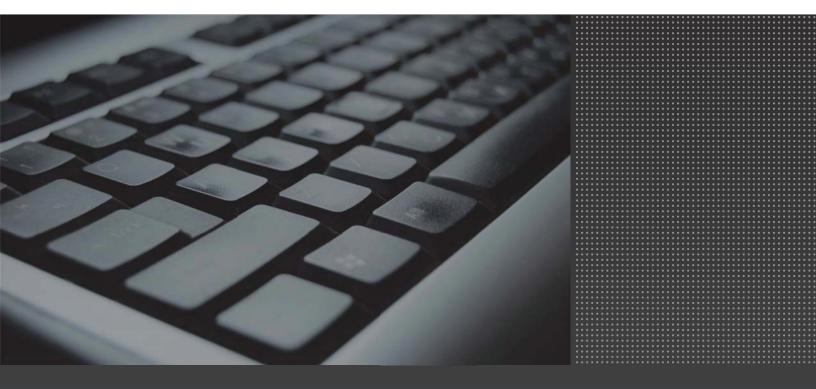
ARGENT

Argent Atlas Secrets



Argent Atlas is Argent's open CMDB-X database that is not only a network inventory but also the modeling product for both network topology and infrastructure dependency.

The network inventory stores nodal information that can be shared among all Argent AT products, as well as thirdparty products.

CMDB-X	CMDB-X						
Display Options	*						C 0
Enterprise Network Display Option	Network Group	Server/Device	Domain	Туре	Location	Vendor	Make
	Demo URLs						
Show All Servers/Devices	Demo Web Servers						
Filter By Server/Device Type	E First Network Group						
Filter By Network Group		DBMMIRR	A	Windows Servers	NEW YORK	Microsoft	Windows
Filter By Monitoring Group		DBMPRIN	A	Windows Servers	NEW YORK	Microsoft	Windows
		DBMWIT	A	Windows Servers	NEW YORK	Microsoft	Windows
Filter By License Of Current Product	H H	DELL4WAY	A	Windows Servers	NEW YORK	Microsoft	Windows
		EX2007	A	Windows Servers	NEW YORK	Microsoft	Windows
<u>U</u> pdate		ORCL10	A	Windows Servers	NEW YORK	Microsoft	Windows
		PANA01	A	Windows Domain Controllers	NEW YORK	Microsoft	Windows
Auto Update When Selection Changes		PANA32	A	Windows Servers	NEW YORK	Microsoft	Windows
Group By: Server/Device		PANA35	A	Windows Workstations	NEW YORK	Microsoft	Windows
croup by. Estiment senses		PANA36	A	Windows Servers	NEW YORK	Microsoft	Windows
Filter By:		PANA40	A	Windows Workstations	NEW YORK	Microsoft	Windows
Twee by		PANA53	A	Windows Servers	NEW YORK	Microsoft	Windows
		PANA54	A	Windows Servers	NEW YORK	Microsoft	Windows
Vindows Domain Controllers		PANA60	A	Windows Servers	NEW YORK	Microsoft	Windows
✓ Windows Servers ✓ Windows Workstations		PANW5	A	Windows Servers	NEW YORK	Microsoft	Windows
INT Backup Controllers		SP2010	A	Windows Servers	NEW YORK	Microsoft	Windows
Solaris Servers		utestserver	A	Linux Servers	NEW YORK		
HP-UX Servers		W2003R2XEN	A	Windows Servers	NEW YORK	Microsoft	Windows
AIX Servers		W2008DEV-64	A	Windows Servers	NEW YORK	Microsoft	Windows
SCD Servers		W2008R264XEN	A	Windows Servers	NEW YORK	Microsoft	Windows
Linux Servers		W2008R2DEV	A	Windows Servers	NEW YORK	Microsoft	Windows
TCP/IP Addresses		W7-32-PL2	A	Windows Servers	NEW YORK	Microsoft	Windows
Series Server		WS-DEV8	A	Windows Servers	NEW YORK	Microsoft	Windows
Cluster Nodes	ID SNMP	no bero			ine in room	The court	in the second se
Cluster Groups	· ·	192,168,2,189	SNMP	TCP/IP Addresses	NEW YORK	LINUX Server	Server and Wo
Select All Deselect All		192.168.2.211	SNMP	TCP/IP Addresses	NEW YORK	LINUX Server	Server and Wo
Select All Deselect All		192.168.2.3	SNMP	TCP/IP Addresses	NEW YORK	{1.3.6.1.4.1.29999.1}	{1.3.6.1.4.1.2
		192.168.2.5	SNMP	TCP/IP Addresses	NEW YORK	Netgear	Switch
Events And Alerts	VMware	19211001210	2000	i di fa manosios	inclusion room	The goal	Shiten
🕮 Enterprise Objects							
Scheduled Monitoring Tasks							
CMDB-X							
Control Information	4			III			
Reports	Network Inventory	Network Topology					

The network topology is useful for root cause analysis.

Here are some common chores that Argent Atlas can automate:

- Automated application monitoring using CLI and Argent AT maintenance scripts
- Detect newly installed SQL Servers
- Notify the changes of Exchange infrastructure
- Alert on installation of rogue SMTP services
- Maintain a master network inventory of Linux/Unix servers
- Bulk import IP addresses for the entire network
- Use third-party data source as data feed for Argent Atlas
- Implement third-party GUI and Web Interface to manage Argent Atlas
- Pass network inventory information between separate network locations
- Determine how servers and devices are connected
- Discover SNMP devices and information of vendor, make, model, etc
- Find MAC addresses of connected wireless devices
- Manage Monitoring Groups used by Argent AT
- Manage license to all Argent AT products
- Manage all Argent AT services

How Do I Assign A Node To A Daughter Engine For Monitoring When {Dynamic} Monitoring Engine Is Used?

The Argent AT Engine determines which Supervising Engine to use to schedule a monitored task for a node by inspecting the associated Monitoring Engine in the Relator.

The controlling Supervising Engine for the Monitoring Engine will be responsible for monitoring the node.

By default, {Dynamic} monitoring engine is used.

🚛 🔟 💿 💊 🖛 🧼 🐏 😒 = 🖓 Argent Guardian Ultra (3.1A-13	08-A)							- " X
Control Information	Relator Definition: RE	L_DEMO						
Definitions								G7A
System Down Rules System File Rules System File Rules Service Pack Rules	Production Mode							
Service Pack Rules E Server Connectivity Rules		e Rules Must Pass For Main Rule						<u>></u> × ⇒ ∕++
⊕ ⇒ystem Management Scripts ⊕ ⊕ ⊕ Windows Protess ⊕ ₩ Windows Protess ⊕ ➡ Windows Protess ⊕ ➡ Windows Protess ⊕ ➡ Mark Rules ⊕ ➡ Relates ⊕ ■ Relates ⊕ ■ Relates ⊕ ■ Relates ⊕ ■ Relates	Rule	Туре	Ins	tant Correction	Alert	Root Cause	Analysis	
	🧾 Run Prerequisite Rules On Cust	om Node:		<u>n</u>				
REL_DEMO_LINUX (Test Mode)	Main Rules:							🖺 🗙 🖾 🖉 🛧 🗲
Network Connectivity	Rule	Туре	Ins	tant Correction	Alert	Root Cause	Analysis	
	PRF_DEMO	Performance			Always	No	13	
B APPLICATION SERVERS B I P B I SERIES C LOCAL B SIMP B I LAUX B I LAUX B I MARARE								
Book WINDOWS Main_controllers	Monitoring Group List							*= × +
- & &MG_WINDOWS	Monitoring Group	Node Type	Excluded	Monitoring Engine	Backup Mo	nitoring Engines	Use Local If Installed	
- 📥 &MG_WINDOWS_SERVERS	E &MG_WINDOWS		1997	({Dynamic}				
- AMG_WINDOWS_WORKSTATIONS	PANA01 PANA35	Windows Domain Controllers Windows Workstations						
	PANWS	Windows Servers						
Events And Alerts	W2003R2XEN	Windows Servers	(E)					
	W2008R264XEN	Windows Servers	(E)					
Enterprise Objects								
Scheduled Monitoring Tasks	- How To Run Monitoring Tasks							
CMDB-X	Spawn New Monitor Engine I	Process						
Control Information	Use Shared Monitor Engine F	Process In Pool : (Dynamic)						
Reports	What To Run (Rules)	When To Run (Schedule) What	To Do (Alerts)	Advanced Features				
Ready			31 Jul 2	2013 09:14:58 NUP	M Argent Guardian	Ultra - Scheduling Engine	on W2008R264XEN is running	

The Argent AT engine uses the following algorithm to determine which Supervising Engine to use:

- Find the Network Group a node belongs under
- Get the 'Default Monitoring Engine' for the Network Group
- Determine which Supervising Engine controls the Monitoring Engine, and the Supervising Engine is the one that schedules tasks for the node

Network Group Properties	s	x				
		G15				
Name:	First Network Group					
Network Connection:	T1 🔹					
	Protected By Firewall					
Network Administrator:	admin					
Contact Email:	admin@a.local					
Contact Phone:	(800) 674-1234					
Default Alert:	EMAIL_GENERAL					
Default Alert Executor:	•					
2↓						
🗆 Default Node Prop	erties					
Default Monitoring		-				
	{Product Main Engine} PANA35					
	Cancel					

Which Logon Credential Does Argent for VMware Use To Monitor VMware Objects?

To determine the logon credential for a VMware object, Argent for VMware uses the following logic:

- First check if the VMware object has explicitly set a user/password at the licensed node level
- If default, check the logon credential specified in the Network Group that the node belongs to
- If set, use it
- If not set, use the logon credential at the system level specified in the Supervising Engine setting

Network Group Properties					
				V15	
Name:	VMware				
Network Connection:	T1		-		
	Protected	By Firewall			
Network Administrator:]	
Contact Email:					
Contact Phone:				1	
Default Alert:				1	
Derault Alert:			*		
Default Alert Executor:			-		
₽					
🗆 Default Node Prop	erties				
Default Monitoring Er	igine				
VCenter or ESX Host		192.168.2.187		וה	
Port Protocol		https	4	43	
Logon User		root		-	
Password		****			
		Cancel			

How Do I Fire An Alert Through A Node-Specific Argent Alert Executor?

The Argent Alert Executor allows Argent AT to fire alerts from a different machine other than the Argent Console main engine.

Customers can specify to use the Argent Alert Executor when defining Alerts in a Relator.

Argent Guardian Ultra	(3.1A-1308-A)	_ = ×
Control Information	Relator Definition: REL_DEMO_LINUX (Test Mode)	
Definitions		G7C
	Notification And Correction Alerts (Dr Alert Macros) To Fire, In Following Order: File Subma Alem Alam Alert AARM DE MO File SMS Alert SMS_USA_MOBILE Select An Alert Or Alert Macro Alert Or Alert Macro Optional Time Alert Or Alert Macro Diplay Calor: No Special Coloring Alert To Send Diplay Calor: No Special Coloring Alert To Send Event Picote Alert To Send Diplay Calor: No Special Coloring Alert To Send Event Picote Event Picote Event Picote Event Picote Event Picote Event Picote Picote To Send Event Picote Event Picote Event Picote Event Picote Event Picote Event Picote Event To Send You can also Ding and Diop an Alert or Alert Macro from the tree You can also Ding and Diop an Alert or Aler	• • • × •
Events And Alerts		
Scheduled Monitoring Tasks		
CMDB-X		
Control Information		
Reports	What To Run (Rules) When To Run (Schedule) What To Do (Alerts) Advanced Features	
Ready	29 Jul 2013 12:39:42 NUM Argent Guardae Ultra - Scheduling Engine on W2008R264VEN is running	

The Alert Executor can be either explicit or node specific.

When it is node specific, the Argent Console engine use the following algorithm to determine which Alert Executor should be used:

Node 'PANA32' Common Propertie	es X
	V15
<u>₽</u> 2↓	
🗉 Windows Machine	
Name	PANA32
Domain	A
OS	Windows Servers
NetBios Name	
Internal Name	
Alias	PANA32\$
Alternative IP	
Use Alert Executor	PANA57
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows Server 2003
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
🕀 Contact	
🕀 Time Zone Settings	
🗄 Logical Drives	
Appearance Used In Even	t Console (A1A)
Installed Applications	
OK	Cancel

• If the node has an Alert Executor specified, use it

• If the Network Group that node belongs to has an Alert Executor specified, use it

	1		
Name:	VMware		
Network Connection:	T1		
	Protecte	ed By Firewall	
Network Administrator:			
Contact Email:		<u></u>	
Contact Phone:			
Default Alert:	-	×	
Default Alert Executor:	PANA56		-
2↓			
Default Node Prop	erties		
Default Monitoring En	igine		
vCenter or ESX Host		192.168.2.187	
		443	3
Port		https	
Port Protocol		N 10 10	L
		root	

• Otherwise, use the Argent Console Main Engine to fire the Alert

How Do I Specify What Alert To Fire When Doing Automated Monitoring In Argent for SNMP?

Argent for SNMP provides a powerful heuristic self-learning facility. This is explained in more detail in the document "Argent for SNMP Self-Learning Facility".

Customers can select a monitoring level at the Node Manager, and the Argent for VMware engine synthetically generates internal Relators to monitor.

👔 🔟 🔕 🗲 🧰 🐏 😫 = Argent for SNMP (3.1A-13	308-A)					_ = X
(23)						(
Control Information	Node Manager					
Definitions	-		-			N
🕀 🧰 Rules	Server/Device	Monitor Level	Maintenance	Туре	Location	
Ketwork Management Brei Gin System Down Rules	192.168.2.187	Manual	1	ESX Host	NEW YORK	
Service Level Agreement Rules	192.168.2.189	Manual 🔹		TCP/IP Addresses	NEW YORK	
SNMP Rules	192.168.2.211			TCP/IP Addresses	NEW YORK	
🗄 🫅 SNMP Trap Monitors Rules	192.168.2.3	Manual 💌		TCP/IP Addresses	NEW YORK	
😟 💼 System Management Scripts	192.168.2.5	High 💌		TCP/IP Addresses	NEW YORK	
Relators		Low				
Node Manager		Medium High				
🗄 🚰 Monitoring Groups		Manual				
🗈 🫅 Automatic Report Distributions						
🗉 🧰 Macros						
🖲 🧰 Calendars						
🖻 🗁 Administration						
Engine Manager Sources Manager						
- Housekeeping						
🗄 🛅 Advanced						
🛶 👌 Total Support Interface	1					
Search Argent Instant Help	1					
Events And Alerts						
⊠(∰ Enterprise Objects						
Scheduled Monitoring Tasks						
CMDB-X						
Control Information						
Reports						
Ready				29 Jul 2	2013 12:27:03 NUM	Argent for SNMP - Scheduling Engine on W200BR264XEN is running

Because the synthetically generated internal Relator does not exist physically, the engine needs to know what Alert to fire if the Rule is broken.

Network Group Properties	s		x			
			V15			
Name:	First Network	Group				
Network Connection:	T1					
	Protected	Protected By Firewall				
Network Administrator:	admin	admin				
Contact Email:	admin@a.local					
Contact Phone:	(800) 674-1234					
Default Alert:	EMAIL_GENE	ERAL)			
Default Alert Executor:						
₽ ₽ 2 ↓						
🗆 Default Node Prop	erties					
Default Monitoring En	igine	{Product Main Engine}				
Protocol		SNMPv1				
Community		public				
SNMP User						
Auth. Protocol		Not Used				
Auth. Password			Ŧ			
		Cancel				

The Alert is defined as the Default Alert in the Network Group the node belongs to.

How Do I Add Linux/Unix Servers To Argent Atlas?

To add a few Linux/Unix servers, add them manually by right-clicking and 'Add Server Or Device' on CMDB-X screen.

Manually Add An Enti	γy	x
		V5E
Domain:	А	
Node Name:	utestserver2	
Alternative IP:	192.168.2.106	
Node Type ————————————————————————————————————		_
🔘 Windows 200	x/Windows XP	
🔘 Windows NT	3.51 And 4.0	
Windows Ser Windows Wo NT Backup C Windows 9x 9	rkstation Controller	
Unix Server	LINUX	•
 iSeries Server Cluster 		
Cluster Node Cluster Group Cluster Netwo Cluster Netwo Cluster Resol	ork ork Interface	*
O TCP/IP Devic	e 📃 This Is An Aggregate Node	
🔘 Print Queue		
 Internet Object 		
🔘 VMware Obje	ct	M
O XenServer		
<u>0</u> K	Cancel	

If a large number of servers are to be added, use the Argent AT command-line facility.

ARGENT_CMDB_CLI -n node [-o "property:value"] [-g group] -a

- Argument '-n' specifies the node name
- Argument '-g' specifies the network group that the node will be added to; it is optional; if not specified, the default 'First Network Group' is assumed
- Argument '-o' specifies relevant pairs of property and value

To add a Linux server, specify the OS as 'Linux Servers'. Example:

ARGENT_CMDB_CLI -n TestNode1 -o "Domain:A" -o "OS:Linux Servers" -o "Alternative IP:192.168.2.106" -a

For details see Argent AT command-line facilities

Customers can read the Linux/Unix servers from another data source, and repeatedly call the command line to add all the servers.

How Do I Programmatically Remove Server/Devices From Argent Atlas?

Customers can use the Argent AT command-line facility to accomplish it.

ARGENT_CMDB_CLI -n node -r

Argument '-n' specifies the node name.

For example, the following command removes node 'W2008R264XEN' from Argent Atlas.

ARGENT_CMDB_CLI -n W2008R264XEN -r

Note: The operation will fail if the server/device is licensed in <u>any</u> Argent AT product.

In that case, customers should first call the following to <u>unlicense</u> the node from the Argent AT products.

ARGENT_LICENSE_CLI -n node -p product -r

For example, the following command unlicenses the node 'W2008R264XEN' from Argent Guardian Ultra.

ARGENT_LICENSE_CLI -n W2008R264XEN -p "Argent Guardian Ultra" -r

How Do I Add Servers In An Active Directory Environment To Argent Atlas?

Scanning Windows network using Active Directory is the most reliable way to accomplish this.

For details, see section 'Scan Windows Network Using Active Directory' in Appendix B.

How Do I Add Servers In A Workgroup Environment To Argent Atlas?

Scanning Windows network using Network Browser is the easiest way, but the Microsoft Network Browser must be treated with caution, as it is sometimes unreliable.

For small amounts of servers, customers can opt to add manually.

For details, see section 'Scan Windows Network Using Network Browser' in Appendix B.

How Do I Add Servers In A Different Domain To Argent Atlas?

Use the option 'Use Explicit Domain Account' when doing Active Directory scanning.

Customers are prompted to enter the logon credentials and domain controllers before the actual scanning.

Windows Domair Windows Servers Windows Workst NT Backup Contr	: ations	 Printer Queu ✓ Windows 9x ✓ Unknown Sy 	Systems		
Use Explicit Don	ters In The Active Direc			×	dc=domain)
tering Option: Fi Use FDQN Nam Active Directo	Domain Account: Password:	B\Administrator		V18 (Domain\User)	are
Ignored	Domain Controller:	PANA38		j	Vend
l	OK		C	ancel	

How Do I Scan A Large TCP/IP Network Quickly?

	Start	End	No. Of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16777216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1048576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65536

IANA-reserved private IPv4 network ranges

Theoretically customers can pick any of the above as a whole for the network.

