Audit de satisfaction de la solution netMET
Novembre 2002 – Janvier 2003

1 Pourquoi cet audit et comment ?

1.1 Pourquoi ?

netMET - Network's METrology est aujourd'hui déployé dans de multiples réseaux régionaux, de campus ou de sites en France. Il nous parait essentiel de faire le point sur ces déploiements et de connaître le niveau de satisfaction des personnes qui ont choisit netMET comme solution de métrologie.
Pour ceci, nous avons invité les utilisateurs netMET à répondre à un questionnaire électronique dans la période de novembre 2002 à janvier 2003.

Les résultats de ce questionnaire devaient permettre:

- de faire le point sur le déploiement réalisé dans chaque site qui ont choisi netMET comme solution de métrologie,
- de vérifier si netMET est adapté aux besoins des administrateurs et des utilisateurs,
- de voir quelles ont pu être les difficultés de déploiement
- et si netMET s'inscrit dans un schéma de déploiement et d'utilisation le plus convivial possible.

Ce questionnaire s'adressait:

- aux "administrateurs netMET": les personnes ayant installées et administrant la solution au quotidien
- aux "utilisateurs netMET": les personnes utilisant et exploitant les informations fournies par netMET.

Vous trouverez dans les pages suivantes :

- les résultats des questions adressées aux "administrateurs netMET" à partir de la page 2,
- les résultats des questions adressées aux "utilisateurs netMET" à partir de la page 2.

1.2 Comment ?

Nous n'avons modifié aucun des résultats présentés ci-après sauf pour:

- les questions 4 page 3 et 7 page 10, pour lesquels nous avons reporté les scores de la possibilité de choix "200 %" dans les scores de la possibilité "100 %" (si les gens sont satisfaits à 200 %, c'est qu'il le sont au moins à 100 % ☺)
- les questions 4 et 5 page 9, qui étaient des questions à choix multiples par ordre d'importance. Nous avons donc établi un système de pondération permettant d'en sortir les fonctionnalités les plus importantes,
- certains commentaires libres comportaient des "phottes d'orthaugrafe", nous avons alors apporté quelques corrections.

Nous n'avons pas fait de conclusion ou d'analyse spécifique à chaque question, et pour des questions d'intégrité nous ne voulons pas non plus faire de conclusion générale. Tout à chacun pourra tirer les conclusions qui s'imposent… Nous pouvons juste préciser que l'ensemble des réponses nous conforte dans nos choix de développement et nous permettront à l'avenir de répondre au mieux aux attentes des administrateurs et utilisateurs netMET.

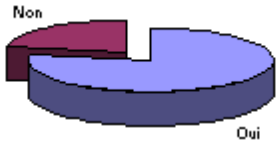
L'équipe netMET.
netmet@netmet-solutions.org

2 Résultats questionnaire "administrateur netMET"

32 administrateurs netMET ont répondu à ce questionnaire.

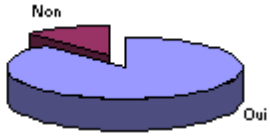
1 - Avez-vous essayé d'installer netMET ?

	Nombre	Pourcentage
Oui	25	78.1%
Non	7	21.9%
Total	32	100%



Si oui fonctionne-t-il ?

	Nombre	Pourcentage
Oui	22	88.0%
Non	3	12.0%
	25	100%

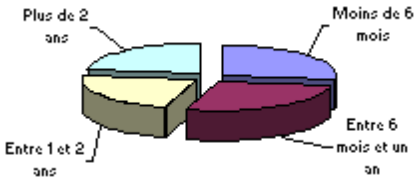


Si non quelle en est la raison principale ?

	Nombre	Pourcentage
Je n'ai pas encore réussi à l'installer	1	14.3%
Je n'ai pas encore eu le temps	6	85.7%
netMET n'est plus dans mes priorités	0	0.0%
Des problèmes techniques m'empêchent de l'installer	0	0.0%
Autre	0	0.0%
Total	7	100%

2 - Depuis combien de temps utilisez-vous netMET ?

