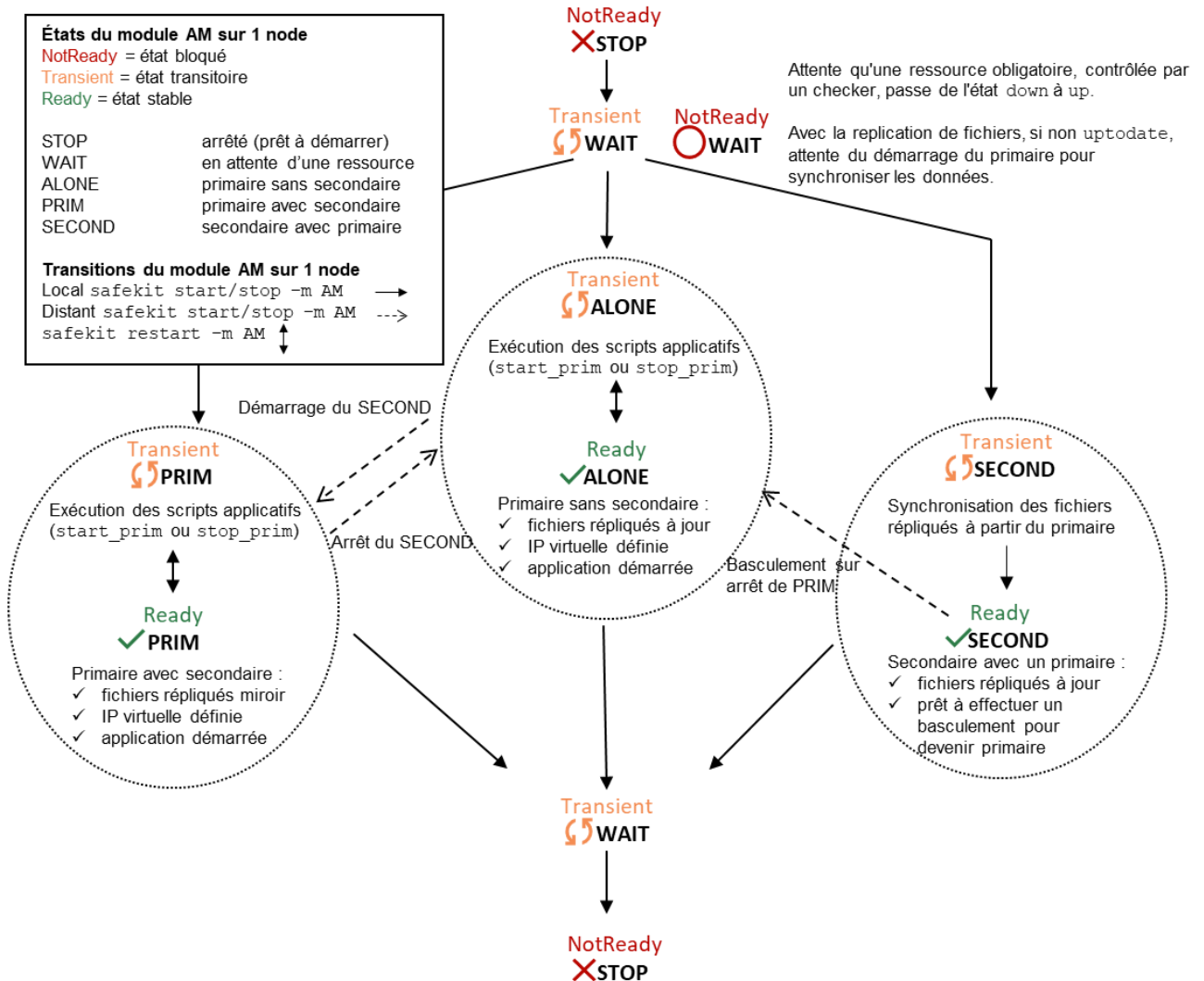
Synchronisation automatique des fichiers sans arrêt de l'application et mise à jour uniquement des fichiers modifiés sur le nœud primaire pendant que l'autre nœud était arrêté.

### 4. Retour à la normale

État stable : primaire avec secondaire.



## 5.2 Automate d'état d'un module miroir (STOP, WAIT, ALONE, PRIM, SECOND - NotReady, Transient, Ready)



## 5.3 Premier démarrage d'un module miroir (commande prim)

Au premier démarrage d'un module miroir, si les deux serveurs sont démarrés avec la commande `start`, ils se bloquent tous les deux dans l'état `WAIT` (NotReady) avec le message dans le journal :

```
"Data may be not uptodate for replicated directories (wait for the start of the remote server)"
"If you are sure that this server has valid data, run safekit prim to force start as primary"
```



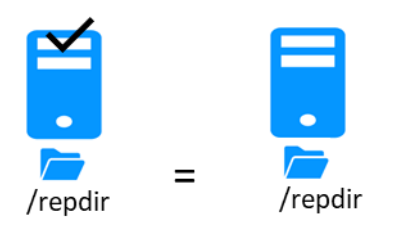
Au premier démarrage, il faut utiliser la commande `prim` pour démarrer en primaire le serveur avec les répertoires à jour, afin de les synchroniser sur l'autre serveur. Ce dernier est démarré avec la commande `second`.

Aux démarrages suivants, utiliser la commande `start` pour démarrer les serveurs.

### 1. État initial

X<sub>STOP</sub>

X<sub>STOP</sub>

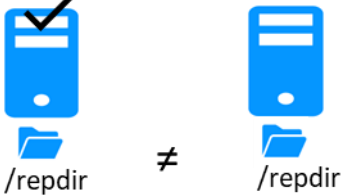
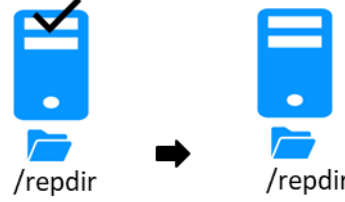
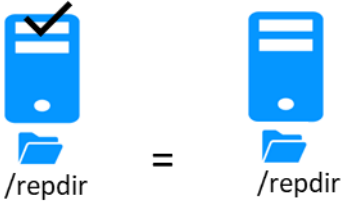
<ul style="list-style-type: none"> <li>le module miroir vient juste d'être configuré avec un nouveau répertoire à répliquer entre node1 et node2</li> <li>node1 a le répertoire à jour</li> <li>node2 a le répertoire vide</li> </ul>	<p>(NotReady)                      (NotReady)</p> 
<p><b>2. Commande prim sur serveur 1</b></p> <ul style="list-style-type: none"> <li>utiliser la commande spéciale <code>safekit prim -m AM</code> (où <code>AM</code> est le nom du module) pour forcer node1 à démarrer en primaire</li> <li>pour les démarrages suivants, utiliser toujours de préférence <code>safekit start -m AM</code> (où <code>AM</code> est le nom du module) : voir <a href="#">section 5.5</a></li> <li>message dans le log: "Action prim called by admin@&lt;IP&gt;/SYSTEM/root"</li> </ul>	<p>✓ ALONE                      ✗ STOP (Ready)                      (NotReady)</p> 
<p><b>3. Commande second sur node2</b></p> <ul style="list-style-type: none"> <li>démarrer l'autre serveur en tant que secondaire</li> <li>le secondaire réintègre le répertoire répliqué à partir du primaire</li> <li>message dans le journal : "Action second called by admin@&lt;IP&gt;/SYSTEM/root"</li> </ul>	<p>✓ PRIM                      ✓ SECOND (Ready)                      (Ready)</p> 

## 5.4 Différents cas de réintégration (utilisation des bitmaps)

Pour optimiser la réintégration de fichiers, il y a plusieurs cas de figure :

1. Le module doit avoir effectué une réintégration (au premier démarrage du module la réintégration est complète) avant d'activer la gestion des bitmaps de modification
2. Si le module a été proprement arrêté sur le serveur, alors au redémarrage du secondaire, seules les zones modifiées à l'intérieur des fichiers sont réintégrées suivant les bitmaps de modification
3. Si le serveur a crashé (power off), ou a été incorrectement arrêté (exception du processus de réplication `nfsbox`), ou si les fichiers ont été modifiés pendant l'arrêt de SafeKit, les bitmaps de modification ne sont pas sûres et elles ne sont donc pas utilisées. Tous les fichiers qui ont été modifiés pendant et avant l'arrêt suivant une période de grâce (typiquement une heure) sont réintégrés

4. Un appel à la commande spéciale `safekit second|prim fullsync` provoque une réintégration complète de tous les répertoires répliqués sur la secondaire quand elle est démarrée.

<p><b>1. Le serveur2 secondaire a été arrêté</b></p> <ul style="list-style-type: none"> <li>les données sont désynchronisées</li> </ul>	<p>✓ ALONE (Ready)      ✗ STOP (NotReady)</p>  <p><b>uupdate</b>      <b>not uupdate</b></p>
<p><b>2. Commande <code>start</code> sur node2</b></p> <ul style="list-style-type: none"> <li>les données sont réintégrées avec l'optimisation des bitmaps (voir ci-dessus)</li> </ul>	<p>✓ ALONE (Ready)      ↻ SECOND (Transient)</p>  <p><b>uupdate</b>      <b>not uupdate</b></p>
<p><b>3. Fin de la réintégration</b></p> <ul style="list-style-type: none"> <li>les données sont les mêmes sur les 2 serveurs</li> <li>seules les modifications à l'intérieur des fichiers sont répliquées en temps réel et de manière synchrone</li> </ul>	<p>✓ PRIM (Ready)      ✓ SECOND (Ready)</p>  <p><b>uupdate</b>      <b>uupdate</b></p>

Le système de réplication maintient en plus sur chaque nœud la dernière date à laquelle les données étaient synchronisées. Cette date de synchronisation, nommée `synctimestamp`, est affectée à l'issue de la réintégration et évolue dans l'état ✓ PRIM (Ready) et ✓ SECOND (Ready). Quand le module est arrêté sur le nœud secondaire puis redémarré, la date de synchronisation est un des critères de réintégration : tous les fichiers modifiés autour de cette date sont potentiellement non à jour sur la secondaire et doivent être réintégrés. Depuis SafeKit 7.4.0.50, la date de synchronisation est aussi exploitée pour implémenter une sécurité supplémentaire. Lorsque l'écart entre la date de synchronisation stockée sur la primaire et celle stockée sur la secondaire est supérieur à 90 secondes, les données répliquées sont considérées non synchronisées dans leur globalité. La réintégration est interrompue avec le message suivant dans le journal du module :






| 2021-08-06 08:40:20.909224 | reintegre | E | La synchronisation automatique ne peut être appliquée en raison d'un delta trop important entre les dates de dernière synchronisation

L'administrateur peut forcer le démarrage en secondaire avec synchronisation complète des données, en exécutant la commande : `safekit second fullsync -m AM`

## 5.5 Démarrage d'un module miroir avec les données à jour ✗

STOP (NotReady) - ○ WAIT (NotReady)

SafeKit choisit quel serveur doit démarrer en tant que primaire. Pour cela, il retient le serveur avec les répertoires répliqués à jour. Pour profiter de cette fonctionnalité, utiliser la commande `start` et NON la commande `prim`.

<p><b>1. État initial</b></p> <ul style="list-style-type: none"> <li>node1 est primaire ALONE</li> <li>les répertoires sont à jour sur ce serveur</li> <li>le module est arrêté sur node2</li> <li>node2 a des répertoires répliqués désynchronisés</li> </ul>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>✓ ALONE (Ready)</p>  <p>/readdir</p> <p>uptodate</p> </div> <div style="text-align: center;"> <p>✗ STOP (NotReady)</p>  <p>/readdir</p> <p>not uptodate</p> </div> </div> <p style="text-align: center;">≠</p>
<p><b>2. Commande stop sur node1</b></p> <ul style="list-style-type: none"> <li>arrêt du serveur avec les répertoires à jour</li> </ul>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>✗ STOP (NotReady)</p>  <p>/readdir</p> <p>uptodate</p> </div> <div style="text-align: center;"> <p>✗ STOP (NotReady)</p>  <p>/readdir</p> <p>not uptodate</p> </div> </div> <p style="text-align: center;">≠</p>
<p><b>3. Commande start sur node2</b></p> <ul style="list-style-type: none"> <li>le module est mis dans l'état WAIT en attendant le démarrage de l'autre serveur. Dans son journal de message :  <div style="background-color: #e0e0e0; padding: 5px; margin: 5px 0;">                     "Potentially not uptodate data for replicated directories (wait for the start of the remote server)"                      "Action wait from failover rule notuptodate_server"                      "If you are sure that this server has valid data, run safekit prim to force start as primary"                 </div> </li> <li>dans ce cas, vous devez démarrer node1 pour resynchroniser node2</li> <li>si vous voulez réellement sacrifier les données à jour et démarrer node2 avec les données non à jour en tant que primaire : commande <code>stop</code> puis commande <code>prim</code> sur node2</li> </ul>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>✗ STOP (NotReady)</p>  <p>/readdir</p> <p>uptodate</p> </div> <div style="text-align: center;"> <p>○ WAIT (NotReady)</p>  <p>/readdir</p> <p>not uptodate</p> </div> </div> <p style="text-align: center;">≠</p> <p style="text-align: right; font-size: small;">rfs.uptodate="down"</p>

Voir aussi la [section 5.9](#)

## 5.6 Mode de réplication dégradé (✓ALONE (Ready) dégradé)

Si le processus de réplication `nfsbox` connaît une défaillance sur la machine primaire (liée par exemple à une mauvaise configuration de la réplication de fichiers), l'application n'est pas basculée inutilement sur le serveur secondaire





Le serveur primaire va dans l'état `ALONE` et dans un mode de réplication dégradé. Cet état dégradé est affiché dans la console. Le message dans le journal est


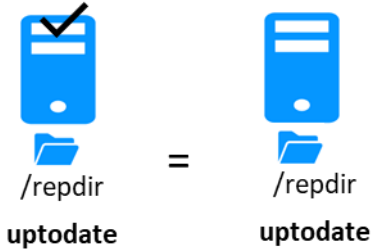
```
"Resource rfs.degraded set to up by nfsadmin"
```

Et `safekit state -v -m AM` (où `AM` est le nom du module) présente la ressource `rfs.degraded up`

Le serveur primaire continue en `ALONE` avec un processus `nfsbox` qui ne réplique plus

Il faut arrêter et redémarrer le serveur `ALONE` pour revenir dans la situation `PRIM - SECOND` avec réplication


<p><b>1. État initial</b></p> <ul style="list-style-type: none"> <li>le miroir est dans l'état stable <code>node1</code> <ul style="list-style-type: none"> <li>✓ <code>PRIM (Ready)</code> - serveur 2 ✓</li> <li><code>SECOND (Ready)</code></li> </ul> </li> </ul>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>✓ <code>PRIM</code> (Ready)</p>  <p>/readdir uptodate</p> </div> <div style="font-size: 2em;">=</div> <div style="text-align: center;"> <p>✓ <code>SECOND</code> (Ready)</p>  <p>/readdir uptodate</p> </div> </div>
<p><b>2. Défaillance du processus de réplication <code>nfsbox</code> sur <code>node1</code></b></p> <ul style="list-style-type: none"> <li><code>node1</code> devient ✓ <code>ALONE (Ready)</code> dégradé avec le message           <pre>"set up of rfs.degraded called by nfsadmin"</pre> <p><code>safekit state -v</code> présente la ressource <code>rfs.degraded="up"</code></p> </li> <li><code>node1</code> continue à exécuter l'application sans réplication</li> <li><code>node2</code> se met dans l'état ○ <code>WAIT (NotReady)</code> en attente du processus de réplication avec le message dans son journal           <pre>"Action wait from failover rule degraded_server"</pre> <p>et avec <code>rfs.uptodate="down"</code></p> </li> </ul>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>✓ <code>ALONE</code> (Ready)</p>  <p>/readdir uptodate</p> </div> <div style="font-size: 2em;">≠</div> <div style="text-align: center;"> <p>○ <code>WAIT</code> (NotReady)</p>  <p>/readdir not uptodate</p> </div> </div> <p><code>rfs.degraded="up" rfs.uptodate="down"</code></p>
<p><b>3. Retour à la réplication</b></p>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>✓ <code>PRIM</code> (Ready)</p> </div> <div style="font-size: 2em;">=</div> <div style="text-align: center;"> <p>✓ <code>SECOND</code> (Ready)</p> </div> </div>





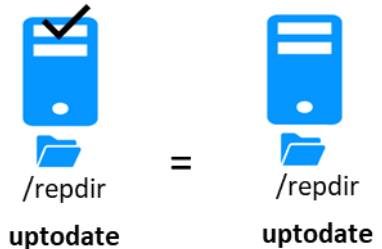


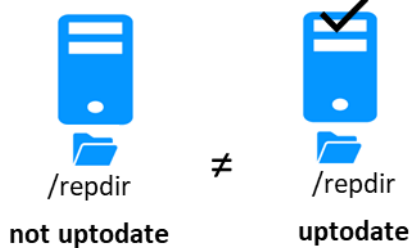


<ul style="list-style-type: none"> <li>l'administrateur réalise <code>stop ; start</code> sur <code>node1 ALONE</code></li> <li>le processus de réplication <code>nfsbox</code> est relancé sur <code>node1</code></li> <li><code>node2</code> réintègre les répertoires répliqués avant de devenir  <code>SECOND (Ready)</code></li> <li><code>node1</code> devient  <code>PRIM (Ready)</code></li> </ul>	
--	--




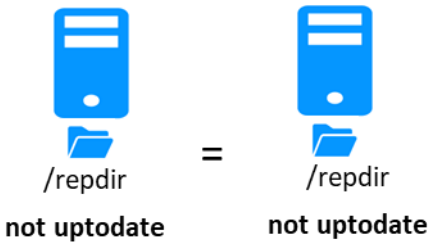
## 5.7 Reprise automatique ou manuelle

La reprise automatique ou manuelle sur le serveur secondaire est définie dans `userconfig.xml` par `<service mode="mirror" failover="on"|"off">`. Par défaut, si la valeur n'est pas définie, `failover="on"`

Le mode `failover="off"` est utile lorsque l'on veut contrôler le basculement par un administrateur. Ce mode assure qu'une application tourne toujours sur le même serveur primaire quel que soit les opérations sur ce serveur (reboot, arrêt temporaire du module pour maintenance...). Seule une commande d'un administrateur (commande `prim`) peut mettre l'autre serveur en primaire.

 Le mode de reprise peut être change dynamiquement avec la commande `safekit failover on|off -m AM` (remplacer `AM` par le nom du module).

<p><b>1. État initial</b></p> <ul style="list-style-type: none"> <li>le miroir est dans l'état stable <code>node1</code>   <code>PRIM (Ready)</code> - serveur 2  <code>SECOND (Ready)</code></li> </ul>	<p> <code>PRIM (Ready)</code>       <code>SECOND (Ready)</code></p> 
<p><b>2. Fonctionnement avec <code>failover="on"</code></b></p> <ul style="list-style-type: none"> <li>si <code>node1</code> anciennement <code>PRIM</code> rencontre une défaillance et s'arrête, <code>node2</code> devient automatiquement primaire <code>ALONE</code> (mode par défaut)</li> </ul>	<p> <code>STOP (NotReady)</code>       <code>ALONE (Ready)</code></p> 
<p><b>3. Fonctionnement avec <code>failover="off"</code></b></p>	<p> <code>STOP (NotReady)</code>       <code>WAIT (NotReady)</code></p>

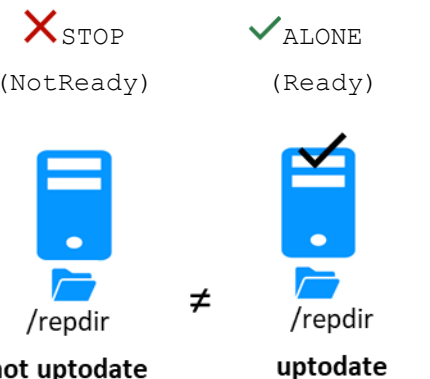

<ul style="list-style-type: none"> <li>Si node1 anciennement <code>PRIM</code> connaît une défaillance et s'arrête, node2 se met en  <code>WAIT (NotReady)</code> avec dans son journal le message  <pre>"Failover-off configuré" "Action stopstart appelé par failover-off" "Transition STOPSTART from failover-off" "Local state WAIT NotReady "</pre> </li> <li>L'administrateur dans cette situation peut redémarrer node1 s'il n'est pas en panne : le miroir redémarre dans son ancien état serveur 1  <code>PRIM (Ready)</code> - serveur 2  <code>SECOND (Ready)</code></li> <li>L'administrateur peut décider de forcer node2 à devenir primaire avec les commandes : <code>stop ; prim</code> sur node2</li> </ul>	
---	--

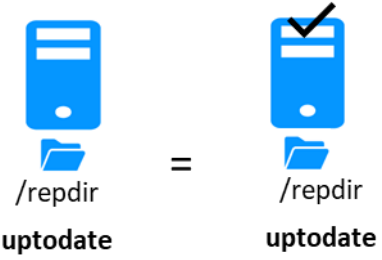
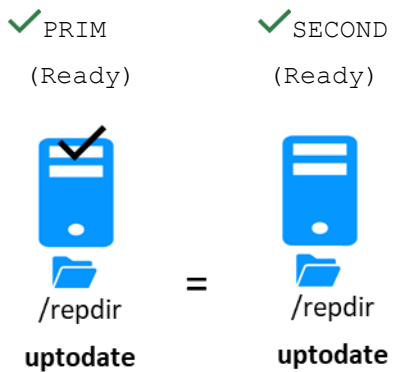
Voir aussi la [section 5.9](#)

## 5.8 Serveur primaire par défaut (swap automatique après réintégration)

A la réintégration après panne, un serveur redevient par défaut secondaire. L'administrateur peut choisir de ramener l'application sur le serveur réintégré à un moment opportun avec la commande `swap`. C'est le comportement par défaut lorsque dans `userconfig.xml` `<service>` est défini sans la variable `defaultprim`

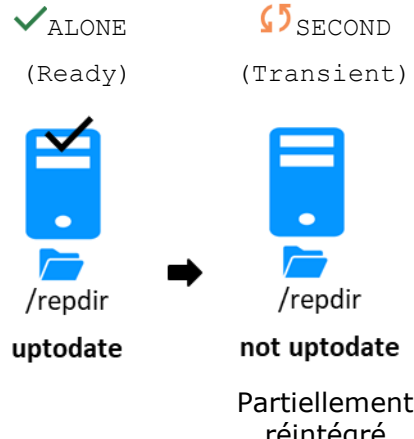

Si l'on veut que l'application revienne automatiquement sur le serveur juste après sa réintégration, il faut configurer dans `userconfig.xml` `<service mode="mirror" defaultprim="hostname serveur 1">`

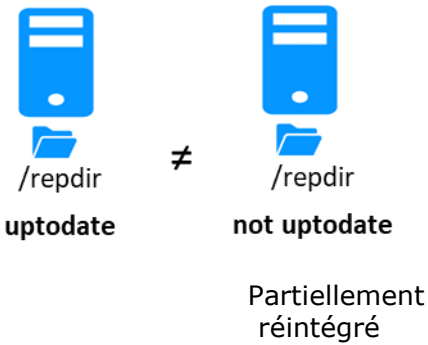

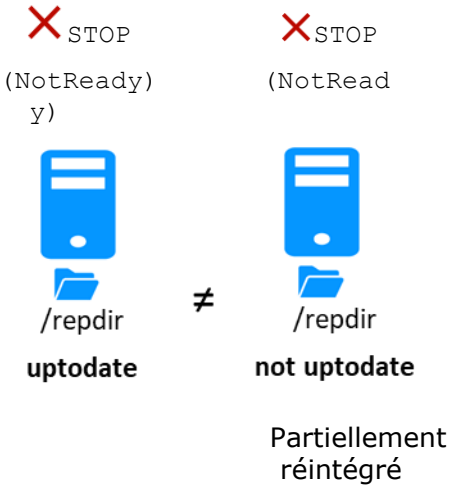
<p><b>1. État initial</b></p> <ul style="list-style-type: none"> <li>node1 (anciennement <code>PRIM</code>) connaît une défaillance et s'arrête</li> <li>node2 secondaire devient automatiquement primaire <code>ALONE</code></li> </ul>	
<p><b>2. Retour sans <code>defaultprim</code></b></p> <ul style="list-style-type: none"> <li>node1 est relancé par la commande <code>start</code> : il réintègre les répertoires répliqués puis devient secondaire</li> <li>un administrateur peut replacer le primaire sur node1 avec la commande <code>stopstart</code> du serveur 2 à une heure propice</li> </ul>	

<ul style="list-style-type: none"> <li>le stopstart provoque l'arrêt de l'application sur node2 et son redémarrage sur node1</li> </ul>	
<p><b>3. Retour avec defaultprim="hostname serveur 1"</b></p> <ul style="list-style-type: none"> <li>node1 <b>X</b>STOP (NotReady) du cas 1 (état initial) est relancé par start</li> <li>il réintègre les répertoires répliqués</li> <li>juste après la réintégration, un swap automatique est réalisé par node1 avec les messages dans son journal :  <pre>"Transition SWAP from defaultprim" "Begin of Swap"</pre> </li> <li>l'application est alors automatiquement arrêtée sur node2 et relancée sur node1</li> <li>à la fin de l'opération, node1 est PRIM</li> </ul>	

### 5.9 La commande prim échoue : pourquoi ? (commande primforce)

Il se peut qu'une commande prim échoue : après une tentative de démarrage, le serveur repasse en **X**STOP (NotReady).

<p><b>1. État initial</b></p> <ul style="list-style-type: none"> <li>node1 ALONE a les répertoires répliqués à jour</li> <li>node2 est en train de réintégrer les fichiers</li> </ul>	
<p><b>2. stop sur node2 puis sur node1</b></p> <ul style="list-style-type: none"> <li>arrêt du serveur 2 pendant sa réintégration : l'arrêt du serveur 2 peut se</li> </ul>	

<p>faire alors qu'un fichier est à moitié recopié (fichier corrompu)</p> <ul style="list-style-type: none"> <li>node1 est lui aussi arrêté</li> </ul>	
<p><b>3. Commande <code>prim</code> sur node2</b></p> <ul style="list-style-type: none"> <li>la commande <code>prim</code> échoue : l'échec produit les messages suivants dans le log  <pre>"Data may be inconsistent for replicated directories (stopped during reintegration)" "If you are sure that this server has valid data, run safekit primforce to force start as primary"</pre> </li> <li>dans ce cas, il faut démarrer node1 par la commande <code>start</code>. Et relancer node2 avec la commande <code>start</code> pour terminer la réintégration des fichiers. Tant que node2 n'a pas atteint l'état  <code>SECOND (Ready)</code>, ses données ne sont pas intègres</li> <li>si vous voulez absolument démarrer sur node2 partiellement réintégré et avec des données potentiellement corrompues, utiliser la commande en ligne <code>safekit primforce -m AM</code> (où <code>AM</code> est le nom du module) sur node2. Message dans le journal :  <pre>"Action primforce called by SYSTEM/root"</pre> </li> </ul>	 <p>la commande <code>prim</code> échoue car les données peuvent être corrompues</p>

Note : La commande `primforce` force une réintégration complète des répertoires répliqués sur la secondaire lorsqu'elle est démarrée.



## 6. Administration d'un module ferme

- ⇒ [Section 6.1](#) « Mode de fonctionnement d'un module ferme »
- ⇒ [Section 6.2](#) « Automate d'état d'un module ferme (STOP, WAIT, UP - NotReady, Transient, Ready) »
- ⇒ [Section 6.3](#) « Démarrage d'un module ferme »

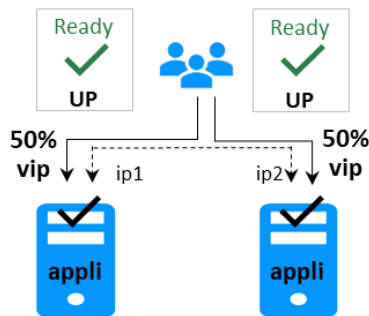
Pour tester un module ferme, voir la [section 4.3](#).

Pour analyser un problème, voir la [section 7](#).

### 6.1 Mode de fonctionnement d'un module ferme

#### 1. Fonctionnement normal

État stable : 2 nœuds actifs.



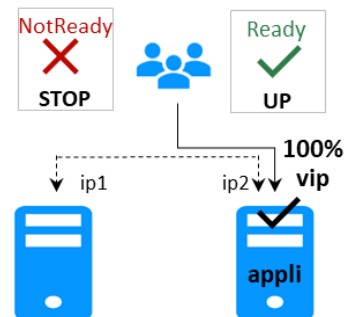
Sur tous les nœuds :

- IP virtuelle définie
- Application démarrée
- La charge du réseau est répartie entre tous les nœuds

Chaque nœud est prêt à effectuer une reprise automatique et assumer 100% de la charge.

#### 2. Reprise automatique

État stable : 1 nœud actif.

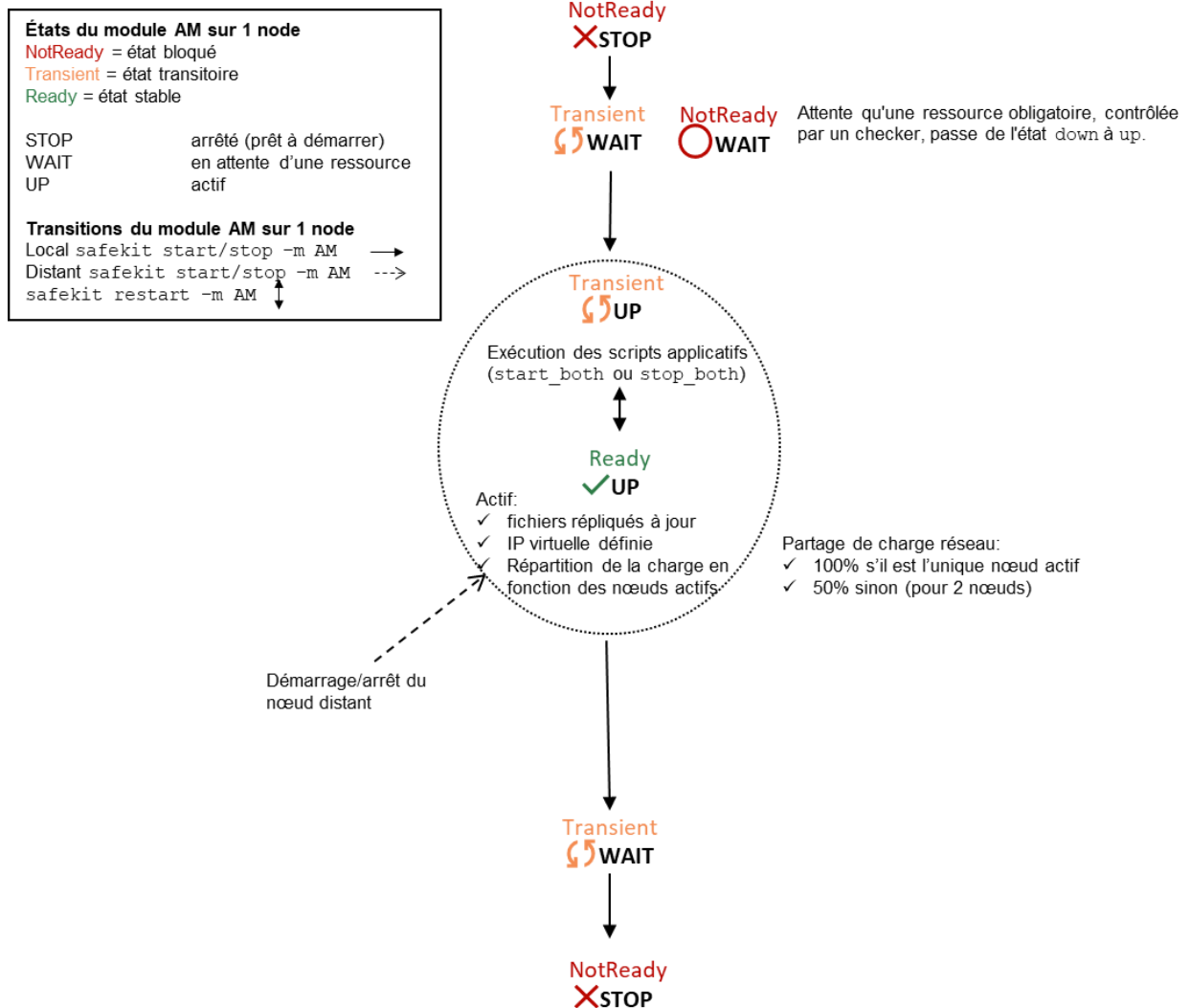


Sur arrêt du nœud distant, reprise automatique de toute la charge réseau.

#### 3. Retour à la normale

État stable : 2 nœuds actifs.

## 6.2 Automate d'état d'un module ferme (STOP, WAIT, UP - NotReady, Transient, Ready)





Note : C'est aussi l'automate d'un module de mode light. Ce mode se configure avec `<service mode="light">` dans le fichier `userconfig.xml` du module sous `SAFE/modules/AM/conf` (où `AM` est le nom du module). Le mode light correspond à un module s'exécutant sur un nœud sans synchronisation avec d'autres nœuds (comme peuvent le faire des modules miroir ou ferme). Un module light intègre les procédures de démarrage et d'arrêt d'une application ainsi que les checkers SafeKit qui permettent de détecter des erreurs.

## 6.3 Démarrage d'un module ferme

Il n'y a pas de procédure spéciale pour démarrer un module ferme : utiliser seulement la commande `start` sur tous les serveurs exécutant le module. Ci-dessous un exemple avec une ferme de 2 serveurs.

<b>1. État initial</b>	<span style="color: red;">X</span> STOP (NotReady)	<span style="color: red;">X</span> STOP (NotReady)
------------------------	---	---

<ul style="list-style-type: none"> <li>le module ferme a été configuré sur 2 serveurs</li> </ul>	 <p>0%                      0%</p>
<p><b>2. Commande start sur node1 et node2</b></p> <ul style="list-style-type: none"> <li>message dans le journal des 2 serveurs :  <pre>"farm membership: node1 node2 (group FarmProto_0)" "farm load: 128/256 (group FarmProto_0)" "Local state UP Ready"</pre> </li> <li>ressource de chaque instance du module sur les 2 serveurs : FarmProto_0 50%</li> </ul>	<p>✓ UP                      ✓ UP (Ready)                      (Ready)</p>  <p>50%                      50%</p>



## 7. Résolution de problèmes

- ⇒ [Section 7.1](#) « Problème de connexion avec la console web »
- ⇒ [Section 7.2](#) « Problème de connexion HTTPS avec la console web »
- ⇒ [Section 7.3](#) « Vérification globale de l'environnement (script `healthcheck`) »
- ⇒ [Section 7.4](#) « Comment lire les journaux et les ressources du module applicatif »
- ⇒ [Section 7.5](#) « Comment lire le journal de commandes du serveur ? »
- ⇒ [Section 7.6](#) « Module stable ✓ (Ready) et ✓ (Ready) »
- ⇒ [Section 7.7](#) « Module dégradé ✓ (Ready) et ✗/○ (NotReady) »
- ⇒ [Section 7.8](#) « Module hors service ✗/○ (NotReady) et ✗/○ (NotReady) »
- ⇒ [Section 7.9](#) « Module ✗STOP (NotReady) : redémarrer le module »
- ⇒ [Section 7.10](#) « Module ○WAIT (NotReady) : réparer la `ressource="down"` »
- ⇒ [Section 7.11](#) « Module oscillant de ✓ (Ready) à ↻ (Transient) »
- ⇒ [Section 7.12](#) « Message sur stop après `maxloop` »
- ⇒ [Section 7.12](#) « Message sur stop après `maxloop` »
- ⇒ [Section 7.13](#) « Module ✓ (Ready) mais application non opérationnelle »
- ⇒ [Section 7.14](#) « Module mirror ✓ALONE (Ready) / ○WAIT ou ✗STOP (NotReady) »
- ⇒ [Section 7.15](#) « Module ferme ✓UP (Ready) mais problème de load balancing »
- ⇒ [Section 7.16](#) « Problème avec l'adresse IP virtuelle après le basculement »
- ⇒ [Section 7.17](#) « Problème après boot »
- ⇒ [Section 7.18](#) « Analyse à partir des snapshots du module »
- ⇒ [Section 7.19](#) « Problème avec la taille des bases de données de SafeKit »
- ⇒ [Section 7.20](#) « Problème pour récupérer le certificat de l'autorité de certification »
- ⇒ [Section 7.21](#) « Problème d'envoi de courriel par l'agent de notification SafeKit »
- ⇒ [Section 7.22](#) « Problème avec les antivirus »
- ⇒ [Section 7.23](#) « Problèmes liés aux modules noyau SafeKit »
- ⇒ [Section 7.24](#) « Dépannage de résolution VIP ↔ MAC »
- ⇒ [Section 7.25](#) « Problème persistant »

### 7.1 Problème de connexion avec la console web

Si vous rencontrez des problèmes de connexion avec la console web, tels que pas de réponse du nœud ou erreur de connexion, appliquez les contrôles et procédures ci-dessous :

- ⇒ [Section 7.1.1](#) « Contrôler le navigateur »
- ⇒ [Section 7.1.2](#) « Supprimer l'état du navigateur »
- ⇒ [Section 7.1.3](#) « Contrôler les serveurs »

Ensuite, il peut être nécessaire de recharger la console dans le navigateur.

### 7.1.1 Contrôler le navigateur

Vérifiez pour le navigateur web :

1. que le navigateur et sa version sont bien supportés (dans certains environnements, Chrome fonctionne mieux qu'Internet Explorer)
2. modifiez le paramétrage du proxy pour définir une connexion directe ou indirecte au serveur
3. pour Internet Explorer, modifiez les paramètres de sécurité (ajoutez l'url dans les zones de sécurité)
4. sur évolution de version de SafeKit, nettoyez le cache du navigateur comme décrit plus loin
5. que la console web et le serveur ont la même version (la compatibilité peut ne pas être préservée)

### 7.1.2 Supprimer l'état du navigateur

Pour supprimer l'état du navigateur :

1. Videz son cache

Ouvrir le navigateur sur n'importe quelle page web, et presser en même temps les touches Ctrl, Shift et Suppr. Cela ouvre une fenêtre de dialogue : cocher tous les items puis cliquez le bouton Nettoyer maintenant ou Supprimer

2. Videz le cache SSL si la console se connecte en HTTPS

Dans les paramètres avancés du navigateur, rechercher le cache SSL et le vider

Fermez le navigateur, arrêtez tous les processus du navigateur qui continueraient à tourner en tâche de fond et relancez-le.

### 7.1.3 Contrôler les serveurs

Vérifiez sur chaque nœud du cluster SafeKit :

1. le pare-feu

Si cela n'a pas encore été fait, exécutez la commande `SAFE/private/bin/firewallcfg add` qui configure le pare-feu du système d'exploitation. Pour les autres pare-feux, ajoutez des exceptions pour autoriser les connexions entre le navigateur web et le serveur. Pour les détails de configuration du pare-feu, voir la [section 10.3](#).

2. la configuration du service web

L'accès à la console web nécessite une authentification. Si cela n'a pas encore été fait, exécutez la commande `SAFE/private/bin/webservercfg -passwd pwd` pour initialiser (ou réinitialiser) cette configuration avec le mot de passe de l'utilisateur `admin`. Pour plus de détails, voir la [section 11.2.1](#).

3. la disponibilité du réseau et du serveur
4. les services `safeadmin` et `safewebsserver`

Ils doivent être démarrés

5. la configuration du cluster

Exécutez la commande `safekit cluster confinfo` (voir [section 9.2](#)). Elle doit retourner sur tous les nœuds, la même liste de nœuds et la même signature de configuration. Si ce n'est pas le cas, réappliquez la configuration du cluster sur tous les nœuds (voir [section 12.2](#))

## 7.2 Problème de connexion HTTPS avec la console web

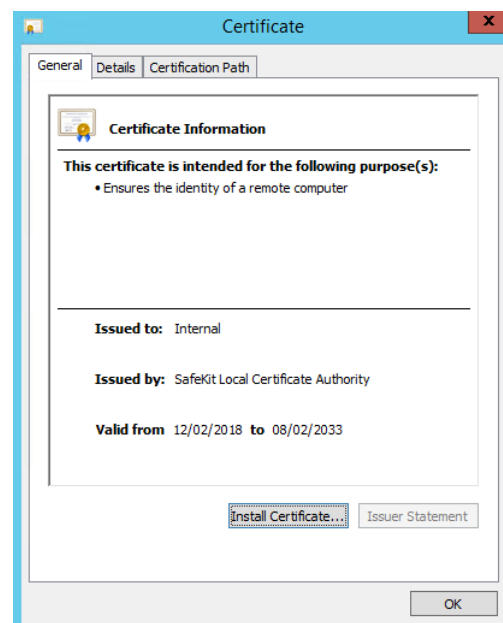
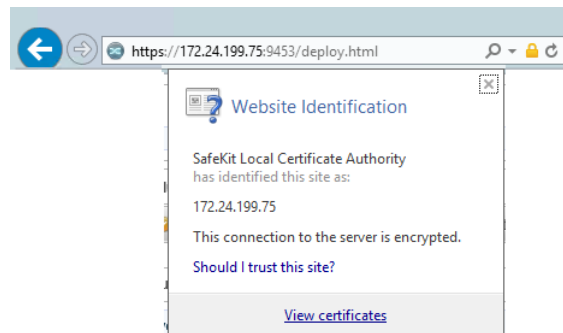
Si vous rencontrez des problèmes de connexion avec la console web en HTTPS, appliquez les contrôles et procédures ci-dessous :

- ⇒ [Section 7.1](#) « Problème de connexion avec la console web »
- ⇒ [Section 7.2.1](#) « Contrôler les certificats serveurs »
- ⇒ [Section 7.2.2](#) « Contrôler les certificats installés dans SafeKit »
- ⇒ [Section 7.2.3](#) « Revenir à la configuration HTTP »

### 7.2.1 Contrôler les certificats serveurs

La console web se connecte à un nœud du cluster identifié par un certificat. Pour obtenir le contenu du certificat associé au nœud, exécutez les opérations suivantes si vous utilisez Edge ou Chrome :

1. Cliquez sur le verrou affiché à côté de l'URL pour ouvrir la fenêtre de sécurité
2. Cliquez sur le lien [View certificates](#). Cela ouvre une fenêtre qui affiche le contenu du certificat
3. Vérifiez l'identité de l'émetteur qui doit être votre autorité de certification
4. Vérifiez la date de validité et la date de station de travail. Remettez la station à la bonne date si nécessaire
5. Vérifiez la date de validité. Si le certificat a expiré, vous devez le renouveler

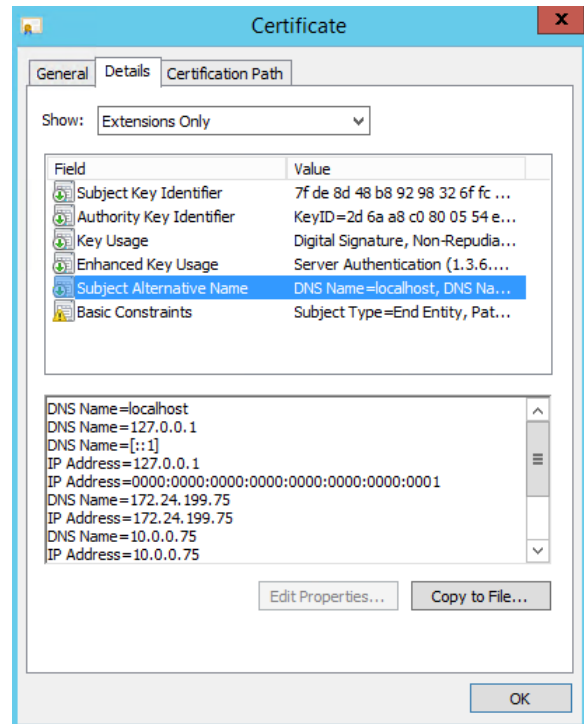


6. Cliquez sur l'onglet **Détails**
7. Sélectionnez le champ **Autre nom de l'objet**. Son contenu est affiché dans le panneau inférieur. Le nom défini dans l'URL pour la connexion à la console web SafeKit doit être inclus dans cette liste. Changer l'URL si nécessaire
8. La valeur de l'attribut `adress` pour le serveur, telle que définie dans la configuration du cluster SafeKit, doit être incluse dans cette liste. Si ce n'est pas le cas, modifiez la configuration du cluster comme cela est décrit en [section 12.2](#).

Si vous utilisez le nom DNS, vous devez mettre le nom en minuscules.



Avec SafeKit <= 7.5.2.9, le nom du serveur doit être obligatoirement inclus.



### 7.2.2 Contrôler les certificats installés dans SafeKit

Vous pouvez utiliser la commande `checkcert` pour contrôler les certificats.

Sur chaque nœud du cluster SafeKit :

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
2. Aller dans le répertoire `SAFE/web/bin`
3. Exécuter `checkcert -t all`
4. La commande contrôle tous les certificats installés et échoue si une erreur est détectée
5. Exécuter la commande suivante pour vérifier que le certificat serveur contient bien un nom DNS ou une adresse IP donné :

```
checkcert -h "DNS name value"  
checkcert -i "Numeric IP address value"
```



Le certificat de serveur doit contenir tous les noms DNS et/ou adresses IP utilisés pour la connexion HTTPS. Ceux-ci doivent également être inclus dans le fichier de configuration du cluster SafeKit.

Si la commande échoue, cela peut être dû à un format incorrect des fichiers.

Le contenu d'un fichier `.crt` ressemble à ceci :

```
-----BEGIN CERTIFICATE (EXAMPLE)-----  
MIID+DCCAuCgAwIBAgIFAJNuUj4wDQYJKoZIhvcNAQELBQAwUjEQMA4GA1UEChMH  
RXhhbXBsZTEQMA4GA1UECzMHU2FmZUtpdDESMDCoGA1UEAxMjU2FmZUtpdCBMb2Nh  
bCBDZXRJ0aWZpY2F0ZSBBdXR0b3JpdHkwHhcNMjQwNTI1MDYyZmZlIiwWcNNDQwNTI0  
...
```

```
H/kG9pfzpnCEtZeyRCxGlowQpEmKtqOS5lXzg+q2tI7uiOaf5SVxHbqj/8c5RNzi
/iYlZg3itzIxLTPBen3BD6pSVmRU33yU2cho6HMsXXwFvo/LMOWNhVrj9I33d7u6
0fooCyU3aFbFCwGx
-----END CERTIFICATE (EXAMPLE) -----
```

Le contenu d'un fichier .key ressemble à ceci :

```
-----BEGIN PRIVATE KEY (EXAMPLE) -----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAQwggSjAgEAAoIBAQCbSAP0f28TR3lj
jMRNabVP6725NQoH6Wt3O238aH8uXKKiI2byzWGxVjnrvT8AK+3lraQ4yLoAGtO3
LTsxsbuOQi90kwfelKNlQsIh3WJ7V6bGltLoQhT+bdDlJAPmLH1nFHKe19Tkvqr/
..
SU15Ap7lplSqrYlvNhhkiOB50Hs34r+iNtPB6GaKtnTHicBjI1i95zrU/J5JKHxBV
uRY4ghOgtJyq9LuZXb2aTOht7K7QTjLRqHS5rdy+alsByhKpD2wR6oqX44mw1wls
eOCnWlvhpFarc9As9BIVGsw=
-----END PRIVATE KEY (EXAMPLE) -----
```

### 7.2.3 Revenir à la configuration HTTP

Si le problème ne peut être résolu, vous pouvez revenir à la configuration HTTP. Sur tous les serveurs :

1. supprimer le fichier `SAFE/web/conf/ssl/httpd.webconsolessl.conf`
2. exécuter `safekit webserver restart`  
(SAFE=C:\safekit en Windows si System Drive=C: ; et SAFE=/opt/safekit en Linux):
3. vider le cache du navigateur comme décrit en [section 7.1.2](#).

### 7.3 Vérification globale de l'environnement (script healthcheck)

Le script `healthcheck`, disponible depuis SafeKit 8.2.6, est un outil de diagnostic qui réalise une vérification globale de l'environnement SafeKit sur un nœud. Il contrôle des composants clés tels que les chemins d'installation, les services SafeKit, l'utilisation du système de fichiers, ainsi que la configuration du cluster et des modules.

Ce script est destiné au diagnostic rapide et au support. Il est automatiquement exécuté lors du dump d'un module et son résultat est inclus dans le snapshot du module.



Exécuter le script `healthcheck` avec :

<b>Windows</b>	<code>safekit -r healthcheck.ps1</code>
<b>Linux</b>	<code>safekit -r healthcheck.sh</code>

Le résultat est généré dans un fichier de log unique (`healthcheck.txt`) dans le répertoire `SAFEVAR`, organisé en sections [TEST], [OK], [WARN] et [ERROR] afin de faciliter l'analyse.

### 7.4 Comment lire les journaux et les ressources du module applicatif ?

Le <b>journal du module</b> et le <b>journal des scripts</b> sur un nœud peuvent être consultés	<ul style="list-style-type: none"> <li>• Vous trouverez une liste des messages du journal en index</li> </ul>
---	---

<p>avec (remplacer ci-dessous <code>node1</code> par le nom du nœud et <code>AM</code> par le nom du module) :</p> <ul style="list-style-type: none"> <li>la console web avec l'URI <a href="/console/fr/monitoring/modules/AM/nodes/node1/logs">/console/fr/monitoring/modules/AM/nodes/node1/logs</a></li> <li>la commande <code>safekit logview -m AM</code> exécutée sur <code>node1</code>, pour le journal du module</li> <li>sur <code>node1</code>, dans les fichiers <code>SAFEVAR/modules/AM/userlog_&lt;year&gt;_&lt;month&gt;_&lt;day&gt;T&lt;time&gt;_&lt;script name&gt;.uolog</code>, pour le journal des scripts</li> </ul> <p>Avec le journal du module, vous pouvez comprendre pourquoi un module n'est plus dans état stable   (Ready).</p> <p>Avec le journal des scripts, vous aurez l'output des scripts utilisateur (<code>start_xxx</code> et <code>stop_xxx</code>).</p> <p>Noter qu'un module peut quitter son état stable   (Ready) à cause d'une commande administrateur : <code>safekit start   stop   restart   swap   stopstart   forcestop</code></p>	<ul style="list-style-type: none"> <li>Les messages dans le journal après une commande administrateur sont :             <pre>"Action start called by admin@&lt;IP&gt;/SYSTEM/root" "Action stop called by admin@&lt;IP&gt;/SYSTEM/root" "Action restart called by admin@&lt;IP&gt;/SYSTEM/root" "Action swap called by admin@&lt;IP&gt;/SYSTEM/root" "Action stopstart called by admin@&lt;IP&gt;/SYSTEM/root" "Action forcestop called by admin@&lt;IP&gt;/SYSTEM/root"</pre> <p>admin@&lt;ip&gt;: via la console  SYSTEM: ligne de commande Windows  root: ligne de commande Linux</p> </li> <li>Si "Action stop called by maxloop" apparaît dans le journal du module, voir la <a href="#">section 7.12</a></li> </ul>
<p>L'état des <b>ressources</b> du module sur un nœud peut être analysé avec (remplacer ci-dessous <code>node1</code> par le nom du nœud et <code>AM</code> par le nom du module) :</p> <ul style="list-style-type: none"> <li>la console web avec l'URI <a href="/console/fr/monitoring/modules/AM/nodes/node1/resources">/console/fr/monitoring/modules/AM/nodes/node1/resources</a></li> <li>la commande <code>safekit state -m AM -v</code> exécutée sur <code>node1</code></li> </ul>	<ul style="list-style-type: none"> <li>status du module             <pre>state.local, state.remote usersetting.errd, usersetting.checker, usersetting.encryption</pre> </li> <li>Checkers             <pre>proc.xxx, intf.xxx, custom.xxx</pre> </li> <li>Réplication de fichiers             <pre>rfs.uptodate, rfs.degraded, rfs.reintegre_failed</pre> </li> </ul>




## 7.5 Comment lire le journal de commandes du serveur ?

Il existe un journal des commandes exécutées sur le serveur Safekit.

Le **journal des commandes** peut être consulté avec la commande `safekit cmdlog`

Pour plus de détails, voir la [section 10.12](#).

## 7.6 Module stable (Ready) et (Ready)

- Un module miroir stable sur 2 serveurs est dans l'état  PRIM (Ready) -  SECOND (Ready) : l'application est opérationnelle sur le serveur PRIM ; en cas de panne, le serveur SECOND est prêt à reprendre l'application.
- Un module ferme stable est dans l'état  UP (Ready) sur tous les serveurs de la ferme : l'application est opérationnelle sur tous les serveurs.

## 7.7 Module dégradé ✓ (Ready) et ✗/○ (NotReady)

Un module miroir dégradé est dans l'état ✓<sub>ALONE</sub> (Ready) - ✗<sub>STOP</sub>/○<sub>WAIT</sub> (NotReady). Il n'y a plus de serveur de reprise mais l'application est opérationnelle sur le serveur `ALONE`.

Un module ferme dégradé est dans l'état ✓<sub>UP</sub> (Ready) sur au moins un serveur de la ferme, les autres serveurs étant dans l'état ✗<sub>STOP</sub>/○<sub>WAIT</sub> (NotReady). L'application est opérationnelle sur le serveur `UP`.

Dans le cas dégradé, il n'y a pas de procédure d'urgence à mettre en œuvre. L'analyse de l'état ✗<sub>STOP</sub>/○<sub>WAIT</sub> (NotReady) peut être réalisée plus tard. Néanmoins, vous pouvez tenter de redémarrer le module :

- ⇒ si le module est ✗<sub>STOP</sub>, voir la [section 7.9](#)
- ⇒ si le module est ✗<sub>WAIT</sub>, voir la [section 7.10](#)

## 7.8 Module hors service ✗/○ (NotReady) et ✗/○ (NotReady)


Un module miroir ou ferme hors service est dans l'état ✗<sub>STOP</sub>/○<sub>WAIT</sub> (NotReady) sur tous les serveurs. Dans ce cas, l'application n'est plus opérationnelle sur aucun serveur. Il faut rétablir la situation et redémarrer le module dans l'état ✓ (Ready) sur au moins un serveur :

- ⇒ si le module est ✗<sub>STOP</sub> (NotReady), voir la [section 7.9](#)
- ⇒ si le module est ○<sub>WAIT</sub> (NotReady), voir la [section 7.10](#)

## 7.9 Module ✗<sub>STOP</sub> (NotReady) : redémarrer le module

1. Redémarrer le module arrêté (remplacer ci-dessous `AM` par le nom du module) avec :
  - o La console web via  Supervision/... du nœud/  Démarrer/
  - o la commande `safekit start -m AM` exécutée sur le nœud
2. Vérifier que le module devient ✓ (Ready).
3. Analyser le résultat du démarrage dans le journal du module et le journal des scripts avec (remplacer ci-dessous `node1` par le nom du nœud et `AM` par le nom du module) :
  - o la console web avec l'URI [/console/fr/monitoring/modules/AM/nodes/node1/logs](#)
  - o la commande `safekit logview -m AM` exécutée sur `node1`, pour le journal du module
  - o sur `node1`, dans les fichiers `SAFEVAR/modules/AM/userlog_<year>_<month>_<day>T<time>_<script name>.uolog`, pour le journal des scripts


## 7.10 Module WAIT (NotReady) : réparer la ressource="down"

Si le module est dans l'état  WAIT (NotReady), il attend que l'état d'une ressource devienne up.

Vous devez réparer la ressource mise à down.

Pour déterminer la ressource à réparer, analyser les messages du journal et l'état des ressources (voir [section 7.4](#)).


### Notes :


Un checker de type wait est à l'origine de l'état  WAIT (NotReady). Il est démarré après le script `prestart` et arrêté avant `poststop`.

Le checker est actif sur tous les serveurs  ALONE/PRIM/SECOND/UP (Ready).

L'action du checker sur erreur est de positionner une ressource à down.

La règle de failover associée à la ressource down exécute l'action wait.

Le module est mis localement dans l'état  WAIT (NotReady) tant que la ressource reste down.

Le module sort de l'état  WAIT (NotReady) dès que le checker positionne la ressource à up.

Messages des checkers wait :

- fichiers non à jour localement : voir [section 5](#)  

```
"Potentially not uptodate data for replicated directories (wait for the start of the remote server)"
>Action wait from failover rule notuptodate_server"
"If you are sure that this server has valid data, run safekit prim to force start as primary"
```
- `<interface check="on">` checker d'une interface réseau locale  

```
"Resource intf.ip.0 set to down by intfcheck"
>Action wait from failover rule interface_failure"
```
- `<ping>` checker d'une adresse IP externe  

```
"Resource ping.id set to down by pingcheck"
>Action wait from failover rule p_id"
```
- `<module>` checker d'un autre module  

```
"Resource module.othermodule_ip set to down by modulecheck"
>Action wait from failover rule module_failure"
```
- `<tcp ident="id" when="pre">` checker d'un service TCP externe  

```
"Resource tcp.id set to down by tcpcheck"
>Action wait from failover rule t_id"
```
- `<custom ident="id" when="pre">` checker personnalisé  

```
"Resource custom.id set to down by customscript"
>Action wait from failover rule c_id"
```
- `<splitbrain>` checker  

```
"Resource splitbrain.uptodate set to down by splitbraincheck"
>Action wait from failover rule splitbrain_failure"
```

Fichiers non à jour localement à cause du split-brain : voir [section 13.18](#)

## 7.11 Module oscillant de ✓ (Ready) à ⚡ (Transient)

Si un module oscille de l'état ✓ (Ready) à l'état ⚡ (Transient), il est soumis à un checker de type restart ou stopstart qui détecte une erreur en boucle.

Par défaut, au 4<sup>ième</sup> redémarrage infructueux sur un serveur, le module s'arrête sur le serveur en ✗<sub>STOP</sub> (NotReady).

Analyser le journal du module pour déterminer quel checker est à l'origine de l'oscillation (pour lire les journaux, voir la [section 7.4](#)).

### Notes :

Un checker restart ou stopstart est défini dans `userconfig.xml` par :

- `when="prim"` pour un module miroir  
Le checker est démarré sur le nœud ✓<sub>PRIM/ALONE</sub> (Ready) après le script `start_prim` (stoppé avant `stop_prim`). Il teste l'application démarrée dans `start_prim`.
- `when="both"` pour un module ferme  
Le checker est démarré sur tous les nœuds ✓<sub>UP</sub> (Ready) après le script `start_both` (stoppé avant `stop_both`). Il teste l'application démarrée dans `start_both`.

L'action du checker sur erreur est d'exécuter un restart ou stopstart du module. stopstart sur ✓<sub>PRIM</sub> (Ready) amène à une reprise du rôle de primaire sur l'autre nœud.

Le module est dans l'état ⚡<sub>PRIM/UP</sub> (Transient) pendant la phase de redémarrage

Après plusieurs oscillations, le module s'arrête avec le message

```
"Action stop called by maxloop"
```

dans le journal du module : voir [section 7.12](#)

Messages des checkers restart ou stopstart :

- `<errd>` dans `userconfig.xml`: checker de processus  

```
"Process appli.exe not running"
>Action restart|stopstart called by errd"
```
- `<tcp ident="id" when="prim"|"both">` dans `userconfig.xml`: checker TCP d'une application  

```
"Resource tcp.id set to down by tcpcheck"
>Action restart|stopstart from failover rule t_id"
```
- `<custom ident="id" when="prim"|"both">` dans `userconfig.xml` : checker personnalisé  

```
"Resource custom.id set to down by
customscript"
>Action restart|stopstart from failover rule c_id"
```

ou

```
"Action restart|stopstart called by
customscript"
```

## 7.12 Message sur stop après maxloop

Si une erreur détectée par un checker se répète plusieurs fois et successivement, le module est arrêté sur le serveur en **✗STOP** (NotReady) car l'erreur est permanente et l'action du checker n'arrive pas à la corriger

Si dans `userconfig.xml`, pas de paramètre `maxloop / loop_interval` dans `<service>` :

- par défaut `maxloop="3"`, `loop_interval="24"`
- si les checkers génèrent plus de 3 redémarrages infructueux (`restart`, `stopstart`, `wait`) en moins de 24H, alors stop du module : **✗STOP** (NotReady)

Le compteur est remis à 0 dès lors qu'une action de type administrateur est réalisée sur le module : comme une commande `start` ou `stop`

Message sur stop après maxloop

"Action stop called by maxloop"

## 7.13 Module **✓** (Ready) mais application non opérationnelle





Si un serveur présente un état **✓** PRIM (Ready) ou **✓** ALONE (Ready) ou **✓** UP (Ready), il se peut que l'application soit non opérationnelle à cause d'erreurs au démarrage non détectées. Dans la suite, remplacer `node1` par le nom du nœud et `AM` par le nom du module.

1. Analyser les messages de sortie de l'application produits par `start_prim(/start_both)` et `stop_prim(/stop_both)`. Ils sont visibles avec :





- o la console web avec l'URI </console/fr/monitoring/modules/AM/nodes/node1/logs>
- o sur `node1`, dans les fichiers `SAFEVAR/modules/AM/userlog_<year>_<month>_<day>T<time>_<script name>.u.log`, pour le journal des scripts

Chercher s'il y a des erreurs dans les phases de démarrage/arrêt de l'application. Attention, parfois le journal des scripts est désactivé car trop volumineux avec `<user logging="none">` dans `userconfig.xml` du module.

2. Vérifier les scripts `start_prim(/start_both)` et `stop_prim(/stop_both)` du module `miroir(/ferme)` et `userconfig.xml` avec :
  - o la console web avec l'URI </console/fr/configuration/modules/AM/config>
  - o sur `node1` dans le répertoire `SAFE/modules/AM`
3. Faire un `restart` du le nœud **✓** PRIM/ALONE/UP (Ready) pour arrêter et redémarrer localement l'application (sans basculement) avec :

- o la console web via  Supervision/... du nœud/Redémarrer/
  - o la commande `safekit restart -m AM` exécutée sur le nœud
4. Si l'application est toujours non opérationnelle, appliquer un `stop` sur le nœud  PRIM/ALONE/UP (Ready) pour arrêter le module et l'application (avec basculement sur l'autre nœud si ce dernier est Ready) :
- o la console web via  Supervision/... du nœud/  Arrêter/
  - o la commande `safekit stop -m AM` exécutée sur le nœud

## 7.14 Module mirror ALONE (Ready) / WAIT OU STOP (NotReady)

Si un module miroir reste dans l'état  ALONE (Ready) /  WAIT (NotReady), vérifier la ressource `state.remote` sur chacun des nœuds (pour lire les ressources, voir la [section 7.4](#)). Si cet état est UNKNOWN sur les deux nœuds, alors il s'agit probablement d'un problème de communication entre nœuds. Cette situation peut aussi amener à l'état  ALONE (Ready) /  STOP (NotReady). Les raisons possibles sont :

1. Problème réseau
  - Vérifier la configuration réseau
2. Règles de pare-feu sur l'un ou les deux nœuds
  - Voir la [section 10.3](#)
3. Configuration du cluster ou clés cryptographiques du cluster non identiques
  - Afin de communiquer entre eux, les nœuds doivent appartenir au même cluster SafeKit et avoir la même configuration (voir [section 12](#)).
  - o La console web émet un message d'avertissement si les nœuds du cluster n'ont pas la même configuration
  - o La commande en ligne : `safekit cluster confinfo` exécutée sur n'importe quel nœud du cluster doit reporter des signatures de configuration de cluster identiques pour tous les nœuds (voir [section 9.2](#))
  - Si la configuration du cluster SafeKit n'est pas identique, il faut réappliquer la configuration sur tous les nœuds comme cela est décrit en [section 3.2.2](#).
4. Clés cryptographiques de module non identiques
  - Quand la cryptographie est activée pour le module, la ressource `usersetting.encryption` est "on" nœuds (pour consulter l'état des ressources, voir la [section 7.4](#)). Si les nœuds ont des clés cryptographiques différentes, alors les deux nœuds ne pourront pas communiquer entre eux.
  - Afin de distribuer des clés identiques, il faut réappliquer la configuration du module sur tous les nœuds.
  - Pour plus de détails, voir la [section 10.7](#)
5. Clés cryptographiques du module expirées
  - Dans SafeKit <= 7.4.0.31, la clé de chiffrement des communications a une durée de validité de 1 an. Quand celle-ci expire dans un module miroir avec la réplification de fichiers, la réintégration sur le secondaire échoue et le module s'arrête avec le message d'erreur suivant dans le journal :

```
reintegre | D | XXX clnttcp_create: socket=7 TLS handshake failed
```

Dans SafeKit > 7.4.0.31, le message est :

```
reintegre | D | XXX clnttcp_create: socket=7 TLS handshake failed. Check server time and module certificate (expiration date, hash)
```

Pour résoudre ce problème, voir la [section 10.7.3.1](#)

### 7.15 Module ferme ✓<sub>UP</sub> (Ready) mais problème de load balancing

Bien que tous les serveurs de la ferme soient ✓<sub>UP</sub> (Ready), le load-balancing ne fonctionne pas.

Pour une analyse plus fine sur ce sujet, voir la section suivante et :

- ⇒ [section 4.3.4](#) pour le test de l'adresse virtuelle
- ⇒ [section 4.3.5](#) pour le test du load-balancing
- ⇒ [section 4.3.7](#) dans le cas d'une adresse MAC invisible
- ⇒ [section 7.24](#) pour la résolution VIP ↔ MAC

#### 7.15.1 Non cohérence des parts de la charge réseau



Dans un module ferme, la somme des parts de la charge réseau des nœuds ✓<sub>UP</sub> (Ready) doit être égale à 100%.

Si ce n'est pas le cas, il est très probable qu'il s'agisse d'un problème de communication entre nœuds. Les causes probables sont les mêmes que pour un module miroir, aussi voir la [section 7.14](#) pour d'éventuelles solutions.

Voir aussi la [section 4.3.6](#).

#### 7.15.2 L'adresse IP virtuelle ne répond pas correctement

Si l'adresse IP virtuelle ne répond pas correctement à toutes les demandes de connexions :

1. choisir un nœud de la ferme qui reçoit et traite des connexions sur l'adresse IP virtuelle (connexions TCP établies) :
  - o sous Windows, utiliser la commande `netstat -an | findstr <adresse IP virtuelle>`
  - o sous Linux, utiliser la commande `netstat -an | grep <adresse IP virtuelle>`
2. arrêter le module ferme sur tous les nœuds excepté celui qui reçoit des connexions et qui doit rester ✓<sub>UP</sub> (Ready) avec :
  - o la console web via  Supervision/... du nœud/  Arrêter/
  - o la commande `safekit stop -m AM` sur les nœuds devant être arrêtés (où *AM* est le nom du module)
3. vérifier que l'ensemble des connexions vers l'adresse IP virtuelle sont traitées par le seul nœud ✓<sub>UP</sub> (Ready)

### 7.16 Problème avec l'adresse IP virtuelle après le basculement

Parfois, les périphériques externes fonctionnent correctement lorsque le serveur principal est le nœud `node1`, mais ils ne fonctionnent pas correctement après le basculement sur l'autre nœud (`node2`).

Il peut s'agir d'un problème avec la configuration des périphériques externes. Deux types de connexions TCP doivent être considérés au niveau des périphériques externes :

- Connexions TCP sortantes émises par les périphériques externes vers le cluster SafeKit.
- Connexions TCP entrantes émises par le cluster SafeKit vers le périphérique externe.

Les connexions TCP sortantes, émises par les périphériques externes au cluster SafeKit, doivent être configurées avec l'adresse IP virtuelle et non l'adresse IP physique de node1. Sinon, ils resteront bloqués sur ce nœud en cas de basculement vers node2. Notez que du côté du nœud, l'application doit écouter sur l'adresse IP virtuelle pour accepter les connexions provenant des périphériques externes. Vous pouvez vérifier les sockets TCP d'écoute à l'aide de la commande `netstat`. Généralement, la socket TCP écoute sur toutes les adresses IP (0.0.0.0), et dans ce cas, il n'y a pas de problème.

Pour les connexions TCP entrantes, si l'application initie une connexion TCP depuis node1 vers un périphérique externe, cette connexion aura comme adresse IP source l'adresse IP physique de node1. Après un basculement vers node2, la connexion aura comme adresse IP source, l'adresse IP physique de node2. Cela est dû au fait que l'adresse IP virtuelle est définie en tant qu'alias sur l'interface réseau du nœud primaire, et que l'adresse IP principale de l'interface réseau reste l'adresse IP physique du nœud. Par conséquent, si les périphériques externes effectuent une vérification de leurs connexions entrantes, il est nécessaire de les configurer pour accepter les connexions issues des adresses IP physiques des deux nœuds du cluster.

Toutefois, si les périphériques externes ne peuvent être configurés qu'avec une seule adresse IP, vous devez changer dans la configuration du module, `userconfig.xml` :

```
<virtual_addr where="one_side_alias">
```

en

```
<virtual_addr where="one_side">
```

De cette façon, l'adresse IP principale sera l'adresse IP virtuelle, et les connexions du nœud primaire aux périphériques externes utiliseront toujours l'adresse IP virtuelle comme adresse IP source. Avec cette configuration `one_side`, les périphériques externes doivent être configurés pour accepter les connexions entrantes sur une seule adresse IP : l'adresse IP virtuelle. Le même problème peut se produire si des périphériques externes communiquent avec le cluster à l'aide d'UDP. Dans ce cas, il peut être préférable de configurer `one_side`.

La dernière possibilité est qu'un périphérique externe n'accepte que les communications issues d'une adresse MAC Ethernet unique. Dans ce cas très spécifique et rare, vous devez configurer l'adresse IP virtuelle avec une adresse MAC `vmac_invisible`. Par exemple, elle peut commencer par '5A:FE' :

```
<virtual_interface type="vmac_invisible" addr="5A:FE:01:02:03:04">
```

Avec `vmac_invisible`, une adresse MAC virtuelle est associée à une adresse IP virtuelle, mais cette adresse MAC n'est jamais visible dans les en-têtes Ethernet. Cette configuration permet à tous les serveurs de recevoir les paquets destinés à l'adresse IP virtuelle sans révéler l'adresse MAC virtuelle aux commutateurs, qui seraient généralement en mesure de la localiser. Comme les commutateurs ne peuvent pas détecter cette adresse, ils diffusent les paquets qui lui sont destinés sur tous les ports du réseau local (LAN). Tous les nœuds reçoivent ces paquets, en particulier les deux nœuds du cluster. Par conséquent, le serveur primaire peut se trouver sur node1 ou node2. `vmac_invisible` nécessite le mode de promiscuité sur les cartes Ethernet physiques des

deux nœuds. De plus, cela nécessite le module de noyau 'vip', qui doit être compilé sous Linux.

Il est préférable de configurer l'adresse IP virtuelle avec `one_side_alias` et de ne pas utiliser `one_side` ou `vmac_invisible` si possible.

Notez qu'aucun de ces problèmes ne se pose avec une solution complète de réplication et de redémarrage de machine virtuelle. Dans ce cas, il n'y a pas besoin d'adresse IP virtuelle. La machine virtuelle est relancée sur le nœud secondaire avec la même adresse IP principale et la même adresse MAC. Cela est fourni par les solutions SafeKit pour Hyper-V ou KVM.

### 7.17 Problème après boot

Si vous rencontrez un problème après le boot, voir la [section 4.1](#).

Notez que par défaut, les modules ne sont pas automatiquement démarrés au boot. Pour cela, vous devez configurer le démarrage au boot :

- avec la console web avec l'URI </console/fr/configuration/modules/AM/config>
- dans le fichier `SAFE/modules/AM/conf/userconfig.xml` sur `node1` avec l'attribut `boot` dans le tag `service` (voir [section 13.3.3](#))

Puis appliquer la nouvelle configuration sur tous les nœuds.

### 7.18 Analyse à partir des snapshots du module applicatif

Lorsque le problème n'est pas facilement identifiable, il est recommandé de prendre un snapshot du module sur tous les nœuds comme décrit dans la [section 3.5](#). Un snapshot est un fichier zip qui rassemble, pour un module, les fichiers de configuration, les dumps... Son contenu permet une analyse hors ligne et approfondie de l'état du module et du nœud.



La structure et le contenu du snapshot varie en fonction de la version de SafeKit.

Depuis SafeKit 8.1, la structure du snapshot complet est la suivante :

<code>snapshot_centos7_test3_mirror/</code>	Répertoire <code>snapshot_nodename_AM</code> Snapshot pour le module <code>AM</code> récupéré depuis le nœud <code>nodename</code>
<code>mirror/</code>	Répertoire <code>AM</code> Nom du module
<code>config_2021_05_05_14_15_42/</code> <code>config_2021_07_08_10_05_02/</code> <code>config_2021_08_18_16_15_25/</code>	Répertoires <code>config_year_month_day_hour_mn_sec</code> Les 3 dernières configurations du module, y compris la courante
<code>dump_2021_05_15_10_15_40/</code> <code>dump_2021_07_20_11_05_35/</code> <code>dump_2021_08_28_08_11_45/</code>	Répertoires <code>dump_year_month_day_hour_mn_sec</code> Les 3 derniers dumps du module, y compris le dernier

tmp/	Répertoire pour le support niveau 3
------	-------------------------------------

Depuis SafeKit 8.2.6, SafeKit propose l'outil `anontool` qui permet de générer à partir d'un snapshot complet, un snapshot filtré et anonymisé. Le snapshot filtré contient le sous-ensemble minimal pour permettre l'analyse d'un problème :

- o la configuration du cluster et du module (répertoire `config_year_month_day_hour_mn_sec` le plus récent)
- o le journal du module, les journaux des scripts du module et le journal des commandes SafeKit du répertoire `dump_year_month_day_hour_mn_sec` le plus récent

Chacun de ces fichiers est anonymisé. Voir la [section 9.6.2.2](#) pour plus de détails.

Le snapshot anonymisé étant restreint il ne permet qu'une analyse partielle.

### 7.18.1 Fichiers de configuration du module

Les fichiers de configuration du module sont sauvegardés comme suit :

<code>config_2021_08_18_16_15_25/</code>	Répertoire des fichiers de configuration du module
<code>module/</code> <code>  bin/</code> <code>  conf/</code> <code>  web/</code> <code>private/</code>	Répertoire <code>module</code> Il contient les fichiers de configuration de l'utilisateur : <ul style="list-style-type: none"> <li>• Répertoire <code>bin</code>  <code>scripts start_xx, stop_xx, ...</code></li> <li>• Répertoire <code>conf</code>            Fichier de configuration XML  <code>userconfig.xml</code></li> </ul>

Vérifier le fichier de configuration XML et les scripts pour résoudre les problèmes d'intégration de l'application dans SafeKit

### 7.18.2 Fichiers de dump du module

Le dump contient l'état du module et du nœud SafeKit tel qu'il était au moment du dump.

<code>dump_2021_08_28_08_11_45/</code>	Répertoire des fichiers de dump du module
<code>csv/</code>  <code>licenses/</code>  <code>notifications/</code>  <code>userlog/</code>	<ul style="list-style-type: none"> <li>• Répertoire <code>csv</code>            Journaux et états dans le format csv</li> <li>• Répertoire <code>licences</code>            Licences SafeKit sauvegardées depuis le répertoire <code>SAFE/conf</code></li> <li>• Répertoire <code>notifications</code></li> </ul>

var/  web/	<p>Fichiers de configuration de l'agent de notification par courriel, copiés depuis le répertoire <code>SAFE/web/notifications</code></p> <ul style="list-style-type: none"> <li>• Répertoire <code>userlog</code></li> </ul> <p>Journaux des scripts</p> <ul style="list-style-type: none"> <li>• Répertoire <code>var</code></li> </ul> <p>Copie d'une partie du répertoire <code>SAFEVAR</code></p> <ul style="list-style-type: none"> <li>• Répertoire <code>web</code></li> </ul> <p>Fichiers de configuration du service web, copiés depuis le répertoire <code>SAFE/web/conf</code></p>
log.txt logverbose.txt	Journaux du module (verbeux et non verbeux)
healthcheck.txt	Depuis SafeKit 8.2.6, un rapport de diagnostic qui permet de réaliser une vérification globale de l'environnement SafeKit sur un nœud (voir <a href="#">section 7.3</a> )
heartplug	<p>Fichier d'informations</p> <p>Diverses informations sur le nœud (liste et état des modules installés, version du système d'exploitation, configuration des disques et du réseau, etc.)</p>
last.txt systemevt.txt  ou applicationevt.txt systemevt.txt	<p>Journaux système</p> <ul style="list-style-type: none"> <li>• Sous Linux, <code>last.txt</code> et <code>systemevt.txt</code></li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• Sous Windows, <code>applicationevt.txt</code> et <code>systemevt.txt</code></li> </ul>
commandlog.txt	Journal des commandes du nœud
heart heart.trc nfsbox nfsbox.trc	Fichiers de trace pour le support niveau 3

- Vérifier le(s) fichier(s) de licence dans le répertoire `licenses` pour résoudre des problèmes concernant le contrôle de licence SafeKit
- Vérifier les fichiers de configuration Apache dans le répertoire `web` pour résoudre des problèmes concernant le service web SafeKit
- Vérifiez les logs du module, `log.txt` et `logverbose.txt`, pour résoudre des problèmes concernant le comportement du module

- Vérifier le journal des scripts `userlog/userlog_<year>_<month>_<day>T<time>_<script name>.uolog` pour résoudre des problèmes concernant le démarrage/arrêt de l'application
- Depuis SafeKit 8.2.6, vérifier la présence d'erreurs dans le fichier `healthcheck.txt`
- Si nécessaire, consulter le fichier `heartplug` pour obtenir des informations sur le nœud et rechercher dans les journaux du système les événements qui se sont produits en même temps que le problème analysé
- Consulter le journal des commandes `commandlog.txt` pour résoudre des problèmes concernant la gestion du cluster SafeKit ou les commandes distribuées

### 7.18.2.1 Répertoire `var`

Le répertoire `var` est principalement destiné au support de niveau 3. Il s'agit d'une copie d'une partie du répertoire `SAFEVAR`. Dans le répertoire `var/cluster` :

- Consulter le fichier `cluster.xml` pour vérifier la configuration du cluster
- Consulter le fichier `cluster_ip.xml` pour résolution des noms DNS contenus dans la configuration du cluster

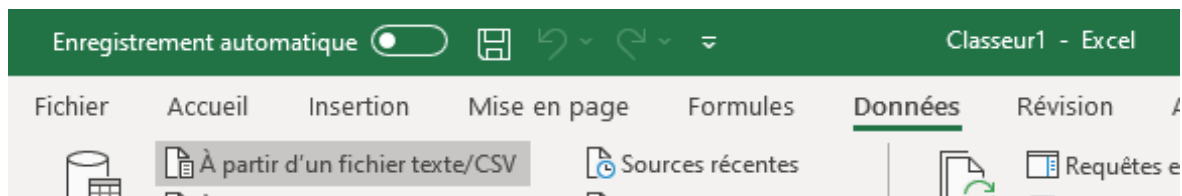
### 7.18.2.2 Répertoire `csv`

Les journaux et états sont aussi exportés au format `csv`, dans le répertoire `csv` :

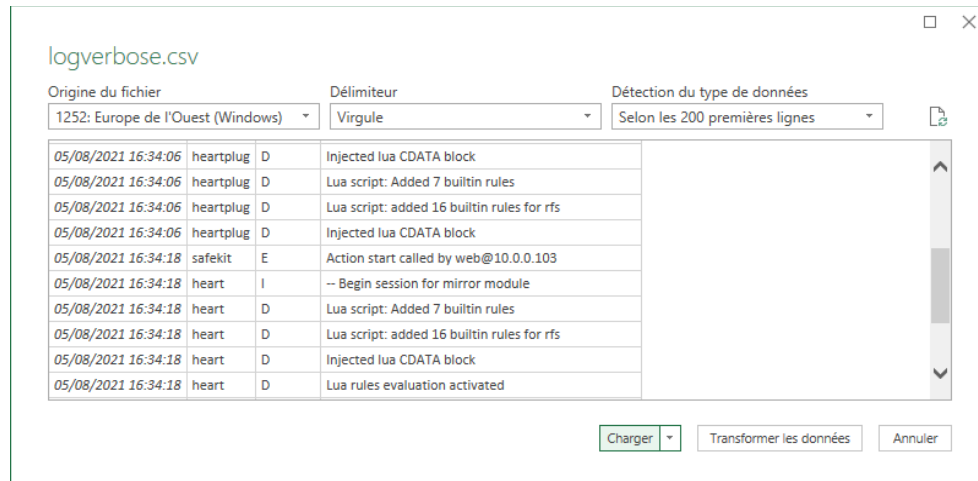
<code>csv/</code>	Répertoire <code>csv</code>
<code>logverbose.csv</code> <code>resource.csv</code> <code>resourcelog.csv</code>	Journaux et état du module <ul style="list-style-type: none"> <li>• Journal verbeux</li> <li>• État des ressources et historique de l'état des ressources</li> </ul>
<code>commandlog.csv</code> <code>modules.csv</code> <code>moduleslog.csv</code> <code>clusterstate.csv</code>	Journaux et états du nœud <ul style="list-style-type: none"> <li>• Journal des commandes</li> <li>• Liste des modules installés</li> <li>• Pour le support niveau 3</li> </ul>

Importer les fichiers `csv` dans Excel pour simplifier leur analyse. Pour importer un fichier :

1. Créer un nouveau classeur
2. Depuis l'onglet `Données`, importer A partir d'un fichier texte/CSV



3. Dans la boîte de dialogue, localiser et double-cliquer sur le fichier `csv` à importer, puis cliquez sur `Importer`
4. Puis cliquer sur `Charger`



Vous pouvez utiliser les fonctionnalités d'Excel pour filtrer les lignes en fonction du niveau des messages, ... et charger dans des feuilles différentes les csv de chaque nœud.



