Page d'authentification

Sommaire

Accéder à l'interface
S'identifier dans Shinken Entreprise

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 SNMPv3** 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**.

? Unknown Attachment

Paramétrage

Le check utilise une des lignes de commandes suivantes selon le modèle d'hôte utilisé :

Commande noAuthNoPriv

```
$LINUX-BY-SNMP__SHINKEN__PLUGINSDIR$/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 "3"
    --user "$_HOSTLINUX-BY-SNMP__V3-LOGIN$"
    --level "noAuthNoPriv"
```

Commande authNoPriv

```
$LINUX-BY-SNMP__SHINKEN__PLUGINSDIR$/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 "3"
    --user "$_HOSTLINUX-BY-SNMP__V3-LOGIN$"
    --auth_password "$_HOSTLINUX-BY-SNMP__V3-PASSPHRASE-AUTH$"
    --auth_protocol "$_HOSTLINUX-BY-SNMP__V3-PROTOCOL-AUTH$"
    --level "authNoPriv"
```

Commande authPriv

```
$LINUX-BY-SNMP__SHINKEN__PLUGINSDIR$/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 "3"
    --user "$_HOSTLINUX-BY-SNMP__V3-LOGIN$"
    --auth_password "$_HOSTLINUX-BY-SNMP__V3-PASSPHRASE-AUTH$"
    --priv_passphrase "$_HOSTLINUX-BY-SNMP__V3-PASSPHRASE-PRIV$"
    --auth_protocol "$_HOSTLINUX-BY-SNMP__V3-PROTOCOL-AUTH$"
    --priv_protocol "$_HOSTLINUX-BY-SNMP__V3-PROTOCOL-PRIV$"
    --level "authPriv"
```

Données utilisées provenant des modèles

Données communes pour les checks des modèles

Commun à tout les modes de connexion

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__V3-LOGIN	l'Hôte *(Onglet Données)*	--	**shinken**	**shinken**	Un nom d'utilisateur SNMPv3 défini sur votre linux : • Un nom unique qui identifie l'utilisateur SNMPv3

Mode de connexion noAuthNoPriv

Pas de données communes supplémentaires pour ce type de connexion SNMPv3

Mode de connexion authNoPriv

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

LINUX-BY-SNMP__V3-PROTOCOL-AUTH	l'Hôte *(Onglet Données)*	--	sha	**sha**	Protocole utilisé pour vérifier l'authenticité des messages SNMPv3
LINUX-BY-SNMP__V3-PASSPHRASE-AUTH	l'Hôte *(Onglet Données)*	--	shinkenpassword	**shinkenpassword**	Chaîne secrète utilisée pour vérifier l'authenticité des messages SNMPv3

Mode de connexion authPriv

Nom	Modifiable sur	Unité	Défaut	Valeur par défaut à l'installation	Description	
LINUX-BY-SNMP__V3-PROTOCOL-AUTH	l'Hôte *(Onglet Données)*	--	sha	**sha**	Protocole utilisé pour vérifier l'authenticité des messages SNMPv3. Valeurs possibles : **sha**, **md5**	
LINUX-BY-SNMP__V3-PASSPHRASE-AUTH	l'Hôte *(Onglet Données)*	--	shinkenpassword	**shinkenpassword**	Chaîne secrète utilisée pour vérifier l'authenticité des messages SNMPv3.	
LINUX-BY-SNMP__V3-PROTOCOL-PRIV	l'Hôte *(Onglet Données)*	--	aes	**aes**	Protocole utilisé pour chiffrer les données SNMPv3. Valeurs possibles : **aes**	
LINUX-BY-SNMP__V3-PASSPHRASE-PRIV	l'Hôte *(Onglet Données)*	--	shinkencryptionkey	**shinkencryptionkey**	Chaîne secrète utilisée pour chiffrer et déchiffrer les données SNMPv3.	

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)

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 :

? Unknown Attachment

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 elles n'y est pas :

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

Error rendering macro 'excerpt-include'

No link could be created for 'Erreurs communes du pack linux-by-SNMP__shinken'.