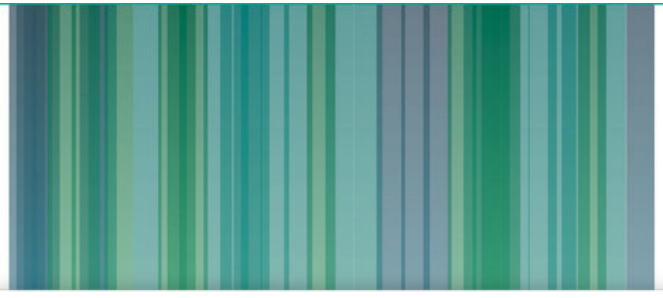


iRODS

Auditing with the Pluggable Rule Engine and AMQP

Terrell Russell, Ph.D.
@terrellrussell
Senior Data Scientist, iRODS Consortium

June 7-9, 2016
iRODS User Group Meeting 2016
Chapel Hill, NC

Rule Engine Plugin Interface

iRODS 4.2 adds a seventh plugin interface:

- microservices
- resources
- authentication
- network
- database
- RPC API
- rule engine

Rule Engine Plugin Interface

Plugin Name	Plugin written in:	Rules written in:
Dispatcher	C++	n/a
iRODS Rule Language	C++	iRODS Rule Language
Python	C++	Python
Javascript	C++	Javascript
Audit	C++	rules are hardcoded
Storage Balancing	C++	rules are hardcoded

Rule Engine Plugin Interface

Default /etc/irods/server_config.json includes...

```
"rule_engines": [
    {
        "instance_name": "re-instance",
        "plugin_name": "re",
        "plugin_specific_configuration": {
            "namespaces": [{"namespace": ""},{"namespace": "audit_"},{"namespace": "indexing_"}]
        }
    },
    {
        "instance_name": "re-irods-instance",
        "plugin_name": "re-irods",
        "plugin_specific_configuration": {
            "re_data_variable_mapping_set": [{"filename": "core"}],
            "re_function_name_mapping_set": [{"filename": "core"}],
            "re_rulebase_set":              [{"filename": "core"}]
        },
        "shared_memory_instance": "legacy_re"
    }
],
```

Rule Engine Plugin Interface

Default /etc/irods/server_config.json includes...

```
"rule_engines": [
    {
        "instance_name": "re-instance",
        "plugin_name": "re",
        "plugin_specific_configuration": {
            "namespaces": [{"namespace": ""},{"namespace": "audit_"},{"namespace": "indexing_"}]
        }
    },
    {
        "instance_name": "re-irods-instance",
        "plugin_name": "re-irods",
        "plugin_specific_configuration": {
            "re_data_variable_mapping_set": [{"filename": "core"}],
            "re_function_name_mapping_set": [{"filename": "core"}],
            "re_rulebase_set":              [{"filename": "core"}]
        },
        "shared_memory_instance": "legacy_re"
    }
],
```

dispatcher

irods rule language

Rule Engine Plugin Interface

Updated /etc/irods/server_config.json
with added custom.re and Python rule engine plugin...

```
"rule_engines": [
    {
        "instance_name": "re-instance",
        "plugin_name": "re",
        "plugin_specific_configuration": {
            "namespaces": [{"namespace": ""},{"namespace": "audit_"},{"namespace": "indexing_"}]
        }
    },
    {
        "instance_name": "irods_rule_engine_plugin_python-instance",
        "plugin_name": "irods_rule_engine_plugin_python",
        "plugin_specific_configuration": {}
    },
    {
        "instance_name": "re-irods-instance",
        "plugin_name": "re-irods",
        "plugin_specific_configuration": {
            "re_data_variable_mapping_set": [{"filename": "core"}],
            "re_function_name_mapping_set": [{"filename": "core"}],
            "re_rulebase_set": [
                {"filename": "custom"},
                {"filename": "core"}
            ]
        },
        "shared_memory_instance": "legacy_re"
    }
],
```

dispatcher

python

irods rule language

Rule Engine Plugin Interface

Updated /etc/irods/server_config.json with added Audit rule engine plugin...

```
"rule_engines": [
    {
        "instance_name": "re-instance",
        "plugin_name": "re",
        "plugin_specific_configuration": {
            "namespaces": [{"namespace": ""},{"namespace": "audit_"},{"namespace": "indexing_"}]
        }
    },
    {
        "instance_name": "re-audit-amqp-instance",
        "plugin_name": "re-audit-amqp",
        "plugin_specific_configuration" : {
            "pep_regex_to_match" : "audit_.*",
            "amqp_topic" : "amq.topic",
            "amqp_location" : "localhost:5672",
            "amqp_options" : ""
        }
    },
    {
        "instance_name": "re-irods-instance",
        "plugin_name": "re-irods",
        "plugin_specific_configuration": {
            "re_data_variable_mapping_set": [{"filename": "core"}],
            "re_function_name_mapping_set": [{"filename": "core"}],
            "re_rulebase_set":              [{"filename": "core"}]
        },
        "shared_memory_instance": "legacy_re"
    }
],
```

dispatcher

audit

irods rule language

Audit (C++) Rule Engine Plugin

The Audit rule engine plugin can emit a single AMQP message to the configured topic for every policy enforcement point (PEP) encountered by the iRODS server.

