Predict | Protect | Prevent

ARCON

Recommendation of PAM|EPM|CIEM|MyVault Deployment v3.0

arcon

Table of Contents

1 Overview

ARCON PAM|EPM|CIEM|MyVault is designed to support large enterprise implementations with hundreds of systems and users. The application is designed to scale in a linear controlled fashion as new systems are integrated into the system. Scalability can be achieved by vertically scaling the resource cluster with the option to make use of hardware and software load balancers if required.

ⓘ Important:

The final architecture and the components will be based on the discussions with the UIDAI Infrastructure and Solution Architecture Team.

The Architecture provided below is based upon our understanding of the UIDAI requirments, general understanding of the UIDAI Infrastructure and best practices for deployement vis-a-vis the requirments and is subject to change

2 Infrastructure Architecture

The fundamental approach of the ARCON PAM Architecture is to segregate logical software components into multiple layers i.e. application layer, database layer, and secured server layer. This offers segregation of server components and flexibility to grow the architecture in the future.

- Application Server (EPAM) – functions as the initial communication point for all users
- Database Server (PVSL) –This component includes secured storage of logs, configuration & policy information, and a highly Secured Password Vault.
- Secure Gateway Server (SGS)- This method creates a secure tunnel from the user machine to the target device via. Gateway.
- **Application Gateway Server (AGW) – Application Gateway Server (AGW+) can be used as an HTML5 Streaming Gateway for sessions to be established between the end user machines to the target devices.

***Usage of this component is optional.*

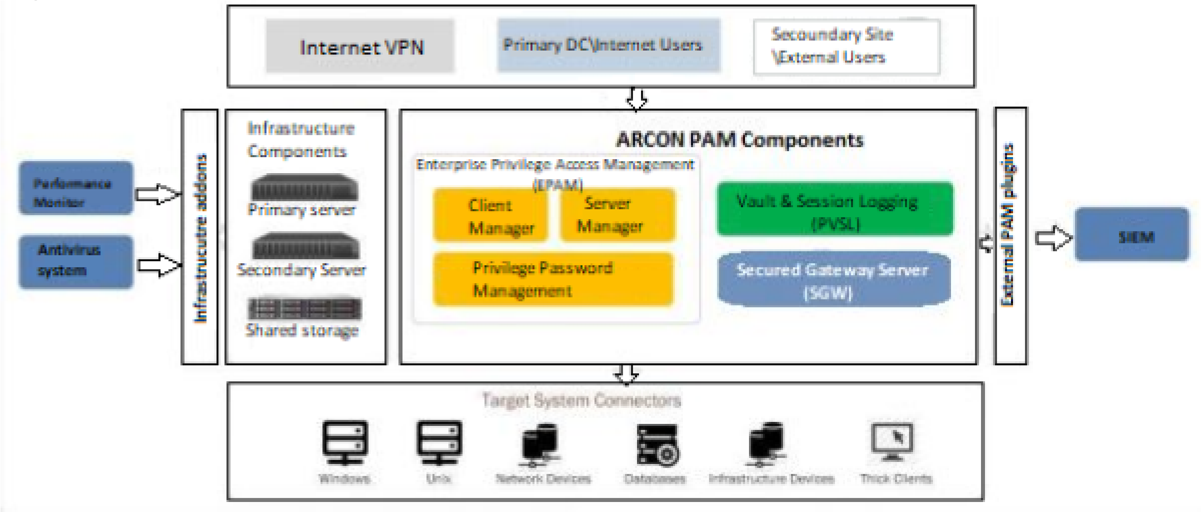


Figure1: Fig1. High Level PAM Architecture with all components.

