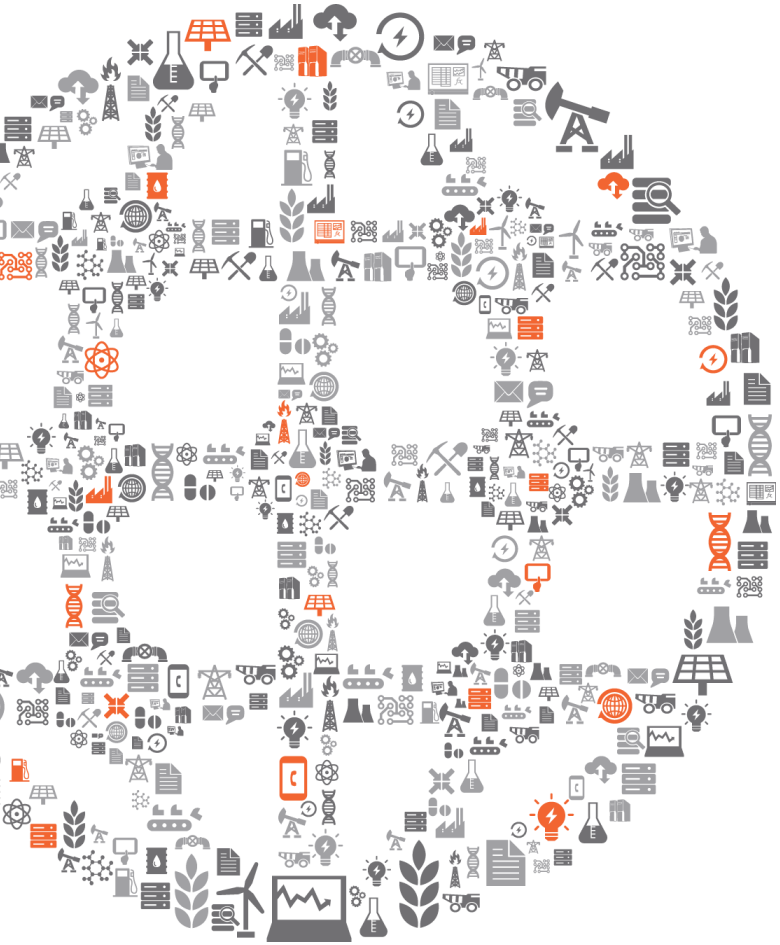


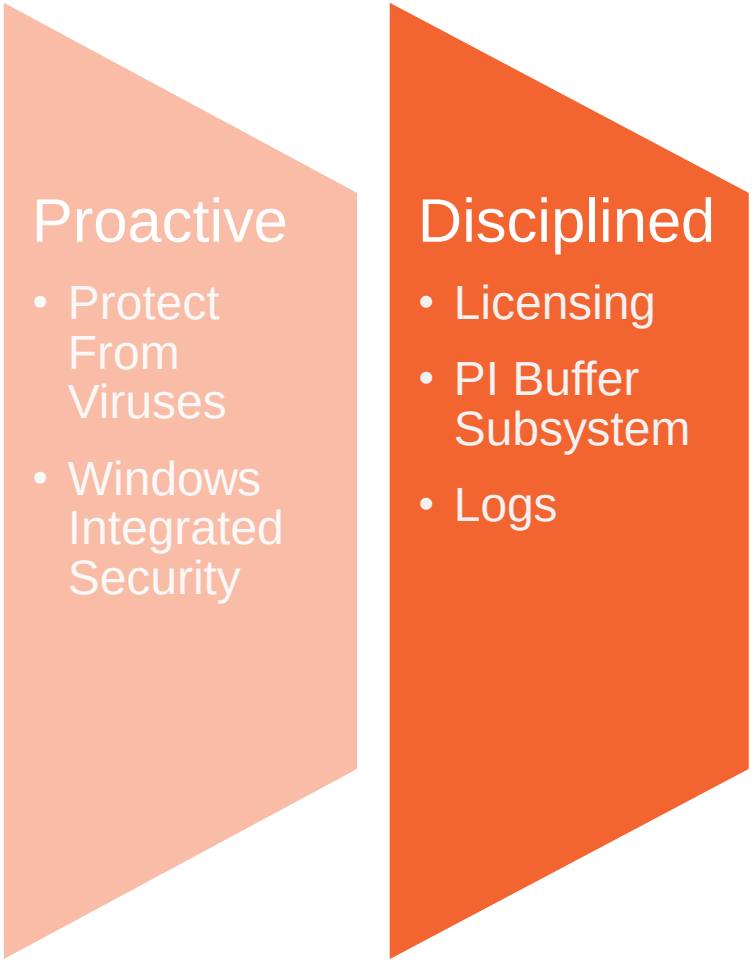
Tips from the Trenches

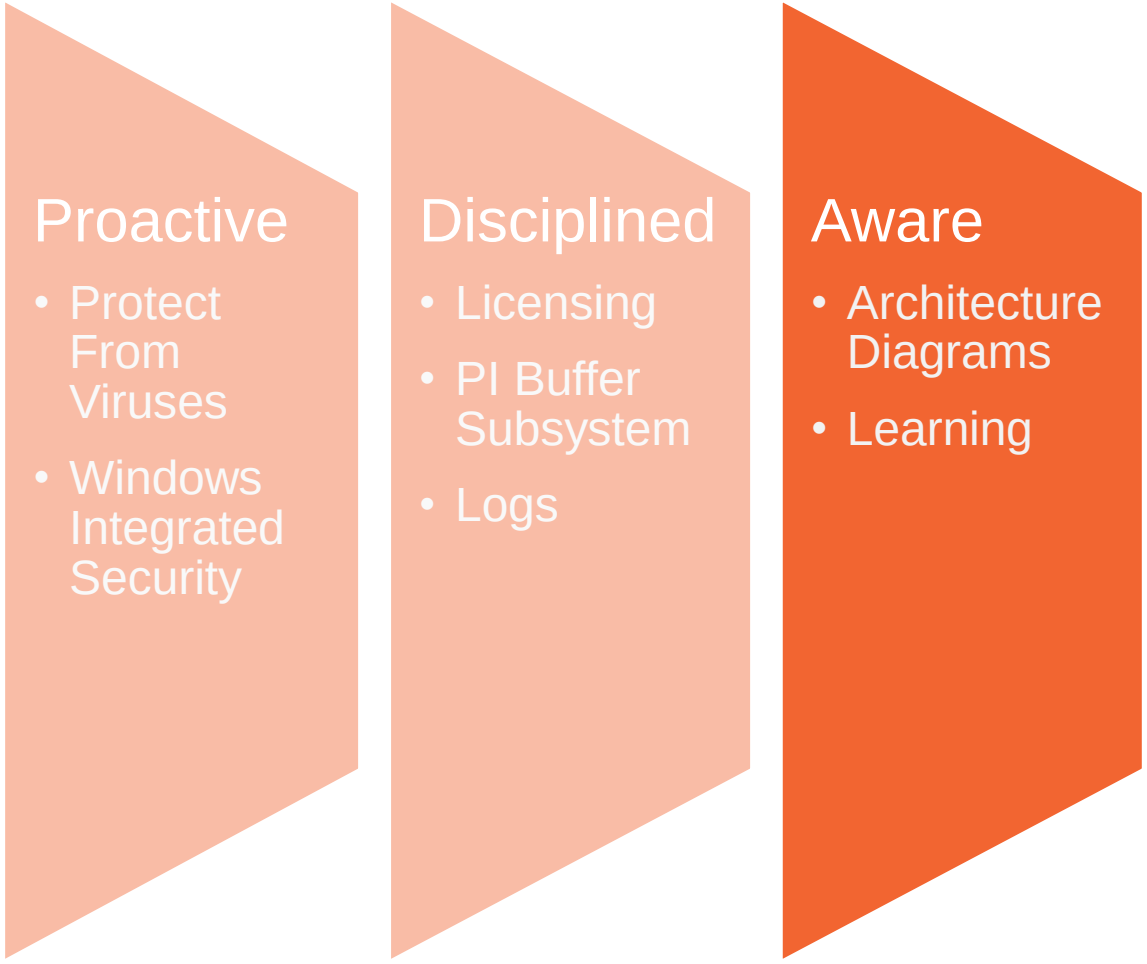
Presented by **Tony Yan Jian** and **Karn Udomsangpetch**

Tech Support and Field Service

Proactive

- Protect From Viruses
- Windows Integrated Security


Proactive
• Protect From Viruses
• Windows Integrated Security
Disciplined
• Licensing
• PI Buffer Subsystem
• Logs


Proactive
• Protect From Viruses
• Windows Integrated Security
Disciplined
• Licensing
• PI Buffer Subsystem
• Logs
Aware
• Architecture Diagrams
• Learning

Virus Infection at an Electric Utility

> "A third-party technician used a USB-drive to upload software updates during a scheduled outage for equipment upgrades. Unknown to the technician, the USB-drive was infected with crimeware. The infection resulted in downtime for the impacted systems and delayed the plant restart by approximately three weeks."

