Predict | Protect | Prevent

ARCON|PAM

Secure Vault

www.arconnet.com |

arcon

Table of Contents

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate a better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.

Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Copyright Notice

ARCON retains the right to make changes to this document at any time without notice. ARCON makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Sales Contact

You can directly contact us with sales-related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Overview

Information Technology today is at the core of every organisation's operations and sometimes the success of the organisation is determined by how well the organisation is able to adapt the changing technology landscape. Digital revolution has added an extra layer of technology which helps organisations meet business objectives in a more efficient manner and some of these digital technologies are disrupting and re-visualising the delivery channels.

The technology disruption also brings with it the challenges of privacy and data security which today carry a high reputation risk for organisations and eventually the survival of businesses are determined by how one is able to effectively use technology with adequate controls.

Identity management has been at the core of technology usage considering that there are now hundreds of applications and systems that one uses in their day to day operations and this gets further complex with the interconnected technologies talking to each other. While identity management is an issue there are even more complex issues surrounding the Privilege Identity Management. Privilege Identities are those which hold the keys to the applications and systems and have access to literally the heart of the various technologies.

ARCON|PAM is a Privilege Access Management Solution designed to address the challenges of privilege identities and provides an added layer of security to help build in controls that ensure access only on "need to know" and "need to do" basis. The PAM solution has several components however the major components are Single Sign-On, Password Management, Access Control, Vault and Session Monitoring.

This document contains the built-in security features of the ARCON|Vault.

2 ARCON Vault

ARCON|PAM has a major component which is called the "ARCON|Vault" and as the term suggest stores critical information such as privileged account passwords, access control policies, configuration data and audit/ session information. ARCON|PAM follows certain in-built security standards to protect the vault and can be categorised as:

- Access to Vault
- Vault Processors
- Data at Rest
- Data in Transit
- Vault Hardening
- Fire-walling the systems

ARCON also suggests that best practices in access management should be followed to ensure that only authorized users have access to the vault.

2.1 Access To Vault

ARCON|PAM provides granular user access rights (segregation of duties) and these should be appropriately set to ensure that access to Vault especially the "passwords" should highly restrictive. There should be limited set of users who can request for "password" release and approval. Users can request for only unique passwords at one time. Further it is suggested that two eyes principle should be used to check-out any passwords.

2.2 Vault Processors

ARCON ensures enhanced performance and scalability for rotation and reconciliation for various types of customers with the help of Vault Processors. Varying the number of Vault Processors, password rotation and reconciliation can be made highly scalable and top-notch. Here is the performance metrics for each depending on the number of Vault Processors used.

Number of Vault Processors	Password Rotation Performance(including re-validation and re-logging procedure)	Password Reconciliation Performance
Single	3 secs per password (20 passwords per minute)	2 secs per password (30 passwords per minute)
20	400 passwords per minute	600 passwords per minute

NOTE :

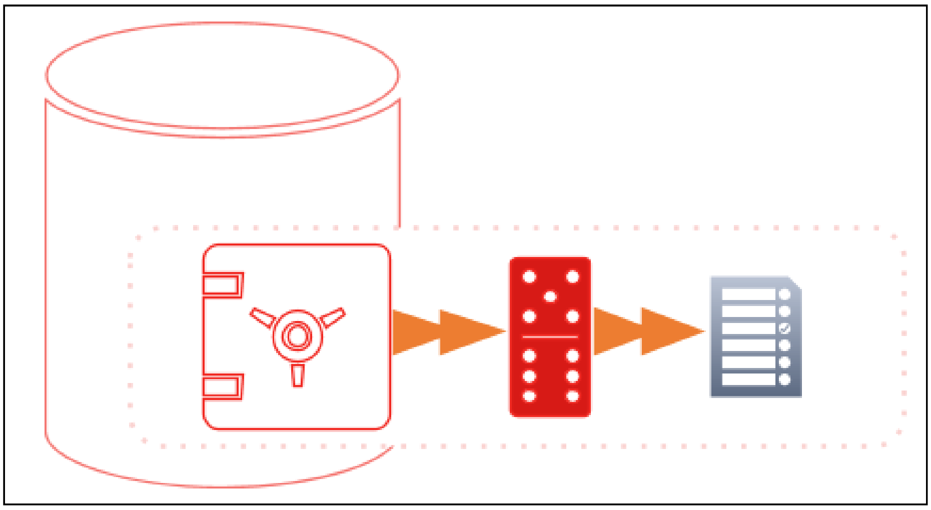
1. From the above metrics, we can thus deduce that, for instance, for 50,000 passwords can be changed in approx 2 hours with the help of 20 vault processors.
2. Use Case: If a company has 10,000 passwords/target servers to be rotated on average, we generally recommend 4 Vault Processors as the minimum requirement for supporting their infrastructure.
3. The Vault processors also provide a feature to enable multi threading. This could further scale up the password change process.Generally multi threading is recommended to be set around 25-50. One can make an optimum use of multiple vault processors in combination with multithreading settings to achieve desired scale of enhanced password rotation performance.

