

---

SDE

# Setting up SDE vApps (one-click apps)

*The article guides engineers through setting up SDE vApps, allowing users to launch single apps as tiles in a secure environment. It covers prerequisites, deployment, and operational details, making it ideal for those managing SDE Remote systems.*

AUTHOR

Paul Flanders

PUBLISHED

26 Oct 2026

DOCUMENT

InfoHub — Knowledge, news, and updates from EssingtonITS

# Setting up SDE vApps (one-click apps)

---

Paul Flanders · 26 Oct 2026

Publish single apps as tiles in SDE Remote: web apps in a locked-down browser (built for you on Proxmox), apps on hosts you build, and RemoteApps on your RDS farm. The user clicks a tile and gets just that app.

Applies to: sde-vapps 0.5.0+, SDE Remote app 1.0.7+, SDE Remote gateway 1.0.8+, Guacamole 1.5+, Proxmox VE 8/9 (pve-container newer than 6.0.9) · Audience: engineers deploying and running SDE vApps · Time: about an hour, plus 5–10 minutes per web template · Updated 26 October 2026

## Contents

1. [What you're setting up](#)
2. [Before you start](#)
3. [Proxmox token](#)
4. [Active Directory \(optional\)](#)
5. [Deploy the sde-vapps unit](#)
6. [Build the templates](#)
7. [Create a web vApp](#)
8. [Catalogue, hosted and RDS vApps](#)
9. [What users see](#)
10. [Acceptance tests](#)
11. [Day-to-day operations](#)
12. [Security model and hardening](#)
13. [Troubleshooting](#)
14. [Removing SDE vApps](#)

## 1. What you're setting up

SDE vApps is an optional add-on to an SDE Remote deployment, in its own GL unit ( `sde-vapps` ) with its own admin page at `https://<portal>/sde-vapps/` . A **vApp** is one app published as a tile. There are five kinds:

| Kind                   | Runs on                                                              | Built by                                       | Good for                                                                                 |
|------------------------|----------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------|
| Modern web app         | Chromium, in its own container                                       | <b>sde-vapps</b> , from the web template       | git, n8n, intranet sites, any current web app on the internal network                    |
| Legacy web app         | Pale Moon (Flash-capable), in its own container, wiped every session | <b>sde-vapps</b> , from the web template       | Old course content (old Moodle with Flash)                                               |
| App from the catalogue | An open-source app, in its own container                             | <b>sde-vapps</b> , from that app's recipe      | Arduino IDE, LibreOffice, GIMP, Inkscape, Thonny, KiCad, Blender, or a recipe you import |
| App on a host          | A Linux CT/VM (or a Windows VM) running one app                      | You ( <a href="#">hosted app KB</a> )          | Line-of-business apps, GPU apps, anything not in the catalogue                           |
| RDS RemoteApp          | Your RDS farm                                                        | Your Windows admins ( <a href="#">RDS KB</a> ) | Word, Excel, Windows line-of-business apps (seamless windows)                            |

**How it fits together.** Each vApp is *one ordinary RDP connection in Guacamole*, which sde-vapps writes and grants to the vApp's groups and users. The gateway launches it like any other connection (natively from SDE Remote), and Guacamole opens it in a browser tab.

**sde-vapps is not in the launch path:** if it's stopped, published apps keep working; only creating and changing them needs it.

**How a web vApp is built.** On "Create", sde-vapps:

1. clones the web template on the node with the most free memory into a container (CT 7000-7099);
2. sizes it, attaches it to the chosen bridge (DHCP) and sets its DNS and inbound firewall;
3. starts it and connects over SSH with its own key;
4. points the browser at the target, allows only the target in the browser and the container's outbound firewall, and sets up sign-in (a kiosk account, or joining AD);
5. publishes the Guacamole connection and grants it. A tile appears about a minute after Create.

### Network paths to allow

- Gateway host (sde-vapps) → Proxmox API: 8006 .
- Gateway host (sde-vapps, guacd, rdpgw) → web hosts: 22 (sde-vapps only) and 3389 .
- Web hosts → their targets (e.g. git on 3000 ), DNS, and the DCs when they use AD sign-in.
- Web template build: the building container needs the internet (or a Debian mirror) for about 5 minutes.
- sde-vapps' own port ( 8097 ) only needs reaching from nginx and the gateway; never publish it outside.

