

## PI System and NERC CIP Security PART II



Ann Moore - Business Development, OSIsoft

Bryan Owen - Cyber Security Manager, OSIsoft

December 1<sup>st</sup>, 2010

- 2011 PI T&D Users Group Meeting:  
Doubletree Hotel Philadelphia, Sept. 21-23, 2011
- T&D Extranet Users Group Site:

<http://extranet.osisoft.com/sites/SIG/TD/default.aspx>

# Trivia Question

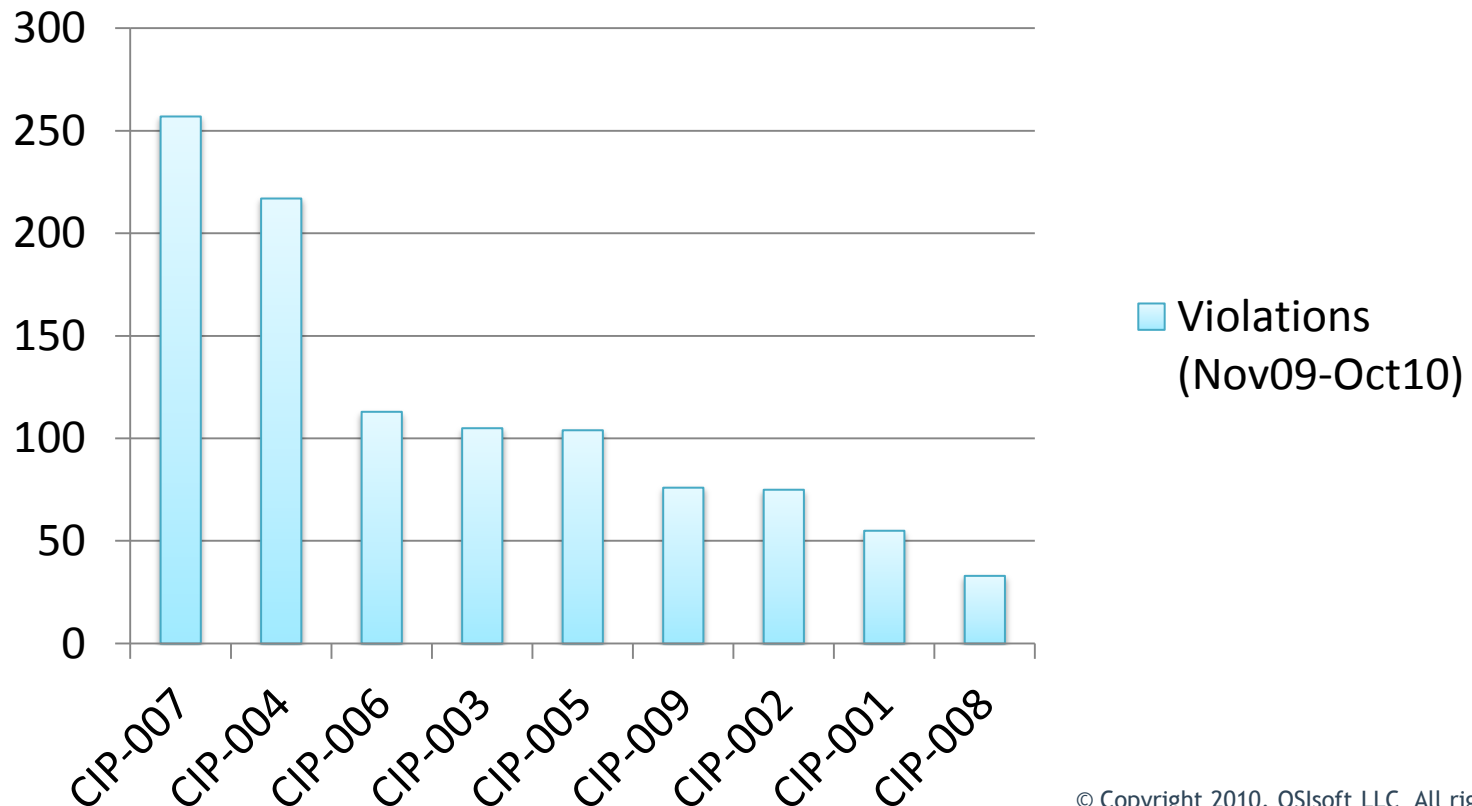


When was the latest Microsoft security bulletin affecting SQL Server 2008:

- a) Sep 29, 2010
- b) Oct 12, 2009
- c) Feb 10, 2009
- d) July 8, 2008
- e) None of the above

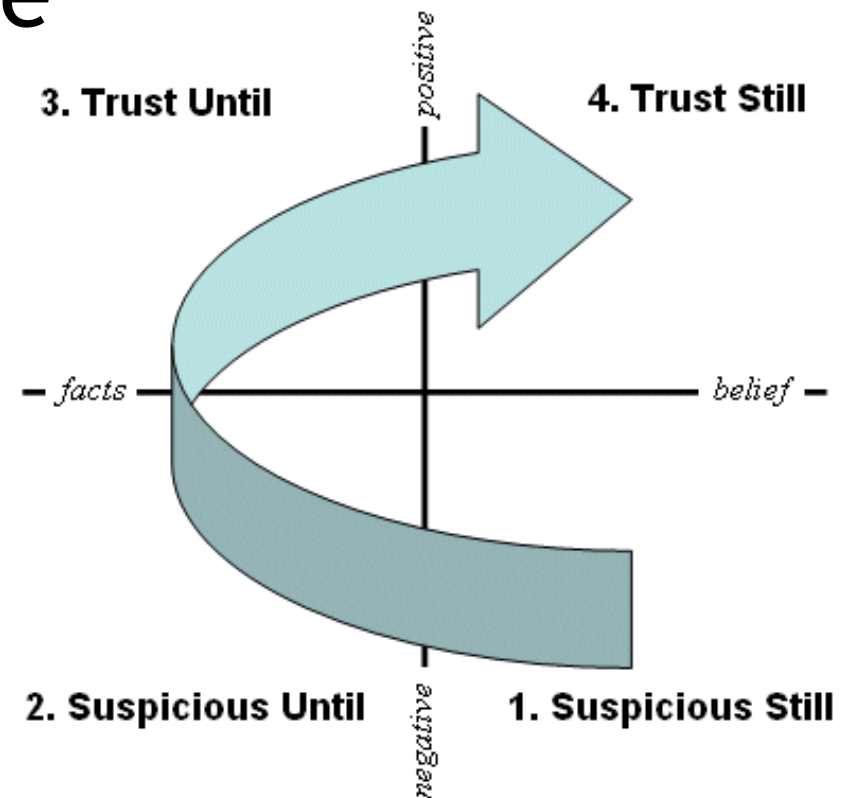
- Intro and Recap
  - Updates to Part I (May 7<sup>th</sup>, 2009)
  - PI 2010 SQL Server
- CIP-007
  - PI System Touch Points
- Questions and Answers

- CIP standards are a good start but...
  - Many unintended consequences
  - Change is proving to be difficult



# High Level Approach

- Provide Trusted Infrastructure
- Enable Platform Defenses
- Grow Knowledge Base



- OSIsoft personnel surety program
  - Background checks
  - Role specific training
  - HR integrated workflow
  - Signed certificate
  - Audit support



# Windows Patch Compatibility

- Timely assessment based on automation

Operating System	Version Number
Windows 7	6.1
Windows Server 2008 R2	6.1
Windows Server 2008	6.0
Windows Vista	6.0
Windows Server 2003 R2	5.2
<b>Windows Server 2003</b>	<b>5.2</b>
Windows XP 64-Bit Edition	5.2
Windows XP	5.1
Windows 2000	5.0



New for 2011!



