Projet profesionnel : Aborder une problématique de Performances dégradées liée au réseau

---

Pré-analyse

Avant toute chose, il est important de bien délimiter ce qui est impacté via les questions suivantes :

- **QUI** : Toute l'étude / certains collaborateurs (étage / bureau) / annexe / personnes en télétravail
- **QUOI** : recherches internet ou sites métiers / modules inot / signatures AAE / etc…
- **QUAND** : période / jours / heures / depuis combien de temps

Cela vous permettra d'effectuer un premier trie dans les vérifications à effectuer en priorité.

Par exemple, une lenteur systématique tous les vendredis à partir de 17h peut signifier qu'une sauvegarde externalisée s'effectue à ce moment, saturant la bande passante de l'étude.

Si l'étude est en cloud, il vous est possible de télécharger leur inot sur votre poste pour effectuer des tests hors LAN / WAN de l'étude.
Attention cependant, nous avons sur le site de Septeo des routes spécifiques vers notre datacenter où sont hébergés nos serveurs cloud. Cela peut donc, dans de très rares cas, fausser le test.
Deux lignes ADNOV sont aussi à dispositions dans nos locaux pour effectuer des tests tout en étant sur le réseau privé du notariat :

- Côté pôle N2
- À côté du bureau responsable plateau.

Il est aussi fortement conseillé de passer un référentiel pour vérifier si des lenteurs sont vraiment présentes, ou si celles-ci sont des ressentis uniquement. Celui-ci est à passer sur

unposte client (ET sur votre poste si cloud)

Analyse WAN

Le WAN (Wide Area Network) est la partie réseau externe de l'étude, internet classique et privé du notariat.

Nous avons à notre disposition deux tests de débit à lancer sur un poste client ou serveur :

Test connexion internet : https://bp-internet.genapicloud.com/

Test connexion privée du notariat : https://bp-real.genapicloud.com/

Ne pas effectuer ces tests sur Firefox ! Certains navigateurs peuvent fausser les résultats. Il est conseillé d'utiliser de préférence Edge ou Chrome.

Il est aussi possible d'effectuer ces tests réseau en branchant un ordinateur directement à l'arrière du routeur FAI métier.
En cas de besoin, ne pas hésiter à contacter le FAI :

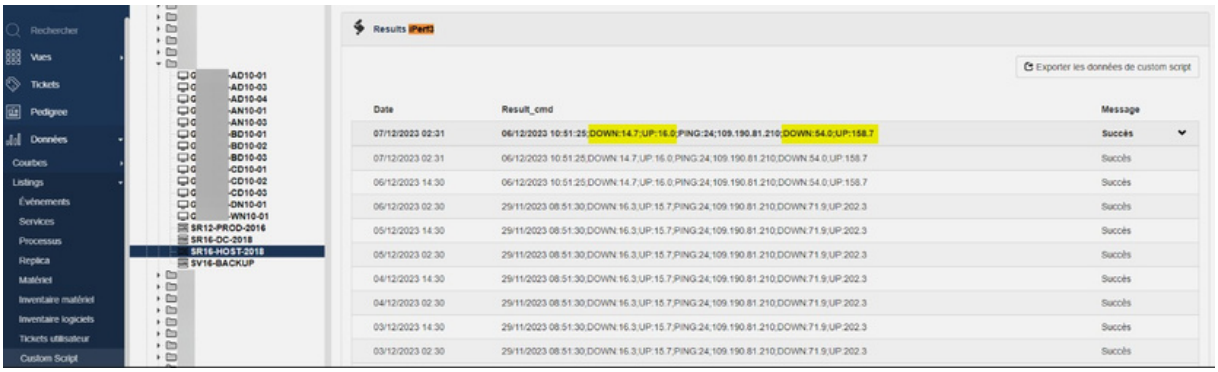
ADNOV :

- Utilisent des routeurs OneAccess.
- Il est possible de se brancher sur le port 0/2 du routeur, qui est un port de test. Attention cependant, il n'est pas rare que ce port soit désactivé par défaut. Dans ce cas, il faut soit demander à ADNOV de l'activer temporairement le temps du test, soit faire le test hors production sur le port 0/0 (port relié au switch de l'étude).
- ADNOV n'apprécient pas l'utilisation de nos outils de test réseau. Il est possible qu'ils demandent l'utilisation d'un outil tiers pour le test internet classique (ex Speedtest).
  Pour le test réseau privé du notariat, ils ont leur propre outil qu'ils peuvent passer en se connectant sur un poste.

