

# Observer Infrastructure

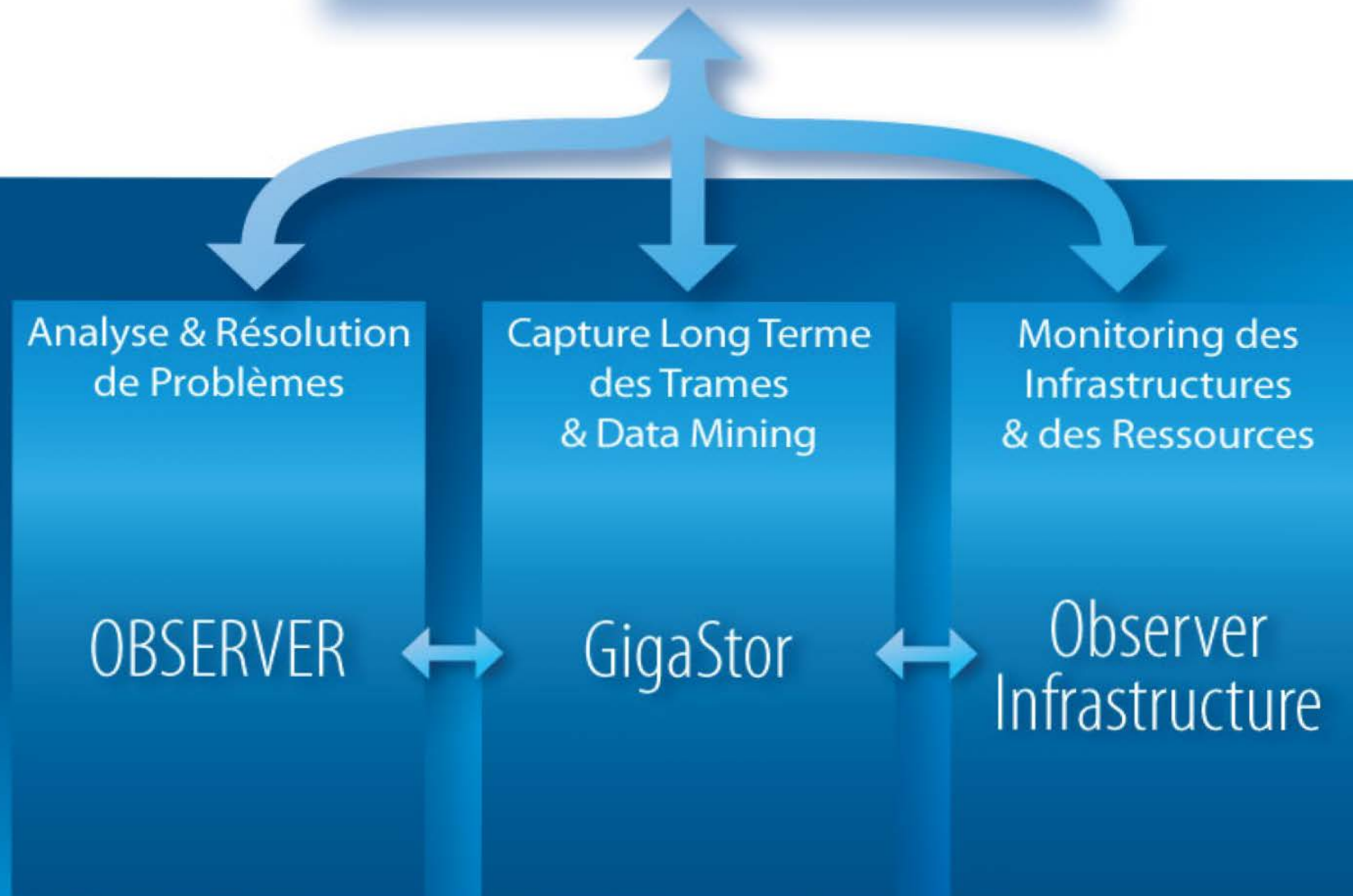
(Anciennement "Link Analyst")

**ELEXO**

20 Rue de Billancourt  
92100 Boulogne-Billancourt  
Téléphone : 33 (0) 1 41 22 10 00  
Télécopie : 33 (0) 1 41 22 10 01  
Courriel : [info@elexo.fr](mailto:info@elexo.fr)  
TVA : FR00722063534