(Continued on next slide)

Virus Infection at an Electric Utility

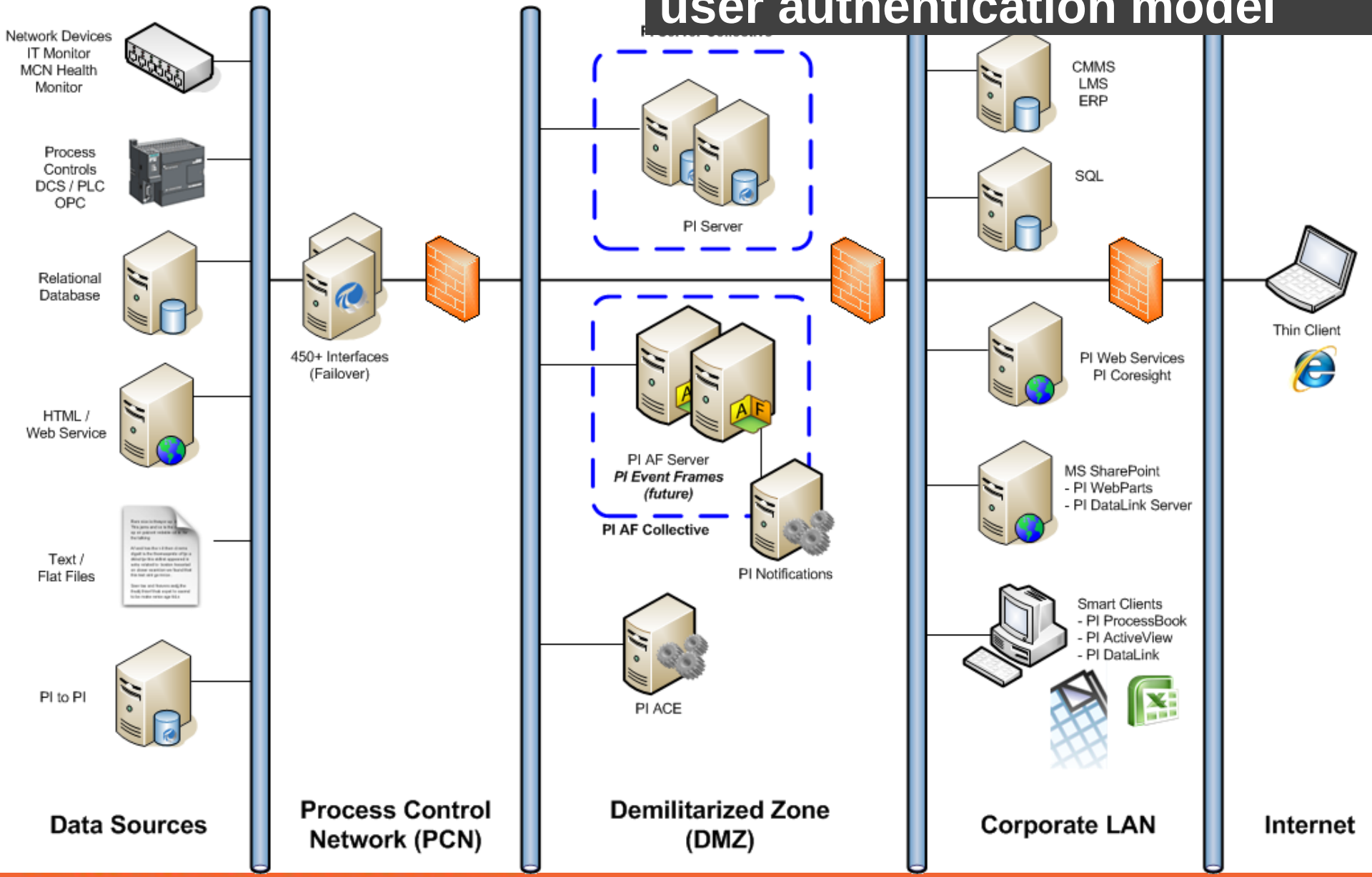
> "A third-party technician used a USB-drive to upload software updates during a scheduled outage for equipment upgrades. Unknown to the technician, the USB-drive was infected with crimeware. The infection resulted in downtime for the impacted systems and delayed the plant restart by approximately three weeks."

(Continued on next slide)

Scan USB Sticks Regularly

- OSIsoft uses endpoint protection
- 3rd parties always have the option to scan the device themselves
- Always scan thumb drives

Small steps to a more secure user authentication model



Explicit Login and Pladmin

- Do not use explicit login anymore
  - Especially for the piadmin user!
- Security Alert: PI Authentication Weakness
  - October 2009
  - Encryption Algorithm is no longer safe

https://www.kb.cert.org/vuls/id/479051

Vulnerability Note VU#4790...

Overview

OSIsoft PI Server provides an insecure authentication mechanism that could allow attackers to read or modify information in databases.

Description

PI Server is a core component of the OSIsoft PI System.

According to a report from C4 Security, OSISoft release notes (login required) for PI Server 3.4.380.36, and OSISoft KB article 5120OSI8, it appears that changes were made to PI Server to better resist brute force authentication attempts. PI Server 3.4.380.36 deprecates an older authentication mechanism in favor of Microsoft Windows authentication.

Windows authentication provides security features such as: logging failed login attempts, enforcing minimum password lengths, and enforcing password time-outs.

Impact

According to reports it appears that the old PI Sever integrated authentication security system method was susceptible to brute force authentication attempts. A successful attempt will allow an attacker to gain access to the PI Server databases.

Solution

OSIsoft recommends upgrading to PI Server version 3.4.380.36.

According to the PI Server 3.4.380.36 release notes the following procedures to mitigate the vulnerability:

Enable the PI Server for Windows authentication and configure PI Trust records
Use IPSec between the PI Server and the different client computers

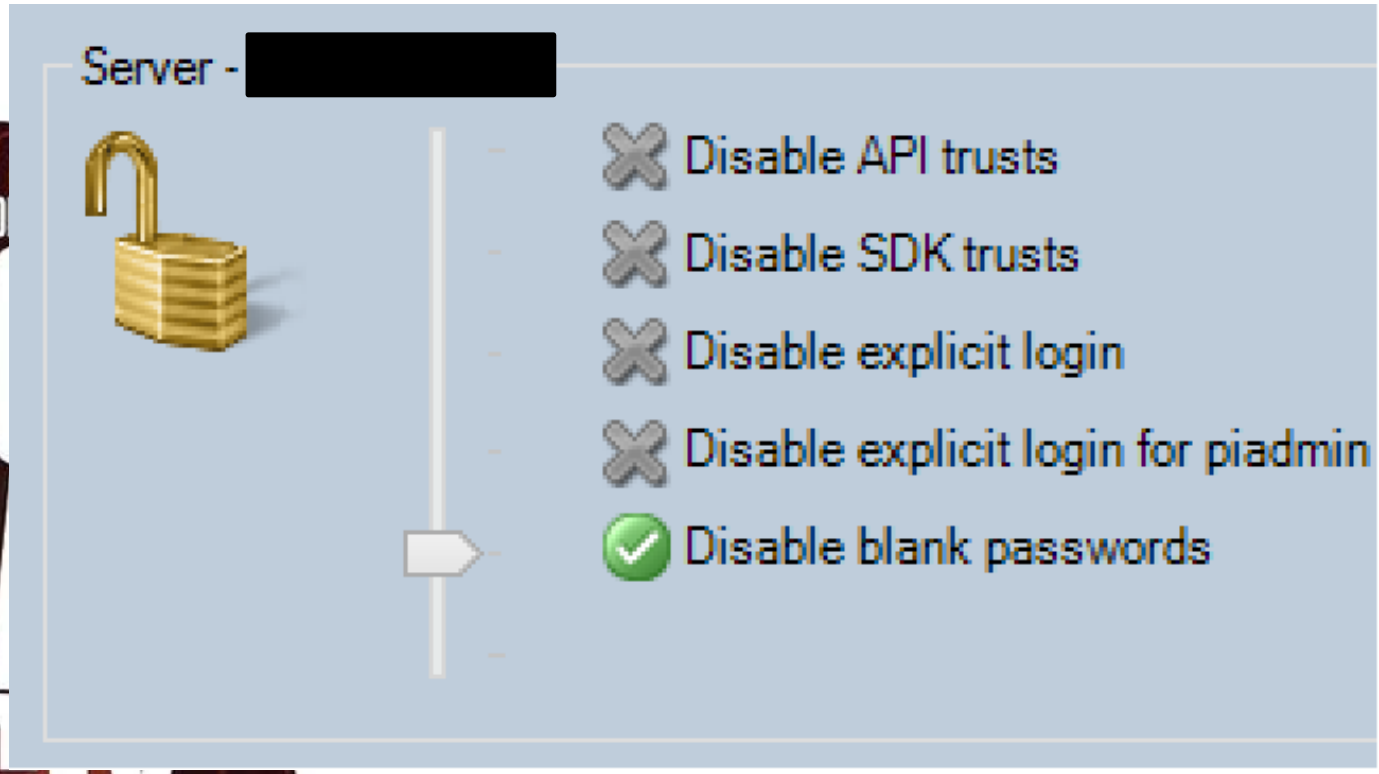
Public security bulletin

Solution

OSIsoft recommends upgrading to PI Server version 3.4.380.36.

According to the PI Server 3.4.380.36 release notes the following procedures to mitigate the vulnerability:

Enable the PI Server for Windows authentication and configure PI Trust records
Use IPSec between the PI Server and the different client computers



Explicit Login: How To

Security Take Home Points

Using long and complex passwords for explicit login protects me?

False

Windows Integrated Security will have the same weakness?