Pour afficher la date exacte, formater les cellules avec  
Nombre/Personnalisée jj/mm/aaaa hh:mm:ss,000.

### 7.19 Problème avec la taille des bases de données de SafeKit

SafeKit utilise le stockage SQLite3 pour sauvegarder :

- Le journal et l'état du nœud
- SAFEVAR/log.db contient le journal des commandes
- SAFEVAR/resource.db contient la liste des modules installés et son historique

Ces bases sont appelées bases de données du nœud.

- Le journal et les ressources du module
  - o SAFEUSERVAR/log.db contient le journal du module.
  - o SAFEUSERVAR/resource.db contient l'état des ressources du module et son historique

Ces bases sont appelées bases de données du module.

La taille des logs et des historiques augmente au fur et à mesure que des événements se produisent sur le nœud SafeKit et les modules. Par conséquent, ils doivent être purgés régulièrement en supprimant les entrées les plus anciennes. Ceci est fait automatiquement grâce à une tâche périodique (task scheduler sous Windows ; crontab sous Linux) qui est contrôlé par le service `safeadmin`. Le nettoyage des bases de données du nœud est toujours actif. Le nettoyage des bases de données du module n'est actif que lorsque le module est en cours d'exécution. Pour vérifier que les tâches sont actives :

- Tâche de nettoyage des bases de données du nœud
  - o Sous Windows, exécutez `schtasks /QUERY /TN safelog_clean`
  - o Sous Linux, exécutez `crontab -u safekit -l`

La sortie de cette commande doit contenir l'entrée `safelog_clean`

- Tâche de nettoyage des bases de données du module *AM* (où *AM* est le nom du module)
  - o Sous Windows, exécutez `schtasks /QUERY /TN safelog_AM`
  - o Sous Linux, exécutez `crontab -u safekit -l`

La sortie de cette commande doit contenir l'entrée `safelog_clean_AM`

La commande qui implémente le nettoyage est localisée sous `SAFEBIN` (en Linux, `SAFEBIN=/opt/safekit/private/bin`; en Windows, `SAFE=C:\safekit\private\bin` - si `%SYSTEMDRIVE%=C:`):

<code>dbclean.ps1</code> en Windows et <code>dbclean.sh</code> en Linux	Purge du journal et de l'historique dans les bases de données du nœud
<code>dbclean.ps1 AM</code> en Windows et <code>dbclean.sh AM</code> en Linux	Purge du journal et de l'historique dans les bases de données du module nommé <i>AM</i>

Si nécessaire, vous pouvez exécuter ce script en dehors de la période prévue pour forcer le nettoyage des bases de données.

## 7.20 Problème pour récupérer le certificat de l'autorité de certification depuis une PKI externe

Lorsque vous utilisez la PKI SafeKit, vous devez fournir le certificat de l'autorité de certification `CA` utilisée pour émettre les certificats des serveurs (fichier `cacert.crt` contenant la chaîne de certificats pour les autorités de certification racine et intermédiaires).

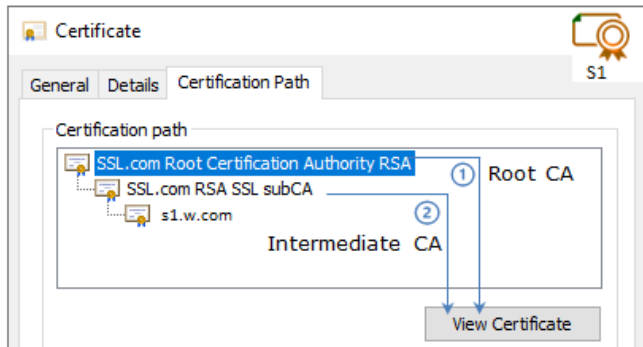
Si vous rencontrez des difficultés à récupérer ce fichier depuis la PKI, vous pouvez le construire en suivant les procédures décrites ci-dessous.

### 7.20.1 Exporter les certificats CA depuis des certificats publics

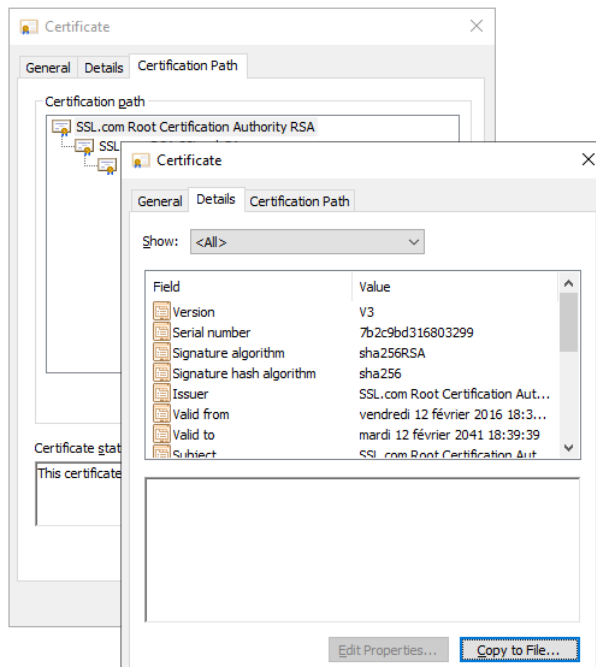
La procédure suivante explique comment construire, le fichier `combined.cer`, la chaîne de certificats pour les Autorités de Certification racine et intermédiaires d'un certificat public.

Lorsque vous avez le certificat public d'un serveur, fichier de certificat au format X.509 encodé en Base-64 (PEM), généré par la PKI :

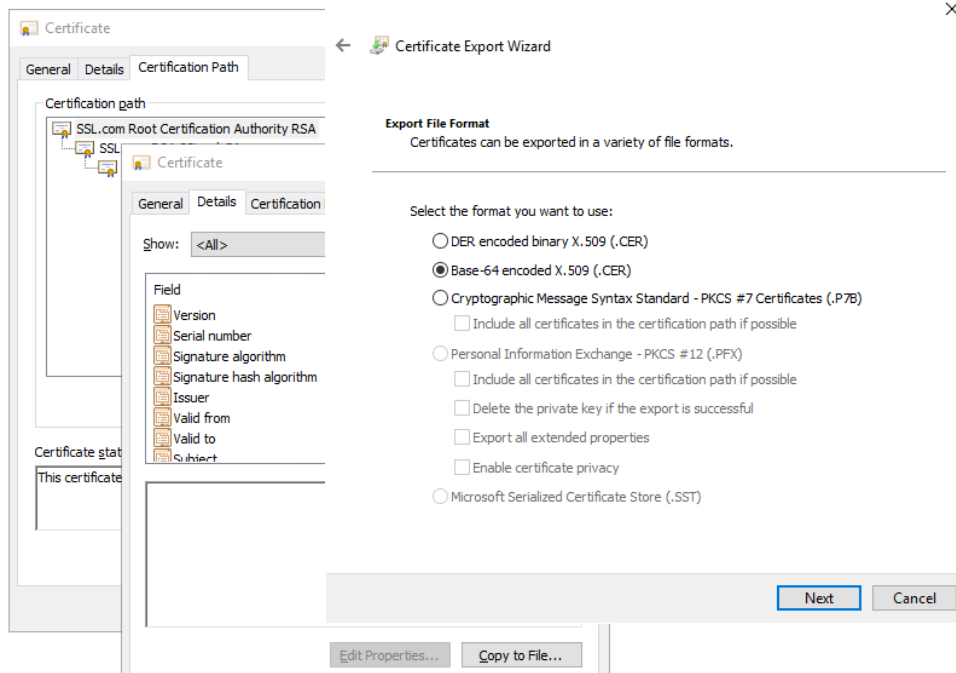
1. Copier ce fichier `.crt` (ou `.cer`) sur une station de travail Windows
2. Double cliquer sur le fichier pour l'ouvrir avec « Extension noyau de chiffrement »
3. Cliquer sur l'onglet « Chemin d'accès de certification » pour afficher l'arbre des autorités de certification
4. Sélectionner une entrée (de haut en bas en excluant la feuille)



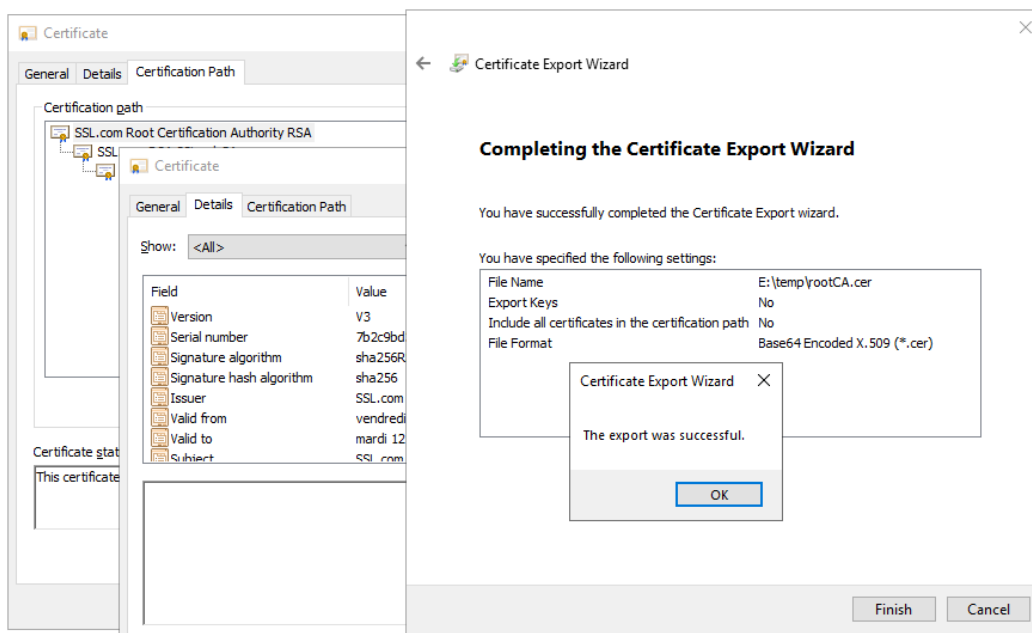
5. Cliquer sur « Afficher le certificat ». Une nouvelle fenêtre s'ouvre pour le certificat sélectionné
6. Dans cette nouvelle fenêtre, sélectionner l'onglet « Details » puis cliquer sur « Copier dans un fichier »



7. Cela ouvre l'Assistant Exportation du certificat :
  - a. Cliquer sur Suivant
  - b. Sur la page « Format de fichier d'exportation », sélectionner « Codé à base 64 X.509 (.cer). », puis cliquer sur « Suivant »



- c. Dans « Fichier à exporter », cliquer sur « Parcourir » pour accéder à l'emplacement vers lequel vous souhaitez exporter le certificat. Pour la zone « Nom de fichier », nommer le fichier de certificat. Cliquer ensuite sur « Suivant ».
- d. Cliquer sur « Terminer » pour exporter le certificat



8. Répéter maintenant les étapes 4 à 7 pour toutes les entrées (sauf la dernière) afin d'exporter tous les certificats des CA intermédiaires. Dans l'exemple, il faut répéter les étapes sur l'AC intermédiaire SSSL.com RSA subCA pour l'extraire en tant que certificat propre.
9. Concaténer tous les certificats obtenus dans un fichier unique `combined.cer`

Exécutez la commande suivante avec tous les certificats CA que vous avez extraits précédemment :

1. sous Windows:

```
type intermediateCA.cer rootCA.cer > combined.cer
```

2. sous Linux:

```
cat intermediateCA.cer rootCA.cer >> combined.cer
```

Le certificat qui en résulte doit ressembler à ce qui suit :

```
-----BEGIN CERTIFICATE-----
MIIGbzCCBFegAwIBAgIIICZftEJ0fB/wDQYJKoZIhvcNAQELBQAwfDELMakGAlUE
BhMCMVVMxMjAMBgNVBAGMBVR1eGFzMRAwDgYDVQQHDAIb3VzdG9uMRgwFgYDVQQK
bRbjat7JD6MBidAWRCJWC1R/5etTzWwWzRCrzvIHC7W06rCzWu69a+17ofCK1Ws
y702dmPTKEdeEfwHgLx0LxJr/Aw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIIeyyb0xaAMpkwDQYJKoZIhvcNAQELBQAwfDELMakGAlUE
BhMCMVVMxMjAMBgNVBAGMBVR1eGFzMRAwDgYDVQQHDAIb3VzdG9uMRgwFgYDVQQK
oYYitmUnDuy2n0Jg5GfCtdpBC8Tt12EbvPofkSvXRadeuims2cXp71NIWuuA8ShY
Ic2wBlX7Jz9TkHcPBB5XJ7k=
-----END CERTIFICATE-----
```

Le fichier résultat peut être utilisé en tant que `SAFE/web/conf/cacert.crt`

## 7.21 Problème d'envoi de courriel par l'agent de notification SafeKit

Depuis SafeKit 8.2.4, SafeKit propose un agent de notification qui envoie des courriels regroupant les événements majeurs sur les modules. Il est décrit dans la [section 10.10](#).

Cette section explique comment dépanner l'agent de notification à l'aide de la commande de test d'envoi de courriel :

1. Se connecter en tant qu'administrateur
2. Aller dans le répertoire `SAFE/notifications`

```
SAFE=C:\safekit (si %SYSTEMDRIVE%=C:)
```

3. Exécuter `./private/bin/safenotif -testemail`

Cette commande peut échouer en raison des problèmes listés ci-dessous.

Si le test réussi et que vous rencontrez toujours des problèmes, veuillez consulter le journal de l'agent de notification SafeKit pour une recherche plus approfondie. Le journal se trouve à l'emplacement suivant : `SAFEVAR\notifications\safenotif.log`. Ce fichier a une taille limitée et est tronqué si la taille limite est atteinte. Par conséquent, il est recommandé d'en faire une copie si vous l'analysez, ou si vous souhaitez que le support SafeKit l'analyse.

### 7.21.1 Failed to read or parse the configuration file

La commande de test d'envoi de courriel peut échouer avec l'erreur suivante :

```
Failed to read or parse the configuration file.
Please verify the "SAFE/conf/notifications/safenotif_conf.json" file exists and
is properly formatted as a JSON file.
```

Cela est dû soit à :

- le fichier `SAFE/conf/notifications/safenotif_conf.json` n'existe pas.

Vous devez configurer l'agent comme décrit dans la [section 10.10.1](#)

- le fichier `SAFE/conf/notifications/safenotif_conf.json` ne respecte pas le format JSON.

Utilisez un outil (sur votre machine ou en ligne) pour vérifier la syntaxe JSON.

- le fichier `SAFE/conf/notifications/safenotif_conf.json` contient des chemins d'accès à un fichier.

Par exemple, la propriété `smtp.expert.caCertificateFile` accepte un chemin. Sous Windows, les chemins contiennent des barres obliques inverses (`\`), qui doivent être précédées avec une autre barre oblique inverse (`\\`), par exemple `C:\\Users\\Administrator\\certfile.pem`.

### 7.21.2 Blocage lors du test d'envoi de courriel

Le test d'envoi de courriel peut se bloquer et ne pas se terminer du tout après l'affichage de la ligne suivante :

```
Sending email from name@my.host to name@my.host with no SMTP authentication...
```

Cela peut être dû à une incompatibilité de protocole.

Pour résoudre ce problème, modifier le fichier

`SAFE/conf/notifications/safenotif_conf.json` afin d'y définir une valeur appropriée pour la propriété `smtp.protocol`.

Noter que d'autres comportements peuvent survenir en cas d'incompatibilité de protocole (voir la section suivante).

### 7.21.3 Erreurs curl

L'agent de notification utilise `curl` comme client SMTP. Par conséquent, lorsqu'une erreur d'envoi de courriel se produit, examiner l'erreur `curl` est essentiel pour comprendre la cause de l'échec. Les erreurs suivantes peuvent survenir. Pour les autres erreurs, consultez la documentation `curl`.

- Adresse de destinataire rejetée

L'adresse d'un destinataire est rejetée par le serveur SMTP avec l'erreur suivante :

```
curl error: curl: (55) RCPT failed: 550
```

Pour résoudre ce problème, modifiez le fichier

`SAFE/conf/notifications/safenotif_conf.json` afin de définir l'adresse correcte du destinataire dans `emailNotifications.recipients`.

- Incompatibilité de protocole

Lorsque le protocole utilisé par l'agent de notification ne correspond pas à celui requis par le serveur SMTP, vous pouvez rencontrer les erreurs `curl` suivantes :

```
curl: (35) OpenSSL/3.2.1: error:0A00010B:SSL routines::wrong version number
curl: (55) MAIL failed: 530
curl: (64) STARTTLS not supported
```

Pour résoudre ces problèmes, modifiez le fichier

`SAFE/conf/notifications/safenotif_conf.json` afin de définir la valeur appropriée pour la propriété `smtp.protocol`.

Noter que d'autres comportements peuvent survenir en cas d'incompatibilité de protocole (voir la section précédente).

- Incompatibilité d'authentification

```
o curl: (35) OpenSSL/3.2.1: error:0A0000C6:SSL routines::packet length too long
```

L'agent de notification a tenté de se connecter au serveur SMTP en s'authentifiant, alors qu'aucune authentification n'est requise.

Pour résoudre ce problème, réinitialisez les identifiants du client SMTP comme décrit dans la [section 10.10.2](#).

```
o curl: (55) RCPT failed: 554
```

L'agent de notification a tenté de se connecter au serveur SMTP sans s'authentifier, alors que l'authentification est requise.

Pour résoudre ce problème, définissez les identifiants du client SMTP comme décrit dans la [section 10.10.2](#).

- Problème de certificat

```
curl: (60) SSL certificate problem: self-signed certificate
```

Cette erreur peut se produire lorsque le serveur SMTP est configuré pour SMTPS ou SMTP+STARTTLS. Elle signifie que le serveur SMTP utilise un certificat auto-signé, plutôt qu'un certificat signé par une autorité de certification de confiance. Le certificat de l'Autorité de Certification (CA) qui a émis le certificat du serveur SMTP est nécessaire pour le vérifier.

Pour cela :

1. Demandez à votre fournisseur PKI de fournir le certificat CA, qui doit inclure la chaîne de certificats pour la CA racine et toutes les CA intermédiaires. Il s'agit d'un fichier de certificat au format X.509 encodé en Base-64 (PEM), avec une extension `.pem` ou `.crt`
2. copiez le sur le serveur SafeKit
3. éditez le fichier `SAFE/conf/notifications/safenotif_conf.json` pour renseigner la propriété `smtp.expert.caCertificateFile` avec le chemin du certificat CA en utilisant `\\` dans la chaîne, e.g. `"C:\\Users\\Administrator\\cacert.crt"`.

## 7.22 Problème avec les antivirus

Certains antivirus peuvent interférer avec le bon fonctionnement de SafeKit. Par exemple, Windows Defender peut mettre en quarantaine certains processus SafeKit (comme le service `safeadmin`, la commande `safekit...`), ou bloquer l'accès aux bases de données SafeKit. Cela peut entraîner l'échec des lignes de commande SafeKit ou l'arrêt de modules. Comme ce dysfonctionnement peut survenir de manière sporadique mais non systématique avec Windows Defender, il est recommandé de configurer l'antivirus afin d'éviter de tels problèmes.

De plus, sous Linux et Windows, tous les dossiers répliqués définis dans les modules miroir doivent être exclus de l'analyse antivirus afin d'éviter des perturbations dans la réplication et la synchronisation SafeKit. Par exemple, sous Windows, ce problème est identifié par le message suivant dans le journal détaillé :

```
| 2025-08-27 16:49:33:662000 | nfsboxv3 | D | WARNING : Process 2980 [ MsSense.exe ] access may interfere with replication, possible stop/start ahead
```

Voir la [section 10.6](#) pour la liste des répertoires et processus légitimes de SafeKit qui ne doivent pas être impactés par les antivirus.

## 7.23 Problèmes liés aux modules noyau SafeKit

### 7.23.1 Module miroir avec le filtre `rfs` en Windows

Le module miroir n'a pas pu démarrer en raison d'un conflit de module :

```
nfsboxv3 | E | Kernel filter configuration failed for E:\replicated_dir. Check for module conflicts.
```

Cette erreur peut survenir dans les situations suivantes :

1. Répertoires répliqués dupliqués dans plusieurs modules miroir

Deux modules miroir sont configurés avec les mêmes répertoires répliqués. Cette configuration n'est pas supportée. Pour résoudre ce problème, spécifiez des répertoires répliqués distincts pour chaque module, puis reconfigurez-les.

2. Configuration interne du filtre `rfs` non à jour

La configuration des répertoires répliqués dans le filtre `rfs` n'a pas été correctement mise à jour, même si aucun doublon n'est actuellement configuré. Pour résoudre ce problème, arrêtez tous les modules puis exécutez la commande suivante :

```
net stop rfsfilter
```

Les modules peuvent ensuite être démarrés.

### 7.23.2 Module ferme avec le module `vip` en Linux

Le module ferme ne démarre pas en raison d'une erreur de chargement :

```
| vipplug | E | Unable to load vip kernel extension
```

De plus, lors d'une tentative de chargement manuel du module `vip` avec la commande `modprobe`, l'une des erreurs suivantes est retournée :

```
modprobe: ERROR: could not insert 'vip': Required key not available
```

or

```
modprobe: could not insert 'vip': Key was rejected by service
```

Ce problème survient lorsque Secure Boot est activé. La solution est décrite dans la [section 10.5](#).

## 7.24 Dépannage de résolution VIP ↔ MAC

Cette section permet de diagnostiquer les problèmes liés à la résolution d'adresse IP ↔ MAC, qui peuvent provoquer des pertes de connectivité, des délais de basculement ou un mauvais routage du trafic vers une VIP.

### 7.24.1 Vérifier les entrées du cache

Les clients conservent une correspondance IP ↔ MAC dans leur cache local. Pour vérifier que le cache contient bien la VIP, utiliser les commandes suivantes.

IPv4	<code>arp -a</code>
------	---------------------

IPv6	<ul style="list-style-type: none"><li>• En Windows <code>Get-NetNeighbor -AddressFamily IPv6</code>  ou <code>netsh interface ipv6 show neighbors</code></li><li>• En Linux : <code>ip neighbour</code></li></ul> L'entrée doit être dans l'état <code>Reachable</code> .
------	---

### 7.24.2 Forcer une nouvelle résolution

Si le cache est suspect, détruire l'entrée avec les commandes suivantes (remplacer les valeurs en italique par vos valeurs).

IPv4	<code>arp -d 192.168.10.100</code>
IPv6	<ul style="list-style-type: none"><li>• En Windows <code>Remove-NetNeighbor -IPAddress</code> <code><i>fd00:1234:5678:1::222</i> -InterfaceAlias "Ethernet 2"</code> ou <code>netsh interface ipv6 delete neighbors "Ethernet 2"</code> <code><i>fd00:1234:5678:1::222</i></code></li><li>• En Linux <code>ip neigh del <i>fd00:1234:5678:1::222</i> dev <i>ens224</i></code></li></ul>

Si besoin, utiliser la commande `ping` (avec l'option `-6` pour IPv6) pour forcer la résolution.

### 7.24.3 Observer les requêtes de résolution

Pour observer les requêtes de résolution sur le réseau, utiliser les commandes suivantes.

IPv4	<ul style="list-style-type: none"><li>• En Windows <code>Wireshark</code></li><li>• En Linux <code>tcpdump -i <i>eth0</i> -nn arp</code></li></ul> La trace contient des messages du type : <pre>ARP, Request who-has 192.168.10.100 tell 192.168.10.10 ARP, Reply 192.168.10.100 is-at 00:50:56:aa:bb:cc</pre>
IPv6	<ul style="list-style-type: none"><li>• En Windows <code>Wireshark</code></li><li>• En Linux <code>tcpdump -i <i>ens224</i> -nn icmp6</code></li></ul> La trace contient des messages du type :

	ICMP6, neighbor solicitation ICMP6, neighbor advertisement
--	---

## 7.25 Problème persistant

- ⇒ voir [l'index des messages](#)
- ⇒ pour obtenir l'assistance du support, créer un incident via [portail du support](#), sans oublier d'y attacher les snapshots



## 8. Support SafeKit

Si vous n'avez pas trouvé de solution à un problème rencontré avec SafeKit, ni dans la [section 7](#), ni dans la partie Troubleshooting de [formation SafeKit](#), vous pouvez demander l'assistance du support. Pour cela :

1. Connectez-vous [portail du support](#)
2. Créez un incident sur le produit SafeKit
3. Décrivez précisément l'incident, en indiquant :
  - o le scénario ayant conduit au problème
  - o la date et l'heure de l'incident
  - o la version de SafeKit et du système d'exploitation (obtenue avec la commande `safekit level`)
4. Joignez les snapshots du module, capturés sur les 2 serveurs SafeKit (voir [section 3.5](#))



## 9. Interface ligne de commande

- ⇒ [Section 9.1](#) « Commandes de contrôle et setup de SafeKit »
- ⇒ [Section 9.2](#) « Commandes de configuration et surveillance du cluster »
- ⇒ [Section 9.3](#) « Commandes de contrôle des modules applicatifs »
- ⇒ [Section 9.4](#) « Commandes de surveillance des modules applicatifs »
- ⇒ [Section 9.5](#) « Commandes de configuration des modules applicatifs »
- ⇒ [Section 9.6](#) « Commandes de support »
- ⇒ [Section 9.7](#) « Commandes lors de la maintenance de l'application du module »
- ⇒ [Section 9.8](#) « Commandes distribuées sur plusieurs serveurs SafeKit »
- ⇒ [Section 9.9](#) « Exemples »

L'interface ligne de commande SafeKit est fournie par la commande `safekit`. Pour l'utiliser :

Windows	<ol style="list-style-type: none"><li>1. Ouvrir une console PowerShell en tant qu'administrateur</li><li>2. Aller à la racine du répertoire d'installation de SafeKit <code>SAFE</code> (par défaut <code>SAFE=C:\safekit</code> si <code>%SYSTEMDRIVE%=C:</code>) <code>cd c:\safekit</code></li><li>3. Exécuter <code>.\safekit.exe &lt;arguments&gt;</code> pour la commande locale</li><li>4. Exécuter <code>.\safekit.exe -H "&lt;hosts&gt;" &lt;arguments&gt;</code> pour la commande distribuée sur plusieurs nœuds</li></ol>
Linux	<ol style="list-style-type: none"><li>1. Ouvrir une console Shell en tant que root</li><li>2. Aller à la racine du répertoire d'installation de SafeKit <code>SAFE</code> (par défaut <code>SAFE=/opt/safekit</code>) <code>cd /opt/safekit</code></li><li>3. Exécuter <code>./safekit &lt;arguments&gt;</code> pour la commande locale</li><li>4. Exécuter <code>./safekit -H "&lt;hosts&gt;" &lt;arguments&gt;</code> pour la commande distribuée sur plusieurs nœuds</li></ol>



Cette section présente d'autres commandes qui doivent elles aussi être exécutées en tant qu'administrateur/root.

### 9.1 Commandes de contrôle et setup de SafeKit

Utilisez les commandes suivantes pour démarrer/arrêter les services SafeKit et configurer leur démarrage automatique au boot.

#### 9.1.1 Service `safeadmin`

Service principal de SafeKit obligatoire et démarré automatiquement au boot.

<p><b>Windows</b></p> <pre>net start safeadmin net stop safeadmin</pre>	<p>safeadmin peut aussi être contrôlé dans l'interface Services de Windows.</p> <p>Pour vérifier l'état du service, exécuter :</p> <ul style="list-style-type: none"> <li>• dans une console command prompt sc query safeadmin</li> <li>• dans une console PowerShell: Get-Service -name safeadmin</li> </ul>
<p><b>Linux</b></p> <pre>systemctl start safeadmin systemctl stop safeadmin</pre>	<p>Pour vérifier l'état du service, exécuter :</p> <pre>systemctl status safeadmin</pre>

### 9.1.2 Service safewebserver

Ce service nécessaire pour la console web SafeKit, le module checker et aux commandes distribuées. Par défaut, il est démarré automatiquement au boot. Pour plus de détails, voir la [section 10.9](#).

<pre>safekit webserver start safekit webserver restart safekit webserver stop</pre>	<p>Contrôle du service via la commande safekit.</p>
<p><b>Windows</b></p> <pre>net start safewebserver net stop safewebserver</pre>	<p>Contrôle du service via la commande net.</p> <p>Pour vérifier l'état du service, exécuter :</p> <ul style="list-style-type: none"> <li>• dans une console command prompt sc query safewebserver</li> <li>• dans une console PowerShell Get-Service -name safewebserver</li> </ul>
<p><b>Linux</b></p> <pre>systemctl start safewebserver systemctl restart safewebserver systemctl stop safewebserver</pre>	<p>Contrôle du service via la commande systemctl.</p> <p>Pour vérifier l'état du service, exécuter :</p> <pre>systemctl status safewebserver</pre>
<pre>safekit boot [webon   weboff   webstatus]</pre>	<p>Contrôle le démarrage automatique au boot du service safewebserver.</p> <p>Par défaut : "on"</p>

La configuration par défaut du service web SafeKit est HTTP avec une authentification à base de fichiers. Lors de l'initialisation de SafeKit, décrite dans la [section 11.2.1](#), deux utilisateurs sont créés par défaut :

1. l'utilisateur `admin` pour authentifier l'accès à la console web SafeKit.
2. l'utilisateur privé `rcmdadmin` pour authentifier l'accès à la commande distribuée `safekit`.

Les commandes suivantes sont utilisées pour changer les noms d'utilisateur et les mots de passe de ces utilisateurs si nécessaire :

<pre>safekit webservercfg -passwd <i>pwd</i> [-user <i>username</i>]</pre>	<p>Configure le mot de passe <i>pwd</i> pour l'utilisateur qui accède à la console web. Optionnellement, configure son nom <i>username</i>, qui vaut <i>admin</i> par défaut.</p>
<pre>safekit webservercfg -rcmdpasswd <i>pwd</i> [-rcmduser <i>username</i>]</pre>	<p>Configure le mot de passe <i>pwd</i> pour l'utilisateur privé qui exécute la commande distribuée. Optionnellement, configure son nom <i>username</i>, qui vaut <i>rcmdadmin</i> par défaut.</p>



- Le script `SAFE/private/bin/webservercfg` peut aussi être exécuté directement
- Les options `-user` et `-rcmduser` sont disponibles à partir de SafeKit 8.2.4

### 9.1.3 Agent de notification par courriel

Depuis SafeKit 8.2.4, SafeKit propose un agent de notification pour envoyer des courriels listant les événements majeurs sur les modules. L'agent de notification n'est pas activé par défaut. Pour le configurer et l'activer, reportez-vous à la [section 10.10](#).

Les commandes suivantes sont utilisées pour contrôler cet agent :

<pre>safekit notification enable safekit notification disable</pre>	<p>Active/désactive l'agent de notification.</p>
<pre>safekit notification status</pre>	<p>Affiche l'état de l'agent de notification.</p>

<p><b>Windows</b></p>	<p>Contrôle de la tâche <code>safenotif</code> via le Task scheduler de Windows.</p> <p>Pour vérifier l'état de la tâche, exécuter :</p> <ul style="list-style-type: none"> <li>• Dans un command prompt <pre>schtasks /query /tn "safenotif"</pre> </li> <li>• En PowerShell <pre>Get-ScheduledTask -TaskName "safenotif"   Select-Object TaskName, State</pre> </li> </ul>
<p><b>Linux</b></p> <pre>systemctl start safenotif systemctl restart safenotif systemctl stop safenotif</pre>	<p>Contrôle du service via la commande <code>systemctl</code>.</p> <p>Pour vérifier l'état du service, exécuter :</p> <pre>systemctl status safenotif</pre>

### 9.1.4 Service SNMP

#### 9.1.4.1 Service Net-SNMP Agent en Windows

La surveillance SNMP pour SafeKit n'est pas activée par défaut. Pour l'activer et le configurer voir la [section 10.11](#).

En Windows, la surveillance SNMP est fournie par le service Net-SNMP Agent.

<pre>safekit safeagent [start   stop   restart   check]</pre>	Contrôle du service via la commande <code>safekit</code> .
<pre>net start "Net-SNMP Agent" net stop "Net-SNMP Agent"</pre>	Pour vérifier l'état du service, exécuter : <ul style="list-style-type: none"><li>• dans une console command prompt <code>sc query "Net-SNMP Agent"</code></li><li>• dans une console PowerShell <code>Get-Service -name "Net-SNMP Agent"</code></li></ul>
<pre>safekit boot [snmpon   snmpoff   snmpstatus]</pre>	Contrôle le démarrage automatique au boot du service Net-SNMP Agent.  Par défaut : "off"

#### 9.1.4.2 Service standard snmpd en Linux

La surveillance SNMP pour SafeKit n'est pas activée par défaut. Pour l'activer et le configurer voir la [section 10.11](#).

En Linux, la surveillance SNMP est fournie par l'agent `snmp` standard du système.

<pre>systemctl start snmpd systemctl stop snmpd</pre>	Pour vérifier l'état du service, exécuter : <code>systemctl status snmpd</code>
---	--

### 9.1.5 Service web safecaserv

Service web optionnel permettant la génération de certificats avec la PKI SafeKit (voir [section 11.3.1](#)).

Pour son démarrage, voir la [section 11.3.1.1](#). Pour son arrêt, voir la [section 11.3.1.4](#).

## 9.2 Commandes de configuration et surveillance du cluster

<pre>safekit cluster config [filepath de .xml ou .zip] [lock unlock]</pre>	Applique la nouvelle configuration du cluster SafeKit avec le contenu du fichier passé en argument, <code>cluster.xml</code> ou <code>cluster.zip</code> : <ul style="list-style-type: none"><li>• <code>cluster.xml</code></li></ul> Configure avec le fichier xml passé en argument et génère de nouvelles clés <ul style="list-style-type: none"><li>• <code>cluster.zip</code></li></ul>
--	--

	<p>Configure avec le <code>cluster.xml</code> et les clés contenues dans le <code>.zip</code></p> <p>Appelée sans argument, cette commande conserve la configuration courante mais génère de nouvelles clés.</p> <p>Si cette commande est appelée avec le paramètre <code>lock</code>, les futurs appels ne seront autorisés que si le paramètre <code>unlock</code> est utilisé.</p> <p>Exemple :</p> <pre>safekit cluster config /tmp/newcluster.xml</pre> <p>A utiliser avec prudence : le nouveau fichier <code>cluster.xml</code> et les clés de chiffrement doivent être impérativement copiés sur les autres nœuds, de façon à s'assurer que tous les nœuds ont bien la même configuration de cluster et les mêmes clés.</p>												
<pre>safekit cluster confcheck filepath</pre>	<p>Contrôle la configuration du cluster, avec le contenu du fichier xml passé en argument, sans l'appliquer</p>												
<pre>safekit cluster confinfo</pre>	<p>Retourne, pour chaque serveur actif du cluster :</p> <ul style="list-style-type: none"> <li>la date de dernière configuration du cluster,</li> <li>la signature digitale de la dernière configuration du cluster.</li> <li>L'état de verrouillage (1 pour <code>lock</code>, 0 pour <code>unlock</code>) de la commande de configuration.</li> </ul> <p>Cette commande permet de vérifier que tous les nœuds d'un cluster ont bien la même configuration de cluster.</p> <p>Exemple :</p> <table border="1"> <thead> <tr> <th>Nœud</th> <th>Signature</th> <th>Date</th> <th>Verrou</th> </tr> </thead> <tbody> <tr> <td>rh6server7</td> <td>6f1032b11a7b2 ...</td> <td>33e67c</td> <td>2016-05-20T17:06:45 0</td> </tr> <tr> <td>rh7server7</td> <td>6f1032b11a4e0 ...</td> <td>33e67c</td> <td>2016-05-20T17:06:45 0</td> </tr> </tbody> </table> <p>Les configurations du cluster SafeKit doivent impérativement être les mêmes sur tous les nœuds appartenant au même cluster. Les configurations asymétriques ne sont pas supportées.</p>	Nœud	Signature	Date	Verrou	rh6server7	6f1032b11a7b2 ...	33e67c	2016-05-20T17:06:45 0	rh7server7	6f1032b11a4e0 ...	33e67c	2016-05-20T17:06:45 0
Nœud	Signature	Date	Verrou										
rh6server7	6f1032b11a7b2 ...	33e67c	2016-05-20T17:06:45 0										
rh7server7	6f1032b11a4e0 ...	33e67c	2016-05-20T17:06:45 0										
<pre>safekit cluster deconfig</pre>	<p>Supprime la configuration du cluster ainsi que les clés associées.</p>												
<pre>safekit cluster state</pre>	<p>Retourne l'état global du cluster</p> <p>Pour chaque module installé et pour chaque nœud actif du cluster cette commande liste :</p> <ul style="list-style-type: none"> <li>nom du nœud,</li> <li>nom du module,</li> </ul>												

	<ul style="list-style-type: none"> <li>• mode du module (farm ou mirror),</li> <li>• n° interne d'id du module,</li> <li>• date de la dernière configuration,</li> <li>• signature digitale de la dernière configuration</li> </ul> <p>Cette commande liste quels modules sont installés et sur quels serveurs. La signature et date de dernière configuration permet de vérifier qu'un module a bien la même configuration sur tous les nœuds et, si ce n'est pas le cas, où est la configuration la plus récente.</p>
<code>safekit cluster genkey</code>	Régénère les clés de chiffrement pour la communication globale Safekit. La configuration du cluster doit être réappliquée (avec <code>safekit -G</code> ) pour que cette modification soit prise en compte.
<code>safekit cluster delkey</code>	Supprime les clés de chiffrement pour la communication globale. La configuration du cluster doit être réappliquée (avec <code>safekit -G</code> ) pour que cette modification soit prise en compte.
<code>safekit -H "*" -G</code>	<p>Distribue la configuration locale du cluster et les clés de chiffrement associées lorsqu'elles existent, sur tous les nœuds.</p> <p>Relance une résolution de nom DNS pour tous les noms spécifiés dans <code>cluster.xml</code> et le <code>userconfig.xml</code> des modules, sans arrêter les modules (quand cela est possible).</p> <p>Voir la <a href="#">section 9.8</a> pour des détails sur cette commande distribuée.</p>

### 9.3 Commandes de contrôle des modules applicatifs

Les commandes s'appliquent au module nommé *AM*, passé en argument avec l'option `-m`.



Lorsque la variable d'environnement `SAFEMODULE` est définie avec le nom du module, l'argument `-m` n'est pas nécessaire. Celle-ci est définie lors de l'exécution des scripts du module (voir [section 14.2](#)).

<code>safekit start -m AM</code>	Démarre le module
<code>safekit waitstart -m AM</code>	Attend la fin du démarrage du module
<code>safekit stop -m AM</code>	Arrête le module
<code>safekit shutdown</code>	Stoppe tous les modules en cours d'exécution et attend leur arrêt complet
<code>safekit waitstop -m AM</code>	Attend la fin de l'arrêt du module

<pre>safekit waitstate -m AM STOP   ALONE   UP   PRIM   SECOND</pre>	<p>Attend que le module atteigne l'état stable demandé (NotReady ou Ready)</p>
<pre>safekit restart -m AM</pre>	<p>Applique les scripts d'arrêt puis de démarrage de l'application sans provoquer de basculement.</p> <ul style="list-style-type: none"> <li>• Pour un module miroir Équivalent à <code>stop_prim ; start_prim</code></li> <li>• Pour un module ferme Équivalent à <code>stop_both ; start_both</code></li> </ul>
<pre>safekit stopstart -m AM</pre>	<p>Contrairement au <code>restart</code>, le <code>stopstart</code> provoque l'arrêt complet du module et son redémarrage automatique. Si le module était <code>PRIM</code>, il y a basculement du module <code>PRIM</code> sur l'autre serveur.</p> <p>Équivalent à <code>safekit stop -m AM ; safekit start -m AM</code> mais sans arrêt des checkers dont l'action est <code>wait</code></p>
<pre>safekit forcestop -m AM</pre>	<p>Force l'arrêt du module lorsque le <code>stop</code> n'a pas d'effet</p>
<pre>safekit swap [nosync] -m AM</pre>	<p><b>Module miroir uniquement</b></p> <p>Échange les rôles des serveurs primaire et secondaire. Utiliser l'option <code>nosync</code> pour permuter les rôles sans synchronisation des répertoires répliqués</p>
<pre>safekit prim [fullsync] -m AM</pre>	<p><b>Module miroir uniquement</b></p> <p>Force le module à démarrer en primaire ; échec si l'autre serveur est déjà primaire.</p> <p>Utiliser l'option <code>fullsync</code> pour forcer la synchronisation complète des répertoires répliqués sur le nœud secondaire lors de son démarrage.</p> <p>Option <code>fullsync</code> supportée depuis SafeKit 8.2.5.</p> <p>Voir le bon usage de cette commande en <a href="#">section 5.3</a></p>
<pre>safekit second fullsync] -m AM</pre>	<p><b>Module miroir uniquement</b></p> <p>Force le module à démarrer en secondaire ; échec si l'autre serveur n'est pas primaire</p> <p>Utiliser l'option <code>fullsync</code> pour forcer une réintégration complète de tous les répertoires répliqués</p>
<pre>safekit primforce -m AM</pre>	<p><b>Module miroir uniquement</b></p> <p>Force le module à démarrer en tant que primaire lorsque la commande <code>prim</code> habituelle échoue en raison d'une</p>

	<p>possible incohérence des données lors de la réintégration des fichiers.</p> <p>La commande <code>primforce</code> doit être utilisée avec précaution, car elle peut entraîner une incohérence des données répliquées. Elle permet toutefois de rétablir la situation lorsque les commandes normales de basculement ou de démarrage échouent en raison d'une synchronisation partielle.</p> <p>Voir l'usage de cette commande en <a href="#">section 5.9</a>.</p>
--	---



Les commandes `restart`, `stop`, `stopstart` et `swap` acceptent également l'argument `-i identity`. Cet argument est défini lorsque l'action est appelée par les checkers ou la failover machine à des fins de journalisation et pour incrémenter le compteur `maxloop`. Quand il n'est pas présent, le compteur `maxloop` est réinitialisé.

Les commandes suivantes sont utiles pour récupérer ou affecter l'état des ressources du module.

<pre>safekit get -m AM -r &lt;resource&gt;</pre>	<p>Récupère l'état d'une ressource :</p> <pre>safekit get -r custom.myresource -m AM safekit get -r state.local -m AM</pre>
<pre>safekit set -m AM -r &lt;resource&gt; -v &lt;state&gt;</pre> <p><code>[-n] [-l]</code></p> <p><code>[-i identity]</code></p>	<p>Affecte la valeur d'une ressource :</p> <pre>safekit set -r custom.myresource -v up -m AM safekit set -r custom.myresource -v down -m AM</pre> <p>Chaque affectation des principales ressources est mémorisée dans un journal afin de conserver l'historique leur état.</p> <p>Utiliser <code>-n</code> pour désactiver la journalisation de l'affectation en cours ou <code>-l</code> pour la forcer.</p> <p>Utiliser <code>-i</code> pour spécifier l'identité du composant, qui affecte la ressource, dans le message logué.</p> <p>Voir l'usage de cette commande dans un custom checker en <a href="#">section 15.7.2</a>.</p>

## 9.4 Commandes de surveillance des modules applicatifs

Les commandes s'appliquent au module nommé `AM`, passé en argument avec l'option `-m`.



Lorsque la variable d'environnement `SAFEMODULE` est définie avec le nom du module, l'argument `-m` n'est pas nécessaire. Celle-ci est définie lors de l'exécution des scripts du module (voir [section 14.2](#)).

<pre>safekit level [-m AM]</pre>	Indique la version de SafeKit et la licence
----------------------------------	---

	Avec le paramètre <i>AM</i> , le script <code>level</code> du module est exécuté et ses résultats affichés
<code>safekit state</code>	Affiche l'état de tous les modules
<code>safekit state -m AM</code> <code>[-v   -lq]</code>	Affiche l'état du module <i>AM</i> Avec l'option <code>-v</code> (verbose), les états de toutes les ressources du module sont listés : voir l'utilité des ressources dans la <a href="#">section 7.10</a> Avec l'option <code>-lq</code> , la commande retourne l'état (et le code d'exit): STOP (0), WAIT (1), ALONE (2), UP (2), PRIM (3), SECOND (4)
<code>safekit log -m AM [-s nb]</code> <code>[-A] [-l en fr]</code>	Affiche les <code>&lt;nb&gt;</code> derniers messages E(vènement) du journal du module <i>AM</i> . Utiliser l'option <code>-A</code> pour afficher tous les messages (y compris les messages de debug). Sélectionner la langue avec l'option <code>-l</code> , <code>en</code> (Anglais) ou <code>fr</code> (Français). Par défaut : <code>-s 300</code>
<code>safekit logview -m AM [-A]</code> <code>[-l en fr]</code>	Visualise en temps réel les derniers messages E(vènement) du journal du module <i>AM</i> . Utiliser <code>-A</code> pour afficher le journal verbeux (tous les messages y compris les messages de debug). Sélectionner la langue avec l'option <code>-l</code> , <code>en</code> (Anglais) ou <code>fr</code> (Français).
<code>safekit logview -m AM [-A]</code> <code>[-l en fr]-s 300</code>	Visualise à partir des 300 derniers messages
<code>safekit logsave -m AM [-A]</code> <code>[-l en fr ja] /tmp/f.txt</code>	Voir <a href="#">section 9.6.1</a>
<code>safekit printi printe -m AM</code> "message"	Les scripts applicatifs start/stop peuvent écrire des messages dans le journal du module avec un niveau I ou E.

## 9.5 Commandes de configuration des modules applicatifs

Les commandes s'appliquent au module nommé *AM*, passé en argument avec l'option `-m`.



Lorsque la variable d'environnement `SAFEMODULE` est définie avec le nom du module, l'argument `-m` n'est pas nécessaire. Celle-ci est définie lors de l'exécution des scripts du module (voir [section 14.2](#)).

<code>safekit module install -m AM</code> <code>[-r] [-M id] [AM.safe]</code>	Installe le module <i>AM.safe</i> avec le nom <i>AM</i> <code>[-r]</code> force la réinstallation du module <code>[-M id]</code> force l'installation du module avec l' <code>id</code> spécifié comme module <code>id</code> <ul style="list-style-type: none"> <li>Le fichier <i>AM.safe</i> est cherché dans le répertoire <code>SAFE/Application_Modules</code> et ses sous répertoires.</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>• Si le nom de fichier <i>AM.safe</i> n'est pas renseigné, le fichier <i>AM.safe</i> est cherché dans <code>SAFE/Application_Modules</code></li> <li>• Un chemin absolu peut aussi être donné.</li> </ul>
<code>safekit config -m AM</code>	<p>A exécuter après avoir modifié un fichier sous <code>SAFE/modules/AM</code> tel que <code>userconfig.xml</code>, <code>start_prim/both</code> ou <code>stop_prim/both</code> (miroir/ferme).</p> <p>Il est recommandé d'appliquer cette commande lorsque le module est arrêté. Cependant, elle est permise dans les états <code>ALONE (Ready)</code>, ou <code>STOP</code> et <code>WAIT (NotReady)</code>. Dans ce cas, il s'agit d'une configuration dynamique où seul un sous-ensemble de paramètres peut être modifié. Les paramètres qui sont modifiables dynamiquement sont indiqués dans la <a href="#">section 13</a>.</p>
<code>safekit module genkey -m AM</code>	Génère les clés de chiffrement associées au module <i>AM</i> . Pris en compte à la prochaine configuration du module.
<code>safekit module delkey -m AM</code>	Efface les clés de chiffrement associées au module <i>AM</i> . Pris en compte à la prochaine configuration du module.
<code>safekit -H "*" -E AM</code>	<p>Distribue la configuration locale du module <i>AM</i> et les clés de chiffrement associées lorsqu'elles existent, sur tous les nœuds du cluster.</p> <p>Voir la <a href="#">section 9.8</a> pour des détails sur cette commande distribuée.</p>
<code>safekit deconfig -m AM</code>	<p>A exécuter avant désinstallation du module</p> <p>Demande à chaque plugin défini dans <code>userconfig.xml</code> <code>&lt;errd&gt;</code>, <code>&lt;vip&gt;</code>, <code>&lt;rfs&gt;</code>, <code>&lt;user&gt;</code>... de prendre en compte la déconfiguration du module</p>
<code>safekit confinfo -m AM</code>	<p>Affiche des informations sur la configuration active et la configuration courante du module <i>AM</i> :</p> <ul style="list-style-type: none"> <li>• la configuration active est la dernière configuration appliquée avec succès. Elle est sous <code>SAFE/private/modules/AM</code></li> <li>• la configuration courante est celle présente sous <code>SAFE/modules/AM</code>. Elle est différente de l'active lorsqu'elle a été modifiée sans avoir encore été appliquée.</li> </ul> <p>Cette commande est utile pour contrôler la configuration du module. Elle affiche :</p> <ul style="list-style-type: none"> <li>• la signature et la date de dernière modification (timestamp Unix) de la configuration active</li> <li>• la signature et la date de dernière modification (timestamp Unix) de la configuration courante</li> </ul>

	<p>Si les signatures sont différentes, cela signifie que les configurations ne sont pas identiques et qu'il est probablement nécessaire d'appliquer la configuration courante.</p> <p>Vous pouvez exécuter cette commande sur tous les nœuds qui implémentent le module, pour contrôler qu'ils ont bien la même configuration.</p>
<code>safekit confcheck -m AM</code>	Contrôle la configuration du module sous <code>SAFE/modules/AM</code> sans l'appliquer
<code>safekit module package -m AM /.../newAM.safe</code>	Package le module <code>AM</code> dans <code>/.../newAM.safe</code> (chemin absolu obligatoire) Commande utilisée par la console pour créer un backup dans <code>SAFE/Application_Modules/backup/</code>
<code>safekit module uninstall -m AM</code>	Désinstalle le module <code>AM</code> . Détruit le répertoire de configuration du module <code>SAFE/modules/AM</code>
<code>safekit module list</code>	Liste les noms des modules installés
<code>safekit module listid</code>	Liste les noms et les ids des modules installés
<code>safekit module getports -m AM (or -i id)</code>	Liste les ports de communication qui synchronisent le module entre les serveurs

## 9.6 Commandes de support

Les commandes s'appliquent au module nommé `AM`, passé en argument avec l'option `-m`.



Lorsque la variable d'environnement `SAFEMODULE` est définie avec le nom du module, l'argument `-m` n'est pas nécessaire. Celle-ci est définie lors de l'exécution des scripts du module (voir [section 14.2](#)).

### 9.6.1 Journal du module applicatif

La commande suivante permet de sauvegarder le journal du module.

<code>safekit logsave -m AM [-A] [-l en fr ja] /tmp/f.txt</code>	<p>Sauvegarde des principaux messages du journal du module <code>AM</code> dans <code>/tmp/f.txt</code> (chemin absolu obligatoire).</p> <p><b>Journal verbeux</b> Utiliser <code>-A</code> pour sauvegarder le journal qui contient tous les messages (y compris les messages de debug).</p> <p><b>Langue</b> Sélectionner la langue avec l'option <code>-l</code>, <code>en</code> (Anglais), <code>fr</code> (Français), <code>ja</code> (Japonais). Par défaut, la langue de l'OS est appliquée.</p>
--	--

### Journal anonymisé

Depuis SafeKit 8.2.6, SafeKit offre l'anonymisation des snapshots du module, en particulier celle du journal du module. Pour construire le snapshot anonymisé et en extraire le journal du module anonymisé, voir la [section 9.9.4.2](#).

### 9.6.2 Snapshot d'un module applicatif

#### 9.6.2.1 Snapshot complet



Voir l'exemple dans la [section 9.9.4.1](#).

<pre>safekit snapshot -m AM /tmp/snapshot_xx.zip</pre>	<p>Sauvegarde le snapshot du module <i>AM</i> dans <code>/tmp/snapshot_xx.zip</code>. Si seul le nom du fichier est spécifié, sans son chemin absolu, le snapshot est généré dans le répertoire <code>SAFEVAR/snapshot/tmp</code>.</p> <p>Un snapshot crée un dump puis récolte sous <code>SAFEVAR/snapshot/modules/AM</code> les 3 derniers dumps et les 3 dernières configurations du module pour les mettre dans le fichier <code>.zip</code></p> <p>Pour analyser les snapshots, voir la <a href="#">section 7.18</a>. Pour obtenir l'assistance du support, créer un incident via <a href="#">portail du support</a>, sans oublier d'y attacher les snapshots.</p> <p>Depuis SafeKit 8.2.4, les zips générés pour les snapshots sont protégés par le mot de passe <code>safekit</code>. Ceci permet de réceptionner le snapshot dans sa totalité lorsqu'il est envoyé dans un courriel.</p>
<pre>safekit dump -m AM</pre>	<p>Pour relever un problème en temps réel sur un serveur, générer un dump du module <i>AM</i></p> <p>Un dump crée un directory <code>dump_year_month_day_hour_mn_sec</code> du côté serveur sous <code>SAFEVAR/snapshot/modules/AM</code>. Le directory <code>dump</code> contient les logs et l'état du module et ainsi que des informations sur l'état du système et des processus SafeKit au moment du dump</p>

Le contenu du snapshot d'un module est décrit dans la [section 7.18](#).

#### 9.6.2.2 Snapshot anonymisé

Depuis SafeKit 8.2.6, SafeKit propose l'outil `anontool` qui permet de générer à partir d'un snapshot complet, un snapshot filtré et anonymisé. Celui-ci peut ensuite être transmis à des tiers, tel que le support SafeKit, tout en limitant la divulgation d'informations sensibles sur le cluster.



Voir l'exemple dans la [section 9.9.4.2](#).

Le snapshot filtré contient le sous-ensemble minimal pour permettre l'analyse d'un problème :

- o la configuration du cluster et du module

- o le journal du module, les journaux des scripts du module et le journal des commandes SafeKit

Si nécessaire, l'outil `anontool` offre la possibilité d'exclure davantage de fichiers du snapshot filtré (paramètre `-fileexclusionpattern`).

Chacun de ces fichiers est anonymisé. Les valeurs sensibles qu'ils contiennent (adresses IP, noms d'hôte, etc.) sont remplacées par un identifiant structuré, permettant de masquer la donnée réelle tout en conservant la possibilité d'analyse par le support.

Les correspondances (mappings) entre les valeurs originales détectées dans le snapshot et leurs identifiants anonymisés sont stockées dans le fichier `xx-catalog.xml`. Ce catalogue doit être conservé localement mais n'est pas inclus dans le snapshot filtré. Il permet à l'utilisateur de :

- faire le lien entre les valeurs anonymisées éventuellement mentionnées par le support et leurs valeurs réelles,
- contrôler quelles valeurs ont été anonymisées.


Si l'utilisateur estime que d'autres valeurs devraient également être anonymisées, l'outil `anontool` accepte un catalogue additionnel pour compléter l'anonymisation par défaut (paramètre `-additionalcatalogfile`).

Le snapshot original doit également être conservé. Comme le contenu du snapshot transmis au support est filtré, certaines analyses ne peuvent être effectuées uniquement à partir de celui-ci (notamment concernant la réplication de fichiers ou la configuration réseau). Le support peut donc être amené à solliciter l'utilisateur afin qu'il effectue lui-même des vérifications complémentaires à partir du snapshot original.

<pre>safekit -r anontool anonymize-snapshot  -insnapshotfile snapshot.zip  [-outsnapshotfile snapshot-anon.zip]  [-additionalcatalogfile extracatalog.xml] [-fileexclusionpattern 'pattern.*']</pre>	<p>Construit le snapshot filtré et anonymisé à partir du snapshot complet <code>snapshot.zip</code>. L'exécution de la commande demande la saisie du mot de passe qui protège le snapshot (<code>safekit</code>). Le snapshot généré est lui-même protégé par ce même mot de passe.</p> <ul style="list-style-type: none"> <li>• <code>-insnapshotfile snapshot.zip</code> Paramètre obligatoire pour spécifier le nom snapshot en entrée</li> <li>• <code>-outsnapshotfile snapshot-anon.zip</code> Paramètre optionnel pour spécifier le nom du snapshot et du catalogue XML générés. Par défaut, rajoute le suffixe <code>-anon</code> au nom du snapshot en entrée : <code>snapshot-anon.zip</code> et <code>snapshot-anon-catalog.xml</code></li> <li>• <code>-additionalcatalogfile extracatalog.xml</code> Paramètre optionnel pour spécifier un catalogue additionnel pour compléter l'anonymisation par défaut. Par exemple, pour anonymiser la version de l'OS :</li> </ul> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;catalog&gt;   &lt;other_addr&gt;</pre>
--	--

	<pre>&lt;value original="Microsoft Windows Server 2019 Standard [64-bit] (10.0.17763 )" anonymized="OS"/&gt; &lt;/other_addr&gt; &lt;/catalog&gt;</pre> <p>Cette option peut également être utile lorsque les noms de nœuds du cluster ont changé depuis la première mise en production. Pour s'assurer que les anciens noms, <code>server1</code> et <code>server2</code>, n'apparaissent pas dans les journaux, utilisez le catalogue additionnel du type suivant :</p> <pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt; &lt;catalog&gt;   &lt;other_addr&gt;     &lt;value original="server1"       anonymized="OLDNODE1NAME"/&gt;     &lt;value original="server2"       anonymized="OLDNODE2NAME"/&gt;   &lt;/other_addr&gt; &lt;/catalog&gt;</pre> <ul style="list-style-type: none"> <li>• <code>-fileexclusionpattern 'pattern.*'</code></li> </ul> <p>Paramètre optionnel pour spécifier une expression régulière sur les noms de fichiers/répertoires à exclure du snapshot.</p> <p>Par exemple, pour exclure tous les journaux des scripts du module :</p> <pre>-fileexclusionpattern 'userlog.*'</pre> <p>Pour exclure en plus les scripts du module :</p> <pre>-fileexclusionpattern 'userlog.*' -fileexclusionpattern 'bin'</pre> <p>ou</p> <pre>-fileexclusionpattern 'userlog.* module/bin'</pre> <p>Le moteur d'évaluation de l'expression régulière est la bibliothèque PCRE2 (Perl Compatible Regular Expressions 2) avec l'algorithme DFA.</p>
<pre>safekit -r anontool -help</pre>	<p>Liste toutes les usages proposés par <code>anontool</code>.</p>

### 9.6.3 Autres commandes

<pre>safekit -r "commande spéciale"</pre>	<p>Exécute une commande sous <code>SAFEBIN</code> après avoir instancié les variables d'environnement SafeKit</p>
<pre>safekit clean [all   log   process   resource] [-m AM]</pre>	<p>Réinitialise les journaux, le fichier de ressources et arrête les principaux processus associés au module.</p> <p> Cette commande doit être utilisée avec précautions puisqu'elle détruit des fichiers de travail et arrête des processus du module.</p>

	<ul style="list-style-type: none"> <li>• <code>safekit clean log -m AM</code> Détruit les journaux du module (verbeux et non verbeux). A utiliser si les journaux sont corrompus (exemple : erreurs retournées lors de l’affichage du journal).</li> <li>• <code>safekit clean resource -m AM</code> Réinitialise le fichier de ressources du module. A utiliser si ce fichier est corrompu (exemple : erreurs retournées lors de l’affichage des ressources).</li> <li>• <code>safekit clean process -m AM</code> Arrête les principaux processus du module (<code>heart</code>). A utiliser lorsqu’à l’issue du <code>stop</code> et du <code>forcestop</code> du module des processus n’ont pas été arrêtés.</li> <li>• <code>safekit clean all -m AM</code> Valeur par défaut. « Nettoie » les journaux, le fichier de ressources et les processus.</li> </ul>
--	--

## 9.7 Commandes lors de la maintenance de l’application du module

Lors de la maintenance ou des tests de l’application, il peut être nécessaire d’arrêter ou de redémarrer les services associés. Cependant, si le module est configuré pour surveiller l’application (surveillance des processus/services, checkers), ces opérations entraîneront une détection d’erreur erronée et un redémarrage automatique ou un basculement du module. Pour éviter cela, suivez l’une des deux solutions décrites ci-dessous.


### 9.7.1 Contrôle du module lors de la maintenance


Les commandes suivantes permettent de modifier dynamiquement le comportement du module sans nécessiter sa reconfiguration.

Les commandes s’appliquent au module nommé *AM*, passé en argument avec l’option `-m`.



Lorsque la variable d’environnement `SAFEMODULE` est définie avec le nom du module, l’argument `-m` n’est pas nécessaire. Celle-ci est définie lors de l’exécution des scripts du module (voir [section 14.2](#)).

<pre>safekit errd off -m AM safekit errd on -m AM</pre>	<p>Désactive/active la surveillance des processus/services définie dans la configuration du module.</p> <p>La ressource <code>usersetting.errd</code> reflète l’état courant.</p> <p> Avec SafeKit &lt; 8.2, utiliser la commande <code>safekit errd suspend resume -m AM</code></p>
<pre>safekit checker off -m AM safekit checker on -m AM</pre>	<p>Désactive/active l’ensemble des checkers (interface, TCP, IP, custom...) définis dans la configuration du module.</p>

	La ressource <i>usersetting.checker</i> reflète l'état courant.
<pre>safekit boot off -m AM safekit boot on -m AM</pre>	<p>Désactive/active le démarrage automatique au boot du module.</p> <p>La ressource <i>usersetting.boot</i> reflète l'état courant.</p>
<pre>safekit boot status [-m AM]</pre>	Sans l'option <code>-m AM</code> , <code>safekit boot status</code> liste l'état de tous les modules au boot.
<pre>safekit failover off -m AM safekit failover on -m AM</pre>	<p>Désactive/active le basculement automatique du module (voir <a href="#">section 13.3.3</a>).</p> <p>La ressource <i>usersetting.failover</i> reflète l'état courant.</p> <p> Cette commande doit être exécutée sur tous les nœuds du module. Si ce n'est pas le cas le comportement n'est pas spécifié</p>

Pour consulter l'état des ressources, voir la [section 7.4](#).



Si le module est démarré, un effet de bord de ces commandes (excepté `safekit boot`) est d'effectuer un `update` du module pour prendre en compte dynamiquement la désactivation/activation.

Avec SafeKit < 8.2, ces commandes (excepté `safekit boot`) ne pouvaient être exécutées que lorsque le module était démarré et dans un état stable. De plus, les options de configuration du module étaient restaurées une fois le module arrêté puis redémarré.



Depuis SafeKit 8.2, ces commandes peuvent être exécutées lorsque le module est arrêté et ne sont pas réinitialisées lorsque le module s'arrête et redémarre. Pour restaurer l'état initial, il faut soit exécuter la commande correspondante, soit réappliquer la configuration du module.

### 9.7.2 Exécution de l'application sans le module

Plutôt que de démarrer le module et de désactiver les vérificateurs, vous pourriez vouloir lancer uniquement l'application sans les processus du module. Pour cela, arrêtez le module et exécutez les scripts suivants, appelés wrappers. Ces scripts sont générés lors de chaque configuration du module dans le répertoire `SAFE/private/modules/AM/bin`.

<code>AM_start_wrapper</code>	<ul style="list-style-type: none"> <li>configure les adresses IP virtuelles définies dans la configuration du module</li> <li>démarré l'application en exécutant les scripts <code>start_prim</code> OU <code>start_both</code></li> </ul>
<code>AM_stop_wrapper</code>	<ul style="list-style-type: none"> <li>arrête l'application en exécutant les scripts <code>stop_prim</code> OU <code>stop_both</code></li> <li>déconfigure les adresses IP virtuelles définies dans la configuration du module</li> </ul>



L'extension de nom de fichier des wrappers est `.ps1` en Windows ; `.sh` en Linux

## 9.8 Commandes distribuées sur plusieurs serveurs SafeKit

SafeKit offre une ligne de commande permettant son exécution sur plusieurs serveurs SafeKit. Chacun des serveurs doit exécuter le service web de SafeKit (voir [section 10.9](#)).



Le mot de passe affecté à l'initialisation du service web de SafeKit, doit être le même sur tous serveurs, même s'ils n'appartiennent pas au même cluster SafeKit.

La commande distribuée s'applique aux serveurs spécifiés avec l'argument `-H` "`<hosts>`" décrit ci-dessous.

<pre>-H "*"  -H "&lt;cluster node names list&gt;"</pre>	<p>La commande s'applique à des nœuds définis dans la configuration locale du cluster (voir <a href="#">section 12</a>).</p> <p>Le protocole et le port sont ceux définis dans la configuration locale du service web de SafeKit. Par défaut, protocole <code>http</code> et port <code>9010</code>.</p> <ul style="list-style-type: none"> <li>• <code>-H "*"        Pour tous les nœuds du cluster</code></li> <li>• <code>-H "&lt;cluster node names list&gt;"        Liste des noms de nœuds tels qu'ils sont définis dans la configuration locale du cluster, avec la virgule comme séparateur. Par exemple :</code> <pre>-H "node1,node2"</pre> </li> </ul>
<pre>-H "[[protocol:port],] &lt;servers list&gt;"</pre>	<p>La commande s'applique aux serveurs listés, qui n'appartiennent pas forcément au cluster local.</p> <ul style="list-style-type: none"> <li>• Spécification optionnelle du protocole (<code>http</code> ou <code>https</code>) et du port à utiliser. Par exemple :</li> </ul> <p>Si ce n'est pas spécifié, le protocole et le port sont ceux définis dans la configuration locale du service web de SafeKit. Par défaut, protocole <code>http</code> et port <code>9010</code>.</p> <ul style="list-style-type: none"> <li>• Liste des serveurs SafeKit (adresse IP ou nom) avec la virgule comme séparateur.</li> </ul> <p>Exemples:</p> <pre>-H "10.0.0.107" -H "[http:9500],10.0.0.107,10.0.0.108" -H "[https],S1.company.com,S2.company.com"</pre>
<pre>-H "&lt;urls list&gt;"</pre>	<p>La commande s'applique aux URLs listées, qui n'appartiennent pas forcément au cluster local.</p> <p>Exemple :</p>

```
-H "http://192.168.0.2:9010,http://192.168.0.3:9010"
```

Les commandes distribuées sont les suivantes.



Voir les exemples dans la [section 9.9.1](#), [section 9.9.2](#), la [section 9.9.3](#).

<pre>safekit -H "&lt;hosts&gt;" &lt;safekit command arguments&gt;</pre>	<p>Exécute la commande <code>safekit</code> sur les serveurs spécifiés par <code>-H</code>.</p> <p>A peu près toutes les commandes SafeKit peuvent être appliquées sur une liste de serveurs.</p> <p>Les exceptions sont les commandes <code>safekit logview</code>, <code>safekit -p</code> et <code>safekit -r</code> qui ne peuvent être exécutées que localement.</p> <p><b>Exemples :</b></p> <pre>safekit -H "http://192.168.0.2:9010,http://192.168.0.3:9010" level  safekit -H "*" cluster confinfo  safekit -H "node2" module list  safekit -H "[http:9500],server1,server2" start -m AM</pre>
<pre>safekit -H "&lt;hosts&gt;" -E AM</pre>	<p>Exporte la configuration du module nommé <code>AM</code> sur les serveurs spécifiés par <code>-H</code>. Le module <code>AM</code> doit être installé localement.</p> <p>Cette commande réalise les actions suivantes :</p> <ul style="list-style-type: none"> <li>• Crée <code>AM.safe</code> à partir du module local <code>SAFE/modules/AM</code> et note son id</li> <li>• Transfère et installe <code>AM.safe</code> sur les serveurs distants</li> <li>• Installe le module sur les serveurs distants avec l'id local du module</li> <li>• Si le module était configuré localement, configure le module sur les serveurs distants</li> </ul> <p> Voir l'exemple dans la <a href="#">section 9.9.3</a>.</p>
<pre>safekit -H "&lt;hosts&gt;" - G</pre>	<p>Exporte la configuration locale du cluster sur les serveurs spécifiés par <code>-H</code>.</p> <p>Cette commande réalise les actions suivantes :</p> <ul style="list-style-type: none"> <li>• Collecte le contenu du répertoire <code>SAFEVAR/cluster</code></li> </ul>

- Transfère les fichiers collectés dans le répertoire `SAFEVAR/cluster` des serveurs distants
- Déclenche le rechargement de la configuration de `safeadmin`.



Voir l'exemple dans la [section 9.9.2](#).

## 9.9 Exemples

### 9.9.1 Commande locale et distribuée

Par exemple, pour afficher la version (SafeKit, OS...) :

- Pour le nœud local

```
safekit level
```

- Pour tous les nœuds configurés dans le cluster SafeKit

```
safekit -H "*" level
```

### 9.9.2 Configuration globale du cluster en ligne de commande

Voir la [section 12.2.2](#).

### 9.9.3 Configuration globale d'un module applicatif en ligne de commande

Les commandes en ligne équivalentes à l'assistant de configuration du module sont listées ci-dessous. Remplacer *AM* par le nom de votre module ; *node1* et *node2* par le nom de vos nœuds tels que définis lors de la configuration du cluster SafeKit.

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes

Se connecter par exemple sur *node1*

2. aller dans le répertoire `SAFE`

`SAFE` vaut `C:\safekit` en Windows quand `%SYSTEMDRIVE%=C:`, `/opt/safekit` en Linux

3. Optionnel

A la première configuration uniquement, exécuter

```
safekit module install -m AM mirror.safe
```

pour installer un nouveau module nommé *AM* à partir du modèle `mirror.safe` localisé dans le répertoire `SAFE/Application_Modules/generic`.

Cela n'est pas nécessaire lors de la reconfiguration d'un module déjà installé.

4. Éditer la configuration du module et les scripts sous `SAFE/modules/AM/conf` et `SAFE/modules/AM/bin`

5. Optionnel

Exécuter

```
safekit module genkey -m AM ou safekit module delkey -m AM
```

pour créer ou détruire les clés d'encryption du module.

Il n'est pas nécessaire de créer une nouvelle clé d'encryption à la reconfiguration du module.

### 6. Exécuter

```
safekit -H "node1,node2" -E AM
```

pour (ré)installer le module *AM* et appliquer sa configuration qui est stockée sur le nœud qui exécute cette commande (*node1* dans cet exemple). Elle est appliquée sur tous les nœuds listés (*node1* et *node2*).

## 9.9.4 Snapshot d'un module applicatif en ligne de commande

### 9.9.4.1 Snapshot complet

Ci-dessous, remplacer *AM* par le nom de votre module ; *node1* et *node2* par le nom de des nœuds de votre cluster SafeKit.

1. se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes

se connecter par exemple sur *node1*

2. aller dans le répertoire *SAFE*

*SAFE* vaut *C:\safekit* en Windows quand *%SYSTEMDRIVE%=C:*, */opt/safekit* en Linux

3. Exécuter

```
safekit snapshot -m AM /tmp/snapshot_node1_AM.zip
```

Pour sauvegarder localement le snapshot du module *AM* (cad sur *node1*) dans le zip passé en paramètre.

**Répéter** ces commandes sur tous les nœuds du module.

### 9.9.4.2 Snapshot anonymisé

Ci-dessous, remplacer *AM* par le nom de votre module ; *node1* et *node2* par le nom de des nœuds de votre cluster SafeKit.

1. se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes

se connecter par exemple sur *node1*.

2. aller dans le répertoire *SAFE*

*SAFE* vaut *C:\safekit* en Windows quand *%SYSTEMDRIVE%=C:*, */opt/safekit* en Linux

3. Exécuter

```
safekit snapshot -m AM /tmp/snapshot_node1_AM.zip
```

Pour sauvegarder localement le snapshot complet du module *AM*.

4. Exécuter

```
safekit -r anontool anonymize-snapshot -insnapshotfile /tmp/snapshot_node1_AM.zip
```

Pour construire le snapshot anonymisé et le catalogue associé dans le répertoire courant avec les noms par défaut *snapshot\_nodes1\_AM-anon.zip* et *snapshot\_nodes1\_AM-anon-catalog.xml*.

L'exécution de cette commande demande la saisie du mot de passe qui protège le snapshot complet (`safekit`). Le snapshot généré est lui-même protégé par ce même mot de passe.

Conservez le snapshot complet ainsi que le catalogue de correspondances entre valeurs originales et valeurs anonymisées.

Voir la [section 9.6.2.2](#) pour la description des snapshots anonymisés.

**Répéter** ces commandes sur tous les nœuds du module.

Si vous souhaitez envoyer au support uniquement le journal du module anonymisé, suivez cette procédure et extrayez du zip généré les fichiers `logverbose.txt` et `anoncatalog.xml`. Cet extrait du catalogue d'anonymisation (sans les valeurs d'origine) permet au support de mieux interpréter les valeurs anonymisées dans le journal.



## 10. Administration et configuration avancées

- ⇒ [Section 10.1](#) « Variables d'environnement et répertoires SafeKit »
- ⇒ [Section 10.2](#) « Services/démons SafeKit et communications »
- ⇒ [Section 10.3](#) « Paramétrage du pare-feu »
- ⇒ [Section 10.4](#) « Configuration au boot et au shutdown en Windows »
- ⇒ [Section 10.5](#) « Paramétrage de Secure Boot en Linux pour les modules kernel SafeKit »
- ⇒ [Section 10.6](#) « Paramétrage des antivirus »
- ⇒ [Section 10.7](#) « Cryptage des communications du module applicatif »
- ⇒ [Section 10.8](#) « Cryptage des fichiers sensibles dans SafeKit »
- ⇒ [Section 10.9](#) « Configuration du service web de SafeKit »
- ⇒ [Section 10.10](#) « Agent SafeKit de notification par courriel »
- ⇒ [Section 10.11](#) « Supervision SNMP »
- ⇒ [Section 10.12](#) « Journal des commandes du serveur SafeKit »
- ⇒ [Section 10.13](#) « Messages SafeKit dans le journal système »

### 10.1 Variables d'environnement et répertoires SafeKit


#### 10.1.1 Global

Variable	Description
<code>SAFE</code> (rendu par <code>safekit -p</code> )	Répertoire d'installation de SafeKit : <b>SAFE=/opt/safekit</b> sur Linux et <b>SAFE=C:\safekit</b> sur Windows si SystemDrive=C:  La licence est sous <b>SAFE/conf/license.txt</b>
<code>SAFEVAR</code> (rendu par <code>safekit -p</code> )	Répertoire des fichiers de travail de SafeKit : <b>SAFEVAR=C:\safekit\var</b> sur Windows et <b>SAFEVAR=/var/safekit</b> sur Linux
<code>SAFEBIN</code> (rendu par <code>safekit -p</code> )	Répertoire d'installation des binaires SafeKit : <b>C:\safekit\private\bin</b> sur Windows et <b>/opt/safekit/private/bin</b> sur Linux. Utile pour accéder aux commandes spéciales de SafeKit
<code>SAFE/Application_Modules</code>	Répertoire des modules <code>.safe</code> installables.  Une fois un module installé, le module se trouve SOUS <b>SAFE/modules</b>

#### 10.1.2 Module applicatif

Variable	Description
----------	-------------

SAFEMODULE	Nom du module. La commande <code>safekit</code> n'a plus besoin du paramètre nom de module ( <code>-m AM = -m SAFEMODULE</code> )
SAFE/Application_Modules	<p>Répertoire des modules contenant les <code>.safe</code> installables.</p> <p>Une fois un module installé, le module se trouve sous <b>SAFE/modules</b></p>
SAFE/modules/AM	<p>Les fichiers de configuration d'un module, nommé <i>AM</i>, se trouvent dans le répertoire <b>SAFE/modules/AM</b> :</p> <ul style="list-style-type: none"> <li>• SOUS <b>SAFE/modules/AM/conf</b>, le fichier <code>userconfig.xml</code></li> <li>• SOUS <b>SAFE/modules/AM/bin</b>, entre autres, les scripts de démarrage et d'arrêt applicatif : <ul style="list-style-type: none"> <li>o <code>start_prim</code>, <code>stop_prim</code> pour un miroir,</li> <li>o <code>start_both</code>, <code>stop_both</code> pour une ferme</li> </ul> </li> </ul> <p>Ces fichiers peuvent être édités directement ou via la console SafeKit. À chaque modification, la configuration doit être appliquée sur tous les nœuds du cluster sur lesquels le module est installé pour être prise en compte.</p>
SAFEUSERBIN SAFEUSERCONF	<p>Une fois le module configuré avec succès, ses fichiers de configuration sont automatiquement copiés dans le répertoire privé <b>SAFE/private/modules/AM</b>. Ce répertoire, utilisé par le runtime SafeKit, ne doit en aucun cas être modifié. Toutefois, les scripts du module peuvent y accéder en lecture seule via les variables d'environnement :</p> <ul style="list-style-type: none"> <li>• <b>SAFEUSERBIN</b> pointe vers <b>SAFE/private/modules/AM/bin</b>, permettant l'accès aux scripts du module</li> <li>• <b>SAFEUSERCONF</b> pointe vers <b>SAFE/private/modules/AM/conf</b>, permettant l'accès au fichier <code>safeconf.xml</code>, qui contient l'intégralité de la configuration XML du module après l'instanciation des macros</li> </ul>
SAFEVAR/modules/AM SAFEUSERVAR	<p>Le répertoire <b>SAFEVAR/modules/AM</b>, accessible via la variable d'environnement <b>SAFEUSERVAR</b>, contient les fichiers de travail du module, nommé <i>AM</i>.</p> <p>Ce répertoire héberge notamment les fichiers de log générés par les scripts du module. Ces fichiers sont nommés selon le format suivant :</p>

	<p>userlog_&lt;year&gt;_&lt;month&gt;_&lt;day&gt;T&lt;time&gt;_&lt;script name&gt;.u.log. Ils permettent de consulter les messages de sortie des scripts, notamment pour vérifier la présence d'éventuelles erreurs lors du démarrage ou de l'arrêt de l'application.</p> <p> Le userlog peut être désactivé dans le userconfig.xml du module avec : &lt;user logging="none"&gt;.</p>
SAFEVAR/snapshot/modules/AM	Ce répertoire contient les 3 derniers dumps et configurations du module, nommé AM. Ceux-ci sont collectés dans le snapshot du module (voir <a href="#">section 9.6</a> )

L'arborescence d'un module (empaqueté dans un .safe ou installé dans SAFE/modules/AM) est la suivante :

AM	Nom du module applicatif
<ul style="list-style-type: none"> <li>└─ conf           <ul style="list-style-type: none"> <li>└─ userconfig.xml</li> <li>└─ userconfig.xml.template</li> <li>└─ modulekey.p12</li> <li>└─ modulekey.dat</li> </ul> </li> <li>└─ bin           <ul style="list-style-type: none"> <li>└─ prestart</li> <li>└─ start_prim or start_both</li> <li>└─ stop_prim or stop_both</li> <li>└─ poststop</li> </ul> </li> <li>└─ web           <ul style="list-style-type: none"> <li>└─ index.html</li> </ul> </li> <li>└─ manifest.xml</li> </ul>	<p>Fichier XML de configuration utilisateur</p> <p>Obsolète (fichier pour la console web de SafeKit &lt; 8)</p> <p>Optionnel. Usage interne uniquement (chiffrement des communications internes du module)</p> <p>Optionnel. Usage interne uniquement (chiffrement des communications internes du module)</p> <p>Script du module exécuté au démarrage du module</p> <p>Script du module pour démarrer l'application en miroir ou ferme</p> <p>Script du module pour arrêter l'application en miroir ou ferme</p> <p>Script du module exécuté à l'arrêt du module</p> <p>Obsolète (fichier pour la console web de SafeKit &lt; 8)</p> <p>Obsolète</p>

Depuis SafeKit 8, vous ne pouvez plus personnaliser l'affichage de la configuration rapide du module (puisque `index.html` est obsolète).

### 10.2 Services/démons SafeKit et communications

SafeKit repose sur différents services et démons par module applicatif s'exécutant sur les nœuds du cluster SafeKit. Les communications entre ces processus, à travers les nœuds, peuvent être sécurisées à l'aide d'OpenSSL :

- en Windows, SafeKit embarque la bibliothèque OpenSSL dans son package. La version installée peut être obtenue à l'aide de la commande `SAFE\web\bin\openssl.exe version` où `SAFE=C:\safekit` (si `%SYSTEMDRIVE%=C:`).
- en Linux, SafeKit s'appuie sur la bibliothèque OpenSSL fournie par le système d'exploitation. La version installée peut être obtenue à l'aide de la commande `openssl version`.

Cette section liste :

- les noms des processus SafeKit et leurs ports associés pour les communications externes
- les mécanismes de chiffrement basés sur OpenSSL
- les exigences en matière de pare-feu

Elle sert de référence pour la configuration des règles de pare-feu et la validation des communications sécurisées entre les nœuds du cluster et les clients externes.



La version de la bibliothèque OpenSSL sous Windows ainsi que les niveaux de chiffrement utilisés peuvent évoluer avec les nouvelles versions de SafeKit. Pour obtenir les informations les plus à jour, reportez-vous au [Software Release Bulletin](#).

#### 10.2.1 Services SafeKit

Pour les commandes de contrôle des services SafeKit, voir [section 9.1](#).



En Windows, les noms de processus ont comme extension `.exe`.

