

Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

20 novembre 9:45 - 10:45

Jean-Sébastien GUINAUDEAU

HELIAQ SOLUTIONS

jean-sebastien.guinaudeau@heliahq.fr

IBM

common
FRANCE

Power Week

18 -19 - 20 novembre
2025



S107 - TCP/IP est-il trop
ouvert sur votre IBM i ?

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

- Nous parlerons « réseau », et des manières/outils permettant de déterminer depuis l'IBM i les périphériques qui communiquent avec ce dernier.
- Nous regarderons dans le détail les informations que permettent d'obtenir les outils natifs du système, comme le NETSTAT, le TRCCNN, la mise en place de filtre sur les interfaces Ethernet, et comment aller chercher dans les informations collectées : analyse PCAP, requêtes SQL dans le QHST, dans le Journal d'Audit, etc.

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

- Déterminer précisément le périmètre réseau d'une partition IBM i est souvent une étape sous-estimée lors d'une opération de « Move to Cloud », mais pourtant primordiale pour assurer la viabilité d'un tel projet.
- Mais cette phase peut également être utilisée dans le cas d'un audit périmétrique, d'un projet de sécurisation de sa partition, etc.

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Pour se donner une idée de la configuration réseau IP en place, il est possible de lister les interfaces déclarées sur le système via la commande native NETSTAT, avec le paramètre *IFC.

On pourra compléter ces informations avec le paramètre *RTE pour connaître les routes définies.

NETSTAT *IFC (ou CFGTCP, option 1)

```
Work with TCP/IP Interface Status

Type options, press Enter.
  5=Display details   8=Display associated routes   9=Start   10=End
 12=Work with configuration status  14=Display multicast groups

Système:  JADEFTR

Opt  Internet      Network      Line      Interface
     Address      Address      Description  Status
---  -
_    1.1.1.2       1.1.1.0      ETHADMIN    Active
_    10.11.164.130 10.11.164.0  ETHLINE     Active
_    10.111.164.130 10.110.0.0   ETHADMIN    Active
_    127.0.0.1      127.0.0.0   *LOOPBACK   Active

Fin
```

NETSTAT *RTE (ou CFGTCP, option 2)

Display TCP/IP Route Information

Systeme: JADEFTR

Type options, press Enter.
5=Display details

Opt	Route Destination	Subnet Mask	Next Hop	Route Available
—	1.1.1.0	255.255.255.0	*DIRECT	*YES
—	10.110.0.0	255.254.0.0	*DIRECT	*YES
—	10.11.164.0	255.255.255.0	*DIRECT	*YES
—	10.40.0.0	255.255.0.0	10.111.255.254	*YES
—	127.0.0.0	255.0.0.0	*DIRECT	*YES
—	224.0.0.0	240.0.0.0	*DIRECT	*YES
—	224.0.0.0	240.0.0.0	*DIRECT	*YES
—	224.0.0.0	240.0.0.0	*DIRECT	*YES
—	224.0.0.0	240.0.0.0	*DIRECT	*YES
—	*DFTRROUTE	*NONE	10.11.164.254	*YES

Fin

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

On peut commencer par regarder les ports ouverts sur le système via la commande NETSTAT (utiliser le paramètre *CNN).

La commande WRKSRVTBLE donnera les noms des services associés aux numéros de ports.

NETSTAT *CNN

En début de liste, les * indiquent les services démarrés et en attentes de connexion.

Work with IPv4 Connection Status

Systeme: JADEFTR

Type options, press Enter.
3=Enable debug 4=End 5=Display details 6=Disable debug
8=Display jobs

Opt	Remote Address	Remote Port	Local Port	Idle Time	State
—	*	*	ftp-con >	364:30:35	Listen
—	*	*	ssh	364:28:49	Listen
—	*	*	telnet	000:06:53	Listen
—	*	*	smtp	364:29:00	Listen
—	*	*	pop3	364:29:18	Listen
—	*	*	ntp	000:29:04	*UDP
—	*	*	netbios >	364:29:26	Listen
—	*	*	netbios >	000:00:59	*UDP
—	*	*	netbios >	000:01:13	*UDP
—	*	*	netbios >	364:29:21	Listen
—	*	*	427	364:29:18	*UDP
—	*	*	cifs	364:29:21	Listen

A suivre...

NETSTAT *CNN

En fin de liste, les adresses IP et numéros de ports indiquent les services pour lesquelles des connexions sont actives.

```
Work with IPv4 Connection Status

Type options, press Enter.
  3=Enable debug  4=End  5=Display details  6=Disable debug
  8=Display jobs

Opt  Remote Address      Remote Port    Local Port    Idle Time    State
--  -
  1  *                  *              hprip-h >    364:33:58    *UDP
  2  *                  *              hprip-med    364:33:58    *UDP
  3  *                  *              hprip-low    364:33:58    *UDP
  4  *                  *              427          364:32:49    Listen
  5  *                  *              427          000:46:54    *UDP
  6  *                  *              as-admi >    364:32:30    Listen
  7  *                  *              as-admi >    364:32:04    Listen
  8  *                  *              as-admi >    364:32:40    Listen
  9  *                  *              as-admi >    364:32:42    Listen
 10  *                  *              as-admi >    364:32:38    Listen
 11  *                  *              4800         364:32:49    Listen
 12  10.40.50.33        63846         telnet        000:00:00    Established

A suivre...
```

