Oracle® Communications Performance Intelligence Center

Security Guide

Release 10.1

E55869 Revision 2

October 2014

ORACLE®

Oracle Communications Performance Intelligence Center Security Guide, Release 10.1

My Oracle Support (MOS) (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

See more information on MOS in the Appendix section.

Contents

Part 1: Overview

This section gives an overview of the Oracle Communications Performance Intelligence Center and explains general principles of application security.

Audience and Scope

This document is provided for administrators who have to make arrangements and configure this product for secure operation.

To avoid replication and fragmentation of information, detailed instructions are only in PIC Installation Procedure. We suggest following usage of the documentation:

- Read this document for overview, key concepts and guidelines
- Perform installation steps following Installation Procedure E53508-01
- Perform user management according to online manual of Security application
- Adjust PDU and field hiding according to online manual of Configuration application

Online documentation can be called from the Help menu in the application banner: Help – User Manual.

Glossary and acronyms

Definition of terms frequently used in this document

PIC: As the product name will be frequently mentioned in this document, Oracle Communications Performance Intelligence Center will be shortened as PIC.

PDU: Protocol Data Units are sequences of bytes captured on the telecommunications network, this is the main data input to PIC. During acquisition PIC adds a time stamp, link information and type code to later know what has been captured, when and where from.

xDR: eXtended Data Records is a generic term introduced by PIC to designate Call Detail Records (CDR), Transaction Detail Records (TDR), Session Detail Records (SDR), IP detail records (IPDR), …

KPI: Key Performance Indicators, statistical counts aggregated by a rules-based engine. For Storage, KPI are considered as statistical xDR.

CLI: Command Line Interface through sh or bash Linux command interpreter. This can be reached either on a physical console or a virtual console (ILO) or over ssh protocol.

ILO: Integrated Lights Out, electronic board inserted in each server allowing out of band access to the server even when it is powered off. This board can be accessed by software over an Ethernet connection and emulate console keyboard and screen or virtual CD drive for remote control of a server.

Glossary

Since PIC has passed a significant rework of its licensing parts, new words have been introduced that are not yet aligned in user interface. Table below provides a mapping between licensing documentation and user interfaces vocabulary.

Licensing name	User Interface Name	Description
Acquisition Datafeed	TADAPT	Direct PDU feed from acquisition servers
Acquisition	xMF	Message Feeder, generic
DR Storage	DWS	Data Warehouse Server
Integrated Acquisition	IMF	Integrated Message Feeder
Management Server	NSP	Network Software Platform, host for configuration and applications
Mediation Datafeed	Datafeed	xDR feed from Mediation servers
Mediation	IXP	Integrated xDR Platform subsystem
Multiprotocol troubleshooting	ProTrace	xDR and call trace browser
Network and Service Alarm	ProAlarm	
Network and Service Dashboard	ProPerf	KPI graphing application
PDU Storage	IXP PDU	Protocol Data Units storage
Performance Intelligence Center	PIC	Performance Intelligence Center, the system as a whole
Probed Acquisition	PMF	Probed Message Feeder
SS7 Network Surveillance	ProDiag	Per Link activity counters

Product Overview

PIC is a Network and Service Performance Management system. It provides dashboard and alarming to monitor 2G/3G/LTE/IMS networks for network and service related criteria. It generates broad KPI to track events impacting the business and to analyze historical trends. It has near real-time call tracing capabilities to locate the source cause of network or service dysfunction. PIC generates purpose built xDR used by various 3rd party applications like Business Intelligence, Revenue Assurance, Location Based Services, Machine to Machine (M2M) databases, or Fraud Management Systems. It can also deliver enriched signaling data and counters in near real-time mode to the service providers accounting system for interconnect billing and billing verification.

PIC is a distributed computing system over several Linux servers with dedicated roles: Management (and applications), Acquisition, Mediation and Storage.

General Security Principles

The following principles are fundamental to using any application securely.

Restrict physical Access to the System

Before considering IT security, consider first that all hardware (power, servers, disks, switches, cabling …) shall be installed in safe locations with restricted access in order prevent from unauthorized or accidental manipulation. Refer to the hardware documentation and make sure the installation is within normal operation range for temperature and electrical constraints.

Restrict Network Access to Critical Services

PIC Management server front-end access shall be limited to your Intranet area. Only authorized workstations of your company and controlled remote access over VPN shall have access to the Management server. Servers and connections are not designed for use on public networks. Even on Intranet we recommend using secure https for Management server interaction with browsers.

PIC Acquisition, Mediation and Storage shall be interconnected by an insulated back-end LAN or VLAN with firewalls filtering access. Management server has a second network access that is dedicated for interfacing with back-end servers. Only PIC administrators and Support teams need access to the back-end LAN. Standard end-users (other than administrators) interact only with Management server only, also operating as Application server.

Back-end VLAN makes use of non-ciphered protocols; detailed lists will be provided later in this document for firewall setup. Restrictive firewall and routing settings are recommended to avoid that those communications can be intercepted or tampered. This also extends to configurations where Acquisition or Mediation servers are deported on a remote site. In such cases PIC customer is requested to provide safe pipes from its own infrastructure to make sure PIC machine to machine communication is safe.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities. PIC Management server provides a security management application, with access restricted to PIC administrators that permits to configure roles, privilege and object ownership.

PIC manages object ownership with the granularity of a “session” which collects a dedicated stream of xDR or statistics reconstituted from a subset of the network activity defined by protocol filters and link or SCTP association or logical flow in IP filters. This allows a segregation of access level considering different activities monitored by PIC. A session permanently gets new records and drops old records based on a lifetime configuration parameter.

Monitor System Activity

Audit log and System alarms are two applications provided to monitor system activity. Use these tools on a regular basis. Audit records normal action, including connections, configuration changes. System alarms is a log of various incidents, when system encounters abnormal conditions.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check this note regularly for revisions.

