ORACLE Linux

ORACLE VM

Oracle Linux and Ksplice: 为关键应用程序提供零停机时间，包括容器部署

构建安全的云基础架构

苏虹林 – Honglin Su
Sr. Director of Product Management
Oracle Linux and Virtualization

张国华 – Frank Zhang
Principal Solution architect

June 27, 2018

ORACLE

IT 经理的一天：降低安全风险

安全港声明

下文旨在综述我们的整体产品方向。 本文件内容仅供参考，不包含在任何合同之中。本文件不构成提供任何材料、代码或功能的承诺，亦不应成为制定购买决策的依据。所述的任何 Oracle 产品特色或功能的开发、发布和时间由 Oracle 自行决定。

议程

1. Oracle Linux介绍
2. Ksplice -为关键应用程序提供零停机时间
3. Oracle Linux，容器部署和Oracle云
4. 问题与解答

Oracle基础架构软件:开放云基础

通过最大限度地提高灵活性来降低业务风险

开放的操作系统

Oracle Linux:最广泛的Linux部署选择

开放的虚机

Oracle VM:基于供应商中立硬件的云管理程序构建

开发/运维

Docker, SCL, VirtualBox and OpenStack:丰富的功能集和支持

零锁定以实现最大的业务灵活性 - 契约式和架构式

ORACLE
Linux

#2企业Linux提供商*

从2006年开始提供Oracle Linux

推动Oracle云和一体机

支持成千上万的企业

数以百万的Docker容器下载

Linux Foundation 白金会员

Cloud Native Computing Foundation (CNCF) 白金会员

Oracle Linux & VM:
Engineered for open cloud

* Based on industry analyst and Oracle data

ORACLE

Oracle Linux:专为开放云而设计

ORACLE
Linux

专为云中的关键业务工作负载设计:

- Unbreakable Enterprise Kernel (UEK) 适用于云基础架构
- Ksplice可实现零停机诊断和修补
- DTrace用于全面的跟踪和诊断

包括Docker容器技术

提供管理选择

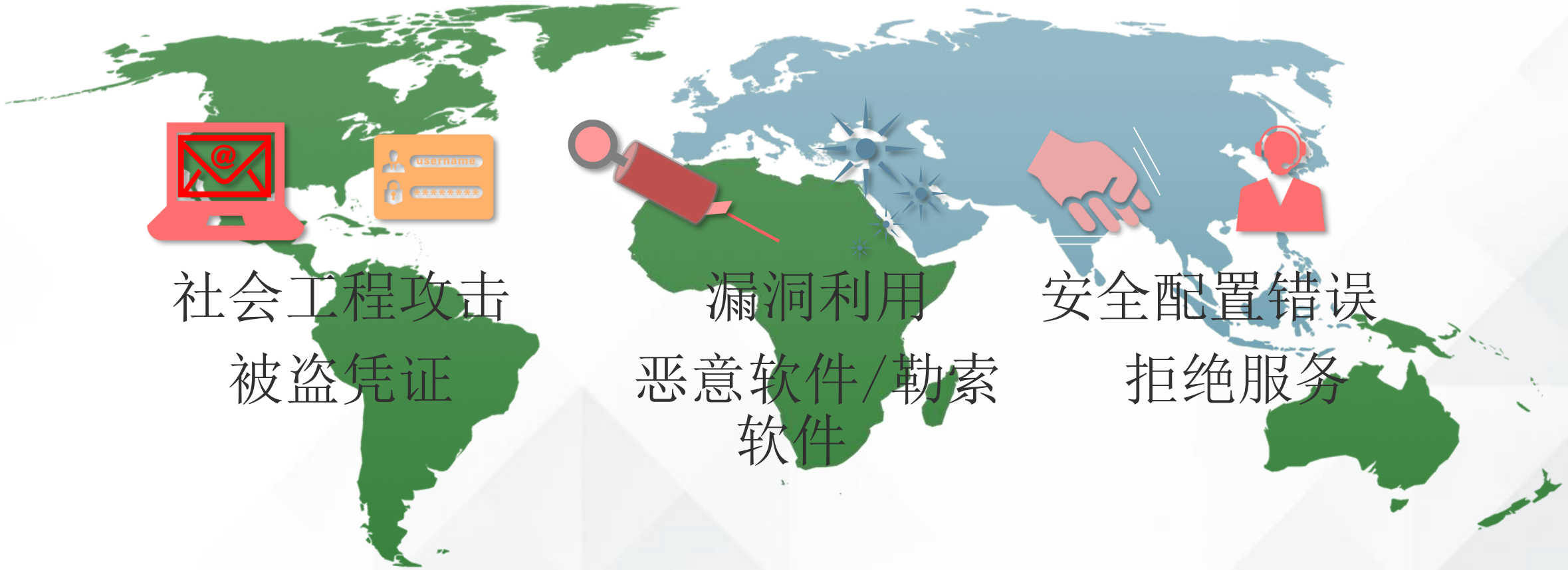
- Oracle Enterprise Manager用于完整的堆栈管理
- Spacewalk 为开源Linux提供管理
- Oracle OpenStack 提供开放云管理平台