False

A Case from the Tech Support Trenches

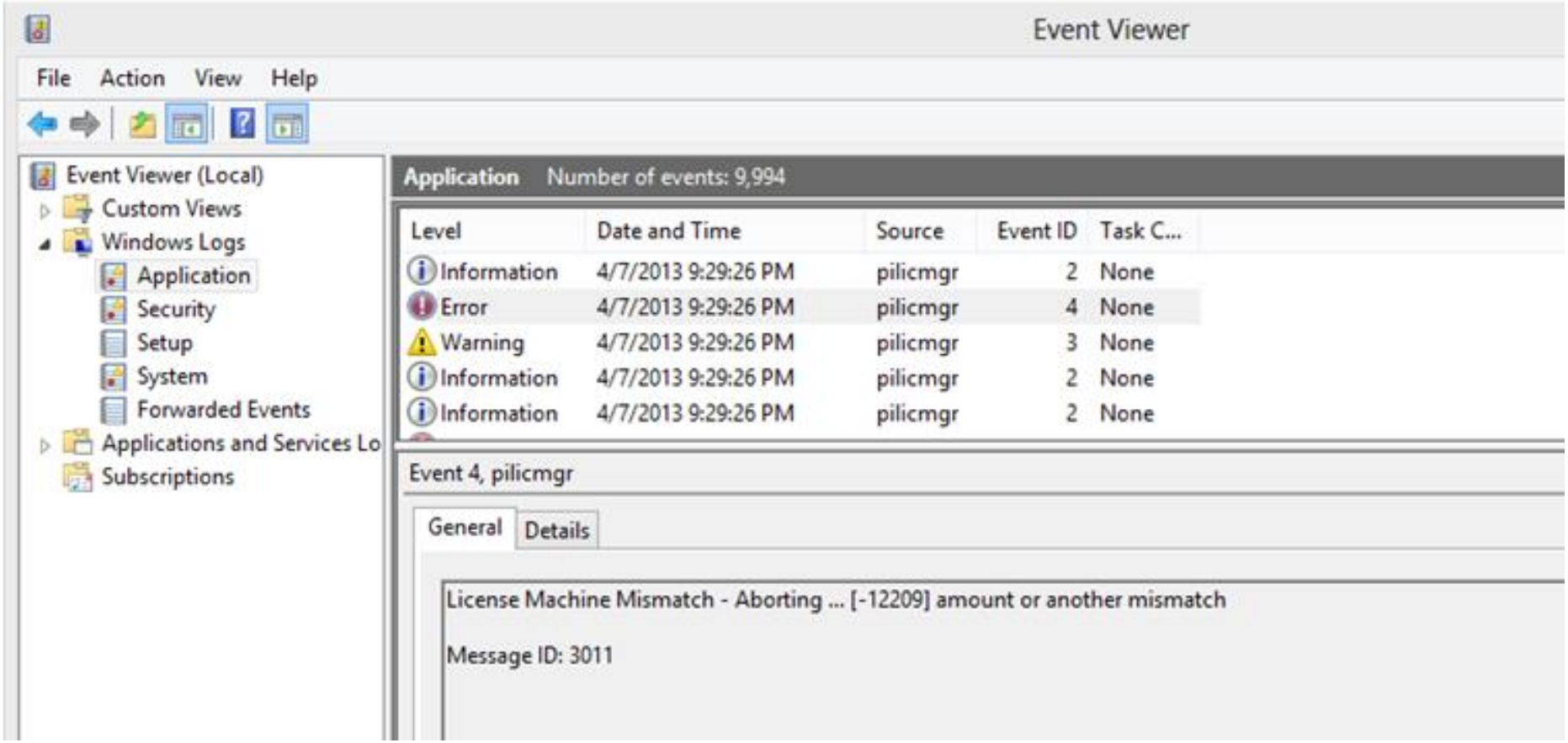
My PI Server will not Start!

Check the PI Server Message Logs

```
C:\Program Files\PI\adm>pigetmsg -st * -et *-15m
> No messages
```

Check the Event Viewer Logs

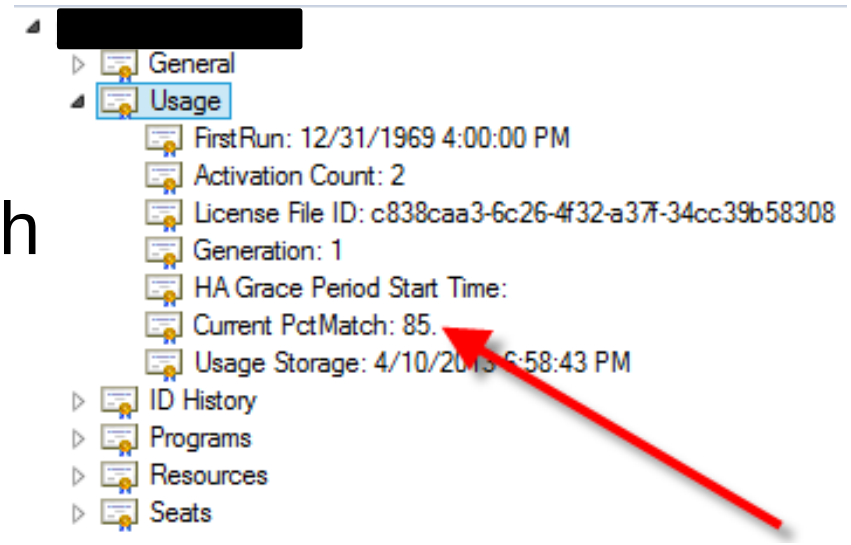
My PI Server will not Start!

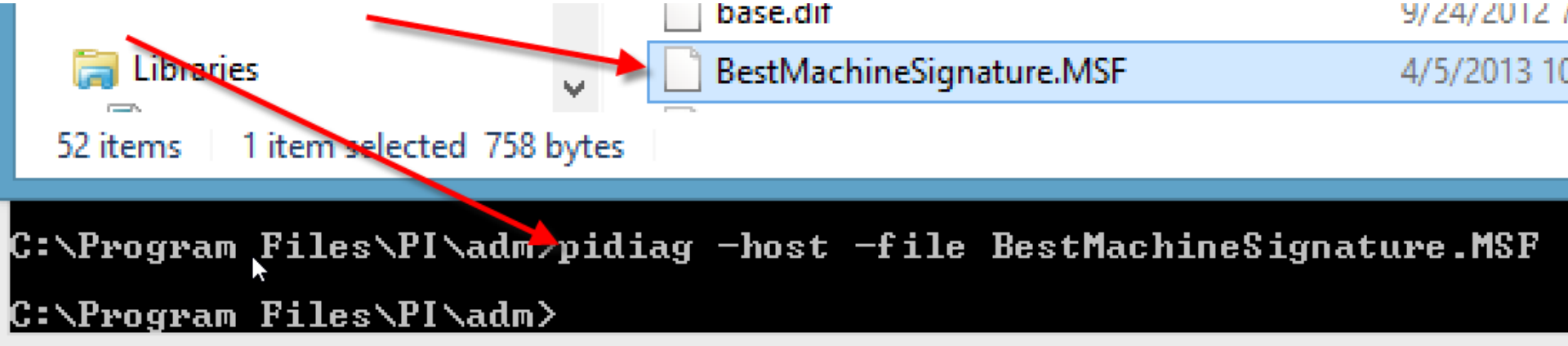


Licensing

Need highest percent match

Field Service Standards





PI Buffer Subsystem Example

- Windows Integrated Security
- Everyone group has read access
- Machines map to the Everyone group

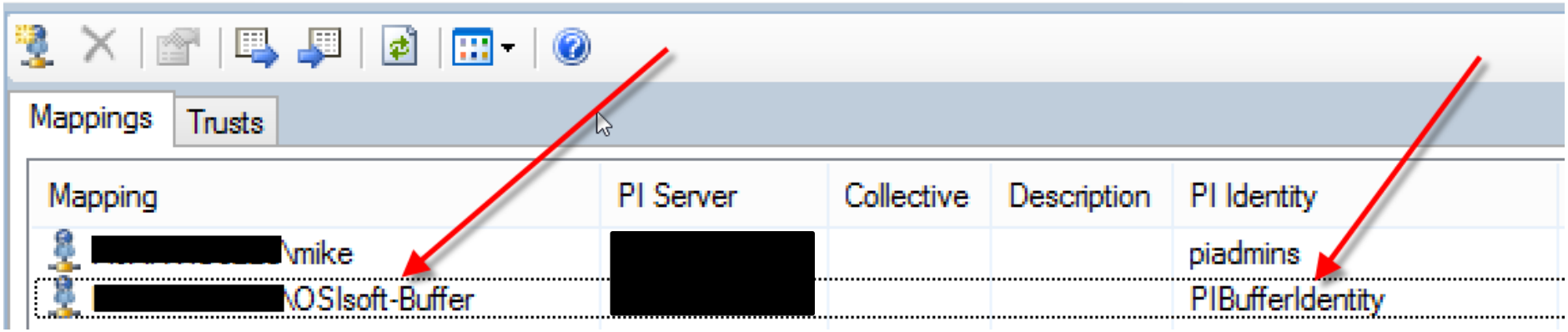
```
D 05-Apr-13 10:30:26 pinetmgr                                          (7082)
 >> Successful login  ID: 63. Address:   . Name: pibufss. Identity List: PIEngine
ers | PIWorld. Environment Username : NT AUTHORITY\SYSTEM. Method: Windows Login
 (SSPI,NTLM)
```

