The Nuclotron and NICA Control System

Evgeny Gorbachev on behalf of team LHEP, JINR

Tango Users Group Russia meeting'2017

Content

- NICA complex
- Main principles and layout.
- Control System infrastructure and services:
 - High availability and scalability.
 - Monitoring
 - Access control and logging.

NICA accelerating complex



- Injection complex
- new superconducting Booster synchrotron
- existing superconducting heavy ion synchrotron Nuclotron
- collider having two new superconducting storage rings
- 🖵 new beam transfer channels

 $2 \cdot 10^9$ ions in a bunch

4.5 GeV/n Au⁷⁹⁺

 $L=10^{27} \text{ cm}^{-2} \cdot \text{c}^{-1}$

NICA accelerating complex

2019:

- Stage I: Experiment "The Baryonic Matter at Nuclotron"
- Injection complex: KRION, HILAc, LU20
- Booster
- BT Line Booster Nuclotron
- Nuclotron upgraded
- BM@N Detector setup

2020:

- Stage II-a: The basic configuration of the NICA complex
- BT Line Nuclotron => Collider
- Collider:
- Collider RF systems in a reduced version
- Stochastic cooling system 1 channel per ring
- Multi-Purpose Detector (MPD) in a reduced version: no Inner Tracker System (ITS) 2023:
- Stage II-b: The full (project) configuration of the NICA complex
- Collider and MPD in full version
- Stage III: Polarized Beams' Mode of The Collider
- Spin Physics Detector (SPD)



Control System development goals

- Centralized control of heterogeneous distributed equipment
- Reliable operation and fast recovery
- Safe operation, access restrictions
- Easy support, modification and scalability
- Fast development and deployment
- Easy integration of third-party systems

Control System layout



Tango Users Group Russia meeting'2017 The Nuclotron and NICA control system, E.Gorbachev

Middleware: TANGO controls



- CORBA based distributed object-oriented control system framework
- Multiplatform
- Hides network location and technical details
- Provides unified interface for hardware equipment or service:
 - Commands
 - Attributes
 - Properties
- Has services and tools for control implementation.

Few possible variants to implement DAQ or control:

- Custom hardware
- Commercial off-the-shelf (COTS)

Primary requirements:

- Ease of development
- Quality, reliability and performance
- Maintenance of equipment during the accelerator complex life-time





National Instruments PXI– high performance Eurocard packaging modular platform for measurements and automation systems:

- PCI express and PCI busses with additional synchronization buses.
- Excellent performance: PXIe-1085 throughput up to 4GB/s per slot and up to 12GB/s per system.
- Wide range of available modules (1500+) controllers, acquisition boards, analog and digital I/O, signal generators, digital multimeters, counters and timers, high speed digitizers, industrial interfaces, RF and others.
- Windows and Linux programming LabVIEW, C++ and C# libraries.
- Excellent support.





- Digital signal processing (DSP) modules FlexRIO –PXI and PXIe modules with Xilinx FPGA and custom I/O modules. Supports peer-to-peer streaming up to 3GB/s.
- Compact RIO High performance embedded systems and intellectual controllers based on Xilinx FPGA + ARM with standard or custom I/O module.

Tango drivers with runtime configurable properties for NI equipment were developed:

- Digitizers and scopes
- Analog and digital I/O
- Timers and counters
- Digital multimeters
- RTD input modules
- TANGO interface for FlexRIO and CompactRIO.

Combination of tango devices can be used to quickly deploy a solution based on almost any NI acquisition equipment.

Client layer

Possible variants:

- usual GUI desktop applications (QTango, Taurus, TangoATK)
- Web applications
- Web-based applications advantages:
- Works on any platform (PC, mobile) and OS.
- Easier development one application for all platforms.
- Easier maintenance: no need to install on PCs, centralized updates.

Client layer: Web apps

Communication between TANGO and Web application is required.

- RestDS Tango module to provide access to TANGO control system devices via http requests (GET, POST).
- WebSocketDS Tango module to read TANGO devices attributes via WebSocket protocol: data can be "pushed" to the browser in realtime on demand.

Client layer: Web apps

ExtJS framework (JavaScript). Web-application developed as a web desktop: a number of widgets(tasks) with dynamic layout.