	Nombre	Pourcentage
Moins de 6 mois	6	27.3%
Entre 6 mois et un an	6	27.3%
Entre 1 et 2 ans	5	22.7%
Plus de 2 ans	5	22.7%
Total	22	100%

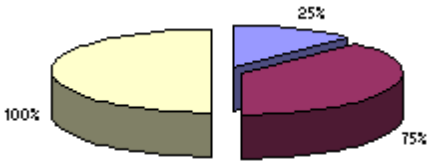


3 - Quelles sont les utilisations que vous faites de netMET ?

	Nombre	Pourcentage
Test	5	22.7%
Production	22	100.0%
Développement	3	13.6%

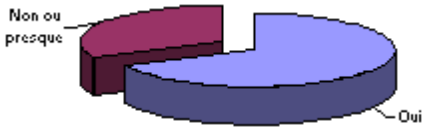
4 - Quel est votre degré de satisfaction ?

	Nombre	Pourcentage
0%	0	0.0%
25%	1	4.5%
50%	0	0.0%
75%	9	40.9%
100%	12	54.5%
Total	22	100%



5 - netMET répond-il entièrement à vos attentes ?

	Nombre	Pourcentage
Oui	15	68.2%
Non ou presque	7	31.8%
Total	22	100%



Pourquoi :

* Repérage temporel des flux insuffisant pour pister un problème spécifique
* Manque les sources ☺

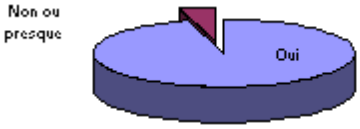
* Actuellement netMET est utilisé pour analyser la "sortie" de notre réseau, j'ai essayé en vain de faire une adaptation pour l'appliquer à notre réseau interne basé sur un commutateur routeur qui "parle" netflow et que netmet comprend mais je n'ai pas enco
* Manque de granularité dans la description des réseaux. Lookup un peu rigide.

* Je suis intéressée par l'intégration d'un métrologie "intra". Si possible, ajouter l'envoi par email d'alertes en cas de dysfonctionnement, par exemple quand netmet détecte que la mémoire est insuffisante et qu'il y a risque de perte de données. Si possible

* Ne fonctionne pas avec tous les routeurs Cisco que j'administre (1600, 1700). Les ports TCP/UDP interessants (Gnutella ...) ou pas connus doivent être entrés à la main. Certaines fonctionnalités de la partie web ne fonctionnent pas.
* Installation fastidieuse, produit trop complexe au regard de solution commerciale proposant pratiquement les mêmes fonctionnalités. Code non ouvert et non évolutif. Mise à jour du système hôte IMPOSSIBLE.
*La gestion multi-site avec un trou RENATER n'est pas évidente. Le manque de suivi sur le rpm Linux rend très complexe la maintenance des systèmes.

6 - L'évolution de la solution et le suivi du projet sont-ils suffisants ?

	Nombre	Pourcentage
Oui	21	95.5%
Non ou presque	1	4.5%
Total	22	100%

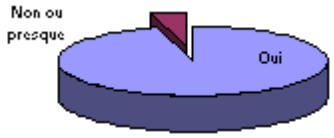


Pourquoi :

* Toujours pas de version debian
* Code non ouvert et non évolutif.
* Choix de ne pas suivre l'évolution de RedHat est pénalisant.

7 - Etes-vous satisfaits du site web officiel de netMET ?

	Nombre	Pourcentage
Oui	21	95.5%
Non ou presque	1	4.5%
Total	22	100%



Pourquoi :

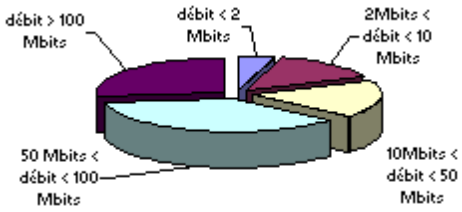
* Pas grand chose de nouveau depuis 2001
* Pas facile de trouver une info claire
* Doc peu interressantes. Pas à jour.

