

Whatsup Gold application et informations

WhatsUp[®] Gold Progress[®]

Brieuc Le Faucheur Fidèle 28/01/2025

Introduction

WhatsUp Gold est une solution logicielle de surveillance réseau développée par Progress. C'est un outil complet pour surveiller les performances et la disponibilité des réseaux, des serveurs, des applications et des périphériques :

Surveillance du Réseau : Il permet de monitorer la disponibilité et les performances des périphériques réseau, des serveurs et des applications, qu'ils soient sur site ou dans le cloud.

Cartographie Automatique : WhatsUp Gold peut détecter et cartographier automatiquement tous les périphériques connectés à votre réseau, incluant les routeurs, commutateurs, serveurs, et points d'accès.

Alertes et Notifications : Vous pouvez configurer des alertes pour être notifié en temps réel des problèmes potentiels, tels que des pics d'utilisation de la CPU, des pannes de réseau, etc.

Gestion des Logs : Il centralise la gestion des logs, vous permettant de surveiller, filtrer, rechercher et alerter sur les activités des périphériques.

Tableaux de Bord Personnalisés : Vous pouvez créer des tableaux de bord personnalisés pour visualiser les données de performance et les états des périphériques. Surveillance des Ressources Cloud : Il permet de détecter, cartographier et surveiller automatiquement les environnements cloud, y compris AWS et Azure.

Dépendances Réseau : Vous pouvez définir les dépendances entre les périphériques pour éviter les alertes en chaîne et assurer une surveillance précise.

Voici quelques exemples de manœuvres que nous pouvons effectuer avec WhatsUp Gold.

Nous allons effectuer différents tests sur des machines, le serveur est en phase de tests c'est donc le moment propice pour tester différentes manœuvres.

Nous allons superviser notre ordinateur, on peut par exemple, avec WhatsUp Gold Créer un analyseur actif pour savoir si un processus est en cours de lancement sur notre ordinateur ou non.

On peut donc vérifier si un processus est lancé, ou s'il ne doit pas être lancé, regardons cela de plus près :

Sur cette image sont présentés les différents matériels informatiques de notre réseau, celui qui nous intéresse ici est le FID085.



On fait clic droit dessus et on va cliquer sur État du périphérique.



Ce qui va nous mener à ceci :



Sur cette page est présent plein d'informations, le temps de réponse des pings, l'état des analyseurs ainsi que leurs pourcentages de fonctionnement.

Commençons maintenant à ajouter ce que l'on appelle un « Analyseurs Actifs » en cliquant sur les 3 traits sur l'image pour accéder aux propriétés.



Propriétés du périphérique	📦 FID085 💌								☆	v 2	; m	≣.	C
V Device Overview													
	Nom complet Modifier FID085	OS Modifie Windows 11	r		État du D périphérique	isponible							
	Nom d'hôte Modifier FID085.legraet.corp Adresse IP Configurer les interfaces réseau			Marque Mo	odifier		Fichier : Indisponib	le au moins 20 minutes					
Conserver les détails à jour				Rôle Modifi Windows Des	l er :ktop		Notes Modifier						
ID d'objet SNMP Modifier la personnalisation			Stratégie d'ac (aucune strat	itratégie d'action Modifier This device was scanned by discovery on 13/12/2024 16:57 aucune stratégie d'action sélectionnée)				:40.					
Analyseurs (9)	Tous les analyseurs (9)	Analyseurs actif	fs (4) Analyseurs de p	erformances (5)	Analyseur	s passifs (0)							
Interrogation	🕂 👻 🥒 📋 Activer	Désactiver	Installation critique (Désac	tivé) 🗌 Masq	uer les analyse	urs désactivés 🗌 Regroupem	ent intelligent 🛛			Rechercl	her		
Actions	Analyseur	É	État	Activé	Critique	Intervalle d'interrogation	Actions & Policies app	lied Thresholds applied	ÉI	éments	hors se	uil	
Informations d'identification (1)	🗌 🛷 CPU Utilization			Oui		10 Minutes		Performance CPU Utilizati	c)			
Groupes (16)	Disk Utilization			Oui		10 Minutes		Performance Disk Utilizati	c)			
Attributs (14)	Eichier Test if ;500		Down at least 20 min	Oui	Non	60 secondes (Par défaut)							
Rôles (3)	🗌 🛅 Fichier Test oui		 Up at least 5 min 	Oui	Non	60 secondes (Par défaut)							
Inventaire	Interface Utilization			Oui		2 Minutes		Performance Interface Uti	c)			
Actualiser la chronologie	Memory Utilization			Qui		10 Minutes		Performance Memory au	1				
Liens (1)	C Ping			0	Nee	60 (D d-f)							
Agent			• Op at least 5 min	Our	NON	ou secondes (Par delaut)							
Applications (0)	Ping Latency and Avail	lability		Oui		10 Minutes		2 Seuils 🛕	C)			
Journaux (0)	processus test		Down (Down for 1 min)	Oui	Non	60 secondes (Par défaut)							