Navista :

- Utilisent quasi uniquement des routeurs Lanner Electrics. Cela tend cependant à changer.
- Quelques personnes au support ont accès à leur console de supervision, permettant entre autres de visualiser l'état du débit sur leur routeur. Se rapprocher d'un N2 si cette vérification vous semble nécessaire, malgré une première analyse commune avec Navista.

Il est aussi possible de vérifier le débit de l'étude sur une période antérieur via la sonde iperf3.
Pour voir les résultats récupérés par la sonde depuis RG (superviseur interne similaire a PRTG) : **Données > Listings > Custom Script > Sélectionner le serveur Host**



À gauche, le débit métier. À droite, le débit internet.

La sonde ne s'exécute pas tous les jours mais une fois toutes les 1 à 3 semaines. Les résultats de celle-ci sont cependant récupérés tous les jours, il est donc normal que vous ayez le même débit d'affiché sur plusieurs jours à la suite.

Analyse LAN

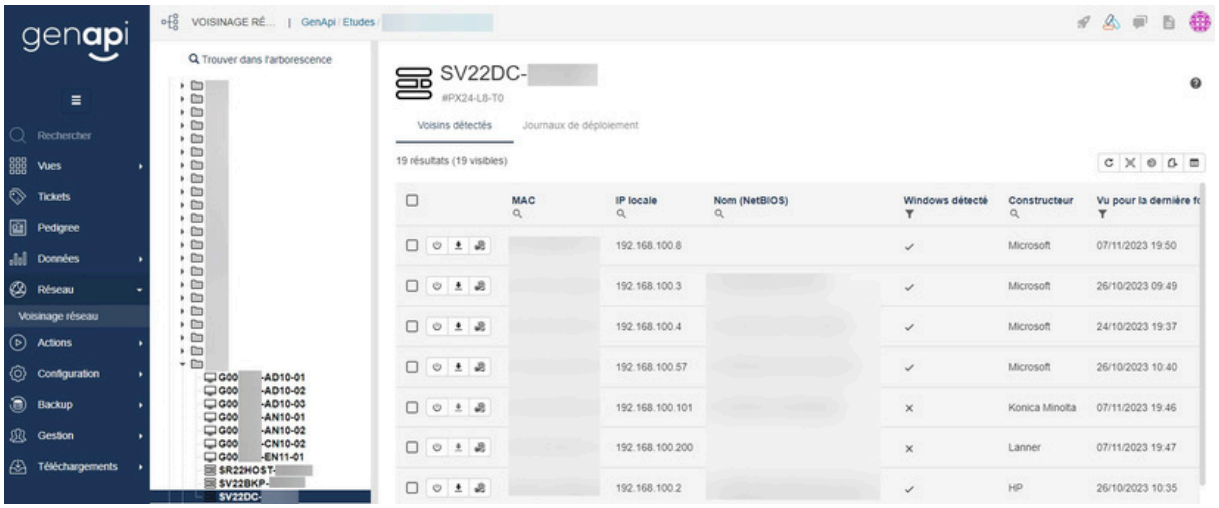
Le LAN (Local Area Network) est la partie locale du réseau de l'étude, donc toute la partie se situant avant le routeur.