## 2. Before you start

| You need                        | Notes                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A working SDE Remote deployment | Guacamole + <code>sde-gateway</code> + <code>sde-nginx</code> . Gateway 1.0.8 or later and SDE Remote 1.0.7 or later give users the Apps section and the sign-in described in section 9; earlier versions still open vApps, as ordinary tiles.                                                                                                              |
| Proxmox VE 8 or 9               | For web and catalogue vApps (sde-vapps builds their hosts). Root on one node once (the token script). <b>pve-container newer than 6.0.9</b> on the nodes that build web hosts: 6.0.9 refuses Debian 13 containers ( <code>apt update &amp;&amp; apt full-upgrade</code> ). Storage that holds containers (LVM-thin, ZFS, directory) and a bridge with DHCP. |
| Active Directory (optional)     | Only for web vApps that sign users in with their own account. A domain admin runs one script once.                                                                                                                                                                                                                                                          |
| Guacamole admin                 | The gateway's <code>gua_srv</code> service account is fine: sde-vapps creates connections, a connection group and user groups.                                                                                                                                                                                                                              |
| Targets                         | The internal address of each web app (e.g. <code>http://10.20.0.15:3000/</code> ), reachable from the bridge the web hosts join.                                                                                                                                                                                                                            |

|                      |                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Legacy Flash content | The Flash plugin (64-bit Linux, 32.0) comes with sde-vapps and is installed on every legacy web host automatically, allowed to run only for that vApp's target. Adobe ended Flash Player's licence after 2020: running contained internal content with it is your decision. Templates built before sde-vapps 0.4.4 lack a library Flash needs: rebuild them (section 6). |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 3. Proxmox token

sde-vapps has its own token, independent of SDE VDI (a site can have either or both). Copy `scripts/vapps/pve-bootstrap-sde-vapps.sh` to any node and run it once as root:

```
bash pve-bootstrap-sde-vapps.sh          # creates everything, prints the env lines
bash pve-bootstrap-sde-vapps.sh --check  # later: OK / FIX per item, changes nothing
```

It also installs a small timer on that node, `sde-vapps-fuse.timer`, that turns on file transfer for every template and host as they're built (section 6.1). Nothing to run again later.

It creates the pool `sde-vapps`, the role `SDEVAPPS` (container and storage privileges only), the user `sde-vapps@pve`, the token `sde-vapps@pve!vapps` (secret shown once) and the ACLs on the pool, the container storages and the SDN zone. `--rotate-token` replaces the token.

What it grants, as commands

```
pveum pool add sde-vapps --comment "SDE vApps web containers and their template"
pveum role add SDEVAPPS --privs "VM.Allocate VM.Clone VM.Audit VM.PowerMgmt
VM.Config.Options VM.Config.Network VM.Config.Memory VM.Config.CPU VM.Config.Disk
Datastore.AllocateSpace Datastore.AllocateTemplate Datastore.Audit"
pveum user add sde-vapps@pve
pveum user token add sde-vapps@pve vapps --privsep 0
pveum acl modify / --users sde-vapps@pve --roles PVEAuditor
pveum acl modify /pool/sde-vapps --users sde-vapps@pve --roles SDEVAPPS
pveum acl modify /storage/<each> --users sde-vapps@pve --roles SDEVAPPS      #
container + image storages
```

```
pveum acl modify /sdn/zones/localnetwork --users sde-vapps@pve --roles PVESDNUser
```

## 4. Active Directory (optional)

Only needed for web vApps where users sign in with their own account (SSO). Kiosk vApps (the default for legacy content) need none of this. On a DC, in an elevated PowerShell:

```
powershell -ExecutionPolicy Bypass -File ad-bootstrap-sde-vdi.ps1 -For vapps
```

It creates `OU=vapps` under `OU=sde`, the join account `sde-vapps-join` (random password, never expires, **not** a Domain Admin: delegated to create, join and delete computers in that OU only, including the attributes Linux's `adcli` writes), and the group `sde-vapps-users`. It prints the `SDE_VAPPS_AD_*` and `SDE_VAPPS_DNS*` lines for the next step. `-Check` reports only.