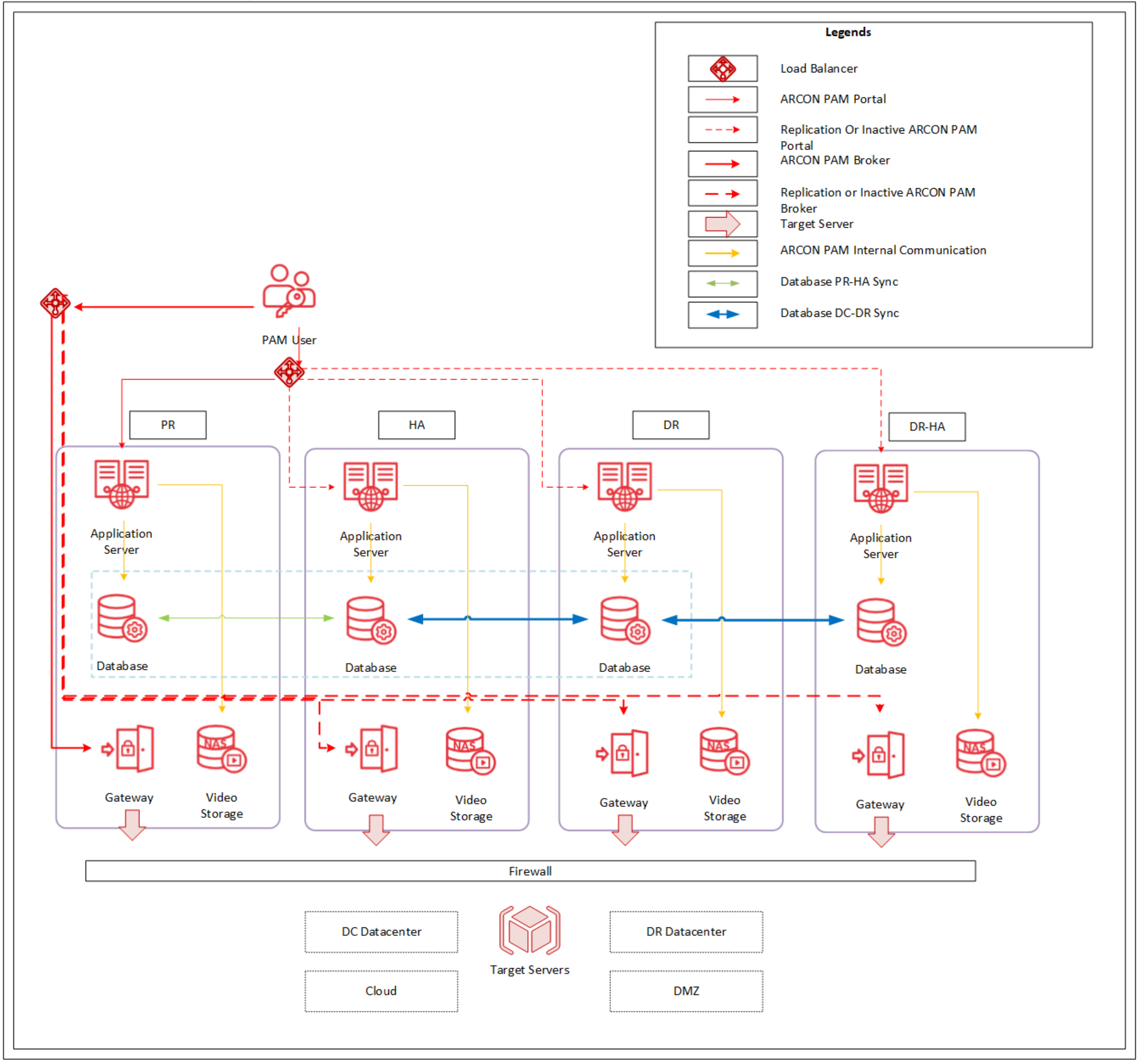
3 Recommendations

The proposed architecture configuration offers the flexibility to segregate the application servers while utilizing a central database. Organizations can linearly scale up this environment by horizontally adding more resources to the existing setup.

The architecture configuration is sized to support the requirement of **350 Users and 10,000 Devices** and the solution can be further scaled to meet the requirements of 20,000 devices and 4000 concurrent users.

4 Architecture

The proposed architecture configuration offers the flexibility to segregate the application servers while utilizing a central database. Organizations can linearly scale up this environment by horizontally adding more resources to the existing setup.



Note: Gateway included tunneling Gateway to ensure high scalability however we may also include the AGW+ gateway (Optional) depending on the use cases.

