IBM eNetwork Firewall pour Windows NT

Guide de référence

Version 3 Édition 2.1.1

SC11-1460-01

IBM eNetwork Firewall pour Windows NT

Guide de référence

Version 3 Édition 2.1.1

SC11-1460-01

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 165.

Réf. US : SC31-8659-01

Deuxième édition (juin 1998)

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.ibm.fr (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux États-Unis)

Par ailleurs, vous pouvez nous adresser tout commentaire sur ce document en utilisant le formulaire intitulé "REMARQUES DU LECTEUR" qui se trouve à la fin du document. IBM pourra disposer comme elle l'entendra des informations contenues dans vos commentaires, sans aucune obligation de sa part. Il va de soi que ces informations pourront continuer à être utilisées par leur auteur.

Dépôt légal : 2e trimestre 1998

Table des matières

À propos de ce guide

Le présent manuel de référence a pour objectif d'assister les administrateurs en charge de la sécurité des systèmes et des réseaux dans les opérations d'installation et de gestion du produit IBM eNetwork Firewall Version 3.2 sur une machine Windows NT**. Pour utiliser des programmes clients tels que Telnet ou FTP, reportez-vous aux sections du guide de l'utilisateur relatives à vos programmes clients TCP/IP.

Connaissances requises

L'installation et la configuration d'IBM eNetwork Firewall requièrent une solide connaissance des procédures d'administration de réseau et du protocole TCP/IP. Dans la mesure où vous allez définir et configurer un pare-feu assurant le contrôle des accès à votre réseau, en entrée comme en sortie, vous devez d'abord bien comprendre le fonctionnement de ce dernier. En particulier, il est important de connaître les principes de base des adresses IP, des noms qualifiés complets et des masques de sous-réseau.

Pour plus d'informations sur TCP/IP et, notamment, sur les fonctions netstat, arp, ifconfig, ping, nslookup, DNS, sendmail et sur le routage, reportez-vous à l'excellent manuel *Administration de réseau TCP/IP*. Pour de plus amples informations, reportez-vous à la *Bibliographie*.

Pour une information tout aussi complète sur TCP/IP et les procédures de routage, les matériels périphériques de réseau, les DNS et sendmail, les administrateurs de réseau UNIX pourront se reporter au manuel *UNIX System Administration Handbook*. Pour de plus amples informations, reportez-vous à la *Bibliographie*.

Fonctions disponibles dans cette version

IBM eNetwork Firewall pour Windows NT propose une grande variété de fonctions et comporte les trois architectures de pare-feu suivantes :

1. Serveurs relais d'applications
   - FTP ;
   - HTTP, avec Gopher et WAIS ;
   - Telnet ;
   - SafeMail.

   HTTP, Telnet et FTP permettent l'authentification des utilisateurs.
2. Passerelle de niveau circuit avec le protocole Socks version 5, une norme Internet
3. Filtrage : ensemble de critères extensifs et sélectifs permettant d'autoriser ou d'interdire les transactions. Ces critères peuvent porter sur l'adresse TCP/IP, le port, le protocole, la direction, la carte (sécurisée/non sécurisée), et sur bien d'autres paramètres.

   Plusieurs services prédéfinis permettent une mise en œuvre rapide du programme.

Protocole Socks version 5

Outre sa simplicité et sa souplesse, le protocole Socks version 5 offre les avantages suivants :

- Méthodes d'authentification et de chiffrement faciles à mettre en œuvre
- Association UDP, qui crée un circuit relais virtuel pour transiter par les circuits relais utilisant UDP
- Programme de surveillance Socks V5 Watcher, qui affiche des informations en temps réel sur les performances Socks

Conversion d'adresse réseau

Avec l'essor considérable du réseau Internet, la limitation des adresses IP devient un véritable problème. La conversion d'adresse réseau (NAT) apporte la solution au problème de la limitation des adresses Internet en permettant la réutilisation de ces adresses.

La NAT présente l'avantage de permettre en toute transparence à un réseau utilisant des adresses privées ou illégales de communiquer avec des hôtes sur l'Internet, procurant ainsi au réseau privé un accès à un vaste espace d'adressage. En outre, l'utilisation de la NAT dissimule les adresses du réseau privé aux yeux du monde extérieur, améliorant d'autant la sécurité du réseau.

Administration simplifiée

L'utilisateur dispose d'une application Java** pouvant être administrée à distance et qui facilite la mise à jour de la configuration du pare-feu. Aux différents administrateurs peuvent être assignés des niveaux d'autorité variables afin de mieux contrôler l'accès au pare-feu. Cette unique interface utilisateur graphique (GUI), simple d'accès, permet d'administrer aussi bien le pare-feu Windows NT que sa version AIX.

Durcissement de NT

Lorsque le pare-feu est installé, sont désactivés les protocoles non TCP/IP, les services système non indispensables et les possibilités de connexions locales des comptes n'appartenant pas à des administrateurs.

Authentification rigoureuse

Les principales méthodes d'authentification par code telles que SecurID, SecureNet Key et autres sont prises en charge.

Utilitaires de génération d'états

Les utilitaires de génération d'états permettent d'adresser une requête SQL au journal système après son exportation vers un moteur de base de données.

Alertes, contrôle et journalisation

Des fonctions de journalisation complètes permettent de consigner l'ensemble des opérations du pare-feu, en plus des adresses TCP/IP, des ID utilisateur, des heures, des noms de fichier, des numéros de port utilisés, etc. Un système de contrôle de journalisation est prévu pour surveiller les activités douteuses et générer des alertes en cas de dépassement de seuil.

Isolation des réseaux

L'utilisation des cartes NIC (Network Interface Card) avec le pare-feu permet d'isoler plusieurs sous-réseaux.

Support de langue nationale

Le support de langue nationale existe pour l'anglais, le japonais, le coréen, le français, le chinois simplifié et traditionnel, l'italien, l'espagnol et le portugais/brésilien.

Saisie d'adresses IP

Lors de la configuration du pare-feu, vous serez amené à saisir des adresses IP. Entrez une adresse IP complète, en notation décimale à point, avec les quatre parties requises, en respectant le format suivant :

`nnn.nnn.nnn.nnn`

où chaque segment `nnn` correspond à trois chiffres compris entre 000 et 255.

Accès à l'assistance IBM

Le centre d'assistance IBM offre des services de diagnostic et de résolution des problèmes en ligne. Ce service peut être appelé à tout moment ; un technicien vous rappellera sous un délai de huit heures dans les heures de travail habituelles suite à votre appel, du lundi au vendredi, de 8h00 à 17h00, heure locale. Le numéro d'appel est le 1-800-237-5511.

Contactez votre représentant IBM ou votre fournisseur agréé pour toute information complémentaire.

Chapitre 1. Utilisation de l'interface de ligne de commande d'IBM Firewall

Ce chapitre détaille les commandes utilisables avec la ligne de commande d'IBM eNetwork Firewall.

Les informations qui suivent se rapportent aux commandes :

- Les commandes détaillées dans ce manuel se présentent de la manière suivante :
  - *souligné* : données saisies par l'utilisateur.
  - [] : paramètre facultatif.
  - {} : plusieurs paramètres au choix de l'utilisateur.
  - | sépare les options.
- Tous les paramètres utilisent le format `mot clé=valeur`.
- Si un paramètre admet plusieurs valeurs, ces valeurs doivent se présenter entre doubles guillemets et être délimitées par des espaces. Par exemple :

  ```
  secaddr="11.22.33.1 11.22.33.2"
  ```
- N'ajoutez aucun espace à l'intérieur d'un paramètre sauf encadré par des doubles guillemets.
- Si vous oubliez des paramètres, l'utilitaire de ligne de commande affiche les paramètres manquants.
- Si la valeur d'un paramètre est incorrecte, l'utilitaire de ligne de commande signale l'erreur.
- Certains services de pare-feu actualisent dynamiquement leur mode opératoire lorsque leurs fichiers de configuration changent. D'autres nécessitent une sous-commande de mise à jour. Vous disposez d'une sous-commande `update` pour les services de pare-feu nécessitant une instruction de mise à jour.
- Seuls les administrateurs principaux du pare-feu peuvent exécuter des programmes depuis la ligne de commande.
- En raison de la complexité des fichiers et de leur interdépendance, il est **interdit d'éditer directement les fichiers de configuration.**

Serveur de configuration

La commande `fwcfgsrv` permet d'afficher ou de modifier les options du serveur de configuration. L'administrateur doit être autorisé à gérer les fonctions de contrôle des transactions pour lancer cette commande.

Pour afficher les options du serveur de configuration, tapez la commande suivante :

```
fwcfgsrv cmd=list
```

La sortie de la commande `fwcfgsrv` a l'aspect suivant :

```
localonly = yes/no
encryption = none/ssl
sslfile = filename if one is defined
```

Pour modifier les options du serveur de configuration, tapez la commande suivante :

```
fwcfgsrv cmd=change
         [localonly={yes|no}]
         [encryption={none|ssl}]
         [sslfile=]
```

Définitions des paramètres :

localonly Indique si le pare-feu doit être administré en mode local exclusivement. Les valeurs admises sont "yes" et "no".

encryption Indique si le serveur de configuration attend des données chiffrées avec l'algorithme SSL ou non. Les valeurs admises sont "none" et "ssl".

sslfile Indique le nom du fichier de clés SSL à utiliser pour le chiffrement SSL. Consultez le Chapitre 6, «Utilisation de l'utilitaire Make Key File (MKKF)», à la page 59.

Serveurs de noms de domaine (DNS)

Le serveur de nom de domaine (DNS) fournit aux hôtes du réseau sécurisé un service de noms de domaines complet tout en délivrant un minimum d'informations aux hôtes extérieurs au réseau. Trois serveurs de noms de domaine sont nécessaires pour remplir ces fonctions :

- Un sur le pare-feu ;
- Un sur le réseau sécurisé ;
- Un à l'extérieur du réseau sécurisé.

Pour plus d'informations, reportez-vous au *guide de l'utilisateur d'IBM eNetwork Firewall*.

Remarque :

1. La chaîne "x.x.x.x" correspond à une adresse IP en notation décimale à point.
2. Les paramètres secaddr et remaddr acceptent une adresse IP unique ou une liste d'adresses IP. Dans ce dernier cas, la liste doit être délimitée par des espaces et encadrée par des doubles guillemets.
3. Les adresses en double sont détectées et signalées comme des erreurs.
4. Lors de la première configuration du DNS, la commande `fwdns cmd=change` crée le nouveau fichier. Le pare-feu ne possédera jamais qu'un seul enregistrement de la configuration du serveur de noms de domaine. Les valeurs de cette configuration pourront être nulles. Modifier tout ou partie des valeurs de l'enregistrement DNS peut se faire simplement par le biais de la sous-commande "change".

La commande suivante affiche la configuration courante du DNS.

```
fwdns cmd=list
```

Pour modifier l'entrée de configuration du DNS et créer un fichier :

```
fwdns cmd=change
    secdomain=nom_domaine_sécurisé
    secaddr=x.x.x.x | "x.x.x.x  x.x.x.x  x.x.x.x"
    remaddr=x.x.x.x | "x.x.x.x  x.x.x.x  x.x.x.x"
```

Définitions des paramètres :

secdomain=*nom_domaine_sécurisé* nom de domaine du réseau sécurisé interne.

secaddr=*adresse_DNS_sécurisé[,...]* adresse IP du serveur de noms de domaine sécurisé.

remaddr=*adresse_DNS_non_sécurisé* Adresse IP des serveurs de noms de domaine extérieurs au réseau sécurisé mis à disposition par votre fournisseur de services Internet.

Filtres

Utilisez la commande `fwfilter` pour activer ou désactiver les règles de filtrage.

```
fwfilter cmd=update | verify | list | shutdown | startlog | stoplog
```

Les définitions des paramètres sont les suivantes :

fwfilter cmd=update rétablit la configuration et active le jeu de règles.

fwfilter cmd=verify examine la disposition de la configuration mais n'active aucune modification.

fwfilter cmd=list affiche la dernière configuration établie.

fwfilter cmd=shutdown désactive le dispositif de filtrage.

fwfilter cmd=startlog consigne les transactions sélectionnées dans le `fichier journal du pare-feu`.

fwfilter cmd=stoplog interrompt la journalisation du filtrage du pare-feu.

Serveur relais HTTP

Serveur relais HTTP gère parfaitement les requêtes du navigateur dans le pare-feu et élimine la nécessité d'un serveur Socks pour la navigation sur le Web. Les utilisateurs peuvent accéder à toutes les informations utiles disponibles sur Internet, sans compromettre la sécurité de leurs réseaux internes ni modifier leur environnement client.

La commande `fwhttp` permet d'afficher ou de modifier la configuration de serveur relais HTTP courante.

Pour afficher la configuration courante du serveur relais HTTP, utilisez la commande suivante :

```
fwhttp cmd=list
```

Pour modifier la configuration courante du serveur relais HTTP, utilisez la commande suivante :

```
fwhttp cmd=change
        [port=]
        [maxcontentlengthbuffer=]
        [minactivethreads=]
        [maxactivethreads=]
        [idlethreadtimeout=]
        [logging=]
        [authenticate=]
        [authenticatetimeout=]
        [maxpersistrequests=]
        [persisttimeout=]
```

Définitions des paramètres :

port Port attribué au serveur relais HTTP.

maxcontentlengthbuffer Taille maximale de la mémoire tampon utilisée pour retourner les documents avec ajout d'un en-tête indiquant le volume de la transaction.

minactivethreads Nombre minimal d'unités d'exécution à lancer à l'initialisation et à conserver actives au cours de l'exécution.

maxactivethreads Nombre maximal d'unités d'exécution pouvant être actives simultanément.

idlethreadtimeout Délai de disponibilité des unités d'exécution inactives.

logging Indique si l'activité HTTP doit être journalisée ou non. ON active la journalisation et OFF la désactive.

authenticate Niveau d'authentification des utilisateurs. Les valeurs sont all pour tous, none pour aucun, ou new pour les nouveaux utilisateurs.

authenticatetimeout Délai d'attente d'une requête client après établissement d'une connexion permanente.

maxpersistrequests Nombre maximal de requêtes autorisé pour une connexion permanente.

persisttimeout Délai de conservation d'une connexion permanente

Interfaces

Les interfaces sécurisées relient l'hôte IBM Firewall aux hôtes de votre réseau interne ; le réseau à protéger. **Vous devez disposer d'au moins une interface sécurisée pour que le pare-feu fonctionne.** Les interfaces non sécurisées relient le pare-feu à un ou plusieurs réseaux externes ou au réseau Internet. Le pare-feu IBM doit comporter au moins une interface non sécurisée.

Cette commande affiche la liste des interfaces réseau du pare-feu. L'administrateur doit être autorisé à gérer les fonctions d'interface pour lancer cette commande.

```
fwinterface cmd=list
                    [addr=x.x.x.x]
```

Pour plus d'informations sur les autorités administratives, reportez-vous au chapitre relatif à l'administration dans le *guide de l'utilisateur d'IBM eNetwork Firewall*.

Définitions des paramètres :

addr=x.x.x.x Affiche la liste de toutes les interfaces réseau configurées sur le pare-feu et précise pour chacune s'il s'agit d'une interface sécurisée ou non. La requête peut aussi préciser un nom d'interface. Si le paramètre facultatif `addr` a été renseigné, seule l'interface correspondante est affichée. Si une adresse IP en notation décimale à point est associée au paramètre `addr`, la liste affichera l'adresse, le statut et le nom attachés à cette seule adresse IP, si elle a été configurée sur le pare-feu.

Cette commande permet de définir les interfaces réseau sur le pare-feu. L'administrateur doit être autorisé à gérer les fonctions d'interface pour lancer cette commande.

```
fwinterface cmd=change
            addr=x.x.x.x
            [state={secure|nonsecure}]
            [name=]
```

Définitions des paramètres :

addr=x.x.x.x Adresse de l'interface à modifier, en notation décimale à point. Si l'interface n'est pas définie sur le pare-feu, la sortie est un message d'erreur.

state={secure|nonsecure} Contient l'un des mots clés "secure" ou "nonsecure" et caractérise le réseau attaché à l'interface spécifiée comme étant sécurisé ou non sécurisé.

name Nom évocateur identifiant l'interface ou le réseau auquel elle est attachée. Ce nom peut comporter des espaces encadrés de doubles guillemets.

Les paramètres de statut et de nom sont optionnels mais l'un au moins doit être spécifié.

Archivage des fichiers journaux

La commande suivante appelle la fonction logfile pour configurer les fonctions de journalisation définies avec l'archivage.

```
fwlogmgmt -1 ou fwlogmgmt -a
```

Cette commande peut être insérée dans un service planifié Windows NT. Pour plus d'informations, reportez-vous au *guide de l'utilisateur d'IBM eNetwork Firewall*.

Gestion des fichiers journaux

La gestion des fichiers journaux permet de définir et de gérer les fichiers journaux et les fichiers d'archive. La commande fwlog permet d'ajouter, de modifier et de supprimer des fonctions de journalisation.

Pour ajouter des fonctions de journalisation, tapez la commande suivante :

```
fwlog cmd=add
      facility=fonction
      priority=priorité
      logfile=nom_journal
       [arcfile=chemin_archive
       logtime=délai_conserv_journal
       arctime=délai_conserv_archive
```

Le paramètre **facility** admet les valeurs suivantes :

- firewall (local4) - journaux de pare-feu de portée générale, notamment de journalisation des filtres
- alert (local1) - journal des alertes (statut du démon de contrôle de journalisation et avertissements de dépassement de seuil)
- adminaudit (local0) - journal d'audit administratif
- mail - journaux de messagerie

Le paramètre **priority** admet les valeurs suivantes :

- debug
- info
- warning
- error
- crit

Le paramètre logfile indique la destination des entrées du journal de pare-feu. La valeur associée à logfile doit être un nom de fichier qualifié complet (format unité:\répertoire) indiquant la destination des entrées de fichier journal.

Remarque : Les fichiers associés aux fonctions de `journal des alertes` ou de `journal de pare-feu` doivent être distincts et différents des fichiers spécifiés pour toute autre fonction de journalisation s'il est prévu d'utiliser les fonctions du pare-feu pour traiter ces fichiers.

Il est important que seuls les messages de journal de pare-feu apparaissent dans les fichiers d'entrée des utilitaires de génération d'états. Aucune autre fonction ne doit être dirigée vers le même fichier que celui du journal de pare-feu ou celui du journal des alertes.

Les paramètres arcfile, logtime et arctime sont des paramètres facultatifs et ne sont valides que lorsque le paramètre logfile spécifie un nom de fichier. Si l'un de ces paramètres est renseigné, vous devez renseigner les deux autres. Ces paramètres contrôlent l'archivage des fichiers journaux. Pour que l'archivage des fichiers journaux entre en action, exécutez la commande `fwlogmgmt` périodiquement. Voir la section «Archivage des fichiers journaux», à la page 5.

Par défaut, le pare-feu utilise ces paramètres pour indiquer où stocker les enregistrements des fichiers d'archive et à quelle fréquence procéder à l'archivage. Ces trois paramètres doivent être renseignés pour permettre l'archivage.

La fonction d'archivage peut être remplacée par l'ajout d'un programme d'archivage écrit par l'utilisateur. Consultez le Chapitre 4, «Module de développement d'un logiciel compagnon d'archivage», à la page 47.

Le paramètre **arcfile** doit indiquer un nom de chemin qualifié complet.

Le paramètre **logtime** indique le nombre de jours minimum pendant lequel une entrée de journal de pare-feu sera conservée dans le fichier journal avant d'être transposée dans le fichier d'archive.

Le paramètre **arctime** indique le nombre de jours minimum pendant lequel un enregistrement de journal de pare-feu sera conservé dans le fichier d'archive avant d'être éliminé.

Pour modifier des fonctions de journalisation, tapez la commande suivante :

```
fwlog cmd=change
       index=index
[facility=fonction]
[priority=priorité]
[logfile=nom_journal]
       [arcfile=nom_fichier_archive]
[logtime=délai_conserv_journal]
[arctime=délai_conserv_archive]
```

Si, suite à une modification, en particulier portant sur la première instance, le fichier de configuration créé contient des erreurs de syntaxe (par exemple des zones non renseignées dans la définition du fichier journal), un avertissement sera généré et les données ne seront pas journalisées.

Pour activer la journalisation sans l'archivage, spécifiez la valeur des paramètres **facility**, **priority** et **logfile**. Pour désactiver l'archivage des journaux, effacez la valeur des paramètres **archive**, **logtime** et **arctime**. Si vous avez planifié un travail d'archivage, supprimez-le.

Pour afficher les données de configuration du fichier journal courant, tapez la commande suivante :

```
fwlog cmd=list
```

Pour supprimer l'entrée de journal de pare-feu désignée par le numéro d'index retourné par la commande fwlog cmd=list, tapez la commande suivante :

```
fwlog cmd=delete
      index=index de l'entrée à supprimer
```

Contrôle de journalisation

Utilisez la commande fwlogmon pour indiquer au contrôle de journalisation quand et comment déclencher des alertes. Les alertes sont déclenchées lorsque les valeurs de seuil spécifiées dans la commande (ou dans le panneau du client de configuration correspondant) sont atteintes dans un délai déterminé. Quand une alerte se déclenche :

1. Un enregistrement est écrit dans le journal des alertes et dans le journal de pare-feu.
2. Une commande spécifiée s'exécute.
3. Une notification est envoyée à un ou à plusieurs utilisateurs.
4. Un message est envoyé à un récepteur de radiomessagerie.

Les trois dernières actions sont contrôlées par la configuration appropriée des valeurs spécifiées en l'espèce.

Affichage des paramètres du contrôle de journalisation

```
fwlogmon cmd=list
```

Spécification des ID utilisateur destinataires des notifications d'alerte

Pour spécifier les ID des utilisateurs devant recevoir les notifications d'alerte (la notification est envoyée à tous les ID ajoutés), tapez la commande suivante :

```
fwlogmon cmd=add|delete
         type=id
         username=
         [comment=]
```

Spécification d'une commande à exécuter en cas d'alerte

```
fwlogmon cmd=add|change
         type=command
         command=
         [comment=]

fwlogmon cmd=delete
         type=command
```

Spécification d'un seuil de déclenchement d'alerte sur la base d'un nombre de tentatives de connexion infructueuses

```
fwlogmon cmd=add
         type=single|multi|host
         count=
         time=
         pager=
         [comment=]

fwlogmon cmd=change
         type=single|multi|host
         [count=]
         [time=]
         [pager=]
         [comment=]

fwlogmon cmd=delete
         type=single|multi|host
```

Spécification d'un seuil de déclenchement d'alerte sur la base d'un nombre d'occurrences d'un ID de message de pare-feu

```
fwlogmon cmd=add
         type=msg
         tag=
         count=
         time=
         pager=
         [comment=]

fwlogmon cmd=change
         type=msg
         tag=
         [count=]
         [time=]
         [pager=]
         [comment=]

fwlogmon cmd=delete
         type=msg
         tag=
```

Définitions des paramètres :

type Identifie le type de la commande de contrôle de journalisation ajoutée ou modifiée.

Les valeurs admises sont id, command, msg, single, multi et host.

id ID de l'utilisateur destinataire des notifications.

command Commande à exécuter.

msg Joue sur le contrôle d'un message de fichier journal spécifique.

single Joue sur le contrôle sur la base d'ID utilisateur isolés. Les tentatives infructueuses associées à chaque ID sont comptées. Si le compteur atteint la valeur de seuil spécifiée avec cette commande, une alerte se déclenche.

multi Joue sur le contrôle sur la base d'une sélection d'ID utilisateur. Si le total des compteurs relevant les tentatives infructueuses de tous les ID de la sélection atteint la valeur de seuil spécifiée avec cette commande, une alerte se déclenche.

host Joue sur le contrôle sur la base des noms d'hôte. Les tentatives infructueuses associées à chaque nom d'hôte sont comptées. Si le compteur d'un nom d'hôte quelconque atteint la valeur de seuil spécifiée avec cette commande, une alerte se déclenche.

username ID de messagerie d'un administrateur de pare-feu ou d'un autre utilisateur devant recevoir notification des alertes. Les notifications d'alerte ne seront transmises par messagerie que si vous avez convenablement configuré un serveur de messagerie du côté sécurisé.

command Nom de la commande à exécuter sur déclenchement d'une alerte. Indiquez le nom de chemin complet d'un fichier exécutable. Il peut s'agir d'un fichier .bat, contenant plusieurs commandes à exécuter. Si ce fichier .bat fait référence à d'autres fichiers, leur nom de chemin complet doit être fourni.

count Définit le seuil d'échecs ou le seuil d'occurrences d'un message de journal particulier, devant déclencher une alerte.

time Définit un délai en minutes. La valeur du seuil doit être atteinte dans ce délai dès la première occurrence, pour qu'une alerte se déclenche. Les occurrences antérieures à ce délai ne sont pas comptabilisées.

pager Indique si un message doit être envoyé ou non lorsque le seuil associé déclenche une alerte. Le message est envoyé selon les paramètres de la configuration de radiomessagerie active.

tag Code du message de journal (avec le préfixe ICA) à contrôler. Les messages de contrôle de journalisation (codes ICA inférieurs à 1000) ne sont pas concernés par cette fonction.

Messagerie

La commande `fwmail` permet de mettre en correspondance des domaines de messagerie sécurisés et des domaines publics.

```
fwmail cmd=list

fwmail cmd=add
        secdomain=
        mail=
        remdomain=

fwmail cmd=change
        secdomain=
        [mail=]
        [remdomain=]

fwmail cmd=delete
        secdomain=
```

Définitions des paramètres :

secdomain Nom sous lequel le domaine de messagerie désigné est connu des utilisateurs du côté sécurisé du pare-feu.

mail Adresse d'un serveur de messagerie.

remdomain Nom sous lequel le domaine de messagerie désigné est connu des utilisateurs du côté non sécurisé du pare-feu.

Conversion d'adresse de réseau (NAT)

La conversion des adresses réseau (NAT) apporte une solution en permettant à un quelconque réseau IP de réutiliser les adresses de votre réseau IP sécurisé.

La NAT prend en charge quatre types de configuration :

- Adresse enregistrée "Plusieurs à un" - La conversion d'adresse enregistrée de type "plusieurs à un" convertit l'adresse sécurisée et le numéro de port d'un paquet de telle façon que plusieurs adresses (jusqu'à 65536) internes puissent partager une seule et même adresse IP enregistrée. Cette adresse IP enregistrée commune dissimulera des adresses locales. Vous devrez lui associer une autre adresse Internet enregistrée, spécifique au pare-feu.

- Conversion d'adresses IP sécurisées - Une entrée de conversion (translate) d'adresse IP sécurisée définit un ensemble d'adresses réseau sécurisées pour la conversion desquelles le service NAT est nécessaire. Par défaut, la conversion d'adresse de réseau se fait sur toutes les adresses IP sécurisées.
- Exclusion d'adresses IP sécurisées - Une entrée d'exclusion (exclude) d'adresse IP sécurisée définit un ensemble d'adresses réseau sécurisées pour la conversion desquelles le service NAT n'est pas obligatoire. Par défaut, la conversion d'adresse de réseau se fait sur toutes les adresses IP sécurisées, sauf sur celles comprises dans une plage définie par une entrée d'exclusion d'adresses IP sécurisées.
- Mise en correspondance d'une adresse IP sécurisée - Une entrée de mise en correspondance (map) d'adresse IP sécurisée définit une relation bilatérale entre une adresse IP sécurisée et une adresse IP enregistrée. Cette mise en correspondance bilatérale des adresses IP permet à des clients externes, tels que des clients FTP ou Telnet, d'ouvrir des sessions TCP sur les serveurs internes au réseau sécurisé.

La syntaxe de la commande NAT est la suivante :

```
fwnat cmd=list | update | verify |shutdown |
startlog | stoplog
```

Définitions des paramètres :

fwnat cmd=list Affiche la configuration NAT courante.

fwnat cmd=update Régénère le moteur NAT.

fwnat cmd=verify Vérifie la syntaxe de la configuration.

fwnat cmd=shutdown Interrompt toutes les conversions d'adresse en cours.

fwnat cmd=startlog Commence à journaliser chaque paquet converti.

fwnat cmd=stoplog Arrête de journaliser chaque paquet converti.

Pour ajouter une entrée "plusieurs à un" à à la configuration NAT, utilisez la commande **type=many-to-one** :

```
fwnat cmd=add
        type=many-to-one
        addr=Addr
        [timeout=minutes]
```

Définitions des paramètres :

type=many-to-one Ajoute une entrée "plusieurs à un".

addr=*adresse* Adresse IP identifiant une série d'adresses IP enregistrées ajoutées au parc d'adresses enregistrées.

timeout=*minutes* Définit le nombre de minutes pendant lequel un processus de conversion d'adresse peut rester inactif avant que le service NAT ne délivre l'adresse IP enregistrée. La valeur par défaut est 15, la plage de valeurs admises allant de 5 à 45.

Pour modifier une entrée "plusieurs à un" dans le fichier de configuration NAT, utilisez la commande suivante :

```
fwnat cmd=change
      index=
        [addr=Addr]
        [timeout=minutes]
```

Définitions des paramètres :

index Lorsque vous exécutez la commande `fwnat cmd=list`, la colonne de gauche contient des nombres correspondant à des entrées NAT. Utilisez le nombre correspondant à votre entrée NAT comme paramètre d'index.

addr=*adresse* Adresse IP identifiant une série d'adresses IP enregistrées ajoutées au parc d'adresses enregistrées.

timeout=*minutes* Définit le nombre de minutes pendant lequel un processus de conversion d'adresse peut rester inactif avant que le service NAT ne délivre l'adresse IP enregistrée. La valeur par défaut est 15, la plage de valeurs admises allant de 5 à 45.

Pour ajouter une entrée de conversion dans le fichier de configuration NAT, utilisez **type=translate** et pour exclure une entrée du fichier de configuration NAT, utilisez **type=exclude** :

```
fwnat cmd=add
        type={translate|exclude}
        addr=adresse
        mask=masque
```

Définitions des paramètres :

type=translate Ajoute une entrée `translate`.

type=exclude Ajoute une entrée `exclude`.

addr=*adresse* Adresse IP identifiant une plage d'adresses IP sécurisées nécessitant une conversion d'adresse réseau.

mask=*masque* Identifie une série d'adresses IP.

Pour modifier une entrée de conversion ou d'exclusion dans le de configuration NAT, utilisez la commande suivante :

```
fwnat cmd=change
      index=
        [addr=adresse]
        [mask=masque]
```

Définitions des paramètres :

index Lorsque vous exécutez la commande `fwnat cmd=list`, la colonne de gauche contient des nombres correspondant à des entrées NAT. Utilisez le nombre correspondant à votre entrée NAT comme paramètre d'index.

addr=*adresse* Adresse IP identifiant une plage d'adresses IP sécurisées nécessitant une conversion d'adresse réseau.

mask=*masque* Identifie une série d'adresses IP.

Pour ajouter une entrée de mise en correspondance à la configuration NAT, utilisez la commande **type=map** :

```
fwnat cmd=add
      type=map
      secaddr=adresse_sécurisée]
      remaddr=adresse_enregistrée]
```

Définitions des paramètres :

type=map Ajoute une entrée `map`.

secaddr Adresse IP devant être convertie en une adresse IP enregistrée déterminée.

remaddr Adresse enregistrée devant résulter de la conversion de l'adresse sécurisée spécifiée.

Pour modifier une entrée de mise en correspondance dans le fichier de configuration NAT, utilisez la commande suivante :

```
fwnat cmd=change
      index=
      [secaddr=SecureAddr]
      [remaddr=RegisteredAddr]
```

Définitions des paramètres :

index Lorsque vous exécutez la commande `fwnat cmd=list`, la colonne de gauche contient des nombres correspondant à des entrées NAT. Utilisez le nombre correspondant à votre entrée NAT comme paramètre d'index.

secaddr Adresse IP devant être convertie en une adresse IP enregistrée déterminée.

remaddr Adresse enregistrée devant résulter de la conversion de l'adresse sécurisée spécifiée.

Messagerie

Vous pouvez activer le support de notification par récepteur de messagerie si vous désirez que le pare-feu avertisse un administrateur système, via son récepteur de messagerie, en cas d'alerte d'intrusion sur le pare-feu. Pour que cela fonctionne, vous devez configurer le récepteur de messagerie, le service de radiomessagerie et un modem, à l'aide des commandes `fwpgr`, `fwcarrier` et `fwmodem`.

Configuration du récepteur de messagerie

La commande `fwpgr` configure les paramètres du récepteur de messagerie actif, celui que le pare-feu contactera.

Pour afficher un récepteur de messagerie, tapez la commande suivante :

```
fwpgr cmd=list
```

Pour ajouter un récepteur de messagerie, tapez la commande suivante :

```
fwpgr cmd=add
       carrier=
       modem=
       pagerid=
       message=
```

Pour modifier les paramètres d'un récepteur de messagerie, tapez la commande suivante :

```
fwpgr cmd=change
        [carrier=]
        [modem=]
        [pagerid=]
        [message=]
```

Définitions des paramètres :

carrier Nom de l'opérateur tel qu'il apparaît dans la base de données des opérateurs (via la commande `fwcarrier`).

modem Nom du modem tel qu'il apparaît dans la base de données des modems (via la commande `fwmodem`).

pagerid ID ou nom unique attribué par l'opérateur au récepteur de messagerie.

message Message à envoyer et devant s'afficher sur le récepteur de messagerie. Chiffres ou texte, selon les capacités de l'opérateur. Le message sera tronqué s'il dépasse la longueur du plus petit paramètre de longueur de l'opérateur (200 caractères).

Opérateur

La commande `fwcarrier` permet de définir les paramètres de n'importe quel service de radiomessagerie.

Pour afficher un opérateur, tapez la commande suivante :

```
fwcarrier cmd=list
        carrier=
```

Pour ajouter un opérateur, tapez la commande suivante :

```
fwcarrier cmd=add
        carrier=
          dial=
          method=
          [password=]
          length=
        baud=
        parity=
        databits=
        stopbits=
```

Pour modifier les paramètres d'un opérateur, tapez la commande suivante :

```
fwcarrier cmd=change
        carrier=
          [dial=]
          [method=]
          [password]
          [length=]
          [baud]
        [parity=]
        [databits=]
        [stopbits=]
```

Pour supprimer un opérateur, tapez la commande suivante :

```
fwcarrier cmd=delete
        carrier=
```

Définitions des paramètres :

carrier Nom de l'opérateur.

dial Numéro de téléphone du modem de l'opérateur attaché au service TAP souscrit.

method Entrez "TAP".

password Mot de passe facultatif sauf si l'opérateur l'exige.

length Longueur de message maximale autorisée par l'opérateur de radiomessagerie.

baud Vitesse de transmission la plus fiable admise par l'opérateur.

parity Type de contrôle de parité pris en charge par l'opérateur. Le protocole TAP est habituellement associé à une parité "égale".

databits Nombre de bits de données pris en charge par l'opérateur. Le protocole TAP est habituellement associé à la valeur 7.

stopbits Nombre de bits d'arrêt pris en charge par l'opérateur. Le protocole TAP est habituellement associé à la valeur 1.

Configuration du modem

Vous devez configurer votre modem pour pouvoir définir le support de notification par récepteur de messagerie.

Utilisez la commande fwmodem pour configurer le modem de sorte qu'il puisse adresser des requêtes d'envoi de messages à l'opérateur de radiomessagerie.

Pour afficher un modem, tapez la commande suivante :

```
fwmodem cmd=list
        modem=
```

Pour ajouter un modem, tapez la commande suivante :

```
fwmodem cmd=add
        modem=
        comport=
        initsting=
        outsideline=
```

Pour modifier les paramètres d'un modem, tapez la commande suivante :

```
fwmodem cmd=change
        modem=
        [comport=]
        [initstring=]
        [outsideline=]
```

Pour supprimer un modem, tapez la commande suivante :

```
fwmodem cmd=delete
        modem=
```

Définitions des paramètres :

modem Nom du modem.

comport Port de communication série dédié au modem. Le modem attaché à ce port de communication ne doit pas être défini dans le système Windows NT.

initstring Chaîne d'initialisation du modem. Les paramètres figurant dans la chaîne doivent convenir pour une commande de modem AT mais la commande AT ne doit pas figurer dans la chaîne proprement dite. Les paramètres spécifiés doivent être en accord avec les conditions de communication du modem de l'opérateur.

outsideline Numéro d'accès à la ligne extérieure.

Test de configuration du récepteur de messagerie

Pour vérifier la configuration du récepteur de messagerie actif, tapez la commande suivante :

```
pager
        carrier=
        modem=
    ID=
    msg=
```

Les définitions des paramètres sont identiques à celles de la commande `fwpgr`.

Utilisation de plusieurs récepteurs de messagerie

Si vous changez périodiquement de récepteur de messagerie actif :

- Assurez-vous que vous avez bien défini tous les opérateur et les modems nécessaires.
- Utilisez la commande `fwpgr` ou le programme client de configuration pour définir et sauvegarder une configuration de récepteur de messagerie.
- Copiez le fichier `ROOTDIR\config\pager.cfg` sous un nom reconnaissable.
- Définissez d'autres configurations de récepteur de messagerie et copiez-les jusqu'à avoir toutes les copies de fichier pager.cfg nécessaires.
- Recopiez le fichier de configuration à activer sous le nom `ROOTDIR\config\pager.cfg`.

Si vous désirez gérer des commutations de récepteur, planifiez un travail avec la commande Windows NT `at` pour répéter automatiquement la dernière puce (point noir) au début de chaque commutation.

Utilisateurs

La commande détaillée ci-dessous permet d'ajouter un nouvel utilisateur au pare-feu ou de modifier les attributs d'un utilisateur existant. Tous les paramètres possèdent des valeurs par défaut ou sont sans objet dans certaines circonstances. Pour `cmd=add`, les valeurs par défaut seront enregistrées ; pour `cmd=change`, les valeurs existantes seront conservées.

```
fwuser cmd={add|change}
       username=nom_connexion
       [fullname="nom_civil_utilisateur]
       [password={yes|no}]
       [pwdvalue=mot de passe]
       [level={proxy|admin}]
       [secftp=authentification FTP sécurisée]
       [remftp=authentification FTP non sécurisée]
       [secauth=authentification Telnet sécurisée]
       [remauth=authentification Telnet non sécurisé]
       [secadmin=authentification administrateur sécurisée]
       [remadmin=authentification administrateur non sécurisée]
       [secsocks=Socks sécurisé]
       [remsocks=Socks non sécurisé]
       [sechttp=HTTP sécurisé]
       [key="clé SecureNet"]
       [histexpire=délai d'expiration historique]
       [histsize=taille historique]
       [loginretries=tentatives connexion]
       [maxage=âge maximum]
       [maxexpired=délai expiration max]
       [maxrepeats=répétitions caractères max]
       [minalpha=caractères alpha min]
       [mindiff=caractères différents min]
       [minlen=longueur minimale]
       [minother=caractères non alpha min]
       [pwdwarntime=préavis mot de passe]
       [userchng={yes|no}]
       [pwlocked={yes|no}]
       [fg_all={yes|no}]
       [fg_dns={yes|no}]
       [fg_interfaces={yes|no}]
       [fg_logmonitor={yes|no}]
       [fg_logs={yes|no}]
       [fg_mail={yes|no}]
       [fg_netobjs1={yes|no}]
       [fg_netobjs2={yes|no}]
       [fg_pagers={yes|no}]
       [fg_proxyserver={yes|no}]
       [fg_user={yes|no}]
       [fg_traffic={yes|no}]
```

Paramètres fondamentaux

username Nom de connexion de l'utilisateur.

fullname Nom complet de l'utilisateur ou ligne d'informations relatives à l'utilisateur. Si la chaîne doit contenir des espaces, elle doit être encadrée par des doubles guillemets.

level La valeur par défaut est "proxy". Elle indique que l'utilisateur créé est un utilisateur relais simple ou un utilisateur Socks. Les groupes de fonctions d'administration et les authentifications d'administrateur ne concernent pas les utilisateurs relais.

key Clé d'authentification de la carte DPSK (Digital Pathways SecureNet Key) de l'utilisateur. Cette valeur qui comporte des espaces doit être encadrée par des doubles guillemets.

Authentifications

Voici présentées des chaînes d'authentification accompagnées des méthodes d'authentification correspondantes. L'utilisation des chaînes d'authentification avec les divers paramètres de la commande `fwuser` est détaillée ci-dessous :

- permit : autorisation globale ;
- deny : interdiction globale ;
- password : mot de passe de pare-feu ;
- NT : mot de passe de connexion NT ;
- snk : clé SNK ;
- sdi : clé SDI ;
- user : authentification fournie par l'utilisateur ;
- userauth2 : authentification fournie par l'utilisateur ;
- userauth3 : authentification fournie par l'utilisateur.

secftp Méthode d'authentification à utiliser pour les connexions FTP établies depuis une interface sécurisée. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3. La valeur par défaut est deny.

remftp Méthode d'authentification à utiliser pour les connexions FTP établies depuis une interface non sécurisée. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3. La valeur par défaut est deny.

secauth Méthode d'authentification à utiliser pour les connexions Telnet établies depuis une interface sécurisée. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi et user. La valeur par défaut est deny.

remauth Méthode d'authentification à utiliser pour les connexions Telnet établies depuis une interface non sécurisée. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3. La valeur par défaut est deny.

secadmin Méthode d'authentification à utiliser pour les connexions du client de configuration Firewall établies depuis une interface sécurisée. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3. La valeur par défaut est deny pour les utilisateurs relais et NT pour les administrateurs de pare-feu principaux.

remadmin Méthode d'authentification à utiliser pour les connexions du client de configuration Firewall établies depuis une interface non sécurisée. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3. La valeur par défaut est deny pour les utilisateurs relais et NT pour les utilisateurs de pare-feu principaux.

secsocks Méthode d'authentification Socks V5 à utiliser pour les connexions de client Socks provenant du côté sécurisé du pare-feu. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3.

Si le serveur Socks V5 est configuré pour mettre en œuvre des méthodes d'authentification de type saisie de l'ID utilisateur/mot de passe au lieu de méthodes d'authentification avec dialogue (CRAM), SNK ne fonctionnera pas puisque le protocole ID utilisateur/mot de passe Socks V5 ne peut pas afficher le dialogue SNK.