# Observer Reporting Server

Monitoring Aggrégé des Performances



# Observer Infrastructure

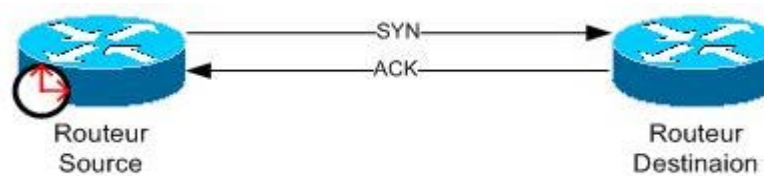
- Remplace Link Analyst
- Désormais conçu pour fournir des informations à ORS
- Architecture distribuée
- Utilise SNMP, WMI, IP SLA, WAAS, Ping, TraceRT, Transactions synthétiques, WSD, et NBAR
- Utilisé en tant que produit seul ou intégré à ORS

# Les nouveautés

- Fonctionne en service Windows
- Alarmes supplémentaires en SNMP et Syslogs
- Rapports planifiés
- IP SLA, NBAR, WSD, WAAS et Transactions Synthétiques
- Encore plus de moniteurs prédéfinis :
  - Cisco NBAR
  - Citrix Secure Gateway
  - Exchange Server 2000, 2003, et 2007
  - IP SLA
  - VMware ESX Server
  - WAAS Core et Edge Server
  - Wireless Access Point

# Cisco Internet Protocol Service Level Agreements

- Analyse les niveaux de service pour les applications et services IP
- Utilise une technologie de monitoring active



- Mesures périodiques des routeurs ou commutateurs afin de générer des métriques de performance réseau et de services

DHCP	HTTP (Raw)	LSP Path Echo	UDP Jitter
DLSw+	ICMP Echo	Metro-Ethernet Echo	UDP Jitter for VoIP
DNS	ICMP Jitter	Metro-Ethernet Jitter	VoIP Call Setup (Post-Dial Delay)
FTP	ICMP Path Echo	TCP Connect	VoIP Gatekeeper Registration Delay
HTTP (Get)	LSP Echo	UDP Echo	VoIP RTP-Based

- Observer Infrastructure interroge routeurs et commutateurs en SNMP pour récupérer les résultats des tests

# Observer Infrastructure : Equipements IP SLA



## Discovered IP SLA Operations Report


**Device Group:** NI-US  
**Report Generated:** 2010/04/25 22:22:07  
**Last Poll Time:** 2010/04/25 22:21:50

Device ▲ (IP)	Type	Monitors						
		N	S	A	✓	!	!	?
IP_SLA_1 (10.0.38.180)	Router	--	--	--	--	--	--	--
IP_SLA_1 (10.0.192.1)	Router	--	--	--	--	--	--	--
IP_SLA_2 (10.0.192.2)	Router	--	--	--	--	--	--	--
IP_SLA_2 (10.0.193.1)	Router	--	✓	--	63	--	--	--
NI_VOIP_2851.netinst.com (10.0.240.9)	Router	--	✓	--	63	--	--	--
NICat6506 (10.0.32.1)	Wireless Access Point	--	--	--	--	--	--	--
	Switch	--	--	--	--	--	--	--


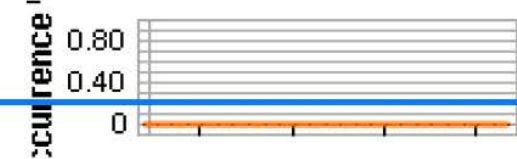
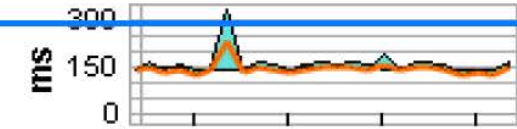
# Observer Infrastructure : Operations IP SLA



## Discovered IP SLA Operations Report for IP\_SLA\_2

<b>Business Group:</b>	NI-US
<b>Report Generated:</b>	2010/04/25 22:25:54
<b>Device:</b>	 IP_SLA_2
<b>Network Address:</b>	10.0.192.2
<b>Monitor:</b>	Discovered IP SLA Operations

### Discovered IP SLA Operations:

Monitor Element	Object (Index)	Monitor Category	Status	Value	Last 4 Hours	Time
Discovered DNS - Availability	www.cisco.com	System	✓	100 Availability %		2010/04/25 22:22:02
Discovered DNS - Connection loss occurred	www.cisco.com	System	✓	0 Occurrence %		2010/04/25 22:22:02
Discovered DNS - Latest RTT	www.cisco.com	System	✓	153 ms		2010/04/25 22:22:02