# Windows Server Core

- PI Server is Microsoft certified on core
- Reduces attack surface and patching

```
C:\Windows\system32\cmd.exe - sconfig

=====
Server Configuration
=====

1) Domain/Workgroup:          Workgroup:  OSISDL
2) Computer Name:            R2CORE1
3) Add Local Administrator
4) Configure Remote Management

5) Windows Update Settings:   Manual
6) Download and Install Updates
7) Remote Desktop:           Enabled <all clients>

8) Network Settings
9) Date and Time

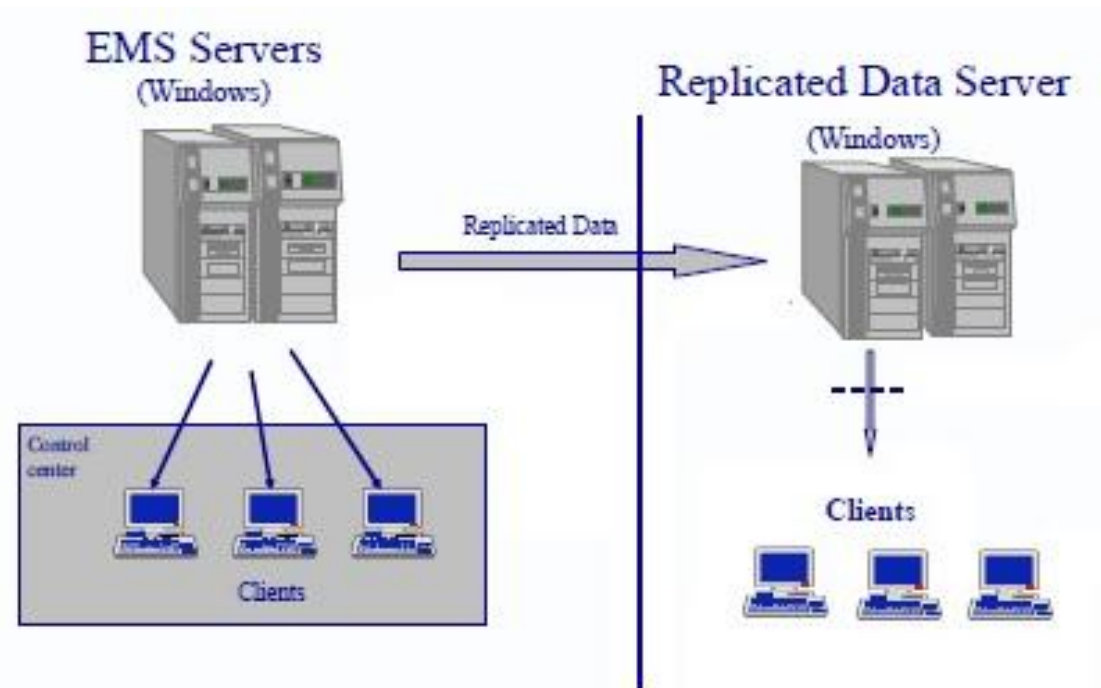
10) Log Off User
11) Restart Server
12) Shut Down Server
13) Exit to Command Line

Enter number to select an option: _
```

MS Bulletins	Server Core	Other Role
Jan-2010		2
Feb-2010	5	8
Mar-2010		3
Apr-2010	4	7
May-2010		2
Jun-2010	4	6
Jul-2010		4
Aug-2010	9	6
Sep-2010	2	8
Oct-2010	2	14
Nov-2010		3
Total	26	63



