



深圳站

# GOPS 全球运维大会

2023 - XOps 风向标

时间：2023年4月7日-8日 地址：中国·深圳

指导单位：



主办单位：



承办单位：



# 软件制品管理之道 - The JFrog Way



## 王青 JFrog (中国) 技术总监

十五年敏捷研发管理与软件工程实践经验，目前任 JFrog 中国技术团队负责人  
为大型企业制品库建设提供咨询  
Qcon明星讲师, GOPS金牌讲师



# 目录

## 01 企业在软件制品管理遇到的挑战

## 02 软件制品管理之道 JFrog Way

## 03 回顾

01

# 企业在软件制品管理 遇到的挑战

# 企业在软件制品管理遇到的挑战

## 开发者

制品版本管理混乱  
如何修复漏洞？

## 测试

无法自动获取最新版本  
无法关联测试结果

## 运维

缺乏唯一可信源制品库

## 安全

安全扫描和DevOps流程脱节  
无法阻止高危漏洞版本的使用



02

# 软件制品管理之道

## The JFrog Way

## JFrog 流动式软件交付

“我们的目标是把软件更新的方式，从传统大块，低频率的变更模式，转变成成为细小的，极其频繁的变更模式。

变更变得极其细微和频繁，以至于看起来就像水流一样流动到目标环境”