与红帽保持应用程序完全的二进制兼容

推动Oracle云和一体机

ORACLE

典型的攻击向量



社会工程攻击

被盗凭证

漏洞利用

恶意软件/勒索软件

安全配置错误

拒绝服务

解决系统漏洞所面临的挑战

如何让所有利益相关者都满意？

您必须根据安全运营中心的建议修补系统，但要遵从变更管理部门

变更管理

我的应用程序正在进行开发，我们正在为下一个月的发行计划努力。 我不能容许任何停机时间

应用程序所有者

我有最新的安全修补程序，但我如何可以进行修复，而不用中断应用程序和等待变更管理部门的批准。

基础架构主管

借助 Oracle：

- 通过持续提供风险缓解技术助力 IT 主管。
- 为应用程序获取 100% 的正常运行时间，同时仍然保持安全。
- 改善整体安全态势，让人放心。

全新云时代中依然存在原有挑战

防御漏洞和攻击

92.5%

最新研究表明： 前 50 名应用程序中，**92.5%** 的应用程序在发现漏洞后，当天便能提供修补程序

81%

在所有已知漏洞中，**81%** 的漏洞具有可解决漏洞的修补程序

来源：https://info.flexerasoftware.com/SVM-WP-Vulnerability-Review-2017

ORACLE
Linux

ORACLE
VM

针对安全、合规和补救的 Ksplice

维持业务正常运转

ORACLE

修补业务影响

无 Ksplice 的管理和业务流程资源

典型修补周期任务

Linux 管理员							
数据库管理员							
中间件 管理员							
应用程序 数据库管理员							
业务 用户							

Ksplice 修补业务影响 - 零停机

使用 Ksplice 改进管理和业务流程 – 减少资源成本

Ksplice 修补周期任务

变更管理	计划停机时间	关闭堆栈	修补操作系统	启动堆栈	分诊	验证和发布

Linux 管理员							
数据库管理员							
中间件管理员							
应用程序数据库管理员							
业务用户							

任务资源减少 60 %

Ksplice 完善当前修补流程

实现按要求的“无重启”修复和根据需要的按需安全修补

示例：减少其他 Heart Bleed 安全漏洞

适用于用户空间的 Ksplice

Heartbleed 导致成千上万的提供商重新签发安全证书，估计损失 **5** 亿美元

一些引人注目的攻击对数百万用户造成影响
并导致不可计量的损失

Ksplice 使客户可以立即修补

- 修补无需计划停机时间
- 可显著缓解攻击造成的影响
  如 Heartbleed

Ksplice 是什么？

业务影响：降低风险和暴露；维持生产率

- Ksplice 技术无需重启即可应用更新
  - 无需重启对 Oracle Linux 和 Oracle VM 的好处：
    - 增强安全性 - 应用安全修补程序而无需重启
    - 可靠（合规） - 更新整个系统，不仅仅是用户区
    - 主动支持 - 适用于在测试中运行单元
    - 减少运营成本 - 没有工作日夜晚升级/周末升级或非计划维护
- 将不合规暴露限制在尴尬的品牌利用上
- 使高层目标与IT保证和生产力保持一致

使用 Ksplice 的三大业务实践

生产率与收益率成正比

- 确保机器百分之百合规
  - 照常修补用户空间
  - 使用 Ksplice 修补内核和系统空间
  - 无需重启，系统百分之百合规
- 修补常见漏洞和披露（CVE）
  - 立即修补安全漏洞或错误
  - 无需重启
- 支持补救
  - 与 Oracle 技术支持合作，以提供 Ksplice
  - 将 Ksplice 安装到运行系统中
  - 无需重启和重置问题域

系统需要保持合规

提高了合规性以限制企业暴露

- 您的首席信息安全官 (CISO) 和信息保障团队告知您需要修补系统
  - 很简单，您只需确定适用于用户空间的修补程序
  - 并不简单，您需要安装新的内核 RPM
    - 但您需要确定 Ksplice 修补程序，以使您的内核合规，而非影响您的客户
- 安装用户空间和 Ksplice 修补程序
- 结果：
  - 合规机器，无需重启
  - 您的客户不会察觉到任何中断
  - 信息保障团队验证系统合规性

存在常见漏洞暴露的系统

预防和限制安全漏洞利用

- 您的首席信息安全官 (CISO)和团队确定受 CVE 影响的系统
- 您负责确定满足信息保障条件的 Ksplice
- 您负责安装 Ksplice 修补程序以修复 CVE
- 您的客户不会察觉到任何中断
- 您的信息保障团队验证一致性

