Unattended CDN OS Upgrade

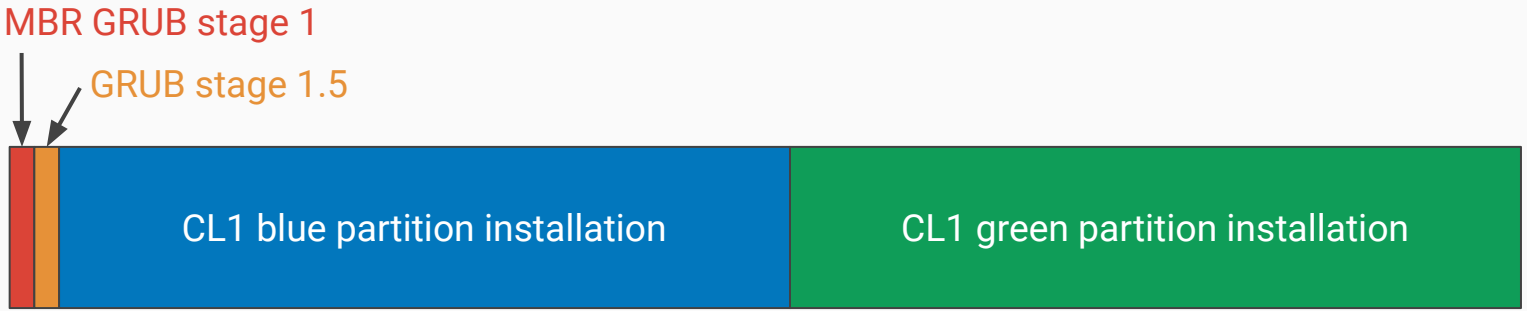
Velocix, Nokia Video Business Unit

Background

- Velocix video CDN deployed within large media and telco enterprises.
- Commodity server hardware operated as “black box” appliances.
- Appliances run a custom OS called “CL1” loosely based on an old Fedora build with hotchpotch of custom and backported packages.

CL1 disk partition layout

- CL1 uses a blue/green partition configuration, allowing the update of the software in a different partition to the current running operating system.
- This allows for pre-installation of updates prior to a scheduled reboot into the new OS, as well as rollback to the previous partition in the event of failure.



CL1 to CL1 upgrade process

- Boot into blue partition.
- Download and stage updated RPM packages into blue partition.
- Install updated RPM packages into green partition.
- Update GRUB bootloader to boot green partition by default.
- Reboot.

Problem definition

- Engineering effort needed to patch and maintain CL1 was unsustainable.
- Implement an automated upgrade path from CL1 to the latest RHEL or CentOS. Henceforward referred to as EL7.

Available installation mechanisms

- Installation media via ISO image, physical media or network HTTPS RPM repository.
- Anaconda installation wizard loadable via local bootloader or PXE netboot.

Constraints

- No physical access to hardware appliance.
- No physical or virtual removable media capability.
- No access to out-of-band/lights-out management or BIOS boot order.
- Network access restricted to SSH via point-to-point VPN tunnel.
- Limited maintenance window.
- Rigid network topology precludes temporary servers or services to support an upgrade path.

Available installation mechanisms

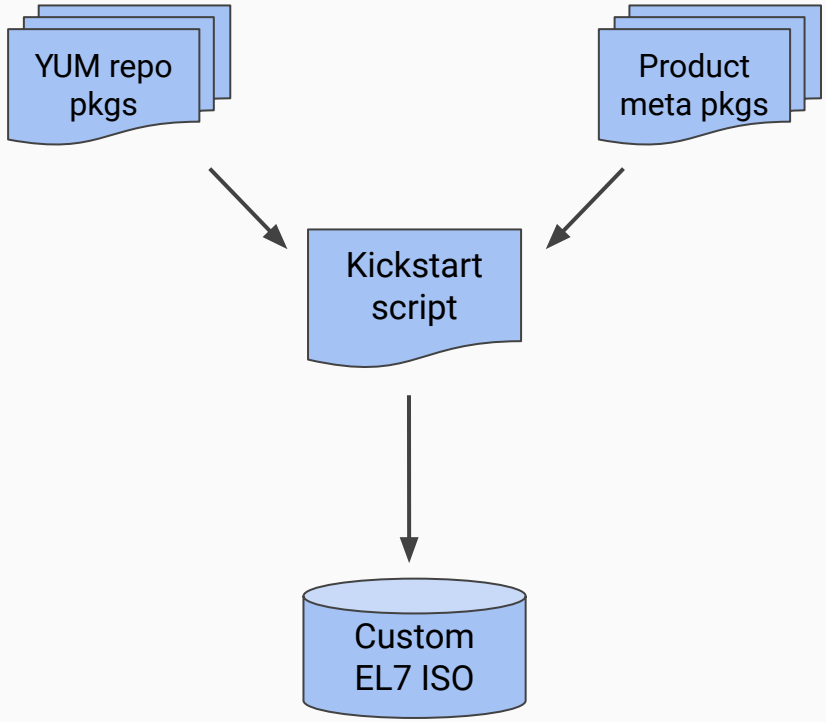
- Installation media via ISO image, ~~physical media~~ or network HTTPS RPM repository.
- Anaconda installation wizard loadable via local bootloader ~~or PXE netboot~~.
- Dismissed “hand-crafted” installation of RPMs and GRUB bootloader directly as it would partially defeat the goal of moving to a standardised commodity OS installation.
- Consequently limited to delivery of EL7 software over SSH and HTTPS, and invocation of installation bootloader from a local filesystem.