This AMQP message has all of the information related to that particular operation, including username, filepath, filesize, etc.

Catching and analyzing these messages will allow visualization of totals and trends.

Inside an iCommand

Parsing the operation from each AMQP message lets us see the full flow of a client request through the server's code.

Client Request	Dynamic PEPs	Static PEPs
ils	174	4
iget	148	6
ireg	168	7
iput	234	11
iput (1GB large file)	978	44
imeta	106	6

Inside an iCommand

A sample of the PEPs hit by an iget:

```
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_obj_stat_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
```

Inside an iCommand

iget

audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_database_open_pre
audit_pep_database_open_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_microservice_pre
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_network_agent_start_pre
audit_pep_network_agent_start_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_auth_request_pre
audit_pep_auth_agent_auth_request_pre
audit_pep_auth_agent_auth_request_post
audit_pep_auth_request_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_auth_response_pre
audit_pep_auth_agent_auth_response_pre
audit_pep_database_check_auth_pre
audit_pep_database_check_auth_post
audit_pep_auth_agent_auth_response_post
audit_pep_auth_response_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post

audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_obj_stat_pre
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_obj_stat_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_data_obj_get_pre
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_resource_resolve_hierarchy_pre
audit_pep_resource_resolve_hierarchy_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_resource_open_pre
audit_pep_resource_open_post
audit_pep_resource_read_pre
audit_pep_resource_read_post
audit_pep_resource_close_pre
audit_pep_resource_close_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_data_obj_get_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_network_agent_stop_pre
audit_pep_network_agent_stop_post
audit_pep_database_close_pre
audit_pep_database_close_post

Inside an iCommand

iget

connection setup

audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_database_open_pre
audit_pep_database_open_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_microservice_pre
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_network_agent_start_pre
audit_pep_network_agent_start_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post

auth

audit_pep_auth_request_pre
audit_pep_auth_agent_auth_request_pre
audit_pep_auth_agent_auth_request_post
audit_pep_auth_request_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_auth_response_pre
audit_pep_auth_agent_auth_response_pre
audit_pep_database_check_auth_pre
audit_pep_database_check_auth_post
audit_pep_auth_agent_auth_response_post
audit_pep_auth_response_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post

audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post

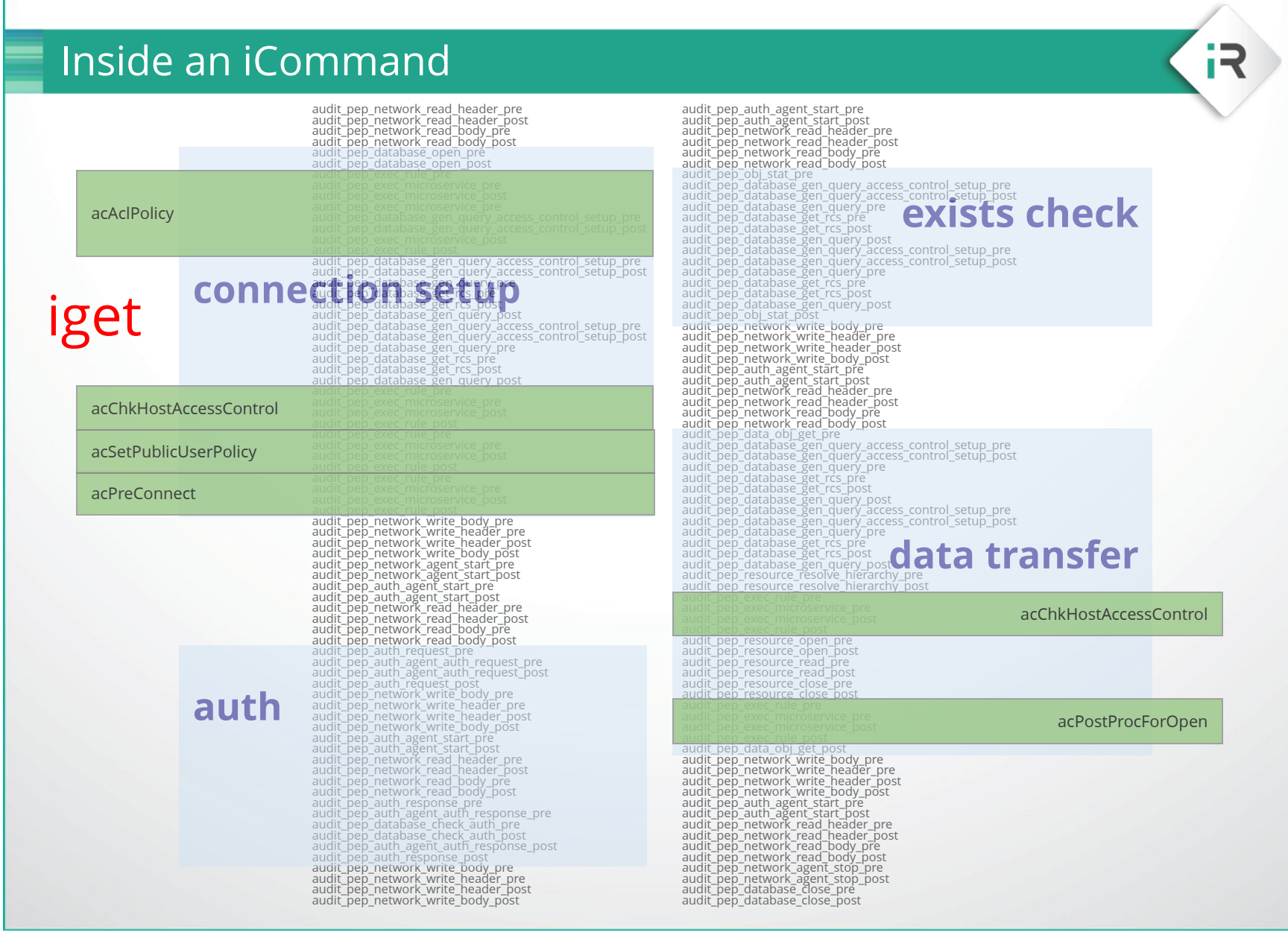
exists check

audit_pep_obj_stat_pre
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_obj_stat_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post

data transfer

audit_pep_data_obj_get_pre
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_database_gen_query_access_control_setup_pre
audit_pep_database_gen_query_access_control_setup_post
audit_pep_database_gen_query_pre
audit_pep_database_get_rcs_pre
audit_pep_database_get_rcs_post
audit_pep_database_gen_query_post
audit_pep_resource_resolve_hierarchy_pre
audit_pep_resource_resolve_hierarchy_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_resource_open_pre
audit_pep_resource_open_post
audit_pep_resource_read_pre
audit_pep_resource_read_post
audit_pep_resource_close_pre
audit_pep_resource_close_post
audit_pep_exec_rule_pre
audit_pep_exec_microservice_pre
audit_pep_exec_microservice_post
audit_pep_exec_rule_post
audit_pep_data_obj_get_post
audit_pep_network_write_body_pre
audit_pep_network_write_header_pre
audit_pep_network_write_header_post
audit_pep_network_write_body_post
audit_pep_auth_agent_start_pre
audit_pep_auth_agent_start_post
audit_pep_network_read_header_pre
audit_pep_network_read_header_post
audit_pep_network_read_body_pre
audit_pep_network_read_body_post
audit_pep_network_agent_stop_pre
audit_pep_network_agent_stop_post
audit_pep_database_close_pre
audit_pep_database_close_post

