Modèle shinken

Sommaire

Contexte

Les tentatives d'intrusion pour corruption ou vol de données ne doivent pas être sous-estimées dans le cadre de votre supervision de vos postes et serveurs Linux. Ce check a donc été conçu pour vous permettre de garder le maximum de vigilance sur les échecs de connexion sur votre parc.

Le check **Connection Failed by SNMPv1v2** va vérifier vos logs dans un laps de temps donné (*24h par défaut, modifiable dans les données*) et vous donner le nombre total de tentatives de connexions échouées, et un tableau comportant une ligne par trio IP-Host-Interface (*dans le cas d'une connexion réseau*) ou couple Host-Interface (*dans le cas d'une connexion locale sans adresse IP*).

- Vous obtiendrez alors le nombre de tentatives au cas par cas, la date de la première et de la dernière tentative, et les informations précédemment énoncées.
    - Le tableau est classé par le nombre total de tentatives de connexion pour le trio IP-Host-Interface ou Host-Interface.
- Deux seuils configurables permettent de déterminer quand le check passe en **ATTENTION**, puis en **CRITIQUE**.

Le check ne supporte pas certaines distributions, où la commande 'lastb' n'est plus disponible :

- >= Debian 12
- >= Ubuntu 22
- >= FreeBSD 13
- >= OpenSuse 13

Un status **INCONNU** sera renvoyé si le check ne peut pas s'exécuter.

? Unknown Attachment

Paramétrage

Le check utilise la ligne de commande suivante :

```
$LINUX-BY-SNMP__SHINKEN__PLUGINSDIR$/check_linux_health_by_snmp_rust --check check_connection_failed
    -H "$HOSTADDRESS$"
    -p "$_HOSTLINUX-BY-SNMP__PORT$"
    -t "$_HOSTLINUX-BY-SNMP__TIMEOUT$"
    -w "$_HOSTLINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-WARN$"
    -c "$_HOSTLINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-CRIT$"
    -i "$_HOSTLINUX-BY-SNMP__CONNECTION-FAILED__INTERFACES$"
    -n "$_HOSTLINUX-BY-SNMP__CONNECTION-FAILED__TIME-LIMIT$"
    --snmp_version "2"
    --community "$_HOSTLINUX-BY-SNMP__V1V2-COMMUNITY$"
```

Données utilisées provenant des modèles

Données communes pour les checks des modèles

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation de Shinken	Description

LINUX-BY-SNMP__TIMEOUT	l'Hôte *(Onglet Données)*	seconde	5	**5**	Temps maximal en seconde pour réussir une connexion SNMP avant que le check ne renvoi une erreur ***INCONNU*** *(La valeur doit être comprise entre 2 et 60).*
LINUX-BY-SNMP__PORT	l'Hôte *(Onglet Données)*	---	161	**161**	Port pour la connexion SNMP.

LINUX-BY-SNMP__V1V2-COMMUNITY	l'Hôte *(Onglet Données)*	---	public	**public**	La Communauté SNMP v1/v2 défini sur votre linux : • En SNMP v1/v2, la communauté est un équivalent à un ID ou à un mot de passe pour se connecter aux équipements.
LINUX-BY-SNMP__V1V2-VERSION	l'Hôte *(Onglet Données)*	---	2	**2**	Sélectionne la version SNMP 1 ou 2 à utiliser.