Il est recommandé dans un premier temps, avant toute analyse, d'effectuer un scan IP du réseau.
Cela vous permettra d'avoir un meilleur vue sur l'infrastructure de l'étude, et d'identifier certain point important comme :

- Le nombre d'appareils présent sur l'étude (très important pour les études en cloud, pour s'assurer qu'ils respectent nos prérequis de débit, soit 3-4 Mo par utilisateur).
- Le nombre de switchs ainsi que leur IP.
- Si du matériel prestataire est présent sur le LAN, par exemple de la téléphonie ou des switch tiers, pouvant potentiellement perturber le réseau.

Il est aussi possible de visualiser les appareils présents sur le LAN de l'étude depuis RG.

Pour cela, sélectionnez l'un des serveurs (de préférence le DC) puis allez dans les onglets à gauche : **Réseau > Voisinage réseau**.



Les appareils remontant ici sont ceux détectés par la sonde lors de son exécution vers minuit (mis à part les appareils ayant un agent RG d'installer, ex poste et serveur). Il n'est donc pas possible d'avoir une vue à l'instanté.

Petite précision, si l'étude a de la téléphonie par IP, nos prérequis demandent à ce que celle-ci soit isolée de notre réseau. Cette scission peut être faite soit physiquement, auquel cas le switch du prestataire ne doit en aucun cas être connecté ni à l'un de nos switchs ni au routeur FAI métier, soit virtuellement via une VLAN configurée par le prestataire téléphonique sur son propre switch, auquel cas celui-ci peut être branché sur l'un des nôtres.
Il reste cependant possible de croiser des configurations atypiques, ne vous bloquez donc pas inutilement dessus si vous en rencontrez.

Transfert de fichier volumineux

Il est important de tester le débit interne de l'étude via un transfert de fichier volumineux.
Le test est à faire dans les deux sens : **poste > serveur** et **serveur > poste**.

Un test de transfert du host vers une VM n'est pas pertinent. Même s'ils utilisent des cartes réseau physiques différentes, Hyper-V utilise un protocole particulier. Le test s'en retrouvera donc faussé.

Pour cela, vous pouvez via la commande ci-dessous générer un fichier faisant artificiellement une taille prédéfinie, ici 5 Go :

fsutil file createnew c:\fichier5Go.txt 5242880000

Si vous n'avez pas la main sur un poste, vous pouvez vous connecter à son lecteur C:\ depuis l'un des serveurs, via un explorateur Windows en tapant ceci dans la barre de chemin d'accès : ***\\IpDuPoste\c$***
Il vous sera demandé de vous authentifier, vous pouvez utiliser le compte administrateur du domaine.
Si l'étude est en full cloud, le compte à utiliser et soit celui de l'utilisateur distant, soit le compte administrateur local.
Le transfert doit être autour de 100 Mo/s.
Petite précision, si vous effectuez un ping en parallèle de votre transfert de fichier, il est tout à fait normal que le temps de réponse monte autour des 60ms même pour un ping LAN.

Bien penser à supprimer le fichier des deux côtés une fois le test effectué !

Fping

un fping permet d'effectuer en simultané des ping vers plusieurs hôtes sur une période étendue, et de récupérer l'intégralité des résultats sur cette période (ce qui n'est pas le cas pour un ping classique, l'historique ne pouvant dépasser une certaine taille).
Cela permet d'identifier de possibles perturbations sur le réseau LAN ou WAN hors période d'intervention, en croisant avec un horodatage.
Les adresses suivantes sont obligatoires lors d'un fping : site métier / Google / PROD / switchs / passerelle.
Voir KB ci-dessous pour le téléchargement de l'outil + explication de son utilisation :

