Autoprovisioning IdM Clients in OpenStack

Rob Crittenden
Juan Antonio Osorio Robles
Adé Lee
May 8, 2017

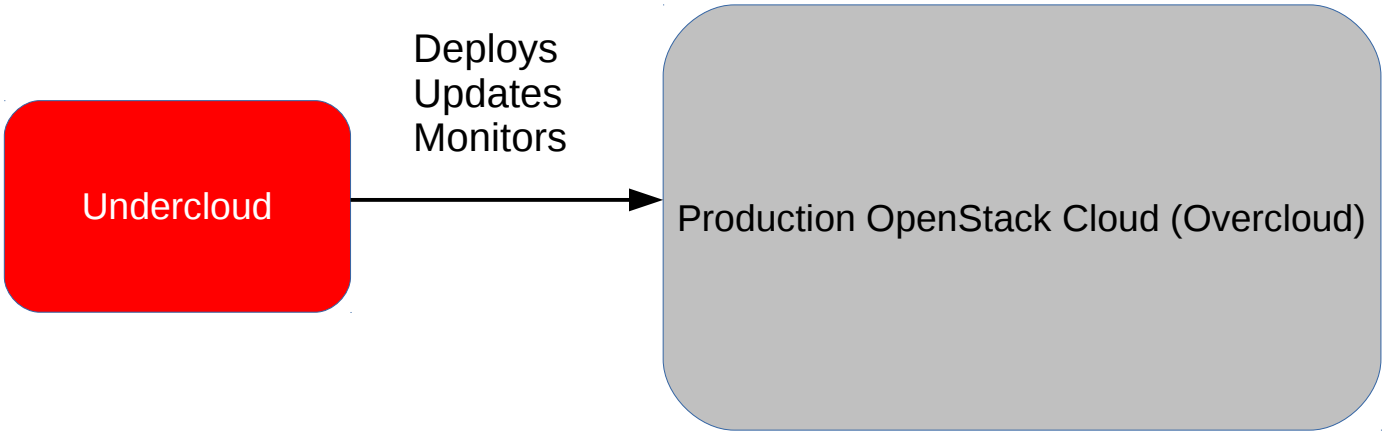
What is FreeIPA (IPA, IdM)?

- Centralized Identity
  - CA to generate SSL Certificates
  - Host-Based Access Control via sssd
  - Centralized sudo
  - Kerberos
  - Client can enroll using admin credentials/password or a One Time Password (OTP)

What is autoprovisioning?

- After first boot new OpenStack instances are enrolled as IPA clients.

Why Autoprovisioning?



- Deploying in TripleO, “OpenStack on OpenStack”
- Want the Overcloud to be deployed with TLS-enabled endpoints

The Problem

- How to get SSL certificates into an Openstack instance?
  - Push – generate outside instance
    - As metadata, like SSH public keys
    - Heat, puppet, ansible, etc.
  - Pull – generate inside instance
    - Use certmonger to request keys. Requires credentials.

Related Questions

- How to automatically issue certificates as instances are added?
- How to revoke certificates when instances are removed?
- How to re-issue certificates when they expire?