For example, a large network may have a range of 10.0.0.0 – 10.255.255.255, while SOHO can use 192.168.1.0 – 192.168.1.255.

If more than 256 IP addresses are needed, then 192.168.0.0 can be selected with a network mask 255.255.0.0.

In most cases, customers will pick multiple network segments such as 192.168.0.x, 192.168.1.x, 192.168.2.x etc.

To scan such a network, it is a lot faster to do it by scanning each segment of 256 addresses instead of scanning the whole range of 65,536 addresses.

Vorldwide Enterprise	Network Scanning				X N12
IP Address Range:	192 , 168 , 2 ,	1 - 192 ,	168 , 2 , 254		
Subnet:	255 . 255 . 255 .	0			
Timeout (seconds):	10 🜻				
Retry:	0	0	N		
Thread Limit:	128 🜻	Une t	ime one segment		
Active Directory	Network Browser	CMP Ping Window	vs Cluster External File	SNMP Discovery	
	Network Browser II	CMP Ping Window Domain	vs Cluster External File	/~/	endor
				/~/	endor
				/~/	endor
				/~/	endor
				/~/	endor
				/~/	endor
Ignored 1	Machine	Domain		Y	endor •

How Do I Scan A Mixed Cluster Environment?

Microsoft Clusters for W2003 and W2008 do not talk to each other.

As a result, native cluster WIN32 API does not work on W2003 querying a remote W2008 cluster, and vice versa.

To handle a mixed cluster environment, the option 'Failover Cluster WMI Provider' should be used.

	rise Network Scanning	1		х
Cluster Node Cluster Group Cluster Netwo Cluster Netwo Cluster Resol	os orks ork Interfaces			N12
Cluster Names:	PANCLUSTER		🔽 Use Failover Cli	uster WMI Provider
Active Direct	ory Network Brows	er ICMP Ping Windows	Cluster External File SN	MP Discovery
Ignored	Machine	Domain	Туре	Yendc 🔺
	, isching	Domain	17pc	Felluc -
	PANA54 PANA53 Group 0 Cluster 0 Local Are Local Are	or SNMP (3.1A-1308-A) Windows cluster scanning c	ompleted successfully.	
	PANA54 PANA53 Group 0 Cluster 6 Local Are Local Are	for SNMP (3.1A-1308-A) Windows cluster scanning c	ompleted successfully.	X
	PANA54 PANA53 Group 0 Cluster 6 Local Are Local Are	ior SNMP (3.1A-1308-A) Windows cluster scanning c	ompleted successfully.	X

Because it relies on WMI, the security on the cluster must be adjusted to allow the Argent AT engine access to the WMI name space 'root\mscluster'.

WMI Control Properties	? X	
General Logging Backup/Restore Security Advanced		×
	w Help	<
Namespace navigation allows you to set namespace specific sec		
⊟ 📄 Root 5	Security for RODT\MSCluster	7
	Security entation (WMI)	
teria Cli teria DEFAULT teria directory	Group or user names: hent Instrumentation (WMI)	
	Generation Generation Generation Generation	
MicrosoftNI B MSCluster perfmon		
	Add <u>R</u> emove	
🕀 🧰 ServiceModel	Permissions for Administrators Allow Deny	
⊕ subscription ⊕ WMI	Execute Methods Full Write	
S	Execute Methods Image: Constraint of the second s	
	Provider Write	
OK Cancel	Enable Account	
	Remote Enable	
	For special permissions or for advanced settings, Advanced	
	OK Cancel Apply	

Why Are Some SNMP Device Not Discovered?

Scanning SNMP devices is similar to ICMP Ping by enumerating all the possible IP addresses in the range. As a result, the recommendation of using small network segments in <u>How To Scan A Large TCP/IP Network Quickly</u> also applies here.

Customers may find some or all SNMP devices are not found during network scanning. The possible causes include the following:

- Each SNMP device has a built-in configuration of allowed management workstations. In other words, it
 only handles requests from certain IP addresses. Contact the Network Administrator, ensure the machine
 where the scanning is done (e.g. Argent Main Engine) is listed as a management workstation in the SNMP
 devices.
- 2. Check supported SNMP version. Version 1 and 2c are most common, and version 3 is the most complicated. Scan the network using the appropriate SNMP version setting.
- 3. If it is v1 or v2c, ensure the community string is correct. The string is the password in the SNMP world.
- 4. If it is v3, double check the password and protocol for authentication and encryption. If any of them mismatches, the scanning won't work.
- If the network segment for scanning is outside of the local network segment, ensure the option 'Active Poll Each IP Address' is checked. Most routers won't forward SNMP broadcast packets out of a local segment.

What Do I Do When Two Cluster Objects Have The Same Name But Are From Different Clusters?

Give each Cluster Object distinct node names while using the 'Internal Name' field to hold the real object name.

When monitoring multiple Windows Clusters there may be naming conflicts.

For example, two SQL Clusters have resource 'Disk Q:'. Clearly both cannot use 'Disk Q:' for the cluster object name.

Instead, use DISK_Q_OF_CLUSTER_A and DISK_Q_OF_CLUSTER_B for the two objects, and specify 'Disk Q:'. Because the Cluster is determined by the property 'Cluster Name', the two objects are fully defined without conflict.

Node 'PANCLUSTER_DISK_Q' Common Properties Image: Pancluster Name PancLUSTER_DISK_Q Cluster Name PANCLUSTER_DISK_Q Cluster Name PANCLUSTER Real Name Internal Name DISK Q: Alias Alternative IP Use Alert Executor Dependency Vendor Make Model 64-bit OS SIMP sysObjectId Location NEW YORK Description	,••		
Image: Second	Node 'PANCLU	CLUSTER_DISK_Q' Common Pro	perties X
Windows Cluster Name PANCLUSTER_DISK_Q Cluster Name PANCLUSTER Real Name PANCLUSTER Internal Name DISK Q: Alias Internative IP Use Alert Executor Internative IP Dependency Vendor Make Internative IP Vendor Internative IP Dependency Internative IP Use Alert Executor Internative IP Dependency Internative IP Vendor Internative IP Dependency Internative IP Vendor Internative IP Dependency Internative IP Vendor			N15
Windows Cluster Name PANCLUSTER_DISK_Q Cluster Name PANCLUSTER Real Name DISK Q: Internal Name DISK Q: Alias I Alternative IP Use Alert Executor Dependency I Vendor I Make I 64-bit OS Unknown SNMP sysObjectId I Location NEW YORK Description I Time Zone Settings I	91 A.L		
Name PANCLUSTER_DISK_Q Cluster Name PANCLUSTER Real Name PANCLUSTER Internal Name DISK Q: Alias I Alternative IP I Use Alert Executor I Dependency I Vendor I Make I 64-bit OS Unknown SNMP sysObjectId I Location NEW YORK Description I Image Zone Settings I			
Cluster Name PANCLUSTER Real Name DISK Q: Internal Name DISK Q: Allas I Alternative IP I Use Alert Executor I Dependency I Vendor I Make I Model I 64-bit OS Unknown SNMP sysObjectId I Location NEW YORK Description I Time Zone Settings I		ws Cluster	
Real Name DISK Q: Alternal Name DISK Q: Alternative IP Image: Comparison of the second of the se			
Internal Name DISK Q: Allas I Alternative IP I Use Alert Executor I Dependency I Vendor I Make I Model I 64-bit OS Unknown SNMP sysObjectId I Location NEW YORK Description I Imate Zone Settings I			PANCLUSTER
Alias Alternative IP Use Alert Executor Dependency Vendor Make Model 64-bit OS SNMP sysObjectId Location Description			
Alternative IP Image: Contact State St		al Name	DISK Q:
Use Alert Executor Use Alert Executor Dependency Vendor Make Model 64-bit OS Unknown SNMP sysObjectId Location NEW YORK Description Cutatt Time Zone Settings			
Dependency - Vendor - Make - Model - 64-bit OS Unknown SNMP sysObjectId - Location NEW YORK Description - Time Zone Settings -			
Vendor Image: Simple system Make Image: Simple system 64-bit OS Unknown 64-bit OS Unknown SNMP sysObjectId Image: Simple sysObjectId Location NEW YORK Description Image: Simple sysObjectId Image: Simple sysObjectId Image: Simple sysObjectId<			
Make Model 64-bit OS Unknown SNMP sysObjectId Location NEW YORK Description Time Zone Settings		iency	
Model 4 64-bit OS Unknown SNMP sysObjectId 4 Location NEW YORK Description 4 Contact Time Zone Settings	Vendor		
64-bit OS Unknown 5NMP sysObjectId Location NEW YORK Description Escription Escriptio	Make		
SNMP sysObjectId NEW YORK Location NEW YORK Description Contact Time Zone Settings	Model		
Location NEW YORK Description Contact Time Zone Settings	64-bit OS)S	Unknown
Description	SNMP sysC	ysObjectId	
 ☑ Contact ☑ Time Zone Settings 	Location	n	NEW YORK
Time Zone Settings	Description	tion	
-	🕀 Contact	t	
Appearance Used In Event Console (A1A)	🕀 Time Zon	one Settings	
Appearance osca in Evene console (HTH)	🕀 Appeara	rance Used In Event Conso	le (A1A)
Installed Applications	⊞ Installed	ed Applications	
OK		ОК	Cancel

How Do I Define Monitoring Groups Based On Node Type?

This is can be done by using an ODBC query-based Monitoring Group.

📑 🔤 💽 💊 🗰 🤿 🛄 😫 🐑 Argent for VMware (3.1A-	1308-A)	_ ~ ×
3		
Control Information	Monitoring Group Definition: &MG_WINDOWS	
Definitions		V7
Duks Duks	Ute fix Tab to specify a ODBC Query to kno against the Algord CMOBX statest assort generation of anotany utral leteresponse work name from argon tradeoff about during the leternoid mode, argonoff at mode while a legord labort during letteresponse work name from argonoff about during utral leternoid mode, argonoff at mode and argonoff labort during the Algord CMOB. And argonoff at mode in the Algord and the Algord CMOB. Mode argon	
Automatic Report Distributions		*
e 🛅 Macros		•
🛛 🧰 Calendars 🔹 👻	Server/Device ODBC Query	
—	Exclude Server/Devices:	
Events And Alerts	(Separated By Comma)	View Selected Nodes By Notepad
Enterprise Objects		Tiew adiected House by Hotepau
Scheduled Monitoring Tasks	Description: This is a sample monitoring group definition installed by Setup. It includes all licensed Windows machines.	
CMDB-X	n an	
Control Information		
Reports		+

The query uses the column 'NODE_TYPE' to specify Windows OS. The possible values are as follows:

0x1 (1) – Windows Domain Controller

– Linux

- IP Address

– Cluster Node

- 0x2 (2) Windows Backup Domain Controller
- 0x4 (4) Windows Server
- 0x8 (8) Windows Workstation
- 0x10 (16) Sun Solaris
- 0x20 (32) HP-UX
- 0x40 (64) AIX
- 0x80 (128) SCO UNIX
- 0x100 (256)
- 0x200 (512)
- 0x400 (1,024) iSeries Server
- 0x800 (2,048)
- 0x1000 (4,096)
- Cluster Group Trade Secret of ArgSoft Pacific Intellectual Property Holdings (HK), Limited Proprietary Information

0x2000 (8,192)

0x4000 (16,384)

0x8000 (32,768)

0x10000 (65,536)

- Cluster Network
 - Cluster Network Interface

– Windows 9x (obsolete)

– Novell Server (obsolete)

- Cluster Resource
- Printer Queue
- 0x20000 (131,072)
- 0x40000 (262,144)

0x80000 (524,288)

- Unknown
- 0x100000 (1,048,576) URL Object
- 0x200000 (2,097,152) Mail Object
- 0x400000 (4,194,304) FTP Object

How Do I Add Two Machines With The Same Machine Name But In Separated Unrelated Networks?

ISP customers can run into such a situation. Two accounts may have machines of the same name. It happens when the machine is either cloned or installed with default settings of a Microsoft small business suite. Because each account has its own network, there is no conflict until the ISP needs to monitor both of them.

To address the issue, customers can add two machines using arbitrary names, <u>but specify the NetBIOS property</u> <u>with the real machine name</u>. As long as two machines are monitored by separate Daughter Engines, it will work as expected.

Node 'W2008R2DEV' Common Prop	nerties)
	N15
1 2↓	
Windows Machine	
Name	W2008R2DEV
Domain	А
OS	Windows Servers
(NetBios Name	W2008R2DEV.a.local
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows Server 2008 R2 Standard
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
∃ Contact	
Time Zone Settings	
∃ Logical Drives	
Appearance Used In Event	Console (A1A)
Installed Applications	
OK	Cancel

When An ESX Host Is Offline, A Flood Of Alerts Are Sent About Offline VMs. How Do I Receive Just One Alert Telling The Root Cause?

Specify the ESX host as a Logical Dependency for the VMs and enable Root Cause Analysis in the Relator definition.

	N15
∄ ∎ 2↓	
🖃 Windows Machine	
Name	DBM_MIRR 31/31
Domain	VMware
OS	Windows Servers
NetBios Name	
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	192.168.2.187
Vendor	Microsoft
Make	Windows
Model	Microsoft Windows Server 2003, Standard
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	VirtualMachine-528
🗄 Contact	
🗄 Time Zone Settings	
🕀 Logical Drives	
🕀 Appearance Used In Eve	nt Console (A1A)
Installed Applications	

👔 💿 💿 🍬 🛶 🤐 😫 🖘 Argent for VMware (3		e x
Control Information	Relator Definition: REL_VMWARE_CONNECTIVITY (Test Mode)	
Definitions		V7D
b) ● Tool Rules b) ● Tool Rules b) ● ● Version And Pack Rules b) ● Persion And Pack Rules b) ● Persion And Pack Rules b) ● Persion And Pack Rules b) ● Packato Statist Number b) ● Packato Number b)	II Precquate Rides Fall Mark Servers As: The Same Status DI Previous Direck.	
Conception	Description	*
- Security		
Events And Alerts		
Canterprise Objects		
Scheduled Monitoring Tasks		
CMDB-X		
Control Information		
Reports	What To Run (Rulen) When To Run (Schedule) What To Do (Wents) Advanced Fealures	
eady	31.3ul 2013 13:04:53 NUM Argent for VMware - Scheduling Engine on W2000R26WEN is running	

When the Argent AT engine cannot access the VM, it will check the accessibility of its logical dependency. In this case, it is the ESX host. If the ESX host is offline, the event will be raised about the dependency instead of the offline VM.

How Can IP Addresses In An Excel File Be Imported To Argent Atlas?

Compose COMPUTERS.TXT then import into CMDB-X. Do the following:

- 1. Copy out the IP address column in the Excel into notepad.
- 2. Put 'TCP/IP<TAB>' in front of each line.
- 3. Put '<TAB><TAB>TCP' in end of each line.
- 4. Save file as COMPUTERS.TXT
- 5. Import into CMDB-X (See Import And Export CMDB-X Data)

Note the count of one <TAB> and then three <TAB> is essential.

👔 🔟 🖉 🔕 🗰 👳 🞯 😫 = 🕅 Argent Guardan Ultra (3	1A-1308-T1)								- = ×
CMDB-X	CMDB-X								
Display Options 2									CBA
C Enterprise Network Display Option	Network Group		Server/Device	Domain	Тур	e	Location	Vendor	Make
Show All Servers/Devices	Demo URLs Demo Web Servers								
Filter By Server/Device Type	Demo web servers First Network Group	Construction				×			
C Filter By Network Group	+	Worldwide E	nterprise Network Scanning				NEW YORK		
C Filter By Monitoring Group						612	NEW YORK		
Fitter By License Of Current Product		File Path.	Z:\COMPUTERS.TXT		in and		NEW YORK		
			Option						
Update									
Auto Update When Selection Changes			Import Network XML						
			Import Computer Test Fil	e (Advanced Feature)					
Group By: Server/Director			You may either manually	edit COMPUTER, TXT					
Filter By:				GSOFT_NETWORKSCAN	IDC to appearate this file				
			or for the contributed At	Idoor I jaci wonkookki	roo to generale dist ne				
Windows Doman Controllers									
Windows Servers Windows Workstations		Active	Directory Network Browser	ICMP Ping Windows Clu	ster External File				
✓ NT Backup Controllers			ed Machine	Bernahr		Handar			
Solaris Servers	-	Ignor	ed Machine 192.168.2.101	Domain TCP/IP	TCP/IP Address	Vendor			
HP-LDC Servers	1	1	192.168.2.102	TCP/IP	TCP/IP Address				
SCO. Servers		13	192.168.2.103	TCP/IP	TCP/IP Address				
Linux Servers		- E	192.168.2.104	TCP/IP	TCP/IP Address	5			
TCP/IP Addresses			COMP.	UTERS.TXT - Notepad					
Cluster Nodes				t Fgrmat View Help					
Cluster Groups					TCP			-	
Cluster Networks			TCP/IP TCP/IP	192.168.2.101 192.168.2.102 192.168.2.103 192.168.2.104	TCP TCP TCP TCP				
Select All Deselect All			and a second sec	192.168.2.104	TCP				
		Save To N	etwork Group: First f						
Events And Alerts			an Network					N A	
D Enterprise Objects	1	Sc	an Network						
Scheduled Monitoring Tasks	1								
СМОВ-Х									
Control Information									,
Reports	Network Inventor	Netwo	vk Topology						9

There are Many Devices in the DMZ; They Cannot Be Scanned By The Argent AT Engine; There Are Too Many To Add Manually.

How Can The Devices Be Added To Argent Atlas?

Customers can do a quick install of Argent Guardian Ultra using SQL Server Compact on a machine of DMZ, then do the following:

- 1. Do a network scan using from the Argent GUI
- 2. Export the result as an XML file
- 3. Copy the XML file to the Main Engine
- 4. Import the XML file
- 5. Uninstall Argent AT from the machine in the DMZ

How Do I Determine All The Known SQL Servers In Argent Atlas?

Run the following SQL query using 'osql':

SELECT ARGSOFT_AT_NODE.NAME FROM ARGSOFT_AT_NODE, ARGSOFT_AT_NODE_APPLICATION WHERE ARGSOFT_AT_NODE.UUID = ARGSOFT_AT_NODE_APPLICATION.NODE_UUID AND ARGSOFT_AT_NODE_APPLICATION.NAME = 'MSSQL'

The key is to query with the qualified application name 'MSSQL'.

The same technique can be used to find Exchange servers, Oracle servers etc.

For the command syntax of 'osql', see: http://msdn.microsoft.com/en-us/library/aa213087(v=sql.80).aspx

How To Detect Whether Puppet Is Installed On A Linux Server?

The Puppet product has two components: Puppet master and Puppet client.

The easiest way to detect Puppet master is to use the method 'TCP service' to check if the Linux server is listening on port 8140. This generally is sufficient but be careful -- some rogue program may use the same port.

The most reliable way is to define an application using SSH methods to detect if the daemon 'puppetmaster' or 'puppet' is running.