- OSIsoft Technical Support
  - Bomgar jump technology
- Replicated data server

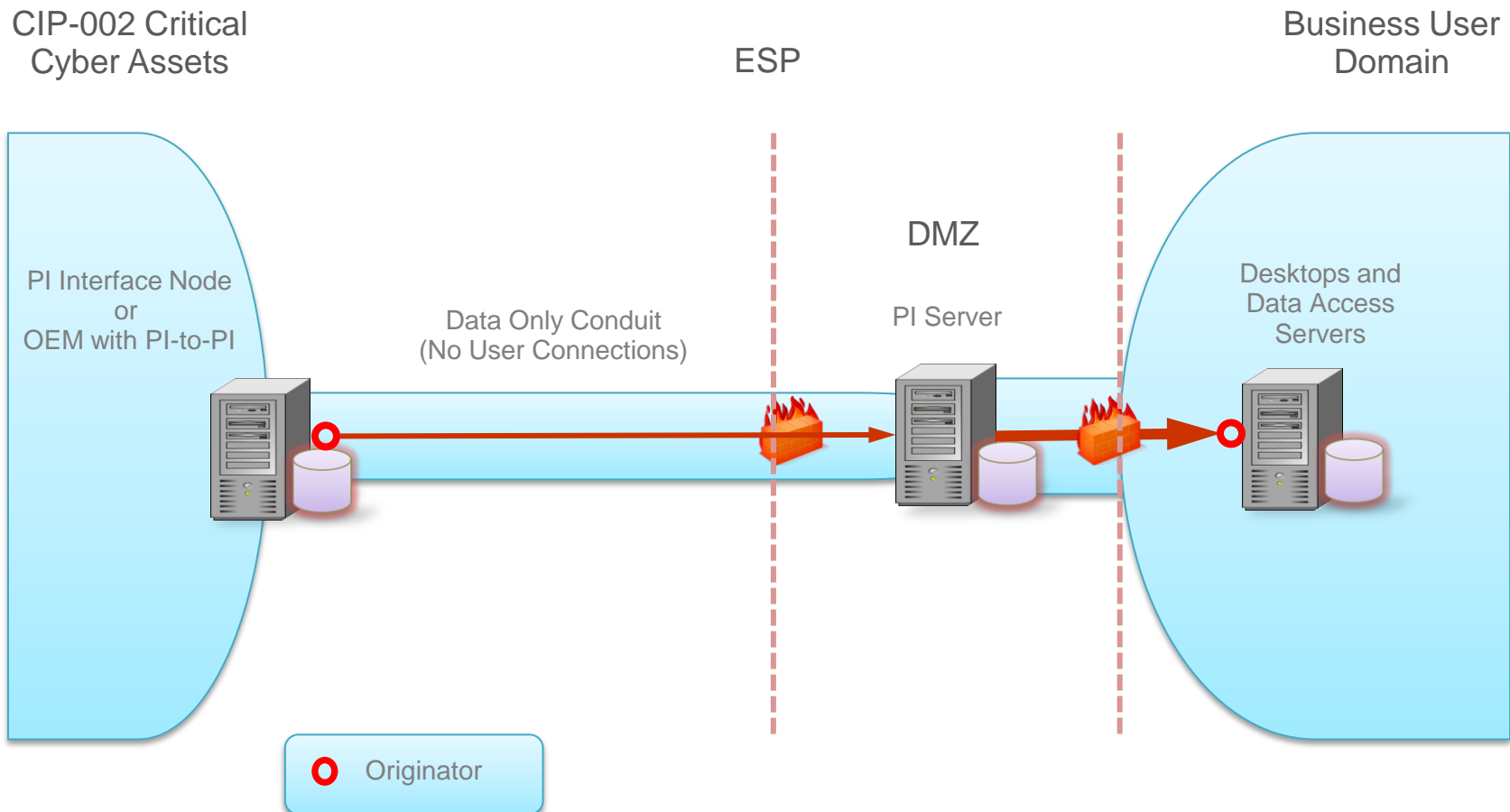


Source:

NERC Case Study 2

# Part I Deployment Patterns

- PI and NERC CIP Essentials (May 7th, 2009)  
[http://www.osisoft.com/resources/webinars/Webinars\\_On\\_Demand.aspx](http://www.osisoft.com/resources/webinars/Webinars_On_Demand.aspx)



# Traffic Update - WIS & PI 2010



Role	AD traffic to DC*	AF traffic to AF Server	PINET traffic To PI Server	MSSQL traffic to SQL Server
PI Client	✓		✓	
AF Client	✓	✓		
DMZ Firewall				
PI Server	✓	✓ (PI 2010)	✓ (PI HA)	
AF Server	✓	✓ (AF HA)		✓
SQL Server	✓			
ESP Firewall				
PI interface node			✓	
AMI interface node		✓	✓	

**\*KB00354: Windows Security Requirements for PI Server 3.4.380.36 and later**

## PI Server API Translator Vulnerability

- patch released

2008

2009

2010

## PI AF External Table Vulnerability

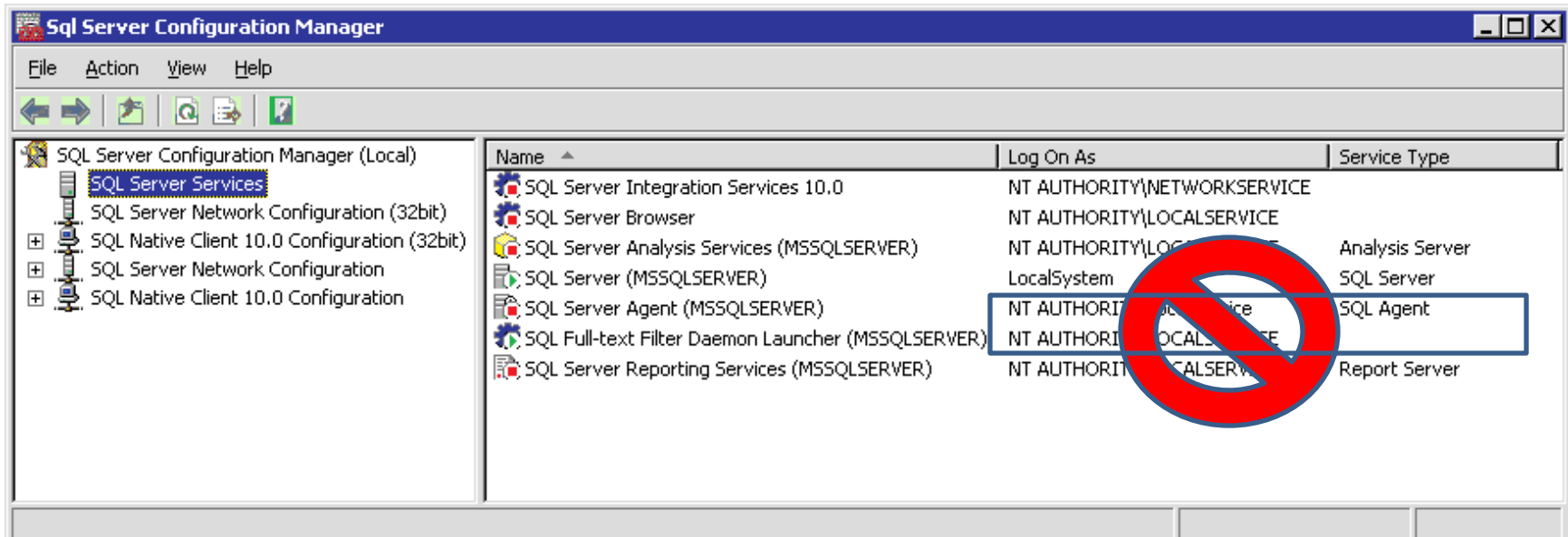
- SQL server sysadmin  
privilege check

## PI Server Authentication Weakness

- Windows Integrated  
Security released

# SQL Server Least Privilege

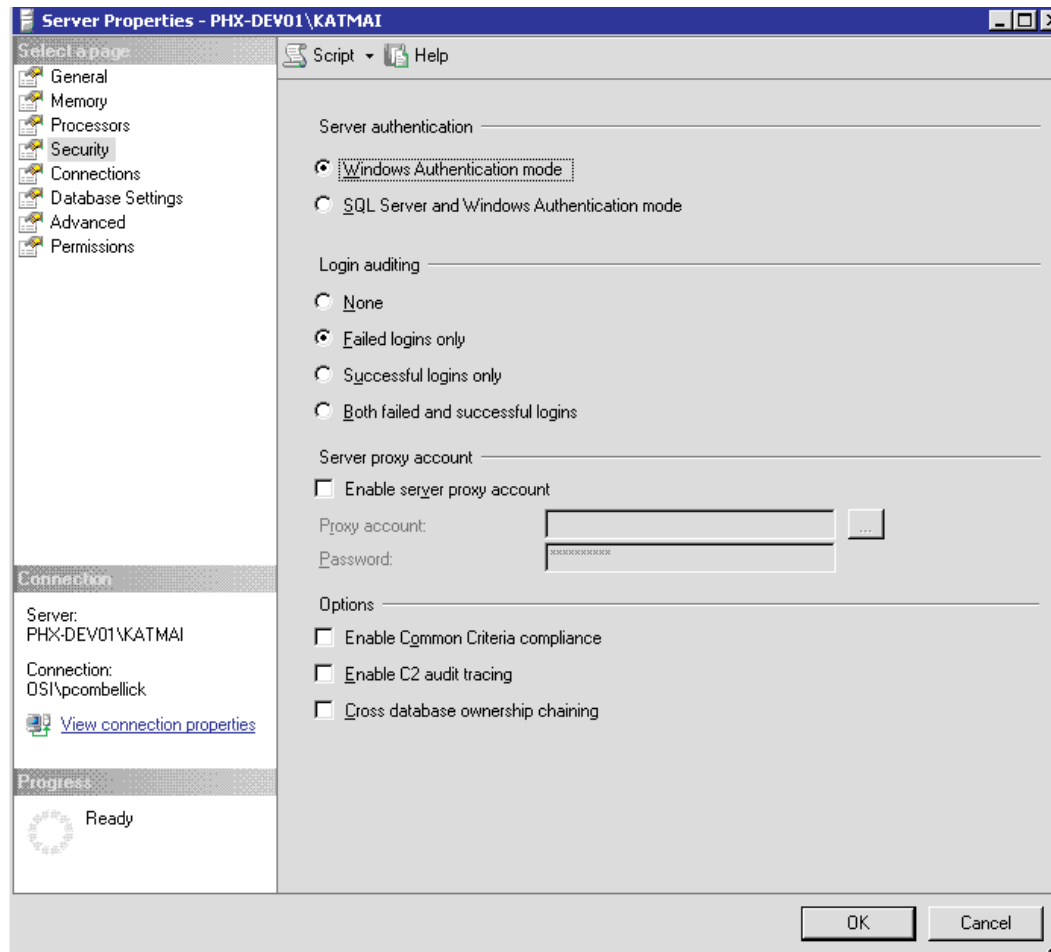
- NEVER run SQL Server as Local System or Administrator