La valeur par défaut est deny.

remsocks Méthode d'authentification Socks V5 à utiliser pour les connexions de client Socks provenant du côté non sécurisé du pare-feu. Les valeurs acceptées sont deny, permit, password, NT, snk, sdi, user, userauth2 et userauth3.

Si le serveur Socks V5 est configuré pour mettre en œuvre des méthodes d'authentification de type saisie de l'ID utilisateur/mot de passe au lieu de méthodes d'authentification avec dialogue (CRAM), SNK ne fonctionnera pas puisque le protocole ID utilisateur/mot de passe Socks V5 ne peut pas afficher le dialogue SNK.

La valeur par défaut est deny.

sechttp Méthode d'authentification à utiliser pour les requêtes HTTP provenant d'une interface sécurisée. Les valeurs acceptées sont deny, permit, password, NT, sdi, user, userauth2 et userauth3.

Le protocole HTTP n'ayant pas la possibilité d'afficher le dialogue SNK, cette méthode d'authentification ne peut pas être exploitée dans ce contexte. La méthode SDI est prise en charge mais l'utilisateur devra fournir un mot de passe au lieu d'un code d'accès SDI. L'utilisateur doit entrer son code d'accès SDI personnel.

Remarque : `fwdfuser` n'autorise pas la sélection de SNK ou de Firewall Password (mot de passe de pare-feu) dans ses zones de méthode d'authentification.

Paramètres du mot de passe de pare-feu

password Indique si l'utilisateur devra fournir un mot de passe. Par défaut, vous devrez préciser si une méthode d'authentification a été définie. Vous pourrez opter pour la méthode par défaut ; l'authentification par mot de passe.

pwdvalue Principalement utilisé dans la programmation de scripts, le paramètre pwdvalue permet de définir la valeur d'un paramètre sur la ligne de commande. Notez que cette valeur est saisie en clair et n'est pas abritée des regards indiscrets. Ce paramètre n'a pas de valeur par défaut.

userchng Détermine la valeur du code de modification de l'administrateur dans la base de données des utilisateurs. Si la valeur est "yes", l'utilisateur devra modifier son mot de passe lors de sa première connexion. La valeur par défaut est "no". Ce paramètre n'est valable que si les paramètres password=yes et pwdvalue='' ont été fournis.

pwlocked Indique si le mot de passe a été verrouillé. La valeur est "yes" lorsque le nombre maximal d'échecs de connexion autorisé a été dépassé ou que le mot de passe n'a pas été utilisé pendant le nombre de semaines spécifié par le paramètre de délai maximal avant verrouillage.

histexpire Caractérise la période (en semaines) durant laquelle un mot de passe ne peut pas être réutilisé. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 52. La valeur 0 indique qu'aucune limite de durée n'a été définie. La valeur par défaut est 0.

histsize Définit le nombre de mots de passe antérieurs ne pouvant plus être réutilisés. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 20. Valable uniquement si on a `histexpire=0`. La valeur par défaut est 5.

loginretries Définit le nombre maximum de tentatives de connexion infructueuses, consécutives à une connexion établie, avant que l'accès au compte utilisateur ne soit bloqué. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 20. La valeur par défaut est 10. La valeur 0, ou une valeur négative, indique qu'aucune limite n'a été définie. Une fois le compte d'un utilisateur verrouillé, celui-ci ne pourra plus se connecter au réseau tant que l'administrateur système n'aura pas affecté la valeur "no" à `pwlocked`.

maxage Définit la durée de validité maximale (en semaines) d'un mot de passe. Le mot de passe doit être modifié au cours de cette période. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 52. La valeur 0 indique qu'aucune limite de validité n'a été définie. La valeur par défaut est 13.

maxexpired Définit le délai maximum (en semaines) pendant lequel un utilisateur peut encore modifier un mot de passe arrivé à expiration. Une fois ce délai écoulé, seul un administrateur pourra modifier le mot de passe. La valeur est un nombre entier. Les valeurs admises sont comprises entre -1 et 26. Si la valeur de maxexpired est 0, le mot de passe arrive à expiration lorsque la valeur de maxage est atteinte. Si la valeur de maxage est 0, l'attribut maxexpired est ignoré. La valeur par défaut est 3.

maxrepeats Définit le nombre maximum d'occurrences d'un même caractère dans un nouveau mot de passe. Les valeurs admises sont comprises entre 0 et 8, la valeur 0 étant sans effet. La valeur 8 indique qu'aucun maximum n'est imposé. La valeur par défaut est 2.

minalpha Définit le nombre minimum de caractères alphabétiques devant composer un nouveau mot de passe. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 8 ; la valeur 0 indique qu'aucun minimum n'est imposé. La valeur par défaut est 4.

mindiff Définit le nombre minimum de caractères inédits devant composer un nouveau mot de passe. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 8 ; la valeur 0 indique qu'aucun minimum n'est imposé. La valeur par défaut est 3.

minlen Définit la longueur maximale d'un mot de passe. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 8 ; la valeur 0 indique qu'aucun minimum n'est imposé. La valeur par défaut est 8.

minother Définit le nombre minimum de caractères non alphabétiques devant composer un nouveau mot de passe. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 8 ; la valeur 0 indique qu'aucun minimum n'est imposé. La valeur par défaut est 1.

pwdwarntime Définit le délai (en jours) devant s'écouler avant que le système ne demande à l'utilisateur de modifier son mot de passe. La valeur est un nombre entier. Les valeurs admises sont comprises entre 0 et 30. La valeur 0, ou une valeur négative, indique qu'aucun message ne sera émis. La valeur par défaut est 5.

Groupes de fonctions d'administration

fg_all Entrez "yes" si l'administrateur est autorisé à gérer le pare-feu dans tous ses aspects. La valeur par défaut est "no".

fg_dns Entrez "yes" si l'administrateur est autorisé à gérer les serveurs de noms de domaine. La valeur par défaut est "no".

fg_interfaces Entrez "yes" si l'administrateur est autorisé à définir des interfaces de pare-feu. La valeur par défaut est "no".

fg_logmonitor Entrez "yes" si l'administrateur est autorisé à gérer les seuils du contrôle de journalisation. La valeur par défaut est "no".

fg_logs Entrez "yes" si l'administrateur est autorisé à gérer les fonctions de journalisation. La valeur par défaut est "no".

fg_mail Entrez "yes" si l'administrateur est autorisé à gérer la passerelle de messagerie du pare-feu. La valeur par défaut est "no".

fg_netobjs1 Entrez "yes" si l'administrateur est autorisé à opérer des tâches de base sur les objets réseau. La valeur par défaut est "no".

fg_netobjs2 Entrez "yes" si l'administrateur est autorisé à opérer des tâches avancées sur les objets réseau. La valeur par défaut est "no".

fg_pagers Entrez "yes" si l'administrateur est autorisé à gérer la configuration du récepteur de messagerie. La valeur par défaut est "no".

fg_proxyserver Entrez "yes" si l'administrateur est autorisé à configurer les démons relais du pare-feu. La valeur par défaut est "no".

fg_traffic Entrez "yes" si l'administrateur est autorisé à gérer le contrôle des transactions. La valeur par défaut est "no".

fg_user Entrez "yes" si l'administrateur est autorisé à gérer les utilisateurs du pare-feu. La valeur par défaut est "no".

Pour afficher les attributs de tous les utilisateurs du pare-feu ou d'un utilisateur spécifique :

```
fwuser cmd=list
       [username=nom utilisateur]
       [type={short|long}]
```

type={short|long} Le type par défaut est "long" si vous utilisez un nom utilisateur. Dans le cas contraire, la valeur par défaut est "short" (nom court).

Pour supprimer un utilisateur du pare-feu :

```
fwuser cmd=delete
       username=nom utilisateur
```

Chapitre 2. Emploi des utilitaires de génération d'états

Cette section aborde l'emploi des utilitaires de génération d'états d'IBM Firewall. La vocation première des utilitaires de génération d'états est de produire des fichiers sous forme de tableaux contenant des informations d'ordre administratif à partir des fichiers du `journal de pare-feu`.

En outre, des fichiers texte sous forme de tableaux peuvent être générés et importés dans les tables d'un système de gestion de base de données comme DB2/6000 ou DB2/2 . L'administrateur peut ensuite utiliser le langage SQL (Structured Query Language) pour lancer des requêtes et générer des états. Les utilitaires permettent également de créer un fichier texte parfaitement lisible à partir des messages du journal de pare-feu.

Les utilitaires de génération d'états se composent des programmes et fichiers suivants :

fwlogtxt Programme permettant de générer des messages textuels à partir d'un fichier journal du pare-feu.

fwlogtbl Programme permettant de générer des fichiers de base de données au format DEL (délimité) à partir d'un fichier journal de pare-feu et d'un fichier journal su.

Pour utiliser le programme fwlogtbl et les fichiers DDL, DML et DEL, vous devez connaître le fonctionnement des bases de données relationnelles en général et en employer une en particulier.

fwschema.ddl Fichier d'instructions DDL (Data Definition Language) SQL permettant de définir les tables de la base de données.

fwimport.dat Fichiers d'instructions d'importation DB2 permettant d'importer les fichiers DEL dans les tables de la base de données.

fwqrysmp.dml Fichier d'instructions DML (Data Manipulation Language) SQL permettant de générer des états types.

fwlogcvrt Programme de conversion des journaux de pare-feu Windows NT au format des journaux de pare-feu AIX. Cette fonction permet d'utiliser d'autres programmes de génération d'états, comme précédemment, sachant que les nouveaux messages peuvent ne pas être reconnus.

Les fichiers DDL et DML sont prévus pour les produits DB2 mais peuvent être adaptés à d'autres systèmes de gestion de base de données. Les fichiers DEL peuvent être importés (chargés) tels quels dans DB2/6000, DB2/2 et autres bases de données et systèmes de fichiers. Leur format conventionnel permet leur conversion dans d'autres formats si nécessaire.

Emploi des utilitaires de génération d'états

Cette section détaille l'emploi des utilitaires de génération d'états avec la ligne de commande. Reportez-vous au *guide de l'utilisateur d'IBM eNetwork Firewall* pour plus d'informations sur l'emploi des utilitaires de génération d'états à partir du programme client de configuration.

Pour visualiser le fichier journal du pare-feu à partir de la ligne de commande, employez l'utilitaire **fwlogtxt**. Pour plus d'informations, consultez la section «Création de messages à partir du fichier journal du pare-feu», à la page 25.

Pour générer des états à partir des données du fichier journal :

1. Installez la base de données relationnelles.
2. Créez une base de données vide.
3. Créez des tables de fichier journal de pare-feu vides dans la base de données.
4. Pour générer des fichiers sous forme de tableaux, tapez la commande **fwlogtbl** sur la ligne de commande.
5. Importez ensuite les données des fichiers créés dans les tables de la base de données.
6. Créez les états avec des instructions SQL ou des programmes SQL.

Remarque : Les trois premières étapes n'ont lieu qu'une seule fois. Les suivantes se répètent chaque fois qu'arrivent de nouvelles données de fichier journal.

Format du fichier journal d'IBM Firewall

Les entrées du fichier journal du pare-feu ont le format suivant :

```
date heure nom_pare-feu:année;PID:Anum_msg;
ID_msg;var_1;...;var_n;
```

où

- Les valeurs des trois premières zones, **date, heure et nom du pare-feu** sont ajoutées par la fonction de journal de pare-feu.
- **année** est une année à quatre chiffres.
- **PID** est l'ID de l'unité d'exécution à laquelle l'entrée s'applique.
- **Anum_msg** est un nombre entier séquentiel utilisé par les utilitaires de génération d'états pour accéder au texte converti du message approprié dans le fichier fw_log.cat. Le paramètre numérique num_msg est immédiatement précédé d'un indicateur de niveau de journalisation (lettre A). Cet indicateur caractérise à la fois la plate-forme d'où vient le fichier journal et les différences éventuelles de format de journal.
- **ID_msg** est le code externe du message (par exemple ICA0001e).
- **var_1-n** et les autres variables du même type sont les valeurs des variables du message, **n** correspondant au nombre de variables contenues dans la définition du message.

Remarque : Ne dirigez aucun autre enregistrement vers le fichier utilisé comme fichier journal du pare-feu. Ces enregistrements n'ont pas le format requis par les utilitaires de génération d'états et les résultats sont incertains.

Utilisez la commande `fwlogcvrt` pour passer du format de journal Windows NT au format de journal AIX. Cette opération peut s'avérer nécessaire si vous désirez utiliser des outils de génération d'états non IBM capables de traiter les fichiers journaux au format IBM Firewall pour AIX. La conversion de format supprimera

l'indicateur de niveau de journalisation 'A' précédant le paramètre num_msg et insérera deux espaces autour du signe ':' séparant le nom du pare-feu de l'année.

Les paramètres sont les suivants :

entrée Entrée standard redirigée depuis un journal de pare-feu Windows NT.

sortie Sortie standard pouvant être redirigée vers un fichier.

Syntaxe de la commande fwlogcvrt

```
fwlogcvrt
```

Exemple :

```
fwlogcvrt < fw980212.log >logcvrt.out
```

Création de messages à partir du fichier journal du pare-feu

Utilisez la commande **fwlogtxt** pour générer des messages lisibles à partir des entrées d'un fichier journal de pare-feu.

Les paramètres de cette commande sont les suivants :

entrée Entrée standard provenant d'un fichier journal de pare-feu

sortie Sortie standard

Syntaxe de la commande fwlogtxt

```
fwlogtxt
```

Exemple :

```
fwlogtxt < fw980212.log >logtxt.out
fwlogtxt < my.log | find "ICA0"
```

La commande fwlogtxt ne requiert aucun paramètre ; les informations proviennent de l'entrée standard et les résultats sont générés en sortie standard.

Création de fichiers de base de données

Utilisez la commande **fwlogtbl** pour créer, insérer ou annexer des données aux fichiers sous forme de tableaux qui serviront à remplir les tables de la base de données en vue d'établir des états.

Les paramètres de cette commande sont les suivants :

entrée Journal de pare-feu.

sortie Noms de fichier :

a_alert.tbl
f_rule.tbl
f_info.tbl
f_match.tbl
f_stat.tbl
interfaces.tbl
nat_info.tbl

p_info.tbl
p_ftp.tbl
p_http.tbl
p_info.tbl
p_login.tbl
p_stat.tbl
server_info.tbl
session.tbl
s_ftp.tbl
s_info.tbl
ssl_info.tbl

Syntaxe de la commande fwlogtbl

```
fwlogtbl  -w [-d rép_sortie] [-su]nom_journal
           ‘
          -a
```

Exemple :

```
fwlogtbl -a  -d :c\reports fw961031.log
```

-w Indique que le fichier de sortie existant doit être remplacé. Si le fichier n'existe pas, fwlogtbl le crée.

-a Indique que le fichier généré doit être annexé au fichier de sortie existant. Si le fichier n'existe pas, fwlogtbl le crée.

-d Désigne le répertoire de sortie.

rép_sortie Indique dans quel répertoire stocker les fichiers de sortie. A défaut de spécification, les fichiers de sortie iront dans le répertoire courant.

-su Indique que le nom de fichier journal est celui d'un fichier journal AIX su. Le pare-feu Windows NT peut traiter aussi bien les fichiers journaux de pare-feu que les fichiers journaux SU créés sous des versions antérieures d'IBM Firewall pour AIX.

nom_journal Désigne un fichier journal de pare-feu ou un fichier journal AIX SU.

Les noms des fichiers de sortie sont prédéfinis mais peuvent être copiés ou renommés après l'exécution de la commande fwlogtbl. Les fichiers de sortie sont au format ASCII délimité (DEL), ne comportent pas de délimiteurs de chaînes de caractères et utilisent le point virgule comme délimiteur de colonne.

Pour plus d'informations sur les messages, reportez-vous à l'Annexe A, «Messages», à la page 75 .

Utilisation d'une base de données avec les utilitaires de génération d'états

Cette section décrit les fichiers fournis avec le pare-feu en vue de créer la base de données, d'y importer les données et de générer des états. Si vous disposez de DB2, vous pouvez utiliser la commande db2 avec ces fichiers. (Des fonctions semblables à la commande db2 peuvent exister avec d'autres systèmes de gestion de base de données. Les fichiers nécessitent alors des modifications pour être utilisés avec ces fonctions).

Pour exécuter la commande db2, DB2 doit être installé et une 'instance' doit être déjà définie. Reportez-vous au guide d'installation de DB2. Au départ, utilisez la commande DB2 appropriée pour créer une base de données vide (vous pourrez l'appeler 'fwlog' par exemple). Pour ce faire, tapez la commande suivante sur la ligne de commande :

```
db2cmd
```

Dans la fenêtre de commande DB2 qui s'ouvre, tapez ensuite :

```
db2 create database fwlog
```

Vous devez ensuite relier la base de données fwlog :

```
db2 connect to fwlog
```

Les options -vf de la commande db2 peuvent être utilisées de la manière suivante :

```
              db2 -vf fwschema.ddl > schema.out
db2 -vf fwimport.dat > import.out
              db2 -vf fwqrysmp.dml > report.out
```

Ces étapes sont détaillées dans les sections suivantes. Dans chaque cas, l'utilisateur doit contrôler soigneusement la sortie standard (redirigée vers un fichier dans chacun de ces exemples). Pour l'importation, il est également nécessaire de contrôler le fichier .msg généré par chacune des instructions d'importation.

Création des tables

La commande **db2 -vf fwschema.ddl > schema.out** génère toutes les tables et les index nécessaires. Elle ne doit être exécutée qu'une seule fois, de préférence peu de temps après l'installation du pare-feu. L'ID affecté au créateur des tables sera l'ID utilisateur courant. Cet ID sera parfois utilisé comme qualificateur de nom de table (par exemple IDcréateur.NomTable), notamment avec des instructions SQL lancées par d'autres utilisateurs que le créateur. A défaut d'utiliser l'ID créateur, l'utilisateur devra modifier les fichiers fwimport.dat et fwqrysmp.dml pour insérer cet ID devant chaque nom de table.

Le fichier `ROOTDIR\sample\report\fwschema.ddl`, contient les instructions DDL servant à créer les tables de base de données devant recueillir les enregistrements issus des fichiers sous forme de tableaux créés par la commande **fwlogtbl**. *ROOTDIR* est le répertoire sélectionné pendant la procédure d'installation comme emplacement de destination pour IBM Firewall. Prenez le temps d'examiner le fichier schema.out pour vérifier la réussite de l'opération. Les instructions du fichier `fwschema.ddl` peuvent être utilisées telles quelles ou être adaptées à différents systèmes de gestion de base de données. (Notez que les noms des colonnes et des tables ne doivent pas être modifiés).

Importation des données

La commande**db2 –vf fwimport.dat > import.out** charge les données de tous les fichiers DEL dans les tables générées par la commande **db2-vf fwschema.ddl**.

Le fichier `ROOTDIR\sample\report\fwimport.dat` contient des instructions types permettant d'importer les données depuis les fichiers *.tbl vers la base de données DB2. Comme déjà mentionné dans la section «Création des tables», si les tables sont importées par un utilisateur autre que leur créateur, l'ID de ce créateur doit être inséré devant chaque nom de table.

Chaque instruction d'importation génère des données en sortie standard et enregistre d'autres données dans un fichier `tblname.msg` (un fichier tblname spécifique par instruction d'importation). L'utilisateur doit contrôler ces deux types de sortie pour s'assurer de l'aboutissement de l'importation. Si l'utilisateur exécute toutes les instructions de ce fichier avec un programme tel que DB2, il devra diriger la sortie standard vers un fichier, la contrôler puis vérifier chacun des fichiers .msg. Chaque commande d'importation génère un fichier .msg distinct. L'utilisateur devra relancer la commande **db2 –vf fwimport.dat > import.out** pour chaque nouveau fichier journal à répercuter dans la base de données.

Lors de l'importation de fichiers journaux volumineux, des codes d'erreur SQL pourront s'afficher, signalant un besoin supplémentaire en mémoire ou en espace disque. Ainsi vous pourrez voir s'afficher des messages signalant une `mémoire insuffisante` ou un `espace de journalisation des transactions insuffisant`. Ces messages doivent être suivis d'une modification des paramètres du système de gestion de base de données utilisé ou de la base de données fwlog. Reportez-vous à la documentation de DB2 pour plus d'informations. Alternative temporaire à la modification des paramètres de DB2, vous pouvez aussi décomposer les fichiers journaux ou les fichiers sous forme de tableaux volumineux en fichiers plus réduits.

Exécution des requêtes types

La commande **db2 -vf fwqrysmp.dml > report.out** exécute les requêtes types. Le fichier `ROOTDIR:\sample\report\fwqrysmp.dml` contient des instructions SQL types produisant des états sur la base de conditions de requêtes. Vous pouvez partir de ces exemples pour créer vos propres états. Comme déjà mentionné dans la section «Création des tables», à la page 27, si les tables sont importées par un utilisateur autre que leur créateur, l'ID de ce créateur doit être inséré devant chaque nom de table.

Lorsque l'utilisateur lance ses requêtes depuis la ligne de commande, DB2 alloue l'espace mémoire maximum requis pour chacune des colonnes de sortie. Les états ainsi générés sont parfois d'une lecture délicate. Vous obtiendrez des résultats plus satisfaisants en demandant moins de colonnes dans chaque requête ou en regroupant les instructions de requête dans un programme qui vous permettra de mieux contrôler la présentation de la sortie.

Utilitaires de génération d'états et interface utilisateur

Les utilitaires de génération d'états sont installés en même temps que le pare-feu. Il peuvent cependant être installés séparément et exécutés sur un hôte non utilisé comme pare-feu. Le client de configuration ou la commande `fwlogtbl` permettent de les exécuter sur un pare-feu. Sur un hôte non pare-feu, utilisez la ligne de commande.

Tables SQL

Cette section détaille l'organisation des tables SQL.

Chaque message de fichier journal de pare-feu ou message de fichier journal AIX su est associé à l'une des tables SQL suivantes :

```
ADMIN_ALERT
FILTER_INFO
FILTER_MATCH
FILTER_ACTIVE_RULE
FILTER_STATUS
INTERFACES
NAT_INFO
PAGER_INFO
PROXY_FTP
PROXY_HTTP
PROXY_INFO
PROXY_LOGIN
PROXY_STATUS
SERVER_INFO
SESSION
SOCKS_FTP
SOCKS_INFO
SSL_INFO
SU
TUNNEL_CONTEXT
TUNNEL_POLICY
TUNNEL_STATUS
```

Ne modifiez pas les noms des tables ni ceux des colonnes. Vous pouvez par contre augmenter la largeur d'une colonne de caractères si les valeurs qu'elle contient sont tronquées.

Index

Un enregistrement de fichier journal rattaché à un événement de pare-feu déterminé ne doit apparaître qu'une seule fois dans la base de données. Si un administrateur importe plusieurs fois un même fichier sous forme de tableaux, ou si un autre fichier sous forme de tableaux issu du même fichier journal est importé, un enregistrement de fichier journal peut apparaître plusieurs fois.

Pour éviter ce problème, vous disposez d'un fichier d'exemple de définition de base de données, fwschema.dll, qui définit un unique index sur chacune des tables à l'aide des trois zones suivantes :

- Le nom de fichier du fichier journal source de l'enregistrement (LOG_FILE) ;
- Le numéro de ligne de l'enregistrement dans le fichier journal (LINE_NUM) ;
- Le nombre d'occurrences de la ligne, sur la base du message syslog 'dernier message répété n fois' (REPEAT_NUM).

Cet index vous empêche de charger plusieurs fois le même numéro de ligne du fichier désigné. Cette mesure, appuyée par une gestion adéquate des noms des fichiers journaux, doit permettre d'éviter la duplication des événements dans votre base de données.

Le fait d'ajouter d'autres index ne peut qu'accroître les performances des requêtes les plus courantes. Reportez-vous à la documentation de votre base de données pour plus d'informations.

Descriptions des tables

Cette section explique la relation unissant les messages des fichiers journaux du pare-feu aux tables et aux colonnes, et détaille les informations susceptibles d'être demandées pour générer des états. Tous les messages associés à une table donnée sont répertoriés dans une annexe apparaissant en fin de table. Les messages fournissant les données des colonnes sont répertoriés dans les descriptions de ces colonnes. Les tables contiennent des messages prévus pour IBM Firewall pour AIX, IBM Firewall pour Windows NT et des messages communs aux deux types de pare-feu.

Pour plus d'informations sur les messages des fichiers journaux de pare-feu, reportez-vous à l'Annexe A, «Messages», à la page 75.

Dans les descriptions qui suivent, la mention 'entier' apparaissant dans la colonne Type de données fait référence au type de colonne DB2 SMALLINT tandis que la mention 'entier long' correspond au type DB2 INTEGER. Le type de données date-heure fait référence au type DB2 TIMESTAMP (horodate). Notez que la valeur des microsecondes donnée par l'horodate sera toujours "000000".

Si une description est signalée *obligatoire*, une valeur doit être indiquée pour accéder à l'enregistrement correspondant de la table.

Les trois colonnes servant d'unique index et la colonne prévue pour l'indicateur de niveau de journalisation n'apparaissent pas dans ces descriptions de table car leurs définitions sont identiques et elles ne font en général pas l'objet de requête.

Tableau 1 (page 1 de 2). ADMIN_ALERT. Cette table contient des messages rattachés à des alertes d'intrusion, issus du fichier a_alert.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (ICA0001, ICA0002, ICA0003, ICA0004, ICA2001, ICA2002, ICA2003, ICA2026, ICA2043, ICA2068, ICA2167, ICA2168, ICA 2170, ICA2173, ICA3001, ICA3012, ICA3018)
ACTION	caractères (7)	connect (ICA3012) ou bind (ICA3018)
NUM_COUNT	entier	Nombre d'échecs d'authentification (ICA0001, ICA0002, ICA0003) ; nombre d'entrées de journal pour TAG_MSG_NUM (ICA0004) ; nombre de jours (ICA9000)
TAG_MSG_NUM	caractères (8)	Numéro de code du message (ICA0004)
SRC_IP	caractères (15)	Adresse IP source (ICA2001, ICA2028, ICA2079, ICA2167, ICA3012, ICA3018)

Tableau 1 (page 2 de 2). ADMIN_ALERT. Cette table contient des messages rattachés à des alertes d'intrusion, issus du fichier a_alert.tbl.

Colonne	Type de données	Description
DST_IP	caractères (15)	Adresse IP de destination (ICA2001, ICA2028, ICA2079, ICA3012, ICA3018)
AUTH_METHOD	caractères (20)	Méthode d'authentification (ICA2002, ICA2167, ICA2170)
NETWORK	caractères (25)	Nom de réseau (ICA2001, ICA2002, ICA2167)
HOST_NAME	caractères (100)	Nom d'hôte (ICA0003, ICA2002)
TIMEOUT_SEC	entier	Délai d'expiration en secondes (ICA2026)
CONN_USERID	caractères (16)	Nom utilisateur de connexion Socks (ICA3001)
APPLICATION	caractères (30)	Nom d'une application telle que Telnet, FTP, ... (ICA2167, ICA2168, ICA2170, ICA3012)
Remarque : Messages rattachés : ICA0001 ICA0002 ICA0003 ICA0004 ICA0005 ICA0006 ICA0007 ICA0008 ICA0009 ICA0010 ICA0011 ICA0012 ICA0013 ICA0014 ICA0015 ICA0016 ICA0017 ICA0018 ICA0019 ICA0020 ICA0021 ICA0022 ICA1010 ICA2001 ICA2002 ICA2003 ICA2020 ICA2026 ICA2028 ICA2037 ICA2040 ICA2042 ICA2043 ICA2079 ICA2167 ICA2168 ICA2170 ICA2173 ICA3001 ICA3012 ICA3018 ICA9000 ICA9001		

Tableau 2. FILTER_ACTIVE_RULE. Cette table contient les règles de filtrage actives contenues dans le fichier f_rule.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
RULE_NUM	entier	Numéro de règle (obligatoire)
RULE	caractères (150)	Règle (obligatoire)
Remarque : Message rattaché : ICA1037		

Tableau 3 (page 1 de 2). FILTER_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés aux filtres, contenus dans le fichier f_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)

Tableau 3 (page 2 de 2). FILTER_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés aux filtres, contenus dans le fichier f_info.tbl.

Colonne	Type de données	Description
MSG_NUM	entier	Numéro de message (obligatoire)
RULE_NUM	entier	Numéro de règle de filtrage (ICA1005)
ERROR_NUM	entier	Code d'erreur système : code d'erreur AIX ou dernière erreur Windows NT (ICA1007, ICA1008, ICA1009, ICA1011 ICA1013, ICA1015, ICA1021, ICA1023, ICA1024) Le texte associé à chaque code d'erreur peut être obtenu par le biais de la fonction _strerror. Le texte associé à la dernière erreur Windows NT peut être obtenu par le biais de la fonction de formatage des messages ou dans l'annexe A du Manuel de référence du programmeur Win32, volume 2.
LOAD_PATH	caractères (100)	Chemin de chargement de l'extension noyau (ICA1011, ICA1012)
DVC_DRV	caractères (25)	Pilote de périphérique (ICA1021)
TERM_SIG	caractères (25)	Signal de fin (ICA1260)
FILE_NAME	caractères (100)	Nom de fichier (ICA1024)
RC	entier	Code retour interne au pare-feu (ICA1019)
Remarque : Messages rattachés : ICA1001 ICA1002 ICA1003 ICA1005 ICA1007 ICA1008 ICA1009 ICA1011 ICA1012 ICA1013 ICA1014 ICA1015 ICA1016 ICA1017 ICA1019 ICA1021 ICA1022 ICA1023 ICA1024 ICA1200 ICA1260		

Tableau 4 (page 1 de 2). FILTER_MATCH. Cette table contient les règles de filtrage satisfaites contenues dans le fichier f_match.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
RULE_NUM	entier	Numéro de règle (obligatoire)
ACTION	caractères (6)	Type de règle : Autorisation, Interdiction, etc.
DIRECTION	caractères (8)	Direction du paquet : entrant ou sortant (obligatoire).
SRC_IP	caractères (15)	Adresse IP de l'émetteur (obligatoire)
DST_IP	caractères (15)	Adresse IP du destinataire (obligatoire)

Tableau 4 (page 2 de 2). FILTER_MATCH. Cette table contient les règles de filtrage satisfaites contenues dans le fichier f_match.tbl.

Colonne	Type de données	Description
PROTOCOL	caractères (7)	Protocole haut niveau tel que UDP, IPIP, ICMP, TCP ou TCP/ACK (obligatoire)
SRC_PORT	entier	• Type de paquet IP pour ICMP • Numéro de port du protocole de ressource pour les autres (obligatoire)
DST_PORT	entier	• Code de paquet IP pour ICMP • Numéro de port du protocole de destination pour les autres (obligatoire)
ROUTING	caractères (5)	Mode de routage des paquets : routage ou local (obligatoire)
INTERFACE	caractères (10)	Type d'interface : sécurisée ou non sécurisée (obligatoire)
FRAGMENT	caractères (8)	Indique si le paquet est fragmenté ou non (obligatoire)
TUNNEL_ID	entier	ID de tunnel (obligatoire)
ENCRYPTION	caractères (7)	Algorithme de chiffrement : DES_CBC ou CDMF ou aucun
BYTES	entier long	Longueur du paquet (obligatoire)
Remarque : Message rattaché : ICA1036		

Tableau 5 (page 1 de 2). FILTER_STATUS. Cette table contient des informations sur les changements de statut des filtres, issues du fichier f_stat.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
DAEMON	caractères (25)	Démon de journalisation des filtres AIX (ICA1004), ou service de journalisation des filtres Windows NT.
VERSION	entier	Numéro de version (ICA1004, ICA1033)
RELEASE	entier	Numéro d'édition (ICA1004, ICA1033)
PACKET_LOGGING	caractères (8)	Statut de la journalisation de paquets - activé ou désactivé (ICA1035)

Tableau 5 (page 2 de 2). FILTER_STATUS. Cette table contient des informations sur les changements de statut des filtres, issues du fichier f_stat.tbl.

Colonne	Type de données	Description
Remarque : Messages rattachés : ICA1004 ICA1032 ICA1033 ICA1034 ICA1035. Le détail des mises à jour des règles de filtrage (ICA1032) peut être obtenu dans la table FILTER_ACTIVE_RULE.		

Tableau 6. INTERFACES. Cette table contient des informations relatives aux messages de configuration des interfaces (cartes), issues du fichier interface.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
IP	caractères (15)	Adresse IP de la carte (ICA9038, ICA9039, ICA9040)
OLD_MASK	caractères (15)	Ancienne valeur de masque (ICA9040)
NEW_MASK	caractères (15)	Nouvelle valeur de masque (ICA9040)
Remarque : Messages rattachés : ICA9037, ICA9038, ICA9039, ICA9040, ICA9041		

Tableau 7. NAT_INFO. Cette table contient les données des messages de conversion d'adresse réseau (NAT), issues du fichier nat_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
VERSION	entier	Numéro de version NAT (ICA9033)
RELEASE	entier	Numéro d'édition NAT (ICA9033)
IP	caractères (15)	Adresse IP (ICA9035, ICA9036)
Remarque : Messages rattachés : ICA9032, ICA9033, ICA9034, ICA9035, ICA9036		

Tableau 8. PAGER_INFO. Cette table contient des informations rattachées aux fonctions de messagerie du pare-feu, issues du fichier pgr_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (ICA4036, ICA4174, ICA4175)
ERROR_NUM	entier	Code d'erreur système - code d'erreur AIX ou dernière erreur Windows NT (ICA4371)
PROGRAM	caractères (25)	Nom de programme (ICA4000)
SIGNAL	entier	Signal de fin (ICA4000)
ID	entier	Identificateur (ICA4036)
PRIORITY	entier	Niveau de priorité (ICA4036)
PERIOD	entier	Période (ICA4036)
RETRY_COUNT	entier	Nombre de tentatives (ICA4036, ICA4313, ICA4314, ICA4364, ICA4365)
FROM_ENTRY	caractères (15)	Nom de fonction (ICA4036)
HOST_NAME	caractères (100)	Nom d'hôte (ICA4174, ICA4175)
MESSAGE_TEXT	caractères (250)	Texte du message (ICA4036, ICA4353 - 4360, ICA4368, ICA4372)
SERVICE	caractères (25)	Nom de service (ICA4017)
SOCKET	entier	Numéro de socket (ICA4017)
FILENAME	caractères (100)	Nom de fichier (ICA4154, ICA4351, ICA4352)
Remarque : Messages rattachés : ICA4000 ICA4001 ICA4007 ICA4017 ICA4036 ICA4154 ICA4168 ICA4174 ICA4175, ICA4300 - 4303, ICA4305 - 4315, ICA4351 - 4360, ICA4362 - 4372)		

Tableau 9 (page 1 de 2). PROXY_FTP. Cette table contient des informations rattachées aux actions FTP des sessions FTP, issues du fichier p_ftp.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (obligatoire)

Tableau 9 (page 2 de 2). PROXY_FTP. Cette table contient des informations rattachées aux actions FTP des sessions FTP, issues du fichier p_ftp.tbl.

Colonne	Type de données	Description
SRC_IP	caractères (15)	Adresse IP de l'utilisateur (obligatoire)
DST_IP	caractères (15)	Adresse IP de la machine distante (obligatoire)
ACTION	caractères (5)	Action de transfert de fichier : PUT ou GET (obligatoire)
FILE_NAME	caractères (100)	Nom de fichier
BYTES	entier long	Quantité de données transmises
SID	entier long	ID de session unique (obligatoire)
Remarque : Message rattaché : ICA2075		

Tableau 10. PROXY_HTTP. Cette table contient des informations rattachées aux actions des sessions relais, issues du fichier p_http.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
STATUS	entier	Statut (obligatoire)
SRC_IP	caractères (15)	Adresse IP de l'utilisateur (obligatoire)
REQUEST	caractères (250)	Contenu de la requête HTTP (obligatoire)
BYTES	entier long	Quantité de données transmises
Remarque : Message rattaché : ICA2099		

Tableau 11 (page 1 de 3). PROXY_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés au serveur relais, issus du fichier p_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (ICA2018, ICA2019, ICA2057, ICA2058, ICA2166, ICA2177, ICA2172)

Tableau 11 (page 2 de 3). PROXY_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés au serveur relais, issus du fichier p_info.tbl.

Colonne	Type de données	Description
ERROR_NUM	entier	Code d'erreur système - code d'erreur AIX ou dernière erreur Windows NT (ICA2005, ICA2006, ICA2009, ICA2029, ICA2035, ICA2038, ICA2039, ICA2052, ICA2054, ICA2055, ICA2056, ICA2057, ICA2058, ICA2059, ICA2063, ICA2064, ICA2065, ICA2066, ICA2067, ICA2068, ICA2069, ICA2069, ICA2070, ICA2071, ICA2074, ICA2110, ICA2111, ICA2113, ICA2114, ICA2115, ICA2118, ICA2119, ICA2121, ICA2122, ICA2123, ICA2124, ICA2200, ICA2201, ICA2202, ICA2203) Les textes rattachés aux différents codes d'erreur (erreurs système AIX) peuvent être obtenus par le biais de la fonction _strerror. Le texte associé à la dernière erreur Windows NT peut être obtenu par le biais de la fonction de formatage des messages ou dans l'annexe A du Manuel de référence du programmeur Win32, volume 2.
OPTION_VAL	caractères (20)	Attribut d'option ou valeur de paramètre (ICA2014, ICA2015, ICA2049, ICA2050)
TIME	caractères (15)	Délai incorrect (ICA2044, ICA2202)
RC	entier	Code retour interne au pare-feu (ICA2007, ICA2030, ICA2031, ICA2033, ICA2034, ICA2054, ICA2057, ICA2058, ICA2065, ICA2120 ICA2166, ICA2203)
INVOC_NAME	caractères (20)	Nom d'appel utilisé pour la socket ou le port au moment de l'erreur système (ICA2055, ICA2056)
AUDIT_TYPE	caractères (7)	Type d'audit inconnu (7 valeurs hexadécimales) (ICA2004)
HOST_NAME	caractères (100)	Nom d'hôte (ICA2106, ICA2107, ICA2126)
FILE_NAME	caractères (100)	Nom de fichier (ICA2029, ICA2030, ICA2072, ICA2183, ICA2204, ICA2205, ICA2206, ICA2207)
LINE_NUM	entier	Numéro de ligne (ICA2029, ICA2030)
PROTOCOL	caractères (25)	Nom de protocole incorrect (ICA2112, ICA2116)
CUSTOMIZED_ATTR	caractères (25)	Numéro de ligne (ICA2105, ICA2106, ICA2125, ICA2166)
ODM_ERR_NUM	entier	Code d'erreur issu de l'ODM (ICA2102, ICA2103, ICA2104, ICA2105, ICA2107, ICA2108, ICA2109,ICA2125)
APPLICATION (NT uniquement)	caractères (30)	Nom d'application (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)
CALLER (NT uniquement)	caractères (25)	Fonction émettant l'appel (ICA2200, ICA2201, ICA2202, ICA2203, ICA2204, ICA2205, ICA2206, ICA2207)

Tableau 11 (page 3 de 3). PROXY_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés au serveur relais, issus du fichier p_info.tbl.

Colonne	Type de données	Description
FAILED_IN (NT uniquement)	caractères (25)	Fonction ayant échoué (ICA2201, ICA2203)

Remarque : Messages rattachés : ICA2004 ICA2005 ICA2006 ICA2007 ICA2009 ICA2014 ICA2015 ICA2018 ICA2019 ICA2023 ICA2029 ICA2030 ICA2031 ICA2032 ICA2033 ICA2034 ICA2035 ICA2038 ICA2039 ICA2044 ICA2045 ICA2046 ICA2047 ICA2048 ICA2049 ICA2050 ICA2051 ICA2052 ICA2053 ICA2054 ICA2055 ICA2056 ICA2057 ICA2058 ICA2059 ICA2060 ICA2061 ICA2062 ICA2063 ICA2064 ICA2065 ICA2066 ICA2067 ICA2068 ICA2069 ICA2070 ICA2071 ICA2072 ICA2073 ICA2074 ICA2100 ICA2102 ICA2103 ICA2104 ICA2105 ICA2109 ICA2110 ICA2111 ICA2112 ICA2113 ICA2114 ICA2115 ICA2116 ICA2117 ICA2118 ICA2119 ICA2120 ICA2121 ICA2122 ICA2123 ICA2124 ICA2125 ICA2126 ICA2127 ICA2166 ICA2171 ICA2172 ICA2183 ICA2200 ICA2201 ICA2202 ICA2203 ICA2204 ICA2205 ICA2206 ICA2207

Tableau 12. PROXY_LOGIN. Cette table contient des informations (essentiellement en rapport avec l'authentification) rattachées aux connexions relais établies, issues du fichier p_login.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (obligatoire)
APPLICATION	caractères (30)	Nom d'application : Telnet, FTP, ... (obligatoire)
AUTH_METHOD	caractères (15)	Méthode d'authentification (obligatoire)
NETWORK	caractères (25)	Réseau (sécurisé/non sécurisé et autres informations le cas échéant) (obligatoire)
HOST_NAME	caractères (100)	Nom d'hôte (obligatoire)

Remarque : Messages rattachés : ICA2024 ICA2025 ICA2169

Tableau 13 (page 1 de 2). PROXY_STATUS. Cette table contient des informations relatives au statut du serveur relais, issues du fichier p_stat.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)

Tableau 13 (page 2 de 2). PROXY_STATUS. Cette table contient des informations relatives au statut du serveur relais, issues du fichier p_stat.tbl.