Part 2: Secure Installation and Configuration

Installation Overview

This section outlines the planning process for a secure installation and describes recommended deployment topologies for the system.

Understand Your Environment

Which resources am I protecting?

PIC is a distributed system over several standard servers and storage systems. Each server holds its own resources that require adapted level of protection:

Management server: is the central application and configuration server for PIC. It holds system and session configuration and user information (login, credentials) as well as saved query results in an embedded database. It runs applications with an Apache http(s) front-end server and multiple Weblogic web container instances. The server acts as a web server but the type of application is meant for Intranet access level only. Security application in the Management server is the place where permissions are granted to users to browse all or parts of the data contained in sessions. Security application is restricted to administrators.

Storage servers: There are two types of storage servers. DWS store network reconstituted transactions (xDR) and statistics (KPI). IXP PDU storage servers store PDU in flat files. Storage servers shall be connected to restricted back-end VLAN. They answer to queries from the Management server and work as high bandwidth data sink for meditation servers. Direct access to storage server would bypass the screening rules implemented in the Applications and therefore shall be protected. PDU storage servers share flat files on NFS shares.

Mediation servers: These servers perform real time correlation of PDU and generate xDR. They also aggregate xDR to generate KPI. Network tapped data transitions and is transformed on these servers. It is present from one minute to a few hours according to buffer management and aggregation level. Mediation servers get their configuration by replicating data from the Management server database.

Acquisition servers: They collect frames from the monitored network, reassemble segments, split multiple chunks (in case of SCTP), timestamp each resulting PDU, and route it to Mediation servers according to filtering rules set on the Management server. Acquisition servers get their configuration by replicating data from the Management server database.

All servers are Linux based servers with their standard access protection (file system access protection for root and other users). By default all servers listen ssh, rmi and https ports in addition to dedicated ports that will be described later in this document. ssh access requires loging as per standard Linux account management, accounts are independent for each server. Excepted when

running on HP C-Class blades, PIC does not use DHCP it connects configured IP addresses that are stored in the configuration database. Please refer to PM&C security guide for this exception. External servers can be addressed by names and needing a DNS service: alarms forwarding, emailing passwords.

From whom am I protecting the resources?

All servers other than Management should be protected from any user access except administrators and support for maintenance.

Management server shall be accessible to identified Intranet users. They are asked for a personal login but this web server. PIC profile based permissions discriminate different levels of data access as configured by PIC administrators. Access can be granted by users to sessions and this access can be full or with hidden fields according to user profile (more information in the online manual of Security application). Sessions containing call detail records can be restricted to Customer service troubleshooting teams, whereas sessions containing anonymized statistics (KPI) can be allowed for Network Planning or Marketing teams according to their nature. On sessions containing call detail records, a default field hiding mechanism applies to mask sensitive field content such as passwords or PIN codes or SMS content. Activate this mechanism (PDU hiding) from central configuration main page and make sure each user is associated with an appropriate profile.

What will happen if the protections on strategic resources fail?

Audit logs keep track over a few days of actions performed by users on the Management server. It is recommended to periodically browse these records to check if actions performed by each identified user are in the expected scope. Multiple condition filters allow looking at this from different perspectives. Excessive access permissions can be a result of misinterpreted application or privacy rules.

Failed login attempts are tracked as system alarms. An abnormal increase of such alarms could be a sign. System Alarms log is another part of PIC that shall be watched at least daily because it also reports hardware failures.

OS level login attempts are tracked by standard Linux log services. Typically no such attempt is expected on any server for normal PIC usage because all is managed by a web application portal. There is segregation on each server between system accounts (root) and application accounts (cfguser or tekelec) and Linux file permissions is a protection against unwanted access. OS account passwords shall be periodically changed and kept secret from end-users. There is minimal enforcement of password setting rules (like MAXDAYS for a password) but each site administrator should follow its local policy (strength, period) when changing passwords. Keep in mind that application users shall not get OS level login.

The list of sessions with their timestamp of last insertion constitutes a valuable dashboard to watch because an intrusion as well as a hardware failure might interrupt the insertion of records to the sessions.

Recommended Deployment Topologies

This section describes recommended architectures for deploying Oracle Communication Performance Intelligence Center to secure access.

Intranet delimitation

PIC is an application designed to work inside an secured Intranet environment. It has not been specifically hardened to be exposed on The Internet. Computers able to reach PIC servers are expected to have passed a first level of authentication which is independent of PIC and relies on local IT infrastructure (physical LAN connection, VPN connectors, MPLS, …)

Front-end and Back-end

The deployment recommendation is to use the well-known and generally accepted front-end back-end separation. Several variations of this architecture are possible depending on the number of locations for data collection and their distance from the Network operation Center (NOC):