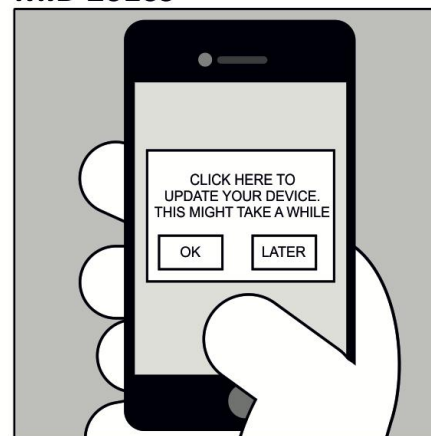
LATE 1990s



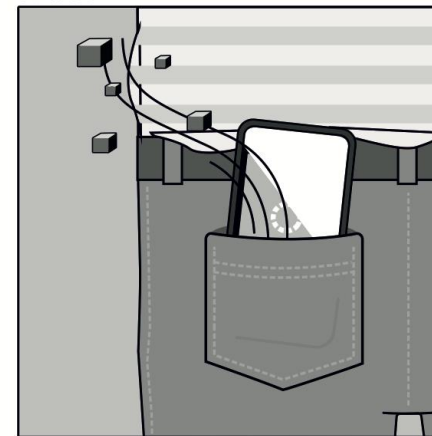
MID 2000s



MID 2010s

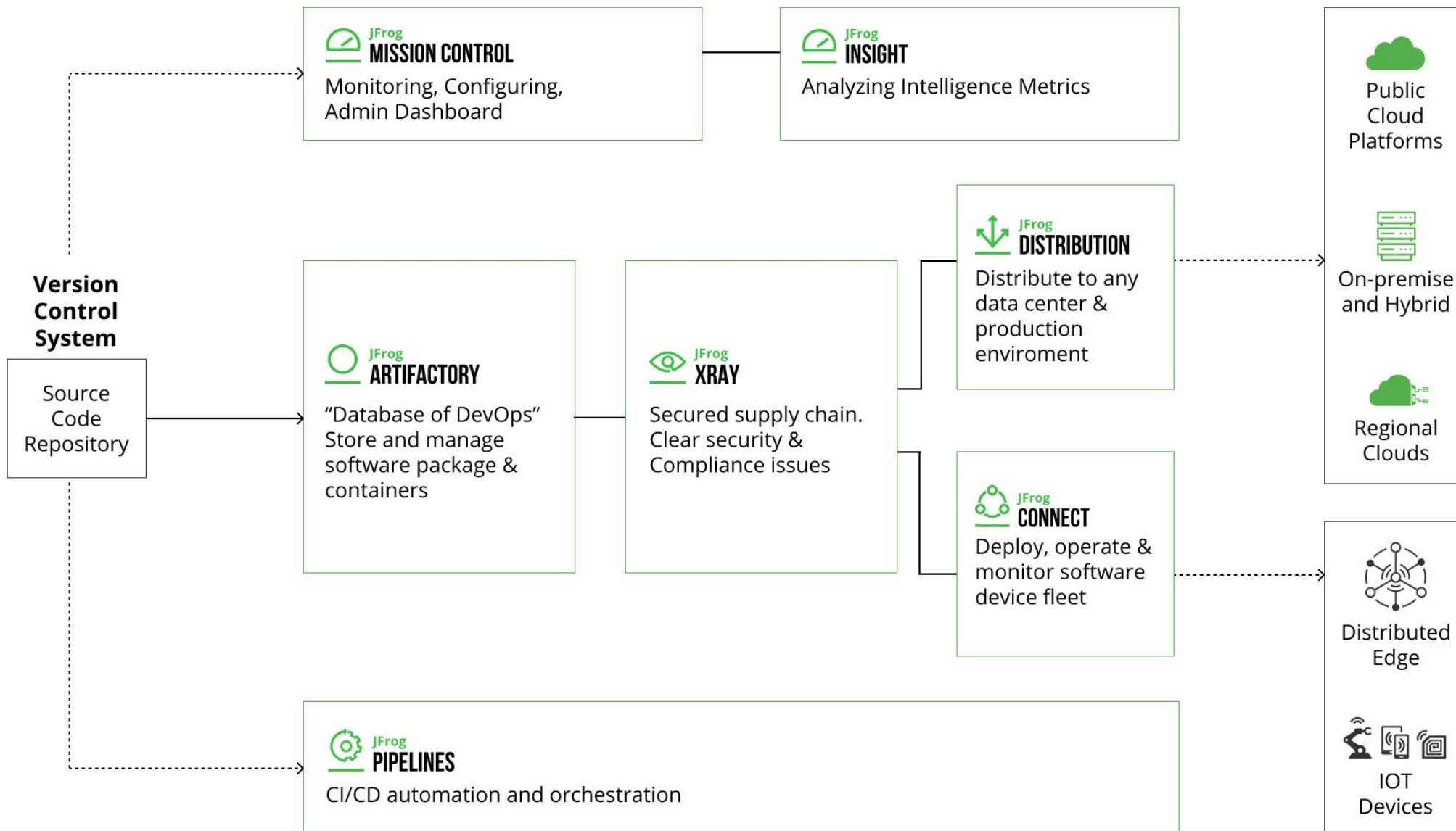


NOW



The Evolution of Mobile Updates

# 流动式软件交付





# The JFrog Way



## 开发者

构建加速  
专业的制品版本管理

## 测试

自动获取最新版本  
自动关联测试结果



## 运维

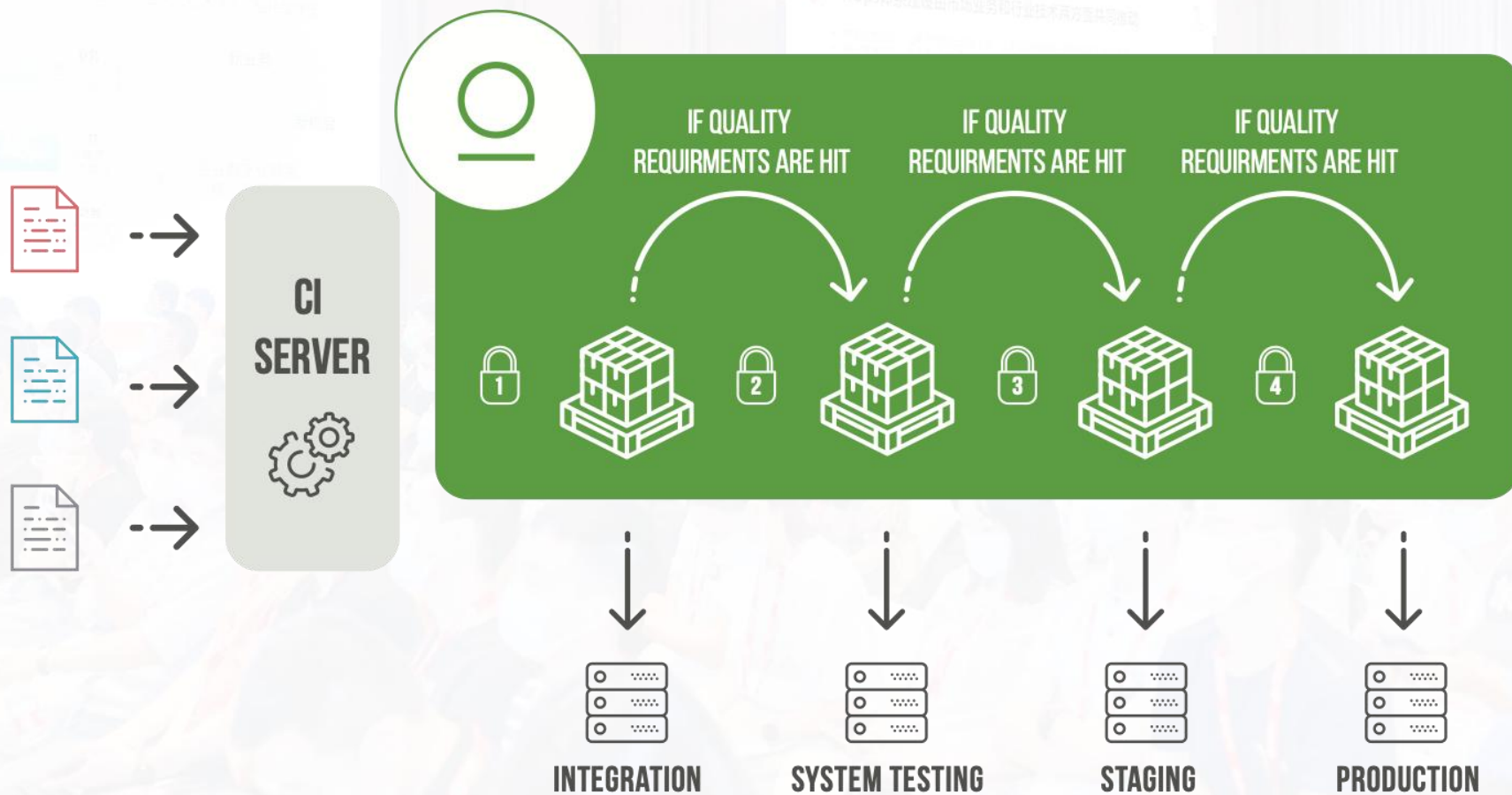
高可用的制品库  
多地制品快速同步和分发

## 安全

安全扫描融入DevOps流程  
阻止高危漏洞版本的使用

