ALPINE SSHD BYPASS

Four conditions and a restart.

Exposure is host state, not a version number.

RACK2CLOUD
THINK LIKE AN ARCHITECT.
BUILD LIKE AN ENGINEER.

Exposure needs four conditions at once.

1 No PAM in the password path

AND

2 PasswordAuthentication yes

AND

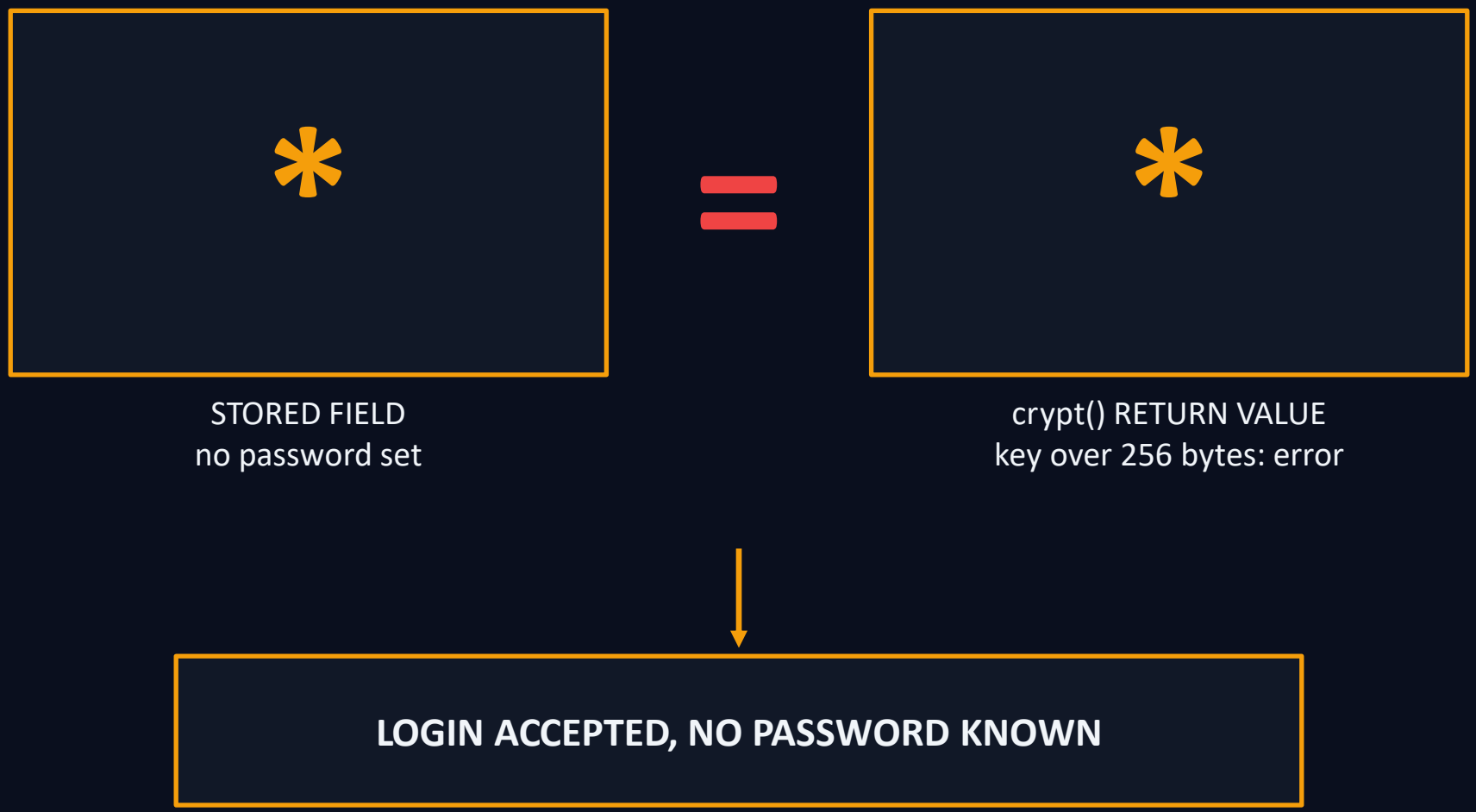
3 An account whose password field is exactly *

AND

4 Another account with a 5 or 6 hash

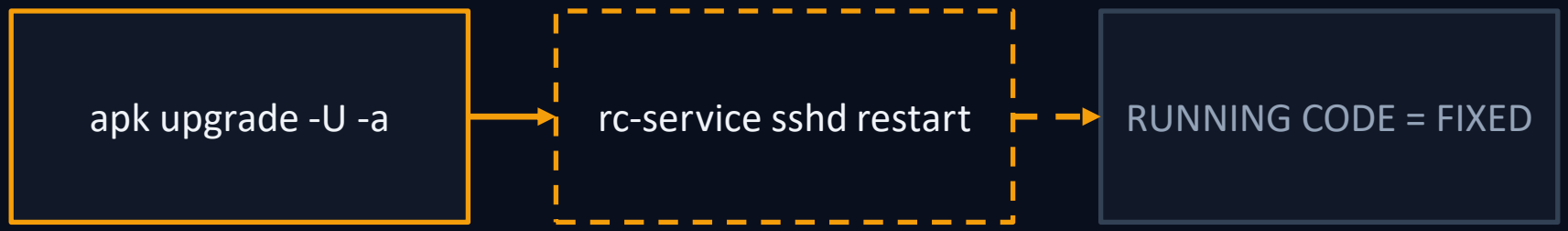
Condition 3 is key-only hygiene. Condition 4 is one console password.