Colonne	Type de données	Description
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (ICA2008, ICA2016, ICA2021)
SRC_IP	caractères (15)	Adresse IP source (ICA2000, ICA2008, ICA2010, ICA2011, ICA2012, ICA2013, ICA2141, ICA2180)
DST_IP	caractères (15)	Adresse IP de destination (ICA2000, ICA2010, ICA2011, ICA2012, ICA2013)
REMOTE_HOST	caractères (100)	Nom de l'hôte distant (au niveau de la machine pare-feu) (ICA2021, ICA2022, ICA2027)
SID (NT uniquement)	entier	ID de session (ICA2177, ICA2180, ICA2181 ICA2182)
SOCKET (NT uniquement)	caractères (25)	Nom de socket (ICA2177)
RC (NT uniquement)	entier	Code retour ou code raison (ICA2181, ICA2182)
CMD (NT uniquement)	caractères (36)	Carte SMTP (ICA2182)
Remarque : Messages rattachés : ICA2000 ICA2010 ICA2011 ICA2012 ICA2013 ICA2016 ICA2021 ICA2022 ICA2027 ICA2097 ICA2098 ICA2141 ICA2163 ICA2164 ICA2165 ICA2177 ICA2180 ICA2181 ICA2182		

Tableau 14. SERVER_INFO. Cette table contient des informations relatives au statut et à l'activité du serveur de configuration, issues du fichier srv_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (ICA9003, ICA9004)
ERROR_NUM	entier	Code d'erreur système - code d'erreur AIX ou dernière erreur Windows NT (ICA9008, ICA9009) Les textes rattachés aux différents codes d'erreur (erreurs système AIX) peuvent être obtenus par le biais de la fonction strerror. Le texte associé à la dernière erreur Windows NT peut être obtenu par le biais de la fonction de formatage des messages ou dans l'annexe A du Manuel de référence du programmeur Win32, volume 2.
Remarque : Messages rattachés : ICA9003 ICA9004 ICA9005 ICA9006 ICA9007 ICA9008 ICA9009 ICA9010 ICA9011 ICA9012 ICA9013 ICA9014 ICA9015		

Tableau 15. SESSION. Cette table contient des informations relatives aux démarrages/arrêts de sessions SOCKS et PROXY, issues du fichier session.tbl.

Colonne	Type de données (longueur)	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (obligatoire)
SERVICE_TYPE	caractères (10)	Type de serveur : 'Socks' ou 'proxy' (relais) (obligatoire)
APPLICATION	caractères (30)	Nom d'application : Telnet, FTP, ... (obligatoire)
SRC_IP	caractères (15)	Adresse IP de l'utilisateur (obligatoire)
DST_IP	caractères (15)	Adresse IP de la machine distante (obligatoire)
SESSION_EVENT	caractères (5)	• 'begin' lorsqu'une session est établie. • 'end' lorsqu'une session s'arrête. (obligatoire)
BYTES	entier long	Quantité de données transmises au cours de la session. La valeur est 0 pour toute application Telnet.
SID	entier long	Identificateur de session unique généré par le pare-feu sur la base de l'heure interne.

Remarque :

Messages rattachés :

- Démarrage de session Safemail : ICA2178 ;
- Arrêt de session Safemail : ICA2179 ;
- Démarrage de la session Socks : ICA3011 ;
- Arrêt de la session Socks : ICA3015 ;
- Démarrage de la session Telnet relais : ICA2036 (journaux AIX) ICA2208, ICA2218 (journaux NT) ;
- Arrêt de la session Telnet relais : ICA2077 (journaux AIX) ICA2209, ICA2219 (journaux NT) ;
- Démarrage de la session FTP relais : ICA2041 (journaux AIX) ICA2208, ICA2218 (journaux NT) ;
- Arrêt de la session FTP relais : ICA2076 (journaux AIX et NT).

Le détail des actions intervenues au cours des sessions Socks FTP se trouve dans la table SOCKS_FTP. Le détail des actions intervenues au cours des sessions FTP relais se trouve dans la table PROXY_FTP.

Tableau 16. SOCKS_FTP. Cette table contient des informations relatives aux actions SOCKS FTP intervenues au cours des sessions FTP, issues du fichier s_ftp.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (obligatoire)
SRC_IP	caractères (15)	Adresse IP de l'utilisateur (obligatoire)
DST_IP	caractères (15)	Adresse IP de la machine distante (obligatoire)
DATA_BIND	caractères (5)	• 'start' lorsque la liaison de données s'établit (ICA3010) • 'stop' lorsque la liaison de données prend fin (ICA3014) (obligatoire)
BYTES	entier long	Quantité de données transmises
Remarque : Messages rattachés : ICA3010 ICA3014		

Tableau 17 (page 1 de 2). SOCKS_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés à Socks, issus du fichier s_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
USERID	caractères (16)	ID utilisateur (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
ACTION	caractères (7)	'connect' (ICA3044, ICA3049) ou 'bind' (ICA3046, ICA3047)
ERROR_NUM	entier	Code d'erreur système - code d'erreur AIX (ICA3013, ICA3019, ICA3031, ICA3032, ICA3040, ICA3044, ICA3101, ICA3102, ICA3103, ICA3104, ICA3106, ICA3107, ICA3108, ICA3122, ICA3124, ICA3125, ICA3126, ICA3128)
SRC_HOST	caractères (25)	Nom de l'hôte source (ICA3019, ICA3035)
DST_HOST	caractères (25)	Nom de l'hôte de destination (ICA3016, ICA3045)

Tableau 17 (page 2 de 2). SOCKS_INFO. Cette table contient des messages d'erreur ou d'information générale rattachés à Socks, issus du fichier s_info.tbl.

Colonne	Type de données	Description
SRC_IP	caractères (15)	Adresse source (ICA3042, ICA3043, ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
DST_IP	caractères (15)	Adresse de destination (ICA3044, ICA3045, ICA3046, ICA3047, ICA3049)
LINE_NUM	entier	Numéro de ligne (ICA3022, ICA3023, ICA3024, ICA3025, ICA3026, ICA3109, ICA3110, ICA3111, ICA3112, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120); ou nombre de lignes (ICA3113)
EXEC_STATUS	entier	Statut de la commande exécutable (ICA3027)
CMD	caractères (36)	Commande telle que login (ICA3027, ICA3039, ICA3042, ICA3044, ICA3048). Remarque : pour ICA3042, la commande est en format hexadécimal.
FILE_NAME	caractères (100)	Nom de fichier (ICA3030, ICA3032, ICA3105, ICA3109, ICA3110, ICA3111, ICA3112, ICA3113, ICA3114, ICA3115, ICA3116, ICA3117, ICA3118, ICA3119, ICA3120)
APPLICATION	caractères (30)	Nom d'application : Telnet, FTP, ... (ICA3044, ICA3045, ICA3049)
VERSION	caractères (10)	Numéro de version de Socks en format hexadécimal (ICA3043)

Remarque : Messages rattachés : ICA3013 ICA3016 ICA3017 ICA3019 ICA3022 ICA3023 ICA3024 ICA3025 ICA3026 ICA3027 ICA3030 ICA3031 ICA3032 ICA3033 ICA3035 ICA3039 ICA3040 ICA3041 ICA3042 ICA3043 ICA3044 ICA3045 ICA3046 ICA3047 ICA3048 ICA3049 ICA3052 ICA3101 ICA3102 ICA3103 ICA3104 ICA3105 ICA3106 ICA3107 ICA3108 ICA3109 ICA3110 ICA3111 ICA3112 ICA3113 ICA3114 ICA3115 ICA3116 ICA3117 ICA3118 ICA3119 ICA3120 ICA3121 ICA3122 ICA3123 ICA3124 ICA3125 ICA3126 ICA3127 ICA3128

Tableau 18 (page 1 de 2). SSL_INFO. Cette table contient des informations relatives au statut et à l'activité SSL, issues du fichier ssl_info.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
Client_IP	caractères (15)	Adresse IP du client

Tableau 18 (page 2 de 2). SSL_INFO. Cette table contient des informations relatives au statut et à l'activité SSL, issues du fichier ssl_info.tbl.

Colonne	Type de données	Description
Remarque : Messages rattachés : ICA5015 ICA5022 ICA5023 ICA5028 ICA5029 ICA5036 ICA5039 ICA5060 ICA5063 ICA5082 ICA5120		

Tableau 19. SU. Cette table contient des informations relatives à l'activité de la commande SU, issues du fichier su.tbl, en cas de chargement d'un fichier journal AIX su.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire) Dans la mesure où AIX ne consigne pas l'année dans le fichier journal SU, la partie de la colonne DATE_TIME réservée à l'année prend la valeur de l'année en cours ou de l'année précédente, selon la valeur du mois et du jour (si le mois/jour est postérieur au mois/jour courant, l'année définie est l'année précédente).
FROM_USERID	caractères (16)	ID utilisateur (obligatoire)
TO_USERID	caractères (16)	ID utilisateur (obligatoire)
LOGIN_STATUS	caractères (7)	Statut de la tentative de connexion : réussite ou échec (obligatoire)

Tableau 20. TUNNEL_CONTEXT. Cette table contient les spécifications du contexte de tunnel actif, issues du fichier t_cntxt.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
TUNNEL_ID	entier long	ID de tunnel (obligatoire)
SRC_IP	caractères (15)	Adresse IP source (obligatoire)
DST_IP	caractères (15)	Adresse IP de destination (obligatoire)
ENCRYPTION	caractères (7)	Algorithme de chiffrement DES_CBC ou CDMF
Remarque : Message rattaché : ICA1043		

Tableau 21. TUNNEL_POLICY. Cette table contient des instructions de mise en œuvre de tunnel, issues du fichier t_policy.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
POLICY	caractères (60)	Instruction de mise en œuvre lue dans le ficher fwpolicy (obligatoire)

Remarque : Message rattaché : ICA1040

Tableau 22. TUNNEL_STATUS. Cette table contient des informations sur les changements de statut des tunnels, issues du fichier t_stat.tbl.

Colonne	Type de données	Description
DATE_TIME	date-heure	Date et heure de l'action (obligatoire)
FIREWALL	caractères (100)	Nom qualifié complet de la machine pare-feu (obligatoire)
PID	entier	ID processus AIX, ID d'unité d'exécution NT (obligatoire)
MSG_NUM	entier	Numéro de message (obligatoire)
SESSION_SCKT	entier long	Port de la socket de session (pour ICA1038)
MASTER_SCKT	entier long	Port de la socket maître (pour ICA1038)
TUNNEL_ID	entier long	ID de tunnel supprimé (pour ICA1041)

Remarque :

Messages rattachés : ICA1038 ICA1039 ICA1041 ICA1042

- Le détail de la mise en œuvre définie (ICA1039) peut être consulté dans la table TUNNEL_POLICY.
- Le détail du contexte de tunnel défini (ICA1042) peut être consulté dans la table TUNNEL_CONTEXT.

Chapitre 3. Module de développement d'un logiciel compagnon de SafeMail

Le principal objectif de la passerelle SafeMail d'IBM Firewall est d'acheminer les messages entre réseaux sécurisés et non sécurisés tout en masquant les noms d'hôte sur le réseau sécurisé.

La passerelle SafeMail ne propose aucune fonction de filtrage. Toutefois, vous pouvez écrire un programme de filtrage (Content Screener) et l'installer dans le pare-feu comme logiciel compagnon de la passerelle SafeMail. Ce logiciel compagnon de la passerelle SafeMail permet de visualiser l'intégralité des messages et de les afficher en fonction des critères définis par l'utilisateur. Le logiciel compagnon de la passerelle SafeMail peut décider si la passerelle SafeMail doit interrompre le transfert d'un message ou autoriser l'envoi d'un message via la passerelle.

Généralités sur le fonctionnement de SafeMail

Lorsqu'un client SMTP se connecte à la passerelle SafeMail, celle-ci contacte le serveur de destination SMTP et achemine le message ligne par ligne depuis le client vers le serveur destinataire à mesure de la réception des lignes du message. Si nécessaire, la passerelle SafeMail réécrit certaines lignes d'en-tête du message afin de masquer les noms d'hôte du réseau sécurisé.

Si un logiciel compagnon de filtrage est installé, la passerelle SafeMail y fait appel chaque fois qu'une ligne de message utilise la passerelle. La passerelle SafeMail transmet, entre autres, des informations concernant l'origine et la destination du message de manière à ce que le logiciel de filtrage puisse relier les multiples appels à un message. Ceci s'avère utile dans le cas où le logiciel de filtrage doit analyser le message tout entier avant de décider de le transmettre ou non via le pare-feu.

Si la passerelle SafeMail doit réécrire l'un des en-têtes afin de masquer les noms d'hôte sur le réseau sécurisé, elle fait appel au logiciel de filtrage avant de procéder à la réécriture des en-têtes.

Création d'un logiciel compagnon pour la passerelle SafeMail

Pour créer et installer un logiciel compagnon pour la passerelle SafeMail, procédez comme suit :

- Écrivez le code source de la DLL du logiciel compagnon,
- Créez la DLL,
- Installez la DLL sur le pare-feu.

`ROOTDIR\samples\safemail` contient un code type permettant de créer un logiciel compagnon de filtrage, les fichiers d'en-tête requis et des exemples de make files pour IBM Visual Age et Microsoft Visual C++. *ROOTDIR* est le répertoire sélectionné pendant la procédure d'installation comme emplacement de destination pour IBM Firewall.

Écriture du code source

Le logiciel compagnon de filtrage doit mettre en œuvre une fonction appelée UsrCheck dont le prototype est le suivant :

```
int _Export UsrCheck(pCheckData Data);
```

Il s'agit du point d'entrée que la passerelle SafeMail utilise pour appeler le logiciel de filtrage lorsqu'une ligne de message doit être contrôlée. Cette fonction analyse la ligne de message et renvoie un 0 pour indiquer que le message peut poursuivre sa route via la passerelle SafeMail ou une valeur non nulle pour demander à SafeMail d'interrompre le traitement du message.

Le fichier usrcheck.c de `ROOTDIR\samples\safemail` contient un code type décrivant complètement l'interface entre la passerelle SafeMail et le logiciel de filtrage.

Le paramètre pCheckData de la fonction Check est une structure C documentée dans le fichier usrcheck.h du répertoire `ROOTDIR\samples\safemail`. Cette structure contient des informations importantes concernant le message en cours de traitement, telles les adresses source et cible des serveurs SMTP et les types de réseaux (sécurisés ou non sécurisés) des serveurs SMTP émetteurs et destinataires. Cette structure contient également un programme permettant au logiciel de filtrage de relier plusieurs appels à un même message.

Création de la DLL

Une fois le code source du logiciel compagnon de filtrage écrit, vous devez le compiler et le relier dans une DLL. Cette DLL doit s'appeler smusr.dll. En outre le point d'entrée de UsrCheck doit être exporté depuis la DLL. `ROOTDIR\samples\safemail` contient des exemples de make files dont les options de compilation et de liaison permettent de créer correctement la DLL. Des exemples de makefiles sont proposés pour IBM VisualAge C++ et Microsoft Visual C.

Installation de la DLL

Une fois le fichier smusr.dll terminé et correct, vous devez l'installer sur le pare-feu. Copiez le fichier smusr.dll dans le répertoire `\bin` du pare-feu. Puis, dans le panneau de configuration de Windows NT, utilisez le Services Control Manager pour arrêter et relancer le serveur SafeMail d'IBM Firewall de manière à charger le logiciel compagnon.

IBM Firewall envoie le fichier smusr.dll de l'exemple dans le répertoire `\bin` du pare-feu. Renommez cette DLL avant de copier votre smusr.dll dans ce répertoire au cas où vous auriez à la restaurer ultérieurement.

Dans ce chapitre et dans les deux chapitres suivants, les noms de compilateur varient selon les cas. Les trois chapitres font référence aux deux mêmes compilateurs.

Chapitre 4. Module de développement d'un logiciel compagnon d'archivage

Le démon du journal d'IBM Firewall enregistre les informations de journalisation dans les fichiers que vous avez indiqués dans la boîte de dialogue **Fonctions de journalisation** du client de configuration. Vous lancez ensuite la commande `fwlogmgmt` pour archiver périodiquement les anciens enregistrements du journal. Généralement, vous lancez la commande `fwlogmgmt` dans le Programmateur de Windows NT. Par défaut, la commande `fwlogmgmt` archive les anciens enregistrements de journalisation dans un répertoire et les compresse en utilisant la commande de compression de Windows NT. Toutefois, vous pouvez créer un logiciel compagnon pour remplacer la procédure d'archivage définie par défaut.

Création d'un logiciel compagnon d'archivage

Pour créer un logiciel compagnon d'archivage, procédez comme suit :

1. Écrivez le code source de la DLL du logiciel compagnon,
2. Créez la DLL,
3. Installez la DLL sur le pare-feu.

Le répertoire `ROOTDIR\sample\logarch` contient un code type permettant de créer un logiciel compagnon d'archivage qui reproduit la procédure par défaut du pare-feu, et un make file pour IBM Visual Age et C++. *ROOTDIR* est le répertoire sélectionné pendant la procédure d'installation comme emplacement de destination pour IBM Firewall.

Écriture du code source

Le logiciel compagnon d'archivage doit mettre en œuvre un ensemble de fonctions que le pare-feu utilisera pour réaliser les opérations d'archivage. Les prototypes de ces fonctions sont définis dans le fichier fwarch.h du répertoire `ROOTDIR\sample\logarch`.

Ces fonctions mettent en place les procédures de base telles que l'ajout d'un fichier aux fichiers archivés, la restauration d'un fichier à partir de fichiers archivés, la régénération et l'affichage de fichiers archivés.

Pour de plus amples informations concernant ces fonctions, reportez-vous au code type décrit dans le fichier fwarch.c du répertoire `ROOTDIR\sample\logarch`.

Création de la DLL

Une fois le code source du logiciel compagnon d'archivage écrit, vous devez le compiler et le relier dans une DLL. Cette DLL doit s'appeler fwarch.dll. Toutes les fonctions figurant dans fwarch.h doivent être exportées à partir de la DLL.

Un exemple de make file permettant de créer le code type dans la DLL appropriée est proposée dans le répertoire `ROOTDIR\sample\logarch` pour IBM VisualAge et C++.

Installation de la DLL

Une fois le fichier fwarch.dll terminé et correct, vous devez l'installer sur le pare-feu. Copiez le fichier fwarch.dll dans le répertoire `ROOTDIR\bin`.

Le fichier fwarch.dll par défaut du pare-feu est également stocké dans ce répertoire. Sauvegardez ou renommez cette DLL avant de copier la vôtre dans ce répertoire.

En outre, vérifiez que la commande `fwlogmgmt` et le démon du journal d'IBM Firewall ne sont pas en cours d'exécution lorsque vous remplacez la DLL par défaut. Utilisez le Services Control Manager pour interrompre le démon du journal d'IBM Firewall et le relancer une fois la DLL remplacée.

Chapitre 5. Méthodes d'authentification personnalisées

Ce chapitre explique comment mettre en œuvre des méthodes d'authentification personnalisées.

Authentification fournie par l'utilisateur

Un exemple de programme d'authentification fournie par l'utilisateur est disponible dans le répertoire `ROOT_DIR\bin\authsdk`. Les fichiers concernés par ce programme sont les suivants :

- authschm.h - fichiers de définition d'interface ;
- authus.cpp - modèles de fichiers sources ;
- gwauth4.lib - bibliothèque du pare-feu ;
- msvc++.mak - fichier Makefile Microsoft Visual C ;
- schmname.h - fichiers de définition d'interface ;
- vac++.mak - fichier Makefile IBM Visual Age.

Utilisez les commandes suivantes pour compiler le modèle de programme d'authentification fournie par l'utilisateur pour IBM Visual Age :

- nmake -f vac++.mak - génère la DLL ;
- nmake -f vac++.mak install - génère et installe la DLL ;
- nmake -f vac++.mak clean - vide le répertoire local.

Utilisez les commandes suivantes pour compiler le modèle de programme d'authentification fournie par l'utilisateur pour Microsoft Visual C :

- nmake -f msvc++.mak - génère la DLL ;
- nmake -f msvc++.mak install - génère et installe la DLL ;
- nmake -f msvc++.mak clean - vide le répertoire local.

Création d'un programme d'authentification fournie par l'utilisateur avec le kit de développement logiciel

IBM Firewall est doté d'une interface optionnelle qui permet l'intégration de programmes d'authentification non IBM. Pour ce faire, le pare-feu écrit une DLL de programme d'authentification et l'intègre à sa propre interface de programme d'authentification.

Présentation générale du processus d'authentification

Les services de pare-feu suivants doivent authentifier les utilisateurs avant de leur permettre d'y accéder :

- Serveur de configuration IBM Firewall ;
- Démon FTP relais IBM Firewall ;
- Démon HTTP relais IBM Firewall ;
- Démon Telnet IBM Firewall ;

- Serveur Socks IBM Firewall.

IBM Firewall propose les méthodes d'authentification suivantes :

Interdiction globale (Deny All) L'accès au service est toujours interdit.

Autorisation globale (Permit All) L'accès au service est autorisé sans vérification.

Mot de passe de pare-feu (Firewall Password) L'utilisateur doit indiquer un mot de passe, lequel est défini dans la base de données des utilisateurs du pare-feu.

Mot de passe de connexion NT (NT Logon Password) L'utilisateur doit indiquer son mot de passe de connexion Windows NT.

Clé SecureNet (SecureNet Key) L'utilisateur est authentifié au moyen d'une clé AssureNet Pathways SecureNet Key.

Carte SecurID (SecurID Card) L'utilisateur est authentifié au moyen d'une clé de sécurité Security Dynamics SecurID.

La méthode d'authentification utilisée peut être définie par utilisateur ou par service. Par exemple, le pare-feu peut être configuré de telle sorte que lorsque l'utilisateur *Jean* essaie de se connecter au serveur de configuration du pare-feu, il doive indiquer son mot de passe de connexion Windows NT. Mais, lorsque *Jean* désirera utiliser le serveur relais Telnet du pare-feu, il devra utiliser sa carte SecurID pour être authentifié. Pour sa part, lorsque *Marie* tentera de se connecter au serveur de configuration du pare-feu, elle devra indiquer son mot de passe de pare-feu. Pour plus d'informations sur les méthodes d'authentification associées au pare-feu IBM et sur leur utilisation, reportez-vous au *guide de l'utilisateur d'IBM eNetwork Firewall*.

Outre les méthodes d'authentification fournies avec IBM Firewall, vous pouvez installer jusqu'à trois méthodes d'authentification fournie par l'utilisateur. Ces méthodes viendront s'intégrer dans le dispositif de sécurité du pare-feu IBM que vous les ayez élaborées personnellement ou qu'elles proviennent d'un autre fournisseur qu'IBM.

Chaque méthode d'authentification présente sur le pare-feu, y compris celles fournies par l'utilisateur, est représentée par une bibliothèque DLL qui met en œuvre l'API (interface de programme d'application) correspondante. Cette API définit la manière dont la méthode d'authentification se fait reconnaître du pare-feu et comment le pare-feu lui transmet les requêtes d'authentification.

Création d'une méthode d'authentification fournie par l'utilisateur

La création d'une méthode d'authentification fournie par l'utilisateur implique les étapes suivantes :

- Écriture du code source mettant en œuvre l'API de la méthode d'authentification ;
- Compilation et liaison du code source dans une DLL ;
- Installation de la DLL sur le pare-feu.

Des fichiers d'en-tête source C et des fichiers de bibliothèque servant à créer une méthode d'authentification fournie par l'utilisateur, ainsi que des modèles de code et de fichier makefile pour Microsoft Visual C++ et IBM Visual Age pour C++ sont disponibles dans le répertoire `ROOTDIR\bin\authsdk`.

Écriture du code source

Toutes les méthodes d'authentification doivent faire deux choses :

1. Se faire enregistrer sur le pare-feu ;
2. Mettre en œuvre la fonction AuthSchmFn.

Enregistrement sur le pare-feu : Avant l'initialisation de ses services, le pare-feu tente de charger toutes les DLL trouvées dans le sous-répertoire `\bin\authschm`. Chaque fois qu'une DLL se charge, sa routine d'initialisation appelle une fonction du pare-feu, nommée registerAuthSchm, qui va l'enregistrer sur le pare-feu.

La définition de notre modèle de fonction registerAuthSchm se trouve dans le fichier d'en-tête authschm.h. La fonction n'utilise qu'un seul paramètre ; un pointeur désignant une structure AuthSchmInfo (également définie dans authschm.h). La structure AuthSchmInfo associe un nom de méthode d'authentification avec l'adresse de la fonction AuthSchmFn que le pare-feu devra appeler pour passer les requêtes d'authentification à la méthode d'authentification.

Les méthodes d'authentification fournie par l'utilisateur doivent porter l'un des trois noms suivants :

1. user
2. userauth2
3. userauth3

Le fichier d'en-tête schmname.h contient les noms symboliques définis pour ces noms. Les méthodes d'authentification fournie par l'utilisateur doivent permettre à l'utilisateur final de spécifier lesquels des trois noms sont utilisés, de sorte que plusieurs méthodes puissent être installées sur le même pare-feu et que ces différentes méthodes puissent utiliser le même nom sans difficulté.

Une fois que la routine d'initialisation de la DLL a appelé la fonction d'enregistrement AuthSchm et retourné sa sortie, la DLL doit être prête à traiter les requêtes d'authentification. Pour cette raison, il sera également parfois nécessaire d'inclure une chaîne d'initialisation spécifique à la méthode dans la routine d'initialisation de la DLL.

Mise en œuvre de la fonction AuthSchmFn : Chaque DLL de méthode d'authentification doit mettre en œuvre une fonction appelée AuthSchmFn à l'aide du modèle défini dans le fichier authschm.h. La fonction AuthSchmFn est assortie d'un paramètre ; un pointeur désignant la structure AuthReq. La structure AuthReq est une structure C simple qui contient toutes les information rattachées à la requête d'authentification courante. La structure AuthReq est définie dans le fichier authschm.h. Outre le nom de l'utilisateur en cours d'authentification, elle contient le composant/service du pare-feu demandant l'authentification et d'autres informations relatives à la requête. Pour obtenir la liste et la description des informations contenues dans la structure AuthReq, reportez-vous aux commentaires la concernant dans authschm.h.

Outre le nom utilisateur et le composant du pare-feu, la structure AuthReq contient trois paramètres particulièrement importants pour la mise en œuvre d'une méthode d'authentification :

gwaput Adresse d'une routine de retour d'appel fournie par le pare-feu, que la méthode d'authentification peut utiliser chaque fois qu'elle doit envoyer un message à l'utilisateur. Si, par exemple, la méthode d'authentification doit envoyer un message d'invite à l'utilisateur, elle appellera le point d'entrée défini par le paramètre gwaput pour le faire. Un modèle de fonction de retour d'appel gwaput se trouve dans le fichier authschm.h (section de définition du type de AuthSchmPut). Reportez-vous aux commentaires sur la définition du type de AuthSchmPut pour obtenir la liste des paramètres que la fonction AuthSchmFn doit passer avec l'appel.

gwaget Adresse d'une routine de retour d'appel fournie par le pare-feu, que la méthode d'authentification peut utiliser chaque fois qu'elle doit récupérer une réponse de la part de l'utilisateur en cours d'authentification. Si, par exemple, la méthode d'authentification doit obtenir un mot de passe de la part de l'utilisateur, elle appellera le point d'entrée défini par le paramètre gwaget pour le faire. Un modèle de fonction de retour d'appel gwaget se trouve dans le fichier authschm.h (section de définition du type de AuthSchmGet). Reportez-vous aux commentaires sur la définition du type de AuthSchmGet pour obtenir la liste des paramètres que la fonction AuthSchmFn doit passer avec l'appel. L'un des paramètres les plus importants est le paramètre "echo". La fonction AuthSchmFn peut utiliser ce paramètre pour indiquer si la réponse de l'utilisateur doit lui être restituée ou non à l'écran.

opaque_data La zone opaque_data (données masquées) est utilisée par le pare-feu pour faire coïncider les appels à la fonction AuthSchmFn avec les appels à ses routine de retour d'appel. Qu'elle appelle la routine gwaget ou gwaput, la fonction AthSchmFn doit passer la même valeur opaque_data que celle reçue par elle dans la structure AuthReq.

Notez que les méthodes d'authentification doivent pouvoir s'articuler avec tous les composants du pare-feu. Certains de ces composants peuvent gérer plusieurs types de dialogue interactif avec l'utilisateur final. Ces composants sont appelés des composants de pare-feu interactifs. D'autres composants, du fait de la nature des protocoles qu'ils utilisent, ne peuvent gérer qu'un seul type de dialogue. Ces éléments sont appelés des composants de pare-feu non interactifs.

La méthode d'authentification fournie par l'utilisateur doit pouvoir modifier son mode opératoire en fonction du composant qui l'appelle, comme indiqué dans la zone Composant de la structure AuthReq. Les valeurs admises pour la zone Composant sont définies dans authschm.h. Ces valeurs sont les suivantes :

Tableau 23. Valeurs admises pour la zone Composant

Symbole du composant pour AuthSchm.h	**Composant de pare-feu**	**Interactif ou non interactif**
AUTHSCHM_UNKNOWN	Composant de pare-feu nouveau ou non reconnu	En principe, interactif
AUTHSCHM_REMADMIN	Serveur de configuration	interactif
AUTHSCHM_FTP	Serveur relais FTP	non interactif
AUTHSCHM_TELNET	Serveur relais Telnet	interactif
AUTHSCHM_HTTP	Serveur relais HTTP	interactif
AUTHSCHM_SOCKS_PWD	Serveur Socks avec authentification par mot de passe	non interactif
AUTHSCHM_SOCKS_CRAM	Serveur Socks avec authentification CRAM	interactif
AUTHSCHM_REMIPSEC	Serveur IPSEC pour client distant (non disponible pour Windows NT à ce jour)	interactif

Une fois achevé le traitement de la fonction AuthSchmFn, celle-ci retourne au programme appelant l'un des codes retour GWA définis dans authschm.h. Ce code retour indique si l'utilisateur a été authentifié et si une erreur s'est produite au cours du traitement.

Tableau 24. Codes retour GWA

Code retour	Signification
GWA_OK	Aucune erreur au cours du traitement. L'utilisateur a été authentifié.
GWA_DENY	Aucune erreur au cours du traitement mais l'utilisateur n'a pas pu être authentifié.
GWA_IOFAILURE	Une erreur s'est produite lors de l'envoi des invites à l'utilisateur ou lors de la récupération de ses réponses. On rencontre ce cas lorsque les routines de retour d'appel contiennent des erreurs.
GWA_BUFFERTOOSMALL	La fonction AuthSchmFn n'a pas pu récupérer la réponse de l'utilisateur faute d'avoir pu attribuer assez de mémoire tampon pour la contenir.
GWA_NOAUTHFN	Erreur sans lien avec les méthodes d'authentification.
GWA_FNNOTREG	Erreur sans lien avec les méthodes d'authentification.
GWA_RSVNAME	Erreur - la requête d'authentification contient un nom réservé ne pouvant pas être utilisé pour la méthode d'authentification employée.
GWA_BADNETTYPE	Erreur sans lien avec les méthodes d'authentification.
GWA_BADAPP	Erreur sans lien avec les méthodes d'authentification.
GWA_BADADDR	Erreur - l'adresse fournie dans la requête d'authentification est incorrecte.
GWA_MEMSHORTAGE	Erreur - la requête d'authentification n'a pas pu être traitée faute de mémoire suffisante.
GWA_USERDBFAIL	Erreur - Impossible d'interroger la base de données demandée.
GWA_REGFAILED	Erreur sans lien avec les méthodes d'authentification.
GWA_AUTHERROR	Erreur - erreur liée à la méthode d'authentification utilisée.
GWA_INTERNAL	Erreur - erreurs diverses dans la méthode d'authentification utilisée.

Lorsque la fonction AuthSchmFn revient au pare-feu, si le code retour est GWA_OK, l'utilisateur est considéré comme authentifié et peut accéder au service demandé. Le code retour GWA_DENY n'est pas traité comme une erreur mais l'accès au service demandé est refusé à l'utilisateur. Tous les autres codes retour traduisent des situations d'erreur et l'utilisateur se voit refusé l'accès au service demandé.

Compilation et liaison du code source : Lors de la compilation et de la liaison du code source dans une DLL, vous devez lier la DLL à gwauth4.dll avec le fichier gwauth4.lib présent dans le répertoire `\bin\authsdk`, afin de convertir les noms des points d'entrée définis dans authschm.h. Important : le fichier de la fonction AuthSchmFn ne doit pas être exporté de la DLL. Des modèles de fichier makefile pour IBM VisualAge pour C++ et Microsoft Visual C++ sont disponibles dans le répertoire `\bin\authsdk`.

Installation de la DLL : Une fois la DLL créée, copiez-la dans le répertoire `ROOTDIR\bin\authschm` puis réamorcez la machine pare-feu. Le réamorçage est impératif pour que le pare-feu charge la DLL et enregistre ses méthodes d'authentification.

Assemblage des éléments : La figure 1, à la page 56 montre comment sont chargées les méthodes d'authentification et les principaux appels de fonction intervenant au cours du traitement d'une requête d'authentification.

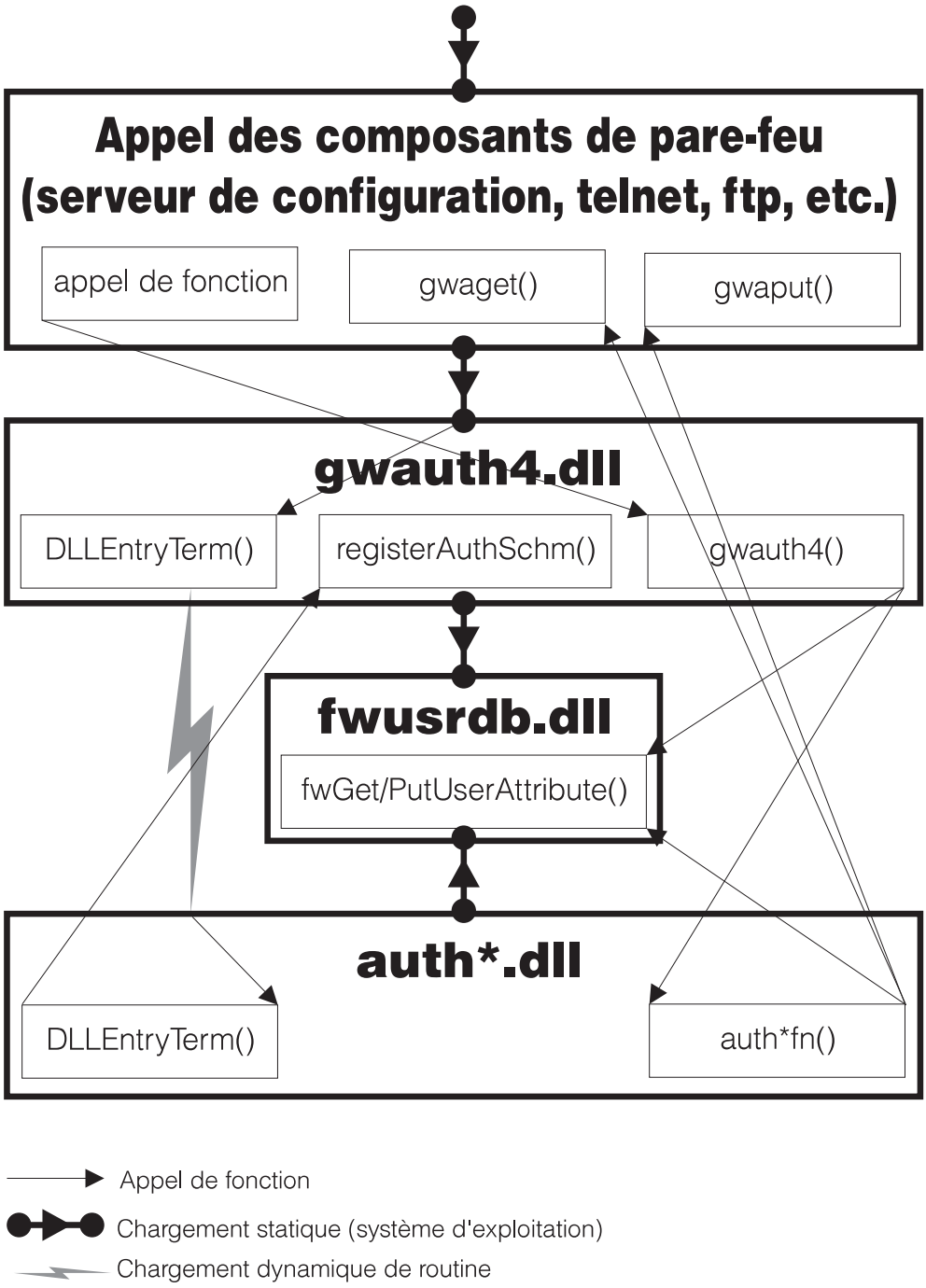

Figure 1. Initialisation et enregistrement de la DLL

Les composants de pare-feu nécessitant les services d'authentification sont liés à une DLL de pare-feu appelée gwauth4. Une fois chargée la DLL gwauth4, sa routine DLLEntryTerm est appelée et tente de charger toutes les DLL présentes dans le répertoire `ROOTDIR\bin\authschm`. Si une DLL de méthode d'authentification n'arrive pas à se charger, le chargement de la DLL gwauth4 ne sera pas considéré comme raté. Pour effectuer ces chargements, la DLL gwauth4 procède par séries.

Chaque fois que la routine DLLEntryTerm d'une méthode d'authentification s'exécute, elle prend en charge l'enregistrement de cette méthode dans la DLL gwauth4. Cette opération s'effectue par l'appel de la fonction registerAuthSchm. La

DLL authschm doit appeler registerAuthSchm pour chaque méthode d'authentification gérée par la DLL. La structure AuthSchmInfo passée à la fonction registerAuthSchm associe le nom de la méthode d'authentification, tel qu'il est défini dans la base de données des utilisateurs, avec le point d'entrée de la fonction AuthSchmFn. La fonction d'enregistrement effectue des copies de la structure passée de sorte que authschm dll puisse réutiliser/modifier cette structure selon ses besoins. La DLL de la méthode d'authentification doit également délivrer la structure AuthSchmInfo.

La fonction registerAuthSchm élabore une liste liée représentant l'ensemble des méthodes d'authentification enregistrées. La routine DLLEntryTerm de gwauth4 affecte la valeur NULL à l'ancre de la liste. Ensuite, lorsque les DLL authschm appellent la fonction registerAuthSchm, celle-ci procède aux opérations suivantes :

1. Elle recherche dans la liste des méthodes d'authentification une entrée correspondant au nom passé. S'il en existe une, elle la supprime de la liste et supprime toutes les données associées stockées.
2. Elle crée une structure AuthSchmEntry sur la base de la structure AuthSchmInfo et l'ajoute à la liste des méthodes d'authentification.
3. Elle retourne au programme appelant un code indiquant si l'enregistrement a abouti (GWA_OK) ou échoué (GWA_REGFAILED).

Lorsque la routine DLLEntryTerm de gwauth4 a chargé chacune des DLL authschm et que ces DLL ont enregistré leurs méthodes d'authentification, elle retourne au programme appelant. A ce stade, tous les autres composants peuvent commencer à demander des services d'authentification en appelant la fonction gwauth4.

Une fois déchargée gwauth4.dll, la routine DLLEntryTerm sera rappelée pour le processus de fin. Au cours de ce processus de fin, la routine va supprimer tous les éléments AuthSchmEntry de la liste AuthSchmList et les données associées stockées. De cette manière, les méthodes d'authentification n'ont pas besoin d'annuler leur enregistrement sur le pare-feu.

Traitement des requêtes d'authentification : Lorsqu'un service de pare-feu a besoin d'authentifier un utilisateur, il appelle les fonctions de gwauth4.dll. La fonction gwauth4 recueille les informations fournies par le composant à l'origine de l'appel et interroge la base de données des utilisateurs du pare-feu pour déterminer le nom de la méthode d'authentification à utiliser pour traiter la requête.

Lorsque la fonction gwauth4 a identifié le nom de la méthode d'authentification à utiliser, elle recherche dans sa liste de méthodes d'authentification enregistrées une méthode portant le même nom. S'il en existe une, la fonction créé une structure AuthReq représentant la requête en cours et appelle le point d'entrée de la DLL de la méthode d'authentification associée au nom.

La fonction AuthSchmFn appelée par gwauth4 traite la requête et appelle les retours d'appel gwaget et gwaput selon ses besoins pour dialoguer avec l'utilisateur final. Une fois le traitement terminé, elle renvoie le contrôle à gwauth4 avec un code retour approprié.

gwauth4 écrit les enregistrements de fichier journal appropriés pour accompagner la requête d'authentification puis revient au composant de pare-feu à l'origine de la requête en lui restituant le code retour reçu de la DLL de la méthode d'authentification.

Chapitre 6. Utilisation de l'utilitaire Make Key File (MKKF)

Pour utiliser une connexion de réseau SSL sécurisé, vous devez avoir :

- Configuré le serveur de configuration pour SSL
- Créé une clé pour les communications sécurisées
- Été désigné comme utilisateur root habilité sur le serveur
- Caché le mot de passe de votre fichier de clés

Utilisez MKKF pour créer la clé de serveur initiale, le fichier de clés et la requête de certificat. MKKF permet également de recevoir le premier certificat dans un fichier de clés et de dissimuler le mot de passe du fichier des clés.

Création d'un fichier de clés

Connectez-vous sous un compte d'administrateur Windows NT pour utiliser cette fonction.

1. Passez dans le répertoire ROOTDIR\config et lancez l'utilitaire MKKF en entrant ce qui suit :

   ```
   c:\program files\IBM\Firewall\config > mkkf

   MKKF Key Manager
   Copyright IBM Corp. 1996
   All Rights Reserved
   ```

2. Créez un fichier de clés.

   ```
   Key Ring Menu
   Currently Selected Key Ring: (none)

   N - Create New Key Ring File
   O - Open Key Ring File
   X - Exit

   Enter a command: n
   ```

   Entrez 'n' comme ci-dessus pour créer un fichier de clés.

   Vous devrez indiquer le nom de fichier du fichier de clés. Vous pouvez choisir n'importe quel nom de fichier se terminant par l'extension .kyr. Par défaut, le pare-feu recherche un fichier nommé fwkey.kyr.

   Entrez le nom du fichier de clés ou appuyez sur Entrée pour accepter le nom par défaut **fwkey.kyr**.

   MKKF va créer un fichier de clés et afficher le menu du fichier de clés. Notez que le fichier de clés que vous venez de créer apparaîtra comme le fichier de clés courant.

3. Créez une clé et une requête de certificat.

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: w
```

Entrez 'w', comme ci-dessus, pour accéder au menu des clés.

```
Key Menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: (none)

L - List/Select a key to work with
C - Create a New Key and Certificate Request
I - Import a key from an Armored key file
X - Exit this menu

Enter a command: c
```

Entrez 'c' comme ci-dessus pour créer une clé.

Pour qu'une nouvelle clé puisse s'insérer dans un fichier de clés, celui-ci doit être protégé par un mot de passe. MKKF vous demande d'entrer le mot de passe qui protégera le fichier de clés. Ce mot de passe ne s'affichera pas lorsque vous le taperez. MKKF demande également si le mot de passe est assorti d'un délai d'expiration. Entrez 'n' comme ci-dessous :

```
Enter password to use for the key file:
password
Enter the password again for verification: password
Should the password expire?
Enter Y for yes or N for no:
n
Password successfully set.
Press ENTER to continue
```

MKKF vous demande de préciser le type de clé à créer.