du poste, le domaine, son LP, son US etc... Pour ajouter un nouvel élément actif on va aller dans la bibliothèque :

					Ŷ	💄 brieuc	AIDE
			☆	♥;	C III =' Biblio	⑦ □ X	
État du périphérique	Disponible						0 E.
Fichier : Indispo	nible au moins 20 minutes						
Notes Modifier	r						u <u>bavantage</u>
This device was	scanned by discovery on 1.	3/12/2024 1	6:57:40.				
							0 E

Et ensuite -> Bibliothèque d'analyseurs. On fait « + » et Analyseurs actifs

On a donc maintenant accès à plein de types d'analyseurs, des analyseurs actifs PowerShell, SSH, un d'imprimante, de dossier etc... Pour cet exemple celui qui va nous intéresser ici est

l'analyseur de processus

Sélection d'un type d'analyseur actif

Les analyseurs actifs vous permettent de vérifier l'intégrité, de simuler des événements utilisateur et de tester des conditions spécifiques.

② ×

Nom de l'analyseur	Rechercher	Q
Analyseur de contenu HTTP	,	
Analyseur de dossier		
Analyseur de gigue inter-arr	rivée ping	
Analyseur de lecteurs de dis	sque de stockage	
Analyseur de processus		
Analyseur de propriétés de	fichiers	
Analyseur de radio WAP		
Analyseur de requêtes SQL		
Analyseur de ressources ba	sées sur le cloud	
		Ŧ

Description

Sélectionner un analyseur actif à afficher



On sélectionne, et on configure :

iounier Analyseur de processus	• /
Nom	
Processus Taskmgr	
Description	
Cette analyseurs vas analyser si le gestionnaire de tâche est ouvert ou non	
✔ Utiliser lors d'une nouvelle analyse	
Protocole à utiliser	
O WMI	
O SNMP	
Nom du processus	
Taskmgr.exe	Parcourir
Surveiller la condition d'indisponibilité	
○ Si le processus est en cours	
 Si le processus n'est pas chargé 	

Précisons ce que l'on a fait, on a mis comme nom très explicitement le but de cet analyseur, avec une description. Le plus important est maintenant de déterminer quel protocole nous allons utiliser, dans ce cas nous allons utiliser pour tout ce qui est poste informatique le protocole WMI.

Mais qu'est-ce que le WMI ?

Annuler

Enregistrer

WMI (Windows management instrumentation) est un système de gestion interne de Windows qui permet de contrôler et surveiller les ressources systèmes.