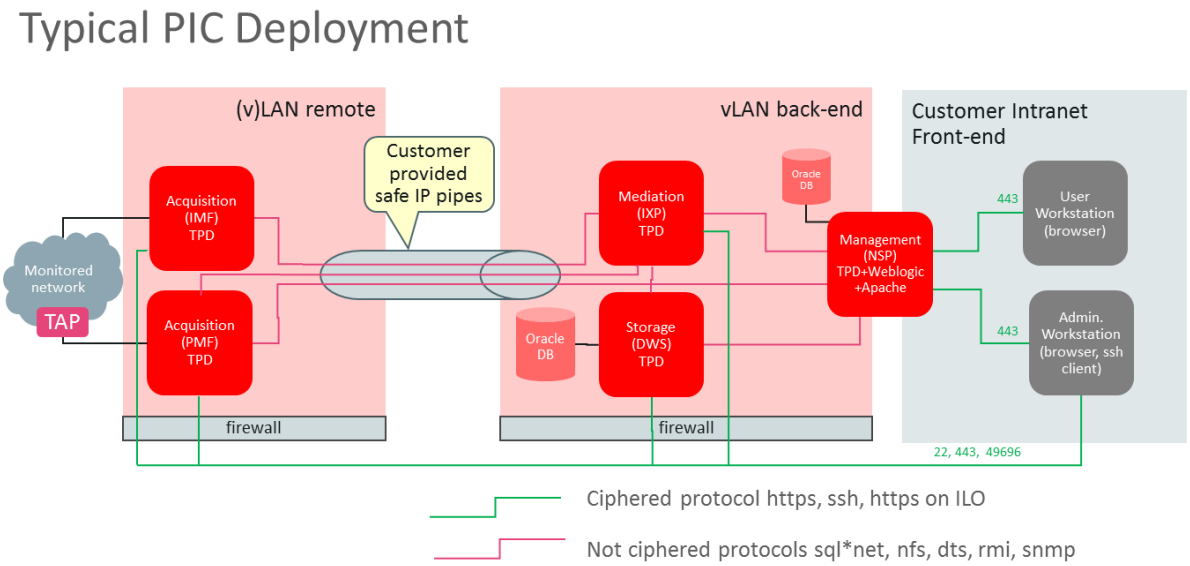


Figure 2-1 Traditional front-end back-end deployment

Alternatives are possible: Mediation and Storage can be on a remote site, multiple remote sites can exist, and Acquisition can exist on local back-end at NOC.

It is important to get this point for securing the system: Communication channels between Management, Mediation, Storage, and Acquisition are not on ciphered protocols and need a fence protection against unauthorized access. This extends to end-users who are only allowed to view parts of the contained information after screening has been performed by the application. Tapping internal links could lead to unwanted disclosure of information although this requires directed search and intrusion.

Each server has an out of band management port (Integrated Lights Out – ILO). These ports shall be connected to an independent LAN or VLAN, restricted to support and Maintenance. These ports

allow access via a virtual console. Security of this maintenance access mode can be enhanced for strong encryption, please refer to HP ILO documentation.

Installing Management

This section describes how to install and configure Management component securely. Please use Installation manual for step by step operation after security guidelines have been read in this document.

Management Key Concepts

Management (NSP) is a web server that is seen as the PIC façade by end-users. Except administrators for maintenance, no-one needs to connect on another server than the management server. This server runs administrative tools as well as applications in a web server mode.

Management has several sub-components that can collaborate either in a single physical server or over a group of 4 servers. Apache web server is serving https requests and load sharing over several application servers. Weblogic instances, 2 per physical server on one or on a couple of servers (primary, secondary), are in charge of the application logic in J2EE architecture. An Oracle Database Instance is used for persistence of user permissions, session configuration, application preferences, scheduled tasks, KPI parameters, temporary data queries and historical result sets.

Management server(s) run with a dedicated and pre-configured version of Linux based on CentOS and called TPD. This version is adapted and tested for a given application version and shall not be changed or tuned.

Management Installation Security Steps

Once Management ISO is installed on Management server (or for older sites upgrade Management ISO on one box or 4 box servers) according to installation manual, take care of these aspects:

- Perform password handover with Professional Services: change OS accounts with strong passwords in accordance to your local policy. OS and application accounts are listed in Appendix C.
- According to your local policies, set parameters for end user management. There is an option to send initial password if you agree to connect Management server to a mail service (optional). As an alternative you can choose default initial passwords and communicate them without application support, flagged for change on first connection. Details can be found in the online guide of the Security application.
- Create or update end-user accounts in Security application. Each end-user shall have his personal identifier and password. We discourage you from sharing team accounts…
- Define session boundaries and allocate ownership of sessions to end-users. This definition requires both security and telecom skills to define adequately the boundaries of each session. It can happen that because of important throughput a functional boundary may require several sessions in the configuration.

Management Ports

PIC does not provide firewalls or setup files for such equipment. Please use the list of ports that can connect to a Management server to create your firewall configurations. PIC can use various configurations and not all connections are needed, open only those that are active for your configuration and that come from outside the area delimited by your firewall.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Acquisition	Managmt_Primary	0	ICMP	-	Ping	TEMPORARY
Acquisition	Managmt_Primary	7	TCP/UDP	-	echo	N
Acquisition	Managmt_Secondary	7	TCP/UDP	-	echo	N
Support_remote	Managmt_Apache_BE	22	TCP	SSHv2	ssh	N
PM&C	Managmt_Apache_BE	22	TCP	SSHv2	ssh	N
Support_remote	Managmt_OracleDB	22	TCP	SSHv2	ssh	N
PM&C	Managmt_OracleDB	22	TCP	SSHv2	ssh	N
Acquisition	Managmt_Primary	22	TCP	SSHv2	ssh	N
Support_remote	Managmt_Primary	22	TCP	SSHv2	ssh	N
PM&C	Managmt_Primary	22	TCP	SSHv2	ssh	N
Support_remote	Managmt_Secondary	22	TCP	SSHv2	ssh	N
PM&C	Managmt_Secondary	22	TCP	SSHv2	ssh	N
Support_remote	Managmt_Apache_FE	80	TCP	-	http	OR HTTPS
Customer_Workstn	Managmt_Apache_FE	80	TCP	-	http	OR HTTPS
Acquisition	Managmt_NTP	123	UDP	-	ntp	N
Support_remote	Managmt_NTP	123	UDP	-	ntp	N
Blades_OA	Managmt_NTP	123	UDP	-	ntp	N
Managmt_Apache_BE	Managmt_NTP	123	UDP	-	ntp	N
Managmt_OracleDB	Managmt_NTP	123	UDP	-	ntp	N
Managmt_Primary	Managmt_NTP	123	UDP	-	ntp	N
Managmt_Secondary	Managmt_NTP	123	UDP	-	ntp	N
Mediation	Managmt_NTP	123	UDP	-	ntp	N
MicrotelInnovation	Managmt_NTP	123	UDP	-	ntp	N
MSW	Managmt_NTP	123	UDP	-	ntp	N
PM&C	Managmt_NTP	123	UDP	-	ntp	N
SAN_Controller	Managmt_NTP	123	UDP	-	ntp	N
SAN_Switch	Managmt_NTP	123	UDP	-	ntp	N
SWITCH	Managmt_NTP	123	UDP	-	ntp	N
Customer_SNMP	Managmt_Primary	161	UDP	-	snmp.a	N
Blades_OA	Managmt_Primary	162	UDP	-	snmp.b	Y
MicrotelInnovation	Managmt_Primary	162	UDP	-	snmp.b	Y
NEPTUNE	Managmt_Primary	162	UDP	-	snmp.b	Y
SAN_Controller	Managmt_Primary	162	UDP	-	snmp.b	Y
SAN_SWITCH	Managmt_Primary	162	UDP	-	snmp.b	Y
Support_remote	Managmt_Apache_FE	443	TCP/UDP	SSLv3 TLSv1	https	N
Customer_Workstn	Managmt_Apache_FE	443	TCP/UDP	SSLv3 TLSv1	https	N
Mediation	Managmt_Primary	1099	TCP	-	RMI	N
Support_remote	Managmt_OracleDB	1158	TCP	-	OracleDBEM.a	N
Acquisition	Managmt_OracleDB	1521	TCP	-	OracleDBNet8	N
Support_remote	Managmt_OracleDB	1521	TCP	-	OracleDBNet8	N
Mediation	Managmt_OracleDB	1521	TCP	-	OracleDBNet8	N
Support_remote	Managmt_OracleDB	5520	TCP	-	OracleDBEM.b	N
Support_remote	Managmt_Primary	8001	TCP	-	nsp.admin.ldap	N