Service layer

Contain high-level TANGO device servers, representing whole subsystem:

- Collects and process data from low-level devices.
- Performs control loop.
- Provides standard interface to client applications: commands, attributes.

Service layer: Virtualization

Applications running on service layer are hardware independent and can be virtualized (run on VM):

- Easier management fast VM deployment from templates, cloning, backups.
- Better tasks isolation assign VM per task or group of tasks.
- Resources tuning can assign appropriate CPU cores, disk space, RAM size, ۲ disk I/O.
- Resource utilization efficient usage of host's RAM and CPU.
- High Availability restore VM from failed server. •

Proxmox VE - complete open source virtualization management solution for servers. It manages virtual machines, storage, virtualized networks, HA clustering and supports both: PROXMOX

- Kernel-based Virtual Machine (KVM)
- **Container-based virtualization** \cap

Service layer: Shared storage

- Crucial component of virtualization to provide high availability of VMs
- Need good performance , both transfer rate and IOPS to manage read/write operations of number of VM images
- Have to be redundant to provide data consistency in case of hardware or network failure
- Need to be scalable should be able to add more storage space without loosing performance

CEPH storage

(ceph is a distributed object store and file system. Ceph is highly reliable, easy to manage and open-source. It provides redundancy, excellent performance and scalability. Ceph storage cluster consists of large number of nodes which communicate with each other to distribute and replicate data dynamically.



Scalability

The scalability can be achieved by adding nodes to cluster. CEPH retains most characteristics at scale or even improves. Adding more nodes to run more VMs:

- Capacity increases
- Throughput increases
- IOPS increase
- CPU cores and RAM increase

Temporary impact during re-balancing.

High availability

- We need to provide high availability of Tango services and fast failover in case of hardware problems.
- Hardware measures (UPS devices controlled by Network UPS tools, reliable enterprise class hard drives) + data redundancy (RAID, replication) + backups (VMs and databases):
- Virtual machines are running on Proxmox VE cluster with VM images stored on CEPH storage (replication=3). Any VM can be started on any node.
- TANGO database: vital for all other Control System Tango devices, running in Linux container on <u>local</u> storage for performance reasons.

High availability: TANGO DB

High Availability for Tango database can be achieved:

- Master-Master replication in active-passive mode.
- Load balancing and backup via HAPROXY



Hardware and software monitoring

Zabbix – monitoring hardware and software of Control System cluster: power, fans, CPU, RAM, disk space, network traffic, disk I/O, CEPH health and many other items. Alerts and notifications are sent via e-mail to cluster admins.



Tango Users Group Russia meeting'2017

The Nuclotron and NICA control system, E.Gorbachev

າາ

TANGO devices monitoring

Astor/Starter –tools for remote control and monitoring of TANGO applications



Tango Users Group Russia meeting'2017

The Nuclotron and NICA control system, E.Gorbachev 23

TANGO devices monitoring

Special TANGO services to check frontend computers resources and states of TANGO devices. Alerts and notifications are sent via e-mail to tango admins.

			1				Tema Monitoring alert - Nuclotron extraction, device: extraction/
AtkPanel 4.8 : sys/moni	toring/159.93.126.118	Ľگا	AtkPanel 4.8 : sys	monitorin	g/nuclextr	_ 🗆 🗵	Кому "E. Gorbachev"🏠
File View Preferences	Help		le View Preferences Help				
sys/monitoring/15	9.93.126.118	-	sys/monitoring/nuclextr			•	extraction/usb6259ds/slow1 state was changed to UNKNOWN
- sys/monitoring/150 03 126	6 1 1 0		sys/monitoring/nucle	extr			
CPUL opd: 1.1 Momon: 14	0.110		Device is ON			^	o⊤ tango@tangodevel.jinr.ruఏ
03-14 10:47:00	4.0, DISK. 90.7, Opuille. 2014-	-					Tema Monitoring alert - Nuclotron extraction
Alarm : Value too high for D	liskUsed					-	Kowy "E Carbacharth
	_						
] [States[0]		ON		
			States[1]		UNKNOWN		Subsystem: Nuclotron extraction
			States[2]		UNKNOWN		Name: sys/dbstorageds/dbsds1, State: FAULT, Status: MySQL server has gone av
			States[3]		UNKNOWN		
DiskUsed	98,70 %		States[4]		UNKNOWN		
CPULoad	1,50 %		States[5]		UNKNOWN		
			States[6]		UNKNOWN		0⊤ tango@tangodevel.jinr.ru☆
Uptime 2	2014-03-14 10:47:00		States[7]		UNKNOWN		Tema Monitoring alert - Nuclotron qmeter
MemoryUsed	14,00 %		States[8]		FALILT		Komy "E Gorbachey"
			States[0]		FALILT		
CPULoadAverage 1,10 %			States[3]	1			
			States[10				Subsystem: Nuclotron gmeter
			States[11		UNKNOWN		Name: gmeter/nivisa/fungen1, State: FAULT, Status: Device disconnected from
Scalar			States[12		UNKNOWN		Name, gmeter/himsa/hampi, state, PAOLI, status, eror, unied out
,		7	Scalar Names	Statuses	States		