- PI Buffer Subsystem may connect as a read-only user

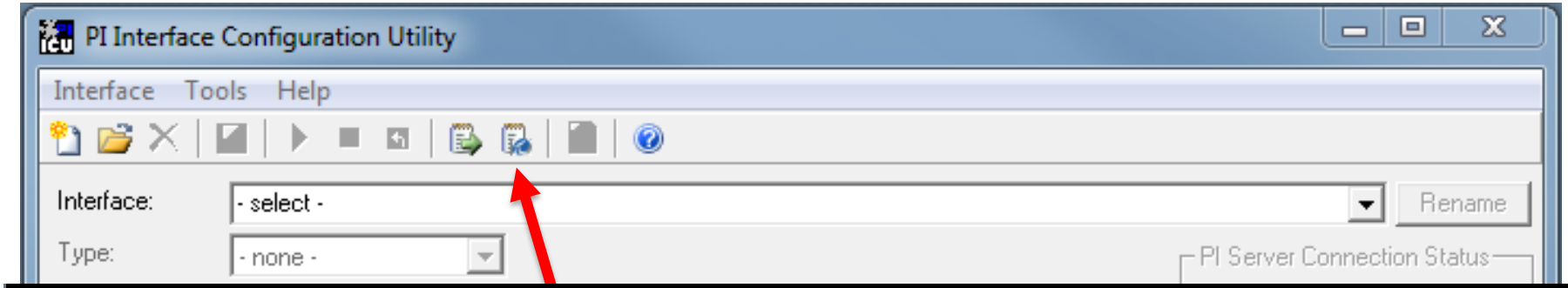
PI Buffer Subsystem Example

- Use Windows Integrated Security
- Allow the buffer to connect as a PI Identity with write access to the Points which it owns

PI Buffer Subsystem: How To

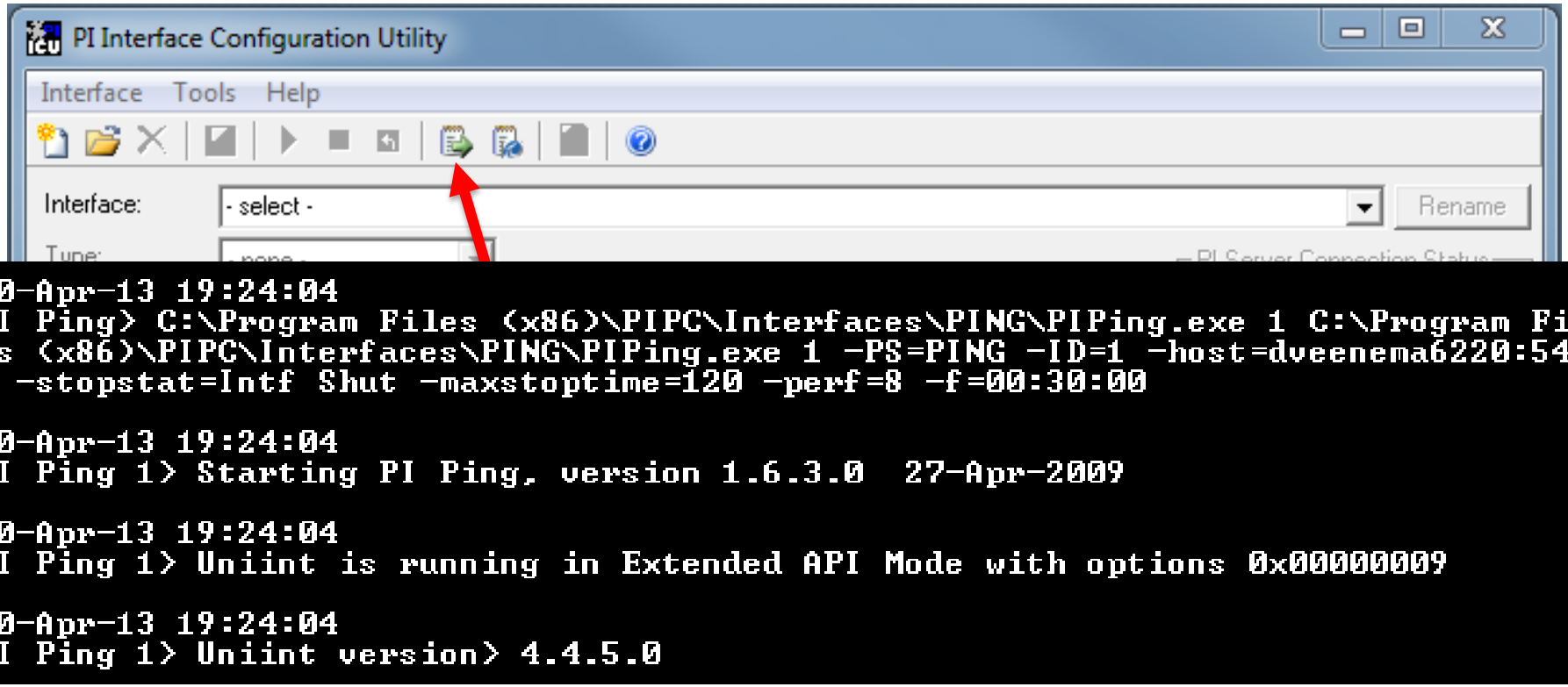


Listen to your system: PI Message log

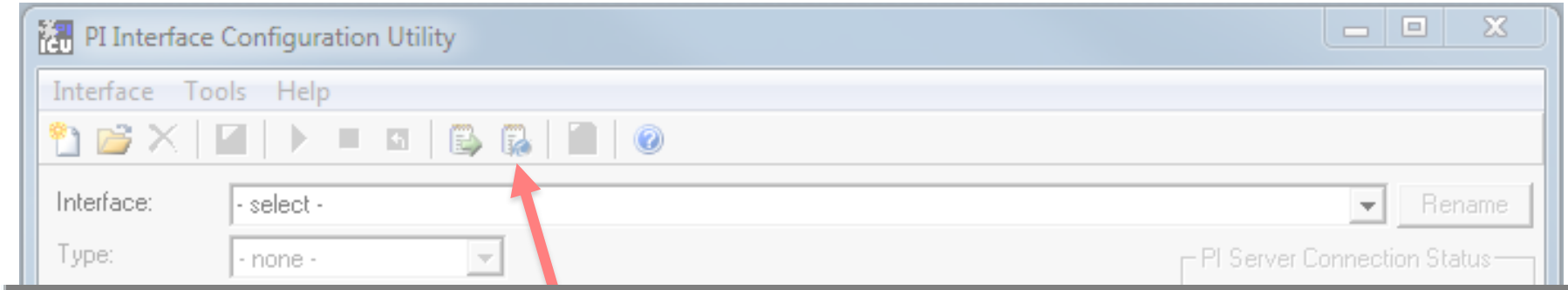



```
I 10-Apr-13 19:16:16 pinetmgr:Connection Information                    (7080)
 >> New Connection ID: 47 ; Process name: Procbook.exe(8772) ; User: piadmins !
PIWorld ; OS User: OSI\karn     ; Hostname: ; IP:    ; AppID: 552 ; AppName: Proc
essBook

I 10-Apr-13 19:16:16 Procbook                                              (4)
 >> Successfully connected to server   karne4300   as piadmins ! PIWorld

I 10-Apr-13 19:16:27 piaflink                                          (17002)
 >> Retrieved migration configuration information from PI Base Subsystem.
```