# SQL Server Authentication Mode

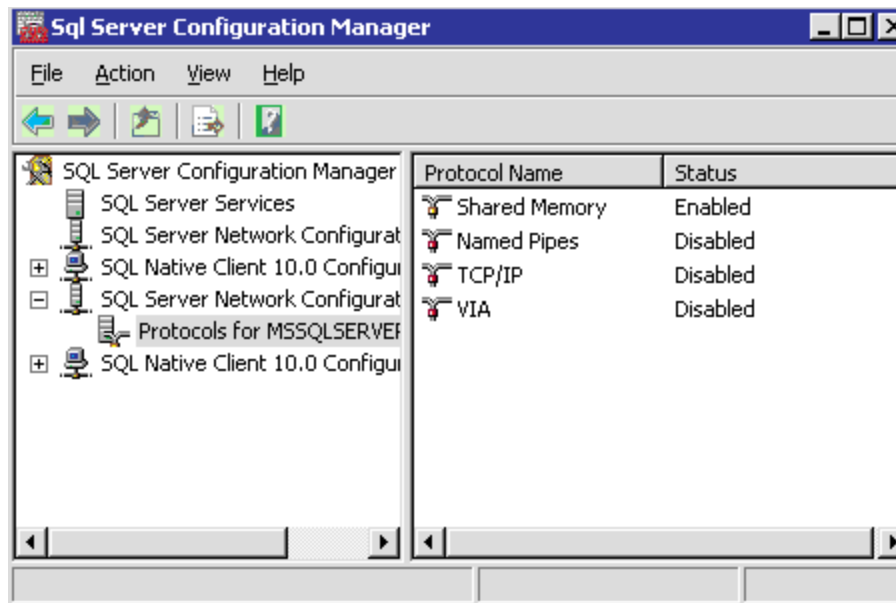


- Recommend using Windows authentication mode only

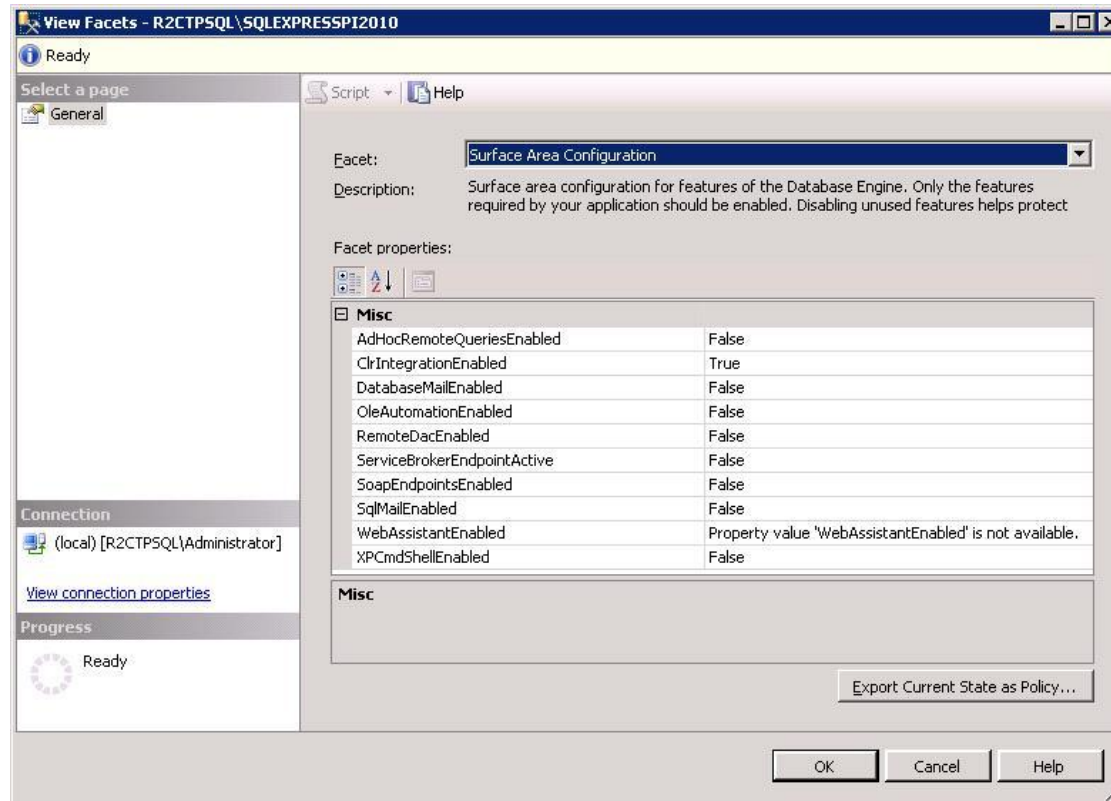


# SQL Server Network Protocols

- Disable network protocol listeners for remote clients (default for SQL Express)



- Disable extended spprocs (xp\_\*), OLE Automation, SQL Mail





# AFDiag - Linked Table: User Impersonation



- Disable non-impersonated access to external tables

```
Command Prompt

C:\pisoft\PIHOME\AF>afdiag /DTImp-

SQL Connection String: 'Persist Security Info=False;Integrated
Security=SSPI;server=.\KATMAI;database=PIFD;Application Name=AF Application
Server;'
Updating 'ExternalDataTablesAllowNonImpersonatedUsers' to 'False'.

System Name = PIFD
SystemID = f2518f40-a3ec-4aae-9c1f-212527c12ede
Default AFDatabase =
Audit Trail = Disabled
Is SQL Express = False
Database Version = 2.2.2.3870
Database Schema Version = 2.3787
Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
Jul 9 2008 14:43:34
Copyright (c) 1988-2008 Microsoft Corporation
Developer Edition on Windows NT 5.2 (X86) (Build 3790: Service Pack 2)

Configuration Settings:
  EnableExternalDataTables = True
  ExternalDataTablesAllowNonImpersonatedUsers = False
  EnableExternalDataTablesWithAF20 = False
  EnableEventFrames = False

Configuration change will be delayed until the AF Server reads its updated
configuration (default is every 5 minutes) or is restarted.

C:\pisoft\PIHOME\AF>_
```