[Réseau] FPING : pings en boucle sur plusieurs adresses avec log datés

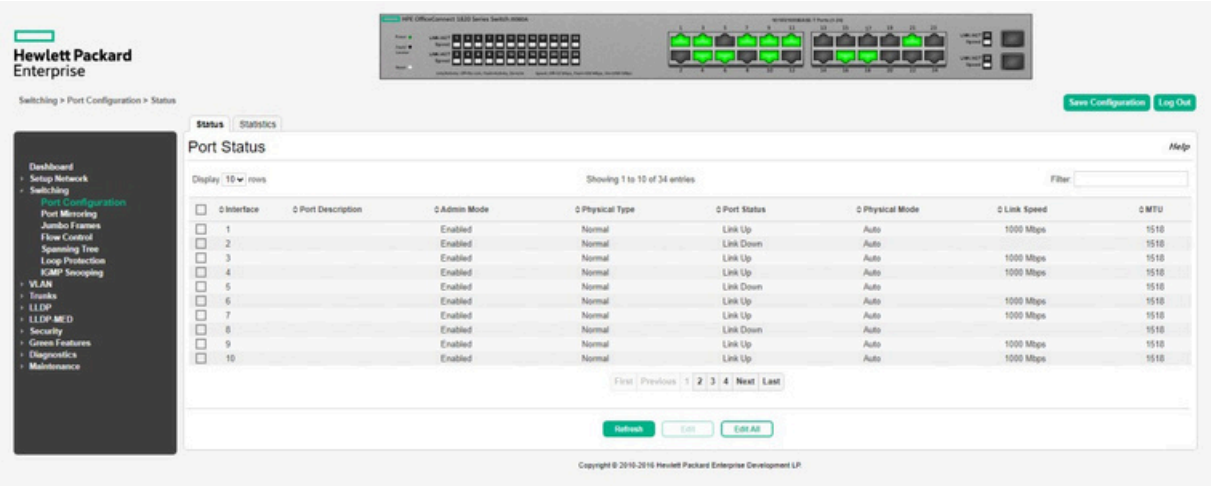
Switch

Il ne sera présenté ici que les points importants à vérifier sur les switchs dans le cas de lenteurs réseau.

Pour tout détail quant aux autres fonctionnalités sur un switch HPE / Aruba, se référer à la KB ci-dessous :

[Réseau] Présentation fonctionnalités switch HPE / ARUBA

Configuration des ports



Ici, deux choses importantes sont à vérifier :

> **Le Physical Mode :** est configuré par défaut en Auto. La vitesse définie dépend donc de celle négociée avec l'appareil en face, selon celle qu'il peut supporter. Il n'est donc pas nécessaire de changer le mode dans ce cas-là.
>
> **Le Link Speed :** vitesse max actuel. Dépend soit de la vitesse max défini sur le port, soit de la vitesse négociée avec l'appareil distant.

Il faut donc s'assurer que tous les ports sont configurés en négociation automatique, et voir quelle est la vitesse actuelle sur les ports.

Si la vitesse sur un port est à 100 Mbps, il faut regarder quels appareils sont branchés dessus.
Vous pouvez pour cela vous aider du tableau d'adresse MAC du switch.
La première chose à regarder dessus est le nombre d'appareils remontant sur le port.
Si plusieurs appareils remontent dessus, il y a de très fortes chances qu'un switch soit de l'autre côté.
Reste ensuite à identifier si ce switch est à nous, si son port est configuré en automatique, etc.
Si un seul appareil remonte, il y a de fortes chances que la carte réseau de celui-ci ne supporte que le 100 Mbps (généralement des imprimantes). Vous pouvez confirmer le type de l'appareil via son adresse MAC, soit en croisant avec un scan IP, soit en vérifiant le constructeur de ce type d'adresse MAC via un site spécialisé.

Vérification brassage / câblage

Il est possible qu'une défaillance physique sur l'infrastructure réseau soit à l'origine de lenteurs de l'étude.
Sur ce plan-là, plusieurs points sont à vérifier :

Câbles réseau : les câbles en eux-mêmes peuvent être défectueux, soit celui reliant la prise murale à la baie de brassage, soit celui allant de la baie de brassage au switch.
Vous pouvez changer le câble entre la baie et le switch ou changer de prise réseau mural pour vous en assurer.