Acquisition	Managmt_Primary	16810	TCP	-	inetsync	N
Acquisition	Managmt_Primary	16878	TCP	-	inetmerge	N
Mediation	Managmt_Primary	41090	TCP	SSLv3	NFM.b	N
Mediation	Managmt_Secondary	41090	TCP	SSLv3	NFM.b	N
Support_remote	Managmt_Apache_BE	49696	TCP	-	JMX(https)	N
Support_remote	Managmt_OracleDB	49696	TCP	-	JMX(https)	N
Support_remote	Managmt_Primary	49696	TCP	-	JMX(https)	N
Support_remote	Managmt_Secondary	49696	TCP	-	JMX(https)	N
Acquisition	Managmt_Primary	7001;7003	TCP	-	jms,t3	N
Support_remote	Managmt_Primary	7001;7003	TCP	-	jms,t3	N
Mediation	Managmt_Primary	7001;7003	TCP	-	jms,t3	N
Acquisition	Managmt_Secondary	7001;7003	TCP	-	jms,t3	N
Support_remote	Managmt_Secondary	7001;7003	TCP	-	jms,t3	N
Mediation	Managmt_Secondary	7001;7003	TCP	-	jms,t3	N

Installing Storage

Storage Key Concepts

Storage servers are used for large capacity data storage. There are two types of storage in PIC:

xDR storage is based on an Oracle Database and provides structured tables for session data (call legs records, transaction records as well as statistics – KPI). Only Management server applications shall have access to xDR storage in a machine to machine paradigm. This server does not use accounts for end users. Latest baseline xDR storage server has a capacity of 8.4 TB, up to 4 xDR storage servers can work together in a pool performing load sharing.

PDU storage is based on shared directories with flat files. File sharing is based on NFS. Due to the huge size of PDU data, even with a few days lifetime only, it is difficult to find something specific in those large files. Applications use indexing through xDR to show right PDU content. Like for xDR no end user shall access directly to PDU storage; ProTrace application does this after checking individual permissions. Latest baseline PDU storage server has a capacity of 9.4 TB. Up to 4 PDU storage servers can work together in a pool performing load sharing.

Both types of servers are Linux servers in a dedicated and pre-configured distribution. This distribution is aligned with PIC version and updates for Linux components come with PIC upgrades. One PIC site can use several independent storage pools.

Storage Installation Security Steps

Storage servers shall be installed from their respective ISO images: DWS ISO for xDR storage and IXP ISO for PDU storage. Each storage server has to be declared on the Management server. The connection is set on behalf of IPv4 addresses. PIC does not use DNS.

These servers do not require additional steps other than ensuring that the back-end delineation is effective: their IP should not be visible from computers of application users. This back-end separation is the duty of local network and firewalls setup that are out of scope of PIC.

Storage Ports

Storage servers (DWS, IXP PDU) are listening on a number of ports each dedicated for a special use:

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Mediation	Storage_PDU	0	ICMP	-	Ping	N
Mediation	Storage_PDU	111	TCP	-	portmap	N
Support_remote	Storage_DR	1158	TCP	-	OracleDBEM.a	N
Support_remote	Storage_DR	1521	TCP	-	OracleDBNet8	N
Managmt_Primary	Storage_DR	1521	TCP	-	OracleDBNet8	N
Managmt_Secondary	Storage_DR	1521	TCP	-	OracleDBNet8	N
Mediation	Storage_DR	1521	TCP	-	OracleDBNet8	N
Mediation	Storage_PDU	2049	UDP	-	NFS	N
Support_remote	Storage_DR	5520	TCP	-	OracleDBEM.b	N

Installing Mediation

Mediation Key Concepts

Mediation (IXP) is performed on servers with specific and pre-configured Linux distribution. Linux modules come with Mediation ISO image. Mediation servers work in groups called subsystems in an operation mode similar to clusters. Servers belonging to the same subsystem shall be on a single site because inside the subsystem there are local communications that implement a middleware layer to make the subsystem working as a consistent entity. These communication shall not operate over long distance links (no WAN) due to both security and performance. PDU storage servers are also contributors to the subsystem because in addition to storing large files they can run mediation processes.