8 - Que proposeriez-vous pour la suite de ce projet ?

* Beaucoup de choses qui viennent d'être annoncées pour la nouvelle version : meilleure navigation web, application à des traffics sur des réseaux "internes" (la notion de trou noir moins restrictivre)
* Continuez a faire vivre ce produit. Encore chapeau pour le travail fourni
* Evolution vers l'aspect sécurité (détection d'intrusion)
* Je ne sais pas
* Matrices graphiques des différents flux (par protocole, services....). Selon les trafics, par port par exemple, une liaison avec les avis de sécurité du CERT… Pour terminer : peut-etre moins lié à Cisco
* Pour l'instant pas d'idées
* Pouvoir modifier le fichier /etc/services "sans casse". Stabilité du produit - certains dysfonctionnements restent sans explication.
* How-to
* Prise en compte d'IPv6

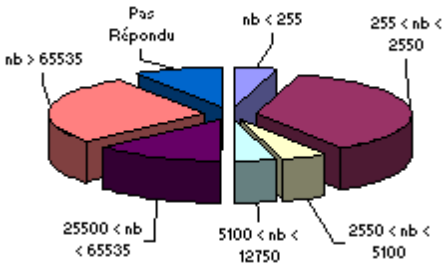
9 - Quelle est la taille de la connexion vers le réseau fédérateur ?

	Nombre	Pourcentage
débit < 2 Mbits	1	4.5%
2Mbits < débit < 10 Mbits	3	13.6%
10Mbits < débit < 50 Mbits	4	18.2%
50 Mbits < débit < 100 Mbits	8	36.4%
débit > 100 Mbits	6	27.3%
Total	22	100%



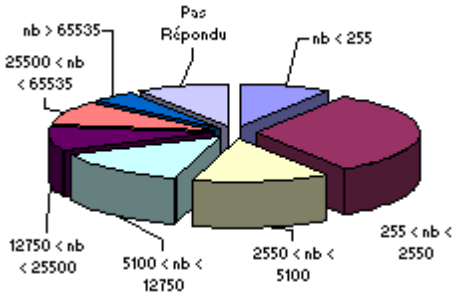
10 - Combien comptabilisez-vous de machines potentielles sur votre réseau ?

	Nombre	Pourcentage
nb < 255	1	4.5%
255 < nb < 2550	8	36.4%
2550 < nb < 5100	1	4.5%
5100 < nb < 12750	1	4.5%
12750 < nb < 25500	0	0.0%
25500 < nb < 65535	3	13.6%
nb > 65535	6	27.3%
Pas Répondu	2	9.1%
Total	22	100%



11 - Combien comptabilisez-vous de machines réelles sur votre réseau ?

	Nombre	Pourcentage
nb < 255	2	9.1%
255 < nb < 2550	7	31.8%
2550 < nb < 5100	3	13.6%
5100 < nb < 12750	3	13.6%
12750 < nb < 25500	2	9.1%
25500 < nb < 65535	2	9.1%
nb > 65535	1	4.5%
Pas Répondu	2	9.1%
Total	22	100%



12 - Quelle est la technologie de cette connexion vers le réseau fédérateur ?

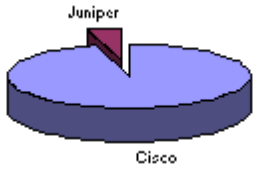
	Nombre	Pourcentage
ATM	6	27.3%
Ethernet	15	68.2%
Autre	1	4.5%
Total	22	100%

Autre :

* Liaison 43Mb sur le réseau Régional Megalis, puis Renater 3 pour le trafic IPV4. Liaison ATM 4Mb direct sur Renater3 pour IPV6 et MBONE (1VP, 2VC)

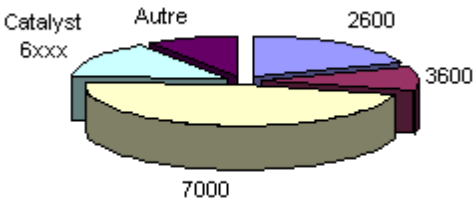
13 - De quelle marque est votre matériel (routeur) d'interconnexion vers le réseau fédérateur ?