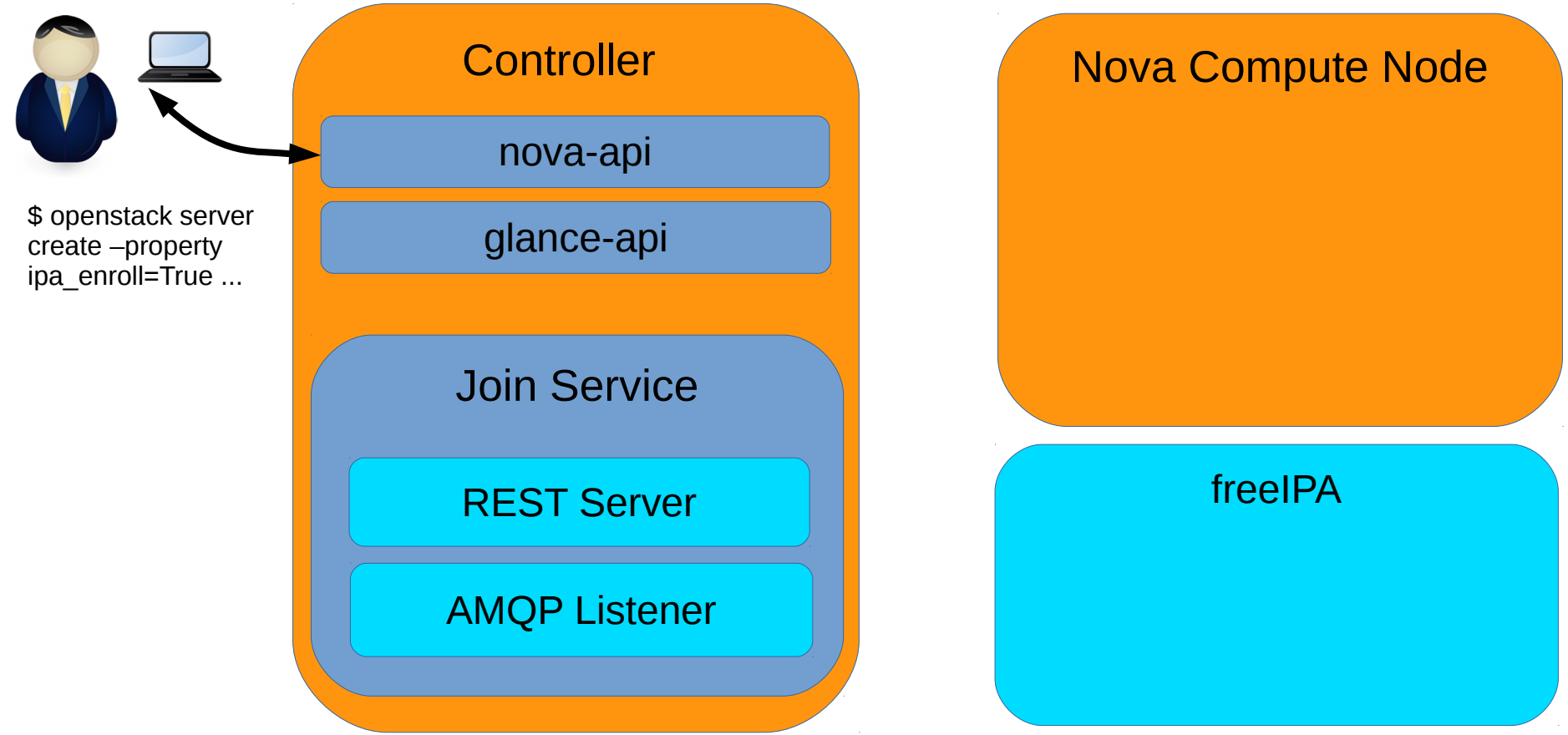
novajoin project

- **https://github.com/openstack/novajoin**
- Two servers
  - REST
    - Handle host ADD requests
    - Generates hostname and OTP, adds hosts to IPA
    - Connection should be limited to nova
  - Notification listener
    - Waits for instance DELETE request, removes host from IPA
    - Limited support for floating IP association/disassociation and IPA-based DNS updates