WRKSRVTBLE (ou CFGTCP, option 21, puis option 1)

La table des services fait la relation entre un nom de service, un numéro de port et un type de protocole. Les fameux « well-known ports »...

```
Work with Service Table Entries                                     Système:  JADEFTR

Type options, press Enter.
  1=Add    4=Remove    5=Display

Opt  Service                                     Port  Protocol
---  -
  1  snmp                                     161   udp
  2  snmp-mgr                               10163  tcp
  3  snmp-mgr                               10163  udp
  4  snmp-trap                              162   tcp
  5  snmp-trap                              162   udp
  6  sqlserv                                118   tcp
  7  sqlserv                                118   udp
  8  src                                    200   tcp
  9  src                                    200   udp
 10  ssh                                    22    tcp
 11  ssh                                    22    udp

Parameters for options 1 and 4 or command
===>
```

A suivre...

NETSTAT *CNN – Via les « SQL Services »

IBM i Services (SQL)

```
SELECT DISTINCT REMOTE_ADDRESS, REMOTE_PORT, REMOTE_PORT_NAME, LOCAL_PORT, LOCAL_PORT_NAME, CONNECTION_TYPE  
FROM QSYS2.NETSTAT_JOB_INFO  
WHERE REMOTE_ADDRESS = '0.0.0.0'  
ORDER BY LOCAL_PORT;
```

REMOTE_ADDRESS	REMOTE_PORT	REMOTE_PORT_NAME	LOCAL_PORT	LOCAL_PORT_NAME	CONNECTION_TYPE
0.0.0.0	0	-	21	ftp-control	IPV4
0.0.0.0	0	-	22	ssh	IPV4
0.0.0.0	0	-	23	telnet	IPV4
0.0.0.0	0	-	25	smtp	IPV4
0.0.0.0	0	-	110	pop3	IPV4
0.0.0.0	0	-	137	netbios-ns	IPV4
0.0.0.0	0	-	139	netbios-ssn	IPV4
0.0.0.0	0	-	427	-	IPV4

```
SELECT DISTINCT REMOTE_ADDRESS, REMOTE_PORT, REMOTE_PORT_NAME, LOCAL_PORT, LOCAL_PORT_NAME, CONNECTION_TYPE  
FROM QSYS2.NETSTAT_JOB_INFO  
WHERE REMOTE_PORT <> '0'  
ORDER BY LOCAL_PORT;
```

REMOTE_ADDRESS	REMOTE_PORT	REMOTE_PORT_NAME	LOCAL_PORT	LOCAL_PORT_NAME	CONNECTION_TYPE
10.40.50.33	54 662	-	23	telnet	IPV4
10.40.50.33	54 614	-	8 471	as-database	IPV4
127.0.0.1	36 367	-	8 473	as-file	IPV4
10.40.50.33	54 615	-	8 475	as-rmtcmd	IPV4
127.0.0.1	28 423	-	8 475	as-rmtcmd	IPV4
127.0.0.1	8 475	as-rmtcmd	28 423	-	IPV4
127.0.0.1	8 473	as-file	36 367	-	IPV4

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Il y a la possibilité d'utiliser un outil natif appelé TRCCNN (disponible à partir de la 7.2), permettant l'enregistrement des flux IP traités par le système.

Les traces sont enregistrées localement, et il est ensuite possible de les exporter au format PCAP.

TRCCNN

Liens vers les documentations officielles :

How To Use TRCCNN : <https://www.ibm.com/support/pages/how-use-trccnn>

Trace Connection (TRCCNN) : https://www.ibm.com/docs/en/i/7.3.0?topic=ssw_ibm_i_73/cl/trccnn.htm

TRCCNN – Lancement d'une trace

TRCCNN SET(*ON) TRCTYPE(*IP) TRCFULL(*STOPTRC) TRCTBL(*GEN)

Trace Connection (TRCCNN)

Indiquez vos choix, puis appuyez sur ENTREE.

Option de trace	> <u>*ON</u>	*ON, *OFF, *END, *FORMAT
Type de trace	> <u>*IP</u>	*IP, *SSL, *IPV4, *IPV6
Trace pleine	> <u>*STOPTRC</u>	*WRAP, *STOPTRC
Trace table name	> <u>*GEN</u>	
Taille:		
Nombre d'unités	<u>16000</u>	1-998000, 16000
Unit of measure	<u>*KB</u>	*KB, *MB

Action à réaliser lorsque le fichier de trace est complet

A suivre...