高效

# 流动式软件交付

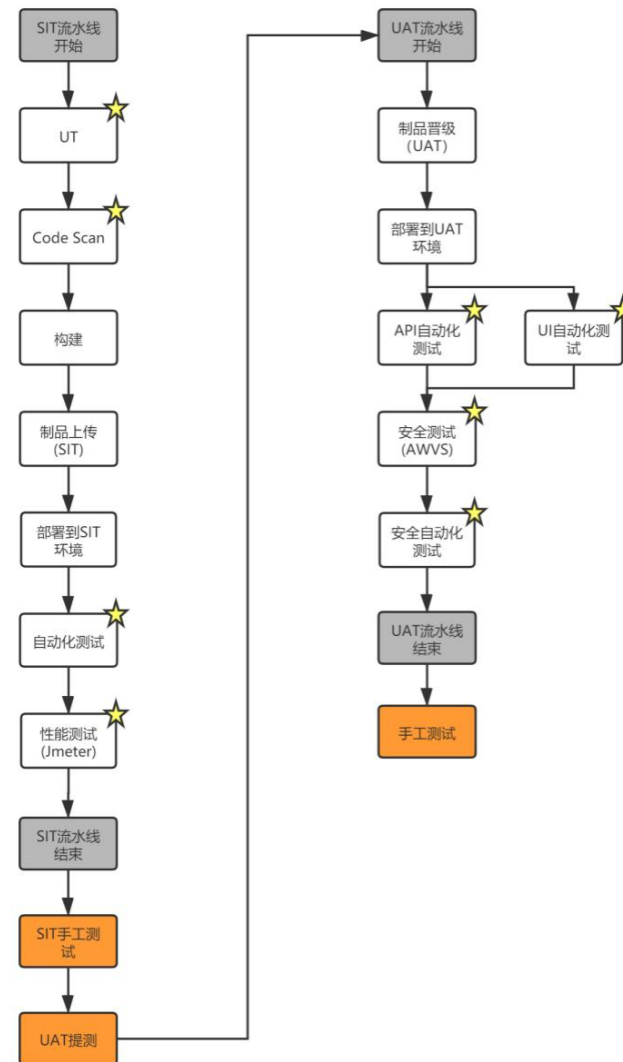


- QUALITY GATES -

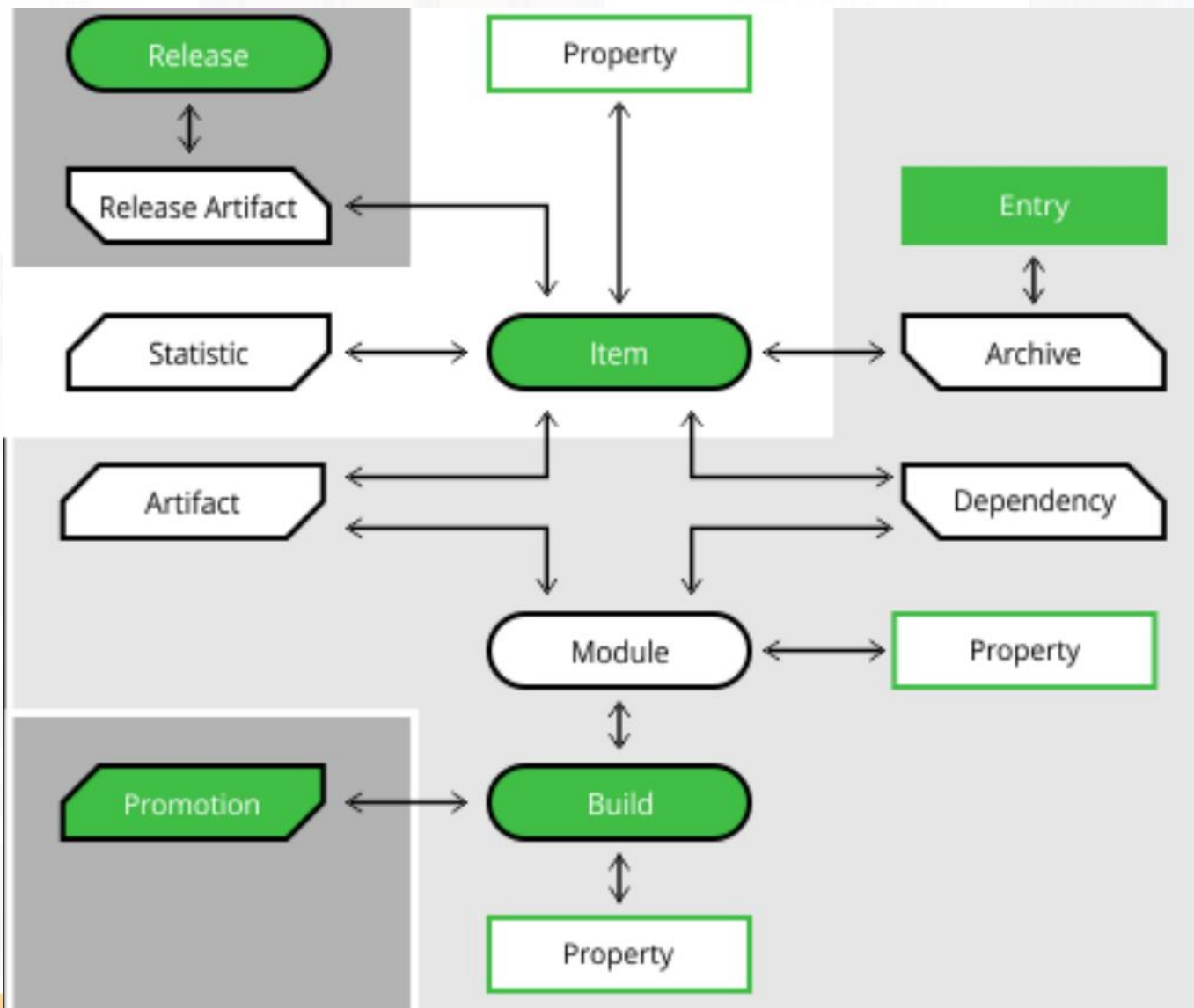
# 记录制品流转元数据，实现质量可信

10.0-9.tar.gz

General	Effective Permissions	Xray	Properties
<input checked="" type="checkbox"/> Property		Value(s)	
<input type="checkbox"/> branchName		release	
<input type="checkbox"/> build.name		pipeline-10311-10.0-9	
<input type="checkbox"/> build.number		9	