EL7 upgrade preparation

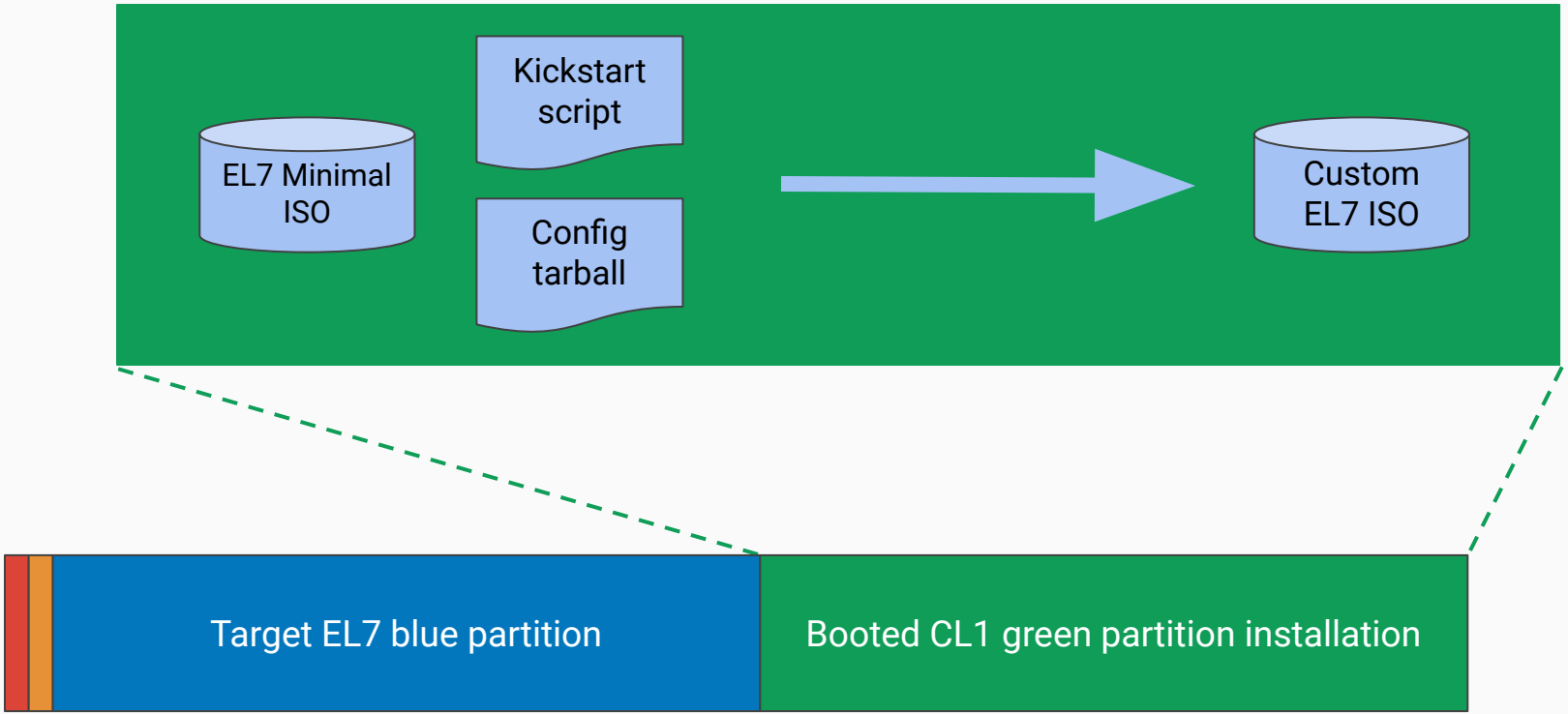
- Boot into green CL1 partition.
- Download and stage EL7 ISO into green partition.
- Tarball of configuration file is created.
- Custom Anaconda Kickstart script generated to automate EL7 install.
- Custom EL7 ISO image is built, incorporating new packages, tarball of configuration files and custom Anaconda Kickstart script.

Product packages

- One or more “YUM repo” packages, which install the correct repository definitions for the target product release.
- One or more “product meta packages” which contain a product name and version, required dependencies on all RPM packages necessary to install the particular appliance type.

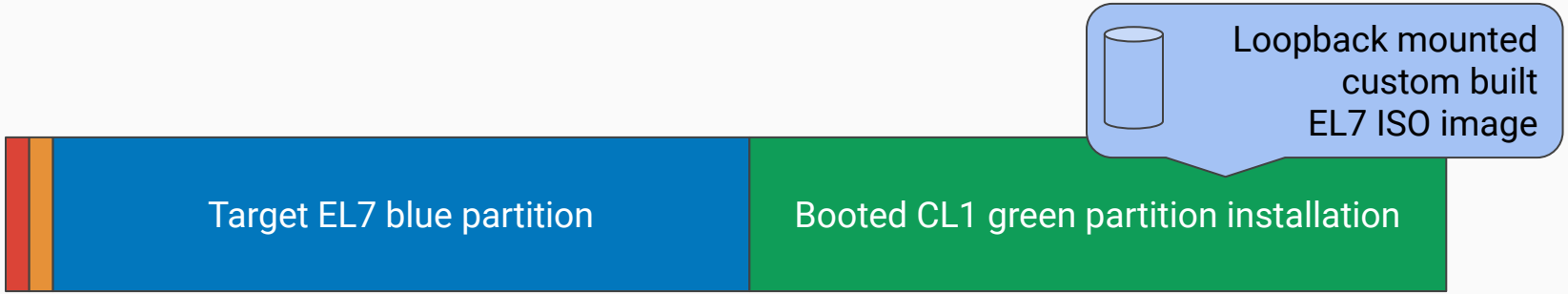


EL7 upgrade preparation



EL7 upgrade process

- Custom EL7 ISO image is loopback mounted from green partition.
- Kernel pivot into EL7 installer located on the loopback mounted EL7 ISO image, passing in the location of the custom Kickstart install script.