TANGO devices monitoring

Desktop and web clients to represent states and statuses of TANGO

e	State	Status
Nuclotron Extraction		
sys/dbstorageds/dbsds1	ON	DB connention succeed. Device is fully operational.
extraction/dagmxaisoftretrig/	ON	ON: USB-6259 (BNC) initialized
- extraction/dagmxao/septum1	ON	ON: USB-6259 (BNC) initialized
extraction/dagmxdi/septum1	ON	ON: USB-6259 (BNC) initialized
extraction/dagmxdo/septum1	ON	ON: US8-6259 (BNC) initialized
extraction/dagmxpulseout/se	ON	ON: USB-6259 (BNC) initialized
extraction/pci6101/intensity	ON	ON: PCI-6601 initialized
extraction/oci6101/profilomet	ON	ON: PCI-6601 initialized
extraction/server/sentim1	ON	Sentim is ON
extraction/server/slow1	ON	ON: LISB-6259 (BNC) initialized
extraction/ush6259ds/slow1	ON	ON: USB-6259 (BNC) initialized
extraction/internolation/adc	ON	The device is in ON state.
extraction interpolation /dac	ON	The device is in ON state
Audiotron Imection	-	The define is in on state.
inflector/modbus/rtu1	ON	Modbus node address 10 protocol RTU iphost UNDEFINED !
		Current parameters of the serial line:
		serialine : com8
		baudrate : 38400
		byte size : 8
		stop bits : 0 (0-2=1,1,5,2bit)
		parity : 2 (0-4=no.odd.even.mark.space)
		reading timeout : 0 (mS)
		fourty cheflow to
		DutyDerFlow : 0
		fDtrControl : 1 (0=dis 1=epa 2=band)
		fDerSencitivity : 0
		fU Continue Ch Xoff: 0
- inflector /serial /rtu1	OPEN	fourty in
anneeder pacing from a	OF LOT	flex -0
		Recontrol : 1 (0-ds 1-ana 2-hand)
		Current parameters of the device server.
		control parameters of the device server.
		Series te statistics
		antity - 2 (O-more 1-odd 2-mum)
		dedecath is
		etachite : 0 (0-thit 1-1 thite 2-3hite)
		Supers : 0 (0 = 101 1 = 1.3015 2 = 2015)
		baurate : 5000
		newarie : 13
inflector/usb6259ds/hvcontrol1	ON	ON: USB-6259 (BNC) initialized
injection/niscopeds/domik1	ON	ON: NI PCI-5105 initialized
injection/usb6259ds/domik1	ON .	ON: USB-6259 (BNC) initialized
injection/server/domik1	ON:	Injection control is ON
gmeter/dagmxpulseout/meas	ON .	ON: US8-6259 (BNC) initialized
luciotron monitoring	2011	CONTRACT 52 21 Memory 10 5 Cide 20 0 Linkers 2014 02 14 10 47-02
sys/monitoring/159.93.126.118	1011	CPU Load: 53.31, memory: 18.5, Disk: 29.9, Uptime: 2014-03-14 10:47:00
sys/monitoring/159.93.126.123	ON	CPU Load: 56.02, Memory: 38.7, Disk: 74.5, Uptime: 2014-05-13 15:19:46
sys/monitoring/159.93.126.232	ON	CPU Load: 11.6, Memory: 37.0, Disk: 44.7, Uptime: 2014-05-13 15:03:02
sys/monitoring/159.93.126.121	UN	CPU Load: U.52, memory: 46.7, Disk: 64.8, Uptime: 2014-05-22 13:52:54
 sys/monitoring/159.93.126.251 	ON	CPU Load: 23.76, Memory: 68.7, Disk: 39.9, Uptime: 2014-06-09 18:48:45
meter/dagmxpulseout/1	ON.	ON: PXI-6733 initialized
gmeter /niscopeds/bpm	ON	ON: NI PXIe-5122 initialized
gmeter/nivisa/fungen1	FALKT	Device disconnected from US8
- ometer /nivisa /rfamp1	FALET	error:timed out
ometer/tegam-90-90/1	ON .	Tegam4040 is ON
ometer/hune/fft	OFF	Device is OFF
dure ser lan welse a		AND THE REAL PLANE

