Invicro
A Konica Minolta Company

iPACS® Server Installation Requirements Guide

Original Document Release: 1 July 2020
Document Version 1.0

iPACS Server Installation Requirements Guide

Objective

Server administrators can use this guide in combination with a testing trial period to evaluate their server hardware requirements. Because server load is difficult to predict, live testing is the best way to determine what hardware an iPACS instance will require in production.

Table of Contents

iPACS Server Configuration

For versions 2.03, 2.5 and 2020 in a Docker environment.

Hardware/OS

The iPACS software runs on a wide array of hardware, depending on the number of concurrent users, amount of data and meta data stored, as well as installed and used plugins. For testing, the iPACS can be installed in small local virtual machines and scales well up to multi-server setups with dedicated application, database, and indexing servers.

iPACS Installation

Invicro does not currently support an end-user iPACS installer, which means that the installation must be done by an Invicro technician. The technician will require root/sudo level access to perform the installation.

Minimum Hardware Requirement

Invicro suggests **minimum** server requirements consisting of a QuadCore CPU (e.g. Xeon E5504 2.0 GHz), 16-32 GB RAM (ECC), 1 GBit network. The system makes heavy use of multiple CPUs/Cores and more memory allows for greater image processing power, as well as serving a larger number of concurrent users.

Storage

The iPACS application server should have minimum 200 GB storage for the local application. NFS/Network storage can be attached to the server to provide additional storage as needed. This storage has to be POSIX compatible; Windows-based back-ends often lead to permission issues outside of the control of the iPACS.

For testing or staging systems, generally a total capacity of 500gb with a single disk will be sufficient.

Invicro will install the iPACS to /home/ipacs/<instance name>. The installer will create the user 'ipacs' and its associated home directory, and a new installation requires that the /home partition be available with enough storage for application installation (typically 500 GB is enough to accommodate index growth).

Please inform Invicro about the storage solution you have planned, in particular which SAN/NAS and protocol are to be used. If you intend to use an external storage solution for the iPACS install, it is possible to have this automount to the /home directory.

Disk Redundancy

It is highly recommended to provide storage with sufficient redundancy layers to cope with hard drive or storage node failures. For local storage (application files, database and indices) we recommend RAID 10 for improved read performance and RAID 6 for the actual data storage for a good compromise between storage space and redundancy.

Antivirus

Please inform Invicro iPACS team if on-site IT is responsible for antivirus installation or if you would like ClamAV installed on the server during the iPACS installation procedure.

Remote Access

To service the iPACS system, Invicro prefers to establish a VPN (based on OpenVPN) connection that allows technicians to connect to the system remotely. Once configured, the local host initiates the connection, meaning the customer keeps full control of when Invicro technicians are able to access the system. The VPN requires an outgoing connection to Port 443 (HTTPS) of Invicro's VPN server, either directly or via a HTTP or SOCKS proxy; Invicro can also arrange for one-time access using the on-site technician's computer over a Zoom (or similar screen sharing tool) session.

AWS Deployments

Invicro **minimum** requirements are using the latest CentOS 7 (HVM) marketplace image on an m5.xlarge EC2 instance.

AWS Instance: m5.xlarge

Features:

- Up to 3.1 GHz Intel Xeon® Platinum 8175 processors with new Intel Advanced Vector Extension (AVX-512) instruction set vCPU: 4
- Memory (GiB): 16
- Requires HVM AMIs that include drivers for ENA and NVMe
- Powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor EBS optimized Instance physically attached to the host server EBS Bandwidth (Mbps): Up to 3,500
- Network Bandwidth (Gpbs): Up to 10

Invicro recommend requirements are using the latest CentOS 7 (HVM) marketplace image on an m5.2xlarge instance.