TRCCNN – Gestion des traces

WRKTRC *LIC

```
Work with Traces                                     Système:  JADEFTR

Type options, press Enter.
  2=End   3=Hold   4=Delete   6=Print   7=Save   8=Change Table Size

Opt      Trace/Identifier      Status      Library
--      -
--      TRCCNN Trace
--      QTRCCNN673945          ACT-ENB

                                Status - Help
                                _ACT
                                The trace table is actively being
                                written to. Trace data cannot be
                                displayed or dumped while the trace
                                table is active.

Parameters or command      Fin
===>
```


TRCCNN – Arrêt d'une trace avec génération PCAP

TRCCNN SET(*OFF) OUTPUT(*STMF) TOSTMF('/home/cisjsg/trc01')

```
Trace Connection (TRCCNN)

Indiquez vos choix, puis appuyez sur ENTREE.

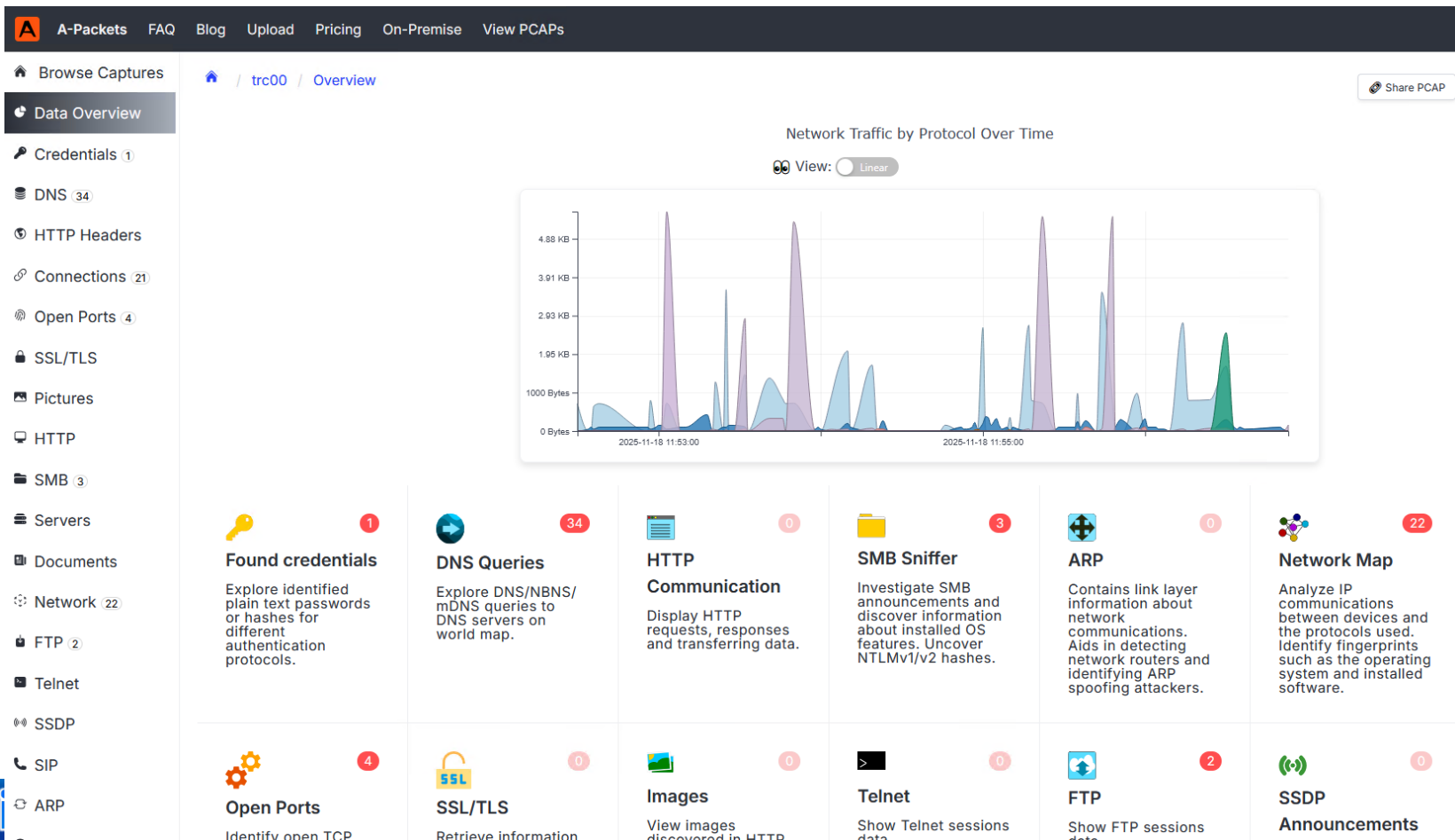
Option de trace . . . . . > *OFF          *ON, *OFF, *END, *FORMAT
Trace table name . . . . . > *GEN
Sortie . . . . . > *STMF          *PRINT, *STMF
Stream file options:
  Stream file . . . . . > '/home/cisjsg/trc01'
Remplacer fichier . . . . . > *NO          *NO, *YES
```



Avec le paramètre *STMF, le fichier 'trc01' sera lisible au format PCAP

Fin

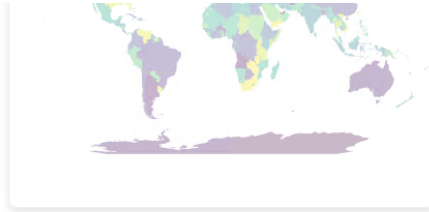
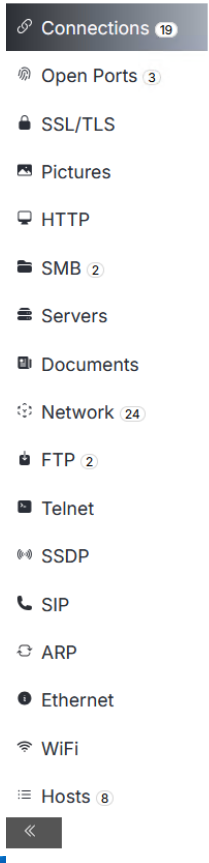
TRCCNN – Analyse du fichier PCAP généré