**ID limit for AD users** Web hosts are unprivileged containers, which can use only user IDs 0-65535, so AD accounts are mapped into 2000-65000. That covers accounts whose RID (the last number of the SID) is below 63000: most domains. In a larger or very old domain, a user with a higher RID can't sign in ( `Failed to set real GID in /var/log/sss/krb5_child.log` ); widening the containers' ID map is a one-off root change on each node. Ask for it.

## 5. Deploy the sde-vapps unit

On the gateway host, from the SDE Remote deployment files, one interactive run installs and wires everything:

```
sudo deploy/glitch-units/deploy-sde-vapps.sh --wire --dry-run    # shows what it would change
sudo deploy/glitch-units/deploy-sde-vapps.sh --wire
sudo deploy/glitch-units/deploy-sde-vapps.sh --check           # any time: the tests only
```

Paste the lines from sections 3 and 4 when asked. It defaults the Guacamole URL and `gua_srv` password from the gateway's settings, generates the shared secret, writes the unit's environment (backing up any file it changes), adds the `/sde-vapps/` route to sde-inginx, restarts with confirmation, and tests that the admin page answers and that `/sde-`

vapps/v1/ and /sde-vapps/host/ are refused through the portal.

| Setting                                               | Value                                                                                                                                                            |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SDE_VAPPS_GUAC_URL / _ADMIN_USER / _ADMIN_PASS        | The gateway's Guacamole URL and <code>gua_srv</code>                                                                                                             |
| SDE_VAPPS_SHARED_SECRET                               | <code>openssl rand -hex 32</code>                                                                                                                                |
| SDE_VAPPS_PVE_URL / _TOKEN_ID / _TOKEN_SECRET / _POOL | From section 3. Without them, web vApps point at hosts you build by hand, and catalogue apps can't be created.                                                   |
| SDE_VAPPS_PVE_CA_FILE or _INSECURE                    | Trust Proxmox's CA ( <code>/etc/pve/pve-root-ca.pem</code> ), or <code>INSECURE=true</code> on test sites only                                                   |
| SDE_VAPPS_DNS / _DNS_SEARCH                           | Resolvers and search domain for the web hosts. <b>Set them</b> when DHCP's DNS can't resolve the targets or the domain, or when its search domain is a wildcard. |
| SDE_VAPPS_AD_DOMAIN / _USER / _PASS / _OU             | From section 4 (optional)                                                                                                                                        |
| SDE_VAPPS_RDP_FROM / _SSH_FROM                        | Who may reach the web hosts' 3389 and 22. Default: the Guacamole URL's host (where the gateway, guacd and sde-vapps run).                                        |
| SDE_VAPPS_V1_NETWORKS                                 | <code>172.16.0.0/12</code> : only the gateway's docker network may call the catalog API                                                                          |
| Gateway: SDE_VAPPS_URL / SDE_VAPPS_SECRET             | Optional ( <code>--wire</code> asks): lets links open a page in a web vApp that's already open. The secret is <code>SDE_VAPPS_SHARED_SECRET</code> .             |

|                      |                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------|
| SDE_VAPPS_ALLOW_OPEN | <b>Testing sites only.</b> Lets a web vApp's Lock-down be set to Off (section 7). Never on a production site. |
|----------------------|---------------------------------------------------------------------------------------------------------------|

State lives in `/var/glitch-units/sde-vapps/data/state` : the vApps, kiosk passwords, sde-vapps' SSH key, and a daily copy of the state (14 kept). It must persist; include it in the host backup.

## 6. Build the templates

Every host sde-vapps builds is cloned from a **template** on its node: the **Web browsers** template (Chromium and Pale Moon, for every web vApp) and one for each catalogue app you use. Open `https://<portal>/sde-vapps/` (sign in as a Guacamole administrator) → **Hosts** → **Templates**, choose **Web browsers** and a node (or Best node), and click **Build**. Catalogue apps' templates are built the same way, or from their card on the Catalogue tab. sde-vapps:

1. downloads the Debian 13 container image to the node (if it isn't there);
2. creates a container with its own SSH key, and installs xrdp (from backports), the vApp kit, and what the template holds: Chromium, Pale Moon and the Flash plugin's libraries for Web browsers, or the app for a catalogue template;
3. removes the container's identity (SSH host keys, machine id: every clone gets its own) and turns it into a template.