- AF DB install requires SysAdmin privilege
  - Can install DB manually
- Run as account with minimum privilege
  - Don't run as Local System or Administrator
- Connect to SQL with minimum privilege
  - Don't connect with SysAdmin privilege

**If the privilege level on the sql connection is unnecessarily high...  
AF Server will write a warning to the Windows AF Event log!**

- Ports and Services
- Account Management
- Security Status Monitoring
- Vulnerability Assessment

# Securing Network Traffic: WCF




- PI System traffic protected by default
  - Windows integrated authentication messages
  - Middle tier server applications

Service Endpoint	Platform Library	Port (TCP)	Protected
MS SQL Server	WinSock	1433	
Managed PI Agent	WCF	5449	✓
PI Server	WinSock	5450	
ACE Web Service	ASP.NET	5456	
AF Server	WCF	5457	✓
PI Notifications	WCF	5458	✓
AF Server (Streaming)	WCF	5459	✓
PI SQL Data Access Server	WCF	5461	✓

# Configuring Connection Security



Connection Security Rules						
Name	Endpoint 1	Endpoint 2	Authentication method	Endpoint 1 port	Endpoint 2 port	Protocol
 PINET-over-IPsec	Any	Any	Computer (Kerberos V5)	Any	5450	TCP

- IP Security is built-in to Windows since 2000
  - Added to Windows Advanced Firewall (Server 2008)
    - Add rule on each endpoint
    - Most manageable between domain members
  - Preparation
    - Verify hardware compatibility on bench
    - Consider “Request” mode rather than “Require”

- Register PI SCW Extension (xml)
  - PI Server Security Best Practices
- Set Roles and Optional Features
  - Disable Unused Services
- Apply Security Templates
  - Windows SSIF
  - US DoD (DISA STIG)
  - Corporate policy

**Security Configuration Wizard**

**Select Server Roles**

These server roles are used to enable services and open ports. A server can perform multiple roles.

View: Installed roles

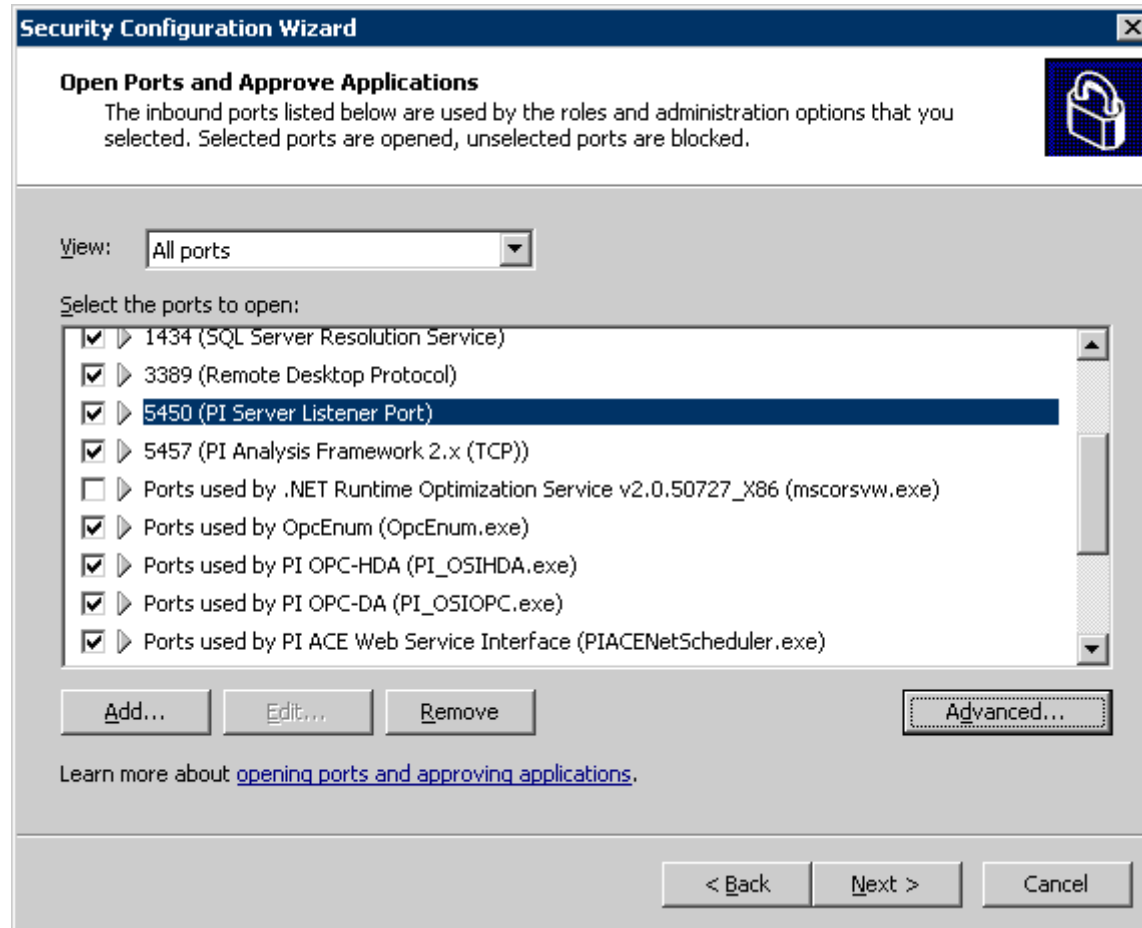
Select the server roles that the selected server performs:

- ☐ DNS server
- ☐ File server
- ☐ Internet Connection Sharing server
- ☒ **PI Enterprise Server Base Services**
  - Description:** Core services required for the PI archive
  - Required services:** PI Network Manager, PI Message Subsystem, PI License Manager, PI Update Manager, PI Base Subsystem, PI Snapshot Subsystem, PI Archive Subsystem, PI Backup Subsystem, PI SQL Subsystem, PI Shutdown Subsystem
  - Required roles:** PI-SDK
- ☒ **PI-SDK**
  - Description:** The SDK is required to enable PI system client or server role(s) on MS Windows platforms.
  - Required services:** PI Network Manager, PI Message Subsystem, PIPC Log Service

Learn more about [server roles](#).