##### 10.2.1.1 Service `safeadmin`

**Processus** : `safeadmin`

**Description** : Service principal requis pour la gestion du cluster SafeKit (voir la [section 12.1.3](#) les détails de configuration du port)

**Protocol / port** : UDP 4800

**Pare-feu** : Autoriser les communications entre les nœuds du cluster

**Chiffrement** : Activé (chiffrement symétrique AES-128-CBC avec intégrité SHA256)

##### 10.2.1.2 Service `safewebserver`

**Processus** : `httpd` (Apache HTTP server)

**Description** : Fournit les services web pour la console SafeKit, les module checkers et l'interface en ligne de commande distribuée (voir la [section 10.9](#) pour les détails de

configuration). Il fournit également des sondes de supervision de l'état des modules (voir [section 13.6.3](#) et [section 16](#))

**Protocol / port :**

- TCP 9010 (HTTP, défaut)
- TCP 9453 (HTTPS)

**Pare-feu :** Autoriser pour la commande distribuée entre les nœuds du cluster, pour les clients de la console Web et les module checkers

**Chiffrement :**

- HTTP (défaut) : désactivé
- HTTPS : TLS 1.3 (TLS 1.2 optionnel)  
(voir la [section 11.3](#) pour la configuration HTTPS)

### 10.2.1.3 Service SNMP

#### 10.2.1.3.1 Service Net-SNMP Agent en Windows

**Processus :** `safeagent`

**Description :** Agent SNMP optionnel pour la supervision de SafeKit (voir la [section 10.11](#) pour la configuration de la supervision SNMP)

**Protocol / port :** UDP 3600 (SNMP v2)

**Pare-feu :** Autoriser pour les clients SNMP

**Chiffrement :** -

#### 10.2.1.3.2 Service `snmpd` en Linux

Agent SNMP optionnel pour la supervision de SafeKit basé sur le service standard `snmpd` (voir la [section 10.11](#) pour la configuration de la supervision SNMP).

#### 10.2.1.4 `safecaserv` service

**Processus :** `httpd` (Apache HTTP server)

**Description :** Service web optionnel permettant la génération de certificats à l'aide de la PKI SafeKit (voir la [section 11.3.1.8.5](#) pour les détails de configuration).

**Protocol / port :** TCP 9001 (HTTPS)

**Pare-feu :** Autoriser les communications entre les nœuds du cluster

**Chiffrement :** TLS 1.3

## 10.2.2 Démons SafeKit par module applicatif

Par défaut, les communications inter-nœuds des modules ne sont pas chiffrées. Pour activer le chiffrement, voir la [section 10.7](#).

Les valeurs des ports pour un module sont automatiquement calculées en fonction de son identifiant (`id`). Exécuter la commande `safekit module listid` pour lister tous les modules installés avec leur nom et leur identifiant.

### 10.2.2.1 Module applicatif miroir

Pour lister les ports utilisés par le module miroir nommé *AM*, exécutez la commande `safekit module getports -m AM`. Par exemple, si le module a l'identifiant 1, la commande retourne :

List of the ports used by SafeKit

```
Process    Ports
safeadmin
  port    UDP 4800

webconsole
  port    TCP 9010
heart
  port    UDP 8888
rfs
  safenfs_port    TCP 5600
```



Dans la suite, les noms de processus ont comme extension `.exe` en Windows.

#### 10.2.2.1.1 Gestion de l'état du module et des heartbeat

**Processus :** `heart`

**Description :** Gère les communications inter-nœuds (heartbeat), l'automate d'état du module et le contrôle du basculement (voir la [section 13.4](#) pour plus de détails)

**Protocol / port :** UDP 8888 +(id-1) (`heart port`)

**Pare-feu :** Autoriser les communications entre les nœuds du cluster

**Chiffrement :**

- Défaut : désactivé
- Optionnel : activé (chiffrement symétrique AES-128-CBC avec intégrité SHA256)

#### 10.2.2.1.2 Gestion de la réplication de fichiers

**Processus :** `nfsbox`, `reintegre`

**Description :** Gère la réplication en temps réel et la synchronisation des données entre les nœuds du cluster (voir la [section 13.7](#) pour plus de détails)

**Protocol / port :** TCP 5600 +(id-1) x 4 (`safenfs_port`)

**Pare-feu :** Autoriser les communications entre les nœuds du cluster

**Chiffrement :**

- Défaut : désactivé
- Optionnel : activé (TLS 1.3)

**Processus :** `nfsadmin`

**Description :** gestionnaire de la réplication de fichiers

**Protocol / port :** -

**Pare-feu :** -

**Chiffrement :** -

### 10.2.2.1.3 Gestion de l'IP virtuelle

**Processus :** `arpreroute`

**Description :** Émet automatiquement des paquets ARP gratuits pour les adresses IP virtuelles IPv4 afin d'accélérer le basculement (voir la [section 13.6](#) pour plus de détails)

**Protocole / port :** ARP

**Pare-feu :** -

**Chiffrement :** -

### 10.2.2.2 Module applicatif ferme

Pour lister les ports utilisés par le module ferme nommé *AM*, exécutez la commande `safekit module getports -m AM`. Par exemple, si le module a l'identifiant 2, la commande retourne :

List of the ports used by SafeKit

Process	Ports
safeadmin	
port	UDP 4800
webconsole	
port	TCP 9010
farm	
port	UDP 4806



Dans la suite, les noms de processus ont comme extension `.exe` en Windows.

#### 10.2.2.2.1 Gestion de l'IP virtuelle et du load balancing

**Processus :** `vipd`

**Description :** Gère les communications inter-nœuds au sein de la ferme (heartbeat) et contrôle l'équilibrage de charge (voir la [section 13.6](#) pour plus de détails)

**Protocole / port :**  $\text{UDP } 4803 + (\text{id}-1) \times 3$  (*farm port*)

**Pare-feu :** Autoriser les communications entre les nœuds du cluster

**Chiffrement :**

- Défaut : désactivé
- Optionnel : activé (chiffrement symétrique AES-128-CBC avec intégrité SHA256)

**Processus :** `arpreroute`

**Description :** Émet automatiquement des paquets ARP gratuits pour les adresses IP virtuelles IPv4 afin d'accélérer le basculement (voir la [section 13.6](#) pour plus de détails)

**Protocole / port :** ARP

**Pare-feu :** -

**Chiffrement :** -

### 10.2.2.3 Checkers pour les modules applicatifs miroir et ferme



Dans la suite, les noms de processus ont comme extension `.exe` ou `.ps1` en Windows.

#### 10.2.2.3.1 Checker de processus/service

**Processus :** `errd`

**Description :** Surveille les processus et services (voir la [section 13.10](#) pour plus de détails)

**Protocol / port :** -

**Pare-feu :** -

**Chiffrement :** -

#### 10.2.2.3.2 TCP checker

**Processus :** `tcpcheck`

**Description :** Vérifie une connexion TCP vers l'adresse et le port configurés (voir la [section 13.12](#) pour plus de détails)

**Protocol / port :** TCP port cible

**Pare-feu :** Autoriser le trafic TCP entrant sur l'adresse et le port cibles

**Chiffrement :** -

#### 10.2.2.3.3 Ping checker

**Processus :** `pingcheck`

**Description :** Envoie des requêtes ICMP (echo) vers l'adresse configurée (voir la [section 13.13](#) pour plus de détails)

**Protocol / port :** ICMP

**Pare-feu :** Autoriser le trafic ICMP entrant sur l'adresse cible

**Chiffrement :** -

#### 10.2.2.3.4 Interface checker

**Processus :** `intfcheck`

**Description :** Teste une interface réseau (voir la [section 13.14](#) pour plus de détails)

**Protocol / port :** -

**Pare-feu :** -

**Chiffrement :** -

#### 10.2.2.3.5 IP checker

**Processus :** `ipcheck`

**Description :** Vérifie l'IP configurée (voir la [section 13.15](#) pour plus de détails)

**Protocol / port :** -

**Pare-feu :** -

**Chiffrement :** -

### 10.2.2.3.6 Module checker

**Processus :** modulecheck

**Description :** Vérifie l'état d'un module applicatif (voir la [section 13.17](#) pour les détails de configuration)

**Protocole / port :**

- TCP 9010 (HTTP, défauts)
- TCP 9453 (HTTPS)

**Pare-feu :** Autoriser le trafic entrant vers le service `safewebserver` du nœud SafeKit cible

**Chiffrement :**

- HTTP (défaut) : désactivé
- HTTPS : TLS 1.3 (TLS 1.2 optionnel)

### 10.2.2.3.7 Splitbrain checker

**Processus :** splitbraincheck

**Description :** Envoie des requêtes ICMP (echo) vers les witness (voir la [section 13.18](#) pour plus de détails)

**Protocole / port :** ICMP

**Pare-feu :** Autoriser le trafic ICMP entrant sur les witness

**Chiffrement :** -

## 10.3 Paramétrage du pare-feu

Si un pare-feu est actif sur le serveur SafeKit, il faut ajouter les règles autorisant les échanges réseau :

- Entre les serveurs pour les communications internes (échanges globaux et échanges spécifiques aux modules)
- Entre les serveurs et les stations de travail exécutant la console

Voici ci-dessous la commande pour configurer le pare-feu Microsoft Windows sur Windows ; `firewalld/iptables` sur Linux. Si vous avez choisi la configuration automatique du pare-feu pendant l'installation de SafeKit, cette commande déjà été exécutée.

<pre>SAFE/private/bin/firewallcfg add</pre> <p>où</p> <pre>SAFE=C:\safekit en Windows (si %SYSTEMDRIVE%=C:)</pre> <pre>SAFE=/opt/safekit en Linux</pre>	<p>Sur tous les serveurs SafeKit :</p> <ol style="list-style-type: none"> <li>1. Ouvrir une console PowerShell/shell en tant qu'administrateur/root</li> <li>2. Exécuter <code>SAFE/private/bin/firewallcfg add</code></li> </ol> <p>Cela configure le pare-feu du système.</p>
---	---

Si vous utilisez un autre pare-feu ou souhaitez vérifier les règles par rapport à la politique locale, reportez-vous à la [section 10.2](#). Celle-ci répertorie les services et démons SafeKit par module nécessitant une configuration spécifique du pare-feu.

### 10.3.1 Paramétrage du pare-feu en Linux

Si la configuration automatique du pare-feu a été sélectionnée lors de l'installation de SafeKit, les commandes suivantes ne sont pas nécessaires.

Si la configuration automatique du pare-feu n'a été pas été faite, vous devez configurer le pare-feu.

Lorsque le pare-feu du système (firewalld/iptables) est utilisé, vous pouvez utiliser la commande `firewallcfg`. Celle-ci insère (ou supprime) les règles de pare-feu requises par les services SafeKit (`safeadmin` et `safewebserver`) et les modules.

Les administrateurs doivent s'assurer de l'absence de conflit avec une politique locale avant d'appliquer ces règles.

<pre>SAFE/private/bin/firewallcfg add SAFE/private/bin/firewallcfg del</pre> <p>où SAFE=/opt/safekit</p>	<p>Ajout (ou suppression) des règles pour le pare-feu firewalld ou iptable pour les ports des services <code>safeadmin</code> et <code>safewebserver</code></p> <ul style="list-style-type: none"> <li>SAFE/private/bin/firewallcfg add</li> </ul> <p>Ajout des règles pour les services <code>safeadmin</code> et <code>safewebserver</code></p> <ul style="list-style-type: none"> <li>SAFE/private/bin/firewallcfg del</li> </ul> <p>Suppression des règles pour les services <code>safeadmin</code> et <code>safewebserver</code></p>
<pre>SAFE/private/bin/firewallcfg add AM SAFE/private/bin/firewallcfg del AM</pre> <p>où SAFE=/opt/safekit</p>	<p>Ajout (ou suppression) des règles pour le pare-feu firewalld ou iptable pour les ports des modules SafeKit</p> <ul style="list-style-type: none"> <li>SAFE/private/bin/firewallcfg add <i>AM</i></li> </ul> <p>Ajout des règles pour le module nommé <i>AM</i></p> <ul style="list-style-type: none"> <li>SAFE/private/bin/firewallcfg del <i>AM</i></li> </ul> <p>Suppression des règles pour le module nommé <i>AM</i></p>

Depuis la version 8.2.5 de SafeKit, la commande `firewallcfg add` active également la configuration automatique du pare-feu pour les modules à leur configuration. Avant cette version, il fallait exécuter la commande `firewallcfg add AM` (où *AM* est le nom du module) :

- après la première configuration du module
- après les configurations suivantes si celles-ci modifient les ports utilisés (à vérifier avec la commande `safekit module getports -m AM`)

### 10.3.2 Paramétrage du pare-feu en Windows

Si la configuration automatique du pare-feu a été sélectionnée lors de l'installation de SafeKit, les commandes suivantes ne sont pas nécessaires.

Si la configuration automatique du pare-feu n'a été pas été faite, vous devez configurer le pare-feu.

Lorsque le pare-feu du système (Microsoft) est utilisé, vous pouvez utiliser la commande `firewallcfg`. Celle-ci insère (ou supprime) les règles de pare-feu requises par les services SafeKit (`safeadmin`, `safewebserver`, `safeacaserv` et `Net-SNMP Agent`) et les modules.

Les administrateurs doivent s'assurer de l'absence de conflit avec une politique locale avant d'appliquer ces règles.

<pre>SAFE/private/bin/firewallcfg add SAFE/private/bin/firewallcfg del</pre> <p>où <code>SAFE=C:\safekit</code> (si <code>%SYSTEMDRIVE%=C:</code>)</p>	<p>Ajout (ou suppression) des règles pour le pare-feu de Microsoft</p> <ul style="list-style-type: none"> <li><code>SAFE/private/bin/firewallcfg add</code></li> </ul> <p>Ajout des règles pour les services SafeKit et les modules</p> <ul style="list-style-type: none"> <li><code>SAFE/private/bin/firewallcfg del</code></li> </ul> <p>Suppression des règles pour les services SafeKit et les modules</p>
--	--

## 10.4 Configuration au boot et au shutdown en Windows

Le service `safeadmin` est configuré pour démarrer automatiquement au boot et s'arrêter proprement au shutdown. A son tour, ce service démarre les modules configurés pour démarrer au boot et arrête les modules.

Sur certaines plateformes Windows, le démarrage au boot de `safeadmin` échoue car la configuration réseau n'est pas prête ; au shutdown, les modules n'ont pas le temps de s'arrêter proprement car le délai d'attente de l'arrêt du service est trop court. Si vous rencontrez ce type de problème, appliquez l'une des procédures suivantes.



Si vous utilisez l'agent SNMP de SafeKit, adaptez la procédure suivante pour positionner le démarrage manuel du service `Net-SNMP Agent` et inclure son démarrage/arrêt dans les scripts de démarrage (`safekitbootstart.cmd`) et arrêt de SafeKit (`safekitshutdown.cmd`).

### 10.4.1 Procédure automatique

1. Ouvrir une console PowerShell en tant qu'administrateur
2. `cd SAFE\private\bin\`
3. Exécuter le script `addStartupShutdown.cmd`

Ce script positionne le démarrage manuel de `safeadmin` et ajoute dans les objets stratégies de groupe, les scripts de démarrage (`safekitbootstart.cmd`) et d'arrêt (`safekitshutdown.cmd`) de SafeKit. Si le script échoue, appliquez la procédure manuelle.

### 10.4.2 Procédure manuelle

Vous devez appliquer la procédure suivante qui utilise l'éditeur d'objets de stratégie de groupe :

1. Positionner en démarrage manuel le service `safeadmin`
2. Ouvrir une console PowerShell en tant qu'administrateur
3. Lancer la console MMC à l'aide de la commande `mmc`

4. Fichier - Ajouter/Supprimer un composant logiciel enfichable ; Ajouter - "Editeur d'objets de stratégie de groupe" - OK
5. Sous "Racine de la console"/"Stratégie ordinateur local"/"Configuration ordinateur"/"Paramètres Windows"/"Scripts (démarrage/arrêt)", double cliquer sur "Démarrage". Cliquer sur ajouter puis entrer pour le nom du script :  
`c:\safekit\private\bin\safekitbootstart.cmd`. Ce script lance le service `safeadmin`.
6. Sous "Racine de la console"/"Stratégie ordinateur local"/"Configuration ordinateur"/"Paramètres Windows"/"Scripts (démarrage/arrêt)", double cliquer sur "Arrêt du système". Cliquer sur ajouter puis entrer pour le nom du script :  
`c:\safekit\private\bin\safekitshutdown.cmd`. Ce script arrête proprement tous les modules en cours d'exécution.

### 10.5 Paramétrage de Secure Boot en Linux pour les modules kernel SafeKit

Lorsque Secure Boot est activé sous Linux, chaque module kernel doit être signé et enregistré dans l'UEFI.

Utiliser la commande suivante pour vérifier si le Secure Boot est activé :



```
mokutil --sb-state
```

```
SecureBoot enabled
```

Étant donné que SafeKit utilise les modules kernel `vip` et `tcpseq` pour implémenter le load balancing des modules ferme, ces modules kernel doivent également être signés et enregistrés. Sinon, leur chargement échouera lors du démarrage du module SafeKit avec le message suivant dans le journal du module :

```
| vipplug | E | Unable to load vip kernel extension
```

Par ailleurs, une tentative de chargement du module `vip` via la commande `modprobe vip` entraîne l'une des erreurs suivantes :

```
modprobe: ERROR: could not insert 'vip': Required key not available
```

ou

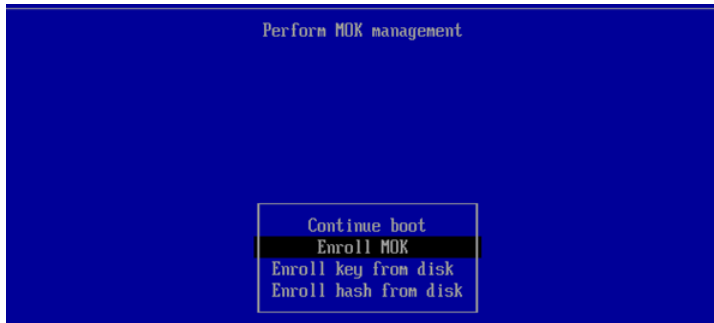
```
modprobe: could not insert 'vip': Key was rejected by service
```

Depuis SafeKit 8.2.4, pour utiliser le module ferme avec load balancing et Secure Boot activé, suivez la procédure décrite ci-dessous. Cette procédure doit être appliquée sur tous les nœuds SafeKit et peut être effectuée avant ou après la configuration du module ferme.

1. se connecter en tant que root et ouvrir un terminal
2. aller dans le répertoire `/opt/safekit/kernel`
3. exécuter la commande `make enroll`

Il vous sera demandé de créer un mot de passe. Souvenez-vous de ce mot de passe pour l'étape 5.

4. Rebooter le serveur
5. Au démarrage, l'UEFI demandera l'enregistrement de la nouvelle clé pour SafeKit :



Acceptez et entrez le mot de passe créé à l'étape 3. La procédure n'est nécessaire qu'après le premier reboot.

6. Une fois le reboot terminé, vous pouvez vérifier que la clé SafeKit a été enregistrée en exécutant :

```
mokutil --list-enroll | grep SafeKit
... SafeKit ...
```

Vous pouvez également vérifier que le module kernel `vip` peut être chargé sans erreurs en exécutant :

```
modprobe vip
```

Pour SafeKit < 8.2.4, suivre la procédure décrite dans [Q009176](#).

## 10.6 Paramétrage des antivirus

Les antivirus peuvent rencontrer des problèmes de détection avec SafeKit en raison de son intégration étroite avec le système d'exploitation, des mécanismes d'IP virtuelle, de la réplication en temps réel et du redémarrage des services critiques. Il peut alors être nécessaire de paramétrer l'antivirus pour exclure certains répertoires et processus. La liste des répertoires et processus est donnée ci-dessous.

### Répertoires

SAFE	<p>Répertoire d'installation de SafeKit :</p> <ul style="list-style-type: none"> <li>Sous Windows C:\safekit si SystemDrive=C:</li> <li>Sous Linux /opt/safekit</li> </ul>
SAFEVAR	<p>Répertoire des fichiers de travail de SafeKit :</p> <ul style="list-style-type: none"> <li>Sous Windows C:\safekit\var si SystemDrive=C:</li> <li>Sous Linux /var/safekit</li> </ul>
Répertoires répliqués	Tous les répertoires répliqués définis dans les modules miroir

### Processus

Les processus SafeKit pour les services et démons sont listés dans la [section 10.2](#).

Les exécutable sont localisés sous :

SAFE	safekit command
SAFE/private/plugin/**/*	Exécutables qui sont lancés sur changement d'état d'un module
SAFE/private/bin	Exécutables SafeKit
SAFE/web/bin	Exécutables pour le SafeKit web service

### 10.7 Cryptage des communications du module applicatif

Il est possible de sécuriser les communications internes du module, telles que les heartbeat ou la réplication, en créant les clés de cryptographiques associées au module. Ces mécanismes de sécurité reposent sur la bibliothèque OpenSSL utilisée par SafeKit pour le chiffrement et la gestion des certificats.

Par défaut, les clés sont générées par SafeKit avec une autorité de certification interne (SafeKit PKI). Avec SafeKit <= 7.4.0.31, la clé générée a une durée de validité de 1 an. Voir la [section 10.7.3.1](#) pour les solutions quand la clé expire.

Depuis SafeKit 7.4.0.16, vous pouvez également fournir vos propres clés générées avec votre autorité de certification de confiance (PKI d'entreprise ou PKI commerciale). Voir [section 10.7.3.2](#) pour plus de détails.

Depuis SafeKit 7.4.0.32, le module peut être reconfiguré avec de nouvelles clés même dans l'état ALONE (reconfiguration dynamique).



Lorsque toutes les instances du module n'ont pas la même clé de chiffrement, la communication entre instances est impossible. Réappliquer la configuration contenant la clé valide sur tous les nœuds pour rétablir une configuration correcte.

Il est possible de visualiser la configuration en exécutant la commande `safekit confinfo -m AM` sur chaque nœud (voir [section 9.5](#)). Cette information est également affichée par la console web avant d'éditer la configuration du module et avant le démarrage global

La ressource `encryption` reflète le mode de communication courant du module : "on"/"off" lorsque le chiffrement est actif/inactif. Pour voir l'état des ressources, voir la [section 7.4](#). Cette ressource se nomme `usersetting.encryption`. Pour consulter l'état des ressources, voir la [section 7.4](#).

#### 10.7.1 Configuration avec la console web de SafeKit

Lors de la configuration du module avec la console Web SafeKit, le cryptage de la communication est activé à l'étape 3 de l'assistant de configuration du module (voir [section 3.3.2](#)).

#### 10.7.2 Configuration en ligne de commandes

Les commandes équivalentes pour créer les clés de chiffrement associées à un module sont :

1. `safekit module genkey -m AM`

2. `safekit -H "server1,server2" -E AM`

où `server1` et `server2` sont les nœuds qui implémentent le module

Les commandes équivalentes pour supprimer les clés de chiffrement associées à un module sont :

1. `safekit module delkey -m AM`

2. `safekit -H "server1,server2" -E AM`

où `server1` et `server2` sont les nœuds qui implémentent le module

Pour la description des commandes, voir la [section 9.5](#).

### 10.7.3 Configuration avancée

SafeKit peut sécuriser la communication interne avec des certificats qui sont générés avec une autorité de certification « privée » (SafeKit PKI). Depuis SafeKit 7.4.0.16, vous pouvez également fournir vos propres certificats générés avec votre autorité de certification de confiance (PKI d'entreprise ou PKI commerciale).

#### 10.7.3.1 Configuration avancée avec la PKI SafeKit

Dans SafeKit <= 7.4.0.31, la clé de chiffrement des communications a une durée de validité de 1 an. Quand celle-ci expire dans un module miroir avec la réplication de fichiers, la réintégration sur le secondaire échoue. Pour revenir à une situation normale, il faut reconfigurer le module avec une nouvelle clé. A partir de SafeKit > 7.4.0.31, la durée de validité est de 20 ans.

Si vous ne pouvez pas upgrader SafeKit, vous pouvez générer de nouvelles clés avec une période de validité plus longue. Pour cela, appliquez la procédure suivante :

1. Arrêter le module `AM` sur tous les nœuds
2. Sur l'un des nœuds, se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
3. Exécuter `safekit module genkey -m AM`
4. Supprimer le fichier `SAFE/modules/AM/conf/modulekey.p12`
5. Aller dans le répertoire `SAFE/web/bin`
6. Exécuter `./openssl req -config ../conf/ssl.conf -subj "/O=SafeKiModule/CN=mirror" -new -x509 -sha256 -nodes -days 3650 -newkey rsa:2048 -keyout pkey.key -out cert.crt`

Affecter à l'argument `-days`, la nombre de jours que vous souhaitez comme durée de validité

7. Exécuter `./openssl pkcs12 -export -inkey ./pkey.key -in ./cert.crt -name "Module certificate" -out modulekey.p12`

Cette commande nécessite de renseigner un mot de passe. Contactez le support SafeKit pour obtenir la valeur correcte du mot de passe

8. Supprimer les fichiers `pkey.key` et `cert.crt`
9. Déplacer le fichier `modulekey.p12` sous `SAFE/modules/AM/conf`
10. Aller dans le répertoire `SAFE`

11. Exécuter `safekit -H "server1,server2" -E AM`

où `server1` et `server2` sont les nœuds qui implémentent le module

Le module est configuré sur les 2 nœuds avec sa nouvelle clé et prêt à être démarré.

### 10.7.3.2 Configuration avancée avec une PKI externe

Depuis SafeKit 7.4.0.16, vous pouvez fournir votre propre clé générée avec votre autorité de certification de confiance (PKI d'entreprise ou PKI commerciale).. Pour cela, appliquez la procédure suivante :

1. Arrêter le module `AM` sur tous les nœuds
2. Sur l'un des nœuds, se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
3. Exécuter `safekit module genkey -m AM`
4. Supprimer le fichier `SAFE/modules/AM/conf/modulekey.p12`
5. Ajoutez le fichier de certificat au format X.509 encodé en Base-64 (PEM), pour votre autorité de certification (certificat de l'AC ou bundle de certificats de toutes les autorités de certification) au fichier `SAFE/web/conf/cacert.crt`
6. Aller dans le répertoire `SAFE/web/bin`
7. Générer votre certificat à l'aide de la PKI en spécifiant dans le sujet :  
`"/O=SafeKiModule/CN=mirror"`
8. Copier les fichiers générés `pkey.key` et `cert.crt` dans le répertoire `SAFE/web/bin`
9. Exécuter `./openssl pkcs12 -export -inkey ./pkey.key -in ./cert.crt -name "Module certificate" -out modulekey.p12`  
  
Cette commande nécessite de renseigner un mot de passe. Contactez le support SafeKit pour obtenir la valeur correcte du mot de passe
10. Supprimer les fichiers `pkey.key` et `cert.crt`
11. Déplacer le fichier `modulekey.p12` sous `SAFE/modules/AM/conf`
12. Exécuter `SAFE/safekit -H "server1,server2" -E AM`  
où `server1` et `server2` sont les nœuds qui implémentent le module

Le module est configuré sur les 2 nœuds avec sa nouvelle clé et prêt à être démarré.

## 10.8 Cryptage des fichiers sensibles dans SafeKit

Depuis la version 8.2.4, SafeKit intègre un mécanisme configurable permettant de chiffrer et de déchiffrer les données sensibles utilisées au sein de ses composants.

Ce mécanisme permet de chiffrer des données sensibles dans un fichier, puis de les déchiffrer ultérieurement à l'aide d'un algorithme de chiffrement symétrique, basé sur une seule phrase secrète racine. Cette phrase secrète racine est récupérée et affichée par un exécutable dédié. Le chemin de cet exécutable est configuré dans le fichier `SAFECONF/crypto.json` (où `SAFECONF=C:\safekit\private\conf` en Windows, si `%SYSTEMDRIVE%=C:`, et `SAFECONF=/opt/safekit/private/conf` en Linux). Voici le

contenu par défaut de ce fichier de configuration (où `SAFEBIN=C:\safekit\private\bin` en Windows, si `%SYSTEMDRIVE%=C:`, et `SAFEBIN=/opt/safekit/private/bin` en Linux):

```
{
  // ...
  "rootPassphraseExecutable": "SAFEBIN/print_default_root_passphrase"
}
```

Il est fortement recommandé de remplacer l'exécutable par défaut de la phrase secrète racine par un exécutable personnalisé, conçu pour récupérer et afficher cette phrase de manière sécurisée. Cela vous donne un contrôle total sur la stratégie de chiffrement et renforce la sécurité en intégrant votre propre logique de gestion des phrases secrètes.

Actuellement, cette fonctionnalité est utilisée dans SafeKit uniquement pour le stockage sécurisé du mot de passe du client SMTP. Cela est réalisé via la procédure décrite dans la [section 10.10.2](#). Par conséquent, si la valeur de `rootPassphraseExecutable` est modifiée, vous devez réappliquer cette procédure.

Cette procédure repose sur les commandes suivantes pour crypter et décrypter :

<pre>safekit -r safeenc -e   -encrypt [-infile plaintext.txt] [-outfile cms.pem]</pre>	<p>Chiffre de manière sécurisée l'entrée provenant soit de l'entrée standard, soit du fichier spécifié via l'argument <code>-infile</code>. Le texte chiffré est affiché sur la sortie standard ou enregistré dans le fichier spécifié via l'argument <code>-outfile</code>.</p>
<pre>safekit -r safeenc -d   -decrypt [-infile cms.pem] [-outfile plaintext.txt]</pre>	<p>Déchiffre de manière sécurisée l'entrée provenant de l'entrée standard ou du fichier spécifié via <code>-infile</code>. Le texte déchiffré est affiché sur la sortie standard ou enregistré dans le fichier spécifié via <code>-outfile</code>.</p>



Ce mécanisme de chiffrement n'est pas destiné à sécuriser les fichiers répliqués par SafeKit.

## 10.9 Configuration du service web de SafeKit

SafeKit livre le service web, `safewebserver`, qui s'exécute sur chaque serveur SafeKit. C'est un serveur Apache standard obligatoire pour :

- la console web (voir [section 3](#))
- l'interface en ligne de commandes distribuées sur le cluster (voir [section 9.8](#))
- les checkers de type `<module>` (voir [section 13.17](#))

Le service `safewebserver` démarre automatiquement à la fin de l'installation du package SafeKit et au reboot des serveurs. Si vous n'avez pas besoin de ce service et souhaitez supprimer son démarrage automatique au boot, référez-vous à la [section 9.1.29.1](#).

La configuration par défaut est HTTP avec authentification à base de fichiers, initialisée avec :

- un seul utilisateur `admin` ayant le rôle Admin. Ce rôle peut être changé via l'édition de fichiers de configuration.
- un utilisateur privé `rcmdadmin` pour exécuter la commande `safekit` distribuée.

Les noms d'utilisateur et les mots de passe de ces utilisateurs peuvent être modifiés, si nécessaire, comme décrit dans à la [section 9.1.29.1](#).

### 10.9.1 Serveur Apache HTTP

Le service web SafeKit est un service web léger basé sur Apache utilisé comme serveur HTTP(S) intégré :

- en Windows, SafeKit embarque un serveur Apache http dans son package. La version installée peut être obtenue à l'aide de la commande  
`SAFE\web\bin\httpd.exe -v`



La version du serveur Apache HTTP sous Windows peut évoluer avec les nouveaux packages SafeKit. Référez-vous au [Software Release Bulletin](#) pour obtenir les informations les plus à jour.

- en Linux, SafeKit s'appuie sur le serveur Apache HTTP fourni par le système d'exploitation. La version installée peut être obtenue à l'aide de la commande  
`httpd -v`

Les modules Apache pour SafeKit sont chargés via les fichiers de configuration principaux `SAFE/web/conf/httpd.conf` et `SAFE/web/conf/httpd_main.conf`. Vous pouvez lister les modules chargés à l'aide de la commande suivante :

- en Windows

```
SAFE\web\bin\httpd.exe -f SAFE\web\conf\httpd.conf -M
```

```
Loaded Modules:
core_module (static)
win32_module (static)
mpm_winnt_module (static)
http_module (static)
so_module (static)
request_module (shared)
session_module (shared)
session_cookie_module (shared)
session_crypto_module (shared)
auth_form_module (shared)
alias_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_groupfile_module (shared)
authz_host_module (shared)
authz_user_module (shared)
expires_module (shared)
cgi_module (shared)
dir_module (shared)
log_config_module (shared)
mime_module (shared)
negotiation_module (shared)
setenvif_module (shared)
env_module (shared)
headers_module (shared)
rewrite_module (shared)
reqtimeout_module (shared)
ssl_module (shared)
proxy_module (shared)
proxy_http_module (shared)
proxy_wstunnel_module (shared)
```

```
macro_module (shared)
lua_module (shared)
```

- In Linux

```
httpd -f SAFE/web/conf/httpd.conf -M
```

```
Loaded Modules:
core_module (static)
so_module (static)
http_module (static)
mpm_prefork_module (shared)
unixd_module (shared)
request_module (shared)
session_module (shared)
session_cookie_module (shared)
session_crypto_module (shared)
auth_form_module (shared)
alias_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_groupfile_module (shared)
authz_host_module (shared)
authz_user_module (shared)
expires_module (shared)
cgi_module (shared)
dir_module (shared)
log_config_module (shared)
mime_module (shared)
negotiation_module (shared)
setenvif_module (shared)
env_module (shared)
headers_module (shared)
rewrite_module (shared)
reqtimeout_module (shared)
ssl_module (shared)
proxy_module (shared)
proxy_http_module (shared)
proxy_wstunnel_module (shared)
macro_module (shared)
lua_module (shared)
```

Les modules suivants sont chargés sous condition :

- si `useldap` est défini (chargé par `httpd.webconsoleldap.conf`)

```
ldap_module
authnz_ldap_module
```

- si `useopenid` est défini (chargé par `httpd.webconsoleopenidauth.conf`)

```
auth_openidc_module
```



Les modules Apache HTTP chargés peuvent changer avec les nouveaux packages SafeKit.

### 10.9.2 Fichiers de configuration

La configuration de `safewebserver` est définie dans les fichiers livrés sous `SAFE/web/conf`. Il s'agit de fichiers de configuration Apache standards (voir

<https://httpd.apache.org>). La configuration du service est décomposée dans plusieurs fichiers mais, pour les configurations les plus usuelles seul le fichier `httpd.conf` nécessite d'être modifié.



- Après modification, vous devez redémarrer le service pour charger la nouvelle configuration avec la commande : `safekit webserver restart` (voir [section 9.1.2](#)).
- Ne pas modifier les fichiers `.default` sous **SAFE/web/conf** car il s'agit de sauvegarde de la configuration livrée.

Le fichier `httpd.conf` est essentiellement constitué d'une série de `Define`. Le caractère de commentaire `#` désactive la définition.

Les principaux `Define` sont :

---

Définition du port de connexion :

```
Define httpport 9010
Define httpsport 9453
```

Définit les numéros de ports d'écoute en mode HTTP et HTTPS. Voir la [section 10.9.3](#) pour leur utilisation.

---

Définition de l'authentification utilisateur

```
Define usefile
#Define useldap
#Define useopenid
...
```

Sélectionne l'authentification utilisateur voulue. Une seule méthode doit être définie. Voir la [section 11.4](#) pour plus de détails.

---

Définition de la journalisation Apache

Désactivé par défaut

```
#Define Loglevel info
#Define accesslog
```

Décommenter ces lignes pour activer la journalisation. Les journaux sont `httpd.log` et `access.log`. Ils sont générés dans le répertoire `SAFEVAR`.

---

Définition de la durée de validité d'une session :

```
Define SessionMaxAge 28800
```

Depuis SafeKit 8.2.1, l'utilisateur est automatiquement déconnecté après 8 heures d'inactivité (28800 secondes). Si nécessaire, ajustez cette valeur.

---

Les autres `Define` sont documenté dans le fichier `httpd.conf`.

Les autres fichiers de configuration sont listés ci-dessous. La modification de l'un d'entre eux peut causer des problèmes lors de la mise à jour de SafeKit.

---

Configuration globale	<code>httpd_main.conf</code>
Configuration de l'authentification à base de fichier	<code>httpd.webconsolefileauth.conf</code>

---

	Utilisation des fichiers <code>user.conf</code> et <code>group.conf</code> dans <code>SAFE/web/conf</code>
Configuration de l'authentification à base de formulaire	<code>httpd.webconsoleformauth.conf</code>
Configuration de l'authentification à base de serveur LDAP/AD	<code>httpd.webconsoleldap.conf</code> Utilisation d'un serveur LDAP/AA
Configuration de l'authentification à base de serveur OpenID Connect	<code>httpd.webconsoleopenidauth.conf</code> Utilisation d'un fournisseur d'identité OpenID connect
Configuration HTTPS	<code>httpd.webconsolessl.conf</code> (dans le sous-répertoire <code>ssl</code> ) Utilisation du fichier <code>sslgroup.conf</code> dans <code>SAFE/web/conf</code>

### 10.9.3 Configuration des ports de connexion

Par défaut, connectez la console web avec l'URL `http://host:9010`. Le serveur web SafeKit redirigera vers la page appropriée en fonction de vos paramètres de sécurité.

Si vous devez modifier la valeur par défaut :

1. Éditez `SAFE/web/conf/httpd.conf` et modifiez la valeur des variables `httpport` ou `httpsport`
2. Redémarrez le service avec la commande `safekit webserver restart`

Les configurations HTTP et HTTPS ne doivent pas être activées simultanément. Voir la [section 11.3](#) pour la configuration HTTPS.

La valeur par défaut `9010 (HTTP) / 9453 (HTTPS)` est également utilisée le module `checker`. Par conséquent, dans la configuration des modules qui définissent un `checker` de type `<module>` :

1. Éditez le fichier `userconfig.xml` du module
2. Rajoutez l'attribut `port` et lui affecter la nouvelle valeur du port

```
<check>
  <module name="mirror">
    <to addr="192.168.1.31" port="9010"/>
  </module>
</check>
```

3. Appliquez la nouvelle configuration du module

### 10.9.4 Configuration de HTTP/HTTPS et de l'authentification utilisateur

- La configuration par défaut est pour HTTP. Elle inclut l'authentification à base de fichier, initialisée avec un seul utilisateur `admin` ayant le rôle Admin.
- La configuration HTTPS requiert l'installation de certificats ainsi qu'une méthode d'authentification des utilisateurs.

Pour une description détaillée et leur mise en œuvre, voir la [section 11](#) .

Pour revenir à la configuration HTTP si celle-ci a été changée pour HTTPS, voir la [section 11.2.1.1](#).

### 10.9.5 API SafeKit

Utilisez Swagger UI pour visualiser et interagir avec l'API SafeKit fournie par le service web SafeKit. Pour y accéder, ouvrez un navigateur à l'URL suivante :

```
http://localhost:9010/swagger-ui
```

Les points d'entrée présentés sont utilisés par la console web de SafeKit mais peuvent également être appelés depuis des scripts ou des outils de gestion externes afin d'automatiser les opérations sur le cluster SafeKit.

Depuis le nœud local, l'API de n'importe quel nœud du cluster est accessible en mode proxy. Dans ce cas, le point d'entrée de l'API est préfixé par :

```
/nodes/<nodename>
```

où <nodename> correspond au nom du nœud tel que défini dans la configuration du cluster.

Les requêtes vers l'API utilisent le même mécanisme d'authentification que celui configuré pour la console web SafeKit (voir [section 11.4](#)).

Depuis SafeKit 8.2.6, pour faciliter l'automatisation de la gestion du cluster, il est également possible de s'authentifier par Bearer token, mais uniquement pour les appels directs à l'API (et non depuis la console web SafeKit).

Vous trouverez ci-dessous des exemples d'accès à l'API via la commande `curl`. En Windows, cette commande est livrée sous `SAFE/private/bin`.

#### 10.9.5.1 Accès à l'API via l'authentification par défaut

La configuration par défaut est pour http et inclut l'authentification à base de fichier, initialisée avec un seul utilisateur `admin` ayant le rôle Admin.

Les exemples suivants montrent comment s'authentifier auprès du service web SafeKit, récupérer le cookie de session puis appeler des requêtes de l'API SafeKit avec ce cookie.



Les exemples suivants sont pour HTTP. Lorsque HTTPS est configuré, remplacer l'URL par `https://localhost:9453` et ajouter l'option `--cacert $SAFE/web/conf/cacert.crt` à la commande `curl`.

### Authentification

La requête suivante envoie les identifiants, de l'utilisateur `admin` avec son mot de passe `passwd`, au point d'entrée `/login`.

```
curl -c cookies.txt -d "httpd_username=admin&httpd_password=passwd&login=Login" http://localhost:9010/login
```

Le serveur renvoie un cookie de session (`sessionSK`) qui est stocké dans le fichier `cookies.txt`.

### Appel de l'API

La requête suivante récupère les informations sur le nœud local en passant le cookie récupéré précédemment dans le fichier `cookie.txt`.

```
curl -b cookies.txt http://localhost:9010/api/v1.0/level
```

La requête suivante récupère les informations du nœud node2 du cluster.

```
curl -b cookies.txt http://localhost:9010/api/v1.0/nodes/node2/level
```

Si vous préférez vous pouvez passer explicitement la valeur du cookie dans l'entête de la requête comme suit :

```
curl -H "Cookie: sessionSK=<cookie>" http://localhost:9010/api/v1.0/level
```

Des appels similaires peuvent être réalisés pour n'importe quel point d'entrée de l'API.

### 10.9.5.2 Accès à l'API via Bearer token

Les exemples suivants montrent comment gérer un Bearer token, puis appeler des requêtes de l'API SafeKit en l'utilisant.

La gestion des Bearer tokens est elle-même exposée via l'API `apikeyes` dans Swagger. Pour y accéder, il est nécessaire de s'authentifier au préalable avec un utilisateur disposant du rôle Admin. Elle permet de :

- créer une nouvelle clé en spécifiant son rôle (Admin, Control ou Monitor) et son nom logique. Une fois créée, la valeur du Bearer token associé est retournée et doit être conservée dans un emplacement sûr. Il n'existe aucun moyen de récupérer ce token si sa valeur est perdue.
- propager cette nouvelle clé sur tous les nœuds du cluster. Cela permet d'utiliser un unique Bearer token pour accéder à l'API SafeKit en local ou en mode proxy sur les autres nœuds.
- détruire une clé.

Ces fonctionnalités sont accessibles soit directement, par exemple avec la commande `curl`, soit via une interface web dédiée.



Les exemples suivants sont pour HTTP. Lorsque HTTPS est configuré, remplacer l'URL par `https://localhost:9453` et ajouter l'option `--cacert $SAFE/web/conf/cacert.crt` à la commande `curl`.

### Gestion du Bearer token via son interface web

L'interface web dédiée à la gestion des Bearer tokens n'est pas accessible par défaut pour des raisons de sécurité. Pour y accéder :

1. éditer le fichier `SAFE/web/conf/httpd.conf`
2. décommenter `ApiKeyManagement`

```
Define ApiKeyManagement
```
3. redémarrer le service web avec `safekit webserver restart`
4. ouvrir un navigateur sur l'URL `http://localhost:9010/keymgmt/keymgmt.html`  
Dans la page de login, s'identifier avec un utilisateur ayant le rôle Admin

### Gestion du Bearer token via `curl`

1. s'authentifier avec un utilisateur ayant le rôle Admin

```
curl -c cookies.txt -d
"httpd_username=admin&httpd_password=passwd&login=Login"
http://localhost:9010/login
```

Le serveur renvoie un cookie de session (`sessionSK`) qui est stocké dans le fichier `cookies.txt`.

2. créer une nouvelle clé avec le rôle Admin et , par exemple, le nom logique `administrator`

- en PowerShell sur Windows

```
$token=curl -b cookies.txt
http://localhost:9010/api/v1.0/apikey/Admin/administrator -d " "
```

- en bash sur Linux

```
token=`curl -b cookies.txt
http://localhost:9010/api/v1.0/apikey/Admin/administrator -d " "`
```

Le serveur renvoie le Bearer token associé qui est stocké dans la variable `token` pour la suite de l'exemple.

3. propager cette nouvelle clé sur tous les nœuds du cluster

```
curl -b cookies.txt http://localhost:9010/api/v1.0/apikey/push/administrator -d " "
```

### Appel de l'API avec le Bearer token

La requête suivante récupère les informations sur le nœud local en passant le Bearer token stocké précédemment dans la variable `token`.

```
curl -H "Authentication: Bearer $token" http://localhost:9010/api/v1.0/level
```

La requête suivante récupère les informations du nœud `node2` du cluster.

```
curl -H "Authentication: Bearer $token"
http://localhost:9010/api/v1.0/nodes/node2/level
```

Des appels similaires peuvent être réalisés pour n'importe quel point d'entrée de l'API.

## 10.10 Agent SafeKit de notification par courriel

Depuis SafeKit 8.2.4, SafeKit propose un agent de notification qui envoie des courriels lors d'événements majeurs sur les modules. Ces événements sont extraits du journal système (voir [section 10.13](#)), qui est alimenté par les messages de journal des modules configurés sur le serveur SafeKit. L'utilisation de cette fonctionnalité nécessite que l'équipe informatique de votre entreprise ait configuré un serveur SMTP accessible par l'agent s'exécutant sur les nœuds SafeKit.

Lors de l'installation de SafeKit, l'agent de notification est installé mais désactivé par défaut.

La procédure suivante est requise pour le configurer et l'activer. Appliquez-la sur tous les nœuds SafeKit :

- ⇒ Configuration de l'agent de notification SafeKit décrite en [section 10.10.1](#)

Elle permet de définir le serveur SMTP, les destinataires des courriels, la sélection des événements à envoyer...

- ⇒ Configuration optionnelle des identifiants du client SMTP décrite en [section 10.10.2](#)

Elle permet de définir le nom d'utilisateur et le mot de passe qui sont nécessaires pour envoyer un courriel si le serveur SMTP requiert une authentification.

⇒ Test d'envoi de courriel décrit en [section 10.10.3](#)

Ce test permet de vérifier que votre configuration est fonctionnelle pour l'envoi de courriels.

⇒ Activation de l'agent de notification SafeKit décrite en [section 10.10.4](#)

Une fois activé, les événements majeurs des modules de ce serveur seront automatiquement envoyés par courriel aux destinataires configurés.



Sous Windows, PowerShell 5, qui est la version par défaut, est requis car l'agent n'est pas compatible avec PowerShell 7.

Ci-dessous un exemple d'un courriel émis par l'agent de notification SafeKit configuré sur le node1 :

node1: New SafeKit message(s)

The following 5 noteworthy messages have been emitted on node1:

Node	Module	Timestamp	Origin	Level	Message	Message key
node1	mirror	2025-03-07T11:28:35.598077+01:00	heart	E	Local state WAIT Transient	512
node1	mirror	2025-03-07T11:28:35.582446+01:00	heart	C	License : NO license : Demo 3 days	537
node1	mirror	2025-03-07T11:28:19.156327+01:00	heart	E	Local state STOP NotReady	512
node1	mirror	2025-03-07T11:28:00.195159+01:00	heart	E	Local state WAIT Transient	512
node1	mirror	2025-03-07T11:27:41.183999+01:00	heart	E	Local state PRIM Transient	512

Avec la configuration par défaut de l'agent, lorsqu'un événement critique ou un changement d'état d'un module se produit sur le node1, l'agent regroupe tous les autres événements survenus dans la minute suivante et les envoie dans un unique courriel.

En cas de problèmes, reportez-vous à la [section 7.21](#) pour obtenir de l'aide.

### 10.10.1 Configuration de l'agent de notification SafeKit

Suivre les étapes ci-dessous pour configurer l'agent de notification SafeKit :

1. Ouvrir une console PowerShell/shell en tant qu'administrateur/root
2. Aller dans le répertoire `SAFE/notifications`

`SAFE=C:\safekit` en Windows (si `%SYSTEMDRIVE%=C:`) ; et `SAFE=/opt/safekit` en Linux

3. Copier `safenotif_conf.json.default` dans `safenotif_conf.json`
4. Éditer `safenotif_conf.json` pour le paramétrer

Le fichier de configuration `safenotif_conf.json` est auto documenté, et vous devez au minimum renseigner les champs dans l'extrait ci-dessous :

```
{
  // ...
  "emailNotifications": {
    // ...
  }
}
```

```
"sender": "noreply@it-smtp-server.my.company.com",
"recipients": [
  "my.name@my.company.com"
],
// ...
},
"smtp": {
  "host": "it-smtp-server.my.company.com",
  "port": 25,
  "protocol": "smtp+starttls"
  // ...
}
}
```

Où

- "sender" est l'adresse à partir de laquelle les courriels seront envoyés
- "recipients" est la liste des destinataires
- "host" est le hostname ou l'adresse IP du serveur SMTP
- "port" est le port du serveur SMTP
- "protocol" est le protocole à utiliser pour se connecter au serveur SMTP. Dans cet exemple, il est configuré pour une connexion cryptée, initiée par une commande STARTTLS.

Par défaut, seuls les messages critiques et les changements d'état locaux du module sont envoyés. Consulter le fichier `safenotif_conf.json` pour sélectionner d'autres messages, si nécessaire, modifier le délai d'envoi ou pour d'autres options de configuration.



Après l'upgrade de SafeKit, il pourra peut-être être nécessaire de reconfigurer l'agent de notification SafeKit si son fichier de configuration a évolué entre les 2 versions.

Le fichier `safenotif_conf.json` peut être vérifié pour les erreurs logiques courantes avec :

```
SAFE/private/bin/safenotif -testconfiguration
```

Cette commande retourne une erreur si un problème est détecté. Corrigez-le avant de passer à l'étape suivante.



Sous Linux, une fois l'agent de notification activé, toute modification du fichier `safenotif_conf.json` nécessite de redémarrer le service afin que les changements soient pris en compte, à l'aide de la commande suivante:

```
systemctl restart safenotif.service.
```

### 10.10.2 Configuration des identifiants du client SMTP pour l'authentification

Les serveurs SMTP sont généralement configurés pour exiger que les clients SMTP s'authentifient via leur identifiant (nom d'utilisateur, mot de passe). L'agent de notification SafeKit (qui intègre un client SMTP) stocke ces identifiants dans le système de fichiers de manière sécurisée et chiffrée. Pour cela, suivez les étapes ci-dessous :

1. Ouvrir une console PowerShell/shell en tant qu'administrateur/root



Pour certaines versions de Windows, une console Windows Terminal (`wt`) est requise à la place d'une console PowerShell.

2. Aller dans le répertoire `SAFE`

`SAFE=C:\safekit` en Windows (si `%SYSTEMDRIVE%=C:`) ; et `SAFE=/opt/safekit` en Linux

3. Exécuter `./private/bin/smtpcfg credentials set`

Cette commande vous invite à entrer le nom d'utilisateur et le mot de passe correspondant au compte de l'expéditeur du courriel.

Ces identifiants seront utilisés par l'agent de notification SafeKit pour envoyer des courriels.

Pour réinitialiser les identifiants, et par conséquent désactiver l'authentification, exécutez :

```
SAFE/private/bin/smtpcfg credentials none
```

### 10.10.3 Test d'envoi de courriel

Une fois l'agent de notification SafeKit configurée (voir [section 10.10.1](#)), et les identifiants SMTP définis si une authentification est requise (voir [section 10.10.2](#)), la procédure suivante peut être utilisée pour envoyer un courriel de test en utilisant ces paramètres.

1. Ouvrir une console PowerShell/shell en tant qu'administrateur/root
2. Aller dans le répertoire `SAFE`

`SAFE=C:\safekit` en Windows (si `%SYSTEMDRIVE%=C:`) ; et `SAFE=/opt/safekit` en Linux

3. Exécuter `./private/bin/safenotif -testemail`

Voici un exemple de sortie de cette commande :

```
Sending email from noreply@it-smtp-server.my.company.com to  
my.name@my.company.com with SMTP account noreply on server it-smtp-  
server.my.company.com...  
Email sending successful, check your mailbox(es).
```

Même si la commande réussie, il est conseillé de vérifier la boîte de réception du destinataire que vous avez configuré pour vous assurer que le courriel a bien été reçu. Si le test échoue, résolvez le problème avant de passer à l'étape suivante. Reportez-vous à la [section 7.21](#) pour obtenir de l'aide.

### 10.10.4 Activation de l'agent de notification SafeKit

Une fois que vous avez vérifié que votre configuration est fonctionnelle, appliquez la procédure suivante pour activer l'agent de notification :

1. Ouvrir une console PowerShell/shell en tant qu'administrateur/root
2. Aller dans le répertoire `SAFE`

`SAFE=C:\safekit` en Windows (si `%SYSTEMDRIVE%=C:`) ; et `SAFE=/opt/safekit` en Linux

3. Exécuter `./safekit notification enable`

Une fois activé, les événements majeurs sur les modules de ce serveur seront automatiquement envoyés par courriel aux destinataires configurés.

Pour désactiver la notification, exécutez :

```
SAFE/safekit notification disable
```

Pour vérifier son status, exécutez :

```
SAFE/safekit notification status
```

### 10.11 Supervision SNMP

SafeKit peut être surveillé via SNMP. Depuis la version 8, les implémentations pour Windows et Linux diffèrent. En Windows, SafeKit utilise son propre agent SNMP, alors qu'en Linux, l'agent SNMP du système est utilisé.

#### 10.11.1 Supervision SNMP en Windows

Pour utiliser l'agent SNMP de SafeKit, `Net-SNMP Agent`, vous devez :

1. le configurer pour démarrer au boot avec la commande :

<pre>safekit boot [snmpon   snmpoff   snmpstatus]</pre>	Contrôle le démarrage automatique au boot du service <code>Net-SNMP Agent</code> ("on" ou "off" ; par défaut "off")
---	---

2. ajouter la règle de pare-feu correspondante

Si vous utilisez le pare-feu du système, le pare-feu a déjà été configuré si vous avez appliqué la commande :

```
SAFE/private/bin/firewallcfg add
```

3. le démarrer avec la commande :

<pre>safekit safeagent [start   stop   restart   check]</pre>	Contrôle le démarrage/arrêt du service <code>Net-SNMP Agent</code> qui met en œuvre un agent SNMP SafeKit.
---	--

La configuration du service `Net-SNMP Agent` est définie dans le fichier auto-documenté **SAFE/snmp/conf/snmpd.conf**. C'est un fichier de configuration net-snmp standard décrit dans <http://net-snmp.sourceforge.net>. Par défaut, le service écoute sur le port UDP `agentaddress` 3600 et accepte des requêtes de lecture de la communauté publique et des requêtes d'écriture de la communauté privée. Les requêtes de lecture sont utilisées pour lire l'état d'un module alors que les requêtes d'écriture permettent de réaliser des actions sur le module.

Vous pouvez changer la configuration par défaut suivant vos besoins. Lorsque vous modifiez `snmpd.conf`, vous devez redémarrer l'agent pour charger la nouvelle configuration : `safekit safeagent restart`.



Depuis SafeKit 8, le service se nomme `Net-SNMP Agent` au lieu de `safeagent` dans les versions antérieures.

#### 10.11.2 Supervision SNMP en Linux

Depuis la version 8.0, SafeKit ne vient plus avec son propre agent snmp, aussi les commandes suivantes sont obsolètes en Linux : `safeagent install`, `safeagent start`, `safeagent stop`, `boot snmpon`, `boot snmpoff`, `boot snmpstatus`.

En remplacement, il est possible de configurer l'agent SNMP standard du système pour accéder la mib safekit :

1. Installer net-snmp  

```
dnf install net-snmp net-snmp-utils
```
2. Si selinux est en mode *enforced*, il doit être mis en mode *permissive* pour snmp :  

```
semanage permissive -a snmpd_t
```
3. Si le pare-feu est actif, le port snmp doit être ouvert :  

```
firewall-cmd --permanent --add-service snmp  
  
firewall-cmd --reload
```
4. Éditer `/etc/snmp/snmpd.conf`  
Ajouter les lignes suivantes :  

```
pass .1.3.6.1.4.1.107.175.10 /opt/safekit/snmp/bin/snmpsafekit  
view systemview included .1.3.6.1.4.1.107.175.10
```
5. Activer et démarrer l'agent snmp  

```
systemctl enable snmpd  
systemctl start snmpd
```

Note : La ligne "view systemview" assigne les droits d'accès. Il peut être nécessaire de la modifier suivant les contraintes locales.

### 10.11.3 La MIB SafeKit

La MIB SafeKit est livrée dans `SAFE/snmp/mibs/safekit.mib`.

La MIB SafeKit est accessible avec l'identifiant suivant (OID, préfixe des variables SNMP de SafeKit SNMP): = **enterprises.bull.safe.safekit (1.3.6.1.4.1.107.175.10)**.

La MIB SafeKit définit :

- la table de modules : `skModuleTable`

L'index dans cette table correspond à l'id du module applicatif tel qu'il est retourné par la commande `safekit module listid`.

A travers la MIB, vous pouvez lire et afficher l'état des modules applicatifs sur un serveur (`STOP`, `WAIT`, `ALONE`, `UP`, `PRIM`, `SECOND`) ou vous pouvez agir sur un module (`start`, `stop`, `restart`, `swap`, `stopstart`, `prim`, `second`).

Par exemple, l'état du module d'id 1 est lu avec un get sur la variable SNMP suivante :

```
enterprises.bull.safe.safekit.skModuleTable.skModuleEntry.skModuleCurrentState.1 = stop (0)
```

Utiliser la commande `snmpwalk` pour voir l'ensemble des entrées de la MIB (commande non livrée avec le produit).

- La table de ressources : **`skResourceTable`**

Chaque élément définit une ressource comme un checker d'interface réseau "`intf.192.168.0.0`" et son status (`unknown`, `init`, `up`, `down`).

Exemple: requête SNMP get sur

```
enterprises.bull.safe.safekit.skResourceTable.skResourceEntry.skResourceName.1.2
```

veut dire nom de la ressource 2 dans le module applicatif 1.

### 10.12 Journal des commandes du serveur SafeKit

Il existe un journal des commandes exécutées sur le serveur SafeKit. Ce journal permet d'effectuer un audit des actions réalisées sur le serveur pour aider au support par exemple. Il enregistre toutes les commandes `safekit` qui sont exécutées sur le serveur et qui modifient le système telles que l'installation d'un module, sa configuration, son lancement/arrêt, le lancement/arrêt du service web de SafeKit, ...

Le journal des commandes est stocké dans le fichier `SAFEVAR/log.db` au format SQLite3. Pour lire son contenu :

- exécuter la commande `safekit cmdlog` sur le serveur SafeKit
- ou
- cliquer sur l'onglet le journal de commandes depuis la console web.

Ci-dessous un extrait du contenu « brut » du journal de commandes :

```
| 2021-07-27 14:37:33.205122 | safekit | mirror | 6883 | START | config -m mirror
| 2021-07-27 14:37:33.400513 | cluster | mirror | 0 | 1 | update cluster state
| 2021-07-27 14:37:33.405597 | cluster | mirror | 0 | 1 | module state change on node centos7-
test3
| 2021-07-27 14:37:34.193280 | | | 6883 | END | 0
| 2021-07-27 14:37:34.718292 | cluster | mirror | 0 | 1 | update cluster state
| 2021-07-27 14:37:34.722080 | cluster | mirror | 0 | 1 | module state change on node centos7-
test4
| 2021-07-27 14:37:37.510971 | | | 6871 | END | 0
| 2021-07-27 14:38:05.092924 | safekit | mirror | 7017 | START | prim -m mirror -u
admin@10.0.0.103
| 2021-07-27 14:38:05.109368 | | | 7017 | END | 0
```

Chaque champ a la signification suivante :

- le 1<sup>er</sup> correspond à la date d'écriture de l'entrée dans le journal
- le suivant correspond au type d'action exécutée.
- le suivant porte le nom du module si l'action s'applique à un module en particulier
- le suivant contient le pid du processus exécutant l'action
- le suivant vaut `START` au lancement de la commande, suivi du contenu de la commande ; ou bien, il vaut `END` lorsque la commande s'est terminée suivi du code de retour.

### 10.13 Messages SafeKit dans le journal système

Depuis SafeKit 8, les messages de log des modules SafeKit sont aussi envoyés vers le journal système. Pour les consulter :

- en Windows, ouvrir une console PowerShell et exécuter  
`Get-EventLog -Logname Application -Source Evidian.SafeKit`

```
47086 Nov 23 11:27 Information Evidian.SafeKit 1073873154 mirror | heart | Remote state
UNKNOWN Unknown...
47085 Nov 23 11:27 Information Evidian.SafeKit 1073873154 mirror | heart | Resource
heartbeat.flow set to down by heart...
47084 Nov 23 11:26 Information Evidian.SafeKit 1073873154 mirror | heart | Local state
ALONE Ready...
```

```
47082 Nov 23 11:26 Warning Evidian.SafeKit 2147614977 mirror | heartplug | Action
alone called by heart : remote stop...
47081 Nov 23 11:25 Information Evidian.SafeKit 1073873154 mirror | heart | Remote state
PRIM Ready...
47080 Nov 23 11:25 Information Evidian.SafeKit 1073873154 mirror | heart | Local state
SECOND Ready...
47079 Nov 23 11:25 Information Evidian.SafeKit 1073873154 mirror | rfsplug |
Reintegration ended (default)...
```

- en Linux, ouvrir une console Shell et exécuter

```
journalctl -r -t safekit
```

```
Nov 23 15:22:43 localhost.localdomain safekit[3689940]: mirror | heart | Local state ALONE Ready
Nov 23 15:22:43 localhost.localdomain safekit[3689940]: mirror | heart | Local state PRIM Ready
Nov 23 15:16:48 localhost.localdomain safekit[3689940]: mirror | heart | Local state ALONE Ready
Nov 23 15:16:48 localhost.localdomain safekit[3690096]: mirror | userplug | Script start_prim >
userlog_2023-11-23T151648_start_prim.uolog
Nov 23 15:16:48 localhost.localdomain safekit[3690066]: mirror | rfsplug | Uptodate replicated file
system
Nov 23 15:16:24 localhost.localdomain safekit[3689940]: mirror | heart | Remote state UNKNOWN
Unknown
```



# 11.Sécurisation du service web de SafeKit

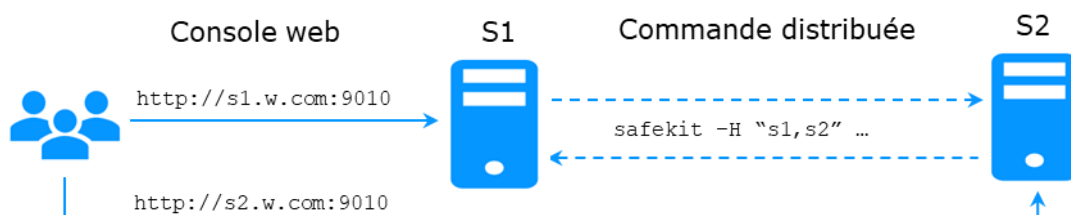
- ⇒ [Section 11.1](#) « Vue générale »
- ⇒ [Section 11.2](#) « Configuration HTTP »
- ⇒ [Section 11.3](#) « Configuration HTTPS »
- ⇒ [Section 11.4](#) « Configuration de l'authentification utilisateur »

## 11.1 Vue générale

Le service web de SafeKit est principalement utilisé par :

- La console web (voir [section 3](#))
- L'interface en ligne de commandes distribuées sur le cluster (voir [section 9.8](#))

SafeKit fournit différentes configurations pour ce service afin de renforcer la sécurité de la console web SafeKit et des commandes distribuées.



Protocole	Authentification	Gestion de rôle
✓ HTTP	✓ Aucune (http seulement)	✓ Admin
✓ HTTPS	✓ A base de fichiers	✓ Control
	✓ LDAP/AD	✓ Monitor
	✓ OpenID Connect	

Les configurations les plus sûres sont basées sur HTTPS et l'authentification des utilisateurs.

SafeKit fournit une autorité de certification "privée" (la PKI de SafeKit). Cela permet de sécuriser rapidement SafeKit sans avoir besoin d'une PKI externe (PKI d'entreprise ou PKI commerciale) qui fournit une autorité de certification de confiance.

SafeKit propose également une gestion de rôles basée sur 3 rôles :

Rôle Admin 👁️ ⚙️	Ce rôle accorde tous les droits d'administration en autorisant l'accès à ⚙️ Configuration et 👁️ Supervision dans la barre latérale de navigation
Rôle Control 👁️	Ce rôle accorde les droits de contrôle et de supervision en autorisant seulement l'accès à 👁️ Supervision dans la barre latérale de navigation

Rôle Monitor 👁	Ce rôle accorde uniquement le droit de supervision en interdisant la possibilité d'actions sur les modules (start, stop...) sous 👁 Supervision dans la barre latérale de navigation
-------------------	---

### 11.1.1 Configuration par défaut

La configuration par défaut est la suivante :

Configuration	Protocole	Authentification/Gestion de rôles
Par défaut	✓ HTTP	<ul style="list-style-type: none"> <li>✓ Authentification à base de fichiers</li> <li>✓ Initialisation avec un unique utilisateur <code>admin</code>, ayant le rôle Admin</li> <li>⇒ Pour la configuration, voir <a href="#">section 11.2.1</a></li> </ul>

### 11.1.2 Configurations prédéfinies

Les configurations prédéfinies sont les suivantes :

Configuration	Protocole	Authentification/Gestion de rôles
Non sécurisée	✓ HTTP	<ul style="list-style-type: none"> <li>✓ Pas d'authentification</li> <li>✓ Rôle identique pour tous les utilisateurs</li> </ul> <p>Pour faciliter le dépannage</p> <p>⇒ Pour la configuration, voir <a href="#">section 11.2.2</a></p>
A base de fichiers	<ul style="list-style-type: none"> <li>✓ HTTP</li> <li>✓ HTTPS</li> </ul> <p>Pour configurer HTTPS avec :</p> <ul style="list-style-type: none"> <li>⇒ la PKI SafeKit, voir <a href="#">section 11.3.1</a></li> <li>⇒ une PKI externe, voir <a href="#">section 11.3.2</a></li> </ul>	<ul style="list-style-type: none"> <li>✓ Authentification à base de fichiers (nom/mot de passe des utilisateurs stockés dans un fichier Apache)</li> <li>✓ Gestion de rôles facultative (stockée dans un fichier Apache)</li> </ul> <p>⇒ Pour la configuration, voir <a href="#">section 11.4.1</a></p>
LDAP/AD	<ul style="list-style-type: none"> <li>✓ HTTP</li> <li>✓ HTTPS</li> </ul> <p>Pour configurer HTTPS avec :</p> <ul style="list-style-type: none"> <li>⇒ la PKI SafeKit, voir <a href="#">section 11.3.1</a></li> <li>⇒ une PKI externe, voir <a href="#">section 11.3.2</a></li> </ul>	<ul style="list-style-type: none"> <li>✓ Authentification à base de serveur LDAP/AD</li> <li>✓ Gestion de rôles facultative</li> </ul> <p>⇒ Pour la configuration, voir <a href="#">section 11.4.2</a></p>

OpenID Connect	<ul style="list-style-type: none"> <li>✓ HTTPS</li> <li>Pour configurer HTTPS avec : <ul style="list-style-type: none"> <li>⇒ la PKI SafeKit, voir <a href="#">section 11.3.1</a></li> <li>⇒ une PKI externe, voir <a href="#">section 11.3.2</a></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ Authentification à base de serveur OpenID Connect</li> <li>✓ Gestion de rôles facultative</li> <li>⇒ Pour la configuration, voir <a href="#">section 11.4.3</a></li> </ul>
----------------	--	---

En Linux, pour tous les fichiers ajoutés sous `SAFE/web/conf`, changer leurs droits avec :



```
chown safekit:safekit SAFE/web/conf/<filename>
chmod 0440 SAFE/web/conf/<filename>.
```

## 11.2 Configuration HTTP

Par défaut, après l'installation de SafeKit, le service web est configuré pour HTTP avec une authentification à base de fichiers qui doit être initialisée.

La configuration par défaut peut être étendue comme décrit en [section 11.2.1](#).

Elle peut aussi être remplacée par la configuration minimale décrite en [section 11.2.2](#) ou une des autres configurations prédéfinies.

### 11.2.1 Configuration par défaut

La configuration par défaut repose sur HTTP avec une authentification à base de fichiers. Elle nécessite d'être initialisée comme décrit ci-dessous. C'est une étape obligatoire.

Cette configuration par défaut peut être étendue :

- pour rajouter des utilisateurs et leur affecter un rôle, comme décrit en [section 11.4.1](#)
- pour passer en HTTPS, avec :
  - ⇒ la PKI SafeKit, décrit en [11.3.1](#)
  - ⇒ une PKI externe, décrit en [section 11.3.2](#)

Après l'installation de SafeKit, la configuration et le redémarrage du service web ne sont pas nécessaires puisqu'il s'agit de la configuration par défaut, et que le service web a été démarré avec celle-ci.

#### 11.2.1.1 Revenir à la configuration HTTP par défaut

Si vous avez modifié la configuration d'authentification utilisateur par défaut et que vous souhaitez revenir à celle-ci, voir la [section 11.4.1](#).

Si vous désirez revenir au mode HTTP, sur tous les serveurs SafeKit :

1. Supprimer le fichier `SAFE/web/conf/ssl/httpd.webconsolessl.conf`
2. Exécuter `safekit webserver restart`

(SAFE=C:\safekit en Windows si System Drive=C: ; et SAFE=/opt/safekit en Linux)

Vous pouvez également exécuter la commande `SAFE/web/bin/rmcerts`, qui en plus de faire les opérations précédentes, supprime tous les fichiers relatifs aux certificats.

### 11.2.1.2 Initialisation pour la console Web et la commande distribuée

SafeKit fournit un script pour que la console Web et les commandes distribuées soient rapidement opérationnelles.

En Linux, ce script peut être appelé automatiquement lors de l'installation de SafeKit. En Windows, il doit être exécuté manuellement. Dans les deux cas, vous devez spécifier la valeur du mot de passe, *pwd* pour l'utilisateur `admin`.

<pre>SAFE/private/bin/webservercfg -passwd <i>pwd</i></pre> <p>où</p> <pre>SAFE=C:\safekit en Windows (si %SYSTEMDRIVE%=C:) SAFE=/opt/safekit en Linux</pre>	<p>Sur tous les nœuds :</p> <ol style="list-style-type: none"><li>1. Ouvrir une console PowerShell/shell en tant qu'administrateur/root</li><li>2. Exécuter la commande</li></ol> <pre>SAFE/private/bin/webservercfg -passwd <i>pwd</i></pre> <p><i>pwd</i> est la valeur du mot de passe</p> <p>Vous devez affecter le même mot de passe sur tous les nœuds.</p>
--	---



Le mot de passe doit être identique sur tous les nœuds du cluster. Dans le cas contraire, la console web et les commandes distribuées échoueront avec des erreurs d'authentification.

Une fois cette initialisation effectuée sur tous les nœuds du cluster :

- Vous pouvez vous authentifier dans la console web avec le nom `admin` et le mot de passe que vous avez fourni. Le rôle est Admin par défaut (à moins que vous ne changiez le comportement par défaut en fournissant le fichier `group.conf` comme décrit en [section 11.4.1.1](#)).

En cas d'échec de l'authentification dans la console, vous devrez peut-être réinitialiser le mot de passe. Pour cela, exécutez à nouveau `SAFE/private/bin/webservercfg -passwd pwd` sur tous les nœuds.

- Vous pouvez exécuter des commandes distribuées. Leur authentification est basée sur un utilisateur dédié `rcmdadmin` avec le rôle Admin. Il est géré dans un fichier utilisateur différent et privé que vous n'avez pas à modifier.

En cas d'échec de l'authentification pour la commande distribuée, vous devrez peut-être réinitialiser le mot de passe de `rcmdadmin`. Pour réinitialiser uniquement celui-ci, sans modifier le mot de passe de `admin`, exécutez `SAFE/private/bin/webservercfg -rcmdpasswd pwd` sur tous les nœuds.

### 11.2.1.3 Tester la console web et la commande distribuée

La configuration est terminée ; vous pouvez maintenant vérifier qu'elle est opérationnelle :


- Tester la console web
  1. Démarrer un navigateur web
  2. Le connecter à l'URL `http://host:9010` (où `host` est l'adresse IP ou le nom d'un nœud SafeKit)
  3. Dans la page de connexion, entrer le nom `admin` et le mot de passe spécifié lors de l'initialisation
  4. La page chargée autorise toutes les fonctionnalités (rôle Admin par défaut)
  
- Tester une commande distribuée
  1. Se loguer sur S1 ou S2 en tant que administrateur/root
  2. Ouvrir un terminal (PowerShell, shell, ...)
  3. Aller dans le répertoire `SAFE`
  4. Exécuter `safekit -H "*" level`  
qui doit retourner le résultat de la commande `level` sur tous les nœuds

### 11.2.2 Configuration non sécurisée basée sur un rôle identique pour tous

Elle est basée sur la configuration d'un rôle unique qui est appliqué à tous les utilisateurs sans nécessiter d'authentification. Cette solution ne peut être mise en œuvre qu'en HTTP et est incompatible avec les méthodes d'authentification des utilisateurs. Elle est présente à des fins de dépannage seulement.

#### 11.2.2.1 Configurer et redémarrer le service web

Pour configurer (`SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C:` ; et `SAFE=/opt/safekit` en Linux) :

	<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"> <li>5. éditer le fichier <code>SAFE/web/conf/httpd.conf</code></li> <li>6. commenter <code>usefile</code>, <code>uselldap</code> et <code>useopenid</code> <pre style="background-color: #f0f0f0; padding: 5px;">#Define usefile ... #Define uselldap ... #Define useopenid</pre> </li> <li>7. sélectionner le rôle souhaité en décommentant le port associé et en commentant tous les autres ; si tous les rôles sont commentés, le rôle sélectionné est <b>Monitor</b>. <pre style="background-color: #f0f0f0; padding: 5px;">Define httpadmin #Define httpcontrol</pre> <ul style="list-style-type: none"> <li>• <code>httpadmin</code> pour le rôle Admin</li> <li>• <code>httpcontrol</code> pour le rôle Control</li> </ul> </li> </ol>
	<p>Sur S1 et S2, désactiver HTTPS s'il avait été active :</p>

	8. détruire le fichier <code>SAFE/web/conf/ssl/httpd.webconsolessl.conf</code>
	Sur S1 et S2 :
	9. exécuter <code>safekit webserver restart</code>



### 11.2.2.2 Tester la console web et la commande distribuée

La configuration est terminée ; vous pouvez maintenant vérifier qu'elle est opérationnelle :

- Tester la console web
  1. Démarrer un navigateur web
  2. Le connecter à l'URL `http://host:9010` (où `host` est l'adresse IP ou le nom d'un nœud SafeKit)
  3. La page chargée donne accès aux fonctionnalités du rôle sélectionné précédemment
- Tester une commande distribuée
  1. Se loguer sur S1 ou S2 en tant que administrateur/root
  2. Ouvrir un terminal (PowerShell, shell, ...)
  3. Aller dans le répertoire `SAFE`
  4. Exécuter `safekit -H "*" level`  
qui doit retourner le résultat de la commande `level` sur tous les nœuds

## 11.3 Configuration HTTPS

Le service web HTTPS s'appuie sur la présence d'un ensemble de certificats énumérés ci-dessous :

	Le certificat de l'Autorité de Certification CA utilisée pour générer les certificats serveur de S1 et S2
	Les certificats serveur de S1 et de S2 permettant de s'assurer de l'identité des nœuds

Appliquez l'une des 2 procédures suivantes pour la configuration HTTPS et des certificats associés :

⇒ [Section 11.3.1 « Configuration HTTPS avec la PKI SafeKit »](#)

Aller à cette section pour une configuration rapide de HTTPS avec l'autorité de certification « privée » de SafeKit

⇒ [Section 11.3.2 « Configuration HTTPS avec une PKI externe »](#)

Aller à cette section pour configurer HTTPS à l'aide de la PKI externe (PKI d'entreprise ou PKI commerciale) qui fournit une autorité de certification de confiance



A l'issue de cette configuration, vous devez mettre en œuvre une des méthodes d'authentification décrites dans la [section 11.4](#).

### 11.3.1 Configuration HTTPS avec la PKI SafeKit

Tout d'abord, vérifiez que l'horloge système est correctement réglée à la date et à l'heure actuelles sur tous les nœuds SafeKit et les postes de travail qui exécuteront la console web HTTPS de SafeKit. Les certificats portant une date de validité, toute différence de temps entre les systèmes peut affecter leur validité.

Ensuite, choisissez un nœud SafeKit pour agir en tant que serveur d'Autorité de Certification (CA). Ce nœud sera désigné ci-après comme le `serveur CA` (par ex, S1). Les autres nœuds du cluster seront appelés `serveurs non-CA` (par ex, S2).

Enfin, suivez la procédure décrite ci-dessous pour activer la configuration HTTPS avec la PKI de SafeKit.

Serveur CA :	Serveur non-CA :
<p>S1</p> 	<p>S2</p> 
<p>Sur S1 :</p> <ol style="list-style-type: none"> <li>« Démarrer le service web CA sur le serveur CA » (voir <a href="#">section 11.3.1.1</a>)</li> <li>« Générer les certificats sur le serveur CA » (voir <a href="#">section 11.3.1.2</a>)</li> </ol>	
	<p>Sur S2 :</p> <ol style="list-style-type: none"> <li>« Générer les certificats sur le serveur non-CA » (voir <a href="#">section 11.3.1.3</a>)</li> </ol>
<p>Sur S1 :</p> <ol style="list-style-type: none"> <li>« Arrêter le service web CA sur le serveur CA » (voir <a href="#">section 11.3.1.4</a>)</li> </ol>	
<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"> <li>« Configurer le service web en HTTPS sur les serveurs CA et non-CA » (voir <a href="#">section 11.3.1.5</a>)</li> <li>« Changer les règles du pare-feu sur les serveurs CA et non-CA » (voir <a href="#">section 11.3.1.6</a>)</li> </ol>	
<p>Sur S1, S2 et tous les postes de travail externes qui exécuteront la console web :</p> <ol style="list-style-type: none"> <li>« Utiliser la console web SafeKit en HTTPS » (voir <a href="#">section 11.3.1.7</a>)</li> </ol>	

En cas de dysfonctionnement de la configuration HTTPS, vous pouvez la réinitialiser complètement en suivant la procédure décrite dans la [section 11.3.1.8.1](#), puis la relancer depuis le début.



La configuration HTTPS échoue si le service web CA a été démarré sur les serveurs non-CA (par ex, S2).

### 11.3.1.1 Démarrer le service web CA sur le serveur CA

Sur le serveur CA (par ex, S1) :

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
2. Aller dans le répertoire `SAFE/web/bin`
3. Exécuter la commande `./startcaserv`

A l'invite, entrer le mot de passe qui protégera l'accès à ce service pour l'utilisateur `CA_admin` (par exemple, `PasW0rD`).

Dans les prochaines étapes, ce mot de passe devra être fourni pour se connecter à ce service.



Le service web CA qui s'exécute sur le premier serveur, est aussi accédé par les serveurs supplémentaires non-CA.



Etant donné que ce service écoute sur le port TCP 9001, s'assurer que ce port n'est pas déjà utilisé et qu'il n'est pas bloqué par la configuration du pare-feu. En Linux, le port 9001 est automatiquement ouvert par la commande `startcaserv`. En Windows, la commande `SAFE/private/bin/firewallcfg add` ouvre les communications pour le service `safeacaserv`.

### 11.3.1.2 Générer les certificats sur le serveur CA

Pendant cette étape, l'environnement de génération des certificats est mis en place ; les certificats de l'autorité de certification et du serveur CA sont générés et installés à l'emplacement attendu par la configuration HTTPS.

Sur le serveur CA (par ex, S1) :

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
2. Aller dans le répertoire `SAFE/web/bin`
3. Répertorier les noms DNS et adresses IP du serveur

Par défaut, le certificat serveur inclut toutes les adresses IP définies localement, les noms DNS et d'hôte associés. Ils sont répertoriés dans les fichiers

`SAFE/web/conf/ipv4.json`, `SAFE/web/conf/ipv6.json` et

`SAFE/web/conf/ipnames.json`. Pour générer ces fichiers, exécutez la commande :

- o sous Linux  
`./getipandnames`
- o sous Windows  
`./getipandnames.ps1`



Si vous souhaitez accéder à la console web depuis un nom DNS ou une adresse IP non répertorié, modifiez le fichier correspondant pour insérer la nouvelle valeur avant d'exécuter la commande `initssl`. Cela est nécessaire par exemple pour accéder depuis internet à un cluster SafeKit dans le cloud, quand les serveurs ont une adresse publique mappée sur une adresse privée.

#### 4. Exécuter la commande :

```
./initssl sca
```

Cette commande :

- o Crée le certificat CA `conf/ca/certs/cacert.crt` et de la clé associée `conf/ca/private/cacert.key`
- o Crée le certificat du serveur `conf/ca/certs/server_<HOSTNAME>.crt` et de la clé associée `conf/ca/private/server_<HOSTNAME>.key`
- o Copie le certificat du CA, le certificat serveur et la clé du certificat serveur dans le répertoire `conf`

Cette commande crée un certificat CA avec un « subject name » par défaut (« SafeKit Local Certificate Authority »). Pour spécifier sa valeur, exécuter plutôt la commande étendue :



```
./initssl sca "/O=My Company/OU=My Entity/CN=My Company Private Certificate Authority".
```

### 11.3.1.3 Générer les certificats sur le serveur non-CA

Pendant cette étape, le certificat du serveur local est généré, les certificats signés sont téléchargés depuis le serveur CA, et enfin les certificats sont installés à l'emplacement prévu par la configuration HTTPS.