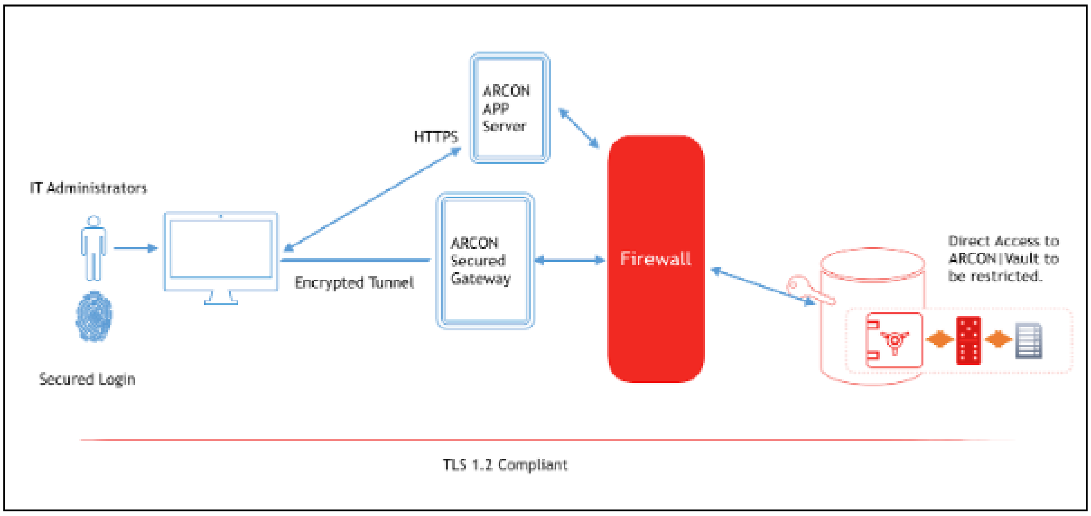
2.3 Data at Rest

ARCON|Vault as described above holds critical information, the Vault sits deep within the database. The Vault in not a single component i.e it has multiple components which interact internally and all such components are scrambled this dramatically reduces the attack vector as all the components have to be compromised to create a single view. The data within all these components/objects are encrypted using FIPS 140-2 compliant encryption. ARCON|Vault uses a layered encryption approach infact there are two levels of encryption for critical elements. At the first level, ARCON|Vault uses AES-256 symmetric algorithm and at level two ARCON users its proprietary encryption algorithm.

2.4 Data in Transit

ARCON|Vault encrypts all critical data in transit. The Vault uses TLS1.2 compliant communication layer between systems. This is further enhanced as the data flow between the end devices is through the proprietary encrypted tunnel up to the Secured Gateway or on HTTPS. The methodology adopted significantly reduces the attack vector especially around the wiretapping or packet sniffing over the network. While an attacker inside the network may be able to see traffic between systems, however data will be indecipherable and thus useless.





2.5 Vault Hardening

ARCON|Vault is installed on a server and as such it is important that all such machines/systems are hardened using best practices. ARCON|PAM is built to work on CIS hardening benchmarks without compromising the PAM's functionality. These CIS benchmarks are applied during the installation of the systems on the all the components of ARCON|PAM including operating systems, databases and gateways servers. While these guidelines are strongly recommended and adopted, some organisations use specific hardening guidelines, ARCON|PAM is built to generally work with least privileges and limited OS services etc.

In fact, it is critical that all systems hosting components of ARCON|PAM are hardened as much as possible to reduce its attack surface.

2.6 Fire-walling the Systems

ARCON|Vault hardening will lock down the server OS as well as the Database, however the Vault server can be further locked down by restricting the traffic to and from the Vault Server. ARCON|Vault leverages the host machine's built-in Windows Firewall to restrict traffic only on certain ports required by the software and block all other traffic.

The Vault Server is further placed behind the organisations corporate firewall and behind the ARCON|Secured Gateway this ensures that only ARCON systems talk to each other and no end-device can directly access the Vault.

It is further expected that organisation use the least access privilege standards and ensure adequate segregation of duties between the ARCON|PAM administrator for the application and the administrators for the ARCON components or systems. The Vault Server and Database is also managed by ARCON|PAM thus ensuring that every change is also monitored.

2.7 Improvised Password Process

The improvised password process consists of the following steps:
1. Log on into the system and check if the user is present and what was the last password change date
2. Password change
3. Validation of new password by login into the system,

> **Step 3** normally takes more than 70% of the total time of the Password change process. If the validation was avoided then the time taken for password change per second will be reduced to 1/3rd. This can be achieved by configuration of validation as OFF, which could be very useful for password change at super scale during times of cyber attack etc.

1. Single Server - 50000 Password Changes with Validation.
Validation includes logging in to the system and confirming that the password is correct. The test conducted was 1 worker 0 subprocesses and 1 worker with 10 subprocesses. The results of the test are below

A process running in parallel per machine	Password Change Assigned to each Process	Total Password changed	Password Change Failed	Post password change Validation	Total Time Taken in Sec	Effective Seconds per Password Change
1	2500	2500	3	Yes	2207	0.88
10	250	2500	64	Yes	1200	0.48

Now in order to further test for 50000 passwords on a single server, with 1 worker and 10 subprocesses, Please find the table below:

IF DONE ON A SINGLE MACHINE (LOOPING OVER MULTIPLE TIMES)							
A process running in parallel per machine	Password Change Assigned to each Process	No of Loops	Total Password Changed	Post password change Validation	Total Time per Loop	Total Time Taken in seconds	Effective Seconds per Password Change
10	250	20	50000	Yes	1200	24000	0.48

Please find Log File Reference

2. Assuming that the 50,000 passwords are distributed on 20 servers, the following is the result.

A process running in parallel per machine	Password Change Assigned to each Process	No of Machines fired in parallel	Total Password Changed	Post password change Validation	Total Time Taken in Sec	Effective Seconds per Password Change
10	250	20	50000	Yes	1200	0.02400

Privileged Access Management Suite

arcon

Predict | Protect | Prevent