Listen to your system: PIPC log

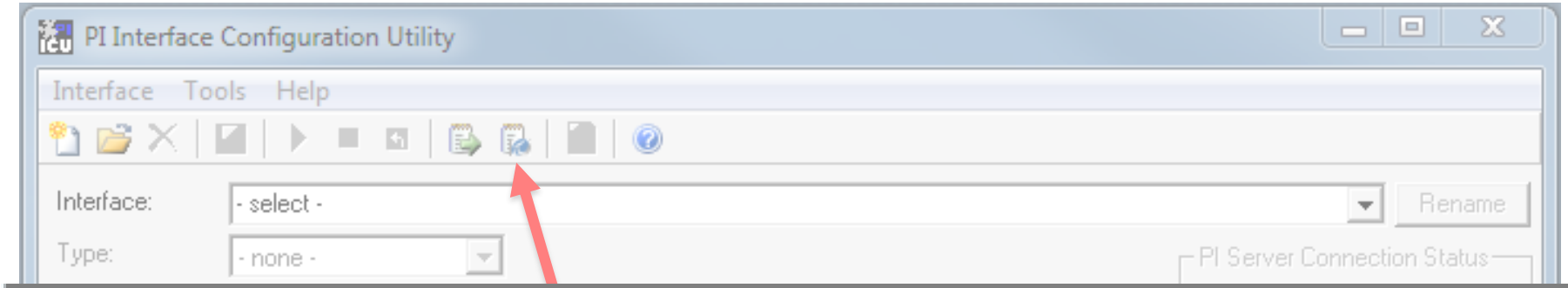


Listen to your system: PI Message log



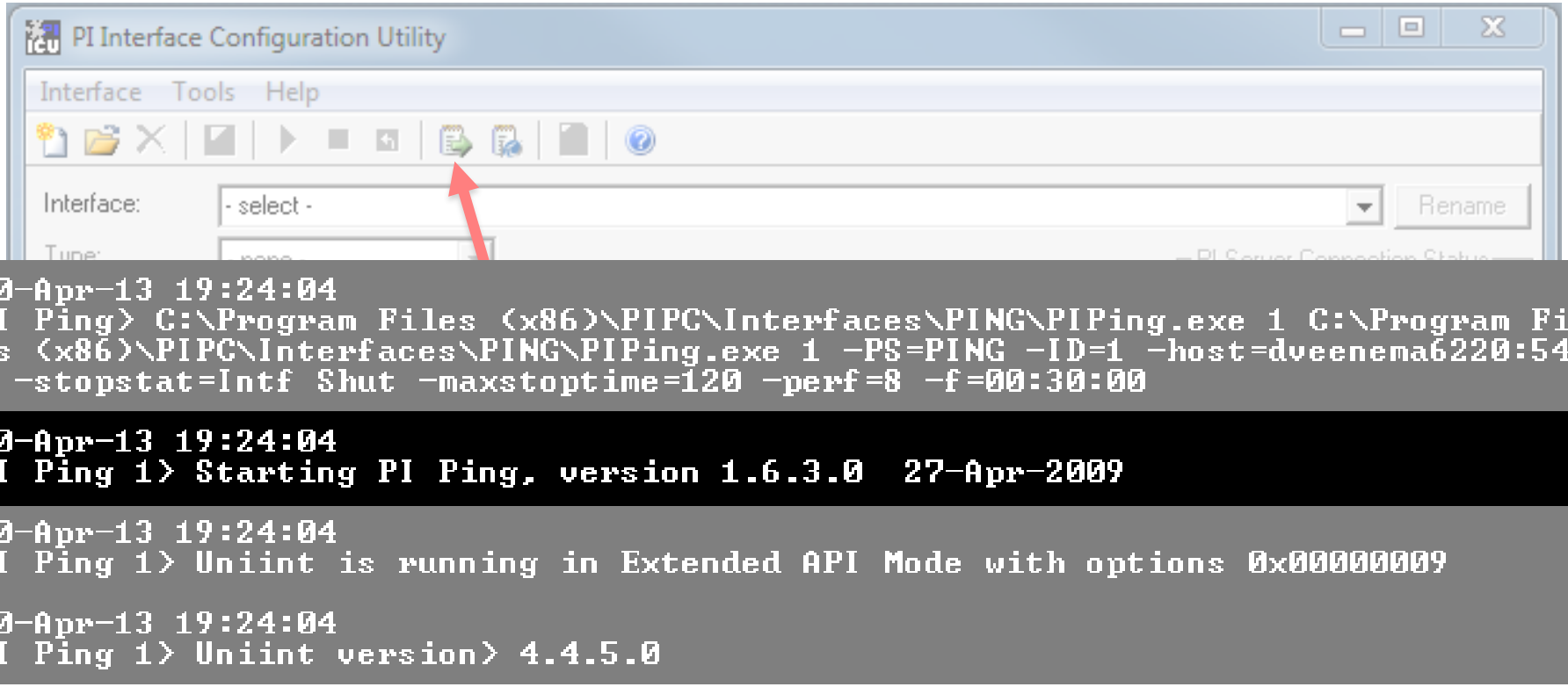

```
I 10-Apr-13 19:16:16 pinetmgr:Connection Information                    (7080)
 >> New Connection ID: 47 ; Process name: Procbook.exe(8772) ; User: piadmins !
PIWorld ; OS User: OSI\karn     ; Hostname: ; IP:    ; AppID: 552 ; AppName: Proc
essBook

I 10-Apr-13 19:16:16 Procbook                                              (4)
 >> Successfully connected to server DVEENEMA6220 as piadmins ! PIWorld

I 10-Apr-13 19:16:27 piaflink                                          (17002)
 >> Retrieved migration configuration information from PI Base Subsystem.
```

Listen to your system: PI Message log

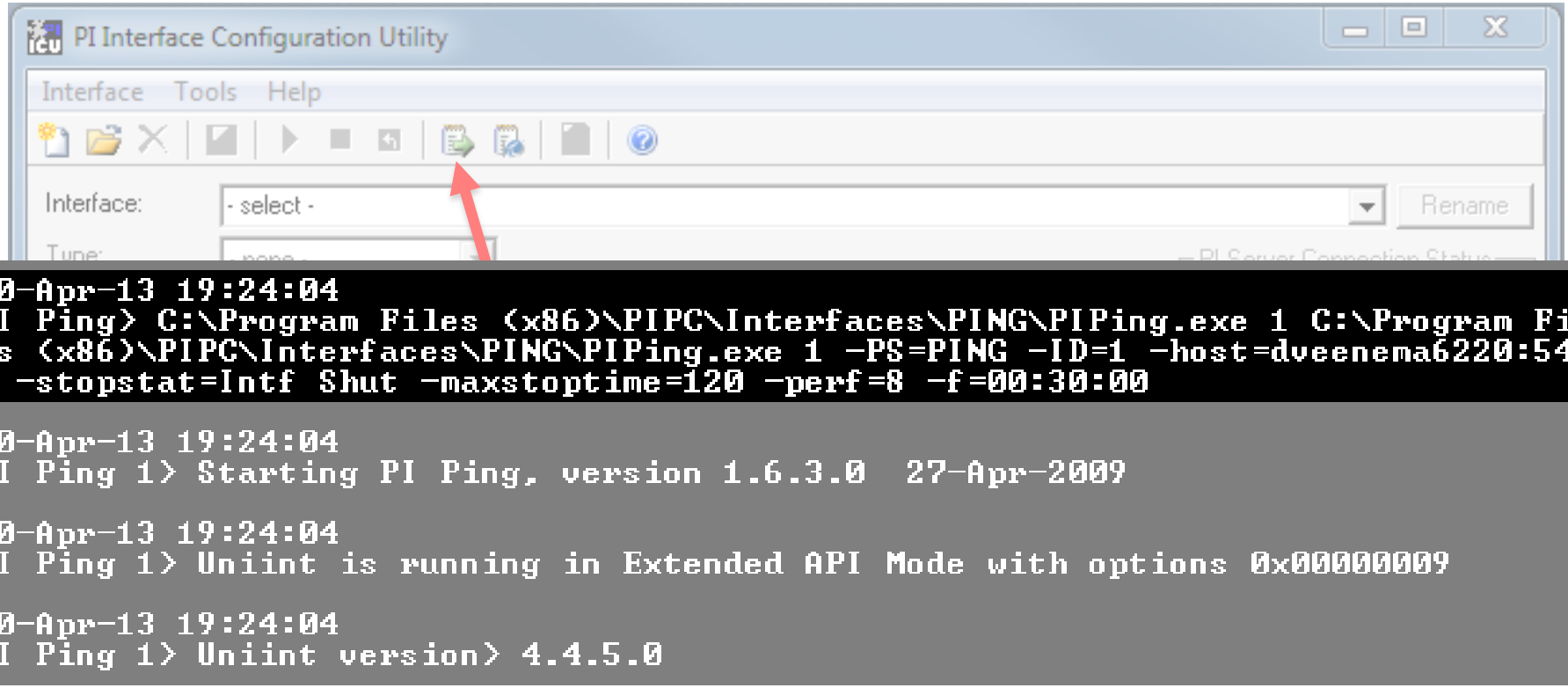



```
I 10-Apr-13 19:16:16 pinetmgr:Connection Information                    (7080)
 >> New Connection ID: 47 ; Process name: Procbook.exe(8772) ; User: piadmins !
PIWorld ; OS User: OSI\karn     ; Hostname: ; IP:    ; AppID: 552 ; AppName: Proc
essBook

I 10-Apr-13 19:16:16 Procbook                                             (4)
 >> Successfully connected to server karne4300     as piadmins ! PIWorld

I 10-Apr-13 19:16:27 piaflink                                          (17002)
 >> Retrieved migration configuration information from PI Base Subsystem.
```