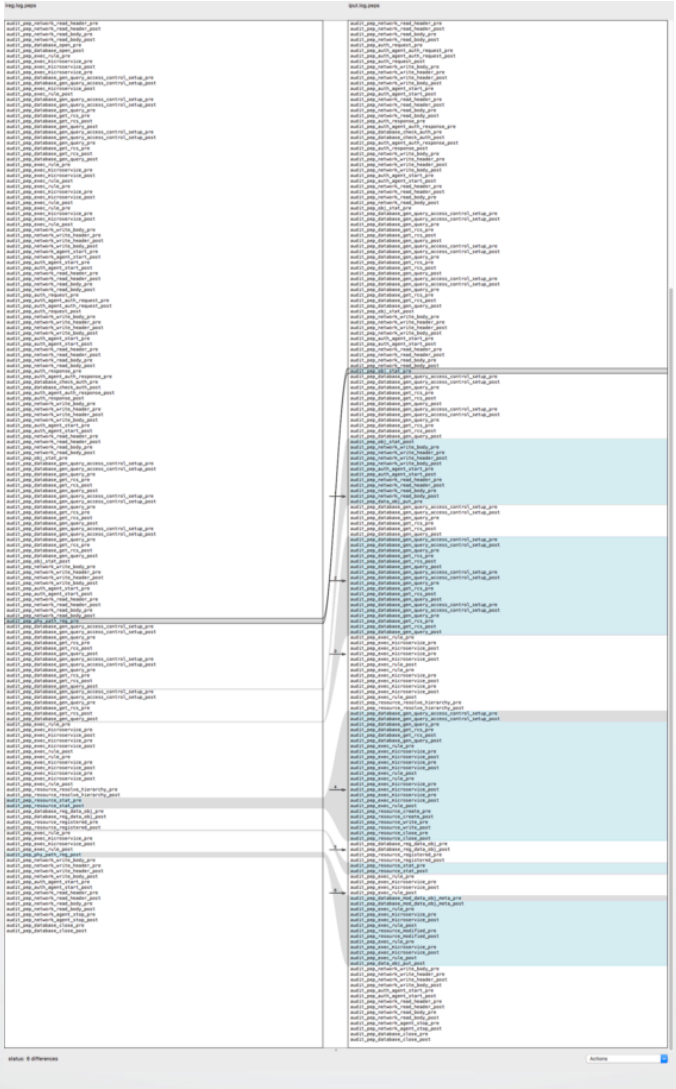
Inside an iCommand



Inside an iCommand

ireg

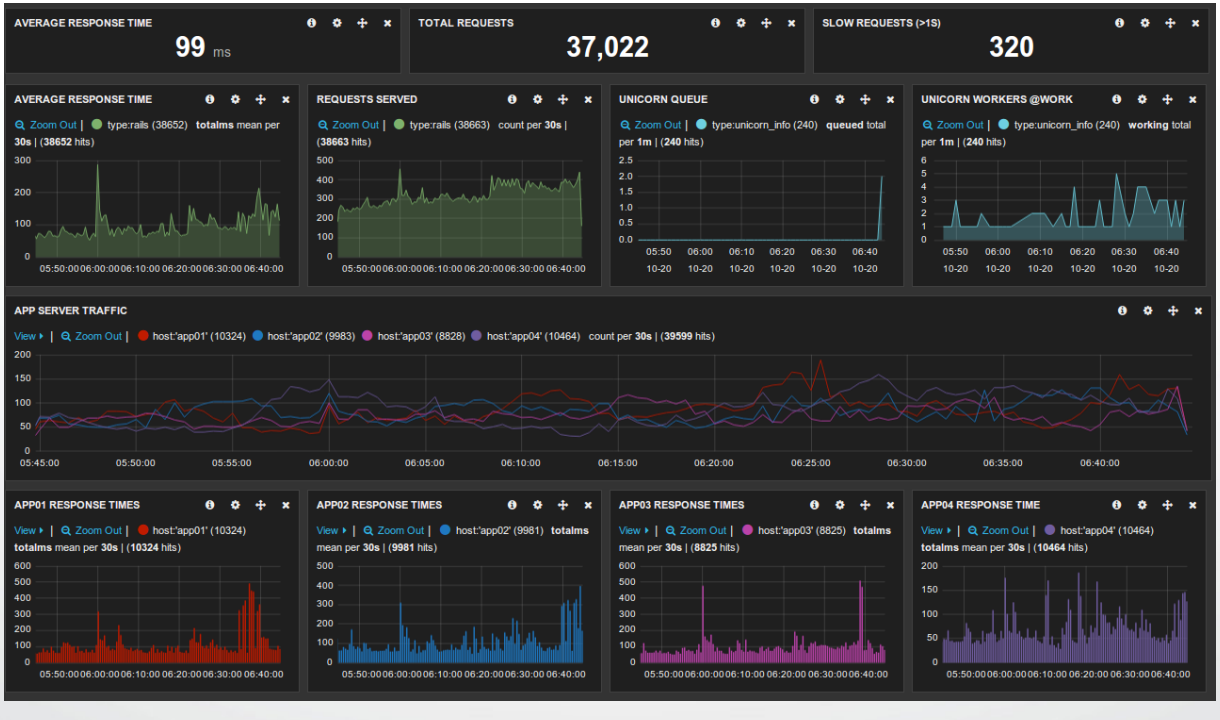
iput



Analysis Pipeline

iRODS → ActiveMQ ← Logstash → ElasticSearch ← Kibana

AMQP STOMP



Questions / Discussion

Thank you

Terrell Russell, Ph.D.
@terrellrussell