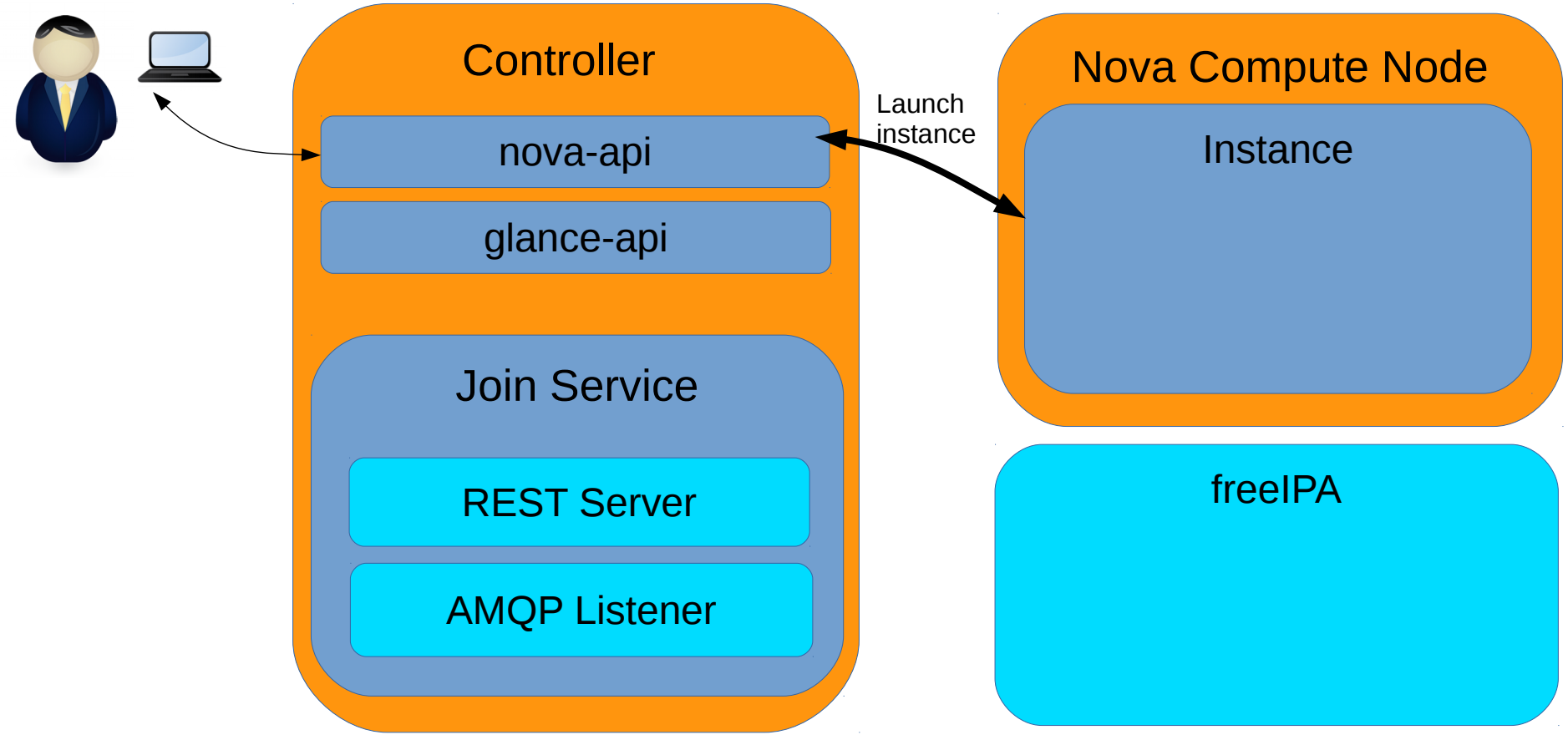
The Toolbox

- Nova metadata service
- cloud-init
- freeIPA
- certmonger