Données spécifiques pour ce check

Nom	Modifiable sur	Unité	Valeur par défaut	Description
LINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-WARN	l'Hôte *(Onglet Données)*	-	*5*	Définit le nombre de connexions échouées à partir duquel le check passe en **ATTENTION**.
LINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-CRIT	l'Hôte *(Onglet Données)*	-	*10*	Définit le nombre de connexions échouées à partir duquel le check passe en **CRITIQUE**.
LINUX-BY-SNMP__CONNECTION-FAILED__TIME-LIMIT	l'Hôte *(Onglet Données)*	heures	*24*	Les **X dernières heures** de logs lus pour identifier les connexions échouées.
LINUX-BY-SNMP__CONNECTION-FAILED__INTERFACES	l'Hôte *(Onglet Données)*	-	*ssh,tty*	Filtres des interfaces de connexion à prendre en compte dans le check, séparées par des virgules. Les interfaces prisent en compte doivent commencer par au moins un des filtres de cette liste. Exemples : ▪ 'ssh' prendra en compte 'ssh:notty' ▪ 'tty' ne prendra pas en compte 'ssh:notty' ▪ 'tty' prendra en compte 'tty/0' La valeur **ALL** peut être utilisé afin de prendre en compte toutes les interfaces.

Données DFE (Duplicate Foreach)

Pas de données DFE pour ce check

Données utilisées provenant du check

Pas de données provenant du check pour ce modèle

Données globales

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation	Description
`USERPLUGINSDIR`	Non modifiable *(Sauf Admin Shinken)*	--	/var/lib/shinken/libexec	**/var/lib/shinken/libexec**	Chemin absolu contenant les sondes installés par Shinken
`LINUX-BY-SNMP__SHINKEN__VENDOR`	Non modifiable *(Sauf Admin Shinken)*	--	shinken-additional-packs	**shinken-additional-packs**	Dossier fournit par shinken
`LINUX-BY-SNMP__SHINKEN__PACKNAME`	Non modifiable *(Sauf Admin Shinken)*		linux-by-SNMP__shinken	**linux-by-SNMP__shinken**	Dossier contenant les sondes
`LINUX-BY-SNMP__SHINKEN__PLUGINSDIR`	Non modifiable *(Sauf Admin Shinken)*	--	`USERPLUGINSDIR /LINUX-BY-SNMP__SHINKEN__VENDOR/ LINUX-BY-SNMP__SHINKEN__PACKNAME`	**/var/lib/shinken-user/libexec /shinken-additional-packs/linux-by-SNMP__shinken**	Chemin absolu du dossier contenant les sondes du pack **linux-by-SNMP__shinken** (*non modifiable*)

Propriétés de l'hôte

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut	Description
`HOSTADDRESS`	l'Hôte *(Onglet Général)*	--	Nom de l'hôte	**Nom de l'hôte**	Adresse de l'hôte

Résultat

Exemple

? Unknown Attachment

Interprétation des données

Statut

- Il peut prendre 4 valeurs ***OK*** / ***CRITIQUE*** / ***ATTENTION*** / ***INCONNU*** .
    - Le statut va dépendre du retour de sonde et de la configuration spécifique du check pour les données suivantes :
        - **LINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-WARN**
        - **LINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-CRIT**
    - Voici un tableau récapitulatif du statut attendu suivant le retour de sonde :

la colonne "Affichage des seuils" montre les paramètres utilisés et leur valeur définie sur l'équipement supervisé.

? Unknown Attachment

Situation	Statut	Exemple
• Les nombre de tentatives de connections échoués est supérieur ou égal à **LINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-CRIT**	CRITIQUE	? Unknown Attachment
• Les nombre de tentatives de connections échoués est supérieur ou égal à **LINUX-BY-SNMP__CONNECTION-FAILED__CONNECTION-WARN**	ATTENTION	? Unknown Attachment

Résultat

Le résultat contient un message indiquant le nombre de tentatives de connexions échoués et le status de la sonde.

Résultat long

Le résultat long contient un tableau affichant l'ensemble des tentatives de connexions échoués par :

- IP
- nom d'utilisateur
- Nombre de tentatives
- Date de dernière connexion
- Date de première connexion

Métriques

Nom de la métrique	Description
total	Nombre de connexions échouées

Erreurs et pré-requis

Erreurs de configuration de l'hôte à superviser (spécifique à ce check)

The command 'lastb' is not found. This check may not work with your Linux distribution.
Le check va exécuter à distance la commande '*lastb*' mais qui n'est pas disponible sur votre machine.