# Observer Infrastructure :

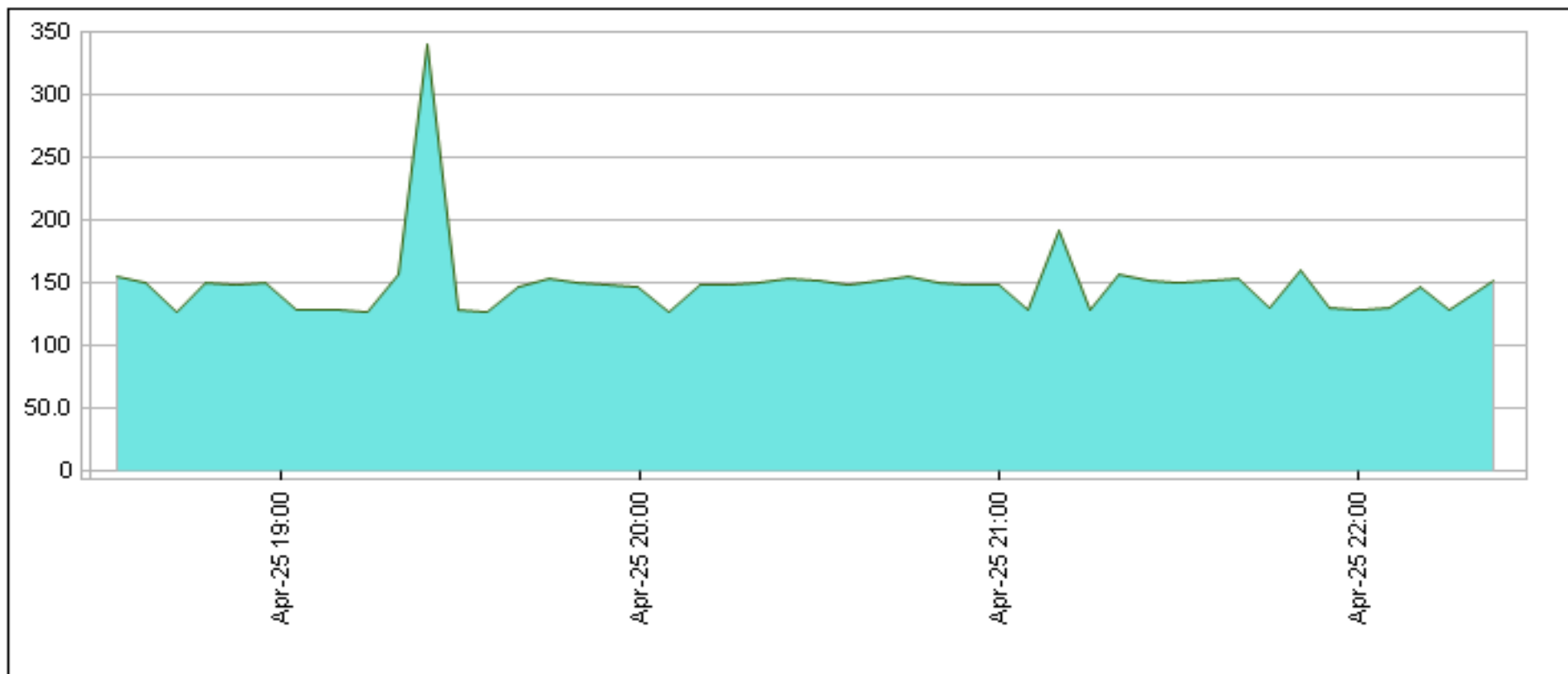
## Historique des opérations IP SLA



### Discovered DNS - Latest RTT Report

Device Group:	NI-US
Device:	IP_SLA_2
Network Address:	10.0.192.2
Monitor Item:	Discovered DNS - Latest RTT -- "www.cisco.com"
Reporting Period:	last 4 hours
Start Time:	2010/04/25 18:28:00
End Time:	2010/04/25 22:27:48

Discovered DNS - Latest RTT -- "www.cisco.com"






# Network Based Application Recognition (NBAR)

- Mécanisme utilisé par les routeurs Cisco pour reconnaître un flux de données en inspectant les paquets envoyés
- Observer Infrastructure interroge le routeur en SNMP pour obtenir les statistiques
- Fournit les statistiques de volume des protocoles par port

