PVA Gateway
Production Requirements

June 13, 2018

Bruce Hill

SLAC NATIONAL ACCELERATOR LABORATORY

SLAC production deployment of PVAccess

- Only within accelerator control subnet and within development subnets.
- No access security in current PVAccess.
- Not deployed on critical IOCs where access security is used.
- Primarily for higher level data aggregation and analysis.

SLAC is also working towards LCLS2 where we plan to utilize PVAccess extensively.

To that end, we're working on defining requirements for PVA Gateway improvements to allow PVAccess to be utilized between subnets with configurable access security.

EPICS V4 Gateway Requirements document

Thanks to the efforts of Ralph Lange and the EPICS V4 Working Group, we have an existing requirements document which served as an excellent reference and baseline for our discussions.

http://epics-pvdata.sourceforge.net/doc/pvGateway/requirements.html

We would also like to thank Michael Davidsaver for his work on the pva2pva module which provides qsrv and p2p which implements most of the features from the V4 Gateway requirements.

Broader production use of PVAccess at SLAC will require:

- PVAccess between subnets via PVA gateway proxy
- Access Security on IOCs and on gateway
- Testing for stable reliable performance under load
- Diagnostic PVs
- Logging, including Put Logs
- Documentation
- Configurable bandwidth limits by channel name
- Performance enhancements

SLAC expects there will be several years of overlap where we need to support both CA and PVA.

- An IOC SecurityPlugin is required for pvAccess which works with the existing EPICS Access Security and utilizes the same access security configuration files.
- PVA gateway requires a pvAccess SecurityPlugin that can utilize the same Access Security configuration files as the CA Gateway.
- A single plugin could potentially satisfy both these requirements.

Differences vs CA Access Security

- Hostname shall be derived via ipAddrToHostName().
- Clients trusted to provide username, same as CA. Will need a way to send username to PVA server.
- Future SecurityPlugin would provide secure authentication of username. Considering Kerberos, Java Web Tokens, and other approaches.
- Extend EPICS Access Security to allow specifying UAG via posix groupname.

Testing

- Unit tests shall be provided to verify these V4 Working Group Gateway Requirements:
  - PVGW-REQ-F-001 pvAccess Client
  - PVGW-REQ-F-002 pvAccess Server
  - PVGW-REQ-F-101 Full pvData Support
  - PVGW-REQ-F-102 Full Normative Type Support
  - PVGW-REQ-F-141 Transparent Data Behavior
  - PVGW-REQ-F-142 Transparent Out -of-Band Behavior
  - PVGW-REQ-F-143 Transparent Timeout Behavior
  - PVGW-REQ-F-151 Name Server
  - PVGW-REQ-F-161 Connection Cache

Testing

- Test plans shall be documented and executed to verify these V4 Working Group Gateway Requirements
  - PVGW-REQ-F-021 Configurable Server Side Network Binding
- Test plans shall be documented and executed to verify gateway performance and operation under bottleneck conditions. Update rates can slow but new connections must still succeed.
  - Bandwidth to internal PVA servers exceeding network adapter capacity.
    - Ex: Monitoring numerous large arrays with high update rates
  - Bandwidth to external PVA clients exceeding network adapter capacity.
    - Ex: Numerous clients monitoring the same large array with a high update rate.
  - Test performance when CPU capacity is the bottleneck.
    - Ex: Load testing with clients and servers on the same host as the gateway.

- PVGW-REQ-I-001 Statistics Data
  - V4 WG Text: The Gateway should provide statistical and performance data s pvData NT structures.
  - SLAC Requirement: Diagnostics PV's shall include at least the following:
    - EPICS style alarm limits, severity and status for each PV
    - Number of client side PVA connections
    - Number of server side PVA connections
    - Total client bandwidth
    - Total server bandwidth
    - CPU usage
    - Memory usage
    - Thread count for both client side and server side
    - Client side server list w/ bandwidth for each server
    - Client side PV list w/ bandwidth for each PV
    - Server side client list w/ bandwidth for each client
    - Server side PV list per client w/ bandwidth for each PV
- PVGW-REQ-I-002 Network Binding for diagnostic PVs

Diagnostics

- Additional SLAC Diagnostic Requirements:
  - Diagnostic PVs that trigger generation of status report files.
  - Status reports shall include current value of the diagnostic PV's
    - Separate status reports for Client side PV list and Server side PV list.
  - Debug level shall be configurable to enable output of diagnostic messages to aid in debugging and diagnosing gateway issues with higher debug levels generating more diagnostic output to the gateway log files.

Logging

- Configuration options shall be added to enable put logging of all PVA put operations including channel name, timeStamp, value, client username and client IP to a configurable put log filename.
- Configuration options shall include a configurable gateway log file for normal gateway startup, status, and shutdown messages, along with any enabled debug level based output.

Documentation

- Threading model for the PVA gateway including diagrams as appropriate.
- Memory management model for the PVA gateway.
- HTML pages shall be generated to describe how to launch and configure the PVA gateway, including details on all configuration options including access control configuration.
- Doxygen compatible and descriptive comments shall be added for each of the following:
    - Source files
    - Classes
    - Structures
    - Variables
    - Typedefs
    - Functions
- Additional comments shall be added to source code which is complicated or whose purpose is not readily apparent.

Caching

- PVGW-REQ-F-131 Data Cache
  - Monitoring and caching of new values from the internal servers shall be implemented to reduce network bandwidth and support higher update rates.
- PVGW-REQ-F-132 Configurable Data Cache
  - Enable or disable caching globally and by channel name regex.

Channel Sharing

- PVGW-REQ-F-121 Combine Sub-Structure Subscriptions
  - The Gateway should be able to combine external clients' subscriptions to different sub-structures of the same channel into one subscription to the internal server.

Data Reduction

- Similar to PVGW-F-112, Quality of Service Mechanisms
  - WG text: The Gateway should implement mechanisms to avoid negative effects of connections with large structures and arrays on connections to other PVs on the same internal server.
- SLAC Requirements
  - PVA Gateway must support CA style array filter to allow fetching or monitoring sub-arrays.
  - Bandwidth limit filter by channel with global default
    - Allows prioritizing some PVA channels over others.
    - Guard against naive PVA clients consuming too much bandwidth.
  - Rate limit filter by channel with global default

Notable omissions from EPICS V4 WG Requirements

- PVGW-REQ-F-011 Channel Access Client
- PVGW-REQ-F-012 Channel Access Server
  - While these features are tempting as they would allow discontinuation of CA Gateways, it's not clear that they are feasible.
  - SLAC consensus is to prioritize other PVA Gateway features over this.
- Other requirements were seen as nice to have, but not required at this time.
  - PVGW-REQ-F-004 Redundant pvAccess Server Operation
  - PVGW-REQ-F-111 Low Latency for Large Structures/Arrays
  - PVGW-REQ-F-203 Proxy AuthN/AuthZ
  - PVGW-REQ-I-011 Debugging Shell

SLAC PVA Gateway Requirements

The EPICS Collaboration is invited to access and add comments to the SLAC PVA Gateway Requirements document via this google docs linik:

https://docs.google.com/document/d/1y2SBxUJ-fy8L37uG-lDlyEK5KgfEz-ecnyo9OJFwctw/edit?usp=sharing