👔 🔟 💽 🧿 🗰 🖝 🔄 😫 🖬 Argent Guardan Ultra	(3.1A-1308-A)				- P.X
(23)					۲
Control Information	Detect Installed	Applications			
Definitions					C16
🛞 💼 Advanced Monitoring	Methods To Detect Insta	a di Analiana d			
🗄 🧰 СЕМО					
C REL_DEMO	Name	Group CORP_COMMUNICATIONS	Method Registry		
REL_DEMO_ISERIES (Test Mode)	MSSOL	CORP_DATABASES	Windows Service		
E Connectivity	Oracle	CORP_DATABASES	Windows Service		
🖲 🛅 System Baseline	Exchange	CORP_COMMUNICATIONS	Registry		
🖲 🧰 Alerts	Puppet	CORP_INFRASTRUCTURE	Unix SSH		
🖻 😂 Monitoring Groups	Pupper	CORP_INFRASTRUCTURE	Unix 33H		
III CATION SERVERS					
18 🧰 IP	m				
I ISERIES					
H COCAL H SMMP					
H-G UND		Specify Details Of Application		- x	
H C VMWARE				CTEA	
H Ca WINDOWS				LISA.	
🖻 🧰 Automatic Report Distributions		Application Name: Bugga			
🕀 🚞 Macros		Appression reality. attents			
🕀 🧰 Calendars	-	Display Group: CORP_INFRASTR	UCTURE		
Administration Engine Manager		Detect Method: Unix/LINUX SSH			
- 5 License Manager		Detect method Of twentow 3311			
- Housekeeping		Unix Shell Script. #!/bin/sh		-	
- A Security		#			
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
E C Advanced		# Copyrig	ht (c) 2012 ArgSoft Pacific In	cellectual Property Holdi:	
- Argent SuperMaps		H 111 Dec	hts Reserved.		
Enterprise Application View		# All Rig	nts weserved.		
Application Definitions		# ARB Int	ellectual Property Holdings (H	0. Limited	
Console Application Columns			18 Metropolis Tower	47 million	
Console Application Colonits	•		ropolis, 10 Metropolis Drive	· ·	
		4		•	
Events And Alerts					
		OK		Cancel	
Enterprise Objects				.i.	
Scheduled Monitoring Tasks					
CMDB-X					
Control Information					
Reports					
Ready			31 Jul 2013 13:21:14 CAP NUM	Argent Guardian Ultra - Scheduling Engine on W2008R26498	N is running

Sample code is shown as follows:

```
#!/bin/sh
#
#
# Copyright (c) 2013 ArgSoft Pacific Intellectual Property Holdings (HK), Limited
#
# All Rights Reserved.
#
# ARB Intellectual Property Holdings (HK), Limited
# 2017-2018 Metropolis Tower
# The Metropolis, 10 Metropolis Drive
# Hong Kong
#
#
#
# This is PROPRIETARY SOURCE CODE of ARB Intellectual Property Holdings (HK), Limited.
#
# The contents of this file may not be disclosed to third parties, copied or
# duplicated in any form, in whole or in part, without the prior written
# permission of ArgSoft Pacific Intellectual Property Holdings (HK), Limited.
# RESTRICTED RIGHTS LEGEND:
# Use, duplication or disclosure by the Government is subject to restrictions
# as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data
# and Computer Software clause at DFARS 252.227-7013, and/or in similar or
# successor clauses in the FAR, DOD or NASA FAR Supplement.
# Unpublished - rights reserved under the Copyright Laws of the United States
# and other countries.
#
#
#
#
# This rule checks the status of the Puppet daemon.
# The rule fails if puppet is not running.
#
# For more information: email Unix@Argent.com.
```

```
STATUS=NOVAL
```

SUMMARY=NOVAL

COMMENT=NOVAL

#

xmlOut() - prints an entire XML output for a command script.

```
#
#
  Used for The Argent Guardian rules that return a PASS/FAIL
#
  status and summary and comment descriptions.
#
#
xmlOut()
{
xmlBegin
xmlStatus
xmlEnd
}
#
# xmlBegin() - Prints out the definition of the XML format used to
#
#
  send status data to The Argent Guardian.
#
xmlBegin()
{
cat <<!
<?xml version="1.0"?>
<!DOCTYPE TAGResult
Ε
<!ELEMENT TAGResult (QEResult+)>
<!ELEMENT QEResult (status, summary, comment)>
<!ELEMENT status (#PCDATA)> <!-- (PASS | FAIL) -->
<!ELEMENT summary (#PCDATA) >
<!ELEMENT comment (#PCDATA) >
]>
<TAGResult>
1
} # End of xmlBegin()
#
# xmlStatus() - Send a status block to The Argent Guardian.
#
# The status should be 'PASS' or 'FAIL'.
#
# The summary explains the result and the comment is a generic description of the Unix rule.
#
                       Trade Secret of ArgSoft Pacific Intellectual Property Holdings (HK), Limited
                                                                                            Page 33 of 115
```

Proprietary Information

```
xmlStatus()
{
cat <<!
<QEResult>
<status>$STATUS</status>
<summary>$SUMMARY</summary>
<comment>$COMMENT</comment>
</QEResult>
!
} # End of xmlStatus()
#
# xmlEnd() - Completes the XML data block.
#
xmlEnd()
{
cat <<!
</TAGResult>
!
} # End of xmlEnd()
DAEMON=puppet
COMMENT="Using ps and grep to determine if $DAEMON is running."
#
# Using the 'ps -ae' command, search for the process and extract the
#
# process ID.
#
DAEMON_PID=`ps -ae | grep $DAEMON | grep -v daemon | awk '{ print $1 }'`
#
# Generate status based on whether the process is running or not.
#
if [ -z "$DAEMON_PID" ]; then
STATUS=FAIL
```

SUMMARY="The \$DAEMON daemon is not running."

EXIT_CODE=1

```
else
```

STATUS=PASS

SUMMARY="The \$DAEMON daemon is running. PID: \$DAEMON_PID"

EXIT_CODE=0

fi

#

- # Report the findings back to The Argent Guardian
- #

xmlOut

exit \$EXIT_CODE

Servers Are Assigned To Different Administrators. When A Rule Is Broken, The Assigned Administrator Should Be Notified In One Relator.

How Is This Done?

Assume within one Relator, there is one Email Alert. The actual 'To' field in the Email Alert cannot be fixed when sending emails to a range of different recipients. Otherwise, an Alert for *any* node in the Relator will be sent to the fixed and static 'To' email address. Instead, the 'To' field must be a node-specific <u>variable</u>

Therefore the <u>variable</u> '%DefaultNode%+a@a.com' does just that. Before the Argent Console engine fires the Alert, it sees %DefaultNode% in the To/CC field.

It then looks up the CMDB-X to find out the contact email address for the node that breaks the rule. If the engine finds it, it use it as the To/CC email address. If the engine does not find it, it uses 'a@a.com' as fallback.

Do the following:

- 1. Assign the email address in the CMDB-X property 'Contact\Email Address' of the servers/devices
- 2. Define email alert using '%DefaultNode%+some_backup_email_address' in the To/CC field
- 3. Use the Email Alert in the Relator that monitors all server/devices

Node 'PANA01' Common Properties	•	x
	61	5
₽Ţ		
🗄 Windows Machine		
🖂 Contact		
Email Address	admin@argent.com	
Phone#		
Remote Desktop		
Support URL		
🕀 Time Zone Settings		
🕀 Logical Drives		
🕀 Appearance Used In Event Con	sole (A1A)	
Installed Applications		

How Do I Monitor Server/Devices During Local Work Hours Only?

Do the following:

- 1. Configure the time zone settings for each relevant node first
- 2. In the Relator schedule, use 'Schedule Monitoring Task Based On Time Zone Settings Of Monitored Server/Device' in the Relator
- 3. Define time exclusions, such as 00:00-07:59 and 17:00-23:59.

Argent for Shifty ((1.14-1385-A) _ 0
- March -	
Control Information	Relator Definition: REL_DEMO_SLA
Definitions	137
🖶 🚔 Relators	
PRL_DOPO PRL_DPRO_LPC_UPS (Tree Hode) PRL_DPRO_LPRO_L (Les Mode) PRL_DPRO_LPRO_L (Les Mode) PRL_PRO_LPRO_LPRO_L (Les Mode) PRL_PRO_LPRO_LPRO_L (Les Mode) PRL_PRO_LPRO_LPRO_LPS PRO_PRO_LPRO_LPS PRO_PRO_LPRO_LPS PRO_PRO_LPRO_LPS PRO_PRO_LPS PRO_PRO_LPS	I When To Execute This Relator I I I I I I I I I I I I I I I I I I I
A conf, NETWORK, PRINTER A conf, SAMP, DEVICE A conf, SAMP, DEVICE A conf, SAMP, DEVICE A conf, SAMP, VINDOWS A construction A construction A construction A construction Confidence Confi	Enveron 1000 00 And 67 58 59 Edwards 10000 And 67 58 59
Administration	
C Enterprise Objects	
Scheduled Monitoring Tasks	
CMDB-X	
Control Information	C Schedule Monkoing Tasks Based On Time Zone Sentings Of Monkored Server/Device
Reports	What To Run (Rules) When To Run (Schedule) What To Do (Alerts) Advanced Features
Ready	30 Jul 2013 15:13:43 NUM Repetit for SMMP - scheduling Engine on W2008R249/XEN is running

How Do I Detect Whether Application 'XXX' Is Installed?

Most Windows applications always leave some footprint in registry.

Server programs are generally installed as Windows services.

Application detection can be defined either by using the Windows Registry or Windows Service method.

For rare exceptions, use the VBScript method to implement any kind of custom logic.

For Linux/Unix application, the easiest way is to use the TCP Service method.

Using port scanning and simple chat, it is straightforward to pick up well known TCP services such SSH, Telnet, SMTP, POP3, IMAP, HTTP/HTTPS etc.

For applications not exposed to a TCP port, SSH or Telnet method can be used to physically logon to the box to check the existence of running processes.

Argent Guardan Ultra (3.1A	i-1308-A)			- F X
Control Information	Detect Installed	Applications		
Definitions				016
C REL_DEMO_ISERIES (Test Mode)	· Methods To Detect Insta	lad Applications		[]X + 4
REL_DEMO_LINUX (Test Mode)	Name	Group	Method	
Ketwork Connectivity System Baseline	IIS	CORP_COMMUNICATIONS		
The Contract of the Contract o	MSSQL	CORP_DATABASES	Windows Service	
😑 🧰 Monitoring Groups	Oracle	CORP DATABASES	Windows Service	
E C APPLICATION SERVERS	Exchange	CORP_COMMUNICATIONS	Registry	
II D IP	Puppet	CORP_INFRASTRUCTURE	Unix SSH	
II 🧰 LOCAL				
B Constant SMMP				
E CONDA	-	Specify Details OF Ap	okration 🗆 🗙	
E G WINDOWS		specify becauser wh	KING AND	
🕀 🚞 Automatic Report Distributions			C164	·
🛞 🛅 Macros		Application Name:	TISSAN	
Calendars Administration			and the second se	
III - Cin Engine Manager		Display Group	CORP_DATABASES	
- 2 License Manager		Detect Method:	Windows Service	
- Housekeeping		Windows Service:		
- Security 	- C	Windows Service:	(Wildcards " and ? are supported)	
Advanced			(Wildcards " and ? are supported)	
- Argent SuperMaps				
 Enterprise Application View 				
Application Definitions				
Detect Installed Applications Console Application Columns				
Location Definitions				
- 👌 Total Support Interface				
- Stand Argent Instant Help	-	OK	Cancel	
		UK	Cancer	
Events And Alerts				
Enterprise Objects				
Scheduled Monitoring Tasks				
CMDB-X				
Control Information				
Reports				
Ready			31 Jul 2013 15:11:15 NL	UM, Argent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

How Do I Automate Application Detection?

The Argent AT Command Line can run application detection at the command line.

For example, the following command line can pick up applications including Linux/Unix servers and SNMP devices.

ARGENT_DETECTAPP_CLI -all -user user -pswd pswd -snmp v1 -comm public

Put the command line in a product maintenance script, and configure it to run once every x minutes.

How Do I Determine My Network Topology?

Argent Atlas supports network topology generation.

There is an option to scan network topology by polling SNMP managed switches, as well as to maintain topology manually.

MDB-X	CMDB-X						
Display Options	*						
Enterprise Network Display Option	Device Name	Device Type	MAC Address	Port/Interface	Bandwidth Usage (Mb/s)	sysObjectId	
	{default}	Network Segment					
Show All Servers/Devices	ciscoasa (192.168.2.1)	Gateway		G5108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	1.3.6.1.4.1.9.1.745	
Filter By Server/Device Type	☐ GS108T (192.168.2.	5) Switch	00-22-3f-f4-16-2e			1.3.6.1.4.1.4526.100.4.8	
Filter By Network Group	filer.a.local (192	.168.2.1	00-c0-9f-1f-75-de	G5108T (192.168.2.5) - IfIndex(3)	1,000/0.02 (in) - 1,000/0.21 (out)	1.3.6.1.4.1.8072.3.2.10	
Contraction and the second	⊞ Hub#1	Unmanaged Switch/Hub		G5108T (192.168.2.5) - IfIndex(6)			
Filter By Monitoring Group	Hub#2	Unmanaged Switch/Hub		G5108T (192.168.2.5) - IfIndex(4)			
Filter By License Of Current Product	🕀 Hub#3	Unmanaged Switch/Hub		G5108T (192.168.2.5) - IfIndex(1)			
		05	00-0c-29-09-5a-96		1,000/0.23 (in) - 1,000/0.03 (out)		
Update		06	00-50-56-86-00-75		1,000/0.23 (in) - 1,000/0.03 (out)		
	192.168.2.1	87	00-24-e8-75-f4-49		1,000/0.23 (in) - 1,000/0.03 (out)		
Auto Update When Selection Changes		17	00-50-56-86-18-ee		1,000/0.23 (in) - 1,000/0.03 (out)		
Group By: Server/Device	PANA01 (19)	2.168.2.	00-0c-29-21-44-21		1,000/0.23 (in) - 1,000/0.03 (out)		
Citotp By. Maintainfactures	PANA32 (19)	2.168.2.	00-0c-29-55-92-59		1,000/0.23 (in) - 1,000/0.03 (out)		
Filter By:	PANA35 (19)	2.168.2.	00-0c-29-a8-ba-19		1,000/0.23 (in) - 1,000/0.03 (out)		
radiug.	- PANA38 (19)	2.168.2.	00-0c-29-24-52-92		1,000/0.23 (in) - 1,000/0.03 (out)		
Vindows Domain Controllers	PANA53 (19)	2.168.2.	00-0c-29-6e-f7-db		1,000/0.23 (in) - 1,000/0.03 (out)		
Windows Domain Controllers Windows Servers	PANA54 (19)	2.168.2.	00-0c-29-e8-93-40		1,000/0.23 (in) - 1,000/0.03 (out)		
Windows Vorkstations	- PANA60 (19)	2.168.2.	00-0c-29-c4-16-31		1,000/0.23 (in) - 1,000/0.03 (out)		
NT Backup Controllers	PANCLUSTER	R (192.1)	00-0c-29-e8-93-40		1,000/0.23 (in) - 1,000/0.03 (out)		
Solaris Servers	PANSQLCLU:	STER (15	00-0c-29-e8-93-40		1,000/0.23 (in) - 1,000/0.03 (out)		
HP-UX Servers		192.168	00-50-56-86-2c-c2		1,000/0.23 (in) - 1,000/0.03 (out)		
AIX Servers	WS-DEV8 (1	92.168.2	00+0c-29-6a-69-92		1,000/0.23 (in) - 1,000/0.03 (out)		
SCO Servers	openfiler2.a.loca	l (192.1)	00-14-d1-25-83-35	G5108T (192.168.2.5) - IfIndex(5)	1,000/0 (in) - 1,000/0.02 (out)	1.3.6.1.4.1.8072.3.2.10	
Linux Servers	PANWS (192.16)	8.2.188)	00-24-e8-75-f3-28	G5108T (192.168.2.5) - IfIndex(2)	1,000/0 (in) - 1,000/0 (out)		
TCP/IP Addresses	OFFICE390 (192.16)	3.2.34)	00-1d-09-18-0c-37	G5108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)		
iSeries Server							
Cluster Nodes							
Cluster Groups	100						
Cluster Networks							
Select All Deselect All							
Events And Alerts							
Enterprise Objects							
Scheduled Monitoring Tasks							
CMDB-X							
Control Information							

How Can The MAC Address Of A Switch Be Determined?

The Argent Atlas Network Topology shows the MAC address in the column "MAC Address".

How Can A DMZ Topology Be Added To Argent Atlas?

If the DMZ topology cannot be directly added by the Argent AT engine due to router settings, do the following:

1: Copy ARGSOFT_SNMP_TOPOLOGY.EXE to any machine in the DMZ

2: Run ARGSOFT_SNMP_TOPOLOGY.EXE generating found_snmp_topology.xml

3: Import found_snmp_topology.xml into Network Topology

This topic is about discovering network topology.

Also see "There are Many Devices in the DMZ; They Cannot Be Scanned By The Argent AT Engine; There Are Too Many To Add Manually.", which is about discovering <u>all</u> active IP devices.

How Can All the SNMP Devices In The Network Be Determined Without Installing Argent For SNMP?

See topic, "How Can A DMZ Topology Be Added To Argent Atlas" and use the same approach of importing the generated found_snmp_topology.xml file.

I Have Been Alerted With A Flood Of Alerts When A Switch Went Bad. How Can Argent AT Just Tell Me That Switch Is Bad?

Turn on the option Execute Topology Root Cause Analysis And Suppress Alert Accordingly in the Relator.

Argent Guardian Ultra (3.1A-	308-A) X
Control Information	Relator Definition: REL_IP_CONNECT (Test Mode)
Definitions	G70
🖃 🚞 Rules	
😑 🚞 Windows Rules	If Prerequisite Rules Fail Mark Servers As The Same Status Of Previous Check 🚽
🕀 🛅 Performance Rules	
🗈 🧰 Service Level Agreement Rules	Execute Topology Root Cause Analysis And Suppress Alert Accordingly
🗈 🚞 Service Rules	 Relator Trigger
🗄 🚞 System Command Rules	
🗄 💼 System Down Rules	T If Any Of Rules Are Broken, Execute Relator
System File Rules Service Pack Rules	
	(e) Once
Gerver Connectivity Roles System Management Scripts	🕐 Once Every 5 😓 Minutes For 60 🔿 Minutes
E C Registry Rules	
Windows Printer Share	Execute Relator Only For The Node That Breaks The Rules
Windows Process	
Contraction of the second	
🗄 🛅 iSeries Rules	Description
E P Relators	
🕀 💼 Advanced Monitoring	
🗄 🛅 DEMO	
😑 🚞 Network Connectivity	
REL_IP_CONNECT (Test Mode)	
REL_ISERIES_CONNECT (Test Mode)	
REL_WINDOWS_API_CONNECT (Test Mode)	
🗄 🧰 System Baseline	
Alerts Monitoring Groups	
Automatic Report Distributions	
Addinade Report Distributions Addinade Report Distributions	T. T
Calendars	
Administration	
🗄 🛅 Engine Manager	×
Events And Alerts	
Enterprise Objects	
Scheduled Monitoring Tasks	
CMDB-X	
Control Information	
Reports	What To Run (Rules) When To Run (Schedule) What To Do (Alerts) Advanced Features
Ready	1 Aug 2013 11:07:00 NUM Arcent Guardian Ultra - Scheduling Engine on W2008R264XEN is running

Root cause analysis relies on the topology dependency being accurate. Therefore it is essential to maintain the accuracy of the network topology by using Argent's automatic scanning facilities. Discuss with an Argent engineer to learn more about these facilities.

