

# Requirements

## Server Stack

### Operating system

- Supported: Debian/Ubuntu and RHEL family (AlmaLinux, Rocky, CentOS).
- Init: systemd (required — agent is designed as a systemd unit).
- Architecture: Linux x86\_64 (typical VPS; agent uses standard distro package managers).

### Runtime dependencies

Component	Required	Notes
Python 3.9+	Yes	Stdlib only; on EL8 minimal images may need <code>python39</code>
systemd	Yes	Service: <code>balctl-heartbeat.service</code>
wget or curl	Install-time	Download <code>agent.zip</code>
unzip	Install-time	Extract bundle
sudo / root	For full feature set	Heartbeat itself can run unprivileged; most panel jobs need root

### Optional packages (installed by agent jobs when needed)

Package	When
haproxy	Install HAProxy job or <code>BALCTL_PROVISION_HAPROXY=1</code>
socat	Admin socket drain/ready, runtime HAProxy commands
firewalld	RHEL-family firewall jobs (auto-installed on first “Refresh rules” if missing, agent v78+)
ufw	Debian firewall backup jobs

## Network requirements

# Outbound HTTPS (required)

The VM must reach:

Destination	Purpose
<code>https://serversctl.com</code> (or your <code>BALCTL_API_BASE</code> )	Heartbeat, job claim/complete, backup upload/download
<code>https://download.serversctl.com/agent.zip</code>	Self-update (default)
<code>https://api.ipify.org</code> (optional)	Public IPv4 discovery when <code>BALCTL_PROBE_PUBLIC_IP=1</code>

All agent API traffic must use HTTPS — the agent refuses plaintext `BALCTL_API_BASE` / `BALCTL_UPDATE_URL` (v28+).

# Inbound (not required)

Panel-driven operations use the outbound job queue. No inbound SSH or agent port is required if the agent runs as root for privileged jobs.

# IP allowlisting (enrollment)

When you create a pool member, you must supply at least one allowed source IPv4. This is the VM's outbound/egress IP as seen when it calls the control plane — not necessarily its SSH IP or the IP traffic should hit.

The control plane validates `CF-Connecting-IP` against the enrolled allowlist on every agent request. Mismatch → 403.

# Enrollment requirements

Before the agent can heartbeat, create the member in the dashboard (Add pool member):

Field	Requirement
Hostname	Must match the JSON <code>hostname</code> the agent sends (case-insensitive). Override with <code>BALCTL_HOSTNAME</code> if OS hostname differs.
Allowed source IPs	One or more IPv4 addresses (comma-separated). Must include egress IP to control plane.
Enrollment secret	48 hex characters, no hyphens. Shown once in the modal. Not the member UUID on the card.
Member template	e.g. HAProxy balancer — determines which panel commands are available.
Linux family	Debian/Ubuntu vs RHEL — affects generated install one-liner.

# Authentication model

- Header: `Authorization: Bearer <48-char-enrollment-secret>`
- Secret stored server-side as SHA-256 hash only.
- 401 = wrong/unknown secret.
- 403 = IP not allowlisted, or hostname mismatch, or missing `CF-Connecting-IP`.

---

Revision #5

Created 2026-06-15 23:37:28 UTC by ServersCTL

Updated 2026-06-16 00:06:50 UTC by ServersCTL