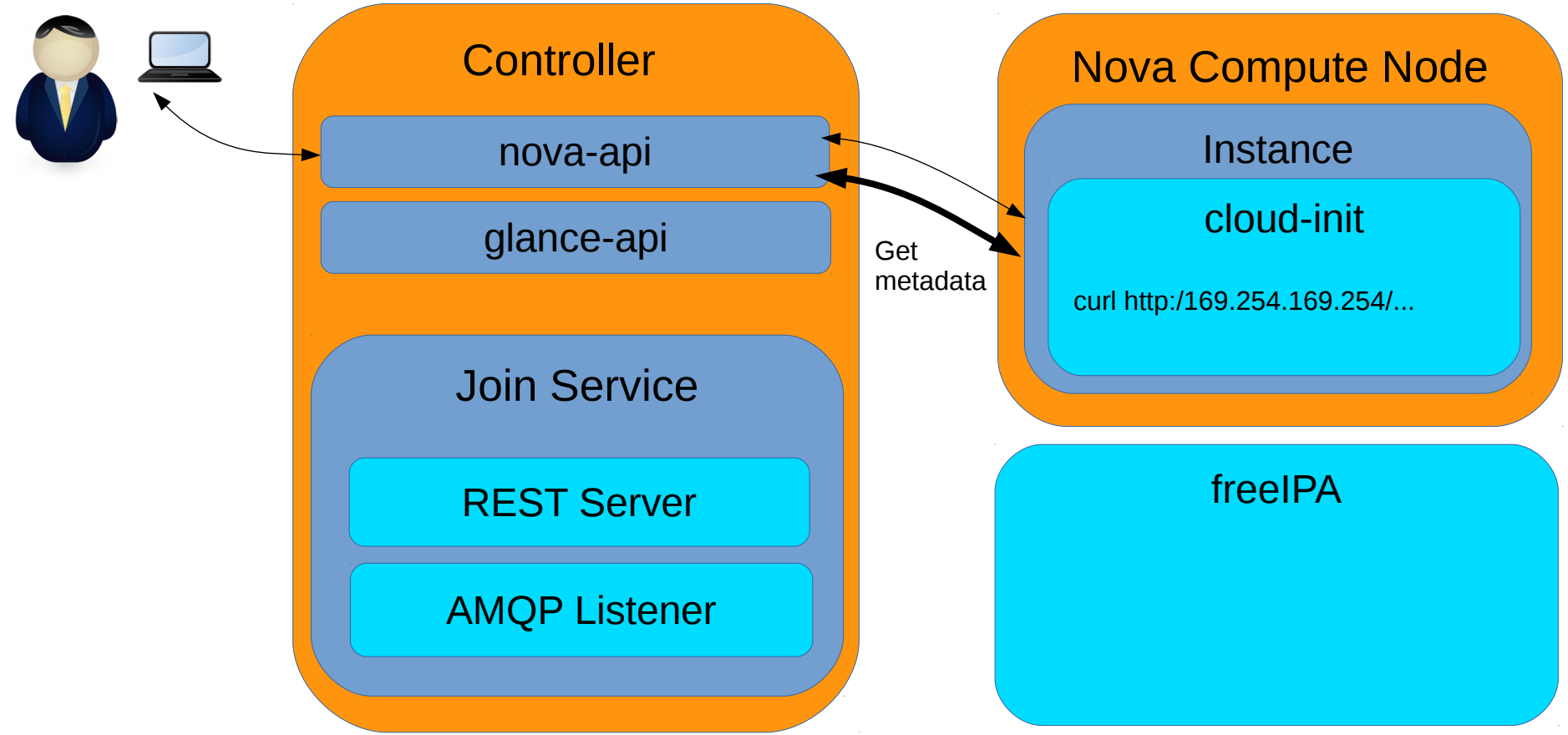
Create a new instance, VM case



Create a new instance



Retrieve metadata



POST to REST server