Appendix A – Networking Scanning

Scan Windows Network Using Active Directory

The most convenient way to add a bulk of server/devices into Argent Atlas is to scan the network.

Windows Do Windows Se Windows Wo NT Backup (orkstations	 Printer Queues Windows 9x Systems Unknown Systems 	
Only Find Co	mputers In The Ac	ive Directory Container:	
Use Explicit [) omain Account	(Example: LDAP://cn=com	puters,ou=Asia,dc=domain)
Itering Option:	Find Computers I	n Domains	
ane samanan	1		
Use FDQN N		(Separated By Comma)	
Active Dire	ctory Networ	Browser ICMP Ping Windows Cluster Exte	mal File VMware
Ignored	Machine	Domain Type	. Vendo
	PANA01	A Windo	ows Domain Controllers Microso
	PANA32	Argent for VMware (3.1A-1308-A)	x
Lines 1	WS-DEV8	Argenetor (mware (3.1A-1300-A)	~
	PANWS	Windows network scanning completer	t successfullu
	PANWS EX2007	Windows network scanning completed	d successfully.
		Windows network scanning completed	d successfully.
	EX2007	Windows network scanning completer	d successfully.
	EX2007 PANA36		d successfully.

Scanning Options

Save To Network Group

Specifies the Network Group that the scanning result will be save to.

Keep Original Network Group

If a found server/device is already in the CMDB-X, it will be moved to a new Network Group specified in 'Save To Network Group' with this option unchecked. The default is checked.

Only Find Computers In The Active Directory Container

This option can be useful for a very big Active Directory network, where a specific container can be targeted

Filter Option

Customers can specify whether to find computers for specific domains.

Use FDQN Name Format

Some networks require FDQN name due to DNS configuration. For example, if the option is checked, machine 'PANA01' is saved as 'pana01.a.local'.

Use Explicit Domain Account

This option is useful when the Argent AT engine is in a workgroup, or customers try to scan computers at another domain. Customers need to enter the logon credentials and domain controller before the actual scanning.

Scan Windows Network Using Network Browser

Using Network Browser is another method to scan Windows network.

It is useful for workgroup environments.

It is not recommended for Domain environments, as it is less reliable than the Active Directory method.

All scanning options on screen are self-explanatory.

Worldwide	e Enterprise Network Scanning					X
						V12
✓ Wind✓ Wind	lows Domain Controllers lows Servers lows Workstations ackup Controllers	Printer Q V Windows V Unknown	9x Systems			
Option:	Find Computers In Domains	*				
	Only Find Print Queues Of imeout For Querying Node (sectory Pre Directory Network Brow	Node: *	ited By Comma)	ter External File	VMware	
Ign	ored Machine	Doma	in	Туре	1	Vendor
•						•
Save To	Network Group: First Network	Group	👻 🔽 Kee	ep Original Network	Group	

Scan TCP/IP Network Using ICMP Ping

This method scans the whole TCP/IP network segment by pinging each possible IP address in the segment.

All scanning options on screen are self-explanatory.

Worldwide Enterprise	Network Scanning				x
					/12
IP Address Range:	192 , 168 , 2	, 1 - 192 ,	168 , 2 , 254		
: Subnet:	255 , 255 , 255	. 0			
Timeout (seconds):	10 🚖				
Retry:	0				
Thread Limit:	128				
Active Directory	Network Browser	ICMP Ping Window	vs Cluster 👢 External File	VMware	_
	I NEWUK DIUWSEL				
	Machine	Domain	Type	Vendo)r
)r
					or
)r
	Machine	Domain		Vendo	
Ignored	Machine	Domain	Туре	Vendo	

Scan Windows Cluster Objects

Argent AT scans Windows Cluster Objects using either native WIN32 API or Failover Cluster WMI Provider.

Native WIN32 API is faster but requires both Argent AT engine and Windows Cluster run the same Windows operating system -- Cluster API on W2003 works only for W2003 cluster. Cluster API on W2008 works only for W2008 cluster. If customer has mixed cluster versions, or AT on W2008 and cluster is W2003, native API won't work.

"Failover Cluster WMI Provider" works for all Windows versions. But it requires the Windows Cluster to allow the Argent AT service account access to its WMI name space 'root\mscluster'.

It is recommended to use 'Failover Cluster WMI Provider' in a mixed W2003 and W2008 environment.

Worldwide Enterp	ise Network Scanning			x
Cluster Node	5/6			V12
Cluster Group Cluster Netwo Cluster Netwo Cluster Reso	orks ork Interfaces			
Cluster Names:	PANCLUSTER	ICMP Ping Windows	Use Failover Cluster WN	1l Provider
Ignored	Machine	Domain	Тупе	Vendr 🔶
	PANA54	Argent for VMware (3.1A-13	308-A)	X
	PANA53			E.
	Group 0	Windows clust	er scanning completed successfully.	P
	Cluster Group			
	Local Area Connectio			
	Local Area Connectio			
	Local Area Connectio	and the second	Cluster Networks	
	Local Area Connectio	on 2 - PAN PANCLUSTER	Cluster Network Interfaces	-
4	- IIII			•
Save To Network	Group: First Network	Group 👻	Keep Original Network Group	

Scan Network Using SNMP Discovery

Argent for SNMP discovers SNMP devices by querying well-known OIDs for each possible IP address in the specified network segment.

If it discovers nothing, customers should go through the following checklist:

- 1. Is the current machine a management workstation for SNMP devices? This has to be configured on each SNMP device. Contact the Network Administrator.
- 2. Is it the right SNMP protocol? v1, v2c or v3.
- 3. If it is SNMP v1 or v2c, is the community string specified correctly? Community string is like the password for SNMPv1 and v2c.
- 4. If it is SNMPv3, there are more passwords, authentication and encryption protocols to specify.

iawide Enterprise Net	twork Scanning					
Query OID:	1.3.6.1.2.1.1.5.0			Protoco	: SNMPv1	
Community:	public			User Name	e [
SNMP Port:	161 🤶			Auth. Password	t:	None
Timeout (seconds):	10 🚖			Encryption Password	:	None
Thread Limit:	999 🜻				Active Po	II Each IP Addres
Scan IP Range:	192 . 168 .	2.1 -	192	. 168 . 2 . 254	/ 255 . 2	55.255.0
	Network Browser	ICMP Ping	-	ws Cluster External		
	Network Browser	Doma	-	vs Cluster External		
			-			
			-			
			-			
			-			
	chine		-			Vendo
	chine	Doma	-			
	uchine III	Doma	-			

Scan VMware Objects

Argent AT scans VMware objects through VMware PowerCLI.

It is easier to scan vCenter than individual ESX hosts, as it	t returns all objects on all included ESX hosts.
---	--

Worldwide Enterprise Netw	vork Scanning				x
					V12
vCenter Or ESX Host:	192.168.2.187				
Logon:	root	Port:	443	Protocol:	https
Password:	•••••	Domain:	VMware		
Scan Selected Objects:				r VM Types	
		ux/UNIX VM	C.		
	1				
Active Directory N	etwork Browser 👢 ICMP Ping 👢 Windo	ws Cluster	External File VMv	vare	
		ws Cluster		vare	iner des
Active Directory N Ignored Mac		ws Cluster	External File VMv	vare	Vendor
		ws Cluster		vare	Vendor
		ws Cluster		vare	Vendor
		ws Cluster		vare	Vendor
		ws Cluster		vare	Vendor
		ws Cluster		vare	Vendor
		ws Cluster		vare	¥endor
Ignored Mac	hine Domain				¥endor ↓

Scanning Options

vCenter or ESX Host

This option determines where the result will be read from.

Logon/Password

Logon credential for PowerCLI session.

Port

TCP/IP port used by PowerCLI session. The default value is 443.

Protocol

The web service protocol. It is either 'https' or 'http'.

Domain

It specifies the domain of found VMware object. The default value is 'VMware'.

Use VM Guest Host Name For CMDB-X

VM name can be different from the VM guest host name.

For example, a VM machine named 'W2008R2DEV 212/212' has the host name 'W2008R2DEV'.

The VM machine name is defined in VMware Sphere, while host name is specified when the OS is installed.

Do Not Populate Alternative IP for Linux Guest VM

Alternative IP field is not filled for Linux VM if this option is checked. It is useful when the VM has multiple NIC cards, and the customer does not want to use the main IP address.

Import And Export CMDB-X Data

Export CMDB-X Data

For backup purposes or exchanging data between installations, customers can export CMDB-X data to an XML file.

CMDB-X	CMDB-X						
Display Options	*						
Enterprise Network Display Option	Network Group	Server/Device	Domain	Туре	Location	Yendor	Make
Show All Servers/Devices	Demo URLs						
	Demo Web Servers						
Filter By Server/Device Type	First Network Group	DBMMIRR	A	In the design of the second second	NEU SODK	Minute and the	100 states
Filter By Network Group		DBMPRIN	A	Windows Servers Windows Servers	NEW YORK NEW YORK	Microsoft Microsoft	Windows Windows
Filter By Monitoring Group		DBMWIT	A	Windows Servers	NEW YORK	Microsoft	Windows
Filter By License Of Current Product		DELL4WAY	A	Windows Servers	NEW YORK	Microsoft	Windows
O The by clease of conerci found		EX2007	A	Windows Servers	NEW YORK	Microsoft	Windows
Update		ORCL10	A	Windows Servers	NEW YORK	Microsoft	Windows
		PANA01		Windows Domain Controllers	NEW YORK	Microsoft	Windows
Auto Update When Selection Changes		PANA32	Add Server Or Device	Windows Servers	NEW YORK	Microsoft	Windows
		PANA35	Delete This Server Or Device	Windows Workstations	NEW YORK	Microsoft	Windows
Group By: Server/Device 👻		PANA36		Windows Servers	NEW YORK	Microsoft	Windows
Filter By:		PANA40	Scan Or Import Network	Windows Workstations	NEW YORK	Microsoft	Windows
Filter By:		PANA60	Export CMDB-X	Windows Servers	NEW YORK	Microsoft	Windows
		PANWS	CMDB-X Properties	Windows Servers	NEW YORK	Microsoft	Windows
Windows Domain Controllers		SP2010	CMDB-X Propercies	Windows Servers	NEW YORK	Microsoft	Windows
Windows Servers Windows Workstations		utestserver	Add New Network Group	Linux Servers	NEW YORK		
INT Backup Controllers		W2003R2XEN	Delete This Network Group	Windows Servers	NEW YORK	Microsoft	Windows
Solaris Servers		W2008DEV-64	Bename	Windows Servers	NEW YORK	Microsoft	Windows
HP-UX Servers		W2008R264XEN	Rename	Windows Servers	NEW YORK	Microsoft	Windows
AIX Servers		W2008R2DEV	Assign Network Group	Windows Servers	NEW YORK	Microsoft	Windows
SCD Servers	-	W7-32-PL2	Detect Installed Applications	Windows Servers	NEW YORK	Microsoft	Windows
	in the second	WS-DEV8		Windows Servers	NEW YORK	Microsoft	Windows
			Security Settings				
	SNMP		Toggle Full Screen				
	VMware						
Unur Serves Serves Serves Server Server Server Server Server Server Server Sever Sever	▼ ^{II} ^{VMware}		Detect Installed Applications Security Settings Toggle Full Screen				
Enterprise Objects Scheduled Monitoring Tasks							
CMDB-X							
Control Information							

The exported CMDB-X data is stored in XML format. A sample XML is shown as follows:

C:\TEMP\w.xml	P to CitEMP(w.smi X	
model at="w2008B264XE	N" created_by="A\Administrator" create_time="30 Jul 2013 09:51:35">	
<pre>- <group name="Demo URLs"></group></pre>	A Created_by- A (Administrator Create_line - 30 Jul 2013 05.31.33 2	
	EVISION" tz="-8" location="BURBANK" type="URL Object" domain="A"/>	
	"tz="5" location="New YORK" type="URL Object domain="A"/>	
	HELP" tz="-6" location="HOUSTON" type="URL Object" domain="A"/>	
	AMERICA" tz="-8" location="WALNUT CREEK" type="URL Object" domain="A"/>	
	F_CHINA" tz="8" location="CHINA" type="URL Object" domain="A"/>	
	="-5" location="ELMHURST" type="URL Object" domain="A"/>	
<node name="URL_CNN" tz="</td"><td>"-5" location="RESTON" type="URL Object" domain="A"/></td><td></td></node>	"-5" location="RESTON" type="URL Object" domain="A"/>	
<node domain="A" location="NEW YORK" name="URL_FINANCI</td><td>AL_TIMES" type="URL Object" tz="-5"></node>		
	O_SERVER_1" tz="8" location="HONG KONG" type="URL Object" domain="A"/>	
	O_SERVER_2" tz="8" location="HONG KONG" type="URL Object" domain="A"/>	
	O_SERVER_3" tz="8" location="HONG KONG" type="URL Object" domain="A"/>	
	O_SERVER_4" tz="8" location="HONG KONG" type="URL Object" domain="A"/>	
	"-5" location="UNITED STATES" type="URL Object" domain="A"/>	
	NION" tz="-5" location="ALBANY" type="URL Object" domain="A"/>	
	REET_JOURNAL" tz="-5" location="MONMOUTH JUNCTION" type="URL Object" domain="A"/>	
	GTON_MUTUAL! 'tz="-8" location="SEATTLE" type="URL object" domain="A"/>	
	zz="-5" location="SUNNYVALE - CALIFORNIA" type="URL Object" domain="A"/>	
<pre> </pre>		
	" tz="-5" location="NEW YORK" type="Cluster Groups" domain="PANCLUSTER" alias="Cluster Group"/>	
	ters" to "solo = 'NEW YORK" type="Cluster Resource" International a solution of the solution o	
	tz="-5" location=""NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Cluster Name"/>	
	" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Disk 0:"/>	
<node alias="Disk S:" domain="PANCLUSTER" location="NEW YORK" name="Disk S:" type="Cluster Resource" tz="-5</td><td>"></node>		
<node alias="Group 0" domain="PANCLUSTER" location="NEW YORK" name="Group 0" type="Cluster Groups" tz="-</td><td>5"></node>		
<node alias="Local Area Connection" domain="PANCLUSTER" location="NEW YORK" name="Local Area Con</td><td>nnection" type="Cluster Networks" tz="-5"></node>		
	nnection - PANA53" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection - PANA53"/>	
	nnection - PANA54" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection - PANA54"/>	
	nnection 2" tz="-5" location="NEW YORK" type="Cluster Networks" domain="PANCLUSTER" alias="Local Area Connection 2"/>	
	nnection 2 - PANA53" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 2 - PANA53"/>	
	mection 2 - PANA54" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 2 - PANA54"/>	
	mection 3" tz="-5" location="NEW YORK" type="Cluster Networks" domain="PANCLUSTER" alias="Local Area Connection 3"/>	
	nection 3 - PANA53* tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 3 - PANA53"/> Inection 3 - PANA54" tz="-5" location="NEW YORK" type="Cluster Network Interfaces" domain="PANCLUSTER" alias="Local Area Connection 3 - PANA54"/>	
	mections - PARASA (2= 5) locations - New York (yp= closer reterrates domains - PARCISTER and - Local Area connections - PARASA (2= 5) locations - NEW YORK (type= "Windows" servers" domains 'A" allas= "PARASA" model="Windows" server 2003" make="Windows" vendor="Windows" vendos="Windows" vendos="Windows" vendos="Windows" vendos="Windows" vendos="	
	5" location="NEW YORK" type="Windows Servers" domain="A" alas="PANA54\$" model="Windows Server 2003" make="Windows" vendor="Microsoft"/>	
	s (PANSOLCLUSTER)" tz="5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="Sol IP Address 1 (PANSOLCLUSTER)"/>	
	name (PARSQLCLOSTER)" tz="-5" location="NEW YORK" type="cluster Resource" domain="PARCLUSTER" alias="SOL Network Name (PARSQLCLOSTER)"/>	
	="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL Server"/>	
	ent" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" allas="SQL Server Agent"/>	
	litext" tz="-5" location="NEW YORK" type="Cluster Resource" domain="PANCLUSTER" alias="SQL Server Fulltext"/>	
<pre><group name="SNMP"></group></pre>		
	" tz="-5" location="NEW YORK" type="TCP/IP Addresses" domain="SNMP" alias="filer.a.local" model="UCD-SNMP" make="Server and Workstation" vendor="Li	INUX Server"
sysobjectid="1.3.6.1.4.1.8	072.3.2.10"/>	

Import CMDB-X Data

Use 'Scan Or Import Network' to bring up network scanning dialog box, then select the tab 'External File'.

ile Path: 🛛	C:\TEMP\w.xml			
~	Option			
	Import Network XML			
	Import Computer Text File	(Advanced Feature)		
	You may either manually (edit COMPUTER.TXT		
	or run the customized AR	GSOFT_NETWORKSCAN.VE	3S to generate this file	
4				
Active Dire	ectory Network Browser	ICMP Ping 🔍 Windows Clust	er External File	
				Vendr
Active Dire	Ctory Network Browser Machine 192,168,2,187	ICMP Ping Windows Clust Domain VMware	er External File Type	
	Machine	Domain	Type ESX Host	Vendo VMwar LINUX
Ignored	Machine 192.168.2.187	Domain VMware	Туре	4.00000.00
Ignored	Machine 192.168.2.187 192.168.2.189	Domain VMware SNMP	Type ESX Host TCP/IP Addresses	VMwar LINUX
Ignored	Machine 192.168.2.187 192.168.2.189 192.168.2.211	Domain VMware SNMP SNMP	Type ESX Host TCP/IP Addresses TCP/IP Addresses	VMwar LINUX LINUX {1.3.6
Ignored	Machine 192.168.2.187 192.168.2.189 192.168.2.211 192.168.2.3	Domain VMware SNMP SNMP SNMP	Type ESX Host TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses	VMwar LINUX LINUX
Ignored	Machine 192.168.2.187 192.168.2.189 192.168.2.211 192.168.2.3 192.168.2.5	Domain VMware SNMP SNMP SNMP SNMP SNMP SNMP	Type ESX Host TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses	VMwar LINUX LINUX {1.3.6 Netgea
Ignored	Machine 192.168.2.187 192.168.2.189 192.168.2.211 192.168.2.3 192.168.2.5 AppPool	Domain VMware SNMP SNMP SNMP SNMP SNMP SNMP VMware	Type ESX Host TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses ESX Resource Pool	VMwar LINUX LINUX {1.3.6 Netgea
Ignored	Machine 192.168.2.187 192.168.2.189 192.168.2.211 192.168.2.3 192.168.2.5 AppPool Cluster Group	Domain VMware SNMP SNMP SNMP SNMP SNMP VMware PANCLUSTER	Type ESX Host TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses TCP/IP Addresses ESX Resource Pool Cluster Groups	VMwar LINUX LINUX {1.3.6 Netgea

Use the option 'Import Network XML' if the XML file is an exported XML file from Argent AT or Argent XT.

Argent AT can also import the nodes from a text file, which is very useful for importing from external sources such as SQL queries, Excel files, etc.

COMPUTERS.TXT Format

Each line consists of 5 fields separated by a TAB.

