

Dépannage de la configuration de « tampon » sous le contexte d'interception légale dans StarOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Abréviations](#)

[Problème](#)

[Interception légale](#)

[Dépannage](#)

[Résolution](#)

[Configuration](#)

Introduction

Ce document décrit comment dépanner la configuration "buffer" dans le contexte d'interception légale dans StarOS.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître StarOS.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Abréviations

LI
PÂTURAGE
AF
MF
DF
CF

Interception légale
service répressif
Fonction Access
Fonction De Médiation
Fonction de livraison
Fonction de contrôle

IRI	Intercepter les informations associées
CC	Contenu de la communication
CLI	Interface de ligne de commande

AF peut être n'importe quel noeud StarOS. Les FC résident dans les locaux de LEA ou dans le domaine administratif.

Problème

Au moment de la configuration de l'option de mise en mémoire tampon sous le module d'interception légale, on observe que le paramètre lié à l'option de mise en mémoire tampon basée sur un événement/contenu n'était pas disponible dans la liste de configuration CLI.

Cette option permet de définir la valeur de mémoire tampon de 5 000 enregistrements IRI par défaut et de 1 000 enregistrements CC par contexte LI.

La seule option disponible dans la liste de configuration était « dest-addr ».

```
[li-context]<hostname>(config-ctx)# lawful-intercept tcp event-delivery  
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
```

Idéalement, il devrait afficher le mot clé "buffer" avec l'option "dest-addr" dans la liste d'options mentionnée précédemment.

Interception légale

Note: L'interception légale est une fonctionnalité activée par licence. La licence Basic Lawful Intercept prend en charge UDP en tant que protocole de transport pour l'interception de contenu d'appel (CC) pour les abonnés actifs. L'interception d'événements (IRI) et TCP en tant que protocole de transport pour la livraison ne sont pas pris en charge sous la licence Basic. La licence Enhanced Lawful Intercept prend en charge toutes les fonctionnalités de licence Basic LI, ainsi que l'interception d'événements (IRI) et TCP comme protocole de transport pour la livraison des paquets interceptés.

La fonctionnalité d'interception légale permet à l'opérateur de réseau d'intercepter les messages de contrôle et de données des utilisateurs mobiles ciblés. Afin d'invoquer cette prise en charge, le LEA demandera à l'opérateur de réseau de commencer l'interception d'un utilisateur mobile particulier. Cette demande sera appuyée par une ordonnance ou un mandat du tribunal. Différentes normes sont suivies pour l'interception légale dans différents pays.

Un processus d'interception légale typique comprend la séquence d'événements suivante :

1. La LEA demande au FST de commencer à intercepter une session d'une personne particulière, qui doit habituellement être appuyée par une ordonnance ou un mandat du tribunal. Des

renseignements permettant d'identifier la personne seront fournis (comme le numéro de téléphone ou le nom/l'adresse, etc.).

2. L'administrateur du fournisseur de services de télécommunications (TSP) configure la fonction d'accès/de livraison TSP pour commencer à intercepter les événements de contrôle/données de l'abonné ciblé. Si la session d'abonné est déjà en cours, l'interception se produit immédiatement. Sinon, la fonction d'accès doit attendre que la session de l'abonné se connecte.

3. La fonction d'accès envoie une copie des événements de contrôle/données pour la session interceptée à la fonction de remise.

4. La fonction de remise envoie les informations interceptées à une ou plusieurs fonctions de collecte, qui sont dans le domaine administratif de la LEA. Une fonction Collection analyse et stocke les informations interceptées.

5. Lorsque le LEA demande l'arrêt de l'interception, l'administrateur du FST configure la fonction d'accès et la fonction de remise pour arrêter l'interception pour cette session d'abonné particulière.

Une interface de ligne de commande (CLI) sur une session SSH est utilisée par le DF pour le provisionnement et le déprovisionnement de l'identité cible, ainsi que pour surveiller les statistiques de l'LI.

Ces protocoles/modes (IPv4 et IPv6) sont pris en charge sur StarOS pour fournir des événements et du contenu LI au DF :

·Mode UDP (désactivation) : L'adresse de DF2 et DF3 est fournie au moment de la mise en service du mode UDP sans accusé de réception.

·Mode TCP : Pour le mode TCP, la configuration fournit uniquement l'adresse de l'homologue. Toute remise d'événement interceptée (IRI) est envoyée à DF2 et toutes les remises de données interceptées (CC) sont envoyées à DF3.