	Nombre	Pourcentage
Cisco	21	95.5%
Juniper	1	4.5%
Extrem Network	0	0.0%
Autre	0	0.0%
Total	22	100%



Si votre matériel est du Cisco, pouvez-vous préciser la gamme.

	Nombre	Pourcentage
2600	4	19.0%
3600	2	9.5%
7000	10	47.6%
12000	0	0.0%
Catalyst 4xxx	0	0.0%
Catalyst 6xxx	3	14.3%
Autre	2	9.5%
Total	21	100%

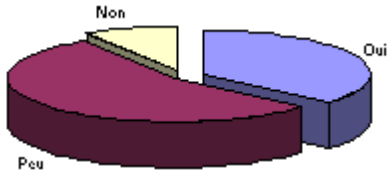


Autre :

* 2514
* 37xx

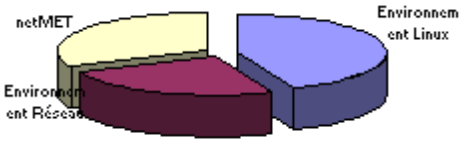
14 - Avez-vous rencontré des difficultés particulières à la mise en place de netMET ?

	Nombre	Pourcentage
Oui	8	36.4%
Peu	12	54.5%
Non	2	9.1%
Total	22	100%



15 - Ces difficultés étaient liées à ?

	Nombre	Pourcentage
Environnement Linux	11	50.0%
Environnement Réseau	6	27.3%
netMET	8	36.4%
Autre	2	9.1%

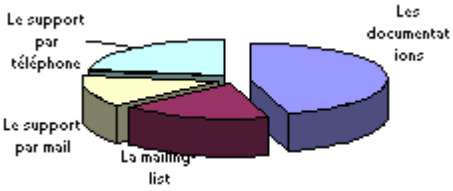


Autre :

* Avant une version statique, difficultés sur les versions des librairies utilisées
* Version IOS posait des pb d'exportation de flows

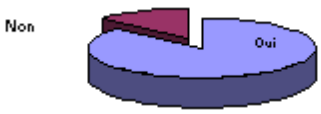
16 - Quelle a été votre source principale de recherche d'informations sur vos problèmes ?

	Nombre	Pourcentage
Les documentations	10	45.5%
La mailing-list	4	18.2%
Le support par mail	3	13.6%
Le support par téléphone	5	22.7%
Total	22	100%



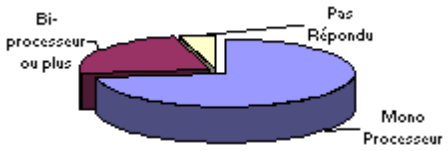
17 - Avez-vous trouvé facilement les réponses à vos questions dans les différentes sources ?

	Nombre	Pourcentage
Oui	19	86.4%
Non	3	13.6%
Total	22	100%

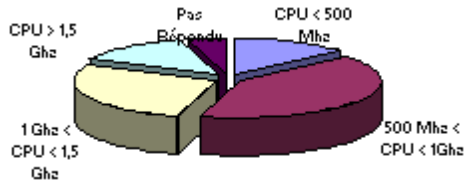


18 - pouvez-vous fournir des informations sur votre serveur netMET ?