```
Choose Certificate Type Menu
S - PEM Certificate Request Format (Private Enhanced Message)
P - PKCS10 Certificate Request Format
C - Cancel

Enter a command: s
```

Entrez 's' comme ci-dessus pour créer un format de requête de certificat PEM. MKKF va générer un certificat vide :

```
Compose Secure Server Certificate Menu

Current Certificate Information
Key Name: (none)
Key Size: 0
Server Name: (none)
Organization: (none)
Organization Unit: (none)
City/Locality: (none)
State/Province: (none)
Postal Code: (none)
Country: (none)

M - Modify the Certificate Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: m
```

Entrez 'm' pour modifier le certificat vide. Vous devrez saisir les informations relatives au nouveau certificat :

- Entrez le nom à utiliser. Le choix du nom est libre. Il sera exclusivement utilisé par l'utilitaire MKKF :

  ```
  Enter a name to use for the key entry:

  Firewall Key
  ```

- Précisez la taille de la clé. IBM Firewall ne propose que la version exportable de l'utilitaire MKKF. La taille de clé maximale est de 1024 octets.

  ```
  1:   508
  2:   512
  3:   768
  4:   896
  5:   1024
  Enter the number corresponding to the key size you want:

  2
  ```

- Entrez le nom d'hôte TCP/IP qualifié complet du pare-feu (par exemple jupiter.raleigh.ibm.com) :

  ```
  Enter the server's fully qualified TCP/IP domain name or press
  Enter by itself to leave the field blank

  jupiter.raleigh.ibm.com
  ```

- Entrez le nom de l'organisme à associer au certificat. (Par exemple, le nom de votre société) :

  ```
  Enter Organization Name for the certificate
  or press ENTER by itself to leave the field blank.

  AAA Inc.
  ```

- Entrez le nom désignant votre unité au sein de votre organisme. (Par exemple, un nom de service) :

  ```
  Enter Organizational Unit Name for the certificate
  or press ENTER by itself to leave the field blank.
  ```

  Network Security Products

- Précisez la ville où le certificat sera utilisé :

  ```
  Enter Locality/City Name for the certificate
  or press ENTER by itself to leave the field blank.
  ```

  RTP

- Précisez le département géographique ou la région.

  Remarque : Les spécifications des certificats imposent un minimum de trois caractères dans cette zone, les abréviations en deux lettres ne sont donc pas admises.

  ```
  Enter State/Province Name for the certificate
  or press ENTER by itself to leave the field blank.
  State/Province must be at least three characters long.
  ```

  N.C.

- Entrez le code postal à associer au certificat :

  ```
  Enter Postal Code for the certificate
  or press ENTER by itself to leave the field blank.
  ```

  27709

- Entrez un code de pays à deux lettres :

  ```
  Enter Country Code for the certificate
  or press ENTER by itself to leave the field blank.
  Country code must be exactly two characters long.
  ```

  US

Lorsque MKKF aura réuni toutes les informations fournies, le certificat s'affichera :

```
Compose Secure Server Certificate Menu

Current Certificate Information
Key Name: Firewall Key
Key size: 512
Server Name: jupiter.raleigh.ibm.com
Organization: AAA Inc.
Organizational Unit: Network Security Products
City/Locality: RTP
State/Province N.C.
Postal Code: 27709
Country: US

M - Modify the Certificate Fields
R - Ready To Create Key and Certificate Request
C - Cancel

Enter a command: r
```

Si les données du certificat comportent des erreurs, entrez 'm' pour les corriger. Dans le cas contraire, tapez 'r' pour créer une clé et le fichier de clés associé.

MKKF vous demande de désigner le fichier devant contenir le nouveau certificat. Vous pouvez choisir n'importe quel nom mais l'usage veut que l'on reprenne le nom donné au fichier de clés et qu'on lui ajoute l'extension .cert.

```
Enter file to store the certificate request in:
fwkey.cert
Creating Private Key...
Private key was successfully created.
Creating certificate request...
certificate request was successfully created
Adding new key to key file.
The new key and certificate request were created successfully.
Press ENTER to continue
```

4. Faites de la nouvelle clé la clé par défaut.

   Une fois la clé et le certificat créés, le menu des clés apparaît. La nouvelle clé apparaît comme la clé courante.

```
Key Menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: Firewall Key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
U - Unmark Selected Key's Trusted Root Status
R - Create A Certificate Request for Selected Key
X - Exit This Menu

Enter a command: f
```

La nouvelle clé doit être désignée comme clé par défaut dans le fichier de clés. Tapez 'f' comme montré dans l'exemple précédent. Vous devrez confirmer l'action :

```
Key Menu
Currently selected key: Firewall Key
Are you sure you want to make this key the default?
Enter Y for yes or N for No:
y
Key was made the default key.
Press ENTER to continue
```

Une fois la nouvelle clé définie comme clé par défaut, le menu Key s'affiche :

```
Key menu
Currently Selected Key Ring: fwkey.kyr
Selected Key Entry: Firewall Key

L - List/Select a Key To Work With
S - Show Information about Selected Key
D - Delete Selected key
C - Create a New Key and Certificate Request
I - Import a Key From an Armored Key File
E - Export Selected Key To an Armored Key File
F - Make Selected Key the Default Key for this Key Ring
U - Unmark Selected Key's Trusted Root Status
R - Create A Certificate Request for Selected Key
X - Exit This Menu

Enter a command: x
```

Quittez le menu des clés en tapant 'x'.

5. Réceptionnez le certificat dans le fichier de clés.

   Le menu Key Ring s'affiche.

   ```
   Key Ring Menu
   Currently Selected Key Ring: fwkey.kyr

   N - Create New Key Ring File
   O - Open Key Ring File
   S - Save Key Ring File
   A - Save Key Ring as Another File
   P - Set Password for Key Ring File
   C - Create Stash File for Key Ring File
   R - Receive a Certificate into a Key Ring File
   W - Work with Keys and Certificates
   X - Exit

   Enter a command: r
   ```

   Remarque : Dans la mesure où le pare-feu n'utilise pas SSL pour l'authentification, votre certificat n'a pas besoin d'être visé par une autorité habilitée.

```
Enter file name or press ENTER for Cert.txt.
fwkey.cert
This is a self-signed certificate. Add it to the key file?
Enter Y for yes or N for no:
y
Certificate added to key ring.
Press ENTER to continue
```

6. Créez un fichier cache pour le fichier de clés.

   Une fois le certificat ajouté au fichier de clés, le menu Key Ring s'affiche :

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: c
```

   Vous devez créer un fichier cache pour le fichier de clés. Tapez 'c' comme montré dans l'exemple précédent. MKKF reprendra le nom du fichier de clés et lui adjoindra l'extension .sth :

```
Stashed password file saved to fwkey.sth
Press ENTER to continue
```

   Une fois le fichier cache créé, le menu Key Ring s'affiche :

```
Key Ring Menu
Currently Selected Key Ring: fwkey.kyr

N - Create New Key Ring File
O - Open Key Ring File
S - Save Key Ring File
A - Save Key Ring as Another File
P - Set Password for Key Ring File
C - Create Stash File for Key Ring File
R - Receive a Certificate into a Key Ring File
W - Work with Keys and Certificates
X - Exit

Enter a command: x
```

   Votre fichier de clés est à présent prêt à l'emploi. Tapez 'x' comme montré plus haut pour quitter MKKF et tapez 'y' pour sauvegarder les modifications du fichier de clés :

```
Key ring file has been changed. Save?
Enter Y for yes or N for no:
y
Key ring saved to fwkey.kyr
Press ENTER to continue
#
```

7. Mise à jour du fichier de configuration

   Une fois créé le fichier de clés, vous devez indiquer son nom dans le fichier des paramètres du serveur de configuration à l'aide de la commande `fwcfgsrv`.

   Si vous utilisez l'option de chiffrement SSL pour le serveur de configuration, vous devez également définir l'option encryption=ssl à l'aide de la commande `fwcfgsrv`.

   Une fois exécutée la commande `fwcfgsrv`, arrêtez le serveur puis réamorcez-le.

Chapitre 7. Résolution de problèmes et évaluation

Ce chapitre explique comment résoudre les problèmes le plus fréquemment rencontrés lors de la mise en œuvre et de la configuration du pare-feu IBM Firewall.

Si vous rencontrez des difficultés, créez tout d'abord un fichier `journal de pare-feu` avec niveau de priorité `débogage` pour accroître la quantité des informations dirigées vers les fichiers journaux. Pour plus d'informations, consultez la section «Gestion des fichiers journaux», à la page 5.

Installation et configuration

Échec de la prise en charge des filtres

Explication du problème Vous recevez les messages d'erreur suivants :

```
La vérification du support de filtrage n'a pas abouti. La création de
socket n'a pas abouti.
L'un des fichiers ou répertoires mentionnés dans le chemin d'accès
n'existe pas.
```

Ce problème survient lorsque le pare-feu n'a pas été réinitialisé après son installation.

Solution recommandée Réamorcez le pare-feu et relancez la procédure.

Problèmes de routage

La boîte de dialogue **Règles de sécurité** d'IBM Firewall propose une fonction appelée *Test de routage IP* dont la vocation est d'aider au débogage des problèmes de routage. Sélectionnez cette case à cocher et activez la configuration de la connexion et la journalisation des règles de connexion. Examinez ensuite le contenu du `journal de pare-feu` pour consulter les informations relatives aux paquets transitant par le pare-feu.

Faites d'abord ces tests avec les adresses IP puis avec les noms d'hôte. Si le routage des transactions s'effectue normalement avec les adresses mais pas avec les noms d'hôte, reportez-vous à la section «Problèmes de DNS», à la page 69, pour plus d'informations.

Procédure ping impossible entre les hôtes et le pare-feu

Explication du problème Votre interface réseau n'est pas configurée comme il convient.

Solution recommandée Reportez-vous à la documentation de votre système d'exploitation.

Explication du problème La connexion avec le réseau non sécurisé n'est pas configurée comme il convient.

Solution recommandée Demandez une assistance à votre fournisseur de service Internet.

Explication du problème Si votre réseau sécurisé est isolé par un routeur, le pare-feu doit disposer d'une route statique menant à ce routeur. Utilisez la commande `netstat -rn` pour vérifier le routage statique :

```
netstat -rn
```

La sortie attendue pour la famille de protocoles 2 doit avoir l'aspect suivant :

```
Destination  Gateway          Flags     ....
default      nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

Figure 2. Exemple de sortie de la commande netstat -rn.

nrr.nrr.nrr.nrr correspond au routeur Internet et représente la route par défaut. La route par défaut est une route statique (Flag=UG).
nnn.nnn.nnn correspond au domaine non sécurisé. Il s'agit d'une route d'interface (Flag=U).
nnn.nnn.nnn.nnn correspond à l'interface non sécurisée.
sss.sss.sss correspond au domaine sécurisé. Il s'agit d'une route d'interface (Flag=U).
sss.sss.sss.sss correspond à l'interface sécurisée.
ss1.ss1.ss1 correspond à un sous-domaine du côté sécurisé du réseau. srr.srr.srr.srr correspond au routeur menant à ce sous-domaine. Il s'agit d'une route statique (Flag=UG).
127.0.0.1 correspond à l'hôte de bouclage ou à l'hôte local. Il s'agit d'une route d'interface (Flag=U).

Il doit exister une route d'interface pour chaque interface et la route par défaut doit référencer le routeur du côté non sécurisé du pare-feu.

Solution recommandée Ajoutez une route statique au routeur. Contactez l'administrateur du routeur. Utilisez la commande `route add`.

Explication du problème Le masque de sous-réseau défini sur l'interface sécurisée ou sur l'hôte que vous essayez de contacter est peut-être incorrect.

Solution recommandée Utilisez les utilitaires de configuration du client concerné pour modifier les valeurs de masque.

Procédure ping impossible entre les hôtes non sécurisés et les hôtes sécurisés

Explication du problème Chaque routeur associé au pare-feu doit définir une route statique spécifiant le pare-feu comme passerelle pour les réseaux destinataires situés en dehors de la sphère du pare-feu.

Solution recommandée Contactez l'administrateur du programme de routage.

Explication du problème Si le réseau sécurisé utilise des adresses non enregistrées et pour lesquelles il n'a été défini aucune route vers le réseau non sécurisé, y compris s'agissant d'adresses privées telles que celles décrites dans la RFC 1597, les paquets ne seront pas renvoyés à l'émetteur.

Solution recommandée Utilisez un client doté d'une adresse enregistrée.

Problèmes de DNS

Le serveur de noms de domaine (DNS) du pare-feu convertit les noms en interrogeant le serveur de noms sécurisé. Le serveur de noms sécurisé convertit tous les noms existant dans le réseau sécurisé. Le serveur de noms sécurisé transmet les requêtes de noms d'hôte non sécurisé au serveur de noms du pare-feu. Le serveur de noms du pare-feu interroge le serveur de noms non sécurisé pour répondre à ces requêtes.

Les problèmes de DNS peuvent avoir des répercutions sur d'autres fonctions du pare-feu. Il est judicieux de vérifier le DNS même si le problème semble sans rapport avec lui à première vue.

Les exemples suivants vous guideront à travers les étapes de cette méthode. On a recours à l'utilitaire `nslookup` pour mieux isoler le problème. Ces exemples utilisent les valeurs suivantes :

www.ibm.com nom de système hôte d'un réseau non sécurisé

nns.nns.nns.nns adresse du serveur de noms non sécurisé

sns.sns.sns.sns adresse du serveur de noms sécurisé

host.secure.company.com nom d'un système hôte membre du réseau sécurisé

127.0.0.1 adresse de bouclage définie sur le pare-feu

Ces valeurs peuvent être obtenues à partir de la boîte de dialogue des services de noms de domaine dans le programme client de configuration. Elles vous seront nécessaires au cours de ces exercices.

Remarque : La commande `nslookup` requiert d'insérer un point à la suite du nom d'hôte pour éviter l'ajout automatique du nom de domaine sécurisé.

Le DNS n'a pas encore été configuré

Explication du problème Vous n'avez pas configuré les fonctions DNS du pare-feu.

Solution recommandée Remplissez les zones de la boîte de dialogue **Services de noms de domaine**.

Échec ou expiration des requêtes DNS

Explication du problème Le contrôle des transactions du pare-feu empêche les paquets DNS de circuler.

Solution recommandée Allez à la boîte de dialogue **Règles de sécurité**, sélectionnez la case à cocher autorisant les requêtes DNS et réactivez le contrôle des transactions.

Échec de la commande nslookup www.ibm.com. nns.nns.nns.nns

Explication du problème Le serveur de noms non sécurisé n'utilise pas l'adresse indiquée ou n'est pas configuré comme il convient.

Solution recommandée Demandez au fournisseur de services DNS de vous fournir une adresse de serveur de noms valide.

nslookup www.ibm.com. Échec de 127.0.0.1

Explication du problème Le service `DNS Microsoft` est sans doute désactivé. Utilisez le gestionnaire de contrôle des services pour vous en assurer.

Solution recommandée Démarrez le DNS à l'aide du gestionnaire de contrôle des services.

Échec de la commande nslookup host.secure.company.com. sns.sns.sns.sns

Explication du problème Le serveur de noms sécurisé est désactivé.

Solution recommandée Relancez le serveur de noms.

Échec de la commande nslookup www.ibm.com. sns.sns.sns.sns

Explication du problème Mauvaise interaction entre le serveur de noms sécurisé et le pare-feu pour cause de défaut de configuration du serveur de noms.

Solution recommandée Pour plus d'informations sur les règles de configuration, reportez-vous au *guide de l'utilisateur d'IBM eNetwork Firewall*.

Client de configuration

Pas de réponse du serveur

Explication du problème Le client de configuration et le serveur de configuration utilisent des langues différentes.

Solution recommandée Dans le panneau des paramètres de connexion du client de configuration, sélectionnez la langue utilisée pour l'installation du pare-feu.

Explication du problème Le programme de chiffrement SSL est probablement mal configuré.

Solution recommandée Assurez-vous que SSL a été sélectionné dans le panneau de connexion du client. Arrêtez le serveur de configuration du pare-feu à l'aide du gestionnaire de contrôle des services, puis réamorcez-le.

Explication du problème Le serveur de configuration du pare-feu est peut-être désactivé.

Solution recommandée Assurez-vous que le serveur de configuration du pare-feu est activé.

Explication du problème Le serveur de configuration du pare-feu contrôle peut être un port non standard.

Solution recommandée Examinez le fichier `c:\winnt\system32\drivers\etc\services` et assurez-vous qu'il contient la ligne `ibmfwrcs 1014/tcp`. Si vous désirez utiliser le serveur sur un autre port, modifiez la ligne `ibmfwrcs 1014/tcp` en conséquence et reportez le nouveau port dans le panneau de connexion du client. Arrêtez le serveur de configuration à l'aide du gestionnaire de contrôle des services, puis réamorcez-le.

Explication du problème Le contrôle des transactions du pare-feu ne permet peut-être pas les communications depuis et vers le serveur de configuration. Ceci n'a d'effets que sur les clients de configuration tournant sur un système hôte distant.

Solution recommandée Établissez une connexion entre la machine du client de configuration et le pare-feu. Le client de configuration doit être la source de la connexion et le pare-feu sa destination. Régénérez la configuration et activez la connexion. Pour plus d'informations, reportez-vous au *guide de l'utilisateur d'IBM eNetwork Firewall*.

Explication du problème La configuration du serveur de configuration n'autorise peut-être pas les connexions provenant d'un système hôte distant.

Solution recommandée À l'aide de la commande `fwcfgsrv`, vérifiez que la valeur affectée au paramètre `localonly` est bien "no".

Impossible de se connecter au serveur de configuration

Explication du problème Chaque nom utilisateur authentifié par le pare-feu est configuré pour utiliser l'une ou l'autre des méthodes d'authentification disponibles. On utilise `Deny All` (Interdiction globale) pour interdire à un utilisateur l'accès à un service déterminé.

Solution recommandée Examinez le contenu des zones Administration sécurisée et Administration non sécurisée du nom utilisateur utilisé. Ces zones ne s'appliquent qu'aux administrateurs et pas aux utilisateurs du pare-feu.

Contrôle des transactions

Les modifications apportées aux connexions sont sans effet

Explication du problème Les modifications des composants du contrôle des transactions restent sans effet tant qu'elles ne sont pas activées. Ceci vaut également pour les paramètres de la boîte de dialogue **Règles de sécurité** du menu Administration système.

Solution recommandée Utilisez la boîte de dialogue **Activation des connexions** pour régénérer et activer la nouvelle configuration.

Serveurs relais

Pas de transmission des données

Explication du problème Les serveurs relais du pare-feu ne s'initialisent pas tant que la machine n'a pas été réamorcée après l'installation.

Solution recommandée Réamorcez la machine pare-feu.

Explication du problème Le contrôle des transactions du pare-feu doit être configuré de manière à permettre la transmission des paquets via le serveur relais et non directement à travers le pare-feu.

Solution recommandée Configurez chaque côté de la connexion relais comme décrit dans le *guide de l'utilisateur d'IBM eNetwork Firewall*.

Utilisez les services prédéfinis autant que possible, particulièrement pour les transactions FTP.

Impossible de se connecter au système hôte désiré

Explication du problème Si les données peuvent transiter par le serveur relais mais que le système hôte ne peut pas être contacté, probablement le client n'arrive-t-il pas à convertir les noms d'hôte comme il convient.

Solution recommandée Allez à la boîte de dialogue **Règles de sécurité**, assurez-vous que la case à cocher autorisant les requêtes DNS a été sélectionnée et que la configuration des connexions a été activée. Pour plus d'informations, consultez la section «Problèmes de DNS», à la page 69.

Explication du problème Chaque nom utilisateur authentifié sur le pare-feu par l'un ou l'autre de ses services peut être configuré pour utiliser l'une ou l'autre des méthodes d'authentification disponibles. On utilise `Deny All` (Interdiction globale) pour interdire à un utilisateur l'accès à un serveur relais déterminé.

Solution recommandée Examinez les paramètres d'authentification du compte utilisateur dans la boîte de dialogue **Utilisateurs** du client de configuration.

Services d'authentification

Impossible d'authentifier un compte d'administrateur Windows NT

Explication du problème Les attributs de pare-feu attachés à un compte d'administrateur Windows NT sont stockés dans la base de données des utilisateurs du pare-feu, sous le nom `fwdfadm`.

Solution recommandée Vérifiez que `fwdfadm` est associé à la méthode d'authentification qui convient pour le service désiré.

Impossible d'authentifier un utilisateur relais du pare-feu

Explication du problème Si l'utilisateur relais concerné n'est pas défini dans la base de données des utilisateurs du pare-feu, le système utilise le nom `fwdfuser` pour définir ses attributs.

Solution recommandée Vérifiez que la méthode d'authentification associée à `fwdfuser` convient pour le service que l'utilisateur demande.

Conversion d'adresse de réseau (NAT)

Échec de la connexion NAT

Explication du problème Vous avez défini et activé la conversion d'adresse réseau mais la connexion ne fonctionne pas.

Solution recommandée Il existe un problème de configuration soit au niveau des tables de routage soit au niveau de la conversion d'adresse réseau.

Comment établir une route pour des paquets NAT ?

Explication du problème Aucune route n'est établie pour les paquets NAT.

Solution recommandée Ajoutez une route statique pour le routeur en dehors du pare-feu, en indiquant la destination, la ou les adresses NAT et la passerelle du pare-feu.

Quels sont les outils de débogage disponibles pour les problèmes de conversion d'adresse réseau ?

Explication du problème Quels sont les outils de débogage disponibles pour les problèmes de conversion d'adresse réseau ?

Solution recommandée La journalisation NAT permet de garder la trace des opérations de gestion des adresses enregistrées dynamiquement.

Fonctions de journalisation

Les modifications des fonctions de journalisation n'ont aucune incidence sur le serveur

Explication du problème La suppression ou la modification d'une fonction de journalisation semble prendre effet sur l'interface utilisateur graphique mais n'a aucune incidence sur le serveur.

Solution recommandée Réamorcez le système.

Utilitaires de génération d'états

Erreur d'accès au fichier :

Explication du problème Cette erreur se manifeste avec toutes les commandes suivantes :