5 ARCON|PAM & CIEM Application Server

Specification	Minimum Recommended	Production	HA	DR	DR-HA
CPU Speed	2.1 GHz or Higher	1	1	1	1
Processor	Intel Xeon Processor (16 Cores)				
Memory / RAM	128 GB or higher				
Hard Disk Space	100 GB Data Drive for OS				
	500 GB Data Drive for App				
Video Log	Please ref. to ANNEXURE I Storage Requirement for Video Logs				
	*SSD or Flash drive recommended for Log Manager Process.				
Class of Storage Required	Required ISCSI or SATA				
Operating System: Windows Server 2016 standard edition or Higher					
Microsoft .Net Framework: 3.5 & 4.7.2					
ARCON PAM **Service** Recommended to configure windows cluster for arcon services to achieve automatic failover PR-HA, DR will be a manual failover.					
Recommended Layer 7 Load Balancer to Achieve High Availability					

5.1 ANNEXURE I Storage Requirements for Video Logs

Depending upon the duration of online storage, additional storage must be provided for online logs.

No of Concurrent User Sessions	3 Months Online logs	6 months Online logs	12 Months of Online Logs
50	500 GB	1 TB	2 TB
75	750 GB	1.5 TB	3 TB
100	1 TB	2 TB	4 TB
125	1.25 TB	2.5 TB	5 TB
150	1.5 TB	3 TB	6 TB
175	1.75 TB	3.5 TB	7 TB
200	2 TB	4 TB	8 TB

6 ARCON|PAM Database Server (PVSL Component)

Specification	Minimum Recommended	Production	HA	DR	DR-HA
CPU Speed	2.1 GHz or Higher	1	1	1	1
Processor	Intel Xeon Processor (24 Cores)				
Memory / RAM	256 GB or higher				
Hard Disk Space	100 GB Drive for OS				
	500GB Data Drive				
Class of Storage Required	Required ISCSI or SATA				
	Recommended Fash or SSD				
Operating System: Any Linux OS compatible with MySQL version specified below					
Supported MySQL Version 8.0.29					
Recommended MySQL Innodb Cluster for HA and Master / Slave configuration for DR.					

7 ARCON|PAM Secure Gateway Server

Specification	Minimum Recommended	Production	HA	DR	DR-HA
CPU Speed	2.1 GHz or Higher	1	1	1	1
Processor	Intel Xeon Processor (8 Cores)				
Memory / RAM	64 GB or higher				
Hard Disk Space	100 GB Data Drive for OS				
Class of Storage Required	ISCSI or SATA				
Aprox 350 concurrent sessions.					
Operating System: Any Linux with OpenSSH.					
Recommended Load Balancer to Achieve High Availability					