It takes 3–15 minutes. The Templates table shows each step and the build log, then, for each template: when it was built, by which sde-vapps and from which recipe version, and what it holds (xrdp, browser and app versions). **Out of date** means its recipe or sde-vapps has changed since: rebuild it. Each row has **Rebuild** and **Remove**; removing a template leaves the hosts already built from it running. With local storage, each node that should run a kind of vApp needs that template ("Best node" picks the one with the most free memory). Nodes whose pve-container is too old are listed with the reason.

## 6.1 File transfer (automatic)

A vApp's **Drive** passthrough (moving files between the user's PC and the app: downloads and uploads, section 7.2) needs FUSE in its host. Proxmox lets only `root@pam` turn that on, so no API token can do it. The bootstrap script (section 3) installs `sde-vapps-fuse.timer` on its node, which turns FUSE on for every container in the `sde-vapps` pool every 2 minutes: templates, web hosts and catalogue hosts. A running host only gets it after a restart, so sde-vapps restarts each Drive host once nobody is signed in to it (activity log: *reason=fuse*).

```
bash pve-bootstrap-sde-vapps.sh --enable-files      # do it now (and install the timer)
bash pve-bootstrap-sde-vapps.sh --enable-files --check  # just report
bash pve-bootstrap-sde-vapps.sh --remove-timer      # take the timer away
journalctl -u sde-vapps-fuse                        # what the timer changed
```

Readiness lists any template or host still without it ("File transfer (FUSE)"); on a site set up before the timer existed, run the script once more as root. Proxmox notes that FUSE in a container can stop snapshot-mode backups from freezing it: vApp hosts are rebuilt from templates rather than restored, so that's rarely a concern.

In a session, each mapped drive appears in `~/thinclient_drives/<display>/`, a separate folder for each session, so two users of one kiosk account never see each other's PC.

**Rebuild it monthly** The template is what you patch. Building a new one replaces the old one on that node once the new one is ready; existing web hosts keep running, and "Rebuild host" moves one onto the new template. Readiness warns when a template is over 45 days old.

## 7. Create a web vApp

**vApps → New vApp → Modern web app** (or Legacy web app). The fields:

| Field                   | What to enter                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name, icon, description | What users see on the tile, e.g. <i>Git</i> with the code icon                                                                                                                                                                                                                                                                                                                     |
| Target                  | The app's internal address, e.g.<br><code>http://10.20.0.15:3000/</code> . The browser opens it and can reach nothing else.                                                                                                                                                                                                                                                        |
| Also allow              | Other addresses the app needs, such as a sign-in server ( <code>https://sso.corp.local</code> ). Separate with <code>;</code> .                                                                                                                                                                                                                                                    |
| Named pages (for links) | Pages a link or desktop shortcut can open directly ( <code>sde-remote://vapp/&lt;id&gt;?p=&lt;name&gt;</code> ), e.g. one per Flash activity, each with a Copy link button. See <a href="#">Links and shortcuts</a> .                                                                                                                                                              |
| Host names (hosts file) | For a target whose name DNS doesn't know, or knows wrongly (an old Moodle that must keep its own FQDN, e.g.<br><code>moodle.school.ac.uk</code> , outside the SDE domain): one line per entry, <code>10.20.0.15 moodle.school.ac.uk</code> . The web host uses these before DNS, so the site keeps its real address, links and certificate; Locked allows exactly these addresses. |

