Arcus

System Administrator's Manual

Date: 27 AUG 2020

Prepared by:

Jackpine Technologies Corporation

On behalf of

xxxxxxxxxx

Table of Contents

Document Control

Version	Date Released	Description of Change	Pages Affected	Changes Made By
1.0	July 2013	Draft Release	All	Peter Walsh
2.0	September 2015	Overhaul for addition incident management	All	Peter Walsh
2.1	November 2015	Edits based on accreditation feedback	All	Ray Smith
3.0	January 2016	Sync with DISA CEMS CONOPS	All	Peter Walsh
4.0	January 2017	Updates for RMF conversion	All	Ray Smith
4.1	October 2017	Add section on system accounts and decomm steps	All	Peter Walsh
5.0	March 2020	Transition HmC to Arcus	All	Ray Smith
5.1	September 2020	Adapt to xxxxxxxxx	All	Ray Smith

1. Overview

This document describes system administration measures taken to configure and secure application and infrastructure hosts, networks and operating systems.

2. Policy

All policies will be reviewed no less than annually and updated as necessary. Please see overarching policy maintenance document “Arcus Policy Management”. A change control log should be included at the top of each policy document.

RMF controls will be assessed continually over the course of the year so any configuration change that affects a control becomes part of the package. The package is considered a living document that is continually improved and always ready for submission.

Roles

The roles responsible for updating and writing policy include:

- System Administrator Lead
- Program Manager
- Engineering Manager
- Government PM
- Test Lead
- Cyber Security Manager
- Operations Manager

Each applicable area of expertise contributes to ensure policy is effectively written and reviewed. Current assignments of individuals to roles are listed in Appendix 1.

3. Accounts

Every system administrator has an unprivileged account to gain access to the network. Two factor authentication is enabled with ssh key enforced to enter into the access point. Every trusted user comes in as him or herself, on infrastructure systems using unprivileged individual LDAP accounts. Users can then elevate privileges using (sudo) on linux boxes or runas on windows. This allows traceability between people and events on the systems.

Users will automatically be logged out of all systems after 600 seconds of inactivity. Accounts will be locked for 15 minutes after three bad passwords. Passwords are required to be reset every 30 days.

System Accounts

The use of system accounts is limited to only when necessary for automation and monitoring. All infrastructure system accounts are part of the LDAP managed authentication and authorization process with the same policies applied. No system accounts are allowed external ssh access. Whenever supported by the target application, system accounts will use a token/secret key for authentication. In the event of a change in personnel, ALL system account passwords and tokens are reset.

4. Security & Management Stack

Below represents security measures maintained by the Arcus team in order to ensure Arcus remains secure and performant at all times. Standard configuration a for all external and internal network security appliance:

1. **Network Security Appliances** - The external facing network security appliance is the single entry and egress point into Arcus (fully redundant) so it is a critical point of focus for security and system administration. The second layer involves network security appliances in front of each cloud resource pool. These communicate over a backbone network that includes the security stack for monitoring, detection and prevention.
2. **Firewall** - Boundary protection is critically important to protecting any enclave of systems. Arcus is no different although more firewalls come into play when dealing with cloud spaces because each space becomes an enclave with its own boundary. Arcus layers firewalls so they are active on each host and then secure each boundary to protect the network that those hosts reside on. Every firewall ruleset is built with the philosophy of deny all/permit by exception. Each cloudspace (public or private) is also fronted by an edge device/firewall. The ports and protocols required by CONS3RT in and out of any enclave are well documented in the Arcus Network Diagram.
3. **DoS and Fail2Ban -** Denial of service "is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled." DoS is a very real threat and can sometimes happen inadvertently with the same net effect of rendering machines unavailable by flooding them with traffic. To that end Fail2Ban is implemented on all hosts. Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show signs of malicious intent -- too many password failures, probing for exploits, etc. Fail2Ban is then used to update firewall rules to reject the IP addresses for 60 minutes. Fail2Ban provides a core (simple but effective) Network Protection System (NPS) for Arcus.
4. **Routing and NAT** are used to obfuscate internal networks as well as protect sensitive traffic by keeping it from being exposed at all to the Internet. Arcus uses a two-tiered network approach, one external firewall router guards the single point of entry. Behind that, each production enclave is fronted by an internal router/firewall pair so adversaries would need to penetrate security stack and then a second router/firewall to gain access to internal networks where they would then confront local firewalls described in 4.2.1, tcp-wrappers, LDAP, etc.
5. **IDS** - Intrusion Detection Systems capability in Arcus proper is handled by a combination of AlienVault and Elastic Stack. This part of the security stack basically monitors all incoming traffic and inspects it based on a rule set. The IDS actually works in concert with the network protection system so administrators not only gain visibility of what's happening but also are able to defend real time. All data is persisted locally (or archived on network attached storage) in case any forensics are required after the fact. Additional IDS services are inherited from the upstream HCIC Cyber Security team and DREN Network Operations Center (NOC).
6. **SIEM** - Security information and event management provides real-time analysis of security alerts generated by network hardware and applications. The Arcus security stack includes AlienVault for SIEM with an active subscription to the Open Threat Exchange (OTX). OTX delivers crowd sourced threat data, enables collaborative research, and automates the process of updating the security infrastructure with threat data.
7. **DNS** - Domain name service is provided for milcloud to the hanscom.hpc.mil subdomain. A split view is used to serve out the Arcus domain to customers. Internal views are used to manage all hosts inside the DREN facing network security appliance. A production enclave is in place for each Arcus cloud as well as the CONS3RT infrastructure systems. Each of these DNS zones is fronted by an internal network security appliance that handles lookups and forwarding back up to the external facing network security appliance.
8. **LDAP** – Centralized directory control of user accounts, passwords and permissions.

9. **NTP** – Time services fed (currently ntp.dren.mil) are made available at the network security appliance layer.
10. **Nessus -** Automated scans are the cornerstone of maintaining a security posture. Automated Nessus scans are run weekly with reports published in an easy to use format so the system administration team can review them during the weekly planning meeting, create task tracker issues and then mitigate vulnerabilities.
11. **Monit** - Monit is used to ensure services are available and resources are in good shape. Monit will watch configured thresholds and configurations and if exceeded (e.g. if a file system fills up) or violated, an alert will be sent to the production monitoring channel in the team messaging center.
12. **AntiVirus** - Virus scanning, patching & system updates are an integral part of maintenance windows. Keeping systems up to date is the front line of defense as most exploited vulnerabilities are older findings that have not been patched or addressed for whatever reason. Virus definitions are updated bi-weekly as part of standard maintenance window.
13. **Proxy** - A proxy server using blacklist http://urlblacklist.com prevents traffic to designated sites.
14. **Crypto key management** - Keys are checked into a secure repository and made available to project members as necessary for maintaining systems. The automated installation process can also pull them out of the repo.
15. **Bitwarden** – A secure encrypted vault is used to house any administrative, vendor account or sensitive passwords that need to be shared for any reason. Collections and permissions are used to minimize exposure to only the individuals who absolutely require it.

5. System Configuration Guidelines

Application

CONS3RT is unique in that it offers a method to maintain system designs i.e. configuration-managed baselines that can be deployed into attached cloud spaces on demand. It can literally use itself to deploy itself because the baseline is maintained as part of the project. The location of the cons3rt specific baseline can be found at: https://app.cons3rt.com/#/software/3354/overview.

The following additional steps are applied to specific systems:

Toolbox/Evergreen

- TCP wrappers restricting management access from the router only

CONS3RT Infrastructure

- TCP wrappers restricting management access from toolbox / evergreen only
- Access Control Lists (ACLs) on all services limited to approved and registered clouds

Infrastructure

The standard configuration for any infrastructure system includes the following items:

- Configure LDAP to manage unprivileged accounts; users must sudo to elevate privileges when necessary.
- Disable root/administrator login (permitted during implementation; disabled prior to going live)
- Install Fail2Ban
- Configure firewall (iptables or Windows Firewall) [deny all/permit as needed]
- Configure tcp-wrappers

- Set SE Linux to targeted & enforcing
- Install monit agent
- SSH Configuration (See Appendix 2 for details)

- Install Anti Virus (ClamAV on Linux, Windows Security Essential on Windows)
- Automate sleep state of Windows admin systems when not in use
- Configure NTP for local time servers (network security appliances)

- The following command is run (on linux) systems to ensure memory protection is properly configured (result should be 2):

```
cat /proc/sys/kernel/randomize_va_space
```

- Any implementation that requires encryption, FIPS approved algorithm will be used. Note that even though SHA-1 is on the FIPS list, it is **not** approved for use in Arcus. Preferred defaults are AES256 and SHA 256.