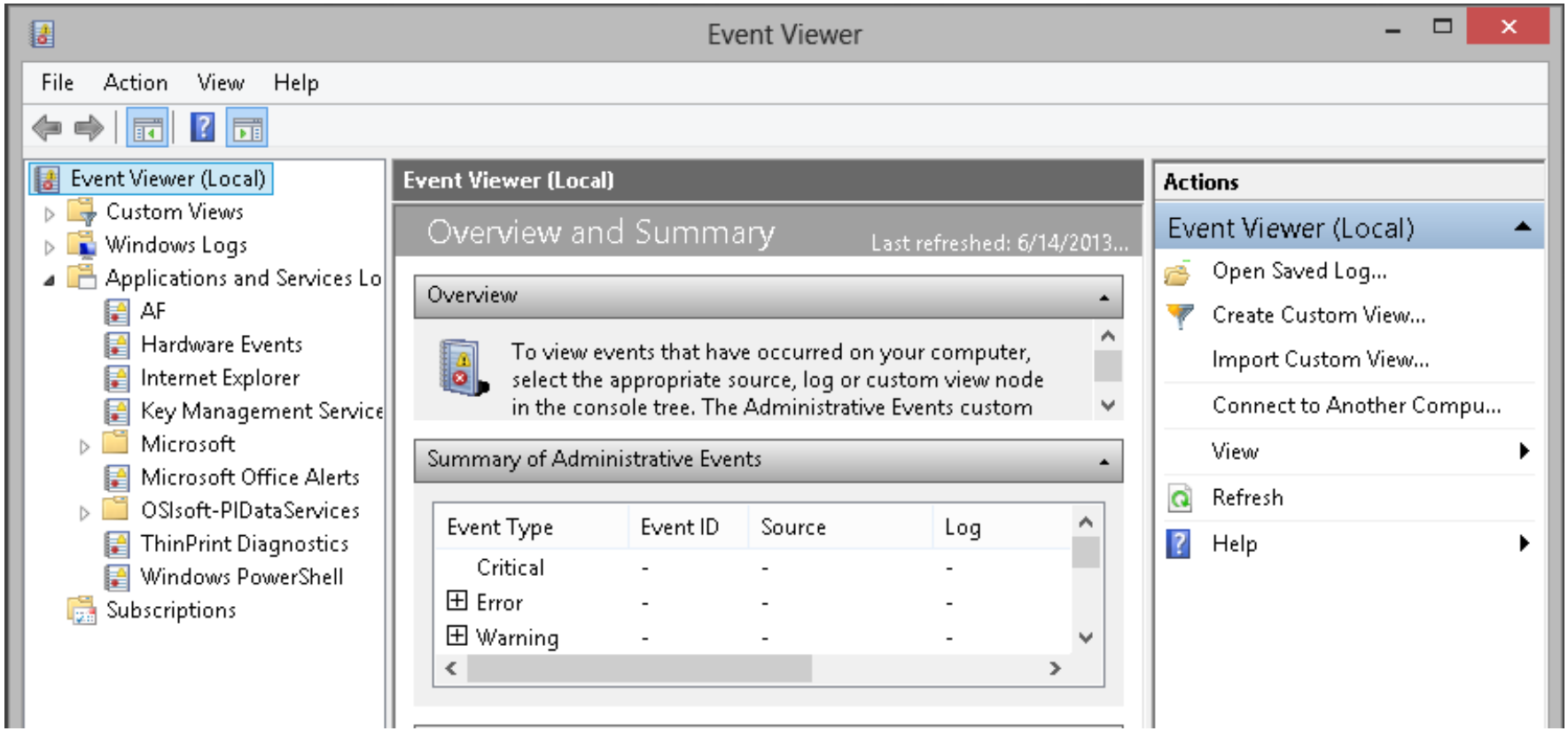
Listen to your system: PIPC log



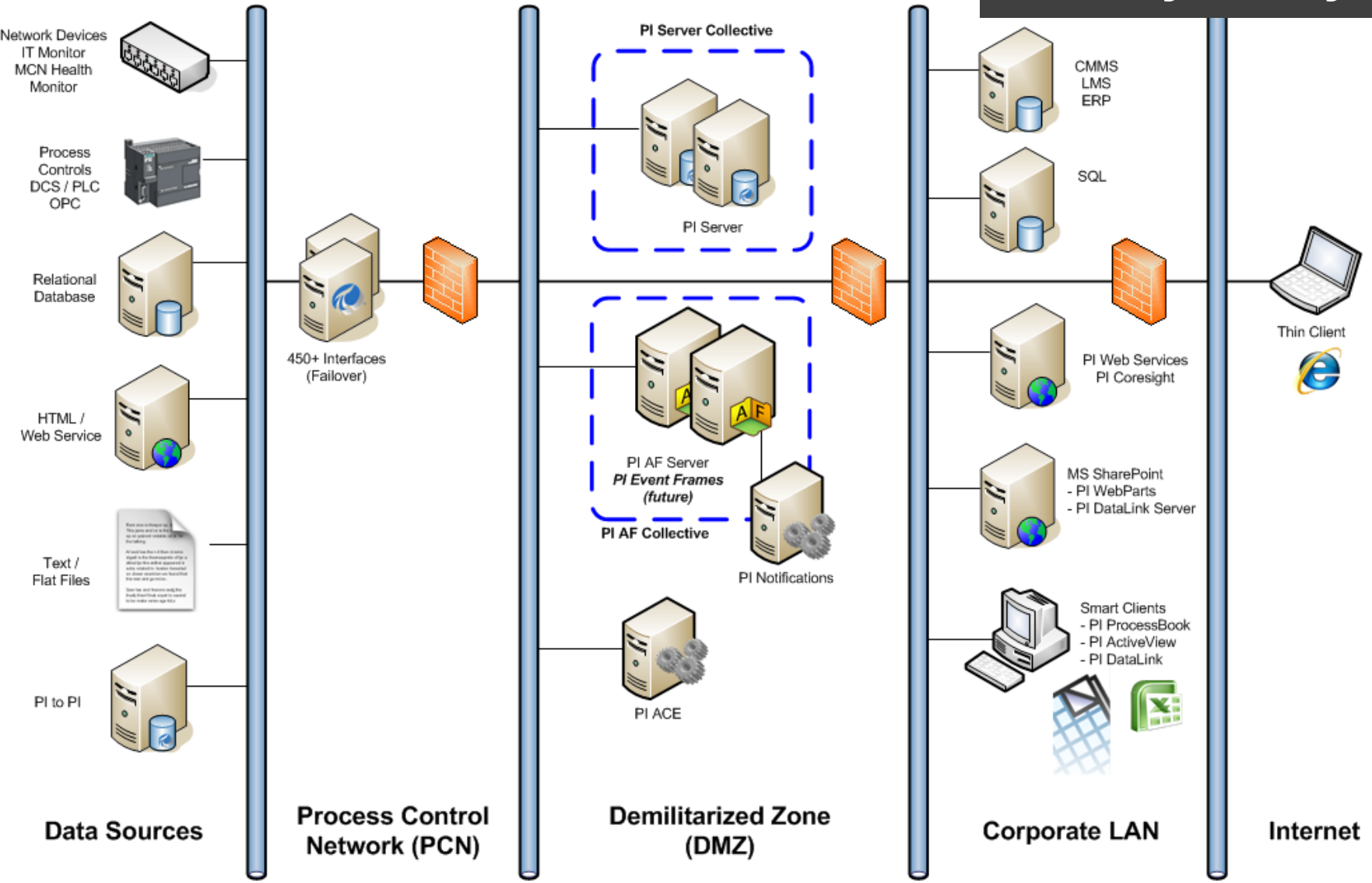
Listen to your system: PIPC log



Listen to your system: eventvwr



Know your system



Knowing Your System

```
1   HQ server HQPI1
2
3   PI to PI - on it's own machine
4
5   site server
6   name Mountain View MtnViewPI
7
8
9   data not matching
0
```

We start simple …

Knowing Your System

```
HQ server
  HQPI1
  PI server 2010
  3.4.385.59 64bit

PItoPI - get version.
  HQ-Int1 local to HQPI1

site server
  MtnViewPI
  3.4.385.77 32bit


data not matching
looks ok on the source PI server
```

…and we build

Knowing Your System

HQ-Int1 192.168.xxx.113	pitopi-PA1
	pitopi-PA1
	pitopi-WC1
	pitopi-MV1

Collective: HQ-PI
HQPI1 192.168.xxx.x01 primary 3.4.385.59 64bit
HQPI2 192.168.xxx.x02 secondary 3.4.385.59 64bit

10 ms	250 ms	50 ms
PaloAlto (PA)	WalnutCreek (WC)	MountainView (MV)
192.168.xxx.248	192.168.xxx.xxx	192.168.xxx.xxx
PaloAltoPI	name?	MtnVwPI
3.4.385.77 32bit	3.4.385.77 32bit	3.4.385.77 32bit
opcint1	opcint1	opcint1
opcint2	opcint2	--
rdbms1	rdbms1	rdbms1

…and build

Knowing Your System

HQ-Int1 192.168.xxx.113	pitopi-PA1
	pitopi-PA1
	pitopi-WC1
	pitopi-MV1

Collective: HQ-PI
HQPI1 192.168.xxx.x01 primary 3.4.385.59 64bit
HQPI2 192.168.xxx.x02 secondary 3.4.385.59 64bit

10 ms	250 ms	50 ms
PaloAlto (PA)	WalnutCreek (WC)	MountainView (MV)
192.168.xxx.248	192.168.xxx.xxx	192.168.xxx.xxx
PaloAltoPI	name?	MtnVwPI
3.4.385.77 32bit	3.4.385.77 32bit	3.4.385.77 32bit
opcint1	opcint1	opcint1
opcint2	opcint2	--
rdbms1	rdbms1	rdbms1

+12?