Mediation consists of several software operations based on a concept of data flows. A dataflow is a sequence of processes that get data from an acquisition or a mediation process. Some of them forward their result to another process, some forward data to storage servers. The connection between two processes is called a stream. It is based on a proprietary protocol on top of TCP/IP, not ciphered. A stream can get data from a distant server, from a server on the LAN or from the local loopback interface (process on the same server). Typical mediation processes are

- Build: input streams collect PDU from acquisition servers, several input streams can be involved. The process correlates PDU to generate xDR according to plug-in modules for various protocols (xDR builders). Output streams are made of xDR.
- Operate: operate takes one or several xDR streams as input and generates one or several xDR streams as output. The process works based on rules stored in scripts and provided by the Management server. Some scripts perform static enrichment (mapping values based on xDR field content), other scripts perform aggregation (counting records and summing variables based on rules) to generate KPI
- Store: input streams collect xDR either from Build or Operate and output is database insertion or CSV file generation. Note: this process is running on a mediation server as a client of the Storage server where records are actually preserved.

Each subsystem shares a virtual IP address (VIP) to designate its active master server which is the preferred interface to the Management server. In case of failure the VIP moves to the standby master, then becoming active. This VIP shall be reserved in the same range than other IP addresses for Mediation servers. Only Management server shall connect to the VIP and occasionally PIC administrators to physical server IP addresses for maintenance. End users shall not be allowed in this address space.

Management server shall be allowed to connect on any Mediation server because these mediation servers provide answers to PDU queries once the Management server has found xDR on a storage server.

Mediation Installation Security Steps

Mediation server installation ISO image comes with pre-configured settings that do not require special security actions on the server itself, except:

- Declare each Mediation server on the Management server by its IPv4 address. PIC does not use DHCP, however IP setting and hostnames shall match naming convention.
- Setup firewalls between Intranet, Back-end and hardware support LAN.
- Make sure IP range for Mediation servers, including VIP are on a LAN or VLAN segregated from the end users and the visitors.

Mediation Ports

Firewall setup is proposed considering that usually mediation servers are connected to the same LAN than Storage servers and Management back-end.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Managmt_OracleDB	Mediation	0	ICMP	-	Ping	TEMPORARY
Support_remote	Mediation	22	TCP	SSHv2	ssh	N
Managmt_OracleDB	Mediation	22	TCP	SSHv2	ssh	N
Managmt_Primary	Mediation	22	TCP	SSHv2	ssh	N
Managmt_Secondary	Mediation	22	TCP	SSHv2	ssh	N
PM&C	Mediation	22	TCP	SSHv2	ssh	N
Managmt_Primary	Mediation	1099	TCP	-	RMI	N
Managmt_Secondary	Mediation	1099	TCP	-	RMI	N
Mediation	Mediation	2222	TCP	-	DTS	N
Managmt_Primary	Mediation	5031	TCP	-	DSAPI.a	N
Managmt_Secondary	Mediation	5031	TCP	-	DSAPI.a	N
Managmt_Primary	Mediation	5055	TCP	-	DSAPI.b	N
Managmt_Secondary	Mediation	5055	TCP	-	DSAPI.b	N

Installing Acquisition

Acquisition Key Concepts

Acquisition servers are frequently installed on remote sites to collect PDU from redundant points of the monitored network. When this is not needed they can be on the same LAN than Mediation servers. In case of installation on a remote site, IP connections flowing from site to site shall be protected by network provided encryption such as VPN or MPLS. This encryption is not provided by PIC but is needed because those links forward PDU captured on the live network.

Acquisition servers have independent NIC. Standard Ethernet ports are connected to the LAN or a remote connection to Mediation LAN. Other ports, dedicated to acquisition are connected to devices that provide PDU data. In Integrated mode these ports are on a dedicated VLAN shared with Eagle™. In probed mode these ports are either connected to a switch capable of port mirroring or to a tapping device. This side of the connection shall get the same level of protection than the network links. PIC does not provide encryption.

Acquisition Installation Security Steps

Acquisition servers installation ISO image comes with pre-configured settings that do not require extra security steps except to make sure connections with Acquisition servers are on a segregated LAN or VLAN protected by firewall settings.

Acquisition ports

Following list of ports have to be configured in firewalls or other network equipment surrounding acquisition servers:

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Managmt_OracleDB	Acquisition	0	ICMP	-	Ping	TEMPORARY
Managmt_Primary	Acquisition	7	TCP/UDP	-	echo	N
Managmt_Secondary	Acquisition	7	TCP/UDP	-	echo	N
Support_remote	Acquisition	22	TCP	SSHv2	ssh	N
Managmt_OracleDB	Acquisition	22	TCP	SSHv2	ssh	N
Managmt_Primary	Acquisition	22	TCP	SSHv2	ssh	N
Managmt_Secondary	Acquisition	22	TCP	SSHv2	ssh	N
PM&C	Acquisition	22	TCP	SSHv2	ssh	N
Managmt_Primary	Acquisition	1099	TCP	-	RMI	N
Managmt_Secondary	Acquisition	1099	TCP	-	RMI	N
Mediation	Acquisition	2222	TCP	-	DTS	N
Managmt_Primary	Acquisition	3306	TCP	-	MySql	N
Managmt_Primary	Acquisition	15616	TCP	-	JDBC	N
Managmt_Secondary	Acquisition	15616	TCP	-	JDBC	N
Acquisition	Acquisition	16810	TCP	-	inetsync	N
Managmt_Primary	Acquisition	16810	TCP	-	inetsync	N
Acquisition	Acquisition	16878	TCP	-	inetmerge	N
Managmt_Primary	Acquisition	16878	TCP	-	inetmerge	N
Managmt_Primary	Acquisition	41000	TCP	-	RMI-JMX-sec	N
Managmt_Secondary	Acquisition	41000	TCP	-	RMI-JMX-sec	N
Support_remote	Acquisition	49696	TCP	-	JMX(https)	N

Connecting other servers

Customer connection

PIC interacts with your local IT equipment to use standard IT services:

NTP

All PIC servers have a constraint to have a redundant connection to a reliable Network Time Protocol source. The most frequent option to address this is to select Management primary server and one Mediation server as local NTP relays and connect only these two servers to an accurate NTP source. Then every PIC server must be provided with a non-filtered NTP access to the Management server and to the first Mediation server.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Managmt_NTP	Customer_NTP	123	UDP	-	ntp	N
Acquisition	Managmt_NTP	123	UDP	-	ntp	N
Support_remote	Managmt_NTP	123	UDP	-	ntp	N
Blades_OA	Managmt_NTP	123	UDP	-	ntp	N
Managmt_Apache_BE	Managmt_NTP	123	UDP	-	ntp	N
Managmt_OracleDB	Managmt_NTP	123	UDP	-	ntp	N
Managmt_Primary	Managmt_NTP	123	UDP	-	ntp	N
Managmt_Secondary	Managmt_NTP	123	UDP	-	ntp	N
Mediation	Managmt_NTP	123	UDP	-	ntp	N
MicrotelInnovation	Managmt_NTP	123	UDP	-	ntp	N
MSW	Managmt_NTP	123	UDP	-	ntp	N
PM&C	Managmt_NTP	123	UDP	-	ntp	N
SAN_Controller	Managmt_NTP	123	UDP	-	ntp	N
SAN_Switch	Managmt_NTP	123	UDP	-	ntp	N
SWITCH	Managmt_NTP	123	UDP	-	ntp	N

Mail

By default, passwords can be sent by a mail to application users. To achieve this you need to configure an access to a mail service and allow this destination in firewall settings.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Managmt_Primary	Customer_MAIL	25	TCP	-	smtp	Y
Managmt_Secondary	Customer_MAIL	25	TCP	-	smtp	Y

PIC feed targets

There are use cases where the data collected by PIC is not only processed by PIC applications but also feeds local applications. There are two ways to get data from PIC, either by providing an Oracle Database server connection with a customized schema (Customer_DWH) or by providing NFS shared directories where PIC can drop CSV files (Customer_NFS). These servers shall come with their own protection mechanisms and allow PIC access as defined in next table.

NFS sharing to destinations out of back-end LAN shall not be used. Rather use a standard server and configure it as a file repository inside back-end LAN. Allow remote file access with secure standard services such as scp or sftp.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Support_remote	Customer_DWH	22	TCP	SSHv2	ssh	N
Support_remote	Customer_DWH	80	TCP	-	http	OR HTTPS
Mediation	Customer_feed	111	TCP	-	portmap	N
Support_remote	Customer_DWH	443	TCP/UDP	SSLv3 TLSv1	https	N
Support_remote	Customer_DWH	1521	TCP	-	OracleDBNet8	N
Managmt_Primary	Customer_DWH	1521	TCP	-	OracleDBNet8	N
Managmt_Secondary	Customer_DWH	1521	TCP	-	OracleDBNet8	N
Mediation	Customer_DWH	1521	TCP	-	OracleDBNet8	N
Mediation	Customer_feed	2049	UDP	-	NFS	N
Acquisition	Customer_TADAPT	9090	TCP	-	MFP.a	TADAPT
Support_remote	Customer_DWH	9300	TCP	SSL	iLO.a	N
Support_remote	Customer_DWH	17988	TCP	-	iLO.b	N
Support_remote	Customer_DWH	17990	TCP	-	iLO.c	N

Support and troubleshooting workstations

There are two ways to provide support access to PIC servers: either with ssh protocol which is implemented in each of them or by ILO access. ILO access is an out of band management board installed in each HP server used by PIC. This ILO access shall be dedicated to maintenance VLAN with highly controlled access because with adequate HP software is possible to open a virtual console and also mount virtual media. On the other hand this type of access allows almost any maintenance operation from a remote location, including OS fresh installation and server power off/on.

Rather than managing access of a large number of servers it is recommended to add one server to the LAN and use it as a jump-off server. With secure access to this single server, after authentication, it is then possible to open local connections to perform maintenance and investigation when support is needed.

For systems using Blade servers and SAN storage, plan also for a maintenance access to these controllers over this maintenance LAN.

PM&C is a server added to support installation, upgrade and maintenance on HP C-class blades in combination with SAN storage and Onboard-Administrator (OA) of C-Class enclosures. PM&C creates a closed and dedicated VLAN on which DHCP is active. This VLAN is separated from the site LAN.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
PM&C	Blades_OA	22	TCP	SSHv2	ssh	N
Support_remote	ILO	22	TCP	SSHv2	ssh	N
Support_remote	SAN_Controller	22	TCP	SSHv2	ssh	N
PM&C	SAN_Controller	22	TCP	SSHv2	ssh	N
Support_remote	SAN_SWITCH	22	TCP	SSHv2	ssh	N
PM&C	SAN_SWITCH	22	TCP	SSHv2	ssh	N
Support_remote	ILO	80	TCP	-	http	OR HTTPS
Support_remote	Blades_OA	443	TCP/UDP	SSLv3 TLSv1	https	N
Support_remote	ILO	443	TCP/UDP	SSLv3 TLSv1	https	N
Support_remote	SAN_Controller	443	TCP/UDP	SSLv3 TLSv1	https	N
Support_remote	SAN_SWITCH	443	TCP/UDP	SSLv3 TLSv1	https	N
Support_remote	ILO	3389	TCP	TLS (option)	RDP	Y

Support_remote	ILO	9300	TCP	SSL	iLO.a	N
Support_remote	ILO	17988	TCP	-	iLO.b	N
Support_remote	ILO	17990	TCP	-	iLO.c	N
Support_remote	SWITCH_3020	23	TCP	-	Telnet	N

Third party acquisition devices

PIC can collect data from third party devices. Follow secure setup guidelines provided with these products. Consider their criticality as similar to the network links from where they tap frames. When the device is connected to a probed acquisition server it can be on a dedicated acquisition LAN. When the device interacts directly with a mediation server, then we recommend connecting this device to the back-end LAN.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Support_remote	MicrotelInnovation	22	TCP	SSHv2	ssh	N
Support_remote	MicrotelInnovation	23	TCP	-	telnet	Y
Managmt_Primary	NEPTUNE	80	TCP	-	http	OR HTTPS
Support_remote	TAP	80	TCP	-	http	OR HTTPS
Support_remote	MicrotelInnovation	161	UDP	-	snmp.a	N
Support_remote	NEPTUNE	22222	TCP	SSL	Neptune.https	Y
Mediation	NEPTUNE	56000	TCP	-	Neptune.up	Y
Mediation	NEPTUNE	56001	TCP	-	Neptune.cp	Y

Post Installation Configuration

Security configuration changes that must be considered after installation.