Ce qui va donc nous servir pour récupérer les informations. Ensuite il faut préciser le nom du processus à surveiller. Comme nous l'avons dit précédemment nous allons donc surveiller le gestionnaire de tâche. Ensuite le paramètre suivant est déterminant, c'est la cause à effet qui va déterminer si nous

serons dans le vert ou si nous serons dans le rouge. Dans cet exemple nous allons donc cocher la case « Si le processus n'est pas chargé ». Il faut donc que le processus soit ouvert pour que tout aille bien.

Mais nous aurions aussi pu faire l'inverse, par exemple faire en sorte que si tel processus soit ouvert alors une alerte aurait été déclenchée.

On peut maintenant faire terminer et nous allons retourner dans les propriétés du périphérique pour appliquer l'analyseur.

On fait le + et on va sélectionner dans la liste l'analyseur qu'on a créé :



On fait suivant et terminer.

Maintenant retournons sur la page d'état de notre périphérique. On peut maintenant voir dans la partie « state change timeline » nos analyseurs. On voit donc sur l'image l'analyseur que nous avons créé et son état, par exemple le gestionnaire de tâches n'a pas été ouvert pendant 10 min, l'état est donc passé au rouge, je l'ai donc réouvert et là l'état est passé au vert.

9	✓ Monitoring	0085 -									습
/Memo	= <u>a</u> q			-							
d`heu	Processus		Exécuter u	une nouvelle t	tâche •••	 ✓ State Change Timeline Aujourd'hui ▼ ★ 					¢
			10%	84%	~́2%	Analyseur	Heure de dét	ut 🖡 Durée	État	Message	
	Nom	Statut	Processeur	Mémoire	Disque	Processus Taskmgr	01/29/2025 9	:33:55 6 min	Up at	processus test:PayLoad=succeeded	
	🔲 System		0,6%	0,1 Mo	1,6 Mo/s	Processus Taskmgr	01/29/2025 9	:28:50 5 min	Up	processus test:PayLoad=succeeded	
	> M Gestionnaire des tâches		2,0%	41,2 Mo	0,5 Mo/s	*** Processus Taskmør	01/29/2025 9	18·44 10 min	Dow	The process "Taskmgr.exe" was not running when it shou Moi	15
	🚬 Explorateur Windows		0%	102,8 Mo	0,2 Mo/s	i locessos roskingi	01/25/2025 5		Down	FAILED.	
	> 🏥 SentinelOne Agent		0%	112,6 Mo	0,1 Mo/s	Drocassus Tashmer	01/20/2025.0	03-20 15 min	Dow	The process "Tackmar ave" was not running when it should be	-*
	> 🔝 appmodel		0%	9,2 Mo	0,1 Mo/s	V Down Active Monitors					Φ
	Gestionnaire de fenêtres du B		0,5%	49,5 Mo	0,1 Mo/s	Analyseur	Date de début	Durée	État	Message	
	> 🔀 Rechercher (4)		0%	8,9 Mo	0,1 Mo/s	Fichier Test if ;500	01/28/2025 3:33:13 pm	18 h 30 min 2	6 s Indisponible au moins 20 mi	\\fls01\mesdocuments\$\ exists.Actual folder size (3750786	avant
02:00	> 🥑 Microsoft Management Cons		0%	7,3 Mo	0,1 Mo/s						

Mais comme nous l'avons dit précédemment nous aurions pu échanger de procéder, faire en sorte que si le gestionnaire soit ouvert, alors le state serait passé au rouge, alors que s'il avait été fermé il serait au vert. Encore une fois ceci était un test, mais nous pourrions faire ça avec d'autres processus cela pourrait être n'importe quoi, comme un antivirus par exemple etc...