6. Maintenance

Arcus maintenance includes the communication of major events such as planned or unplanned outages and Authorized Service Interruptions (ASIs), to Arcus users. Planned outages and ASIs may include Arcus maintenance, upgrades, patch updates and/or configuration changes. The process for handling planned and unplanned outages described here pertain to Arcus as it is currently hosted inside the AFLCMC/HNID HCIC. The HCIC is responsible for the maintenance of all facility infrastructure level capabilities – physical security, power, cooling, and network connectivity. The Arcus Ops Team is responsible for all application and infrastructure level updates to production systems.

Planned Arcus outages will provide users with at least a seven-day notice; emergency upgrades and releases should provide users with a twenty-four hour notice. Once the team approves an ASI, the Arcus System Administration Team executes the ASI in the approved window. Unless the downtime is of a critical nature, the maintenance window is scheduled for off-peak hours, typically late in the evening or on the weekend.

Once the maintenance window is determined, Arcus system administrators alert users of the upcoming event by posting a message on the Arcus main page and via an opt-out email list. The system is then brought down at the designated time. In the event that the system goes down unexpectedly, Arcus administrators are immediately alerted by the external management system. Should Arcus experience unexpected downtime, system administrators will post customizable error messages to any systems that may remain online, including the Arcus homepage and/or news pages alerting users that the system is down or degraded.

Arcus maintenance windows are set for every other week, lagging the release of a new version by approximately five business days.

Infrastructure changes are proposed at the weekly System Administration team planning meeting and require concurrence from the team and approval from the Operations Manager and Program Manager. Task trackers are created for approved changes to manage and monitor the implementation.

Backups

The core data for the application will be backed up according to the process in Table 6. Backups are automated via application utilities or management scripts. Backups are ultimately moved offsite to support disaster recovery.

Table 6: Backup Schedule

Data	Hourly	Dail	Weekly	Monthly
Database	local	local	local	offsite
Asset Library	-	local	local	offsite
Deployment Run Data	-	local	local	offsite

For infrastructure, configurations will be stored in the help-desk repo (which is also backed up and offsite) for access control and configuration management.

7. Management Access

Protection

An IP based whitelist is in place to enforce approved connections allowed into the management access point. List is generated from active LDAP users every hour and on demand if person leaves the approved group.

Connections

Since ssh is used for management access systems remotely, a global known_host key file is distributed amongst systems that contains the approved key files. Each client is set to enforce the use of that file to determine if the server side key is valid. If there is a mismatch, the user is forced validate the known_hosts file. The presence of the alerts adds an extra precaution against man in the middle type attacks such as DNS hijacking.

A passphrase is required on all keys which provides a two factor key based authentication so passphrase and key exchange required to gain access to any external gateways. No static authenticators such as password files are allowed in any instance for management access.

Equipment

All work performed in support of Arcus will either use a) company issued equipment configured & locked down in accordance with the list below or b) government issued workstation locked down in accordance with DoD standards.

Only approved laptop devices are allowed on the DREN network. No personal devices of any type are allowed into the secure datacenters where all infrastructure equipment is housed.

The following practices are required to be followed on all company issued laptop(s) and workstation(s):

- enable full disk encryption (e.g. on Mac OS, FileVault)
- enable firewall
- DoD compliant passwords
- do not enable auto login or login without a password
- require password to wake from sleep and/or screen saver
- application sandbox controls set to enforce

- set auto logout
- enable auto updates on OS
- enable auto updates on key apps
- apply application security updates regularly (key apps with regular vulnerabilities inc. Java, Adobe products, Silverlight, MS Office, browsers)
- regular backups are enabled
- enable junk mail/spam filtering

The requirements apply to the primary operating system and all local virtual machines.

8. Acquisition

Software

Performed through approved channels to combat counterfeiting and malicious code insertion. All vendor software must be professionally supported through a legitimate approved company. Open source software will be professionally supported either by paid subscription to a company or via donation/relationship with a foundation (Apache for example), with full access to source code. These rules apply to all third party software components and code libraries.