…and build

Knowing Your System

HQ-Int1 192.168.xxx.113	pitopi-PA1
	pitopi-PA1
	pitopi-WC1
	pitopi-MV1

36 instances

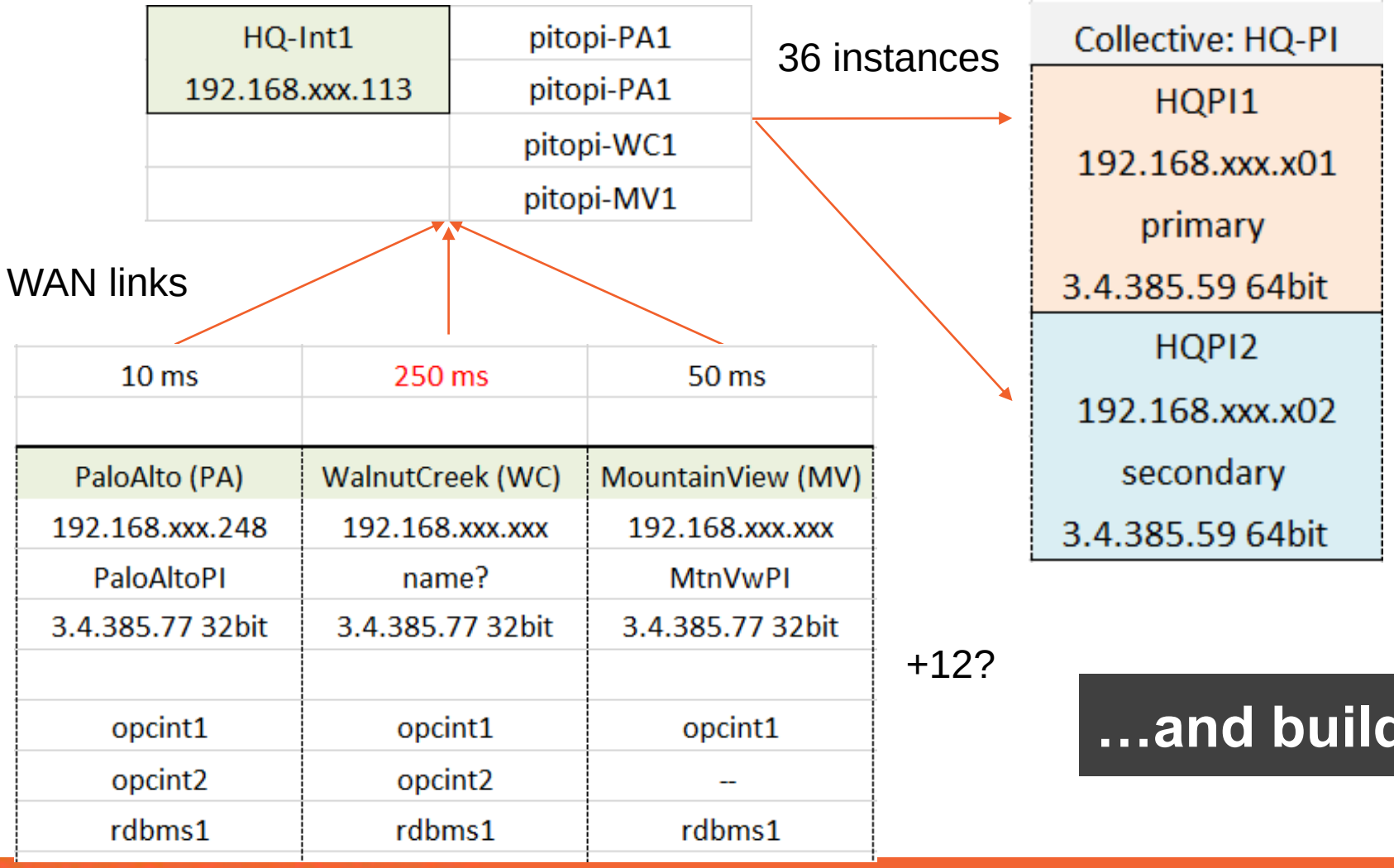
Collective: HQ-PI
HQPI1 192.168.xxx.x01 primary 3.4.385.59 64bit
HQPI2 192.168.xxx.x02 secondary 3.4.385.59 64bit

10 ms	250 ms	50 ms
PaloAlto (PA)	WalnutCreek (WC)	MountainView (MV)
192.168.xxx.248	192.168.xxx.xxx	192.168.xxx.xxx
PaloAltoPI	name?	MtnVwPI
3.4.385.77 32bit	3.4.385.77 32bit	3.4.385.77 32bit
opcint1	opcint1	opcint1
opcint2	opcint2	--
rdbms1	rdbms1	rdbms1

+12?