Nous pouvons aussi le faire avec des services Windows, par exemple si nous cherchons les services activés dans Windows, on pourrait prendre par exemple le Fusion Inventory

🌼 Services					-		\times
Fichier Action At	ffichage ?						
(= → 📰 📴 🕻	i 📑 🛛 📷 🕨 🔳 💵 🕨						
🔍 Services (local)	🔍 Services (local)						
	FusionInventory Agent Description : Service FusionInventory Agent.	Nom Fichiers hors connexion Filtre clavier Microsoft Flux d'appareils_840a9eb Flux d'appareils_e747743 Fournisseur de cliché instan FusionInventory Agent GameInput Service Générateur de points de ter Gestion à distance de Wind Gestion d'applications Gestion des niveaux de stoc Gestionnaire d'installation d Gestionnaire d'installation d	Description Le service Fi Contrôle le Permet à C Gère les cop Service Fusi Enables key Gère les péri Le service G Traite les de Optimise le Active la dé Fournit des	État En co En co En co En co En co En co	Type de dén Automatiqu Désactivé Manuel Manuel Manuel Automatiqu Automatiqu Automatiqu Manuel Manuel Manuel Manuel Manuel Manuel Manuel	narrage Ie (décle. Le clenche. Je Je Je (débu, Sclenche,	
		Gestionnaire de comptes de Gestionnaire de comptes web Gestionnaire de session loc Gestionnaire des cartes télé Gestionnaire des connexion	Ce service e Service Win Service Win Crée une co	En co En co En co	Automatiqu Manuel Automatiqu Automatiqu Manuel	ie je je (débu.	
	\Etendu (Standard /						

Maintenant reprenons les étapes antérieures. La seule subtilité ici est que nous n'allons pas prendre le même type d'analyseurs.

On va dans les propriétés du périphérique, et on va dans la bibliothèque.



Et on va sélectionner dans la liste comme nouveau analyseur celui de service :

Sélection d'un type d'analyseur actif 🛛 🗇 🗙							
Les analyseurs actifs vous permetter des conditions spécifiques.	nt de vérifier l'intégrité, de simuler des événements utilisateur et de tes	ter					
Nom de l'analyseur	Rechercher	Q					
Analyseur de requêtes SQL							
Analyseur de ressources ba	sées sur le cloud						
Analyseur de script actif							
Analyseur de service							
Analyseur de statistiques réseau							
Analyseur de système de fie	thiers de stockage						
Analyseur de température							
Analyseur de test ping		Ŧ					
Description							
L'analyseur de service vérifie l'état d Le redémarrage du service peut se p existent. Veuillez noter que le périph (Windows Management Instrumenta	'un service sur une machine Windows et tente de redémarrer ce servic roduire uniquement si les autorisations administrateur appropriées érique à surveiller pour un service doit répondre aux protocoles WMI tion) ou SNMP (Simple Network Management Protocol).	e.					

5	électio	nner	Annuler							
0r	va	le	nommer,	le	décrire	et	activer	le	protocole	WMI.

Ajouter Analyseur de service

	Nom						
	Service FusionInventor	у					
	Description						
	Cet analyseur vas déte	cter si le service Fusion Inve	entory est en mare	che ou non			
	✓ Utiliser lors d'une no	uvelle analyse					
	🗌 Redémarrer en cas d	'échec					
	Protocole à utiliser						
	O WMI						
	O SNMP						
	Nom du service						
	FusionInventory Agent				Parcourir		
	Note:					_	
	Selecting Multiple Servic Name]".	es: Creates multiple monito	ors, using the form	nat "[User-given name]] - [Service		
	Selecting Single Service:	Creates a single monitor w	ith the specified u	ser-given name.			
	Enregistrer Annu	ller					
0	n va mainter	nant aller ch	nercher :	le nom du	service	en fa	isant
«	parcourir >	».					
0	n enregistre	e et on fait	le même	procédé q	ue la pi	remièr	e fois.
	-						
🗌 🗼 Service Fusionl	nventory		🌒 Up		Oui	Non	60 secondes (Par défaut)
E	t notre serv	vice marche H	bien !				
Service FusionInv	ventory	01/31/2025 8:54:40 3	3 min	Up	Service Fusion service is in Ru	Inventory:Pay Inning state.	Load="FusionInventory Agent" Moin

Nous avons donc testé les services et les processus, maintenant intéressons-nous au contenue d'un dossier ou d'un disque par exemple. Si nous aurions envie de surveiller un fichier, son existence, sa taille etc… c'est possible, essayons de créer une panne

Nous allons réutiliser les mêmes procédés qu'avant, on va sélectionner l'analyseur de dossier :

Sélection d'un type d'analyseur actif

Les analyseurs actifs vous permettent de vérifier l'intégrité, de simuler des événements utilisateur et de tester des conditions spécifiques.