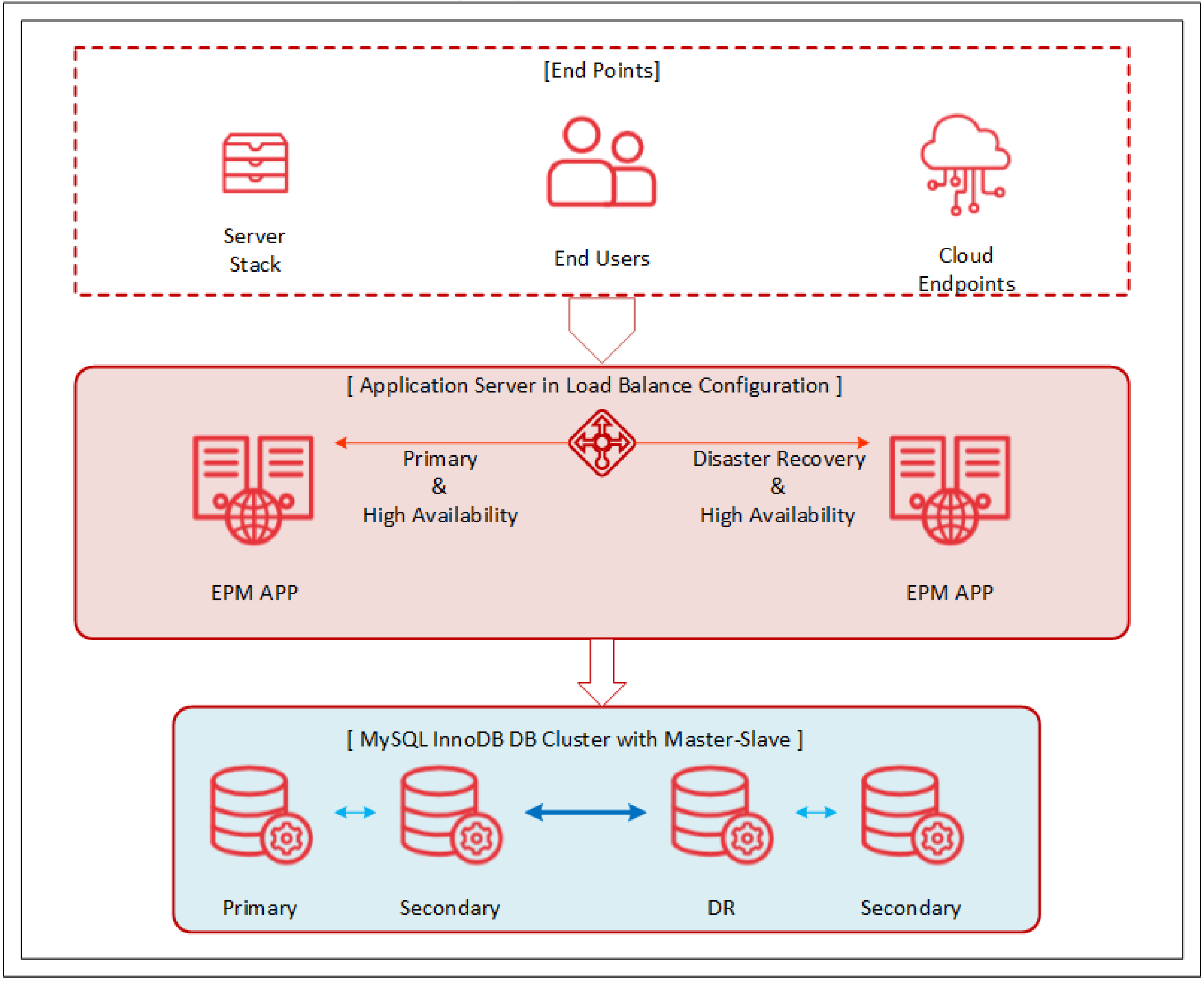
8 ARCON Gateway - AGW+ (Optional)

Specification	Minimum Recommended	Production	HA	DR	DR-HA
CPU Speed	2.5 GHz or Higher	1	1	1	1
Processor	Intel Xeon Processor (8 Cores)				
Memory / RAM	32 GB or higher				
Hard Disk Space	100 GB Data Drive for OS				
Class of Storage Required	ISCSI or SATA				
50 concurrent sessions.					
Running resource-intensive applications like Toad, vSphere Client and so on, on the AGW+ server will result in lower concurrency.					
AGW+ requires 1 RDS User MS-CAL License per server and only in case of windows-based target devices customers should already have RDS Device MS-CAL License. For more information about purchasing an RDS CAL, contact your Microsoft representative.					
Operating System: Windows Server 2016 standard edition or Higher					
Microsoft .Net Framework: 3.5 & 4.7.2					
Recommended Load Balancer to Achieve High Availability					