< Back   Next >   Cancel

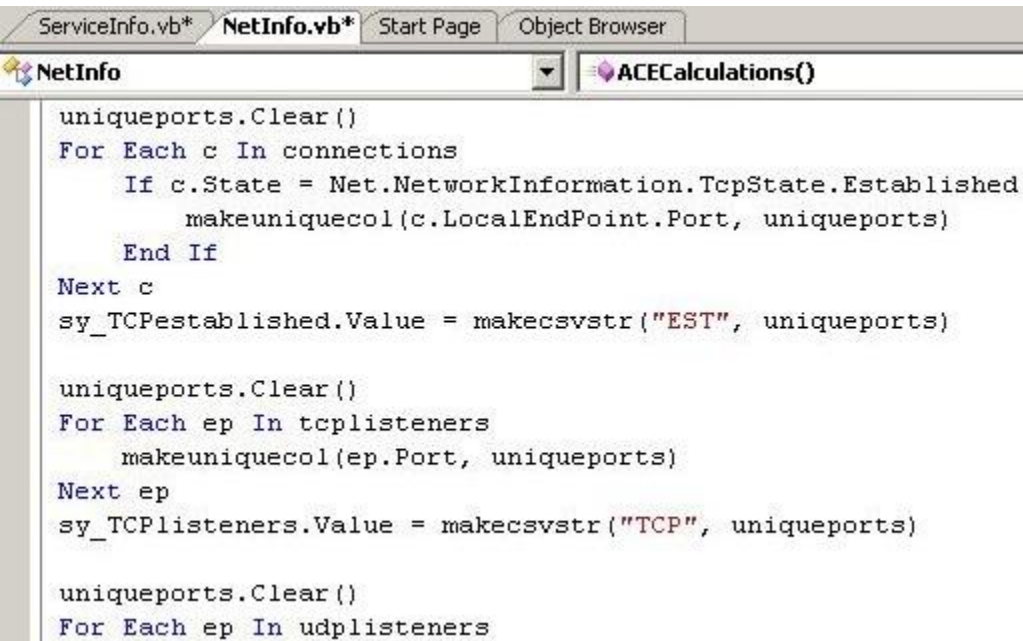
# Configure Open Ports





# Monitoring Ports and Services

- Ports and services exposed in .Net
  - Use PI Advanced Calculation Engine
  - Write to archive, trigger PI Notification

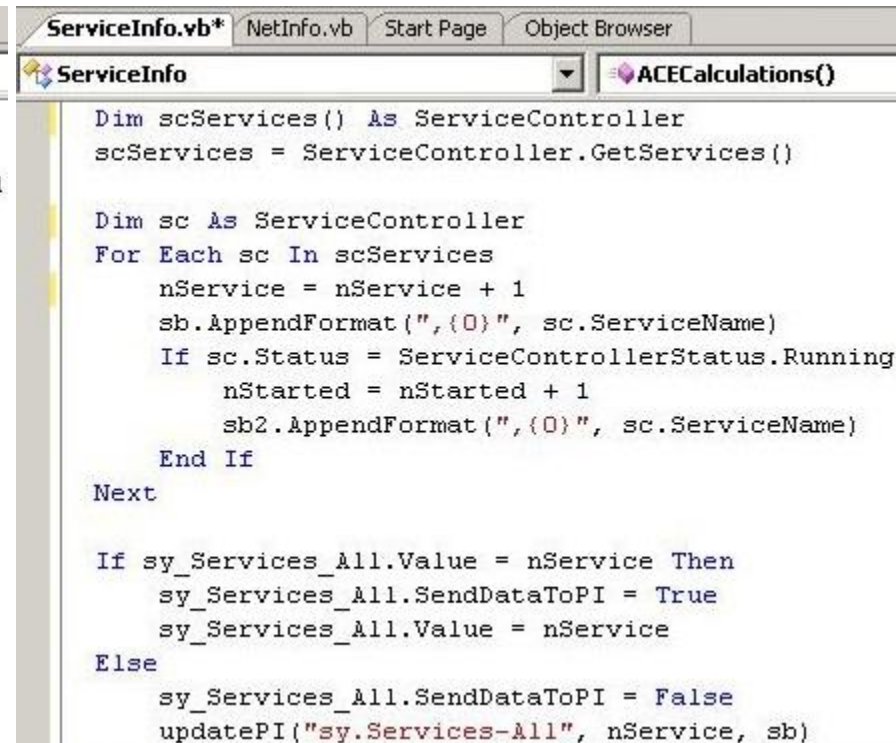


```
ServiceInfo.vb* NetInfo.vb* Start Page Object Browser
NetInfo
ACECalculations()

uniqueports.Clear()
For Each c In connections
    If c.State = Net.NetworkInformation.TcpState.Established
        makeuniquecol(c.LocalEndPoint.Port, uniqueports)
    End If
Next c
sy_TCPestablished.Value = makecsvstr("EST", uniqueports)

uniqueports.Clear()
For Each ep In tcplistenrs
    makeuniquecol(ep.Port, uniqueports)
Next ep
sy_TCPlistenrs.Value = makecsvstr("TCP", uniqueports)

uniqueports.Clear()
For Each ep In udplistenrs
```



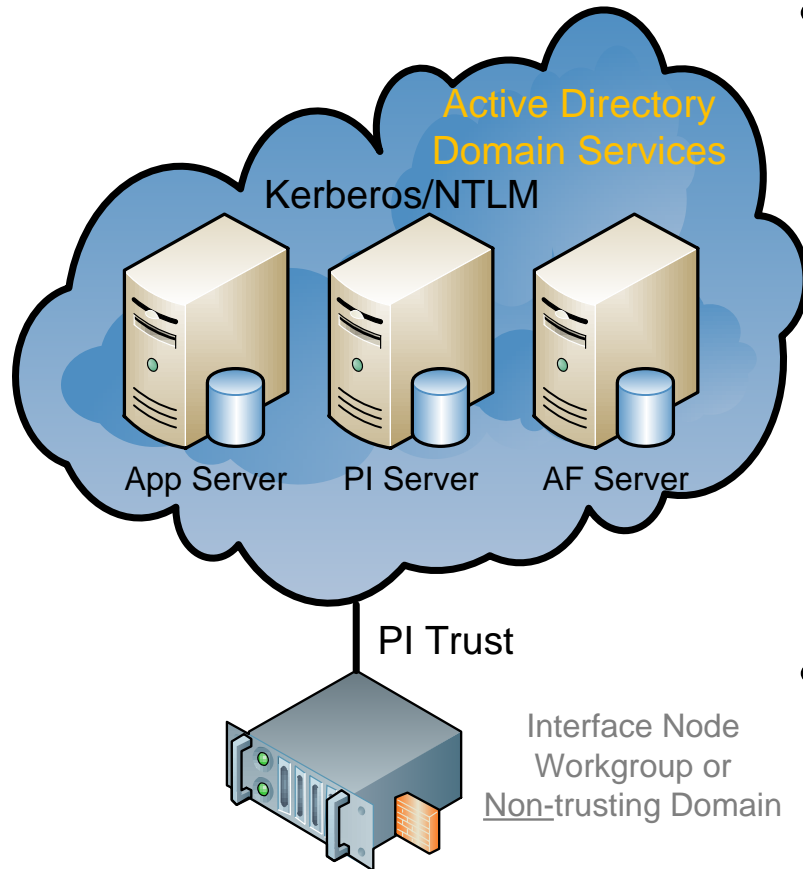
```
ServiceInfo.vb* NetInfo.vb Start Page Object Browser
ServiceInfo
ACECalculations()

Dim scServices() As ServiceController
scServices = ServiceController.GetServices()

Dim sc As ServiceController
For Each sc In scServices
    nService = nService + 1
    sb.AppendFormat("{0}", sc.ServiceName)
    If sc.Status = ServiceControllerStatus.Running
        nStarted = nStarted + 1
        sb2.AppendFormat("{0}", sc.ServiceName)
    End If
Next

If sy_Services_All.Value = nService Then
    sy_Services_All.SendDataToPI = True
    sy_Services_All.Value = nService
Else
    sy_Services_All.SendDataToPI = False
    updatePI("sy.Services-All", nService, sb)
```