② X

Nom de l'analyseur	dossier	×
Analyseur de dossier		

Et lui paramétrer ce que l'on souhaite

Dans ce cas, les chiffres sont bien évidemment démesurés, le but est bien de créer une panne.

✓ Down Active Monitors								
Analyseur	Date de début	Durée 🕇	État	Message				
Fichier Test if ;500	01/28/2025 3:33:13 pm	2 jours 18 h 17	Indisponible au moins 20 min	\\fis01\mesdocuments\$\ exists.Actual folder size (375078 <u>Moins</u> 654,49 KB) is greater than the threshold set (620 KB) Folder size on disk (375563736 KB) is greater than the thr eshold set (655 KB) Number of files in the folder (239546) is NOT less than th e threshold set (9) FAILED				

Et comme on peut le voir, l'analyseur est dans la partie « Down active monitor » en mettant ce message :

« fls01mesdocuments\$ existe. La taille réelle du dossier (375078654,49 Ko) est supérieure au seuil défini (620 Ko) La taille du dossier sur le disque (375563736 Ko) est supérieure au seuil défini (655 Ko) Le nombre de fichiers dans le dossier (239546) n'est PAS inférieur au seuil défini (9) RATÉ »

Notre panne fonctionne donc bien.

 FID085	Fichier Test if ;500	Indisponible	100%	01/31/2025 12:00:00	9 h 27 mi

Maintenant, essayons de voir pour d'autres types de périphériques. Prenons l'exemple d'un switch. Je vais aller dans la section « mon réseau » de WhatsUp Gold et sélectionner un switch :



Allons sur sa page :

~	State Change Timeline				0	≣⁺
	Aujourd'hui 👻 🖈					
	Analyseur	✓ Heure de début ↓	Durée	État	at Message	
•	 Interface (17) 	01/31/2025 10:52:5	5 min	Dow	w Interface "17" (SNMP index 17) is Down. IfOperStatus value <u>Davant</u>	age
	 Interface (17) 	01/31/2025 10:37:4	15 min	Dow	ow Interface "17" (SNMP index 17) is Down. IfOperStatus value <u>Davant</u>	age
	Interface (17)	01/31/2025 10:34:4	3 min	Dow	ow Interface "17" (SNMP index 17) is Down. IfOperStatus value <u>@avant</u>	age
	Interface (17)	01/31/2025 10:32:4	2 min	Dow	own Interface "17" (SNMP index 17) is Down. IfOperStatus value <u>Davant</u>	age

On voit que le port 17 est down, ce qui signifie que cela pourrait par exemple être un ordinateur éteint, ce qui peut poser problèmes car à cause de cela tout l'état du périphérique passe au rouge

Pour cela nous allons y remédier en faisant une étape, on va dans ses propriétés et on va sélectionner le port 17.