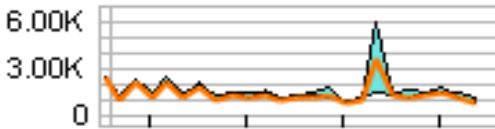
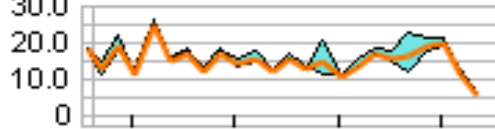
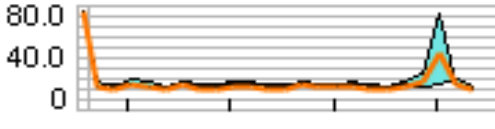
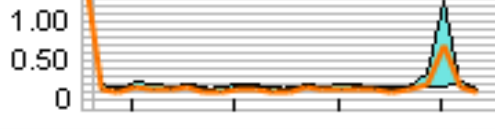
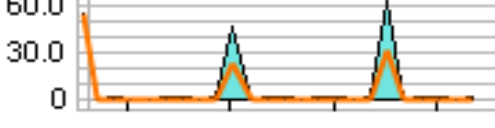
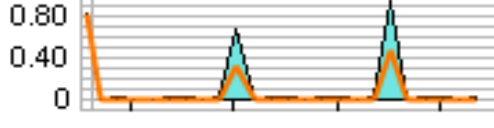
# Observer Infrastructure : Volume par Protocole par Interface



## Cisco NBAR Raw Protocol Report for NI\_GW\_2851.netinst.com

Business Group:	NI-US
Report Generated:	2010/04/25 22:35:12
Device:	 NI_GW_2851.netinst.com
Network Address:	10.0.1.1
Monitor:	Cisco NBAR Raw Protocol

### Protocol Statistics

Monitor Element	Inbound bytes/sec ( Bytes/Sec )		Inbound packets/sec ( Pkts/Sec )	
GigabitEthernet0/0_http	✓ 931,128		✓ 5,194	
GigabitEthernet0/0_icmp	✓ 8,089		✓ 0,097	
GigabitEthernet0/0_imap	✓ 1,969		✓ 0,026	

# Observer Infrastructure :

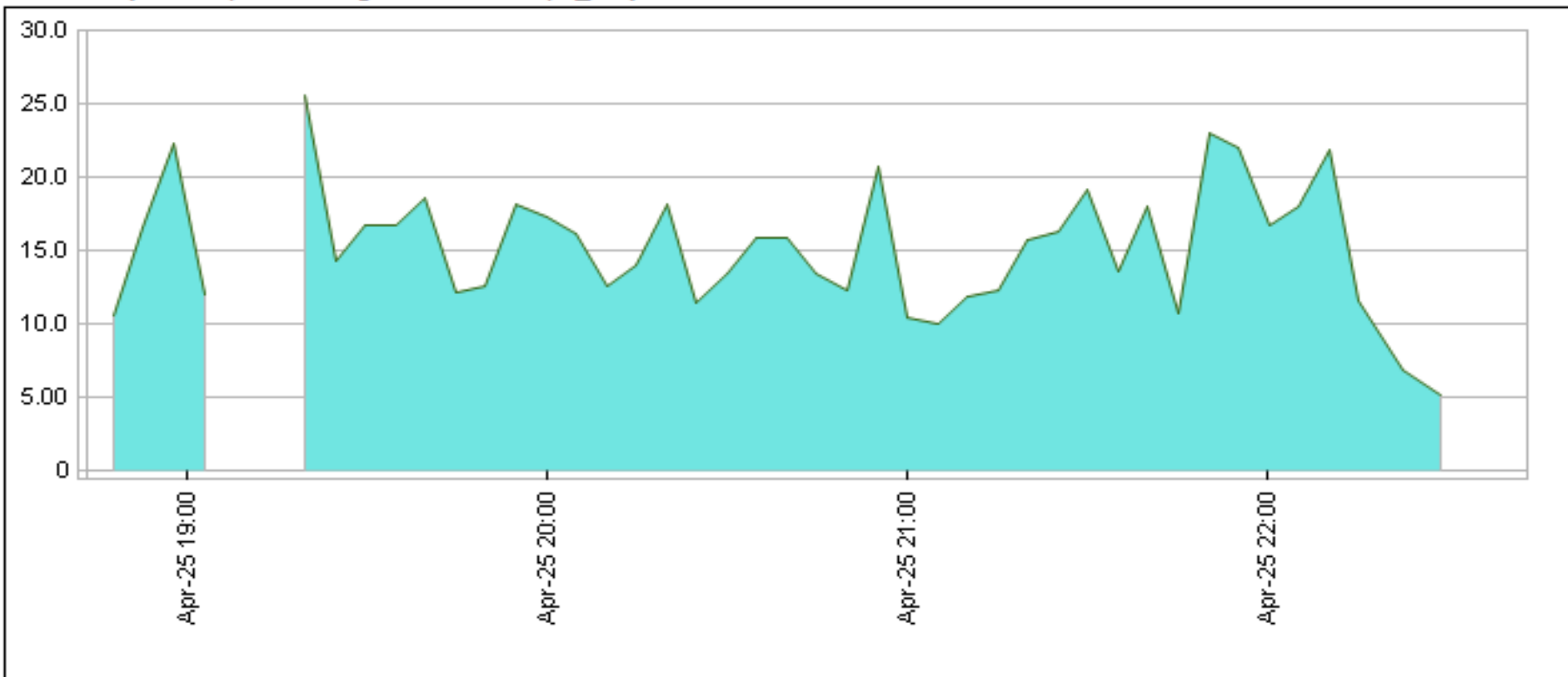
## Historique de l'utilisation des protocoles