- Windows Integrated Security
- “Need to know” Authorization
- Manage Shared Accounts



- Windows Integrated Security
  - Domain Membership (trust relationship with users)
  - Local accounts supported (eg. emergency access)
  - Set Password Policy
  - Set Audit Policy
- PI Authentication
  - Disable explicit login
  - PI trust still required (limit scope)

# Built-in “piadmin” Account



- Still needed for system recovery
- Instead use “piadmins” if full access permissions are required
- Better to create database identities with least required privilege

**PIADMIN = NO SECURITY**

# Authorization - Contributor Role

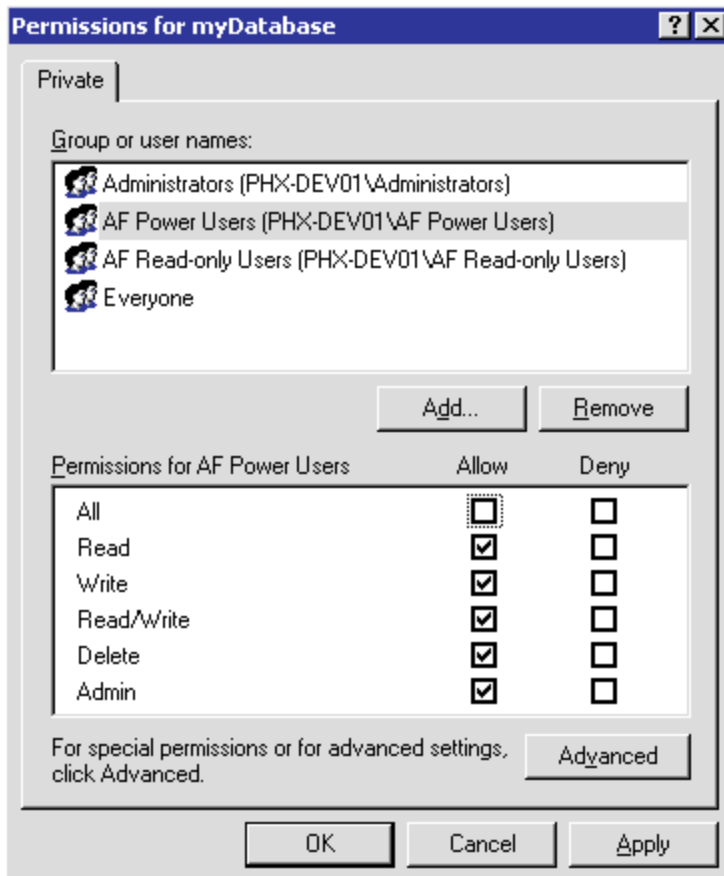


Database Security - PI System Management Tools (Administrator)		
File View Tools Help		
Table Name	Security	Description
PIBatch	piadmins: A(r,w)   PIContributor: A(r,w)   PIWorld: A(r)	Controls access to PIBatch objects in the Batch Database (BDB)
PIBATCHLEGACY	piadmins: A(r,w)   PIContributor: A(r,w)   PIWorld: A(r)	Controls access to unit configuration and batch data in the legacy Batch Database
PICampaign	piadmins: A(r,w)   PIContributor: A(r,w)   PIWorld: A(r)	Controls access to PICampaign objects in the Batch Database (BDB)
PIModules	piadmins: A(r,w)   PIContributor: A(r,w)   PIWorld: A(r)	Controls top-level access to Modules
PIPOINT	piadmins: A(r,w)   PIContributor: A(r,w)   PIWorld: A(r)	Controls top-level access to Points, Point Classes, and Attribute Sets
PITransferRecords	piadmins: A(r,w)   PIContributor: A(r,w)   PIWorld: A(r)	Controls access to PITransferRecord objects in the Batch Database
PIMSGSS	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A(w)	Controls access to the message log
PIDBSEC	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A(r)	Controls top-level access to this table
PIDS	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A(r)	Controls access to Digital States and Digital Sets
PIHeadingSets	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A(r)	Controls top-level access to Headings and Heading Sets
PIUSER	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A(r)	Controls access to Users, Groups, and Identities
PIAFLINK	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access for MDB-AF synchronization management
PIARCAADMIN	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access for archive management: creating, (un)registering, and deleting archives
PIARCDATA	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access to archive information other than tag data: archive lists, archive metadata, and archive statistics
PIAUDIT	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls read access to the audit log
PIBACKUP	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access for backup management
PIMAPPING	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access to Identity Mappings
PIReplication	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access to Servers, Collectives, and their management: standbys, replication, and monitoring
PITRUST	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access to Trusts
PITUNING	piadmin: A(r,w)   piadmins: A(r,w)   PIWorld: A()	Controls access to Timeout parameters and the Firewall

OSISDL\administrator | piadmins, PIContributor, PIWorld

# AF Least Privilege

- Create domain groups to grant specific, least privileges
- Remove access for “Everyone”



Permissions for myDatabase

Private

Group or user names:

- Administrators (PHX-DEV01\Administrators)
- AF Power Users (PHX-DEV01\AF Power Users)
- AF Read-only Users (PHX-DEV01\AF Read-only Users)
- Everyone