Appliquer en séquence la procédure suivante sur chaque serveur non-CA (par ex, S2) :

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
2. Aller dans le répertoire `SAFE/web/bin`
3. Répertorier les noms DNS et adresses IP du serveur

Par défaut, le certificat serveur inclut toutes les adresses IP définies localement, les noms DNS et d'hôte associés. Ils sont répertoriés dans les fichiers

`SAFE/web/conf/ipv4.json`, `SAFE/web/conf/ipv6.json` et

`SAFE/web/conf/ipnames.json`. Pour générer ces fichiers, exécutez la commande :

- o sous Linux

```
./getipandnames
```

- o sous Windows

```
./getipandnames.ps1
```

Si vous souhaitez accéder à la console web depuis un nom DNS ou une adresse IP non répertorié, modifiez le fichier correspondant pour insérer la nouvelle valeur avant d'exécuter la commande `initssl`. Cela est nécessaire par exemple pour accéder depuis internet à un cluster SafeKit dans le cloud, quand les serveurs ont une adresse publique mappée sur une adresse privée.



#### 4. Exécuter la commande :

```
./initssl req https://CAserverIP:9001 CA_admin
```

(CAserverIP est l'adresse IP ou le nom DNS du serveur CA).

A chaque fois que cela est demandé, entrer le mot de passe qui a été utilisé au moment du démarrage du service web CA du serveur CA (PasWOrD). Pour ne pas avoir à saisir le mot de passe, exécuter plutôt la commande :

```
./initssl req https://CAserverIP:9001 CA_admin:PasW0rD
```



Si nécessaire, définissez les variables d'environnement `HTTPS_PROXY` and `HTTP_PROXY` avec les valeurs adéquates.



Si la commande retourne l'erreur "Certificate is not yet valid", cela signifie que les horloges des deux serveurs ne sont pas synchronisées. Pour corriger le problème, il faut changer la date et l'heure des serveurs puis réexécuter la commande `initssl`.

#### 11.3.1.4 Arrêter le service web CA sur le serveur CA

Une fois tous les serveurs configurés, il est recommandé d'arrêter le service web CA (service `safecaserv`) sur le serveur CA. Cela limite le risque d'accès accidentel ou malveillant à l'assistant de configuration HTTPS.

Pour arrêter le service web CA sur le serveur CA (par ex, S1) :

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
2. Aller dans le répertoire `SAFE/web/bin`
3. Exécuter la commande `./stopcaserv`



En Windows, cette commande supprime également l'entrée du service `safecaserv` pour empêcher son démarrage accidentel par la suite.

En Linux, le port 9001 est automatiquement fermé sur le pare-feu local.

Cette étape n'est pas obligatoire, mais en production il est préférable de ne pas laisser accessible les fichiers sensibles.

Les fichiers présents sur le serveur CA, dans le répertoire `SAFE/web/conf/ca` (en particulier les clés privées sous `SAFE/web/conf/ca/private/*.keys`) doivent être sauvegardés dans un espace de stockage sûr et détruits sur le serveur. Ces fichiers devront être restaurés à leur emplacement initial si le serveur CA est à nouveau nécessaire (par exemple pour sécuriser un nouveau serveur SafeKit).

Pour les serveurs non-CA, il faut sauvegarder et détruire les fichiers présents sous le répertoire `SAFE/web/conf/ca`.

Le certificat de l'autorité de certification (fichier `cacert.crt`) situé dans `SAFE/web/conf/ca/certs` doit être importé dans le navigateur qui exécute la console web SafeKit. La procédure d'importation est décrite dans la [section 11.3.1.7](#).

#### 11.3.1.5 Configurer le service web en HTTPS sur les serveurs CA et non-CA

Pour activer la configuration HTTPS, sur tous les serveurs SafeKit (par ex, S1 et S2) :

1. copier `SAFE/web/conf/httpd.webconsolessl.conf` dans  
`SAFE/web/conf/ssl/httpd.webconsolessl.conf`

2. En Linux exécuter :

```
chown safekit:safekit SAFE/web/conf/ssl/httpd.webconsolessl.conf
chmod 0440 SAFE/web/conf/ssl/httpd.webconsolessl.conf
```

3. exécuter `safekit webserver restart`

(Où `SAFE=C:\safekit` en Windows si System Drive=C: ; et `SAFE=/opt/safekit` en Linux).

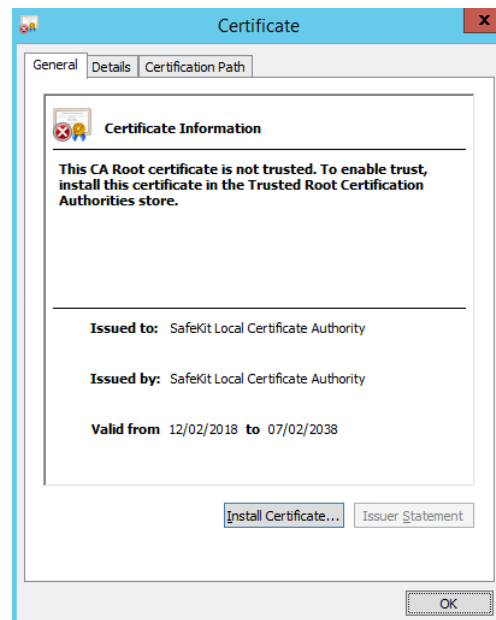
### 11.3.1.6 Changer les règles du pare-feu sur les serveurs CA et non-CA

Une fois le service Web SafeKit configuré en HTTPS, les communications réseau peuvent être ouvertes en configurant le pare-feu, si cela n'a pas été déjà fait, comme décrit en section 10.3.

### 11.3.1.7 Utiliser la console web SafeKit en HTTPS

Tant que le certificat de l'autorité de certification n'a pas été importé, le navigateur émet des alertes de sécurité lorsque l'utilisateur se connecte à la console web avec son certificat client. Si l'importation n'a pas déjà été faite, appliquez la procédure ci-dessous en Windows :

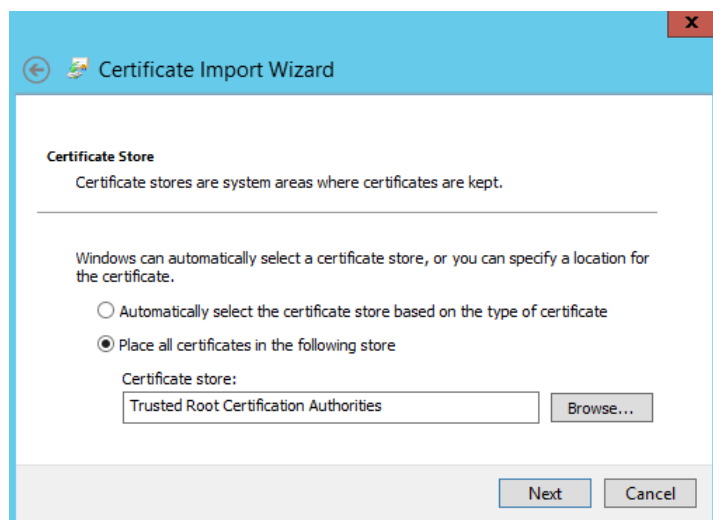
1. Connectez-vous sur la station de travail qui exécute la console web (par ex, S1, S2 et toutes autres stations de travail externes)
2. Télécharger depuis le serveur CA le certificat du serveur CA (par ex, S1) (`cacert.crt` file), localisé dans `SAFE/web/conf/ca/certs`
3. Cliquer sur le fichier `cacert.crt` téléchargé pour ouvrir la fenêtre Certificate. Cliquer ensuite sur le bouton `Install Certificate`



4. L'assistant d'importation de certificat s'ouvre. Sélectionner Current User
5. Cliquer sur le bouton Next



6. Parcourir les magasins pour sélectionner le magasin Trusted Root Certification Authorities.
7. Cliquer sur le bouton Next



8. Enfin terminer l'importation du certificat

### 11.3.1.8 Configuration avancée avec la PKI SafeKit

#### 11.3.1.8.1 Suppression des certificats

Si vous souhaitez revenir à HTTP depuis HTTPS et supprimer tous les fichiers relatifs aux certificats, sur tous les serveurs SafeKit :

1. Se connecter en tant qu'administrateur/root et ouvrir une fenêtre d'invite de commandes
2. Aller dans le répertoire `SAFE/web/bin`
3. Exécuter la commande `./stopcaserv` si celui-ci est démarré
4. Exécuter la commande `./rmcerts CA` (à partir de SafeKit 8.2.5)  
Cette commande redémarre également le service `safewebserver`.



Avant SafeKit 8.2.5, exécuter la commande `./rmcerts` puis supprimer le répertoire `SAFE/web/conf/ca`.

Cette procédure doit également être appliquée pour réinitialiser complètement la configuration HTTPS en cas d'échec, afin de permettre une nouvelle configuration.

#### 11.3.1.8.2 Renouvellement des certificats

Chaque certificat possède une date d'expiration. Par défaut, la date d'expiration du certificat CA est fixée à 20 ans après la date d'installation. Par défaut, la date d'expiration des certificats serveur est fixée à 20 ans après la date de demande de certificat.

Lorsque le serveur est expiré, la console web émet une alerte lors de la connexion au serveur. Une fois le certificat CA expiré, il sera impossible pour le service web SafeKit de valider les certificats présentés.

Il est possible de renouveler les certificats ou de régénérer une requête de création de certificat à partir des clés privées utilisées précédemment. Cette procédure n'est pas explicitée dans ce document. Il est proposé à la place de créer de nouveau jeu de certificats, pour remplacer les anciens :

1. Supprimer le répertoire `web/conf/ca` sur tous les serveurs, y compris le serveur CA
2. Supprimer les certificats des magasins des stations de travail des utilisateurs
3. Réappliquer complètement les procédures décrites en [section 11.3](#)

#### 11.3.1.8.3 Révocation des certificats

Il est possible de modifier la configuration des serveurs web SafeKit pour utiliser une liste de révocation de certificats (CRL). Cette procédure n'est pas explicitée dans ce document. Reportez-vous à la documentation apache et openssl.

Vous pouvez sinon créer un nouveau jeu de certificats, y compris celui de l'autorité de certification, pour remplacer le précédent. Cela a pour effet de révoquer les anciens certificats, car le certificat de l'autorité de certification a changé.

#### 11.3.1.8.4 Commandes pour la génération des certificats

Les commandes doivent être exécutées depuis le répertoire `SAFE/web/bin`.

Tous les chemins d'accès ci-dessous sont relatifs au répertoire `SAFE/web`.

##### **initssl sca [<subject>]**

##### **Paramètres**

<Subject> : le sujet du certificat du CA, qui identifie le propriétaire du CA.

##### **Exemples**

```
initssl sca "/O=My Company/OU=My Unit/CN=My Company Private Certificate Authority"
```

##### **Description**

Cette commande :

- Crée le certificat CA `conf/ca/certs/cacert.crt` et la clé associée `conf/ca/private/cacert.key`
- Crée le certificat du serveur `conf/ca/certs/server_<HOSTNAME>.crt` et la clé associée `conf/ca/private/server_<HOSTNAME>.key`

- Copie le certificat du CA, le certificat serveur et la clé du certificat serveur dans le répertoire conf

Cela initialise le répertoire conf/ca pour les besoins de la PKI SafeKit.



Habituellement, il est préférable de protéger les clés privées par un mot de passe. Cela impliquant une configuration plus complexe, ce n'est pas mis en place. Si besoin, voir la documentation d'Apache et d'OpenSSL.

### initssl rca

Comme *initssl sca*, mais réutilise l'autorité de certification préexistante pour régénérer le certificat serveur et sa clé privée, puis installe le certificat de l'autorité de certification, le certificat serveur, et la clé du certificat serveur dans le répertoire conf.

### initssl req <url> <user>[:<password>]]

#### Paramètres

- <url>: Url du service web du serveur CA (<https://CAserveur:9001>)
- <user>, <password>: utilisateur et mot de passe protégeant l'accès au service web.

La valeur par défaut pour <user> est `CA_admin`. La valeur pour <password> doit être celle affectée au moment du lancement du service web. Si ce champ n'est pas donné en argument, le script demandera sa saisie.

#### Exemple

```
initssl req https://CAserveur:9001 CA_admin:PasW0rD
```

#### Description

Cette commande :

- Crée une requête de certificat pour la génération du certificat serveur. La requête contient toutes les adresses IP et noms DNS associés au serveur local. La requête de certificat est stockée dans `conf/ca/private/server_<hostname>.csr` et la clé associée dans `conf/ca/private/server_<hostname>.key`.
- Crée une requête de certificat pour la génération du certificat client avec le rôle Admin (nécessaire pour les commandes distribuées sur le cluster). La requête de certificat est stockée dans `conf/ca/private/user_Admin_<hostname>.csr` et la clé associée dans `conf/ca/private/user_Admin_<hostname>.key`.
- Télécharge certificat du CA depuis le serveur CA
- Télécharge depuis le serveur CA, des certificats signés qui ont été générés à partir des requêtes construites précédemment
- Installe les certificats et des clés dans le répertoire conf
- Contrôle de validité des certificats

Si <url> n'est pas spécifié, la commande se termine après avoir généré les requêtes de certificats pour :

- le serveur local (`conf/ca/private/server_<hostname>.csr`)
- le certificat client avec le rôle Admin (`conf/ca/private/user_Admin_<hostname>.csr`)

Ces requêtes sont stockées dans le format base64 pour pouvoir être transmises à un CA externe tel Microsoft Active Directory Certificate Services (voir la documentation de Microsoft).

**makeusercert <name> <role>**

### Paramètres

<name> correspond au champ CN du sujet du certificat, habituellement le nom de l'utilisateur du sujet

<role> correspond au rôle lors de l'utilisation de la console web. Les valeurs valides sont Admin **OU** Control **OU** Monitor.

### Exemples

```
makeusercert administrator Admin
makeusercert manager Control
makeusercert operator Monitor
```

### Description

Création d'une requête de certificat client (ainsi que le certificat, le fichier pkcs12, et la clé associée si la commande est exécutée sur le serveur CA) pour <name> et <role>.

Lors de la génération du fichier pkcs12, le script demande d'entrer deux fois le mot de passe qui sera utilisé pour protéger son accès. La clé privée non cryptée est stockée dans `conf/ca/private/user_<role>_<name>.key` file. Quand ils ont générés, le certificat est stocké dans `conf/ca/certs/user_<role>_<name>.crt` et le pkcs12 dans `conf/ca/private/user_<role>_<name>.p12`.

Les certificats clients peuvent être utilisés pour authentifier le client lorsqu'il se connecte au service web en HTTPS. Pour pouvoir connecter la console web, le certificat client correspondant au rôle désiré doit d'abord être importé dans le magasin des certificats du navigateur web.

#### 11.3.1.8.5 Service web du serveur de CA

La configuration du service web du serveur de CA se trouve dans le fichier `SAFE/web/conf/httpd.caserv.conf`.

Ce service implémente une sous-partie des fonctionnalités d'un PKI :

- Le certificat CA est accessible depuis l'URL `https://CAserverIP>:9001/<certificate name>.crt`  
Le téléchargement de ce fichier ne nécessite pas de s'authentifier.
- Les requêtes de certificats sont soumises par l'envoi d'un POST à l'URL `https://<CA server IP>:9001/caserv`

Les arguments sont :

action = signrequest

name = <certificate name>

servercsr = <file content of the server certificate request>

or

usercsr = <file content of the client certificate request>






### 11.3.2 Configuration HTTPS avec une PKI externe

Appliquez les étapes ci-dessous pour configurer HTTPS avec votre autorité de certification de confiance (PKI d'entreprise ou commerciale).

#### 11.3.2.1 Récupérer et installer les certificats serveur

##### 11.3.2.1.1 Récupérer les fichiers certificat

Vous devez récupérer les certificats depuis la PKI dans le format décrit ci-dessous.

 CA	<p>Les certificats serveur de S1 et S2 doivent être signés par l'autorité de certification CA</p>
 S1	<p>Le certificat serveur de S1 permettant de l'authentifier</p>
 S2	<p>Le certificat serveur de S2 permettant de l'authentifier</p>
<p>s1.crt s2.crt</p>	<p>Fichier de certificat au format X.509 encodé en Base-64 (PEM) Le sous-champ CN (Common Name) du champ Objet (Subject) ou le champ Autre nom de l'objet (Subject Alternative Name), doit contenir :</p> <ul style="list-style-type: none"> <li>• noms et/ou adresses IP de S1 pour s1.crt</li> <li>• noms et/ou adresses IP de S2 pour s2.crt</li> </ul> <p> Voir l'exemple dans la <a href="#">section 11.3.2.1.3</a>.</p> <p>Attention : vous devez fournir tous les noms et/ou adresses IP utilisés pour la connexion HTTPS :</p> <ul style="list-style-type: none"> <li>•  Celles incluses dans le fichier de configuration du cluster SafeKit</li> <li>• Celles utilisées dans l'URL du navigateur pour charger la console web depuis un nœud du cluster et qui ne sont pas présentes dans la configuration du cluster.</li> </ul>
<p>s1.key s2.key</p>	<p>La clé privée, *non cryptée*, associée au certificat s1.crt et s2.crt</p>

##### 11.3.2.1.2 Installer les fichiers dans SafeKit

Installer les certificats comme suit (SAFE=C:\safekit en Windows si System Drive=C: ; et SAFE=/opt/safekit en Linux) :

 S1	<p>Sur S1 :</p> <ol style="list-style-type: none"> <li>1. copier s1.crt dans SAFE/web/conf/server.crt</li> </ol>
---	--

s1.crt s1.key	2. copier s1.key dans SAFE/web/conf/server.key
 S2 s2.crt s2.key	Sur S2 : 3. copier s2.crt dans SAFE/web/conf/server.crt 4. copier s2.key dans SAFE/web/conf/server.key

5. En Linux, sur S1 et S2, exécuter :

```
chown safekit:safekit SAFE/web/conf/server.crt SAFE/web/conf/server.key
chmod 0440 SAFE/web/conf/server.crt SAFE/web/conf/server.key
```

Vous pouvez contrôler les certificats installés sur le nœud SafeKit avec :

```
cd SAFE/web/bin
checkcert -t server
```

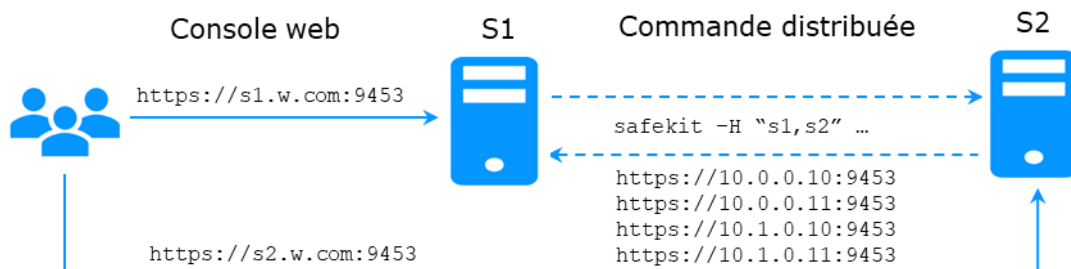
Cette commande retourne en échec si une erreur est détectée.

Vous pouvez également vérifier que le certificat contient bien un nom DNS ou une adresse IP :

```
checkcert -h "nom DNS"
checkcert -i "adresse IP"
```

### 11.3.2.1.3 Exemple

Prenons comme exemple l'architecture suivante :



Le fichier de configuration pour le cluster SafeKit, SAFEVAR/cluster/cluster.xml, contient les valeurs suivantes pour le champ addr :


```
<?xml version="1.0"?>
<cluster>
<lans>
  <lan name="default">
    <node name="s1" addr="10.0.0.10"/>
    <node name="s2" addr="10.0.0.11"/>
  </lan>
  <lan name="private">
    <node name="s1" addr="10.1.0.10"/>
    <node name="s2" addr="10.1.0.11"/>
  </lan>
</lans>
</cluster>
```

Le certificat serveur et la configuration du cluster doivent contenir la même liste de valeurs (noms DNS et/ou adresses IP) et les valeurs utilisées pour connecter la console web. Si ce n'est pas le cas, la console web SafeKit et les commandes distribuées ne fonctionneront pas correctement.

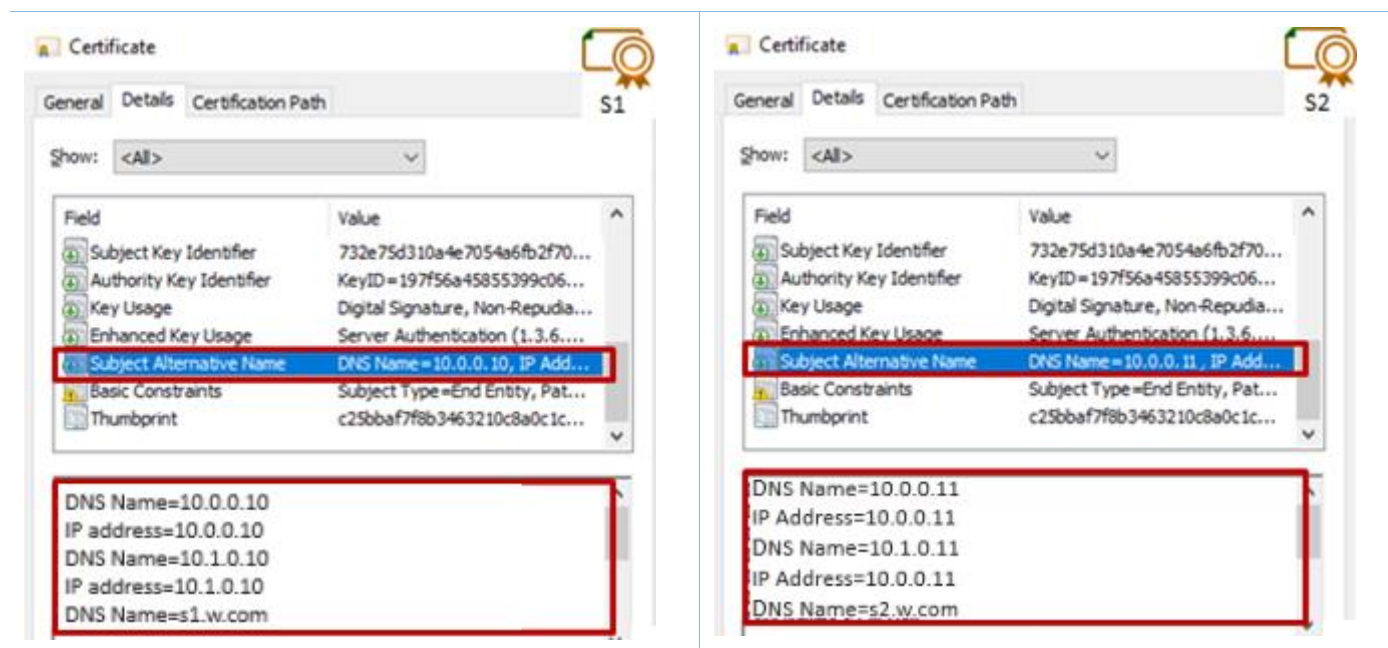
Pour vérifier que cela est bien le cas :

1. Copier le fichier .crt (ou .cer) sur une station de travail Windows
2. Double cliquer sur le fichier pour l'ouvrir avec Extension noyau de chiffrement
3. Cliquer sur l'onglet Détails
4. Vérifier le contenu du champ Autre nom de l'objet (Subject Alternative Name)

Si vous préférez utiliser la ligne de commande, exécutez sur chaque nœud :

 SAFE/web/bin/openssl.exe x509 -text -noout -in  
SAFE/web/conf/server.crt



Et vérifier le contenu de la valeur après Subject Alternative Name.



### 11.3.2.2 Récupérer et installer le certificat CA

#### 11.3.2.2.1 Récupérer le fichier du certificat

Vous devez récupérer le certificat de l'Autorité de Certification CA (chaîne de certificats pour la CA racine et les intermédiaires, s'il y en a) utilisé pour générer les certificats serveur de S1 et S2. Le format attendu est le suivant :

 <p>CA cacert.crt</p>	<p>Le certificat de l'Autorité de Certification CA utilisée pour générer les certificats serveur.</p> <p>Fichier de certificat au format X.509 encodé en Base-64 (PEM)</p> <p>La chaîne de certificats pour la CA racine et les intermédiaires, s'il y en a</p>	 <p>S1 S2</p> <p>Certificats serveur pour S1 et S2</p>
--	---	---

Si vous rencontrez des difficultés pour récupérer ce fichier depuis la PKI, vous pouvez le construire à l'aide de la procédure décrite en [section 7.20](#).

### 11.3.2.2 Installer le fichier dans SafeKit

Installer le certificat comme suit (`SAFE=C:\safekit` en Windows si System Drive=C: ; et `SAFE=/opt/safekit` en Linux) :

 <p>cacert.crt</p>	<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"> <li>1. copier <code>cacert.crt</code> dans <code>SAFE/web/conf/cacert.crt</code></li> <li>2. en Linux, exécuter :             <pre>chown safekit:safekit SAFE/web/conf/cacert.crt chmod 0440 SAFE/web/conf/cacert.crt</pre> </li> </ol>
---	--

Vous pouvez contrôler l'installation avec :

```
cd SAFE/web/bin
checkcert -t CA
```

Cette commande retourne en échec si une erreur est détectée.

Vous devez également vérifier que le fichiers `cacert.crt` contient bien la chaîne de certificats pour les autorités de certification racine et intermédiaires.

### 11.3.2.3 Configurer et redémarrer le service web HTTPS

Pour activer la configuration HTTPS, sur tout les serveurs:

- copier `SAFE/web/conf/httpd.webconsolessl.conf` dans `SAFE/web/conf/ssl/httpd.webconsolessl.conf`
- En Linux exécuter :
 

```
chown safekit:safekit SAFE/web/conf/ssl/httpd.webconsolessl.conf
chmod 0440 SAFE/web/conf/ssl/httpd.webconsolessl.conf
```
- exécuter `safekit webserver restart`

(`SAFE=C:\safekit` en Windows si System Drive=C: ; et `SAFE=/opt/safekit` en Linux)

### 11.3.2.4 Changer les règles du pare-feu

Vous pouvez exécuter la commande `firewallcfg` pour appliquer les règles pour SafeKit au pare-feu du système d'exploitation (en Windows, Microsoft Windows Firewall ; en Linux, `firewalld` ou `iptables`).

<p>Pare-feu</p>	<p>Sur tous les nœuds SafeKit :</p> <ol style="list-style-type: none"> <li>1. exécuter <code>SAFE/private/bin/firewallcfg add</code></li> </ol> <p>où <code>SAFE=C:\safekit</code> en Windows si <code>%SYSTEMDRIVE%=C: ;</code> et <code>SAFE=/opt/safekit</code> en Linux</p>
-----------------	---

N'exécutez pas cette commande si vous souhaitez configurer vous-même le pare-feu ou si vous utilisez un pare-feu différent de celui du système. Pour la liste des processus et ports de SafeKit, voir la [section 10.3](#).

## 11.4 Configuration de l'authentification utilisateur



Mettez en œuvre l'une des méthodes suivantes pour l'authentification utilisateur :

- ⇒ [Section 11.4.1](#) « Configuration l'authentification à base de fichier »
- ⇒ [Section 11.4.2](#) « Configuration de l'authentification à base de serveur LDAP/AD »
- ⇒ [Section 11.4.3](#) « Configuration de l'authentification à base de serveur OpenID Connect »

À l'issue de cette configuration, vous pouvez utiliser la console web sécurisée.

### 11.4.1 Configuration l'authentification à base de fichier

L'authentification à base de fichier peut être appliquée en HTTP ou HTTPS. Elle repose sur les fichiers suivants :

 <p>user.conf</p>	<p>Contrôle d'accès à partir du fichier des utilisateurs</p>
 <p>group.conf</p>	<p>Configuration facultative pour restreindre le rôle de l'utilisateur. Si le fichier <code>group.conf</code> n'est pas présent, tous les utilisateurs authentifiés auront le rôle Admin.</p>

#### 11.4.1.1 Gérer les utilisateurs et groupes

Les utilisateurs et groupes doivent être identiques sur S1 et S2, ainsi que les mots de passe. Ils sont définis par les fichiers `user.conf` et `group.conf` dans le répertoire `SAFE/web/conf` (`SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C: ;` et `SAFE=/opt/safekit` en Linux).



Pendant l'initialisation de la configuration par défaut, décrite dans la [section 11.2.1](#), l'utilisateur nommé `admin` a été créé et est donc présent dans `user.conf`. Vous pouvez décider de le supprimer si vous en créez d'autres.


#### 1. Création d'un utilisateur

Les utilisateurs sont créés avec la commande `SAFE/web/bin/htpasswd`.

Par exemple, pour ajouter le nouvel utilisateur `manager` et lui affecter son mot de passe à `managerpassword`, exécutez :

```
SAFE/web/bin/htpasswd -bB SAFE/web/conf/user.conf manager managerpassword
```

Le nouvel utilisateur est inséré dans le fichier `SAFE/web/conf/user.conf` :


 <p>user.conf</p>	<pre>admin:\$2y\$05\$opQuL6Z2Y78QcXpHIako.O58Z61Wfa5A86XD.eCbEnbRcguJln9Ce <b>manager</b>:\$apr1\$U2GLivF5\$x39WKmSpq6BGmLybESgNV1 operator1:\$apr1\$DetdwaZz\$hy5pQzpU1Pny3qsXrIS/z1 operator2:\$apr1\$ICiZv2ru\$wRkc3BclBhXzc/4llofocl</pre>
--	--

#### 2. Affecter un rôle au nouvel utilisateur

Par défaut, tous les utilisateurs ont le rôle Admin. Si vous souhaitez affecter des rôles différents en fonction des utilisateurs, vous devez créer le fichier `SAFE/web/conf/group.conf` et y définir le rôle de chaque utilisateur. Ce fichier peut contenir les 3 groupes : Admin, Control, Monitor. Les utilisateurs auront le rôle correspondant au groupe auquel ils appartiennent.

+ Chaque ligne débute par le nom du groupe, suivi de `:`, suivi de la liste des utilisateurs (dont le séparateur est l'espace). Voir l'exemple ci-dessous.

Par exemple, pour affecter le rôle Control au nouvel utilisateur `manager` :

 <p>group.conf</p>	<pre>Admin : admin Control : <b>manager</b> Monitor : operator1 operator2</pre>
---	---



+ Si vous activez la gestion de rôle, vous devez insérer l'utilisateur admin dans `group.conf`. Sinon, cet utilisateur ne sera plus opérationnel.

### 3. Supprimer un utilisateur, ...

Exécuter `htpasswd -?` Pour lister toutes les options de gestion des utilisateurs.

#### 11.4.1.2 Installer les fichiers

Installer les fichiers comme décrit ci-dessous (`SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C;` ; et `SAFE=/opt/safekit` en Linux):

 <p>user.conf</p>	<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"> <li>copier <code>user.conf</code> dans <code>SAFE/web/conf/user.conf</code></li> </ol>
 <p>group.conf</p>	<p>Sur S1 et S2, si les groupes sont définis :</p> <ol style="list-style-type: none"> <li>copier <code>group.conf</code> dans <code>SAFE/web/conf/group.conf</code></li> </ol>


### 3. En Linux, sur S1 et S2, exécuter :

```
chown safekit:safekit SAFE/web/conf/user.conf SAFE/web/conf/group.conf
chmod 0440 SAFE/web/conf/user.conf SAFE/web/conf/group.conf
```

Ces fichiers doivent être identiques sur tous les nœuds.

#### 11.4.1.3 Configurer et redémarrer le service web

Pour activer l'authentification à base de fichier (`SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C;` ; et `SAFE=/opt/safekit` en Linux) :

 <p>httpd.conf</p>	<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"> <li>éditer le fichier <code>SAFE/web/conf/httpd.conf</code></li> <li>si nécessaire, décommenter <code>usefile</code></li> </ol>
---	--

	Define usefile
	Sur S1 et S2 : 3. exécuter <code>safekit webserver restart</code>



### 11.4.1.4 Tester la console web et la commande distribuée

La configuration est terminée ; vous pouvez maintenant vérifier qu'elle est opérationnelle :

- Tester la console web
  1. Démarrer un navigateur web
  2. Le connecter à l'URL `http://host:9010` (où `host` est l'adresse IP ou le nom d'un nœud SafeKit). Si HTTPS est configuré, il y a une redirection automatique sur `https://host:9453`.
  3. Dans la page de login, entrer le nom d'utilisateur et le mot de passe.  
Avec la configuration par défaut, vous pouvez vous connecter avec l'utilisateur `admin` en donnant le mot de passe que vous lui avez attribué lors de l'initialisation.
  4. La page chargée ne permet que les accès autorisés en fonction du rôle de l'utilisateur. Si les groupes n'ont pas été définis, tous les utilisateurs ont le rôle Admin.
- Tester une commande distribuée
  1. Se loguer sur S1 ou S2 en tant que administrateur/root
  2. Ouvrir un terminal (PowerShell, shell, ...)
  3. Aller dans le répertoire `SAFE`
  4. Exécuter `safekit -H "*" level`  
qui doit retourner le résultat de la commande `level` sur tous les nœuds

### 11.4.2 Configuration de l'authentification à base de serveur LDAP/AD

L'authentification LDAP/AD peut être appliquée en HTTP ou HTTPS. Elle repose sur :

	Contrôle d'accès à partir d'un compte LDAP/AD associé à l'utilisateur
	Configuration facultative des groupes LDAP/AD pour restreindre le rôle de l'utilisateur. Lorsque les groupes ne sont pas définis, tous les utilisateurs authentifiés ont le rôle Admin.

Appliquer les étapes décrites ci-dessous après avoir vérifié que S1 et S2 peuvent bien se connecter au port du domaine contrôleur LDAP (par défaut est 389).



### 11.4.2.1 Créer les utilisateurs et groupes

Si nécessaire, demandez à l'administrateur LDAP de créer les utilisateurs de la console web SafeKit.

Si vous souhaitez restreindre les accès en fonction des rôles, demandez à l'administrateur LDAP de créer les groupes Admin, Control, Monitor et d'affecter les utilisateurs au groupe adéquate. Si les groupes ne sont pas définis, tous les utilisateurs auront le rôle Admin.

### 11.4.2.2 Configurer et redémarrer le service web

Pour activer l'authentification LDAP/AD (`SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C;` ; et `SAFE=/opt/safekit` en Linux) :

	<p>Sur S1 et S2 :</p> <p>Initialiser l'authentification pour la commande distribuée. Cela peut avoir déjà été fait si vous avez initialisé la configuration par défaut après l'installation de SafeKit. Sinon :</p> <ol style="list-style-type: none"> <li>1. exécuter <code>SAFE/private/bin/webservercfg -rcmdpasswd <i>pwd</i></code> où est le <i>pwd</i> est le mot de passe pour l'utilisateur privé <code>rcmdadmin</code>. Vous n'avez pas besoin de le mémoriser.</li> </ol>
 <p>httpd.conf</p>	<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"> <li>2. éditer le fichier <code>SAFE/web/conf/httpd.conf</code></li> <li>3. décommenter <code>uselldap</code></li> </ol> <pre>Define uselldap</pre> <ol style="list-style-type: none"> <li>4. décommenter les lignes suivantes et remplacer les valeurs en gras par celles correspondant à la configuration de votre service LDAP/AD :</li> </ol> <pre>Define binddn "CN=<b>bindCN</b>, OU=<b>bindOU1</b>, OU=<b>bindOU2</b>, DC=<b>domain</b>, DC=<b>fq</b>, DC=<b>dn</b>"  Define bindpwd "<b>Password0</b>"  Define searchurl "ldap://<b>ldaporad.fq.dn:389</b>/OU=<b>searchou</b>, DC=<b>domain</b>, DC=<b>fq</b>, DC=<b>dn</b> ?sAMAccountName, memberOf?sub?(objectClass=*)"</pre> <p>les variables <code>binddn</code> et <code>bindpwd</code> doivent contenir les identifiants d'un compte possédant les droits de recherche dans le répertoire LDAP</p> <p>la variable <code>searchurl</code> définit l'url de recherche (au sens RFC2255) permettant d'authentifier l'utilisateur</p> <p>CN: common name</p> <p> OU: organization unit</p> <p>DC: domain component (one field for each part of the FQDN).</p> <p>Si aucun groupe n'est défini, tous les utilisateurs authentifiés auront le rôle Admin.</p>

<p>Sur S1 et S2 :</p> <p>Pour activer la gestion de groupes :</p> <ol style="list-style-type: none"><li>5. éditer le fichier <code>SAFE/web/conf/httpd.conf</code></li><li>6. décommenter les lignes suivantes et remplacer les valeurs en gras par celles correspondant à la configuration de votre service LDAP/AD :</li></ol> <pre>Define admingroup "CN=<b>Group1CN</b>, OU=<b>Group1OU1</b>, OU=<b>Group1OU2</b>, DC=<b>domain</b>, DC=<b>fq</b>, DC=<b>dn</b>"  Define controlgroup "CN=<b>Group2CN</b>, OU=<b>Group2OU1</b>, OU=<b>Group2OU2</b>, DC=<b>domain</b>, DC=<b>fq</b>, DC=<b>dn</b>"  Define monitorgroup "CN=<b>Group3CN</b>, OU=<b>Group3OU1</b>, OU=<b>Group3OU2</b>, DC=<b>domain</b>, DC=<b>fq</b>, DC=<b>dn</b>"</pre> <p>Les utilisateurs appartenant au groupe <code>admingroup</code>, <code>controlgroup</code> ou <code>monitorgroup</code>, auront respectivement les rôles Admin, Control et Monitor.</p> <p>Pour une configuration plus avancée, voir la documentation du service web Apache (voir <a href="https://httpd.apache.org">https://httpd.apache.org</a>).</p>
<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"><li>7. exécuter <code>safekit webserver restart</code></li></ol>

### 11.4.2.3 Tester la console web et la commande distribuée

La configuration est terminée ; vous pouvez maintenant vérifier qu'elle est opérationnelle :



- Tester la console web
  1. Démarrer un navigateur web
  2. Le connecter à l'URL `http://host:9010` (où `host` est l'adresse IP ou le nom d'un nœud SafeKit). Si HTTPS est configuré, il y a une redirection automatique sur `https://host:9453`.
  3. Dans la page de connexion, entrer le nom de l'utilisateur et son mot de passe
  4. La page chargée ne permet que les accès autorisés en fonction du rôle de l'utilisateur. Si les groupes n'ont pas été configurés, tous les utilisateurs ont le rôle Admin.
- Tester une commande distribuée
  1. Se loguer sur S1 ou S2 en tant que administrateur/root
  2. Ouvrir un terminal (PowerShell, shell, ...)
  3. Aller dans le répertoire `SAFE`
  4. Exécuter `safekit -H "*" level`  
qui doit retourner le résultat de la commande `level` sur tous les nœuds

### 11.4.3 Configuration de l'authentification à base de serveur OpenID Connect



Depuis SafeKit 8.2.3, l'authentification à base de serveur OpenID Connect fonctionne uniquement avec HTTPS. Pour configurer HTTPS, voir la [section 11.3](#).

L'authentification OpenID connect s'appuie sur le module Apache `mod_auth_openidc`. Elle doit être appliquée en HTTPS. Elle repose sur :

	<p>Contrôle d'accès à partir d'un compte OpenID associé à l'utilisateur et de l'enregistrement d'une application cliente auprès du fournisseur d'identité OpenID.</p>
	<p>Configuration facultative des attributs utilisateurs pour restreindre le rôle de l'utilisateur.</p> <p>Lorsque les attributs ne sont pas définis, tous les utilisateurs authentifiés ont le rôle Admin.</p>



Sur certaines distributions Linux il peut être nécessaire d'installer le module `mod_auth_openidc`.

Appliquer les étapes décrites ci-dessous après avoir vérifié que S1 et S2 peuvent bien se connecter au fournisseur d'identité OpenID Connect. Il peut être nécessaire de spécifier la configuration d'un mandataire, cf. la section correspondante dans `httpd.conf` ainsi que la documentation de `mod_auth_openidc` pour plus de détails.

#### 11.4.3.1 Créer les utilisateurs et groupes

Si nécessaire, demandez à l'administrateur OpenID de créer les utilisateurs de la console web SafeKit.

Demandez à l'administrateur OpenID d'enregistrer l'app console web `safeKit` et noter les valeurs des identifiants (Client ID et Client Secret) ; ces valeurs seront nécessaires pour effectuer la configuration du serveur web ci-après.


Affecter l'Uri de redirection de l'app à la <https://host:9453/openid>. S'il est nécessaire de se connecter à plusieurs serveurs, entrer la liste des urls correspondantes.

Si vous souhaitez restreindre les accès en fonction des rôles, demandez à l'administrateur OpenID de créer les groupes ou rôles OpenID Admin, Control, Monitor et d'affecter les utilisateurs au groupe ou rôle OpenID adéquat, puis renseignez les variables `AdminClaim`, `ControlClaim` et `MonitorClaim` avec les valeurs correspondantes dans le fichier `httpd.conf`. Si les groupes ne sont pas définis, tous les utilisateurs auront le rôle Admin.

Il est également possible de définir les rôles au niveau des serveurs web en affectant des utilisateurs à des rôles dans le fichier `group.conf` comme dans le cas de l'authentification par fichier.

#### 11.4.3.2 Configurer et redémarrer le service web

Pour activer l'authentification OpenID Connect (`SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C;` ; et `SAFE=/opt/safekit` en Linux) :

	<p>Sur S1 et S2 :</p> <p>Initialiser l'authentification pour la commande distribuée. Cela peut avoir déjà été fait si vous avez initialisé la configuration par défaut après l'installation de SafeKit. Sinon :</p> <ol style="list-style-type: none"><li>1. exécuter <code>SAFE/private/bin/webservercfg -rcmdpasswd <i>pwd</i></code> où est le <i>pwd</i> est le mot de passe pour l'utilisateur privé <code>rcmdadmin</code>. Vous n'avez pas besoin de le mémoriser.</li></ol>
 httpd.conf	<p>Sur S1 et S2 :</p> <ol style="list-style-type: none"><li>2. éditer le fichier <code>SAFE/web/conf/httpd.conf</code></li><li>3. décommenter <code>useopenid</code> <pre>Define useopenid</pre></li><li>4. Localisez les lignes suivantes et remplacez les valeurs correspondant à votre fournisseur d'identité OpenID Connect: <pre>OIDCProviderMetadataURL &lt;Your OpenId provider metadata URL&gt; OIDCClientID &lt;Your OpenID client ID&gt; OIDCClientSecret &lt;Your OpenID client secret&gt; OIDCRemoteUserClaim &lt;The Claim in ID token that identifies the user, if not set, defaults to sub&gt; ## openid connect scope request; this defines which claims are returned by the IDP. OIDCScope "openid email"</pre><p>Les variables <code>OIDCClientID</code> et <code>OIDCClientSecret</code> doivent contenir les identifiants obtenus lors de l'enregistrement de l'application auprès du fournisseur d'identité OpenID Connect.</p><p>La variable <code>OIDCScope</code> définit les périmètres nécessaires pour obtenir l'attribut défini par <code>OIDCRemoteUserClaim</code>, et optionnellement les attributs définissant les rôles. <code>openid</code> doit toujours être spécifié.</p><p>Si aucune des variables <code>AdminClaim</code>, <code>ControlClaim</code> et <code>MonitorClaim</code> n'est définie, tous les utilisateurs authentifiés auront le rôle Admin.</p></li></ol>
	<p>Sur S1 et S2 :</p> <p>Pour activer la gestion de groupes :</p> <ol style="list-style-type: none"><li>5. éditer le fichier <code>SAFE/web/conf/httpd.conf</code></li><li>6. décommenter les lignes suivantes et remplacer les valeurs en gras par celles correspondant à la configuration de votre service OpenID Connect : <pre># Define AdminClaim roles:SKAdmin # Define ControlClaim roles:SKControl # Define MonitorClaim roles:SKMonitor</pre><p>Les utilisateurs portant les attributs <code>AdminClaim</code>, <code>ControlClaim</code> ou <code>MonitorClaim</code> auront respectivement les rôles Admin, Control et Monitor.</p><p>Pour une configuration plus avancée, voir la documentation du module <code>mod_auth_openidc</code> (voir <a href="#">GitHub</a> -</p></li></ol>

	OpenIDC/mod_auth_openidc: OpenID Certified™ OpenID Connect Relying Party implementation for Apache HTTP Server 2.x).
	Sur S1 et S2 : 7. exécuter <code>safekit webserver restart</code>

### 11.4.3.3 Tester la console web et la commande distribuée

La configuration est terminée ; vous pouvez maintenant vérifier qu'elle est opérationnelle :

- Tester la console web
  1. Démarrer un navigateur web
  2. Le connecter à l'URL `http://host:9010` (où `host` est l'adresse IP ou le nom d'un nœud SafeKit). Comme HTTPS doit être configuré, il y a une redirection automatique sur `https://host:9453`.
  3. Dans la page de connexion, entrer le nom de l'utilisateur et son mot de passe
  4. La page chargée ne permet que les accès autorisés en fonction du rôle de l'utilisateur. Si les groupes n'ont pas été configurés, tous les utilisateurs ont le rôle Admin.
- Tester une commande distribuée
  1. Se loguer sur S1 ou S2 en tant que administrateur/root
  2. Ouvrir un terminal (PowerShell, shell, ...)
  3. Aller dans le répertoire `SAFE`
  4. Exécuter `safekit -H "*" level`  
qui doit retourner le résultat de la commande `level` sur tous les nœuds



## 12.Cluster.xml pour la configuration du cluster SafeKit

⇒ [Section 12.1](#) « Le fichier `cluster.xml` »

⇒ [Section 12.2](#) « Configuration du cluster SafeKit »

SafeKit utilise le fichier de configuration `cluster.xml`. Ce fichier définit tous les serveurs qui composent le cluster SafeKit ainsi que l'adresse IP (ou nom) de ces serveurs sur les réseaux utilisés pour communiquer avec les nœuds du cluster. Il s'agit des communications globales au cluster et internes aux modules ; ces communications étant cryptées. Ce réseau est aussi utilisé pour l'exécution la commande globale `safekit` (avec l'argument `-H`).

Vous devez définir au moins un réseau qui inclut tous les nœuds du cluster. Il est recommandé de définir plusieurs réseaux de type pour tolérer au moins une défaillance réseau.

Le cluster peut être configuré :

- soit via l'assistant de configuration du cluster de la console web SafeKit
- soit en éditant directement le fichier de configuration du cluster et en appliquant la configuration en ligne de commandes

Ces deux méthodes sont décrites en [section 12.2](#).



Pour des exemples complets de configuration voir la [section 15.1.1](#) et la [section 15.2.1](#). Elles présentent la configuration via la console web ainsi que le `cluster.xml` correspondant.

### 12.1 Le fichier `cluster.xml`

Chaque réseau (`lan`) possède un nom logique qui sera utilisé dans la configuration des modules pour nommer les réseaux de surveillance :

- dans la section `heartbeat` pour un module miroir (voir la [section 13.4](#))
- dans la section `lan` pour un module ferme (voir la [section 13.5](#))

Le nom du nœud est utilisé par le service d'administration de SafeKit (`safeadmin`) pour identifier de manière unique un nœud SafeKit. Vous devez toujours utiliser le même nom pour désigner le même serveur sur les différents réseaux. Ce nom est aussi utilisé par la console web SafeKit lors de l'affichage du nom du nœud.

#### 12.1.1 Cluster.xml exemple

- Dans l'exemple ci-dessous, 2 réseaux sont définis. L'un des réseaux peut être dédié au flux de la réplication de fichiers pour un module miroir.

```
<cluster>
  <lans>
    <lan name="default">
      <node name="node1" addr="192.168.1.67"/>
      <node name="node2" addr="192.168.1.68"/>
    </lan>
    <lan name="repli">
      <node name="node1" addr="10.0.0.1"/>
    </lan>
  </lans>
</cluster>
```

```

    <node name="node2" addr="10.0.0.2"/>
  </lan>
</lans>
</cluster>

```

- Dans l'exemple ci-dessous, un seul réseau est utilisé, mais dans une configuration NAT (Network address translation). Pour chaque nœud du cluster deux adresses doivent être définies : l'adresse locale `laddr` (celle de l'interface locale) et l'adresse externe `addr` (celle connue des autres nœuds).

```

<cluster>
  <lans>
    <lan name="default">
      <node name="node1" addr="server1.dns.name" laddr="10.0.0.1"/>
      <node name="node2" addr="server2.dns.name" laddr="10.0.0.2"/>
    </lan>
  </lans>
</cluster>

```

Tous les nœuds doivent pouvoir communiquer avec les autres via les adresses externes.

### 12.1.2 Cluster.xml syntaxe

```

<cluster>
  <lans [port="4800"]>
    <lan name="lan_name" [command="on|off"] >
      <node name="node_name" addr="IP1_address"|"IP1_name"
        [ laddr="local_IP1_address" ]/>
      <node name="node_name" addr="IP2_address"|"IP2_name"
        [ laddr="local_IP2_address" ]/>
      ...
    </lan>
    ...
  </lans>
</cluster>

```

### 12.1.3 <lans>, <lan>, <node> attributs

<code>&lt;lans</code>	Début de la définition des nœuds du cluster et de la topologie réseau
<code>[port="xxxx"]</code>	Port UDP sur lequel le protocole <code>membership</code> échange. Valeur par défaut : 4800
<code>[pulse="100"]</code>	Délai, en millisecondes, entre deux paquets heartbeat émis par le protocole de <code>membership</code> . Un <code>pulse</code> élevé utilise moins de bande passante, mais entraîne un délai de réaction plus long. Valeur par défaut : 100 (100 millisecondes)
<code>[mlost_count="20"]</code>	Nombre de paquets heartbeat non reçus avant d'élire un nouveau nœud leader. Valeur par défaut : 20 ~ 20 x pulse (2000 millisecondes)

<p>[slost_count="10"]</p>	<p>Nombre de paquets heartbeat non reçus avant de déclarer un nœud follower hors ligne. Valeur par défaut : 10 ~ 10 x pulse (1000 millisecondes)</p>
<p>&lt;lan</p>	<p>Définition d'un réseau sur lequel s'exécute le protocole membership. Au moins un réseau. Autant de sections qu'il y a de LANs entre les serveurs.</p>
<p>name="lan name"</p>	<p>Nom logique unique pour le réseau Ce nom est utilisé dans la configuration du module pour définir les réseaux utilisés.</p>
<p>command="on" "off"</p>	<p>Mettre <code>command="on"</code> pour utiliser ce réseau pour l'exécution des commandes distribuées sur le cluster. Dans ce cas, la section <code>&lt;lan&gt;</code> doit inclure tous les nœuds qui composent le cluster. Il faut définir une unique section <code>&lt;lan&gt;</code> avec <code>command="on"</code>. Quand cet attribut n'est pas positionné, c'est la première section <code>&lt;lan&gt;</code> qui est utilisée pour l'exécution des commandes distribuées sur le cluster. Valeur par défaut : <code>off</code></p>
<p>&lt;node</p>	<p>Définition d'un nœud dans le réseau. Positionner autant de nœuds qu'il y a de serveurs dans le cluster (au moins 2).</p>
<p>name="node name"</p>	<p>Nom unique logique pour le serveur SafeKit Vous devez toujours utiliser le même nom pour désigner le même serveur sur les différents réseaux.</p>
<p>addr= "IP_address"   "IP_name"</p>	<p>Adresse IPv4 ou IPv6, ou nom du nœud tel qu'il est connu par les autres nœuds dans le LAN (préférer une adresse IP pour être indépendant d'un serveur de noms DNS). Pour des configurations NAT, c'est l'adresse extérieure qui doit être indiquée. Lors de la définition d'une adresse IPv6, utiliser le format littéral : l'adresse est placée entre crochets (par exemple [2001::7334])</p>
<p>laddr= "local_IP_address"</p>	<p>Adresse IP locale dans le LAN. A utiliser uniquement pour les configurations NAT.</p>



Dans SafeKit < 8.2, la configuration du cluster avait des attributs `console` et `framework` sur la balise `<lan>`. Ces attributs étaient nécessaires pour l'ancienne console web et sont obsolètes avec la nouvelle. S'ils sont présents, ces attributs sont ignorés en SafeKit 8.2..

## 12.2 Configuration du cluster SafeKit

### 12.2.1 Configuration avec la console web de SafeKit

La console web de SafeKit fournit un assistant de configuration pour éditer le fichier `cluster.xml` et appliquer la configuration sur tous les nœuds qui composent le cluster.



- La configuration du cluster nécessite de se connecter à la console web avec un utilisateur ayant le rôle Admin
- Si le cluster n'est pas encore configuré, la console web ouvre automatiquement l'« Assistant de configuration du cluster »
- Quand le cluster est configuré, la configuration courante du cluster est chargée depuis le nœud de connexion spécifiée dans l'URL du navigateur

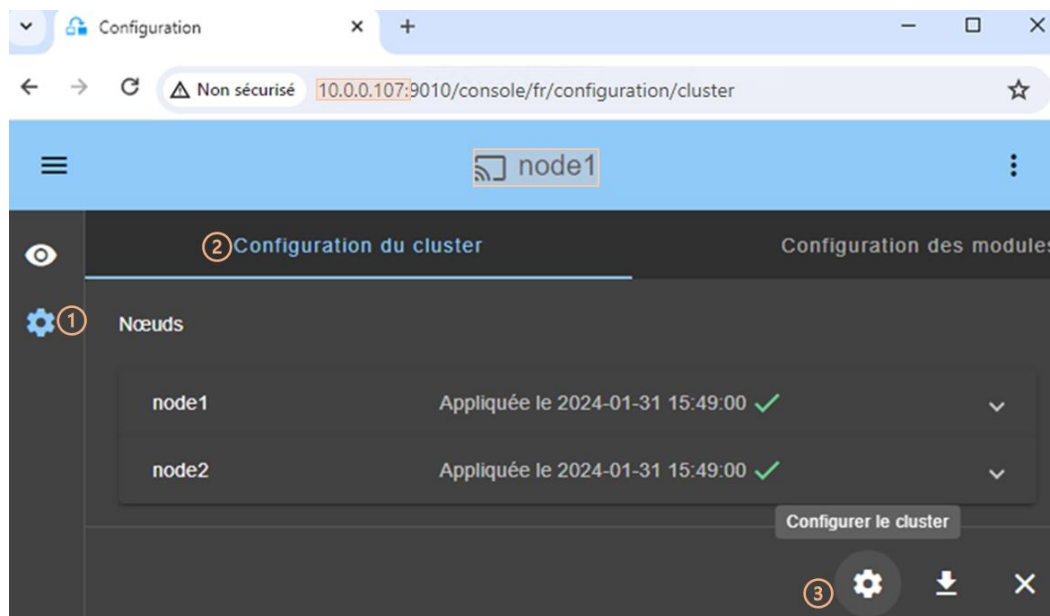
Ouvrir l'assistant de configuration du cluster

- Directement via l'URL <http://host:9010/console/fr/configuration/cluster/config>


Ou

- En naviguant dans la console

Dans cet exemple, la console est chargée depuis `10.0.0.107` qui correspond au nœud `node1` dans le cluster existant.



- (1) Cliquer sur  « Configuration » dans la barre de navigation latérale
- (2) Cliquer sur l'onglet « Configuration du cluster »

- (3) Cliquer sur le bouton  « Configurer le cluster »

Pour des détails sur l'assistant de configuration du cluster, voir la [section 3.2.1](#).

### 12.2.2 Configuration en ligne de commande

- (1) Se loguer en tant que administrateur/root
- (2) Éditer le fichier `SAFEVAR/cluster/cluster.xml`  
sur Windows, `SAFEVAR= C:\safekit\var` si `%SYSTEMDRIVE%=C:`  
sur Linux, `SAFEVAR=/var/safekit`
- (3) Appliquer la configuration du cluster avec une nouvelle clé de chiffrement en exécutant :
  1. `safekit cluster config`  
configure localement, depuis le fichier `cluster.xml`, et génère une nouvelle la clé de chiffrement pour la communication entre les nœuds
  2. `safekit -H "*" -G`  
la configuration local, définie dans le fichier `cluster.xml`, est appliquée sur tous les nœuds du cluster

Pour reconfigurer le cluster sans clé de chiffrement :

1. `safekit cluster delkey`
2. `safekit -H "*" -G`

Pour régénérer des clés de chiffrement et les propager sur les nœuds du cluster :

1. `safekit cluster genkey`
2. `safekit -H "*" -G`



Pour la description complète des commandes, se référer à la [section 9.2](#).

### 12.2.3 Changements de configuration

Lorsque la configuration du cluster SafeKit est modifiée, la nouvelle configuration doit impérativement être appliquée sur tous les serveurs qui composent le cluster. Si la configuration n'est appliquée que sur un sous-ensemble des nœuds présents dans la configuration du cluster, seul le sous-ensemble des nœuds sera en mesure de communiquer. Cela peut avoir pour conséquence de perturber le fonctionnement des modules installés sur les serveurs. Pour rétablir un fonctionnement correct, vous devez réappliquer la configuration sur tous les nœuds du cluster comme décrit précédemment.



Il est possible d'afficher la configuration courante en exécutant la commande `safekit cluster confinfo` sur chaque nœud (voir [section 9.2](#)). Quand la configuration est correcte, cette commande retourne sur tous les nœuds, la même liste de nœuds et la même signature de configuration.

Changer la configuration du cluster peut aussi avoir un impact important sur la configuration des modules car les noms logiques de réseau `<lan>` sont utilisés dans les configurations de modules. Tout changement de configuration déclenche une mise à jour des modules démarrés pour prendre en compte ces modifications. Cela peut conduire à un arrêt de ces modules en cas d'incompatibilité (par exemple sur destruction d'un



réseau alors qu'il est utilisé par un module). Aussi, il faut être prudent lors de la modification de la configuration du cluster quand des modules sont en cours de fonctionnement.

## 13. Userconfig.xml pour la configuration du module applicatif

- ⇒ [Section 13.1](#) « Attributs temporels »
- ⇒ [Section 13.2](#) « Macros - <macro> »
- ⇒ [Section 13.3](#) « Module ferme ou miroir - <service> »
- ⇒ [Section 13.4](#) « Heartbeats - <heart>, <heartbeat> »
- ⇒ [Section 13.5](#) « Topologie d'une ferme - <farm>, <lan> »
- ⇒ [Section 13.6](#) « Adresse IP virtuelle - <vip> »
- ⇒ [Section 13.7](#) « Réplication de fichiers - <rfs>, <replicated> »
- ⇒ [Section 13.8](#) « Scripts du module - <user>, <var> »
- ⇒ [Section 13.9](#) « Hostname virtuel - <vhost>, <virtualhostname> »
- ⇒ [Section 13.10](#) « Surveillance de processus ou services - <errd>, <proc> »
- ⇒ [Section 13.11](#) « Checkers - <check> »
- ⇒ [Section 13.12](#) « TCP checker - <tcp> »
- ⇒ [Section 13.13](#) « Ping checker - <ping> »
- ⇒ [Section 13.14](#) « Interface checker - <intf> »
- ⇒ [Section 13.15](#) « IP checker - <ip> »
- ⇒ [Section 13.16](#) « Custom checker - <custom> »
- ⇒ [Section 13.17](#) « Module checker - <module> »
- ⇒ [Section 13.18](#) « Splitbrain checker - <splitbrain> »
- ⇒ [Section 13.19](#) « Failover machine - <failover> »

Chaque fois que vous modifiez `userconfig.xml`, la configuration doit être appliquée à tous les nœuds du cluster sur lesquels le module applicatif est installé pour être prise en compte.


Pour appliquer la nouvelle configuration, modifiée sur `node1`, sur tous les nœuds, suivre la procédure suivante (remplacer `node1`, `node2` par le nom des nœuds et `AM` par le nom du module) :

- la console web, connectée à `node1`, en naviguant sur  « Configuration/Configuration des modules/ Configurer le module »
- ou en entrant directement l'URL <http://node1:9010/console/en/configuration/modules/AM/config/>
- ou avec la commande `safekit config -H "node1,node2" -E AM` exécutée sur `node1`


Exemple de `userconfig.xml` :

```
<safe>
  <!-- Insert below <macro> <service> tags -->
</safe>
```

Avec la console web, le module doit être arrêté avant d'appliquer la configuration.

Avec la commande, il est possible d'appliquer la configuration alors que le module est démarré, mais uniquement dans l'état  `ALONE (Ready)` et



 `WAIT (NotReady)`. Cette fonctionnalité est appelée *configuration dynamique*. Uniquement un sous-ensemble restreint de la configuration peut être modifié dynamiquement. Quand la nouvelle configuration ne peut être appliquée, un message d'erreur est affiché. Les attributs de configuration pouvant être changés dynamiquement sont listés ci-après.

### 13.1 Attributs temporels

Avant SafeKit 8.2.5, les attributs de configuration représentant une durée (tel que `timeout`, `interval`, `pulse...`) étaient exprimés sous forme de valeurs numériques, sans indication explicite de l'unité de temps. L'utilisateur devait alors consulter la documentation pour connaître l'unité associée.

Depuis SafeKit 8.2.5, la plupart des attributs temporels incluent désormais explicitement l'unité de temps dans leur valeur. Cette amélioration permet une lecture plus intuitive et évite toute ambiguïté. L'ancienne syntaxe sans unité explicite reste entièrement supportée dans SafeKit 8.2.5. Ainsi, les configurations existantes, utilisant des valeurs numériques seules, continuent de fonctionner sans modification.



Les attributs temporels conservent une valeur et une unité de temps par défaut, ce qui influence la manière dont les valeurs fournies par l'utilisateur sont interprétées (voir [section 13.1.2](#)).

Dans la suite du document, les valeurs par défaut des attributs prenant en charge une unité de temps sont exprimées avec l'unité associée. Pour les versions antérieures à SafeKit 8.2.5, il suffit de supprimer l'unité pour connaître la valeur par défaut.

#### 13.1.1 Exemple d'attributs temporels

Par exemple, avant la version 8.2.5 de SafeKit, l'attribut `loop_interval`, qui représente un intervalle de temps en heures sur lequel s'applique `maxloop`, s'exprimait comme suit :

```
<service mode="mirror" maxloop="3" loop_interval="24">
...
</service>
```

Depuis SafeKit 8.2.5, la nouvelle syntaxe est la suivante :

```
<service mode="mirror" maxloop="3" loop_interval="24h">
...
</service>
```

Cette nouvelle notation rend la configuration plus lisible et évite toute ambiguïté sur l'unité utilisée.

#### 13.1.2 Syntaxe des attributs temporels

Les unités disponibles, depuis SafeKit 8.2.5, pour les attributs temporels sont les suivantes :

- `d` pour jour (ex. `"1d"`)
- `h` pour heure (ex. `"2h"`)
- `m` pour minute (ex. `"3m"`)

- s pour seconde (ex. "10s")
- ms pour milliseconde (ex. "700ms")
- us pour microseconde (ex. "50us")

Les attributs temporels conservent une valeur et une unité de temps par défaut, ce qui influence la manière dont les valeurs fournies par l'utilisateur sont interprétées.

Par exemple, si un attribut a une valeur par défaut de 10s, l'unité implicite est la seconde. Si l'utilisateur spécifie une valeur comme 5ms, celle-ci sera convertie en secondes (0.005s) et arrondie à 0s. Dans ce cas, la configuration du module échouera avec, par exemple, l'erreur suivante :

Erreur : valeur invalide "500ms" pour l'attribut boot\_delay (unité de temps attendue : "s")

Si la valeur 0 est légitime dans la configuration du module, l'affecter sans unité de temps ou avec l'unité attendue.

### 13.2 Macros - <macro>

Utiliser une macro pour associer un nom à une valeur. Dans le `userconfig.xml`, le nom, encadré par le caractère %, est remplacé par la valeur de la macro portant ce nom.



La syntaxe `%identifiant%` peut être aussi utilisée dans `userconfig.xml` pour récupérer la valeur d'une variable d'environnement de nom `identifiant`. En cas de conflit, c'est la valeur de macro qui prime.

#### 13.2.1 <macro> Exemple

Dans l'exemple suivant, `%PATH%` est remplacé par `e:\path`.

```
<macro name="PATH" value="e:\path"/>
<service>
  ...
  <rfs>
    <replicated dir="%PATH%" />
  </rfs>
</service>
```



Un exemple d'utilisation des macros est donné dans la [section 15.3](#). Il décrit la configuration via la console web ainsi que le `userconfig.xml` correspondant.

#### 13.2.2 <macro> Syntaxe

```
<macro
  name="identifiant"
  value="value"
/>
```

#### 13.2.3 <macro> Attributs

<code>&lt;macro</code>	
<code>name="identifiant"</code>	Une chaîne de caractères qui identifie la macro.

<code>value="value"</code>	La valeur qui remplacera chaque occurrence de <code>%identifiant%</code> dans la suite de <code>userconfig.xml</code> .
<code>/&gt;</code>	

### 13.3 Module ferme ou miroir - `<service>`

`<service>` est la section de niveau supérieur définissant la configuration d'un module, en particulier le mode du module (`mirror`, `farm` ou `light`) et son démarrage au boot.

#### 13.3.1 `<service>` Exemple

##### 13.3.1.1 Exemple pour un module miroir

```
<service mode="mirror" boot="on">
  <!-- Insérer ci-dessous les tags <heartbeat> <rfs> <vip> <user> <vhost> <errd>
<check> <failover> -->
</service>
```



Pour un exemple complet d'un module miroir, voir la [section 15.1](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

##### 13.3.1.2 Exemple pour un module ferme

```
<service mode="farm" boot="on">
  <!-- Insérer ci-dessous les tags <farm> <vip> <user> <vhost> <errd> <check>
<failover> -->
</service>
```



Pour un exemple complet d'un module ferme, voir la [section 15.2](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

##### 13.3.1.3 Exemple pour un module light


```
<service mode="light" boot="on">
  <!-- Insérer ci-dessous les tags <user> <vhost> <errd> <check> <failover> -->
</service>
```





Pour un exemple d'un module light, voir le module follower de la [section 15.9.2](#).


#### 13.3.2 `<service>` Syntaxe





```
<service mode="mirror"|"farm"|"light"
  [boot="off"|"on"|"auto"|"ignore"]
  [boot_delay="0s"]
  [failover="on"|"off"]
  [defaultprim="alone"|"server_name"|"lastprim"]
  [maxloop="3"] [loop_interval="24h"]
  [automatic_reboot="off"|"on"]>
</service>
```

 Seuls les attributs `boot`, `boot_delay`, `maxloop`, `loop_interval` et `automatic_reboot` peuvent être modifiés dynamiquement.

### 13.3.3 <service> Attributs

<pre>&lt;service</pre>	<p>Première section à définir dans un module</p>
<pre>mode= "mirror"  "farm"  "light"</pre>	<ul style="list-style-type: none"> <li>• <code>mode="mirror"</code> pour un module miroir (voir <a href="#">section 1.2</a>) Le protocole de synchronisation entre les 2 serveurs est défini en <a href="#">section 13.4</a>.  Pour un exemple complet d'un module miroir, voir la <a href="#">section 15.1</a>.</li> <li>• <code>mode="farm"</code> pour un module ferme (voir <a href="#">section 1.3</a>) Le protocole de synchronisation entre les serveurs est défini en <a href="#">section 13.5</a>.  Pour un exemple complet d'un module ferme, voir la <a href="#">section 15.2</a>.</li> <li>• <code>mode="light"</code> (voir <a href="#">section 1.2.9</a>) Configuration sur un seul serveur avec uniquement la détection d'erreur et le redémarrage local.</li> </ul>
<pre>[boot= "on"  "off"  "auto"  "ignore"]</pre>	<ul style="list-style-type: none"> <li>• <code>boot="on"</code> le module est automatiquement démarré au boot de la machine.</li> <li>• <code>boot="off"</code> le module n'est pas démarré au boot de la machine.</li> <li>• <code>boot="auto"</code> le module est démarré automatiquement au boot de la machine s'il était démarré avant le reboot.</li> <li>• <code>boot="ignore"</code> Avant SafeKit 7.5, la configuration du démarrage au boot du module se faisait avec la commande <code>safekit boot -m AM on off</code> (qui devait être exécutée sur chaque nœud). Si vous préférez continuer à utiliser cette commande, supprimez l'attribut <code>boot</code> ou affectez-lui la valeur <code>ignore</code> (valeur par défaut). Le module ne sera pas démarré au boot, à moins que la commande <code>safekit boot -m AM on</code> ne soit exécutée.  L'état de la configuration du démarrage au boot est visible dans la ressource <code>usersetting.boot</code>. Pour consulter l'état des ressources, voir la <a href="#">section 7.4</a>.  Valeur par défaut : <code>ignore</code></li> </ul>

<pre>[boot_delay="0s"]</pre>	<p>Le délai, en secondes, avant le démarrage du module au boot.</p> <p>Valeur par défaut : 0s (pas de délai)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>
<pre>[failover="on"   "off"]</pre>	<p>Pour un module miroir seulement.</p> <ul style="list-style-type: none"> <li>failover="on" <p>reprise automatique sur le serveur secondaire lorsque le serveur primaire est arrêté.</p> </li> <li>failover="off" <p>lorsque le serveur primaire est arrêté, le serveur secondaire se met en attente (pas de reprise automatique). Seule la commande <code>safekit prim</code> peut forcer le démarrage du serveur secondaire en primaire. Pour une description, voir la <a href="#">section 5.7</a>.</p> </li> </ul> <p>Valeur par défaut : on</p>
<pre>[defaultprim="alone"   "server_name"   "lastprim"]</pre>	<p>Pour un module miroir seulement.</p> <p>defaultprim décide quel serveur parmi 2 serveurs est le serveur primaire par défaut pour un module applicatif.</p> <p>Cette option est utile quand un module est ALONE sur un serveur et que le module est démarré sur l'autre serveur.</p> <ul style="list-style-type: none"> <li>defaultprim="alone" <p>le module ALONE devient PRIM alors que le module redémarré devient SECOND. Valeur recommandée pour éviter les basculements d'application juste après la réintégration.</p> </li> <li>defaultprim="server_name" <p>lorsque le module tourne sur deux serveurs, le serveur PRIM est celui indiqué dans defaultprim. Cette valeur peut être utile dans les architectures actif/actif (voir <a href="#">section 1.4.2</a>) ou N-1 (voir <a href="#">section 1.4.3</a>).</p> </li> <li>defaultprim="lastprim", le serveur redémarré redevient PRIM s'il était PRIM avant son dernier arrêt.</li> </ul> <p>Valeur par défaut : alone</p>
<pre>[maxloop="3"]</pre>	<p>Nombre de détections d'erreur successives avant arrêt.</p> <p>Cet attribut définit le nombre maximum d'actions (<code>restart</code>, <code>stopstart</code>, <code>wait</code>) pouvant être exécutées, à la suite d'une</p>

	<p>détection d'erreur émise par <code>&lt;errd&gt;</code> ou un <code>&lt;checker&gt;</code>, avant d'arrêter localement le module.</p> <p>Ce compteur est réinitialisé à l'expiration du délai <code>loop_interval</code> ou lors d'une commande manuelle <code>safekit start, restart, swap, stopstart...</code></p> <p>Noter qu'une commande <code>safekit</code> émise par un détecteur avec l'option <code>-i identity</code> incrémente le compteur, alors qu'une commande manuelle sans cette option le réinitialise.</p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p> <p><code>maxloop</code> est représenté par la ressource <code>heart.stopstartloop</code>. Sa valeur courante correspond à la date à laquelle le compteur a été initialisé (sous la forme d'un timestamp Epoch Unix) ; et sa date d'affectation correspond soit à son initialisation, soit à un rebouclage (<code>stopstart, restart</code>). Consulter l'historique des ressources pour visualiser chaque incrémentation du compteur.</p> <p>Valeur par défaut : 3</p>
<pre>[loop_interval= "24h"]</pre>	<p>Intervalle de temps, en heures, sur lequel <code>maxloop</code> s'applique.</p> <p>Affectez sa valeur à 0 pour désactiver le compteur <code>maxloop</code>.</p> <p>Valeur par défaut : 24h (24 heures)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>
<pre>[automatic_reboot ="off"  "on"]</pre>	<p>Si positionné à <code>on</code>, reboot sur <code>safekit stopstart</code> au lieu de stopper puis redémarrer.</p> <p>Valeur par défaut : <code>off</code></p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>

## 13.4 Heartbeats - `<heart>`, `<heartbeat >`

### Module miroir uniquement

Les heartbeats doivent être utilisés seulement avec les modules miroirs. La topologie d'une ferme est décrite dans la [section 13.5](#).

Le mécanisme basique pour synchroniser deux serveurs et détecter les défaillances d'un serveur est le heartbeat (battement de cœur), qui consiste en un échange de paquets UDP entre les serveurs. Normalement, on met autant de heartbeats qu'il y a de réseaux connectant les 2 serveurs. Dans une situation normale, les 2 serveurs échangent leurs

états (`PRIM`, `SECOND`, les états des ressources) à travers les heartbeats et synchronisent ainsi les procédures de démarrage arrêt applicatif.

Si tous les heartbeats sont perdus, cela signifie que l'autre serveur est en panne. Le serveur local décide de devenir `ALONE`. Bien que non obligatoire, il est préférable d'avoir deux voies de heartbeats sur deux réseaux différents afin de distinguer une panne réseau d'une panne serveur et d'éviter le cas du split-brain.

Le réseau utilisé par le heartbeat est défini par le nom logique d'un réseau de la configuration du cluster SafeKit (voir [section 12](#)).

### 13.4.1 `<heart>` Exemple



Pour un exemple complet d'un module miroir, voir [section 15.1](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

- Exemple pour configurer un heartbeat sur le réseau du cluster nommé `default`

```
<heart>
  <heartbeat name="default" />
</heart>
```

- Exemple avec 2 heartbeats, dont un réseau de réplication dédié, configuré avec `ident="flow"` sur le réseau du cluster nommé `private`

```
<heart>
  <heartbeat name="default" />
  <heartbeat name="private" ident="flow"/>
</heart>
```

### 13.4.2 `<heart>` Syntaxe




```
<heart
  [port="xxxx"] [pulse="700ms"] [timeout="30000ms"]
  [permanent_arp="on"]
>
  <heartbeat
    [pulse="700ms"] [timeout="30000ms"] name="network" [ident="name"]
  >
</heartbeat>
...
</heart>
```






Le tag `<heart>` et son sous-arbre peuvent être entièrement modifiés dynamiquement.

### 13.4.3 `<heart>`, `<heartbeat>` Attributs

<code>&lt;heart</code>	
<code>[port="xxxx"]</code>	Port UDP sur lequel les heartbeats sont échangés. Valeur par défaut : dépend de l'id du module applicatif. Rendu par la commande <code>safekit module getports</code> .
<code>[pulse="700ms"]</code>	Délai en millisecondes entre l'émission de 2 paquets de <code>heartbeat</code> .

	<p>Valeur par défaut : 700ms (700 millisecondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<p>[timeout="30000ms"]</p>	<p>Timeout de détection en millisecondes de la perte d'un heartbeat.</p> <p>Valeur par défaut : 30000ms (30000 millisecondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<p>[permanent_arp="on" "off"]</p>	<p>Régulièrement, <code>heart</code> positionne un ARP permanent pour ses voies de heartbeats.</p> <p>Cette procédure peut geler <code>heart</code> sur certains systèmes (Linux). Dans ce cas, positionner à "off" et affecter l'ARP permanent sur les voies de heartbeats au boot. Sur Linux, ceci peut être fait en ajoutant la commande suivante dans un script exécuté au boot :</p> <pre>arp -s hostname hw_addr</pre> <p>Valeur par défaut : on</p>
<p>&lt;heartbeat</p>	<p>Définition d'un heartbeat. Il y a autant de sections &lt;heartbeat&gt; qu'il y a de voies de heartbeats (réseaux connectant les serveurs). Au moins 1 heartbeat.</p>
<p>name="network"</p>	<p>Nom du réseau utilisé par le heartbeat. "network" doit être le nom d'un réseau défini dans la configuration du cluster SafeKit (voir <a href="#">section 12</a>).</p>
<p>[ident="name"]</p>	<p>Donne le nom qui sera utilisé pour ce heartbeat dans la console web ainsi que pour la ressource interne correspondante, i.e. : <code>heartbeat.name</code> peut être utilisé dans la failover machine (voir <a href="#">section 13.19</a>).</p> <p>Si l'attribut <code>ident</code> n'est pas défini la valeur de l'attribut <code>name</code> est utilisée.</p> <p>Si vous positionnez un heartbeat <code>ident="flow"</code>, le flux de réplication sera positionné automatiquement sur la même voie.</p> <p> Si vous positionnez <code>ident="flow"</code> sans configuration &lt;rfs&gt;, le démarrage du module bloque dans l'état <code>WAIT</code>.</p>
<p>[pulse="700ms"]</p>	<p>Redéfinition du délai en milliseconde entre l'émission de 2 paquets de heartbeat. Par défaut le même que celui dans &lt;heart&gt;.</p> <p>Valeur par défaut : 700ms (700 millisecondes)</p>

	 Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a> ).
<pre>[timeout= "30000ms"]</pre>	<p>Redéfinition du timeout de détection en ms de la perte d'un heartbeat. Par défaut le même que celui dans <code>&lt;heart&gt;</code>.</p> <p>Valeur par défaut : 30000ms (30000 millisecondes)</p>  Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a> ).
<pre>&lt;server addr= "IP1_address" /&gt;</pre>	<p><b>Ancienne</b> définition de l'adresse ip du serveur pour ce heartbeat</p> <p>Le tag <code>&lt;server&gt;</code> était utilisé dans l'ancienne syntaxe de configuration (avant SafeKit 7.2). Il est supporté pour assurer la compatibilité ascendante, mais ne doit pas être utilisé pour la configuration de nouveaux modules.</p>  Vous ne devez pas utiliser dans le même <code>userconfig.xml</code> , la syntaxe de SafeKit 7.1 et celle introduite depuis SafeKit 7.2.

### 13.5 Topologie d'une ferme - `<farm>`, `<lan>`

#### Module ferme uniquement


Le mécanisme basique pour synchroniser une ferme de serveurs est un protocole de groupe qui détecte automatiquement les membres disponibles dans le groupe (protocole membership).

Le réseau utilisé par le protocole est défini par le nom logique d'un réseau de la configuration du cluster SafeKit (voir [section 12](#)).

#### 13.5.1 `<farm>` Exemple


Exemple d'utilisation du réseau du cluster nommé `default`.

```
<farm>
  <lan name="default" />
</farm>
```




 Pour des exemples complets de configuration dans un module ferme, voir la [section 15.2](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

#### 13.5.2 `<farm>` Syntaxe

```
<farm [port="xxxx"]>
  <lan name="network">
    </lan>
  ...
</farm>
```

 Le tag `<farm>` et son sous-arbre **ne peuvent pas** être modifiés dynamiquement.

### 13.5.3 <farm>, <lan> Attributs

<farm	
[port="xxxx"]	<p>Port UDP sur lequel le protocole membership échange.</p> <p>Valeur par défaut : dépend de l'id du module applicatif.</p> <p>Rendu par la commande <code>safekit module getports</code></p>
[pulse= "100ms"]	<p>Délai, en millisecondes, entre deux paquets heartbeat émis par le protocole de membership.</p> <p>Un pulse élevé utilise moins de bande passante, mais entraîne un délai de réaction plus long.</p> <p>Valeur par défaut : 100ms (100 millisecondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
[mlost_count="20"]	<p>Nombre de paquets heartbeat non reçus avant d'élire un nouveau nœud leader.</p> <p>Valeur par défaut : 20 -&gt; 20 x 100ms (2000 millisecondes)</p> <p>Si le journal verbeux du module contient des messages de déconnexion répétés émis par <code>vipd</code>, tels que :</p> <p>   vipd   D   Lost contact from peer=171.27.1.60   vipd   D   Lost contact from node1</p> <p>il est recommandé d'augmenter cette valeur à 80 afin d'améliorer la stabilité de la connexion.</p>
[slost_count="10"]	<p>Nombre de paquets heartbeat non reçus avant de déclarer un nœud follower hors ligne.</p> <p>Valeur par défaut : 10 -&gt; 10 x 100ms (1000 millisecondes)</p> <p> En cas de messages de déconnexion récurrents émis par <code>vipd</code> dans le journal verbeux du module, augmentez cette valeur à 40.</p>
<lan	<p>Définition d'un lan sur lequel s'exécute le protocole membership. Au moins un lan doit être défini. Autant de sections qu'il y a de réseaux entre les serveurs.</p>
name="network"	<p>Nom du réseau utilisé. <code>network</code> doit être le nom d'un réseau défini dans la configuration du cluster SafeKit (voir <a href="#">section 12</a>).</p>
< node name="identity" addr= "IP1_address" >	<p>Adresse IP et nom du nœud dans ce lan. Le tag &lt;node&gt; était utilisé dans l'ancienne syntaxe de configuration (avant SafeKit 7.2). Il est supporté pour assurer la compatibilité ascendante, mais ne doit pas être utilisé pour la configuration de nouveaux modules.</p>



Vous ne devez pas utiliser dans le même `userconfig.xml`, la syntaxe de SafeKit 7.1 et celle introduite depuis SafeKit 7.2.