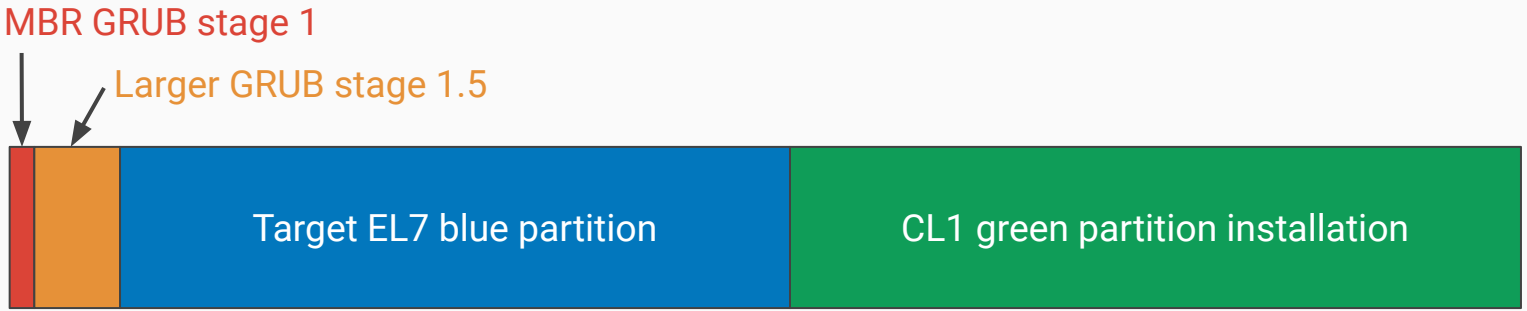


EL7 upgrade process

```
kexec -l \
  "/loopbackpath/isolinux/vmlinuz" \
  "--initrd=/loopbackpath/isolinux/initrd.img" \
  "--append=inst.stage2=hd:/dev/xdc2:/somepath/el7.iso
   biosdevname=1 net.ifnames=1
   inst.ks=hd:/dev/xdc2:/somepath/ks.cfg"
kexec -e
```

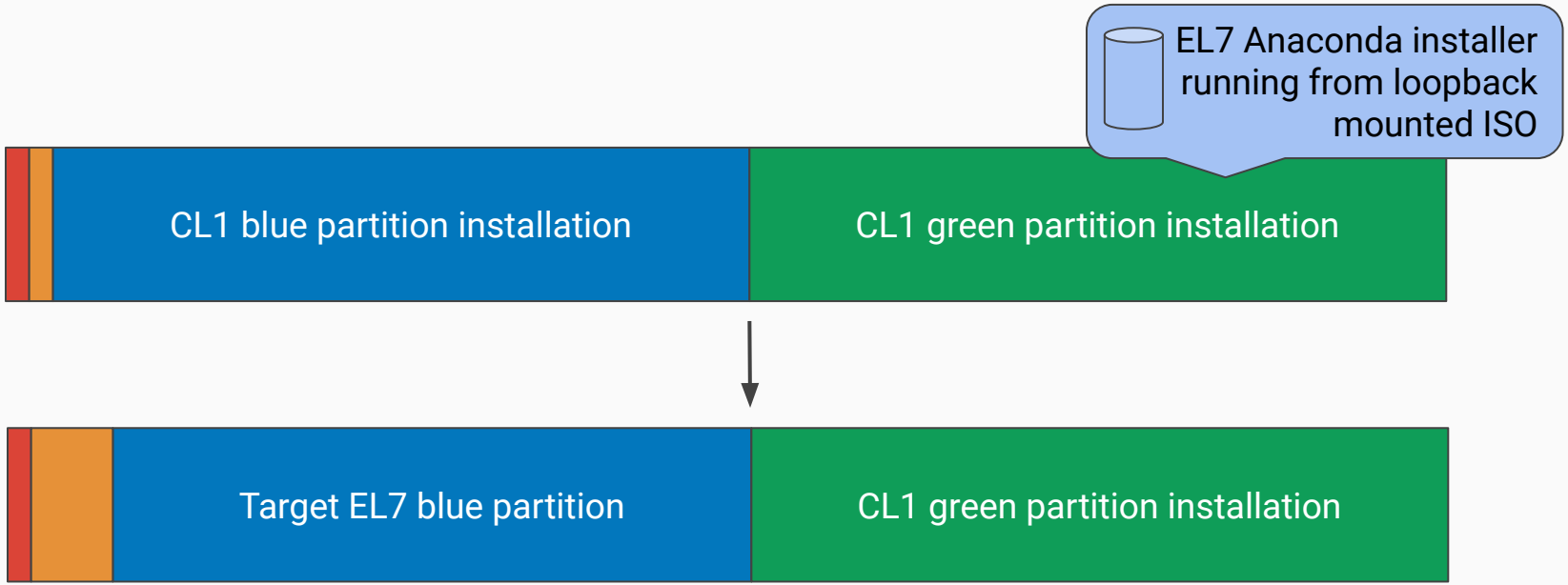
Target EL7 disk partition layout

- The GRUB stage 1.5 is much larger in EL7 compared to the version of GRUB used in CL1, and will no longer fit in the space between the MBR and the start of the blue partition at the start of the disk.
- This necessitated the slight shrinking and shifting of the blue partition by a few MB, and thus consequently required that EL7 be installed into this newly created blue partition.