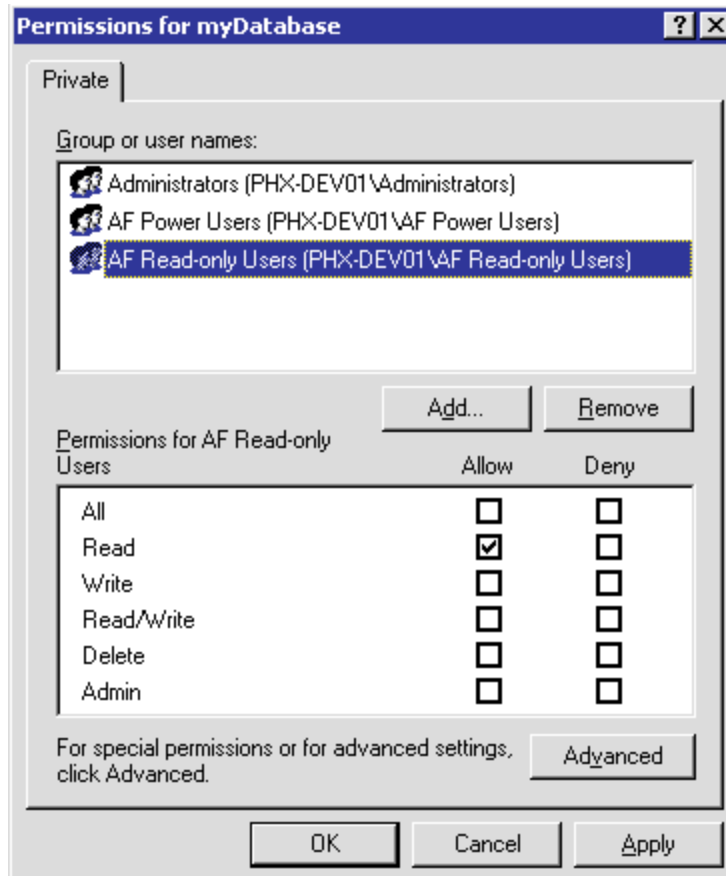
Add... Remove

Permissions for AF Power Users	Allow	Deny
All	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read/Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Admin	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or for advanced settings, click Advanced.

Advanced

OK Cancel Apply



Permissions for myDatabase

Private

Group or user names:

- Administrators (PHX-DEV01\Administrators)
- AF Power Users (PHX-DEV01\AF Power Users)
- AF Read-only Users (PHX-DEV01\AF Read-only Users)

Add... Remove

Permissions for AF Read-only Users	Allow	Deny
All	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Read/Write	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="checkbox"/>	<input type="checkbox"/>
Admin	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or for advanced settings, click Advanced.

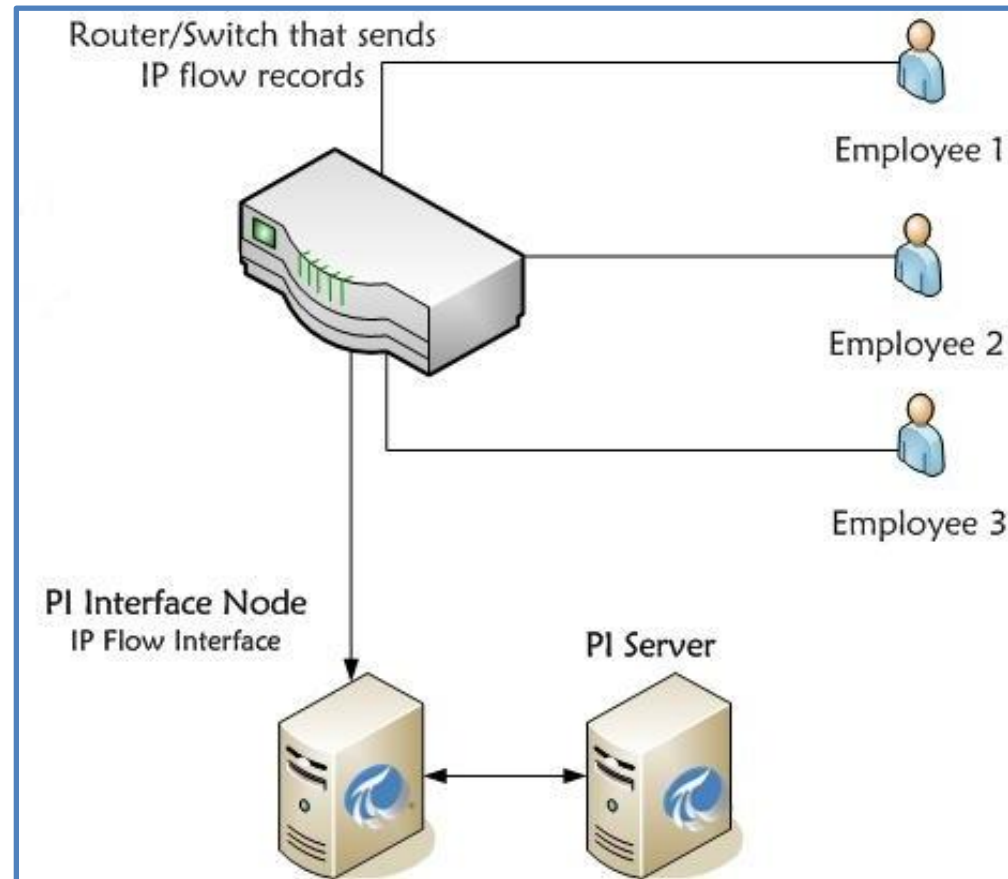
Advanced

OK Cancel Apply



- PortalEdge Enumeration Events

- FIN Port Scan
- Finger User
- ICMP Scan
- Syn Portscan
- TCP Portscan
- Traffic Monitor
- UDP Portscan



- Inputs
  - IP Flow record details (8 tag aliases)
  - Monitored ip address
    - Severity factor for rollup calculation
    - Traffic white list (destination, port, protocol)
- Outputs
  - Out of bounds Communication
  - Enumeration rollup class event



- **Credentialed Scanning Tools**
  - **Nessus with SCADA plugins (Bandolier)**  
<http://www.digitalbond.com/index.php/research/bandolier/bandolier-demonstration-video>
  - **Microsoft Baseline Security Analyzer**

- Scans for security updates, administrative vulnerabilities, additional system information, sql server, iis, and desktop applications

## Additional System Information

Score	Issue	Result												
	Windows Version	Computer is running Microsoft Windows Server 2008 R2.												
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.												
	Shares	<p>2 share(s) are present on your computer.</p> <table><thead><tr><th>Share</th><th>Directory</th><th>Share ACL</th><th>Directory ACL</th></tr></thead><tbody><tr><td>ADMIN\$</td><td>C:\WindowsAdmin</td><td>NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX</td><td></td></tr><tr><td>C\$</td><td>C:\</td><td>Admin ShareNT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\</td><td></td></tr></tbody></table>	Share	Directory	Share ACL	Directory ACL	ADMIN\$	C:\WindowsAdmin	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX		C\$	C:\	Admin ShareNT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\	
Share	Directory	Share ACL	Directory ACL											
ADMIN\$	C:\WindowsAdmin	NT SERVICE\TrustedInstaller - F, NT AUTHORITY\SYSTEM - RWXD, BUILTIN\Administrators - RWXD, BUILTIN\Users - RX												
C\$	C:\	Admin ShareNT AUTHORITY\SYSTEM - F, BUILTIN\Administrators - F, BUILTIN\												
	Services	No potentially unnecessary services were found.												

- PI 2010 Security Best Practices
  - White paper update
  - vCampus Live! VoX session follow up
  - vSIG collaboration by invitation



# Contact information and Q&A

Ann Moore [amoore@osisoft.com](mailto:amoore@osisoft.com)

Bryan Owen [bowen@osisoft.com](mailto:bowen@osisoft.com)



Thank you

© Copyright 2010 OSIsoft, LLC

777 Davis St., San Leandro, CA 94577