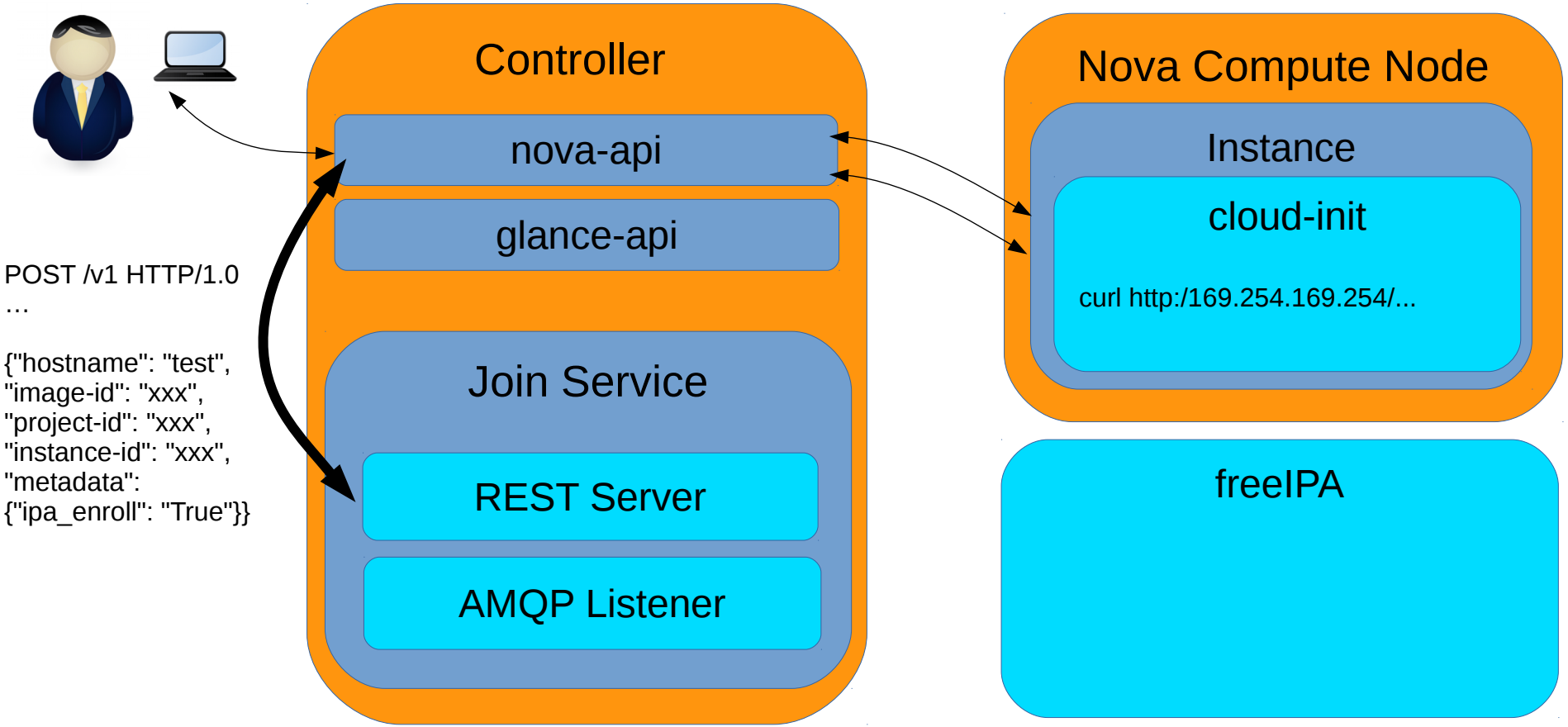
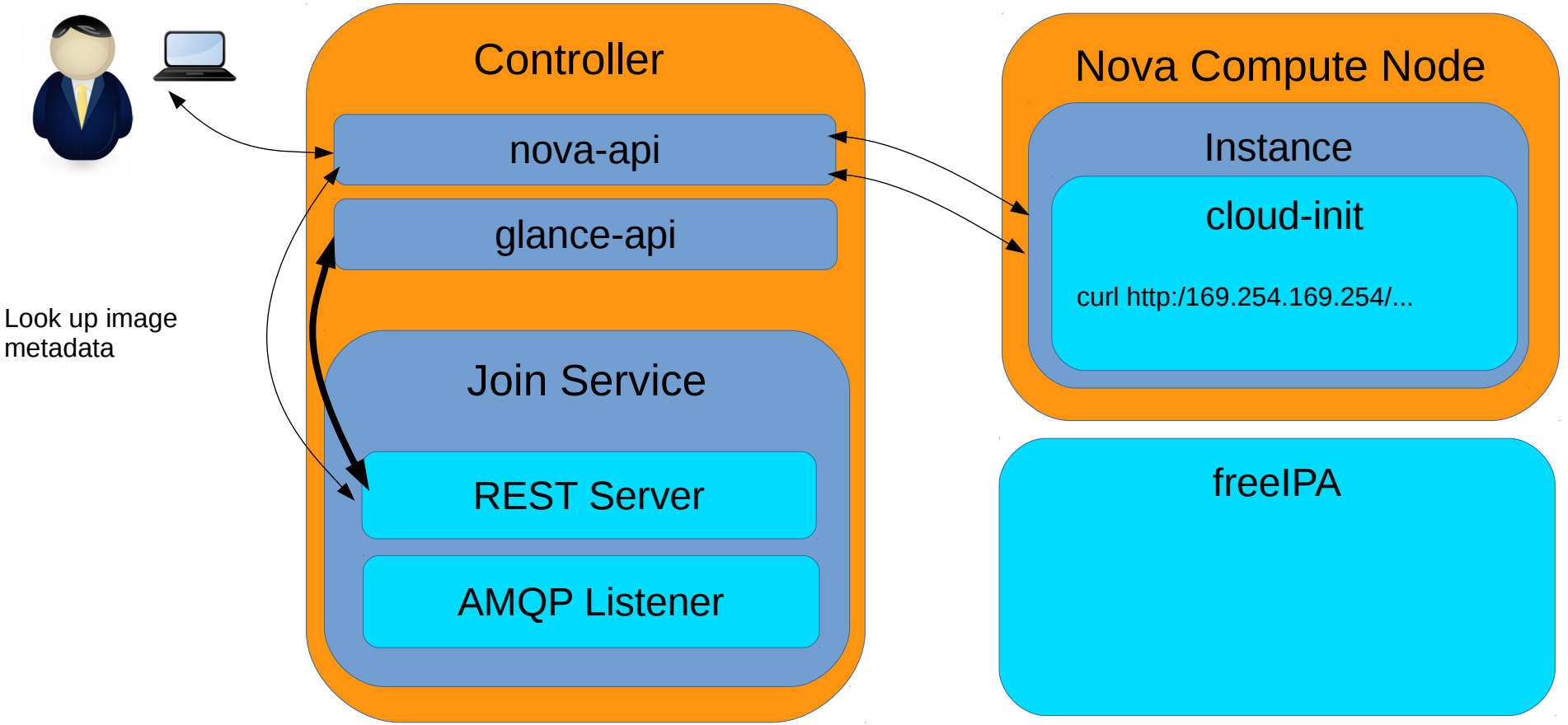
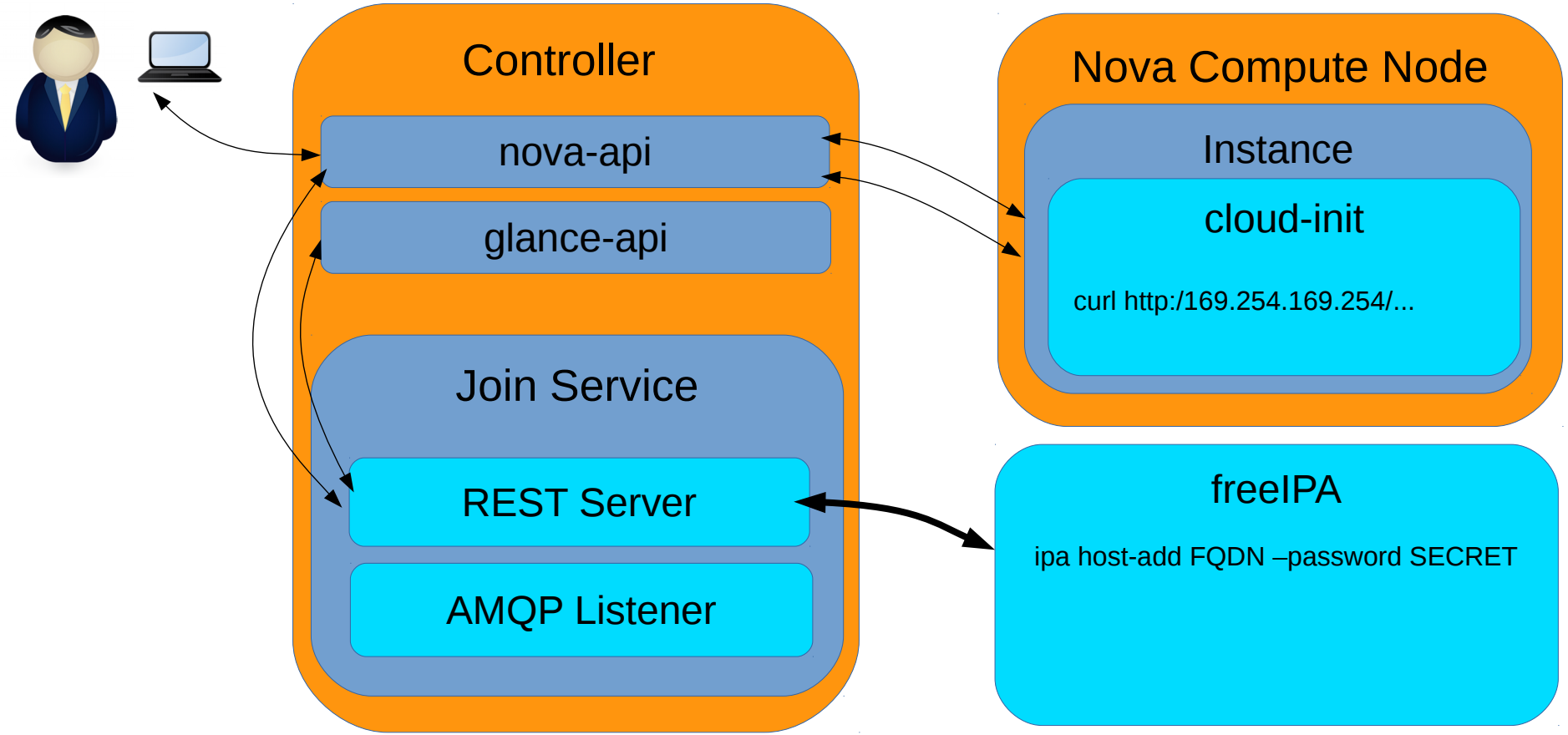