### Inbound packets/sec Report

<b>Device Group:</b>	NI-US
<b>Device:</b>	NI_GW_2851.netinst.com
<b>Network Address:</b>	10.0.1.1
<b>Monitor Item:</b>	Inbound packets/sec -- "GigabitEthernet0/0_http"
<b>Reporting Period:</b>	last 4 hours
<b>Start Time:</b>	2010/04/25 18:43:00
<b>End Time:</b>	2010/04/25 22:43:00

Inbound packets/sec -- "GigabitEthernet0/0\_http"




# Web Services on Devices (WSD)


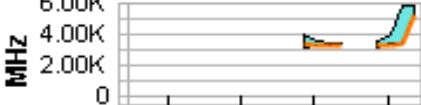
- Découverte et accès aux périphériques distants et aux services associés au travers du réseau
- Observer Infrastructure interroge les informations concernant les ressources comme la CPU et la mémoire



## VMware ESX Server-Host (WSD) Report for QA-ESX.netinst.com

Business Group:	NI HQ
Report Generated:	2010/04/23 16:26:25
Device:	 QA-ESX.netinst.com
Network Address:	10.0.38.82
Monitor:	VMware ESX Server-Host (WSD)

### VMware ESX Server-Host (WSD):




Monitor Element	Object (Index)	Monitor Category	Status	Value	Last 4 Hours
Host CPU - Usage MHz	<a href="#">QA-ESX.netinst.com ([Total])</a>	System		5105 MHz	

# Résumé des machines virtuelles d'un VM Host



## VMware ESX Server-VM (WSD) Report


**Device Group:** NI HQ  
**Report Generated:** 2010/04/25 08:15:00  
**Last Poll Time:** 2010/04/25 08:14:20

Device ▲ (IP)	Type	Monitors						
		N	S	A	✓	!	!	?
 10.0.40.51	VMware Virtual Server	--	✓	--	92	--	--	--
 QA-ESX.netinst.com (10.0.38.82)	VMware Virtual Server	--	--	--	--	--	--	--
 sander-vm40.netinst.com (10.0.38.223)	VMware Virtual Server	--	✓	--	226	--	--	--

# Détail de chaque machine virtuelle



## VMware ESX Server-VM (WSD) Report for sander-vm40.netinst.com

<b>Business Group:</b>	NI HQ
<b>Report Generated:</b>	2010/04/25 08:18:21
<b>Device:</b>	 sander-vm40.netinst.com
<b>Network Address:</b>	10.0.38.223
<b>Monitor:</b>	VMware ESX Server-VM (WSD)

### Virtual Machines:


Virtual Machine	Guest OS	Memory Size	State	Monitors						
				N	S	A	✓	!	!	?
252 W764 OBS v14.1	Microsoft Windows 7 (64-bit)	1280 (MB)	ON	--	✓	--	21	--	--	--
XP64_BASE3	Microsoft Windows XP Professional (64-bit)	800 (MB)	OFF	--	--	--	--	--	--	--
226 W764 NIMS v14.1	Microsoft Windows 7 (64-bit)	768 (MB)	ON	--	✓	--	21	--	--	--
W764_BASE	Microsoft Windows Vista (64-bit)	1280 (MB)	OFF	--	--	--	--	--	--	--
232 2KSV V12	Microsoft Windows 2000 Server	640 (MB)	OFF	--	--	--	--	--	--	--
231 UBUNTU sFlow	Ubuntu Linux (32-bit)	640 (MB)	ON	--	✓	--	18	--	--	--
228 XP32 OBS v14.0	Microsoft Windows XP Professional (32-bit)	1536 (MB)	OFF	--	--	--	--	--	--	--
238 0864	Microsoft Windows Server 2008 (64-bit)	1024 (MB)	ON	--	✓	--	21	--	--	--
vCenter Server	Microsoft Windows XP Professional (64-bit)	1024 (MB)	ON	--	✓	--	21	--	--	--




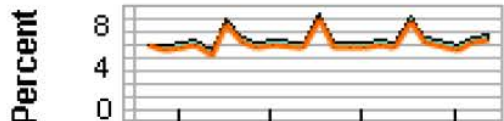

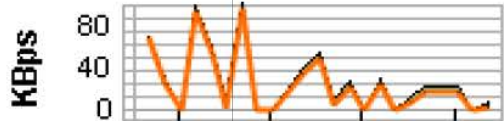
# Détails des ressources des machines virtuelles