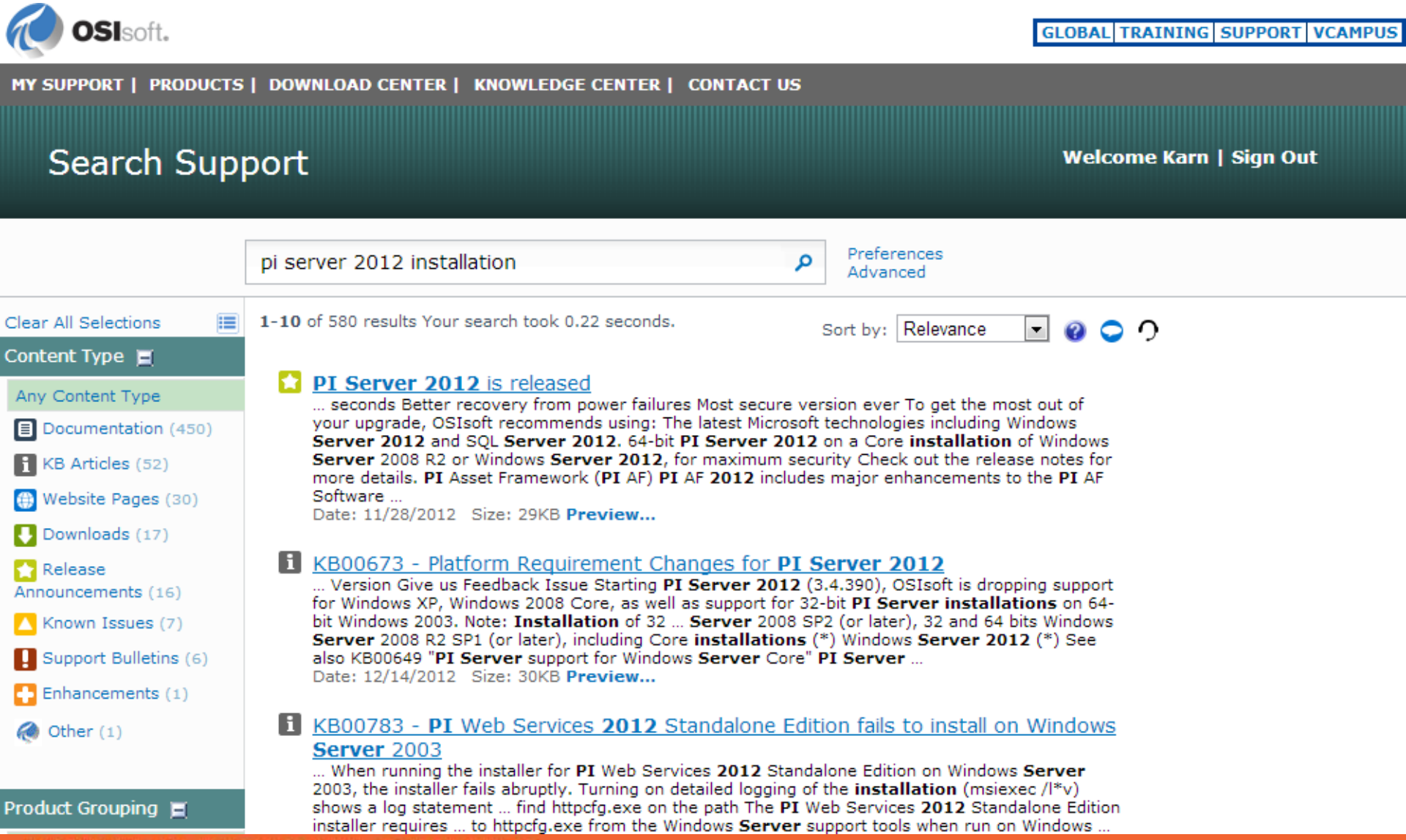
…and build

Knowing Your System

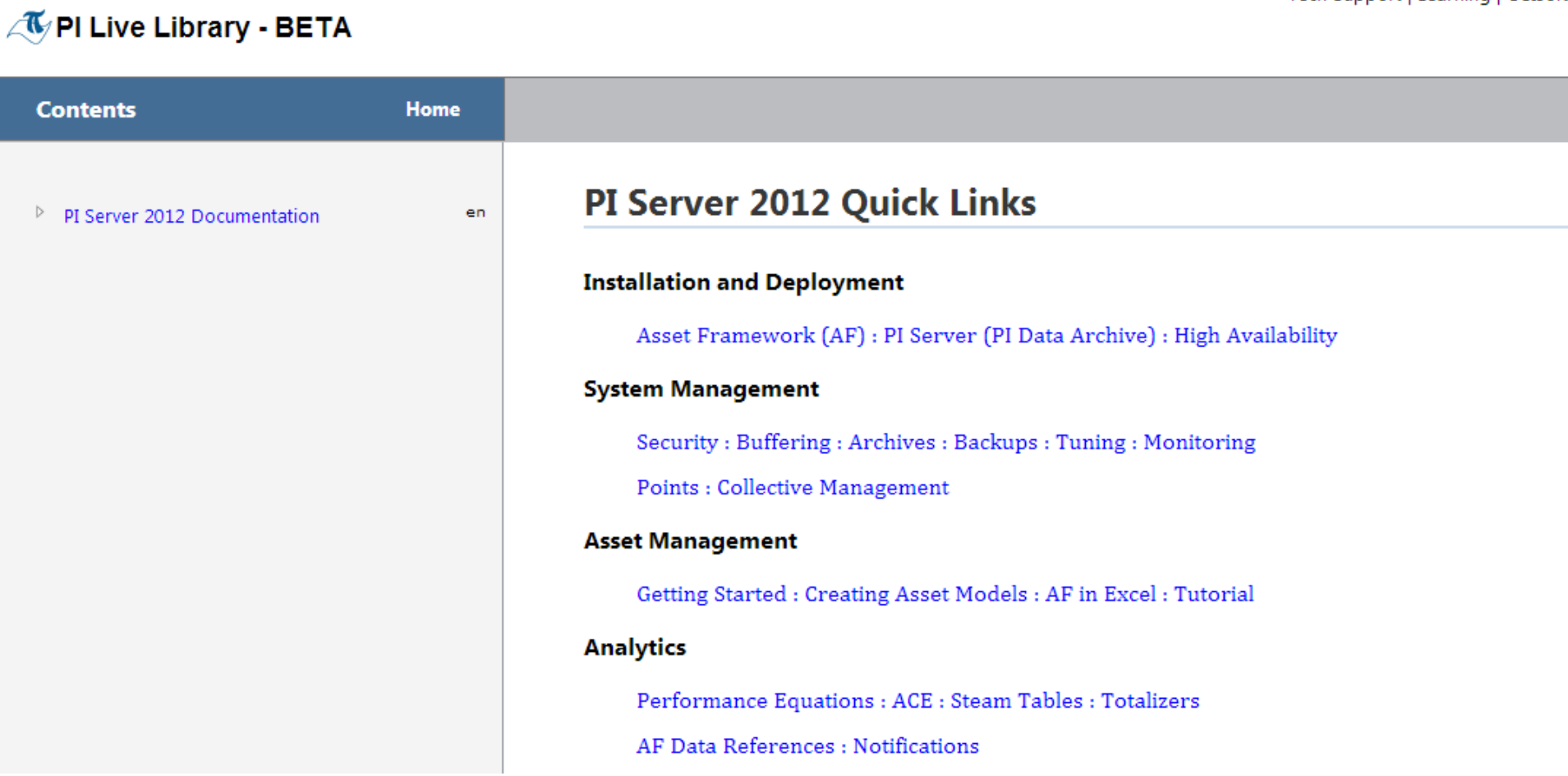


Available Resources Online

Available Resources

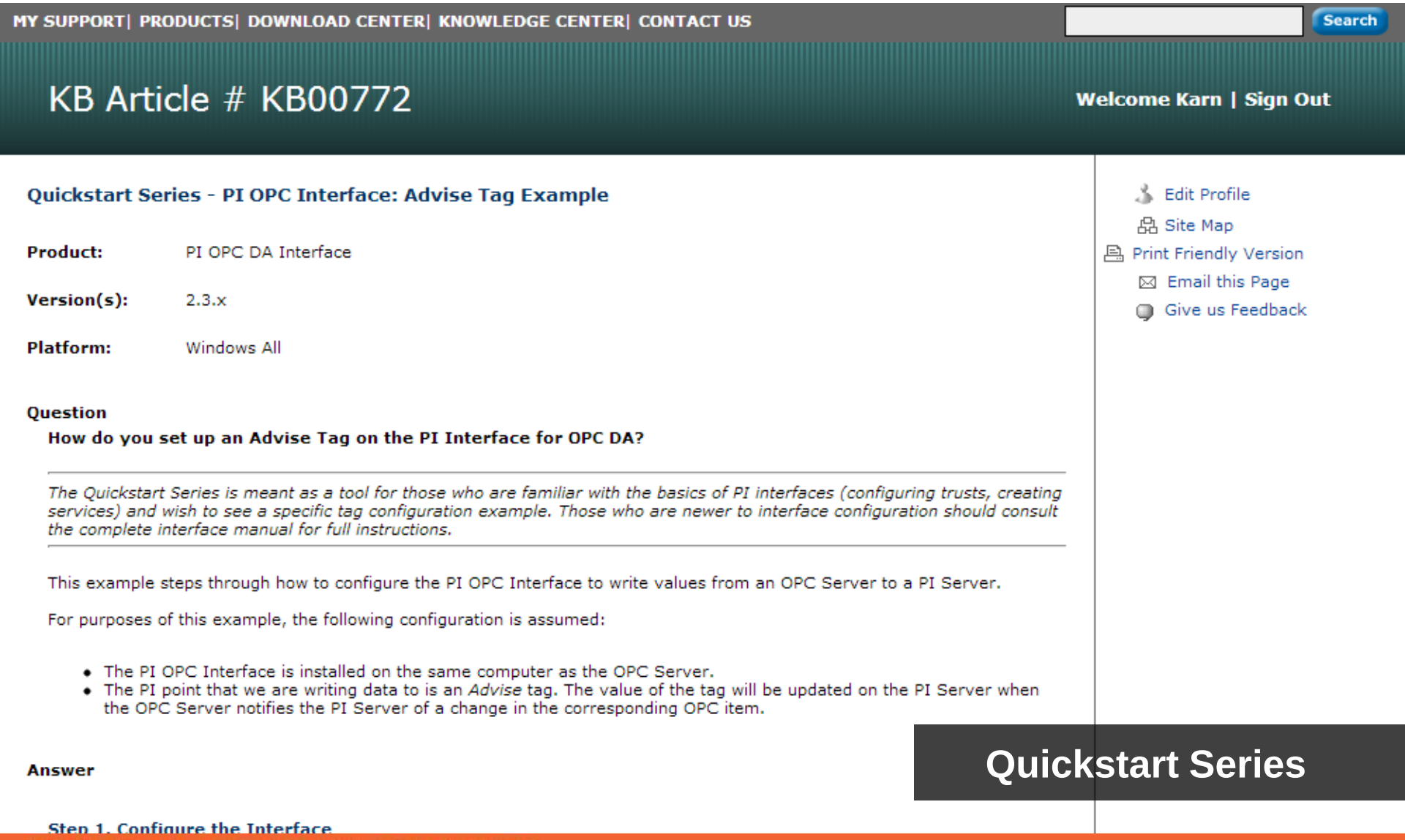


Available Resources



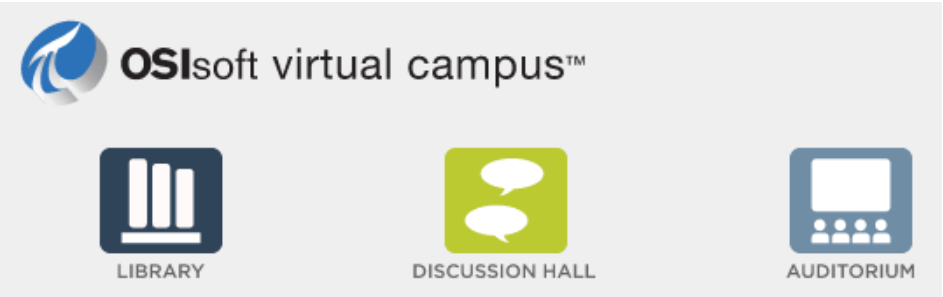
Livelibrary.osisoft.com

Available Resources



Quickstart Series

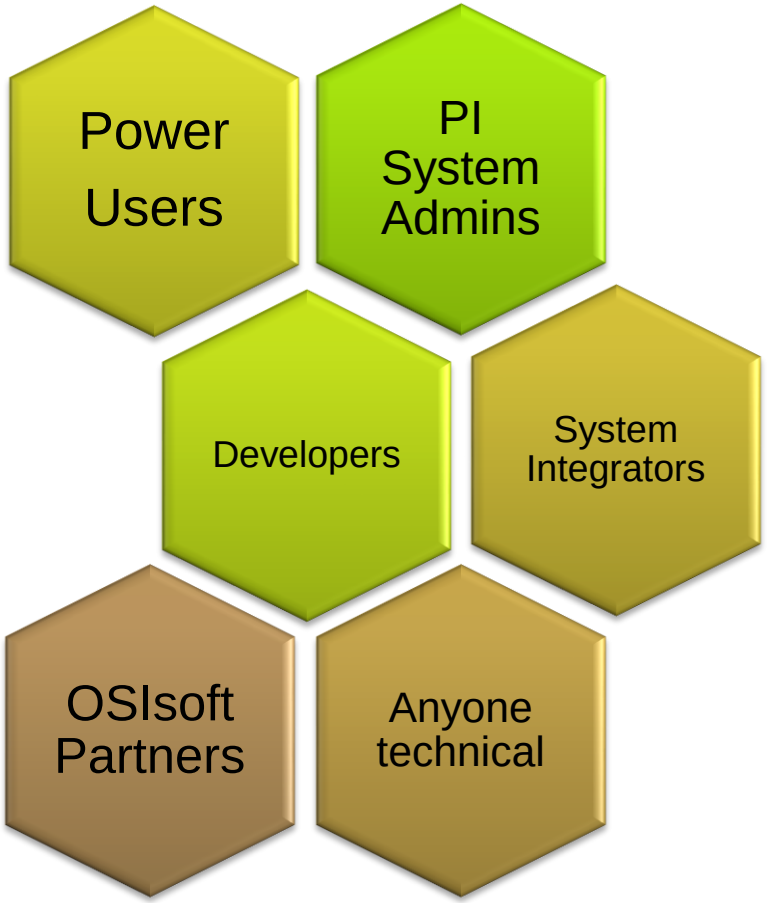
Available Resources



community.osisoft.com

vcampus.osisoft.com

Get hands on knowledge of how to use and get value from the PI System



OSIsoft. DECEMBER 3 - 6, GRAND HYATT SAN FRANCISCO

vCampus Live! 2013

WHERE PI GEEKS MEET

SAVE THE DATE

Tony Yan Jian

tyan@osisoft.com

Customer Support Engineer

OSIsoft Asia Pte. Ltd.

Karn Udomsangpetch

karn@osisoft.com

Customer Support Engineer

OSIsoft Asia Pte. Ltd.

THANK YOU