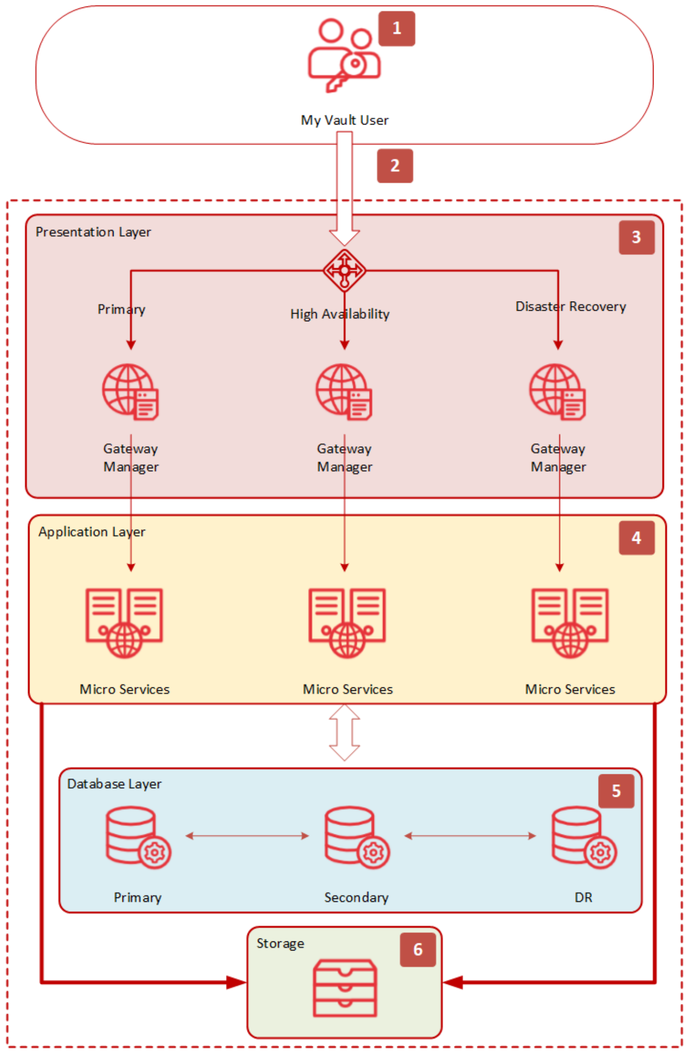
9 ARCON| EPM|MyVault

Specification	Minimum Recommended	Production	HA	DR	DR-HA
CPU Speed	2.1 GHz or Higher	1	1	1	1
Processor	Intel Xeon Processor (32 Cores)				
Memory / RAM	256 GB or higher				
Hard Disk Space	100 GB Data Drive for OS				
	500 GB Data Drive for App				
MyVault Storage	1TB Data Drive may increase upon usage				
	NAS or SAS storage can be used				
Class of Storage Required	Required ISCSI or SATA				
Operating System: Any Linux OS compatable with MySQL version specified below					
Supported MySQL Version 8.0.29					
Recommended Load Balancer to Achieve High Availability					
Recommended MySQL Master / Slave configuration for DR.					

10 EPM (Stand Alone) Deployment Architecture


[End Points]
Server Stack
End Users
Cloud Endpoints
[Application Server in Load Balance Configuration]
Primary & High Availability
Disaster Recovery & High Availability
EPM APP
EPM APP
[MySQL InnoDB DB Cluster with Master-Slave]
Primary
Secondary
DR
Secondary

11 MyVault (Stand Alone)Deployment Architecture



1 My Vault HTTPS Secure URL should be accessable from the end users system.

2 Firewall for My Vault should be allowed on Port 443

3 Presentation Layer needs to be hosted at the **internet facing Subnet** or **Outside DMZ**. This layer can have a Load Balancer configured for **High Availability**

4 **Gateway Manager** from the Presentation Layer will submit the request to the **micro services** residing in the application layer

5 Database should be configured with **MySQL InnoDB Cluster** to achieve High Availability.

6 NAS Storage should be used to save the Uploaded files.

12 Supported High Availability & DR Strategy

ARCON PAM SUITE	High Availability	DR
Application Layer	Load Balancing	VM Motion
	Windows Clustering	
	Windows NLB	
	VM Motion	
Database Layer	MySQL Clustering	MySQL (Master-Slave)
	VM Motion	VM Motion
Application Gateway Layer	Load Balancing	VM Motion

13 ARCON PAM Additional Requirements

13.1 SMTP Configuration Details

- SMTP relay permission required from PAM Server
- SMTP Server: Server DNS/IP of SMTP Server
- SMTP Port: Port number of SMTP Server (Port must be open from PAM Servers)
- Mail from: Sender Email ID
- User Name / Password: User name / Password for the mail ID mentioned in mail from (if applicable as per SMTP configuration)
- Certificate: (if applicable)
- Proxy Setting: (if applicable)

14 Recommended specification to Virtual Deployments

- Systems virtualization is greatly becoming an efficient way of consolidating and managing enterprise infrastructure. ARCON PAM fully endorses virtualization of the application server layer as long as adequate memory and resource allocation configurations are taken into consideration.
- Another consideration is that Virtual Machines (VMs) often run in a shared host. Because of this shared host environment, adequate resource allocation and management is needed to maintain a stable virtual environment. These resources can be everything from network access, to disk space, to memory, to CPU cycles. Providing a stable environment with adequate resources will ARCON PAM to run without conflict.
- Solution can be hosted on VMware, KVM & MS Hypervisor.