|                                   |                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lock-down                         | <p><b>Locked to the target (recommended):</b> always, in production. The field appears only where <code>SDE_VAPPS_ALLOW_OPEN=true</code> , and offers <b>Off: any site (testing only):</b> any site works, for trying out internet sites on a test network. Tiles set to Off are marked and Readiness warns.</p> |
| Browser profile                   | <p><b>Remember sign-ins</b> (per user; good for git and n8n) or <b>Clean every session.</b> Legacy is always clean.</p>                                                                                                                                                                                          |
| Node, Proxmox bridge, Memory, CPU | <p>Automatic picks the node with a template and the most free memory, and <code>vmbr0</code> . In production, choose the bridge for the secure network the target is on. Allow about 0.5 GiB per active user plus 0.5 GiB.</p>                                                                                   |
| Who gets it                       | <p>Guacamole groups (use AD group names when Guacamole reads groups from LDAP; created in Guacamole if missing) and/or users (who have signed in once). With AD sign-in, the web host also lets in only these.</p>                                                                                               |
| Users sign in with                | <p><b>Their own account (AD):</b> needs section 4; the host joins the domain as <code>SDEWEB&lt;ctid&gt;</code> . <b>Kiosk account:</b> a local account sde-vapps creates; everyone shares it; always a clean profile. <b>Ask when it opens:</b> the host's sign-in screen.</p>                                  |

|             |                                                                                                                                                                                                                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Passthrough | Copy out / paste in (separately), drive, printing, sound (off by default for modern web apps), microphone; quality. <b>Drive</b> is what lets users download to and upload from their own PC (section 7.2; needs section 6.1). USB isn't offered for web vApps (xrdp can't redirect it). The gateway's site-wide lock-down still wins. |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Create, then watch the tile on the Overview: "cloning", "starting", "configuring", then **Published**, usually within a minute or two. Edits reach the host within seconds of saving.

**Open sessions and edits.** Clicking the tile again reconnects users to the session they left (it carries on where they were). A running browser can't pick up a new target, extra addresses, host names, lock-down or profile, so saving one of those **closes that app's open sessions**, and the next click opens the new settings. Other changes (who gets it, passthrough, size) leave open sessions alone. **Rebuild host** replaces the container (users on it are disconnected).

## 7.1 The browser users get

- **Modern web apps** open in a full Chromium window, maximised: address bar, tabs, back and forward, and the downloads button. Only the target, the "Also allow" addresses and the host names you listed load. Anything else typed in the address bar, or reached by a link, is refused by the browser's policy. There are no developer tools, extensions, guest profiles or browser sign-in.
- **Legacy web apps** open in Pale Moon with its full toolbar, downloads button included, and with Flash. The container's outbound firewall lets it reach only the target, and Flash runs only for the target's address.
- Closing the browser window ends the session. Dialogs (save, upload, print) always open in the middle of the screen.

**After upgrading sde-vapps** A web host picks up new browser settings when it's next set up. Save each web vApp once (or use Rebuild host) after an upgrade. Sessions that are already open keep the old browser until the user closes them.

## 7.2 Files and downloads

With the vApp's **Drive** passthrough on (and FUSE turned on, section 6.1), users can move files between the web app and their own PC:

- **Downloads:** both browsers ask where to save every download. The save dialog's sidebar has a **Mapped folders** entry, which holds the folders the user's PC shares into this session. In SDE Remote, that's the user's own Windows profile folder, shown as **Home**. Files Chromium flags as dangerous are blocked.
- **Uploads:** the site's upload button opens the same dialog; the user picks a file from Mapped folders.
- **In a browser tab** (Guacamole rather than SDE Remote), Mapped folders holds Guacamole's own file drive instead. Users move files between it and their PC from Guacamole's menu (Ctrl+Alt+Shift).
- **Drive off** (on the vApp, or site-wide on the gateway): there are no mapped folders. A file saved anywhere else stays on the web host, out of the user's reach, and is wiped at the end of the session when the profile is clean.

Each session has its own folder of mapped drives, so two people using one kiosk account never see each other's files.

## 8. Catalogue, hosted and RDS vApps

### 8.1 Apps from the catalogue

The **Catalogue** tab lists open-source apps sde-vapps can build and run for you, each from a **recipe**: what to install, and which app(s) it publishes. Built in, by category:

- **Programming:** Visual Studio Code, VSCodium (its open-source build), Kate, Notepadqq (like Notepad++), Geany, Code::Blocks, Spyder, Thonny.