<input type="checkbox"/> build.timestamp		1598451773217	
<input type="checkbox"/> itilIsSubmit		false	
<input type="checkbox"/> itilStatus		0	
<input type="checkbox"/> portalVersion		beta2020082602	
<input type="checkbox"/> projectId		trade	
<input type="checkbox"/> sitPassTest		true	
<input type="checkbox"/> tag		2.10.0-9	
<input type="checkbox"/> uatIsDeploy		true	
<input type="checkbox"/> uatPassTest		true	
<input type="checkbox"/> version		2.10.0	



# 通用部署包的数据模型





# 创建和分发发布单元



Distributable > guestbook > 1.0.15

Version Actions ▾

## Version 1.0.15

State: Ready | Created 22-07-20 17:57:01 +0800

**Completed**  
Status

**100% (1 / 1 Nodes)**  
Delivered

**197MB**  
Size

**Availability**

Actions Tracking Content Release Notes Xray Data Pipelines Spec Effective Permissions

Artifacts Builds Release Bundle Info

discovery-service (5)



gateway-service (5)



Files (1)



guestbook-1.0.15.tgz

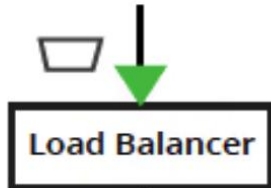
demo-helm-dev-local/guestbook/1.0.15/guestbook-1.0.15.tgz

## 制品库的性能 - 读、写缓存

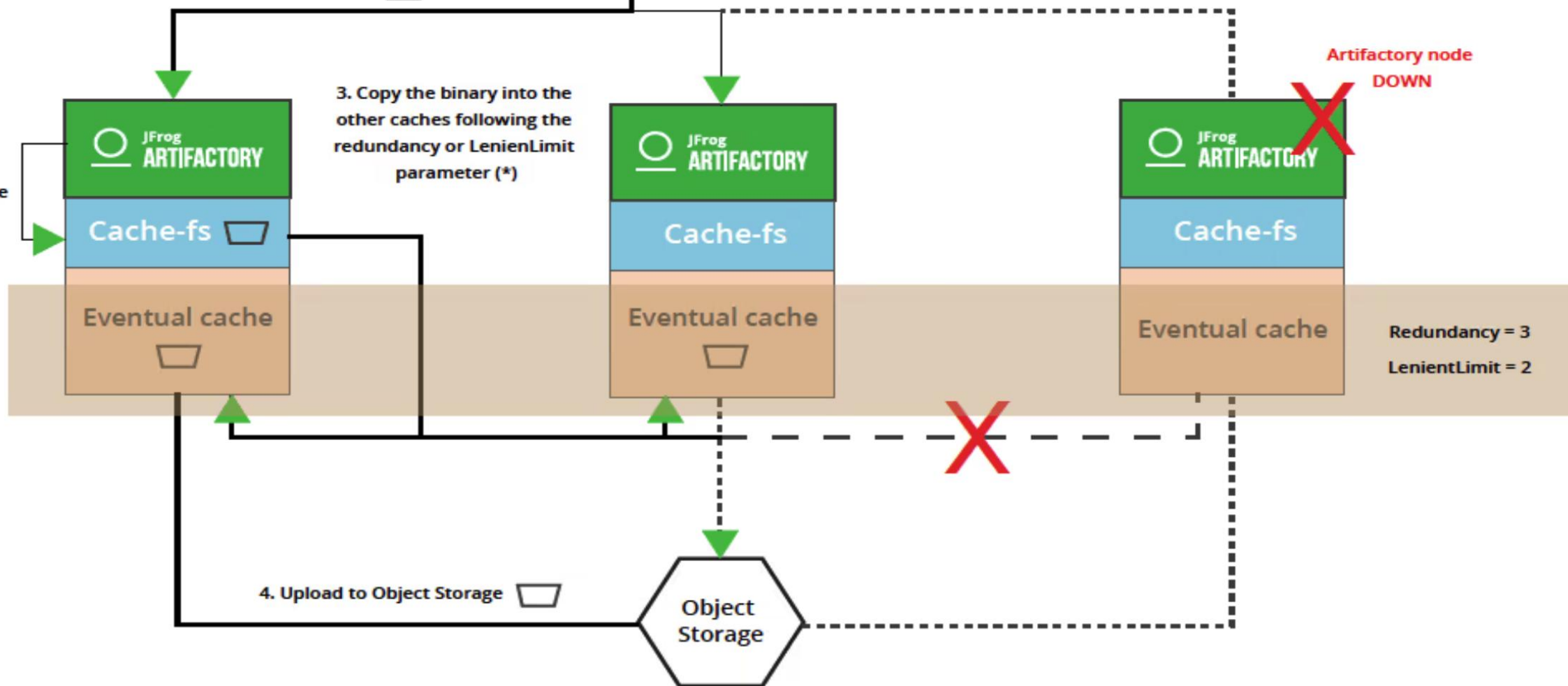
Cache-fs：读取缓冲区，用于优化 Artifactory 和远程存储（例如 NAS 或云存储）之间的流量。这个“最近使用”（LRU）缓存将托管最近上传和下载的工件。启用它可以减少对网络存储的请求数量，从而减少响应时间。