### 13.6 Adresse IP virtuelle - `<vip>`

L'adresse IP virtuelle (VIP) permet d'assurer un accès hautement disponible aux applications critiques et, selon l'architecture, la répartition de charge de ces accès. La VIP constitue un point d'accès unique pour les clients.

La configuration d'une VIP est supportée uniquement :

- dans un cluster sur site (on-premise)
- dans un cluster où les serveurs appartiennent au même sous-réseau, les mécanismes de basculement et d'équilibrage de charge reposant sur des opérations de niveau 2 (couche liaison).

Les environnements cloud ou certaines configurations réseau ne permettent donc pas l'utilisation directe de la VIP. Voir la [section 13.6.3](#) pour des solutions alternatives.



Si vous installez plusieurs modules applicatifs sur le même serveur, l'adresse IP virtuelle doit être différente pour chaque module.

#### 13.6.1 `<vip>` Exemple dans un module miroir

Dans un module miroir :

- la VIP est active uniquement sur le nœud primaire ✓ PRIM/ALONE (Ready)
- la VIP est transférée automatiquement sur le nœud secondaire après basculement en cas de défaillance du primaire

L'exemple ci-dessous illustre la configuration d'une VIP pour un module miroir d'un cluster sur site :

```
<vip>
  <interface_list>
    <interface check="on">
      <real_interface>
        <virtual_addr addr="192.168.1.222" where="one_side_alias"
check="on"/>
      </real_interface>
    </interface>
  </interface_list>
</vip>
```



Voir aussi l'exemple complet en [section 15.1](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

#### 13.6.2 `<vip>` Exemple dans un module ferme

Dans un module ferme :

- la VIP est active simultanément sur tous les nœuds actifs ✓ UP (Ready)
- le trafic est réparti entre les nœuds. La répartition est assurée par SafeKit au niveau kernel selon les règles de load balancing configurées

L'exemple ci-dessous illustre la configuration d'une VIP pour un module ferme d'un cluster sur site. Les connexions TCP à destination de la VIP sur le port 80 sont réparties entre les nœuds tandis que le reste du trafic est refusé.

```
<vip>
  <interface_list>
    <interface check="on">
      <virtual_interface type="vmac_directed">
        <virtual_addr addr="192.168.1.222" where="alias" check="on"/>
      </virtual_interface>
    </interface>
  </interface_list>
  <loadbalancing_list>
    <group name="FarmProto">
      <rule port="80" proto="tcp" filter="on_port"/>
    </group>
  </loadbalancing_list>
</vip>
```



Voir aussi l'exemple complet en [section 15.2](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

### 13.6.3 Alternative à <vip>

La configuration d'une adresse IP virtuelle avec une section `<vip>` dans `userconfig.xml` est supportée uniquement :



- dans un cluster sur site (on-premise)
- dans un cluster où les serveurs appartiennent au même sous-réseau

Si votre cluster ne répond pas à ces prérequis, une alternative consiste à configurer l'adresse IP virtuelle dans un équilibreur de charge. L'équilibreur de charge achemine les paquets vers les adresses IP physiques des serveurs en testant la valeur retournée par une URL nommée vérificateur d'état (health check) et géré par SafeKit.


SafeKit fournit donc un vérificateur d'état pour chaque module. Vous devez configurer le test de vérification dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où `AM` est le nom du module

Pour un module miroir, le test retourne :

- OK, qui signifie que l'instance est saine, quand le module est dans l'état  PRIM (Ready) ou  ALONE (Ready)
- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états

Pour un module ferme, le test retourne :

- OK, qui signifie l'instance est saine, quand le module est dans l'état  UP (Ready)
- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états

Voir la [section 16](#), pour une description de la mise en œuvre de cette solution dans le Cloud.

Une autre alternative consiste à ce que vous implémentiez une configuration DNS spéciale et une commande de redirection DNS insérée dans les scripts de redémarrage de SafeKit.

### 13.6.4 <vip> Syntaxe

#### 13.6.4.1 Partage de charge réseau dans une architecture ferme

```
<vip [tcpreset="off"|"on"] [scriptcontrol="off"|"on"]>
  <interface_list>
    <interface
      [check="off"|"on"]
      [arpreroute="off"|"on"]
      [arpinterval="60s"]
      [arpelapse="1200s"]
    >
    <virtual_interface
      [type="vmac_directed"|"vmac_invisible"]
      [addr="xx:xx:xx:xx:xx"]
    >
      <virtual_addr
        addr="virtual_IP_name"|"virtual_IP_address"
        [where="alias"]
        [check="off"|"on"]
        [connections="off"|"on"]
      />
      ...
    </virtual_interface>
  </interface_list>
  <loadbalancing_list>
    <group name="group_name"
      <cluster>
        <host name="node_name" power="value" />
        ...
      </cluster>
      <rule
        [virtual_addr="*"|"virtual_IP_name"|"virtual_IP_address"]
        [port="*"|"value"]
        proto="udp"|"tcp"|"arp"
        filter="on_addr"|"on_port"|"on_ipid"
      />
      ...
    </group>
    ...
  </loadbalancing_list>
</vip>
```



Le tag <vip> et son sous-arbre **ne peuvent pas** être modifiés dynamiquement.

#### 13.6.4.2 Basculement réseau dans une architecture miroir

Pour un cluster sur site :

```
<vip [tcpreset="off"|"on"]>
  <interface_list>
    <interface
      [check="off"|"on"]
```



```
[arpreroute="off"|"on"]
[arpinterval="60s"]
[arpelapse="1200s"]
>

<real_interface>
<virtual_addr
  addr="virtual_IP_name"|"virtual_IP_address"
  where="one_side_alias"
  [check="off"|"on"]
  [connections="off"|"on"]
/>
...
</real_interface>
</interface>
...
</interface_list>

</vip>
```


### 13.6.5 <interface\_list>, <interface>, <virtual\_interface>, <real\_interface>, <virtual\_addr> Attributs

<vip>	
[tcpreset="off" "on"]	<p>Avant de déconfigurer l'adresse IP virtuelle, les connexions l'ayant comme IP source, sont rompues. La rupture de connexion est désactivée en positionnant cet attribut à <code>off</code>.</p> <p>Valeur par défaut : <code>on</code></p>
[scriptcontrol="off" "on"]	<p><b>Ferme seulement</b></p> <p>Avec <code>scriptcontrol="on"</code>, l'ouverture et la fermeture du trafic vers la VIP sont pilotés manuellement dans les scripts du module (<a href="#">section 15.2.3.2</a>). Pour une description détaillée, se référer à la <a href="#">section 15.2.2.5</a>.</p> <p>Valeur par défaut : <code>off</code></p>
<interface_list>	
<interface	<p>Définition des adresses IP virtuelles sur une interface. Mettre autant de sections &lt;interface&gt; que vous avez d'interfaces réseau à configurer.</p>
[check="off" "on"]	<p>Positionner un checker sur l'interface réseau. Le module est mis dans l'état <code>WAIT</code> tant que l'interface est down. Le nom du checker d'interface est <code>intf.&lt;network_IP_mask&gt;</code> (<code>intf.192.168.0.0</code>).</p> <p>Valeur par défaut : <code>on</code></p> <p>Pour plus d'informations, voir <a href="#">section 13.14</a>.</p>
[arpreroute="off" "on"]	<p><b>VIP IPv4 seulement</b></p>

	<p>Broadcast de gratuitous ARP pour le reroutage des adresses IP virtuelles définies dans les sections <code>&lt;real_interface&gt;</code>.</p> <p>Valeur par défaut : <code>off</code></p>
<code>[arpinterval="60s"]</code>	<p><b>VIP IPv4 seulement</b></p> <p>Délai en secondes entre 2 gratuitous ARP.</p> <p>Valeur par défaut : <code>60s</code> (60 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<code>[arpelapse="1200s"]</code>	<p><b>VIP IPv4 seulement</b></p> <p>Durée totale, en secondes, pendant lequel des gratuitous ARP sont émis.</p> <p>Valeur par défaut : <code>1200s</code> (1200 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<code>[name="interface name"]</code>	<p><b>Linux seulement</b></p> <p>Vous pouvez spécifier le nom de l'interface. Exemple, positionner <code>name="bond0"</code></p> <p>Par défaut, SafeKit détecte l'interface réseau à configurer à partir des adresses IP virtuelles configurées sur cette interface.</p>

### 13.6.5.1 `<virtual_interface>`, `<virtual_addr>` Attributs dans une architecture ferme

A utiliser pour les modules ferme avec partage de charge sur l'IP virtuelle :

<code>&lt;virtual_interface</code>	<p>Définition des adresses IP virtuelles configurées sur une interface Ethernet.</p>
<pre>type= "vmac_directed"  "vmac_invisible"</pre>	<ul style="list-style-type: none"> <li><code>type="vmac_directed"</code> Associe l'adresse MAC de l'un des serveurs à l'adresse IP virtuelle, comme pour le reste du trafic normal. Voir la description en <a href="#">section 13.6.7.3</a>.</li> <li><code>type="vmac_invisible"</code> Adresse MAC virtuelle jamais visible dans les entêtes Ethernet pour permettre le broadcast des switches. Nécessite le support du mode promiscuous. Voir la description en <a href="#">section 13.6.7.2</a>.</li> </ul> <p> Lorsque vous exécutez SafeKit dans une machine virtuelle, il faut activer le mode promiscuous sur l'adaptateur réseau virtuel. Voir <a href="#">SK-0099</a> pour la procédure à suivre pour Hyper-V et VMware ESX.</p>

	Note : configuration possible pour un module miroir et pour un reroutage transparent sans gratuitous ARP.
[addr="xx:xx:xx:xx:xx"]	Unicast virtual MAC adresse. Si non positionné, par défaut concaténation de "5A:FE" (Safe) et de la 1 <sup>ère</sup> adresse IP virtuelle en hexadécimal. Ignoré lorsque type="vmac_directed"
<virtual_addr	Définition d'une adresse IP virtuelle. Mettre autant de lignes <virtual_addr> qu'il y a d'adresses IP virtuelles à configurer sur l'interface.
addr="virtual_IP_name"   "virtual_IP_address"	Nom ou adresse IP virtuelle (préférer une adresse IP pour être indépendant de la panne du serveur de nom). Adresse IPv4 ou IPv6.
where="alias"	L'adresse IP virtuelle est définie sur tous les serveurs de la ferme en alias. Note : Dans le cas particulier d'une configuration d'un module miroir avec VMAC mettre ici where="one_side_alias".
[check="off"   "on"]	Positionner un IP checker sur l'adresse virtuelle. Le module exécute un stopstart quand l'IP virtuelle est détruite. Le nom de l'IP checker est ip.<virtual addr value> (ip.192.168.1.99). Valeur par défaut : on Pour plus d'informations, voir <a href="#">section 13.15</a> .
[connections="off"   "on"]	Active le comptage du nombre de connexions actives sur l'adresse virtuelle. Ce nombre est stocké dans la ressource nommée connections.<addr value> (par exemple : connections.192.168.1.99) qui est affectée toutes les 10 secondes. Cette valeur est fournie à un titre indicatif uniquement. Valeur par défaut : off
netmask="defaultnetmask"	<b>Linux et IPv4 seulement</b> Par défaut, prend le netmask de l'interface. A positionner si l'interface a plusieurs netmasks.
</virtual_interface>	

### 13.6.5.2 <real\_interface>, <virtual\_addr> Attributs dans une architecture miroir

A utiliser pour les modules miroir avec basculement de l'IP virtuelle :

<code>&lt;real_interface&gt;</code>	Définition d'adresses IP virtuelle associée avec l'adresse MAC réelle de l'interface.
<code>&lt;virtual_addr</code>	Définition d'une adresse IP virtuelle. Mettre autant de lignes <code>&lt;virtual_addr&gt;</code> qu'il y a d'adresses IP virtuelles à configurer sur l'interface.
<code>addr= "virtual_IP_name"  "virtual_IP_address"</code>	Nom ou adresse IP virtuelle (préférer une adresse IP pour être indépendant de la panne du serveur de nom).  Adresse IPv4 ou IPv6.
<code>where="one_side_alias"</code>	Adresse mise en alias sur le serveur <code>PRIM</code> ou <code>ALONE</code> .
<code>[check="off" "on"]</code>	Positionner un IP checker sur l'adresse virtuelle. Le module exécute un <code>stopstart</code> quand l'IP virtuelle est détruite. Le nom de l'IP checker est <code>ip.&lt;addr value&gt;</code> ( <code>ip.192.168.1.99</code> ).  Valeur par défaut : <code>on</code>  Pour plus d'informations, voir <a href="#">section 13.15</a> .
<code>[connections="off" "on"]</code>	Active le comptage du nombre de connexions actives sur l'adresse virtuelle. Ce nombre est stocké dans la ressource nommée <code>connections.&lt;virtual addr value&gt;</code> (par exemple : <code>connections.192.168.1.99</code> ) qui est affectée toutes les 10 secondes. Cette valeur est fournie à un titre indicatif uniquement.  Valeur par défaut : <code>off</code>
<code>netmask="defaultnetmask"</code>	<b>Linux et IPv4 seulement</b>  Par défaut, prend le netmask de l'interface. A positionner si l'interface a plusieurs netmasks.
<code>&lt;/real_interface&gt;</code>	


### 13.6.6 `<loadbalancing_list>`, `<group>`, `<cluster>`, `<host>` Attributs

A utiliser uniquement avec un module ferme.



Voir aussi l'exemple complet en [section 15.2](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

<code>&lt;loadbalancing_list &gt;</code>	
<code>&lt;group</code>	Définition d'un groupe de load balancing. Mettre autant de sections qu'il y a de groupes.

	 Voir l'exemple de plusieurs groupes en <a href="#">section 15.2.2.4</a> .
<code>name="group_name"</code>	Nom du groupe de load balancing.
<code>&lt;cluster</code>	Définition des serveurs et des poids. Sans la section <code>&lt;cluster&gt;</code> , les règles s'appliquent sur tous les serveurs de la ferme.
<code>&lt;host</code>	Définition d'un nœud dans le groupe
<code>name="node_name"</code>	Nom du nœud utilisé. <code>node_name</code> doit être le nom d'un serveur défini dans la configuration du cluster SafeKit (voir <a href="#">section 12</a> ).
<code>power="value"</code>	Poids du nœud dans le groupe. Peut-être égal à 0 si l'on ne veut aucun trafic sur le nœud. Pour plus d'informations, voir <a href="#">section 13.6.7.4</a> .
<code>&lt;/cluster&gt;</code>	
<code>&lt;rule</code>	Définition d'une règle de load balancing dans le groupe. Autant de lignes que de règles de load balancing.
<code>[virtual_addr="*"   "virtual_IP_address"   "virtual_IP_name"]</code>	Adresses IP virtuelles concernées par le load balancing. Par défaut toutes : *
<code>[port="*"   "value"]</code>	Port TCP ou UDP sur lequel s'applique la règle de load balancing Par défaut tous les ports : *
<code>proto="udp"   "tcp"   "arp"</code>	<ul style="list-style-type: none"> <li>• <code>proto="udp"</code> règle de load balancing pour le trafic UDP</li> <li>• <code>proto="tcp"</code> règle de load balancing pour le trafic TCP</li> <li>• <code>proto="arp" avec filter="on_addr" et vmac_directed</code> règle de load balancing pour les réponses aux requêtes de résolution IP ↔ MAC (ARP pour IPv4, Neighbor Discovery pour IPv6). Pour plus de détails, voir la <a href="#">section 13.6.7.3</a>.</li> </ul>
<code>filter="on_addr"   "on_port"   "on_ipid"</code>	<ul style="list-style-type: none"> <li>• <code>filter="on_addr"</code> La règle de load balancing est réalisée sur l'adresse IP client en entrée.</li> <li>• <code>filter="on_port"</code></li> </ul>

	<p>La règle de load balancing est réalisée sur le port client en entrée.</p> <ul style="list-style-type: none"><li>• <code>filter="on_ipid"</code></li></ul> <p>La règle de load balancing est réalisée sur l'<code>ip_id</code> en entrée. Utile pour UDP seulement</p>
--	--

### 13.6.7 <vip> Description

#### 13.6.7.1 <vip> prérequis

Voir les prérequis réseau décrits en [section 2.3.2](#).

#### 13.6.7.2 Qu'est-ce que le type "`vmac_invisible`" ?

La configuration `type="vmac_invisible"` associe une adresse MAC virtuelle à l'adresse IP virtuelle. Avec une adresse MAC virtuelle, les paquets émis vers l'adresse IP virtuelle sont reçus par tous les serveurs. Dans un module noyau, chaque serveur décode le paquet réseau et l'accepte ou le rejette. Après une sélection à très bas niveau des paquets réseau, l'application sur le serveur gère seulement le trafic réseau sélectionné par le module noyau.

Le mécanisme d'adresse MAC virtuelle consiste à associer une adresse MAC unicast dite virtuelle à l'adresse IP virtuelle. Quand un routeur ou une machine réseau recherche l'adresse IP virtuelle, les serveurs SafeKit répondent avec l'adresse MAC virtuelle (via le protocole standard). Cependant, chaque serveur utilise son adresse MAC physique pour communiquer. Ainsi, l'adresse MAC virtuelle est invisible et non localisable par les switchs Ethernet. Par défaut, les switchs émettent ce type de paquet sur tous leurs ports (flooding), ceux-ci sont alors reçus par tous les serveurs de la ferme.

Avec la technologie d'adresse MAC virtuelle, le reroutage en cas de panne et de reprise est immédiat. Tous les équipements conservent l'association adresse IP virtuelle, adresse MAC virtuelle dans leur cache ARP.



Lorsque vous exécutez SafeKit dans une machine virtuelle, il peut être nécessaire d'activer le mode promiscuous sur l'adaptateur réseau virtuel. Voir [SK-0099](#) pour la procédure à suivre pour Hyper-V et VMware ESXi.

Pour tester une adresse MAC virtuelle sur votre réseau, faire d'abord le test de compatibilité décrit en [section 4.3.7](#).

#### 13.6.7.3 Qu'est-ce que le type "`vmac_directed`" ?

La configuration `type="vmac_directed"` modifie le fonctionnement du filtre. Dans ce mode, il n'y a pas de MAC virtuelle ; vu de l'extérieur, l'adresse IP virtuelle se comporte comme une adresse IP normale :

- Les clients émettent des requêtes de résolution d'adresses IP ↔ MAC pour la VIP (protocole ARP pour IPv4 et Neighbor Discovery pour IPv6).
- Chaque serveur répond à la requête avec sa propre adresse MAC. Pour éviter ces réponses multiples, rajouter la règle de load balancing suivante :

```
<loadbalancing_list>
  <group name="FarmProto">
    <rule proto="arp" filter="on_addr"/>
  ...
```

Les réponses seront réparties entre les nœuds en fonction de l'adresse source de l'émetteur de la requête.

- Le client stocke la MAC physique reçue dans son cache d'adresses MAC. Tout trafic ultérieur vers la VIP est envoyé sur cette adresse.
- Le module noyau filtre les paquets entrants à destination de la VIP et les transmet au serveur désigné par l'algorithme de répartition de charge, qu'il s'agisse du nœud local ou d'un autre nœud du cluster.

Le mode `vmac_directed` peut introduire un délai de basculement pour les clients ayant mis en cache la VIP avec la MAC d'un serveur devenu indisponible. Ce comportement est similaire à celui observé en cas de basculement de la VIP dans un module miroir (avec `<real_interface>`). La VIP redevient accessible une fois que ce client met à jour la résolution IP ↔ MAC pour la VIP. Les autres clients de la ferme ne sont pas affectés.

Lorsque la VIP est de type IPv4, le cache ARP des clients n'est normalement mis à jour qu'à l'expiration de l'entrée ARP. Pour accélérer cette mise à jour et minimiser le délai de basculement, positionner `arpreroute="on"` comme décrit ci-dessous :

```
<vip>
  <interface_list>
    <interface arpreroute="on" [arpinterval="60s"] [arpelapse="1200s"]>
      <virtual_interface type="vmac_directed">
...

```

Cette option active le démon `arpreroute` qui envoie des Gratuitous ARP afin d'inciter les clients à mettre à jour leur entrée ARP sans attendre son expiration. Par défaut, le démon envoie des Gratuitous ARP toutes les 60 s (`arpinterval`) pendant 1200 secondes (`arpelapse`).

Lorsque la VIP est de type IPv6, aucune configuration supplémentaire n'est nécessaire. Le protocole Neighbor Discovery gère en effet automatiquement la détection des voisins et la mise à jour du cache des clients lorsqu'un voisin devient indisponible ou change d'adresse MAC.

### 13.6.7.4 Comment fonctionne le load balancing ?

Dans un module kernel, l'algorithme de load balancing est réalisé par filtrage sur les l'identité des paquets en réception. Cette identité est définie par configuration dans `userconfig.xml` : adresse IP client, port client ... (i.e. : load balancing de niveau 4). L'identité est passée dans une table de hachage (une bitmap de 256 bits) qui indique si le paquet doit être accepté ou rejeté sur le serveur. Un seul filtre accepte le paquet dans la ferme de serveurs. Quand un serveur est défaillant, le protocole membership reconfigure les filtres pour redistribuer le trafic du serveur défaillant sur les serveurs disponibles.

Chaque serveur peut avoir un poids (=1, 2...) et prendre plus ou moins de trafic. Le poids est mis en œuvre par le nombre bits à 1 dans la table de hachage (la bitmap de 256 bits).



Un exemple de bitmap est donné en [section 4.3.5](#).

## 13.7 Réplication de fichiers - `<rfs>`, `<replicated>`

### Module miroir uniquement

La réplication de fichiers (RFS) permet d'assurer la haute disponibilité, synchronisation immédiate et tolérance aux pannes des données critiques.

La configuration de RFS est soumise aux restrictions suivantes :

- Sur Linux, vous devez définir la même valeur pour les `uid/gid` sur les deux nœuds pour la réplication des permissions sur les fichiers. Lors de la réplication d'un point de montage du système de fichiers, vous devez appliquer une procédure spéciale décrite en [section 13.7.4.2](#).
- Sur Windows, il est vivement recommandé d'activer le journal USN sur le lecteur contenant le répertoire répliqué, comme décrit en [section 13.7.4.3](#).
- Sur Windows, le déplacement d'un fichier vers la Corbeille à l'aide de la touche Suppr dans l'Explorateur de fichiers n'est pas pris en charge. Seule la suppression définitive à l'aide de Shift + Suppr est supportée.
- Les répertoires répliqués sont accessibles en écriture uniquement sur le nœud primaire
- L'arborescence répliquée ne peut contenir de chemins avec des espaces qu'en Windows
- Les liens physiques (hard links) et les transactions de système de fichiers sous Windows ne sont pas pris en charge



Si vous exécutez plusieurs modules simultanément, les répertoires répliqués doivent être différents pour chaque module.

### 13.7.1 <rfs> Exemple

- Exemple en Windows

```
<rfs>
  <replicated dir="c:\safedir"/>
</rfs>
```

- Exemple en Linux

```
<rfs>
  <replicated dir="/safedir"/>
</rfs>
```



Voir aussi l'exemple complet en [section 15.1](#). Pour la configuration d'un réseau de réplication dédié, voir la [section 15.1.2.2](#). Elles présentent la configuration via la console web ainsi que le `userconfig.xml` correspondant.

### 13.7.2 <rfs> Syntaxe

```
<rfs
  [acl="on"|"off"]
  [async="second"|"none"]

  [iotimeout="300s"]
  [roflags="0x10"|"0x10000"]
  [locktimeout="100s"]
  [sendtimeout="30s"]

  [nbrei="6"]
  [ruzone_blocksize="8388608"]
  [namespacepolicy="0"|"1"|"3"|"4"]
```

```
[reitimeout="150s"]
[reicommitt="0"]
[reidetail="on"|"off"]
[allocthreshold="0"]
[nbremconn ="1"]


[checktime="22000ms"]
[checkintv="120s"]


[nfsbox_options="cross"|"nocross"]
[scripts="off"]
[reiallowdbw="20000"]
[syncdelta="0m"]
[syncat="planification de la synchronisation"]
>
<replicated dir="absolute path of a directory"
  [mode="read_only"]>
  <tocheck path="relative path of a file or subdir" />
  <notreplicated path="relative path of a file or subdir" />
  <notreplicated regxpath="regular expression on relative path of a file or
subdir" />
  ...
</replicated>
</rfs>
```







Seuls les attributs `async`, `nbrei`, `reitimeout` et `reidetail` du tag `<rfs>` peuvent être modifiés par une configuration dynamique. Le tag `<flow>`, qui décrit le flux de réplication, peut également être changé dynamiquement.


### 13.7.3 <rfs>, <replicated> Attributs



<rfs	
[acl= "on"   "off"]	<p>Active la réplication des ACLs sur les fichiers et répertoires. Valeur par défaut : <code>off</code></p> <p><b>Restrictions sur Windows</b></p> <p>La réplication des ACLs ne fonctionnera pas si le compte SYSTEM n'a pas les droits "Full control" sur toute la forêt répliquée. Le service <code>safeadmin</code> s'exécute dans le compte SYSTEM.</p> <p> Les ACLs sont répliqués littéralement (SID), sans translation, donc les ACLs "local users/groups" ne sont pas utilisables sur le serveur distant.</p> <p>Le cryptage et la compression des fichiers ne sont pas supportés.</p>
[async= "second"   "none"]	<p>Positionner <code>async="second"</code> améliore les performances de la réplication de fichiers : les opérations d'écriture répliquées sont mises en cache sur le serveur secondaire et les acquittements sont envoyés plus rapidement au serveur primaire.</p>



	<ul style="list-style-type: none"> <li>• <code>async="none"</code> Cela assure plus de sécurité : les opérations d'écriture répliquées sont mises sur disque avant d'envoyer les acquittements au serveur primaire.</li> <li>• <code>async="second"</code> En cas de double panne simultanée des 2 serveurs <code>PRIM</code> et <code>SECOND</code>, si le serveur <code>PRIM</code> ne peut pas redémarrer, alors le serveur <code>SECOND</code> n'a pas les données à jour sur son disque. Il y a perte de données si on force le serveur <code>SECOND</code> à redémarrer en primaire avec la commande <code>prim</code>.</li> </ul> <p>Valeur par défaut : <code>second</code></p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>
<p><code>[packetsize]</code></p>	<p><b>Linux seulement</b></p> <p>Taille maximale en octet des paquets de réplication NFS. Elle doit être inférieure ou égale à la taille maximale des paquets supportée par le serveur NFS des 2 serveurs. Quand cet attribut est affecté dans la configuration, il est utilisé pour affecter <code>rsize</code> et <code>wsize</code> au montage NFS.</p> <p>Par défaut, la taille est celle du serveur NFS.</p>
<p><code>[reipacketsize = "8388608"]</code></p>	<p>Taille maximale en octets des paquets de réintégration.</p> <p>En Linux, cette taille doit être inférieure ou égale à <code>packetsize</code>.</p> <p>Valeur par défaut en Linux : valeur de <code>packetsize</code> si elle est affectée dans la configuration et est <math>&lt; 8388608</math>; sinon <code>8388608</code></p> <p>Valeur par défaut en Windows : <code>8388608</code> octets</p>
<p><code>[ruzone_blocksize="8388608"]</code></p>	<p>Taille en octet d'une zone pour la bitmap de modification d'un fichier.</p> <p>Ça doit être un multiple de l'attribut <code>reipacketsize</code>.</p> <p>Valeur par défaut : valeur de <code>reipacketsize</code> si elle est affectée dans la configuration ; sinon <code>8388608</code></p>
<p><code>[iotimeout="300s"]</code></p>	<p><b>Windows seulement</b></p> <p>Timeout en seconde sur les IO gérées dans le filtre file system Windows. Si une IO ne peut pas être répliquée et si le timeout du filtre expire, alors le serveur <code>PRIM</code> devient <code>ALONE</code>.</p> <p>Valeur par défaut : <code>300s</code> (300 secondes)</p>






	<p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[roflags="0x10"   "0x10000"]</pre>	<p><b>Windows seulement</b></p> <ul style="list-style-type: none"> <li>roflags="0x10" Pour garantir la cohérence des données répliquées sur les 2 serveurs, la modification des répertoires/fichiers répliqués ne doit avoir lieu que sur le serveur PRIM. Si des modifications ont lieu sur le serveur SECOND, celles-ci sont notifiées dans le journal du module avec l'identification du processus responsable afin que l'administrateur puisse corriger cette anomalie. C'est le comportement avec roflags="0x10".</li> <li>roflags="0x10000" Depuis SafeKit 7.4.0.31, le module peut en plus être arrêté sur le serveur SECOND en définissant roflags="0x10000".</li> </ul> <p>Valeur par défaut : 0x10</p>
<pre>[locktimeout= "100s"]</pre>	<p>Timeout en secondes des requêtes répliquées. Si une requête ne peut pas être traitée dans cet intervalle de temps, le serveur PRIM devient ALONE</p> <p>Valeur par défaut : 100s (100 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[sendtimeout= "30s"]</pre>	<p>Depuis SafeKit&gt; 7.4.0.5</p> <p>Timeout en secondes pour l'envoi de paquets TCP au nœud distant. Si l'envoi du paquet n'a pas pu être effectué dans le délai imparti, le serveur PRIM devient ALONE. Augmentez cette valeur en cas de réseau lent.</p> <p>Valeur par défaut : 30s (30 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p> <p> Dans SafeKit 7.4.0.5, la valeur par défaut était de 120 secondes.</p>
<pre>[nbrei="6"]</pre>	<p>Nombre de threads de réintégration s'exécutant en parallèle pour resynchroniser les fichiers.</p> <p>Valeur par défaut : 6</p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>





	<p> La valeur par défaut valait 3 avant SafeKit 8.2.5.3.</p>
<pre>[namespacepolicy="0" "1" "3" "4"]</pre>	<ul style="list-style-type: none"> <li>• namespacepolicy="0" pour désactiver la synchronisation par zones sur Windows ou Linux.</li> <li>• namespacepolicy="1" En Windows, la réintégration par zones ne peut être assurée après l'arrêt propre du module, puis reboot du serveur.</li> <li>• namespacepolicy="3" En Windows, cela permet la réintégration par zones après reboot quand cela est possible. Cette option exploite l'USN journal du volume qui contient le répertoire répliqué (voir la commande <code>fsutil usn</code> pour la création du journal). Malgré cette option, la réintégration complète doit être appliquée lorsque :             <ul style="list-style-type: none"> <li>o l'USN journal associé au volume a été détruit/recréé par l'administrateur</li> <li>o une discontinuité dans le journal est détectée</li> </ul> </li> <li>• namespacepolicy = "4" Lorsque la synchronisation par zones n'est pas possible (lors de la première réintégration ou lorsque les zones ne sont pas disponibles), les fichiers devant être synchronisés sont entièrement copiés. Si cette réintégration ne se termine pas, la suivante copiera à nouveau ces fichiers. Pour éviter cela, définissez <code>namespacepolicy = "4"</code>. Cette option active également la vérification de journal USN en Windows.</li> </ul> <p>Valeur par défaut : 4 pour SafeKit &gt; 7.4.0.5 (non supporté dans les versions antérieures)</p>
<pre>[reitimeout="150s"]</pre>	<p>Timeout en seconde des requêtes de réintégration. Ce timeout peut être augmenté pour éviter les arrêts de réintégration à cause d'une machine primaire chargée.</p> <p>Valeur par défaut : 150s (150 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>
<pre>[reicommit="0"]</pre>	<p><b>Linux seulement</b></p> <p>Positionner <code>reicommit="nb blocks"</code> pour commiter sur disque tous les <code>(nb blocks)*reipacketsize</code> lors de la réintégration d'un fichier (en plus du commit réalisé à la fin</p>



	<p>de la copie). Ceci peut aider la réintégration de gros fichiers mais ralentit le temps de réintégration global.</p> <p>Valeur par défaut : 0 signifie pas de commit intermédiaire.</p>
<pre>[reidetail= "on" "off"]</pre>	<p>Journal détaillé de la réintégration.</p> <p>Valeur par défaut : <code>off</code></p> <p> La valeur de cet attribut peut être modifiée dynamiquement.</p>
<pre>[allocthreshold= "0"]</pre>	<p><b>Windows seulement</b></p> <p>Taille en Go pour appliquer la politique d'allocation avant réintégration.</p> <p>Quand <code>allocthreshold &gt; 0</code>, activation de l'allocation rapide de l'espace disque pour les fichiers à réintégrer sur le nœud secondaire. Cette fonctionnalité permet, quand le fichier est très gros (&gt; 200 Go) et pas encore complètement recopié, d'éviter le timeout de l'écriture du primaire en fin de fichier.</p> <p>Depuis SafeKit 7.4.0.64, la politique d'allocation a changé et est appliquée :</p> <ul style="list-style-type: none"> <li>• pour les nouveaux fichiers (fichiers n'existant pas sur la secondaire quand la réintégration commence)</li> <li>• quand la taille du fichier sur la primaire est <math>\geq</math> <code>allocthreshold</code> (taille en Go)</li> <li>• pour une synchronisation de type <code>full</code>: <ul style="list-style-type: none"> <li>o Lors de la 1ère réintégration</li> <li>o Lors d'un démarrage en réintégration complète (<code>safekit second prim fullsync</code>)</li> <li>o Quand la réintégration par zone est désactivée (<code>namespacepolicy="0"</code>).</li> </ul> </li> </ul> <p>Valeur par défaut : 0 (qui désactive la fonctionnalité)</p>
<pre>[nbremconn="1"]</pre>	<p>Nombre de connexions TCP entre les nœuds primaire et secondaire.</p> <p>Cette valeur peut être augmentée pour améliorer le débit de réplication et de synchronisation lorsque le réseau présente une latence élevée (dans le cloud, par exemple).</p> <p>Valeur par défaut : 1</p>
<pre>[checktime= "22000ms"]</pre>	<p><b>Linux seulement</b></p> <p>Timeout en millisecondes pour une requête null qui vérifie le bon fonctionnement local de la réplication de fichiers. Commande <code>stopstart</code> si le timeout est atteint.</p> <p>Valeur par défaut : <code>22000ms</code> (22000 millisecondes)</p>

	<p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[checkintv= "120s"]</pre>	<p><b>Linux seulement</b></p> <p>Intervalle en secondes entre 2 requêtes null.</p> <p>Valeur par défaut : 120s (120 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[nfsbox_options= "cross" "nocross"]</pre>	<p><b>Windows seulement</b></p> <p>Cette option spécifie la politique à appliquer lorsqu'un reparse point du type <code>MOUNT_POINT</code> est présent dans l'arborescence répliquée. Cette politique est globale à tous les répertoires répliqués.</p> <p>Dans NTFS, les reparse point de type <code>MOUNT_POINT</code> représentent :</p> <ul style="list-style-type: none"> <li>• soit un point de montage NTFS (par exemple <code>D:\directory</code>)</li> <li>• soit un "directory junction" NTFS (en quelque sorte un lien symbolique vers une autre partie du système de fichiers)</li> </ul> <ul style="list-style-type: none"> <li>• <code>nfsbox_options="cross"</code> les points de montages sont évalués avant réplification et le contenu de la cible du point de montage est répliqué, ce qui rend le point de montage équivalent à un répertoire normal. Ce comportement est utile lorsque le répertoire répliqué est la racine d'un système de fichier (par exemple <code>D:\</code>). C'est le comportement par défaut.</li> <li>• <code>nfsbox_options="nocross"</code> les points de montages ne sont pas évalués et sont répliqués en tant que point de montage (fichier de type « reparse point »). Le contenu de la cible du point de montage n'est pas répliqué ou réintégré lorsque le point de montage est sollicité. Ce comportement est utile lorsque la cible du point de montage est située dans un autre répertoire répliqué (fichier de type « junctions »). Par exemple, les bases de données PostgreSQL utilisent des fichiers de ce type.</li> </ul> <p>Valeur par défaut : <code>cross</code></p>
<pre>[scripts= "on"   "off"]</pre>	<p><code>scripts="on"</code> active les callback vers les scripts <code>_rfs_*</code> utilisés pour mettre en œuvre une réplification de données particulière</p> <p>Valeur par défaut : <code>off</code></p>

<pre>[reallocatedbw= "20000"]</pre>	<p>Quand cet attribut est défini, il spécifie la bande passante maximum susceptible d'être utilisée par la phase de réintégration (par exemple 20000 KB/s), en kilo octets par secondes (KB/s).</p> <p>Etant donné l'implémentation retenue, une fluctuation de +/- 10% de la bande passante réellement utilisée est observable.</p> <p> La bande passante utilisée par la réplication n'est pas affectée par ce paramètre.</p> <p>Par défaut : l'attribut n'est pas défini et la bande passante utilisée par la réintégration n'est pas limitée</p>
<pre>[syncdelta="0m"]</pre>	<ul style="list-style-type: none"> <li>• <code>syncdelta &lt;=1</code> l'attribut est ignoré et la politique par défaut de démarrage et de reprise sur panne est appliquée : seul le serveur avec les données à jour peut démarrer en primaire ou effectuer une reprise sur panne.</li> <li>• <code>syncdelta &gt;1</code> la politique par défaut de démarrage et de reprise sur panne est modifiée. Le serveur avec des données non à jour peut devenir primaire mais uniquement si le temps écoulé depuis sa dernière synchronisation est inférieur à la valeur de <code>syncdelta</code> (en minutes).</li> </ul> <p>Valeur par défaut : 0m (0 minute)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[syncat="planification de la synchronisation"]</pre>	<p>Valeur par défaut : réplication temps réel et synchronisation automatique (pas de planification)</p> <p>Utiliser l'attribut <code>syncat</code> pour planifier la synchronisation des répertoires répliqués sur le nœud secondaire à des dates/heures données. Pour plus de détails, voir <a href="#">section 13.7.4.10</a>.</p> <p>Le module doit être démarré pour activer cette fonctionnalité. Une fois synchronisé, le module se bloque dans l'état <code>WAIT (NotReady)</code> jusqu'à la prochaine synchronisation. La planification est basée sur le gestionnaire de tâches du système d'exploitation :</p> <ul style="list-style-type: none"> <li>• en Windows, la tâche est définie comme tâche système</li> <li>• en Linux, la tâche est insérée dans la <code>crontab</code> de l'utilisateur <code>safekit</code></li> </ul> <p>Vous devez simplement configurer <code>syncat</code> avec la syntaxe du gestionnaire de tâche du système. Par exemple, pour une synchronisation quotidienne, après minuit :</p>

	<ul style="list-style-type: none"> <li>• en Windows synccat="/SC DAILY /ST 00:01:00"</li> <li>• en Linux synccat="01 0 * * *"</li> </ul> <p> Voir la documentation de <code>crontab</code> en Unix et de <code>schtasks.exe</code> en Windows, pour une description complète de la syntaxe.</p> <p> Si la configuration ou la planification ne fonctionnent pas correctement, vérifier d'abord les erreurs de syntaxe ou d'utilisation du gestionnaire de tâches du système.</p>
<pre>[mountoversuffix= "suffix"]</pre>	<p><b>Linux seulement</b></p> <p>À la configuration du module miroir, le répertoire répliqué <code>/a/dir</code> est renommé en <code>/a/dirsuffix</code>. Le répertoire <b>/a/dir</b> est créé et c'est :</p> <ul style="list-style-type: none"> <li>• un point de montage vers <code>/a/dirsuffix</code> lorsque le module est démarré</li> <li>• un lien vers <code>/a/dirsuffix</code> lorsque le module est arrêté</li> </ul> <p>Par défaut le suffix est « <code>_For_SafeKit_Replication</code> »</p> <p> S'il y a une défaillance matérielle, le lien symbolique n'est pas restauré. Dans ce cas, vous devez le restaurer manuellement.</p> <p><b>Restriction</b></p> <p> Vous ne pouvez pas spécifier directement une racine de système de fichiers comme répertoire répliqué (car le renommage du répertoire racine ne fonctionne pas). Le contournement est décrit sous <a href="#">SK-0030</a>.</p> <p> Lorsque le module est démarré, <b>NE PAS ACCEDER</b> les fichiers dans <code>/a/dirsuffix</code>, car les modifications ne seront pas répliquées et le système deviendra incohérent. <b>TOUJOURS ACCEDER</b> les fichiers via <code>/a/dir</code>.</p>
<pre>[&lt;flow name="network" &gt; &lt;server addr="IP_1" /&gt; &lt;server addr="IP_2" /&gt; &lt;/flow&gt;]</pre>	<p><b>Ancienne</b> configuration préservée pour la compatibilité ascendante.</p> <p>Quand cette section n'est pas définie, le flux de réplication passe par le heartbeat défini avec <code>ident="flow"</code> s'il y en a un, sinon par la voie du 1<sup>er</sup> heartbeat (pour la description des heartbeats, voir <a href="#">section 13.4</a>).</p> <p>Si vous utilisez cette configuration, il faut assurer la cohérence avec la définition d'un heartbeat avec</p>

	<p>ident=flow" car des règles de failover par défaut sont définies (décrites en <a href="#">section 13.19.4</a>).</p> <p> Le sous-arbre &lt;flow&gt; peut être modifié dynamiquement, pour changer le flux de réplication par exemple.</p> <p>L'attribut name de &lt;flow&gt; nommé le réseau utilisé pour le flux de réplication. network doit être le nom d'un réseau défini dans la configuration du cluster global (voir <a href="#">section 12</a>).</p> <p>Le tag &lt;server&gt; était utilisé dans l'ancienne syntaxe de configuration (avant SafeKit 7.2). Il est supporté pour assurer la compatibilité ascendante, mais ne doit pas être utilisé pour la configuration de nouveaux modules.</p> <p> Vous ne devez pas utiliser dans le même userconfig.xml, la syntaxe de SafeKit 7.1 et celle introduite depuis SafeKit 7.2.</p>
<pre>&lt;replicated</pre>	<p>Définition des répertoires répliqués Mettre autant de sections que de répertoires à répliquer</p>
<pre>dir="abs_path"</pre>	<p>Chemin absolu du répertoire à répliquer.</p> <p> Les espaces dans les chemins ne sont supportés qu'en Windows.</p>
<pre>[mode="read_only"]</pre>	<p>Accès en read-only sur la machine secondaire pour éviter la corruption.</p>
<pre>&lt;notreplicated path="relative" /&gt;</pre>	<p>Path relatif d'un fichier ou d'un sous répertoire d'un répertoire répliqué. Le fichier (ou sous répertoire) est non répliqué. Autant de lignes que de fichiers ou sous répertoire à non répliquer.</p> <p> Les espaces dans les chemins ne sont supportés qu'en Windows.</p>
<pre>&lt;notreplicated regxpath="expression régulière" /&gt;</pre>	<p>Expression régulière sur le nom des entrées sous le répertoire répliqué :</p> <ul style="list-style-type: none"> <li>• Réplication du contenu du répertoire <b>excepté</b> les entrées qui correspondent à l'expression régulière</li> </ul> <p>Par exemple, pour ne pas répliquer les entrées dont l'extension est .tmp ou .bak dans le répertoire /safedir ou ses sous-répertoires :</p> <pre>&lt;replicated dir="/safedir"&gt;   &lt;notreplicated regxpath=".*\.tmp\$" /&gt;   &lt;notreplicated regxpath=".*\.bak\$" /&gt; &lt;/replicated&gt;</pre> <p>Notez que /safedir/conf/config.tmp.swap est répliqué.</p>

	<ul style="list-style-type: none"><li>• Réplication dans le répertoire <b>uniquement</b> des entrées qui correspondent par l'expressions régulière après le ! Par exemple, pour ne répliquer que les entrées dont l'extension est .mdf ou .ldf dans le répertoire /safedir ou ses sous-répertoires :<pre data-bbox="598 421 1393 539">&lt;replicated dir="/safedir"&gt; &lt;notreplicated regexpath="!\.*\.mdf\$" /&gt; &lt;notreplicated regexpath="!\.*\.ldf\$" /&gt; &lt;/replicated&gt;</pre></li></ul> <p data-bbox="563 573 1310 633"> Le renommage entre des fichiers non répliqués et répliqués n'est pas supporté.</p> <p data-bbox="563 678 1374 739">Le moteur d'évaluation des expressions régulières est POSIX Extended regex (voir la documentation POSIX) :</p> <ul style="list-style-type: none"><li>• en Windows, mode insensible à la casse</li><li>• en Linux, mode sensible à la casse</li></ul> <p data-bbox="563 857 1310 981"> Comme les expressions régulières sont définies dans un fichier XML, les caractères spéciaux interprétés par XML comme '&lt;' ou '&gt;' ne peuvent pas être utilisés dans les expressions régulières.</p>
<pre data-bbox="220 1048 512 1108">&lt;tocheck path="relative" /&gt;</pre>	<p data-bbox="563 1014 1382 1142">Path relatif d'un fichier ou d'un sous répertoire dans un répertoire répliqué. Vérifier sa présence avant de démarrer. Evite un démarrage sur un répertoire vide. Mettre autant de lignes que nécessaire.</p>

### 13.7.4 <rfs>Description

#### 13.7.4.1 <rfs> prérequis

Voir les prérequis décrits en [section 2.2.4](#).

En Windows, activez le journal USN sur le lecteur qui contient les répertoires répliqués afin d'activer la réintégration par zones, après redémarrage du serveur, à condition que le module ait été arrêté proprement.

#### 13.7.4.2 <rfs> Linux

Sur Linux, l'interception des données répliquées est basée sur un montage NFS local. Et le flux de réplication entre les serveurs est basé sur le protocole NFS v3 / TCP.

Le montage NFS des répertoires répliqués à partir de clients Linux externe n'est pas supporté. En revanche, le montage d'autres répertoires peut être réalisé avec les commandes standards.

### Procédure pour répliquer un point de montage

Quand un répertoire répliqué est un point de montage, la configuration du module échoue avec l'erreur suivante :

```
Erreur: périphérique ou ressource occupée
```

Dans la suite, nous prenons l'exemple du module PostgreSQL qui définit en tant que répertoires répliqués `/var/lib/pgsql/var` et `/var/lib/pgsql/data`. Le fichier `userconfig.xml` du module contient :

```
<rfs ... >
  <replicated dir="/var/lib/pgsql/var" mode="read_only" />
  <replicated dir="/var/lib/pgsql/data" mode="read_only" />
</rfs>
```

Ces répertoires sont des points de montage comme le montre le résultat de la commande `df -H`. La commande retourne par exemple :

```
/dev/mapper/vg01-lv_pgs_var ... /var/lib/pgsql/var
/dev/mapper/vg02-lv_pgs_data ... /var/lib/pgsql/data
```

Vous devez appliquer la procédure suivante pour configurer le module avec la réplication de ces répertoires.



C'est la même procédure pour tous les points de montage qui doivent être répliqués.

1. démonter les systèmes de fichiers en exécutant :

```
umount /var/lib/pgsql/var
umount /var/lib/pgsql/data
```

2. configurer le module en exécutant :

```
/opt/safekit/safekit config -m postgresql
```

La configuration se termine avec succès.

3. vérifier l'existence des liens symboliques créés lors de la configuration en exécutant `ls -l /var/lib`. La commande retourne :

```
lrwxrwxrwx 1 root root var -> var_For_SafeKit_Replication
lrwxrwxrwx 1 root root data -> data_For_SafeKit_Replication
```

4. éditer `/etc/fstab` et modifier les 2 lignes :

```
/dev/mapper/vg01-lv_pgs_var /var/lib/pgsql/var ext4...
/dev/mapper/vg02-lv_pgs_data /var/lib/pgsql/data ext4...
```

par

```
/dev/mapper/vg01-lv_pgs_var /var/lib/pgsql/var_For_SafeKit_Replication ext4...
/dev/mapper/vg02-lv_pgs_data /var/lib/pgsql/data_For_SafeKit_Replication
ext4..
```

5. monter les systèmes de fichiers en exécutant :

```
mount /var/lib/pgsql/var_For_SafeKit_Replication
mount /var/lib/pgsql/data_For_SafeKit_Replication
```



Appliquez cette procédure sur les deux nœuds si les répertoires répliqués sont des points de montage sur les deux nœuds. Une fois appliquée, vous pouvez utiliser le module comme d'habitude : par exemple `safekit start stop` etc ...

Pour empêcher le démarrage du module quand le répertoire est non monté et vide, vous pouvez insérer dans `userconfig.xml` la vérification de la présence d'un fichier dans le répertoire répliqué. Exemple pour `/var/lib/pgsql/var` (faire de même pour `/var/lib/pgsql/data` en testant un fichier toujours présent dans ce répertoire) :



```
<replicated dir="/var/lib/pgsql/var" mode="read_only">
  <tocheck path="postgres.conf" />
</replicated>
```

A la déconfiguration du module (ou désinstallation du package SafeKit), vous devez appliquer la procédure inverse pour restaurer l'état initial :

1. démonter les systèmes de fichiers en exécutant :

```
umount /var/lib/pgsql/var_For_SafeKit_Replication
umount /var/lib/pgsql/data_For_SafeKit_Replication
```

2. déconfigurer le module en exécutant `/opt/safekit/safekit deconfig -m postgresql`
3. éditer `/etc/fstab` pour y restaurer son état initial
4. monter les systèmes de fichiers en exécutant :

```
mount /var/lib/pgsql/var
mount /var/lib/pgsql/data
```

### 13.7.4.3 <rfs> Windows

Sur Windows, l'interception des données est basée sur un filtre file system. Et le flux de répllication entre les serveurs est basé sur le protocole NFS v3 / TCP.

Certains anti-virus peuvent empêcher le fonctionnement correct de la répllication.

Sur Windows, il est possible de monter à distance un répertoire répliqué. Si vous voulez pouvoir monter avec le nom et non l'adresse IP virtuelle, vous devez positionner les valeurs suivantes dans les bases de registre des deux serveurs SafeKit :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"DisableLoopbackCheck"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters] "DisableStrictNameChecking"=dword:00000001
```

En Windows, pour activer la réintégration par zones après le redémarrage du serveur, lorsque le module a été correctement arrêté, le composant <rfs> utilise le journal NTFS USN pour vérifier que les informations enregistrées sur les zones sont toujours valables après le redémarrage. Lorsque le contrôle réussit, la réintégration par zones peut être appliquée sur le fichier ; sinon, le fichier doit être recopié dans sa totalité.

Par défaut, seul le lecteur système a un journal USN actif. Si les répertoires répliqués sont situés sur un lecteur différent du lecteur système, vous devez créer le journal (avec commande `fsutil usn`).



Voir [SK-0066](#) pour un exemple.

### 13.7.4.4 <rfs> Répllication et reprise sur panne

Avec la répllication de fichiers, l'architecture miroir est particulièrement adaptée à la haute disponibilité des applications base de données avec des données critiques à protéger contre les pannes. En effet, les données du serveur secondaire sont fortement

synchronisées avec celles du serveur primaire. Le serveur est dit à jour et seul un serveur à jour peut démarrer en primaire ou effectuer une reprise sur panne

Si la disponibilité de l'application est plus critique que la synchronisation des données, la politique par défaut peut être relâchée pour autoriser un serveur non à jour à devenir primaire mais uniquement si la date de la dernière synchronisation est inférieure à un délai configurable. Cela est configuré avec l'attribut `syncdelta` du tag `<rfs>` dont la valeur est exprimée en minutes :

- `syncdelta <= 1`

L'attribut est ignoré et la politique par défaut de démarrage en primaire et de reprise sur panne est appliquée. La valeur par défaut 0.

- `syncdelta > 1`

Si le serveur à jour ne répond pas, le serveur non à jour peut devenir primaire mais uniquement si le temps écoulé depuis la dernière synchronisation est inférieur à la valeur de `syncdelta` (en minutes).

Cette fonctionnalité est implémentée à l'aide de :

- la ressource `rfs.synced`

Quand `syncdelta` est `> 1`, la gestion de la ressource `rfs.synced` est activée. Cette ressource est dans l'état `UP` si les données répliquées sont cohérentes et le temps écoulé depuis la dernière synchronisation est inférieur à la valeur de `syncdelta`.

- Le checker `syncedcheck`

Quand `syncdelta` est `> 1`, ce checker est activé. Il affecte la valeur de la ressource `rfs.synced`.

- La règle de failover `rfs_forceuptodate`

Quand `syncdelta` est `> 1`, la règle de failover suivante est valide :

```
rfs_forceuptodate:    if (heartbeat.* == down && cluster() == down &&
rfs.synced == up && rfs.uptodate == down) then rfs.uptodate=up;
```

Cette règle provoque le démarrage en primaire du serveur lorsque le serveur à jour ne répond pas, et à condition que ce serveur soit isolé et considéré synchronisé en fonction de la valeur de `syncdelta`.

### 13.7.4.5 <rfs> Vérification de la réplication

Vous pouvez vérifier que les fichiers sont identiques sur le primaire et le secondaire avec la commande suivante à passer sur la machine `SECOND` : `safekit rfsverify -m AM`. Exécuter `safekit rfsverify -m AM > log` pour rediriger la sortie de la commande dans un fichier nommé `log`.


La sortie de la commande est un journal similaire à celui de la réintégration dans lequel sont indiqués les fichiers à recopier (donc différents).

Quand sur la primaire, il y a de l'activité sur les répertoires répliqués, il se peut qu'une anomalie soit détectée alors qu'il n'y a pas de différence entre les fichiers. Cela se produit dans les cas suivants :

- sur Windows à cause des modifications faites sur disque avant d'être répliquées,
- avec `async="second"` (défaut) car les lectures peuvent dépasser les écritures.

Pour vérifier s'il y a vraiment une incohérence, vous devez relancer la commande sur le serveur secondaire en s'assurant qu'il n'y plus d'activité sur le serveur primaire.

Sur Windows, certains fichiers modifiés avec l'option `SetvalidData` sont systématiquement détectés différents car ils sont étendus sans reset des données : le contenu en lecture des zones étendues est le contenu aléatoire du disque au moment de la lecture.


 Il est fortement recommandé d'exécuter cette commande uniquement lorsqu'il n'y a pas d'accès aux répertoires répliqués sur le primaire.

### 13.7.4.6 <rfs> Fichiers modifiés depuis la dernière synchronisation

Avant de démarrer le serveur secondaire, il peut être utile d'évaluer le nombre de fichiers et la quantité de données qui ont été modifiés sur le serveur primaire depuis l'arrêt du serveur secondaire. Cette fonctionnalité est fournie en exécutant la commande suivante sur le serveur ALONE : `safekit rfsdiff -m AM`. Exécuter `safekit rfsdiff -m AM > log` pour rediriger la sortie de la commande dans un fichier nommé `log`.

Cette commande exécute des vérifications en ligne du contenu des fichiers réguliers du module `AM`. Elle analyse l'arborescence répliquée entièrement et affiche le nombre de fichiers qui ont été modifiés ainsi que la taille qui doit être recopiée. Elle affiche également une estimation du temps total de réintégration. Ceci n'est qu'une évaluation car seuls les fichiers réguliers sont analysés et d'autres modifications peuvent se produire jusqu'à ce que la synchronisation soit exécutée par le serveur secondaire.

Cette commande doit être utilisée avec précaution sur un serveur en production car elle entraîne une surcharge sur le serveur (pour la lecture, avec verrouillage, de l'arborescence et des fichiers). En Windows, le renommage des fichiers peut échouer pendant cette évaluation.

 Il est fortement recommandé d'exécuter cette commande uniquement lorsqu'il n'y a pas d'accès aux répertoires répliqués.

### 13.7.4.7 <rfs> Bande passante de réplication et de réintégration

Le composant de réplication collecte sur le serveur `PRIM` la bande passante utilisée par les opérations d'écritures de réplication et de réintégration.

Deux ressources (`rfs_bandwidth.replication` et `rfs_bandwidth.reintegration`), exprimées en kilo octet par seconde (KB/s), reflètent la bande passante moyenne utilisée respectivement par la réplication et la réintégration durant les 3 dernières secondes.

Si la charge de réplication est très active en écriture, une saturation du lien réseau peut se produire lors de la phase de réintégration, entraînant un ralentissement significatif de l'application. Dans ce cas, l'attribut `<rfs> reiallowedbw` peut être utilisé pour limiter la bande passante utilisée par la phase de réintégration (voir [section 13.7.3](#)). Il faut cependant considérer que la limitation de la bande passante de réintégration allongera la durée de la phase de réintégration.

Il y a aussi 2 nouvelles ressources qui reflètent la bande passante réseau (en KOctets/sec), utilisée entre les processus `nfsbox`, qui s'exécutent sur chaque nœud pour implémenter la réplication et la réintégration :

- `rfs.netout_bandwidth` est la bande passante utilisée en sortie
- `rfs.netin_bandwidth` est la bande passante utilisée en entrée

Vous pouvez observer la valeur de `rfs.netout_bandwidth` sur le primaire ou de `rfs.netin_bandwidth` sur le secondaire pour connaître le taux de modification au moment de l'observation (écriture, création, suppression, ...). L'historique des valeurs de la ressource donne un aperçu de son évolution dans le temps.

La valeur de la bande passante dépend de l'activité applicative, système et réseau. Sa mesure n'est disponible qu'à titre d'information.

### 13.7.4.8 <rfs> Synchronisation par date

Depuis SafeKit 7.2, SafeKit offre la nouvelle commande `safekit secondforce -d date -m AM` qui force le module `AM` à démarrer comme secondaire après avoir copié uniquement les fichiers modifiés après la date spécifiée.



Cette commande doit être utilisée avec précautions car la synchronisation ne copiera pas les fichiers modifiés avant la date spécifiée. Il incombe à l'administrateur de s'assurer que ces fichiers sont cohérents et à jour.

La date est dans le format `YYYY-MM-DD[Z]` ou `"YYYY-MM-DD hh:mm:ss[Z]"` ou `YYYY-MM-DDThh:mm:ss[Z]`, où :

- `YYYY-MM-DD` indique l'année, le mois et le jour
- `hh:mm:ss` indique l'heure, les minutes et secondes
- `Z` indique que la date est exprimée dans le fuseau horaire UTC ; s'il n'est pas spécifié, la date est exprimée dans le fuseau horaire local

Par exemple :

- `safekit secondforce -d 2016-03-01 -m AM` copie uniquement les fichiers modifiés après le 1er Mars 2016
- `safekit secondforce -d "2016-03-01 12:00:00" -m AM` copie uniquement les fichiers modifiés après le 1er Mars 2016 à 12h, heure locale
- `safekit secondforce -d 2016-03-01T12:00:00Z -m AM` copie uniquement les fichiers modifiés après le 1er Mars 2016 à 12h, dans le fuseau horaire UTC

Cette commande peut être utile dans le cas suivant :

- le module est arrêté sur le serveur primaire et une sauvegarde des données répliquées est effectuée (sur un lecteur amovible par exemple)
- le module est arrêté sur le serveur secondaire et les données répliquées sont restaurées à partir de la sauvegarde. Il peut s'agir du premier démarrage ou de la réparation du serveur secondaire.
- le module est démarré sur le serveur primaire qui devient `ALONE`
- le module est démarré sur le secondaire avec la commande `safekit secondforce -d date -m AM` où la date est la date de sauvegarde

Dans ce cas, seuls les fichiers modifiés depuis la date de la sauvegarde seront copiés (dans leur totalité), au lieu de la copie complète de tous les fichiers.



En Windows, la date de modification du fichier sur le serveur secondaire est affectée lorsque le fichier est copié par le processus de réintégration. Par conséquent, `safekit secondforce -d date -m AM`, dont la date est antérieure à la dernière réintégration sur ce serveur, n'a aucun intérêt.

### 13.7.4.9 <rfs> Synchronisation externe

Lors de la première synchronisation, tous les fichiers répliqués sont copiés dans leur totalité du nœud principal vers le nœud secondaire. Lors des synchronisations suivantes, nécessaires lors du redémarrage du nœud secondaire, seules les zones modifiées des fichiers sont recopiées. Lorsque les répertoires répliqués sont volumineux, la première synchronisation peut prendre beaucoup de temps en particulier si le réseau est lent. C'est pourquoi, depuis SafeKit> 7.3.0.11, SafeKit fournit une nouvelle fonctionnalité pour synchroniser un grand volume de données qui doit être utilisée conjointement avec un outil de sauvegarde.

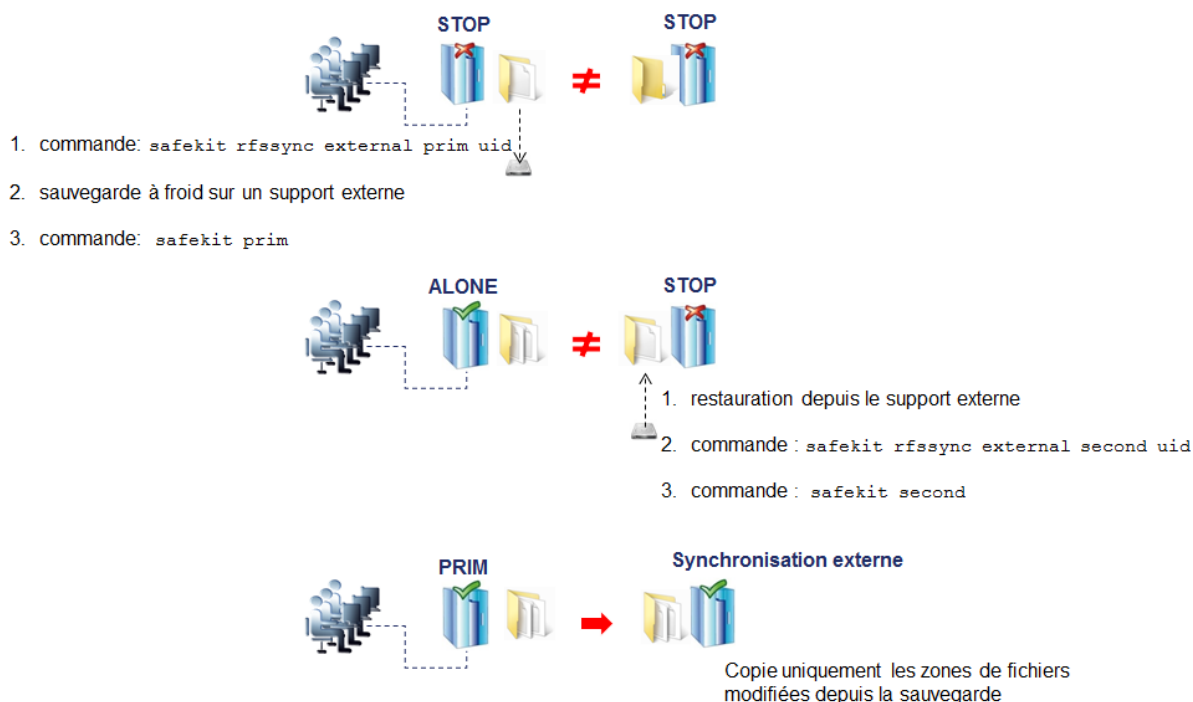
Sur le nœud principal, il suffit d'effectuer une sauvegarde des répertoires répliqués et de passer la politique synchronisation au mode externe. La sauvegarde est transportée (en utilisant un lecteur externe par exemple) et restaurée sur le nœud secondaire, qui est aussi configuré pour effectuer une synchronisation externe. Lorsque le module est démarré sur le nœud secondaire, il recopie uniquement les zones de fichiers modifiées sur le nœud principal depuis la sauvegarde.

La synchronisation externe repose sur une nouvelle commande `safekit rfssync` qui doit être appliquée sur les deux nœuds afin de positionner le mode de synchronisation à `external`. Cette commande prend comme arguments :

- le rôle du nœud (`prim` | `second`)
- un identificateur unique (`uid`)

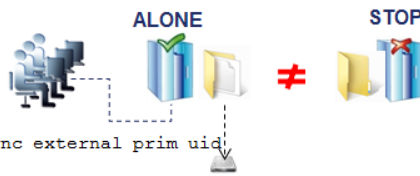
#### Procédure de synchronisation externe

La procédure de synchronisation externe, décrite ci-dessous, est la procédure à appliquer dans le cas d'une sauvegarde à froid des répertoires répliqués. Dans ce cas, l'application doit être arrêtée et toute modification des répertoires répliqués est interdite jusqu'au démarrage du module, et de l'application, en `ALONE (Ready)`. L'ordre des opérations doit être strictement respecté.

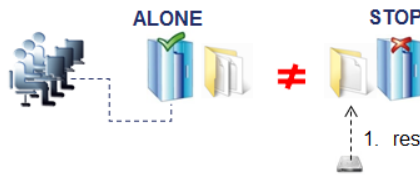


La procédure de synchronisation externe, décrite ci-dessous, est la procédure à appliquer dans le cas d'une sauvegarde à chaud des répertoires répliqués. Dans ce cas, le module

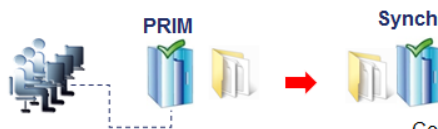
est ALONE (Ready); l'application est démarrée et les modifications du contenu des répertoires répliqués sont autorisées. L'ordre des opérations doit être strictement respecté.



1. commande: `safekit rfssync external prim uid`
2. sauvegarde à chaud sur un support externe




1. restauration depuis le support externe
2. commande: `safekit rfssync external second uid`
3. commande: `safekit second`



Copie uniquement les zones de fichiers modifiées depuis la sauvegarde

### Commande safekit rfssync

<pre>safekit rfssync external prim uid [-m AM]</pre>	<p>Positionne la politique de synchronisation à <code>external</code>. Elle est identifiée par la valeur de <code>uid</code> (max 24 char).</p> <p>Le nœud est le primaire, source pour la synchronisation des données.</p>
<pre>safekit rfssync external second uid [-m AM]</pre>	<p>Positionne la politique de synchronisation à <code>external</code>. Elle est identifiée par la valeur de <code>uid</code> (max 24 char).</p> <p>Le nœud est le secondaire, destination de la synchronisation des données.</p>
<pre>safekit rfssync -d prim uid [-m AM] safekit rfssync -d second uid [-m AM]</pre>	<p>Désactive le contrôle des modifications des répertoires répliqués entre le moment de la sauvegarde à froid/la restauration et le démarrage du module.</p> <p> Cette option doit être utilisée avec précautions puisque la synchronisation externe peut dans ce cas ne pas détecter toutes les modifications à recopier.</p>
<pre>safekit rfssync full [-m AM]</pre>	<p>Positionne la politique de synchronisation à <code>full</code>. Celle-ci entraîne la recopie de tous les fichiers dans leur totalité à la prochaine synchronisation.</p>
<pre>safekit rfssync</pre>	<p>Affiche la politique de synchronisation courante.</p>

### Internes

La politique de synchronisation est représentée par des ressources du module : `usersetting.rfssyncmode`, `usersetting.rfssyncrole`, `usersetting.rfssyncuid` et `rfs.rfssync` :

- `usersetting.rfssyncmode="default"`  
(`usersetting.rfssyncrole="default"`, `usersetting.rfssyncuid="default"`)

Ces valeurs sont associées à la politique de synchronisation standard, celle appliquée par défaut. Elle consiste à ne copier que les zones modifiées des fichiers. Quand cette stratégie ne peut être appliquée, les fichiers modifiés sont recopiés dans leur totalité.

- `usersetting.rfssyncmode="full"`  
(`usersetting.rfssyncrole="default"`, `usersetting.rfssyncuid="default"`)

Ces valeurs sont associées à la politique de synchronisation `full`. Elle est appliquée :

- au premier démarrage du module après sa première configuration
- sur commandes `safekit` (`safekit second fullsync ; safekit prim fullsync ; safekit rfssync full ; safekit primforce ; safekit config ; safekit deconfig`)
- sur changement d'appariement du module

La politique de synchronisation `full` entraîne la recopie de tous les fichiers dans leur totalité à la prochaine synchronisation.

- `usersetting.rfssyncmode="external"`, `usersetting.rfssyncrole="prim" | "second"` and `usersetting.rfssyncuid="uid"`

Ces valeurs sont associées à la politique de synchronisation `external` affectée avec les commandes `safekit rfssync external prim uid` ou `safekit rfssync external second uid`. La prochaine synchronisation appliquera la politique de synchronisation externe.

- `rfs.rfssync="up" | "down"`

Cette ressource vaut `up` uniquement lorsque la politique de synchronisation, définie par les ressources précédentes, peut être appliquée.

Quand la politique de synchronisation n'est pas celle par défaut, celle-ci repasse automatiquement dans le mode par défaut une fois la synchronisation appliquée avec succès. Pour consulter l'état des ressources, voir la [section 7.4](#).

Dans certains cas, la synchronisation externe ne peut être appliquée et le nœud secondaire s'arrête avec une erreur indiquée dans le journal du module. Dans cette situation, il faut soit :

- compléter la procédure de synchronisation externe si celle-ci n'a pas été effectuée dans sa totalité sur les 2 nœuds
- réappliquer complètement la procédure de synchronisation sur les 2 nœuds
- appliquer la politique de synchronisation `full` (commande `safekit rfssync full`)
- appliquer la synchronisation par date, en utilisant la date de la sauvegarde (voir [section 13.7.4.8](#)). Contrairement à la synchronisation externe, la synchronisation par date va copier dans leur totalité (et non par zones) les fichiers modifiés sur le nœud primaire.

### 13.7.4.10 <rfs> Synchronisation planifiée

Par défaut, SafeKit offre la réplication de fichiers en temps réel et une synchronisation automatique. Si la charge est importante sur le nœud primaire ou si le réseau a une forte latence, il peut être préférable d'accepter que le nœud secondaire ne soit pas fortement synchronisé avec le nœud primaire. Pour cela, vous pouvez utiliser l'attribut `syncat` pour planifier une synchronisation régulière des répertoires répliqués sur le nœud secondaire. Le module doit être démarré pour activer cette fonctionnalité. Une fois synchronisé, le module se bloque dans l'état `WAIT (NotReady)` jusqu'à la prochaine synchronisation planifiée. Cette fonctionnalité est implémentée avec :

- la ressource `rfs.syncat` affectée à `up` aux dates planifiées et affectée à `down` une fois le nœud secondaire synchronisé
- la règle de failover `rfs_syncat_wait` qui bloque le nœud secondaire dans l'état `WAIT (NotReady)` jusqu'à ce que la ressource `rfs.syncat` soit `up`

Si vous souhaitez forcer la synchronisation en dehors des dates planifiées, il faut exécuter la commande `safekit set -r rfs.syncat -v up -m AM` quand le module est dans l'état `WAIT (NotReady)`.

La configuration de `syncat` se fait simplement en utilisant la syntaxe du gestionnaire de tâches du système d'exploitation : `crontab` en Linux et `schtasks.exe` en Windows (voir [section 13.7.3](#)).

## 13.8 Scripts du module - <user>, <var>

Cette section décrit uniquement les options de configuration du tag `<user>`. Pour une description complète des scripts, voir la [section 14](#). Quand ce tag n'est pas présent, les scripts du module ne sont pas exécutés.

### 13.8.1 <user> Exemple

```
<user>
  <var name="name1" value="value1" />
</user>
```



Pour un exemple de l'utilisation de `<var>`, voir la [section 15.3](#). Voir aussi l'exemple complet d'un module miroir en [section 15.1](#), et d'un module ferme en [section 15.2](#). Elles présentent la configuration via la console web ainsi que le `userconfig.xml` correspondant.



### 13.8.2 <user> Syntaxe

```
<user
  [nicestoptimeout="300s"]
  [forcestoptimeout="300s"]
  [logging="userlog"|"none"]
  [userlogsize="2048"]
>
  [<var name="name1" value="value1" />]
  ...
</user>
```



Le tag `<user>` et son sous-arbre peuvent être entièrement modifiés dynamiquement.

### 13.8.3 <user>, <var> Attributs

<pre>&lt;user</pre>	
<pre>[nicestoptimeout= "300s"]</pre>	<p>Timeout en secondes pour exécuter les scripts <code>stop_xx</code>.  Valeur par défaut : 300s (300 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[forcestoptimeout= "300s"]</pre>	<p>Timeout en secondes pour exécuter les scripts <code>stop_xx - force</code>  Valeur par défaut : 300s (300 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[logging="userlog"  = "none"]</pre>	<ul style="list-style-type: none"> <li>• <code>logging="userlog"</code> : les messages stdout et stderr de l'application démarrée dans les scripts redirigés dans le journal des scripts dans le fichier <code>SAFEVAR/modules/AM/userlog_&lt;year&gt;_&lt;month&gt;_&lt;day&gt;T&lt;time&gt;_&lt;script name&gt;.ulog</code> où <code>AM</code> est le nom du module (SAFEVAR=C:\safekit\var sur Windows et /var/safekit sur LINUX).</li> <li>• <code>logging="none"</code> : les messages stdout et stderr de l'application démarrée dans les scripts ne sont pas logués</li> </ul> <p>Valeur par défaut : userlog</p>
<pre>[userlogsize="2048"]</pre>	<p>Taille limite en KO du journal des scripts.  Au démarrage du module, le fichier est reseté si sa taille a dépassé la limite.  Valeur par défaut : 2048 KO</p>
<pre>&lt;var   name="ENV_VAR_1"   value="VALUE_1" /&gt;</pre>	<p>Nom de la variable d'environnement et sa valeur exportée avant l'exécution des scripts. Mettre autant de lignes que de variables.</p>

### 13.9 Hostname virtuel - <vhost>, <virtualhostname>

Le hostname virtuel (vhost) permet de présenter un nom d'hôte virtuel aux applications, indépendant du nom réel du serveur. Cela est utile notamment lorsque certaines applications doivent voir un même nom d'hôte sur tous les nœuds, par exemple parce que ce nom est stocké dans un fichier répliqué.

#### 13.9.1 <vhost> Exemple

```
<vhost>
  <virtualhostname name="vhostname" envfile="vhostenv" />
</vhost>
```



Voir l'exemple en [section 15.12](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

### 13.9.2 <vhost> Syntaxe

```
<vhost>
  <virtualhostname
    name="virtual_hostname"
    envfile="path_of_a_file"
    [when="prim"|"second"|"both"]
  />
</vhost>
```



Le tag `<vhost>` et son sous-arbre **ne peuvent pas** être modifiés dynamiquement.

### 13.9.3 <vhost>, <virtualhostname> Attributs

<code>&lt;vhost&gt;</code>	
<code>&lt;virtualhostname</code>	
<code>name="virtual_hostname"</code>	Définition du nom virtuel.
<code>envfile="path_of_envfile"</code>	Chemin d'un fichier d'environnement généré automatiquement par SafeKit à la configuration. Si le chemin du fichier est relatif, le fichier est généré dans les fichiers d'environnement du module, i.e. : <code>SAFEUSERBIN</code> Ce fichier est utilisé dans les scripts pour positionner le hostname virtuel. Voir le module <code>vhost.safe</code> livré avec le package Linux et Windows.
<code>[when="prim" "second" "both"]</code>	Définis quand le hostname virtuel doit être rendu. Par défaut, <code>prim</code> signifie quand le module est primaire ( <code>PRIM</code> ou <code>ALONE</code> ).
<code>/&gt;</code>	
<code>&lt;/vhost&gt;</code>	

### 13.9.4 <vhost> Description

Certaines applications ont besoin de voir le même hostname quel que soit le serveur d'exécution (typiquement, elles stockent le hostname dans un fichier répliqué). Le hostname virtuel peut être présenté à ces applications alors que les autres applications voient le hostname physique des serveurs.

- Sur Linux

La mise en œuvre est basée sur la variable d'environnement `LD_PRELOAD` : les fonctions `gethostname` et `uname` sont surchargées.

- Sur Windows
- La mise en œuvre est basée sur la variable d'environnement `CLUSTER_NETWORK_NAME_` : les fonctions de l'API name query (`GetComputerName`, `GetComputerNameEx`, `gethostname`) sont surchargées.

Pour utiliser `vhost` avec un service, utiliser les commandes `vhostservice` `<service>` [`<file>`] avant/après le démarrage/arrêt du service dans les scripts du module.

### 13.10 Surveillance de processus ou services - `<errd>`, `<proc>`

Cette section décrit les options de configuration disponibles pour la balise `<errd>`. `errd` assure la surveillance des processus et des services critiques au sein d'un module SafeKit. Il détecte automatiquement leur défaillance et déclenche une action corrective telle que le `restart` ou bien le `stop/stopstart` du module, ces 2 dernières provoquant un basculement (failover).

Spécifier `class="prim"` pour activer la surveillance uniquement sur le nœud primaire ✓  
`ALONE | PRIM(Ready)` pour un module miroir.

Spécifier `class="both"` pour activer la surveillance sur tous les nœuds ✓ `UP(Ready)` pour un module ferme.

L'attribut `maxloop` limite le nombre de tentatives de récupération après la détection d'une erreur (voir [section 13.3](#)). Si le problème persiste au-delà de cette limite, le module est arrêté localement et un basculement est initié.



La section `<errd>` nécessite d'avoir défini la section `<user/>`.

#### 13.10.1 `<errd>` Exemple



Voir aussi un exemple complet en [section 15.4](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

##### 13.10.1.1 Surveillance de processus

- Linux et Windows

`myproc` est le nom de la commande associée au processus à surveiller.

```
<errd>
  <proc name="myproc" action="restart" class="prim" />
</errd>
```

- Linux uniquement (pour SafeKit > 7.2.0.29)

`oracle_.*` est une expression régulière sur le nom de la commande associée au processus à surveiller.

```
<errd>
  <proc name="oracle" nameregex="oracle_.*" action="restart" class="prim"/>
</errd>
```



Spécifier `class="prim"` pour un module miroir ; `class="both"` pour un module ferme.

### 13.10.1.2 Surveillance de service

`myservice` est le nom du service à surveiller. En Windows (pour `safeKit > 7.3`), il s'agit du nom du service Windows. En Linux, il s'agit du nom du service `systemd` (pour `safeKit > 7.4.0.19`).

```
<errd>
  <proc name="myservice" service="yes" action="restart" class="prim" />
</errd>
```



Spécifier `class="prim"` pour un module miroir ; `class="both"` pour un module ferme.

### 13.10.1.3 Surveillance de service avec redémarrage ciblé de services

Depuis SafeKit 8.2.6, le nouvel attribut `restart_services` permet d'effectuer un redémarrage ciblé de certains services plutôt qu'un redémarrage global de tous les services. Cet attribut contient les noms des services à redémarrer, listés dans l'ordre de démarrage et séparés par des virgules.

```
<errd>
  <proc name="Service1" service="yes" action="restart"
    restart_services="Service1" class="prim" />
  <proc name="Service2" service="yes" action="restart"
    restart_services="Service2, Service3" class="prim" />
</errd>
```



Spécifier `class="prim"` pour un module miroir ; `class="both"` pour un module ferme.

Dans l'exemple ci-dessus, si `Service2` s'arrête, `errd` déclenche l'action `restart` du module. Cela entraîne l'exécution de `stop_prim` puis `start_prim` avec le paramètre supplémentaire `-Services "Service2, Service3"`. Si les scripts sont conçus pour traiter ce paramètre, ils pourront ainsi arrêter/démarrer uniquement la liste de services spécifiés plutôt que tous les services.

Cette fonctionnalité est particulièrement utile lorsque les services sont indépendants, car elle permet de réduire le temps de redémarrage.

Les modules `mirror.safe` (voir la [section 15.1](#)) et `farm.safe` (voir la [section 15.2](#)), livrés depuis SafeKit 8.2.4, contiennent les scripts `start_xx/stop_xx` qui prennent en charge le paramètre `-Services`.

Si vous migrez en SafeKit 8.2.6 et que votre ancien module n'inclue pas ces nouveaux scripts :

- soit modifiez les scripts existants du module pour gérer le paramètre `-Services`
- soit migrez la configuration existante dans le nouveau modèle de module



Soyez conscient que si les scripts ne prennent pas en charge le paramètre `-Services`, le redémarrage s'appliquera à tous les services malgré la configuration de `restart_services`.

Par ailleurs, si votre ancien module contenait une configuration avec un handler spécifique comme illustré ci-dessous, cette configuration peut éventuellement être

migrée vers la nouvelle implémentation basée sur l'attribut `restart_services` et les scripts du module qui prennent en charge le paramètre `-Services`.

