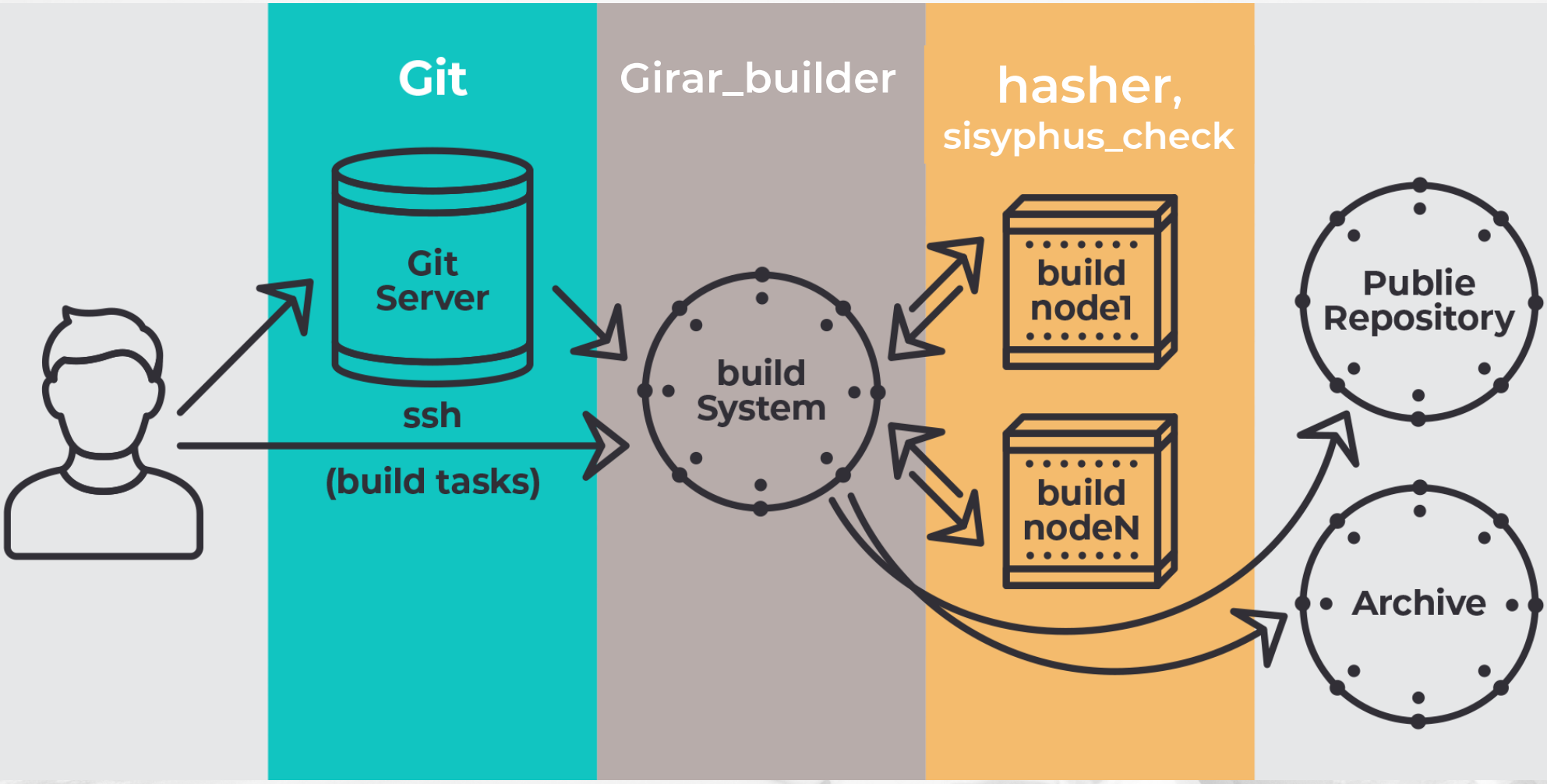
ООО «Базальт СПО»

Развитие инструментария безопасной сборки «Альт»

Алексей Шабалин
Начальник отдела систем виртуализации и облачных технологий
ООО «Базальт СПО»
shaba@basealt.ru


Git
Girar_builder
hasher,
sisyphus_check
Git
Server
ssh
(build tasks)
build
System
build
node1
build
nodeN
Publie
Repository
Archive

hasher

- **hasher** — это инструмент безопасной и воспроизводимой сборки пакетов. Все пакеты Sisyphus собираются с его помощью. https://www.altlinux.org/Hasher
- Весь «опасный» код с повышенными привилегиями вынесен в **hasher-priv**. Минимален и легко читаем для упрощения аудита кода.
- **sisyphus_check** — инструмент для проверки пакетов на соответствие правилам Sisyphus https://www.altlinux.org/Sisyphus_check
- Используется с 2003 года
- Доклад «Инфраструктура разработки Sisyphus» от 2017 OSDAY, Дмитрий Левин

hasher

#hasher-useradd user:

- user:x:500:500: System User:/home/user:/bin/bash
- user_a:x:501:501:1st hasher satellite for shaba:/dev/null:/dev/null - rooter
- user_b:x:502:502:2nd hasher satellite for shaba:/dev/null:/dev/null - builder

#hsh ~/hasher path/to/foobar-0.0-alt0.src.rpm

- Установка в ~/hasher базовой системы(apt-get install) от пользователя user_a (fakeroot)
- Установка сборочного окружения на основе анализа BuildRequires (apt-get build-dep) от пользователя user_a (fakeroot)
- chroot в ~/hasher
- Сборка rpm пакета (rpmbuild) от пользователя user_b

*** сборка пакетов от root запрещена по-умолчанию.**

vm-run

- Vm-run (rpm-build-vm) — инструмент для запуска команд под qemu с псевдо-рутовыми привилегиями

https://www.altlinux.org/Hasher/vm-run

- Используется с 2019 года.

- %check
- make check

- %check
- vm-run make check

OCI Image

- Docker, buildah, buildkit — все требуют **root** привелегий
- kernel.unprivileged_userns_clone=1 представляет еще большую угрозу безопасности
- **Позволить запуск таких инструментов внутри hasher невозможно.**

- Vm-run позволит запускать сборочные утилиты OCI образов

Интеграция инструментов

- Git хостинг git.altlinux.org
- Hasher инструмент безопасной и воспроизводимой сборки
- Vm-run инструмент для безопасного запуска команд в qemu
- Girar_builder сборочница rpm пакетов и публикация в репозитории Sisyphus. Для сборки используется hasher.
- registry.altlinux.org реестр OCI (docker) образов

Вопросы?

Контакты
Тел.: +7 (495) 123-47-99
basealt.ru
E-mail:
sales@basealt.ru

оптовые продажи:
sales@basealt.ru

Офисы:

Москва,
ул. Бутырская, д. 75

Санкт-Петербург,
Коломяжский пр-т, 27,
БЦ «Содружество», 3
этаж

Саратов,
ул. Октябрьская 44,
корпус А, офис № 3

Обнинск,
ул. Королёва, д. 4Б, БЦ
“Британика”