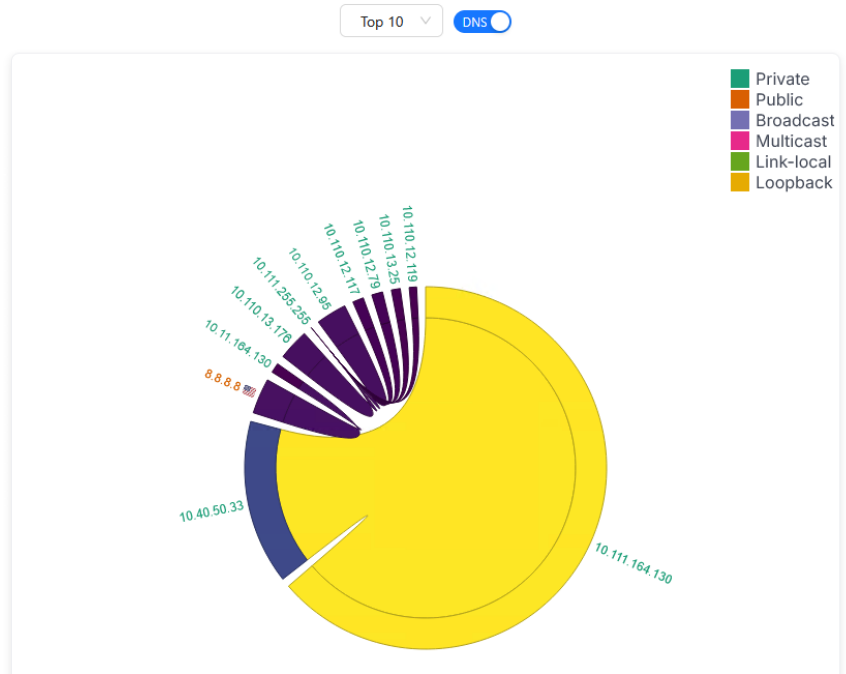
TRCCNN – Analyse du fichier PCAP généré



TRCCNN – Analyse du fichier PCAP généré



Network Traffic Distribution Among Endpoints



TRCCNN – Analyse du fichier PCAP généré

Connections 19

Open Ports 3

SSL/TLS

Pictures

HTTP

SMB 2

Servers

Documents

Network 24

FTP 2

Telnet

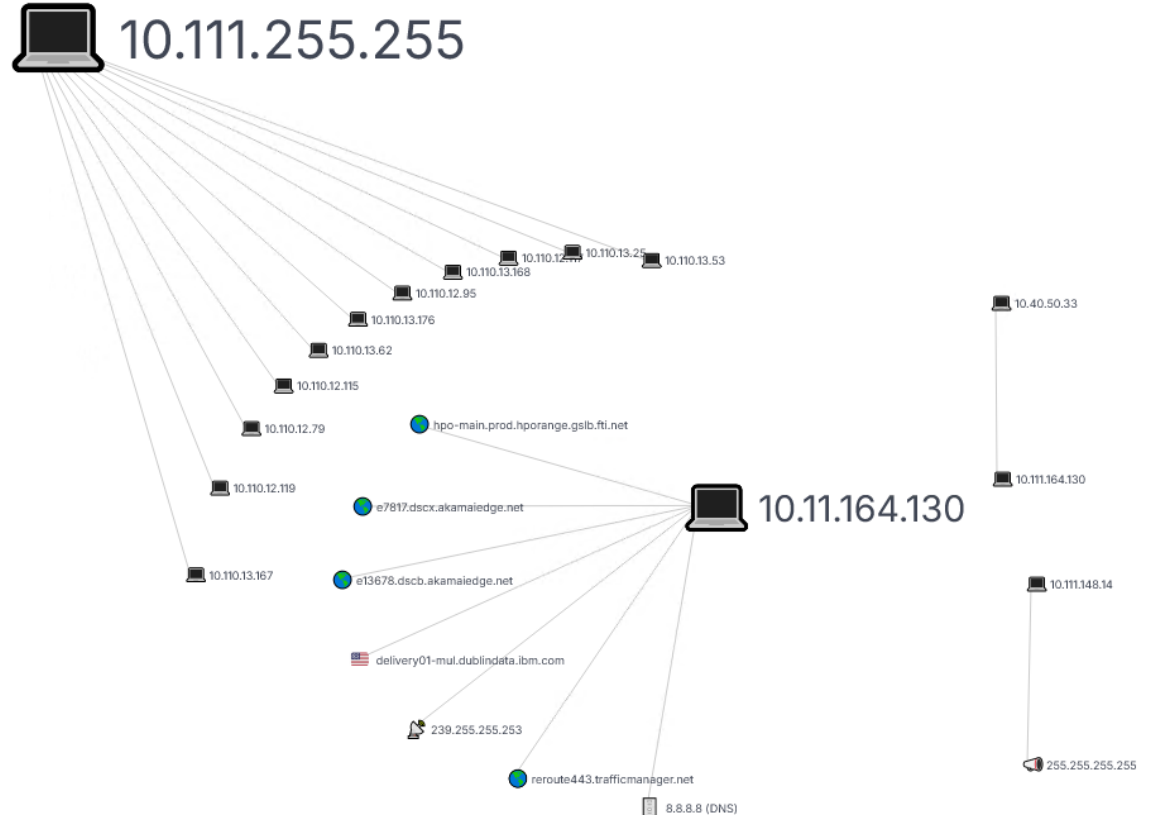
SSDP

SIP

ARP

Ethernet

WiFi



TRCCNN – Analyse du fichier PCAP généré

🔑 Credentials ①

🌐 DNS 25

🌐 HTTP Headers

🔗 Connections 19

🔑 Open Ports 3

🔒 SSL/TLS

🖼️ Pictures

🌐 HTTP

📁 SMB 2

🖨️ Servers

📄 Documents

🌐 Network 24

🔑 FTP 2

🌐 Telnet

🌐 SSDP

▼ 10.40.50.33 → 10.111.164.130

```
220-QTCP at JADEFTR.JADEFTR.INTRA.  
220 Connection will close if idle more than 5 minutes.  
OPTS UTF8 ON  
501 OPTS unsuccessful; specified subcommand not recognized.  
USER jeanseb  
331 Enter password.  
PASS pWeek25  
230 JEANSEB logged on.  
CWD /home/cisjsg  
250-NAMEFMT set to 1.  
250 "/home/cisjsg" is current directory.  
PORT 10,40,50,33,196,17  
200 PORT subcommand request successful.  
NLST  
125 List started.  
250 List completed.  
QUIT  
221 QUIT subcommand received.
```

▼ 10.11.164.130 → 🇺🇸 delivery01-mul.dubindata.ibm.com (170.225.119.157)

```
220 ProFTPD Server (proftpd) [170.225.119.157]  
USER D50C77  
550 SSL/TLS required on the control channel  
QUIT  
221 Goodbye.
```

TRCCNN – Options de filtrage

```
TRCCNN SET(*ON) TRCTYPE(*IP) TRCTBL(*GEN) SIZE(64000) TCPDTA(*TCP (21) ()  
'10.111.164.130') WCHMSG((CPF1124)) WCHMSGQ((*HSTLOG))
```

Trace Connection (TRCCNN)

Indiquez vos choix, puis appuyez sur ENTREE.

TCP/IP data:

Protocol	> <u>*TCP</u>	*TCP, *UDP, *ICMP, *IGMP...