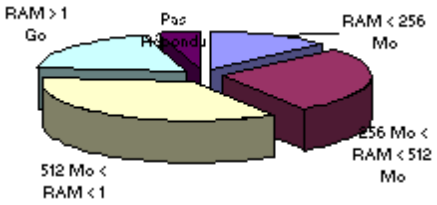
	Nombre	Pourcentage
Mono Processeur	16	72.7%
Bi-processeur ou plus	5	22.7%
Pas Répondu	1	4.5%
Total	21	100%



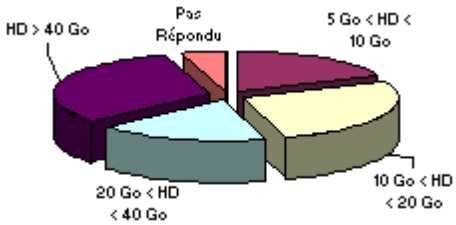
	Nombre	Pourcentage
CPU < 500 Mhz	3	13.6%
500 Mhz < CPU < 1Ghz	9	40.9%
1 Ghz < CPU < 1,5 Ghz	6	27.3%
CPU > 1,5 Ghz	3	13.6%
Pas Répondu	1	4.5%
Total	22	100%



	Nombre	Pourcentage
RAM < 256 Mo	3	13.6%
256 Mo < RAM < 512 Mo	6	27.3%
512 Mo < RAM < 1 Go	8	36.4%
RAM > 1 Go	4	18.2%
Pas Répondu	1	4.5%
Total	22	100%

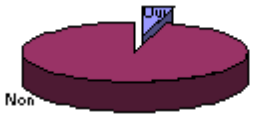


	Nombre	Pourcentage
HD < 5 Go	0	0.0%
5 Go < HD < 10 Go	4	18.2%
10 Go < HD < 20 Go	6	27.3%
20 Go < HD < 40 Go	4	18.2%
HD > 40 Go	7	31.8%
Pas Répondu	1	4.5%
Total	22	100%



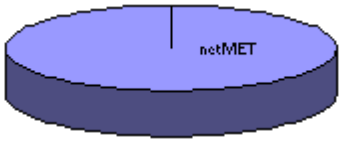
19 - Trouvez-vous que l'administration de netMET soit compliquée ?

	Nombre	Pourcentage
Oui	1	4.5%
Non	21	95.5%
Total	22	100%



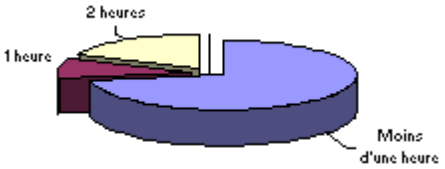
Si oui, ces difficultés étaient liées à ?

	Nombre	Pourcentage
Environnement Linux	0	0.0%
netMET	1	100.0%
Autre	0	0.0%



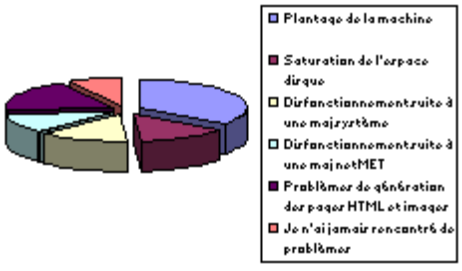
20 - Cette administration vous prend en moyenne combien de temps par semaine ?

	Nombre	Pourcentage
Moins d'une heure	16	72.7%
1 heure	2	9.1%
2 heures	4	18.2%
3 heures ou plus	0	0.0%
Total	22	100%



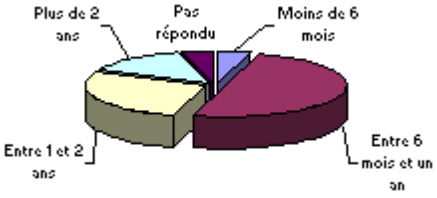
21 - Les problèmes que vous avez déjà rencontrés concernaient ?