```
db2 -vf fwschema.dll > schema.out
db2 -vf fwimport.dat > import.out
db2 -vf fwqrysmp.dml > sample.out
```

Solution recommandée Spécifiez comme il convient les noms de fichier qualifiés complets pour les fichiers .ddl, .dat ou .dml.

Erreurs lors de l'importation de données dans la base de données

Explication du problème Le fichier import.out créé par la commande `db2 -vf fwimport.dat>import.out` contient des messages qui indiquent que l'une des importations a échoué ou n'a que partiellement abouti.

Solution recommandée Contrôlez le fichier .msg lié à l'instruction d'importation à l'origine du problème. Ce fichier vous renseignera sur sa nature. Recherchez le ou les enregistrements rattachés dans le fichier .tbl correspondant pour examiner les données d'entrée et déterminer en quoi elles ne conviennent pas. Peut-être sont-elles trop longues pour la colonne devant les contenir dans la base de données. Ces données sont peut-être d'un type inapproprié pour ce type de colonne. S'il semble que les données d'entrée ne conviennent pas, recherchez l'enregistrement de fichier journal initial pour vous assurer que la fonction `fwlogtbl` a généré un fichier .tbl acceptable.

Si vous ne pouvez pas résoudre le problème, sauvegardez les fichiers import.out, .msg, le fichier .tbl associé et le fichier journal d'origine avant d'appeler l'assistance IBM.

Annexe A. Messages

Cette annexe contient des messages prévus pour IBM Firewall pour AIX, IBM Firewall pour Windows NT et des messages communs aux deux types de pare-feu. Elle fournit également les informations suivantes sur les messages d'IBM Firewall : :

- Format des messages ;
- Degrés de gravité des messages ;
- Messages et explications.

Si vous avez pris connaissance d'un message et de son explication mais que vous désirez des informations supplémentaires, reportez-vous au Chapitre 7, «Résolution de problèmes et évaluation», à la page 67.

Code de message

ICA Trois premiers octets fixes.

xxxx Valeur comprise entre 0000 et 9999.

a Indicateur de gravité. Les messages sont classés par degré de gravité.

- i – information
- w– avertissement
- e – erreur
- s – erreur grave

Les valeurs de 0000 à 9999 sont réparties selon les catégories suivantes :

- 0000 – 0999 intrusions
- 1000 – 1999 filtres
- 2000 – 2999 serveur relais
- 3000 – 3999 Socks
- 4000 – 4999 récepteur de messagerie
- 5000 – 8999 disponibles
- 9000 – 9999 événements autres/généraux

Messages

ICA0001 ALERTE - *nombre* **échec(s) d'authentification.**

Explication : Les conditions de seuil d'échec d'authentification ont été satisfaites.

ICA0002 ALERTE - *nombre* **échec(s) d'authentification de l'utilisateur** *nom_utilisateur***.**

Explication : Les conditions de seuil de détection d'un message déterminé ont été satisfaites.

ICA0003 ALERTE - *nombre* **échec(s) d'authentification de l'hôte** *adresse IP de l'hôte***.**

Explication : Les conditions de seuil d'échec d'authentification d'un hôte déterminé ont été satisfaites.

ICA0004 ALERTE - Code *id_message* **avec** *nombre* **entrée(s) de fichier journal.**

Explication : Les conditions de seuil de détection d'un message déterminé ont été satisfaites.

ICA0005 Contrôle de journalisation - mémoire pleine.

Explication : Arrêt du processus pour cause de mémoire insuffisante.

ICA0006 Contrôle de journalisation - erreur d'accès au fichier de service *numéro d'erreur*

Explication : Impossible de trouver une entrée fwlogmond dans /etc/services.

ICA0007 Contrôle de journalisation - impossible de créer la socket *numéro d'erreur*

Explication : Impossible d'ouvrir la socket ; voir le message d'erreur.

ICA0008 Contrôle de journalisation - échec de la commande bind *numéro d'erreur*

Explication : Impossible de lier la socket ; voir le message d'erreur.

ICA0009 Impossible d'ouvrir le fichier de définition de seuil *numéro d'erreur*

Explication : Problème d'accès au fichier de définition de seuil ; voir le message d'erreur.

ICA0010 Contrôle de journalisation - erreur de lecture fatale *numéro d'erreur*

Explication : Problème de lecture depuis la socket ; voir le message d'erreur.

ICA0011 Impossible d'obtenir le statut du fichier de définition de seuil *numéro d'erreur*

Explication : Problème d'accès au fichier de définition de seuil ; voir le message d'erreur.

ICA0012 Arrêt du démon du contrôle de journalisation.

Explication : Arrêt du démon par abend ou par signal de fin. Voir les messages de journal précédents pour info.

ICA0013 Contrôle de journalisation - Interception d'un signal de fin.

Explication : Le démon a intercepté un signal de fin et va s'arrêter.

ICA0014 Démarrage du démon du contrôle de journalisation.

Explication : Le démon s'est initialisé.

ICA0015 Impossible de créer le démon de contrôle de journalisation *numéro d'erreur*

Explication : La création du démon a échoué ; voir le message d'erreur.

ICA0016 Impossible d'ouvrir *fichier d'ID processus* **- le démon est peut-être déjà actif.**

Explication : Le démon n'a pas pu ouvrir le fichier du processus indiqué.

ICA0017 Impossible d'écrire l'ID processus (*ID processus***) dans** *fichier***.**

Explication : Le démon n'a pas pu écrire l'ID processus (PID) dans le fichier.

ICA0018 Contrôle de journalisation - aucune donnée.

Explication : Reçu un paquet sans données, le paquet est ignoré.

ICA0019 Contrôle de journalisation - données trop peu nombreuses. Code ignoré.

Explication : Reçu un paquet contenant trop peu de données, le paquet est ignoré.

ICA0020 Contrôle de journalisation - erreur de format du code ICA.

Explication : Reçu un paquet avec des données d'un format incorrect, le paquet est ignoré.

ICA0021 Contrôle de journalisation - erreur de format des données d'authentification.

Explication : Reçu un paquet avec des données d'un format incorrect, le paquet est ignoré.

ICA0022 Erreur de syntaxe dans le fichier de définition de seuil (*entrée incorrecte***).**

Explication : La syntaxe de l'entrée du fichier de définition de seuil indiquée est incorrecte.

ICA0023 Impossible d'ouvrir le fichier fwmail.conf.

Explication : L'ouverture du fichier fwmail.conf a échoué ou le fichier est vide.

ICA0024 Impossible de se connecter au serveur SMTP.

Explication : Le serveur SMTP est mobilisé ou refuse la connexion.

ICA0025 Échec de transmission du message d'alerte par e-mail.

Explication : Impossible d'envoyer le message d'alerte à l'adresse spécifiée par messagerie électronique.

ICA0051 Le nombre de jours de conservation dans le fichier journal *nom de fichier journal* **doit être un nombre entier court non signé.**

Explication : La valeur de conservation dans le fichier journal doit être un nombre entier valide.

ICA0052 Le nombre de jours de conservation en archive, *nom de fichier journal***, doit être un nombre entier court non signé.**

Explication : La valeur de conservation en archive doit être un nombre entier valide.

ICA0053 Il n'est pas permis d'avoir plusieurs entrées pour le fichier journal *nom de fichier journal* **dans le fichier logmgmt.cfg.**

Explication : Le fichier logmgmt.cfg ne peut contenir qu'une seule entrée pour un même fichier journal.

ICA0054 Impossible d'ouvrir le fichier *$ Variables :***.**

Explication : Impossible d'ouvrir le fichier logmgmt.cfg.

ICA0055 Le fichier logmgmt.cfg ne contient aucune entrée valide.

Explication : Le fichier logmgmt.cfg ne contient aucune entrée valide.

ICA0056 Le message de fichier journal "*$ Variables :***" est incorrect.**

Explication : Le message de fichier journal est incorrect.

ICA1001 Impossible de créer un fichier avec cet ID processus.

Explication : Le démon de journalisation des filtres a rencontré une erreur lors de l'écriture du fichier fwlogd.pid.

Action de l'utilisateur : Contrôlez le système de fichiers contenant /etc/security. Possibilité de manque d'espace disque.

ICA1002 Impossible de communiquer avec le programme cfgfilt.

Explication : Du fait que le fichier fwlogd.pid n'a pas été créé, la communication entre le démon fwlogd et l'application cfgfilt (nécessaire au contrôle des filtres) ne peut pas s'établir.

Action de l'utilisateur : Contrôlez le système de fichiers contenant /etc/security. Possibilité de manque d'espace disque.

ICA1003 Poursuite de l'initialisation du démon de journalisation.

Explication : Le démon fwlogd continuera le processus de démarrage.

ICA1004 Démon de journalisation de filtrage *fwlogd* **(niveau** *version***.***édition***) initialisé à** *heure* **le** *date*

Explication : Le démon de journalisation des paquets IP a été initialisé. Quand/si la journalisation des paquets est activée, le démon fwlogd écrit les enregistrements nécessaires dans le fichier syslog local4.

ICA1005 Journalisation supprimée pour le(s) message(s) de paquets *n°_règle_filtrage* **suite à un débordement de la mémoire tampon.**

Explication : Dépassement de la mémoire tampon des filtres du démon fwlogd. Impossible de journaliser l'un des paquets associés à la règle de filtrage spécifiée.

Action de l'utilisateur : Contrôlez le fichier journal. Le pare-feu fait peut-être l'objet d'une tentative d'accès en fraude à un service interdit ou vous journalisez des messages non obligatoires. Par exemple, la diffusion des messages doit avoir une règle d'interdiction avec le contrôle de journalisation réglé sur "Non" (l=n) pour empêcher la saturation du fichier journal.

ICA1006 Erreur fwlogd fatale - *fonction en échec***:** *message d'erreur*

Explication : Le serveur fwlogd n'a pas pu exécuter la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon fwlogd.

ICA1007 Impossible de générer un processus fils : *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

Action de l'utilisateur : Remédiez au problème signalé en fonction des informations affichées.

ICA1008 Erreur renvoyée par la procédure setpgrp : *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1009 Impossible de générer un second processus fils : *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1010 Ce démon doit être exécuté avec une autorisation root.

Explication : Le démon de journalisation des filtres doit être exécuté avec une autorisation root.

Action de l'utilisateur : Recommencez l'opération avec une autorisation root.

ICA1011 Erreur lors de la demande d'extension noyau *chemin_chargement* **effectuée par sysconfig** *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1012 Extension noyau *netinet* **AIX non chargée -- impossible de continuer.**

Explication : Le pilote de périphérique **netinet** ne possède pas de support de filtrage.

Action de l'utilisateur : Installez le code d'IBM Firewall. Autre possibilité, le code a peut-être été installé mais la machine n'a pas été réamorcée par un *reboot*.

ICA1013 La création de socket n'a pas abouti : *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1014 Le gestionnaire de périphérique netinet AIX n'est pas au niveau requis.

Explication : Le pilote de périphérique netinet et le démon fwlogd n'ont pas le même niveau.

Action de l'utilisateur : Corrigez le problème. Vous devrez peut-être réamorcer la machine après avoir modifié le niveau du pare-feu.

ICA1015 Erreur pendant l'appel ioctl (SIOCGFWLOG) : *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1016 Impossible de trouver la file d'attente différée actuelle.

Explication : Voir les informations associées précédant immédiatement ce message.

ICA1017 Erreur renvoyée par l'appel SIOCGFWLOG ioctl().

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1018 Erreur fwlogd fatale - *fonction en échec* **:** *message d'erreur système*

Explication : Le serveur fwlogd n'a pas pu exécuter la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon fwlogd.

ICA1019 Sortie avec erreur inattendue de code retour *code_retour_fw_interne*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

ICA1020 Erreur fwlogd fatale - *fonction en échec* **: code retour = 0x***code retour fonction*

Explication : Le serveur fwlogd n'a pas pu exécuter la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon fwlogd.

ICA1021 Erreur lors de l'ouverture de */dev/ipsp_poif* **:** *numéro d'erreur*

Explication : Le pilote de périphérique indiqué n'a pas été installé.

Action de l'utilisateur : Si le code du pare-feu a été installé, contrôlez l'existence de messages d'erreur dans le fichier /tmp/rc/net.out.

ICA1022 Erreur de la vérification du support de filtrage.

Explication : Le support de filtrage ne peut pas être vérifié par suite d'une erreur enregistrée avant ce message.

ICA1023 Erreur pendant l'appel ioctl (SIOCGFWLVL) : *numéro d'erreur*

Explication : L'erreur système signalée a été rencontrée au cours du lancement du démon de journalisation des filtres.

Action de l'utilisateur : Procédez à l'une des opérations suivantes :

- Pour AIX : Vérifiez que le pilote de périphérique netinet du pare-feu a été installé avec le niveau requis et que la machine a été réamorcée après l'installation.
- Pour OS/390 : Vérifiez que TCP/IP a été installé avec le niveau requis et a été initialisé avec l'instruction de configuration **IPCONFIG FIREWALL**.

ICA1024 Erreur pendant l'écriture sur le fichier */etc/security/fwlogd.pid* **:** *numéro d'erreur*

Explication : Suite à l'erreur système signalée, fwlogd n'a pas pu écrire le fichier indiqué.

Action de l'utilisateur : Corrigez le problème signalé et réamorcez le démon de journalisation des filtres.

ICA1032 Règles de filtrage mises à jour à *heure* **le** *date*

Explication : Les règles de filtrage des paquets IP ont été mises à jour.

ICA1033 Support de filtre (niveau *version.édition***) initialisé à** *heure* **le** *date*

Explication : Le support de filtrage du pare-feu a été initialisé.

ICA1034 Support de filtre désactivé à *heure* **le** *date*

Explication : Le filtrage des paquets IP utilise à présent les règles de filtrage par défaut au lieu de celles définies dans le fichier /etc/security/fwfilters.cfg.

ICA1035 Etat de la journalisation des paquets défini à *activé/désactivé* **à** *heure* **le** *date*

Explication : Le statut de la journalisation des paquets a changé. Le message indique le statut courant avec une horodate.

ICA1036 *#:num_règle R: type_règle direction: interface s:adr_source d: adr_dest p: protocole code: port_source/type_icmp code: port_dest/code_icmp r:routage/local a: sécurisé/non_sécurisé f:oui/non T:id_tunnel e:C/D/n l:longueur_paquet*

Explication : Enregistrement de fichier journal mentionnant un paquet IP traité et la règle de filtrage correspondante. Pour que cet enregistrement s'écrive, le paramètre de contrôle de journalisation de la règle de filtrage correspondante doit avoir la valeur *Oui*. Dans le cas d'un paquet IP fragmenté, les informations relatives aux ports/type ICMP/code apparaissent pour le paquet d'en-tête mais sont remplacées par des 0 pour les autres paquets.

ICA1037 *#:num_règle action adr_src masque_src adr_dest masque_dest protocole valeur op_logique valeur op_ logique type_interface sens_routage l= contr_journal f=contr_fragmentt= ID_tunnel alg_chiff alg_auth*

Explication : Lorsque les règles de filtrage sont mises à jour, les règles activées sont enregistrées dans le fichier journal. Ce message de fichier journal porte sur l'une des règles activées.

ICA1038 **Générateur de clé de session initialisé, utilise le port de socket de :***numéro_port* **et le port de connexion maître :***numéro_port***.**

Explication : Démarrage du tunnel de chiffrement avec les numéros de port UDP spécifiés, comme défini dans /etc/services.

ICA1039 **Règle de sécurité (re)définie sous le nom :**

Explication : Antémémoire de la règle de sécurité (re)définie avec le fichier /etc/security/fwpolicy. Les lignes suivantes affichent le contenu de la nouvelle antémémoire de la règle.

ICA1040 >**Enoncé de la règle de sécurité :** *début_tunnel extrémité_tunnel ID_tunnel code_chiffrement/code_authentification*

Explication : La ligne journalisée est extraite du fichier /etc/security/fwpolicy.

ICA1041 **Spécification du contexte supprimée pour le tunnel :***ID_tunnel*

Explication : Le contexte de tunnel correspondant à l'ID indiqué n'est plus opérationnel.

ICA1042 **La(les) spécification(s) de contexte(s) suivante(s) a(ont) été définie(s) :**

Explication : Les spécifications de contexte de tunnel sont en cours de définition comme indiqué dans les enregistrements de journal suivants.

ICA1043 >**ID_tunnel :***numéro***, adr_src :***adr_IP***, adr_dest :***adr_IP***, chiffrement :***algorithme*

Explication : Le message affiche les attributs spécifiques au contexte de tunnel activé.

ICA1044 **Avertissement - Compteur de l'hôte : IP(***Adresse IP***), dépassement de limite**

Explication : Les hôtes sécurisés essayant de se connecter à la machine du pare-feu sont trop nombreux.

Réaction du système : Passage des connexions

ICA1045 **Dépassement de limite TCP :** *Adresse IP***(***Port***)->***Adresse IP***(***Port***) rejetés.**

Explication : Les sessions TCP utilisant la machine du pare-feu sont trop nombreuses.

Réaction du système : Rejet des connexions

ICA1046 Dépassement de limite UDP : *Adresse IP*(*Port*)->*Adresse IP*(*Port*) **rejetés.**

Explication : Les sessions UDP utilisant la machine du pare-feu sont trop nombreuses.

Réaction du système : Rejet des connexions

ICA1047 Avertissement - Délai de grâce : les sessions TCP sont trop nombreuses,*Adresse IP*(*Port*)->*Adresse IP*(*Port*) **transmis.**

Explication : Les sessions TCP utilisant la machine du pare-feu sont trop nombreuses.

Réaction du système : Passage des connexions

ICA1048 Avertissement - Délai de grâce : les sessions UDP sont trop nombreuses,*Adresse IP*(*Port*)->*Adresse IP*(*Port*) **transmis.**

Explication : Les sessions UDP utilisant la machine du pare-feu sont trop nombreuses.

ICA1049 Progiciel IPSEC non valable : s:*Adresse IP* **d:***Adresse IP* **protocole :***Protocole* **spi :***Index des paramètres de sécurité*

Explication : Le progiciel ipsec ne peut pas être désencapsulé par le pare-feu destinataire.

Action de l'utilisateur : Assurez-vous que la définition de tunnel a été exportée correctement et a été activée sur chaque pare-feu.

ICA1050 Spécification supprimée pour le tunnel :*ID_tunnel*

Explication : La spécification de tunnel correspondant à l'ID indiqué n'est plus opérationnelle.

ICA1051 La(les) spécification(s) de tunnel suivante(s) a(ont) été définie(s) :

Explication : Les spécifications de tunnel sont en cours de définition comme indiqué dans les enregistrements de journal suivants.

ICA1052 >**ID_tunnel :***numéro***, adr_src :***adresse_IP***, adr_dest :***adresse_IP***, chif_scr :***algorithme* **chif_rem :***algorithme* **mac_src :***algorithme* **mac_rem :***algorithme* **mac_chif_src :***algorithme* **mac_chif_rem :***algorithme* **règ_src :***règle* **règ_rem :***règle* **mode :***mode_transport*

Explication : Le message affiche les attributs spécifiques au tunnel activé.

ICA1200 Arrêt du démon de journalisation suite aux erreurs ci-dessus.

Explication : Suite aux erreurs enregistrées avant ce message, le démon fwlogd a été arrêté.

Réaction du système : La journalisation des filtres IP ne sera pas activée.

Action de l'utilisateur : Corrigez les erreurs signalées et relancez fwlogd.

ICA1260 Arrêt du démon de journalisation de filtrage à *heure* **le** *date***, suite à la réception d'un signal** *fin***.**

Explication : Le démon fwlogd a reçu le signal de fin indiqué et s'arrête.

ICA1305 \"inconnu\"

Explication : Au cours du formatage d'un paquet IP pour syslog, il a été trouvé un enregistrement contenant une spécification de protocole inconnu. Les protocoles reconnus sont IP, ICMP, TCP, UDP et IPSP. Notez que IPSP est l'appellation IBM pour les paquets chiffrés passés via un tunnel.

ICA1400 Erreur fwtimernat fatale - *fonction en échec* **:** *message d'erreur système*

Explication : Le serveur fwtimernat n'a pas pu exécuter la fonction indiquée. Le serveur fwtimernat a été arrêté.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon fwtimernat.

ICA1401 Erreur fwtimernat fatale - *fonction en échec* **: code retour = 0x***code retour fonction*

Explication : Le serveur fwtimernat n'a pas pu exécuter la fonction indiquée. Le serveur fwtimernat a été arrêté.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon fwtimernat.

ICA1402 Erreur fwtimernat fatale - *fonction en échec* **:** *message d'erreur*

Explication : Le serveur fwtimernat n'a pas pu exécuter la fonction indiquée. Le serveur fwtimernat a été arrêté.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon fwtimernat.

ICA2000 Nouvelle session FTP sur *adresse_IP* **depuis** *adresse_IP* **(site non sécurisé).**

Explication : Démarrage d'une session FTP depuis un site non sécurisé.

ICA2001 Echec d'authentification de l'utilisateur *nom* **(inconnu) depuis** *net ftp* **:***adresse_IP***.**

Explication : Un utilisateur sans compte a tenté une connexion relais FTP à partir du réseau.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de créer un compte relais.

ICA2002 Echec d'authentification de l'utilisateur *nom* **avec la méthode** *méthode d'authentification* **depuis le** *réseau* **:***nom d'hôte***.**

Explication : Le pare-feu ne peut pas authentifier le nom utilisateur indiqué avec la méthode d'authentification spécifiée.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2003 Aucun shell configuré pour *nom d'utilisateur***.**

Explication : L'utilisateur indiqué a tenté une connexion relais alors qu'aucun shell de connexion n'a été défini.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de modifier le profil de connexion de cet utilisateur.

ICA2004 Evénement d'audit inconnu de 0x*valeur_hex* **reçu.**

Explication : Une requête d'audit inconnue a été réceptionnée par le module tcpip_audit.c.

ICA2005 Erreur d'écriture vers le client : *numéro d'erreur***.**

Explication : Impossible de communiquer avec le client. Reportez-vous au message système journalisé.

ICA2006 ptelnetd: auditproc: *numéro d'erreur***.**

Explication : L'erreur indiquée a été retournée par le processus d'audit de Telnet. Possibilité d'altération des fichiers système.

ICA2007 ptelnetd: niveau d'urgence=*valeur***.**

Explication : Erreur inconnue détectée. Possibilité d'altération des fichiers système.

ICA2008 Utilisateur non inscrit dans le pare-feu *nom* **depuis :***adresse_IP* **a démarré une session telnet.**

Explication : Un utilisateur sans compte a tenté une connexion relais Telnet.

Réaction du système : Utilise l'authentification générique.

ICA2009 /bin/login: *numéro d'erreur***.**

Explication : Erreur fatale au cours de la connexion système. Reportez-vous au message d'erreur système indiqué.

ICA2010 Connexion sur *adresse_IP* **par** *adresse_IP* **(non sécurisé).**

Explication : Établissement d'une connexion entre les adresses IP indiquées via l'interface non sécurisée.

ICA2011 Connexion sur *adresse_IP* **par** *adresse_IP* **(sécurisé).**

Explication : Établissement d'une connexion entre les adresses IP indiquées via l'interface sécurisée.

ICA2012 Nouvelle session FTP sur *adresse_IP* **depuis** *adresse_IP* **(site sécurisé).**

Explication : Démarrage d'une session FTP.

ICA2013 Nouvelle session Telnet sur *adresse_IP* **depuis** *adresse_IP***.**

Explication : Établissement d'une session Telnet.

ICA2014 Option *valeur* **non supportée.**

Explication : L'indicateur mentionné n'est pas pris en charge. Reportez-vous au message précédent.

ICA2015 Option -*valeur* **non supportée.**

Explication : L'indicateur mentionné n'est pas pris en charge. Reportez-vous au message précédent.

ICA2016 ID utilisateur distant \"*nom***\".**

Explication : Requête de connexion FTP pour l'utilisateur indiqué.

ICA2017 Déboguez *- à ligne***.**
ICA2018 Clé SNK non trouvée pour l'utilisateur *nom***.**

Explication : La valeur de la clé SecureNetKey correspondant à l'ID utilisateur mentionné n'a pas été identifiée.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de vérifier l'existence d'un problème de configuration de connexion.

ICA2019 Clé SNK lue incorrectement pour l'utilisateur *nom***.**

Explication : La clé SecureNetKey correspondant à l'ID utilisateur mentionné n'est pas composée de valeurs octales.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de vérifier l'existence d'un problème de configuration de connexion.

ICA2020 /usr/bin/fwuserau ou /usr/bin/fwuserpt n'existe pas.

Explication : Arrêt de la procédure d'authentification par méthode fournie par l'utilisateur.

Réaction du système : Abandon de la procédure d'authentification.

Action de l'utilisateur : Assurez-vous que /usr/bin/fwuserau et /usr/bin/fwuserpt existent effectivement et que leur propriétaire est root. Si aucun de ces fichiers n'existe, créez un fichier exécutable nommé /usr/bin/fwuserau ou /usr/bin/fwuserpt avec un compilateur compatible avec le système d'exploitation du pare-feu.

ICA2021 Tentative de connexion sur l'hôte distant *nom***avec l'ID utilisateur** *nom***.**

Explication : Nouvelle connexion FTP en cours d'établissement.

ICA2022 Tentative de connexion sur l'hôte distant *nom***.**

Explication : Nouvelle connexion FTP en cours d'établissement.

ICA2023 Syntaxe : ptelnetd [-n] [-s].

Explication : Utilisation d'un paramètre inconnu lors du lancement du démon ptelnet.

Action de l'utilisateur : Utilisez les paramètres -n et/ou -s exclusivement.

ICA2024 Utilisateur *nom* **authentifié avec la méthode** *méthode* **depuis le** *réseau* **:***nom d'hôte***.**

Explication : Le pare-feu a authentifié le nom utilisateur indiqué avec la méthode d'authentification spécifiée.

ICA2025 Utilisateur *nom* **connecté avec la méthode** *méthode* **depuis le** *réseau* **:***nom d'hôte***.**

Explication : Utilisateur FTP connecté.

ICA2026 Utilisateur *nom* **arrivé à échéance après** *n* **secondes à** *heure***.**

Explication : Fin du délai d'attente pour la tentative de connexion de cet utilisateur. Possibilité de problème de routage dans le réseau ou d'indisponibilité du système hôte distant.

ICA2027 Connexion depuis *hôte distant* **à** *heure***.**

Explication : Établissement d'une nouvelle connexion FTP sur le pare-feu.

ICA2028 Tentative de connexion FTP sur *adresse_IP* **depuis** *adresse_IP* **refusée. Cette machine ne supporte pas les FTP effectués depuis un site non sécurisé.**

Explication : Indique généralement une tentative de connexion FTP sur le pare-feu via l'interface non sécurisée.

Réaction du système : Rejet de la connexion.

ICA2029 Erreur système avec l'erreur = - **dans** *dans* **ligne** *ligne***.**

Explication : Problème rencontré lors de l'exécution d'un appel système.

Réaction du système : Arrêt de l'exécution.

Action de l'utilisateur : Consultez le fichier journal, recherchez la signification du code d'erreur et corrigez le problème. Contactez l'assistance IBM si vous n'y parvenez pas.

ICA2030 Code retour de l'appel de fonction = - **dans** *dans* **ligne** *ligne***.**

Explication : Problème rencontré lors de l'appel de fonction.

Réaction du système : Retour d'un message d'erreur.

Action de l'utilisateur : Consultez le fichier journal, recherchez la signification du code retour et corrigez le problème. Contactez l'assistance IBM si vous n'y parvenez pas.

ICA2031 Code retour de l'appel de fonction sdi creadcfg() = -**.**

Explication : Problème rencontré lors de l'appel de fonction.

Réaction du système : Retour d'un message d'erreur.

Action de l'utilisateur : Recherchez une explication dans la référence de sdi.

ICA2032 Connexion perdue.

Explication : La connexion FTP a été perdue.

Action de l'utilisateur : Rétablissez la session.

ICA2033 Code retour de l'appel de fonction sdi sd_init = -**.**

Explication : Problème rencontré lors de l'appel de fonction.

Réaction du système : Retour d'un message d'erreur.

Action de l'utilisateur : Recherchez une explication dans la référence de sdi.

ICA2034 Code retour de l'appel de fonction sdi sd_check = -**.**

Explication : Problème rencontré lors de l'appel de fonction.

Réaction du système : Retour d'un message d'erreur.

Action de l'utilisateur : Recherchez une explication dans la référence de sdi.

ICA2035 setsockopt() : *numéro d'erreur***.**

Explication : Erreur système lors de l'appel de la fonction setsocketopt.

ICA2036 Session Telnet *ID session* **démarrée pour l'utilisateur** *ID utilisateur* **(***adr IP source* **:***adr IP dest***).**

Explication : Message généré au démarrage de toute session Telnet. Une session peut commencer lorsque le pare-feu a pris connaissance de l'ID utilisateur et des adresses IP source et destination. L'ID de session est un identificateur unique généré par le pare-feu.

ICA2037 Tentative de connexion de l'utilisateur fwdfuser ou fwdpuser interdite.

Explication : Les utilisateurs fwdfuser et fwdpuser sont des utilisateurs réservés qui ne doivent pas être utilisés.

Réaction du système : La connexion est refusée.

Action de l'utilisateur : L'administrateur devrait rechercher qui se sert de ces ID utilisateur.

ICA2038 ttloop : processus pair mort : *numéro d'erreur***.**

Explication : Erreur lors du vidage de la mémoire tampon de sortie du réseau. Il semble que le processus pair soit mort.

ICA2039 ttloop : lecture : *numéro d'erreur***.**

Explication : Erreur lors du vidage de la mémoire tampon de sortie du réseau.

ICA2040 Authentification définie par mot de passe - "aucun" ou "SNK" ne sont pas admis pour l'ID utilisateur fwdfuser.

Explication : fwdfuser est un ID utilisateur réservé et ne doit pas utiliser les méthodes d'authentification "mot de passe" ou "aucun".

Réaction du système : La connexion est refusée.

Action de l'utilisateur : L'administrateur doit changer la méthode d'authentification associée à l'ID utilisateur fwdfuser.

ICA2041 Session FTP *ID session* **démarrée pour** *ID utilisateur* **(***adr IP source* **:***adr IP dest***).**

Explication : Message généré au démarrage de toute session FTP. Une session peut commencer lorsque le pare-feu a pris connaissance de l'ID utilisateur et des adresses IP source et destination. L'ID de session est un identificateur unique généré par le pare-feu.

ICA2042 req_rsp_code est défini de manière incorrecte sur FW_AUTH_REQ.

Explication : La fonction fw_tn_authenticate n'est pas autorisée à définir req_rsp_code sur FW_AUTH_REQ.

Réaction du système : Procédure d'authentification abandonnée.

Action de l'utilisateur : Modifiez fw_tn_authenticate, recréez la bibliothèque fwuser.o et intégrez-la au pare-feu.

ICA2043 Mot de passe introuvable pour *nom_utilisateur***.**

Explication : Cet utilisateur requiert une authentification par mot de passe ; aucun mot de passe n'a été trouvé.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2044 Heure spécifiée (*valeur***) incorrecte pour -t.**

Explication : L'heure indiquée contient des valeurs hors de la plage numérique 0 à 9 ou excède la valeur maximale autorisée.

ICA2045 Option -T non supportée sur le pare-feu.

Explication : L'option indiquée n'est pas prise en charge.

ICA2046 Option -k non supportée sur le pare-feu.

Explication : L'option indiquée n'est pas prise en charge.

ICA2047 Option -s non supportée sur le pare-feu.

Explication : L'option indiquée n'est pas prise en charge.

ICA2048 Option -u non supportée sur le pare-feu.

Explication : L'option indiquée n'est pas prise en charge.

ICA2049 Indicateur -*valeur* **inconnu ignoré.**

Explication : Le paramètre indiqué a été spécifié et n'a pas été reconnu.

ICA2050 Paramètre *valeur* **inconnu.**

Explication : La valeur indiquée a été spécifiée comme option et n'a pas été reconnue.

ICA2051 Erreur de conversion de l'adresse dans adr_adapt.

Explication : L'adresse IP indiquée n'est pas valide.

Action de l'utilisateur : Possibilité d'altération du fichier /etc/security/fwsecadpt.cfg. Supprimez le fichier, reconfigurez la ou les interfaces sécurisées et réinitialisez les filtres.

ICA2052 afopen n'a pas pu ouvrir /etc/security/login.cfg : *numéro d'erreur***.**

Explication : Impossible d'authentifier l'utilisateur indiqué ; erreur d'ouverture sur le fichier mentionné.

ICA2053 Impossible d'ouvrir un fichier d'interface sécurisée.

Explication : Une interface sécurisée n'a pas été configurée.

Action de l'utilisateur : Utilisez les commandes IBM Firewall ou les panneaux SMIT pour définir la ou les interfaces sécurisées.

ICA2054 Code retour enduserdb =*valeur***,** *numéro d'erreur***.**

Explication : Le code d'erreur système indiqué a été reçu suite à une tentative de récupération d'un profil de connexion utilisateur.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de vérifier le compte de connexion.

ICA2055 getpeername() (*nom invoqué***) :** *numéro d'erreur***.**

Explication : Une erreur système s'est produite quand le démon ftp a tenté d'obtenir le nom de la paire de sockets.

ICA2056 getsockname() (*nom invoqué***) :** *numéro d'erreur***.**

Explication : Une erreur système s'est produite quand le démon ftp a tenté d'obtenir le nom de la socket.

ICA2057 getuser shell non sécurisé, code retour = *valeur* **pour** *ID_utilisateur***,** *numéro d'erreur***.**

Explication : Le code d'erreur système indiqué a été reçu suite à une tentative de récupération d'un nom de shell pour établir une connexion depuis le côté non sécurisé du pare-feu.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de définir un shell dans votre profil de connexion utilisateur.

ICA2058 getuser shell sécurisé, code retour = *valeur* **pour** *ID_utilisateur***,** *numéro d'erreur***.**

Explication : Le code d'erreur système indiqué a été reçu suite à une tentative de récupération d'un nom de shell pour établir une connexion depuis le côté sécurisé du pare-feu.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de définir un shell dans votre profil de connexion utilisateur.

ICA2059 ioctl() : *numéro d'erreur***.**

Explication : Erreur système pendant l'appel ioctl() de SIOCSPGRP.

ICA2060 ptelnetd: ftok pour mémoire partagée n'a pas abouti.

Explication : Impossible d'attribuer un segment de mémoire partagée.

Action de l'utilisateur : Contactez l'administrateur du pare-feu ; problème de mémoire probable.

ICA2061 ptelnetd: shmat pour mémoire partagée n'a pas abouti.

Explication : Impossible d'attribuer un segment de mémoire partagée.

Action de l'utilisateur : Contactez l'administrateur du pare-feu ; problème de mémoire probable.

ICA2062 ptelnetd: shmget pour mémoire partagée n'a pas abouti.

Explication : Impossible d'attribuer un segment de mémoire partagée.

Action de l'utilisateur : Contactez l'administrateur du pare-feu ; problème de mémoire probable.

ICA2063 setsockopt() (SO_DEBUG) : *numéro d'erreur***.**

Explication : Le message d'erreur indiqué a été retourné par l'appel système 'setsockopt'.

ICA2064 setsockopt() (SO_KEEPALIVE) : *numéro d'erreur***.**

Explication : Le message d'erreur indiqué a été retourné par l'appel système 'setsockopt'.

ICA2065 Code retour setuser =*valeur***,** *numéro d'erreur***.**

Explication : Mauvais code retour retourné par un appel système pour la raison indiquée.

ICA2066 signal() : *numéro d'erreur***.**

Explication : Une erreur système s'est produite quand le démon ftp a tenté d'établir le gestionnaire de signaux.

ICA2067 Erreur d'initialisation fatale de pftpd - bind() : *numéro d'erreur*

Explication : L'initialisation du serveur pftpd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon pftpd. La cause la plus probable de cet incident est qu'un autre démon ftp est déjà en écoute sur le port FTP standard (port 21).

ICA2068 Erreur d'initialisation fatale de pftpd - listen() : *numéro d'erreur*

Explication : L'initialisation du serveur pftpd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon pftpd.

ICA2069 Erreur fatale de pftpd - accept() principal : *numéro d'erreur*

Explication : La routine principale du serveur pftpd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon pftpd.

ICA2070 Erreur d'initialisation fatale de pftpd - socket() : *numéro d'erreur*

Explication : L'initialisation du serveur pftpd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon pftpd.

ICA2071 Connexion refusée - nombre maximal de connexions atteint.

Explication : Le serveur pftpd ne peut pas créer d'autre session FTP parce que le nombre maximal autorisé a déjà été atteint.

Réaction du système : La connexion est refusée.

Action de l'utilisateur : Attendez la fin d'une des connexions en cours et réessayez.

ICA2072 Le fichier de configuration ftp (*nom de fichier***) n'est pas disponible.**

Explication : Le démon ftp a essayé d'ouvrir le fichier de configuration ftp indiqué qui, soit n'existe pas, soit ne peut pas être ouvert.

Réaction du système : Le démon ftp utilise la configuration par défaut pour les traitements.

Action de l'utilisateur : Aucune, sauf si le fichier est censé exister, auquel cas l'utilisateur doit le créer ou le déplacer vers l'emplacement mentionné dans le message.

ICA2073 Impossible d'obtenir de la mémoire pour la table des langues FTP.

Explication : L'espace mémoire nécessaire à l'insertion d'une instruction REPLYLANGUAGE dans le fichier de configuration ftp n'a pas pu être obtenu.

Réaction du système : Poursuite du traitement.

Action de l'utilisateur : Augmentez la taille de la région ou éliminez des entrées dans le fichier de configuration.

ICA2074 Fin du traitement de l'instruction de configuration FTP : *instruction de configuration*

Explication : ftp a traité l'instruction de configuration indiquée.

Réaction du système : Poursuite du traitement.

Action de l'utilisateur : Aucune

ICA2075 FTP pour *ID utilisateur* **(***adr IP source* **:***adr IP dest***),** *opération nom de fichier***,** *nombre d'octets* **octets. sid :** *ID session***.**

Explication : Message généré pour chaque transfert de fichier lors de sessions FTP ouvertes. Le SID (ID de session) est un identificateur unique généré par le pare-feu au démarrage de toute session.

ICA2076 Session FTP *ID session* **terminée pour** *ID utilisateur* **(***adr IP source* **:***adr IP dest***),** *durée* **secondes,** *nombre d'octets* **octets.**

Explication : Message généré au terme de toute session FTP. Le SID (ID de session) est un identificateur unique généré par le pare-feu au démarrage de toute session.

ICA2077 Session Telnet *ID session* **terminée pour** *ID utilisateur* **(***adr IP source* **:***adr IP dest***),** *nombre d'octets* **octets.**

Explication : Message généré au terme de toute session Telnet. Le SID (ID de session) est un identificateur unique généré par le pare-feu au démarrage de toute session.

ICA2078 Utilisateur relais *utilisateur* **déconnecté - inactif depuis** *durée* **minutes.**

Explication : La session a dépassé le délai d'inactivité autorisé.

ICA2079 Attention : Tentative de connexion non autorisée sur *adresse_IP* **par** *adresse_IP***.**

Explication : Indique généralement une tentative de connexion sur le pare-feu via l'interface non sécurisée.

Réaction du système : Rejet de la connexion.

ICA2080 Erreur de syntaxe (*raison***), près de la colonne** *colonne* **dans le fichier de configuration FTP, ligne** *ligne* **:** *instruction de configuration*

Explication : L'instruction de configuration ftp comporte une erreur à la ligne indiquée. La nature et l'emplacement de l'erreur détectée sont indiqués dans le message.

Réaction du système : L'instruction est ignorée.

Action de l'utilisateur : Corrigez l'instruction erronée contenue dans le fichier de configuration ftp.

ICA2081 Aucun des catalogues de messages spécifiés par les instructions de configuration FTP n'est utilisable.

Explication : Les tentatives d'ouverture des catalogues de messages spécifiés par les instructions de configuration ftp REPLYLANGUAGE n'ont pas abouti. Aucun catalogue de messages client ne peut être utilisé.

Réaction du système : Le catalogue de messages client utilise obligatoirement l'anglais dans le répertoire C.

Action de l'utilisateur : Assurez-vous que des fichiers de catalogue sont présents dans chacun des répertoires de langues référencés dans les instructions REPLYLANGUAGE de la configuration FTP. Vérifiez également que la variable d'environnement NLSPATH est définie comme il convient pour permettre le remplacement du sous-répertoire par la variable d'environnement LANG (%L) comme par le nom de catalogue (%N).

ICA2082 Impossible de définir la variable d'environnement ftp LANG dans *sous-répertoire***, raison :** *raison*

Explication : Une erreur système (expliquée dans "raison") s'est produite quand le démon ftp a tenté d'associer la variable d'environnement LANG au sous-répertoire indiqué.

Réaction du système : Poursuite du traitement. La reprise après incident peut générer d'autres messages.

Action de l'utilisateur : D'après la raison indiquée, déterminez s'il s'agit d'une erreur système ou d'une erreur de programmation.

ICA2083 Impossible d'ouvrir le catalogue de messages clients ftp dans le répertoire *sous-répertoire***, raison :** *raison*

Explication : Le démon ftp n'a pas pu ouvrir le catalogue de messages contenu dans le sous-répertoire indiqué. La raison donnée est le code d'erreur retourné par catopen().

Réaction du système : Poursuite du traitement. La reprise après incident peut générer d'autres messages.

Action de l'utilisateur : Assurez-vous qu'un catalogue est présent dans le répertoire de langue spécifié. Vérifiez également que la variable d'environnement NLSPATH est définie comme il convient pour permettre le remplacement du sous-répertoire (%L) et celui du nom de catalogue (%N).

ICA2084 Catalogue de messages client ftp utilisant obligatoirement l'anglais via le sous-répertoire C.

Explication : Suite aux erreurs signalées précédemment, le démon ftp a forcé la catalogue de messages client à adopter l'anglais via le sous-répertoire C.

Réaction du système : Si la variable LANG peut être associée au sous-répertoire C, le traitement du catalogue de messages se poursuit. Dans le cas contraire, le programme est arrêté.

Action de l'utilisateur : Corrigez les erreurs signalées dans les messages précédents. Si le programme existait déjà, créez le catalogue de messages dans le sous-répertoire C et affectez la valeur qui convient à la variable d'environnement NLSPATH.

ICA2085 Interruption de la session Telnet pour l'ID processus *ID processus* **(***adresse IP source***).**

Explication : Message généré au terme de toute session Telnet.

ICA2086 Défaut de configuration du fichier utilisateur ; utilisateur *utilisateur* **sans clé (***clé***).**

Explication : Le démon ftpd a trouvé l'utilisateur demandé dans le fichier des utilisateurs mais n'a pas trouvé la clé correspondante ; défaut de configuration du fichier des utilisateurs.

Action de l'utilisateur : Corrigez le problème avec les commandes IBM Firewall ou avec les panneaux SMIT.

ICA2087 ftpd n'a pas trouvé l'utilisateur *utilisateur* **dans le fichier de configuration utilisateur.**

Explication : Le nom utilisateur spécifié n'a pas été configuré ou le fichier user.cfg est altéré.

Action de l'utilisateur : Corrigez le problème avec les commandes IBM Firewall ou avec les panneaux SMIT.

ICA2088 ftpd n'a pas pu ouvrir le fichier de configuration utilisateur.

Explication : ftpd a appelé la fonction fopen qui n'a pas abouti faute d'avoir pu ouvrir le fichier de configuration utilisateur.

Action de l'utilisateur : Assurez-vous que le fichier de configuration utilisateur (user.cfg par défaut) est accessible. Utilisez les commandes IBM Firewall ou les panneaux SMIT.

ICA2089 Le type d'autorisation spécifié dans le fichier utilisateur (*type d'autorisation***) ne correspond à aucune des entrées de la table (struct tab2 authtab).**

Explication : Le type d'autorisation associé à l'utilisateur spécifié dans user.cfg ne correspond à aucun type pris en charge (deny, none, snk, sdi, password, etc.)

Action de l'utilisateur : Vérifiez l'intégrité ou la configuration du fichier user.cfg ; corrigez le problème avec les commandes IBM Firewall ou avec les panneaux SMIT.

ICA2090 Echec d'authentification de l'utilisateur '*nom d'utilisateur***' depuis** *IP client* **- le fichier user.cfg contient l'instruction KEY=DENY.**

Explication : La procédure d'authentification a échoué en raison des spécifications du fichier user.cfg définies par l'administrateur du pare-feu.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2091 L'utilisateur '*nom d'utilisateur***' n'est pas autorisé à utiliser FTP avec le port non sécurisé (***IP pare-feu***).**

Explication : L'utilisateur a tenté une connexion FTP sur le serveur de pare-feu via un port non sécurisé (NSP) ; pour tous les utilisateurs NSP, la clé 'fwnsftp' doit être associée à un type d'autorisation valide (dans le fichier user.cfg).

Action de l'utilisateur : Vérifiez l'intégrité ou la configuration du fichier user.cfg ; corrigez le problème avec les commandes IBM Firewall ou avec les panneaux SMIT.

ICA2092 Erreur interne : Échec de nt_gwauth().

Explication : La fonction nt_gwauth() retourne normalement l'une des trois valeurs AUTHENTICATED, NOT_AUTHENTICATED ou DENY. Dans le cas présent, nt_gwauth a retourné un entier non valide.

ICA2093 L'utilisateur '*nom d'utilisateur***' n'est pas autorisé à utiliser FTP avec le port sécurisé (***numéro de port***).**

Explication : L'utilisateur a tenté une connexion FTP sur le serveur de pare-feu via un port sécurisé (SP) ; pour tous les utilisateurs SP, la clé 'fwsftp' doit être associée à un type d'autorisation valide (dans le fichier user.cfg).

Action de l'utilisateur : Vérifiez l'intégrité ou la configuration du fichier user.cfg ; corrigez le problème avec les commandes IBM Firewall ou avec les panneaux SMIT.

ICA2094 Echec de la connexion : format attendu : "PASS <**mot de passe**>**" après : "USER** <*nom d'utilisateur*>**" ; reçu** *cmd incorrecte***.**

Explication : La procédure d'authentification a échoué car le client ftp n'a pas utilisé le format attendu (PASS 'mot de passe' conformément à la RFC959)

Action de l'utilisateur : Tapez "user <nom utilisateur>" et entrez le mot de passe qui convient. Contactez l'administrateur du pare-feu.

ICA2095 Echec de la connexion : (via la méthode *méthode d'authentification***) échec d'authentification de l'utilisateur '***nom d'utilisateur***' depuis** *IP client* **(site client).**

Explication : La procédure d'authentification a échoué suite à une entrée non valide (par le client pour le type d'authentification spécifié) telle qu'un mot de passe incorrect, une clé SNK non valide, etc.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2096 Authentifié : (via la méthode *méthode d'authentification***) authentification réussie de l'utilisateur '***nom d'utilisateur***' depuis** *IP client* **(site client).**

Explication : L'authentification a abouti.

ICA2097 httpd --> Démarrage du serveur relais HTTP version *Version du relais HTTP***.**

Explication : Démarrage du serveur relais HTTP pour accès au Web.

ICA2098 httpd --> Arrêt du serveur relais HTTP.

Explication : Arrêt du serveur relais HTTP pour accès au Web.

ICA2099 httpd --> Statut : <*Code statut HTTP*> **depuis le client** <*adresse IP*>**, ayant demandé** <**\"***requête GET HTTP***\"**> **pour** <*nombre d'octets*> **octets.**

Explication : Statut d'une requête HTTP de fichier adressée par un fichier via le serveur relais. Pour plus d'informations sur le code de statut, reportez-vous aux documents sur HTTP 1.0 (RFC 1945) ou HTTP 1.1 (RFC 2068) (ou aux RFC les remplaçant) disponibles sur les différents sites Internet dont ds.internic.net.

ICA2100 L'adresse de la socket est égale à zéro.

Explication : La requête locale comporte une adresse de destination non valide.

ICA2101 Erreur dans la famille d'adresses de la socket : *type_famille_sin***.**

Explication : La requête locale comporte un type de famille d'adresses non valide.

ICA2102 Erreur lors de l'initialisation de l'ODM : *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_initialize() portant sur l'ODM (gestionnaire d'objets).

ICA2103 Erreur lors de la définition du chemin d'accès par défaut de l'ODM : *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_path() portant sur l'ODM (gestionnaire d'objets). Classe d'objets : OCSvhost.

ICA2104 Erreur lors du verrouillage de la base de données de l'ODM : *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_lock() portant sur l'ODM (gestionnaire d'objets).

ICA2105 Erreur lors de l'ouverture de l'objet ODM *Attribut_personnalisé* **:** *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_open_class() portant sur l'ODM (gestionnaire d'objets).

ICA2106 Erreur lors de la recherche de l'objet ODM *hôte_virtuel_OCS* **:** *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_get_first() portant sur l'ODM (gestionnaire d'objets). Classe d'objets : OCSvhost.

ICA2107 Erreur lors de la fermeture de l'objet ODM *hôte_virtuel_OCS* **:** *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_close_class() portant sur l'ODM (gestionnaire d'objets). Classe d'objets : OCSvhost.

ICA2108 Erreur lors du déverrouillage de la base de données de l'ODM : *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_unlock() portant sur l'ODM (gestionnaire d'objets).

ICA2109 Erreur lors de l'arrêt de l'ODM : *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_terminate() portant sur l'ODM (gestionnaire d'objets).

ICA2110 Erreur lors de la recherche du serveur par son nom : *numéro d'erreur***.**

Explication : Erreur de la fonction getservbyname(). Le service de contrôle des connexions du système hôte, lm, n'est pas défini correctement dans le fichier /etc/services.

ICA2111 byname() erreur : *numéro d'erreur***.**

Explication : Erreur de la fonction gethostbyname(). Le nom du système hôte n'est pas spécifié correctement dans le fichier /etc/hosts.

ICA2112 Nom de protocole incorrect : *nom_protocole***.**

Explication : Le nom de protocole spécifié dans la classe d'objets ODM "OCSvhost" n'est pas pris en charge.

ICA2113 Erreur lors de l'ouverture de la socket sur le contrôle de journalisation : *numéro d'erreur***.**

Explication : Erreur de la fonction socket() sur le système hôte où réside le contrôle de journalisation.

ICA2114 Erreur lors de la liaison de l'adresse locale : *numéro d'erreur***.**

Explication : Erreur de la fonction bind() avec l'adresse locale associée à ce nœud OCS.

ICA2115 Erreur lors de la connexion de la socket sur le contrôle de journalisation : *numéro d'erreur***.**

Explication : Erreur de la fonction connect() sur le système hôte où réside le contrôle de journalisation.

ICA2116 Erreur de type de protocole : *type_protocole***.**

Explication : Le type de protocole de terminal virtuel utilisé pour communiquer avec le LM du système hôte est incorrect.

ICA2117 Erreur d'allocation de mémoire sur le message du contrôle de journalisation.

Explication : Erreur malloc() lors du processus d'attribution dynamique d'espace pour le message du LM.

ICA2118 Erreur lors de la transmission du message au contrôle de journalisation : *numéro d'erreur***.**

Explication : Erreur send() lors de l'envoi au LM d'une requête d'ouverture du système hôte requis.

ICA2119 Erreur lors de la réception du message du contrôle de journalisation : *numéro d'erreur***.**

Explication : Erreur recv() lors du renvoi d'un accusé de réception par le contrôle de journalisation.

ICA2120 Erreur de statut du contrôle de journalisation : *statut***.**

Explication : L'accusé de réception émis par le contrôle de journalisation indique que le système hôte n'a pas pu être ouvert.

ICA2121 Erreur lors de l'ouverture de l'unité administrative OCS : *numéro d'erreur***.**

Explication : L'unité administrative OCS n'a pas pu être ouverte.

ICA2122 Echec de la conversion de l'adresse IP en ID TBM : *numéro d'erreur***.**

Explication : Erreur de la commande ioctl() OCS_GET_TBMID. La commande ioctl OCS_GET_TBMID a échoué sur l'unité administrative OCS.

ICA2123 Erreur lors de la connexion du TBM déterminé par rlogin : *numéro d'erreur***.**

Explication : Erreur de la commande ioctl() OCS_IS_TBM_CONNECTED. La commande ioctl OCS_IS_TBM_CONNECTED a échoué sur l'unité administrative OCS.

ICA2124 Aucun nœud hôte connecté : *numéro d'erreur***.**

Explication : Aucun nœud hôte n'est connecté à ce nœud OCS parmi les nœuds hôtes possibles.

ICA2125 Erreur lors de l'obtention de la liste pour l'ODM (gestionnaire d'objet) : *Attribut_personnalisé* **:** *numéro d'erreur odm***.**

Explication : Erreur de la fonction odm_get_list() pour la classe d'objets ODM, CuAt(attribut personnalisé).

ICA2126 Aucun nom de nœud hôte OCS n'est associé à : *nœud hôte_à_connecter***.**

Explication : L'entrée CuAt(attribut personnalisé) a été identifiée mais aucun couple nœud hôte/nœud OCS n'a été trouvé.

ICA2127 Erreur d'allocation de mémoire sur la table des hôtes.

Explication : Erreur malloc() lors du processus d'attribution dynamique d'espace pour la table des noms d'hôte possibles

ICA2128 L'utilisateur (inconnu) a tenté d'exécuter une commande '*commande incorrecte* **depuis** *IP client* **avant la procédure d'authentification.**

Explication : Un utilisateur a tenté des actions avant d'entrer son nom utilisateur et son mot de passe pour l'authentification. L'authentification de l'utilisateur est un préalable impératif à toute poursuite des opérations.

Action de l'utilisateur : Connectez-vous en indiquant un nom utilisateur et un mot de passe.

ICA2129 gethostbyname (*nom invoqué***) :** *numéro d'erreur*

Explication : Une erreur système s'est produite quand ftpd a tenté d'extraire les données de l'hôte spécifié.

ICA2130 L'utilisateur (*nom d'utilisateur***) a tenté d'exécuter une commande '***commande incorrecte***' depuis** *IP client* **(site client).**

Explication : L'utilisateur indiqué a tenté d'exécuter une commande non valide.

Action de l'utilisateur : Seules les commandes USER, QUOTE SITE et QUIT sont admises tant que vous ne tapez pas "quote site destination".

ICA2131 Echec d'authentification de l'utilisateur '*nom d'utilisateur***' depuis** *IP client* **- le fichier user.cfg contient une erreur.**

Explication : La procédure d'authentification a échoué en raison des spécifications du fichier user.cfg définies par l'administrateur du pare-feu (vérifiez les journaux précédents).

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2132 L'utilisateur '*utilisateur***' a tenté d'exécuter une commande '***commande incorrecte***' depuis** *IP client* **(site client).**

Explication : L'utilisateur a tenté d'exécuter une commande non valide. Les seules commandes admises à ce stade sont SITE, USER et QUIT.

ICA2133 Erreur : Echec de l'appel de *fonction* **dans** *instance* **:***ligne***,** *WSAGetLastError*

Explication : Message d'erreur générale ; reportez-vous aux fichiers journaux.

ICA2134 Note : ftpd: connect() (dans *instance***) n'a pas pu atteindre** *IP***,** *WSAGetLastError***.**

Explication : La fonction connect() n'a pas trouvé l'adresse demandée ; reportez-vous à la sortie de WSAGetLastError.

Action de l'utilisateur : Contrôlez encore l'adresse ; l'erreur peut venir du DNS ou du réseau.

ICA2135 Fin du transfert de données : *octets* **octets reçus (de** *IP source***) ;** *octets* **octets envoyés (vers** *IP destination***).**

Explication : Ces informations ne concernent qu'un seul transfert de données opéré au cours d'une session FTP spécifique. Notez cependant que le transfert de données peut ne pas avoir abouti totalement (contrôlez le fichier journal et cherchez une entrée d'échec de réception ou d'envoi d'appel).

ICA2136 Erreur : Echec de la commande CreateThread() dans *instance* **:** *numéro d'erreur***.**

Explication : ftpd n'a pas pu créer l'unité d'exécution requise.

ICA2137 Connexion établie entre le serveur *IP source* **et le client** *IP destination***.**

Explication : La connexion de données a été établie.

ICA2138 Mémoire insuffisante : pftpd : malloc(*octets***) a renvoyé la valeur NULL dans la fonction** *instance***.**

Explication : Impossible d'attribuer une mémoire suffisante ; la fonction malloc a retourné une valeur NULL.

ICA2139 Echec de la commande LogonUser() : *raison***.**

Explication : Échec de l'authentification du mot de passe de connexion sous l'API Windows NT (SAM) pour la ou les raison invoquées.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2140 httpd --> Authentification par serveur relais HTTP *résultat* **pour l'utilisateur** < *utilisateur*>**, sur** < *IP utilisateur*>**, via** *réseau* **... Code retour :**< *raison*>**.**

Explication : Le serveur relais HTTP a tenté une authentification d'utilisateur. L'échec ou la réussite de l'opération est indiqué avec la raison correspondante.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA2141 Fin de la session FTP sur *adresse_IP* **depuis** *adresse_IP***.**

Explication : La session FTP avec le pare-feu prend fin.

ICA2142 fw_tn_authenticate a authentifié *ID utilisateur***.**
ICA2143 fw_tn_authenticate n'a pas authentifié *ID utilisateur***.**

Explication : La fonction fw_tn_authenticate ne peut pas authentifier l'ID utilisateur spécifié.

Réaction du système : La connexion est refusée.

Action de l'utilisateur : Si la fonction fw_tn_authenticate est associée à une fonction de journalisation, l'administrateur pourra se reporter au fichier journal pour déterminer la cause de l'échec.

ICA2144 fw_tn_authenticate n'a pas abouti.

Explication : La valeur retournée par fw_tn_authenticate est différente de zéro. La fonction fw_tn_authenticate est peut-être absente.

Réaction du système : La connexion est refusée.

Action de l'utilisateur : Voyez s'il arrive que la fonction fw_tn_authenticate retourne une autre valeur que zéro et corrigez l'erreur dans ce cas. Recréez la bibliothèque fwuser.o et intégrez-la au pare-feu.

ICA2145 Le système a retourné le code *code retour* **dans le fichier** *nom fichier* **à la ligne** *numéro ligne***.**

Explication : Un appel système a échoué. La bibliothèque fwuser.o est peut-être absente.

Réaction du système : Abandon de la procédure d'authentification.

Action de l'utilisateur : Assurez-vous que la bibliothèque /usr/lib/fwuser.o est présente. Dans l'affirmative, contactez le représentant IBM.

ICA2146 Le fichier IBM fwuser.o n'a pas été remplacé.

Explication : Vous utilisez actuellement la bibliothèque fwuser.o IBM faute de l'avoir remplacée par votre version.

Réaction du système : Abandon de la procédure d'authentification.

Action de l'utilisateur : Écrivez et compilez votre propre programme d'authentification si un utilisateur a été défini comme utilisant l'authentification fournie par l'utilisateur. La bibliothèque fwuser.o d'IBM interdit l'accès à tous les utilisateurs non AIX ou non définis sur le pare-feu.