## VMware ESX Server-VM (WSD) Report for sander-vm40.netinst.com

<b>Business Group:</b>	NI HQ
<b>Report Generated:</b>	2010/04/25 08:23:26
<b>Device:</b>	 sander-vm40.netinst.com
<b>Network Address:</b>	10.0.38.223
<b>Monitor:</b>	VMware ESX Server-VM (WSD)
<b>Virtual Machine:</b>	252 W764 OBS v14.1

### VMware ESX Server-VM (WSD):

Monitor Element	Monitor Category	Object (Index)	Status	Value	Last 4 Hours	Time
VM CPU - Utilization %	System	252 W764 OBS v14.1 ([Total])		4.430 Percent		2010/04/25 08:00:20
VM Disk - Reads KBps	System	252 W764 OBS v14.1 ([Total])		0 KBps		2010/04/25 08:00:20



# Wide Area Application Services (WAAS)

- Combinaison de services d'optimisation WAN et d'accélération des applications basées sur TCP et des fichiers
- Présente des difficultés pour le monitoring
- Observer Infrastructure utilise SNMP pour rassembler les statistiques des Serveurs de cœurs et de périphérie:
  - Taux de compression
  - Volume du trafic reçu et envoyé
  - Messages reçus et envoyés
  - Lecture et écriture
  - Sessions connectées
  - Fichiers ouverts
  - Demandes distantes

# Moniteur WAAS

- Établir des performances avant et après déploiement.
- Comparer la performance d'une application optimisée de celle non-optimisée.
- Vérifier l'amélioration attendue des performances.

Monitor Elements ▲	Alarm Condition	Response	
		Alarmed	Back to normal
CoreServer Received - Compression Ratio			
CoreServer Received - KBytes/sec			
CoreServer Received - Messages/sec			
CoreServer Sent - Compression Ratio			
CoreServer Sent - KBytes/sec			
CoreServer Sent - Messages/sec			
CoreServer Status - Connection			
CoreServer Status - Running			

Monitor Elements ▲	Alarm Condition	Response	
		Alarmed	Back to normal
EdgeServer Cache - Current Resources			
EdgeServer Cache - Current Volume			
EdgeServer Cache - Disk Space Utilization			
EdgeServer Cache - Evicted Age			
EdgeServer Cache - Resources Evicted/sec			
EdgeServer Cache - Resources Utilization			
EdgeServer CIFS - Bytes Read/sec			
EdgeServer CIFS - Bytes Written/sec			
EdgeServer CIFS - Connected Sessions			
EdgeServer CIFS - Local Requests %			
EdgeServer CIFS - Local Requests/sec			
EdgeServer CIFS - Local Time %			
EdgeServer CIFS - Open Files			
EdgeServer CIFS - Remote Requests/sec			
EdgeServer Received - Compression Ratio			
EdgeServer Received - KBytes/sec			
EdgeServer Received - Messages/sec			
EdgeServer Sent - Compression Ratio			
EdgeServer Sent - KBytes/sec			
EdgeServer Sent - Messages/sec			
EdgeServer Status - Connection			
EdgeServer Status - Running			