	Nombre	Pourcentage
Plantage de la machine	13	59.1%
Saturation de l'espace disque	5	22.7%
Disfonctionnement suite à une maj système	5	22.7%
Disfonctionnement suite à une maj netMET	4	18.2%
Problèmes de génération des pages HTML et images	7	31.8%
Je n'ai jamais rencontré de problèmes	3	13.6%



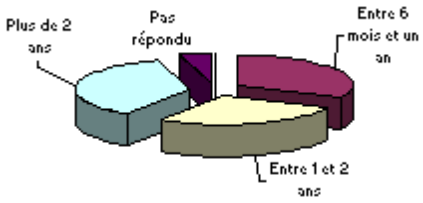
22 - Combien de temps conservez-vous les fichiers de collecte ?

	Nombre	Pourcentage
Moins de 6 mois	1	4.5%
Entre 6 mois et un an	11	50.0%
Entre 1 et 2 ans	6	27.3%
Plus de 2 ans	3	13.6%
Pas répondu	1	4.5%
Total	22	100%



23 - Combien de temps conservez-vous les fichiers html et images ?

	Nombre	Pourcentage
Moins de 6 mois	0	0.0%
Entre 6 mois et un an	7	31.8%
Entre 1 et 2 ans	6	27.3%
Plus de 2 ans	8	36.4%
Pas répondu	1	4.5%
Total	22	100%



3 Résultats questionnaire "utilisateurs netMET"

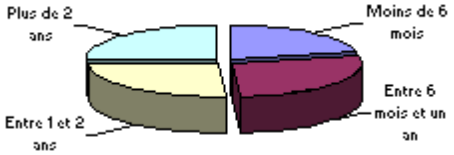
47 utilisateurs netMET ont répondu à ce questionnaire.

1-Quelle est votre fréquence d'utilisation de netMET ?

	Nombre	Pourcentage
Plusieurs fois par jour	16	34.0%
Une fois par jour	7	14.9%
Plusieurs fois par semaine	8	17.0%
Une fois par semaine	8	17.0%
De temps en temps	8	17.0%
Total	47	100%

2 - Depuis combien de temps utilisez-vous netMET ?

	Nombre	Pourcentage
Moins de 6 mois	10	21.3%
Entre 6 mois et un an	13	27.7%
Entre 1 et 2 ans	12	25.5%
Plus de 2 ans	12	25.5%
Total	47	100%

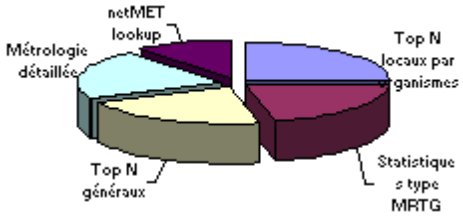


3 - Quelle est la principale utilisation que vous faites de netMET ?

	Nombre	Pourcentage
Métrologie et statistiques	22	46.8%
Sécurité	25	53.2%
Total	47	100%

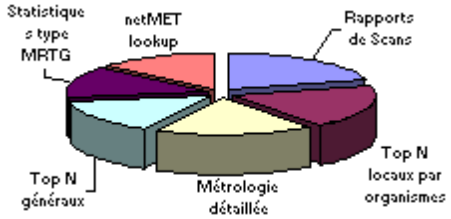
4 - Dans l'utilisation pour la métrologie et les statistiques, classez les fonctionnalités netMET par ordre d'importance.

	Pourcentage
Top N locaux par organismes	25.0%
Statistiques type MRTG	21.7%
Top N généraux	21.3%
Métrologie détaillée	21.1%
netMET lookup	10.9%
Total	100%



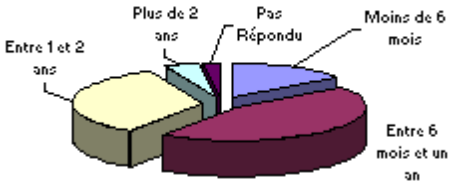
5 - Dans l'utilisation pour la sécurité, classez les fonctionnalités netMET par ordre d'importance.