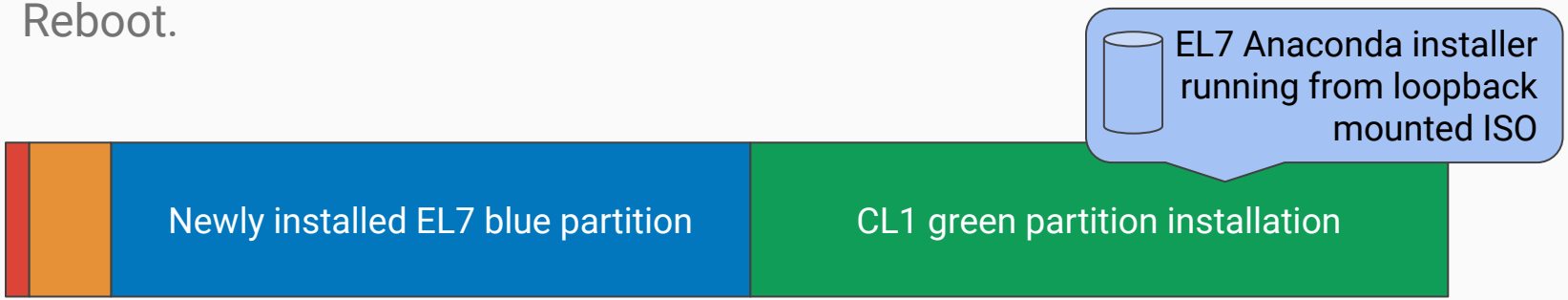
EL7 upgrade process

- Kickstart install script deletes and recreates the blue partition to start further into the disk, to allow for the larger GRUB stage 1.5 bootloader.



EL7 Kickstart script summary

- Partitions are analysed, and blue partition is recreated as necessary.
- EL7 is installed into the blue partition.
- Package repositories defined and product packages are installed.
- Configuration files are put back in place and file permissions fixed up.
- Update GRUB bootloader to boot blue partition by default.
- Reboot.