Eventual：一个写缓冲区，用于在使用慢速和/或远程存储时优化上传过程中的减速。默认情况下，所有依赖对象存储（例如 AWS S3、Azure Blob 存储等）的 Artifactory 存储模板都启用此缓冲区。这允许实现异步上传，不用等工件上传到远程存储即可立即使用。一旦工件上传到存储并在 Artifactory 中可用，它将从最终缓存中删除。

# 链式存储设计



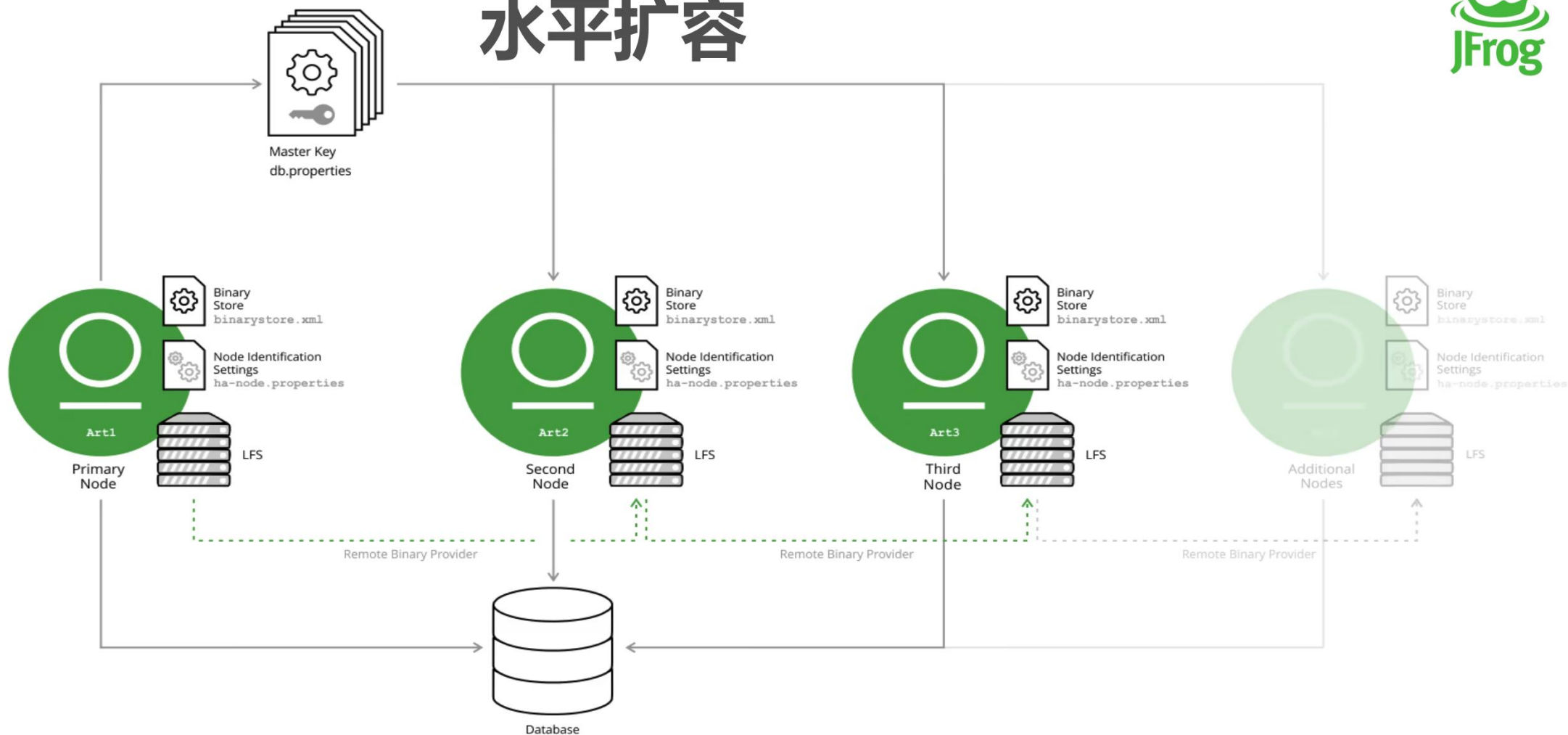
1.Upload binary to Artifactory



# 制品库的高可用性



## 水平扩容

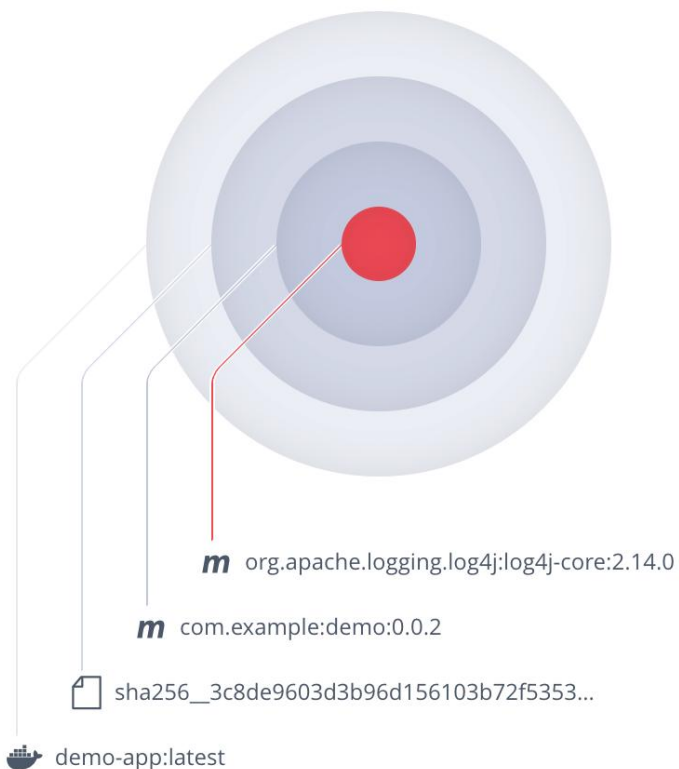




# 制品库的开源组件漏洞扫描

## 漏洞影响范围分析

Jfrog Research Contextual Analysis Public Sources **Impact Paths** References



## 基于漏洞的上下文分析

! CVE-2021-44228

JFrog research last updated on 29 Mar 2023 11:21 AM  
This CVE is enriched by JFrog research and provides more accurate information

Xray ID XRAY-191654

Contextual Analysis **APPLICABLE**

JFrog Severity ! Critical

Component org.apache.logging.log4j:log4j-core

Version 2.14.0

Upgrade to 2.12.2, 2.15.0, 2.3.1

CVSS Score 9.3 (v2) 10 (v3)