ICA2147 fwtelnet: l'utilisateur *ID utilisateur* **a lancé une session Telnet transparente depuis** *adresse IP source* **(côté sécurisé) sur** *adresse IP dest***.**

Explication : Message généré au début de toute session relais transparente (fwtelnet). Une session commence lorsque le pare-feu a pris connaissance des adresses IP source et destination. Seules les sessions partant du côté sécurisé sont admises.

Réaction du système : Permet les sessions Telnet en mode transparent.

ICA2148 Attention : Tentative de connexion non autorisée de l'utilisateur *ID utilisateur* **depuis** *adresse IP source* **(côté non sécurisé) sur** *adresse IP dest***.**

Explication : Indique généralement une tentative de connexion sur le pare-feu via l'interface non sécurisée.

Réaction du système : Rejet de la connexion.

Action de l'utilisateur : Établissez la session Telnet depuis le côté sécurisé via le serveur relais en mode transparent.

ICA2149 fwtelnet: erreur LOGIN_ADAPTER_ERROR lors du lancement d'une session Telnet transparente depuis *adresse IP source* **sur** *adresse IP dest***.**

Explication : Une erreur LOGIN_ADAPTER_ERROR s'est produite lors de l'appel de la fonction q_check_secure(0).

Réaction du système : Rejet de la connexion.

Action de l'utilisateur : Contrôlez la carte sécurisée.

ICA2150 Erreur Pftpd - *fonction en échec* **: code retour = 0x***code retour fonction*

Explication : Le serveur pftpd a détecté une erreur dans la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon pftpd.

ICA2151 Connexion refusée.

Explication : Ce message se présente à tout utilisateur dont la tentative de connexion est refusée.

ICA2152 fwlogin : erreur d'écriture sur *périphérique***.**

Explication : Impossible d'écrire sur l'unité indiquée.

ICA2153 fwlogin : erreur de lecture depuis *périphérique***.**

Explication : Impossible de lire sur l'unité indiquée.

ICA2154 Erreur dans *port* **avec** *raison***.**

Explication : Le pare-feu a rencontré un problème.

ICA2155 Erreur Pftpd - *fonction en échec* **:** *message d'erreur système*

Explication : Le serveur pftpd a détecté une erreur dans la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon pftpd.

ICA2156 Attention : L'utilisateur *ID utilisateur* **a tenté d'utiliser FTP en mode transparent depuis le côté NON SECURISE** *adr IP source* **sur** *adr IP dest* **- tentative refusée.**

Explication : Indique généralement une tentative de connexion sur le pare-feu via l'interface non sécurisée.

Réaction du système : Rejet de la connexion.

Action de l'utilisateur : Établissez la session FTP depuis le côté sécurisé via le serveur relais en mode transparent.

ICA2157 L'utilisateur *ID utilisateur* **n'est pas autorisé à utiliser le serveur relais en mode transparent sur** *dest IP addr* **depuis** *adr IP source***.**

Explication : Indique généralement une tentative de connexion sur le pare-feu alors que le relais transparent n'a pas été configuré.

Réaction du système : Rejet de la connexion.

Action de l'utilisateur : Insérez l'entrée suivante dans le fichier de configuration : fwtpproxy ftp = on

ICA2158 L'option *valeur* **a été spécifiée incorrectement.**

Explication : La valeur de paramètre indiquée est incorrecte.

ICA2159 Valeur de dépassement de durée non spécifiée pour l'option -t.

Explication : Une valeur de dépassement de durée doit être spécifiée pour l'option -t.

ICA2160 Modification de mot de passe pour l'utilisateur *ID utilisateur* **depuis** *réseau* **:***nm d'hôte***.**

Explication : Un utilisateur d'une session FTP a modifié son mot de passe dans la base de données des mots de passe.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA2161 L'utilisateur *ID utilisateur* **a tenté de se connecter sous un mot de passe arrivé à expiration depuis** *réseau* **:***nom d'hôte***.**

Explication : Un utilisateur FTP a tenté une connexion sur le pare-feu sous un mot de passe arrivé à expiration.

Réaction du système : La connexion FTP n'a pas été validée et l'utilisateur a été renvoyé au shell de commandes FTP.

Action de l'utilisateur : L'utilisateur doit tenter une nouvelle validation de la connexion via la commande FTP USER ou en rétablissant la connexion FTP et en passant la chaîne de mot de passe sous la forme "ancien_mot_de_passe/nouveau_mot_de_passe/nouveau_mot_de_passe".

ICA2162 Echec de modification du mot de passe pour l'utilisateur *ID utilisateur* **depuis** *réseau* **:** *nom d'hôte***.**

Explication : Un utilisateur FTP a tenté de modifier son mot de passe et la routine de validation du mot de passe n'a pas abouti. L'échec peut avoir les causes suivantes : l'ancien mot de passe spécifié est incorrect, le nouveau mot de passe n'a été passé qu'une seule fois, les deux occurrences du nouveau mot de passe sont différentes, le délimiteur utilisé pour séparer les mots de passe n'était pas "/".

Réaction du système : Le mot de passe FTP n'a pas été validé et l'utilisateur a été renvoyé au shell de commandes FTP.

Action de l'utilisateur : Essayez une nouvelle validation auprès du serveur FTP et prenez soin d'entrer les mots de passe comme il convient. Si le problème persiste, contactez le responsable de la maintenance.

ICA2163 Démarrage de safemaild.

Explication : Démarrage de safemaild.

ICA2164 Arrêt de safemaild

Explication : Arrêt de safemaild en cours.

ICA2165 Session Telnet interrompue.

Explication : La session Telnet prend fin sans pouvoir extraire les informations de la session depuis le tube. La session a probablement été interrompue pendant son initialisation par le client et n'a donc pas été complètement initialisée.

ICA2166 Impossible de récupérer l'attribut *attribut* **pour l'utilisateur** *ID utilisateur***. Code retour =** *code retour***.**

Explication : Le service d'authentification n'a pas pu récupérer l'attribut de l'utilisateur spécifié dans la base de données des utilisateurs. Action système : Échec de l'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système pour modifier l'enregistrement de base de données rattaché à l'utilisateur concerné.

ICA2167 Echec d'authentification de l'utilisateur *ID utilisateur* **pour le service** *service* **avec la méthode** *procédure d'authentification* **depuis** *adresse client* **sur** *type réseau*

Explication : L'utilisateur indiqué n'a pas été authentifié pour le service demandé avec la méthode d'authentification spécifiée. L'utilisateur demandait ce service depuis l'adresse et le type de réseau indiqués. Action système : Échec de l'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système.

ICA2168 Echec d'authentification de l'utilisateur *ID utilisateur* **pour le service** *service***, pour cause de mémoire insuffisante.**

Explication : L'ID utilisateur n'a pas été authentifié pour le service demandé en raison d'un échec de la procédure d'attribution de mémoire au cours de la procédure d'authentification. Action système : Échec de l'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système.

ICA2169 Utilisateur *nom* **authentifié pour** *service* **avec l'authentification** *méthode* **depuis** *réseau* **:***nom d'hôte***.**

Explication : Le pare-feu a authentifié le nom utilisateur indiqué pour le service demandé avec la méthode d'authentification spécifiée.

ICA2170 Echec d'authentification de l'utilisateur *ID utilisateur* **pour le service** *service***. La méthode** *méthode d'authentification* **n'est pas enregistrée sur le pare-feu.**

Explication : L'ID utilisateur n'a pas pu être authentifié pour le service demandé. La méthode d'authentification demandée n'est pas enregistrée sur le pare-feu. Action système : Échec de l'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système.

ICA2171 Le compte *nom_utilisateur* **a été verrouillé pour cause d'expiration du mot de passe.**

Explication : Le mot de passe est arrivé à expiration sans avoir été modifié. Ce compte a été verrouillé.

Réaction du système : Le compte est verrouillé et les tentatives d'authentification de son mot de passe de pare-feu n'aboutiront pas.

ICA2172 Le compte *nom_utilisateur* **est verrouillé.**

Explication : Ce compte a été verrouillé.

Réaction du système : Le compte est verrouillé. Les tentatives d'authentification de son mot de passe de pare-feu n'aboutiront pas.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de déverrouiller le compte.

ICA2173 L'utilisateur a tenté de se connecter sour le nom d'utilisateur réservé *ID utilisateur***.**

Explication : L'ID fourni par l'utilisateur est réservé à l'usage du pare-feu.

Réaction du système : La connexion est refusée.

Action de l'utilisateur : L'administrateur devrait rechercher qui se sert de ce nom utilisateur.

ICA2174 Echec d'authentification de l'utilisateur *ID utilisateur* **pour le service** *service* **avec la méthode** *procédure d'authentification* **depuis** *adresse client* **sur** *type réseau***, par suite d'une erreur de traitement interne.**

Explication : L'utilisateur indiqué n'a pas été authentifié pour le service demandé avec la méthode d'authentification spécifiée. L'utilisateur demandait ce service depuis l'adresse et le type de réseau indiqués. La requête d'authentification a échoué par suite d'une erreur de traitement interne. Action système : Échec de l'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système.

ICA2175 Echec de l'appel de connexion sous Windows NT pour l'utilisateur *nom d'utilisateur***. Dernière erreur :** *dernière erreur***.**

Explication : Le nom utilisateur spécifié n'a pas été authentifié par l'appel de l'API Windows NT LogonUser. Windows NT a affiché la dernière erreur survenue après l'échec de la fonction LogonUser. Action système : Échec de l'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système.

ICA2176 La méthode d'authentification inconnue *procédure d'authentification* **a été définie pour l'utilisateur** *nom d'utilisateur* **avec** *composant* **depuis** *réseau***.**

Explication : La méthode d'authentification indiquée a été définie pour cet utilisateur avec l'élément de pare-feu et le réseau indiqués mais cette méthode n'est pas enregistrée sur le pare-feu. Action système : Échec de la requête d'authentification de l'utilisateur.

Action de l'utilisateur : Contactez l'administrateur système.

ICA2177 Connexion SafeMail 0x*ID session* **réceptionnée depuis** *nom de paire socket***.**

Explication : SafeMail a reçu une connexion entrante depuis le nom de paire indiqué. L'identificateur de connexion indiqué a été attribué pour la fonction de trace (niveau débogage).

Réaction du système : Une unité d'exécution a été chargée de gérer cette connexion.

ICA2178 La session SafeMail 0x*ID session* **a été établie entre** *adresse IP expéditeur* **et** *adresse IP destinataire***.**

Explication : SafeMail a établi le contact avec le serveur de messagerie destinataire et est prêt à transmettre les messages (niveau informations).

Réaction du système : Le transfert de données va commencer.

ICA2179 SafeMail a transmis *taille du message* **octets pour la connexion 0x***ID session* **depuis** *adresse serveur expéditeur* **sur** *adresse serveur destinataire***.**

Explication : SafeMail a transmis un message entre les deux serveurs de messagerie indiqués. Cette session a déjà été identifiée dans un message ICA2166. Ce message contenait le nombre d'octets indiqué (niveau informations).

ICA2180 SafeMail a rejeté la session 0x*ID session* **demandée depuis** *adresse expéditeur***.**

Explication : SafeMail a refusé de transférer le message transmis au cours de la session indiquée (niveau informations).

Réaction du système : La session a été arrêtée.

Action de l'utilisateur : Augmentez le niveau de priorité de journalisation pour obtenir des données de diagnostic plus détaillées.

ICA2181 SafeMail a rejeté la session 0x*ID session***. Code :** *code raison***.**

Explication : Le programme principal de SafeMail a mis fin à la session indiquée suite à la détection d'une condition d'erreur primaire. Les codes de raison possibles sont les suivants : 01 - impossible de localiser le serveur de messagerie destinataire ; 02 - l'émetteur a tenté de transférer un message entre deux serveurs non sécurisés ; 03 - le serveur de messagerie destinataire a rejeté la demande de connexion, panne ou arrêt possible ; 04 - le serveur de messagerie destinataire a refusé le message ; 05 - une ou plusieurs connexions sont arrivées à expiration (le serveur de messagerie source ou destination est inopérant) ; 06 - recv() a retourné 0 octet (le serveur de messagerie source ou destination est inopérant) ; 07 - recv() a retourné une valeur négative (le serveur de messagerie source ou destination est inopérant) ; 08 - trop de commandes non valides ont été reçues ; 09 - select() a retourné une valeur négative (le serveur de messagerie source ou destination est inopérant. Ce message fait l'objet d'une journalisation de niveau débogage.

Réaction du système : La connexion a été arrêtée.

ICA2182 SafeMail a rejeté la session 0x*ID session* **pour cause de commande** *commande SMTP* **incorrecte. Code :** *code raison***.**

Explication : Le sous-programme de validation des commandes de SafeMail a détecté une commande non valide ou dangereuse. Les codes de raison varient avec les commandes SMTP. Reportez-vous à la page Web du service d'assistance IBM Firewall pour les valeurs courantes (niveau débogage).

Réaction du système : La connexion a été arrêtée.

Action de l'utilisateur : Corrigez l'erreur au niveau du client/serveur à l'origine du message pour garantir l'envoi de données valides et sûres.

ICA2183 httpd --> Le fichier de configuration du serveur relais HTTP (*nom de fichier***) n'est pas disponible.**

Explication : Le démon du serveur relais HTTP a essayé d'ouvrir le fichier de configuration indiqué qui, soit n'existe pas, soit ne peut pas être ouvert.

Réaction du système : Le serveur relais HTTP ne démarre pas.

Action de l'utilisateur : Configurez le serveur relais via l'interface utilisateur graphique ou la commande fwhttp et redémarrez le serveur relais.

ICA2184 Erreur signal() avec le signal *Numéro signal***. Arrêt de safemaild.**

Explication : Une erreur système s'est produite quand le démon safemaild a tenté d'établir le gestionnaire de signaux.

ICA2185 Impossible d'ouvrir la socket. Arrêt de safemaild.

Explication : Échec de l'ouverture de la socket.

ICA2186 Impossible de lier la socket à un port. Arrêt de safemaild.

Explication : Échec de la liaison de la socket avec le port.

ICA2187 Impossible d'accepter la nouvelle connexion. Nouvel essai de safemaild.

Explication : Échec pendant l'acceptation d'une nouvelle connexion.

ICA2188 Heure spécifiée (*valeur***) incorrecte pour -l.**

Explication : L'heure indiquée contient des valeurs hors de la plage numérique 0 à 9 ou excède la valeur maximale autorisée.

ICA2189 Valeur de dépassement de durée non spécifiée pour l'option -l.

Explication : Une valeur de dépassement de durée doit être spécifiée pour l'option -l.

ICA2200 Erreur d'initialisation de WinSocket(*service* **:***fonction***) :** *WSAGetLastError*

Explication : Une erreur s'est produite pendant l'initialisation de WinSocket.

Action de l'utilisateur : Corrigez l'incident système signalé par WSAGetLastError et relancez le service indiqué (premier paramètre).

ICA2201 (*service* **:***fonction appelante***) Echec de la fonction** *fonction en échec***, ligne** *numéro de ligne* **:** *WSAGetLastError*

Explication : Le composant de réseau indiqué a échoué.

Action de l'utilisateur : Corrigez l'incident système signalé par WSAGetLastError et relancez le service indiqué (premier paramètre).

ICA2202 (*service* **:***fonction appelante***) Expiration de la fonction** *délai* **après** *WSAGetLastError* **secondes :**

Explication : La fonction indiquée est arrivée à expiration au terme de la durée d'inactivité spécifiée.

Action de l'utilisateur : Rétablissez la connexion avec le service et répondez avant la fin du délai prescrit.

ICA2203 (*service* **:***fonction appelante***) Erreur de mémoire ; la fonction** *fonction en échec* **a renvoyé** *valeur de retour* **ligne** *numéro de ligne* **:** *WSAGetLastError*

Explication : Une erreur de mémoire s'est produite (habituellement une insuffisance). Consultez le contenu du message WSAGetLastError.

Action de l'utilisateur : Libérez de l'espace disque et/ou contactez l'administrateur système.

ICA2204 (*service* **:***fonction appelante***) erreur dans le fichier** *nom de fichier* **: accès refusé ou création impossible.**

Explication : Le service indiqué a rencontré un problème en tentant d'ouvrir ou de créer le fichier spécifié ou le fichier associé au paramètre de fichier.

Action de l'utilisateur : Assurez-vous que le fichier indiqué existe et que ses droits d'accès permettent son ouverture.

ICA2205 (*service* **:** *fonction appelante***) Le fichier** *nom de fichier* **requis est introuvable.**

Explication : Le fichier spécifié n'existe pas. La raison la plus probable de cet échec est que la configuration par défaut du pare-feu a été effacée. Restaurez la configuration à partir d'une sauvegarde.

Action de l'utilisateur : Vérifiez que le fichier de configuration n'existe pas. Le programme de configuration s'attend à ce que ce fichier existe. Si vous ne disposez pas d'une sauvegarde, contactez le responsable de la maintenance.

ICA2206 (*service* **:** *fonction appelante***) Le fichier de configuration** *nom de fichier* **est endommagé.**

Explication : Le fichier de configuration indiqué n'est pas d'un format utilisable. Son contenu a été altéré. La raison la plus probable de cette altération est que le fichier a été modifié manuellement et que des données incorrectes y ont été insérées.

Action de l'utilisateur : Le fichier de configuration devra être recréé correctement. Copiez d'abord le fichier avec la commande cat (ou faites-en une copie pouvant être affichée) puis effacez le fichier d'origine. Modifiez le fichier avec la commande de configuration de pare-feu adaptée en vous basant sur le fichier d'origine si nécessaire.

ICA2207 (*service* **:** *fonction appelante***) Le fichier de configuration** *nom de fichier* **est vide.**

Explication : Le fichier de configuration indiqué n'a pas été trouvé ou, s'il l'a été, est vide. La raison la plus probable pour laquelle le fichier n'a pas été trouvé est que la configuration du service indiqué n'a pas été faite.

Action de l'utilisateur : Vérifiez le statut du fichier de configuration. Si ce fichier existe, la commande de configuration s'attend à y trouver des données. Pour plus d'informations, consultez le manuel.

ICA2208 *service* **Démarrage de la session** *ID session* **pour l'utilisateur** *ID utilisateur* **à partir d'une carte non sécurisée (***adresse IP source* **:***adresse IP dest***).**

Explication : Message généré au démarrage de toute session de ce type.

ICA2209 *service* **Arrêt de la session** *ID session* **pour l'utilisateur** *ID utilisateur* **à partir d'une carte non sécurisée (***adresse IP source* **:***adresse IP dest***) ; octets** *nombre total***.**

Explication : Message généré au terme de toute session de ce type. Le nombre d'octets donné indique le nombre d'octets transmis au cours de la session. Les services (ex : ptelnetd) ne donnant pas cette information indiqueront la valeur zéro.

ICA2210 **(***service***) L'utilisateur** *ID utilisateur* **a tenté de se connecter sous un mot de passe obsolète depuis** *adresse IP source* **(non sécurisé).**

Explication : L'utilisateur indiqué a tenté une connexion sur le pare-feu sous un mot de passe arrivé à expiration depuis l'adresse IP source indiquée (carte non sécurisée).

Action de l'utilisateur : Le mot de passe fourni est arrivé à expiration en application du jeu de règles de mot de passe. Contactez l'administrateur système.

ICA2211 **(***service***) L'utilisateur** *ID utilisateur* **a tenté de se connecter sous un mot de passe obsolète depuis** *adresse IP source* **(sécurisé).**

Explication : L'utilisateur indiqué a tenté une connexion sur le pare-feu sous un mot de passe arrivé à expiration depuis l'adresse IP source indiquée (carte sécurisée).

Action de l'utilisateur : Le mot de passe fourni est arrivé à expiration en application du jeu de règles de mot de passe. Contactez l'administrateur système.

ICA2212 **(***service***) Authentification de l'utilisateur** *nom* **depuis** *adresse IP source* **(sécurisé).**

Explication : Le pare-feu a authentifié ce nom utilisateur connecté depuis la source spécifiée (carte sécurisée).

ICA2213 **(***service***) Authentification de l'utilisateur** *nom* **depuis** *adresse IP source* **(non sécurisé).**

Explication : Le pare-feu a authentifié ce nom utilisateur connecté depuis la source spécifiée (carte non sécurisée).

ICA2214 **(***service***) Echec d'authentification de l'utilisateur** *nom* **depuis** *adresse IP source* **(non sécurisé).**

Explication : Le pare-feu n'a pas authentifié ce nom utilisateur connecté depuis la source spécifiée (carte non sécurisée).

Action de l'utilisateur : La cause la plus probable est une erreur de saisie du nom utilisateur ou du mot de passe ; les noms utilisateur et les mots de passe distinguent majuscules et minuscules (vérifiez que la touche Maj n'est pas enfoncée).

ICA2215 **(***service***) Echec d'authentification de l'utilisateur** *nom* **depuis** *adresse IP source* **(sécurisé).**

Explication : Le pare-feu n'a pas authentifié ce nom utilisateur connecté depuis la source spécifiée (carte sécurisée).

Action de l'utilisateur : La cause la plus probable est une erreur de saisie du nom utilisateur ou du mot de passe ; les noms utilisateur et les mots de passe distinguent majuscules et minuscules (vérifiez que la touche Maj n'est pas enfoncée).

ICA2216 **(***service***) L'utilisateur** *nom* **connecté depuis** *adresse IP source* **(non sécurisé) a saisi des mots de passe non identiques (vérification).**

Explication : Une modification du mot de passe a été demandée ou était nécessaire et l'utilisateur connecté depuis l'adresse IP source indiquée (carte non sécurisée) a saisi des mots de passe différents. Les données d'authentification de l'utilisateur n'ont pas été modifiées.

Action de l'utilisateur : Modifier un mot de passe nécessite de le saisir deux fois : une fois pour le valider, une deuxième fois pour le confirmer. La cause probable est que le deuxième mot de passe saisi était différent du premier.

ICA2217 **(***service***) L'utilisateur** *nom* **connecté depuis** *adresse IP source* **(sécurisé) a saisi des mots de passe non identiques (vérification).**

Explication : Une modification du mot de passe a été demandée ou était nécessaire et l'utilisateur connecté depuis l'adresse IP source indiquée (carte sécurisée) a saisi des mots de passe différents. Les données d'authentification de l'utilisateur n'ont pas été modifiées.

Action de l'utilisateur : Modifier un mot de passe nécessite de le saisir deux fois : une fois pour le valider, une deuxième fois pour le confirmer. La cause probable est que le deuxième mot de passe saisi était différent du premier.

ICA2218 *service* **Démarrage de la session** *ID session* **pour l'utilisateur** *ID utilisateur* **à partir d'une carte sécurisée (***adresse IP source* **:***adresse IP dest***).**

Explication : Message généré au démarrage de toute session de ce type.

ICA2219 *service* **Arrêt de la session** *ID session* **pour l'utilisateur** *ID utilisateur* **à partir d'une carte sécurisée (***adresse IP source* **:***adresse IP dest***) ; octets** *nombre total***.**

Explication : Message généré au terme de toute session de ce type. Le nombre d'octets donné indique le nombre d'octets transmis au cours de la session. Les services (ex : ptelnetd) ne donnant pas cette information indiqueront la valeur zéro.

ICA2220 **(***service***) L'utilisateur** *ID utilisateur* **a lancé une session relais transparente depuis** *adr IP source* **(côté sécurisé) sur** *adr IP dest***.**

Explication : Message généré au début de toute session relais transparente. Une session commence lorsque le pare-feu a pris connaissance des adresses IP source et destination. Seules les sessions partant du côté sécurisé sont admises.

Réaction du système : Autorise l'utilisation du serveur relais en mode transparent.

ICA2221 **(***service***) Avertissement : l'adresse IP (***adr IP contrôle***) figurant à l'extrémité paire de la ligne Control est différente de l'adresse IP (***adr IP données***) figurant à l'extrémité paire de la ligne Data.**

Explication : Pour des raisons de sécurité (contre les intrusions), assurez-vous que l'adresse IP de la paire sur laquelle la socket de la connexion de contrôle est connectée est identique à celle de la socket de la connexion de données. Elles peuvent différer si vous utilisez un répartiteur de réseau ou si l'hôte de destination utilise plusieurs cartes de réseau.

Réaction du système : Voyez si le serveur FTP de destination utilise plusieurs cartes ou un répartiteur de réseau. Assurez-vous que les filtres n'autorisent que des adresses IP valides via les ports 20 et 21.

ICA2222 **(***service***) Avertissement ! Violation de protocole. Reçu une commande Non-RFC** *chaîne incorrecte* **; commande requise :** *chaîne protocole***.**

Explication : Le service indiqué a reçu une chaîne qui ne respecte pas les règles de la RFC associée ; possibilité d'intrusion.

Réaction du système : Utilisez un client respectant la RFC pour le service spécifié.

ICA3001 ***Alerte* : le véritable utilisateur est** *nom utilisateur ident***, et non** *nom utilisateur connexion socks*

Explication : Possibilité de tentative d'atteinte à la sécurité, le nom utilisateur n'a pas été authentifié.

ICA3006 *nombre* **octets depuis** *client***,** *nombre* **octets depuis** *serveur*

Explication : Message indiquant le nombre d'octets transférés entre le démon sockd et ses hôtes client et serveur.

ICA3007 **Nombre maximal de connexions atteint - Connexion refusée.**

Explication : Le serveur Socks est configuré de manière à n'accepter qu'un certain nombre maximal de sessions de client. Ce message est généré lorsque le seuil a été atteint et que d'autres requêtes de connexion se présentent.

Réaction du système : Les nouvelles demandes de connexion sont rejetées.

Action de l'utilisateur : Le nombre maximal de connexions simultanées est déterminé par le paramètre SOCKS5_MAXCHILD dans le fichier de configuration socks5.conf. Augmentez la valeur de ce paramètre et régénérez le serveur. Pour plus d'informations, reportez-vous au guide de référence d'IBM Firewall.

ICA3010 **connecté -- Lié par** *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***port destinataire***)**

Explication : La connexion a été établie.

ICA3011 **connecté -- Connexion de** *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***application***)**

Explication : Connexion établie entre la socket et l'extérieur.

ICA3012 **refusé -- Connexion de** *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***application***)**

Explication : Le système hôte distant a refusé la connexion.

ICA3013 **select()** *numéro d'erreur*

Explication : Erreur système.

ICA3014 **terminé -- Lié par** *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***port destinataire***).(***nombre* **octets depuis** *client***,** *nombre* **octets depuis** *serveur***)**

Explication : Arrêt de la connexion.

ICA3015 **terminé -- Connexion de** *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***hôte destinataire***).(***nombre* **octets depuis** *client***,** *nombre* **octets depuis** *serveur***)**

Explication : Arrêt de la connexion au serveur.

ICA3016 ***Impossible de trouver l'interface adéquate pour communiquer avec *hôte destinataire*

Explication : Le fichier /etc/sockd.route ne contient pas les données de routage de l'hôte de destination spécifié.

ICA3017 Impossible d'exécuter la commande shell pour l'ID processus *processus sockd*

Explication : Le démon sockd n'a pas pu exécuter une commande /bin/sh.

Action de l'utilisateur : Vérifiez que le shell /bin/sh est présent sur le système.

ICA3018 refusé -- Lié par *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst*

Explication : Le système hôte distant a refusé la connexion.

ICA3019 Erreur dans GetDst() depuis l'hôte *nom_src_socks* **:** *numéro d'erreur*

Explication : Erreur de conversion de l'adresse de destination de la connexion demandée.

ICA3022 Zone ?= incorrecte, ligne *numéro de ligne*

Explication : Une entrée non valide a été trouvée dans le fichier /etc/sockd.conf.

ICA3023 Comparaison non admise, ligne *numéro de ligne*

Explication : Une entrée non valide a été trouvée dans le fichier /etc/sockd.conf.

ICA3024 Entrée incorrecte, ligne *numéro de ligne*

Explication : Une entrée non valide a été trouvée dans le fichier /etc/sockd.route.

ICA3025 Zone d'autorisation/interdiction incorrecte, ligne *numéro de ligne*

Explication : Une entrée non valide a été trouvée dans le fichier /etc/sockd.conf.

ICA3026 Numéro de port incorrect, ligne *numéro de ligne*

Explication : Une entrée non valide a été trouvée dans le fichier /etc/sockd.conf.

ICA3027 Echec de la commande shell (*statut exécution***) pour \"***cmd***\"**

Explication : La commande shell affichée n'a pas abouti.

Action de l'utilisateur : Vérifier que le processeur shell est présent sur le système.

ICA3030 Impossible d'ouvrir le fichier de configuration (*/etc/sockd.conf***)**

Explication : La requête d'ouverture du fichier indiqué n'a pas abouti.

ICA3031 Impossible d'ouvrir le fichier de routage (*/etc/sockd.route***) :** *numéro d'erreur*

Explication : La requête d'ouverture du fichier indiqué n'a pas abouti.

Action de l'utilisateur : Contactez l'administrateur du pare-feu. Un fichier par défaut a été installé avec le pare-feu.

ICA3032 Impossible d'ouvrir le fichier utilisateur (*nom fichier utilisateur***) :** *numéro d'erreur*

Explication : Le nom de fichier spécifié pour le paramètre *=userlist d'une règle d'autorisation n'a pas été trouvé.

ICA3033 Résultat inattendu retourné par la commande Validate()

Explication : Une vérification du nom utilisateur a été spécifiée et la fonction identd a retourné un résultat inattendu.

ICA3035 Impossible de se connecter à identd sur *hôte client*

Explication : Une vérification du nom utilisateur a été spécifiée et la fonction identd ne répond pas.

ICA3039 Erreur -- la commande shell \"*cmd***\" ne contient aucun caractère alphanumérique.**

Explication : Commande shell non valide, voir le message du fichier journal.

ICA3040 Erreur -- commande shell fork() *numéro d'erreur*

Explication : Le démon sockd n'a pas pu passer au processus fils via 'fork()'

ICA3041 Erreur -- adresse client introuvable.

Explication : Erreur retournée par l'appel de la fonction 'getpeername()'.

Action de l'utilisateur : Vérifiez la configuration du routage et du DNS.

ICA3042 Erreur -- commande non définie (0x*commande-hex-reçue***) provenant de l'hôte** *adresse client*

Explication : Commande non valide reçue de l'application client.

Action de l'utilisateur : Possibilité de problème dans la configuration du client ou différence des niveaux de prise en charge entre le client et le pare-feu.

ICA3043 Erreur -- L'hôte *adresse client* **a donné une version incorrecte (0x***numéro-version-hex***).**

Explication : Firewall prend en charge Socks V4.2.

Action de l'utilisateur : Possibilité de problème dans la configuration du client ou différence des niveaux de prise en charge entre le client et le pare-feu.

ICA3044 Erreur -- Connexion de *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***application***). Code d'erreur :** *commande générant l'erreur numéro d'erreur***.**

Explication : La requête de connexion n'a pas abouti.

ICA3045 Erreur -- Lié par *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **Erreur : connecté à un hôte incorrect** *nom_dst* **(***port_dst (application)***).**

Explication : La requête de liaison n'a pas abouti.

ICA3046 Erreur -- Lié par *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst***. Code d'erreur :** *commande générant l'erreur numéro d'erreur***.**

Explication : La requête de liaison n'a pas abouti.

ICA3047 Hors délai -- Lié par *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst***.**

Explication : Fermeture de la connexion pour cause de délai d'inactivité dépassé.

ICA3048 Commande shell trop longue : *commande***...**

Explication : La commande à exécuter dans le fichier /etc/sockd.conf est trop longue.

ICA3049 Hors délai -- Connexion de *utilisateur***(***véritable_utilisateur***)@***adr_src* **pour** *adr_dst* **(***application***).**

Explication : Fermeture de la connexion pour cause de délai d'inactivité dépassé.

ICA3050 *règle de filtrage correspondant à sockd.conf*

Explication : Règle de filtrage contenue dans le fichier /etc/sockd.conf qui correspond à la connexion Socks.

ICA3051 AIX sockd_route() - interface pour *adresse distante* **introuvable.**

Explication : Impossible de trouver les données de routage de l'interface.

ICA3052 Erreur lors de la définition de l'ID utilisateur "nobody".

Explication : Impossible d'affecter l'ID utilisateur "nobody" au processus sockd fils.

ICA3053 Erreur lors de la lecture de popen (script de routage AIX) : *message d'erreur système*

Explication : Échec de l'exécution du script pour la recherche des données de routage.

ICA3054 Erreur fatale d'allocation de mémoire dans AIX sockd_route().

Explication : Échec de la procédure d'allocation de mémoire pendant la collecte des données de routage.

ICA3055 Erreur fatale lors de l'analyse de AIX sockd_route() - premier espace dans : *ligne saisie*

Explication : Erreur d'analyse des données de routage du système.

ICA3056 Erreur fatale lors de l'analyse de AIX sockd_route() - deuxième espace dans : *ligne saisie*

Explication : Erreur d'analyse des données de routage du système.

ICA3057 Erreur fatale lors de la lecture de la sortie du script de routage AIX sockd_route() : *message d'erreur système*

Explication : Erreur de lecture de la sortie du script.

ICA3058 Erreur lors de la lecture de popen (script d'adaptateur AIX) : *message d'erreur système*

Explication : Échec de l'exécution du script pour la recherche des données d'interface.

ICA3101 Erreur sockd lors de l'envoi de données - select() : *message d'erreur système*

Explication : (SOCKS422) Erreur pendant l'envoi des données.

ICA3102 Erreur sockd lors de l'envoi de données - write() : *message d'erreur système*

Explication : (SOCKS422) Erreur pendant l'envoi des données.

ICA3103 Erreur sockd lors de la réception de données - select() : *message d'erreur système*

Explication : (SOCKS422) Erreur pendant la réception des données.

ICA3104 Erreur sockd lors de la réception de données - read() : *message d'erreur système*

Explication : (SOCKS422) Erreur pendant la réception des données.

ICA3105 Impossible de créer un ID processus pour le fichier *nom de fichier***.**

Explication : (SOCKS422) L'écriture ou la création de l'ID processus du fichier n'a pas abouti.

ICA3106 Sockd n'a pas pu générer un processus fils : *message d'erreur système*

Explication : (SOCKS422) La tentative de création d'un processus fils pour gérer une requête SOCKS a échoué.

ICA3107 La définition de l'option SO_LINGER pour la socket entrante n'a pas abouti : *message d'erreur système*

Explication : (SOCKS422) erreur non critique

ICA3108 La définition de l'option SO_LINGER pour la socket sortante n'a pas abouti : *message d'erreur système*

Explication : (SOCKS422) erreur non critique

ICA3109 Entrée incorrecte ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3110 Zone d'interface illégale ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3111 Destination IP illégale ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3112 Masque de destination illégal ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3113 *nombre de lignes* **analysées dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3114 Aucune ligne correcte trouvée dans le fichier *nom de fichier***.**

Explication : (SOCKS422) fichier de configuration vide ou erreur de syntaxe.

Action de l'utilisateur : Rectifiez le fichier de configuration indiqué.

ICA3115 Zone d'autorisation/interdiction incorrecte ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3116 Zone '?=' incorrecte ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3117 Source IP illégale ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3118 Masque de source illégal ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3119 Comparaison non admise ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3120 Numéro de port incorrect ligne *numéro de ligne* **dans le fichier** *nom de fichier***.**

Explication : (SOCKS422) La syntaxe de l'entrée de configuration est incorrecte.

ICA3121 SIGUSR1 reçu - purge de la configuration du serveur Socks.

Explication : (SOCKS422) Un signal de purge de la configuration active vers le fichier journal succède à ce message.

ICA3122 Aucun démon n'a pu être créé par Sockd : *message d'erreur système*

Explication : (SOCKS422) Échec de l'initialisation du démon sockd par la commande fork.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3123 Démarrage du serveur Sockd.

Explication : (SOCKS422) Sockd s'est initialisé et attend les connexions.

ICA3124 Erreur fatale d'initialisation de sockd - bind() : *message d'erreur système*

Explication : (SOCKS422) L'initialisation du serveur sockd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3125 Erreur fatale d'initialisation de sockd - listen() : *message d'erreur système*

Explication : (SOCKS422) L'initialisation du serveur sockd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3126 Erreur fatale de sockd - accept() principal : *message d'erreur système*

Explication : (SOCKS422) La routine principale du serveur sockd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3127 Signal de fin reçu par le serveur sockd.

Explication : L'utilisateur root ou "nobody" a interrompu le processus ; arrêt du démon.

Action de l'utilisateur : Relancez sockd si vous le désirez (tapez "sockd").

ICA3128 Erreur fatale d'initialisation de sockd - socket() : *message d'erreur système*

Explication : L'initialisation du serveur sockd a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3129 Erreur fatale d'initialisation de sockd - *fonction en échec* **:** *message d'erreur système*

Explication : Le serveur sockd n'a pas pu exécuter la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3130 Erreur de sockd - *fonction en échec* **:** *message d'erreur système*

Explication : Le serveur sockd a détecté une erreur dans la fonction indiquée. Le démon reste actif mais les connexions pourront être refusées ou arrêtées.

Action de l'utilisateur : Si le problème persiste, arrêtez sockd, corrigez l'incident système signalé et relancez le démon sockd.

ICA3131 Erreur lors de la lecture de *nom de fichier***. Les données mises en antémémoire seront utilisées.**

Explication : Le fichier n'a pu être lu ou contenait des données incorrectes. L'un des messages précédents doit décrire le problème. Le démon sockd continuera d'opérer avec les données d'antémémoire de la précédente version du fichier.

Action de l'utilisateur : Corrigez l'erreur signalée dans ce fichier.

ICA3132 Indicateur -*valeur* **inconnu.**

Explication : L'indicateur mentionné n'est pas reconnu. Arrêt du démon.

Action de l'utilisateur : Corrigez la syntaxe et relancez sockd.

ICA3133 Paramètre *valeur* **inconnu.**

Explication : Le paramètre mentionné n'est pas reconnu. Arrêt du démon.

Action de l'utilisateur : Corrigez la syntaxe et relancez sockd.

ICA3134 Conflit entre les options *option1* **et** *option2***.**

Explication : Les options indiquées ne peuvent pas être spécifiées ensemble. Arrêt du démon.

Action de l'utilisateur : Corrigez la syntaxe et relancez sockd.

ICA3135 Erreur de sockd - *fonction en échec* **: code retour = 0x***code retour fonction*

Explication : Le serveur sockd a détecté une erreur dans la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA3700 Erreur d'initialisation de WinSocket : *erreur WinSocket*

Explication : Une erreur s'est produite pendant l'initialisation de WinSocket.

Action de l'utilisateur : Corrigez l'incident système signalé et relancez le démon sockd.

ICA4000 *programme* **- Avertissement : Reçu un signal** *signal***, arrêt du processus en cours ...**

Explication : Opération abandonnée suite à la réception d'un signal.

ICA4001 **STOP** *programme* **comme PID** *ID processus*

Explication : Signale l'arrêt total du démon. Message d'informations.

ICA4002 **ID temporaire**

Explication : Message d'informations.

ICA4003 **Problème avec le processus fils** *ID processus***.**

Explication : Impossible de créer un processus fils.

ICA4004 **Erreur fatale. Arrêt de fwpagerd lors de la réception du signal** *signal***.**

Explication : Gestionnaire de signaux.

ICA4005 **Aucun démon fwpagerd actif,** *programme* **non trouvé.**

Explication : Le message n'a pas pu être envoyé car le démon était inactif.

ICA4006 **Aucun démon fwpagerd actif sous l'ID processus** *ID processus***.**

Explication : Impossible de trouver l'ID processus (PID) du démon.

ICA4007 **START** *programme* **comme PID** *ID processus*

Explication : Signale le démarrage du programme indiqué. Message d'informations.

ICA4008 **Impossible de définir sigignore pour SIGPIPE.**

Explication : Échec de l'opération de configuration visant à ignorer le signal d'interruption du tube.

ICA4009 **Impossible de configurer sigset pour SIGCHILD.**

Explication : Échec de l'opération de configuration visant à intercepter un signal d'arrêt de processus fils.

ICA4010 **Impossible de configurer le processus d'arrêt.**

Explication : Échec lors de la définition d'un signal d'interception des processus d'arrêt.

ICA4011 **Impossible d'ouvrir la socket.**

Explication : Échec lors de l'ouverture de la socket.

ICA4012 **Impossible de configurer sigset pour SIGTERM.**

Explication : Échec de l'opération de configuration visant à intercepter les signaux SIGTERM et SIGINT.

ICA4013 **Impossible de configurer l'option de réutilisation de la socket.**

Explication : Échec lors de la configuration de l'option de réutilisation de la socket.

ICA4014 Impossible de définir l'option linger de la socket.

Explication : Échec lors de la configuration de l'option linger de la socket.

ICA4015 Impossible de lier la socket à un port.

Explication : Échec de la liaison de la socket avec le port.

ICA4016 Impossible de configurer la socket en mode écoute.

Explication : Échec de la configuration de la socket en mode écoute.

ICA4017 Le service *nom service* **utilise la socket TCP** *socket***.**

Explication : Message d'informations.

ICA4018 L'appel de la fonction select() n'a pas abouti.

Explication : Erreur interne pendant l'appel de fonction.

ICA4019 Erreur grave dans new_work().

Explication : Erreur interne grave dans la routine new_work.

ICA4020 Erreur (*programme***) : Impossible d'écrire dans la socket en continu :** *socket*

Explication : Possibilité d'erreur système.

Action de l'utilisateur : Contrôlez l'utilisation de la socket.

ICA4021 Problème de réception des réponses.

Explication : Problème de réception des réponses du modem.

Action de l'utilisateur : Contrôlez les connexions du modem et la chaîne d'initialisation.

ICA4022 La requête a abouti.

Explication : Message d'informations.

ICA4023 La requête n'a pas abouti.

Explication : La requête d'envoi de message n'a pas abouti.

ICA4024 Erreur (*programme***) : Priorité incorrecte (***priorité minimale* **-** *priorité maximale***).**

Explication : Plage de priorités incorrecte.

Action de l'utilisateur : Modifiez la plage de priorités incorrecte. Les valeurs admises vont de -1 à 5.

ICA4025 Erreur (*programme***) : L'adresse doit avoir la forme ID@opérateur quand l'option -n est utilisée.**

Explication : La syntaxe de la commande est incorrecte.

Action de l'utilisateur : Rectifiez la syntaxe de la commande.

ICA4026 Erreur (*programme***) : hôte** *nom d'hôte* **inconnu.**

Explication : Impossible de convertir ce nom de système hôte.

Action de l'utilisateur : Vérifiez le nom d'hôte.

ICA4027 **Erreur (***programme***) : Impossible d'ouvrir la socket en continu** *numéro d'erreur*

Explication : Impossible de créer la socket.

ICA4028 **Erreur (***programme***) : Impossible de définir les options de la socket :** *numéro d'erreur*

Explication : Impossible de définir l'option linger de la socket.

ICA4029 **Erreur (***programme***) : Impossible de se connecter sur** *hôte* **:** *numéro d'erreur***.**

Explication : Impossible de se connecter à l'hôte indiqué.

Action de l'utilisateur : Contrôlez la configuration du port série et vérifiez l'existence d'un fichier de pilote de périphérique.

ICA4030 **Erreur (***programme***) : Impossible d'écrire sur la socket en continu :** *numéro d'erreur*

Explication : Impossible d'écrire sur la socket en continu.

ICA4031 **Problème de réception des réponses. Statut du message inconnu.**

Explication : Problème de réception des réponses du modem.

ICA4032 **Message envoyé dans la file d'attente.**

Explication : Message d'informations. Le message a été envoyé dans la file d'attente.

ICA4033 **Le message n'a pas abouti. Pas de message envoyé.**

Explication : Impossible d'envoyer le message vers la file d'attente du récepteur de messagerie.

ICA4034 *date* **n'a pas abouti (ID** *ID* **Pri** *priorité* **Secs** *période* **Essais** *nombre essais***) [***depuis entrée***]** *nom personne* **:** *message***.**

Explication : Ce message s'affiche lorsque l'envoi d'un message se solde par un échec.

ICA4035 **Impossible de faire passer le message** *message* **de la file d'attente** *programme* **à la file d'attente** *personne***.**

Explication : Impossible de mettre ce message en file d'attente.

ICA4036 **A ABOUTI (ID** *ID* **Pri** *priorité* **Secs** *période* **Essais** *nombre essais***) [***depuis entrée***]** *nom personne* **:** *message***.**

Explication : Ce message s'affiche lorsque l'envoi d'un message aboutit.

ICA4037 **VIDE DANS** *fichier cliché* **(ID** *ID* **Pri** *priorité* **Secs** *période* **Essais** *nombre essais***) [***depuis entrée***]** *nom personne* **:** *message***.**

Explication : Les messages non immédiatement envoyés sont sauvegardés dans un fichier pour envoi ultérieur.

ICA4038 **Impossible d'écrire dans le fichier de cliché** *fichier cliché***.**

Explication : Le fichier de cliché n'est pas accessible en écriture.

Action de l'utilisateur : Contrôlez les droits d'accès du système de fichiers.

ICA4039 IpcKey : 0x*IpcKey*

Explication : Message d'informations.

ICA4040 Le délai de relance de *valeur* minutes est dépassé.

Explication : Le modem n'a pas été initialisé au terme du délai indiqué.

Action de l'utilisateur : Contrôlez la chaîne d'initialisation.

ICA4041 Un message alphanumérique a été trouvé pour un récepteur de radiomessagerie numérique.

Explication : Les récepteurs de messagerie numériques n'acceptent pas les données alphanumériques.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4042 La personne ne peut pas recevoir de messages.

Explication : Le récepteur de messagerie n'est probablement pas activé.

Action de l'utilisateur : Contrôlez l'activation du récepteur de messagerie.

ICA4043 L'opérateur *opérateur* n'existe pas.

Explication : L'opérateur indiqué n'existe pas.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4044 L'opérateur *opérateur* n'a pas de numéro de téléphone multifréquence.

Explication : L'opérateur indiqué n'a pas de numéro de téléphone multifréquence.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4045 Le numéro du récepteur de radiomessagerie *numéro récepteur* est trop long par rapport à la valeur maximale de *opérateur* définie.

Explication : Le numéro du récepteur de radiomessagerie est trop long par rapport à la valeur maximale définie pour l'opérateur.

Action de l'utilisateur : Utilisez un numéro de récepteur de messagerie plus court que le maximum autorisé pour l'opérateur.

ICA4046 Le numéro du récepteur de radiomessagerie *numéro récepteur* est trop long par rapport à la longueur par défaut de *opérateur* définie.

Explication : Ce message s'affiche lorsque la valeur par défaut est trop faible.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT. Augmentez la longueur par défaut.

ICA4047 Problème à la ligne *numéro ligne* du fichier de modem *chemin de fichier modem*.

Explication : Le fichier de définition des modems contient un caractère non valide.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4048 Impossible d'ouvrir le modem sur le périphérique /dev/*nom périphérique*.

Explication : Impossible d'ouvrir le modem sur le périphérique indiqué.

Action de l'utilisateur : Contrôlez ou reconfigurez le port série. Contrôlez le périphérique.

ICA4049 Modem ouvert sur /dev/*nom périphérique***.**

Explication : Message d'informations. Un modem a été détecté sur le port série.

ICA4050 Impossible de définir les caractéristiques du modem.

Explication : Échec pendant la configuration des caractéristiques du modem.

Action de l'utilisateur : Contrôlez la chaîne d'initialisation du modem.

ICA4051 Impossible d'initialiser le modem après *nombre* **essais.**

Explication : Impossible d'initialiser le modem.

Action de l'utilisateur : Contrôlez la chaîne d'initialisation du modem et la configuration du port série.

ICA4052 Impossible d'appeler le numéro du récepteur de radiomessagerie *numéro récepteur*

Explication : Impossible de composer ce numéro de récepteur de messagerie.

Action de l'utilisateur : Contrôlez la validité de ce numéro.

ICA4053 Impossible de faire raccrocher le modem.

Explication : Impossible de faire raccrocher le modem.

Action de l'utilisateur : Contrôlez la chaîne d'initialisation du modem et la commande de raccrochage utilisée.

ICA4054 Impossible d'appeler le message *message*

Explication : Impossible d'envoyer le message indiqué.

ICA4055 Problème à la ligne *numéro ligne* **du fichier de modem** *nom fichier***.**

Explication : Ficher de définition de modem non valide.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4056 Impossible d'appeler le numéro multifréquence (*numéro***) de l'opérateur** *opérateur***.**

Explication : Le numéro multifréquence a peut-être changé ou ne correspond pas à l'opérateur spécifié.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4057 Impossible d'émettre le bloc.

Explication : Échec pendant la tentative de transmission du bloc.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4058 Pas de réponse au bloc transmis.

Explication : Aucune réponse obtenue de l'opérateur après la transmission du bloc.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4059 Impossible de recevoir une réponse à la distribution du message.

Explication : Aucune réponse obtenue de l'opérateur après la transmission du message.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4060 Impossible d'émettre l'ID du récepteur de radiomessagerie.

Explication : Impossible d'émettre l'ID du récepteur de radiomessagerie.

Action de l'utilisateur : Contrôlez le numéro du récepteur de messagerie et les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4061 Impossible d'émettre le <RC> final de la requête de mode automatique.

Explication : Impossible d'émettre le <RC> final de la requête de mode automatique.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4062 Impossible d'émettre la requête de mode automatique.

Explication : Impossible d'émettre le signal de la requête de mode automatique.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4063 Le signal d'invitation à émettre de l'opérateur *opérateur* **n'a pas été reçu après** *nombre* **essais.**

Explication : L'opérateur est probablement occupé.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur avec le menu smitty/SMIT et réessayez ultérieurement.

ICA4064 Erreur de communication avec l'opérateur *opérateur* **pendant le message d'invite.**

Explication : Une erreur de communication peut avoir différentes causes. Réessayez ultérieurement.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur avec le menu smitty/SMIT et réessayez ultérieurement.

ICA4065 Impossible de recevoir une réponse au logon.

Explication : Le modem ne peut pas recevoir aucune réponse à la demande de connexion (logon).

Action de l'utilisateur : Contrôlez la chaîne d'initialisation du modem et les paramètres de l'opérateur.

ICA4066 L'opérateur *opérateur* **n'a pas répondu à la tentative de connexion.**

Explication : L'opérateur n'a pas répondu à la demande de connexion (logon).

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur avec le menu smitty/SMIT et réessayez ultérieurement.

ICA4067 L'opérateur *opérateur* **a répondu** *chaîne de données***.**

Explication : L'opérateur a renvoyé un message d'erreur ou un message indiquant son statut occupé.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur avec le menu smitty/SMIT et réessayez ultérieurement.

ICA4068 L'opérateur *opérateur* **a provoqué une déconnexion pendant le logon.**

Explication : L'opérateur a provoqué une déconnexion pendant la procédure de connexion.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4069 Sauvegarde des messages vers l'opérateur *opérateur* **provoquée par** *valeur* **essais.**

Explication : Si l'opérateur est occupé, le programme sauvegarde les messages et réessaie ultérieurement.

ICA4070 Messages vers l'opérateur *opérateur* **ignorés suite à** *valeur* **tentatives de connexion.**

Explication : L'opérateur ne peut plus être contacté après un certain nombre d'essais.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur puis recommencez ultérieurement.

ICA4071 Erreur (*programme***) : Impossible d'allouer de la mémoire pour essayer une nouvelle fois l'opérateur :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système ou d'erreur d'allocation de mémoire.

ICA4072 Erreur (*programme***) : Impossible d'ajouter une entrée à la liste de relance de l'opérateur :** *numéro d'erreur***.**

Explication : L'opérateur indiqué n'existe peut-être pas.

Action de l'utilisateur : Contrôlez la validité de l'opérateur et recommencez.

ICA4073 La connexion de données avec l'opérateur *opérateur***, au numéro** *téléphone***, n'a pas abouti après** *valeur* **essais.**

Explication : La connexion de données n'a pas abouti.

Action de l'utilisateur : Contrôlez les connexions du modem et les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4074 La demande d'ID de l'opérateur *opérateur* **n'a pas été reçue après** *valeur* **essais.**

Explication : L'opérateur n'a renvoyé ni demande d'ID ni demande d'accusé de réception.

Action de l'utilisateur : Assurez-vous que l'opérateur emploie le protocole TeleAlphanumeric (TAP).

ICA4075 Erreur de communication pendant la connexion avec l'opérateur *opérateur***.**

Explication : Une erreur de communication peut avoir différentes causes.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4076 Le nombre maximal de tentatives de connexions avec l'opérateur *opérateur* **a été dépassé.**

Explication : L'opérateur n'a pas répondu au terme des tentatives de connexion.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur puis recommencez ultérieurement.

ICA4077 Le signal d'invitation à émettre de l'opérateur *opérateur* **n'a pas été reçu.**

Explication : L'opérateur n'a pas retourné de signal d'invitation à émettre.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur puis recommencez ultérieurement.

ICA4078 Impossible de créer des blocs.

Explication : L'opérateur ne peut pas créer de blocs en vue d'une transmission.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4079 L'opérateur *opérateur* **n'a pas répondu à la distribution de message.**

Explication : L'opérateur a rencontré des difficultés dans la distribution du message.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4080 L'opérateur *opérateur* **a provoqué une déconnexion pendant la distribution du message.**

Explication : L'opérateur a provoqué une déconnexion pendant la distribution du message.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur et la chaîne d'initialisation du modem.

ICA4081 L'opérateur *opérateur* **a rejeté l'ID du message ou du récepteur de radiomessagerie.**

Explication : L'opérateur a rejeté l'ID du message ou du récepteur de radiomessagerie.

Action de l'utilisateur : Contrôlez la validité de l'ID du récepteur de messagerie, son activation et les paramètres de l'opérateur.

ICA4082 Erreur de communication pendant la distribution du message à l'opérateur *opérateur***.**

Explication : Une erreur de communication peut avoir différentes causes.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4083 La confirmation de l'opérateur *opérateur* **n'a pas été reçue après** *nombre* **essais.**

Explication : Ce message s'affiche si l'opérateur est occupé ou ne peut pas établir de connexion.

Action de l'utilisateur : Contrôlez les paramètres de l'opérateur avec le menu smitty/SMIT et recommencez après quelques minutes.

ICA4084 Impossible d'émettre le signal <EOT>.

Explication : Le modem ne peut pas transmettre le signal <EOT>.

Action de l'utilisateur : Contrôlez les connexions du modem et la chaîne d'initialisation.

ICA4085 Impossible de recevoir une réponse au signal <EOT>.

Explication : Le modem ne peut recevoir aucune réponse au signal <EOT>.

Action de l'utilisateur : Contrôlez les connexions du modem et la chaîne d'initialisation.

ICA4086 L'opérateur *opérateur* **n'a pas répondu au signal <EOT>.**

Explication : L'opérateur ne peut pas répondre aux données transmises.

Action de l'utilisateur : Contrôlez la validité de l'opérateur et les connexions du modem.

ICA4087 L'opérateur *opérateur* **a répondu par un message d'erreur de données inacceptables lié au contenu du message.**

Explication : L'opérateur ne peut pas répondre aux données transmises.

Action de l'utilisateur : Corrigez les paramètres de l'opérateur avec le menu smitty/SMIT.

ICA4088 Impossible d'ouvrir le fichier des valeurs par défaut *chemin par défaut***.**

Explication : Le fichier des valeurs par défaut du modem n'existe pas ou ses droits d'accès ne permettent pas son ouverture.

Action de l'utilisateur : Contrôlez l'existence du fichier et/ou ses droits d'accès.

ICA4089 Le fichier des valeurs par défaut *chemin par défaut* **est incomplet.**

Explication : Des données sont absentes du fichier des valeurs par défaut du modem.