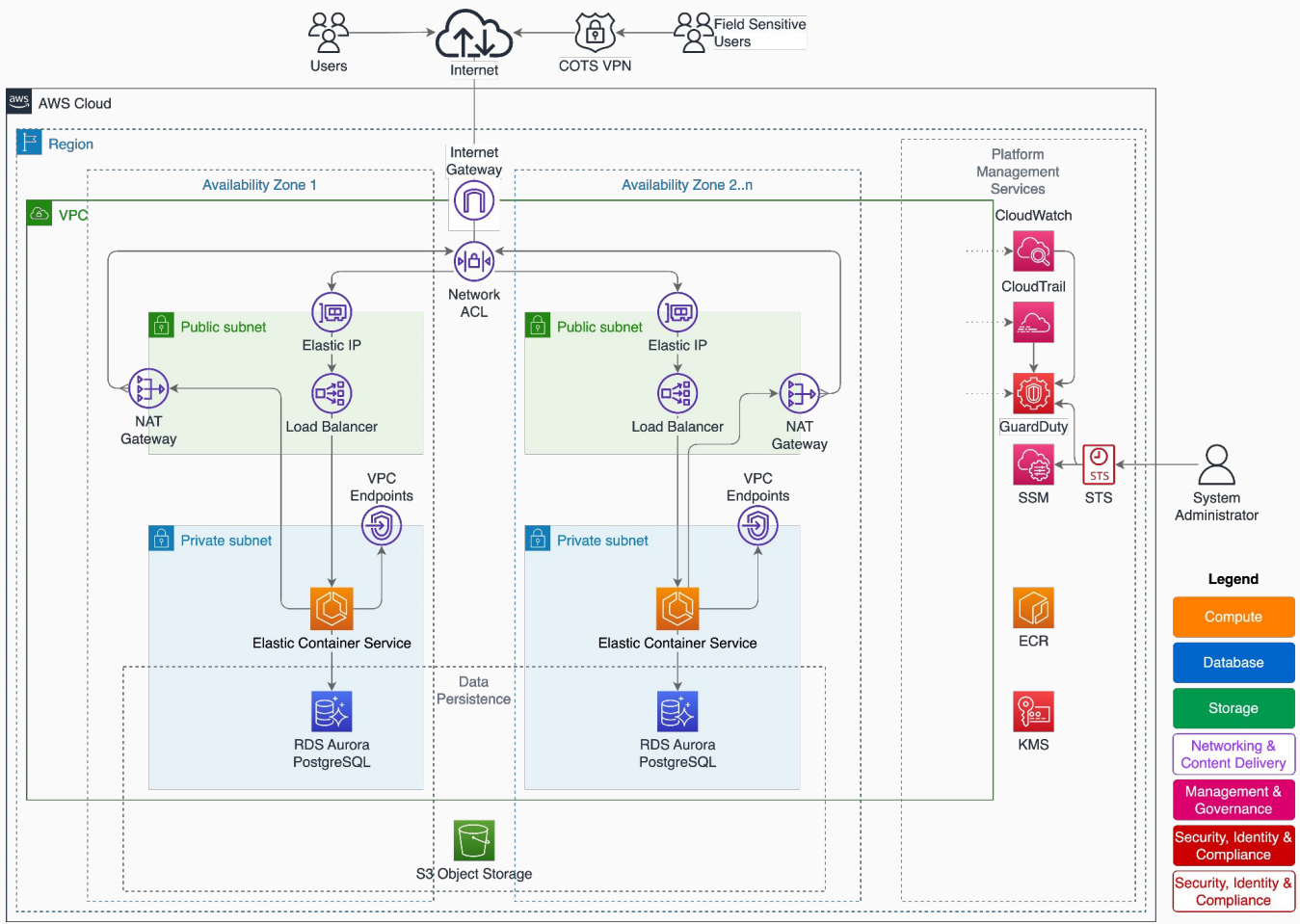


DFI SaaS Platform

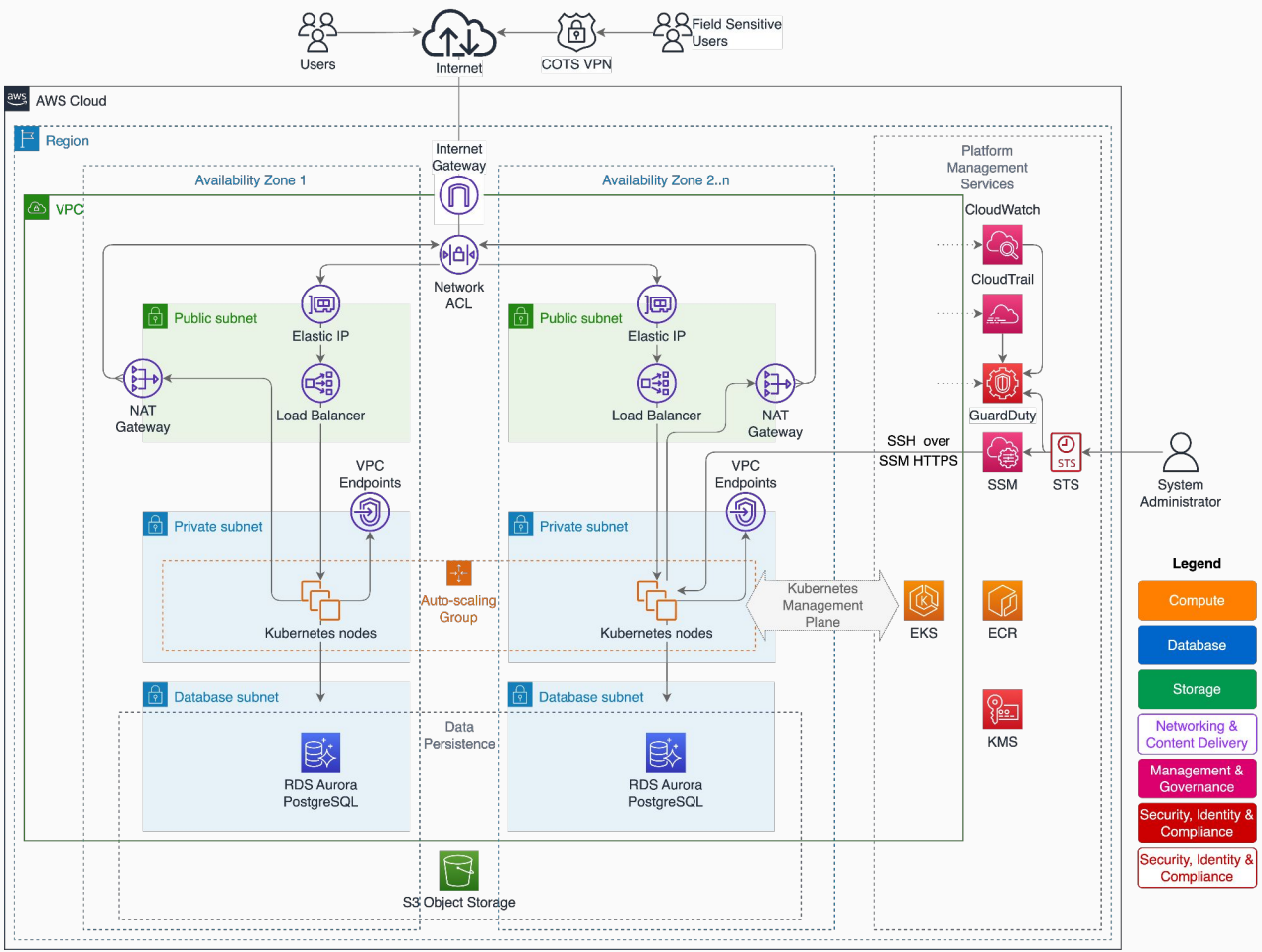
Excession Technologies

DFI SaaS platform

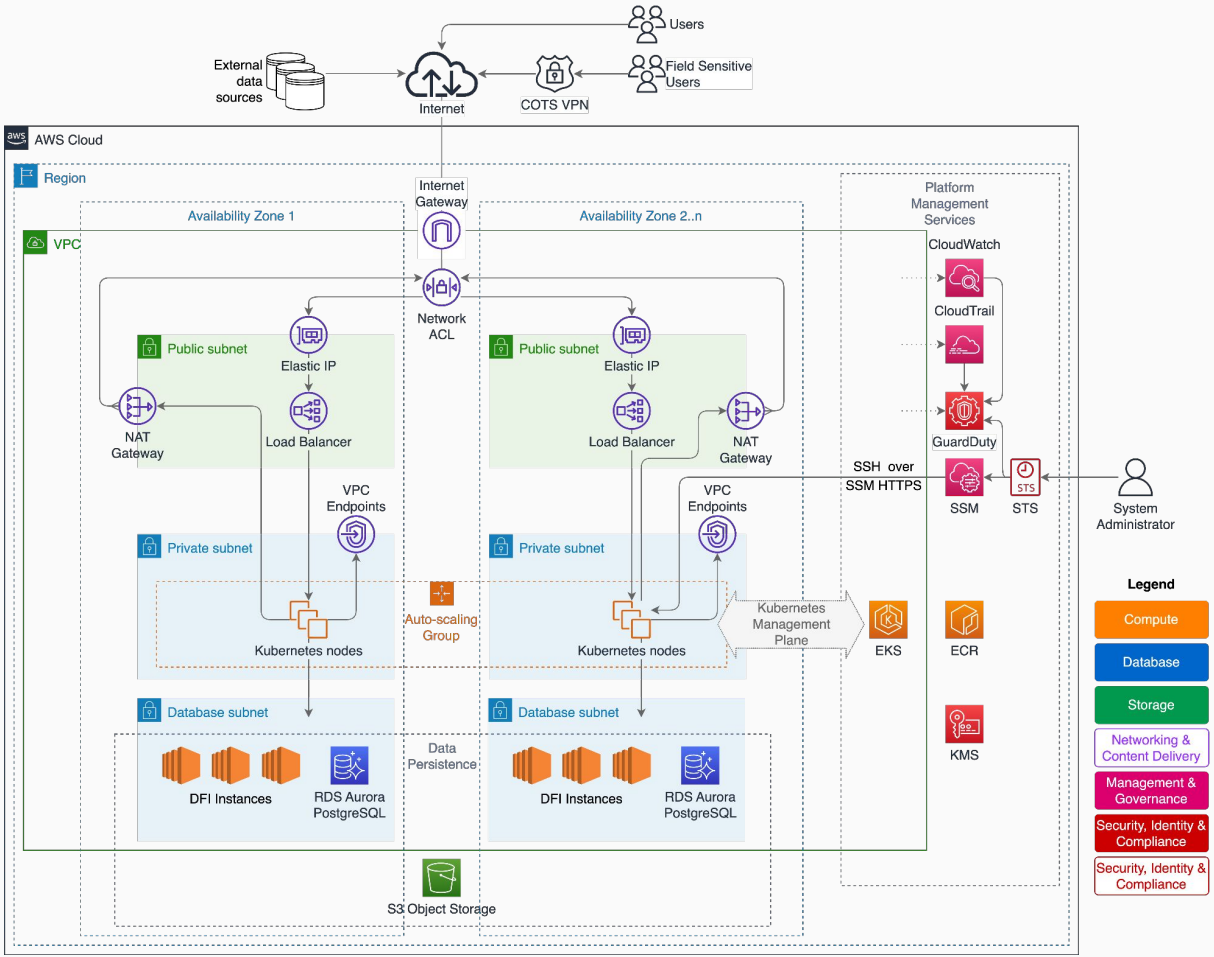
- AWS infrastructure diagrams for the Excession DFI SaaS platform as a discussion point for something more contemporary in case the previous fun problem was a bit too far off-piste.
- These are diagrams that I compiled over time to illustrate our platform infrastructure to our developers and customers alike.
- I can talk about the logical progression of the platform over time, from proof-of-concept, to early alpha to delivery of our first production MVP.