Prise réseau : défaillance directement sur la prise réseau, soit celle du switch soit la prise réseau mural.
Même chose que plus haut, vous pouvez vous en assurer en changeant de prise.

Si une défaillance est trouvée au niveau d'une prise réseau mural ou de son câble allant vers la baie de brassage, il faut demander à l'étude qu'ils fassent intervenir un électricien basse tension.

NE PAS HÉSITER À DEMANDER UNE PHOTO DE LA BAIE DE BRASSAGE !

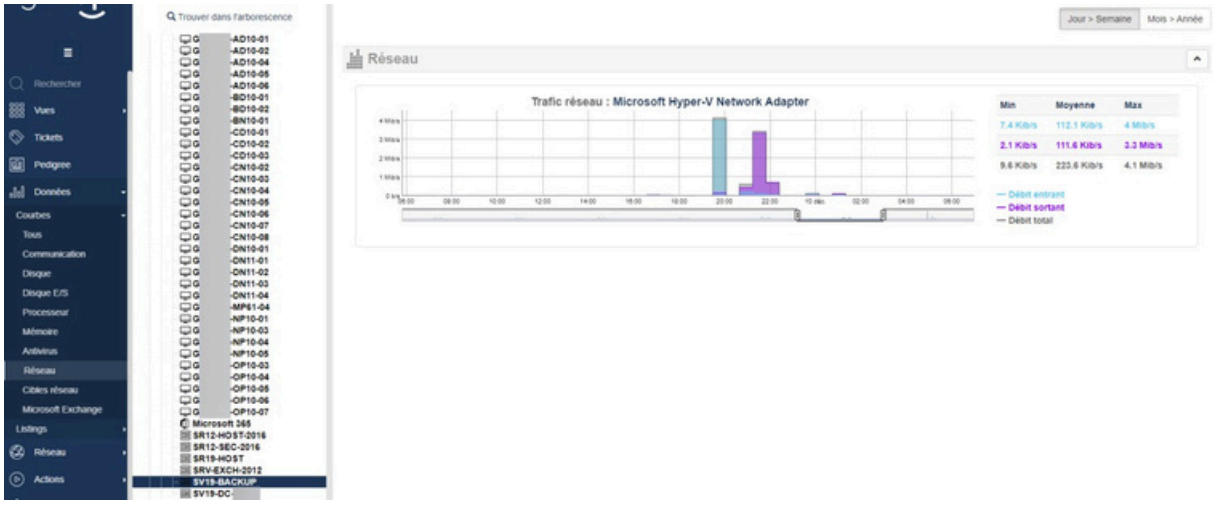
Les prises réseau mural sont généralement numérotées. Ces numéros correspondent à ceux du bandeau de brassage, pas ceux du switch !

Sauvegarde externalisée

Il peut arriver que les sauvegardes externalisées saturent la bande passante de l'étude en journée.
Vous pouvez vous en assurer en allant vérifier sur Veeam, sur la VM backup.
Ci-dessous la KB expliquant comment effectuer ces vérifications :

Il est aussi possible de voir directement depuis RG l'historique du débit de la VM backup, à croiser avec le débit internet de l'étude et les heures où surviennent les lenteurs.
La seule courbe importante ici est la violette, représentant le débit sortant.