Lock root ssh access

It is a good security practice to disallow ssh connection to the super user account “root”. Default installation allows root ssh. This can be changed with CLI:

```
/usr/TKLC/plat/sbin/rootSshLogin --revoke
```

Note: Be aware that after root ssh login has been revoked, remote access is only possible with a dedicated OS user on the server, followed by an **su –** command when need be. An alternative is the ILO access to a virtual console.

For additional options, e.g. or restoring root access, please refer to

```
man rootSshLogin
```

Change default OS user passwords

Security is most easily broken when a default database server user account still has a default password even after installation. Consider Appendix C with the list of all accounts and change their default passwords.

Install a signed certificate for the web server

By default after installation, Management server has a self-signed certificate for the https protocol. This mode of operation is mentioned as not safe by most modern web browsers and shall not be used in production. Consider acquiring a certificate signed by a third party authority and install this certificate according to detailed steps available in Installation Procedure (Configure Apache HTTPS Certificate). More information in Installation Procedure.

Enforce password management.

Activate password enforcement verifications, such as password length, history, and complexity. This can be set in Management – Security Application. More information in online documentation of Security Application.

Activate and tune PDU hiding

PDU hiding is a mechanism that restricts access to certain fields of the xDR or of the PDU decoding (PIN codes, private identifiers, passwords) or even full PDU content, depending on each user profile. Administrators and users with “Business manager” role in their profile will be allowed to view values in such fields as well as fine-tune the list of these fields; keep such profiles restricted to people who have adapted level of permission in the company.

Configure session protection

The “session” is a basic object in PIC delimiting permissions. A smart way to keep control of data access is to define a session owner for each of them. Then the session owner can grant permission to another user to access his data

More information in the online guide of Management – Security.

Part 3: Security Features

In this section outline the specific security mechanisms offered by the product.

The Security Model

The security Model used by PIC is based on roles and profiles with one user id and password for each identified application user. Detailed documentation of the security model is provided in the online manual of the Security Application. Only administrators of the Management server are allowed to run Security Application.

Security model of Management server implements all critical mechanisms:

Authentication: each user is prompted for an identifier and password to open a working session. PIC Administrator can set a session timeout timer in Security – Actions – Manage tokens.

Authorization: an authenticated user can only access applications and objects as defined in his user profile by the administrator.

Audit: important steps of user interaction with PIC are logged and can be browsed by an Administrator in the Audit application.

Configuring and Using Authentication

Authentication is managed inside PIC application by an embedded directory server. In PIC, Security application is available to configure and manage user accounts. This application has an online user manual in PDF format that can be downloaded and printed.

Managing Authentication

PIC has a built-in super-user to create and manage other user's accounts. This user's login is TklcSrv. Users created with administrator privilege are granted to create additional users.

Password Policy

Only user TklcSrv in Security application is allowed to set password policy for all PIC application users. There are two levels of password strength:

Default: only checks length

Strong: checks length and complexity (upper/lower case, digits, symbols) and history (not reusing one of last used passwords)

It is also possible to force maximum age, minimum age, grace period and expire warning periods for password changes.

More details are explained in the Security Application online documentation.

Locked accounts

After three failed login attempts, an account is locked. There is no self-service or timeout option, a PIC administrator has to go into Security application and unlock the account. In case the user has lost his password it is possible to reset the password to a known value that will be changed on first login.