15 High Level Port Requirements

Source Device	Destination Device	Port	Protocol	Description	Unidirectional / Bi directional
End User	MyVault	443	HTTPS Port	MyVault On-premise	Unidirectional
EPM Server	Domain Controller (AD)	389	LDAP Port	AD Authentication	Unidirectional
User Zone	EPM Dashboard Server (Intranet)	443	HTTPS Port	EPM On-premise	Unidirectional
	EPM authentication Server	443	HTTPS Port	To open an access channel through EPM	Unidirectional
	EPM Dashboard Server (Public IP)	443	HTTPS Port	EPM Over Internet	Unidirectional
EPM Server	EPM authentication Server	443	HTTPS Port	Client Server communication	Unidirectional
EPM Server	EPM Database Server	3306	Database Port	Client Server communication	Unidirectional
ARCON PAM Administrator	PAM Servers / Load Balancer IP, ARCON Database Server	443, 8444, 3306(DB)	Database Port and HTTPS Port HTTPS Port (View Video Logs)	ClientManager Online, API and DB	Unidirectional
ARCON PAM Administrator (View Video Logs)	PAM Servers / Load Balancer IP	8442, 3306(DB)	Database Port and HTTPS Port	LogViewerWeb and DB	Unidirectional
ARCON Users/ Admin	ARCON Secured Gateway Server	22	SSH Port	Secure Gateway Server (SGS)	Unidirectional
ARCON Users/ Admin	ARCON PAM Gateway	1433	HTTPS Port	ARCON Gateway Server	Unidirectional

Source Device	Destination Device	Port	Protocol	Description	Unidirectional / Bi directional
ARCON Secured Server (Gateway)	Windows Servers / AD	45045	Custom	Winvaulting Installed on target device Port for Password Change.(Used by ARCON Password change service for Local Accounts) Or AD if the users are AD users	Unidirectional
ARCON Secured Server (Gateway)	Respective Target Servers/ Devices	Respective Target Servers/ Devices Ports	(Eg: For Windows - 3389, Linux - 22, Web Browsers - 443/8080 and so on)	Respective Target Servers/ Devices Ports	Unidirectional
ARCON Application Server (AGW)	Respective Target Servers/ Devices	Respective Target Servers/ Devices Ports	(Eg: For Windows - 3389, Linux - 22, Web Browsers - 443/8080 and so on)	Respective Target Servers/ Devices Ports	Unidirectional
ARCON Application Server	LDAP	389	LDAP Port	AD Authentication	Unidirectional
ARCON Application Server	LDAP SSL	636	LDAP Port	AD Authentication	Unidirectional
ARCON Application Server	ARCON Database Server	1450	DB Port	For ARCON Application to Connect to ARCON Database.	Unidirectional
ARCON JOB Server (Alert Service Installed Server)	Mail Server	25 for SMTP 456 for SMTP SSL 143 for IMAP 993 for IMAP	IMAP/ SMTP	relay is required to send the alerts from Alert Service Server to the designated email id	Unidirectional

Source Device	Destination Device	Port	Protocol	Description	Unidirectional / Bi directional
Audit Team	Spection	8447	HTTPS	Reporting Tool	Unidirectional
Audit Team	Knight Analytics	8446	HTTPS	Analytics Tool	Unidirectional
ARCON PAM Services	ARCON DB Server	1450	DB Port	All ARCON PAM Services require access to Database	Unidirectional
APP Server	2FA Server	Respective Port Number e.g. for RSA 1812, 1813	2FA Port number for authentification	If the 2FA is enabled the respective port has to be opened	Unidirectional
AGW Server	API Server	8443	Https	For log transfer	Unidirectional
Staging Server	DB Server	1450	DB Port	Staging Service to access DB	Unidirectional
Staging Server	APP Server	443	HTTPs	Web Service API access	

- Port can be customized while implementation however we recommend to use defined ports.