		Pourcentage
Rapports de Scans		20.4%
Top N locaux par organismes		19.0%
Métrologie détaillée		18.5%
Top N généraux		14.6%
Statistiques type MRTG		13.9%
netMET lookup		13.6%
	Total	100%



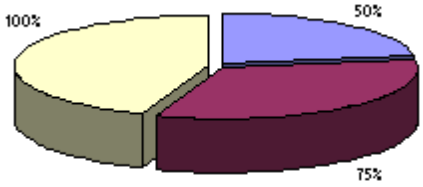
6 - Combien de temps souhaiteriez-vous que les archives soient conservées ?

	Nombre	Pourcentage
Moins de 6 mois	7	14.9%
Entre 6 mois et un an	21	44.7%
Entre 1 et 2 ans	16	34.0%
Plus de 2 ans	2	4.3%
Pas Répondu	1	2.1%
Total	47	100%



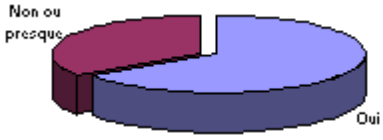
7 - Quel est le degré de pertinence des informations fournies par netMET ?

	Nombre	Pourcentage
0%	0	0.0%
25%	0	0.0%
50%	3	6.4%
75%	19	40.4%
100%	25	53.2%
Total	47	100%



8 - netMET répond-il entièrement à vos attentes ?

	Nombre	Pourcentage
Oui	31	66.0%
Non ou presque	16	34.0%
Total	47	100%

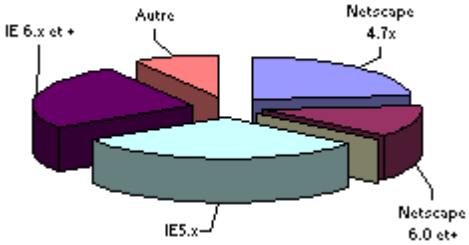


Pourquoi :

* Avoir le traffic détaillé par site
* Car pas d'accès aux rapports de SCAN et à NETMET lookup
* C'est très bien, mais il y a des difficultés d'interprétation avec nos VPN (tunnels GRE)
* Comme tout logiciel, il faut affiner, mais c'est déjà un super début pour enquêter plus loin
* La consultation des archives (semaines et mois) est buggée.
* La partie métrologie détaillée n'affiche que les ports décrits dans /etc/services, malheureusement les "malins" Gnutella et autres utilisent d'autres ports. Netmet affiche alors le 65535.
* Les résultats sont discontinus
* Pas d'accès à netMET Lookup - Manque une décomposition par composante, le niveau UHP est trop vaste pour être représentatif, ensuite accès à chaque correspondant de site pour son propre site
* Pas le temps de consulter régulierement, je voudrais pouvoir postionner facilement des seuils d'alerte... je t'en avais déjà parlé - le traitement de NetLookup est un peu lent
* Pour les postes "natés" pas possible d'avoir de detail par ip privé
* Toutes les fonctionalités ne marchent pas encore. Il n'y a pas d'appercu global des problèmes
* Trop d'informations pour un petit site. Pour le rapport scan, il faudrait n'avoir que ses réseaux. La métrologie détaillée ne nous est pas utile, trop vaste. Dans details du trafic pour une machine (lorsqu'une machine "consomme" beaucoup, le tableau rep

9 - Quel navigateur utilisez-vous principalement ?

	Nombre	Pourcentage
Netscape 4.5 et antérieur	0	0.0%
Netscape 4.7x	11	23.4%
Netscape 6.0 et supérieur	6	12.8%
Internet Explorer 4.5 et antérieur	0	0.0%
Internet Explorer 5.x	14	29.8%
Internet Explorer 6.x et supérieur	12	25.5%
Autre	4	8.5%
Total	47	100%



10 - Avez-vous déjà rencontré des problèmes d'affichage avec votre navigateur ?

	Nombre	Pourcentage
Oui	9	19.1%
Non	38	80.9%
Total	47	100%

11 - Que proposeriez vous comme évolution et/ou nouvelles fonctionnalité ?