? Unknown Attachment

Les commandes 'lastb' et 'last' permettent de récupérer les dernières connexions réussies et échouées à une machine.
Ces commandes sont fournies par le paquet 'util-linux', installé par défaut sur la plupart des distributions Linux.
Cependant, sur certaines distributions récentes, 'lastb' n'est plus distribué et 'last' a été remplacé par une implémentation d'un nouveau paquet : 'wtmpdb'.
Alors le check ne supporte pas la supervision des hôtes aillants les distributions suivantes :

- >= Debian 12
- >= Ubuntu 22
- >= FreeBSD 13
- >= OpenSuse 13

Permission denied: SNMP daemon (snmpd) cannot access /var/log/btmp using 'lastb' command.
Le check va exécuter à distance la commande '*lastb*' qui nécessite les droits de lecture sur le fichier '*/var/log/btmp*'.

? Unknown Attachment

RESOLUTION :
RHEL / Alma / Rocky
Cette erreur est très fréquemment générée par le module de sécurité SELinux.
Vous pouvez vérifier si SELinux est activé avec la commande :

```
sestatus
```

Vous devriez observer parmi le résultat les ligne suivante :

```
SELinux status:                 enabled
Current mode:                   enforcing
```

Si SELinux est bien activé et en mode 'enforcing', vous pouvez alors rajouter des règles afin de permettre au service SNMP (*snmpd*) à accéder aux fichiers voulus.
Si un autre module de sécurité est installé sur votre hôte distante, il faudra le configurer de façon similaire.

RÉSOLUTION PAR SCRIPT :

Dans le script de configuration d'hôte livré dans le pack, une option permet de rajouter ces règles.
Déployez le dossier '*supervised-host*' sur votre hôte (*scp, ftp ...*).
Sur l'hôte distante, exécutez :

```
cd supervised-host
./configure-host.sh --configure-selinux
```

RÉSOLUTION MANUELLE :

Sur l'hôte distante, exécutez les commandes suivantes :

```
mkdir -p /etc/selinux/shinken
vim /etc/selinux/shinken/linux-by-SNMP__shinken.te
```

Dans le fichier, remplissez et sauvegardez :

```
module linux-by-SNMP__shinken 1.0;
require {
    type snmpd_t;
    type sysctl_rpc_t;
    type faillog_t;
    class file { read open getattr };
    class dir { search };
}
# Rules for check Stats NFS by SNMPvXXX
# Allow snmpd to read /proc/net/rpc/nfsd
allow snmpd_t sysctl_rpc_t:file { read open getattr };
# Autorisation pour accéder au dossier /proc/net/rpc
allow snmpd_t sysctl_rpc_t:dir { search };

# Rules for check Connection Failed by SNMPvXXX
# Allow snmpd to read /var/log/btmp
allow snmpd_t faillog_t:file { read open getattr };
```

Puis exécutez :

```
checkmodule -M -m -o "/etc/selinux/shinken/linux-by-SNMP__shinken.mod" "/etc/selinux/shinken/linux-by-
SNMP__shinken.te"
semodule_package -o "/etc/selinux/shinken/linux-by-SNMP__shinken.pp" -m "/etc/selinux/shinken/linux-by-
SNMP__shinken.mod"
semodule -i "/etc/selinux/shinken/linux-by-SNMP__shinken.pp"
```

Ces commandes vont compiler, empaqueter et installer le module SELinux créé.

Debian

Sur Debian, un utilisateur est créé spécifiquement pour le serveur snmpd de l'hôte supervisé : "Debian-snmp".

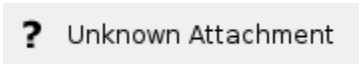
- Il suffit de lui ajouter les droits nécessaires en l'ajoutant dans le groupe "utmp", qui a accès aux fichiers demandés.