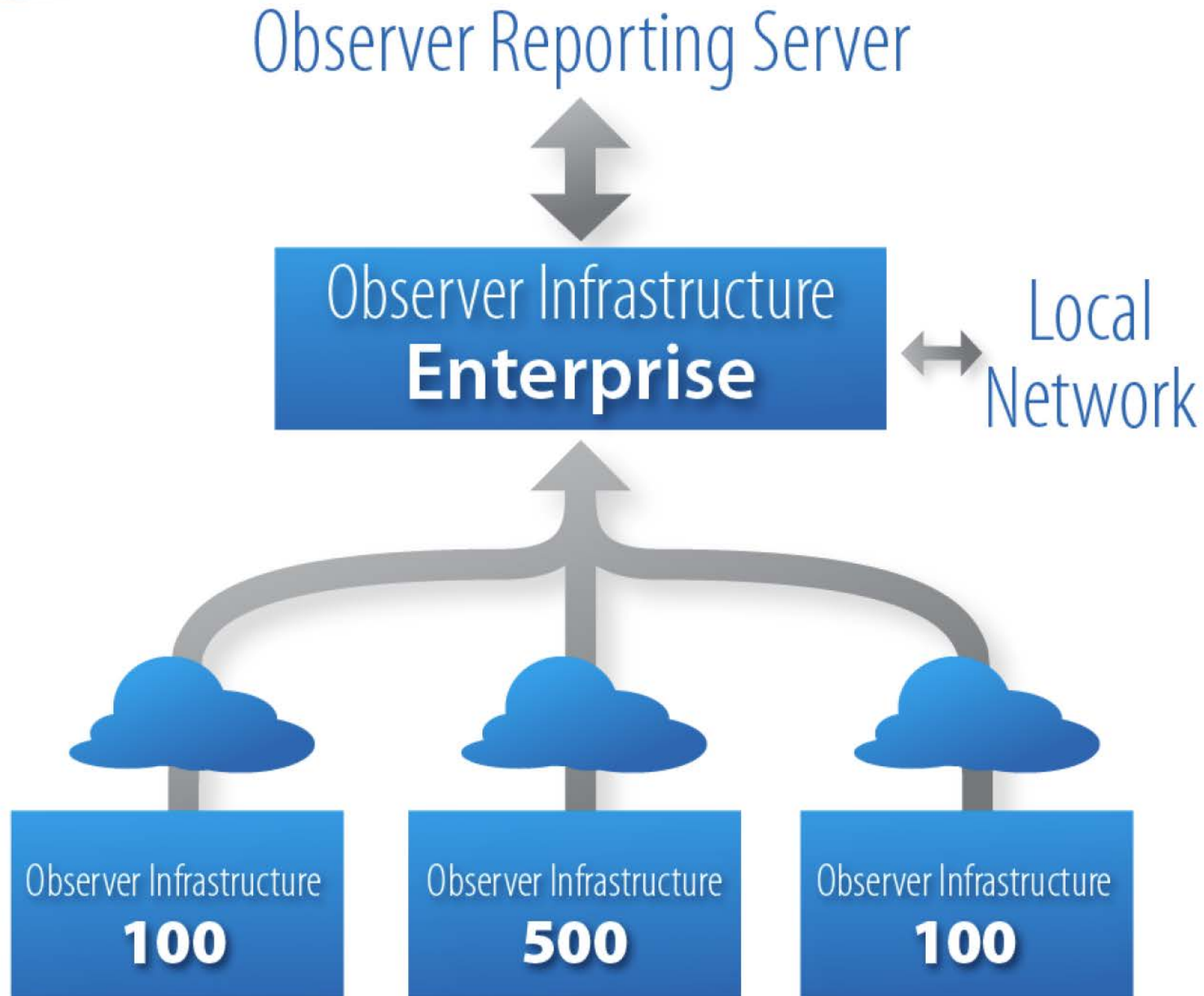
# Transactions synthétiques

- Allez plus loin que l'interrogation d'ouverture de socket
- Permet de traquer si un services particulier est fonctionnel ou non
- Permet d'obtenir une vue détaillée des services
- Permet de tester les réponses aux messages applicatifs
- Permet d'écrire des requêtes spécifiques et personnalisables

# Surveillance des services au travers des transactions synthétiques

Program Options					
Monitors		Notifications		Probes	
General		Alarm Responses		Data Management	
Discovery		Global Inventory Alarms		IP Applications	
Reports		Schedules		Inventory Objects	
Service	Type	Port	Description	Script	
DNS(UDP)	UDP	53	Domain Name Service(UDP)		Add...
FTP	TCP	21	File Transfer Protocol	Expect="^220";Send="QUIT\r\n";	Edit...
HTTP	TCP	80	Web Service	Send="HEAD / HTTP/1.0\r\nAccept: */*\r\nUser-Agent: Mozil	Remove
LPD	TCP	515	Printer Connection		Reset
NNTP	TCP	119	USENET News Transfer Protocol	Expect="^2";Send="QUIT\r\n";	
POP3	TCP	110	Post Office Protocol	Expect="^.+OK";Send="QUIT\r\n";	
SMTP	TCP	25	Simple Mail Transport Protocol	Expect="^2";Send="QUIT\r\n";	
SNMP	UDP	161	Simple Network Management Protocol		
TELNET	TCP	23	Terminal Connection		
HTTPS	TCP	443	HTTP-Secure Sockets Layer (SSL/T...	Send="\$SSL_CLIENT_HELLO\$";Expect="\$SSL_SERVER_HE	
GOPHER	TCP	70	Internet Gopher Protocol	Send="\r\n";Expect="(.+)";	
SSH	TCP	22	Secure Shell Protocol	Expect="^SSH";	
IMAP4	TCP	143	Internet Message Access Protocol V4	Expect="^\" OK\"";	
RTSP	TCP	554	Real Time Streaming Protocol	Send="OPTIONS * RTSP/1.0\r\nCSeq: 1\r\n\r\n";Expect="^F	
SNPP	TCP	444	Simple Network Paging Protocol	Expect="^2";Send="QUIT\r\n";	
RADIUS	UDP	1812	Remote Authentication Dial In User S...		
IMAP(SSL/TLS)	TCP	993	IMAP-Secure Sockets Layer (SSL/TLS)	Send="\$SSL_CLIENT_HELLO\$";Expect="\$SSL_SERVER_HE	
POP3(SSL/TLS)	TCP	995	PDP3-Secure Sockets Layer (SSL/T...	Send="\$SSL_CLIENT_HELLO\$";Expect="\$SSL_SERVER_HE	
DNS(TCP)	TCP	53	Domain Name Service(TCP)		
Lotus Notes	TCP	1352	IBM Lotus Notes		