* Amélioration de la navigation entre les pages : passer de jour en jour sans revenir au sommaire.
* Appercu global des problèmes : si un trafic "bizarre" apparaît. Affichage simultané des résultats détaillés sur plusieurs jours
* Avoir la possibilité de visualiser les ip privés des postes natés dans le top N
* Avoir les src/dst dans rapport detaillé d'une machine. Si possible les rapports/scans juste pour les réseaux du site concerné. Métrologie juste pour les reseaux du site. Difficile de répondre au questionnaire (que signifie une satisfaction a 75%, 25%)
* Ce qui pourrait être intéressant ce serait d'avoir un système d'alarme par mail lorsque le profil d'utilisation du réseau en entrée ou en sortie subit un changement de profil important par exemple quand une machine apparaît brutalement dans le top 20 ou/aavec un changement de trafic important.
* J'aimerai avoir le TOP 10 des ports les plus scannes de mon réseau
* Je ne sais pas
* Mettre en évidence les points critiques au niveau des scans. Je n'ai pas accès à netmet lookup
* Outil de consolidation de scan pour centralisation regionale/nationale
* Pas de questions pour le moments
* La possibilité de rajouter "au vol" une surveillance temporaire (tout trafic avec une machine, ou sur un port par exemple)
* Pouvoir créer des "filtres" qui généreraient des alertes, exemple "tel IP envoie plus de tant de bits avec tel port source..."
* Que les problèmes ne puissent se cumuler dans le temps (si on ne peut pas calculet les stats pour un intervalle de temps, oublions-le et passons au suivant sans mémoire)

* Ce n'est pas forcément des évolutions et/ou nouvelles fonctionnalités qui suivent. Pour les pbs d'affichage c'est vraiment rien, ce sont juste les tableaux qui de temps en temps se dessinent mal (cellules trop grde), mais un coup de F5 resoud le pb. Je pense que ça vient de mon IE6, mais bon je le signale qd mm. Je n'ai pas accès à netMET LookUp, mais si c'est possible je veux bien. Lorsque l'on utilise le nouveau lien "Détails" ds la section des top N, cela met bcp de temps à s'afficher, j'imagine très que cela doit être dû au temps de recherche des informations. Je ne sais pas si le génération des graphiques prends du temps, mais peut-être que les faire en mode ASCII ou avoir une version texte pourrait accélérer la chose. Une version ASCII ou texte permettrait de copier/coller les IPs ou noms DNS" pour faire des recherches sur ces IPs, alors qu'actuellement ce n'est pas possible puisque le texte fait partie de l'image. Sinon l'outil est super, mais tout le monde le sait déjà ;)
* Seuils d'alertes ….
* Un peu plus de rapidité. Si possible une analyse scan en temps réel et un rapport de scan plus 'condensé'

* Un rapport de scan réélement utilisable. La page actuelle est beaucoup trop longue ce qui la rend difficilement lisible. Ce qu'il serait bien, sa serait de classer les scans par organismes, voire par établissements. (et eventuellement classes réseau). Amélioration de la vitesse de transfert (typiquement, lors de l'affichage des détails d'une machine) Suivi par machine des transferts avec un graphique retracant l'utilisation sur une semaine/un mois. (un mrtg simplifié en gros). Une option pour pouvoir afficher plus de 10 machines dans les top organismes. Pouvoir descendre encore d'un niveau pour le top 10, par exemple pouvoir avoir le top 10 par composante d'un organisme. (top 10 Mines dans INPL). Le café ? :-)

* Un tableau de bord simplifié selon une configuration que l'utilisateur pourrait définir…. Exemple : en priorité voir le trafic de N machines, le graphe général du jour.....
* Une aletre par mail quand le profil change ou pour un debit très important
* Voir question 8. Mais en résumé, trés bon outil !! :-)

Documentation netMET		
par :	Alexandre Simon	Alexandre.Simon@ciril.fr
crée le :	Juin 2003	
mise à jour le :		