- **Electronics:** Arduino IDE, KiCad, Fritzing.
- **Office and publishing:** LibreOffice (Writer, Calc, Impress), Scribus, Dia.
- **Graphics:** GIMP, Inkscape, Krita, darktable.
- **3D and CAD:** Blender, FreeCAD, OpenSCAD, PrusaSlicer.
- **Audio, music and video:** Audacity, MuseScore 3, LMMS, Kdenlive, Shotcut.
- **Maths, science and geography:** GNU Octave, QGIS. **Game development:** Godot 3.
- **Games:** 0 A.D., OpenTTD, Battle for Wesnoth, Freeciv, Chess (Stockfish).
- **Retro computing:** Commodore 64 (VICE, with the 1541 drive) and ZX Spectrum (Fuse).

The [app catalogue](#) page lists every app with its licence, notes and suggested size.

All are open source except Visual Studio Code (Microsoft's licence, free to use). Downloads from outside Debian (Arduino IDE, VS Code, VSCodium, the C64 ROMs from VICE's release) are checked against the checksums their makers publish.

1. On the app's card, **Build template** (once per node that will run it).
2. **New vApp** on the card (or vApps → New vApp → App from the catalogue): choose the app (LibreOffice: which of Writer, Calc and Impress), who gets it, how users sign in, and whether it may reach the internet.
3. sde-vapps clones a host from the template, sets it up like a web host (sign-in, firewall, file transfer) and publishes the tile.

| Setting         | What it does                                                                                                                                                                                                                                    |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internet access | <b>Off</b> (default for most apps): the host reaches only DNS and the domain controllers. <b>On</b> : it can reach the internet. The Arduino IDE, VS Code and VSCodium have it on by default, for their board, library and extension downloads. |
| Drive           | On by default for catalogue apps, so users can open and save files on their own PC (section 7.2).                                                                                                                                               |
| Memory, CPU     | Preselected from the recipe; add about 1 GiB per extra active user.                                                                                                                                                                             |

**USB devices and containers** A container can't take a USB device, so the Arduino IDE (and Thonny with MicroPython boards) can compile here but not upload to a board. For boards connected with SDE Devices, use a Linux desktop pool (a VM) with the app installed.

**Recipes you add. Import recipe** on the Catalogue tab takes a recipe file (JSON); **Export** on any card saves one, as a starting point or to move it to another site. A recipe has an id, a name, a version, Debian packages, optional shell steps, and its apps (id, name, command). **A recipe runs as root, with internet access, while its template builds:** import only recipes from people you trust, and read "What it installs" on the card first. Imported recipes are kept in `data/recipes` with the unit's state. Change a recipe by importing it again with a higher version: its templates then show Out of date.

## 8.2 Hosted and RDS vApps

- **App on a host:** build the host with the vApp host kit ([hosted app KB](#)), then New vApp → App on a host: the host's address, the app ID from its `/etc/sde/apps.d`, and the sign-in. sde-vapps only publishes it.

- **RDS RemoteApp:** your Windows admins publish the app in the RDS collection ([RDS KB](#)), then New vApp → RDS RemoteApp: the Connection Broker, the RemoteApp alias ( `| |WINWORD` ) and the collection's load-balance info.

## 9. What users see

- **Links and shortcuts:** right-click any tile in SDE Remote → Create desktop shortcut / Copy link; web pages can link straight to a vApp page. See [Links and shortcuts](#).
- **In a browser:** the vApp appears in the Guacamole home page under "Apps (open in SDE Remote)". Clicking it opens just the app in the tab.
- **In SDE Remote:** vApps have their own **Apps** section, above Desktop pools and Remote desktops (the headers show when a user has more than one kind of tile). Clicking a tile opens just the app in its own window through the gateway. RDS RemoteApps open as ordinary windows on the user's taskbar.
- **Signing in:** SDE Remote signs in the way the browser does. A vApp set to *their own account* opens signed in as the user, with no prompt. A *kiosk* vApp signs in with its kiosk account. An *Ask* vApp asks the user for an account when it opens.
- Closing the app ends the session. Reopening within the disconnect limit (2 h) returns to it.

## 10. Acceptance tests

- Readiness: no **Fix** lines.
- The web template is ready on the node(s) you'll use.
- A modern web vApp reaches Published, and a granted user gets just the app (browser and SDE Remote), signed in as themselves (AD) with no password prompt after the first time if "Remember sign-ins" is on.
- In SDE Remote, the tile is under Apps.
- In the app, typing another site in the address bar (or following a link elsewhere) is refused by the browser.