AWS Instance m5.2xlarge

Features:

- Up to 3.1 GHz Intel Xeon® Platinum 8175 processors with new Intel Advanced Vector Extension (AVX-512) instruction set vCPU: 8
- Memory (GiB): 32
- Requires HVM AMIs that include drivers for ENA and NVMe
- Powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor
- EBS optimized Instance physically attached to the host server EBS Bandwidth (Mbps): Up to 3,500
- Network Bandwidth (Gpbs): Up to 10

Backup and Archiving

For customer hosted iPACS servers, data safety will be the responsibility of the customer. For AWS installs, it is recommended to take daily snapshots of the iPACS volumes. The iPACS can also back up the contents of the iPACS install directory (/home/ipacs/<instance-name>) to S3 - this contains the browser and webdisk data as well as various configuration and log files.

Depending on data retention needs, is generally recommended to back up the iPACS installation directory at /home/ipacs/<instance-name>, as this contains the browser and webdisk data, as well as various configuration files and logs.

SELinux

Set to permissive or disabled. The installation utility will configure this automatically if root/sudo access is provided.

Network

iPACS uses standard HTTP/HTTPS (80/443) ports but can be configured to run over non-standard ports. Invicro highly recommends installing a TLS certificate for encryption and server authentication. The iPACS Sync client connects via the ssh protocol (fully encrypted) over the default port 22 (but can be configured to use other ports).

Please provide details and user credentials to any proxy required to access Invicro’s iPACS installation server (Invicro.com).

IPTables

Allow ssh (tcp/22), http (tcp/80) and https (tcp/443) or as required.

FIrewalld

On RHEL/CentOS 7 and newer systems, the "firewalld" daemon will be running and preventing any outside connections to the server besides SSH by default. This service must be either configured to allow the iPACS ports (see: Network) or disabled entirely.

Database

iPACS uses MariaDB 5.5.X, an open source version of MySQL. For simplicity, MariaDB uses the same executable name as MySQL, so any reference to "MySQL" is effectively the same as "MariaDB". This must be installed and accessible per the"Dependencies" section of this document.

iPACS File System Interaction

The iPACS creates a local user named ‘ipacs’ to allow it to interact with the file system. It is recommended in most cases that the user ‘ipacs’ be created without a system password (which also disables login via password completely; the iPACS Sync client uses SSH keys for authentication and thus does not require a password), but if a password is required for security purposes it is recommended to inform the users and/or Invicro staff to prevent loss of functionality in case of an expiring password until the expired password can be reset. The creation of the required users and groups is handled by the installation utility.

Customer Action Required

- Please inform Invicro if MariaDB users require passwords.
- It is best if the MariaDB root user has no password. Please inform Invicro if MariaDB root user has password set, and, if so, create a MariaDB user called: ipacs.
- Please inform Invicro if the MariaDB installation is non-standard in any way, e.g. the executable is located at /etc/init.d/mysql instead of /etc/init.d/mysqld.
- Please inform Invicro if on-site IT installs antivirus on the RHEL server or if this should be installed by the Invicro team alongside the iPACS.
- Ensure the server can connect to Invicro (in order to download the necessary installation files). If you have a proxy server, you must configure it first with the following command: export HTTPS_PROXY=http://your.proxy.com:port
- Ensure that the server can access Dockerhub, git.invicro.com, gitlab.invicro.com, and yum repositories.
- Then, you can run: curl -s https://install.invicro.com | grep -q ipacs && echo 'ok'
- If the connection can be established successfully, you should see the output ‘ok’. In any other case, please review the server network configuration. (see SELinux, IPTables, firewalld, Network).
- On-site IT may install the dependencies below, or allow the install technician to set them up using the installation utility.

Dependencies

The dependencies listed below are based on what is needed for an iPACS install, and is non-inclusive of other required packages that are shipped with a default CentOS/RHEL 7 minimal install.

You may install the required dependencies using the following commands:

```
yum install git docker mysql ntp curl -L
https://github.com/docker/compose/releases/download/1.20.1
/dockercompose-$(uname -s)-$(uname -m) -o /usr/local/bin/docker-compose
chmod +x /usr/local/bin/docker- compose chkconfig ntpd on && systemctl
start ntpd.service
```

List of Dependencies

git docker docker-compose mysql ntp