DFI SaaS platform – single user Streamlit proof-of-concept AWS infrastructure



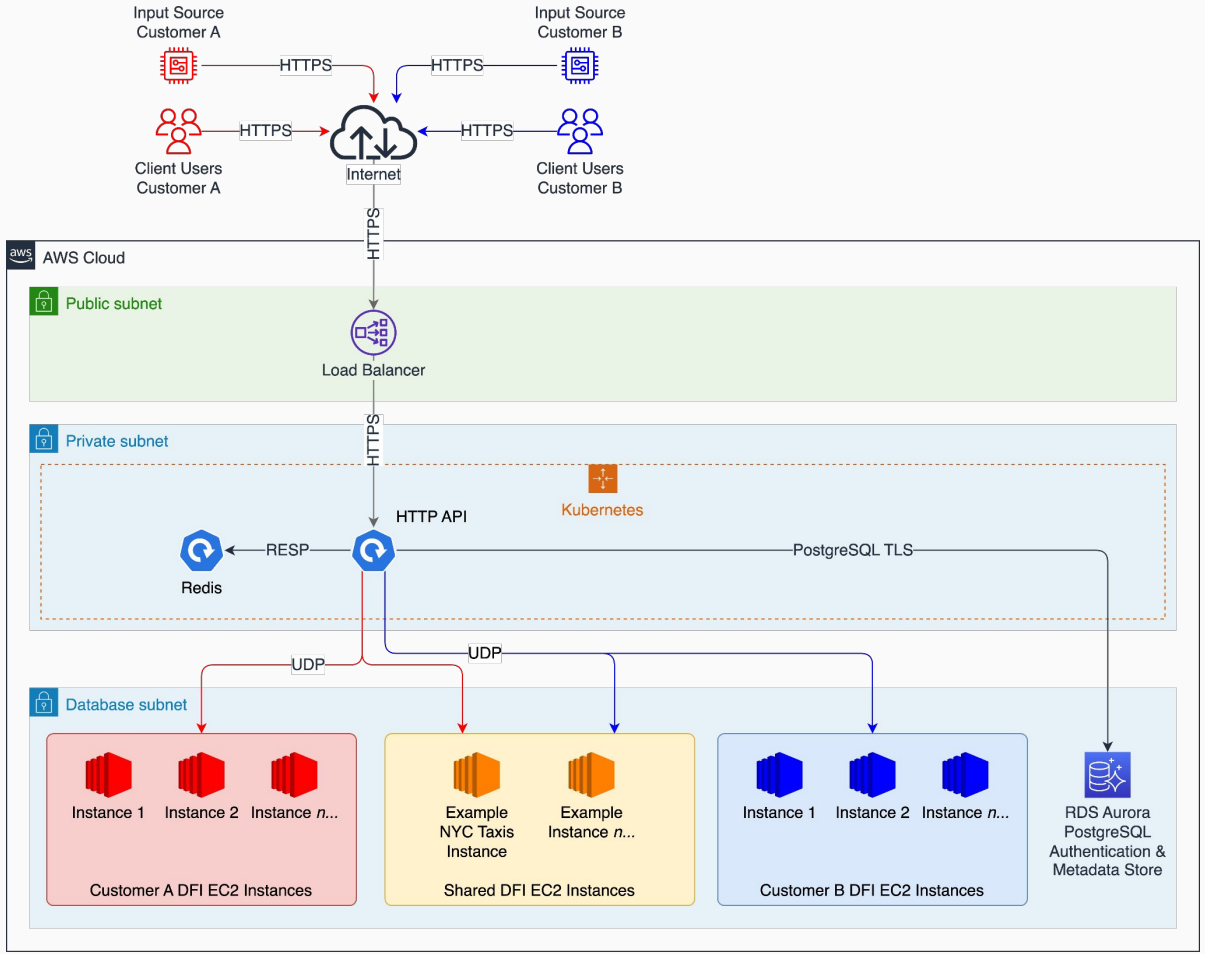
DFI SaaS platform – alpha transition RDS-based AWS infrastructure