Action de l'utilisateur : Corrigez les données avec le menu smitty/SMIT.

ICA4090 Numéro de ligne extérieure incorrect dans le fichier des valeurs par défaut *chemin par défaut* **ligne** *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient un numéro de ligne extérieure non valide.

Action de l'utilisateur : Modifiez le fichier de base de données des opérateurs.

ICA4091 Vitesse non valable dans le fichier des valeurs par défaut *fichier par défaut* **ligne** *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient une vitesse de transmission non valide.

Action de l'utilisateur : Modifiez le fichier de base de données des opérateurs.

ICA4092 Nombre de bits de données incorrect dans le fichier des valeurs par défaut *fichier par défaut* **ligne** *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient un nombre de bits de données non valide.

Action de l'utilisateur : Modifiez le fichier de base de données des opérateurs.

ICA4093 Parité incorrecte dans le fichier des valeurs par défaut *fichier par défaut* **ligne** *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient une parité non valide.

Action de l'utilisateur : Modifiez le fichier de base de données des opérateurs.

ICA4094 Nombre de bits de stop incorrect dans le fichier des valeurs par défaut *fichier par défaut* **ligne** *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient un nombre de bits d'arrêt non valide.

Action de l'utilisateur : Modifiez le fichier de base de données des opérateurs.

ICA4095 Code inconnu *ID code* **dans le fichier des valeurs par défaut** *fichier par défaut* **ligne** *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient un code non valide.

Action de l'utilisateur : Modifiez le fichier de base de données des opérateurs.

ICA4096 Nombre incorrect de paramètres.

Explication : Message d'informations.

ICA4097 Erreur (*programme*) : Impossible de créer la liste des opérateurs. Problèmes de mémoire.

Explication : Possibilité d'erreur système ou de problèmes de mémoire.

ICA4098 Erreur (*programme*) : Erreurs dans le fichier des opérateurs des récepteurs de radiomessagerie *fichier opérateurs*.

Explication : Le fichier de la base de données des opérateurs contient des données non valides.

Action de l'utilisateur : Contrôlez l'existence de codes non valides dans le fichier de la base de données des opérateurs.

ICA4099 Erreur (*programme*) : Impossible d'obtenir le jeton IPC : *numéro d'erreur*.
ICA4100 Erreur (*programme*) : Impossible de créer la liste des essais. Possibilité de problèmes de mémoire.

Explication : Possibilité d'erreur système ou de problèmes de mémoire.

ICA4101 Erreur (*opérateur*) : Impossible de créer la file d'attente page_q_err : *pageQErr*.
ICA4102 Erreur (*programme*) : Impossible de définir le signal de réception pour SIGTERM/SIGINT : *numéro d'erreur*.

Explication : Possibilité d'erreur système.

ICA4103 Erreur (*programme*) : Impossible de définir les caractéristiques du modempour l'opérateur *opérateur*.

Explication : Impossible de configurer le modem.

Action de l'utilisateur : Contrôlez la configuration du port série et la chaîne d'initialisation.

ICA4104 Code manquant *code* pour l'opérateur *opérateur*.

Explication : Certaines données du modem sont absentes. On doit avoir un code pour la vitesse de transmission, le numéro de ligne extérieure, etc...

Action de l'utilisateur : Contrôlez l'existence de caractères non valides dans le fichier de configuration du modem.

ICA4105 Il doit y avoir au moins un numéro de téléphone pour l'opérateur *opérateur*. listed.

Explication : Le fichier de configuration de l'opérateur doit contenir son numéro de téléphone.

Action de l'utilisateur : Ajoutez le numéro de téléphone avec le menu smitty/SMIT.

ICA4106 Impossible d'ouvrir le fichier *nom fichier opérateur*.

Explication : Le fichier de base de données des opérateurs doit exister.

Action de l'utilisateur : Dans le cas contraire, créez-en un avec le menu smitty/SMIT.

ICA4107 La ligne *numéro ligne* **est trop longue.**

Explication : La ligne indiquée dans le fichier de base de données est trop longue.

Action de l'utilisateur : Contrôlez l'existence de lignes non valides dans le fichier de la base de données des opérateurs.

ICA4108 Code inconnu ligne *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient un code inconnu.

Action de l'utilisateur : Contrôlez l'existence de codes non valides dans le fichier de la base de données des opérateurs.

ICA4109 Séquence incorrecte, ligne *numéro ligne***.**

Explication : Le fichier de base de données des opérateurs contient une séquence non valide.

Action de l'utilisateur : Contrôlez l'existence de séquences non valides dans le fichier de la base de données des opérateurs.

ICA4110 L'opérateur *opérateur* **n'est pas valable et est ignoré.**

Explication : Cet opérateur ne permet pas l'envoi de messages.

Action de l'utilisateur : Contrôlez la validité de l'opérateur.

ICA4111 Impossible d'ajouter un opérateur à la liste.

Explication : L'opérateur ne peut pas être ajouté à la liste.

Action de l'utilisateur : Contrôlez la validité de l'opérateur et les numéros de téléphone.

ICA4112 Le nom de l'opérateur est manquant ou est trop long ligne *numéro ligne***.**

Explication : Le nom de l'opérateur est absent.

Action de l'utilisateur : Ajoutez l'opérateur avec le menu smitty/SMIT.

ICA4113 Impossible d'allouer un nouvel opérateur pour récepteur de radiomessagerie : *opérateur***.**

Explication : L'opérateur de radiomessagerie indiqué ne peut pas être ajouté à la liste.

Action de l'utilisateur : Contrôlez la validité de l'opérateur et les numéros de téléphone.

ICA4114 La valeur ligne *numéro ligne* **est trop longue.**

Explication : Le fichier de base de données des opérateurs contient une ligne trop longue.

Action de l'utilisateur : Supprimez la ligne trop longue du fichier de base de données des opérateurs.

ICA4115 Code *code* **doublé ligne** *numéro ligne* **ignoré.**

Explication : Rencontré un code en double.

Action de l'utilisateur : Supprimez le code en double du fichier de base de données des opérateurs.

ICA4116 Une valeur ligne *numéro ligne* **n'existe pas.**

Explication : Rencontré une zone vide.

Action de l'utilisateur : Ajoutez une valeur dans la zone vide avec le menu smitty/SMIT.

ICA4117 La valeur doit être O, Oui, N ou Non ligne *numéro ligne***.**

Explication : Cette zone demande une valeur O, Oui, N ou Non.

Action de l'utilisateur : Ajoutez ou modifiez les données avec le menu smitty/SMIT.

ICA4118 La valeur doit être supérieure à 0 ligne *numéro ligne***.**

Explication : La valeur de cette zone doit être positive.

Action de l'utilisateur : Remplacez la valeur de la zone par une valeur positive avec le menu smitty/SMIT.

ICA4119 Valeur incorrecte, ligne *numéro ligne***.**

Explication : Rencontré une valeur non valide sur la ligne indiquée.

Action de l'utilisateur : Remplacez la valeur avec le menu smitty/SMIT.

ICA4120 L'opérateur *nom* **n'est pas valable et est ignoré.**

Explication : Un opérateur incorrect a été détecté.

Action de l'utilisateur : Ajoutez un opérateur correct à l'aide du menu smitty/SMIT.

ICA4121 Impossible d'ajouter un opérateur à la liste.

Explication : Impossible d'ajouter un opérateur à la liste des opérateurs.

Action de l'utilisateur : Contrôlez la validité de l'opérateur.

ICA4122 Code *code* **doublé ligne** *numéro ligne* **ignoré.**

Explication : Code en double dans une strophe d'opérateur.

Action de l'utilisateur : Rectifiez la strophe d'opérateur contenant des valeurs en double.

ICA4123 Erreur (*programme***) : Impossible d'obtenir un jeton IPC :** *numéro d'erreur*

Explication : Le programme n'a pas obtenu de jeton IPC.

ICA4124 Erreur (*programme***) : Erreur** *pageqErr* **lors de la lecture de la file d'attente.**

Explication : Le programme n'a pas pu lire le contenu de la file d'attente.

ICA4125 *nombre* **entrées de file d'attente.**

Explication : Message d'informations.

ICA4126 Le message ayant l'ID *ID* **a été supprimé.**

Explication : Message d'informations.

ICA4127 L'ID *ID* **n'est pas dans la file d'attente.**

Explication : Message d'informations.

ICA4128 Erreur (*programme***) : Erreur** *pageqErr* **en essayant de supprimer l'ID** *ID***.**

Explication : Le programme a tenté de supprimer un ID de la file d'attente.

ICA4129 La clé est : le contenu de *clé entrée* **est @** *ptr* **:** *ptr***.**

Explication : Message d'informations uniquement.

ICA4130 Caractéristiques du modem :

Explication : Données d'initialisation du modem.

ICA4131 Nom : *nom modem*

Explication : Données d'initialisation du modem.

ICA4132 Init : *chaîne init*

Explication : Données d'initialisation du modem.

ICA4133 Mode commande : *commande*

Explication : Données d'initialisation du modem.

ICA4134 Caractère de fin de commande : 0x*caractère de fin*

Explication : Données d'initialisation du modem.

ICA4135 Appel : *appel*

Explication : Données d'initialisation du modem.

ICA4136 Pause d'appel : *pause*

Explication : Données d'initialisation du modem.

ICA4137 Touche # : *appel lb*

Explication : Données d'initialisation du modem.

ICA4138 Touche * : *étoile*

Explication : Données d'initialisation du modem.

ICA4139 Raccrochage : *raccrochage*

Explication : Données d'initialisation du modem.

ICA4140 Réponse à une commande acceptée : *réponse commande acceptée*

Explication : Données d'initialisation du modem.

ICA4141 Connexion correcte : *connexion correcte*

Explication : Données d'initialisation du modem.

ICA4142 Echo : *écho*

Explication : Données d'initialisation du modem.

ICA4143 Enregistrement de débogage de modem : PUTS(*ID***) txd-**> *outStr*

Explication : Données d'échange de protocoles du modem.

ICA4144 Enregistrement de débogage de modem : PUTC(*ID***) txd-**> *outStr*

Explication : Données d'échange de protocoles du modem.

ICA4145 Enregistrement de débogage de modem : GET rxd-> *ID enregistrement*

Explication : Données d'échange de protocoles du modem.

ICA4146 Enregistrement de débogage de modem : INPUT(*ID enregistrement*

Explication : Données d'échange de protocoles du modem.

ICA4147 Enregistrement de débogage de modem :) rxd->

Explication : Données d'échange de protocoles du modem.

ICA4148 Enregistrement de débogage de modem : WAITFOR(*ID enregistrement*

Explication : Données d'échange de protocoles du modem.

ICA4149 Impossible de débloquer le signal du processus fils.

Explication : Tentative de déblocage du signal SIGCHLD en cours.

ICA4150 Impossible de bloquer le signal du processus fils.

Explication : Tentative de blocage du signal SIGCHLD en cours.

ICA4151 Le fichier de démarrage à chaud *chemin fichier* **n'existe pas.**

Explication : Message d'informations.

ICA4152 Impossible d'ouvrir le fichier de démarrage à chaud *chemin fichier*

Explication : Message d'informations.

ICA4153 Ligne trop longue dans le fichier de démarrage à chaud *chemin fichier***.**

Explication : Le fichier de démarrage à chaud contient des caractères non valides.

ICA4154 Le fichier de démarrage à chaud *chemin fichier* **contient des données inutilisées.**

Explication : Message d'informations.

ICA4155 Le fichier de démarrage à chaud *chemin fichier* **est vide.**

Explication : Message d'informations.

ICA4156 La ligne *numéro ligne* **du fichier de démarrage à chaud** *chemin fichier* **contient une adresse incorrecte** *adresse***, ignorée.**

Explication : Le fichier de démarrage à chaud contient des caractères non valides. Message d'informations.

ICA4157 La ligne *numéro ligne* **du fichier de démarrage à chaud** *chemin fichier* **contient un format incorrect ; ignorée.**

Explication : Le fichier de démarrage à chaud contient des caractères non valides. Message d'informations.

ICA4158 La ligne *numéro ligne* **du fichier de démarrage à chaud** *chemin fichier* **ne contient aucun message ; ignorée.**

Explication : Le fichier de démarrage à chaud ne contient aucun message. Message d'informations.

ICA4159 La ligne *numéro ligne* **du fichier de démarrage à chaud** *chemin fichier* **est incorrecte ; ignorée.**

Explication : Le fichier de démarrage à chaud contient des caractères non valides. Message d'informations.

ICA4160 Le démarrage à chaud des *nombre* **messages du fichier** *chemin fichier* **est terminé.**

Explication : Message d'informations.

ICA4161 Erreur (*programme***) : Trop d'erreurs consécutives dans le processus fils.**

Explication : Le processus fils contient trop d'erreurs consécutives. Ceci se produit si le fichier de définition des opérateurs ou des modems contient des caractères non valides.

Action de l'utilisateur : Contrôlez le fichier de base de données des opérateurs et le fichier de définition des modems avec le menu smitty/SMIT.

ICA4162 Le processus fils ne peut pas exécuter *programme* **:** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4163 Erreur (*numéro d'erreur***) : Le processus fils n'a pas pu générer un processus fils :** *nom programme***.**

Explication : Possibilité d'erreur système.

ICA4164 Impossible de créer la liste des opérateurs de récepteur de radiomessagerie.

Explication : Erreur de programmation interne.

ICA4165 Erreurs dans le fichier des opérateurs des récepteurs de radiomessagerie *fichier opérateurs*

Explication : La base de données des opérateurs contient des données non valides.

Action de l'utilisateur : Contrôlez le fichier de base de données des opérateurs avec le menu smitty/SMIT.

ICA4166 Message d'informations. La clé IPC est : 0x*Clé Ipc***.**

Explication : Message d'informations.

ICA4167 Impossible de créer la file d'attente page_q_err : *pageQerr***.**

Explication : Échec pendant la création de la file d'attente.

ICA4168 Fichier de messages de démarrage à chaud créé à *heure*

Explication : Message d'informations.

ICA4169 priorité -p *priorité numéro récepteur* **provenant de** *origine message*

Explication : Message d'informations.

ICA4170 **priorité -p** *priorité alphaPager@opérateur* **provenant de** *origine message*

Explication : Message d'informations.

ICA4171 **priorité -p** *priorité* **-n** *numéro récepteur@opérateur* **provenant de** *origine message*

Explication : Message d'informations.

ICA4172 **Fin du fichier des messages de démarrage à chaud.**

Explication : Message d'informations. Signale la fin du message.

ICA4173 **Impossible d'écrire dans le fichier des messages de démarrage à chaud** *fichier***.**

Explication : Le fichier des messages de démarrage à chaud indiqué n'existe peut-être pas.

ICA4174 *heure* **STATUS-REQUEST provenant de** *utilisateur@hôte*

Explication : Affiche les données de la requête de statut.

ICA4175 *heure* **SUMMARY-REQUEST provenant de** *utilisateur@hôte*

Explication : Affiche les données de la requête de résumé.

ICA4176 *nombre* **entrées de file d'attente.**

Explication : Décompte le nombre d'entrées contenues dans la file d'attente du récepteur de messagerie.

ICA4177 **Entrée la plus ancienne : ID** *ID* **reçue à** *heure***.**

Explication : Affiche la plus ancienne des entrées de la file d'attente.

ICA4178 **Reconnecte la mémoire après qu'une expansion n'ait pas abouti.**

Explication : Possibilité d'erreur système.

ICA4179 **Reconnecte la mémoire après qu'une expansion ne se soit pas alignée.**

Explication : Possibilité d'erreur système.

ICA4180 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_print() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4181 **Impossible de lever le sémaphore PAGE_Q dans page_q_print() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4182 **lien** *lien* -> **ID message :** *ID***.**

Explication : Message d'informations.

ICA4183 **Priorité :** *priorité***.**

Explication : Message d'informations.

ICA4184 Personne : *nom*

Explication : Message d'informations.

ICA4185 Opérateur : *opérateur***.**

Explication : Message d'informations.

ICA4186 Message : *message***.**

Explication : Message d'informations.

ICA4187 Impossible d'obtenir une mémoire partagée : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4188 Impossible d'obtenir une mémoire partagée auxiliaire : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4189 Impossible d'obtenir le sémaphore PAGE_Q.

Explication : Possibilité d'erreur système.

ICA4190 Impossible d'initialiser le sémaphore PAGE_Q dans page_q_create() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4191 Impossible de définir le sémaphore PAGE_Q dans page_q_create() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4192 Impossible d'abaisser le sémaphore PAGE_Q dans page_q_empty() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4193 Impossible de lever le sémaphore PAGE_Q dans page_q_empty() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4194 Impossible d'abaisser le sémaphore PAGE_Q dans page_q_enq(*nom***,***message***) :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4195 Impossible de lever le sémaphore PAGE_Q dans page_q_enq() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4196 page_q_enq() : ID(*id***) Pri(***priorité***) Person(***name***) Mesg(***message***.**

Explication : Message d'informations.

ICA4197 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_head() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4198 **Impossible de lever le sémaphore PAGE_Q dans page_q_head() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4199 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_first() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4200 **Impossible de lever le sémaphore PAGE_Q dans page_q_first() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4201 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_next() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4202 **Impossible de lever le sémaphore PAGE_Q dans page_q_next() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4203 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_tail() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4204 **Impossible de lever le sémaphore PAGE_Q dans page_q_tail() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4205 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_del() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4206 **Impossible de lever le sémaphore PAGE_Q dans page_q_del() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4207 **page_q_del(***ID***).**

Explication : Informations de débogage.

ICA4208 **Impossible d'abaisser le sémaphore PAGE_Q dans page_q_deq() :** *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4209 Impossible de lever le sémaphore PAGE_Q dans page_q_deq() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4210 page_q_del() : ID(*id***) Pri(***priorité***) Person(***nom***) Mesg(***message***.**

Explication : Message d'informations.

ICA4211 Impossible d'abaisser le sémaphore PAGE_Q dans page_q_walk() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4212 Impossible de lever le sémaphore PAGE_Q dans page_q_walk() : *numéro d'erreur***.**

Explication : Possibilité d'erreur système.

ICA4213 PAGE_Q est plein.

Explication : La file d'attente des messages est pleine.

Action de l'utilisateur : Attendez quelques temps pour envoyer le message.

ICA4300 Raccrochage.

Explication : Raccrochage de la ligne.

ICA4301 Initialisation du modem ...

Explication : Initialisation du modem avec la chaîne d'initialisation.

ICA4302 Numérotation ...

Explication : Composition du numéro de téléphone.

ICA4303 Connexion en attente.

Explication : En attente de la connexion de modem.

ICA4304 CONNEXION ETABLIE *débit*

Explication : Connexion au débit indiqué (débit en bauds)

ICA4305 CONNECTÉ !!!!!!!

Explication : Connecté au fournisseur de service de radiomessagerie.

ICA4306 Invite de mode automatique en demande.

Explication : Requête d'invite de mode automatique en cours de traitement. En attente de l'ID de session.

ICA4307 Invite OK.....

Explication : ID fourni par le service.

ICA4308 Envoi de la requête de mode automatique.

Explication : Envoi de l'ID et du SST au fournisseur de service de radiomessagerie.

ICA4309 Requête de mode automatique envoyée .....OK !

Explication : Reçu [p. La communication a abouti.

ICA4310 Envoi du message

Explication : Transmission du bloc de message.

ICA4311 Réponse en attente.

Explication : Attente de la confirmation.

ICA4312 Accusé de réception reçu. Message transmis.
ICA4313 Accusé de réception négatif reçu, renvoi du bloc. Essai *essais*

Explication : Reçu un accusé réception négatif. Le fournisseur demande un deuxième envoi du message.

ICA4314 Erreur de transaction. Renvoi du bloc. Essai *essais*

Explication : Erreur de transaction. Renvoi du bloc.

ICA4315 Arrêt de la connexion par l'opérateur.

Explication : Le fournisseur de service de radiomessagerie a mis fin à la communication. Contactez le fournisseur pour identifier le problème.

ICA4350 fwpage [opérateur="..."] [modem="..."] [ID="..."] [msg="..."]

Explication : Syntaxe de la commande fwpage. Vérifiez les paramètres et réessayez.

ICA4351 Le fichier *fichier* **n'existe pas.**

Explication : Vérifiez que le fichier figure bien dans le répertoire approprié. Les fichiers carriers.cfg, modems.cfg et pager.cfg doivent être créés avant d'utiliser ce code.

ICA4352 Le fichier *fichier* **est altéré.**

Explication : Le fichier a été modifié par l'utilisateur et n'est plus au format de la strophe. Tous les attributs doivent être entrés via l'interface utilisateur graphique.

ICA4353 Le fichier *fichier* **est trop long. Réduisez sa taille et réessayez.**

Explication : Le paramètre 'fichier' est trop long. Réduisez sa taille et réessayez.

ICA4354 *variable* **incorrecte.**

Explication : Si la vitesse de transmission est incorrecte, les options valides sont : 600, 1200, 2400, 4800, 9600, 14400. Si le nombre de bits de données par octet est incorrect, les options valides sont : 7, 8. Si le nombre de bits d'arrêt est incorrect, les options valides sont : 1, 2. Si l'indicatif de ligne extérieure est incorrect, les valeurs doivent être numériques. Si le protocole de messagerie est incorrect, seul le protocole TAP est pris en charge dans cette version. Dans le cas d'une erreur d'ID, vérifiez que l'ID n'est composé que de valeurs numériques. Si la parité est incorrecte, les options valides sont : P(paire), I(impaire), A(aucune), E(espace), M(marque). Si le port de communication est incorrect, les options valides sont : COM1, COM2 .... Sélectionnez un port de communication en dessous de COM 10 pour cette version. Dans le cas d'une erreur liée aux caractères du message, vérifiez la présence de caractères spéciaux dans le message.

ICA4355 Erreur de définition des paramètres dans *emplacement***.**

Explication : Impossible de définir les paramètres dans (emplacement). Vérifiez les paramètres et réessayez.

ICA4356 si *condition***, erreur de lecture sur port COM.**

Explication : Erreur de lecture sur port COM. Activez l'écho pour le modem et réessayez.

ICA4357 si *emplacement***, erreur d'écriture sur port COM.**

Explication : Erreur d'écriture sur port COM.

ICA4358 Erreur *type*

Explication : Erreur indiquée par 'type'. Contrôlez le fichier journal et corrigez l'erreur.

ICA4359 Nombre d'essais maximal dépassé dans *emplacement***. Abandon du programme .....**

Explication : 60 tentatives d'ouverture du port de communication ont été faites en 60 minutes. Si elles ont toutes échoué, vérifiez les connexions du matériel. Essayez d'envoyer le message 10 fois en 10 minutes. Si toutes les tentatives échouent, le fournisseur de service de messagerie est peut-être en dérangement.

ICA4360 Caractère inconnu dans le numéro de téléphone de l'opérateur : **ptéléphone opérateur*

Explication : Un caractère inconnu a été détecté dans le numéro de téléphone de l'opérateur. Vérifiez le numéro et réessayez.

ICA4361 Avertissement !!! Le modem du récepteur de radiomessagerie doit avoir une vitesse inférieure à 2400 bps.

Explication : Ce message n'a qu'une valeur d'avertissement. La vitesse du modem du fournisseur de service doit normalement être inférieure à 2400 bps.

ICA4362 Impossible d'initialiser le modem

Explication : Modifiez la chaîne d'initialisation du modem et réessayez.

ICA4363 Le modem a renvoyé un message d'erreur.

Explication : Erreur de communication du modem.

ICA4364 *essais* **essai sur port de communication ouvert - erreur. Nouvel essai dans 1 minute**

Explication : Erreur d'ouverture du port de communication. Un autre programme l'utilise probablement déjà. Un nouvel essai sera automatiquement fait dans 1 minute.

ICA4365 Essai *essais* **- le message n'a pas été transmis. Nouvel essai dans 1 minute.**

Explication : L'envoi n'a pas abouti. Contrôlez le fichier journal pour identifier la cause du problème.

ICA4366 Message trop long - Le message a été tronqué.

Explication : Ce message n'a qu'une valeur d'avertissement. Le message est trop long. Le message a été tronqué pour passer.

ICA4367 Ramenez la longueur maximale du message à la valeur interne définie : *longueur message*

Explication : Ramenez la longueur maximale du message à la valeur par défaut définie. La longueur de message définie par l'utilisateur est supérieure à la longueur par défaut qui est de 80 caractères.

ICA4368 Action : *emplacement* **erreur**

Explication : Dans le cas d'une erreur d'ouverture du port de communication, contrôlez la configuration et réessayez. Dans le cas d'une erreur de fermeture, il s'agit d'un incident système. Dans le cas d'une erreur de purge, il s'agit d'un incident système. Dans le cas d'une erreur de numérotation, voyez la commande de numérotation. Vérifiez que le modem est un modèle compatible Hayes. Dans le cas d'une erreur de la requête d'ID, vérifiez que le fournisseur de service de radiomessagerie prend en charge le protocole TAP. Dans le cas d'une erreur d'invite automatique, vérifiez que le service de radiomessagerie fonctionne correctement. Dans le cas d'une erreur d'envoi du message, contrôlez le fichier journal pour identifier la cause de l'échec. Dans le cas d'une erreur d'invite, c'est le fournisseur de service de radiomessagerie qui n'est pas en mesure de renvoyer une invite.

ICA4369 Erreurs de transaction trop nombreuses ... abandon ....

Explication : Les erreurs de transaction sont trop nombreuses. La transmission est abandonnée.

ICA4370 Trop d'accusés de réception négatifs reçus ... abandon du programme ...

Explication : Trop d'accusés de réception négatifs reçus du fournisseur. La transmission est abandonnée.

ICA4371 *szComPort* **sur port COM avec la fonction** *nom fonction* **- retour** *numéro d'erreur*

Explication : Vérifiez les paramètres et réessayez.

ICA4372 Le modem retourne un message d'erreur ..... *message*

Explication : Les messages sont : Not connected, Ringing, but not connected, No carrier, No dial tone, Busy, No answer (Non connecté, Sonnerie mais pas de connexion, Pas de porteuse, Pas de tonalité, Ligne occupée, Pas de réponse).

ICA4373 (*nom fonction***) Code réponse inconnu émis par le modem ou par l'opérateur :** *car1***,** *car2***.**

Explication : Ce message reprend la réponse du modem ou de l'opérateur que la fonction de radiomessagerie du pare-feu ne reconnaît pas. car1 et car2 sont les codes ASCII (hexadécimaux) des deux premiers caractères du message de réponse.

Action de l'utilisateur : Servez-vous de ces informations quand vous consulterez le manuel d'instructions du modem ou l'opérateur pour identifier la signification du message inconnu.

ICA5005 L'initialisation de SKIT n'a pas abouti. Code retour : *code retour*

Explication : L'initialisation de la socket sécurisée n'a pas abouti. Le code retour de SKIT est affiché.

ICA5014 Serveur tunnel pour client distant en écoute sur le port *port serveur #*

Explication : Le numéro du port configuré pour sslrctd est affiché.

ICA5015 Connexion acceptée en provenance de *chp0.chp1.chp2.chp3*

Explication : L'adresse IP du client est affichée.

ICA5017 Impossible d'obtenir une socket sécurisée. Le code retour de la fonction skit_secure_soc_init est : *code retour fonction*

Explication : Impossible d'obtenir une socket sécurisée pour cause d'échec de la fonction skit_secure_soc_init().

ICA5018 Les spécifications chiffrées du serveur esclave utilisées sont : *spec1 spec2 spec3*

Explication : Les spécifications chiffrées sont affichées.

ICA5019 Impossible d'obtenir le parc d'adresses IP de Free Homenet.

Explication : Problème au niveau des filtres dynamiques.

ICA5020 Impossible d'ouvrir le fichier de configuration du client distant.

Explication : Le fichier /etc/security/rcsfile.cfg est introuvable.

Action de l'utilisateur : Vérifiez l'existence du fichier et son contenu éventuel.

ICA5021 Le mot clé '*mot clé***' est introuvable.**

Explication : Le fichier /etc/security/rcsfile.cfg ne contient pas le mot clé indiqué.

Action de l'utilisateur : Contrôlez et rectifiez le fichier /etc/security/rcsfile.cfg.

ICA5024 Erreur de la fonction skit_secure_soc_write() dans *nom routine***.**

Explication : Cette routine de la fonction skit_secure_soc_write() n'a pas abouti.

ICA5025 Erreur de la fonction skit_secure_soc_write() dans ACKClient().

Explication : La routine ACKClient() de la fonction skit_secure_soc_write() n'a pas abouti.

ICA5026 Code retour incorrect reçu du client dans *nom routine***.**

Explication : Un code retour inattendu a été reçu du client dans cette routine.

ICA5027 Reçu un code retour pour une requête incorrecte en provenance du client dans *nom routine***.**

Explication : Le code requête contenu dans le code retour du client est inattendu dans cette routine.

ICA5028 Requête de connexion non valide.

Explication : Le format du message de la requête de connexion n'est pas valide.

ICA5030 ID de client distant inconnu : *ID client distant*

Explication : Cet ID utilisateur n'est pas connu de la machine pare-feu.

Action de l'utilisateur : Modifiez les données de l'utilisateur associées à ce client distant.

ICA5031 Erreur de la fonction skit_secure_soc_write dans RCTLoginPhase().

Explication : La phase de connexion de la fonction skit_secure_soc_write() n'a pas abouti.

ICA5035 Requête de déconnexion non valide.

Explication : Le format du message de la requête de déconnexion n'est pas valide.

ICA5067 Paquet non valide reçu.

Explication : Le format du paquet reçu n'est pas valide.

ICA5078 Reçu une requête non reconnue dans svrReqHandler()

Explication : Une requête non reconnue a été reçue et sera ignorée.

ICA5082 Le tunnel du client *ID client distant* **a été déconnecté.**

Explication : Le tunnel du client distant identifié par cet ID a été déconnecté.

ICA5086 L'ID *ID utilisateur* **n'est pas défini.**

Explication : Cet ID utilisateur n'existe pas sur la machine pare-feu.

ICA5087 Erreur d'authentification pour '*ID utilisateur***'.**

Explication : L'authentification de cet ID utilisateur n'a pas abouti.

ICA5089 La fonction rcFilterClear() n'a pas abouti. Code retour : *code retour***.**

Explication : La fonction rcFilterClear() n'a pas abouti et a retourné le code mentionné.

Action de l'utilisateur : Contrôlez la présence du client LAN IPSEC. Ces produits ne peuvent pas coexister.

ICA5090 La fonction rcFilterInit() n'a pas abouti. Code retour : *code retour***.**

Explication : La fonction rcFilterInit() n'a pas abouti et a retourné le code mentionné.

ICA5091 La fonction TunnelUp() ne peut pas lancer le fichier exécutable *ligne de commande***.**

Explication : L'appel système correspondant à la ligne de commande affichée n'a pas abouti.

ICA5092 Impossible d'obtenir le mot de passe du fichier de clés depuis l'appel de fonction recoverstash.

Explication : Impossible de récupérer le mot de passe du fichier de clés dans le fichier cache.

ICA8001 SYSLOG/udp : service inconnu.
ICA8002 La fonction *nom_fonction* **n'a pas abouti -** *numéro d'erreur***, errno2 = 0x***errno2*

Explication : Syslogd n'a pas pu exécuter la fonction indiquée, le traitement est interrompu. Le numéro d'erreur (num_erreur) est ajouté au message d'erreur.

Action de l'utilisateur : Contactez le responsable du système. Responsable système : Utilisez le numéro d'erreur pour déterminer la cause de la panne.

ICA8004 Erreur détectée sur la socket AF_INET - slogd n'assurera plus la surveillance de la socket.
ICA8006 Nom de priorité \"*priorité***\" inconnu**

Explication : Un nom de priorité incorrect a été détecté dans le fichier de configuration.

Action de l'utilisateur : Contactez le responsable du système. Responsable système : Vérifiez le fichier de configuration.

ICA8007 Nom de fonction \"*fonction***\" inconnu**

Explication : Un nom de fonction incorrect a été détecté dans le fichier de configuration.

Action de l'utilisateur : Contactez le responsable du système. Responsable système : Vérifiez le fichier de configuration.

ICA8008 Message de SYSLOG@*nom d'hôte* **reçu à** *horodatage***...**

Explication : Le fichier de configuration du démon de syslog contient une entrée permettant d'envoyer des messages syslog à tous les utilisateurs connectés. Ce message sera envoyé à tous les utilisateurs actuellement connectés au système sur lequel le démon de syslog s'exécute.

Action de l'utilisateur : Aucune. Responsable système :Aucune

---

ICA8009 Arrêt de SYSLOGD à la réception du signal *signal*

Explication : Le démon de syslog a reçu un signal qui a provoqué son arrêt.

Action de l'utilisateur : Aucune. Responsable système :Aucune

---

ICA8010 Redémarrage de SYSLOGD
ICA8012 SYSLOGD n'a pas pu écrire dans le SMF - *texte_erreur*

Explication : Une erreur s'est produite lors de l'écriture d'un enregistrement dans le SMF. Un texte d'explication est ajouté au message d'erreur.

Action de l'utilisateur : Contactez le responsable du système. Responsable système : Utilisez le texte d'explication pour déterminer la cause de l'erreur d'écriture.

ICA8013 La mise à jour du statut du processus n'a pas abouti - code retour = 0x*code_retour*

Explication : Une erreur s'est produite lors d'une tentative de mise à jour de l'état du processus syslogd dans le cadre de l'exécution du pare-feu. Le code de retour indique l'erreur renvoyée lors de l'appel de l'état du processus de mise à jour.

Action de l'utilisateur : Contactez le responsable du système. Responsable système : Contactez le responsable de la maintenance

---

ICA8014 Option inconnue (-*option_démarrage***) spécifiée dans l'appel de SYSLOGD.**

Explication : Une erreur s'est produite lors d'une tentative de démarrage du processus du démon de syslogd. L'option indiquée n'est pas prise en charge lors de l'appel de syslogd.

Action de l'utilisateur : Vérifiez les options de redémarrage et relancez le démon de syslogd. Responsable système : Si le problème persiste, contactez le responsable de la maintenance

ICA8015 Entrée incorrecte (*données_config*) dans le fichier de configuration

Explication : Une erreur s'est produite lors d'une tentative d'analyse d'une entrée du fichier de configuration de SYSLOG.

Action de l'utilisateur : Vérifiez les entrées du fichier de configuration et relancez le démon de syslogd. Responsable système : Si le problème persiste, contactez le responsable de la maintenance

ICA8016 *nom_fonction* **n'a pas abouti pour** *nom fichier* **-** *numéro d'erreur*

Explication : Une erreur s'est produite lors d'une tentative d'exécution de la fonction sur le périphérique indiqué. Le numéro d'erreur est ajouté au message d'erreur.

Action de l'utilisateur : Vérifiez que le périphérique indiqué existe et relancez la requête. Si le problème persiste, contactez le responsable du système. Responsable système : Si le problème persiste, contactez le responsable de la maintenance

ICA8050 *fonction* **n'a pas abouti.** *texte_erreur*

Explication : Une erreur s'est produite pendant l'exécution de la fonction indiquée dans le message. Le texte du message d'erreur fournit des informations complémentaires sur l'erreur.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message et relancez l'opération si nécessaire.

ICA8051 *fonction* **n'a pas abouti : code retour = 0x***code_retour*

Explication : Une erreur s'est produite pendant l'exécution de la fonction indiquée dans le message. Le code retourné par la fonction est également affiché.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message et relancez l'opération si nécessaire.

ICA8052 Activation de la journalisation des filtres par FWSTACKD pour *nom_pile***.**

Explication : La fonction FWSTACKD tente d'activer la journalisation du filtrage de paquet.

Réaction du système : Poursuite du traitement.

ICA8053 FWSTACKD ne peut pas activer la journalisation des filtres pour *nom_pile***.** *texte_erreur*

Explication : L'activation de la journalisation du filtrage des paquets a échoué pour la raison indiquée dans le message d'erreur joint.

Réaction du système : L'opération demandée ne sera donc pas effectuée.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message d'erreur puis réactivez la journalisation des filtres avec la commande **fwfilter cmd=startlog**.

ICA8054 Activation de la journalisation NAT par FWSTACKD pour *nom_pile***.**

Explication : La fonction FWSTACKD tente d'activer la journalisation des conversions d'adresse réseau (NAT).

Réaction du système : Poursuite du traitement.

ICA8055 FWSTACKD ne peut pas activer la journalisation NAT pour *nom_pile***.** *texte_erreur*

Explication : L'activation de la journalisation des conversions d'adresse réseau a échoué pour la raison indiquée dans le message d'erreur joint.

Réaction du système : L'opération demandée ne sera donc pas effectuée.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message d'erreur puis réactivez la journalisation NAT avec la commande **fwnat cmd=startlog**.

ICA8056 Activation de la NAT par FWSTACKD pour *nom_pile***.**

Explication : La fonction FWSTACKD tente d'activer la conversion d'adresse réseau (NAT).

Réaction du système : Poursuite du traitement.

ICA8057 FWSTACKD ne peut pas activer la NAT pour *nom_pile***.** *texte_erreur*

Explication : L'activation de la conversion d'adresse réseau a échoué pour la raison indiquée dans le message d'erreur joint.

Réaction du système : L'opération demandée ne sera donc pas effectuée.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message d'erreur puis réactivez la conversion d'adresse réseau avec la commande **fwnat cmd=update**.

ICA8058 Réactivation des définitions de tunnel par FWSTACKD pour *nom_pile***.**

Explication : La fonction FWSTACKD tente de réactiver les définitions de tunnel qui étaient actives avant l'arrêt du système.

Réaction du système : Poursuite du traitement.

ICA8059 FWSTACKD ne peut pas réactiver les définitions de tunnel pour *nom_pile***.** *texte_erreur*

Explication : L'activation des définitions de tunnel a échoué pour la raison indiquée dans le message d'erreur joint.

Réaction du système : Les définitions de tunnel ne sont pas activées.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message d'erreur puis réactivez les définitions de tunnel avec la commande **fwtunnl cmd=activate**.

ICA8060 Activation des règles de sockets et des règles de filtrage par FWSTACKD pour *nom_pile***.**

Explication : La fonction FWSTACKD tente d'activer le jeu de règles de sockets et de règles de filtrage courant.

Réaction du système : Poursuite du traitement.

ICA8061 FWSTACKD ne peut pas activer les règles de sockets et les règles de filtrage pour *nom_pile***.** *texte_erreur*

Explication : L'activation des règles de sockets et des règles de filtrage a échoué pour la raison indiquée dans le message d'erreur joint.

Réaction du système : Les règles de filtrage par défaut s'appliqueront. L'accès local sera autorisé mais tous les autres types d'accès seront refusés.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message d'erreur puis réactivez les règles de sockets et de filtrage avec la commande **fwfilter cmd=update**.

ICA8062 Activation du support RealAudio par FWSTACKD pour *nom_pile***.**

Explication : La fonction FWSTACKD tente d'activer le support RealAudio.

Réaction du système : Poursuite du traitement.

ICA8063 FWSTACKD ne peut pas activer le support RealAudio pour *nom_pile***.** *texte_erreur*

Explication : L'activation du support RealAudio a échoué pour la raison indiquée dans le message d'erreur joint.

Réaction du système : Les services RealAudio ne sont pas accessibles.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message d'erreur puis activez le support RealAudio avec la commande **fwaudio cmd=change**.

ICA8064 *fonction* **n'a pas abouti.** *texte_erreur*

Explication : Une erreur s'est produite pendant l'exécution de la fonction indiquée dans le message. Le texte du message d'erreur fournit des informations complémentaires sur l'erreur.

Action de l'utilisateur : Corrigez l'erreur signalée dans le message et relancez l'opération si nécessaire.

ICA9000 La version d'évaluation d'IBM Firewall arrivera à expiration dans *nombre* **jours.**

Explication : Ce logiciel est distribué comme version d'évaluation et se désactivera dans les conditions indiquées.

ICA9001 Avertissement du programme de contrôle d'intégrité du système de fichiers - *texte description avertissement*

Explication : fwfschk a détecté une anomalie dans le système de fichiers constituant un danger potentiel.

ICA9002 Dernier message répété %1$d fois.

Explication : Message généré par syslogd lorsqu'un message identique est journalisé sans s'accompagner d'aucun autre message. Le message est conservé pour que le contrôle de journalisation puisse détecter la condition associée. Ce message doit être dans la même langue que celle utilisée pour écrire le véritable message de syslogd.

ICA9003 Echec d'authentification de l'utilisateur *nom* **sur le serveur de configuration.**

Explication : Le serveur de configuration du pare-feu ne peut pas authentifier le nom utilisateur indiqué.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9004 L'utilisateur *nom* **a été authentifié sur le serveur de configuration.**

Explication : Le serveur de configuration du pare-feu a authentifié l'utilisateur indiqué.

ICA9005 Démarrage du serveur de configuration à distance.

Explication : Le serveur de configuration a été initialisé.

ICA9006 Arrêt du serveur de configuration à distance.

Explication : Le serveur de configuration a été arrêté.

ICA9007 Le serveur de configuration à distance n'a pas pu ouvrir le catalogue de messages.

Explication : Un ou plusieurs des catalogues de messages utilisés par le serveur de configuration à distance sont sans doute manquants.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9008 Le serveur de configuration à distance n'a pas pu exécuter la fonction getpeername() : erreur *numéro d'erreur***.**

Explication : Le serveur de configuration du pare-feu ne peut pas obtenir les informations relatives au client.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9009 Le serveur de configuration à distance n'a pas pu exécuter la fonction getsockname() : erreur *numéro d'erreur***.**

Explication : Le serveur de configuration du pare-feu ne peut pas obtenir les informations le concernant.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9010 Le serveur de configuration à distance n'a pas pu obtenir les informations relatives à la carte.

Explication : Le serveur de configuration du pare-feu ne peut pas obtenir les informations relatives à la carte.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9011 Le serveur de configuration n'est pas activé pour la configuration à distance.

Explication : Le serveur de configuration est configuré en mode local (paramètre local=yes) et le client réside sur une machine distante.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9012 Le serveur de configuration à distance n'a pas pu lire la requête de connexion.

Explication : Le serveur de configuration à distance n'a pas pu lire la requête de connexion du client.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9013 Le serveur de configuration à distance a reçu une requête de connexion incorrecte.

Explication : La requête de connexion contenait des données non valides.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9014 Le serveur de configuration à distance n'a pas pu établir le tube.

Explication : Le serveur de configuration à distance n'a pas pu établir de tube pour l'authentification.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9015 Le serveur de configuration à distance n'a pas pu créer le processus.

Explication : Le serveur de configuration à distance n'a pas pu créer de processus pour l'authentification.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9016 Démarrage du démon EFM.

Explication : Le démon EFM a été initialisé sur le pare-feu géré.

ICA9017 Arrêt du démon EFM - code retour = *valeur***.**

Explication : Le démon EFM s'arrête avec le code retour indiqué.

ICA9018 Le démon EFM n'a pas pu ouvrir le catalogue de messages.

Explication : Un ou plusieurs des catalogues de messages utilisés par le démon EFM sont sans doute absents.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9020 Impossible de commuter l'ID utilisateur en cours.

Explication : Échec de l'appel système destiné à commuter l'ID utilisateur en cours.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9021 Ce pare-feu ne supporte pas le mode *logon***.**

Explication : Ce pare-feu ne supporte pas le mode indiqué.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9022 *utilisateur* **n'est pas autorisé à se connecter au pare-feu en mode** *logon***.**

Explication : Cet utilisateur n'est pas autorisé à se connecter au pare-feu dans le mode indiqué.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9023 Impossible de charger la DLL du démon EFM.

Explication : Impossible de charger la DLL EFM.

Action de l'utilisateur : Contactez l'administrateur du pare-feu.

ICA9024 Requête de transfert envoyée par *utilisateur* **au pare-feu** *machine***.**

Explication : Le transfert a commencé.

ICA9025 Fin de la requête de transfert - code retour : *code retour***.**

Explication : Le transfert a abouti.

ICA9026 Requête de transfert envoyée par *utilisateur* **au pare-feu** *machine* **à** *heure***.**

Explication : Le transfert a commencé à l'heure indiquée.

ICA9027 Le fichier *nom fichier* **dans la fonction** *fonction* **a été ajouté à la requête de transfert.**

Explication : Le fichier spécifié va être transféré.

ICA9028 Requête d'activation envoyée par *utilisateur* **au pare-feu** *machine***.**

Explication : L'activation a commencé.

ICA9029 Fin de la requête d'activation - code retour : *code retour***.**

Explication : L'activation a abouti.

ICA9030 Requête d'activation envoyée par *utilisateur* **au pare-feu** *machine* **à** *heure***.**

Explication : L'activation a commencé à l'heure indiquée.

ICA9031 Fin de l'activation de la fonction *fonction* **- code retour :** *code retour***.**

Explication : L'activation de la fonction indiquée a abouti.

ICA9032 Configuration NAT mise à jour à *heure* **le** *date***.**

Explication : La configuration NAT a été mise à jour.

ICA9033 Support NAT (niveau *version.édition***) initialisé à** *heure* **le** *date***.**

Explication : Le support de conversion d'adresse réseau du pare-feu a été initialisé.

ICA9034 Support NAT désactivé à *heure* **le** *date*

Explication : Le support de conversion d'adresse réseau a été désactivé.

ICA9035 NAT n'a pas pu allouer d'adresse enregistrée pour l'adresse sécurisée *adresse IP sécurisée***.**

Explication : L'adresse sécurisée n'a pas été convertie faute d'adresse disponible dans le parc des adresses enregistrées.

ICA9036 NAT a alloué l'adresse enregistrée *adresse IP enregistrée* **dans le parc d'adresses.**

Explication : L'adresse enregistrée a été replacée dans le parc des adresses IP enregistrées.

ICA9037 Mise à jour automatique des interfaces de pare-feu le *heure_et_date***.**

Explication : Le programme d'initialisation du pare-feu a appelé la fonction **UpdateInterfaces()** pour déclencher la mise à jour automatique du fichier des interfaces du pare-feu fwadpt.cfg.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9038 L'interface *adresse* **a été supprimée de la configuration du pare-feu.**

Explication : L'adresse en notation décimale à point affichée avait été répertoriée dans le fichier de configuration du pare-feu fwadpt.cfg mais était inconnue de la pile de protocoles TCP et, en conséquence, a été supprimée du fichier de configuration.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9039 L'interface *adresse* **a été ajoutée à la configuration du pare-feu.**

Explication : L'adresse en notation décimale à point affichée a été trouvée par la pile de protocoles TCP mais était absente du fichier de configuration du pare-feu fwadpt.cfg et, en conséquence, y a été ajoutée.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9040 Le masque *ancien masque* **de l'interface** *adresse* **a été remplacé par** *nouveau masque***.**

Explication : Le masque contenu dans le fichier fwadpt.cfg ne correspondait pas au matériel installé détecté. La zone du masque correspondant a été mise à jour dans le fichier fwadpt.cfg.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9041 Aucune interface n'a été détectée sur cette machine.

Explication : Aucune carte d'interface n'a été détectée sur cette machine.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9042 NAT activée avec une adresse Plusieurs à un *adresse plusieurs à un***.**

Explication : La NAT a été initialisée et est active. Si l'adresse est 0, on en déduit que la conversion "plusieurs à un" est inactive.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9043 Impossible d'initialiser la NAT ; code retour *code retour***.**

Explication : La NAT ne s'est pas initialisée et est inactive.

Réaction du système : Il n'y aura pas d'appel de fonction NAT.

Action de l'utilisateur : Pour pouvoir utiliser la NAT, examinez préalablement le code retour et corrigez le problème qu'il signale. Contactez l'assistance IBM si vous n'y parvenez pas.

ICA9044 NAT désactivée.

Explication : La NAT a été désactivée et est inactive.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9045 La NAT a alloué la paire adresse:port *adresse***:***port* **pour la paire addresse:port sécurisée** *adresse sécurisée***:***port*

Explication : La NAT a alloué la paire adresse:port du parc d'adresses pour le compte de l'hôte sécurisé.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9046 La NAT n'a pas pu allouer d'adresse "plusieurs à un" pour l'adresse sécurisée *adresse sécurisée***.**

Explication : Il n' y a plus de port disponible pour l'adresse "plusieurs à un".

Réaction du système : Le paquet de l'hôte local a été ignoré.

Action de l'utilisateur : On en déduit que les connexions en attente sont trop nombreuses. L'administrateur pourra réduire le délai d'expiration de l'adresse "plusieurs à un" pour éliminer plus rapidement les entrées de table de conversion inactives.

ICA9047 La NAT a annulé l'attribution de la paire adresse:port *adresse*:*port* **à la paire addresse:port sécurisée** *adresse sécurisée*:*port*

Explication : La NAT a renvoyé la paire adresse:port spécifiée dans le parc d'adresses.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9048 La NAT a détecté un paquet fragmenté avec le protocole : *protocole* **adresse:port** *adresse*:*port* **adresse sécurisée:port** *adresse sécurisée*:*port***.**

Explication : La NAT a détecté un paquet de contrôle FTP fragmenté ou un message d'erreur ICMP fragmenté. La NAT convertira un paquet de contrôle FTP mais la charge utile ne sera pas examinée. Dans le cas d'une commande PORT fragmentée, les données FTP n'aboutiront pas car l'adresse IP contenue dans le message ne sera pas convertie. Dans le cas d'un message d'erreur ICMP fragmenté, le paquet sera ignoré.

Réaction du système : Reportez-vous à l'explication.

Action de l'utilisateur : Si ce phénomène se répète, signalez-le à l'assistance IBM.

ICA9049 La NAT a détecté un fragment inutilisable provenant de *adresse source* **vers** *adresse destination* **et ne peut pas le convertir.**

Explication : La NAT a détecté un fragment de datagramme arrivé avant le premier segment de ce même datagramme.

Réaction du système : La NAT ne peut pas convertir le fragment correctement et le datagramme est ignoré.

Action de l'utilisateur : Si ce phénomène se répète, signalez-le à l'assistance IBM.

ICA9050 La NAT n'a pas pu convertir un paquet avec le protocole :*protocole***, adresse source:port** *adresse*:*port***, adresse destination:port** *adresse sécurisée*:*port* **; code retour :** *code retour***.**

Explication : La NAT n'a pas pu convertir un paquet.

Réaction du système : Le paquet est ignoré.

Action de l'utilisateur : Si ce phénomène se répète, signalez-le à l'assistance IBM.

ICA9051 La NAT a détecté l'arrivée d'un paquet avec le protocole *protocole* **; paire adresse:port cible** *adresse*:*port* **paire adresse:port sécurisée :** *adresse sécurisée*:*port***.**

Explication : La NAT a détecté l'arrivée d'un paquet.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9052 **La NAT a détecté le départ d'un paquet avec le protocole** *protocole* **; paire adresse:port cible :** *adresse*:*port* **paire adresse:port source sécurisée :** *adresse sécurisée*:*port*.

Explication : La NAT a détecté l'envoi d'un paquet.

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9053 *valeur chaîne nom fichier* **ligne %3$d**

Explication : Débogage

Réaction du système : Aucune

Action de l'utilisateur : Aucune

ICA9054 **L'adresse IP** *adresse* **ne peut pas être utilisée simultanément comme une adresse "plusieurs à un" et comme une adresse d'interface sécurisée/non sécurisée.**

Explication : Ces deux adresses ne peuvent pas être identiques.

Réaction du système : L'action demandée ne sera pas exécutée.

Action de l'utilisateur : Choisissez une adresse sécurisée/non sécurisée ou une adresse "plusieurs à un" distincte.

ICA9055 **La NAT a détecté un fragment inutilisable provenant de** *adresse source* **vers** *adresse destination* **mais peut le convertir.**

Explication : La NAT a détecté l'arrivée d'un fragment de datagramme interne ou final inutilisable.

Réaction du système : La NAT a pu convertir correctement le fragment et n'a donc pas ignoré le datagramme.

Action de l'utilisateur : Aucune

ICA9060 **Erreur d'initialisation fatale du serveur de configuration - socket() :** *message d'erreur système*

Explication : L'initialisation du serveur de configuration a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et réinitialisez le serveur de configuration.

ICA9061 **Erreur d'initialisation fatale du serveur de configuration - listen() :** *message d'erreur système*

Explication : L'initialisation du serveur de configuration a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et réinitialisez le serveur de configuration.

ICA9062 **Erreur fatale du serveur de configuration - accept() principal :** *message d'erreur système*

Explication : La routine principale du serveur de configuration a échoué ; arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et réinitialisez le serveur de configuration.

ICA9063 Erreur du serveur de configuration - *fonction en échec* **: code retour = 0x***code retour fonction*

Explication : Le serveur de configuration a détecté une erreur dans la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et réinitialisez le serveur de configuration.

ICA9064 Option -*valeur* **inconnue ignorée.**

Explication : L'option indiquée a été spécifiée et n'a pas été reconnue.

ICA9065 Erreur du serveur de configuration - *fonction en échec* **:** *message d'erreur système*

Explication : Le serveur de configuration a détecté une erreur dans la fonction indiquée. Arrêt du démon.

Action de l'utilisateur : Corrigez l'incident système signalé et réinitialisez le serveur de configuration.

ICA9066 Mémoire insuffisante : serveur de configuration : malloc(*octets***) a renvoyé la valeur NULL dans la fonction** *nom_fonction***.**

Explication : Impossible d'attribuer une mémoire suffisante ; la fonction malloc a retourné une valeur NULL.

ICA9067 La liaison n'a pas abouti ; l'adresse *port* **est déjà utilisée.**

Explication : L'adresse de port fournie est déjà utilisée.

Réaction du système : Arrêt du serveur de configuration.

Action de l'utilisateur : Connectez-vous au serveur de configuration avec une autre adresse de port ou contactez l'administrateur de pare-feu.

ICA9068 L'option -*valeur* **option n'a pas abouti ou a été spécifiée de manière incorrecte.**

Explication : L'option indiquée n'a pas abouti ou a été spécifiée de manière incorrecte.

Réaction du système : Arrêt du serveur de configuration.

Action de l'utilisateur : Spécifiez l'option comme il convient et réinitialisez le serveur de configuration.

ICA9069 L'initialisation de SSL n'a pas abouti.

Explication : L'algorithme de chiffrement SSL ne s'est pas initialisé ou l'échange de protocoles avec le co-exploitant a échoué.

Réaction du système : Arrêt du serveur de configuration.

Action de l'utilisateur : Demandez à l'administrateur du pare-feu de vérifier l'algorithme SSL.

Annexe B. Durcissement de la configuration du système Windows NT

Le durcissement est un processus visant à optimiser la sécurité et le rendement du système en désactivant les démons inutiles et les ID utilisateur non autorisés. Le durcissement se fait dans le cadre de l'installation du logiciel IBM Firewall et consiste à modifier les fichiers des ressources système susceptibles de menacer la sécurité du système.

Les services non nécessaire à la configuration du pare-feu et pouvant constituer une menace pour la sécurité du système sont désactivés. Tous les protocoles non TCP/IP sont supprimés.

Annexe C. Comment se procurer les spécifications techniques (RFC)

Les spécifications techniques (RFC) sont des documents qui présentent de nouveaux protocoles et établissent des normes pour l'ensemble des protocoles Internet. Vous pouvez vous procurer des exemplaires imprimés de toutes les RFC auprès du centre NIC (Network Information Center), soit de façon ponctuelle soit par abonnement. Voici à qui adresser vos commandes :

Government Systems, Inc.
Attn: Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

Les RFC peuvent être obtenues à l'adresse URL suivante :

http//www.cis.ohio-state.edu/hypertext/information/rfc.html.

Vous pouvez également en obtenir des exemplaires électroniques par télématique, toujours auprès du centre NIC, en vous connectant via FTP à l'adresse `ds.internic.net`. Voici les formats dans lesquels vous pouvez obtenir le transfert des fichiers :