Données > Courbes > Réseau > serveur Backup



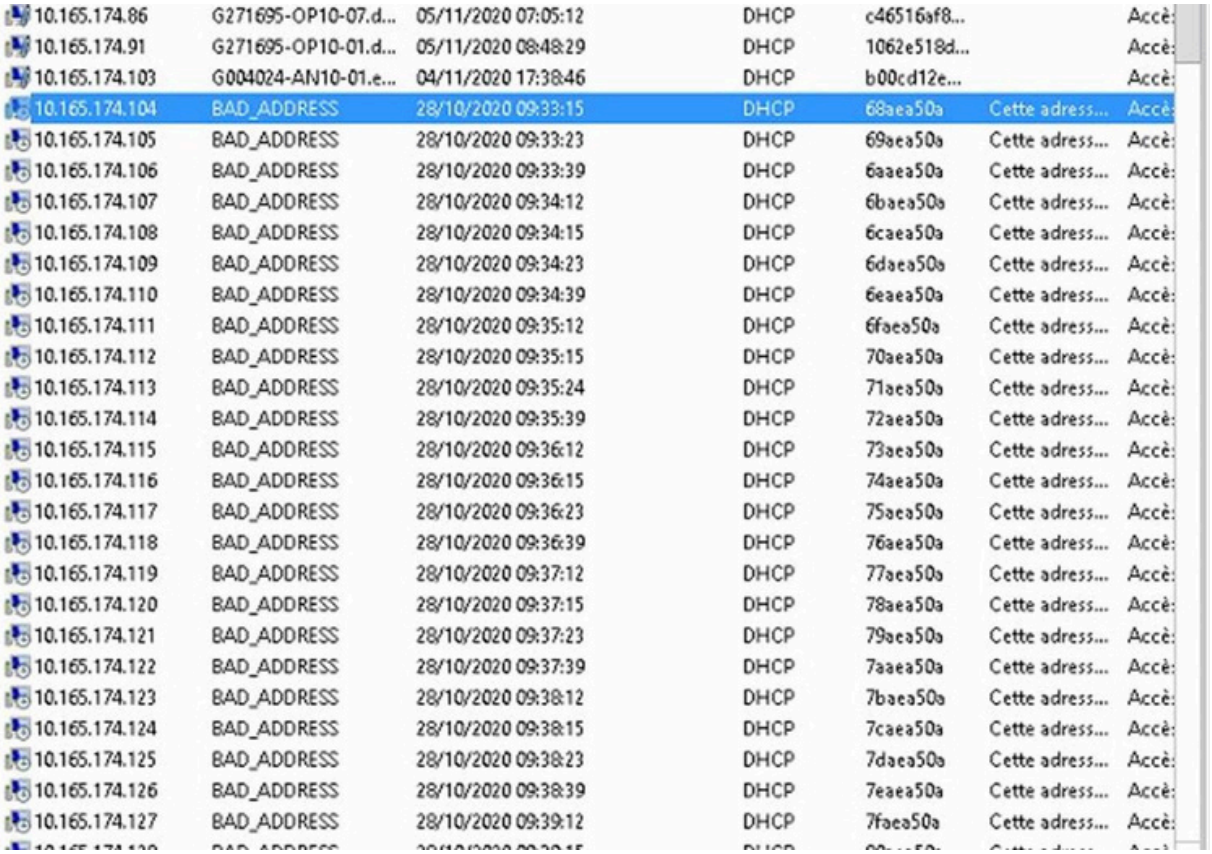
Vérifications DC (serveur Active Directory)

Différents points de vérification peuvent être effectués sur le DC, qu'ils s'apparentent directement ou indirectement au réseau.

DHCP

Il est possible qu'un appareil sur le LAN (ex téléphonie) sature le bail d'adresse DHCP en se les "réservant".
Dans ce cas de figure, les adresses apparaissent prises par des appareils nommés "BAD_ADDRESS".

Cela génère généralement des productions bloquées, mais peut aussi générer des performances dégradées, si une adresse déjà prise par un ordinateur de l'étude est attribuée par cet autre appareil à un autre matériel. Le doublon d'adressage IP créera alors des coupures pour les deux appareils.