Could not connect to device server sys/monitoring/nuclextr

Tangowin 1. jinr. ru: 8080/JMonitoring/		1 🐠 - 😕
асто посещаемые 🥹 Начальная страница 🔊 Лента	новостей 🕕 Tips and tricks - LabVI 🎭 Шахматная библиот 🍠 DDS генератор сигн [] Online	CRC Calculation
Mouuropuur		
мониторин	тапдо-устроиств системы управления нуклотрона	
Name	Status	State
sys/monitoring/nuclextr		
sys/dbstorageds/dbsds1	DB connention succeed. Device is fully operational.	ON
extraction/daqmxaisoftretrig/septum1	ON: USB-6259 (BNC) initialized	ON
extraction/daqmxao/septum1	ON: USB-6259 (BNC) initialized	ON
extraction/daqmxdi/septum1	ON: USB-6259 (BNC) initialized	ON
extraction/daqmxdo/septum1	ON: USB-6259 (BNC) initialized	ON
extraction/daqmxpulseout/septum1	ON: USB-6259 (BNC) initialized	ON
extraction/pci6101/intensity_stop	ON: PCI-6601 initialized	ON
extraction/pci6101/profilometers_sta	ON: PCI-6601 initialized	ON
extraction/server/septum1	Septum is ON	ON
extraction/server/slow1	ON: USB-6259 (BNC) initialized	ON
extraction/usb6259ds/slow1	USB-6259 (BNC) initialized	ON
extraction/interpolation/adc_septum	The device is in ON state.	ON
extraction/interpolation/dac_septum	The device is in ON state.	ON
sys/monitoring/nuclinj		
sys/monitoring/numon		
sys/monitoring/159.93.126.118	CPU Load: 4.25, Memory: 31.6, Disk: 24.0, Uptime: 2015-01-30 12:26:25	ON
sys/monitoring/159.93.126.123	CPU Load: 59.17, Memory: 38.5, Disk: 74.5, Uptime: 2015-02-01 12:57:54	ON
sys/monitoring/159.93.126.232	CPU Load: 36.47, Memory: 52.8, Disk: 45.2, Uptime: 2015-01-26 15:58:15	ON
sys/monitoring/159.93.126.121	CPU Load: 28.62, Memory: 44.9, Disk: 66.9, Uptime: 2015-02-01 14:32:32	ON
sys/monitoring/159.93.126.251	CPU Load: 23.46, Memory: 74.1, Disk: 39.9, Uptime: 2015-02-01 13:38:38	ON
sys/monitoring/nuqm		
qmeter/daqmxpulseout/1	ON: PXI-6733 initialized	ON
qmeter/niscopeds/bpm	UNKNOWN	UNKNOWN
qmeter/nivisa/fungen1	Device is OFF	OFF
qmeter/nivisa/rfamp1	Device is OFF	OFF
qmeter/tegam4040/1	Tegam4040 is ON	ON
qmeter/tune/fft	Device is OFF	OFF

Tango Users Group Russia meeting'2017

25

Access control and security are vital to safely run a distributed control system.

- **1) Network** configuration:
 - Firewall configuration to provide access for certain IP range.
 - Complex list of rules, fixed ports to run device servers
 - Private sub networks for accelerators control systems with restricted access.
 - Need to provide limited access from external networks

Control system communications



Tango Users Group Russia meeting'2017The Nuclotron and NICA control system, E.Gorbachev27

2) Software security checks:

- Ask for username/password on client side to execute certain operations:
 - Can not prevent execution by other clients (jive)
- Checks clients rights on server side:
 - Have to distinguish clients and store information about their rights.