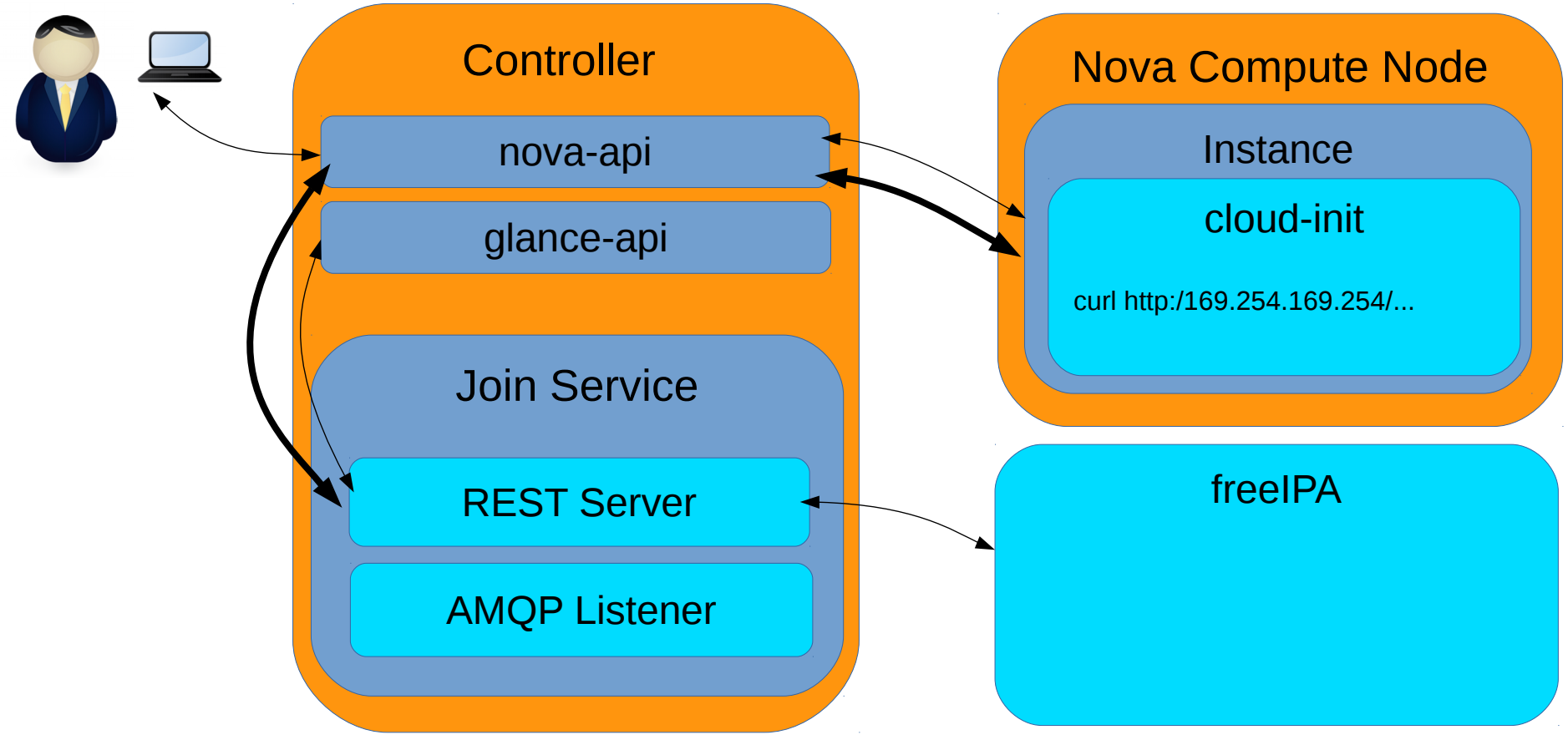
Image metadata lookup



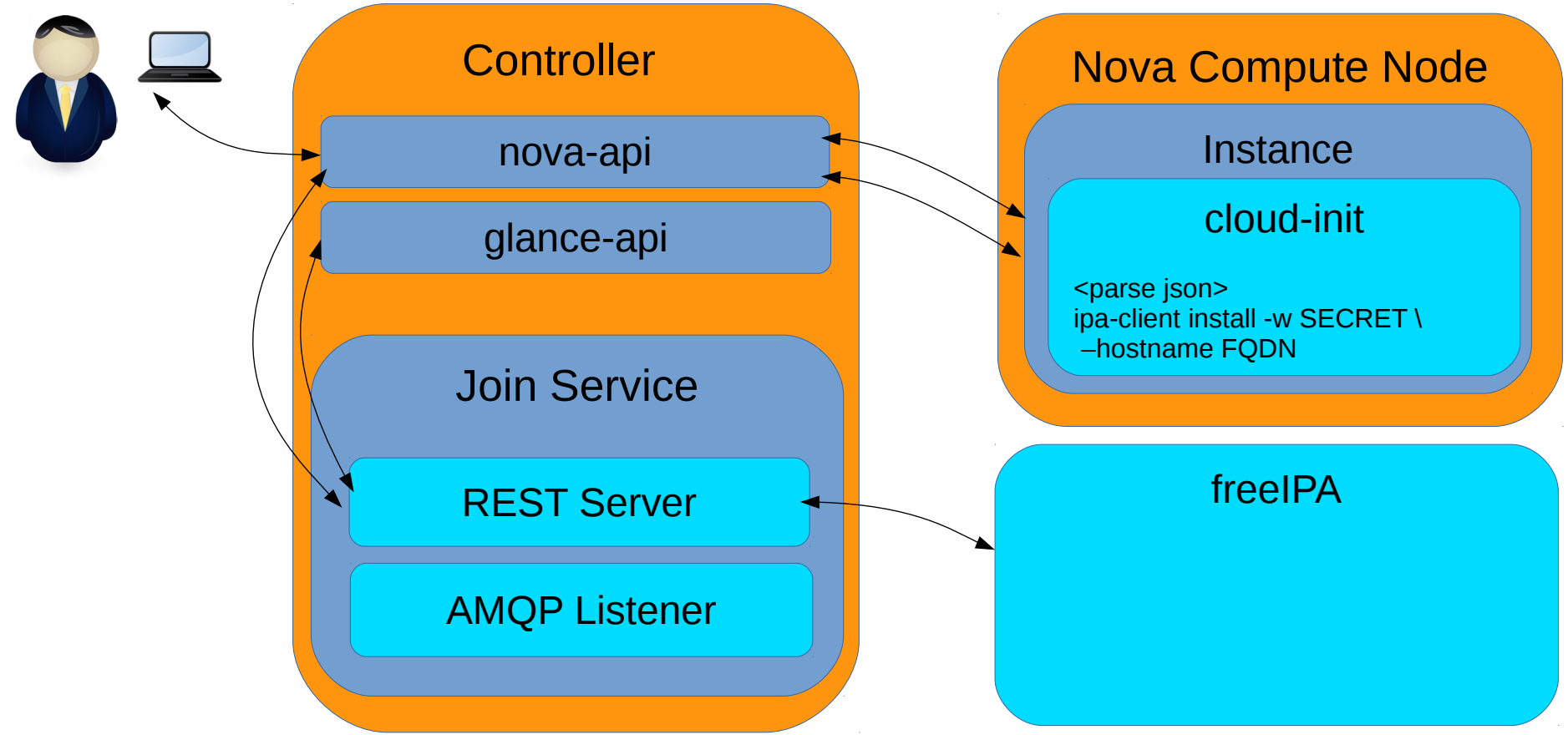
Add host to freeIPA



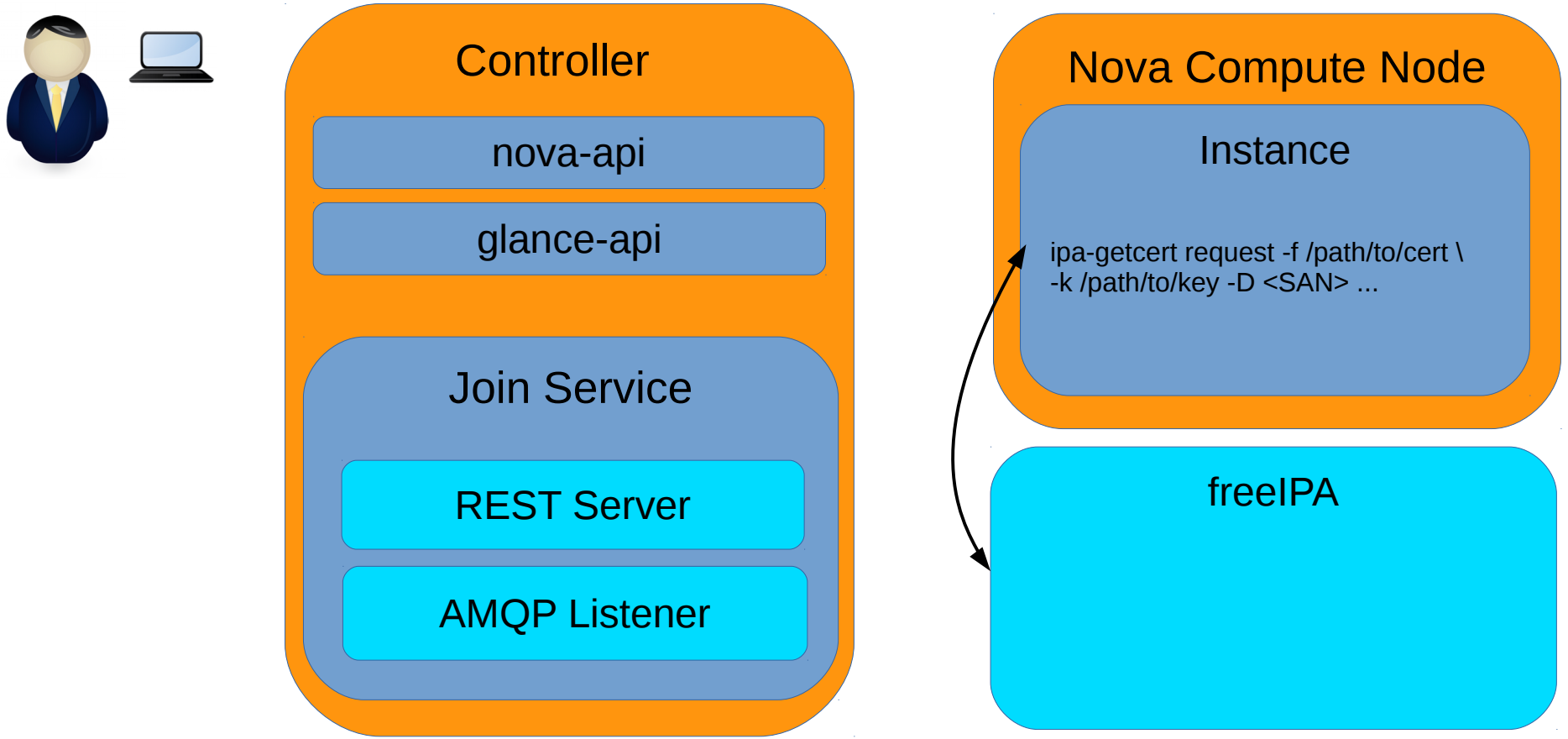
Return OTP and hostname



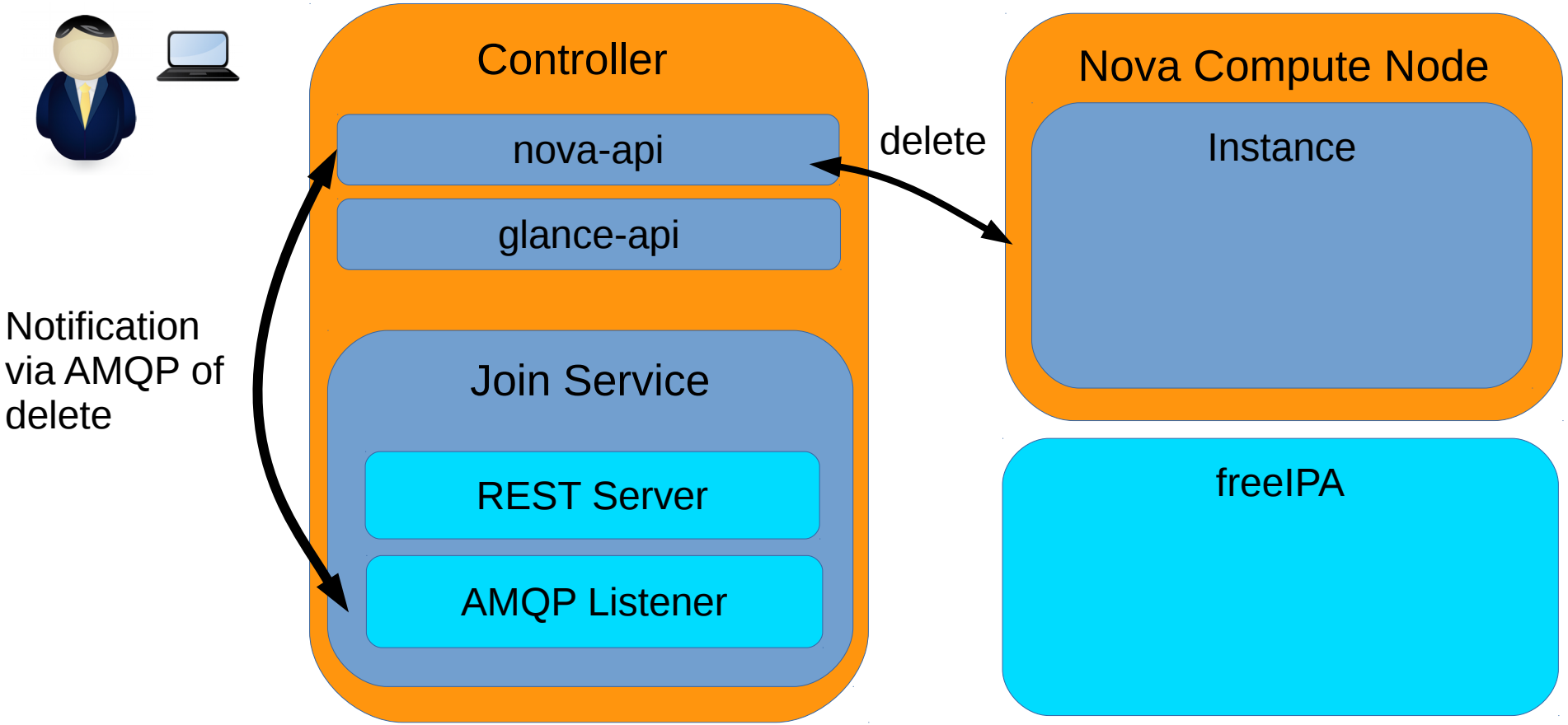