```
RFC:RFCnnnn.TXT
RFC:RFCnnnn.PS
```

Où :

nnnn est le numéro de référence de la RFC désirée

`TXT` est le format de fichier "texte"

`PS` est le format PostScript

Le format de l'index des RFC est le suivant :

```
RFC:RFC-INDEX.TXT
```

Remarque : Beaucoup de RFC ne sont disponibles qu'en format texte. Avant de commander un fichier en PostScript, assurez-vous dans l'index des RFC qu'il existe sous cette forme. Vous pouvez demander également le téléchargement des RFC par messagerie électronique, auprès du serveur de messagerie automatique du centre NIC, en vous adressant à `mailserv@ds.internic.net`. Voici les commandes qui doivent figurer dans votre message :

```
SEND RFCnnnn.TXT
ou
    SEND RFCnnnn.PS
```

Où :

nnnn est le numéro de référence de la RFC désirée

`TXT` est le format de fichier "texte"

`PS` est le format PostScript

Supposons par exemple que vous vouliez un exemplaire en format texte de la RFC 812 ; voici ce que devrait être le contenu de votre message :

```
SEND RFC812.TXT
```

Pour obtenir une copie électronique de l'index des RFC, ajoutez à votre message la commande suivante :

```
SEND RFC-INDEX.TXT
```

Annexe D. Format du fichier de configuration Socks5.conf d'IBM eNetwork Firewall

Le fichier de configuration **socks5.conf** réside dans le répertoire d'installation d'IBM Firewall par défaut. Vous pouvez, si vous le désirez, éditer ce fichier avec un éditeur de texte.

Le fichier de configuration **socks5.conf** est lu au premier appel du serveur. (Pour régénérer sans interrompre, entrez `socks5.config`). Ce fichier contient toutes les données nécessaires à IBM Firewall pour déterminer l'interface à utiliser pour atteindre une adresse donnée, pour s'y connecter directement ou pour utiliser un autre serveur relais. Il indique également les conditions à respecter pour établir une connexion avec un serveur relais.

Le fichier de configuration contient les sections suivantes :

- Alias ;
- Variables ;
- Modules ;
- Authentification ;
- Routage ;
- Serveurs relais ;
- Contrôle d'accès.

Les lignes des sections authentification, routage, serveurs relais et contrôle d'accès sont lues dans l'ordre. Le programme recherche des correspondances pour chaque section, aussi l'ordre des lignes est-il très important. Pour qu'il y ait correspondance, chaque entrée de la ligne doit correspondre à la chaîne recherchée.

Spécification des ports

Les ports peuvent être spécifiés par leur nom, leur numéro ou par une plage. Les plages commencent et finissent soit par un [, soit par un] qu'elles soient inclusives ou exclusives. Les deux noms ou numéros de ports compris entre les délimiteurs de plage doivent être séparés par une virgule. Une spécification de ports est appelée un *modèle de ports*.

Spécification d'hôtes

Les adresses des hôtes et les masques de réseau sont souvent requis pour indiquer quels hôtes sont concernés par une règle. Une spécification d'hôtes est appelée un *modèle d'hôtes*. Le couple hôte/masque peut être spécifié de plusieurs façons :

Paramètre	Description
IP Hôte/masque	L'opérateur logique ET doit produire le même résultat qu'il s'applique au couple adresse d'hôte/masque ou au couple IP hôte/masque. Cet usage vise généralement à masquer la partie de l'adresse se rapportant à l'hôte dans la partie rattachée au réseau ou au sous-réseau.
-	Tout correspond. Tous les systèmes hôtes sont admis.
n1	Equivalent à n1.0.0.0/255.0.0.0.
n1.n2	Equivalent à n1.n2.0.0/255.255.0.0.
n1.n2.n3	Equivalent à n1.n2.n3.0/255.255.255.0.
.domaine.nom	Le nom d'hôte doit finir par la chaîne *.domaine.nom.*
a.hôte.nom	Le nom d'hôte doit correspondre exactement à *a.hôte.nom.*

L'ancienne syntaxe de configuration des hôtes est également prise en charge comme décrit ci-après. Cependant la nouvelle méthode est recommandée et plus lisible.

Paramètre	Description
IP hôte/a	Tout correspond (identique à "-"). Tous les systèmes hôtes sont admis.
IP hôte/n	Le réseau correspond. Les parties de l'adresse rattachées à l'hôte et au sous-réseau sont masquées, ne laissant visible que la partie du réseau. Le masque utilisé dépend de la classe d'adresse IP de système hôte.
IP hôte/s	Le sous-réseau correspond. La partie de l'adresse rattachée à l'hôte est masquée, ne laissant voir que les parties du sous-réseau et du réseau. Le masque utilisé dépend de la classe d'adresse IP de système hôte.
IP hôte/h	L'hôte correspond. Equivalent de IP hôte.

Spécification des méthodes d'authentification

Les méthodes d'authentification fournies sont *ibmcram* et *ibmpwd* mais vous pouvez en ajouter d'autres.

Les méthodes d'authentification peuvent être spécifiées sous la forme d'une liste de méthodes séparées par des virgules. Pour qu'une ligne corresponde, la méthode d'authentification choisie doit également figurer parmi celles de la liste. Cette spécification est appelée un modèle d'authentifications. Par défaut, la méthode d'authentification définie est associée à une valeur NULL. D'autres méthodes

peuvent être ajoutées en chargeant le ou les modules appropriés. A"-" signifie que toute valeur de méthode d'authentification est admise, même la valeur NULL.

Entrées d'authentifications

Les entrées d'authentifications indiquent le ou les types d'authentification pouvant être utilisés. Le format d'une entrée est le suivant :

```
auth/ban   adresse_source  port_source méthodes_authentification
```

Paramètre	Description
auth/ban	Indique si les entrées d'authentification sont admises (auth) ou non (ban).
adresse_source	Modèle d'hôtes valide.
port_source	Modèle de ports valide.
méthodes_authentification	Modèle d'authentifications valide.

Le mot clé "ban" indique que l'authentification ne doit pas même être tentée sur cet hôte pas plus qu'elle ne doit être utilisée en général pour le serveur spécifié.

En l'absence de ligne auth/ban spécifiée, toute méthode d'authentification est admise par défaut. Si la connexion est associée à la valeur par défaut *Interdiction* (Deny), cette connexion ne sera pas rejetée avant la fin de la procédure d'authentification. Dans le protocole SOCKS V5, l'authentification précède l'autorisation. Vous devez décider sur la seule base du système hôte comment il doit authentifier les connexions.

Spécification de commandes

Les commandes peuvent également être spécifiées sous la forme d'une liste de commandes séparées par des virgules. Cette spécification est appelée un modèle de commandes. Les commandes utilisables sont : connect, bind, udp, ping et traceroute. D'autres commandes peuvent être ajoutées par le biais de modules. A "-" (tiret) indique que toutes les commandes sont admises.

Chargement de modules

Les modules permettent une extension personnalisée des fonctions du serveur par l'ajout de nouvelles méthodes d'authentification, de commandes, de contrôles d'autorisation et de filtres de contenu. Le format est le suivant : *module sub nom de fichier options.*

Paramètre	Description
module	Identificateur du module à charger.
raccord	Préfixe dépendant du module, permettant l'accès aux noms des fonctions.
nom de fichier	Nom de fichier du module à charger.
options	Données de configuration spécifiques au module, le cas échéant.

Les modules peuvent définir des zones utilisées ailleurs, il est donc préférable d'insérer les lignes des modules en premier. Par exemple, les modules d'authentification définissent des noms de méthode d'authentification utilisés dans les lignes auth et permit.

Entrées de routage

Sur les machines dotées de plusieurs interfaces réseau (et donc de plusieurs adresses IP), il est souhaitable de s'assurer que certaines interfaces réseau sont bien utilisées en relation avec certaines adresses. On peut éviter les tentatives de perturbation du réseau (il arrive que des utilisateurs de machine externe au réseau tentent de les faire passer pour des machines internes), en s'assurant que les machines internes utilisent l'interface réseau interne et que les machines externes utilisent l'interface réseau externe. Les entrées de routage sont également utilisées par le serveur SOCKS pour déterminer l'interface réseau à associer à une requête BIND acceptée ou à une requête SENDTO émise. Faute d'entrée correspondante, le programme associe INADDR_ANY à toute commande BIND et une connexion pourra être reçue sur n'importe quelle interface. Les hôtes mono-adresse n'ont pas besoin d'entrées de routage ; celles-ci ne sont requises que pour les machines possédant plusieurs interfaces réseau. Le format est le suivant : **route** *adresse_destination port_destination adresse_interface.*

Paramètre	Description
route	Mot clé indiquant les entrées de routage.
adresse_destination	Modèle d'hôtes valide.
port_destination	Modèle de ports valide.
adresse_interface	Adresse IP d'une carte d'interface réseau ou nom de l'interface réseau (par exemple, elnk31).

Entrées de variables

La quantité et le type des messages d'information et de journalisation générés peuvent se contrôler par le biais de certaines variables et indicateurs entrés dans le fichier de configuration. Le format est le suivant : **set** *variable valeur.*

Paramètre	Description
set	Mot clé permettant de limiter les entrées de variables d'environnement à une application locale.
variable	Variable d'environnement valide. Voir «Variables d'environnement», à la page 159 ci-après pour consulter la liste des variables admises.
valeur	Valeur à affecter.

Variables d'environnement

Variable d'environnement	Description
SOCKS5_BINDPORT [port]	Configure IBM Firewall pour utiliser le port indiqué au lieu du port par défaut (port 1080).
SOCKS5_RECVFROMANYONE	Si le support UDP est activé, les clients UDP pourront recevoir des messages provenant de sources inconnues.
SOCKS5_USECLIENTSPORT	Configure IBM Firewall pour uniquement le serveur relais s'il peut se lier au port utilisé par le client pour envoyer ses messages. Ceci est nécessaire pour que les connexions UDP utilisent le serveur relais lorsque le serveur envoie des données en continu au client (envoie des messages au client avant que celui-ci n'en envoie au serveur). Ceci concerne notamment les applications RealAudio .
SOCKS5_MAXCHILD	Nombre maximal d'unités d'exécution.
SOCKS5_NOREVERSEMAP	Désactive le mappage des adresses IP avec les noms d'hôte. Si des alias sont définis dans le fichier de configuration, les performances seront accrues au détriment des données de journalisation.
SOCKS5_NOSERVICENAME	Désactive le mappage des numéros de port aux noms de service. Si des alias sont définis dans le fichier de configuration, les performances seront accrues au détriment des données de journalisation.
SOCKS5_NOIDENT	Désactive les requêtes IDENT même compilées. Cette variable est intéressante dans le cas d'une liaison lente avec des clients n'utilisant pas la fonction IDENTD. Les délais d'expiration seront réduits.
SOCKS5_DEMAND_IDENT	Les authentifications de type NULL n'aboutiront pas si les clients ne fournissent pas d'identifiant. Cette variable permet d'associer de façon certaine un nom utilisateur à une requête de connexion.

Entrées de serveur relais

Les entrées de serveur relais indiquent les adresses des serveurs relais SOCKS. Ces lignes indiquent au serveur comment contacter un système hôte déterminé. Si aucune ligne ne correspond à l'hôte demandé, celui-ci est contacté directement. Le format est le suivant : *type_serveur relais adresse_destination port_destination adresse_serveur relais port_serveur relais.*

Paramètre	Description
type_serveur relais	Type de serveur relais. Les entrées admises sont les suivantes : • socks5 • socks4 • aucun serveur relais
adresse_destination	Modèle d'hôtes valide.
port_destination	Modèle de ports valide.
adresse_serveur relais	Adresse IP ou nom du serveur relais.
port_serveur relais	Port du serveur relais sur lequel le démon SOCKS accepte les connexions.

Entrées de contrôle d'accès

La section rattachée au contrôle d'accès détermine si une requête de connexion sera autorisée ou refusée. Il existe deux types de ligne ; les lignes d'autorisation et les lignes d'interdiction. Chaque entrée de la ligne doit correspondre pour que la ligne corresponde dans son ensemble. Le format d'une entrée est le suivant :

```
permit auth cmd hôte_source hôte_dest port_source port_dest [liste utilisateur]
deny auth cmd hôte_source hôte_dest port_source port_dest [liste_utilisateurs]
```

Paramètre	Description
auth	Liste de méthodes d'authentification spécifiée par un modèle d'authentifications et une entrée d'authentification valides.
cmd	Modèle de commandes valide spécifiant les commandes correspondant à cette ligne.
hôte_source	Modèle d'hôtes valide spécifiant l'hôte source.
hôte_dest	Modèle d'hôtes valide spécifiant l'hôte de destination.
port_source	Modèle de ports valide spécifiant le port de l'hôte source.
port_destination	Modèle de ports valide spécifiant le port de l'hôte de destination.
liste_utilisateurs	Modèle d'utilisateurs valide.

Filtres

Le filtrage par un module chargé est fait au moyen de la directive filter. Le format d'une entrée est le suivant :

```
filter nom auth cmd hôte_source hôte_dest port_source port_dest [liste_utilisateurs]
```

Paramètre	Description
nom	Identificateur du module de filtre.
auth	Liste de méthodes d'authentification spécifiée par un modèle d'authentifications et une entrée d'authentification valides.
cmd	Modèle de commandes valide spécifiant les commandes correspondant à cette ligne.
hôte_source	Modèle d'hôtes valide spécifiant l'hôte source.
hôte_dest	Modèle d'hôtes valide spécifiant l'hôte de destination.
port_source	Modèle de ports valide spécifiant le port de l'hôte source.
port_destination	Modèle de ports valide spécifiant le port de l'hôte de destination.
liste_utilisateurs	Modèle d'utilisateurs valide.

Bibliographie

Pour plus d'informations sur la sécurité dans l'environnement Internet, consultez la page d'accueil d'IBM Firewall à l'adresse suivante : **http://www.software.ibm.com/enetwork/firewall**.

Informations contenues dans les publications IBM

Les autres sources d'informations d'IBM sur les pare-feu, la sécurité sur Internet et la sécurité en général sont répertoriées ci-dessous.

Pare-feu

Les documents suivants sont fournis avec le CD-ROM d'IBM Firewall et sont disponibles sur la page d'accueil d'IBM eNetwork Firewall.

- *Guide de l'utilisateur d'IBM eNetwork Firewall*, GC31-8658
- *Guide de référence d'IBM eNetwork Firewall*, SC31-8659
- *Guarding the Gates Using the IBM eNetwork Firewall for NT 3.2*, SG24-5209

Internet et le Web

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Sécurité générale

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Publications informatiques

Publications consacrées à Sendmail, TCP/IP et UNIX :

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail* O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration* O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook* Prentice Hall. (ISBN: 0-13-151051-7

Publications consacrées aux pare-feu et à la sécurité dans l'environnement Internet :

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)

- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Remarques

La référence faite dans ce manuel aux produits, programmes ou services IBM n'impose pas qu'IBM projette de les distribuer dans tous les pays dans lesquels la compagnie est établie. Toute référence faite à un produit, programme ou IBM ne signifie ni n'implique que seul ce produit, programme ou service d'IBM peut être utilisé. Sous réserve de propriété intellectuelle ou autres droits protégés légalement valides pour IBM, tout produit, programme ou service doté de fonctions équivalentes peut être utilisé à la place du produit, programme ou service IBM. L'évaluation et la vérification de l'utilisation associée à d'autres produits, à l'exception de ceux expressément désignés par IBM, sont la responsabilité de l'utilisateur.

Le contenu décrit dans ce document peut avoir fait l'objet de brevets ou de dépôts de brevets de la part d'IBM. La fourniture de ce document ne concède aucun droit sur ces brevets. Pour toute demande de renseignements concernant les licences, adressez votre courrier à :

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Les détenteurs de ce programme intéressés par (i) un échange d'informations entre des programmes créés indépendamment et autres programmes (y compris celui-ci) et (ii) l'utilisation réciproque des informations qui ont été échangées, doivent contacter :

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Ces informations sont accessibles, conformément aux termes et conditions appropriés et, dans certains cas, moyennant une redevance.

Le programme sous licence décrit dans ce document ainsi que tous les produits associés disponibles sous licence sont fournis par IBM selon les termes du contrat IBM Customer Agreement.

La production de ce document n'étant pas envisagée, il est fourni 'en l'état', sans une quelconque garantie, et IBM décline toute responsabilité, notamment les garanties relatives à la qualité marchande et à l'aptitude à une utilisation particulière.

Ce produit comprend des logiciels développés par l'université de Berkeley en Californie et ses collaborateurs.

Marques

Les termes suivants sont des marques d'International Business Machines Corporation dans certains pays :

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft, Windows, Windows NT, et le logo Windows 95 sont des marques de Microsoft Corporation.

UNIX est une marque dans certains pays, dont seule la société X/Open Company Limited peut concéder la licence.

Java et HotJava sont des marques de Sun Microsystems, Inc.

Glossaire

Vous pouvez accéder au glossaire IBM Software à l'adresse suivante : **http://www.networking.ibm.com/nsg/nsgmain.htm**.

Index

R

S

T

U

REMARQUES DU LECTEUR

Réf. : SC11-1460-01

Titre : IBM eNetwork Firewall pour Windows NT

Guide de référence

Vos commentaires nous permettent d'améliorer la qualité de nos documents : ils jouent un rôle important lors de leur mise à jour.

Si vous avez des observations sur le(s) document(s) ci-joint(s), nous vous serions reconnaissants de nous en faire part en les faisant précéder, au besoin, des rubriques ou des numéros de pages et de lignes concernés. Elles seront étudiées avec le plus grand soin par les responsables du Centre de francisation.

Par ailleurs, nous vous rappelons que pour toute question technique ou pour toute demande de document, vous devez vous adresser à votre partenaire commercial IBM.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie de ces informations que, de votre côté, vous pourrez évidemment continuer à exploiter.

Envoyez vos remarques à :

Pour la France	Pour le Canada
IBM FRANCE	**IBM CANADA Ltée**
Centre de francisation	**Services linguistiques**
4, avenue Montaigne	**1250, boul. René-Levesque ouest**
93881 Noisy-le-Grand Cedex	**Montréal (Québec) H3B 4W2**

Si vous désirez une réponse, n'oubliez pas de mentionner vos nom et adresse.

Merci de votre collaboration.

MODIFICATIONS OU ÉCLAIRCISSEMENTS DEMANDÉS :

Page ou rubrique *Commentaires*

Compagnie IBM France
Tour Septentrion
20, avenue André Prothin
La Défense 4
92400 Courbevoie

Document réalisé et composé par le Centre de francisation

à Noisy-le-Grand

Juin 1998

Imprimé au Danemark par IBM Danmark A/S.

SC11-1460-01