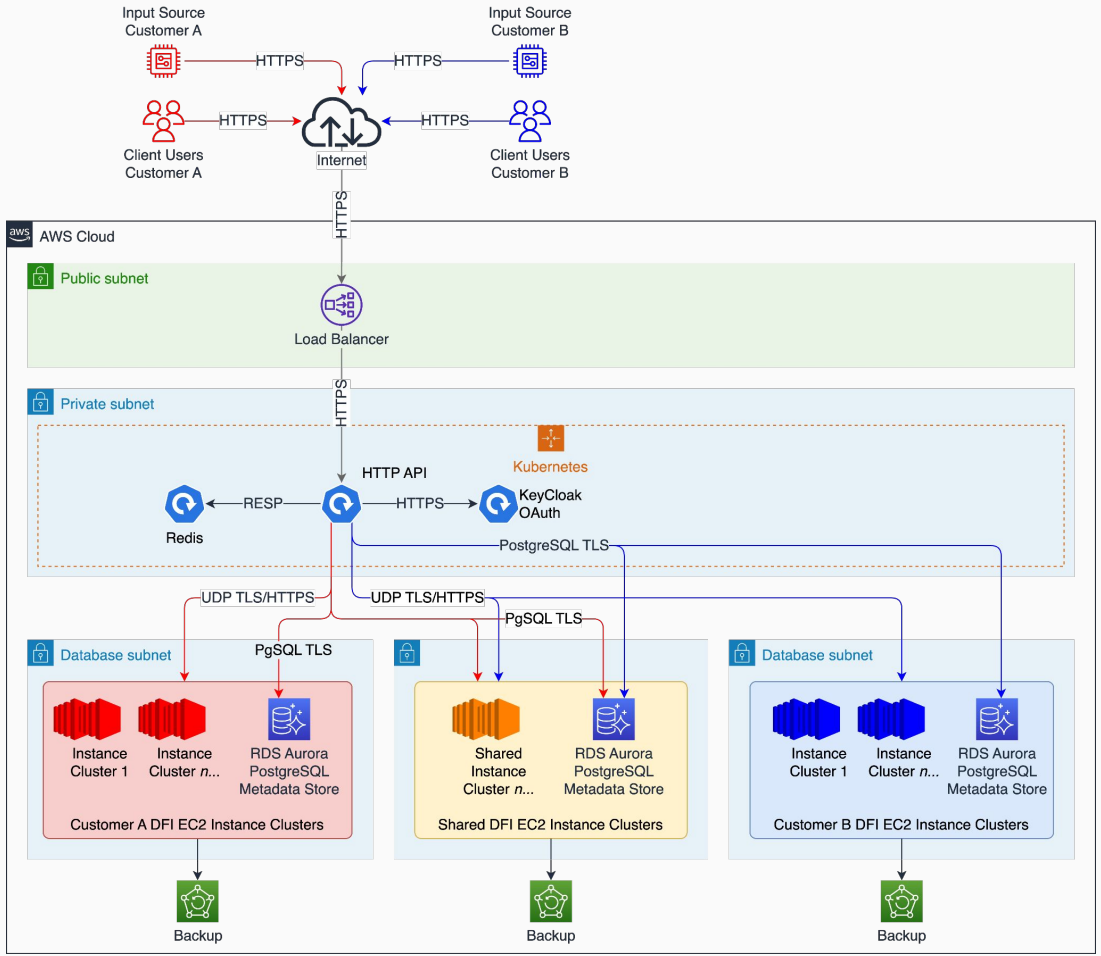
DFI SaaS platform - DFI backed MVP AWS infrastructure

Query path

- The following diagrams show the query path from the end user client, through the platform to the underlying data stores.
- These are tailored to the multi-tenancy SaaS offering.



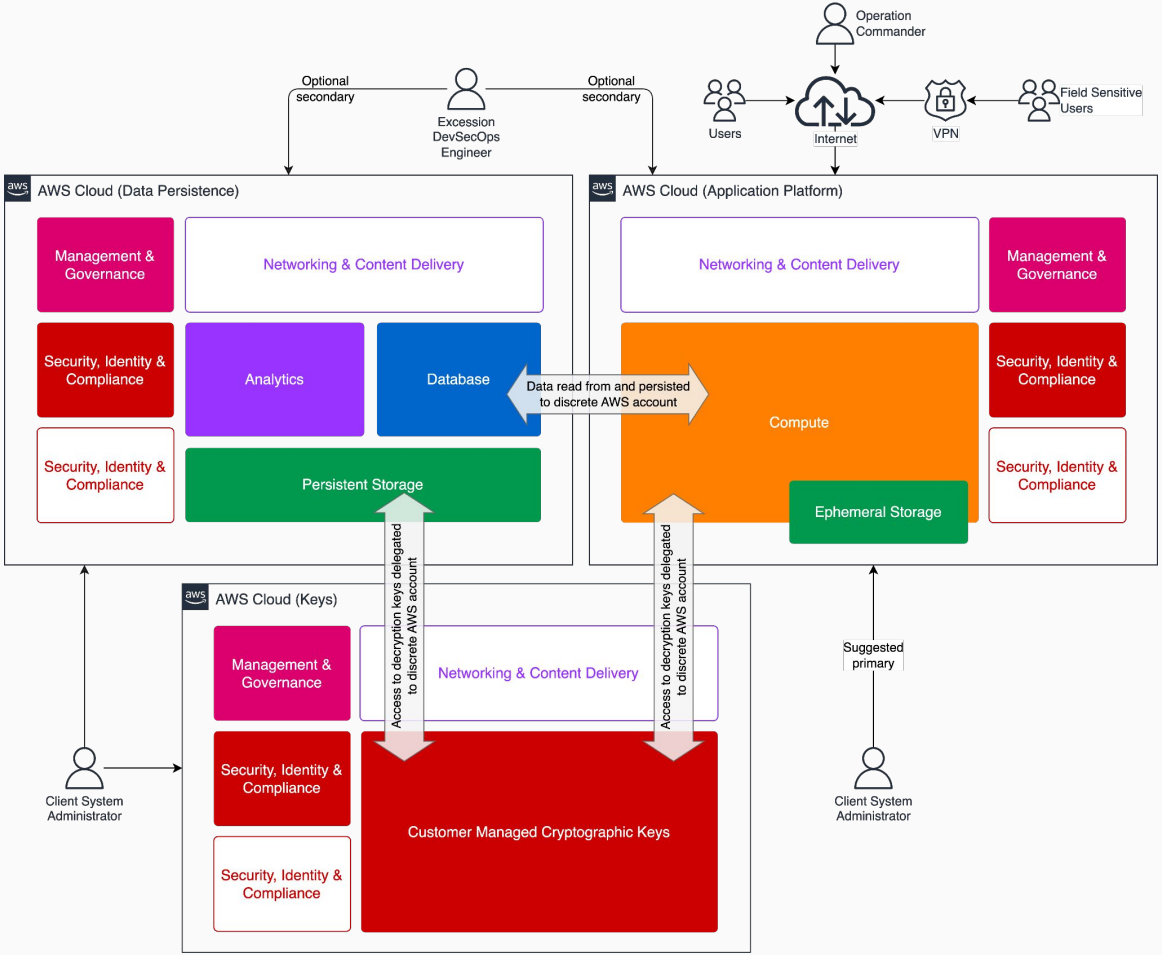
DFI SaaS platform – multi-tenancy logical query path