```
<errd>
  <proc name="myservice" service="yes" action="restart_myservice"
    class="myservice"/>
</errd>
```

Cette migration permet de bénéficier d'une meilleure intégration du redémarrage ciblé des services. La configuration avec un handler spécifique devient donc obsolète, bien qu'elle reste prise en charge pour des raisons de compatibilité ascendante.


### 13.10.2 <errd> Syntaxe


```
<errd
  [polltimer="30s"]
>
  <proc name="command name and/or resource name for the monitored process or
service"
  [service="no"|"yes"]
  [nameregex="regular expression on the command name"]
  [argregex="regular expression on process arguments, including command
name"]
  atleast="1"
  action="stopstart"|"restart"|"stop"|"executable_name"
  [restart_services="targeted services to restart, listed in startup order
and separated by commas"]
  class="prim"|"both"|"pre"|"second"|"sec"|"othername"]
  [start_after="nb polling cycles"]
  [atmax="-1"]
  />
  ...
</errd>
```





Le tag `<errd>` et son sous-arbre peuvent être entièrement modifiés dynamiquement.

### 13.10.3 <errd>, <proc> Attributs

<code>&lt;errd</code>	
<code>polltimer="30s"</code>	<p>Temps de polling, en secondes, entre 2 surveillances des processus.</p> <p>Valeur par défaut : 30s (30 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<code>&lt;proc</code>	<p>Définition du processus à surveiller. Autant de lignes que de processus. Une ressource est associée à chaque <code>&lt;proc&gt;</code> et est nommée <code>proc.&lt;valeur de l'attribut name&gt;</code> (par exemple <code>proc.process_name</code>). La ressource vaut <code>up</code> lorsque la condition de surveillance est vraie ; vaut <code>down</code> sinon.</p>

<p><code>name="command_name"</code></p>	<p><i>command_name</i> est le nom de la commande associée au processus à surveiller. C'est aussi le nom de la ressource associée au processus surveillé.</p> <p>Au maximum 15 caractères pour Linux (le nom de la commande peut être tronqué) ; 63 pour Windows.</p> <p>Exemple :</p> <ul style="list-style-type: none"> <li>• sur LINUX, <code>name="vi"</code></li> <li>• sur Windows <code>name="notepad.exe"</code>.</li> </ul> <p> En Windows, le nom est automatiquement converti en minuscule.</p> <p>Pour retrouver le nom des commandes associées aux processus, voir les commandes décrites en <a href="#">section 13.10.4</a></p>
<p><b>Ou</b></p> <p><code>name="service_name"</code> <code>service="yes"</code></p>	<p><i>service_name</i> est le nom du service à surveiller. C'est aussi le nom de la ressource associée au service surveillé.</p> <p>Au maximum, 63 caractères.</p> <p>Exemple :</p> <ul style="list-style-type: none"> <li>• <code>name="W32Time" service="yes"</code> surveille le service de Temps Windows.</li> <li>• <code>name="ntpd" service="yes"</code> surveille le service de Temps Linux (systemd ntpd.service) .</li> </ul> <p>L'attribut <code>service</code> est facultatif et sa valeur par défaut est : <code>no</code>.</p>
<p><b>Ou</b></p> <p><code>name="resource_name"</code> <code>nameregex="regular expression on the command name"</code></p>	<p><b>Linux uniquement</b></p> <p><i>nameregex</i> est une expression régulière sur le nom de la commande pour sélectionner le processus à surveiller.</p> <p><i>name</i> est le nom de la ressource associée au processus surveillé.</p> <p> Comme les expressions régulières sont définies dans le fichier XML <code>userconfig.xml</code>, certains caractères ne peuvent pas être utilisés '&lt;' ou '&gt;'.</p> <p>Exemple :</p> <ul style="list-style-type: none"> <li>• <code>nameregex = "oracle _.*" name = "oracle"</code> surveille les processus oracle dont le nom de la commande respecte l'expression régulière</li> </ul>

	<p>La ressource associée est <code>proc.oracle</code></p> <p>L'attribut <code>nameregex</code> est facultatif.</p>
<pre>class= "prim"  "both"  "pre"  "second"  "sec"  "othername"</pre>	<p>Le processus appartient à une classe.</p> <p>La surveillance est activée/désactivée avec la commande <code>safekit errd enable disable classname -m AM</code>.</p> <ul style="list-style-type: none"> <li><code>class="prim" "both" "pre" "second" "sec"</code></li> </ul> <p>L'activation/désactivation de ces classes est automatique et faite dans le composant <code>&lt;user/&gt;</code> après/avant <code>start_prim/stop_prim</code>, <code>start_both/stop_both</code>, <code>start_second/stop_second</code>, <code>start_sec/stop_sec</code>. Pour une description des scripts, voir <a href="#">section 14</a>.</p> <ul style="list-style-type: none"> <li><code>class="othername"</code></li> </ul> <p>Avec un autre nom de classe, l'activation/désactivation doit être faite explicitement après/avant le démarrage/arrêt des processus de la classe.</p>
<pre>[argregex="regular expression on process arguments"]</pre>	<p>Expression régulière sur la liste des arguments du processus incluant le nom de l'exécutable.</p> <p>Le moteur d'évaluation des expressions régulières est POSIX Extended regex (voir la documentation POSIX) :</p> <ul style="list-style-type: none"> <li>en Windows, mode insensible à la casse</li> <li>en Linux, mode sensible à la casse</li> </ul> <p> Comme les expressions régulières sont définies dans le fichier XML <code>userconfig.xml</code>, certains caractères ne peuvent pas être utilisés '<code>&lt;</code>' ou '<code>&gt;</code>'.</p> <p>Pour retrouver la liste des arguments d'un processus, utiliser les commandes décrites en <a href="#">section 13.10.4</a>.</p> <ul style="list-style-type: none"> <li>Exemple en Linux avec l'éditeur <code>vi</code> sur le fichier <code>myfile</code> <pre>&lt;proc name="vi" argregex=".*myfile.*" ... &lt;proc name="vi" argregex="/myrep/myfile.*" ... &lt;proc name="vi" argregex="/myrep/myfile" ...</pre> </li> <li>Exemple en Windows avec l'éditeur <code>notepad</code> sur le fichier <code>myfile</code> <pre>&lt;proc name="notepad.exe" argregex=".*myfile.*" ... &lt;proc name="notepad.exe" argregex="c:\\myrep\\myfile.*" ... &lt;proc name="notepad.exe" argregex="c:\\myrep\\myfile" ...</pre> </li> </ul>
<pre>action= "restart" </pre>	<p>Action (ou handler) à exécuter sur le module</p>

<pre>"stopstart"  "stop"  "noaction"  "executable_name"</pre>	<ul style="list-style-type: none"> <li>• action="restart" provoque le restart</li> <li>• action="stopstart" provoque le stopstart et éventuellement un basculement</li> <li>• action="stop" provoque le stop et éventuellement un basculement</li> </ul> <p>Les actions restart/stopstart incrémentent le compteur maxloop pour vérifier que l'on n'est pas sur une faute reproductible. Pour la description de maxloop, voir <a href="#">section 13.3</a>.</p> <ul style="list-style-type: none"> <li>• action="noaction" ne provoque pas d'action mais seulement un message dans le journal</li> <li>• action="executable_name"</li> </ul> <p>Pour un handler, soit mettre le chemin absolu du handler, soit mettre le chemin relatif au répertoire bin du module ("SAFE/modules/AM/bin/"). Nous conseillons un chemin relatif avec un handler défini dans le module.</p> <p>Avec un handler spécial, une classe avec un nom propre doit être définie.</p> <p>Pour un handler spécial en Linux, insérer à la fin du script, <code>exit 0</code></p> <p>Pour un handler spécial en Windows, mettre à la fin <code>%SAFEBIN%\exitcode 0</code>. Sinon, c'est un échec et SafeKit exécute stopstart sur le module.</p> <p>Avec un handler spécial, le compteur maxloop n'est pas incrémenté.</p> <p>Utiliser la commande :</p> <pre>safekit incloop -m AM -i &lt;handler name&gt;</pre> <p>Cette commande incrémente le compteur et retourne quand la limite est atteinte.</p> <p> Voir l'exemple décrit en <a href="#">section 15.4</a>.</p> <p>Valeur par défaut : stopstart</p>
<pre>[restart_services= "targeted_services"]</pre>	<p>Depuis SafeKit 8.2.6, l'attribut restart_services permet de redémarrer uniquement certains services au lieu de redémarrer tous les services globalement. Cet attribut contient les noms des services à redémarrer, listés dans l'ordre de démarrage et séparés par des virgules.</p> <p>Supporté uniquement si :</p> <ul style="list-style-type: none"> <li>• service="yes"</li> <li>• action="restart"</li> </ul>



	<ul style="list-style-type: none"> <li>les scripts du module prennent en charge le paramètre <code>-Services</code></li> </ul> <p>Pour une description complète, voir la <a href="#">section 13.10.1.3</a>.</p>
<pre>start_after=[nb polling cycles]</pre>	<p>Sans le paramètre <code>start_after</code>, la surveillance des processus est effective immédiatement.</p> <p>Sinon elle est retardée de <math>(n-1) * polltimer</math> secondes où :</p> <ul style="list-style-type: none"> <li><code>n</code> est la valeur de <code>start_after</code></li> <li><code>polltimer</code> est le paramètre de <code>polling</code> d'<code>errd</code> (30 secondes par défaut)</li> </ul> <p>Par exemple si <code>start_after="3"</code>, la surveillance est retardée de 60 secondes <math>((3-1)*30)</math>.</p> <p>Le paramètre <code>start_after</code> est utile si le processus prend un certain temps à démarrer.</p> <p>Valeur par défaut : 0</p>
<pre>atleast="1"</pre>	<p>Nombre minimum de processus qui doivent s'exécuter. Si le minimum est atteint, SafeKit déclenche l'action.</p> <ul style="list-style-type: none"> <li><code>name="oracle" argregex=".*db1.*" atleast="1"</code> signifie qu'une action est déclenchée si 0 processus s'exécute sur l'instance <code>oracle/db1</code>.</li> <li><code>atleast="-1"</code> l'attribut n'est pas pris en compte.</li> </ul> <p>Valeur par défaut : 1</p>
<pre>atmax="-1"</pre>	<p>Nombre maximum de processus qui peuvent s'exécuter. Si le maximum est atteint, SafeKit déclenche l'action.</p> <p>Avec <code>atmax="0"</code>, une action est déclenchée à chaque démarrage du processus.</p> <p>Valeur par défaut : -1 critère non pris en compte</p>
<pre>&lt;/errd&gt;</pre>	

### 13.10.4 <errd> Commandes



Si la commande est utilisée dans un script du module, alors la variable d'environnement `SAFEMODULE` est positionnée et le paramètre `"-m AM"` n'est pas nécessaire.

<pre>safekit -r errdpoll_running</pre>	<p>Stocke son résultat dans le fichier <code>&lt;SAFEVAR&gt;/errdpoll_reserrd</code> (<code>SAFEVAR = /var/safekit</code> sur Linux ou <code>c:\safekit\var</code> sur Windows) avec une ligne pour chaque processus :</p>
--	--

	<p>&lt;pid&gt; &lt;command name&gt; &lt;command full name and arguments list&gt; (parent=&lt;parent pid&gt;)</p> <p>En Windows, le nom de la commande est affiché en minuscule.</p> <p>Utile pour déterminer le nom des processus à surveiller et leurs arguments pour une configuration &lt;errd&gt;</p>
<pre>safekit errd disable "classname" -m AM</pre>	<p>Suspend la surveillance des processus de la classe <code>classname</code> (pour le module applicatif <i>AM</i>).</p> <p>Doit être explicitement appelé dans les scripts <code>stop_...</code> avant d'arrêter l'application, pour des processus dans des classes différentes de <code>prim</code>, <code>both</code>, <code>second</code>, <code>sec</code>.</p>
<pre>safekit errd enable "classname" -m AM</pre>	<p>Redémarre la surveillance des processus de la classe <code>classname</code> (pour le module applicatif <i>AM</i>).</p> <p>Doit être explicitement appelé dans les scripts <code>start_...</code> après le démarrage de l'application, pour des processus dans des classes différentes de <code>prim</code>, <code>both</code>, <code>second</code>, <code>sec</code>.</p>
<pre>safekit errd off -m AM</pre>	<p>Suspend la surveillance des processus du module <i>AM</i> (sauf les processus SafeKit).</p> <p>Utile lorsque l'on stoppe manuellement l'application et que l'on ne veut pas de détection.</p> <p> Avec SafeKit &lt; 8.2, utiliser <code>safekit errd suspend -m AM</code></p>
<pre>safekit errd on -m AM</pre>	<p>Redémarre la surveillance des processus du module <i>AM</i></p> <p> Avec SafeKit &lt; 8.2, utiliser <code>safekit errd resume -m AM</code></p>
<pre>safekit errd list -m AM</pre>	<p>Liste tous les processus du module <i>AM</i> surveillés incluant les processus SafeKit.</p> <p>La liste peut être également lue dans <code>SAFEVAR/modules/AM/errdlist</code>.</p>
<pre>safekit kill -name="process_name" [-argregex="..."] -level="kill_level"</pre>	<p>Le composant &lt;errd&gt; doit s'exécuter.</p> <p>Tue le(s) processus identifié(s) par le nom et les arguments.</p> <ul style="list-style-type: none"> <li>• <code>level="test"</code> : affiche seulement la liste des processus</li> <li>• <code>level="terminate"</code> : kill les processus en Windows</li> <li>• <code>level="9"</code> : envoie le signal SIGKILL aux processus en Linux</li> <li>• <code>level="15"</code> : envoie le signal SIGTERM aux processus en Linux</li> </ul>

- Exemples Windows ("class CatIRegExp" pour plus d'information):

```
safekit kill -name="notepad.exe"  
-argregex=".*myfile.*" -level="terminate"  
safekit kill -name="notepad.exe"  
-argregex="c:\\myrep\\myfile.*"  
-level="terminate"
```

- Exemples Linux ("man regex" pour plus d'information) :

```
safekit kill -name="vi"  
-argregex=".*myfile.*" -level="9"  
safekit kill -name="vi"  
-argregex="/myrep/myfile.*"  
-level="9"
```

### 13.11 Checkers - <check>

SafeKit apporte des checkers qui testent un élément critique et affecte l'état d'une ressource du module en fonction du résultat du test. Sur détection d'erreur par un checker, la failover machine exécute une action sur le module d'après la règle de failover associée au checker. Pour leur description complète, voir la [section 13.11.3](#).

Les checkers apportés par SafeKit sont :

- ⇒ [Section 13.12](#) « TCP checker - <tcp> »
- ⇒ [Section 13.13](#) « Ping checker - <ping> »
- ⇒ [Section 13.14](#) « Interface checker - <intf> ».
- ⇒ [Section 13.15](#) « IP checker - <ip> »
- ⇒ [Section 13.16](#) « Custom checker - <custom> »
- ⇒ [Section 13.17](#) « Module checker - <module> »
- ⇒ [Section 13.18](#) « Splitbrain checker - <splitbrain> »

#### 13.11.1 <check> Exemple

Tous les checkers se définissent dans une seule section <check> :

```
<check>  
  <!-- Insérer ci-dessous les tags <tcp> <ping> <intf> <ip> <custom> <module>  
  <splitbrain> -->  
</check>
```


#### 13.11.2 <check> Syntaxe

```
<check>  
  <tcp ...>  
    <to .../>  
  </tcp>  
  ...  
  <ping ...>  
    <to .../>  
  </ping>  
  ...
```

```

<intf ...>
  <to .../>
</intf>
...
<ip ...>
  <to .../>
</ip>
...
<custom .../>
...
<module ...>
  [<to .../>]
</module>
...
<splitbrain .../>
</check>

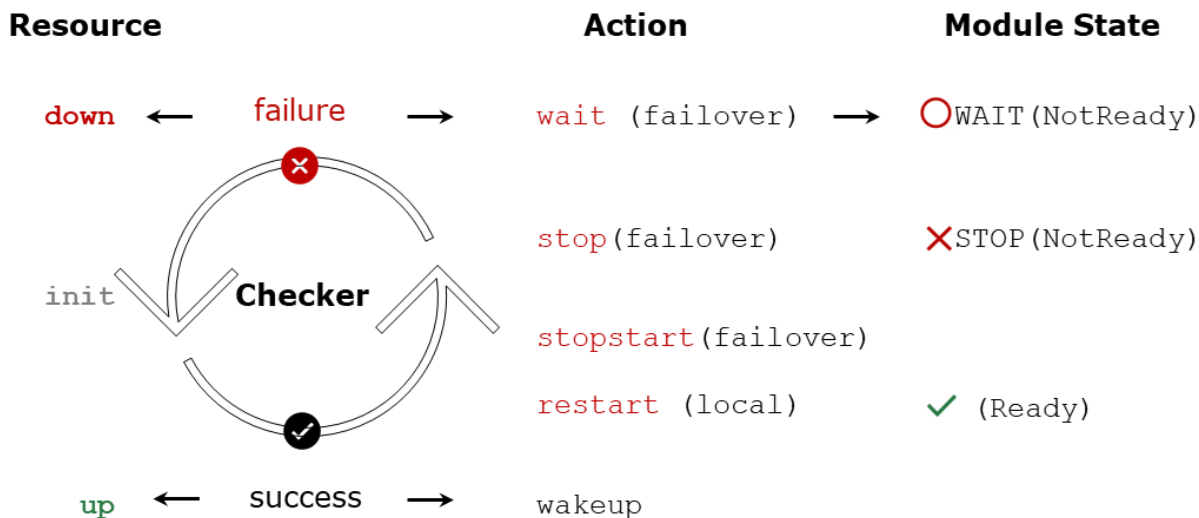
```


 Le tag <check> et son sous-arbre peuvent être entièrement modifiés dynamiquement.



### 13.11.3 <checker> Description

Un checker teste un élément critique (par défaut toutes les 10 secondes) et affecte l'état de la ressource associée, à up ou down, en fonction du résultat du test.


La failover machine évalue les règles de failover et exécute l'action associée au checker lorsque la ressource change d'état.



- L'état initial de la ressource est `init`. La failover machine laisse le module dans l'état  `WAIT (Transient)`, tant qu'au moins une ressource utilisée par une règle avec action `wait` est dans l'état `init`.
- Si le test échoue, la ressource associée est mise dans l'état `down`. La règle de failover associée au checker définit quelle action exécuter dans ce cas. Les actions possibles sur le module sont `restart`, `stop`, `stopstart` ou `wait`.
  - o L'action `restart` provoque le redémarrage local de l'application sans changement d'état du module.

- o Les actions `stop`, `stopstart` et `wait` consistent en l'arrêt du module, par conséquent de l'application, suivi d'un redémarrage automatique dans les cas `stopstart` et `wait`. L'arrêt du module peut entraîner le basculement sur l'autre nœud si celui-ci est  (`Ready`).
- o Lorsque l'action est `wait`, le module se bloque dans l'état  `WAIT (NotReady)` tant que la ressource est `down`.

Les actions `restart`, `stopstart` et `wait` incrémentent le compteur de détection d'erreurs. Lorsque celui-ci dépasse la limite `maxloop` dans l'intervalle de temps `loop_interval` (par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h, voir [section 13.3.3](#)), le module est arrêté définitivement.

- Si le test réussi, la ressource associée est mise dans l'état `up`.  
Cela entraîne l'action implicite `wakeup` si l'action associée est `wait`. Le module sort de l'état  `WAIT (NotReady)` et poursuit son démarrage normal.

La configuration du checker détermine :

- Le nom de la ressource associée
- Optionnellement, le nom de la règle de failover associée ainsi que l'action

### 13.11.3.1 Resource associée au checker

- L'état initial de la ressource est `init`
- Si le test échoue, la ressource associée est mise dans l'état `down`
- Si le test réussi, la ressource associée est mise dans l'état `up`

Pour la description des ressources, voir [section 13.19.4.1](#).

Le nom de la ressource associée au checker est déterminé à partir de sa configuration :

- La classe de la ressource est la valeur du tag XML du checker : `tcp`, `ping`, `intf`, `ip`, `custom`, `module` OU `splitbrain`
- L'id de la ressource est la valeur de l'attribut `ident`

Par exemple, pour la configuration suivante d'un ping checker :

```
<check>
  <ping ident="testR2" action="wait">
    <to addr="R2"/>
  </ping>
</check>
```

la ressource associée se nomme `ping.testR2`.

La valeur courante de la ressource est visible :

- via la console web comme décrit en [section 3.4.4.2](#)
- avec la commande `safekit state -v -m AM` (où `AM` est le nom du module)

```
...
ping.testR2          down          yyyy-mm-dd
```

Les changements d'état de la ressource sont visibles dans le journal du module :

- via la console web comme décrit en [section 3.4.4.1](#)
- avec la commande `safekit logview -A -m AM` (où *AM* est le nom du module)

```
I | Resource ping.testR2 set to up by pingcheck
...
C | Resource ping.testR2 set to down by pingcheck
```

### 13.11.3.2 Règle de failover associée au checker

La règle de failover associée au checker définit quelle action exécuter lorsque sa ressource passe à `down`. Pour la description des règles de failover, voir [section 13.19.4.2](#).

Les actions possibles sur le module sont `restart`, `stop`, `stopstart` ou `wait`.

Le règle de failover associée au checker est déterminé à partir de sa configuration :

- Les checkers `intf`, `ip`, `module` et `splitbrain` ont une règle par défaut prédéfinie qui s'applique à toutes les ressources de ce type :

```
/* rule for module checkers */
module_failure: if (module.? == down) then wait();

/* rule for interface checkers */
interface_failure: if (intf.? == down) then wait();

/* rule for ip checkers */
ip_failure: if (ip.? == down) then stopstart();

/* rules for splitbrain */
splitbrain_failure: if (splitbrain.uptodate == down) then wait();
```

- Les checkers `tcp`, `ping` et `custom` ont une règle générée avec la valeur de l'attribut `action` si celui est défini avec la valeur `stop`, `stopstart`, `restart` ou `wait`.

Par exemple, pour la configuration suivante d'un ping checker

```
<check>
  <ping ident="testR2" action="wait">
    <to addr="R2"/>
  </ping>
</check>
```

la règle générée est :

```
p_testR2 : if (ping.testR2 == down) then wait();
```

Le nom de la règle a pour préfixe la première lettre du nom du checker (`t`, `p` ou `c`), suivie de `_`, puis de la valeur de l'attribut `ident`.

- Les checkers `tcp`, `ping` et `custom` n'ont pas de règle de failover si la valeur de l'attribut `action` dans sa configuration vaut `noaction`. Dans ce cas, l'utilisateur doit rajouter dans la configuration du module la règle de failover associée.

Par exemple, pour la configuration suivante d'un custom checker, la règle de failover est ajoutée explicitement.

```
<check>
  <custom ident="checkfile" exec="checker.ps1"
    arg="c:\safekit\checkfile" when="prim" action="noaction"/>
</check>

<failover>
```

```
<![CDATA[
  checkfile_failure: if( custom.checkfile == down ) then restart();
]]>
</failover>
```

Lorsque la règle de failover est activée, celle-ci est visible :

- via la console web dans l'état détaillé du module décrit en [section 3.4.2.2](#)
- par un message dans le journal du module semblable au suivant :

```
heart | C | Action wait d'après la règle de failover p_testR2
```

Le journal du module pouvant être visualisé :

- via la console web comme décrit en [section 3.4.4.1](#)
- avec la commande `safekit logview -A -m AM` (où *AM* est le nom du module)

### 13.12 TCP checker - <tcp>

Par défaut, il y a une action `restart` du module lorsque le tcp checker détecte un échec de connexion au service TCP.

Depuis SafeKit 8.2.3, l'action peut être configurée avec l'attribut `action` du tag `<tcp>`.



Insérer le tag `<tcp>` dans la section `<check>` si celle-ci est déjà définie.

#### 13.12.1 <tcp> Exemple

```
<check>
  <tcp ident="R1test" when="prim" action="restart" >
    <to addr="R1" port="80"/>
  </tcp>
</check>
```

- La ressource associée au checker se nomme `tcp.R1test` (préfixe `tcp`.)
- La règle de failover générée, qui effectue un `restart` lorsque la ressource passe à `down`, se nomme `t_R1test` (préfixe `t_`). Elle est équivalente à :

```
t_R1test: if (tcp.R1test == down) then restart();
```

Pour une description des checkers, voir la [section 13.11.3](#).



Voir aussi l'exemple en [section 15.5](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

#### 13.12.2 <tcp> Syntaxe

```
<tcp
  ident="tcp_checker_name"
  when="prim|second|both|pre"
  [action=" stop|stopstart|restart|wait|noaction"]
>
  <to
    addr="IP_address" or "name_to_check"
```

```
port="TCP_port_to_check"
  [interval="10s"]
  [timeout="5s"]
/>
</tcp>
```



Le tag <tcp> et son sous-arbre peuvent être entièrement modifiés dynamiquement.

Depuis SafeKit 8.2.3, utilisez l'attribut `action` pour définir l'action à effectuer sur détection d'erreur par le tcp checker.



Avant SafeKit 8.2.3, l'action était statique et définie par la règle de failover par défaut qui s'applique à toutes les ressources de classe `tcp` :

```
tcp_failure: if (tcp.? == down) then restart();
```

### 13.12.3 <tcp> Attributs

<pre>&lt;tcp</pre>	<p>Positionner autant de sections &lt;tcp&gt; qu'il y a de checkers &lt;tcp&gt;.</p>
<pre>  ident="tcp_checker_name"</pre>	<p>Nom du checker TCP. Il définit la ressource associée au checker : <b>tcp.tcp_checker_name</b> (préfixe tcp.)</p>
<pre>  when="prim second both"   [action="stop stopstart restart noaction"]</pre>	<p>Utiliser cette valeur pour tester un service TCP interne à l'application, une fois celle-ci démarrée :</p> <ul style="list-style-type: none"> <li>when="prim" pour une module miroir Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_prim/stop_prim</code></li> <li>when="both" pour une module ferme Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_both/stop_both</code></li> <li>when="second" pour une module miroir Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_second/stop_second</code></li> </ul> <p>Depuis SafeKit 8.2.3, vous pouvez configurer l'action à effectuer en cas de détection d'erreur avec :</p> <ul style="list-style-type: none"> <li>action="stop stopstart restart"</li> <li>stop, stopstart ou restart du module. Le nom de la règle de failover associée est <b>t_tcp_checker_name</b> (préfixe t_)</li> <li>action="noaction"</li> </ul>

	<p>pas de règle de failover générée. L'action doit être écrite explicitement dans le tag <code>&lt;failover&gt;</code> (voir <a href="#">section 13.19</a>).</p> <p>Valeur par défaut : <code>action="restart"</code></p>
<pre>when="pre" action="wait noaction"</pre>	<p>Utiliser cette valeur pour tester un service TCP externe à l'application avant son démarrage :</p> <ul style="list-style-type: none"> <li>when="pre" Le checker est démarré après/arrêté avant, l'exécution des scripts <code>prestart/poststop</code></li> </ul> <p>Depuis SafeKit 8.2.3, vous pouvez configurer l'action à effectuer en cas de détection d'erreur avec :</p> <ul style="list-style-type: none"> <li>action="wait" wait du module. Le nom de la règle de failover associée est <code>t_tcp_checker_name</code> (préfixe <code>t_</code>)</li> <li>action="noaction" pas de règle de failover générée. L'action doit être écrite explicitement dans le tag <code>&lt;failover&gt;</code> (voir <a href="#">section 13.19</a>).</li> </ul>
<code>&lt;to</code>	
<pre>addr="IP_@" or "name"</pre>	<p>Adresse IP ou nom à checker (ex : 127.0.0.1 pour un service local).</p> <p>Adresse IPv4 ou IPv6.</p>
<pre>port="value"</pre>	<p>Port TCP port à checker</p>
<pre>[interval="10s"]</pre>	<p>Temps, en secondes, entre 2 pollings. Valeur par défaut : 10s (10 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[timeout="5s"]</pre>	<p>Délai en secondes pour l'acceptation de la connexion. Valeur par défaut : 5s (5 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<code>&lt;/tcp&gt;</code>	

### 13.13 Ping checker - `<ping>`

Par défaut, il y a un `wait` du module lorsque le ping checker détecte un échec de ping sur l'équipement.

Depuis SafeKit 8.2.3, l'action peut être configurée avec l'attribut `action` du tag `<tcp>`.



Insérer le tag `<ping>` dans la section `<check>` si celle-ci est déjà définie.

### 13.13.1 <ping> Exemple

```
<check>
  <ping ident="testR2" action="wait">
    <to addr="R2"/>
  </ping>
</check>
```

- La ressource associée au checker se nomme `ping.testR2` (préfixe `ping.`)
- La règle de failover générée, qui effectue un `wait` lorsque la ressource passe à `down`, se nomme `p_testR2` (préfixe `p_`) et est équivalente à :

```
p_testR2: if (ping.testR2== down) then wait();
```

Pour une description des checkers, voir la [section 13.11.3](#).



Voir aussi l'exemple en [section 15.6](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

### 13.13.2 <ping> Syntaxe

```
<ping
  ident="ping_checker_name"
  [when="pre|prim|second|both"]
  [action="wait|stop|stopstart|restart|noaction"]
>
  <to
    addr="IP_address" or "name_to_check"
    [interval="10s"]
    [timeout="5s"]
  />
</ping>
```



Le tag `<ping>` et son sous-arbre peuvent être entièrement modifiés dynamiquement.

Depuis SafeKit 8.2.3, utilisez l'attribut `action` pour définir l'action à effectuer sur détection d'erreur par le ping checker.





Avant SafeKit 8.2.3, l'action était statique et définie par la règle de failover par défaut :

```
ping_failure: if (ping.? == down) then wait();
```

### 13.13.3 <ping> Attributs

<code>&lt;ping</code>	Mettre autant de section <code>&lt;ping&gt;</code> qu'il y a de ping checkers.
-----------------------	--

<pre>ident="ping_checker_name"</pre>	<p>Nom du checker ping</p> <p>Il définit la ressource associée au checker : <b>ping.ping_checker_name</b> (préfixe ping.)</p>
<pre>when="pre" action="wait noaction"</pre>	<p>Utiliser cette valeur pour tester un équipement externe à l'application, avant son démarrage :</p> <ul style="list-style-type: none"> <li>when="pre"</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>prestart/poststop</code></p> <p>Depuis SafeKit 8.2.3, vous pouvez configurer l'action à effectuer en cas de détection d'erreur avec :</p> <ul style="list-style-type: none"> <li>action="wait"</li> <li>wait du module. Le nom de la règle de failover associée est <code>p_ping_checker_name</code> (préfixe p_)</li> <li>action="noaction"</li> </ul> <p>pas de règle de failover générée. L'action doit être écrite explicitement dans le tag <code>&lt;failover&gt;</code> (voir <a href="#">section 13.19</a>).</p> <p>Valeur par défaut : <code>when="pre" action="wait"</code></p>
<pre>when="prim second both" [action="stop stopstart restart noaction"]</pre>	<p>Utiliser cette valeur pour tester un équipement après le démarrage de l'application :</p> <ul style="list-style-type: none"> <li>when="prim" pour une module miroir</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_prim/stop_prim</code></p> <ul style="list-style-type: none"> <li>when="both" pour une module ferme</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_both/stop_both</code></p> <ul style="list-style-type: none"> <li>when="second" pour une module miroir</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_second/stop_second</code></p> <p>Depuis SafeKit 8.2.3, vous pouvez configurer l'action à effectuer en cas de détection d'erreur avec :</p> <ul style="list-style-type: none"> <li>action="stop stopstart restart"</li> <li>stop, stopstart ou restart du module. Le nom de la règle de failover associée est <code>p_ping_checker_name</code> (préfixe p_)</li> <li>action="noaction"</li> </ul> <p>pas de règle de failover générée. L'action doit être écrite explicitement dans le tag <code>&lt;failover&gt;</code> (voir <a href="#">section 13.19</a>).</p>

<to	
addr="IP_@ or name"	Adresse IP ou nom à checker Adresse IPv4 ou IPv6.
[interval="10s"]	Intervalle de temps, en secondes, entre 2 pollings. Valeur par défaut : 10s (10 secondes)  Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a> ).
[timeout="5s"]	Délai en secondes sur la réponse au ping. Valeur par défaut : 5s (5 secondes)  Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a> ).
</ping>	

### 13.14 Interface checker - <intf>

Par défaut, il y a un `wait` du module lorsque l'interface checker détecte une erreur sur l'interface.

 Insérer le tag `<intf>` dans la section `<check>` si celle-ci est déjà définie.


#### 13.14.1 <intf> Exemple

```
<check>
  <intf ident="test_eth0">
    <to local_addr="192.168.1.10"/>
  </intf>
</check>
```

- La ressource associée au checker se nomme `intf.test_eth0` (préfixe `intf.`)
- La règle de failover, qui effectue un `wait` lorsqu'une ressource de classe `intf` passe à `down`, est statique et définie par la règle de failover par défaut :

```
interface_failure: if (intf.? == down) then wait();
```

Pour une description des checkers, voir la [section 13.11.3](#).


 Voir aussi l'exemple en [section 15.10](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

#### 13.14.2 <intf> Syntaxe

```
<intf
  ident="intf_checker_name"
  [when="pre"]
```


```
>
  <to
    local_addr="interface_physical_IP_address"/>
</intf>
```

### 13.14.3 <intf> Attributs

<intf	 Les sections <intf> sont automatiquement générées lorsque <interface check="on"> est positionné (voir <a href="#">section 13.6</a> ).
ident="intf_checker_name"	Le nom de l'interface checker (adresse IP du réseau). Il définit la ressource associée au checker : <b>intf.intf_checker_name</b> (préfixe intf.)
[when="pre"]	Valeur fixe <ul style="list-style-type: none"> <li>when="pre"</li> </ul> Le checker est démarré après/arrêté avant, l'exécution des scripts prestart/poststop En cas de détection d'erreur, l'action est wait. Le nom de la règle de failover, <b>interface_failure</b> , est statique et prédéfinie.
<to local_addr="IP_@" />	Adresse IP associée à l'interface à tester. Adresse IPv4 ou IPv6.
</intf>	

### 13.15 IP checker - <ip>

Par défaut, il y a un stopstart du module lorsque l'ip checker détecte que l'adresse IP n'est pas configurée localement. En Windows, il détecte en plus les conflits sur cette adresse.

 Insérer le tag <ip> dans la section <check> si celle-ci est déjà définie.


#### 13.15.1 <ip> Exemple

```
<check>
  <ip ident="ip_check" >
    <to addr="192.168.1.10" />
  </ip>
</check>
```

- La ressource associée au checker se nomme ip.ip\_check
- La règle de failover, qui effectue un stopstart lorsqu'une ressource de classe ip à down, est statique et définie par la règle de failover par défaut :

```
ip_failure: if (ip.? == down) then stopstart();
```



Pour une description des checkers, voir [section 13.11.3](#).

 Voir aussi l'exemple en [section 15.11](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

### 13.15.2 <ip> Syntaxe

```
<ip
  ident="ip_checker_name"
  [when="prim"|"both"]
>
  <to
    addr="IP_address" or "name_to_check"
    [interval="10s"]
  />
</ip>
```

### 13.15.3 <ip> Attributs

<ip	 Les sections <ip> sont automatiquement générées lorsque <virtual_addr check="on"> est positionné (voir <a href="#">section 13.6</a> ).
ident="ip_checker_name"	Nom du checker ip Il définit la ressource associée au checker : <b>ip.ip_checker_name</b> (préfixe ip.)
[when="prim" "both"]	Valeur par défaut <ul style="list-style-type: none"> <li>when="prim" pour une module miroir Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_prim/stop_prim</code></li> <li>when="both" pour une module ferme Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_both/stop_both</code></li> </ul> En cas de détection d'erreur, l'action est <code>stopstart</code> . Le nom de la règle de failover, <b>ip_failure</b> , est statique et prédéfinie.
<to	
addr="IP_@ or name"	Adresse IP locale ou nom DNS à tester. Adresse IPv4 ou IPv6.
[interval="10s"]	Intervalle de temps, en secondes, entre 2 tests. Valeur par défaut : 10s (10 secondes)   Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a> ).

</ip>

### 13.16 Custom checker - <custom>

Un checker personnalisé est un exécutable (script ou binaire) que vous développez pour tester une ressource, l'application.... Il s'agit d'une boucle qui effectue un test suivant une période adéquate. Son rôle est de positionner la ressource associée au checker à "up" ou "down". Puis, une règle de failover décide l'action à exécuter sur le module lorsque la ressource est down.

Depuis SafeKit 8, l'action peut être configurée avec l'attribut `action` du tag `<custom>`.



Insérer le tag `<custom>` dans la section `<check>` si celle-ci est déjà définie. Définir en plus le checker personnalisé.

#### 13.16.1 <custom> Exemple

- Exemple avec `action!="noaction"`

```
<check>
  <custom ident="AppChecker" when="prim" exec="mychecker" action="stopstart"/>
</check>
```

- o La ressource associée au checker se nomme `custom.AppChecker`
- o La règle de failover, qui effectue un `stopstart` lorsque la ressource passe à `down`, se nomme `c_AppChecker` et est équivalente à :

```
c_AppChecker: if (custom.AppChecker == down) then stopstart();
```

- Exemple avec `action="noaction"`

```
<check>
  <custom ident="AppChecker" when="prim" exec="mychecker" action="noaction"/>
</check>
```

Aucune règle de failover n'est générée. L'utilisateur a la possibilité d'en définir une explicitement dans le tag `<failover>`. Par exemple :

```
...
<failover>
  <![CDATA[
    custom_failure: if (custom.AppChecker == down) then stopstart();
  ]]>
</failover>
```

Pour une description des checkers, voir [section 13.11.3](#).



Pour un exemple complet, voir la [section 15.7](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.



Dans SafeKit < 8, l'attribut `action` n'existait pas et l'action était configurée en définissant une règle de failover dans le tag `<failover>` comme l'exemple ci-dessus. C'est pourquoi, la valeur par défaut de l'attribut `action` est équivalente à `"noaction"` est afin de préserver la compatibilité ascendante avec une ancienne configuration.

### 13.16.2 <custom> Syntaxe

```
<custom
  ident="custom_checker_name"
  when="pre|prim|second|both"
  exec="executable_path"
  arg="executable_arguments"
  action="wait"|"stop"|"stopstart"|"restart"|"noaction"
/>
```

### 13.16.3 <custom> Attributs

<pre>&lt;custom</pre>	<p>Positionner autant de sections <code>&lt;custom&gt;</code> qu'il y a de checkers personnalisés.</p>
<pre>  ident="custom_checker_name"</pre>	<p>Nom du checker personnalisé</p> <p>Il définit la ressource associée au checker : <code>custom.custom_checker_name</code> (préfixe <code>custom.</code>)</p> <p>Le checker personnalisé positionne sa ressource avec la commande <code>safekit set -r custom.custom_checker_name -v up down</code>.</p>
<pre>  when="pre"   action="wait" "noaction"</pre>	<p>Utiliser cette valeur pour tester un composant externe à l'application, avant son démarrage :</p> <ul style="list-style-type: none"> <li><code>when="pre"</code></li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>prestart/poststop</code></p> <p>Depuis SafeKit 8, vous pouvez configurer l'action à effectuer en cas de détection d'erreur avec :</p> <ul style="list-style-type: none"> <li><code>action="wait"</code></li> </ul> <p><code>wait</code> du module. Le nom de la règle de failover associée est <code>c_custom_checker_name</code> (préfixe <code>c_</code>)</p> <ul style="list-style-type: none"> <li><code>action="noaction"</code></li> </ul> <p>pas de règle de failover générée. L'action doit être écrite explicitement dans le tag <code>&lt;failover&gt;</code> (voir <a href="#">section 13.19</a>).</p>
<pre>  when="prim" "second" "both"</pre>	<p>Utiliser cette valeur pour tester un composant après le démarrage de l'application :</p> <ul style="list-style-type: none"> <li><code>when="prim"</code> pour une module miroir</li> </ul>

<pre>action="stop" "stopstart" "restart" "noaction"</pre>	<p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_prim/stop_prim</code></p> <ul style="list-style-type: none"> <li>• <code>when="both"</code> pour une module ferme</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_both/stop_both</code></p> <ul style="list-style-type: none"> <li>• <code>when="second"</code> pour une module miroir</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts <code>start_second/stop_second</code></p> <p>Depuis SafeKit 8, vous pouvez configurer l'action à effectuer en cas de détection d'erreur avec :</p> <ul style="list-style-type: none"> <li>• <code>action="stop stopstart restart"</code>  <code>stop</code>, <code>stopstart</code> ou <code>restart</code> du module. Le nom de la règle de failover associée est <code>c_custom_checker_name</code> (préfixe <code>c_</code>)</li> <li>• <code>action="noaction"</code>  pas de règle de failover générée. L'action doit être écrite explicitement dans le tag <code>&lt;failover&gt;</code> (voir <a href="#">section 13.19</a>).</li> </ul>
<pre>exec="executable_path"</pre>	<p>Défini le chemin de l'exécutable du checker customisé (un script ou un binaire).</p> <p>Lorsque le chemin est relatif, le custom checker est recherché dans <code>SAFEUSERBIN</code>. Mettre dans ce cas votre binaire dans <code>SAFE/modules/AM/bin/</code> (pour plus d'information, voir <a href="#">section 10.1</a>).</p> <p>Nous conseillons un chemin relatif avec un exécutable dans le module.</p> <ul style="list-style-type: none"> <li>• En Windows, l'exécutable peut être un binaire ou un script <code>ps1</code>, <code>vbs</code> ou <code>cmd</code>.</li> <li>• En Linux, l'exécutable peut être un binaire ou un script shell.</li> </ul>
<pre>arg="executable_arguments"</pre>	<p>Défini les arguments à passer au checker customisé.</p>

### 13.17 Module checker - <module>

Par défaut, il y a un `wait` du module lorsque le module checker détecte l'indisponibilité d'un autre module SafeKit. Le checker de module effectue également une action `stopstart` lorsqu'il détecte que le module externe a été redémarré (soit par un `restart`, un `stopstart` ou à la suite d'un basculement).

Le checker de module récupère l'état du module en se connectant au service web de SafeKit qui s'exécute sur le serveur sur lequel le module est activé (voir [section 10.9](#)).



Insérer le tag `<module>` dans la section `<check>` si celle-ci est déjà définie.

### 13.17.1 `<module>` Exemple

- Exemple utilisant la configuration par défaut du service web de SafeKit (protocole : HTTP, port : 9010) :

```
<check>
  <module name="mysql">
    <to addr="172.24.190.21" port="9010"/>
  </module>
</check>
```

mysql est le nom du module externe et 172.24.190.21 est son IP virtuelle.

- La ressource associée au checker se nomme `module.mysql_172.24.190.21`
- La règle de failover, qui effectue un `wait` lorsqu'une ressource de classe `module` passe à `down`, est statique et définie par la règle de failover par défaut :

```
module_failure: if (module.? == down) then wait();
```

- Pour le même exemple en utilisant la configuration sécurisée du service web de SafeKit (protocole : HTTPS, port : 9453) :

```
<check>
  <module name="mysql">
    <to addr="172.24.190.21" port="9453" secure="on"/>
  </module>
</check>
```

Pour une description des checkers, voir [section 13.11.3](#).



Pour d'autres exemples, voir la [section 15.9](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.

### 13.17.2 `<module>` Syntaxe

```
<module
  [ident="module_checker_name"]
  name="external_module_name">
  [<to
    addr="IP_@ or name the Safekit server running the external module"
    port="port of the SafeKit web server"
    [interval="10s"]
    [timeout="5s"]
  />]
</module>
```

### 13.17.3 `<module>` Attributs

<code>&lt;module</code>	Positionner autant de sections <code>&lt;module&gt;</code> qu'il y a de checkers de module.
<code>name="external_module_name"]</code>	Nom du checker de module.

<pre>[ident="module_checker_name"]</pre>	<p>Nom du module externe à checker.</p> <p>Il définit la ressource associée au checker :</p> <p><b>module.module_checker_name</b> (préfixe <b>module.</b>)</p> <p>Si cet attribut n'est pas renseigné, le nom de la ressource est construit à partir des attributs <b>name</b> et <b>addr</b> :</p> <p><b>module.external_module_name_address_or_name</b></p>
<pre>[&lt;to</pre>	<p>Définition du/des serveurs exécutant le module externe.</p> <p>Par défaut, le serveur local.</p>
<pre>addr="address_or_name"</pre>	<p>Adresse IP ou nom pour accéder au module externe.</p> <p>Adresse IPv4 ou IPv6.</p>
<pre>port="port du service web de SafeKit"</pre>	<p>Port du service web SafeKit pour le checking.</p> <p>9010 pour HTTP ; 9453 pour HTTPS.</p>
<pre>[interval="10s"]</pre>	<p>Intervalle de temps, en secondes, entre 2 pollings.</p> <p>Valeur par défaut : 10s (10 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[timeout="5s"]</pre>	<p>Délai en secondes pour la réception d'une réponse à la requête check.</p> <p>Valeur par défaut : 5s (5 secondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<pre>[secure="on" "off"]</pre>	<p>Utilisation du protocole HTTP (<b>secure="off"</b>) ou HTTPS (<b>secure="on"</b>)</p> <p>Par défaut : <b>off</b></p>
<pre>/&gt;]</pre>	
<pre>&lt;/module&gt;</pre>	


### 13.18 Splitbrain checker - <splitbrain>


SafeKit offre un checker de split-brain à utiliser pour des architectures miroir. Le split-brain est une situation où, à la suite d'une panne matérielle ou logicielle, les deux nœuds SafeKit deviennent primaires, chaque nœud supposant que l'autre ne fonctionne plus. Ceci implique que l'application tourne sur les deux nœuds et, lorsque la réplication est active, les données peuvent se trouver dans un état incohérent.

Pour prévenir ce phénomène, le checker de split-brain, sur détection d'isolation réseau entre les serveurs, sélectionne un unique nœud pour devenir primaire. L'autre nœud devient non à jour et se bloque dans l'état `WAIT` :

- Jusqu'à ce qu'il reçoive à nouveau les heartbeats de l'autre serveur
- Ou
- Si l'administrateur le juge opportun et s'assure que l'autre serveur n'est plus dans l'état primaire, il peut forcer son démarrage en primaire (par l'exécution des commandes `safekit stop -m AM` puis `safekit prim -m AM`).

L'élection du serveur primaire repose sur le ping d'un composant externe, appelé **witness**. Le réseau doit être configuré de telle manière qu'en cas d'isolation réseau, un seul des deux serveurs a accès au witness (c'est celui-ci qui sera élu primaire). Dans le cas contraire, les deux nœuds deviendront primaires.

- Le ping entre les 2 nœuds et avec le witness doit être ouvert
- 
- Depuis SafeKit 8.2.1, il est possible de définir plusieurs witness. Cela permet de tolérer la panne d'un witness, au moins un devant être accessible.




Insérer le tag `<splitbrain>` dans la section `<check>` si celle-ci est déjà définie.

### 13.18.1 <splitbrain> Exemple

```
<check>
  <splitbrain ident="witness" exec="ping" arg="192.168.1.100 192.168.2.120" />
</check>
```

- La ressource associée au checker se nomme `splitbrain.witness`
- En cas d'isolation réseau entre les nœuds, le split-brain checker affecte la ressource `splitbrain.uptodate` à `up` ou `down` en accord avec l'accès au witness.
- La règle de failover, qui effectue un `wait` lorsque la ressource `splitbrain.uptodate` passe à `down`, est statique et prédéfinie :


```
splitbrain_failure: if (splitbrain.uptodate == down) then wait();
```



Voir aussi l'exemple en [section 15.8](#). Elle présente la configuration via la console web ainsi que le `userconfig.xml` correspondant.


### 13.18.2 <splitbrain> Syntaxe

```
<splitbrain
  ident="witness"
  exec="ping"
  arg="witness1_IP_name witness2_IP_name"
/>
```



Le tag `<splitbrain>` et son sous-arbre peuvent être entièrement modifiés dynamiquement.

### 13.18.3 <splitbrain> Attributs

<splitbrain	Une seule section <splitbrain>.
ident="witness_name"	<p>Nom de checker split-brain</p> <p>Il définit la ressource associée au checker : <b>splitbrain.witness_name</b> (préfixe splitbrain.)</p> <p>Elle représente l'état du ou des witness. La ressource est affectée à :</p> <ul style="list-style-type: none"> <li>• up, si au moins un des witness répond</li> <li>• down, si tous les witness ne répondent pas</li> </ul>
[when="pre"]	<p>Valeur fixe</p> <ul style="list-style-type: none"> <li>• when="pre"</li> </ul> <p>Le checker est démarré après/arrêté avant, l'exécution des scripts prestart/poststop</p> <p>Sur détection de split-brain :</p> <ul style="list-style-type: none"> <li>• Le nœud qui a accès au witness (splitbrain.witness_name="up") affecte la ressource splitbrain.uptodate à up et devient le primaire.</li> <li>• L'autre serveur qui n'a pas accès au witness (splitbrain.witness_name="down") affecte la ressource splitbrain.uptodate à down. Cela déclenche l'action wait de la règle de failover statique et prédéfinie, nommée <b>splitbrain_failure</b>.</li> </ul>
exec="ping"	<p>Valeur fixe.</p> <p>Utilise ping pour tester l'accessibilité au witness et affecte la ressource <b>splitbrain.witness_name</b></p>
arg="witness1_IP_name witness2_IP_name"	<p>Liste des adresses IP ou nom des witness</p> <p>Adresse IPv4 ou IPv6.</p> <p> La définition de plusieurs witness est supportée depuis SafeKit 8.2.1.</p>
</splitbrain>	

### 13.19 Failover machine - <failover>

SafeKit apporte des checkers qui testent un élément critique et affecte l'état de la ressource associée en fonction du résultat du test. Sur détection d'erreur par un checker, la failover machine exécute une action sur le module d'après la règle de failover associée au checker. Pour leur description complète, voir la [section 13.11](#).

Certains composants SafeKit (<heart>, <rfs>, <vipd>, <errd>) gèrent leurs propres ressources et apportent leurs propres règles de failover. Ces dernières ne doivent pas être modifiées ni supprimées, sous peine d'un comportement anormal de SafeKit.

La failover machine évalue régulièrement (par défaut toutes les 5 secondes) l'état global de toutes les ressources et applique une action en fonction des règles de failover qui sont vraies.

Dans un module ferme, la failover machine ne fonctionne que sur les états locaux des ressources alors que dans un module miroir, une règle peut tester une ressource locale ou distante.

Comme les états des ressources transitent par les voies de heartbeat, il est conseillé d'en avoir plusieurs (voir [section 13.4](#)).

Les règles de failover peuvent être écrites dans un langage simple propre à SafeKit ou dans le langage [Lua](#) via l'appel de fonctions SafeKit.

### 13.19.1 <failover> Exemple

Les exemples de règles écrites dans cette section se rajoutent aux règles par défaut ou générées d'après la configuration des checkers.

- Exemple d'ajout d'une règle écrite avec le langage de la failover machine

```
<failover>
  <![CDATA[
    custom_failure: if (custom.AppChecker == down) then stopstart();
  ]]>
</failover>
```


- Exemple d'ajout d'une règle avec le langage Lua et l'appel de la fonction `if_then`

Le préfixe « `--Lua Rules` » indique que la suite de la section doit être interprétée avec l'interpréteur Lua.

```
<failover>
  <![CDATA[
    --Lua Rules
    Rules = Rules +
    {
  custom_failure=if_then("custom.AppChecker","down",Action.stopstart),_group="checker"}
    ]]>
</failover>
```


- Exemple de règle pour désactiver la règle par défaut nommée `ip_failure` et ajouter la règle `allip_failure`

```
<failover>
<![CDATA[
  --Lua Rules
  Rules.disable("ip_failure")
  -- Ajouter ici les éventuelles règles lua destinées à remplacer les règles
  en question, ou écrire les règles legacy dans une autre section CDATA
  ]]>
<![CDATA[
  allip_failure: if (ip.* == down) then stopstart();
  ]]>
</failover>
```




 Utiliser une section `<![CDATA[ ... ]]>` différente pour chaque langage.

### 13.19.2 <failover> Syntaxe

```
<failover [extends="yes"] [period="5000ms"] [handle_time="15000ms"]>
<![CDATA[
  label: if (expression) then action;
  ...
]]>
</failover>
```

 Le tag `<failover>` et son sous-arbre **ne peuvent pas** être modifiés dynamiquement.

### 13.19.3 <failover> Attributs

<code>&lt;failover</code>	
<code>[extends="yes"   "no"]</code>	<ul style="list-style-type: none"> <li><code>extends="yes"</code> les nouvelles règles de failover étendent les règles par défaut (voir <a href="#">section 13.19.4</a>).</li> <li><code>extends="no"</code> les règles par défaut sont écrasées (à éviter) Valeur par défaut : <code>yes</code></li> </ul>
<code>[period="5000ms"]</code>	<p>Période, en millisecondes, entre 2 évaluations. Valeur par défaut : <code>5000ms</code> (5000 millisecondes)</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p>
<code>[handle_time="15000"]</code>	<p>Une action (<code>stop()</code>   <code>stopstart()</code>   <code>wait()</code>   <code>restart()</code>   <code>swap()</code>) doit être stable pendant <code>handle_time</code> (en millisecondes) avant d'être appliquée. Valeur par défaut : <code>15000ms</code> (15000 millisecondes).</p> <p> Unité de temps supportée depuis SafeKit 8.2.5 (voir <a href="#">section 13.1</a>).</p> <p> <code>handle_time</code> doit être un multiple de <code>period</code>.</p>

### 13.19.4 <failover> Description

#### 13.19.4.1 Ressources du module

La syntaxe pour désigner les ressources est la suivante :

```
resource ::= [local. | remote.] 0/1resource_class.resource_id (default: local)
```

```
resource_class ::= ping | intf | tcp | ip | custom | splitbrain | module |  
heartbeat | rfs  
resource_id ::= * | ? | name  
resource_state ::= init | down | up | unknown
```

init	État spécial d'initialisation tant que le checker n'a pas démarré. Si une ressource dans l'état init est testé dans une règle de failover, cette règle n'est pas évaluée tant que la ressource est dans l'état init.
up	État OK
down	État KO
unknown	État inconnu pour une ressource distante (module arrêté sur l'autre nœud)

### 13.19.4.2 Règles de failover

SafeKit apporte des règles de failover par défaut et des règles générées automatiquement en fonction de la configuration des checkers du module. L'utilisateur peut également écrire ses propres règles.

#### Règles de failover par défaut

Les règles de failover par défaut pour les checkers (`module`, `intf`, `ip`, `splitbrain`) sont :

```
<failover>  
<![CDATA[  
  /* rule for module checkers */  
  module_failure: if (module.? == down) then wait();  
  
  /* rule for interface checkers */  
  interface_failure: if (intf.? == down) then wait();  
  
  /* rule for ip checkers */  
  ip_failure: if (ip.? == down) then stopstart();  
  
  /* rules for splitbrain */  
  splitbrain_failure: if (splitbrain.uptodate == down) then wait();  
]]>  
</failover>
```

Il existe en plus :

- Des règles de failover dédiées à la gestion de la réplication, des heartbeats...
- La règle `Implicit_wakeup` qui est appliquée lorsqu'aucune action `wait` n'est applicable. Elle exécute l'action `wakeup`.



Depuis SafeKit 7.5, les règles de failover utilisent une nouvelle syntaxe basée sur le langage Lua.


#### Règles de failover générées

Les checkers `tcp`, `ping` et `custom` ont une règle de failover automatiquement générée lorsque la valeur de l'attribut `action` est définie à `stop`, `stopstart`, `restart` ou `wait`.

Le nom de la règle commence par la première lettre du nom du checker (*t*, *p* ou *c*), suivie de *\_*, puis de la valeur de l'attribut *ident* (par exemple, *p\_router*, *t\_service*, *c\_app*).

### Règles de failover configurées

L'utilisateur peut aussi définir ses propres règles de failover dans la section `<failover><![CDATA[ ... ]]></failover>`. Par défaut, celles-ci s'ajoutent aux règles par défaut et générées.

 Voir les exemples dans la [section 13.19.1](#).

Les règles de failover peuvent être écrites en suivant une des syntaxes suivantes :

- Langage de la failover machine

```
label: if ( expression ) then action;

label ::= string

action ::= stop() | stopstart() | wait() | restart() | swap()

expression ::= ( expression )
| ! expression
| expression && expression
| expression || expression
| expression == expression
| expression != expression
| resource ::= [local. | remote.] 0/1resource_class.resource_id
| resource_state
```

- Langage Lua

- o Appel de la fonction `if_then` pour définir une nouvelle règle

```
--Lua Rules
Rules = Rules +
{ label=if_then("resource","resource_state",action),_group="checker" }

label ::= string

action ::= Action.stop | Action.stopstart | Action.wait | Action.restart
| Action.swap

| resource ::= resource_class.resource_id
| resource_state
```

- o Appel de la fonction `Rules.disable` pour désactiver une règle à partir de son label

```
--Lua Rules
Rules.disable("failover_rule_label")
```

 Utiliser une section `<![CDATA[ ... ]]>` différente pour chaque langage.

### 13.19.4.3 Actions

Les actions `restart()`, `stopstart()`, `stop()`, `swap()` sont équivalentes aux commandes de contrôle (avec le paramètre `-i identity` en plus) décrites en [section 9.3](#).



`maxloop / loop_interval / automatic_reboot` s'appliquent si le paramètre `-i identity` est passé aux commandes (voir [section 13.3](#)). Ce qui est le cas lorsque les commandes sont appelées par la failover machine ou par un checker.



## 14. Scripts du module pour la configuration du module applicatif

- ⇒ [Section 14.1](#) « Liste des scripts »
- ⇒ [Section 14.2](#) « Variables d'environnement et arguments passés aux scripts »
- ⇒ [Section 14.3](#) « Sortie des scripts »
- ⇒ [Section 14.4](#) « Automate d'exécution des scripts »
- ⇒ [Section 14.5](#) « Commandes spéciales SafeKit pour les scripts »



Des exemples de scripts sont donnés en [section 15](#).

Pour activer l'appel des scripts du module applicatif, le tag `<user>` doit être présent dans `userconfig.xml` (voir [section 13.8](#)).

Les scripts doivent être des exécutables :

- en Windows, un exécutable avec l'extension et le type : `.cmd`, `.vbs`, `.ps1`, `.bat` ou `.exe`
- en Linux, tout type d'exécutable

Chaque fois que vous modifiez les scripts, vous devez réappliquer la configuration sur les serveurs (avec la console ou la commande SafeKit).



Au moment de la configuration, les scripts sont copiés de `SAFE/modules/AM/bin` dans le répertoire d'exécution `SAFE/private/modules/AM/bin` (`=SAFEUSERBIN`, ne pas modifier les scripts à cet endroit).

### 14.1 Liste des scripts

Ci-dessous la liste des scripts pouvant être définis par l'utilisateur. Les scripts essentiels sont les scripts `start/stop` qui démarrent et arrêtent l'application au sein du module.

#### 14.1.1 Scripts de démarrage/arrêt

Pour une description détaillée du moment d'appel de ces scripts, se référer à l'automate d'exécution des scripts présenté en [section 14.4](#).

<code>prestart</code>	<code>prestart</code> est appelé au démarrage du module (via la console SafeKit ou la commande <code>safekit start -m AM</code> ). Ce script doit être présent et contenir les appels aux scripts <code>stop_xx</code> pour arrêter l'application avant de mettre en place les ressources du module (IP virtuelle, réplication...).
<code>poststop</code>	<code>poststop</code> est appelé à l'arrêt du module (via la console SafeKit, la commande <code>safekit stop -m AM</code> , ou l'arrêt provoqué par un checker). Ce script est optionnel.
<code>start_prim</code>	<b>Uniquement pour un module miroir</b>

<p>stop_prim</p>	<p>start_prim est appelé lorsque le module va vers les états  PRIM/ALONE (Ready) . Il doit contenir le démarrage des services applicatifs.</p> <p>stop_prim est appelé lorsque le module quitte les états  PRIM/ALONE (Ready) . Il doit contenir l'arrêt des services applicatifs.</p> <p>L'automate d'exécution des scripts garantit que l'application, intégrée dans ces scripts, s'exécute uniquement sur le nœud primaire du module miroir.</p>
<p>start_both stop_both</p>	<p><b>Généralement pour un module ferme</b></p> <p>start_both est appelé lorsque le module va vers l'état  UP (Ready) . Il doit contenir le démarrage des services applicatifs.</p> <p>stop_both est appelé lorsque le module quitte l'état  UP (Ready) . Il doit contenir l'arrêt des services applicatifs.</p> <p>L'automate d'exécution des scripts garantit que l'application, intégrée dans ces scripts, s'exécute sur tous les nœuds du module ferme.</p> <p>Dans le cas exceptionnel où ces scripts sont présents dans un module miroir, ces scripts sont appelés lors des transitions vers ou depuis les états  PRIM/ALONE/SECOND (Ready) . L'automate d'exécution des scripts garantit que l'application, intégrée dans ces scripts, s'exécute sur les nœuds primaire et secondaire du module miroir.</p>
<p>start_second stop_second</p>	<p><b>Exceptionnellement pour un module miroir</b></p> <p>start_second est appelé lorsque le module va vers l'état  SECOND (Ready) .</p> <p>stop_second est appelé lorsque le module quitte l'état  SECOND (Ready) .</p> <p>Ces scripts peuvent contenir des actions à faire/défaire sur un nœud secondaire.</p>
<p>start_sec stop_sec</p>	<p><b>Exceptionnellement pour un module miroir</b></p> <p>start_sec est appelé lorsque le module va vers les états  SECOND/ALONE (Ready) .</p> <p>stop_sec est appelé lorsque le module quitte les états  SECOND/ALONE (Ready) .</p> <p>Ces scripts peuvent contenir des actions à faire/défaire sur un nœud secondaire ou primaire sans secondaire.</p>
<p>transition</p>	<p>transition est appelé lors des principaux changements d'état, tel que décrit en <a href="#">section 14.4</a>.</p>
<p>update</p>	<p>update est appelé lors de la reconfiguration dynamique du cluster ou du module alors que le module est démarré et dans un état stable.</p>



Pour un exemple, voir la [section 15.2.3.2.3](#).

Les scripts de stop, sont appelés 2 fois :



- la 1<sup>ère</sup> fois, pour un arrêt propre (sans le paramètre `force` en premier argument)
- la 2<sup>ème</sup> fois, pour éventuellement un arrêt forcé (avec le paramètre `force` en premier argument)

### 14.1.2 Autres scripts

<code>config</code>	<code>config</code> est appelé dans les premières étapes de la configuration du module (via la console SafeKit ou la commande <code>safekit config -m AM</code> ). Vous pouvez exécuter dans ce script des commandes de configuration applicative.
<code>postconfig</code>	<code>postconfig</code> est appelé dans les dernières étapes de la configuration du module (via la console SafeKit ou la commande <code>safekit config -m AM</code> ). Contrairement au moment de l'appel de <code>config</code> , <code>postconfig</code> dispose d'un accès au contenu final du fichier <code>safeconf.xml</code> , situé dans <code>SAFEUSERCONF</code> . Ce fichier contient l'intégralité de la configuration XML du module, après instantiation des macros.
<code>deconfig</code>	<code>deconfig</code> est appelé lors de la déconfiguration du module (via la console SafeKit ou la commande <code>safekit deconfig -m AM</code> ). La déconfiguration du module est aussi automatiquement effectuée lors de la désinstallation du module. Dans ce script, vous devez « défaire » les actions effectuées dans le script <code>config</code> .
<code>confcheck</code>	<code>confcheck</code> est appelé lors de l'exécution de la commande <code>safekit confcheck -m AM</code> . Vous pouvez exécuter dans ce script des opérations de contrôle de changement de configuration de l'application.
<code>state</code>	<code>state</code> est appelé lors de l'exécution de la commande <code>safekit state -v -m AM</code> .
<code>level</code>	<code>level</code> est appelé lors de l'exécution de la commande <code>safekit level -m AM</code> command.

## 14.2 Variables d'environnement et arguments passés aux scripts

Tous les scripts sont appelés avec 3 paramètres :

- l'état courant (`STOP`, `WAIT`, `ALONE`, `PRIM`, `SECOND`, `UP`)
- le prochain état (`STOP`, `WAIT`, `ALONE`, `PRIM`, `SECOND`, `UP`)
- l'action (`start`, `stop`, `stopstart` ou `stopwait`)



L'argument `stopwait` est passé lors de l'exécution de l'action `wait` provoquée par un checker.

- Les scripts de type `stop` sont appelés 2 fois :
- une première fois pour un arrêt propre de l'application
- une deuxième fois avec l'argument `force` pour un arrêt forcé (avec `force` comme premier argument)

Les variables d'environnement utilisables à l'intérieur des scripts sont :

- `SAFE`, `SAFEMODULE`, `SAFEBIN`, `SAFEUSERBIN`, `SAFEUSERCONF`, `SAFEUSERVAR` (voir [section 10.1](#))



La définition de `SAFEMODULE`, qui contient le nom du module, permet d'omettre l'option `-m AM` avec la commande `safekit` si celle-ci doit s'appliquer au module `SAFEMODULE`.

- toutes les variables définies dans le tag `<user>` de `userconfig.xml` (voir [section 13.8](#)).



Pour un exemple avec les variables d'environnement définies dans le tag `<user>`, voir la [section 15.3](#).

## 14.3 Sortie des scripts

### 14.3.1 Sortie dans le journal du script

Par défaut (`logging="userlog"` dans le tag `<user>` de `userconfig.xml`), les sorties `stdout` et `stderr` du script sont redirigées dans le fichier `SAFEVAR/modules/AM/userlog_<year>_<month>_<day>T<time>_<script name>.ulog` où :

- `SAFEVAR=C:\safekit\var` en Windows et `/var/safekit` en Linux
- `AM` est le nom du module
- `<year>_<month>_<day>T<time>` sont la date et heure d'exécution du script
- `<script name>` est le nom du script exécuté

Pour insérer un `message` dans le journal du script, ajouter la commande suivante dans le script :

```
echo "message"
```

ou en PowerShell :

```
Write-Host "message"
```

### 14.3.2 Sortie dans le journal du module

Pour insérer des messages de niveau E ou I dans le journal du module, ajouter la commande suivante dans le script :

- en Windows

```
"%SAFE%/safekit" printe "message"  
"%SAFE%/safekit" printi "message"
```

- en Linux

```
`${SAFE}/safekit" printe "message"  
`${SAFE}/safekit" printi "message"
```

Les messages de niveau E sont visibles dans le journal non verbeux ; ceux de niveau I dans le journal verbeux.



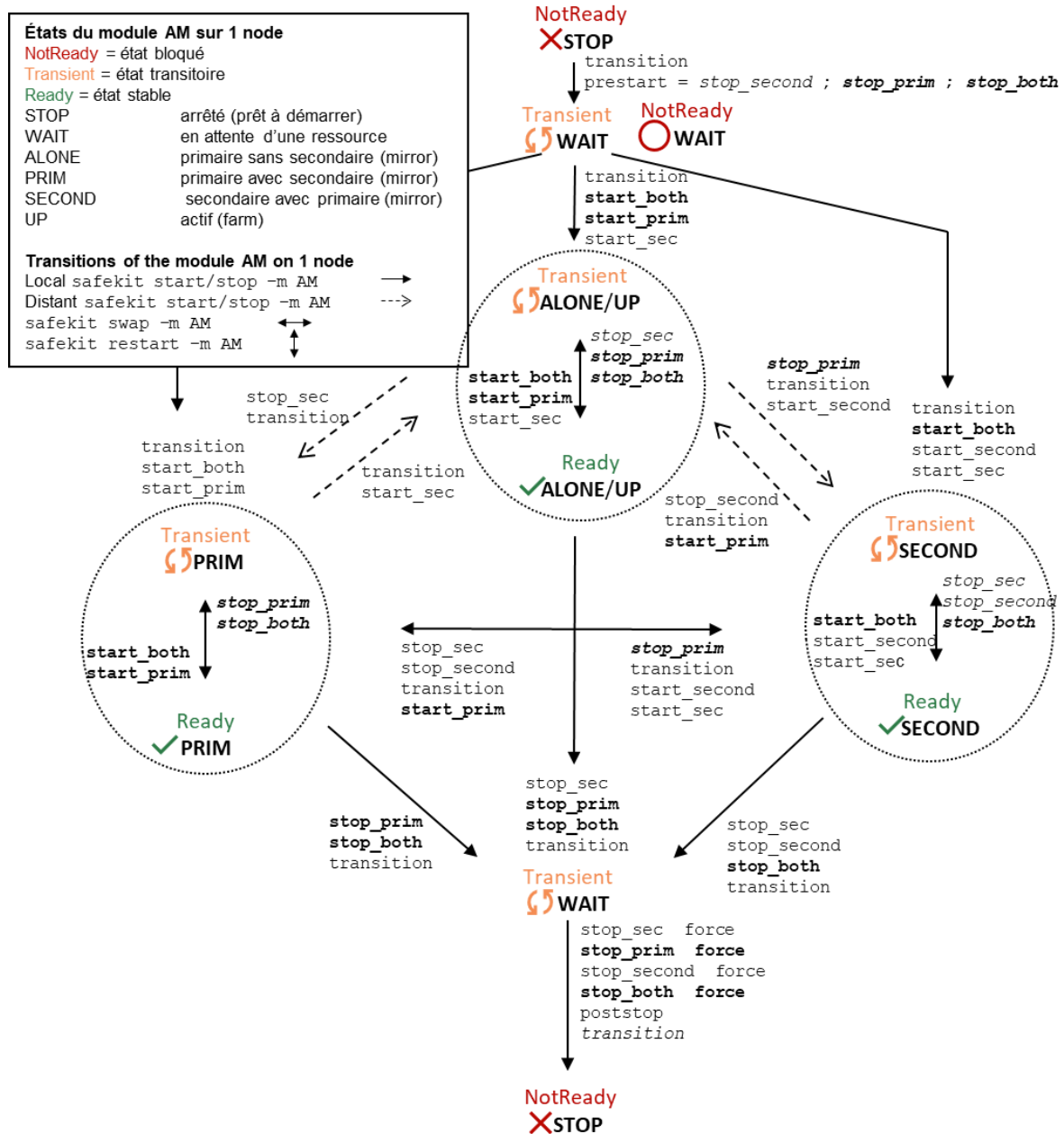
Dans l'environnement d'exécution du script du module *AM*, l'option `-m AM` est inutile pour la commande `safekit`.

### 14.4 Automate d'exécution des scripts

La plupart du temps les scripts stop sont appelés 2 fois (sans l'option force puis avec l'option force). Dans ce cas, le nom du script est en italique.



Par exemple, au démarrage, la première transition de *STOP* vers *WAIT* appelle le script `transition STOP WAIT`.



Depuis SafeKit 8.2.4, lors de l'arrêt du module, les scripts `stop_xxx` avec l'argument `force` peuvent être exécutés un 2<sup>de</sup> fois avant l'appel de `poststop`.

### 14.5 Commandes spéciales SafeKit pour les scripts

Les commandes spéciales sont sous `SAFE/private/bin`. Les commandes peuvent être appelées directement dans les scripts du module avec :

- `%SAFEBIN%\specialcommand` en Windows
- `$(SAFEBIN)/specialcommand` en Linux

En dehors des scripts, il faut utiliser la commande `safekit -r`.

<pre>safekit -r &lt;special command&gt; [&lt;args&gt;]</pre>	<p>&lt;special command&gt; &lt;args&gt; exécuté dans l'environnement SafeKit. Lorsque le path absolu n'est pas spécifié, la commande est recherchée dans <code>SAFEBIN=SAFE/private/bin</code>.</p>
--	---

## 14.5.1 Commandes pour Windows

### 14.5.1.1 Commandes sleep, exitcode, sync

- `%SAFEBIN%\sleep.exe <timeout value in seconds>`  
A utiliser dans les scripts stop car net stop service n'est pas synchrone.
- `%SAFEBIN%\exitcode.exe <exit value>`  
Pour sortir d'un script avec une valeur d'erreur
- `%SAFEBIN%\sync.exe \\.\<drive letter:>`  
Pour synchroniser les caches file system

### 14.5.1.2 Commande namealias

`%SAFEBIN%/namealias [-n | -s ] <alias name>`

-n pour ajouter un nouveau nom NetBIOS en alias (`start_prim`) ou -s pour supprimer un alias NetBIOS (`stop_prim`)

Vous pouvez utiliser la commande SafeKit `netnames` (ou la commande Windows `nbtstat`) pour lister les informations NetBIOS.

## 14.5.2 Commandes pour Linux

### 14.5.2.1 Gestion de la crontab

<pre>\$SAFEBIN/gencron [del   add] &lt;user name&gt; [all  &lt;command name&gt;] -c "&lt;comment&gt;"</pre>	<ul style="list-style-type: none"> <li>• del pour désactiver des entrées dans <code>stop_prim</code> (en insérant des commentaires)</li> <li>• add pour activer des entrées dans <code>start_prim</code> (en retirant les commentaires).</li> <li>• &lt;user name&gt; nom de l'utilisateur dans la crontab</li> <li>• all pour s'appliquer à toutes les entrées</li> <li>• &lt;command name&gt; pour s'appliquer uniquement à au nom de la commande</li> <li>• &lt;comment&gt; entête du commentaire qui sera inséré</li> </ul>
---	---

L'exemple suivant s'applique à l'entrée suivante dans crontab :

```
5 0 * * * $HOME/bin/daily.job >> $HOME/tmp/out 2>&1
```

Pour un module miroir, pour gérer cette entrée sur le primaire, insérer :

- son activation dans `start_prim`  

```
$SAFEBIN/gencron add admin daily.job -c "SafeKit configuration for $SAFEMODULE"
```
- sa désactivation dans `stop_prim`

```
$SAFEBIN/gencron del admin daily.job -c "SafeKit configuration for  
$SAFEMODULE"
```

### 14.5.2.2 Commande bounding

```
$SAFEBIN/boundcmd  
<timeout value> <command  
path> [<args>]
```

- *<timeout value>* temps maximum imparti pour exécuter la commande
- *<command path>* chemin de la commande à exécuter
- *<args>* arguments optionnels de la commande

boundcmd retourne l'exit code de la commande si la commande se termine et 2 sinon.

Par exemple, pour flusher des données sur disque avec un timeout de 30 secondes :

```
$SAFEBIN/boundcmd 30 /bin/sync 1>/dev/null 2>&1
```

### 14.5.3 Commandes pour Windows et Linux

```
safekit -r  
processtree  
list | kill ...
```

Liste les processus en cours d'exécution sous forme d'arbre d'appel (excepté pour l'option all) et arrête les processus (option kill)

- `safekit -r processtree list all`

Liste tous les processus en cours d'exécution.

- `safekit -r processtree list <process command name>`

Liste les processus dont le nom de commande est celui spécifié.

- `safekit -r processtree kill <process command name>`

Liste et arrête les processus en cours d'exécution dont le nom de commande est celui spécifié.

- `safekit -r processtree list | kill <process command name>| all <regular expression on the full command - path and arguments>`

Pour la syntaxe des expressions régulières :



- en Windows, voir class CatIRegExp
- en Linux, voir man regex

- Exemples en Windows