Nom complet Modifier FIDSVT0401 Nom dhôte Modifier 1055.2.14		OS Modifier Not set HP Rôle Modifier Switch Stratégie d'action Modifier (aucune stratégie d'action sélectionnée)		État du Disponible périphérique 17: Indisponible au moins 20 minutes						
									Adresse IP Configurer les interfaces réseau F 10.55.2.14 S ID d'objet SNMP Modifier la personnalisation S 1.3.6.1.4.11.12.37.11.137 G	
This device was scanned by discovery on 13/12/2024 17:02:23.										
Tous les analyseurs (29)	Analyseurs actifs (25)	Analyseurs de per	formances (4) Analyseurs pass	ifs (0)						
+ 🖍 📋 Activer De	+ Activer Désactiver Installation critique (Désactivé)		Masquer les analyseurs désactivés Regroupement in		elligent		Rechercher	Q		
Analyseur	Argument	Commentaire	État	Activé	Critique	Intervalle d'interrogation	Actions & Policies applied			
🗌 🎆 Fan			Up at least 5 min	Oui	Non	60 secondes (Par défaut)				
Interface (1)	1	1	Up at least 5 min	Oui	Non	60 secondes (Par défaut)				
🗹 💷 Interface (17)	17	17	😑 Down at least 20 min (D	lown for 28 Oui	Non	60 secondes (Par défaut)				
🔲 🚽 Interface (2)	2	2	Up at least 5 min	Oui	Non	60 secondes (Par défaut)				
🗌 斗 Interface (21)	21	21	Up at least 5 min	Oui	Non	60 secondes (Par défaut)				
🔲 🛶 Interface (22)	22	22	Up at least 5 min	Oui	Non	60 secondes (Par défaut)				
🗌 🛶 Interface (23)	23	23	Up at least 5 min	Oui	Non	60 secondes (Par défaut)				
Interface (25)	25	25	D Unknown	Non	Non					

Et on va désactiver l'interrogation de l'appareil :

omple	propriétés des analyseurs actifs X	
T047	sactive Activer l'interrogation pour cet analyseur actif	5
2.14	Interface réseau à utiliser pour cette interrogation	
ie IP [Utiliser l'interface réseau par défaut	
ojet SN .4.1.1	✓ Avancé	y on 13
- 1	Argument	
	17	
ous le	Comment	
1	17	
nalyse	🗌 Utilisez une fréquence d'interrogation indépendante pour cet analyseur.	d'inter
🛞 Fa		des (Pa
🔔 In		des (Pa
L, In		des (Pa
🔔 In		des (Pa
🔔 In		des (Pa
🔔 In		des (Pa
J. In		des (Pa
J., In		
L, In		des (Pa
🔔 In	Précédent Subrant Terminer Annuller 1 monitor(s) selected	des (Pa

L'état du switch est repassé au vert et sans erreur :

Propriétés du périphérique	♥ FIDSWT0401 ▼					
V Device Overview						
Conserver les détails à jour	Nom complet Modifier FIDSWT0401 Nom d'hôte Modifier 10.55.2.14 Adresse IP Configurer les interfaces réseau 10.55.2.14 ID d'objet SNMP Modifier la personnalisation 1.3.6.1.4.1.11.2.3.7.11.137			OS Modifier Not set Marque Modifier HP Rôle Modifier Switch Stratégie d'action Modifier (aucune stratégie d'action sélectionnée)		
Analyseurs (29)	Tous les analyseurs (29)	Analyseurs actifs	s (25)	Analyseurs de per	formances (4)	Analyseurs passifs (0)
Interrogation	+ 🖍 📋 Activer	Désactiver Ins	tallation c	ritique (Désactivé)	Masquer les	analyseurs désactivés 🗌 R
Actions	Analyseur	Ar	gument	Commentaire	État	

		(unarjocaro acciro (20)	· · · · · · · · · · · · · · · · · · ·	·····
Interrogation	🕇 💉 📋 Activer	Désactiver Installation c	ritique (Désactivé) 🗌 Ma	asquer les analyseurs désactivés 🗌 R
Actions	Analyseur	Argument	Commentaire	État
Informations d'identification (1)	🗆 🛞 Fan			Up at least 5 min
Groupes (13)	🗌 🚽 Interface (1)	1	1	Up at least 5 min
Attributs (14)	🗌 🚽 Interface (17)	17	17	D Unknown