Dépannage

La configuration StarOS doit disposer d'une licence appropriée pour cette fonction.

```
[local]<hostname># show license information | grep -i lawful
Monday December 10 01:54:13 UTC 2018
Lawful Intercept [ ASR5K-XX-CSXZZLI ]
+ Enhanced Lawful Intercept [ ASR5K-XX-CS0ZZELI / ASR5K-00-CS00XZI ]
Persistent Lawful Intercept [ ASR5K-XX-CS1ZZPLI ]
Segregating Lawful Intercept Context based on Count [ ASR5K-XX-PWXZZICS ]
```

StarOS doit également avoir une « configuration li séparée ».

Avec cette fonctionnalité, seul "li-administrator" pourra afficher et modifier les détails d'intégration de l'interface LI dans un contexte li dédié.

L'utilisateur LI admin doit être mappé sur li-administration dans la configuration.

```
administrator liadmin encrypted password *** ftp li-administration
```

Cependant, il a été constaté que StarOS ne permettait pas de définir l'option « buffer » dans le module de configuration d'interception légale.

```
[local]<hostname># context li
```

```
[li]<hostname># config
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
====> customer do see only this option
```

```
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery buff
Unknown command - "buff", unrecognized keyword
```

Idéalement, une option avec le mot clé « buffer » devrait être affichée pour compléter l'interface de ligne de commande comme ceci pour la configuration de la mémoire tampon.

```
configure
context
lawful-intercept tcp event-delivery buffer max-limit <1000 ... 50000>
end
```

Résolution

Afin d'obtenir les droits li-admin pour n'importe quel utilisateur StarOS, cet utilisateur doit être défini sous le contexte li avec des privilèges admin. C'est l'utilisateur li-admin qui a besoin de se connecter à partir d'un serveur externe (à partir de LEA) afin d'activer cette option "buffer". Tout autre utilisateur administrateur qui tente de se connecter au noeud sous un contexte local ne sera pas autorisé à définir cette option de « tampon ».

Voici les étapes afin d'atteindre la condition pour obtenir l'option "buffer" dans StarOS sous le module LI.

1. Connectez-vous au noeud avec l'utilisateur admin local.
 2. Créez un contexte li (car il n'y avait pas de contexte li dédié).
 3. Créez un utilisateur li avec des privilèges li-admin dans le contexte local.
 4. Créez un utilisateur li avec des privilèges li-admin dans le contexte li.
- <<nous avons supprimé li-admin du contexte local pour ajouter une li dédiée qui nous aidera à séparer le contexte li du contexte local >>
5. Supprimez l'utilisateur li disposant du privilège li-admin du contexte local.
 6. Créez un contexte de li dédié afin d'activer la configuration de li séparée.
 7. Définissez access-list sous li context.
 8. Déconnexion du noeud.
 9. Connectez-vous à nouveau au noeud avec l'utilisateur « li » qui a des privilèges en tant que li-admin.
 10. Configurez l'option de mémoire tampon requise, elle doit vous permettre de la configurer.

Configuration

```
[local]<hostname>(config)# context local
[local]<hostname>(config-ctx)# administrator li-admin password *** li-administration ftp
[local]<hostname>(config-ctx)# end
```

```
[local]<hostname>(config)# context li
[li]<hostname>(config-ctx)# administrator li-admin password *** ftp li-administration
```

<we removed li-admin from local context to add dedicated li which will help us to enable the segregate the li context from local context >

```
[local]<hostname>(config-ctx)# no administrator li-admin
[local]<hostname>(config-ctx)# exit
```

```
[local]<hostname>(config)# dedicated-li context li
Warning: Creating a dedicated LI context is a permanent configuration setting
Info: Context li is dedicated to Lawful-Intercept configuration
Info: Undefined ACLs will be set to deny-all within this context
[li]<hostname>(config-ctx)#
[li]<hostname>(config-ctx)# access-list undefined permit-all
[li]<hostname>(config-ctx)# end
```

Par exemple, après vous être connecté avec l'utilisateur li-admin, vous pouvez voir toutes les options dont nous avons besoin :

```
<local-node><hostname>$ ssh li-admin@li@
```

```
Cisco Systems QvPC-SI Intelligent Mobile Gateway
li-admin@li@aa.bb.cc.dd's password:
Last login: Wed Jan 23 17:32:31 -0500 2019 on pts/2 from 10.xx.yy.zz.
Cisco Systems QvPC-SI
Lawful Intercept Interface
```

```
No entry for terminal type "xterm-256color";
using dumb terminal settings.
```

```
[li] # configure
```

```
Warning: One or more other administrators may be configuring this system
```

```
[li]
```

buffer - This is used to configure the LI buffering >>>>>> **We can see the buffer option now.**
dest-addr - Destination IP address where the intercepted information needs to be forwarded.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.