- Field 1: Domain
- Field 2: Server/Device Name
- Field 3: Make
- Field 4: Model
- Field 5: Node Type.

It can be any of following:

- TCP or TCP/IP IP Address
- SUNOS or SOLARIS Sun Solaris OS
- HP-UX or HPUX HP-UX OS
- AIX AIX OS
- SCO SCO Unix
- LINUX Linux
- PDC Windows Domain Controller

Note: if the string contains 'Professional' or 'XP', it is deemed as Windows Workstation, otherwise, Windows Server.

A sample COMPUTERS.TXT is shown as follows:

COMPUTERS.TXT - Notepad		_ 🗆 🗙
Idc=a,dc=local PANA32 windows dc=a,dc=local WS-DEV8 windows dc=a,dc=local PANWS windows dc=a,dc=local PANA36 windows dc=a,dc=local PANA36 windows dc=a,dc=local PANA36 windows dc=a,dc=local PANA40 windows dc=a,dc=local DBMPRIN windows dc=a,dc=local DBMNIRR windows dc=a,dc=local PANA54 windows dc=a,dc=local PANA54 windows dc=a,dc=local PANA60 windows dc=a,dc=local PANA54 windows dc=a,dc=local PANA54 windows dc=a,dc=local PANA60 windows dc=a,dc=local PANA35 Windows	Server 2003 5.2 (3790) NON-PDC Server 2003 5.2 (3790) NON-PDC 7 Professional 6.1 (7600) NON-PDC 2000 Professional 5.0 (2195) NON-PDC Server 2003 5.2 (3790) NON-PDC	A
4		v

It can be imported into the CMDB-X similar to the Network XML file.

e Path: C:\	And Linn Argeniconsole	COMPUTERS.TXT			
с I	Option				
	Import Network XML				
(Import Computer Text	File (Advanced Feature)			
	You may either manua	ally edit COMPUTER.TXT			
	·	-			
	or run the customized	ARGSOFT_NETWORKSCAN.VBS	δ to generate this file		
<u> </u>					
Active Direct	ory Network Browser	LICMP Ping Windows Cluster	External File		
				Vendor	Make
	ory Network Browser Machine PANA01	ICMP Ping Windows Cluster Domain dc=a,dc=local	External File Type Windows Domain Controllers	Vendor Microsoft	Make Windows Server®
	Machine	Domain	Туре		Windows Server®
Ignored	Machine PANA01	Domain dc=a,dc=local	Type Windows Domain Controllers	Microsoft	Windows Server® Windows Server 20
Ignored	Machine PANA01 PANA32	Domain dc=a,dc=local dc=a,dc=local	Type Windows Domain Controllers Windows Servers	Microsoft Microsoft	
Ignored	Machine PANA01 PANA32 WS-DEV8	Domain dc=a,dc=local dc=a,dc=local dc=a,dc=local	Type Windows Domain Controllers Windows Servers Windows Servers	Microsoft Microsoft Microsoft	Windows Server® Windows Server 20 Windows Server 20 Windows Server 20
Ignored	Machine PANA01 PANA32 WS-DEV8 PANWS	Domain dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local	Type Windows Domain Controllers Windows Servers Windows Servers Windows Servers Windows Servers	Microsoft Microsoft Microsoft Microsoft	Windows Server® Windows Server 20 Windows Server 20
Ignored	Machine PANA01 PANA32 WS-DEV8 PANWS EX2007	Domain dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local	Type Windows Domain Controllers Windows Servers	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Windows Server® Windows Server 20 Windows Server 20 Windows Server 20 Windows Server 20 Windows Server 20 Windows 7 Profess
Ignored	Machine PANA01 PANA32 WS-DEV8 PANWS EX2007 PANA36	Domain dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local dc=a,dc=local	Type Windows Domain Controllers Windows Servers	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Windows Server® Windows Server 20 Windows Server 20 Windows Server 20 Windows Server 20 Windows Server 20
Ignored	Machine PANA01 PANA32 WS-DEV8 PANWS EX2007 PANA36 PANA40	Domain dc=a,dc=local dc=a,dc=local	Type Windows Domain Controllers Windows Servers Windows Workstations Windows Workstations	Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Windows Server Windows Server Windows Server Windows Server Windows Server Windows 7 Prof Windows 2000 f

Upload Remote Network Information From Daughter Engine

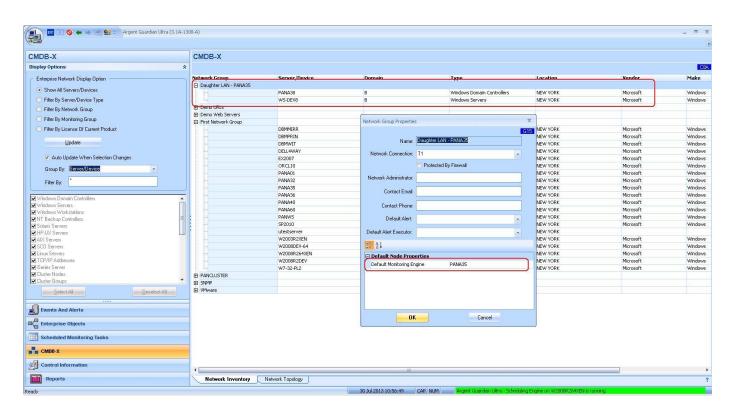
Most of the time it is not feasible to directly scan the remote network from the Argent AT Main Engine.

That is the main reason that customers install the Daughter Engine in the first place.

To include the remote network in the central CMDB-X, customers should scan the network at the Daughter site and upload the network information directly from the GUI.

📄 📴 💽 🛇 🗰 🔿 🤮 = 🖓 Argent Guardian Ultra (3	1A-1308-A)							ат. З
CMDB-X	CMDB-X							
Display Options	Read-Only (Daughter Engine Inst	allation						_
C Enterprise Network Display Option	Network Group	Server/Device	Domain	Туре	Location		Vendor	Make
	Daughter LAN - PANA35							
 Show All Servers/Devices 	_							
Filter By Server/Device Type	Wor	dwide Enterprise Network Scann	ing		×			
Filter By Network Group					612			
Filter By Monitoring Group	P							
Filter By License Of Current Product		Windows Domain Controllers	Printer Queues					
		Windows Servers Windows Workstations	✓ Windows 9x Systems ✓ Unknown Systems					
Update		NT Backup Controllers	Onknown Systems					
Auto Update When Selection Changes		Only Find Computers In The Acti	ve Directoru Container					
Group By: Server/Device								
-	V	Use Explicit Domain Account	(Example: I	DAP://cn=computers.ou=Asia.dc=dom	iain)			
Filter By:	Filt	ering Option: Find Computers In	Domains 👻 🔭					
		Use FDON Name Format	(Separated	Pu Commo)				
Windows Domain Controllers		Use r Digini indille r utilidi		by commaj				
Vindows Servers		Active Directory Network	Browser LICMP Pina Windows	Cluster External File				
NT Backup Controllers		Ignored Machine	Domain	Туре	Vendor			
Solaris Servers	:	PANA38	B	Windows Domain Controllers				
HP-UX Servers	-	WS-DEV8	D D	Windows Servers	Microsoft			
AIX Servers		WJ-DEV0	Argent Guardian Ultra (3.1A-1308-			Y		
SCD Servers			Argenic duardian oldra (3.1A-1500-					
Linux Servers TCP/IP Addresses			Successfully write out	scanning result file. It should be upload	ed to main engine in a few minutes			
Series Server				and the second				
Cluster Nodes			Would you like to wai	until it is uploaded?				
Cluster Groups								
Cluster Networks	1							
Cluster Network Interfaces				Yes	No			
Cluster Resource	Sa	ve To Network Group: Daughte	a la	(L				
Printer Queues Windows 9x Systems								
Novel Systems		Scan Network	Step Scanning	Save Close				
VIRL Object		Coun House	ojop douring	gare gote				
Select All Deselect All								
Scheduled Monitoring Tasks								
CMDB-X								
Control Information	•			ill.				

After successful uploading the information, the remote network information shows up in the central CMDB-X.



Appendix B - Network Group

A Network Group is a logical group to organize server/devices within the same network. Network Groups can be modeled using whatever logic that customers sees fit.

Typical examples include:

- Server/device locations such as main office and remote offices.
- Related services such as Exchange, SQL Server, Oracle, Web etc.
- Management teams such as Enterprise, Linux, Sales department etc.

	14		V	ľ	
Name:	First Netwo	ork Group			
Network Connection:	T1				
	Protect	ted By Firewall	1000		
Network Administrator:	admin	admin			
Contact Email:	admin@a.	local			
Contact Phone:	(800) 674-	(800) 674-1234			
Default Alert:	EMAIL_G	ENERAL	-		
efault Alert Executor:	2				
1 2↓					
] Default Node Prop	erties			and the second s	
Default Monitoring En	igine			1	
vCenter or ESX Host		192.168.2.101			
Port			443		
Protocol		https			
Logon User		A\Administrator			
Password		****			

Use context menu 'Properties' to view or update Network Group properties.

Default Monitoring Engine

This is the most important setting in Mother/Daughter architecture.

When customers uses '{Dynamic}' as the Monitoring Engine in a Relator, Argent AT needs this information to determine which engine should monitor the node in a Relator.

If the Default Monitoring Engine belongs to a Mother Engine, the Mother Engine will schedule the task; if it belongs to Daughter Engine, the Daughter Engine will schedule the task.

🚛 💷 🔇 🖛 🔿 🐏 😫 🗸 Argent Guardian Ultra (3.1A-1308-A)								_ = ×
Control Information	Relator Definition: F	REL_DEMO_LINUX (Te	est Mode)						1
Definitions		e Scheduled Until Changed To Pro							G7A
Windows Rules Derformance Rules	Preroquisite Rules - All Th	ese Rules Must Pass For Mair	- Pular:						
🗉 🧰 Service Level Agreement Rules	Rule	Type		tant Correction	Alert	Death	Cause Analysis		
🗈 🧰 Service Rules	Kule	туре	116	cant correction	Alert	KUUL	Lause Analysis		
😟 🛅 System Command Rules 🗄 🖶 System Down Rules									
E C System File Rules					Client/Monitoring Er	noine Detail		×	
😥 🚞 Service Pack Rules								G7X	
E 🛅 Server Connectivity Rules					10000	Protection and the second s			
😟 🛅 System Management Scripts 🗄 💼 Registry Rules					Monitoring Group:	MG_LINUX			
🗄 🧰 Windows Printer Share					Monitoring Engine	(Dynamic)			
🚊 🚞 Windows Process	🔄 Run Prerequisite Rules On C	Custom Node:			Backup Monitoring	Engines:			
E Contraction Contraction Contraction	Main Rules:	La			W2008R264X	EN .			
E Calebra Relators	Rule	Туре	To	tant Correction					
🕀 🚞 Advanced Monitoring	SCP LINUX DEMO	UNIX		concerned on	-				
REL DEMO									
REL_DEMO_ISERIES (Test Mode)									
REL_DEMO_LINUX (Test Mode)	÷								
Retwork Connectivity	2				🔲 If Monitoring Er	ngine Is Installed, Use Local Eng	ane		
🕀 🧰 System Baseline 🖲 🧰 Alerts						-			
E Contoring Groups					<u></u> 0K		Cancel		
🕀 🚞 Automatic Report Distributions					-				
Gendars	Monitoring Group List								*= 🗙 🗲
Calcindars Calcindars Calcindars Calcindars Calcindars	Monitoring Group	Node Type	Excluded	Monitoring Engin	e	Backup Monitoring Engines	Use Local	If Installed	
🔤 🤮 Argent Instant Help	BMG_LINUX			{Dynamic}					
240	utestserver	Linux Servers)				
Events And Alerts									
Enterprise Objects									
Scheduled Monitoring Tasks									
-	🚽 🦳 How To Run Monitoring Tasl	ks							
CMDB-X	Spawn New Monitor Engl	ine Process							
S. A. M. C. M.		ne Process In Pool : (Dynamic)							
Control Information	Chose shared monitor Engli	is not south in the state of the							
Reports	What To Run (Rules)	When To Run (Schedule)	What To Do (Alerts)	Advanced Feature	:5				
Ready				29 Jul 2013 12:41:33	NUM	Argent Guardian Ultra - Scheo	duling Engine on W200	IBR264XEN is running	

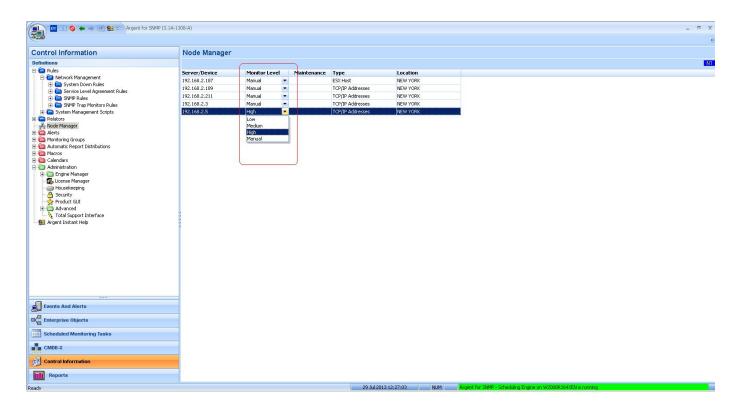
Default Alert

For Argent for SNMP, some monitoring tasks can be automatically generated.

As SNMP covers a wide universe of devices, Argent can automatically generate Alerts – see the topic "How To Specify What Alert To Fire When Doing Automated Monitoring In Argent for SNMP" for details.

Customers can select a monitoring level at the Node Manager, and the Argent for SNMP engine can use the synthetically generated Relator to perform the monitoring. Because the synthetically generated internal Relator does not exist physically, the engine needs to know what alert to fire if the Rule is broken. The Default Alert is used here.

Note: There is also an option to define the Default Alert at the node level. The one in the Network Group level is used only if it is not defined at the node level.



Default Alert Executor

When customers use Argent Alert Executors to fire and Alert without explicitly specifying the Executor, the Argent Console engine uses **Default Alert Executor** to determine which Alert Executor to use.

Note: **Default Alert Executor** is also defined in the node level. The node takes precedence – if specified at the node level and at the Network Group level, then the node level is used only if it is not defined at the node level.

👔 🖭 🔕 🗲 🔿 🕺 😫 🖘 Argent Guardian Ultra	a (3.1A-1308-A)	- a x
	Dublin Dublin DEL DEMO LINUX (Trut Multi)	(1
Control Information	Relator Definition: REL_DEMO_LINUX (Test Mode)	
Definitions		G7C
E Carlos	Notification And Correction Alerts (0r Alert Macros) To Fire, In Following Order:	
🖹 🗁 Windows Rules		
Gervice Level Agreement Rules	Fire Sustem Alam Alert ALARM DEMO Fire SMS Alert SMS_USA_MOBILE (Node Specific)	
🗄 🫅 Service Rules		and a second
😟 🛅 System Command Rules		
🗈 🧰 System Down Rules		
🖻 🛅 System File Rules 🗄 🛅 Service Pack Rules		
E Server Connectivity Rules	Select An Alert Or Alert Macro	
🗉 🛅 System Management Scripts	Alert Or Alert Macro Optional Time	
🗈 🚞 Registry Rules		
B		
	Alerts	
E iSeries Rules		
🖃 🗁 Relators	B- C Apharumeric Pager	
🗄 🧰 Advanced Monitoring	🖽 🗖 🖼 Email	
	B B Event Log	
REL DEMO	👻 🕞 🚔 Help Desk	
REL_DEMO_LINUX (Test Mode)	e Sustanti de la constanti de	
🕀 🧰 Network Connectivity	Relator Recheck Settings	
🕀 🧰 System Baseline	Event Priority: Low SMS_USA_MOBILE	
Alerts Monitoring Groups		
Generatic Report Distributions		
Accondic report bischoddoris	Alert Escalation Plan: Execute This Alert At: Node Specific Engine	
🖲 🧰 Calendars		
Administration		
Search Argent Instant Help		
	You can also Drag and Drop an Alett or Alet Macro from the tree	
Events And Alerts		
Enterprise Objects		
Scheduled Monitoring Tasks		
CMDB-X		
Control Information		
Reports	What To Run (Rules) When To Run (Schedule) What To Do (Alerts) Advanced Features	
Ready	29 Jul 2013 12:39:42 NUM Arcent Guardian Ultra Scheduling Engine on W2008R264/EN is running	
(rosa)		

Product Specific Properties

There may be additional product-specific properties in the list of Default Node Properties. For example, Argent for SNMP has SNMP version, community string etc, Argent for VMware has VMware logon credentials.

The properties are used when the same information is not explicitly specified at the node level.

Network Group Properties	5		x		
			V15		
Name:	First Network	Group			
Network Connection:	T1		-		
	Protected By Firewall				
Network Administrator:	admin	admin			
Contact Email:	admin@a.loca	al			
Contact Phone:	(800) 674-1234				
Default Alert:	EMAIL_GENE	ERAL			
Default Alert Executor:			-		
₽ 2↓					
🖃 Default Node Prop	erties		<u> </u>		
Default Monitoring En	gine				
vCenter or ESX Host		192.168.2.101]		
Port			443		
Protocol		https			
Logon User		A\Administrator	L		
Password		****	,		
ОК		Cancel			

Display-Only Properties

The following fields can be used for customers' own purposes:

- Network Connection
- Protected By Firewall
- Network Administrator
- Contact Email
- Contact Phone

Appendix C - CMDB-X Node Properties

Node properties defined in CMDB-X are shared among Argent AT products.

The properties vary based on the type of node.

Windows Machine

2↓	
Windows Machine	
Name	W2008R264XEN
Domain	A
O5	Windows Servers
NetBios Name	
Internal Name	
Alias	
Alternative IP	
Use Alert Executor	
Dependency	
Vendor	Microsoft
Make	Windows
Model	Windows Server 2008 R2 Standard
64-bit OS	Unknown
SNMP sysObjectId	
Location	NEW YORK
Description	
Contact	
Time Zone Settings	
Logical Drives	
Appearance Used In Event	Console (A1A)
Installed Applications	

Linux/Unix

Node 'utestserver' Common Properties			
Node do	estserver common Properties		
		V15	
an transformation and the second sec			
	Server		
Name)	utestserver	
Doma	in	A	
OS		Linux Servers	
Interr	nal Name		
Alias			
Alterr	native IP	192.168.2.105	
Use A	Alert Executor		
	ndency		
Vende			
Make			
Mode	•		
64-bit		Unknown	
	9 sysObjectId		
Locat		NEW YORK	
	ription		
🕀 Cont			
Time Zone Settings			
	earance Used In Event Conso	ole (A1A)	
Installed Applications			
	OK	Cancel	

IP Address

Node '192.168.2.5' Common Properties X				
V15				
<u>10</u> <u>2</u> ↓				
Ξ	IP Device			
	Name	192.168.2.5		
	Internal Name			
	Alias	GS108T		
Alternative IP				
Use Alert Executor				
	Dependency			
	Vendor	Netgear		
	Make	Switch		
	Model	gs108t		
	64-bit OS	Unknown		
	SNMP sysObjectId	1.3.6.1.4.1.4526.100.4.8		
	Location	NEW YORK		
	Description	G5108T		
⊞ Contact				
Ð	Time Zone Settings			
Đ	Appearance Used In Event Cons	sole (A1A)		
Ð	Installed Applications			
OK				

Windows Cluster Object

	Node 'Disk Q:' Common Properties X			
	Jue Disk Q: Common Properties			
		V15		
	2 2↓			
E	Windows Cluster			
	Name	Disk Q:		
	Cluster Name	PANCLUSTER		
	Real Name			
	Internal Name			
	Alias	Disk Q:		
	Alternative IP			
	Use Alert Executor			
	Dependency			
	Vendor			
	Make			
	Model			
	64-bit OS	Unknown		
	SNMP sysObjectId			
	Location	NEW YORK		
	Description			
11-	Contact			
	Time Zone Settings			
1	Appearance Used In Event Console (A1A)			
Œ	Installed Applications			
	OK	Cancel		

VMware Object

Node 'PanA01 - DC - Domain A (W2008x32) 70/1' Common Properties					
V15					
	2				
	Windows Machine				
	5				
	Name	PanA01 - DC - Domain A (W2008x32) 70/1			
	Domain	VMware			
	os	Windows Servers			
	NetBios Name	PanA01.a.local			
	Internal Name				
	Alias				
	Alternative IP				
	Use Alert Executor				
	Dependency				
	Vendor	Microsoft			
	Make	Windows			
	Model	Microsoft Windows Server 2008 (32-bit)			
	64-bit OS	Unknown			
	SNMP sysObjectId				
	Location	NEW YORK			
	Description	VirtualMachine-64			
Đ	Contact				
Đ	Time Zone Settings				
Đ	Logical Drives				
Đ	Appearance Used In Event Conso	le (A1A)			
Ŧ	Installed Applications				
	OK				

<u>Domain</u>

The Domain property is only used for the cluster objects.