Integrity checks are used to verify third party software during download, usage and installation. Hashes get pulled down from vendors for example GPG Keys from Red Hat. Most companies sign their software using a key. That key when available is incorporated into the upgrade and system maintenance processes used in the biweekly maintenance window.

Hardware

Hardware is acquired through verifiable channels, either a) DoD vendors or b) known vendors with strong anti-counterfeit and security policies. All hardware systems will be validated for integrity (firmware check, disk wiped) before being connected to the network or placed into production. System Administration team maintains a list of suppliers with known issues in help-desk repo.

9. Incident Response

The Arcus Security & Incident Management Guide describes applicable best practices for responding to spillage and/or the threats described.

10. Other

Data Transfer

When extremely large amounts of data need to come into the environments and the DoD SAFE file transfer site can not be used. It may be necessary to send the customer a physical disk. The disk will be scanned before going out, scanned again when it is sent back. Once clean the data can be uploaded and/or imported (for CONS3RT assets).

Information Retention

Information retention policy all audit and system logs will be maintained for a minimum of three years. Given the low cost of storage, in practice logs are maintained for five (5) years.

Inspection

Arcus does not perform "break & inspect" traffic monitoring of any inbound or outbound traffic. Arcus prioritizes the integrity and confidentiality of all data. Furthermore, Arcus seeks to reduce the risk associated with single point of failure key storage.

Key Management

Any keys on the systems will be stored with password. The automation system will store all required passwords in a master file, encrypted with AES256 via published certificate. All passwords, including on keystores, will be rotated during each maintenance window with new randomly generated values.

Appendix 1: Policy Role Assignments

Role	POC	Email
REDACTED		

Appendix 2: SSH Config

Standard configuration of sshd on Linux systems includes:

- Connection idle timeouts
- Disable root login
- Limit login to specified groups
- Disable password login and require key
- Higher log levels
- Disable tunnels & port forwarding (on most systems not needed for admin)
- Higher level ciphers, MACs and Key Exchange
- Add DoD Banner

Configuration script (master managed in source control):

```
function config_ssh() {
    local cf="/etc/ssh/sshd_config"
    local hn=$(hostname -s | cut -d. -f1)
    set_string() {
        local setting="$1"
        local value="$2"
        cat $cf | grep "^$setting" &> /dev/null
        if [ $? -eq 0 ]; then
            sed -i "/^$setting/d" $cf
        fi
        echo "$setting $value" >> $cf
    }
    set_string ClientAliveInterval 900
    set_string ClientAliveCountMax 0
    set_string PermitRootLogin no
    set_string PasswordAuthentication yes
    set_string AllowGroups Users
    set_string LogLevel VERBOSE
    set_string GatewayPorts no
    set_string PermitTunnel no
    set_string AllowTcpForwarding no
    set_string IgnoreRhosts yes
    set_string PermitEmptyPasswords no
    set_string RhostsRSAAuthentication no
    set_string HostbasedAuthentication no
    set_string Ciphers "aes128-ctr,aes192-ctr,aes256-ctr"
    set_string MACs "hmac-sha2-256,hmac-sha2-512"
    set_string   KexAlgorithms   "ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-
hellman-group-exchange-sha256"

    if [ "$hn" == "access" ]; then
        set_string Match "Group Users"
        set_string AllowTcpForwarding yes
    fi

    if [ "$ARG" != "ssh" ]; then
            section "Configuring Banner:"
            cp $dir/template/banner.txt /etc/banner

            cat /etc/ssh/sshd_config | grep "^Banner" &> /dev/null
            if [ $? -eq 0 ]; then
                line=$(cat /etc/ssh/sshd_config | grep "^Banner")
                sed -i "s|$line|Banner /etc/banner|" /etc/ssh/sshd_config
            else
                echo "Banner /etc/banner" >> /etc/ssh/sshd_config
            fi
    fi
section "Restarting sshd"
    case $os_ver in
        6 ) service sshd restart ;;
        7 ) systemctl restart sshd ;;
        99 ) systemctl restart ssh ;;
    esac
```

```
    space
}
```