3) Tango client-side access control

- Optional service restricting devices commands execution and attributes writes based on client username & IP checks.
 - Not flexible
- Applies on Tango::DeviceProxy creation.
 - Need client restart
 - Not applicable for web clients. Username

List of IP addresses

List of devices



20

Idea:

 Improve access control by additional server side security checks

Goals:

- Centralized management of user's permissions
- Centralized access logs
- No complications to both Tango device server and client development
- No modifications to Tango library



31

Realization details:

- 1. Role Based Access Control (RBAC).
 - Each role have a group of permissions.
 - Several roles can be assigned to user/IP pair
 - priorities
- 2. Authentication by location (IP address).
 - Access from operator's PC and CS core servers without passwords.
- 3. Support of MySQL regular or wildcard expressions in rules and addresses: can be configured as Tango property.
- 4. Objects access cache for improving performance.
- 5. Centralized logging service for TANGO devices.
- 6. Providing simple interface for TANGO devices to check client's permissions and to log information in the central database.

27

TANGO database protection



Logging

- Full logs of TANGO database changes exporting devices, changing properties etc.
- Provide easy way for TANGO devices centralized logging command execution, attributes changes and other important information.
- Flexible interface for administrators to find information in logs.

🔳 Ma	Manage Tango Role-Based access control										
File V	ïle View Taurus Tools Help										
	Load Perspectives, 🏊 < 🚸 jive 🚸 astor										
RBAC	RBAC Status Sessions Roles Permissions Users User roles Logs										
From: 10.04.17 10:06:11											
		To: 10.04.1	7 10:06:11				~	now	2017-04-21 1		
Fil	ter by Obj e	ect:							Filter by Facil		
	Filter by	IP:							ALL		
- '	ilter by En	try:				Dationalese			Log history siz		
					1				500		
	id	id facility created source IP object Entry									
485	1939197	1939197 INFO 2017-04-21 13:24:44 check_permissions 159.93.126.70 sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/0 Access granted (and ca									
486	1939199 INFO 2017-04-21 13:24:46 check_permissions 159.93.126.70 sys/database/1/DbExportDevice/diagnostics/daqmxai/1/IOR:01000001700000049444c3a54616e676f2f4465766963655f343a312e30000010000000000000 Access granted (and cached)								ached).		
487	1939201	INFO	2017-04-21 13:24:46	check_permissions	159.93.126.70	$sys/database/1/DbExportDevice/dserver/DAQmxAI/bergoz1/IOR: 010000001700000049444 c_{3}a_{5}4616e676f2f4465766963655f343a_{3}12e_{3}00000010000000000$	Access	granted (and c	ached).		
488	1939203	INFO	2017-04-21 13:24:56	check_permissions	159.93.126.70	sys/database/1/DbUnExportEvent/DServer/Bergoz/bergoz1	Access	granted (and c	ached).		
489	1939205	INFO	2017-04-21 13:24:56	check_permissions	159.93.126.70	$sys/database/1/DbPutClassProperty/Bergoz/4/ProjectTitle/1//Description/1/Bergoz\ subsystem/doc_url/1/http://www.esrf.eu/computing/cs/tango/tang$	Access	granted (and c	ached).		
490	1939207	INFO	2017-04-21 13:24:57	check_permissions	159.93.126.70	$sys/database/1/DbPutDevice Property/diagnostics/daqmxai/1/1/Al_SamplingFrequency/1/50000$	Access	granted (and c	ached).		
491	1939209 INFO 2017-04-21 13:24:57 check_permissions 159.93.126.70 sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/0 Access granted, cached access entry										
492	1939211	1 INFO 2017-04-21 13:24:57 check_permissions 159.93.126.70 sys/database/1/DbPutDeviceAttributeProperty2/diagnostics/daqmxai/1/1/Al_NumberOfSamples/1/_value/1/204800 Access granted (and cached).									
493	1939213	INFO	2017-04-21 13:24:57	check_permissions	159.93.126.70	sys/database/1/DbExportDevice/diagnostics/bergoz/1/IOR:01000001700000049444c3a54616e676f2f4465766963655f343a312e3000000100000000000640	Access	granted (and c	ached).		
494	1939215	INFO	2017-04-21 13:24:58	check_permissions	159.93.126.70	$sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/1/Al_SamplingFrequency/1/50000$	Access	granted, cache	d access entry		
495	1939217	19217 INFO 2017-04-21 13:24:58 check_permissions 159.93.126.70 sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/0 Access granted, cached access ent						d access entry			