It is useful for grouping and display.

The filtering based on domain is available on both CMDB-X and License Manager.

In the case of Windows Cluster, this field is actually the Cluster Name. It is required by the Cluster APIs.

Monitoring Groups can be defined based on node OS type.

The pre-defined '&MG_WINDOWS' provided by Argent Guardian Ultra is a good example.

📳 🔟 🔍 💊 🗲 🤿 🔤 🤮 🗢 Argent for VMware (3.1/	- 1306.4) _ 1	a x
(13)		I
Control Information	Monitoring Group Definition: &MG_WINDOWS	
Definitions Rules Instant Best Practices For VMware Hosts	Use this Tab to specify a ODBC Query to run against the Argent CMDBX	V7
	SELECT ARGSOT_ACHT CUARDLAN ULTALLICENSED NODE.NAME FORM ARGSOT_ANGUNT_CUARDCAM_ULTBA_LICENSED_NODE, ARGSOT_AT_NODE WHERE ARGSOT_ACHT_URADLAN ULTALLICENSED NODE.NAME - ARGSOT_AT_NODE.NAME AND ARGSOT_AT_NODE.NODE_TYPE IN (1, 2, 4, 0)	*
🖶 🧰 Automatic Report Distributions	4	
Calendars -	Server/Device ODBC Query	
Events And Alerts	Exclude Server/Devices: (Separated By Comma)	
C Enterprise Objects	(Septisted By Comma) View Selected Nodes By Not	ihan
Scheduled Monitoring Tasks	Description	
CMDB-X	This is a sample monitoring group definition installed by Setup, It includes all licensed Windows machines.	▲
Control Information		
Reports		÷
Ready	29.3ul 2013 15:29:13 NLM Argent for VMware - Scheduling Engine on W2008R264/XEN is running	

The SQL query uses the column 'NODE_TYPE' to specify Windows OS.

The possible values are as follows:

0x1 (1)	- Windows Domain Controller
0x2 (2)	– Windows Backup Domain Controller
0x4 (4)	– Windows Server
0x8 (8)	– Windows Workstation
0x10 (16)	– Sun Solaris
0x20 (32)	– HP-UX
0x40 (64)	– AIX
0x80 (128)	– SCO UNIX
0x100 (256)	– Linux
0x200 (512)	– IP Address
0x400 (1,024)	– iSeries Server
0x800 (2,048)	– Cluster Node
0x1000 (4,096)	– Cluster Group
0x2000 (8,192)	– Cluster Network
0x4000 (16,384)	– Cluster Network Interface
0x8000 (32,768)	– Cluster Resource
0x10000 (65,536)	– Printer Queue
0x20000 (131,072)	– Windows 9x (obsolete)
0x40000 (262,144)	– Novell Server (obsolete)
0x80000 (524,288)	– Unknown
0x100000 (1,048,576)	– URL Object
0x200000 (2,097,152)	– Mail Object
0x400000 (4,194,304)	– FTP Object

NetBIOS Name (Windows)

This is the real Windows machine name for the entity. There are occasions that monitored machines have the same name. This happens a lot in ISP environments when customers clone machines, and because the machines reside in separate networks monitored by Daughter Engines. There is no network conflict until customers need to differentiate them in Argent Atlas.

To handle such a situation, customers can manually add the machines with distinguishable names, and use property '**NetBIOS Name**' to point to the real machine name.

When the Argent AT engine monitors a Windows machine, if it is specified, the NetBIOS name is used instead of the node name for API calls.

Internal Name (Windows Cluster Object)

Similar to NetBIOS name for Windows machine, Internal Name is the real cluster object name that is used in Windows Cluster API.

<u>Alias</u>

Property 'Alias' is useful for IP address.

Alternative IP

Alternative IP can specify the actual IP address for Linux/Unix and iSeries server. If it is not specified, Argent AT engine will attempt to resolve the IP address from the node name.

Use Alert Executor

This defines the node-specific Alert Executor. When a Relator defines alerts using node-specific Alert Executors, the Argent Console engine uses this property to determine which Argent Alert Executor should be used.

Dependency

This defines the logical dependency for the node. There are two types of dependency supported in Argent AT. One is topology dependency; the other is logical dependency. A typical example is that the ESX host is the logical dependency for a VM running on the ESX host. If the ESX host is offline, all the VM guests running on it will be offline.

The information is used for Root Cause Analysis. Say a customer defines esx1.a.local as the dependency for VM pana01.a.local. When the Argent AT engine detects pana01.a.local is offline, instead of reporting VM outage right away, it checks the VM's dependency. If esx1.a.local is also offline, the Argent AT engine will report a single event of the real root cause instead of flooding the user with VM offline events.

Vendor/Make/Model

These properties are mostly for display except for Argent for SNMP, which uses the information plus sysObjectId, combined with Argent's internal knowledge base to generate synthetic Relators for automated monitoring. See <u>Default Alert</u> in Network Group for details.

<u>64-bit OS</u>

This information can have an important performance impact on situations that require such information. For example, when Argent for Compliance engine reads Windows event log using traditional Event Log API, it must determine whether the target machine is 32-bit or 64-bit. If the property is not specified, the engine needs to run an additional routine to determine it. It can be costly.

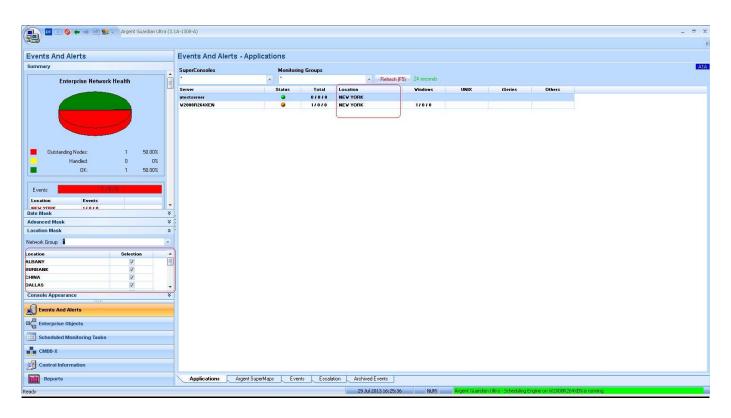
As a result, if customers know exactly what the OS type is, the property should be specified to give Argent AT a little boost.

SNMP sysObjectId

This property is used by SNMP objects. It is another property used in automated monitoring. See <u>Vendor/Make/Model.</u>

Location

The node location is used for filtering in Argent Console A1x screens, and the Argent SuperMaps



Description

Customers can enter any information here about this particular node.

<u>Contact</u>

Node 'PANA01' Common Properties	X
	N15
<u>:</u> 2	
🖽 Windows Machine	
🖂 Contact	
Email Address	
Phone#	
Remote Desktop	
Support URL	
Time Zone Settings	
∃ Logical Drives	
Appearance Used In Event Console	e (A1A)
Installed Applications	
ΟΚ	Cancel

Email Address

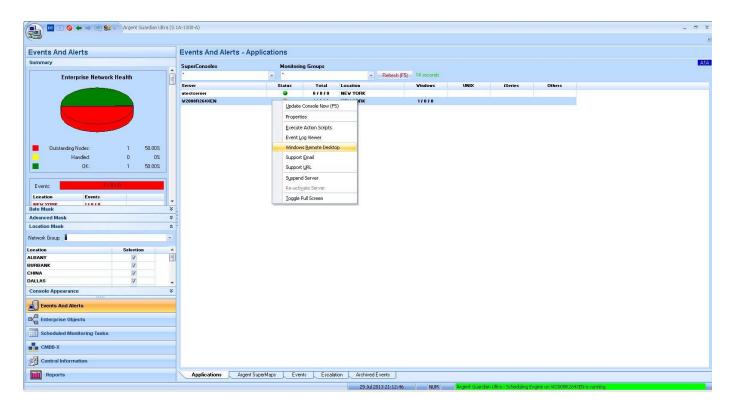
This is the email address of contact for this node. This property is not just for display. It can be used as replacement for the %DefaultNode%. See <u>'KBI 310392 New Feature: Node-Specific Email In Email Alert'</u> for details.

Phone#

It is the phone# of contact for this node. This property is for display only.

Remote Desktop

It is the custom command line to start up remote desktop session for the node from A1A. For example, 'mstsc /v:%AGNodeName%' will connect to the target machine using remote desktop.



Support URL

It is the support URL for the node. Customers can invoke the URL using the context menu on A1A.

Time Zone Settings

This set of properties defines the time zone of the node. The information can be used for scheduling monitoring tasks or putting the node into maintenance mode.

Node 'PANA01' Common Properties	x
	G15
£↓	
 ₩ Windows Machine ① Contact □ Time Zone Settings 	
Time Zone Option	Use Supervising Engine 🗾
Time Zone Time Server	Fixed Hours Dynamic Read From Server Use Trusted Agent
 	Use Supervising Engine
OK	Cancel

Time Zone Option

The available options include following:

• Fixed Hours

It is easy to use and causes little overhead. It assumes the node has the same daylight savings time setting bias as the Supervising Engine. For example, the scheme works well if all servers/devices are in USA and in the same time zone.

Node 'PANA01' Common Properties	x		
	G15		
₽Ţ A↓			
₩ Windows Machine			
Contact			
Time Zone Settings	Fixed Hours		
Time Zone Option	Fixed Hours		
Time Zone			
Time Server	GMT-12:00		
🗄 Logical Drives	GMT-10:00		
Appearance Used In Event Conso	GMT-09:00		
Installed Applications	GMT-08:00		
	GMT-07:00		
	GMT-06:00		
	GMT-05:00		
	GMT-04:00		
	GMT-03:00 GMT-02:00		
	GMT-02:00		
	GMT		
	GMT+01:00		
OK	Cancel		

• Dynamic Read From Server

If the Time Server is not specified, the same node is assumed. The Time Server must be a Windows machine.

Querying time zone information causes some overhead. Because the Argent AT engine caches time zone information, it would make sense to use one or a few common machines as the Time Server for all other machines in the same time zone.

Use Trusted Agent

Queries time zone information from the specified Argent AT Trusted Agent.

• Use Supervising Engine

Assume the node has the same time zone setting as the Supervising Engine that is scheduling the monitoring task. This is the default time zone setting for the node.

Note: the Supervising Engine can be a Mother Engine or a Daughter Engine. The Daughter Engine may not necessarily be in the same time zone as the Mother Engine. As a result, all the nodes monitored by the Daughter Engine are scheduled based on the time zone of Daughter Engine. This makes senses for most situations.

Logical Drives

Logical Drives are used to explicitly ignore some logical drives when checking logical drive related performance data. It can be used to get free disk space when the remote registry service is not running.

Node 'PANA01' Common Propertie	s X
	G15
1 2↓	
Windows Machine	
🖃 Time Zone Settings	
Time Zone Option	Fixed Hours
Time Zone	
Time Server	
🗆 Logical Drives	
Drives Not To Monitor	=
Disk Shares (Used When	h Admin Share Is Off)
C	
D:	
E:	
F:	
G:	
H:	
I:	
J;	
K:	
L:	
M:	
N:	
0:	
OK	Cancel

Drives Not To Monitor

If one or multiple drives should be excluded for all monitored servers, it is easier to exclude drives in the Performance Rule.

Performance Counter Criteria	x	
	G46A	
Type Of Performance Metric	;	
Performance Object:	\LogicalDisk(")\% Free Space	
Algorithm:	Any 👻	
Instances:	Exclude Pattern 👻 X:M:LTotal	
	Regular Expression	
Formula Expression:		
Formula Name:		
 Metric Calculation 		
Method:	Get 👻	
C Rule Is Broken If		
📃 Value Is Greater Than:		
🔽 Value Is Less Than:	15	
Fail Rule If The Data Is Unavailable Or Nonexistent		
🗖 As A Variable		
Retrieve Performance Data For Argent Predictor Only		
<u> </u>	<u>C</u> ancel Help	

If one or multiple drives are only excluded for some servers, or the excluded drives are different for each server, it is better to define the Performance Rule excluding no drives, and use this property to exclude the specific drives for the server.

Disk Shares (Used When Admin Share Is Off)

The remote performance data may not be available due to security settings or the remote registry service is turned off on the remote machine. This is quite common for locked down machines in the DMZ.

Even though customers may still need to get disk information such as free disk space. Fortunately the disk information can be retrieved through WIN32 API 'GetDiskFreeSpaceEx'.

In order to use the API, customers need to specify what drives to check. Customers can do so by assigning drive shares for the used drives. For example, C\$ for C:, D\$ for D: etc.

Sometimes the admin shares (C\$, D\$ etc) are turned off too. If there is any defined share on the drive, not necessarily the admin share, customers can specify the share for the drive. The API works using the share too.

In the following example, machine 'PANA35' has two logical drives 'C:' and 'E:'. Because admin share is turned off, customers define two shares C_DRIVE and E_DRIVE for accessing the drives.

Also see KBI 310607 New Feature: Checking Disk Space When Performance Data Unavailable.

Node 'PANA35' Common Pro	operties	x
	•	G15
₽∎ A		
Model	Windows XP Professional	-
64-bit OS	Unknown	
SNMP sysObjectId		
Location	NEW YORK	
Description		
🕀 Contact		
🕀 Time Zone Settings		
🖃 Logical Drives		
Drives Not To Monitor		
🗆 Disk Shares (Used	When Admin Share Is Off)	
C:	C_DRI¥E	≡
D:		
E:	E_DRIVE	
F:		
G:		
H:		
I:		
J;		
К:		
L:		
M:		
N:		-
- ОК	Cancel	

Appearance Used In Event Console (A1A)

These properties control the text and background color for the specific nodes in Event Console. Customers can customize the colors to make some nodes stand out on the screen.

Node 'PANA35' Common Prope	rties	x
		G15
∄ 2↓		
OS	Windows Workstations	-
NetBios Name		
Internal Name		
Alias	PANA35\$	
Alternative IP		
Use Alert Executor		
Dependency		
Vendor	Microsoft	
Make	Windows	
Model	Windows XP Professional	
64-bit OS	Unknown	
SNMP sysObjectId		_
Location	NEW YORK	=
Description		
🕀 Contact		
🕀 Time Zone Settings		
🕀 Logical Drives		
🖃 Appearance Used In Ev	ent Console (A1A)	
Color Option	Use Default	
Text Color	0, 0, 0	
🗄 Background Color	255, 255, 255	
Installed Applications		-
OK	Cancel	

Installed Applications

These properties simply list out all the known applications installed on the node.

The applications can be entered directly, or discovered by a program (See <u>Detect Installed Applications</u>)

		G15
: : 2↓		
Vendor	Microsoft	-
Make	Windows	
Model	Windows Server 2003	
64-bit OS	Unknown	
SNMP sysObjectId		
Location	NEW YORK	
Description		_
🗄 Contact		
🗄 Time Zone Settings		
] Logical Drives		
Appearance Used In Event Console (A1A)		
Installed Applications		
Application 1	IIS	
Application 2	MSSQL	
Application 3	Oracle	
Application 4		
Application 5		
Application 6		
Application 7		
Application 8		
Application 9		

Customers can define Monitoring Groups based on the installed applications.

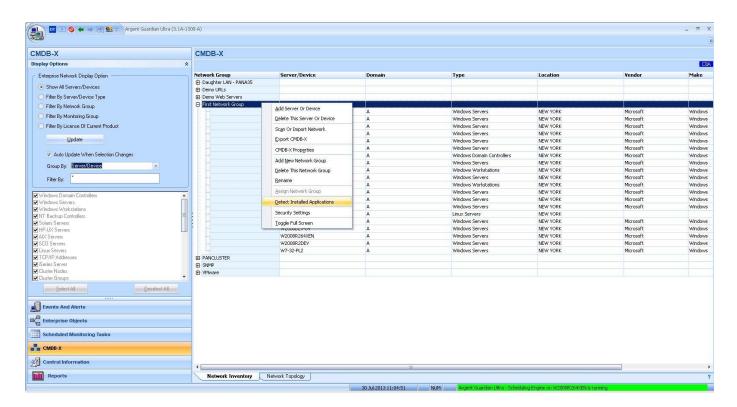
Argent AT provides a few pre-defined sample Monitoring Groups to demonstrate this.