CWE CWE-20, CWE-400, CWE-502

^ Show Less

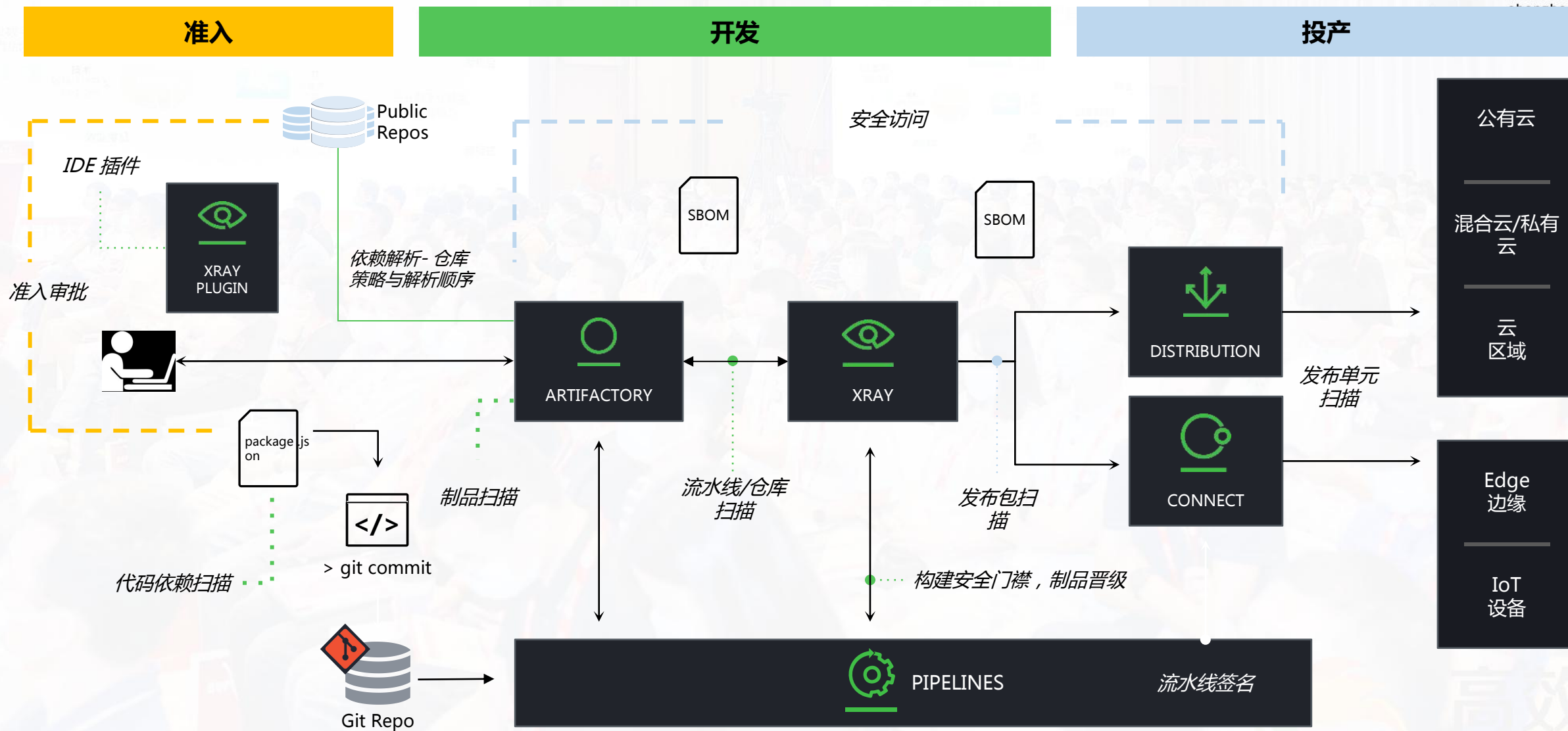
Jfrog Research **Contextual Analysis** Public Sources Impact Paths References

Contextual Analysis Breakdown

Why is this CVE applicable?

Path	Location	Issue Found
...lorConverter.class	ColorConverter::newInstance	The vulnerable function info/f...

# 制品库的开源组件漏洞扫描



03

回顾

## 回顾



流动式软件发布



元数据



性能和高可用



开源组件扫描

高效





# Thanks

开放运维联盟

高效运维社区

DevOps 时代

**荣誉出品**

了解更多关于 JFrog , 欢迎来**313**展位咨询