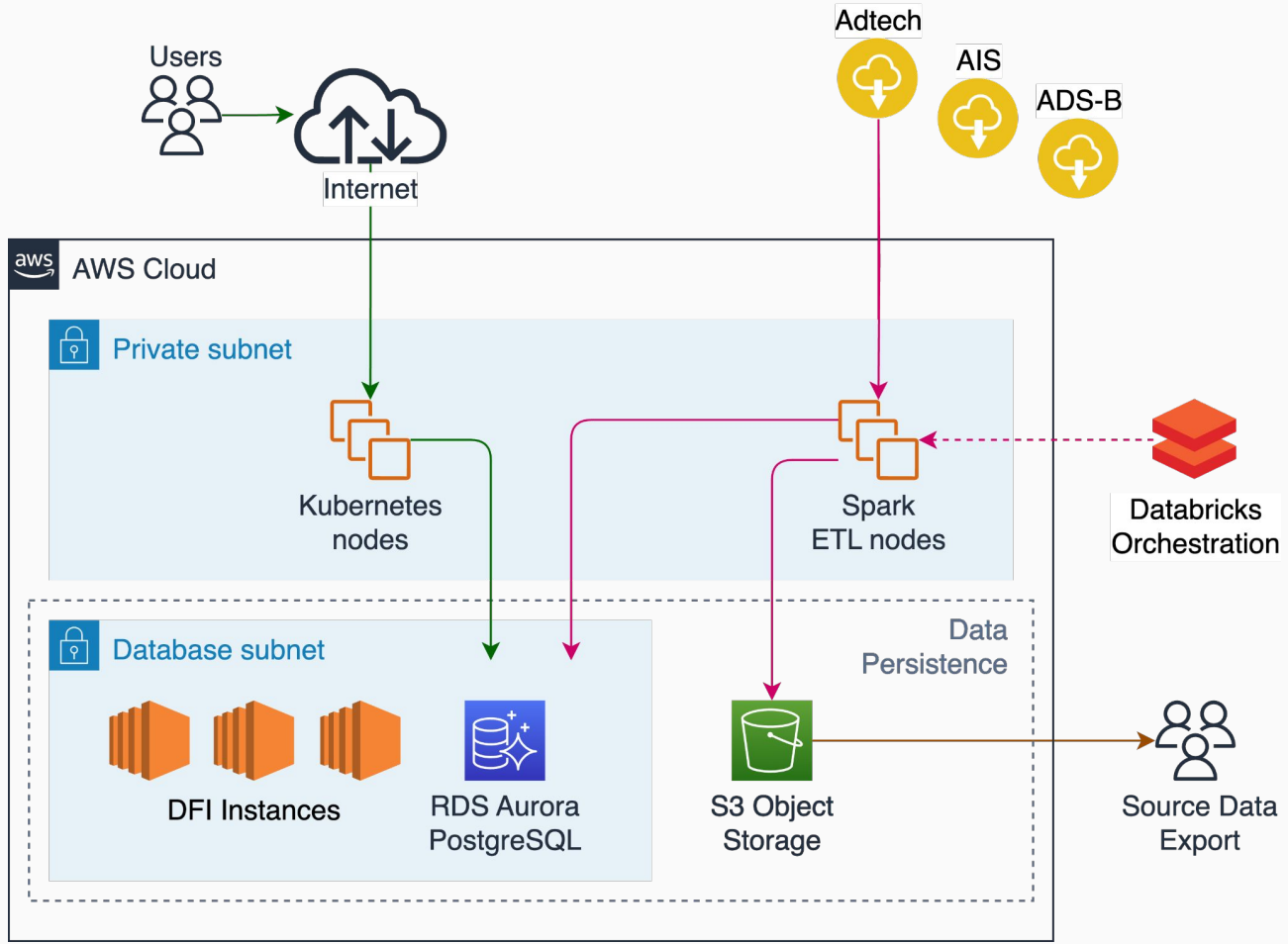
DFI SaaS platform – multi-tenancy logical query path – noisy neighbour metadata store isolation + backup

Dedicated managed platform

- Public sector and fortune 500 customers demand dedicated managed platforms rather than multi-tenancy.



DFI managed platform – separation of data and cryptographic keys from runtime compute



DFI managed platform - data ETL and export path