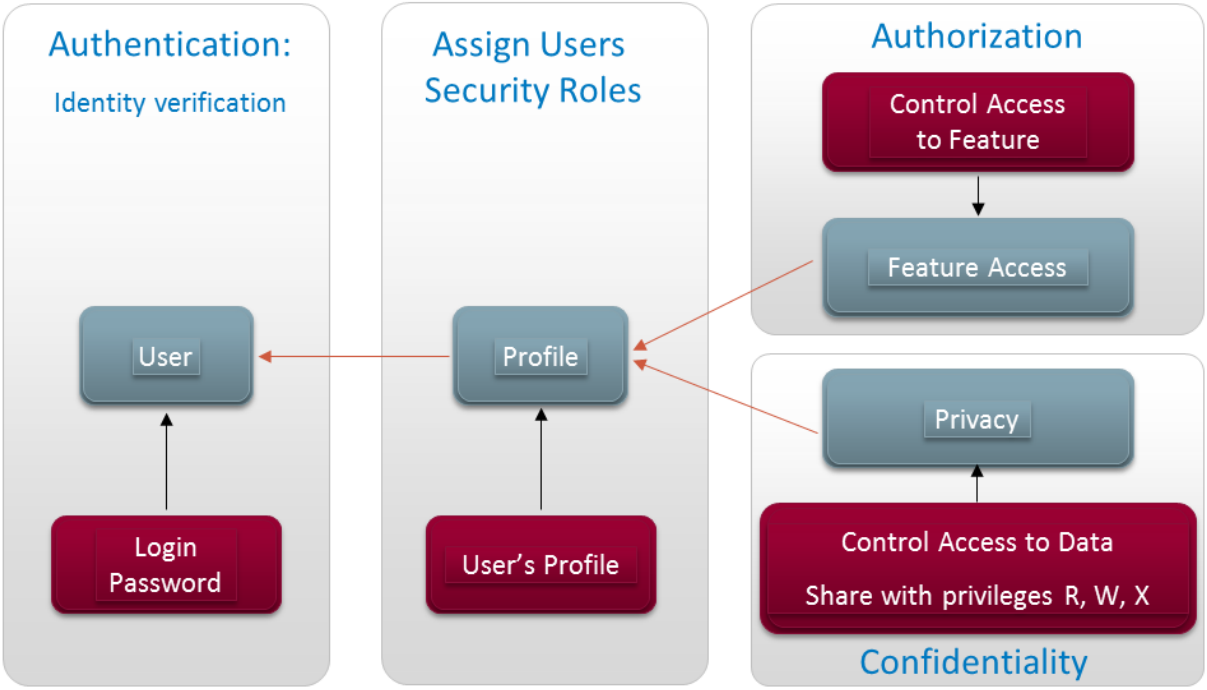
Intrusion attempts

Failed login attempts generate an alarm that needs to be cleared in the System Alarms application. This allows detection of intrusion attempts.

Configuring and Using Access Control

The cornerstone of access control in PIC is the session. A session is determined by a set of PDU captured on selected links or associations and filtered with locally defined criteria. PIC generates xDR based on PDU correlation and stores them in Sessions. The session is a PIC object that has an owner in the security model applied in PIC. So both technical and security criteria define how sessions shall be configured. Session setup will not be described in this document as it is too wide for this context. Usually training sessions are used to become familiar with session configuration.

PIC access works with profiles, each user gets a profile associated to his login. Before creating users, it is important to prepare the Profiles, each Profile defining an access level on two levels:



Authorization is a mapping towards product features (software modules) that are allowed or not according to the user profile.

Confidentiality is a mapping to user groups that are granted read, write or execute permissions on data objects. Most important data object is the session; but there are secondary data objects such as predefined queries or KPI configurations that follow the same data object permission model.

Part 5: Appendices

Appendix A: Secure Deployment Checklist

The following security checklist includes guidelines that help secure PIC:

1. Install only what is required.
2. Enforce password management.
3. Enable session access protection.
4. Practice the principle of least privilege.
    i. Grant necessary privileges only.
5. Enforce access controls effectively and authenticate clients stringently.
6. Restrict network access.
    i. Use a firewall.
    ii. Never poke a hole through a firewall.
    iii. Monitor Audit logs (include who accesses the system)
    iv. Check network IP addresses.
7. Apply all security patches and workarounds.
8. Contact Oracle Security Products if you come across vulnerability in PIC

Appendix B: Open Ports

Please check the list provided for each component, Management, Storage, Mediation, Acquisition and for external systems.

Appendix C: Accounts

Table below provides a list of used account names on different servers. Please make sure that at system handover you go through these accounts and set your private password, compliant with your password strength policy.

OS accounts with same name have independent passwords on each PIC server.

Application accounts exist on Management server only.

ILO accounts are used for the out of band management of each server.

LANSwtch accounts apply to Cisco switches

First table does only document accounts used in a rack mount configuration which is hardware baseline for PIC10.0.

Area	Identifier	Description	Managmnt	Storage	Mediation	Acquisition	Other
Database	IXP	xDR storage schema owner		√			
Database	NSP	Configuration schema owner	√				
Database	sys	Database administrator DBA user	√	√			
Database	system	Database administrator DBA user	√	√			
FC switch	admin	Brocade Fiber Channel switch admin					
GRUB	grub	Linux boot configuration	√	√	√	√	
ILO	Administrator	Integrated Lights Out remote console login https, ssh	√	√	√	√	
ILO	tekelec	Integrated Lights Out remote console login https, ssh	√	√	√	√	
LANSwtch	enable	Internal software password to enable changes					Switch
LANSwtch	root	SSH remote access					Switch
LANSwtch	telnet	Telnet, port 23, configuration access					Switch
MRV	tklc	Terminal server for remote console				√	
OS	admusr	SSH connection account when root ssh is revoked	√	√	√	√	
OS	backup	SFTP access to backup files	√				
OS	cfguser	PIC runtime owner and admin	√		√	√	
OS	grid	Automatic Storage Management admin		√			
OS	oracle	Database runtime owner and admin	√	√			
OS	platcfg	Platform (TPD) configuration utility dedicated	√	√	√	√	
OS	root	Linux server administrator	√	√	√	√	PM&C
OS	syscheck	Platform (TPD) system check utility dedicated	√	√	√	√	
OS	tekelec	Management (NSP) runtime owner and admin	√				
PIC	tekelec	Built-in Application administrator	√				
PIC	TklcSrv	Built-in Application administrator	√				
PIC	<user>	Accounts to be created by an administrator	√				
SNMP	private	Network management MIB	√	√	√	√	
SNMP	public	Network management MIB	√	√	√	√	
Weblogic	console	Web server configuration console	√				

Second table shows additional accounts that are only used in configurations with HP C-Class blades.

Area	Identifier	Description	Managmnt	Storage	Mediation	Acquisition	Other
FCCont	manage	P2000/MSA2012 SAN FC controller manager					Blades
FCCont	monitor	P2000/MSA2012 SAN FC controller monitoring					Blades
FCSwitch	root	Brocade Fiber Channel SAN switch admin					Blades
ILO	root	Integrated Lights Out remote console login https, ssh	√	√	√		Blades
OA	Administrator	Onboard Administrator C7000 enclosure					Blades
OA	pmacadmin	Onboard Administrator C7000 enclosure for PM&C					Blades
OA	root	Onboard Administrator C7000 enclosure					Blades
PM&C	pmacadmin	Platform Management and Configuration UI					Blades
PM&C	pmacftpusr	Plaform Management and Configuration file transfer					Blades
PM&C	pmacop	Platform Management and Configuration UI					Blades
PM&C	pmacuser	Platform Management and Configuration UI					Blades