Control Information Monitoring Group Definition: &MG_UIS_SERVER Image: Server Control Information Monitoring Group Definition: &MG_UIS_SERVER Image: Server Control Information Image: Server Control Information Image: Server Contro	📑 🔟 🔍 🗢 👄 🐏 😫 = 🛛 Argent Guardan Ul	Ira (3.14-1308-A)	_ 6 X
Determine Image: Service May ser			4
	Control Information	Monitoring Group Definition: &MG_IIS_SERVER	
Antris Antris <td>Definitions □ Service Level Agreement, Rules □ System Command Rules □ System Down Rules □ System Down Rules □ System Rown Rules □ Registry Rules □ Registry Rules □ Windows Process □ Windows Rules □ Registry Rules □ Reducts □ Detho □ Detho □ Detho □ Reducts</td> <td>Use this Tab to specily a DDBC Guesy to sun against the Augent CMDB X SILECT ARGODYT_AT NODE.NUME FROM ABGODYT_AT_NODE_APPLICATION.NODE_UTUID INTO ARGODYT_AT_NODE_NUME = ARGODYT_AT_NODE_APPLICATION.NODE_UTUID INTO ARGODYT_AT_NODE_APPLICATION.NAME = 'IIS' If SILE Format. View Help Argent Guardian Ultra 3.1A-1308-A (c) 2012 ArgSoft Pacific Intellectual Property Holdings (HK), Limited For Argent Instant Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php</td> <td>157</td>	Definitions □ Service Level Agreement, Rules □ System Command Rules □ System Down Rules □ System Down Rules □ System Rown Rules □ Registry Rules □ Registry Rules □ Windows Process □ Windows Rules □ Registry Rules □ Reducts □ Detho □ Detho □ Detho □ Reducts	Use this Tab to specily a DDBC Guesy to sun against the Augent CMDB X SILECT ARGODYT_AT NODE.NUME FROM ABGODYT_AT_NODE_APPLICATION.NODE_UTUID INTO ARGODYT_AT_NODE_NUME = ARGODYT_AT_NODE_APPLICATION.NODE_UTUID INTO ARGODYT_AT_NODE_APPLICATION.NAME = 'IIS' If SILE Format. View Help Argent Guardian Ultra 3.1A-1308-A (c) 2012 ArgSoft Pacific Intellectual Property Holdings (HK), Limited For Argent Instant Help 7 by 24 with an Argent engineer, please see http://help.Argent.com/help.php	1 57
Image: Scheduled Monitoring Tasks Description Image: CMDB.X This is sample monitoring group definition installed by Setup. It includes all nodes has application 115' installed	Anexis Anexis	I. PANNS ODBC Query 2. W7-32-PL2 ODBC Query 3. W2008R264XEN ODBC Query 4	•
Image: Control Information Separated By Comma) View Selected Nodes By Noteparated By Comma) Image: Control Information Description: Image: Control Information The sample monitoring group definition initialed by Setup. It includes all nodes has application IIS' initialed		Server/Device ODBC Query	
Image: Enterprise Objects Description:	Events And Alerts		d Nadas Da Natarad
Control Information	Enterprise Objects		u nodes by Notepad
CMDB X	Scheduled Monitoring Tasks		
	CMDB-X		_
	Control Information		
Rearty 20 Jul 2013 09:46:44 NUM Argent, Guardian Ultra - Scheduling Engine on W2008R264/EN is running	Reports		•

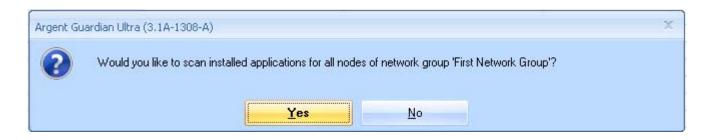
Customers can use these Monitoring Groups in the Relators. Combined with automatic application discovery by using Argent AT Command Line Tools, automatic monitoring of an application can be accomplished.

Appendix D – Detect Installed Applications

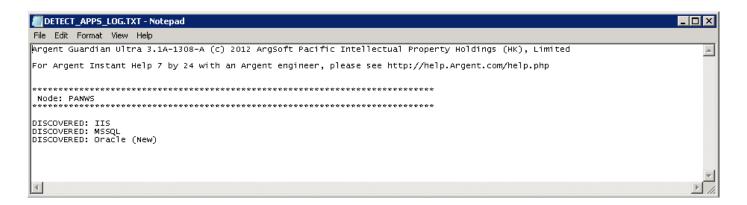
By right-clicking and showing the context menu, customers can use pre-defined mechanisms to scan the selected nodes for installed applications.



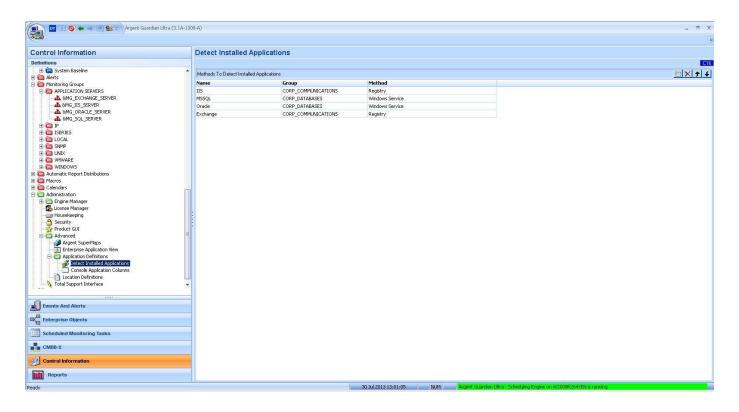
If the current selection is a Network Group, the following prompt is shown:



At the end of detection, the CMDB-X database is updated and the log is shown in notepad.



The detection of installed applications relies on the pre-defined application discovery mechanism.



The supported mechanisms include the following:

- 1. Windows registry
- 2. Windows service
- 3. SNMP OID
- 4. VBScript
- 5. Unix Telnet
- 6. Unix SSH
- 7. TCP service

👔 🔟 🔕 ⇐ 🤿 🔮 😫 = 🛛 Argent Guardian Ultra (3	3.1A-1307-B)			_ o x
<u> </u>				(
Control Information	Detect Installed	etect Installed Applications		
Definitions				IC18
E 🛅 Service Rules 🔺	Methods To Detect Insl	talled Applications		🖺 🗙 🗲 🗲
🗈 🔁 System Command Rules 🗊 🚰 System Down Rules	Name	Group	Method	
E C System Down Rules	IIS	CORP_COMMUNICATIONS	Registry	
	MSSQL	CORP DATABASES	Windows Service	
🗉 🚞 Server Connectivity Rules	Oracle	CORP_DATABASES	Registry	
🕀 🛅 System Management Scripts	Exchange	CORP_COMMUNICATIONS	Registry	
🕀 🛅 Registry Rules	SNMP	CORP_NETWORK	SNMP Search	
🗈 🧰 Windows Printer Share	SMTP	CORP_COMMUNICATION	TCP Service	
E C Windows Process	2011	Cont _Control Control		
🗄 🧰 UNIX Rules				
Relators			, in the second s	
Alerts		Specify D	etails Of Application 🗖 🗶	
🗄 🫅 Monitoring Groups			C164	
🗄 🫅 Automatic Report Distributions				
🖲 🛅 Macros		Applic	ation Name: MSSQL	
🖲 🧰 Calendars				
E C Administration		Di	splay Group: CORP_DATABASES	
B C Engine Manager	Detect Method: Windows Service			
		Dec		
		Windo	ws Service Registry Windows Service SNMP Search	
Product GUI	1		SNMP Search	
E C Advanced			VB Script Unix Telnet	
- 🥔 Argent SuperMaps			Unix Telnet Unix SSH	
- Enterprise Application View			TCP Service	
E C Application Definitions				
Detect Installed Applications				
Console Application Columns				
Total Support Interface				
Argent Instant Help				
as Argone a search rolp			OK	
Events And Alerts				
Enterprise Objects				
Scheduled Monitoring Tasks				
CMDB-X				
Control Information				
Reports				
Ready			4 Jul 2013 13:42:21 NUM Arge	nt Guardian Ultra - Scheduling Engine on PANWS is running

As the majority of Windows applications have Windows services as background processes, or use specific registry hives, the methods of 'Windows Registry' and 'Windows Service' are most commonly used.

For Linux/Unix applications, the method 'TCP Service' is recommended, as it is the easiest and least intrusive.

Argent AT provides command line utilities to accomplish the same functions of detecting installed application as the GUI. It can be very useful to implement automated monitoring by running application detection periodically in a background maintenance script.

Define Applications

(Windows Registry)

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m registry -reg reghive [-val value]

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m registry' specifies the method of Windows registry.
- Argument '-reg' specifies the registry key path
- Argument '-val' specifies the optional value for the registry key.

(Windows Service)

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m service -serv svcname

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m service' specifies the method of Windows service.
- Argument '-serv' specifies the Windows service name.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m snmp -oid oid

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m snmp' specifies the method of SNMP.
- Argument '-oid' specifies the signature OID for the application.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m vbscript -file script

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m vbscript' specifies the method of VBScript.
- Argument '-file' specifies the script file path.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m ssh -file script

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m ssh' specifies the method of SSH.
- Argument '-file' specifies the script file path.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m telnet -file script

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m telnet' specifies the method of Telnet.
- Argument '-file' specifies the script file path.

ARGENT_DETECTAPP_CLI [-add | -update] -p application -g group -m tcp -port port_number [-file script]

- Argument '-add' adds a new application.
- Argument '-update' updates an existing application
- Argument '-p' specifies the application name.
- Argument '-g' specifies the group for the application.
- Argument '-m tcp' specifies the method of TCP service.
- Argument '-p' specifies the TCP port to detect.
- Argument '-file' specifies the script file path.

Delete A Defined Application ARGENT_DETECTAPP_CLI -delete -p application

- Argument '-delete' deletes an existing application
- Argument '-p' specifies the application name.

Detect Installed Applications

ARGENT_DETECTAPP_CLI -s server [-p application] [-user user] [-pswd pswd] [-snmp v1/v2c] [-comm community]

ARGENT_DETECTAPP_CLI -n group [-p application] [-user user] [-pswd pswd] [-snmp v1/v2c] [-comm community]

ARGENT_DETECTAPP_CLI -all [-p application] [-user user] [-pswd pswd] [-snmp v1/v2c] [-comm community]

- Argument '-s' specifies the single server/device to detect.
- Argument '-n' specifies the network group. All server/devices of the network group should be scanned.
- Argument '-all' means that all server/devices should be scanned.
- Argument '-p' specifies the single application to detect. If not specified, all defined applications should be scanned.
- Argument '-user' specifies the logon user for LINUX/UNIX server. It is used only when the application uses SSH or telnet method.
- Argument '-pswd' specifies the logon password for LINUX/UNIX server.
- Argument '-snmp' specifies the SNMP version. SNMP version 1 and 2c are supported. It is used only when the application uses SNMP method.
- Argument '-comm' specifies the SNMP community.

Appendix E – Extended VBScript Syntax For Detecting Installed Application

Customers can use VBScript to implement very complicated logic for determining whether an application is installed. Besides ordinary VBScript syntax, Argent Advanced Technology introduces the following keywords to communicate information back and forth:

TargetServer (Read-Only)Argent AT assigns the real server name to this property.

ApplicationName (Read-Only) Argent AT assigns the application name to this property.

ApplicationFound (Write-Only)

Customers should assign True to this property if the application is determined as being installed; otherwise, assign False.

ScriptHasError (Write-Only) Customers can assign True to this property if encountering some unrecoverable error within script logic.

WriteStatus (Method) Write a line to the log.

Appendix F – UNIX Script Output Syntax For Detecting Installed Application

The UNIX script syntax uses the same format as UNIX script rules.

If the output contains status 'PASS', it means the application is found; if the output contains status 'FAIL', it means the application is not found.

A 'PASS' sample output should look like:

<TAGResult> <QEResult> <STATUS>PASS</STATUS> </QEResult> </TAGResult>

A 'FAIL' sample output should look like:

<TAGResult>

<QEResult>

<STATUS>FAIL</STATUS>

</QEResult>

</TAGResult>

Appendix G – Network Topology

Argent AT can scan the network topology by querying SNMP managed switches. It relies on the support of BRIDGE-MIB to gather the information of port and connections.

🚛 🔟 💿 💊 <table-cell-rows> 🖮 🏨 😫 = 🛛 Argent Guardian Ultra (3.1A-1308-T1) CMDB-X CMDB-X **Display Option** CSB Enterprise Network Display Option Bandwidth Usage (Mb/s) sysObjectId Device Type MAC Address Port/Interface Device Name Network Segmen Gateway Switch Show All Servers/Devices iciscoasa (192.168.2.1) G5108T (192.168.2.5) - IfIndex(7) 100/0.67 (in) - 100/0.02 (out) 1.3.6.1.4.1.9.1.745 Filter By Server/Device Type 00-22-3f-f4-16-2e GS108T (192.168.2.5) 1.3.6.1.4.1.4526.100.4.8 GS108T (192.168.2.5) - IfIndex(3) filer.a.local (192.168.2.1 1,000/0.02 (in) - 1,000/0.21 (out) 1.3.6.1.4.1.8072.3.2.10 Filter By Network Group 00-c0-9f-1f-75-de Hub#1 Unmanaged Switch/Hub G5108T (192.168.2.5) - IfIndex(6) Filter By Monitoring Group - 192.168.2.186 - W2003R2XEN (192.1 - W2008R264XEN (192 00-1d-09-1b-5e-3a 1.000/0 (in) - 1.000/0 (out) Filter By License Of Current Product fe-a7-04-1c-2c-aa 32-8e-f7-25-80-fh 1,000/0 (in) - 1,000/0 (out 1,000/0 (in) - 1,000/0 (out) Update Unmanaged Swi Scan Network Topology GS108T (192.168.2.5) - IfIndex(4) 100/0.02 (in) - 100/0.67 (out) Add Topology Node V Auto Update When Selection Changes Remove 1.3.6.1.4.1.29999.1 Group By: Server/Device CMDB-X Properties Filter By: Import Topology XML Unmanaged Sw G5108T (192.168.2.5) - IfIndex(1) 192.168.2.105 192.168.2.106 Restore Backup XML $\begin{array}{l} 1,000(0.22\,(m)-1,000(0.03\,(wk))\\ 1,000(0.22\,(m)-1,000(0.02\,(wk))\\ 1,000(0.22\,(m)-1,000(0.02\,(wk))\\ 1,000(0.22\,(m)-1,000(0.22\,(wk))\\ 1,000(0.22\,(m)-1,000(0.22\,(wk))\\ 1,000(0.22\,(wk))\\ 1,000(0.22\,$ 1,000/0.23 (in) - 1,000/0.03 (out) 3 3 3 3 3 3 3 3 3 3 3 3 3 5 5 Export indows Servers 192.168.2.187 192.168.2.187 192.168.2.217 PANADI (192.168.2. PANA33 (192.168.2. PANA33 (192.168.2. PANA33 (192.168.2. PANA53 (192.168.2. PANA54 (192.168.2. PANA54 (192.168.2. PANA54 (192.168.2. PANA51 (192.168.2. 'indows Workstation T Backup Controllers Rename Network Segment Delete laris Servers -UX Servers Merge Graft To Switch/Gateway Promote To Switch Role Remove Switch Role Revert Changes PANSQLCLUSTER (19 Add Discovered Server/Device To CMDB-X W7-32-PL2 (192.168 Set In/Out Bandwidth And Bandwidth Usage Deselect All WS-DEV8 (192.168.2 Select All 1,000/0.23 (ii) - 1,000/0.03 (iii) 1,000/0 (iii) - 1,000/0.02 (out) 1,000/0 (iii) - 1,000/0 (out) 100/0.67 (iii) - 100/0.02 (out) openfiler2.a.local (192.1) GS108T (192,168,2,5) - IfIndex(5) 1.3.6.1.4.1.8072.3.2.10 Security Settings PANWS (192.168.2.188) OFFICE390 (192.168.2.34) G5108T (192.168.2.5) - IfIndex(2) G5108T (192.168.2.5) - IfIndex(7) Events And Alerts Toggle Full Screen Enterprise Objects Scheduled Monitoring Tasks CMDB-X Control Information Network Inventory Network Topology Reports

To scan the network topology, use the context menu 'Scan Network Topology'.

A dialog box of options is shown before the actual network topology scanning.

Scan Network To	pology			x
IP Range:	192 . 168 . 2 . 1 1 ✓ Scan All Network Segments That Loc	192 . 168 . 2 . 254	/ 255 . 255 . 2	G8C 255 , 0
Discover Mar	naged Switch Using Following Parameters		(2227101111221)	
Query OID:	1.3.6.1.2.1.1.5.0	Protocol:	SNMPv1	-
Community:	public	User Name:		
SNMP Port:	161	Auth. Password:		None 📩
Timeout	10 🚖	Encryption Password:		None 📩
Thread Limit:	999 🚔 I	nterval To Calculate BPS:	30 🚔 (secon	ds)
OK				

If the local machine has multiple network interfaces, customers can opt to scan all or just one using the option 'Scan All Network Segments That Local Computer Is Attached'.

After scanning is done, the network topology screen is populated with the discovered topology.

Network Topology And Root Cause Analysis

Network Topology allows administrators to see the network layout easily. Argent AT engine also uses this information to do root cause analysis.

One common complaint about other networking products by the Network Administrator is that he is blasted with a flood of alerts of down servers when a switch or router fails.

In contrast, with Argent -- if network topology is maintained and used properly – the Network Administrator is alerted with a <u>single</u> event of the down switch.

To use network topology for root cause analysis, customers need to turn on this option in the Relator.

🚛 💷 🔇 🗮 🤿 🤮 - Argent Guardian Ultra (3.1A-1	308-A) _ = = X
Control Information	Relator Definition: REL_IP_CONNECT (Test Mode)
Definitions	670
Compare Pulse Compar	If Prerequisite Rules Fail Mark Servers As The Same Status Of Previous Check. If Execute Topology Root Cause Analysis And Suppress Alert Accordingly. Relation Trigger If Mary Of Rules Are Broken, Execute Relator In Trigger If Mary Of Rules Are Broken, Execute Relator In Croce Every Image: Minutes If Execute Relator Only For The Node That Breaks The Rules
🗄 🛅 iSeries Rules	Description
Calendars Administration	
Engine Manager	
Enterprise Objects	
Scheduled Monitoring Tasks	
CMDB-X	
Control Information	
Reports	What To Run (Rules) When To Run (Schedule) What To Do (Alerts) Advanced Features
Ready	1 Aug 2013 11:07:00 NUM Argent Guardian Ultra - Scheduling Engine on W2008R264/XEN is running

Command Line Tool - Discover SNMP Devices

Argent AT provides a command line tool to discover SNMP devices in the network.

The executable has no dependency so it can be copied and run from any SNMP management workstation.

Administrator: Command Prompt
C:\ARGENT\ArgentGuardianUltra>argsoft_snmp_discovery /? Argent for SNMP Discovery Utility (3.1A-1308-A)
argsoft_snmp_discovery [/? /help]
argsoft_snmp_discovery [/out:output_file_path] [/v1 ¦ /v2c] [/community:xxxx] [/ start:xxx.xxx.xxx.xxx] [/end:xxx.xxx.xxx] [/mask:xxx.xxx.xxx.xxx] [/ssnmp ¦ /mgmtapi] [/timeout:nn] [/append]
argsoft_snmp_discovery [/out:output_file_path] /v3 /user:xxxx [/authpswd:xxxx] [/encpswd:xxxx] [/protocol:md5 sha] [/algorithm:des aes 3des] [/start:xxx.xxx.xxx .xxx] [/end:xxx.xxx.xxx.xxx] [/mask:xxx.xxx.xxx] [/timeout:nn] [/threads:nnn] [/append]
Examples:
argsoft_snmp_discovery
argsoft_snmp_discovery /out:snmp_devices.txt /v1
argsoft_snmp_discovery /out:snmp_devices.txt /v2c /community:private /start:192. 168.2.1 /end:192.168.2.10
argsoft_snmp_discovery /out:snmp_devices.txt /v3 /user:monitor /authpswd:PATTON /encpswd:PATTON /threads:30
C:\ARGENT\ArgentGuardianUltra>_

The default output file is 'found_snmp_devices.txt' in the same directory as the executable.

A sample result is shown as follows:



Command Line Tool - Discover Network Topology

Argent AT provides a command line tool to scan network topology. The executable has no dependency so it can be copied and run from any SNMP management workstation.