Local port	> <u>21</u>	1-65535
Remote port	<u> </u>	1-65535
Local IP address	> <u>'10.111.164.130'</u>	
Remote IP address	<u> </u>	
Description de ligne	<u> </u>	Nom

TRCCNN – Options d'arrêt

```
TRCCNN SET(*ON) TRCTYPE(*IP) TRCTBL(*GEN) SIZE(64000) TCPDTA(*TCP (21) ()  
'10.111.164.130') WCHMSG((CPF1124)) WCHMSGQ((*HSTLOG))
```

```
Trace Connection (TRCCNN)

Indiquez vos choix, puis appuyez sur ENTREE.

Watch for message:
  Message to watch . . . . . > CPF1124      Nom, générique*, *NONE...
  Donnée de comparaison . . . . . *NONE

Compare against . . . . . *MSGDTA      *MSGDTA, *FROMPGM, *TOPGM
Type de message . . . . . *ALL         *ALL, *COMP, *DIAG...
Opérateur relationnel . . . . . *GE      *GE, *EQ, *GT, *LT, *LE
Code gravité . . . . . 00             0-99
      + si autres valeurs _

Watched message queue:
  File attente messages . . . . . > *HSTLOG    Nom, *SYSOPR, *JOBLOG, *HSTLOG
  Biblio . . . . . _____ Nom, *LIBL
      + si autres valeurs _
```


TRCCNN – Les ‘watches’ (ou triggers de l’IBM i)

WRKWCH *ALL

Work with Watches

Systeme: JADEFTR

Type options, press Enter.
1=Start 2=End 5=Display

Opt	Type/Session	Origin	User	Status
<u>5</u>	Trace QSCCNN0001	TRCCNN	CISJSG	ACTIVE

Display Watch

Systeme: JADEFTR

Session ID : QSCCNN0001 Started: Date : 18/11/25
Started by: Time : 16:51:15
Travail : QPADEV0005 Length of time to
Utilisat : CISJSG watch : *NOMAX
Numéro : 674039 Intervalle : 0
Watch program : *NONE
Biblio :
Origin : TRCCNN
Run priority : 25

Type de message	File Name	attente messages Library	Job Name	Utilisat	Numéro
CPF1124 *ALL	QHST	QSYS			

TRCCNN – Les ‘watches’ (ou triggers de l’IBM i)