- With Drive on: a download asks where to save, Mapped folders → Home is in the dialog's sidebar, and the file arrives on the user's PC. An upload from the same folder works.
- From the web host, nothing but the target answers (sde-vapps' setup proves it: `curl` to another site fails).
- A legacy kiosk vApp opens in Pale Moon on the target, and a new session starts clean.
- Readiness → Flash: the plugin is listed with its version. In a legacy vApp, `about:plugins` lists Shockwave Flash, your Flash content plays, and Flash content from any other address doesn't.
- A user without the grant doesn't see the tile; with AD sign-in, the host refuses them too.
- `deploy-sde-vapps.sh --check` : `/sde-vapps/v1/` and `/sde-vapps/host/` are refused through the portal.

## 11. Day-to-day operations

| Task                        | How                                                                                                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Patch the hosts             | Hosts → Templates → Rebuild each template (monthly), <code>pve-bootstrap-sde-vapps.sh --enable-files</code> as root, then Rebuild host on each web and catalogue vApp at a quiet time |
| Add an app to the catalogue | Catalogue → Import recipe; build its template; New vApp                                                                                                                               |
| Change a vApp               | Edit and Save: the host is re-set up, the Guacamole entry updated                                                                                                                     |
| Upgrade sde-vapps           | Pull the new image and restart the unit, then save each web vApp once so its host gets the new browser settings (section 7.1)                                                         |
| A host misbehaves           | Edit → Rebuild host (a fresh container from the template)                                                                                                                             |
| Hide a vApp for a while     | Untick Published: the tile goes and its web host is stopped                                                                                                                           |
| Remove a vApp               | Delete: the tile goes and its web host is destroyed                                                                                                                                   |
| What happened               | Activity tab; full history: <code>docker logs sde-vapps ( AUDIT vapps-... )</code>                                                                                                    |

|                          |                                                                                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Restore the state        | <code>gl -d sde-vapps</code> , copy a file from <code>data/state/backups</code> over <code>state.json</code> , <code>gl -s sde-vapps</code> |
| Rotate the Proxmox token | <code>pve-bootstrap-sde-vapps.sh --rotate-token</code> , update the unit, restart it                                                        |

## 12. Security model and hardening

- **Everything goes through the gateway.** The user's device only ever receives an RDP stream; the browser that talks to the internal app runs inside your network.
- **Two locks on every web host:** the browser's own policy (only the target and the listed addresses load, whatever is typed in the address bar; no developer tools, extensions or guest profiles), and an outbound firewall inside the container (only DNS, the target and the DCs). The firewall is enforced whatever Proxmox's firewall does.
- **Files:** files reach the user's PC only through the Drive passthrough, and only into the folders the user's PC shares. Turn Drive off on a vApp to stop file transfer for it, or across the site with the gateway's lock-down ( `SDE_DISABLE_DRIVE=true` ). The browser asks where to save every download and blocks files it flags as dangerous.
- **Inbound:** sde-vapps sets each host's Proxmox firewall to accept only RDP from the gateway and SSH from sde-vapps. Those rules apply only when Proxmox's *datacenter* firewall is on (Readiness warns when it's off). Check the node rules allow your management access before turning it on.
- **Unprivileged containers**, one per web vApp, so apps never share a host. Each clone gets fresh SSH host keys and machine id; sde-vapps pins each host's SSH key on first contact.
- **Accounts:** kiosk passwords are random and stored only in sde-vapps' state (mode 600) and the Guacamole connection. The AD join account is delegated to one OU, never a Domain Admin.
- `SDE_VAPPS_V1_NETWORKS` set; `SDE_VAPPS_ALLOW_OPEN` never set on production sites; the environment file `chmod 600` ; Proxmox's certificate verified ( `SDE_VAPPS_PVE_CA_FILE` ).