Two meanings of * collide in one comparison.



A locked account (!) is not equal to the error marker.

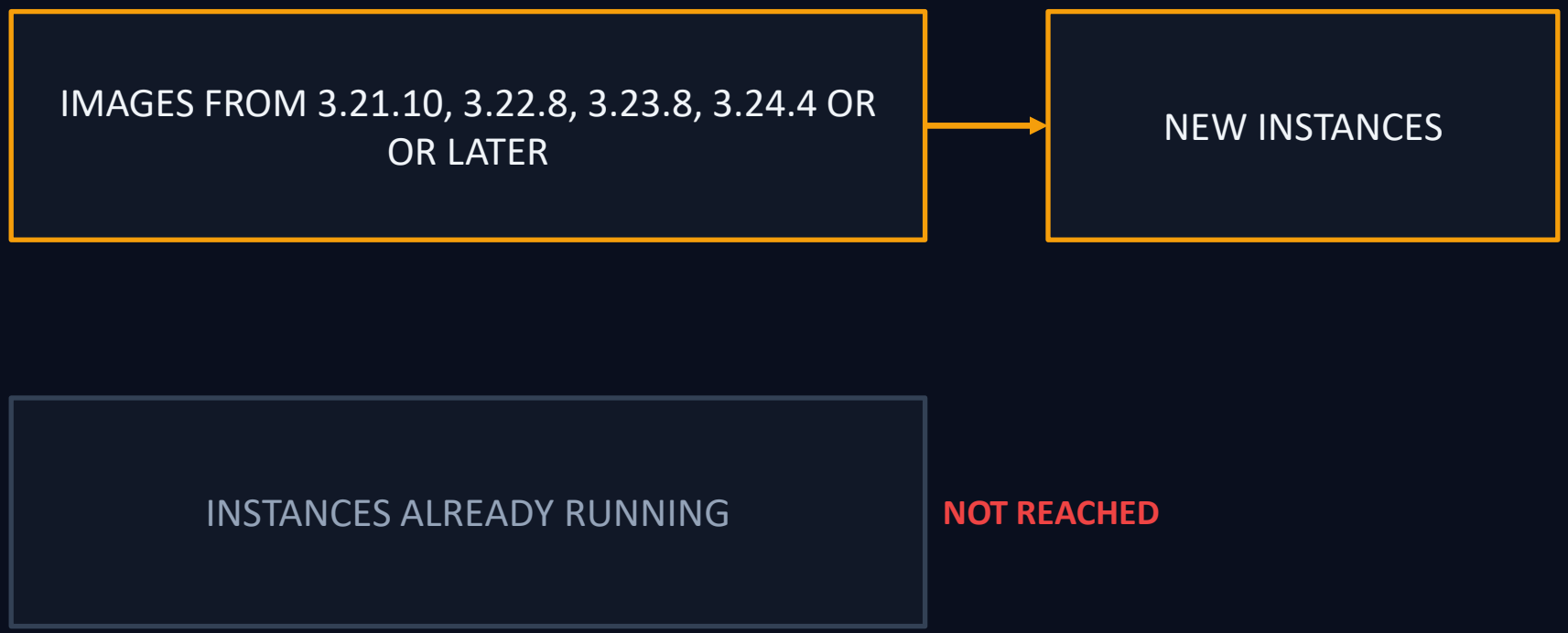
A package upgrade does not replace the the running daemon.



Evidence: the sshd listener started after the package was upgraded. upgraded.

Interim route: PasswordAuthentication no on every such line, Match blocks blocks included, then restart. Either route ends with a restart.

A rebuilt image does not reach running running instances.



Each running instance: update openssh, or disable password authentication.
Fixed packages exist back to 3.16.

Tiny-cloud images: safe at first boot, exposed after the first password.



Images 3.18.11 through 3.24.3, with the other conditions holding. The state
The state change is an ordinary provisioning action.

If a login cannot be ruled out, the verdict verdict stops at exposure.

Not exposed: a condition fails

Exposed and fixed: both fix states verified

Exposed, login history readable or not

Alpine: if a login cannot be ruled out, treat the machine as compromised. A compromised. A rotated or unshipped log cannot show an absence.

What the sources leave open.

ROOT CAUSE	Disputed between projects. No side taken here.
SCOPE	Beyond Alpine: not assessed.
LOWER BOUND	Upstream affected-version start: not stated.
EXPLOITATION	CISA lists it as exploited (Nov 9). Whose hosts: not stated.

Sources: Alpine advisory, OpenSSH 10.6p2 release notes, musl list post (Nov 5), CVE record and CISA alert (Nov 9). Re-read before acting.

A package manager reports what was was installed.

Only the running host can say what is listening.

rack2cloud.com | Follow The Architect for more

RACK2CLOUD
THINK LIKE AN ARCHITECT.
BUILD LIKE AN ENGINEER.