RÉSOLUTION MANUELLE :

```
usermod -a -G utmp Debian-snmp
service snmpd restart
```

SNMP agent is not configured with extended exec 'shinken__linux-by-snmp__connection-failed__lastb'

Le check demande une configuration supplémentaire afin d'exécuter des commandes via des requêtes SNMP. Sans cette configuration, l'erreur suivante sera générée :



RESOLUTION :
Ouvrez le fichier de configuration SNMP. ("**/etc/snmp/shinken/linux-by-SNMP__shinken.conf**" ou "**/etc/snmp/snmpd.conf**" selon votre configuration).

```
vim /etc/snmp/shinken/linux-by-SNMP__shinken.conf
# vim /etc/snmp/snmpd.conf
```

Rajoutez cette ligne si elle n'y est pas :

```
extend shinken__linux-by-snmp__connection-failed__lastb /bin/sh -c "export LC_LANG=C && unset LANG && lastb -F -w"
```

Il faudra ensuite redémarrer le serveur SNMP (snmpd)

```
service snmpd restart
# Ou bien en utilisant systemctl
systemctl restart snmpd
```

Erreurs de connexion (communes à tous les checks)

UNKNOWN – Session error: timeout

La connexion SNMP est configuré par défaut pour se couper si aucune réponse n'est perçu après cinq secondes (*paramétrable avec LINUX-BY-SNMP__TIMEOUT*).

Statut	Nom de check	Résultat	Résultat Long
?	Disks Usage by SNMPv1v2	UNKNOWN Session error: timeout	-

Cette erreur peut intervenir lorsque :

- Aucun accès réseau n'est disponible vers l'hôte.
- En SNMP v1 ou v2, la communauté utilisée est incorrecte.
- En SNMP v3, la clef privée (*LINUX-BY-SNMP__V3-PASSPHRASE-PRIV*) utilisée est incorrecte.

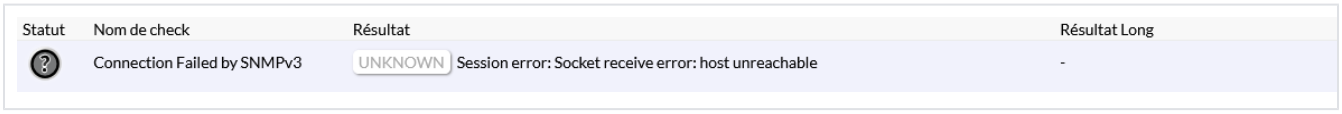
UNKNOWN – Failed to create SNMP session. Got error: failed to lookup address information: Name or service not known

La résolution DNS de l'hôte a échoué.

Statut	Nom de check	Résultat	Résultat Long
?	Disks Usage by SNMPv3	UNKNOWN Failed to create SNMP session. Got error: failed to lookup address information: Name or service not known	-

UNKNOWN – Session error: Socket receive error: host unreachable

La tentative de connexion à l'hôte a échoué à atteindre l'hôte.



Statut	Nom de check	Résultat	Résultat Long
	Connection Failed by SNMPv3	UNKNOWN Session error: Socket receive error: host unreachable	-

Cette erreur peut être générée à cause d'une mauvaise configuration de pare-feu.

UNKNOWN – Session error: Socket receive error: connection refused

La tentative de connexion à l'hôte a été refusé.

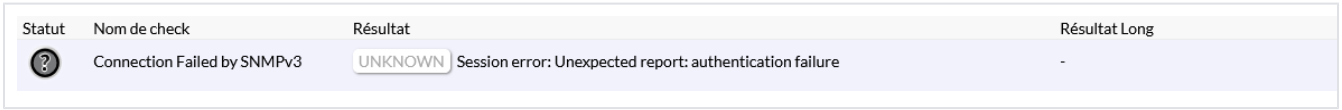
Statut	Nom de check	Résultat	Résultat Long
	Connection Failed by SNMPv3	UNKNOWN Error initializing v3 session: Session error: Socket receive error: connection refused	-

Cette erreur peut intervenir lorsque :

- Un pare-feu bloque la requête
- Le service SNMP du serveur à supervisé n'est pas démarré.

UNKNOWN – Session error: Unexpected report: authentication failure

L'authentification SNMP v3 a échoué.