## 13. Troubleshooting

The common problems are below. More (sound, AD join, template builds, SDE Networks, looking inside a host) are in [Troubleshooting SDE vApps](#).

| Symptom                                                                              | Cause and fix                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "can't create Debian 13 containers" /<br>"unsupported debian version '13.1'"         | The node's pve-container is 6.0.9 or older.<br>Update the node, or build on another one.                                                                                                                             |
| A vApp stuck with "no web template yet"<br>(or "no ... template")                    | Build that template (Hosts → Templates, or the app's card on the Catalogue tab) on a node that can; or set the vApp's Node to Automatic.                                                                             |
| A template shows Out of date                                                         | Its recipe (or sde-vapps) changed since it was built. Rebuild it, then Rebuild host on the vApps that use it.                                                                                                        |
| A catalogue template fails to build                                                  | The build log (Hosts → Templates → the row) shows the step: usually a download the recipe makes. The building container needs the internet (or a Debian mirror) while it builds.                                     |
| "couldn't reach the container over SSH"                                              | The host's bridge has no DHCP, or sde-vapps can't reach that network on port 22.                                                                                                                                     |
| AD join fails: "Can't contact LDAP server",<br>lookups go to public addresses        | The host uses DHCP's DNS, which doesn't know the domain or wildcards it (a public search domain). Set <code>SDE_VAPPS_DNS</code> (the DCs) and <code>_DNS_SEARCH</code> , restart the unit; the hosts are re-set up. |
| AD users can't sign in; <code>krb5_child.log</code><br>says "Failed to set real GID" | The account's RID is above 63000 (see the ID limit in section 4).                                                                                                                                                    |

|                                                                                      |                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "The remote desktop server is currently unreachable" in the browser                  | guacd can't reach the host's 3389, or (older versions) the self-signed certificate was refused. Check Readiness → Hosts.                                                                     |
| A user gets an old session of another app                                            | Shouldn't happen (one container per web vApp). On a shared hosted app server, xrdp reattaches the user's existing session: close the first app.                                              |
| The target's name doesn't resolve, or resolves to the wrong place, from the web host | Add it under Host names (hosts file) with the address it should use. Check from sde-vapps' side: Hosts page error, or <code>getent hosts &lt;name&gt;</code> on the host.                    |
| An internet site half-loads in a Locked vApp                                         | By design: it pulls content from other addresses. Add them to "Also allow", or (testing sites only) set Lock-down to Off.                                                                    |
| A tile stays "waiting for its web host"                                              | Its host hasn't finished its first setup: see the host's error on the Overview or Hosts page.                                                                                                |
| The browser has no address bar or downloads button, or downloads are blocked         | The host still has the settings of an older sde-vapps. Save the vApp (or Rebuild host), then have the user close the app and open it again.                                                  |
| No Mapped folders in the save dialog, or the folder is empty                         | Drive is off on the vApp or on the gateway, or FUSE isn't on for that host (section 6.1; Readiness "File transfer (FUSE)"). A host that was running when FUSE was turned on needs a restart. |

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A vApp's tile is under Remote desktops, not Apps                                | SDE Remote couldn't get the vApp list from the gateway: check the gateway is 1.0.5 or later and reaches sde-vapps. The tile still works.                                                                                                                                                                                                                                     |
| Flash content shows a grey box, "plugin missing", or Flash's end-of-life notice | Readiness → Flash says which. "Can't load, missing ...": the host's template predates sde-vapps 0.4.4; rebuild the web template, then Rebuild host. "Not installed yet": save the vApp. An end-of-life notice: either the content's address isn't the vApp's target (Flash is allowed only there), or this Flash build refuses it; ask SDE support for the 32.0.0.371 build. |
| A save or upload dialog opens off the edge of the screen                        | The host has an older window manager profile. Save the vApp so the host is set up again.                                                                                                                                                                                                                                                                                     |

## 14. Removing SDE vApps

1. Delete each vApp in the admin page (web hosts are destroyed, Guacamole entries removed).
2. Hosts: the web templates can be deleted in Proxmox (pool `sde-vapps` ).
3. `gl -d sde-vapps` , remove the nginx block, reload nginx.
4. Optionally remove the Proxmox pool, role, user and token, and the AD OU and join account.

SDE vApps knowledge base · Setup guide · Related: [Settings reference](#) · [App catalogue](#) · [Troubleshooting](#) · [Hosted apps](#) · [RDS RemoteApp](#) · [Links and shortcuts](#)