10.165.174.86	G271695-OP10-07.d...	05/11/2020 07:05:12	DHCP	c46516af8...		Accè:
10.165.174.91	G271695-OP10-01.d...	05/11/2020 08:48:29	DHCP	1062e518d...		Accè:
10.165.174.103	G004024-AN10-01.e...	04/11/2020 17:38:46	DHCP	b00cd12e...		Accè:
10.165.174.104	BAD_ADDRESS	28/10/2020 09:33:15	DHCP	68aea50a	Cette adress...	Accè:
10.165.174.105	BAD_ADDRESS	28/10/2020 09:33:23	DHCP	69aea50a	Cette adress...	Accè:
10.165.174.106	BAD_ADDRESS	28/10/2020 09:33:39	DHCP	6aaea50a	Cette adress...	Accè:
10.165.174.107	BAD_ADDRESS	28/10/2020 09:34:12	DHCP	6baea50a	Cette adress...	Accè:
10.165.174.108	BAD_ADDRESS	28/10/2020 09:34:15	DHCP	6caea50a	Cette adress...	Accè:
10.165.174.109	BAD_ADDRESS	28/10/2020 09:34:23	DHCP	6daea50a	Cette adress...	Accè:
10.165.174.110	BAD_ADDRESS	28/10/2020 09:34:39	DHCP	6eaea50a	Cette adress...	Accè:
10.165.174.111	BAD_ADDRESS	28/10/2020 09:35:12	DHCP	6faea50a	Cette adress...	Accè:
10.165.174.112	BAD_ADDRESS	28/10/2020 09:35:15	DHCP	70aea50a	Cette adress...	Accè:
10.165.174.113	BAD_ADDRESS	28/10/2020 09:35:24	DHCP	71aea50a	Cette adress...	Accè:
10.165.174.114	BAD_ADDRESS	28/10/2020 09:35:39	DHCP	72aea50a	Cette adress...	Accè:
10.165.174.115	BAD_ADDRESS	28/10/2020 09:36:12	DHCP	73aea50a	Cette adress...	Accè:
10.165.174.116	BAD_ADDRESS	28/10/2020 09:36:15	DHCP	74aea50a	Cette adress...	Accè:
10.165.174.117	BAD_ADDRESS	28/10/2020 09:36:23	DHCP	75aea50a	Cette adress...	Accè:
10.165.174.118	BAD_ADDRESS	28/10/2020 09:36:39	DHCP	76aea50a	Cette adress...	Accè:
10.165.174.119	BAD_ADDRESS	28/10/2020 09:37:12	DHCP	77aea50a	Cette adress...	Accè:
10.165.174.120	BAD_ADDRESS	28/10/2020 09:37:15	DHCP	78aea50a	Cette adress...	Accè:
10.165.174.121	BAD_ADDRESS	28/10/2020 09:37:23	DHCP	79aea50a	Cette adress...	Accè:
10.165.174.122	BAD_ADDRESS	28/10/2020 09:37:39	DHCP	7aaea50a	Cette adress...	Accè:
10.165.174.123	BAD_ADDRESS	28/10/2020 09:38:12	DHCP	7baea50a	Cette adress...	Accè:
10.165.174.124	BAD_ADDRESS	28/10/2020 09:38:15	DHCP	7caea50a	Cette adress...	Accè:
10.165.174.125	BAD_ADDRESS	28/10/2020 09:38:23	DHCP	7daea50a	Cette adress...	Accè:
10.165.174.126	BAD_ADDRESS	28/10/2020 09:38:39	DHCP	7eaea50a	Cette adress...	Accè:
10.165.174.127	BAD_ADDRESS	28/10/2020 09:39:12	DHCP	7faea50a	Cette adress...	Accè:

Antivirus

Certains ralentissements réseau peuvent être engendrer par l'antivirus Bitdefender.

Afin d'identifier ces cas, veuillez effectuer le test suivant :

- Test après désinstallation de l'antivirus (BitDefender : Présentation, Installation / Désinstallation, Console, Assistance) ou test après désactivation des modules de l'antivirus via la console PowerUser ([BitDefender] Guide PowerUser BitDefender)

Si le problème est résolu après désinstallation de l'antivirus, alors il faut se réferrer à la kb

[Bitdefender] Performances dégradées générées par l'antivirus

Si cette dernière kb ne permet pas de résoudre l'anomalie, il faut alors essayer d'identifier quelle module cause l'anomalie en désactivant les modules adjacents.