Statut	Nom de check	Résultat	Résultat Long
	Connection Failed by SNMPv3	UNKNOWN Session error: Unexpected report: authentication failure	-

Cette erreur peut intervenir lorsque :

- En SNMP v3, le mot de passe (*LINUX-BY-SNMP__V3-PASSPHRASE-AUTH*) utilisée est incorrecte.
- En SNMP v3, la méthode de hachage (*LINUX-BY-SNMP__V3-PROTOCOL-AUTH*) utilisée est incorrecte.

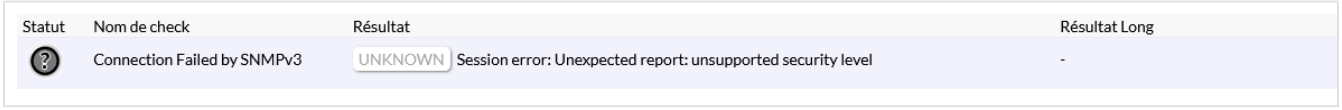
UNKNOWN – Session error: Unexpected report: unknown user name

L'utilisateur SNMP v3 utilisé n'existe pas.

Statut	Nom de check	Résultat	Résultat Long
	Connection Failed by SNMPv3	UNKNOWN Session error: Unexpected report: unknown user name	-

UNKNOWN – Session error: Unexpected report: unsupported security level.

L'authentification SNMP v3 a échoué. La méthode d'authentification n'est pas authorisé.



Statut	Nom de check	Résultat	Résultat Long
	Connection Failed by SNMPv3	UNKNOWN Session error: Unexpected report: unsupported security level	-

Cette erreur peut intervenir lorsque :

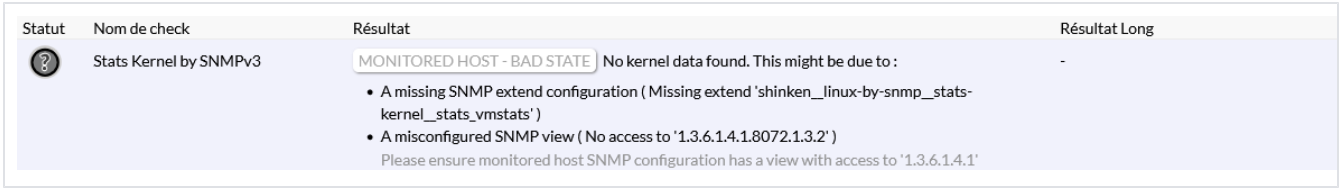
Erreurs de configuration de l'hôte à superviser (communes à tous les checks)

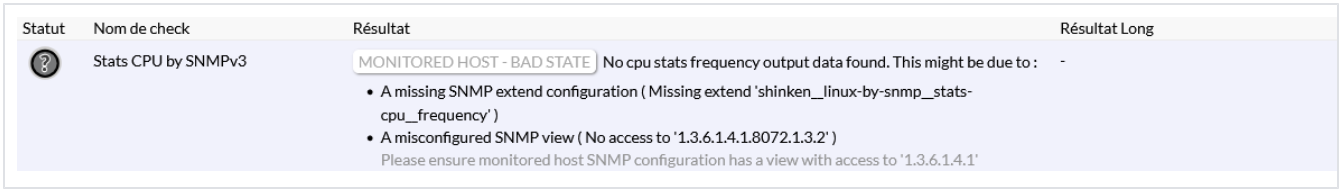
Les erreurs suivantes peuvent arriver sur la version SNMPv2 et SNMPv3.

MONITORED HOST - BAD STATE – No [...] data found. This might be due to :

Deux erreurs sont possibles :

- La vue SNMP configuré n'a pas les droits suffisants.
- La configuration SNMP n'inclus pas les options "extend" nécessaires au bon fonctionnement des checks.





RESOLUTION :

Il faut vérifier les deux étapes suivantes de la configuration :

- Autorisations d'accès aux données
- Configuration nécessaire aux checks