# Observer Infrastructure - Déploiement





# Observer Infrastructure - Déploiement

Observer Infrastructure - [10.0.36.156:Netinst.com]

File Edit View Tools Window Help

Business Groups/Routes:

- Local Business Groups
  - Just Netinst
  - New NI on 7-10
  - NI-World
  - NOC
  - Training App
  - 10.0.36.156
  - Netinst.com
  - NI UK

Monitoring Topology Discovery Inventories

Reports Monitoring Map Devices IP Services Response Times

	State	Device	Type	Critical	IP Address	NIC Address	DNS Name	Microsoft Na
1		NI_GW_2851.netinst.com	Wireless Access Point	<input type="checkbox"/>	10.0.1.1	00:15:62:95:21:39		
2		NICat6506	Switch	<input type="checkbox"/>	10.0.1.4	00:D0:2B:A1:BA:C0		
3		IP_SLA_1	Router	<input type="checkbox"/>	10.0.38.180	00:0C:85:BD:08:80		
4		wap54g	Router	<input type="checkbox"/>	10.0.38.229	00:06:25:3C:09:91		
5		Upstairs_Dell_6200	Switch	<input type="checkbox"/>	10.0.32.3	00:21:9B:B7:67:72		
6		CiscoSwitch.netinst.com	Switch	<input type="checkbox"/>	10.0.38.150	00:90:2B:BA:32:47		
7		vistatest	Web Server	<input type="checkbox"/>	10.0.38.172	00:0E:0C:00:CA:5E	vistatest	
8		10.0.38.64	Web Server	<input type="checkbox"/>	10.0.38.64	00:40:96:53:DE:FA		
9		antivirusserver	Internet Information Server	<input type="checkbox"/>	10.0.38.178	00:0E:0C:6C:C7:8F	antivirusserver	
10		Switch	Switch	<input type="checkbox"/>	10.0.38.50	00:30:F1:8A:75:1A		
11		SUPPORT-WAN	Web Server	<input type="checkbox"/>	10.0.38.102	00:0E:0C:D0:A5:E5	support-wan	SUPPORT-WA
12		10.0.38.205	Web Server	<input type="checkbox"/>	10.0.38.205	00:0D:5D:04:4E:DA		
13		supporttrack105	Web Server	<input type="checkbox"/>	10.0.38.105	00:E0:81:41:A6:59	supporttrack105	
14		SUPPORTTRACK108	Windows Workstation	<input type="checkbox"/>	10.0.38.108	00:22:15:F2:B5:11	supporttrack108	SUPPORTRAC
15		ors-server	Web Server	<input type="checkbox"/>	10.0.38.110	00:22:15:67:5F:DB	ors-server	
16		supporttrack103	Station	<input type="checkbox"/>	10.0.38.103	00:1B:FC:1A:21:17	supporttrack103	
17		supporttrack109	Station	<input type="checkbox"/>	10.0.38.109	00:23:54:8D:6E:48	supporttrack109	
18		supportexpand	Windows Workstation	<input type="checkbox"/>	10.0.38.111	00:1F:C6:84:84:9A	supportexpand	
19		10gig-generator	Station	<input type="checkbox"/>	10.0.38.112	00:50:8D:9C:42:71	10gig-generator	

Polling starts in 1 minute, 20 seconds... Rediscovery starts in 8 minutes, 7 seconds...

Training App NI World NOC New NI on 7 10 Just Netinst SUMMARY 10.0.36.156: NI UK 10.0.36.156: Netinst.com

Log Settings Find Log Filter: NONE

# Observer Infrastructure Appliances

- 100 ou 500 Device Appliance
  - 1.3U chassis
  - 4 Gb RAM
  - Quad core processor
  - 1 TB storage
- Enterprise Appliance
  - 2U chassis
  - 8 Gb RAM
  - Dual Quad Core Processor
  - 2 TB storage (4 x 500 GB)
- Also sold as software only (100/500 Device)