15.1 Password Ports

	Source	Destination	Port	Protocol	Description	Unidirectional / Bidirectional
Centralized Password Change	Schedule Password change Service	WinVaulting Service (Run As Domain Operator Privilidges)	45045	Custom	ARCOS Central Password Change Service	Unidirectional
	WinVaulting Service (Run As Domain Operator Privilidges)	Windows Servers(added in Domain)	88	Kerberos	User and Computer Authentication, Forest Level Trusts	Unidirectional
			135	RPC – Cert	RPC	Unidirectional
			53	DNS	User and Computer Authentication, Name Resolution, Trusts	Unidirectional
		LDAP	389	LDAP	LDAP Port	Unidirectional

	Source	Destination	Port	Protocol	Description	Unidirectional / Bidirectional
Centralized Password Change via. Secure Gateway	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway	Unidirectional
	Secure Gateway	WinVaulting Service (Run As Domain Operator Privilidges)	45045	Custom	ARCOS Central Password Change Service	Unidirectional
	WinVaulting Service (Run As Domain Operator Privilidges)	Windows Servers(added in Domain)	88	Kerberos	User and Computer Authentication, Forest Level Trusts	Unidirectional
			135	RPC – Cert	RPC	Unidirectional
			53	DNS	User and Computer Authentication, Name Resolution, Trusts	Unidirectional
		LDAP	389	LDAP	LDAP Port	Unidirectional
Windows Domain Account	Schedule Password change Service	Windows Servers(added in Domain)	139, 445	NetBIOS Services	Name Resolution Service	Unidirectional
			88	Kerberos	User and Computer Authentication, Forest Level Trusts	Unidirectional
			53	DNS	User and Computer Authentication, Name Resolution, Trusts	Unidirectional
Windows Domain Account	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway	Unidirectional
	Secure Gateway	Windows Servers(added in Domain)	139, 445	NetBIOS Services	Name Resolution Service	Unidirectional

	Source	Destination	Port	Protocol	Description	Unidirectional / Bidirectional
			88	Kerberos	User and Computer Authentication, Forest Level Trusts	Unidirectional
			53	DNS	User and Computer Authentication, Name Resolution, Trusts	Unidirectional
Windows Domain Account via LDAP (AD)	Schedule Password change Service	Windows Servers(added in Domain)	139, 445	NetBIOS Service	Datagram Services (Browsing)	Unidirectional
			88	Kerberos	User and Computer Authentication, Forest Level Trusts	Unidirectional
			53	DNS	User and Computer Authentication, Name Resolution, Trusts	Unidirectional
		LDAP	389	LDAP	LDAP Port	Unidirectional
Windows Domain Account via LDAP (AD)	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway	Unidirectional
	Secure Gateway	Windows Servers(added in Domain)	139, 445	NetBIOS Service	Datagram Services (Browsing)	Unidirectional
			88	Kerberos	User and Computer Authentication, Forest Level Trusts	Unidirectional
			53	DNS	User and Computer Authentication, Name Resolution, Trusts	Unidirectional
		LDAP	389	LDAP	LDAP Port	Unidirectional

	Source	Destination	Port	Protocol	Description	Unidirectional / Bidirectional
Windows Local Acount	Schedule Password change Service	Windows Servers(added in Workgroup)	139, 445	NetBIOS Services	Session Service (net use)	Unidirectional
Linux/ Unix/ Network Devices	Schedule Password change Service	Target Devices	22, 23	SSH/ Telnet	SSH or Telnet Port	Unidirectional
Linux/ Unix/ Network Devices	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway	Unidirectional
	Secure Gateway	Target Devices	22, 23	SSH/ Telnet	SSH or Telnet Port	Unidirectional
Windows Services / COM Plus	Schedule Password change Service	Windows Servers	135, 445	NetBIOS Services	Session Service (net use)	Unidirectional
Windows Schedule Task, IIS APP Pools	Schedule Password change Service	Windows Servers	135, 445, 45045	NetBIOS Services, Custom	Session Service (net use)	Unidirectional
Windows Services / COM Plus	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway	Unidirectional
	Secure Gateway	Windows Servers	135, 445	NetBIOS Services	Session Service (net use)	Unidirectional
Windows Schedule Task, IIS APP Pools	Schedule Password change Service	Secure Gateway	22	SSH	Secure Gateway	Unidirectional
	Secure Gateway	Windows Servers	135, 445, 45045	NetBIOS Services, Custom	Session Service (net use)	Unidirectional

Privileged Access Management Suite

arcon

Predict | Protect | Prevent