Parse output, enroll client



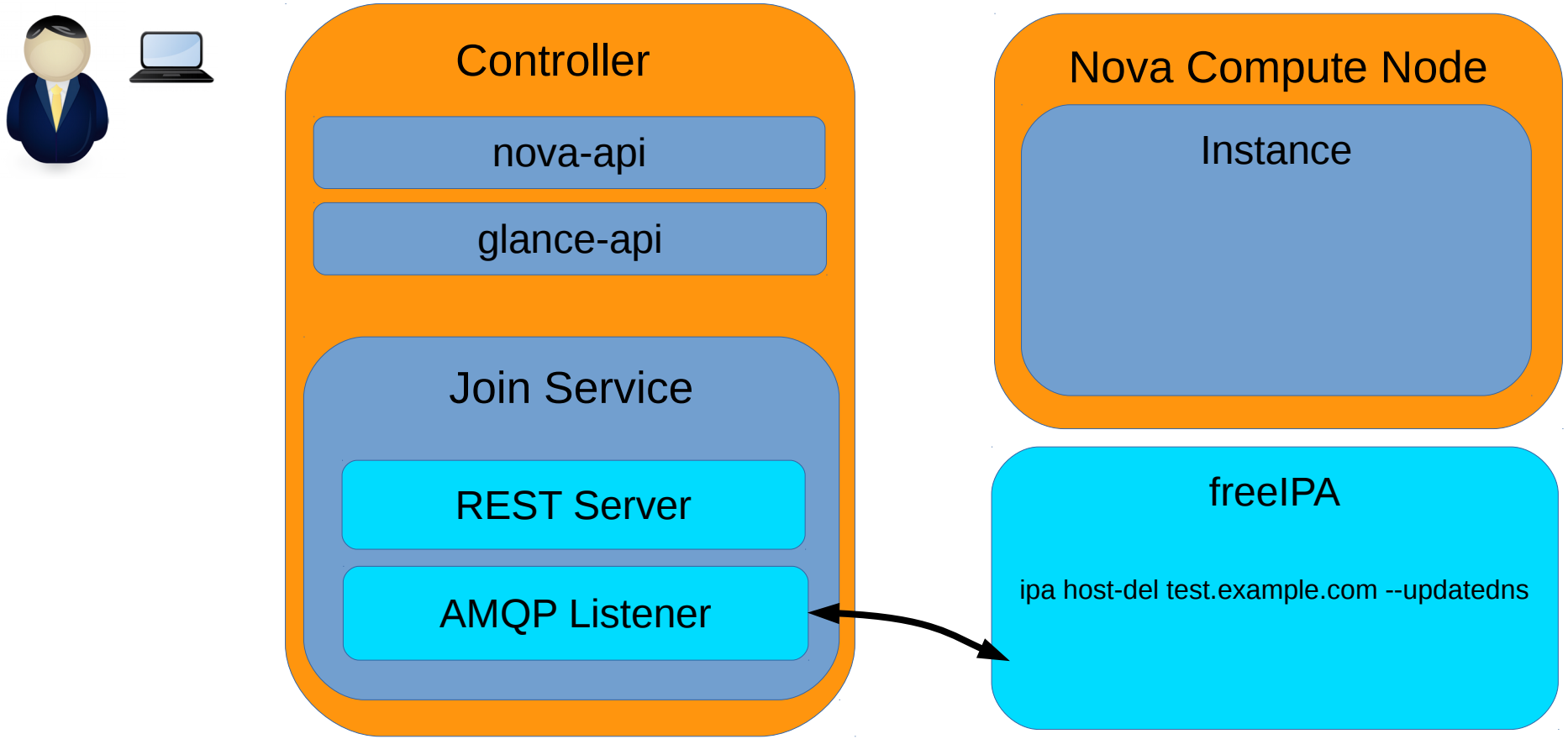
Get a cert with certmonger



Delete notification received by novajoin-notify



Host is removed from IPA



Additional Resources

- Full version of this talk:
  - https://www.youtube.com/watch?v=P86qMU3yN1Y
- TLS setup through novajoin will be delivered in RHOS 12.
- Quickstart script
  - extra node on which IPA server is deployed
  - https://goo.gl/rdTJy3


Questions?