Data archiving

HDB++ archiving system:

- Store TANGO attributes values into a database (SQL or noSQL).
- Publish/subscribe paradigm via TANGO archiving events storing only valuable information.
- Highly scalable multiple archivers to distribute load over few servers and disk storages.
- Under tests now on Superconducting Magnets Test Bench

 storing about 500 TANGO attributes
- JINR data archiving configuration GUI and extractor GUI to be developed.

Integration of third-party systems



Tango device to provide interface to external control system and represent it to NICACS:

- OPC (vacuum, cryocooler)
- NI DataSocket (Electron cooling)
- TCP/IP socket (Booster RF)

Conclusions

Distributed, scalable control system infrastructure based on Tango has been developed to provide fast development, deployment and safe execution:

code generation, TANGO drivers for NI equipment, deployment on dedicated VM in HA cluster, server-based access control, hardware and software monitoring, data archiving, equipment and software database.

Thank you for your attention!

- Tango client-side access control 3)
 - Optional service restricting devices commands execution and attributes writes based on client username & IP checks.
 - Not flexible, easy to pass.
 - Applies on Tango::DeviceProxy creation.
 - Need client restart



Idea:

 Improve access control by additional server side security checks

Goals:

- Centralized management of user's permissions
- Centralized access logs
- No complications to both Tango device server and client development
- No modifications to Tango library



Realization details:

- 1. Role Based Access Control (RBAC).
 - Each role have a group of permissions.
 - Few roles can be assigned to user/IP pair
- 2. Authentication by location (IP address).
 - Default Operator role and user
 - Operator user has no password
- Support of MySQL regular or wildcard expressions in rules and addresses: can be configured as Tango property.
- 4. Objects access cache for improving performance.

Service layer: RBAC

		uid 🚿	/ login	n last nam	e first name	1	phone		email			password			enable	d
0	1		operator	NULL	NULL	NULL		NULL		!] 1	
1	2		gorbe	Gorbachev	Evgeny	6305	63057 eç		egorbe@gmail.co		(MD5}cacbcc3edf3f5f46179588bdd97				j] 1	
2	3		egor	Sedykh	Georgy			egor@	dubna.tk	{MD	5}99907751	155c3518a0d7917f	7780b24a	aa [] 1	
						_										
							USE	er_role	_id	us	er_id	role_id	~	ipac	dr_expr	
						2	3			≥1:opera	itor	2:rbac-admin	127	.0.0.1		
						3	4			≥1:opera	itor	2:rbac-admin	159	.93.5().200	
						4	5			1:opera	itor	2:rbac-admin	159	.93.5().207	
						5	9			1:opera	itor	3:export-device	e 159	.93.5(0.200	
						6	13			1:opera	itor	3:export-device	e 159	.93.5	0.176	
						7	19			1:opera	itor	3:export-device	e 159	.93.5).207	
						8	11			1:opera	itor	4:put-property	159	.93.5(0.200	
						<u> </u>					1					
		r	ole_id	role_name	e des	cripior	٦		enab	led						
	0	1		operator	operator permi	ssions			1							
	1	2		rbac-admin	RBAC authoriza	tion m	anageme	ent [1							
	2	3		export-device	export a tango	device			1							
	3	4		put-property	add/delete a ta	ngo pr	operty		1							