Administrator: Command Prompt

C:\ARGENT\ArgentGuardianUltra>argsoft_snmp_topology /?
Argent for SNMP Topology Utility (3.1A-1308-A)

argsoft_snmp_topology [/? ! /help]

argsoft_snmp_topology [/out:output_file_path] [/v1 ! /v2c] [/community:xxxx] [/s
mgmtapi] [/timeout:nn] [/append]

argsoft_snmp_topology [/out:output_file_path] /v3 /user:xxxx [/authpswd:xxxx] [/
encpswd:xxxx] [/protocol:md5!sha] [/algorithm:des!aes!3des] [/start:xxx.xxx.xxx] [/mask:xxx.xxx] [/mask:xxx.xxx] [/
encpswd:xxxx] [/protocol:md5!sha] [/algorithm:des!aes!3des] [/start:xxx.xxx.xxx] [/append]
Examples:
argsoft_snmp_topology /out:found_snmp_topology.csv /v1
argsoft_snmp_topology /out:found_snmp_topology.csv /v2c /community:private /start:192.168.2.1 / end:192.168.2.10
C:\ARGENT\ArgentGuardianUltra>_

Customers can specify the output file as either XML or CSV format. The default output file is

'found_snmp_topology.xml' in the same directory as the executable.

A sample result is shown as follows:

C:\Argent\ArgentGuardianUltra\found_snmp_topolog	xml	💌 😽 🗙 Live Search	
dit Yiew Favorites Iools Help			
C:\Argent\ArgentGuardianUltra\found_snmp_topolog		🟠 • 🗟 - 🖶 • 🔂 Bag	ge + 🌀 T <u>o</u> o
elp protect your security, Internet Explorer has restricted this we	page from running scripts or ActiveX controls that could access your computer. Click here for options		
OPOLOGY>	S109T" mac_address="0.34.63.244.22.46" sysobjectid="1.3.6.1.4.1.4526.100.4.8">		
	.24.12.55" interface_name="GS108T (192.168.2.5) - IfIndex(7)" in_bandwidth="100.00" out_l	handwidth="100.00" nort="7">102.168.2.24 0</td <td></td>	
	3.72.54.157.233" interface name="G\$108T (192.168.2.5) - IfIndex(7)" in bandwidth="100.00"		0
other ips="192.168.1.242">192.168.2.1 </td <th></th> <td>v dat_bondmaan= 100.00 porte v bybobjecad= 1.0.0.11.1.1.1.1.</td> <td></td>		v dat_bondmaan= 100.00 porte v bybobjecad= 1.0.0.11.1.1.1.1.	
	name="G\$108T (192.168.2.5) - IfIndex(6)" in_bandwidth="1000.00" out_bandwidth="1000.0	JO" port="6">192.168.2.186	
<ip in_bandwidth=":</th><td>1000.00" interface_name="G\$108T (192.168.2.5) - IfIndex(6)" mac_address="{</td><th>.142.247.37.128.251" name="W2008R264XEN" out_bandwidth="1000.00" port="6">192.168.2.221</ip>			
<ip in_bandwidth="1000.</th><td>.00" interface_name="GS108T (192.168.2.5) - IfIndex(6)" mac_address="254</td><th>167.4.28.44.170" name="W2003R2XEN" out_bandwidth="1000.00" port="6">192.168.2.222<!--/IP--></ip>			
	"0.20.209.37.131.53" interface_name="G\$108T (192.168.2.5) - IfIndex(5)" in_bandwidth="1	.000.00" out_bandwidth="1000.00" port="5"	
sysobjectid="1.3.6.1.4.1.8072.3.2.10">19			
	.105.127" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_b		
	.108.143.10.235.109" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="1 229.67.210.113.243" interface_name="GS108T (192.168.2.5) - IfIndex(4)" in_bandwidth="10		
	229.57.210.113.243" Interface_name="G\$1081 (192.168.2.5) - IfIndex(4)" In_bandwidth="10 ="160.33.183.148.205.15" interface_name="G\$1081 (192.168.2.5) - IfIndex(4)" in_bandwidth		
	rface_name="G\$108T (192.168.2.5) - IfIndex(4)" in_bandwidth="100.00" out_bandwidth="100		
	5009" mac_address="244.206.70.198.80.9" interface_name="GS108T (192.168.2.5) - IfIndex		
sysobjectid="1.3.6.1.4.1.29999.1">192.16			
<ip <="" display="filer.a.l</td><th>cal" in_bandwidth="1000.00" interface_name="GS108T (192.168.2.5) - IfIndex(</th><td>(3)" mac_address="0.192.159.31.117.222" name="FILER.A.LOCAL" out_bandwidth="1000.00" port="3" td=""><td></td></ip>			
sysobjectid="1.3.6.1.4.1.8072.3.2.10">19			
	_address="0.36.232.117.243.40" interface_name="G\$108T (192.168.2.5) - IfIndex(2)" in_ba	andwidth="1000.00" out_bandwidth="1000.00"	
port="2">192.168.2.188			
	e_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000.		
	3.68.33" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_b 6.82.146" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_		
	5.146.89" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_		
	106.105.146" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00"		
	10.247.219" interface_name="G\$108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" or		
	68.186.25" interface name="GS108T (192.168.2.5) - IfIndex(1)" in bandwidth="1000.00" out		
<ip <="" mac_address="0.12.41." name="PANA60" td=""><th>96.22.49" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_</th><td>bandwidth="1000.00" port="1">192.168.2.101</td></ip>	96.22.49" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_	bandwidth="1000.00" port="1">192.168.2.101	
<ip in_bandwidth="1000.00" interface_name="GS108T (192.168.2.5) - IfIndex(1)" mac_address="0.12.41.1</td><th>32.147.64" name="PANA54" out<="" th=""><td>t_bandwidth="1000.00" port="1">192.168.2.86</td></ip>	t_bandwidth="1000.00" port="1">192.168.2.86		
	41.232.147.64" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00		
	.12.41.232.147.64" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="100		
	rface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="10		
	ce_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="1000		
	ace_name="G\$108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00" out_bandwidth="100		
<pre></pre>	6.134.44.194" interface_name="GS108T (192.168.2.5) - IfIndex(1)" in_bandwidth="1000.00"	our_panamoni= 1000.00. bout=.1.>1a5.108.5.513	
	iscoasa" gateway="yes" network_mask="255.255.255.0" sysobjectid="1.3.6.1.4.1.9.1.745" ot	ther ins="192 168 1 242" />	
	anws.a.local" gateway="yes" network_mask="255.255.255.0" mac_address="0.36.232.117.24" of anws.a.local" gateway="yes" network_mask="255.255.255.0" mac_address="0.36.232.117.24" of anys.a.local" gateway="yes" network_mask="255.255.255.0" mac_address="0.36.232.117.24" of anys.a.local" gateway="yes" network_mask="255.255.255.255.0" mac_address="0.36.232.117.24" of anys.a.local" gateway="yes" network_mask="255.255.255.255.0" mac_address="0.36.232.117.24" of anys.a.local" gateway="yes" network_mask="255.255.255.255.255.0" mac_address="0.36.232.117.24" of anys.a.local" gateway="yes" network_mask="255.255.255.255.255.255.255.255.255.255		
	5.232.117.243.408.0.39.0.0.46" port="0">192.168.56.1		
(NODE>			
FOPOLOGY>			
		Consultant	A 1000

Maintain Network Topology Manually

Argent AT relies on SNMP managed switches, which must support BRIDGE-MIB, to gather the port and connection information. Not all switches have SNMP feature, let alone BRIDGE-MIB support. As a result, network topology may not always be successful or complete.

Argent AT fully supports manual editing of network topology.

	CMDB-X	CMDB-X					
splay Options	*						1
Enterprise Network Display Option	Device Name	Device Type	MAC Address	Port/Interface	Bandwidth Usage (Mb/s)	sysObjectId	
	{default}	Network Segment					
Show All Servers/Devices	El ciscoasa (192.168.2.1)	Gateway		GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)	1.3.6.1.4.1.9.1.745	
Filter By Server/Device Type	G5108T (192.168.2.5)	Switch	00-22-3f-f4-16-2e			1.3.6.1.4.1.4526.100.4.8	
Filter By Network Group	filer.a.local (192.168.	2.1	00-c0-9f-1f-75-de	GS108T (192.168.2.5) - IfIndex(3)	1,000/0.02 (in) - 1,000/0.21 (out)	1.3.6.1.4.1.8072.3.2.10	
	🖻 Hub#1	Unmanaged Switch		GS108T (192.168.2.5) - IfIndex(6)			
Filter By Monitoring Group	- 192.168.2.186		Scan Network Topology		1,000/0 (in) - 1,000/0 (out)		
Filter By License Of Current Product	- W2003R2XEN (19	2.1	Add Topology Node		1,000/0 (in) - 1,000/0 (out)		
	W2008R264XEN (192			1,000/0 (in) - 1,000/0 (out)		
Update	E Hub#2	Unmanaged Switch	Remove	GS108T (192.168.2.5) - IfIndex(4)			
	192.168.2.249		CMDB-X Properties		100/0.02 (in) - 100/0.67 (out)		
Auto Update When Selection Changes	ANPINGS-IMAC (1	92	Import Topology XML		100/0.02 (in) - 100/0.67 (out)		
Group By: Server/Device	HPC65009 (192.1	68.			100/0.02 (in) - 100/0.67 (out)	1.3.6.1.4.1.29999.1	
Group by: Management	XAVN2001-94CD0	F(Restore Backup XML		100/0.02 (in) - 100/0.67 (out)		
Filter By:	XPVM (192.168.2	31	Export		100/0.02 (in) - 100/0.67 (out)		
Thick by	Hub#3	Unmanaged Switch		G5108T (192.168.2.5) - IfIndex(1)			
	- 192.168.2.105		Rename Network Segment		1,000/0.23 (in) - 1,000/0.03 (out)		
Vindows Domain Controllers	192.168.2.106		Delete		1,000/0.23 (in) - 1,000/0.03 (out)		
Vindows Servers Vindows Workstations	- 192.168.2.187		Merge		1,000/0.23 (in) - 1,000/0.03 (out)		
IT Backup Controllers	192.168.2.217				1,000/0.23 (in) - 1,000/0.03 (out)		
Solaris Servers	PANA01 (192.168	.2.	Graft To Switch/Gateway		1,000/0.23 (in) - 1,000/0.03 (out)		
HP-UX Servers	PANA32 (192.168	.2.	Promote To Switch Role		1,000/0.23 (in) - 1,000/0.03 (out)		
ADX Servers	PANA35 (192.168				1,000/0.23 (in) - 1,000/0.03 (out)		
SCD Servers	PANA38 (192-168	.2.	Remove Switch Role		1,000/0.23 (in) - 1,000/0.03 (out)		
Linux Servers	PANA53 (192.168		Revert Changes		1,000/0.23 (in) - 1,000/0.03 (out)		
CP/IP Addresses	PANA54 (192.168	.2.	Add Discovered Server/Device To CMDB-X		1,000/0.23 (in) - 1,000/0.03 (out)		
Series Server	PANA60 (192.168				1,000/0.23 (in) - 1,000/0.03 (out)		
Duster Nodes	PANCLUSTER (19		Set In/Out Bandwidth And Bandwidth Usage		1,000/0.23 (in) - 1,000/0.03 (out)		
Duster Groups	PANSQLCLUSTER		Security Settings		1,000/0.23 (in) - 1,000/0.03 (out)		
Diuster Networks	W7-32-PL2 (192.				1,000/0.23 (in) - 1,000/0.03 (out)		
Select All Deselect All	WS-DEV8 (192.16		Toggle Full Screen		1,000/0.23 (in) - 1,000/0.03 (out)		
	openfiler2.a.local (19		00-14-d1-25-83-35	GS108T (192.168.2.5) - IfIndex(5)	1,000/0 (in) - 1,000/0.02 (out)	1.3.6.1.4.1.8072.3.2.10	
Events And Alerts	PANW5 (192.168.2.1		00-24-e8-75-f3-28	G5108T (192.168.2.5) - IfIndex(2)	1,000/0 (in) - 1,000/0 (out)		
	OFFICE390 (192.168.2.3		00-1d-09-18-0c-37	GS108T (192.168.2.5) - IfIndex(7)	100/0.67 (in) - 100/0.02 (out)		

Add Topology Node

When customers add a top-level gateway or router, it is handy to use the option 'Add All Known IP Addresses Of Same Subnet'. Of course, customers have to do ICMP Ping scanning of the network segment first to crop all the known IP addresses in the segment.

Manually Add An Topolog	y Node				x
					G5F
IP Address:	192 .	168 .	1	. 1	
Device Type:	Switch				-
Connect To (Uplink):	{TOP LEVEL}				-
Subnet Mask:	255 .	255 .	255	. 0	
	🗸 🤇 🖌 🖌	wn IP Addr	esses (Of Same Su	ubnetj
<u>0</u> K				<u>C</u> ancel	

Remove Topology Node

If a switch is removed, all the child nodes can be removed as well.

Import Topology XML

Typically the XML is the result file of command line utility **ARGSOFT_SNMP_TOPOLOGY.EXE**.

It will add the nodes in the XML into the current topology.

Restore Backup XML

It replaces the current topology with information in the backup XML.

Export

It generates a backup XML that can be used for later restoration.

Rename Network Segment

Rename the network segment name in the topology. It is the folder in the topology, generally representing a gateway, router, switch or hub.

Delete Network Segment

Delete a whole network segment. This is a destructive operation. Argent recommends customersto backup the topology using 'Export' first.

Merge

Merge selected network segments with another network segment.

Craft To Switch Or Gateway

Craft selected network segment under a switch or gateway.

<u>Merge</u>

Merge selected network segment with another network segment.

Promote To Switch Role

Promote a node to a switch role so that child nodes can be added under.

Remove Switch Role

Remove the switch role from a node.

Revert Changes

Undo the change. The undo information is cached in memory. If customers exit the program, all undo information is lost.

Add Discovered Server/Devices To CMDB-X

Add any nodes in topology that is not in CMDB-X yet to CMDB-X database.

Appendix H – CMDB-X SQL Tables

In contrast to most vendors, Argent provides a full and complete schema of the database tables used in the Argent Atlas CMDB-X.

ARGSOFT_AT_LAN

This table stores the information of network segments in the enterprise:

Field	Туре	Description
UUID	varchar(36)	Unique Identifier
CREATE_TIME	datetime	Record creation time
MODIFY_TIME	datetime	Last modified time
NAME	nvarchar(256)	Network segment name
DESCRIPTION	nvarchar(1024)	Description
NETWORK	int	Network type
		1 – T1
		2 – DSL
		3 – Cable Modem
		4 – ISDN
		5 – Frame Relay
		6 – VPN or Dial-up (inbound)
		7 – VPN or Dial-up (outbound)
FIREWALL	int	Firewall (Boolean)
		0 – Not enabled
		1 – Enabled
CONTACT_ADMIN	nvarchar(256)	Administrative contact name
CONTACT_EMAIL	nvarchar(256)	Administrative contact email
CONTACT_PHONE	nvarchar(256)	Administrative contact phone
DEFAULT_ALERT	nvarchar(256)	Default alert
DEFAULT_EXECUTOR	nvarchar(256)	Default Argent Alert Executor

OTHERS	ntext	Container field that holds product specific settings.
OWNER	nvarchar(256)	Owner
CRC_LOW	int	CRC low
CRC_HIGH	int	CRC high

ARGSOFT_AT_NODE

This table stores the information of known servers and devices in the enterprise

Relationship: ARGSOFT_AT_NODE.LAN = ARGSOFT_AT_LAN.UUID

Field	Туре	Description	
UUID	varchar(36)	Unique Identifier	
CREATE_TIME	datetime	Record creation time	
MODIFY_TIME	datetime	Last modified tim	ne
NAME	nvarchar(256)	Node name	
INTERNAL_NAME	nvarchar(256)	Internal name fo	r the node
DESCRIPTION	nvarchar(1024)	Description	
NODE_DOMAIN	nvarchar(256)	Domain name	
NODE_TYPE	int	Node type.	
		0x1 (1) 0x2 (2) 0x4 (4) 0x8 (8) 0x10 (16) 0x20 (32) 0x40 (64) 0x80 (128) 0x100 (256) 0x200 (512) 0x400 (1,024) 0x800 (2,048) 0x1000 (4,096) 0x2000 (8,192) 0x4000 (16,384) 0x8000 (32,768) 0x10000 (65,536) 0x20000 (131,072) 0x40000 (262,144) 0x80000 (524,288) 0x100000 (1,048,576) 0x200000 (2,097,152) 0x400000 (4,194,304)	 Windows Domain Controller Windows Backup Domain Controller Windows Vorkstation Sun Solaris HP-UX AIX SCO Unix Linux IP Address iSeries Server Cluster Node Cluster Resource Cluster Resource Printer Queue Windows 9x (obsolete) Novell Server (obsolete) Unknown URL Object Mail Object FTP Object

NETBIOS_NAME	nvarchar(256)	NETBIOS name
ALTERNATIVE_IP	nvarchar(128)	Alternative IP address
ALIAS	nvarchar(256)	Alias
DEFAULT_ALERT_EXECUTOR	nvarchar(256)	Default Argent Alert Executor
VENDOR	nvarchar(256)	Server/Device vendor
МАКЕ	nvarchar(256)	Server/Device make
MODEL	nvarchar(256)	Server/Device model
SYSOBJECTID	nvarchar(256)	SNMP sysObjectId for the device
LAN	varchar(36)	UUID of Network segment
LOCATION	nvarchar(256)	Location
SUSPEND	int	Boolean value. 0 – Node is active 1 – Node is suspended 2 – (XT Backup Compatible Mode) Node is monitored continuously in the background. The Argent Predictor data is saved but event is fired.
NODE_COLOR	int	Boolean value True – Use explicit color option False – Use default setting
NODE_TX_COLOR	int	Text color when using explicit color option
NODE_BG_COLOR	int	Background color when using explicit color option
TZ_OPTION	int	0 - Fixed Hours 1 - Dynamic Read From Server 2 - Use Trusted Agent 3 - Use Supervising Engine
TZ_HOUR_DIFF	int	Hour difference with GMT
TZ_SERVER	nvarchar(256)	Time server
CONTACT_EMAIL	nvarchar(128)	Contact email address

CONTACT_PHONE	nvarchar(128)	Contact phone number
REMOTE_DESKTOP	nvarchar(256)	Command line for remote desktop session
SUPPORT_URL	nvarchar(256)	Support URL
DISK_SHARES	ntext	Disk shares
LOGIC_DEPENDENCY	nvarchar(256)	Logic dependency
AGGR_DATA_TYPE	int	1 = IP Address And/Or IP Range
		2 = Text File
		3 = SQL Query
AGGR_DATA_SOURCE	ntext	Data source for the aggregate node
AGGR_QUERY_INTERVAL	int	Query interval for the aggregate node
OWNER	nvarchar(256)	Owner
CRC_LOW	int	CRC low
CRC_HIGH	int	CRC high

ARGSOFT_AT_NODE_APPLICATION

This table stores the names of all installed applications for a particular node.

Relationship: ARGSOFT_AT_NODE_APPLICATION.NODE_UUID = ARSOFT_AT_NODE.UUID

Field	Туре	Description
UUID	varchar(36)	Unique Identifier
CREATE_TIME	datetime	Record creation time
MODIFY_TIME	datetime	Last modified time
NODE_UUID	varchar(36)	UUID of node
NAME	nvarchar(256)	Application name
OWNER	nvarchar(256)	Owner
CRC_LOW	int	CRC low
CRC_HIGH	int	CRC high