```
safekit -r processtree kill notepad.exe ".*myfile.*"
```

```
safekit -r processtree list all "mirror"
```

- Exemples en Linux

```
safekit -r processtree kill vi ".*myfile.*"
```

```
safekit -r processtree list all "mirror"
```

<pre>safekit incloop -m AM -i &lt;handler name&gt;</pre>	<p>Le module dispose d'un compteur <code>maxloop</code>, du nombre de <code>restart</code>, <code>stopstart</code> et <code>wait</code> du module sur détection d'erreur. Le module est arrêté lorsque ce compteur atteint la valeur <code>maxloop</code> sur la période <code>loop_interval</code>.</p> <p>Lors de l'exécution d'un handler spécial, le compteur <code>maxloop</code> n'est pas incrémenté. Pour l'incrémenter, utiliser la commande :</p> <pre>safekit incloop -m AM -i &lt;handler name&gt;</pre> <p>La commande augmente le compteur <code>maxloop</code> pour le module <code>AM</code> et retourne 1 lorsque la limite est atteinte.</p> <p> Pour un exemple, voir la <a href="#">section 15.4.2</a>.</p>
<pre>safekit resetloop -m AM [-i &lt;handler name&gt;]</pre>	<p>Réinitialise le compteur <code>maxloop</code> pour le module <code>AM</code> (affectation de la valeur à 0)</p>
<pre>safekit checkloop -m AM</pre>	<p>Pour tester le compteur <code>maxloop</code> pour le module <code>AM</code>, utilisez la commande <code>safekit checkloop -m AM</code></p> <ul style="list-style-type: none"> <li>• elle retourne 0 lorsque la limite <code>maxloop</code> n'est pas atteinte ou si la dernière incrémentation a eu lieu en dehors de la période <code>loop_interval</code></li> <li>• elle retourne 1 quand la limite <code>maxloop</code> a été atteinte dans la période <code>loop_interval</code></li> </ul>



## 15.Exemples de configurations de module applicatif

- ⇒ [Section 15.1](#) « Exemple de module miroir avec `mirror.safe` »
- ⇒ [Section 15.2](#) « Exemple de module ferme avec `farm.safe` »
- ⇒ [Section 15.3](#) « Exemple d'utilisation de macros et variables de script avec `hyperv.safe` »
- ⇒ [Section 15.4](#) « Exemple de surveillance de processus avec `softerrd.safe` »
- ⇒ [Section 15.5](#) « Exemple de TCP checker »
- ⇒ [Section 15.6](#) « Exemple de ping checker »
- ⇒ [Section 15.7](#) « Exemple de custom checker avec `customchecker.safe` »
- ⇒ [Section 15.8](#) « Exemple de splitbrain checker »
- ⇒ [Section 15.9](#) « Exemples de module checker »
- ⇒ [Section 15.10](#) « Exemple de checker d'interface réseau »
- ⇒ [Section 15.11](#) « Exemple d'IP checker »
- ⇒ [Section 15.12](#) « Exemple d'hostname virtuel avec `vhost.safe` »

Certains exemples décrits sont tirés des modules livrés avec le package SafeKit, sous `SAFE/Application_Modules`. De nombreux réels exemples d'intégration sont aussi décrits sous [SafeKit Quick Installation Guides](#).



Les `.safe` sont plate-forme dépendants et, par conséquent, différents en Windows et Linux, principalement en ce qui concerne les scripts du module.

La configuration du module peut être modifiée :

- soit via l'assistant de configuration du module de la console web SafeKit (voir la [section 3.3](#))
- soit en éditant directement les fichiers `SAFE/module/AM/conf/userconfig.xml` ou les scripts sous `SAFE/module/AM/bin` (où `AM` est le nom du module installé)

Pour être prise en compte, au prochain démarrage du module, la nouvelle configuration doit être appliquée :

- soit à la dernière étape de l'assistant de configuration du module
- soit avec la commande `safekit config -H "node1,node2" -E AM` exécutée sur le nœud sur lequel les fichiers ont été modifiés



Avant d'appliquer la configuration, fermez tous les éditeurs, explorateur de fichiers, shells ou cmd qui accèderaient un fichier sous `SAFE/modules/AM` sur les nœuds.

## 15.1 Exemple de module miroir avec `mirror.safe`

Ci-dessous le fichier de configuration et les scripts du module du module miroir générique, `mirror.safe`, pour Windows.

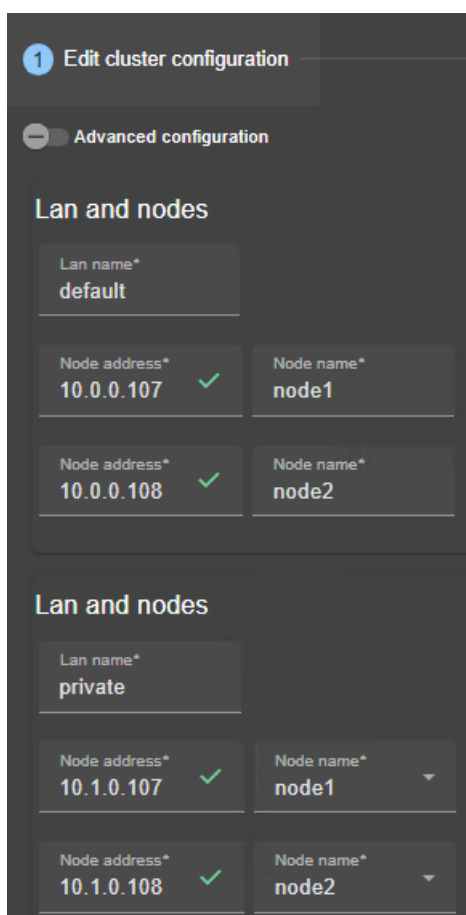
Pour tester un module miroir, voir la [section 4.2](#).



La description suivante est pour Windows. Pour Linux, veuillez consulter `mirror.safe` fourni avec le package Linux qui comprend la configuration et les scripts pour Linux.

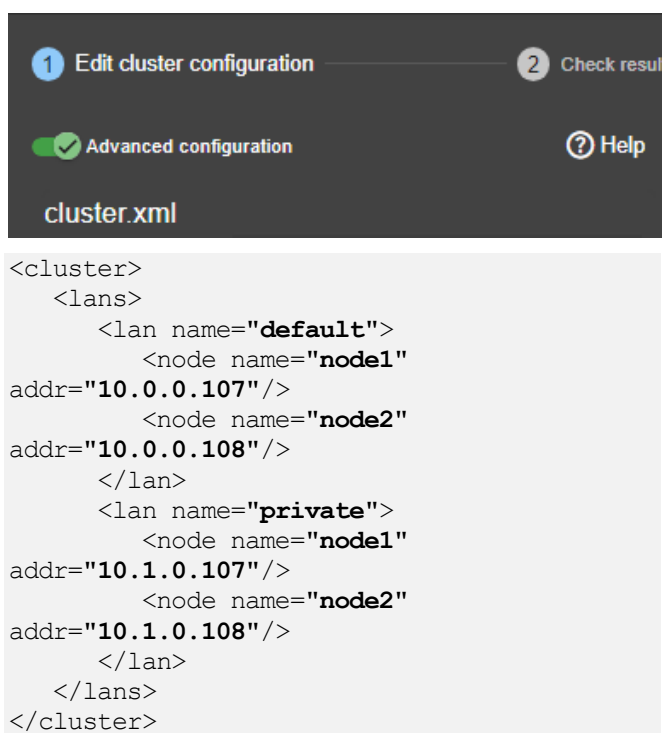
### 15.1.1 Configuration du cluster avec deux réseaux

La configuration du cluster comprend deux réseaux, nommés par exemple `default` et `private`. Le deuxième réseau est défini pour illustrer la configuration d'un réseau dédié au trafic de réplication dans la configuration du module. La plupart des configurations incluent généralement un seul réseau.



Pour lancer l'assistant de configuration du cluster, voir [section 3.2](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.



Pour des détails sur la configuration XML, voir [section 12.1](#).

### 15.1.2 Configurations du module miroir

Le module `mirror.safe`, livré depuis SafeKit 8.2.4, a été amélioré pour permettre la définition de la liste des services à l'aide d'une macro appelée `SERVICES` dans la configuration du module. Les scripts du module utilisent cette valeur pour :

- vérifier que les services listés existent sur le serveur et désactiver leur démarrage automatique au boot, pendant la configuration du module
- démarrer et arrêter automatiquement les services listés lorsque nécessaire, pendant l'exécution du module

Ainsi, l'intégration d'une nouvelle application utilisant `mirror.safe` se limite à :

- obtenir les noms des services pertinents

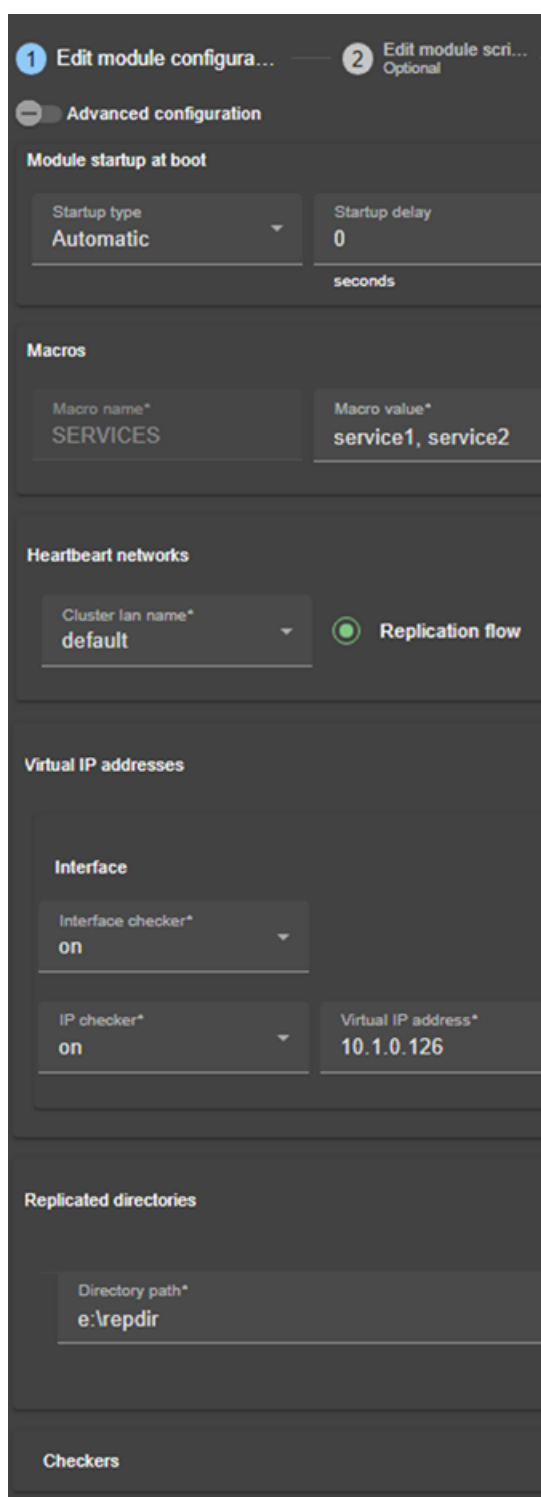
Pour lister tous les services installés sur un serveur, utiliser :

- o la cmdlet PowerShell `Get-Service` en Windows
- o la commande `systemctl list-unit-files --type=service` en Linux
- déterminer les chemins des répertoires à répliquer
- obtenir une adresse IP inutilisée comme adresse IP virtuelle

Ci-dessous des exemples de configurations d'un module miroir avec une adresse IP virtuelle, la réplication de fichiers en temps réel et le basculement automatique.

#### 15.1.2.1 Configuration avec une adresse IP virtuelle, la réplication de fichiers en temps réel et le basculement automatique

La configuration suivante utilise seulement un seul réseau pour le trafic des heartbeats et de la réplication.



Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.

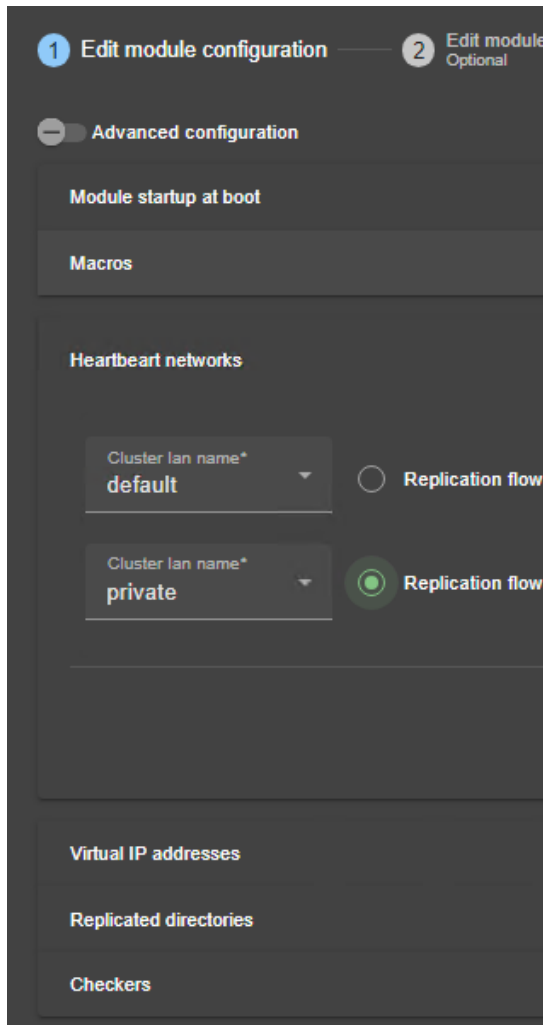
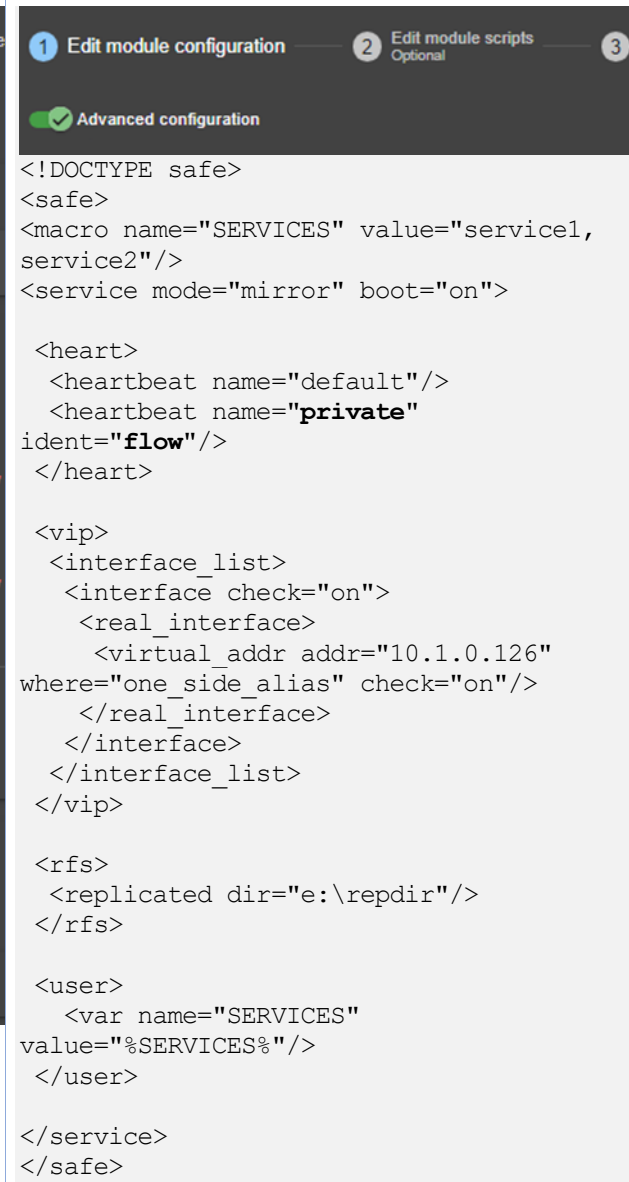


Pour des détails sur la configuration XML :

- <macro> voir [section 13.2](#)
- <service> voir [section 13.3](#)
- <heart> voir [section 13.4](#)
- <vip> voir [section 13.6](#)
- <rfs> voir [section 13.7](#)
- <user>, <var> voir [section 13.8](#)

### 15.1.2.2 Configuration avec un réseau de réplication dédié

Le module est configuré pour utiliser les deux réseaux du cluster définis en [section 15.1.1](#). Celui nommé `private` est sélectionné comme « Flux de réplication ».

 <p>1 Edit module configuration — 2 Edit module Optional</p> <p>Advanced configuration</p> <p>Module startup at boot</p> <p>Macros</p> <p>Heartbeat networks</p> <p>Cluster lan name* default <input type="radio"/> Replication flow</p> <p>Cluster lan name* private <input checked="" type="radio"/> Replication flow</p> <p>Virtual IP addresses</p> <p>Replicated directories</p> <p>Checkers</p>	 <p>1 Edit module configuration — 2 Edit module scripts Optional — 3</p> <p>Advanced configuration</p> <pre>&lt;!DOCTYPE safe&gt; &lt;safe&gt; &lt;macro name="SERVICES" value="service1, service2"/&gt; &lt;service mode="mirror" boot="on"&gt;  &lt;heart&gt;   &lt;heartbeat name="default"/&gt;   &lt;heartbeat name="private" ident="flow"/&gt; &lt;/heart&gt;  &lt;vip&gt; &lt;interface_list&gt;   &lt;interface check="on"&gt;     &lt;real_interface&gt;       &lt;virtual_addr addr="10.1.0.126" where="one_side_alias" check="on"/&gt;     &lt;/real_interface&gt;   &lt;/interface&gt; &lt;/interface_list&gt; &lt;/vip&gt;  &lt;rfs&gt;   &lt;replicated dir="e:\replib"/&gt; &lt;/rfs&gt;  &lt;user&gt;   &lt;var name="SERVICES" value="%SERVICES%"/&gt; &lt;/user&gt;  &lt;/service&gt; &lt;/safe&gt;</pre>
<p>Pour lancer l'assistant de configuration du module, voir <a href="#">section 3.3</a>.</p> <p>Basculer en « Configuration avancée » pour éditer le XML si besoin.</p>	<p>Pour la description de la configuration XML voir <a href="#">section 13</a>.</p>

### 15.1.3 Scripts du module miroir

Ci-dessous les scripts du module pour Windows, pour démarrer/arrêter les service du module miroir sur le nœud primaire. Pour Linux, se référer au module `mirror.safe` livré avec le package Linux.

Pour plus de détails sur les scripts du module, voir [section 14](#).

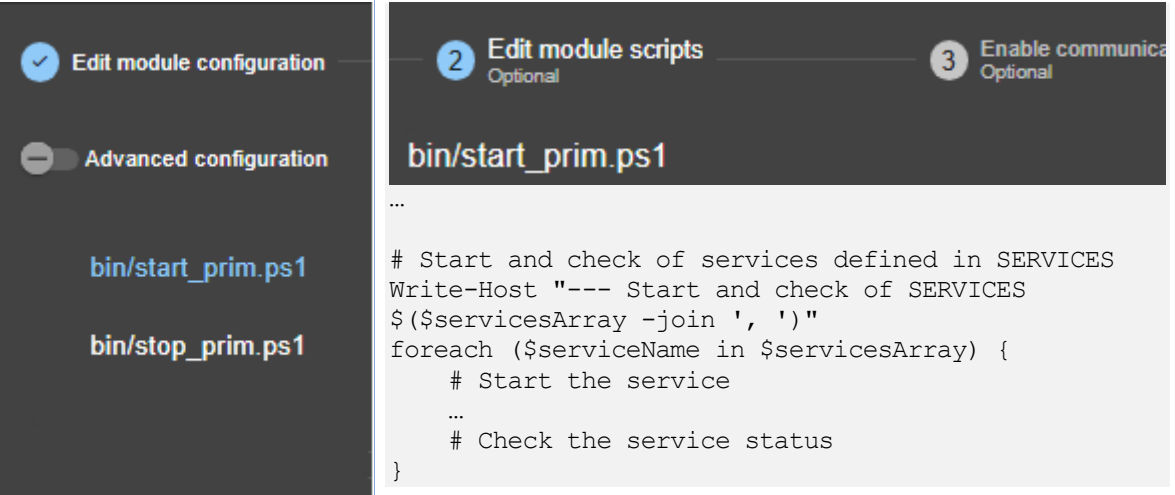
Pour plus de détails sur la sortie des scripts (avec `echo`, `Write-Host` et `safekit printe`), voir la [section 14.3](#).

Avec le module `mirror.safe` livré depuis SafeKit 8.2.4, l'utilisateur n'a plus besoin de modifier les scripts pour insérer les commandes de démarrage et d'arrêt de chaque service. En effet, les nouveaux scripts du module utilisent la valeur de `SERVICES` pour récupérer les noms des services à démarrer ou arrêter.

Ci-dessous, nous montrons quand même la façon d'éditer les scripts si jamais vous aviez besoin de les adapter pour des besoins particuliers. Par exemple, `milestone.safe` nécessite de démarrer des App pools après le démarrage du service IIS. Cela ne présente pas de difficulté particulière d'adapter le script générique pour y insérer cette opération.

### 15.1.3.1 Script `start_prim`

Le script `start_prim` est appelé lorsque le module miroir démarre en tant que primaire (démarrage manuel ou automatique après un `stopstart` ou sortie du `wait`) ou redémarre sur un nœud primaire (`restart`). Il doit contenir le démarrage de l'application intégrée dans le module. L'application s'exécute uniquement sur le nœud primaire.



```
...  
# Start and check of services defined in SERVICES  
Write-Host "--- Start and check of SERVICES"  
$($servicesArray -join ', ')  
foreach ($serviceName in $servicesArray) {  
    # Start the service  
    ...  
    # Check the service status  
}
```



Avec le module `mirror.safe` livré depuis SafeKit 8.2.4, ce script arrête le module si le démarrage d'un service échoue ou n'atteint pas un état démarré. Ce comportement peut être modifié en commentant l'appel à la fonction `Stop_Module_And_Exit`.

### 15.1.3.2 Script `stop_prim`

Le script `stop_prim` est appelé lorsque le module s'arrête (`stop`, `stopstart` ou `wait`) ou redémarre sur un nœud primaire (`restart`). Il doit contenir l'arrêt de l'application intégrée dans le module

The screenshot shows a configuration tool interface with three steps: 1. Edit module configuration (checked), 2. Edit module scripts (Optional), and 3. Enable communication (Optional). The 'Advanced configuration' toggle is turned off. The left sidebar lists 'bin/start\_prim.ps1' and 'bin/stop\_prim.ps1'. The main area displays the content of 'bin/stop\_prim.ps1'.

```
...  
$gracefulStop = ($args[0] -ne "force")  
...  
# Stop and check of services  
if ($gracefulStop) {  
    Write-Host "--- Stop and check of SERVICES  
    $($servicesArray -join ', ')"  
    foreach ($serviceName in $servicesArray) {  
        # Graceful stop  
        # Stop the service  
        ...  
    }  
}
```

### 15.2 Exemple de module ferme avec `farm.safe`

Ci-dessous le fichier de configuration et les scripts du module pour le module ferme générique, `farm.safe`, pour Windows.

Pour tester un module ferme, voir la [section 4.3](#).



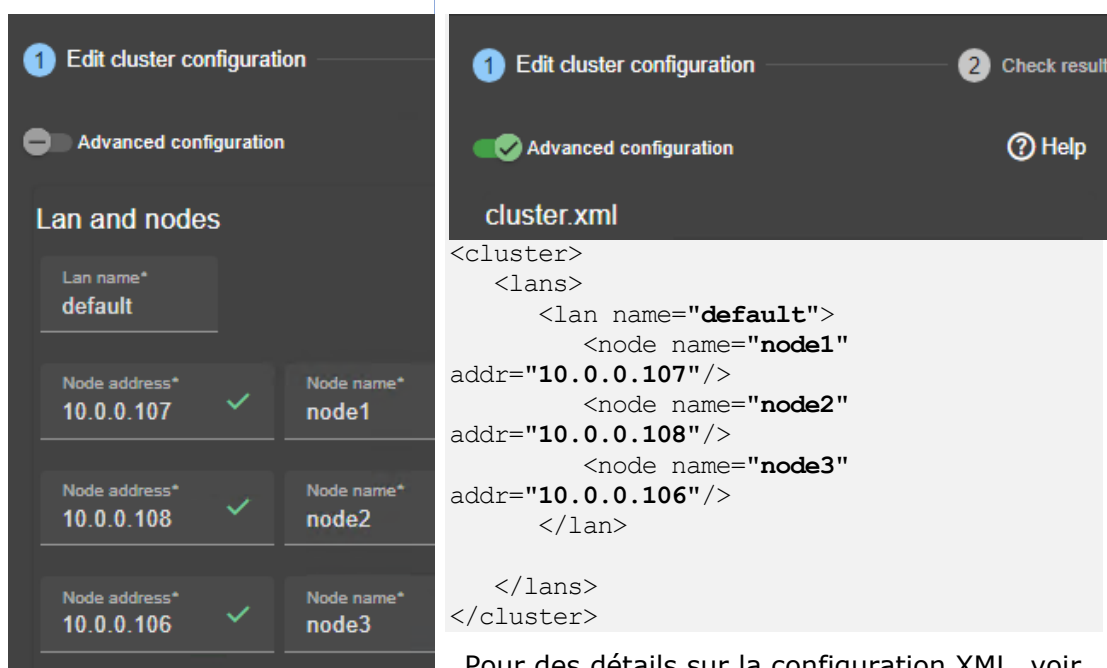
La description suivante est pour Windows. Pour Linux, veuillez consulter `farm.safe` fourni avec le package Linux qui comprend la configuration et les scripts pour Linux.

#### 15.2.1 Configuration du cluster avec trois nœuds

La configuration du cluster comprend un seul réseau nommé `default` et trois nœuds pour démontrer une configuration avancée de répartition de charge. La plupart des configurations de cluster incluent seulement deux nœuds.



Seul un module de ferme avec équilibrage de charge et sans réplication peut être configuré sur plus de deux nœuds. Un module miroir avec réplication ne peut être configuré que sur deux nœuds.



Pour lancer l'assistant de configuration du cluster, voir [section 3.2](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin

Pour des détails sur la configuration XML, voir [section 12.1](#).

### 15.2.2 Configurations du module ferme

Le module `farm.safe`, livré depuis SafeKit 8.2.4, a été amélioré pour permettre la définition de la liste des services à l'aide d'une macro appelée `SERVICES` dans la configuration du module. Les scripts du module utilisent cette valeur pour :

- vérifier que les services listés existent sur le serveur et désactiver leur démarrage automatique au boot, pendant la configuration du module
- démarrer et arrêter automatiquement les services listés lorsque nécessaire, pendant l'exécution du module

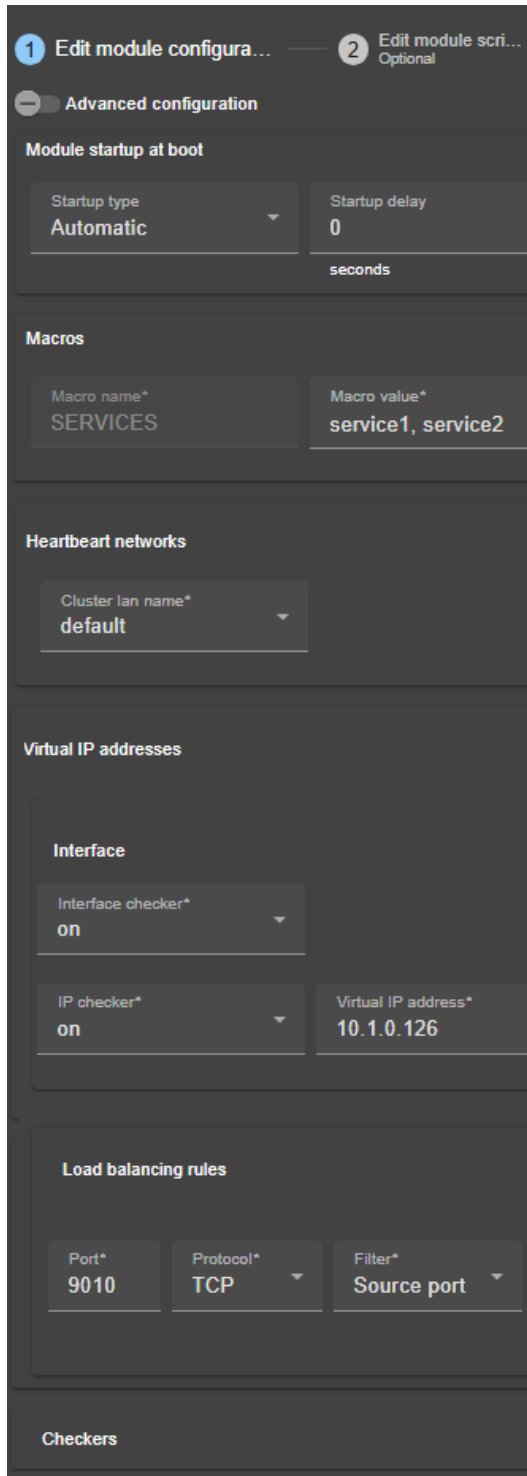
Ainsi, l'intégration d'une nouvelle application utilisant `farm.safe` se limite à :

- obtenir les noms des services pertinents
  - la cmdlet PowerShell `Get-Service` en Windows
  - la commande `systemctl list-unit-files --type=service` en Linux
- obtenir une adresse IP inutilisée comme adresse IP virtuelle
- déterminer les règles de load-balancing

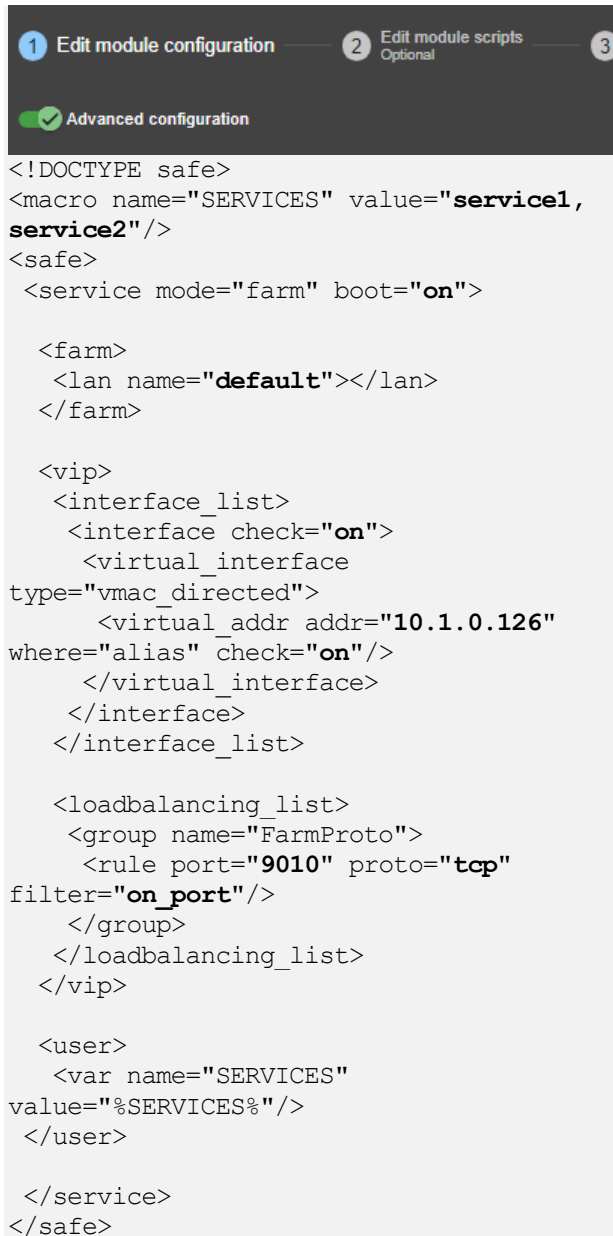
Ci-dessous des exemples de configurations d'un module ferme avec une adresse IP virtuelle, des règles d'équilibrage de charge et le basculement automatique.

### 15.2.2.1 Configuration avec une adresse IP virtuelle, l'équilibrage de charge et le basculement automatique

La règle de répartition de charge définie ci-dessous permet de visualiser la distribution de la charge entre les nœuds en accédant à la page web de SafeKit à l'adresse <http://host:9010/safekit/mosaic.html>.



The screenshot shows the configuration interface for a module. It includes sections for 'Module startup at boot' (Startup type: Automatic, Startup delay: 0 seconds), 'Macros' (Macro name: SERVICES, Macro value: service1, service2), 'Heartbeat networks' (Cluster lan name: default), 'Virtual IP addresses' (Interface checker: on, IP checker: on, Virtual IP address: 10.1.0.126), and 'Load balancing rules' (Port: 9010, Protocol: TCP, Filter: Source port). There are also tabs for 'Edit module configuration' and 'Edit module scripts'.



```

<!DOCTYPE safe>
<macro name="SERVICES" value="service1,
service2"/>
<safe>
  <service mode="farm" boot="on">

    <farm>
      <lan name="default"></lan>
    </farm>

    <vip>
      <interface_list>
        <interface check="on">
          <virtual_interface
type="vmac_directed">
            <virtual_addr addr="10.1.0.126"
where="alias" check="on"/>
          </virtual_interface>
        </interface>
      </interface_list>

      <loadbalancing_list>
        <group name="FarmProto">
          <rule port="9010" proto="tcp"
filter="on_port"/>
        </group>
      </loadbalancing_list>
    </vip>

    <user>
      <var name="SERVICES"
value="%SERVICES%"/>
    </user>

  </service>
</safe>

```

Pour des détails sur la configuration XML de :

- `<macro>` voir [section 13.2](#)
- `<service>` voir [section 13.3](#)
- `<farm>` voir [section 13.5](#)
- `<vip>` voir [section 13.6](#)

<p>Pour lancer l'assistant de configuration du module, voir <a href="#">section 3.3</a>.</p> <p>Basculer en « Configuration avancée » pour éditer le XML si besoin.</p>	<ul style="list-style-type: none"><li>• <code>&lt;loadbalancing_list&gt;</code> voir <a href="#">section 13.6.6</a></li><li>• <code>&lt;user&gt;</code>, <code>&lt;var&gt;</code> voir <a href="#">section 13.8</a></li></ul>
---	---

D'autres exemples de configuration des règles d'équilibrage de charge sont décrits ci-dessous.

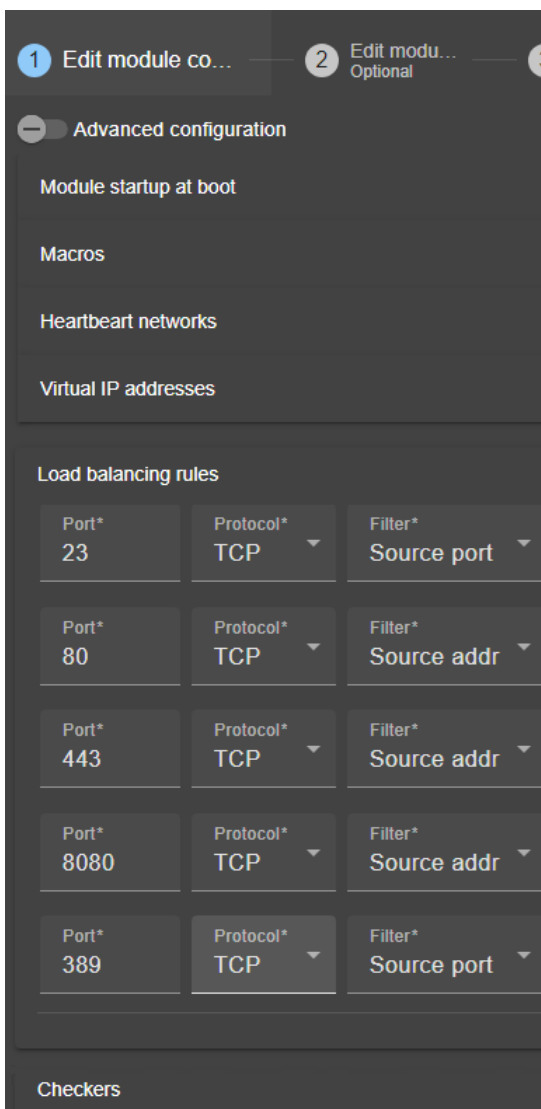
### 15.2.2.2 Configuration avec des règles d'équilibrage de charge pour TCP

Voici la configuration de l'équilibrage de charge pour accéder à l'adresse IP virtuelle en utilisant le protocole TCP sur les ports spécifiés :

- 80 (HTTP), 443 (HTTPS), 8080 (HTTP proxy)

Avec HTTP et HTTPS, le partage de charge est défini sur l'adresse IP client ("`on_addr`") et non sur le port TCP client ("`on_port`"), pour assurer que le même client est toujours connecté sur le même serveur sur plusieurs connexions TCP (service à état versus service sans état ; voir la description en [section 1.3.3](#)).

- 389 (LDAP) et 23 (Telnet)



1 Edit module co... 2 Edit modu... Optional 3

Advanced configuration

Module startup at boot

Macros

Heartbeat networks

Virtual IP addresses


Load balancing rules

Port*	Protocol*	Filter*
23	TCP	Source port
80	TCP	Source addr
443	TCP	Source addr
8080	TCP	Source addr
389	TCP	Source port

Checkers

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.



1 Edit module configuration 2 Edit module scripts Optional 3

Advanced configuration

```
<!DOCTYPE safe>
<safe>
  <macro name="SERVICES" value="service1,
service2"/>
  <service mode="farm" boot="on">
    <farm>
      <lan name="default"></lan>
    </farm>
    <vip>
      <interface_list>
        <interface check="on">
          <virtual_interface
type="vmac_directed">
            <virtual_addr addr="10.1.0.127"
where="alias" check="on"/>
          </virtual_interface>
        </interface>
      </interface_list>
      <loadbalancing_list>
        <group name="FarmProto">
          <rule port="23" proto="tcp"
filter="on_port"/>
          <rule port="80" proto="tcp"
filter="on_addr"/>
          <rule port="443" proto="tcp"
filter="on_addr"/>
          <rule port="8080" proto="tcp"
filter="on_addr"/>
          <rule port="389" proto="tcp"
filter="on_port"/>
        </group>
      </loadbalancing_list>
    </vip>

    <user>
      <var name="SERVICES"
value="%SERVICES%"/>
    </user>
  </service>
</safe>
```

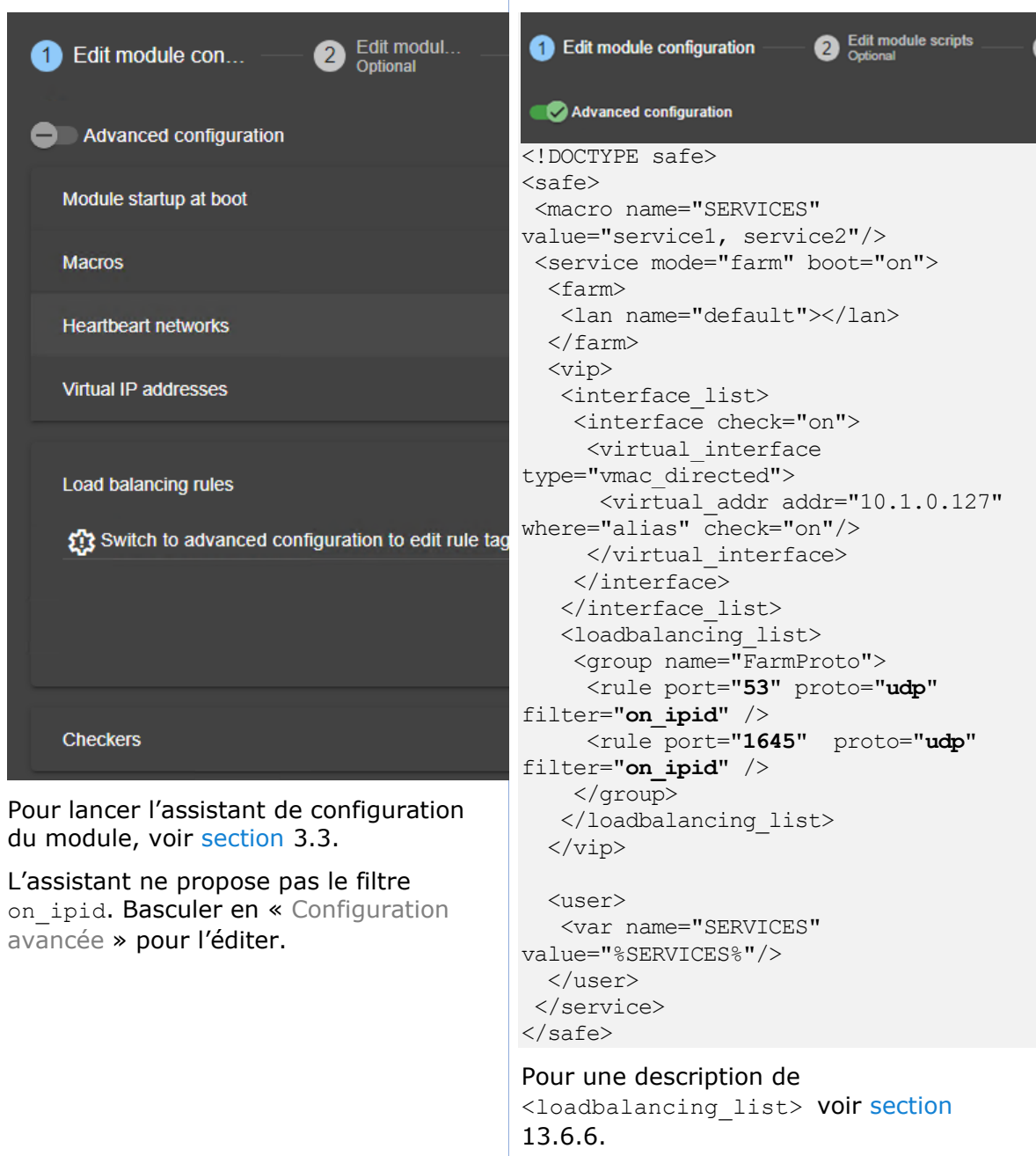
Pour une description de `<loadbalancing_list>` voir [section 13.6.6](#).

### 15.2.2.3 Configuration avec des règles d'équilibrage de charge pour UDP

Voici la configuration de l'équilibrage de charge pour accéder à l'adresse IP virtuelle en utilisant le protocole UDP sur les ports spécifiés :

- 53 (DNS)
- 1645 (RADIUS)

Avec `on_ipid`, l'équilibrage de charge est réalisé sur le champ "IP identifiant" dans l'entête IP du paquet. L'équilibrage fonctionne même si le client présente la même adresse IP client et le même port en entrée.



Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

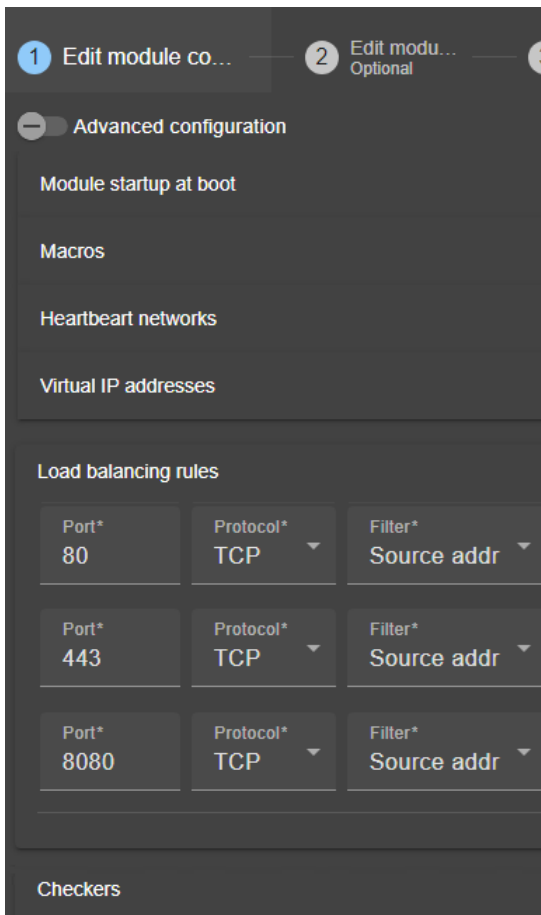
L'assistant ne propose pas le filtre `on_ipid`. Basculer en « Configuration avancée » pour l'éditer.

```
<!DOCTYPE safe>
<safe>
  <macro name="SERVICES"
value="service1, service2"/>
  <service mode="farm" boot="on">
    <farm>
      <lan name="default"></lan>
    </farm>
    <vip>
      <interface_list>
        <interface check="on">
          <virtual_interface
type="vmac_directed">
            <virtual_addr addr="10.1.0.127"
where="alias" check="on"/>
          </virtual_interface>
        </interface>
      </interface_list>
      <loadbalancing_list>
        <group name="FarmProto">
          <rule port="53" proto="udp"
filter="on_ipid" />
          <rule port="1645" proto="udp"
filter="on_ipid" />
        </group>
      </loadbalancing_list>
    </vip>
  </service>
</safe>
```

Pour une description de `<loadbalancing_list>` voir [section 13.6.6](#).

### 15.2.2.4 Configuration avec l'attribut `power`

L'attribut `power` permet de définir des priorités entre les nœuds pour la prise en charge du trafic à destination de l'IP virtuelle. Avec la configuration suivante, vous définissez une ferme de 3 nœuds avec une priorité pour le trafic HTTP pour `node1` (port 80), HTTPS pour `node2` (port 443) et proxy HTTP pour le `node3` (port 8080).



1 Edit module co... 2 Edit modu... Optional 3

Advanced configuration

Module startup at boot

Macros

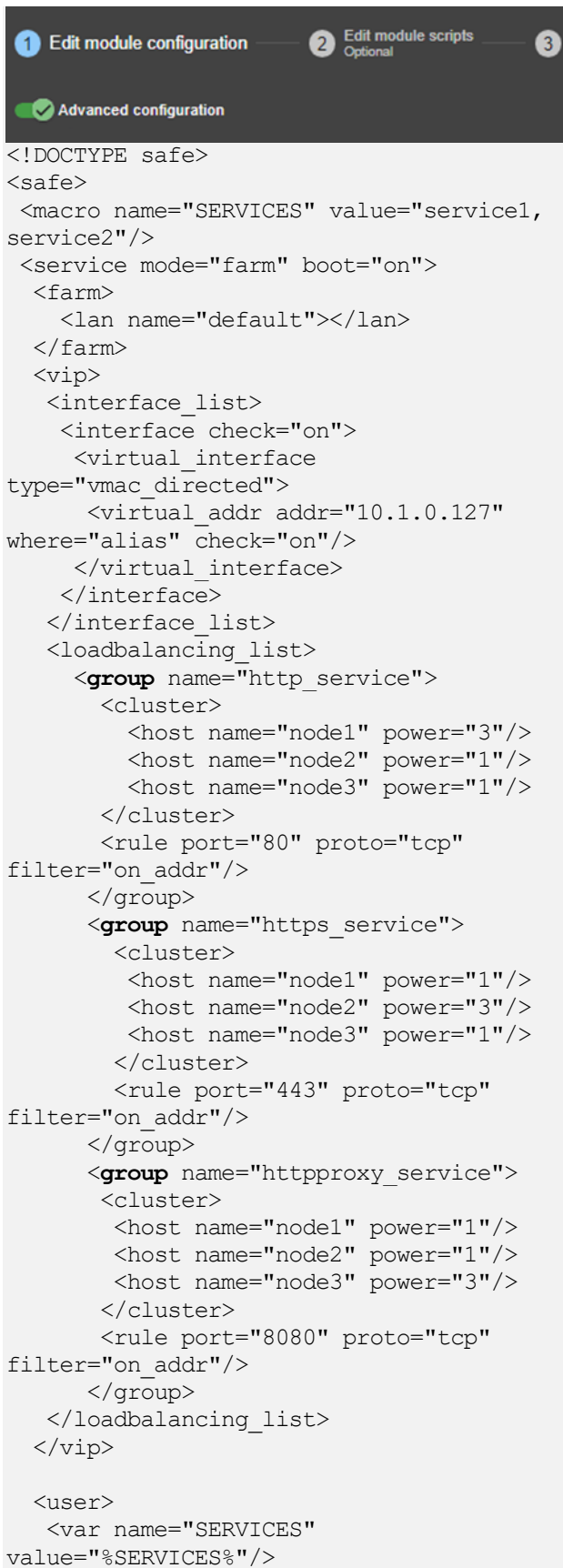
Heartbeat networks

Virtual IP addresses

Load balancing rules

Port*	Protocol*	Filter*
80	TCP	Source addr
443	TCP	Source addr
8080	TCP	Source addr

Checkers



1 Edit module configuration 2 Edit module scripts Optional 3

Advanced configuration

```
<!DOCTYPE safe>
<safe>
  <macro name="SERVICES" value="service1,
service2"/>
  <service mode="farm" boot="on">
    <farm>
      <lan name="default"></lan>
    </farm>
    <vip>
      <interface_list>
        <interface check="on">
          <virtual_interface
type="vmac_directed">
            <virtual_addr addr="10.1.0.127"
where="alias" check="on"/>
          </virtual_interface>
        </interface>
      </interface_list>
      <loadbalancing_list>
        <group name="http_service">
          <cluster>
            <host name="node1" power="3"/>
            <host name="node2" power="1"/>
            <host name="node3" power="1"/>
          </cluster>
          <rule port="80" proto="tcp"
filter="on_addr"/>
        </group>
        <group name="https_service">
          <cluster>
            <host name="node1" power="1"/>
            <host name="node2" power="3"/>
            <host name="node3" power="1"/>
          </cluster>
          <rule port="443" proto="tcp"
filter="on_addr"/>
        </group>
        <group name="httpproxy_service">
          <cluster>
            <host name="node1" power="1"/>
            <host name="node2" power="1"/>
            <host name="node3" power="3"/>
          </cluster>
          <rule port="8080" proto="tcp"
filter="on_addr"/>
        </group>
      </loadbalancing_list>
    </vip>
  </service>
</safe>

<user>
  <var name="SERVICES"
value="%SERVICES%"/>
</user>
```

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).



L'assistant n'affiche pas les détails sur les groupes d'équilibrage de charge. Basculer en « Configuration avancée » pour les éditer.

```
</user>
</service>
</safe>
```

Pour une description de `<loadbalancing_list>` voir [section 13.6.6](#).

### 15.2.2.5 Configuration avec l'attribut `scriptcontrol="on"`

Par défaut, avec `scriptcontrol="off"`, l'ouverture et la fermeture du trafic à destination de l'IP virtuelle sont automatiquement pilotées par SafeKit en fonction de l'état du module :

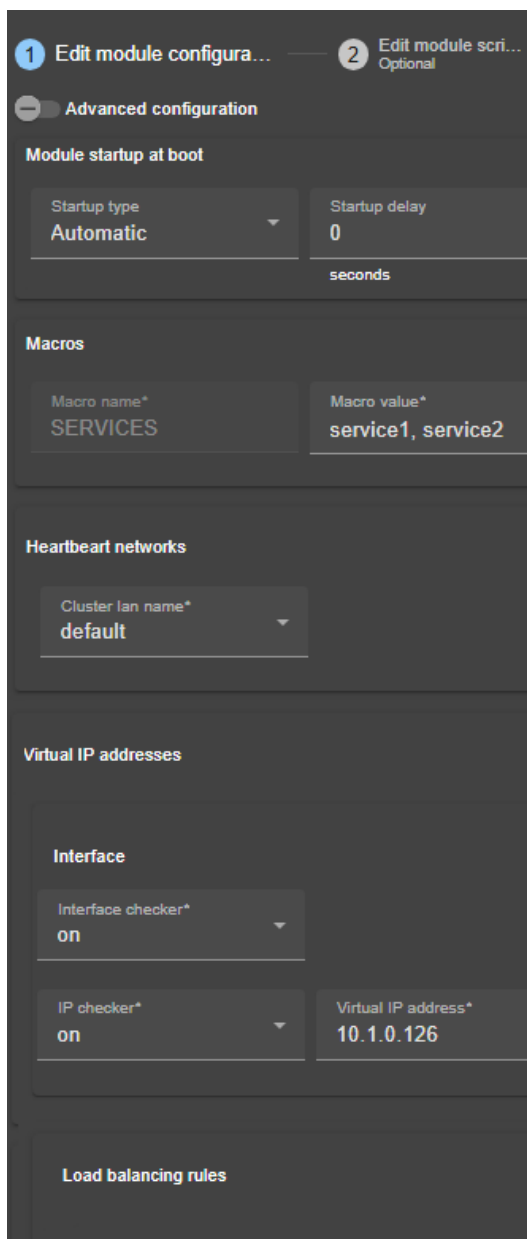

- Les flux vers la VIP sont ouverts avant l'exécution de `start_both`, lorsque le module va vers l'état  `UP (Ready)`. Cela entraîne l'activation de l'équilibrage de charge sur ce nœud.
- Les flux vers la VIP sont fermés après l'exécution de `stop_both`, lorsque le module quitte l'état  `UP (Ready)`. Cela entraîne la désactivation de l'équilibrage de charge sur ce nœud.

Si ce comportement par défaut convient à la plupart des applications, il peut être inadapté pour celles dont le démarrage est particulièrement long. En effet, les flux vers la VIP sont ouverts alors que l'application n'est pas encore prête à les traiter, ce qui provoque une indisponibilité temporaire du service côté client.

Avec `scriptcontrol="on"`, le pilotage automatique est désactivé et peut être effectué en manuellement ligne de commande au moment opportun :

- Les flux vers la VIP peuvent être ouverts dans le script `start_both` après le démarrage de l'application
- Les flux vers la VIP peuvent être fermés dans le script `stop_both` avant l'arrêt de l'application

Ci-dessous l'exemple de configuration d'une ferme en positionnant l'attribut `scriptcontrol="on"` en « Configuration avancée » uniquement.

	 <pre> &lt;!DOCTYPE safe&gt; &lt;macro name="SERVICES" value="service1, service2"/&gt; &lt;safe&gt;   &lt;service mode="farm" boot="on"&gt;      &lt;farm&gt;       &lt;lan name="default"&gt;&lt;/lan&gt;     &lt;/farm&gt;      &lt;vip scriptcontrol="on"&gt;       &lt;interface_list&gt;         &lt;interface check="on"&gt;           &lt;virtual_interface type="vmac_directed"&gt;             &lt;virtual_addr addr="10.1.0.126" where="alias" check="on"/&gt;           &lt;/virtual_interface&gt;         &lt;/interface&gt;       &lt;/interface_list&gt;        &lt;loadbalancing_list&gt;         &lt;group name="FarmProto"&gt;           &lt;rule port="9010" proto="tcp" filter="on_port"/&gt;         &lt;/group&gt;       &lt;/loadbalancing_list&gt;     &lt;/vip&gt;      &lt;user&gt;       &lt;var name="SERVICES" value="%SERVICES%"/&gt;     &lt;/user&gt;    &lt;/service&gt; &lt;/safe&gt; </pre>
--	--

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML.

Pour une description de `<vip>` voir [section 13.6](#)

De plus, lorsque `scriptcontrol="on"` est configuré, il est nécessaire de rajouter le script du module `update` pour supporter les reconfigurations dynamiques du cluster ou du module.

Pour plus de détails sur le contenu des scripts, voir la [section 15.2.3.2](#).

### 15.2.3 Scripts du module ferme

Ci-dessous les scripts du module en Windows, pour démarrer/arrêter les services du module ferme sur tous les nœuds. Pour Linux, se référer au module `farm.safe` livré avec le package Linux.

Pour plus de détails sur les scripts du module, voir [section 14](#).

Pour plus de détails sur la sortie des scripts (avec `echo`, `Write-Host` et `safekit printe`), voir la [section 14.3](#).

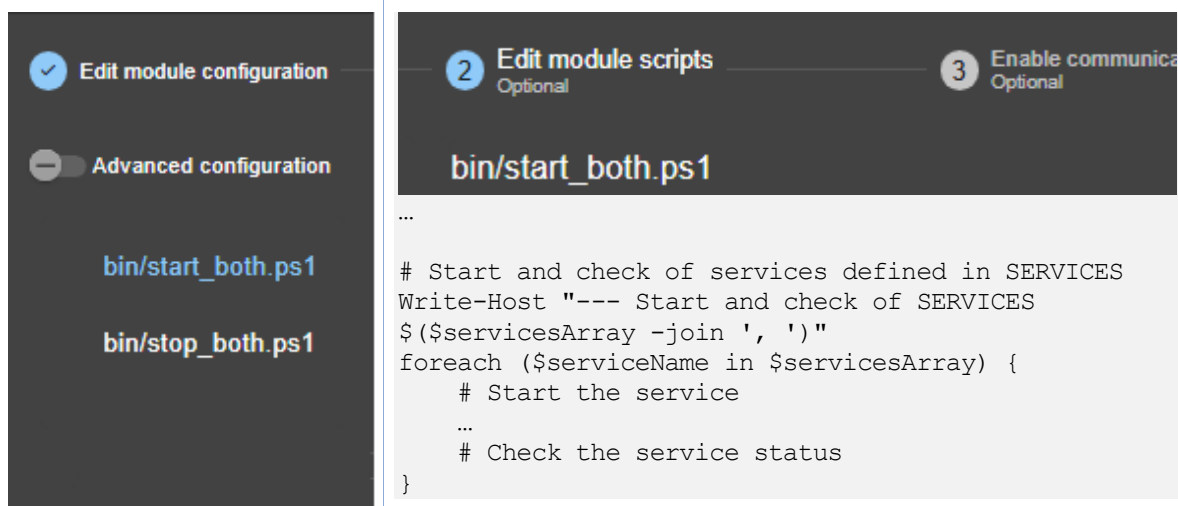
Avec le module `farm.safe` livré depuis SafeKit 8.2.4, l'utilisateur n'a plus besoin de modifier les scripts pour insérer les commandes de démarrage et d'arrêt de chaque service. En effet, les nouveaux scripts du module utilisent la valeur de `SERVICES` pour récupérer les noms des services à démarrer ou arrêter.

Ci-dessous, nous montrons quand même la façon d'éditer les scripts si jamais vous aviez besoin de les adapter pour des besoins particuliers. Par exemple, avec l'attribut `scriptcontrol="on"`, il est nécessaire de rajouter les commandes d'ouverture/fermeture du trafic à destination de l'IP virtuelle. Cela ne présente pas de difficulté particulière d'adapter le script générique pour y insérer ces commandes.

#### 15.2.3.1 Scripts du module ferme (avec l'attribut par défaut `scriptcontrol="off"`)

##### 15.2.3.1.1 Script `start_both`

Le script `start_both` est appelé lorsque le module de ferme démarre (démarrage manuel ou automatique après un `stopstart` ou sortie du `wait`) ou redémarre (`restart`). Il doit contenir le démarrage de l'application intégrée dans le module. L'application s'exécute sur tous les nœuds.



Avec le module `farm.safe` livré depuis SafeKit 8.2.4, ce script arrête le module si le démarrage d'un service échoue ou n'atteint pas un état démarré. Ce comportement peut être modifié en commentant l'appel à la fonction `Stop_Module_And_Exit`.

### 15.2.3.1.2 Script stop\_both

Le script `stop_both` est appelé lorsque le module de ferme s'arrête (`stop`, `stopstart` ou `wait`) ou redémarre (`restart`). Il doit contenir l'arrêt de l'application intégrée dans le module.



### 15.2.3.2 Script du module ferme (avec l'attribut `scriptcontrol="on"`)

Avec `scriptcontrol="on"`, il est nécessaire de rajouter dans les scripts du module les commandes d'ouverture/fermeture du trafic à destination de l'IP virtuelle :

- Les flux vers la VIP sont ouverts avec la commande :  
`SAFE/safekit -r saferpc_send vipd SETGROUPS all all all`
- Les flux vers la VIP sont fermés avec la commande :  
`SAFE/safekit -r saferpc_send vipd SETGROUPS none none none`

De plus, il est nécessaire de rajouter le script du module `update` (au même emplacement que `start_both` et `stop_both`) pour supporter les reconfigurations dynamiques du cluster ou du module.

#### 15.2.3.2.1 Script start\_both

Ci-dessous, le script `start_both` qui comprend en plus, par rapport au script standard, l'appel aux commandes de contrôle du trafic à destination de l'IP virtuelle :

- La fermeture du trafic (par sécurité) avant le démarrage des services
- L'ouverture du trafic après le démarrage des services

<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;"> <input checked="" type="checkbox"/> Edit module configuration         </div> <div style="text-align: center;"> <input type="checkbox"/> Advanced configuration         </div> </div> <div style="text-align: center; margin-top: 20px;"> <p><code>bin/start_both.ps1</code></p> <p><code>bin/stop_both.ps1</code></p> </div>	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;"> <span style="font-size: 24px; color: #00aaff;">2</span> Edit module scripts <small>Optional</small> </div> <div style="text-align: center;"> <span style="font-size: 24px; color: #00aaff;">3</span> Enable communica <small>Optional</small> </div> </div> <div style="text-align: center; margin-top: 10px;"> <p><code>bin/start_both.ps1</code></p> </div> <pre style="background-color: #eee; padding: 10px; font-family: monospace;"> ... # Close traffic to the VIP &amp; "\$env:SAFE\safekit" -r saferpc_send vipd SETGROUPS none none none  # Start and check of services defined in SERVICES Write-Host "--- Start and check of SERVICES" \${\$servicesArray -join ', '}" foreach (\$serviceName in \$servicesArray) {     # Start the service     ...     # Check the service status }  # Open traffic to the VIP &amp; "\$env:SAFE\safekit" -r saferpc_send vipd SETGROUPS all all all                     </pre>
--	--

### 15.2.3.2.2 Script stop\_both

Ci-dessous, le script `stop_both` qui comprend en plus, par rapport au script standard, l'appel aux commandes de contrôle du trafic à destination de l'IP virtuelle :

- La fermeture du trafic avant l'arrêt des services

<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;"> <input checked="" type="checkbox"/> Edit module configuration         </div> <div style="text-align: center;"> <input type="checkbox"/> Advanced configuration         </div> </div> <div style="text-align: center; margin-top: 20px;"> <p><code>bin/start_both.ps1</code></p> <p><code>bin/stop_both.ps1</code></p> </div>	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="text-align: center;"> <span style="font-size: 24px; color: #00aaff;">2</span> Edit module scripts <small>Optional</small> </div> <div style="text-align: center;"> <span style="font-size: 24px; color: #00aaff;">3</span> Enable communica <small>Optional</small> </div> </div> <div style="text-align: center; margin-top: 10px;"> <p><code>bin/stop_both.ps1</code></p> </div> <pre style="background-color: #eee; padding: 10px; font-family: monospace;"> ... # Close traffic to the VIP &amp; "\$env:SAFE\safekit" -r saferpc_send vipd SETGROUPS none none none  \$gracefulStop = (\$args[0] -ne "force")  ... # Stop and check of services if (\$gracefulStop) {     Write-Host "--- Stop and check of SERVICES"     \${\$servicesArray -join ', '}"     foreach (\$serviceName in \$servicesArray) {         # Graceful stop         # Stop the service         ...     } } ...                     </pre>
--	--

### 15.2.3.2.3 Script update

Ce script n'est pas livré en standard et doit être rajouté (au même emplacement que `start_both` et `stop_both`) pour supporter les reconfigurations dynamiques du cluster ou du module. Sur reconfiguration dynamique, le module exécute l'action `update` qui arrête puis relance le gestionnaire d'équilibrage de charge (`vipd`). Avec `scriptcontrol="on"`, ce dernier laisse le trafic vers la VIP fermé. Le script `update` ouvre le trafic vers la VIP si le module est dans l'état `UP`.

The screenshot shows a configuration interface with three steps: 1. Edit module configuration, 2. Edit module scripts (Optional), and 3. Enable communication (Optional). The current view is on step 2, showing the content of the `bin/update.ps1` script. The script is a PowerShell script that runs when the module is updated. It checks if the current state is 'UP' and if the update action is 'UP'. If both are true, it opens traffic to the VIP by running `saferpc_send vipd` with the environment variable `SAFE\safekit` and sets the process group to `all all all`. The script then exits with a status of 0.

```
# Script called on module update

$scriptName = Split-Path -Path $PSCmdPath -Leaf

Write-Host "Running ${scriptName} $args"

if ($args.Count -ge 2 -and $args[0] -eq "UP" -and
    $args[1] -eq "UP") {
    # Open traffic to the VIP
    & "$env:SAFE\safekit" -r saferpc_send vipd
    SETGROUPS all all all
}
exit 0
```

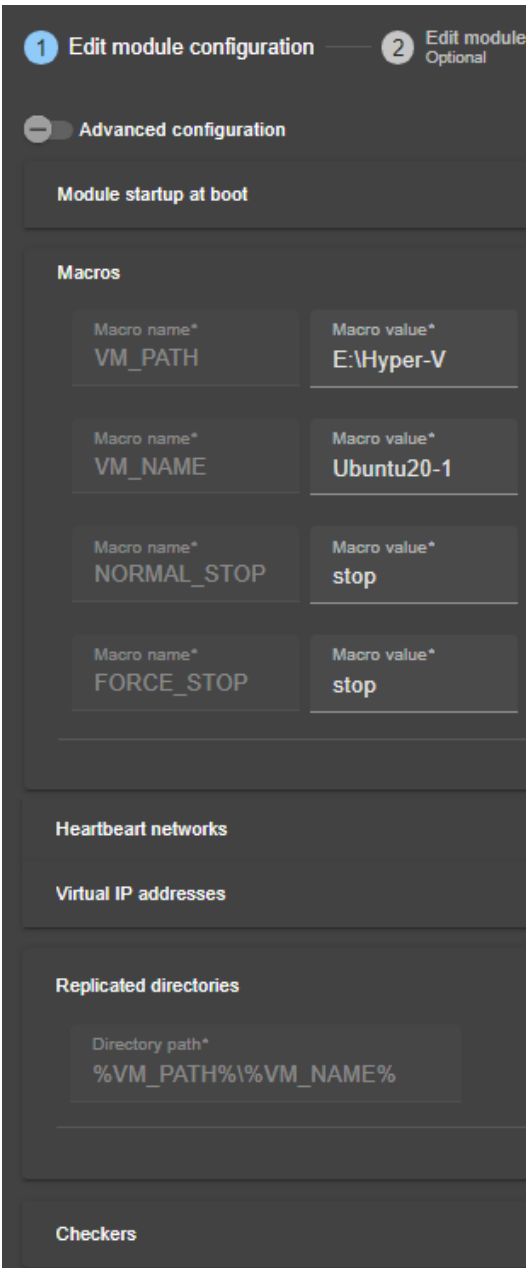
Basculer en  
« Configuration  
avancée » pour ajouter  
ou éditer le script `update`

## 15.3 Exemple d'utilisation de macros et variables de script avec `hyperv.safe`

Le module `hyperv.safe` apporte la haute disponibilité à Hyper-V pour deux serveurs Windows. Il s'agit d'un module miroir, avec une adresse IP virtuelle, la réplication temps réel et le basculement automatique. Il est présenté pour démontrer l'utilisation de macros et de variables d'environnement des scripts du module.

### 15.3.1 Configuration du module avec macro et var

Dans l'exemple suivant, quatre `<macro>` sont configurés, et leurs valeurs sont utilisées pour définir le chemin du répertoire répliqué `<dir>` (c'est-à-dire `E:\Hyper-V\Ubuntu20-1`) et les variables d'environnement `<var>` pour les scripts de module. Noter que dans l'exemple, le nom des macros et des variables sont identiques, ce qui n'est pas une obligation.



1 Edit module configuration — 2 Edit module Optional

Advanced configuration

Module startup at boot

Macros

Macro name*	Macro value*
VM_PATH	E:\Hyper-V
VM_NAME	Ubuntu20-1
NORMAL_STOP	stop
FORCE_STOP	stop

Heartbeat networks

Virtual IP addresses

Replicated directories


Directory path\*

%VM\_PATH%\%VM\_NAME%

Checkers

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

L'assistant n'affiche pas la section user. Basculer en « Configuration avancée » pour l'éditer.



1 Edit module configuration — 2 Edit module scripts Optional — 3

Advanced configuration

```
<!DOCTYPE safe>
<safe>
  <macro name="VM_PATH"
    value="E:\Hyper-V"/>
  <macro name="VM_NAME"
    value="Ubuntu20-1"/>
  <macro name="NORMAL_STOP"
    value="stop"/>
  <macro name="FORCE_STOP"
    value="stop"/>
  <service mode="mirror">
    <heartbeat>
      <heartbeat name="default" />
    </heartbeat>
    <rfs scripts="on" acl="on"
      namespacepolicy="0" allocthreshold="10">
      <replicated
        dir="%VM_PATH%\%VM_NAME%">
      </replicated>
    </rfs>
    <user>
      <var name="VM_PATH"
        value="%VM_PATH%\%VM_NAME%"/>
      <var name="VM_NAME"
        value="%VM_NAME%"/>
      <var name="NORMAL_STOP"
        value="%NORMAL_STOP%"/>
      <var name="FORCE_STOP"
        value="%FORCE_STOP%"/>
    </user>
  </service>
</safe>
```

Pour des détails sur la configuration XML de :

- <macro> voir [section 13.2](#)
- <user>, <var> voir [section 13.8](#)

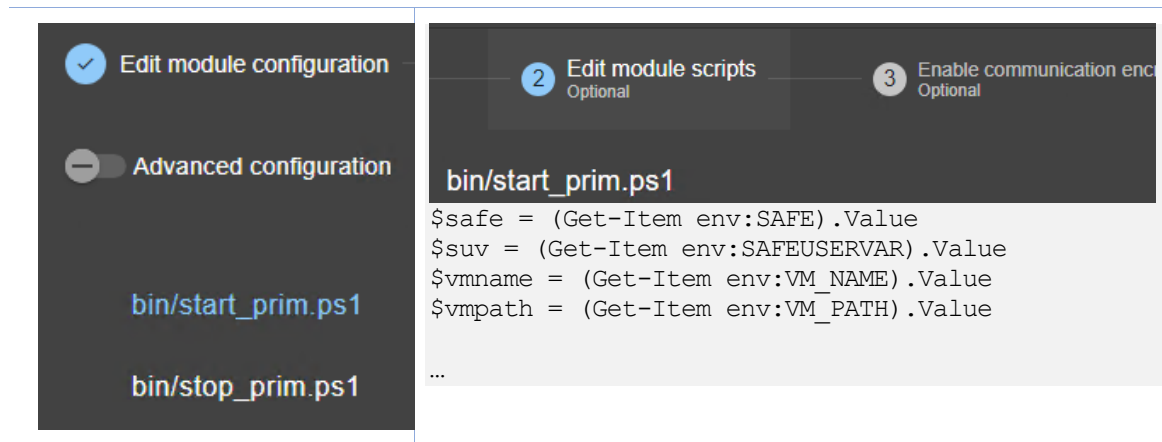
### 15.3.2 Accès des variables par les scripts du module

Ci-dessous, le script `start_prim.ps1` accèdent aux variables d'environnement définies lors de son exécution :

- Les variables d'environnement SafeKit `SAFE` et `SAFEUSERVAR`

- Les variables d'environnement du module `VM_PATH`, `VM_NAME...` définies dans les sections `<var>` de `<user>`

Pour plus de détails, voir [section 14.2](#).



### 15.4 Exemple de surveillance de processus avec `softerrd.safe`

Le module `softerrd.safe` est un module miroir de démonstration de la surveillance de processus. Cette fonctionnalité est disponible également dans un module ferme.

Les tests consistent à tuer les processus surveillés (i.e. `mybin`, `myotherbin` ou `myappli`) avec la commande `safekit kill`.

Pour tester la surveillance de processus, voir la [section 4.4.1](#).



La description suivante est pour Windows. Pour Linux, veuillez consulter `softerrd.safe` fourni avec le package Linux qui comprend la configuration et les scripts pour Linux.

#### 15.4.1 Configuration du module avec surveillance de processus

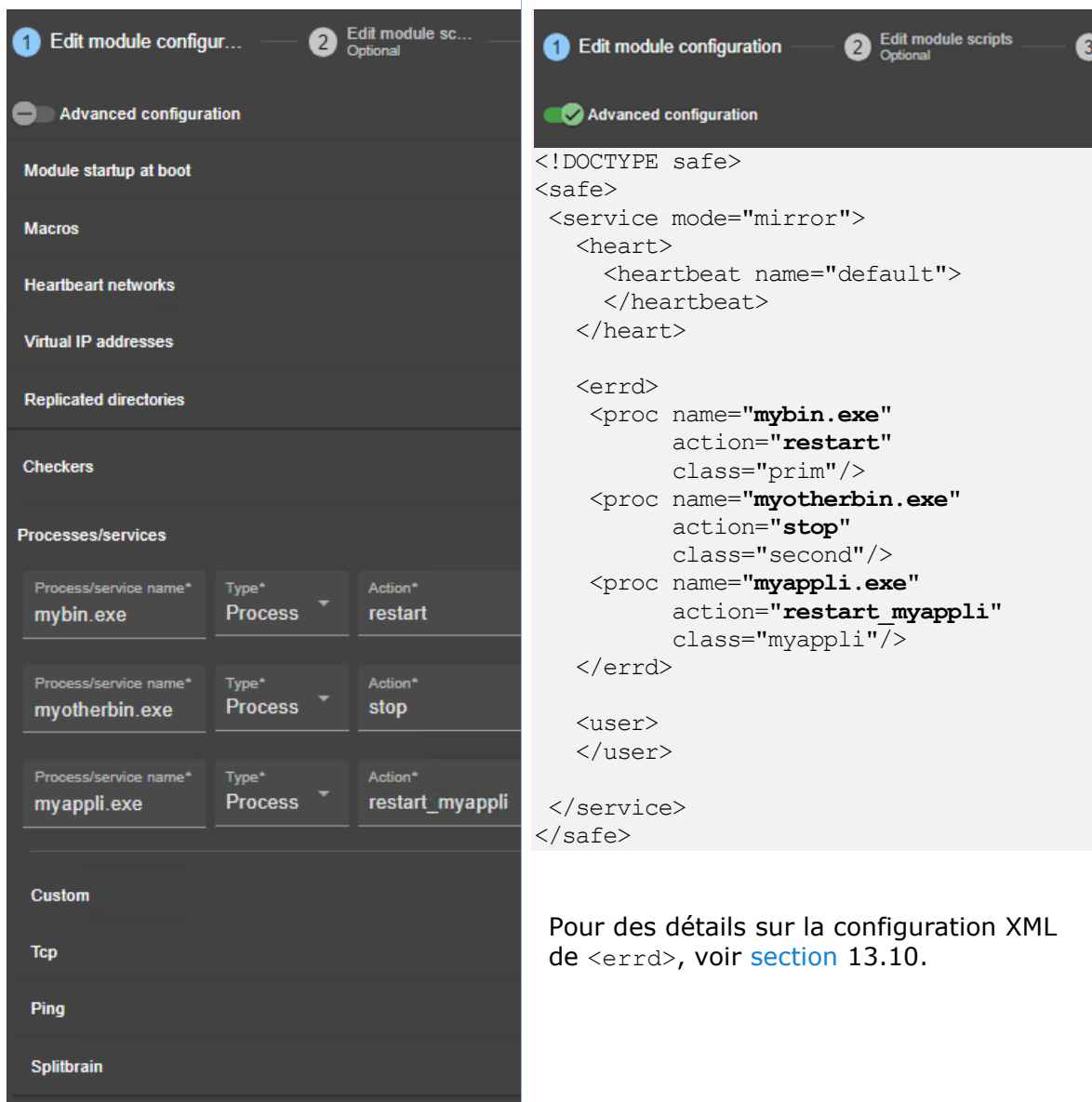
La détection de l'arrêt de :

- `mybin` provoque un restart du module (`action="restart"`). Sa surveillance est activée/désactivée après/avant l'exécution de `start_prim/stop_prim` (`class="prim"`).
- `myotherbin` provoque un stop du module (`action="stop"`). Sa surveillance est activée/désactivée après/avant l'exécution de `start_second/stop_second` (`class="second"`).
- `myappli` provoque l'exécution d'un script spécial `restart_myappli.cmd` (`action="restart_myappli"`) localisé dans le répertoire `bin` du module. La surveillance de `myappli` est activée/désactivée manuellement, dans les scripts du module, après/avant son lancement/arrêt (e.g. `class="myappli"`). Voir les scripts dans la [section 15.4.2](#).

Cette configuration permet de redémarrer individuellement le processus `myappli` sans redémarrer complètement l'application intégrée dans `start_prim/stop_prim`.

Les actions `restart` et `stopstart` incrémentent automatiquement le compteur `maxloop` pour limiter le nombre d'actions automatiques en cas d'erreur persistante. Par défaut, à la 4<sup>ème</sup> détection d'erreur en 24h (voir `maxloop` et `loop_interval` décrits dans la [section 13.3.3](#)), le module est arrêté.

Si l'action consiste en l'exécution d'un script spécial, ce script doit gérer manuellement le compteur `maxloop` (i.e. `restart_myappli.cmd`).



The screenshot shows the configuration interface for a module. On the left, the 'Processes/services' section is visible, showing a table of processes and their actions. On the right, the XML configuration for the module is displayed, showing the configuration for the 'myappli.exe' process.

Process/service name*	Type*	Action*
mybin.exe	Process	restart
myotherbin.exe	Process	stop
myappli.exe	Process	restart_myappli

```
<!DOCTYPE safe>
<safe>
  <service mode="mirror">
    <heart>
      <heartbeat name="default">
      </heartbeat>
    </heart>

    <errd>
      <proc name="mybin.exe"
        action="restart"
        class="prim"/>
      <proc name="myotherbin.exe"
        action="stop"
        class="second"/>
      <proc name="myappli.exe"
        action="restart_myappli"
        class="myappli"/>
    </errd>

    <user>
    </user>

  </service>
</safe>
```

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.

Pour des détails sur la configuration XML de `<errd>`, voir [section 13.10](#).

### 15.4.2 Configuration avancée des scripts du module

Le module surveille la présence des processus :

- mybin et myappli démarrés/arrêtés sur le nœud primaire avec start\_prim/stop\_prim
- myotherbin démarré/arrêté sur le nœud secondaire avec start\_second/stop\_second

<div style="display: flex; justify-content: space-between; align-items: center;"> <span><input checked="" type="checkbox"/> Edit module configuration</span> <span><input type="checkbox"/> Advanced configuration</span> </div> <div style="margin-top: 20px;"> <p style="text-align: center; color: #eee;">bin/start_prim.cmd</p> <p style="text-align: center; color: #eee;">bin/start_second.cmd</p> <p style="text-align: center; color: #eee;">bin/stop_prim.cmd</p> <p style="text-align: center; color: #eee;">bin/stop_second.cmd</p> </div>	<div style="display: flex; justify-content: space-between; align-items: center; border-bottom: 1px solid #ccc; margin-bottom: 10px;"> <span style="color: #007bff;">2</span> Edit module scripts <small>Optional</small> <span style="color: #007bff;">3</span> Enable communication encryption <small>Optional</small> </div> <div style="background-color: #333; color: #eee; padding: 5px; text-align: center; margin-bottom: 10px;">bin/start_prim.cmd</div> <pre style="background-color: #f9f9f9; padding: 10px; border: 1px solid #ddd;">@echo off echo "Running <b>start_prim</b> %*"  %SAFE%\safekit printi "start mybin" start %SAFEUSERBIN%\mybin.exe 10000000  %SAFE%\safekit printi "start myappli" start %SAFEUSERBIN%\myappli.exe 10000000 %SAFE%\safekit errd enable myappli</pre> <p>Noter l'appel à safekit errd enable myappli pour démarrer la surveillance du processus avec class="myappli", une fois ce processus lancé.</p> <p>Voir la <a href="#">section 13.10.4</a> pour la description de cette commande.</p>
<div style="display: flex; justify-content: space-between; align-items: center;"> <span><input checked="" type="checkbox"/> Edit module configuration</span> <span><input type="checkbox"/> Advanced configuration</span> </div> <div style="margin-top: 20px;"> <p style="text-align: center; color: #eee;">bin/start_prim.cmd</p> <p style="text-align: center; color: #eee;">bin/start_second.cmd</p> <p style="text-align: center; color: #eee;">bin/stop_prim.cmd</p> <p style="text-align: center; color: #eee;">bin/stop_second.cmd</p> </div>	<div style="display: flex; justify-content: space-between; align-items: center; border-bottom: 1px solid #ccc; margin-bottom: 10px;"> <span style="color: #007bff;">2</span> Edit module scripts <small>Optional</small> <span style="color: #007bff;">3</span> Enable communication encryption <small>Optional</small> </div> <div style="background-color: #333; color: #eee; padding: 5px; text-align: center; margin-bottom: 10px;">bin/stop_prim.cmd</div> <pre style="background-color: #f9f9f9; padding: 10px; border: 1px solid #ddd;">@echo off echo "Running <b>stop_prim</b> %*" %SAFE%\safekit printi "stop mybin" %SAFE%\safekit kill -level="terminate" - name="mybin.exe"  %SAFE%\safekit printi "stop myappli" %SAFE%\safekit errd disable myappli %SAFE%\safekit kill -level="terminate" - name="restart_myappli.cmd" %SAFE%\safekit kill -level="terminate" - name="myappli.exe" :end</pre> <p>Noter l'appel à safekit errd disable myappli pour arrêter la surveillance du processus avec class="myappli", avant d'arrêter ce processus.</p>

Le handler spécifique restart\_myappli.cmd est éditable en « Configuration avancée ». Ce script incrémente le compteur maxloop et redémarre le processus myappli.

<p>✓ Edit module configuration</p> <p>✓ Advanced configuration</p> <p>bin/start_prim.cmd</p> <p>bin/start_second.cmd</p> <p>bin/stop_prim.cmd</p> <p>bin/stop_second.cmd</p> <p>bin/prestart.cmd</p> <p>bin/myappli.exe</p> <p>bin/mybin.exe</p> <p>bin/myotherbin.exe</p> <p>bin/restart_myappli.cmd</p>	<p>2 Edit module scripts <small>Optional</small></p> <p>3 Enable communication <small>Optional</small></p> <p><b>bin/restart_myappli.cmd</b></p> <pre>@echo off  %SAFE%\safekit printi "restart_myappli"  rem first disable monitoring of the application %SAFE%\safekit errd disable myappli  rem increment loop counter %SAFE%\safekit incloop -i "restart_myappli" if %errorlevel% == 0 goto next rem max loop reached %SAFE%\safekit stop -i "restart_myappli" %SAFEBIN%\exitcode 0  :next rem <b>max loop not reached</b> : go on restarting the application %SAFE%\safekit printi "Restart myappli" %SAFE%\safekit kill -level="terminate" - name="myappli.exe" start %SAFEUSERBIN%\myappli.exe 10000000  rem finally, enable monitoring of the application %SAFE%\safekit errd enable myappli %SAFEBIN%\exitcode 0</pre>
<p>Basculer en « Configuration avancée » pour lister et éditer tous les scripts.</p>	<p>Noter l'incrémentation du compteur de rebouclage avec <code>safekit incloop -i "restart_myappli"</code> et l'arrêt du module quand <code>maxloop</code> est atteint.</p> <p>Voir <a href="#">section 14.5.3</a> pour la description de cette commande.</p>

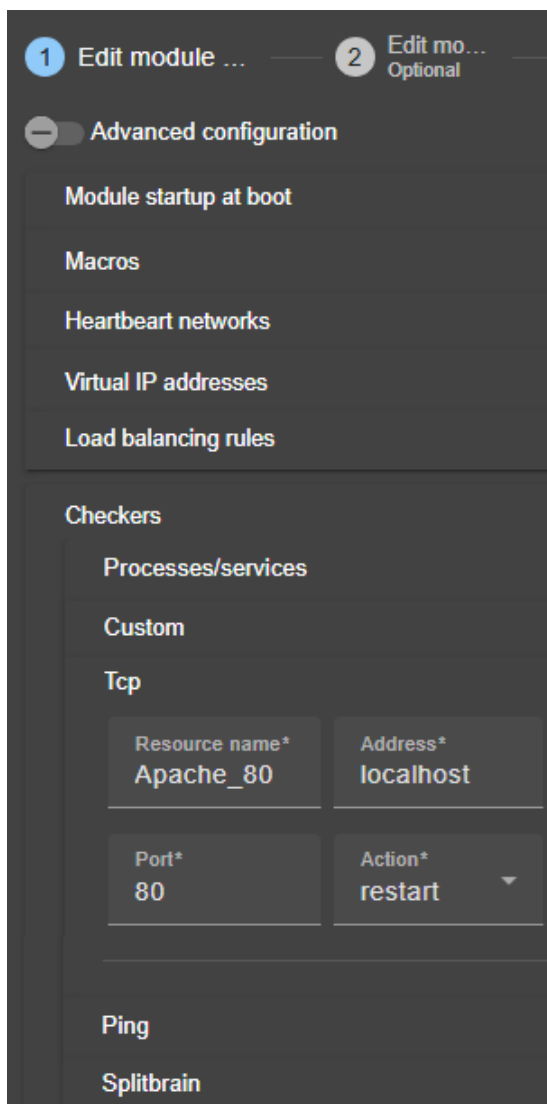
## 15.5 Exemple de TCP checker

Ci-dessous l'exemple de la configuration d'un TCP checker dans un module ferme. Ce checker teste que la connexion au service web local sur le port 80. Si la connexion échoue, le checker met la ressource `tcp.Apache_80` à down. La règle de failover associée, nommée `t_ Apache_80`, exécute un `restart` du module quand la ressource passe à down.

- Le préfixe du nom de la ressource est `tcp`.
- Le préfixe du nom de la règle de failover est `t_`
- Le suffixe est la valeur de l'attribut `ident`

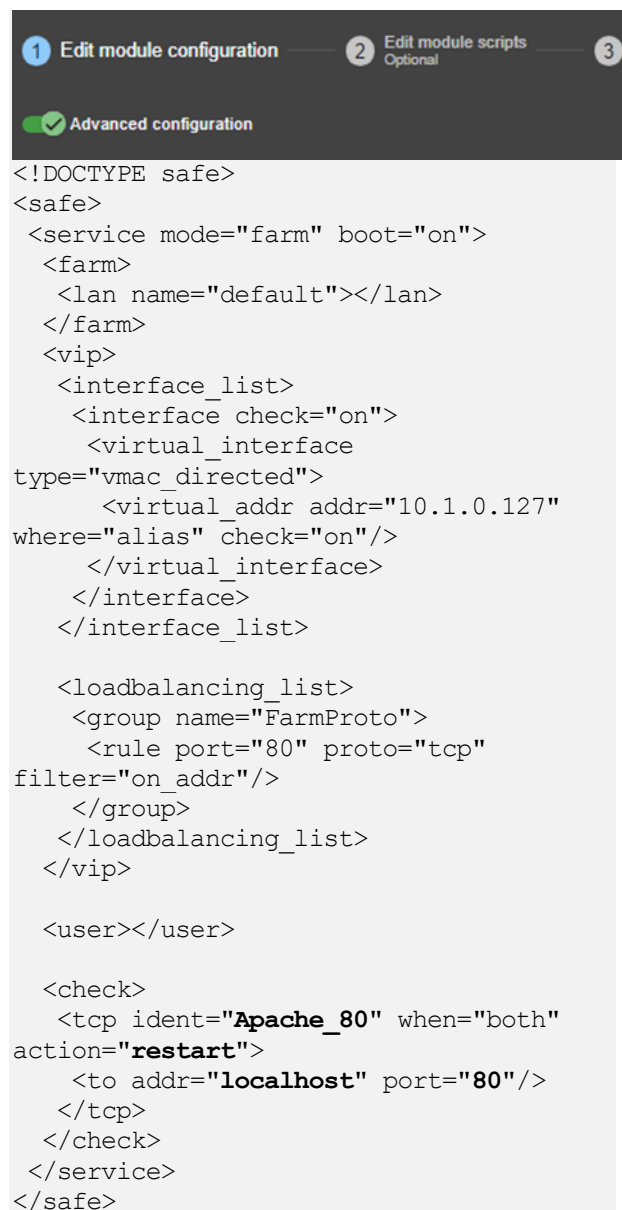
Pour une description des checkers, voir la [section 13.11.3](#).

Pour tester le TCP checker, voir la [section 4.4.2](#) et la [section 4.4.3](#).



Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.



Pour des détails sur la configuration XML de <tcp>, voir [section 13.12](#).

## 15.6 Exemple de ping checker

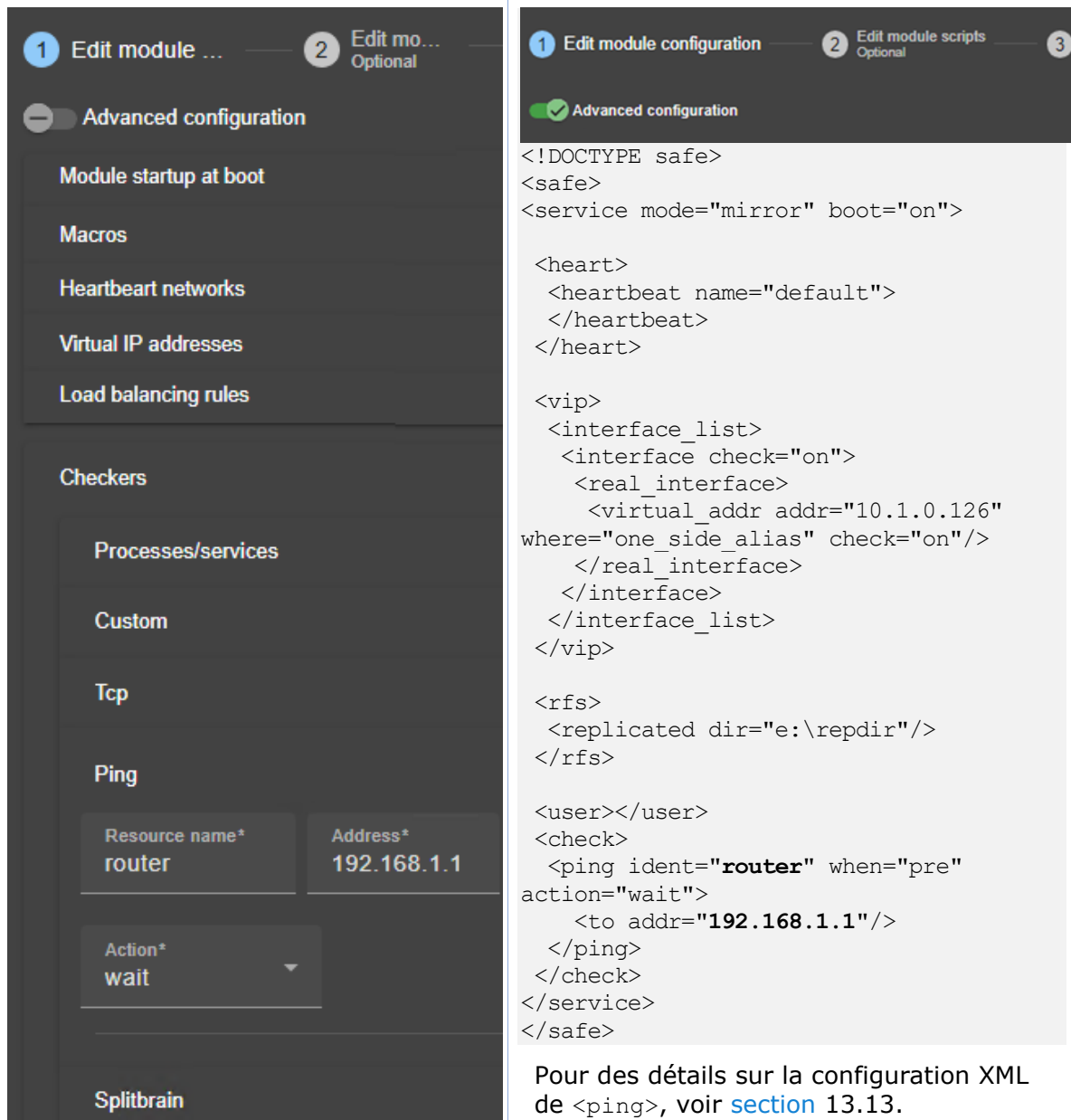
Ci-dessous l'exemple de la configuration d'un ping checker dans un module miroir. Ce checker teste si l'adresse 192.168.1.1 répond au ping. Si le ping échoue, le checker affecte la ressource `ping.router` à `down`. La règle de failover associée, nommée `p_router`, exécute un `wait` du module quand la ressource passe à `down`.



- Le préfixe du nom de la ressource est `ping`.
- Le préfixe du nom de la règle de failover est `p_`
- Le suffixe est la valeur de l'attribut `ident`

Pour une description des checkers, voir la [section 13.11.3](#).

Pour tester le ping checker, voir la [section 4.4.5](#).



The screenshot displays the configuration interface for the 'Ping' checker. On the left, the 'Checkers' section is expanded to 'Ping'. The configuration fields are as follows:

Resource name*	Address*
router	192.168.1.1

The 'Action\*' dropdown menu is set to 'wait'. The 'Splitbrain' option is visible at the bottom of the configuration panel.

On the right, the XML configuration code is shown, corresponding to the settings in the interface:

```
<!DOCTYPE safe>
<safe>
<service mode="mirror" boot="on">

  <heart>
    <heartbeat name="default">
    </heartbeat>
  </heart>

  <vip>
    <interface_list>
      <interface check="on">
        <real_interface>
          <virtual_addr addr="10.1.0.126"
where="one_side_alias" check="on"/>
        </real_interface>
      </interface>
    </interface_list>
  </vip>

  <rfs>
    <replicated dir="e:\replib"/>
  </rfs>

  <user></user>
  <check>
    <ping ident="router" when="pre"
action="wait">
      <to addr="192.168.1.1"/>
    </ping>
  </check>
</service>
</safe>
```

Pour des détails sur la configuration XML de <ping>, voir [section 13.13](#).

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.

### 15.7 Exemple de custom checker avec `customchecker.safe`

Le module `customchecker.safe` est un module miroir de démonstration incluant un custom checker qui teste la présence d'un fichier sur le serveur primaire. Cette fonctionnalité est disponible également dans un module ferme.

Si le fichier est absent, le checker affecte la ressource `custom.checkfile` à `down`. La règle de failover associée, nommée `c_checkfile`, exécute un `restart` du module quand la ressource passe à `down`.

- Le préfixe du nom de la ressource est `custom`.
- Le préfixe du nom de la règle de failover est `c_`
- Le suffixe est la valeur de l'attribut `ident`

Le module `customchecker.safe` est livré avec le package `SafeKit` et peut servir de base pour l'écriture de votre propre checker.

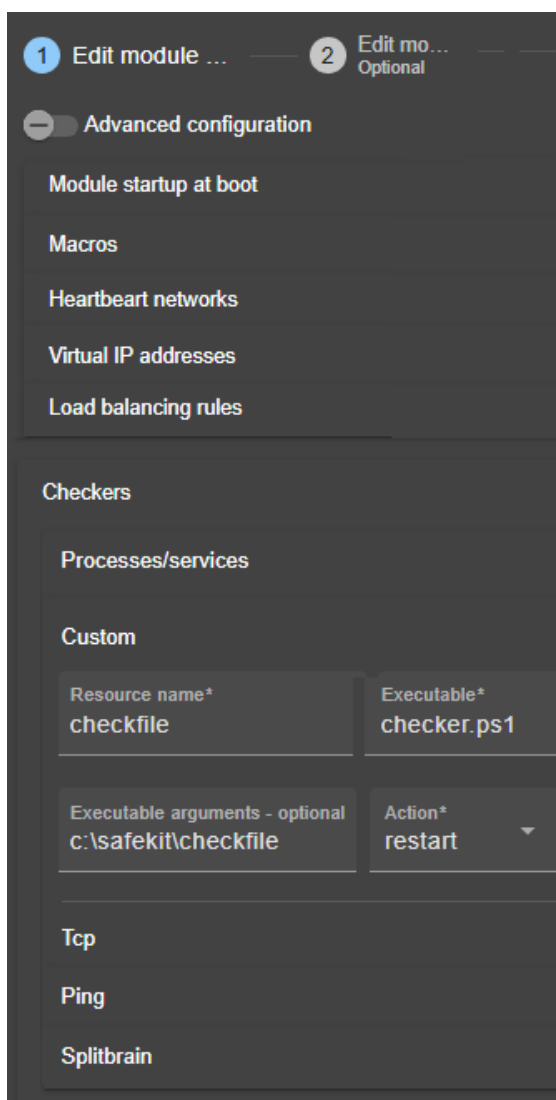
Pour une description des checkers, voir la [section 13.11.3](#).

Pour tester le checker custom, voir la [section 4.4.7](#) et la [section 4.4.8](#).

- La description suivante est pour Windows. Pour Linux, veuillez consulter `customchecker.safe` fourni avec le package Linux qui comprend la configuration et les scripts pour Linux.

#### 15.7.1 Configuration du module avec un custom checker

L'exemple suivant est la configuration du custom checker prise en charge depuis `SafeKit 8` avec l'attribut `action`.



Pour lancer l'assistant de configuration du module, voir [section 3.3](#).  
 Basculer en « Configuration avancée » pour éditer le XML si besoin.



Pour des détails sur la configuration XML de < custom >, voir [section 13.16](#).

La configuration du custom checker pour SafeKit < 8 est toujours prise en charge. Dans les versions précédentes, la configuration du custom checker nécessitait de définir une règle de failover explicite dans le fichier userconfig.xml comme suit :

```

<check>
  <custom ident="checkfile" exec="checker.ps1" arg="c:\safekit\checkfile"
when="prim"/>
</check>
<failover>
  <![CDATA[
    c_checkfile: if( custom.checkfile == down ) then restart();
  ]>
</failover>
    
```

L'attribut `action` n'est pas défini et sa valeur par défaut est `noaction`.

L'assistant de configuration du module ne présente pas la section `failover`. Basculer en « Configuration avancée » pour l'éditer.

### 15.7.2 Configuration avancée du script du module checker

Le custom checker est une boucle infinie qui effectue un test et affecte la ressource associée l'état `up` ou `down` en fonction du résultat du test.

Le checker est automatiquement appelé avec au moins 2 arguments :

- Le 1<sup>er</sup> argument est le nom module
- Le 2<sup>ème</sup> est le nom de la ressource à affecter

Si la configuration `<custom>` contient l'attribut `arg`, sa valeur est passée comme arguments suivants.

Le checker est écrit en respectant les précautions suivantes :

- La ressource n'est affectée que si sa valeur a changé
- Quand la ressource est `down`, le checker consolide cet état (`grace` fois) avant de l'affecter. Cela peut permettre d'éviter de fausses détections d'erreur.

<p> <input checked="" type="checkbox"/> Edit module configuration  <input checked="" type="checkbox"/> Advanced configuration         </p> <p> <a href="#">bin/start_prim.cmd</a>  <a href="#">bin/stop_prim.cmd</a>  <a href="#">bin/prestart.cmd</a>  <a href="#">bin/checker.ps1</a> </p>	<p> <input checked="" type="radio"/> 2 Edit module scripts  <small>Optional</small> </p> <p> <input type="radio"/> 3 Enable communication encryption  <small>Optional</small> </p> <p><b>bin/checker.ps1</b></p> <pre> # Custom checker template that tests if a file exists  param([Parameter(Mandatory = \$true, ValueFromPipeLine = \$true, position=1)][String]\$ModName,       [Parameter(Mandatory = \$true, ValueFromPipeLine = \$true, position=2)][String]\$RName,       [Parameter(Mandatory = \$true, ValueFromPipeLine = \$true, position=3)][String]\$Arg1Value,       [Parameter(Mandatory = \$false, ValueFromPipeLine = \$false, position=4)][String]\$Grace="2",       [Parameter(Mandatory = \$false, ValueFromPipeLine = \$false, position=5)][String] \$Period="5"     )  # return up on success   down on failure Function test([String]\$Arg1Value) {     \$res="down"     if (Test-Path "\$Arg1Value"){         \$res="up"     }     return \$res }  \$customchecker=\$MyInvocation.MyCommand.Name \$safekit="\$env:SAFE/safekit.exe" \$gracecount=0 \$prevrstate="unknown" # wait a little Start-Sleep \$Period                 </pre>
<p>Basculer en « Configuration avancée » pour lister et éditer tous les scripts.</p>	

```
while ($true){
  Start-Sleep $Period
  $rstate = test($Arg1Value)
  if($rstate -eq "down"){
    $gracecount+=1
  }else{
    $gracecount = 0
    if($prevrstate -ne $rstate){
      & $safekit set -r "$RName" -v $rstate -i
$customchecker -m $ModName
      $prevrstate = $rstate
    }
  }
  if($gracecount -ge $Grace){
    if($prevrstate -ne $rstate){
      & $safekit set -r "$RName" -v $rstate -i
$customchecker -m $ModName
      $prevrstate = $rstate
    }
    $gracecount = 0
  }
}
```

Noter l'appel à `safekit set -r custom.checkfile -v up` (ou `down`) pour affecter la valeur de la ressource.

Voir la [section 9.3](#) pour la description de cette commande.

### 15.8 Exemple de splitbrain checker

Ci-dessous l'exemple de la configuration d'un `splitbrain`, configurable uniquement dans un module miroir. Ce checker teste si l'adresse `192.168.1.1` répond au ping. Si le ping échoue, le checker affecte la ressource `splitbrain.witness` à `down`.

En cas d'isolation réseau entre les nœuds, le `splitbrain checker` affecte la ressource `splitbrain.uptodate` à `up` ou `down` en accord avec l'accès au `witness`. La règle de failover statique et prédéfinie, nommée `splitbrain_failure`, exécute un `wait` du module quand cette ressource passe à `down`. Cela garantit que seul le nœud ayant accès au `witness` devient `ALONE`, l'autre se bloquant dans l'état `WAIT`.

- Le préfixe du nom de la ressource est `splitbrain`.
- Le suffixe est la valeur de l'attribut `ident`
- La règle de failover est statique et prédéfinie, et teste l'autre ressource affectée par le `splitbrain checker`, `splitbrain.uptodate`. Elle se nomme `splitbrain_failure`.



Pour une description des checkers, voir la [section 13.11.3](#).

Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

Basculer en « Configuration avancée » pour éditer le XML si besoin.

```

<!DOCTYPE safe>
<safe>
<service mode="mirror" boot="on">

<heartbeat>
  <heartbeat name="default">
  </heartbeat>
</heartbeat>

<vip>
  <interface_list>
    <interface check="on">
      <real_interface>
        <virtual_addr addr="10.1.0.126"
where="one_side_alias" check="on"/>
      </real_interface>
    </interface>
  </interface_list>
</vip>

<rfs>
  <replicated dir="e:\replib"/>
</rfs>

<user></user>

<check>
  <check>
    <splitbrain ident="witness"
exec="ping" arg="10.1.0.112"/>
  </check>
</check>
</service>
</safe>

```

Pour des détails sur la configuration XML de `<splitbrain>`, voir [section 13.18](#).

## 15.9 Exemples de module checker

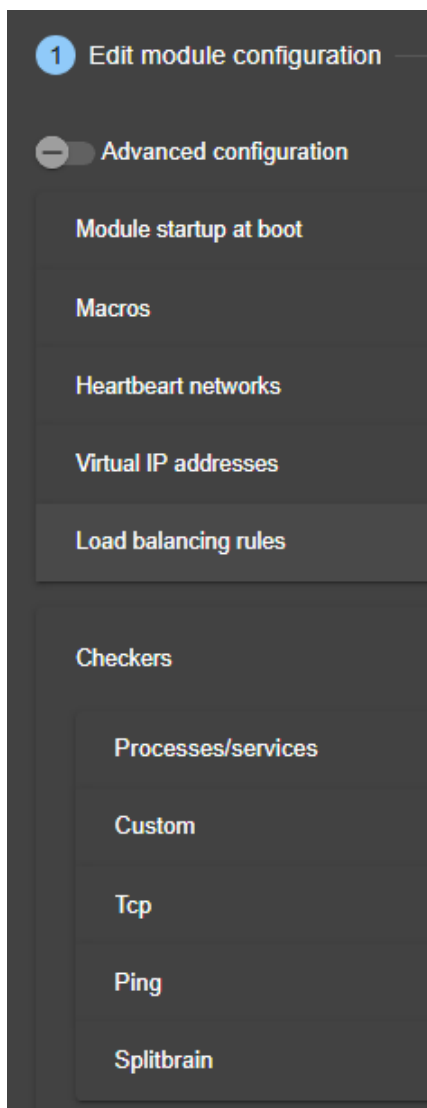
### 15.9.1 Exemple d'un module ferme dépendant d'un module miroir

Ci-dessous un exemple de la configuration d'un module checker dans un module ferme. Ce checker teste que le module nommé `mirror` avec l'adresse IP virtuelle `10.0.0.129` est prêt (`ALONE` ou `PRIM`). S'il n'est pas prêt, le checker affecte la ressource `module.mirror_10.0.0.129` à `down`. La règle de failover statique et prédéfinie, nommée `module_failure`, exécute un `wait` sur le module ferme lorsque cette ressource passe à `down`.

- Le préfixe du nom de la ressource est **module**.
- Le suffixe est la valeur des attributs `name` et `addr`
- La règle de failover est statique et prédéfinie, et se nomme `module_failure`

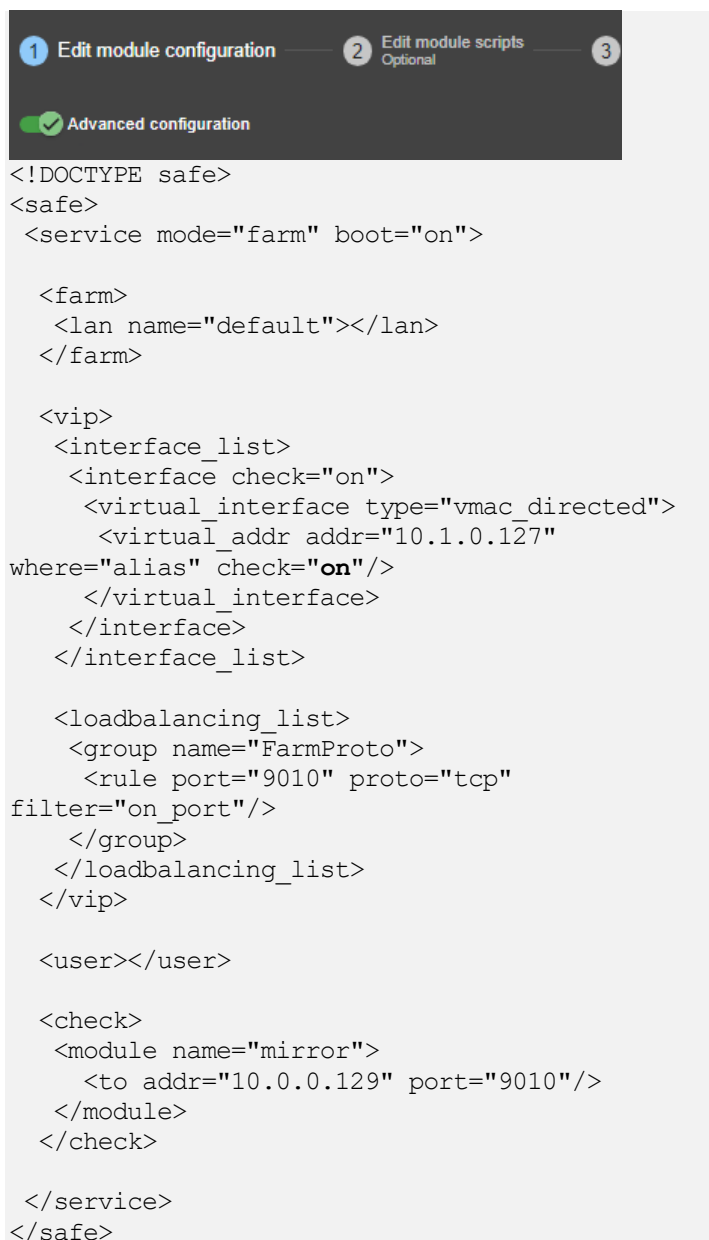
Pour une description des checkers, voir la [section 13.11.3](#).

Pour tester le module checker, voir la [section 4.4.6](#).



Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

L'assistant n'affiche pas le module checker. Basculer en « Configuration avancée » pour le configurer.



Pour des détails sur la configuration XML de `<module>`, voir [section 13.17](#).



La dépendance des modules peut être utilisée lorsque vous déployez des modules ferme et miroir sur le même cluster SafeKit ou lorsque vous déployez des modules ferme et miroir sur deux clusters différents. Dans ce cas, le mot de passe affecté pour initialiser le service web de SafeKit, doit être identique sur les 2 cluster.

### 15.9.2 Exemple avec `leader.safe` et `follower.safe`

Les deux modules de démonstration `leader.safe` et `follower.safe` livrés avec SafeKit permettent de configurer un ou plusieurs modules followers dont le démarrage dépend du démarrage du module miroir principal, nommé leader.

Par exemple, les services principaux d'une application avec des répertoires répliqués peuvent être configurés dans le module leader, et certains services annexes de cette application peuvent être démarrés dans un module follower, si vous considérez que sa défaillance ne doit déclencher que son propre redémarrage ; Les autres modules followers et le module leader ne sont pas impactés, ce qui permet une continuité de service pour ces modules.

Le module leader est un miroir : il inclut dans ses scripts le démarrage/arrêt des modules followers.

Chaque module follower est un module light avec les scripts de démarrage/arrêt d'un service et la détection d'erreur. Chaque module follower est dépendant des défaillances du module leader avec le checker de module suivant :

`follower/conf/userconfig.xml` - voir [section 13](#)

```
...
<check>
  <module name="leader"/>
</check>
...
```

Il s'agit d'une configuration synthétique à la place de :

```
...
<check>
  <module name="leader">
    <to addr="127.0.0.1" port="9010"/>
  </module>
</check>
...
```



Si vous avez modifié le port d'écoute du service web de SafeKit (voir [section 10.9](#)), remplacez la configuration synthétique par la configuration complète et changez la valeur du port.

### 15.10 Exemple de checker d'interface réseau

Ci-dessous, l'exemple d'une configuration d'interface checker générée automatiquement lorsque l'option `<interface check="on">` est définie (voir [section 13.6](#)).

Dans le fichier de configuration d'un module miroir par exemple, l'adresse virtuelle est définie comme suit :

```
<vip>
  <interface_list>
    <interface check="on">
```

```
<real_interface>
  <virtual_addr addr="10.0.0.129" where="one_side_alias" check="on"/>
</real_interface>
</interface>
</interface_list>
</vip>
```

Lors de la configuration du module, SafeKit génère la configuration correspondante pour l'interface checker. Pour l'exemple, la configuration automatiquement générée est :

```
<check>
  <intf when="pre" ident="10.0.0.0">
    <to local_addr="10.0.0.107"/>
  </intf>
</check>
```

où la valeur de `ident` correspond au réseau associé à l'adresse IP virtuelle ; la valeur de `local_addr` est la première adresse IP du réseau correspondant à l'adresse virtuelle.

Le checker vérifie que le câble Ethernet est connecté à cette interface. Si le câble est déconnecté, le checker met la ressource associée `intf.10.0.0.0` à `down`. La règle de failover statique et prédéfinie, nommée `interface_failure`, exécute un `wait` sur le module lorsque cette ressource passe à `down`.

- Le préfixe du nom de la ressource est `intf`.
- Le suffixe est la valeur de l'attribut `ident`
- La règle de failover est statique et prédéfinie, et se nomme `interface_failure`

Pour plus de détails sur la configuration de checker d'interface, voir la [section 13.14](#).

Pour une description des checkers, voir la [section 13.11.3](#).

Pour tester le checker d'interface réseau, voir la [section 4.4.4](#).

### 15.11 Exemple d'IP checker

Ci-dessous, l'exemple d'une configuration d'IP checker générée automatiquement lorsque l'option `<virtual_addr check="on" ...>` est positionnée (voir [section 13.6](#)).

Dans le fichier de configuration d'un module miroir par exemple, l'adresse virtuelle est définie comme suit :

```
<vip>
  <interface_list>
    <interface check="on">
      <real_interface>
        <virtual_addr addr="10.0.0.129" where="one_side_alias" check="on"/>
      </real_interface>
    </interface>
  </interface_list>
</vip>
```

Lors de la configuration du module, SafeKit génère la configuration correspondante pour l'IP checker. Pour l'exemple, la configuration automatiquement générée est :

```
<check>
  <ip ident="10.0.0.129" when="prim">
    <to addr="10.0.0.129"/>
  </ip>
```

```
</check>
```

où les valeurs de `ident` et `addr` correspondent à l'adresse IP virtuelle ; la valeur de `when` est `prim` pour un module miroir, `both` pour un module ferme.

Le checker vérifie que l'adresse IP est configurée localement. Si ce n'est pas le cas, le checker affecte la ressource associée `ip.10.0.0.120` à `down`. La règle de failover statique et prédéfinie, nommée `ip_failure`, exécute un `stopstart` sur le module lorsque cette ressource passe à `down`.

- Le préfixe du nom de la ressource est `ip`.
- Le suffixe est la valeur de l'attribut `ident`
- La règle de failover est statique et prédéfinie, et se nomme `ip_failure`



Pour plus de détails sur la configuration de checker d'IP, voir la [section 13.15](#).

Pour une description des checkers, voir la [section 13.11.3](#).

### 15.12 Exemple d'hostname virtuel avec `vhost.safe`

Le module de démonstration `vhost.safe` montre comment positionner un hostname virtuel dans un module miroir. Cette fonctionnalité est disponible également dans un module ferme. Cette fonctionnalité est disponible également dans un module ferme.

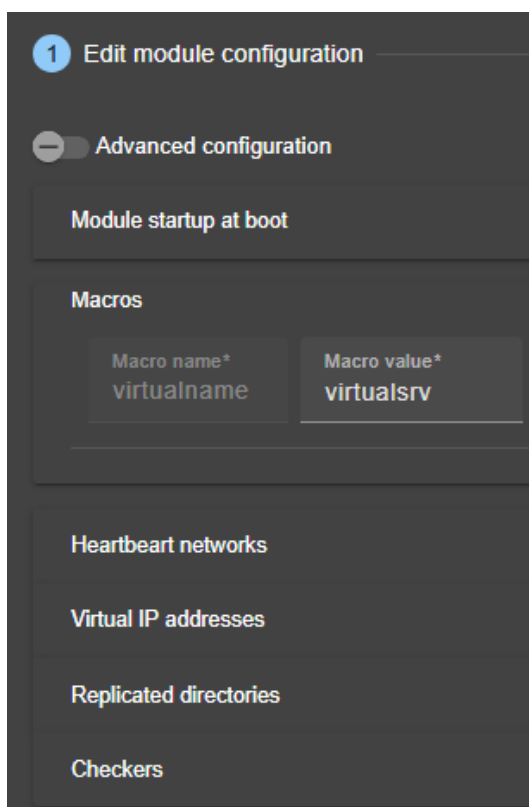


La description suivante est pour Windows. Pour Linux, veuillez consulter `vhost.safe` fourni avec le package Linux qui comprend la configuration et les scripts pour Linux.

En Windows, le module `vhost.safe` livré depuis SafeKit 8.2.4 a été amélioré pour permettre de tester la configuration du nom d'un hostname virtuel pour un service. Il repose sur un service HTTP appelé `testhostname` qui est créé/supprimé lors de la configuration/déconfiguration du module. Ce service est démarré/arrêté par les scripts du module et écoute sur le port 9999. L'URL <http://localhost:9999/hostname> renvoie la valeur du hostname telle que vue par le service `testhostname`, qui est le hostname virtuel lorsque le module est primaire.

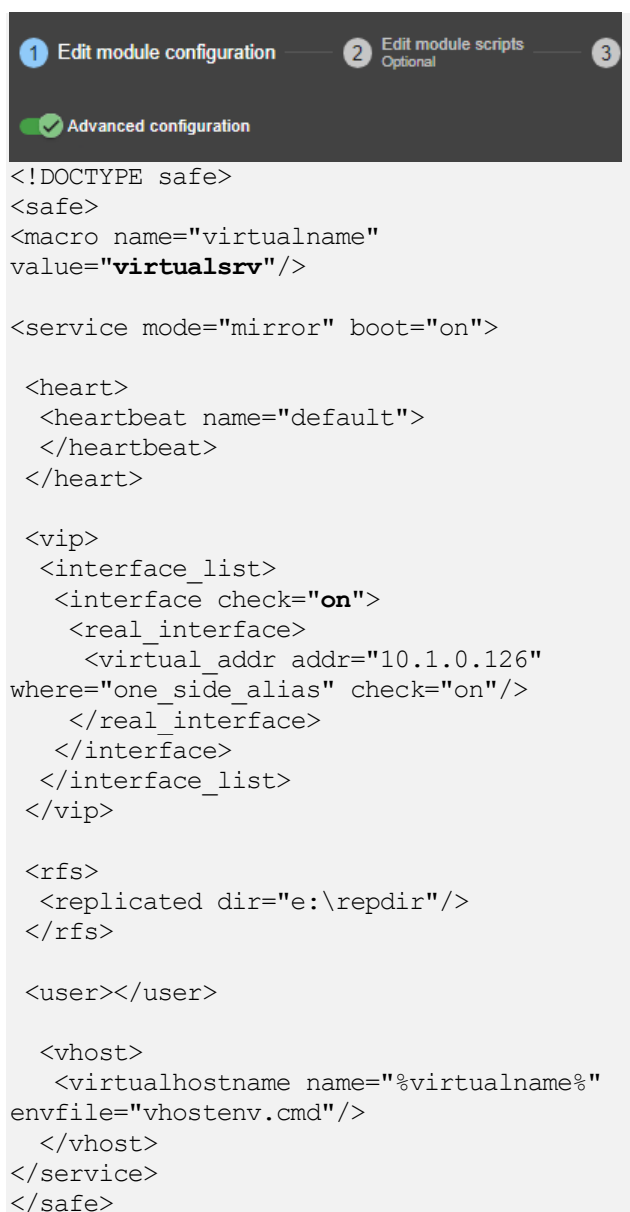
#### 15.12.1 Configuration du module avec un hostname virtuel

Dans l'exemple suivant, une `<macro>` est configurée et sa valeur est utilisée pour définir le nom d'hôte virtuel.



Pour lancer l'assistant de configuration du module, voir [section 3.3](#).

L'assistant n'affiche pas le vhost. Basculer en « Configuration avancée » pour l'éditer.



Pour des détails sur la configuration XML de <module>, voir [section 13.9](#).

### 15.12.2 Scripts du module avec un hostname virtuel

En plus de cette configuration, il faut exécuter des commandes spéciales dans les scripts du module.

#### 15.12.2.1 Script start\_prim

Le script exécute des commandes pour activer le nom hostname virtuel dans l'environnement du script, ainsi que dans celui du service en Windows.

Edit module configuration

Advanced configuration

[bin/start\\_prim.cmd](#)

[bin/stop\\_prim.cmd](#)

**2** Edit module scripts Optional      **3** Enable communication encryption Optional

**bin/start\_prim.cmd**

```
@echo off
echo "Running start_prim %*"

rem Set virtual hostname
CALL "%SAFEUSERBIN%\vhostenv.cmd"

rem Next commands use the virtual hostname
FOR /F %x IN ('hostname') DO SET servername=%x
echo "hostname is "%servername%"

rem WARNING: previous virtual hostname setting is
insufficient to change the hostname for services
rem If one service needs the virtual hostname, you
need also to uncomment the rem following

rem "%SAFE%\private\bin\vhostservice"
SERVICE_TO_BE_DEFINED

set res=0

rem net start "myservice"

set res=%errorlevel%
if %res% == 0 goto end

:stop
"%SAFE%\safekit" printe "start_prim failed"

rem uncomment to stop the module when critical
rem "%SAFE%\safekit" stop -i "start_prim"

:end
```

Pour la description de la commande `safekit`, voir la [section 9](#).

### 15.12.2.2 Script stop\_prim

Le script exécute des commandes pour désactiver le hostname virtuel dans l'environnement du script, ainsi que dans celui du service en Windows.

<p><input checked="" type="checkbox"/> Edit module configuration</p> <p><input type="checkbox"/> Advanced configuration</p> <p>bin/start_prim.cmd</p> <p>bin/stop_prim.cmd</p>	<p>2 Edit module scripts Optional</p> <p>3 Enable communication encryption Optional</p> <p>bin/stop_prim.cmd</p> <pre>@echo off echo "Running stop_prim %*"  rem Reset virtual hostname CALL "%SAFEUSERBIN%\vhostenv.cmd"  rem Next commands use the real hostname FOR /F %x IN ('hostname') DO SET servername=%x echo "hostname is %servername%"  set res=0  rem default: no action on forcestop if "%1" == "force" goto end  rem net stop "myservice" /Y set res=%errorlevel%  rem If necessary, wait for the stop of the services rem "%SAFEBIN%\sleep" 10  if %res% == 0 goto end  "%SAFE%\safekit" printe "stop_prim failed"  :end rem WARNING: if the virtual hostname was set for rem services in start_prim.cmd, rem uncomment the following to restore the real rem hostname in last stop phase :  rem "%SAFE%\private\bin\vhostservice" SERVICE_TO_BE_DEFINED</pre> <p>Pour la description de la commande safekit, voir la <a href="#">section 9</a>.</p>
--	---

## 16.Cluster SafeKit dans le cloud

- ⇒ [Section 16.1](#) « Cluster SafeKit dans Amazon AWS »
- ⇒ [Section 16.2](#) « Cluster SafeKit dans Microsoft Azure »
- ⇒ [Section 16.3](#) « Cluster SafeKit dans Google GCP »

Vous pouvez installer, configurer et administrer des modules SafeKit qui s'exécutent sur des serveurs virtuels dans les clouds Microsoft Azure, Amazon AWS et Google GCP plutôt que sur des serveurs physiques sur site. Cela nécessite un minimum de paramétrage du cloud et/ou des serveurs, en particulier pour mettre en œuvre une adresse IP virtuelle.

### 16.1 Cluster SafeKit dans Amazon AWS

Dans ce qui suit, nous supposons que vous êtes familiers avec :

- Amazon Elastic Compute Cloud (Amazon EC2) qui offre des capacités de calcul dans le cloud Amazon Web Services (AWS). Pour plus d'informations sur les fonctionnalités d'Amazon EC2, consultez la section du [produit Amazon EC2](#).
- AWS CloudFormation qui aide à déployer des instances et des applications dans Amazon EC2. Cela permet de gagner beaucoup de temps et d'efforts d'installation : le temps libéré pour la gestion des ressources EC2 peut être exploité pour se consacrer aux applications qui s'exécutent dans AWS.

Avant de pouvoir mettre en œuvre un module SafeKit, l'administrateur doit :

1. Créer des instances (2 pour un module miroir)
2. Effectuer les paramétrages d'AWS, des instances et de SafeKit
3. Enfin, appliquer des configurations SafeKit spécifiques en fonction du module que vous souhaitez mettre en œuvre.

#### Paramétrage d'AWS

Il faut paramétrer AWS pour :

- associer des adresses publiques à chaque instance si vous souhaitez les administrer avec la console web SafeKit depuis internet
- configurer les groupes de sécurité associés au(x) réseau(x) pour ouvrir les communications du framework SafeKit et de la console web SafeKit. Les ports à ouvrir sont décrits en [section 10.2](#)
- utiliser un réseau à large bande passante et à faible latence si la réplication temps réel est utilisée dans un module miroir

#### Paramétrage des instances

Sur chaque instance, il faut en plus :

- installer le package SafeKit
- appliquer la configuration HTTPS pour sécuriser la console Web SafeKit (voir [section 11](#))

### Paramétrage de SafeKit

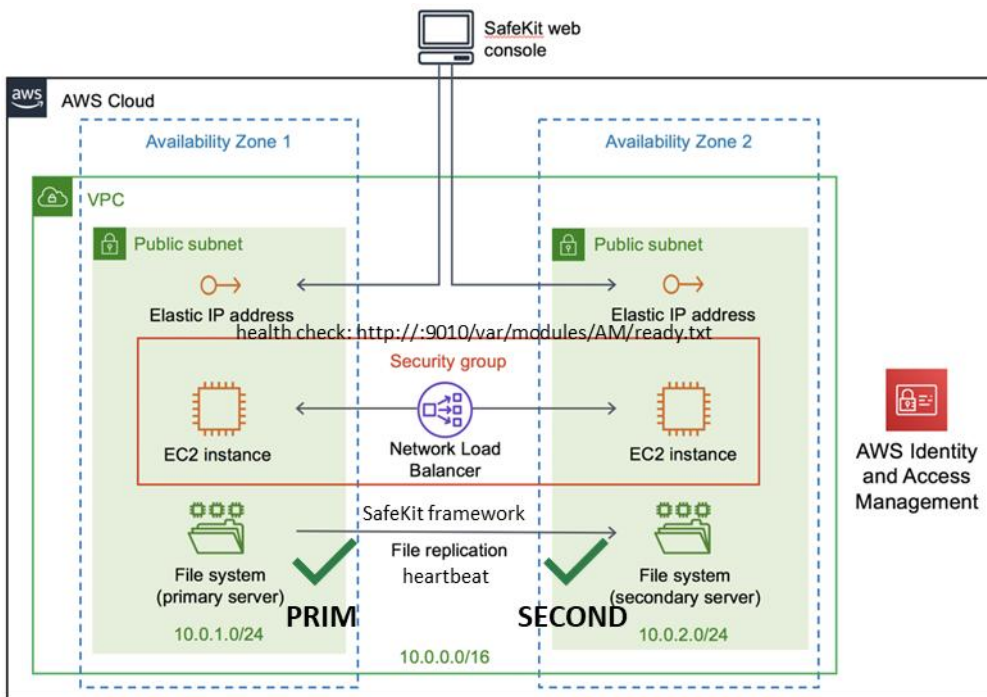
Enfin il faut saisir la configuration du cluster SafeKit et l'appliquer à tous les nœuds (voir [section 12](#)). Par exemple, le fichier de configuration du cluster SafeKit serait :

```
<cluster>
<lans>
  <lan name="default">
    <node name="Server1" addr="10.0.11.10"/>
    <node name="Server2" addr="10.0.12.10"/>
  </lan>
</lans>
</cluster>
```

Le lan `default` est utilisé pour les communications du framework SafeKit entre les nœuds du cluster.

#### 16.1.1 Cluster miroir dans AWS

Les fonctionnalités du module miroir sont opérationnelles dans le cloud AWS (réplication de fichiers temps réel, reprise sur panne, détection de mort de processus, checkers, ...), à l'exception du basculement d'adresse IP virtuelle. A la place, vous pouvez configurer un module miroir sur le cluster et utiliser le produit Elastic Load Balancing d'AWS (voir [Produits Elastic Load Balancing dans AWS](#)) en le configurant de façon à diriger tout le trafic vers le nœud primaire. L'adresse IP et/ou un nom DNS associés au load balancer, jouent le rôle d'IP virtuelle.



Vous devez configurer vous-même le load balancer et le groupe de sécurité AWS.

Pour le load balancer, vous devez :

- spécifier les règles pour votre application
- définir dans le groupe cible du trafic les nœuds du cluster SafeKit



- définir le test de vérification de l'état. Ce test permet de vérifier si l'instance est dans un état sain ou non

Le load balancer achemine le trafic uniquement vers les instances saines. Il reroute le trafic vers l'instance lorsque celle-ci a été restaurée dans un état sain.

SafeKit fournit un testeur de vérification de l'état pour chaque module. Vous devez configurer le test de vérification dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où *AM* est le nom du module

Pour un module miroir, le test retourne :

- OK, qui signifie l'instance est saine, quand le module est dans l'état  PRIM (Ready) ou  ALONE (Ready)
- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états du module

Le groupe de sécurité doit au minimum être configuré pour autoriser les communications pour les protocoles et ports :

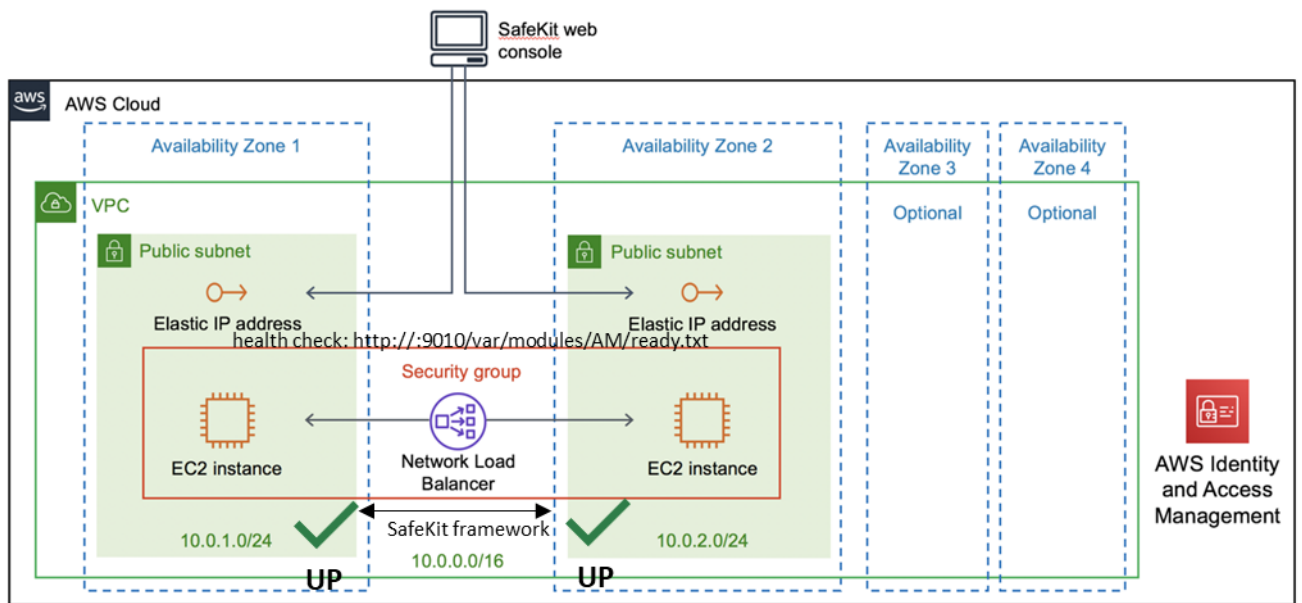
- UDP - 4800 pour le service `safeadmin` (entre les nœuds du cluster SafeKit)
- UDP - 8888 pour le heartbeat du module (entre les nœuds du cluster SafeKit)
- TCP - 5600 pour la réplication temps réelle du module (entre les nœuds du cluster SafeKit)
- TCP - 9010 pour la console web SafeKit en HTTP  
TCP - 9453 pour la console web SafeKit en HTTPS
- TCP - 9001 pour configurer la console web SafeKit en HTTPS



Les valeurs de ports du module dépendent de son id (voir [section Erreur ! Source du renvoi introuvable.](#)). Les valeurs ci-dessus sont pour le premier module installé.

### 16.1.2 Cluster ferme dans AWS

La plupart des fonctionnalités du module ferme sont opérationnelles dans le cloud AWS (détection de mort de processus, checker, ...), à l'exception du partage de charge sur l'adresse IP virtuelle. A la place, vous pouvez configurer un module ferme sur le cluster et utiliser le produit Elastic Load Balancing d'AWS (voir [Produits Elastic Load Balancing dans AWS](#)). L'adresse IP et/ou un nom DNS associés au load balancer, jouent le rôle d'IP virtuelle.



Si vous mettez en place le module ferme en dehors du modèle AWS CloudFormation pour SafeKit, vous devez configurer vous-même le load balancer et le groupe de sécurité AWS.

Pour le load balancer, vous devez :

- spécifier les règles pour votre application
- définir comme cibles du trafic les nœuds du cluster SafeKit
- définir le test de vérification de l'état. Ce test permet de vérifier si l'instance est dans un état sain ou non

Le load balancer achemine le trafic uniquement vers les instances saines. Il reroute le trafic vers l'instance lorsque celle-ci a été restaurée dans un état sain.

SafeKit fournit un testeur de vérification de l'état pour chaque module. Vous devez configurer le test de vérification dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où *AM* est le nom du module

Pour un module ferme, le test retourne :

- OK, qui signifie l'instance est saine, quand le module est dans l'état UP (Ready)
- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états

Le groupe de sécurité doit au minimum être configuré pour autoriser les communications pour les protocoles et ports :

- UDP - 4800 pour le service `safeadmin` (entre les nœuds du cluster SafeKit)
- TCP - 9010 pour la console web SafeKit en HTTP

- TCP - 9453 pour la console web SafeKit en HTTPS
- TCP - 9001 pour configurer la console web SafeKit en HTTPS

## 16.2 Cluster SafeKit dans Microsoft Azure

Dans la suite, nous supposons que vous êtes familiers avec Microsoft Azure, qui est un service de cloud computing créé par Microsoft pour créer, tester, déployer et gérer des applications et des services à travers un réseau mondial de centres de données Microsoft. Pour plus d'informations sur les fonctionnalités et l'utilisation d'Azure, voir le [portail Microsoft Azure](#).

Avant de pouvoir mettre en œuvre un module SafeKit, l'administrateur doit :

1. Créer des machines virtuelles (2 pour un module miroir)
2. Effectuer les paramétrages d'Azure, des machines virtuelles et de SafeKit
3. Enfin, appliquer des configurations SafeKit spécifiques en fonction du module que vous souhaitez mettre en œuvre.

### Paramétrage d'Azure

Il faut paramétrer Azure pour :

- associer des adresses IP publiques (éventuellement nom DNS) à chaque machine virtuelle si vous souhaitez les administrer avec la console web SafeKit depuis internet
- configurer, si nécessaire, le groupe de sécurité réseau pour ouvrir les communications du framework SafeKit et de la console web SafeKit. Les ports à ouvrir sont décrits en [section Erreur ! Source du renvoi introuvable](#).
- utiliser un réseau à large bande passante et à faible latence si la réplication temps réel est utilisée dans un module miroir

### Paramétrage des machines virtuelles

Sur chaque machine virtuelle, il faut en plus :

- installer le package SafeKit
- appliquer la configuration HTTPS pour sécuriser la console Web SafeKit (voir [section 11](#))

### Paramétrage de SafeKit

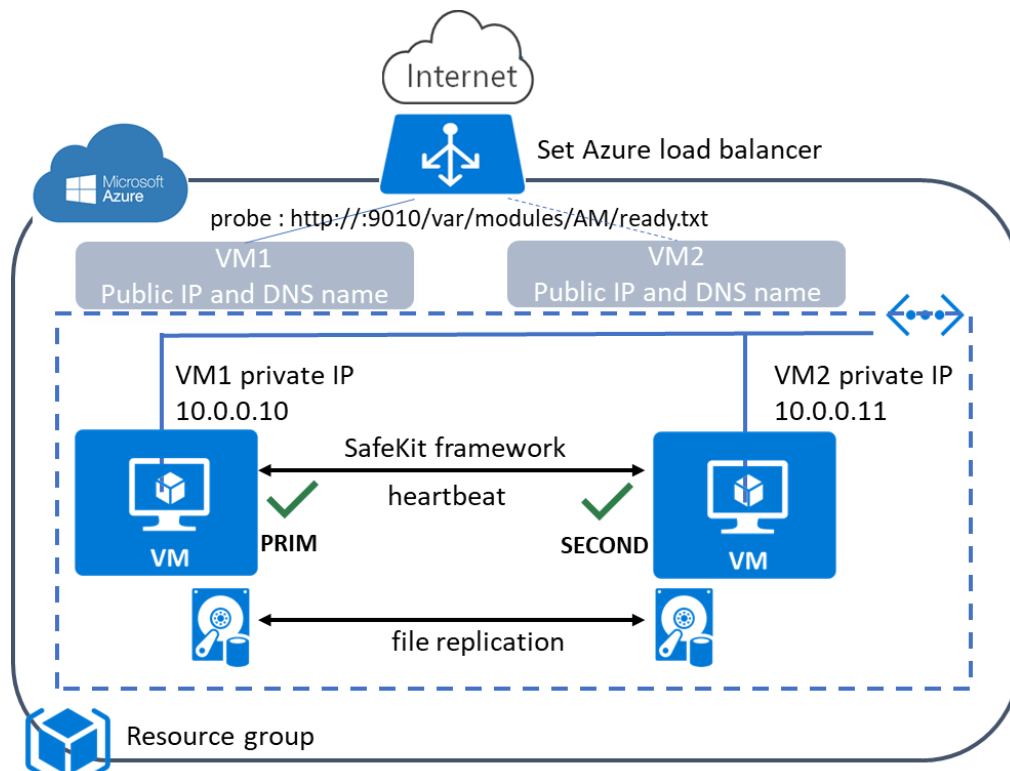
Enfin il faut saisir la configuration du cluster SafeKit et l'appliquer à tous les nœuds (voir [section 12](#)). Par exemple, le fichier de configuration du cluster SafeKit serait :

```
<cluster>
<lans>
  <lan name="default">
    <node name="Server1" addr="10.0.0.10"/>
    <node name="Server2" addr="10.0.0.11"/>
  </lan>
</lans>
</cluster>
```

Le lan `default` est utilisé pour les communications du framework SafeKit entre les nœuds du cluster.

### 16.2.1 Cluster miroir dans Azure

Les fonctionnalités du module miroir sont opérationnelles dans le cloud Azure (réplication de fichiers temps réel, reprise sur panne, détection de mort de processus, checkers, ...), excepté le basculement d'adresse IP virtuelle. A la place, vous pouvez configurer un module miroir sur le cluster et utiliser load balancer proposé par Azure (voir [Load Balancer dans Azure](#)) en le configurant de façon à diriger tout le trafic vers le nœud primaire. L'adresse IP associée au load balancer, jouent le rôle d'IP virtuelle.



Vous devez configurer vous-même le load balancer et le groupe de sécurité Azure.

Pour le load balancer, vous devez :

- spécifier les règles pour votre application
- définir dans le backend pool les nœuds du cluster SafeKit
- définir une sonde d'intégrité. Cette sonde permet de vérifier si l'instance est dans un état sain ou non

Le load balancer achemine le trafic uniquement vers les instances saines. Il reroute le trafic vers l'instance lorsque celle-ci a été restaurée dans un état sain.

SafeKit fournit une sonde d'intégrité pour chaque module. Vous devez configurer la sonde d'intégrité dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où `AM` est le nom du module

Pour un module miroir, le test retourne :

- OK, qui signifie l'instance est saine, quand le module est dans l'état  $\checkmark$  PRIM (Ready) OU  $\checkmark$  ALONE (Ready)
- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états

Le groupe de sécurité réseau doit au minimum être configuré pour autoriser les communications pour les protocoles et ports :

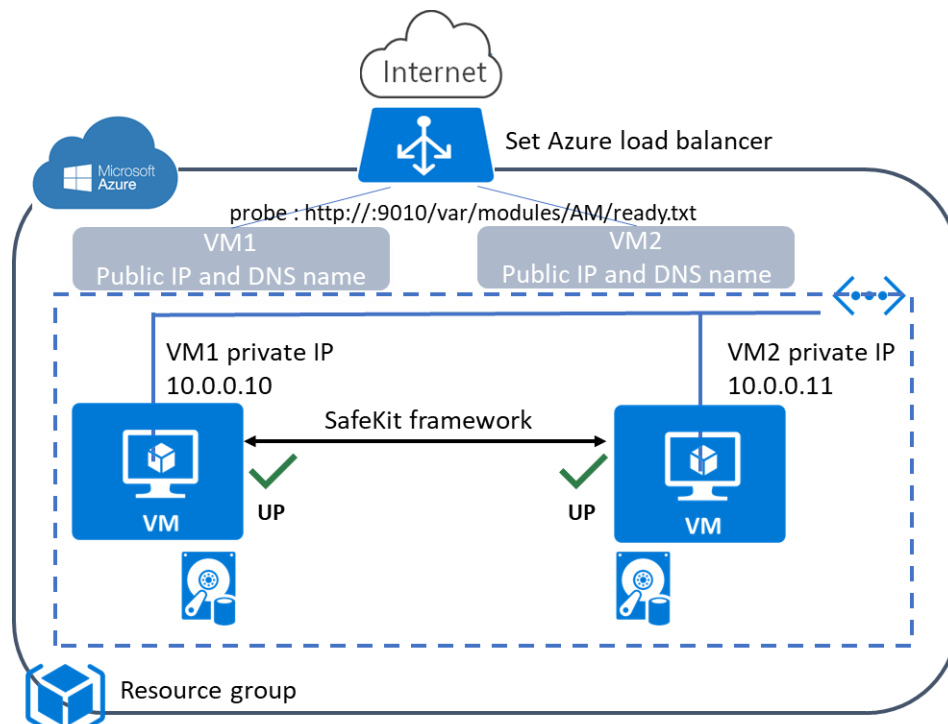
- UDP - 4800 pour le service `safeadmin` (entre les nœuds du cluster SafeKit)
- UDP - 8888 pour le heartbeat du module (entre les nœuds du cluster SafeKit)
- TCP - 5600 pour la réplication temps réel du module (entre les nœuds du cluster SafeKit)
- TCP - 9010 pour la console web SafeKit en HTTP
- TCP - 9453 pour la console web SafeKit en HTTPS
- TCP - 9001 pour configurer la console web SafeKit en HTTPS



Les valeurs de ports du module dépendent de son id (voir [section Erreur ! Source du renvoi introuvable.](#)). Les valeurs ci-dessus sont pour le premier module installé.

### 16.2.2 Cluster ferme dans Azure

La plupart des fonctionnalités du module ferme sont opérationnelles dans le cloud Azure (détection de mort de processus, checker, ...), à l'exception du partage de charge sur l'adresse IP virtuelle. A la place, vous pouvez configurer un module ferme sur le cluster et utiliser load balancer proposé par Azure (voir [Load Balancer dans Azure](#)). L'adresse IP associée au load balancer, jouent le rôle d'IP virtuelle.



Vous devez configurer vous-même le load balancer et le groupe de sécurité Azure. Pour le load balancer, vous devez :


- spécifier les règles pour votre application
- définir dans le backend pool les nœuds du cluster SafeKit
- définir une sonde d'intégrité. Cette sonde permet de vérifier si l'instance est dans un état sain ou non

Le load balancer achemine le trafic uniquement vers les instances saines. Il reroute le trafic vers l'instance lorsque celle-ci a été restaurée dans un état sain.

SafeKit fournit une sonde d'intégrité pour chaque module. Vous devez configurer la sonde d'intégrité dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où `AM` est le nom du module

Pour un module ferme, le test retourne :

- OK, qui signifie l'instance est saine, quand le module est dans l'état  UP (Ready)
- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états

Le groupe de sécurité doit au minimum être configuré pour autoriser les communications pour les protocoles et ports :

- UDP - 4800 pour le service `safeadmin` (entre les nœuds du cluster SafeKit)
- TCP - 9010 pour la console web SafeKit en HTTP  
TCP - 9453 pour la console web SafeKit en HTTPS
- TCP - 9001 pour configurer la console web SafeKit en HTTPS

### 16.3 Cluster SafeKit dans Google GCP

Dans la suite, nous supposons que vous êtes familiers avec Google Cloud Platform (GCP), fournisseur des machines virtuelles (VM) qui s'exécutent dans les centres de données innovants et sur le réseau de fibre optique mondial de Google. Pour plus d'informations sur ses fonctionnalités et son utilisation, voir la documentation [Google Cloud Computing](#).

Avant de pouvoir mettre en œuvre un module SafeKit, l'administrateur doit :

1. Créer des machines virtuelles (2 pour un module miroir)
2. Effectuer les paramétrages de Google Compute Engine (GCP), des machines virtuelles et de SafeKit
3. Enfin, appliquer des configurations SafeKit spécifiques en fonction du module que vous souhaitez mettre en œuvre.

#### Paramétrage de GCP

Il faut paramétrer le GCP pour :

- associer des adresses publiques (External IP), ou noms DNS, à chaque nœud si vous souhaitez les administrer avec la console web SafeKit depuis internet
- configurer les règles de pare-feu pour le réseau Virtual Private Cloud (VPC) pour ouvrir les communications du framework SafeKit et de la console web SafeKit. Les ports à ouvrir sont décrits en [section Erreur ! Source du renvoi introuvable.](#)
- utiliser un réseau à large bande passante et à faible latence si la réplication temps réel est utilisée dans un module miroir

### Paramétrage des instances

Sur chaque instance, il faut en plus :

- installer le package SafeKit
- appliquer la configuration HTTPS pour sécuriser la console Web SafeKit (voir [section 11](#))

### Paramétrage de SafeKit

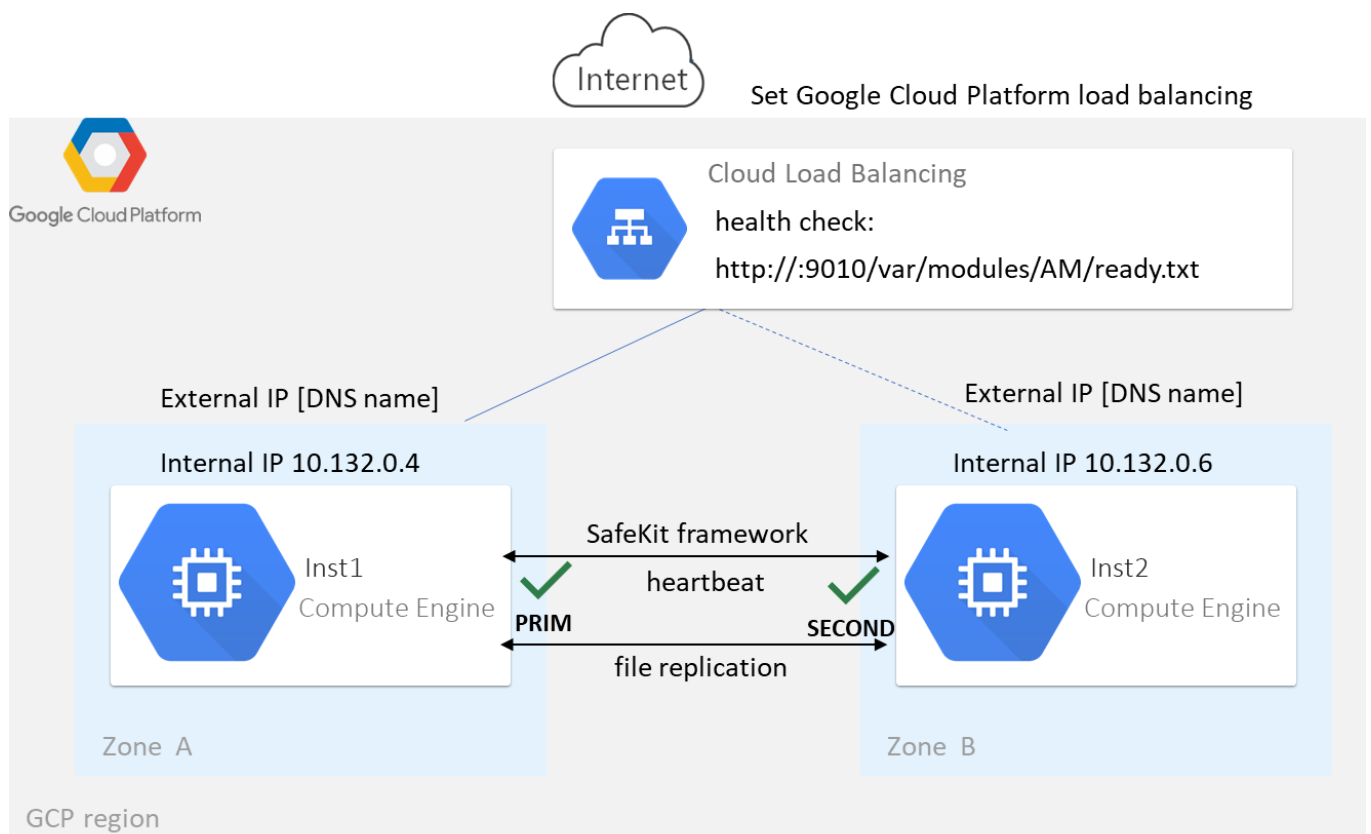
Enfin il faut saisir la configuration du cluster SafeKit et l'appliquer à tous les nœuds (voir [section 12](#)). Par exemple, le fichier de configuration du cluster SafeKit serait :

```
<cluster>
<lans>
  <lan name="default">
    <node name="Server1" addr="10.0.11.10"/>
    <node name="Server2" addr="10.0.12.10"/>
  </lan>
</lans>
</cluster>
```

Le lan `default` est utilisé pour les communications du framework SafeKit entre les nœuds du cluster.

#### 16.3.1 Cluster miroir dans GCP

Les fonctionnalités du module miroir sont opérationnelles dans GCP (réplication de fichiers temps réel, reprise sur panne, détection de mort de processus, checkers, ..) à l'exception du basculement d'adresse IP virtuelle. A la place, vous pouvez configurer un module miroir sur le cluster et utiliser le load balancing GCP (voir [Load Balancer de GCP](#)) en le configurant de façon à diriger tout le trafic vers le nœud primaire. L'adresse IP associée au load balancer, jouent le rôle d'IP virtuelle.



Si vous mettez en place le module miroir en dehors de la solution du Google Marketplace, vous devez configurer vous-même le load balancer et le pare-feu réseau de Google Cloud Platform.

Pour le load balancer, vous devez :

- spécifier les règles pour votre application
- définir comme cibles du trafic les nœuds du cluster SafeKit
- définir le test de vérification de l'état. Ce test permet de vérifier si l'instance est dans un état sain ou non

Le load balancer achemine le trafic uniquement vers les instances saines. Il reroute le trafic vers l'instance lorsque celle-ci a été restaurée dans un état sain.

SafeKit fournit un testeur de vérification de l'état pour chaque module. Vous devez configurer le test de vérification dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où `AM` est le nom du module

Pour un module miroir, le test retourne :

- OK, qui signifie l'instance est saine, quand le module est dans l'état `✓ PRIM (Ready)` ou `✓ ALONE (Ready)`

- NOT FOUND, qui signifie que l'instance est hors service, dans tous les autres états

Le pare-feu du réseau doit au minimum être configuré pour autoriser les communications pour les protocoles et ports :

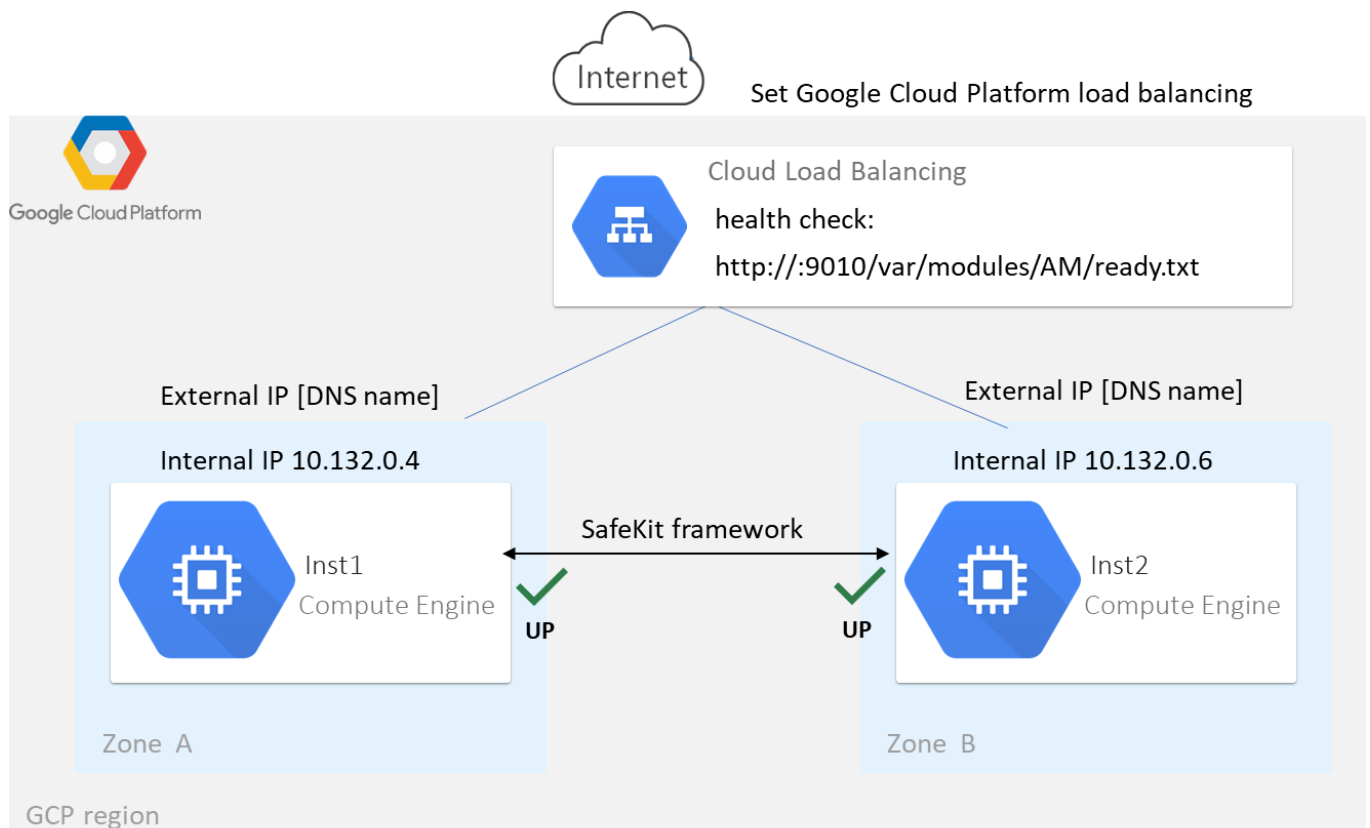
- UDP - 4800 pour le service `safeadmin` (entre les nœuds du cluster SafeKit)
- UDP - 8888 pour le heartbeat du module (entre les nœuds du cluster SafeKit)
- TCP - 5600 pour la réplication temps réel du module (entre les nœuds du cluster SafeKit)
- TCP - 9010 pour la console web SafeKit en HTTP  
TCP - 9453 pour la console web SafeKit en HTTPS
- TCP - 9001 pour configurer la console web SafeKit en HTTPS



Les valeurs de ports du module dépendent de son id (voir [section Erreur ! Source du renvoi introuvable.](#)). Les valeurs ci-dessus sont pour le premier module installé.

### 16.3.2 Cluster ferme dans GCP

La plupart des fonctionnalités du module ferme sont opérationnelles dans GCP (détection de mort de processus, checker, ...), à l'exception du partage de charge sur l'adresse IP virtuelle. A la place, vous pouvez configurer un module ferme sur le cluster et utiliser le load balancing GCP (voir [Load Balancer de GCP](#)). L'adresse IP associée au load balancer, joue le rôle d'IP virtuelle.



Si vous mettez en place le module ferme en dehors de la solution du Google Marketplace, vous devez configurer vous-même le load balancer et le pare-feu réseau de Google Cloud Platform.

Pour le load balancer, vous devez :


- spécifier les règles pour votre application
- définir comme cibles du trafic les nœuds du cluster SafeKit
- définir le test de `vérification de l'état`. Ce test permet de vérifier si l'instance est dans un état sain ou non

Le load balancer achemine le trafic uniquement vers les instances saines. Il reroute le trafic vers l'instance lorsque celle-ci a été restaurée dans un état sain.

SafeKit fournit un testeur de `vérification de l'état` pour chaque module. Vous devez configurer le test de vérification dans le load balancer avec :

- le protocole HTTP
- le port 9010, port du service web de SafeKit
- l'URL `/var/modules/AM/ready.txt` où `AM` est le nom du module

Pour un module ferme, le test retourne :

- `OK`, qui signifie l'instance est saine, quand le module est dans l'état  `UP (Ready)`
- `NOT FOUND`, qui signifie que l'instance est hors service, dans tous les autres états

Le pare-feu du réseau doit au minimum être configuré pour autoriser les communications pour les protocoles et ports :

- UDP - 4800 pour le service `safeadmin` (entre les nœuds du cluster SafeKit)
- TCP - 9010 pour la console web SafeKit en HTTP
- TCP - 9453 pour la console web SafeKit en HTTPS
- TCP - 9001 pour configurer la console web SafeKit en HTTPS

## 17. Logiciels tiers

SafeKit apporte les logiciels tiers listés ci-dessous. Pour les détails des licences, se référer aux liens indiqués ou aux fichiers de licence répertoriés sous `SAFE/licenses` (`SAFE=/opt/safekit` en Linux et `SAFE=C:\safekit` en Windows si `%SYSTEMDRIVE%=C:`).

libnet	<a href="#">Packet Construction and Injection</a> Libnet licence - <a href="#">license</a> Utilisé par arpreroute et ping
swagger-ui	<a href="https://github.com/swagger-api/swagger-ui">https://github.com/swagger-api/swagger-ui</a> Apache2 licence - <a href="https://github.com/swagger-api/swagger-ui/blob/master/LICENSE">https://github.com/swagger-api/swagger-ui/blob/master/LICENSE</a> Swagger UI is a collection of HTML, JavaScript, and CSS assets that dynamically generate beautiful documentation from a Swagger-compliant API Utilisé pour visualiser l'API SafeKit
Sqlite3	<a href="https://www.sqlite.org/about.html">https://www.sqlite.org/about.html</a> Public Domain licence - <a href="https://www.sqlite.org/copyright.html">https://www.sqlite.org/copyright.html</a> SQLite is an in-process library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine Utilisé par le framework SafeKit
Info-ZIP	<a href="https://infozip.sourceforge.net/">https://infozip.sourceforge.net/</a> BSD like licence - <a href="https://infozip.sourceforge.net/license.html">https://infozip.sourceforge.net/license.html</a> Utilisé pour les snapshots et .safe

Et uniquement en Windows :

jansson	<a href="https://github.com/akheron/jansson">https://github.com/akheron/jansson</a> MIT licence - <a href="https://github.com/akheron/jansson/blob/master/LICENSE">https://github.com/akheron/jansson/blob/master/LICENSE</a> Utilisé par le framework SafeKit
libxml	<a href="https://gitlab.gnome.org/GNOME/libxml2/-/wikis/home">https://gitlab.gnome.org/GNOME/libxml2/-/wikis/home</a> MIT licence - <a href="https://gitlab.gnome.org/GNOME/libxml2/-/wikis/FAQ">https://gitlab.gnome.org/GNOME/libxml2/-/wikis/FAQ</a> Utilisé par le framework SafeKit
libxslt	<a href="https://gitlab.gnome.org/GNOME/libxslt/-/wikis/home">https://gitlab.gnome.org/GNOME/libxslt/-/wikis/home</a> MIT licence - <a href="https://gitlab.gnome.org/GNOME/libxslt/blob/master/Copyright">https://gitlab.gnome.org/GNOME/libxslt/blob/master/Copyright</a> Utilisé par le framework SafeKit
Net-SNMP	<a href="https://net-snmp.sourceforge.io/">https://net-snmp.sourceforge.io/</a>

	<p>BSD like licence - <a href="https://www.net-snmp.org/about/license.html">https://www.net-snmp.org/about/license.html</a> Utilisé par l'agent SNMP en Windows</p>
HTTP server	<p><a href="https://httpd.apache.org/">https://httpd.apache.org/</a> Apache licence - <a href="https://www.apache.org/licenses/LICENSE-2.0">https://www.apache.org/licenses/LICENSE-2.0</a> Utilisé par le service web SafeKit pour la console web, les commandes distribuées et le module checker</p>
APR	<p><a href="https://apr.apache.org/">https://apr.apache.org/</a> Apache licence - <a href="https://www.apache.org/licenses/LICENSE-2.0">https://www.apache.org/licenses/LICENSE-2.0</a> Utilisé par le serveur HTTP Apache</p>
PCRE	<p><a href="http://www.pcre.org/">http://www.pcre.org/</a> BSD license - <a href="https://www.pcre.org/licence.txt">https://www.pcre.org/licence.txt</a> Utilisé par le serveur HTTP Apache</p>
PCR2	<p><a href="https://www.pcre.org/">https://www.pcre.org/</a> BSD-3-Clause WITH PCRE2-exception - <a href="https://pcre2project.github.io/pcre2/project/licence">https://pcre2project.github.io/pcre2/project/licence</a> Utilisé pour l'anonymisation des snapshots et journaux</p>
libexpat	<p><a href="https://github.com/libexpat/libexpat">https://github.com/libexpat/libexpat</a> BSD license <a href="https://github.com/libexpat/libexpat/blob/master/expat/COPYING">https://github.com/libexpat/libexpat/blob/master/expat/COPYING</a> Utilisé par le serveur HTTP Apache</p>
mod_auth_oxidc	<p><a href="https://github.com/OpenIDC/mod_auth_oxidc">https://github.com/OpenIDC/mod_auth_oxidc</a> Apache2 licence - <a href="https://github.com/OpenIDC/mod_auth_oxidc/blob/master/LICENSE.txt">https://github.com/OpenIDC/mod_auth_oxidc/blob/master/LICENSE.txt</a> Utilisé par le serveur HTTP Apache</p>
cURL	<p><a href="https://curl.se/">https://curl.se/</a> Curl licence - <a href="https://curl.se/docs/copyright.html">https://curl.se/docs/copyright.html</a> Utilisé par les commandes distribuées et le module checker</p>
OpenSSL	<p><a href="https://www.openssl.org/">https://www.openssl.org/</a> dual OpenSSL and SSLeay licence - <a href="https://openssl-library.org/source/license/index.html">https://openssl-library.org/source/license/index.html</a> Utilisé pour sécuriser la console web, les commandes distribuées et le module checker</p>
Lua	<p><a href="https://www.lua.org/">https://www.lua.org/</a> MIT licence - <a href="https://www.lua.org/license.html">https://www.lua.org/license.html</a></p>

	Utilisé par le framework et service web SafeKit
getopt.c	BSD License. Used to parse command arguments
oncw32	SUN RPC License. Used to transport NFS rpc

SafeKit utilise les logiciels tiers suivants pour la console Web :

Angular	<p><a href="https://angular.dev/">https://angular.dev/</a> MIT licence - <a href="https://github.com/angular/angular-cli/blob/main/LICENSE">https://github.com/angular/angular-cli/blob/main/LICENSE</a></p> <p>Angular is an application-design framework and development platform for creating efficient and sophisticated single-section apps.</p> <p>@angular/material, @angular/animations, @angular/platform-browser, @angular/service-worker, @angular/cdk, @angular/forms, @angular/core, @angular/common, @angular/router,</p>
jszip	<p><a href="https://stuk.github.io/jszip/">https://stuk.github.io/jszip/</a> MIT OR GPL-3.0-or-later licence - <a href="https://github.com/Stuk/jszip/blob/main/LICENSE.markdown">https://github.com/Stuk/jszip/blob/main/LICENSE.markdown</a></p> <p>A library for creating, reading, and editing .zip files with JavaScript, with a lovely and simple API.</p>
rxjs	<p><a href="https://github.com/ReactiveX/rxjs">https://github.com/ReactiveX/rxjs</a> Apache2 licence - <a href="https://github.com/ReactiveX/rxjs/blob/master/LICENSE.txt">https://github.com/ReactiveX/rxjs/blob/master/LICENSE.txt</a></p> <p>Reactive Extensions For JavaScript</p>
tslib	<p><a href="https://www.typescriptlang.org/">https://www.typescriptlang.org/</a> OBSD Copyright (c) Microsoft Corporation Runtime library for typescript</p>
vlq	<p><a href="https://github.com/Rich-Harris/vlq/blob/master/README.md">https://github.com/Rich-Harris/vlq/blob/master/README.md</a> MIT licence - <a href="https://github.com/Rich-Harris/vlq/blob/master/LICENSE">https://github.com/Rich-Harris/vlq/blob/master/LICENSE</a></p> <p>Convert integers to a Base64-encoded VLQ string, and vice versa</p>
ngx-logger	<p><a href="https://github.com/dbfannin/ngx-logger">https://github.com/dbfannin/ngx-logger</a> MIT licence - <a href="https://github.com/dbfannin/ngx-logger?tab=MIT-1-ov-file">https://github.com/dbfannin/ngx-logger?tab=MIT-1-ov-file</a></p> <p>NGX Logger is a simple logging module for angular</p>
zone.js	<p><a href="https://github.com/angular/zone.js">https://github.com/angular/zone.js</a> MIT licence - <a href="https://github.com/angular/zone.js/blob/master/LICENSE">https://github.com/angular/zone.js/blob/master/LICENSE</a></p> <p>Implements Zones for JavaScript</p>

material- icons	<a href="https://github.com/marella/material-icons">https://github.com/marella/material-icons</a> Apache-2.0 licence - <a href="https://github.com/marella/material-icons/blob/main/LICENSE">https://github.com/marella/material- icons/blob/main/LICENSE</a>
--------------------	--

Cette liste est aussi disponible à l'emplacement suivant :  
`safekit/web/htdocs/console/3rdpartylicenses.txt`.

## Index des messages du journal du module

---

### "Action ..."

- "Action forcestop called by admin@<IP>/SYSTEM/root", 127, 158
- "Action prim called by admin@<IP>/SYSTEM/root", 109, 158
- "Action primforce called by SYSTEM/root", 116, 158
- "Action restart called by admin@<IP>/SYSTEM/root", 127, 86, 91, 158
- "Action restart|stopstart called by errd", 97, 131, 158
- "Action restart|stopstart called by c\_id", 104, 131, 158
- "Action restart|stopstart from failover rule t\_id", 98, 131, 158
- "Action second called by admin@<IP>/SYSTEM/root", 109, 158
- "Action shutdown called by SYSTEM", 88, 96, 158
- "Action start called at boot time", 88, 89, 96, 97, 158
- "Action start called automatically", 97, 98, 104
- "Action start called by admin@<IP>/SYSTEM/root", 85, 85, 91, 127, 158
- "Action stop called by admin@<IP>/SYSTEM/root", 85, 91, 127, 158
- "Action stop called by maxloop", 132, 97, 98, 99, 100, 101, 102, 103, 104, 131
- "Action stopstart called by failover-off", 114, 167
- "Action stopstart called by modulecheck", 102, 158
- "Action stopstart called by admin@<IP>/SYSTEM/root", 127, 158
- "Action stopstart from failover rule c\_id", 104, 131, 158
- "Action wait from failover rule c\_id", 103, 130
- "Action wait from failover rule t\_id", 99, 130
- "Action wait from failover rule degraded\_server", 113
- "Action wait from failover rule interface\_failure", 100, 130
- "Action wait from failover rule module\_failure", 102, 130
- "Action wait from failover rule notuptodate\_server", 112, 130
- "Action wait from failover rule p\_id", 101, 130
- "Action wait from failover rule splitbrain\_failure", 130
- "Action alone called by heart: no heartbeat", 88
- "Action alone called by heart: remote stop", 85

---

### Réplication et réintégration

- "Copied <reintegration statistics>", 87
- "Data may be inconsistent for replicated directories (stopped during reintegration)", 116
- "Data may not be uptodate for replicated directories (wait for the start of the remote server)", 109, 112, 130

"If you are sure that this server has valid data, run safekit prim to force start as primary", 109, 112, 130

"If you are sure that this server has valid data, run safekit primforce to force start as primary", 116

"Reintegration ended (synchronize)", 87

"Updating directory tree from /replicated", 87

---

### Load-balancing

"farm load: 128/256 (group FarmProto\_0)" , 120, 93, 94

"farm membership: node1 (group FarmProto\_0)", 93, 94

"farm membership: node1 node2 (group FarmProto\_0)" , 120, 93, 94

"farm membership: node2 (group FarmProto\_0)", 94

---

### "Local state ..."

"Local state ALONE Ready", 109, 85, 89

"Local state PRIM Ready", 109,85

"Local state SECOND Ready",109, 85

"Local state UP Ready",120 ,120

"Local state WAIT NotReady", 130, 114

---

### "Remote state ..."

"Remote state ALONE Ready", 109,89

"Remote state PRIM Ready", 109, 85

"Remote state SECOND Ready",109, 85

"Remote state UNKNOWN Unknown", 88, 89

---

### "Resource ..."

"Resource custom.id set to down by customscript", 103, 104, 130, 131

"Resource custom.id set to up by customscript", 103

"Resource heartbeat.0 set to down by heart", 88, 89

"Resource heartbeat.flow set to down by heart", 88, 89

"Resource intf.ip.0 set to down by intfcheck", 100, 130

"Resource intf.ip.0 set to up by intfcheck", 100

"Resource module.othermodule\_ip set to down by modulecheck", 102, 130

"Resource module.othermodule\_ip set to up by modulecheck", 102

"Resource ping.id set to down by pingcheck", 101, 130

"Resource ping.id set to up by pingcheck", 101

"Resource rfs.degraded set to up by nfsadmin", 113  
"Resource tcp.id set to down by tcpcheck", 98, 99, 130, 131  
"Resource tcp.id set to up by tcpcheck", 99

---

### "Script ..."

"Script start\_prim", 317, 85, 86, 88, 88  
"Script stop\_prim", 317, 85, 88, 89  
"Script start\_both", 317, 91, 96  
"Script stop\_both", 317, 91

---

### "Transition ..."

"Transition RESTART|STOPSTART from failover rule customid\_failure", 104  
"Transition STOPSTART from failover-off", 114  
"Transition SWAP from defaultprim", 115  
"Transition WAIT\_TR from failover rule customid\_failure", 103  
"Transition WAIT\_TR from failover rule interface\_failure", 100  
"Action wakeup from failover rule Implicit\_wakeup", 99, 100, 101, 102, 103

---

### Autres messages

"Process appli.exe not running", "Service mySQL not running", 97, 131  
"Failover-off configured", 114  
"Requested prim start aborted ", 116  
"Split brain recovery: exiting alone", 89  
"Split brain recovery: staying alone", 89  
"Virtual IP <ip 1.10 of mirror> set", 86  
"Virtual IP <virtip of farm> set", 91



## **Index**

---

### **Architectures**

miroir, ferme... - 17  
cloud - 365

---

### **Installation**

installation, upgrade... - 31

---

### **Console**

configuration, supervision - 47  
sécurisation (https,...) - 207

---

### **Configuration avancée**

cluster.xml - 235  
userconfig.xml - 241  
scripts du module - 317  
exemples - 327

---

### **Administration**

mirror - 107  
farm - 119  
avancée - 175  
ligne de commande -153

---

### **Support**

tests - 81  
problèmes - 123  
support SafeKit - 151  
messages du journal - 381

---

### **Autres**

table des matières - 5  
logiciels tiers - 377