Service layer: RBAC

		permission_id	role_id	,	obj	ect_expr		priority		enabled	$\hat{}$	
0	3		1:operator	s	sys/database/1/DbInfo 1			10		1		
1	2		1:operator	sys/database/1/DbImport% 1			10		1			
2	1		1:operator	s	ys/database/1/Db	Get%		10		1		
3	5		2:rbac-admin	s	ys/managerbac/1/	/%		0		1		
4	4		2:rbac-admin	s	ys/authrbac/1/%			0		1		
5	39	_	3:export-device	s	ys/database/1/Db	DeleteAll%		10		1		
6	33		3:export-device	s	ys/database/1/Db	UnExportServer/%		10		1		
7	29		3:export-device		rolo id	rolo nomo		docarinia				apphlad
8	27		3:export-device	0		operator	0.00	erator permissions				1
9	25		3:export-device	1	2	rbac-admin	DD.			aement		1
10	23		3:export-device	2	2	export-device		port a tango device		gement		1
11	31		4:put-property	2	3	export-device	exp			rts /		1
< (3	4	put-property	auc	ardelete a tango pi	ope	rty mala		1
				4	5	authtest	use	e TagoAuthTest col	nma	inas		1
				5	9	add-device	ado	d a new tango devi	ce			1
				6	11	tango-admin	usi	ing astor/logviewe				1
				7	13	tomography	usi	ing diagnostics/ton	nogr	aphy		1

Tango Users Group Russia meeting'2017

The Nuclotron and NICA control system, E.Gorbachev 44

Service layer: Access logs

	id	created \checkmark	source	IP	object	Entry
8	17	2016-06-21 14:50:06	open_session	159.93.50.207	gorbe	Session opened.
9	19	2016-06-21 14:50:11	authenticate	159.93.50.207	gorbe	Authentication successful.
10	21	2016-06-21 14:50:11	close_session	159.93.50.207	gorbe	Session closed
11	23	2016-06-21 14:50:24	authenticate	159.93.50.207	gorbe	Authentication failure - wrong password.
12	25	2016-06-21 14:50:30	authenticate	159.93.50.207	gorbre	Authentication failure - user unknown.
93	187	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/name,exported,version,ior,ser	Access granted (and cached).
94	189	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/name,exported,version,ior,ser	Access granted (and cached).
95	191	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/device,value FROM property_d	Access granted (and cached).
96	193	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/device,value FROM property_d	Access granted (and cached).
97	195	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/device,value FROM property_d	Access granted (and cached).
98	197	2016-06-23 13:45:20	check_permissions	159.93.50.207	sys/database/1/DbAddDevice/LogConsumer/se50-207@68	Access granted (and cached).
99	199	2016-06-23 13:45:20	check_permissions	159.93.50.207	sys/database/1/DbExportDevice/dserver/LogConsumer/se50	Access granted (and cached).
100	201	2016-06-23 13:45:20	check_permissions	159.93.50.207	sys/database/1/DbExportDevice/tmp/log/se50-207@68	Access granted (and cached).
109	219	2016-06-23 16:41:40	check_permissions	159.93.50.207	sys/database/1/DbAddDevice/NIScopeSaver/1	Access granted (and cached).
110	221	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbUnExportEvent/DServer/NIScopeSaver/1	Access granted (and cached).
111	223	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbPutClassProperty/NIScopeSaver	Access granted (and cached).
112	225	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbExportDevice/dserver/NIScopeSaver/1	Access granted (and cached).
113	227	2016-06-23 16:41:58	check permissions	159.93.50.207	svs/database/1/DbDeleteDeviceProperty/dserver/NIScopeSav	Access granted (and cached).

Property:

sys/database/1/DbImportDevice
sys/database/1/DbGet

Tango Users Group Russia meeting'2017 The Nu

skip_logging_for

The Nuclotron and NICA control system, E.Gorbachev

45



Passwords are MD5 hashed

Access control performance

RBAC server performance tests, 10000 permissions checks, 1 thread

Test	Regexp,	Wildcards,	Wildcards,
	no cache	no cache	cached
Time per one permission check, ms	32.95	7.79	0.95



Usage in TANGO device server: 1) Initialization:

#include "TangoAuth.h" TangoAuthClientClass *auth; In init_device(): auth=new TangoAuthClientClass(this); In delete_device(): delete auth;

2) Usage:

In method cmd_name:

auth->CheckAccess("cmd_name");

Or in always_executed_hook():

auth->CheckAccess("any");