DSPLOG

Historique du système

```
Travail 674037/CISJSG/QPADEV0005 arrêté le 18/11/25 à 16:39:44; temps UC 0,03  
Travail 674039/CISJSG/QPADEV0005 démarré le 18/11/25 à 16:39:49 dans le sous-  
Travail 674040/QUSER/QSCWCHPS démarré le 18/11/25 à 16:39:49 dans le sous-sys  
Travail 674041/QUSER/QSCWCHPS démarré le 18/11/25 à 16:39:49 dans le sous-sys  
Watch session QSCNN0002 ended. Reason code: X'02'  
Travail 669543/QUSER/QSCWCHPS arrêté le 18/11/25 à 16:39:52; temps UC 0,010;  
Watch session QSCNN0001 ended. Reason code: X'02'  
Travail 674041/QUSER/QSCWCHPS arrêté le 18/11/25 à 16:39:52; temps UC 0,004;  
Travail 674036/QUSER/QSCWCHMS arrêté le 18/11/25 à 16:39:52; temps UC 0,005;
```

TRCCNN – Les ‘watches’ (ou triggers de l’IBM i)

DSPLOG + F1

```
Complément d'informations sur message

ID message . . . . . : CPI3999
Date d'envoi . . . . . : 18/11/25      Heure d'envoi . . . . . : 16:39:52

Message . . . . . : Watch session QSCCNN0001 ended. Reason code: X'02'

Cause . . . . . : Watch session QSCCNN0001 issued by
674034/CISJSG/QPADEV0005 at 18/11/25 16:29:00 and associated with TRCCNN has
been ended. Reason code: X'02'. The possible reason codes follow:
  00 - Length of time to watch has expired
  01 - Error starting trace function
  02 - Watch for event criteria met because of message id CPI3999 found in
      QSYS/QHST
  03 - Watch for event criteria met because of LIC log *N
```

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Une autre manière d'identifier les flux, c'est d'activer le pare-feu du système (disponible à partir de la 7.1) et de mettre en place des règles qui laissent tout passer mais enregistrent les flux dans un journal local DB2, ensuite requêtable en SQL.

PACKET RULES

Exemple de filtre permettant de tracer tous les flux entrant sur le système :

```
FILTER SET LogConnections ACTION = PERMIT DIRECTION = INBOUND  
SRCADDR = * DSTADDR = * PROTOCOL = TCP/STARTING DSTPORT = *  
SRCPORT = * JRN = FULL
```

```
FILTER SET LogConnections ACTION = PERMIT DIRECTION = * SRCADDR =  
* DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * JRN = OFF
```

```
FILTER_INTERFACE LINE = ETHADMIN SET = LogConnections
```

La seconde règle où "DIRECTION = *" est très importante car elle permet de dire qu'il faut laisser passer tout le reste du trafic entrant mais également tous les paquets sortant en retour !!!

PACKET RULES – Définition et mise en place de filtres

The image shows two screenshots from the IBM Navigator for i interface, connected by a large red arrow pointing from left to right.

Left Screenshot: The 'Network' section is expanded in the left-hand menu. Under 'IP Policies', the 'Packet Rules' option is highlighted with a red box. A tooltip next to it says 'Manage a list of IP policies'. Another tooltip below it says 'View and manage packet rules'. The background shows a graph of 'CPU Utilization (Average)' ranging from 10 to 70.

Right Screenshot: The 'Packet Rules' window is open. The 'Actions' menu is displayed, with a red box around the 'Rules Editor' option. A red arrow points from the 'Rules Editor' option in the menu to the 'Packet Rules' option in the left-hand menu of the left screenshot.

PACKET RULES – Définition et mise en place de filtres

Rules Editor ✕

 File ▼  Insert ▼

File Title:
untitled

Packet Rules Statements Editor:

```
FILTER SET LogConnections ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = * PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = *  
JRN = FULL  
  
FILTER SET LogConnections ACTION = PERMIT DIRECTION = * SRCADDR = * DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * JRN = OFF  
  
FILTER_INTERFACE LINE = ETHADMIN SET = LogConnections
```

✓ Save As

✕ Cancel

PACKET RULES – Définition et mise en place de filtres

Save File

Save In:

Browse

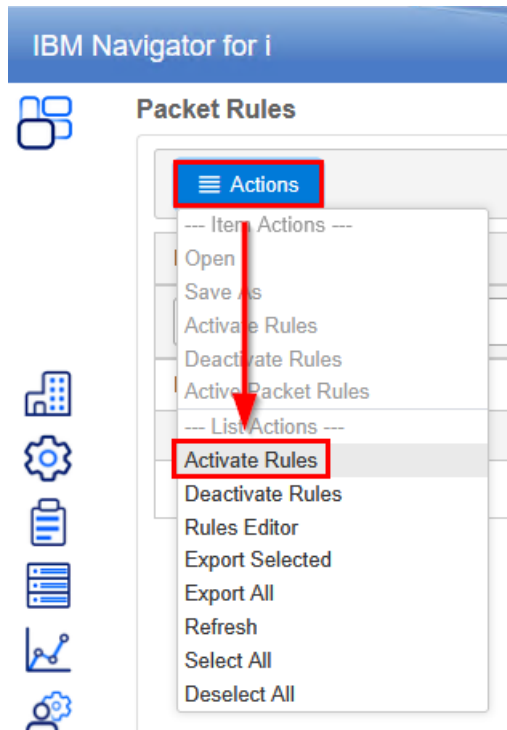
File Name:

File Extension:

✓ OK

✗ Cancel

PACKET RULES – Définition et mise en place de filtres



Activate Packet Rules

Packet rules files

☐ Activate only the VPN generated rules

☒ Activate only the selected files

☐ Activate both the VPN generated rules and selected files

File Name:

Interface

☒ Activate these rules on the following interface

Interface:

☐ Activate these rules on the following point-to-point filter identifier

Filter identifier:

☐ Activate these rules on all interfaces and all point-to-point filter identifier

PACKET RULES – Définition et mise en place de filtres

IBM Navigator for i

 **Packet Rules**

 Actions

Name	Description
Filter	Filter
ETHADMIN	Packet rules loaded for ETHADMIN

<< < 1 > >> 100 ▾

Total Rows: 1

PACKET RULES – Contrôle des règles en place

Active Packet Rules

Filters

Address Translation

Inbound:

Properties

Action	Source	Destination	Source Port	Destination Port	Protocol	Origin	Journaling	Fragments
Permit	*	*	*	*	TCP/STARTING	Manual	Full	*
Permit	*	*	*	*	*	Manual	Off	*
Deny	*	*	*	*	*	Automatic	Off	*

Total Rows: 3

Outbound:

Properties

Security Associations

Action	Source	Destination	Source Port	Destination Port	Protocol	Connection Name	Origin	Journaling	Fragments
Permit	*	*	*	*	*		Manual	Off	*
Deny	*	*	*	*	*		Automatic	Off	*

Total Rows: 2

PACKET RULES – Commandes associées

- **La commande RMVTCPTBL peut être utilisée pour désactiver tous les filtres de règles sur le système => très pratique pour se débloquer si on s'est trompé dans les règles et qu'on s'est coupé l'accès à la machine !**
- Un filtre de règles peut être activé ou désactivé par programme via la commande LODIPFTR.
- Les entrées du journal des filtres de règles peuvent être affichées avec la commande DSPJRN JRN(QIPFILTER).

PACKET RULES – Consulter les paquets capturés

DSPJRN JRN(QIPFILTER)

Postes de journal

Journal : QIPFILTER

Bibliothèque : QUSRSYS

N° séquence le plus élevé à l'écran : 00000000000000000012

Indiquez vos options, puis appuyez sur ENTREE.

5=Poste entier

Opt	Séquence	Code	Type	Objet	Bibliothèque	Travail	Heure
—	1	J	PR			QTOFJRN	12:36:52
—	2	M	TF			QTOFJRN	12:54:22
—	3	M	TF			QTOFJRN	12:55:32
<u>5</u>	4	M	TF			QTOFJRN	12:55:47
—	5	M	TF			QTOFJRN	12:55:47
—	6	M	TF			QTOFJRN	12:55:48
—	7	M	TF			QTOFJRN	12:55:48
—	8	M	TF			QTOFJRN	12:55:50
—	9	M	TF			QTOFJRN	12:55:50
—	10	M	TF			QTOFJRN	12:55:54

PACKET RULES – Consulter les paquets capturés

DSPJRN JRN(QIPFILTER)

```

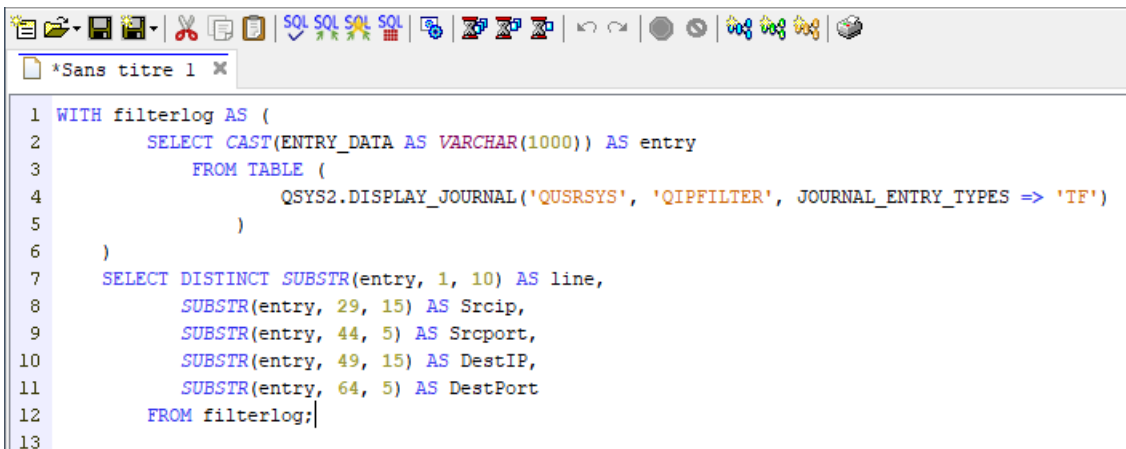
                                Poste de journal
Objet . . . . . :                               Bibliothèque . . . . . :
Membre . . . . . :                               Donn poste réduites :   *NONE
Données incomplètes :   Non
Séquence . . . . . :   4
Code . . . . . :   M - Données de gestion de réseau
Type . . . . . :   TF - Actions relatives aux règles de filtre IP

                                Données spécifiques du poste
Colonne      *...+....1....+....2....+....3....+....4....+....5
00001        'ETHADMIN  A I      2PERMIT   610.40.50.33   4992210'
00051        ' .111.164.130  2002
00101        '              410.40.50.33
00151        '              410.111.164.130
00201        '
00251        '

                                Fin
```