			1	Manage Tango Role-Based access control	~ ^ 🛛
				File View Taurus Tools Help	
				Load Perspectives 💾 🕞 jive 🕞 astor	
				RBAC Status Sessions Roles Permissions Users User roles Logs	
				SYS/MANAGERBAC/1 SYS/AUTHRBAC/1	
X		Ma	nage Tango Role-Based access control		
File	View Taurus Tool	ls Help			
	Load Perspectives	🖹 🕞 jive	▶ astor	Attributes Commands Attributes Commands	
RBA	C Status Sessions	Roles Perm	nissions Users User roles Loo	maxlogdate 2016-09-02 14:57:50	
	permission id	role id 🗸	object expr	permissions Show	
0	3	1:operator	sys/database/1/DbInfo	roles Show	
1	2	1:operator	sys/database/1/DbImport%	session_ist in show	
2	1	1:operator	sys/database/1/DbGet%	user_roles 🗄 Show	
3	5	2:rbac-admin	sys/managerbac/1/%	users 🔲 Show	
4	4	2:rbac-admin	sys/authrbac/1/%	ManageRAC is ready	
5	39	3:export-device	sys/database/1/DbDeleteAll%	Tangorbachutiserveris on	1
6	33	3:export-device	sys/database/1/DbUnExportServer/%		~
7	29	3:export-device	sys/database/1/dbputclassproperty/%		>
8	27	3:export-device	sys/database/1/DbUnExportEvent/%		
9	25	3:export-device	sys/database/1/dbdeletedeviceproperty/%	10 1	
10	23	3:export-device	sys/database/1/dbexportdevice/%	10 1	
11	31	4:put-property	sys/database/1/dbputdeviceproperty/%	10 🔲 1 🗸	
)			
N	ew row Delete row		Data is valid	Apply changes Cancel changes	

Tango Users Group Russia meeting'2017The Nuclotron and NICA control system, E.Gorbachev

49

Protection of TANGO database:

Idea:

• Provide access to TANGO database with security checks and logging.

Possible solutions:

- Modification of each method of original Tango database server.
- Additional layer between clients and Tango database server.

Goals:

- Flexible rights separation export device, add device, edit properties.
- Acceptable performance.



Tango Users Group Russia meeting'2017 The Nuclotron and NICA control system, E.Gorbachev 51

Realization:

1) Initialize

Tango::Util::_UseDb = false;

set_serial_model(Tango::NO_SYNC);

2) Create dynamic commands and attributes.

dbdev = new Tango::DeviceProxy("sys/database/2");

cmdlist=dbdev->get_command_list();

cmdinfo=dbdev->get_command_config(cmdlist);

3) All dynamic commands use the same command class with method execute():

- Check access with command name
- Execute command on original device with arguments
- Return result to client

Database server performance tests:

4 parallel threads executing

time for i in `seq 1 1000`;do ./tango_exec sys/database/1 DbInfo > /dev/null; done

Database server	sys/database/2 (standard DB server)	sys/database/1 (with access control, cached)
Time per one command, ms	23.690	25.245

Global timing and synchronization

Timing and synchronization system is an important part of the accelerating complex:

- Global time reference for geographically distributed equipment.
- Beam diagnostics synchronization closed orbit measurements.
- Beam transfer synchronization with different scenarios: bunch to bucket, barrier buckets.
- Events and signals distribution.

White Rabbit principles

Layout:

- Tree layout with synchronization master on the top.
- Single fiber optic for RX/TX

Features:

- sub-nanosecond synchronization
- connecting thousands of nodes
- typical distances of 10 km between nodes
- Ethernet-based gigabit rate reliable data transfer
- fully open hardware, firmware and software
- multi-vendor commercially produced hardware
- Based on IEEE-1588 (PTP)
- 1Gb/s transfer rate



55

White Rabbit elements

- Designated fiber optic network
- Endpoint devices with embedded *White Rabbit Protocol Core*
- WhiteRabbit switches *WRS-3/18*
- GPS/GLONASS Time receiver
- Rubidium frequency standard generator *Pendulum CNT-91R*



Modules with White Rabbit support



Simple PXI express FMC Carrier Board (SPEXI) Project on www.ohwr.org



NICA CS prototypes

- Booster thermo diagnostics 320 channels NI PXIe based RTD measurements.
- Booster magnetic cycle control FlexRIO + custom IO modules.
- Booster RF integration of third-party CS.
- Booster/Linac vacuum integration of third-party SCADA control.
- NICA injection/extraction control CompactRIO + custom IO modules.
- Booster/NICA orbit correction.
- Beam diagnostics (profiles, intensity, tune measurements) NI PXIe
- SC magnets test bench- thermometry (NI PXIe), satellite refrigerators control (interface to SCADA)
- WhiteRabbit on B@MN aquisition