PACKET RULES – Consulter les paquets capturés

SQL



```
1 WITH filterlog AS (  
2     SELECT CAST(ENTRY_DATA AS VARCHAR(1000)) AS entry  
3     FROM TABLE (  
4         QSYS2.DISPLAY_JOURNAL('QUSRSYS', 'QIPFILTER', JOURNAL_ENTRY_TYPES => 'TF')  
5     )  
6 )  
7 SELECT DISTINCT SUBSTR(entry, 1, 10) AS line,  
8     SUBSTR(entry, 29, 15) AS Srcip,  
9     SUBSTR(entry, 44, 5) AS Srcport,  
10    SUBSTR(entry, 49, 15) AS DestIP,  
11    SUBSTR(entry, 64, 5) AS DestPort  
12 FROM filterlog;  
13
```

LINE	SRCIP	SRCPORT	DESTIP	DESTPORT
*ALL				
ETHADMIN				
ETHADMIN	10.40.50.33	49922	10.111.164.130	2002
ETHADMIN	10.40.50.33	49923	10.111.164.130	2002
ETHADMIN	10.40.50.33	49925	10.111.164.130	23
ETHADMIN	10.40.50.33	49935	10.111.164.130	23
ETHADMIN	10.40.50.33	49943	10.111.164.130	23
ETHADMIN	10.40.50.33	49946	10.111.164.130	23
ETHADMIN	10.40.50.33	49980	10.111.164.130	23
ETHADMIN	10.40.50.33	49992	10.111.164.130	23
ETHADMIN	10.40.50.33	50003	10.111.164.130	23
ETHADMIN	10.40.50.33	50013	10.111.164.130	23
ETHADMIN	10.40.50.33	50093	10.111.164.130	23
ETHADMIN	10.40.50.33	55317	10.111.164.130	2002
ETHADMIN	10.40.50.33	55321	10.111.164.130	2002
ETHADMIN	10.40.50.33	55322	10.111.164.130	2002
ETHADMIN	10.40.50.33	55323	10.111.164.130	2002
ETHADMIN	10.40.50.33	55324	10.111.164.130	2002
ETHADMIN	10.40.50.33	55325	10.111.164.130	21
ETHADMIN	10.40.50.33	55350	10.111.164.130	8476
ETHADMIN	10.40.50.33	55351	10.111.164.130	8475
ETHADMIN	10.40.50.33	55352	10.111.164.130	8476
ETHADMIN	10.40.50.33	55353	10.111.164.130	8471
ETHADMIN	10.40.50.33	55354	10.111.164.130	8475
ETHADMIN	10.40.50.33	55683	10.111.164.130	2002

AUTRES SOURCES – QHST (HISTORY LOG)

Accessible via SQL depuis la 7.1 au travers de la table HISTORY_LOG_INFO.

Compatible avec les formats SYSLOG RFC3164 et RFC5424.

History of connections to IBM i

```
create table qtemp.qhst as
(select * from table(qsys2.history_log_info(current timestamp -1 day)) x) with data;

select count(*) as "Count",
substring(trim(message_tokens), 65) as "IP Address",
substring(from_job, locate('/', substring(from_job, 8))+8) as "Job",
from_user as "Current User"
from qtemp.qhst where message_id = 'CPIAD09'
group by substring(trim(message_tokens), 65), substring(from_job,
locate('/', substring(from_job, 8))+8), from_user
order by 1 desc;
```



Count	IP Address	Job	Current User
7	127.0.0.1	QZDASOINIT	CISJSG
5	10.40.50.33	QZRCRSVS	CISJSG
4	127.0.0.1	QZRCRSVS	CISJSG
4	127.0.0.1	QPWFSEVS	CISJSG
2	10.40.50.33	QZDASOINIT	CISJSG

AUTRES SOURCES – AUDIT JOURNAL

Pour auditer toutes les connexions TCP et UDP entrantes et sortantes du système, indiquez *NETSCK, *NETUDP et *NETTELSVR.

Les enregistrements d'audit SK-A/SK-C (en TCP) et SK-I/SK-O (en UDP) contiennent les informations suivantes :

- ✓ Famille d'adresses (IPv4 ou IPv6)
- ✓ Adresse IP locale
- ✓ Port local
- ✓ Adresse IP éloignée
- ✓ Port éloigné

[Extension de niveau d'audit \(QAUDLVL2\) - Documentation IBM](#)

AUTRES SOURCES – IDS, EXIT PGM, ...

Principalement orienté sur la tâche de détection d'intrusion, la fonctionnalité **IDS** peut aussi permettre d'identifier des connexions entrantes ou sortantes en fonction des politiques mises en place.

[Concepts de détection d'intrusion - Documentation IBM](#)

L'implémentation de **programmes d'exit** est aussi une piste pour tracer les connexions.

[Utilisation des programmes d'exit - Documentation IBM](#)

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Q&A ?

MERC