需要诊断并修复退化的系统

运行时间与生产率成正比

- 系统开始出现退化迹象
  - 性能不佳
  - RAM 消耗
  - 丢失或间歇性 I/O
  - 开始出现错误或警告
- 补救步骤：
  - 您针对系统故障联系支持/提交服务请求
  - 您和支持人员将问题“细化”至内核代码。
    - 修复存在于上游？
    - 需要创建修复？
    - 针对运行系统创建/安装 Ksplice 修补程序
- 验证修复：
  - 已修复？ - 完成
  - 未修复？ 退出 Ksplice 修补程序，然后重复

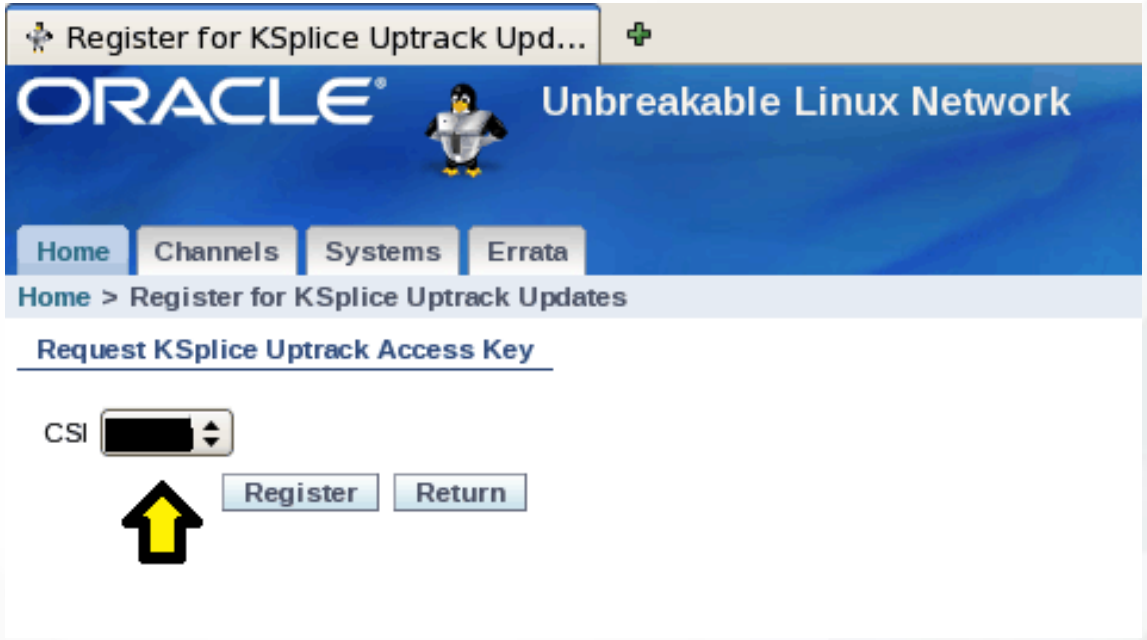
启用 Ksplice 修补 - Unbreakable Linux Network (ULN)

已包含在 Oracle Linux 高级支持中

您将看到一个标有 KSplice Uptrack Registration 的按钮

在 ULN 上注册 Ksplice 用于托管

- Ksplice 需要注册
- Ksplice 将使用您的 CSI
- 选择您要用来生成访问密钥的 CSI
- 单击以注册



益处总结

- 可用性提高
  - 应用关键更新和安全修补程序，无需重启
  - 为用户和客户消除停机时间和中断
    - 在应用程序运行时更新
    - 协调 Ksplice 支持热修补
- 提高了安全性
  - 减少漏洞窗口
  - 提高合规性
- 降低了运营成本
  - 消除计划外维护停机事件
    - 不再需要花费漫长的夜晚和周末来重启服务器进行内核更新
  - 无需与系统用户协调重启造成的运行中断

后续步骤

ORACLE | Ksplice

Sign In/Register for Account Help

```
(root) # ksplice all show
Ksplice user-space updates installed:
rsyslogd (2318)
sshd (2697):
- [qn7jy7c6]: CVE-2015-7547: Remote code execution in glibc DNS resolver.
certmonger (3007):
- [qn7jy7c6]: CVE-2015-7547: Remote code execution in glibc DNS resolver.
- [8v0l3voi]: CVE-2016-0702: RSA key disclosure on Sandy Bridge CPU's (CacheBleed).
Ksplice kernel updates installed:
Installed updates:
[b4ppb8m2] Race condition with outstanding tx counter in IP-over-InfiniBand.
[280qdpcz] CVE-2016-3157: Xen I/O port access privilege escalation in x86-64.
Effective kernel version is 4.1.12-32.2.3.el6uek
(root) #
```

Over 28,500,000 days of uptime.

Technology
Learn how Oracle Ksplice works to make your systems more secure

Software
Explore the clients and tools for managing Ksplice updates

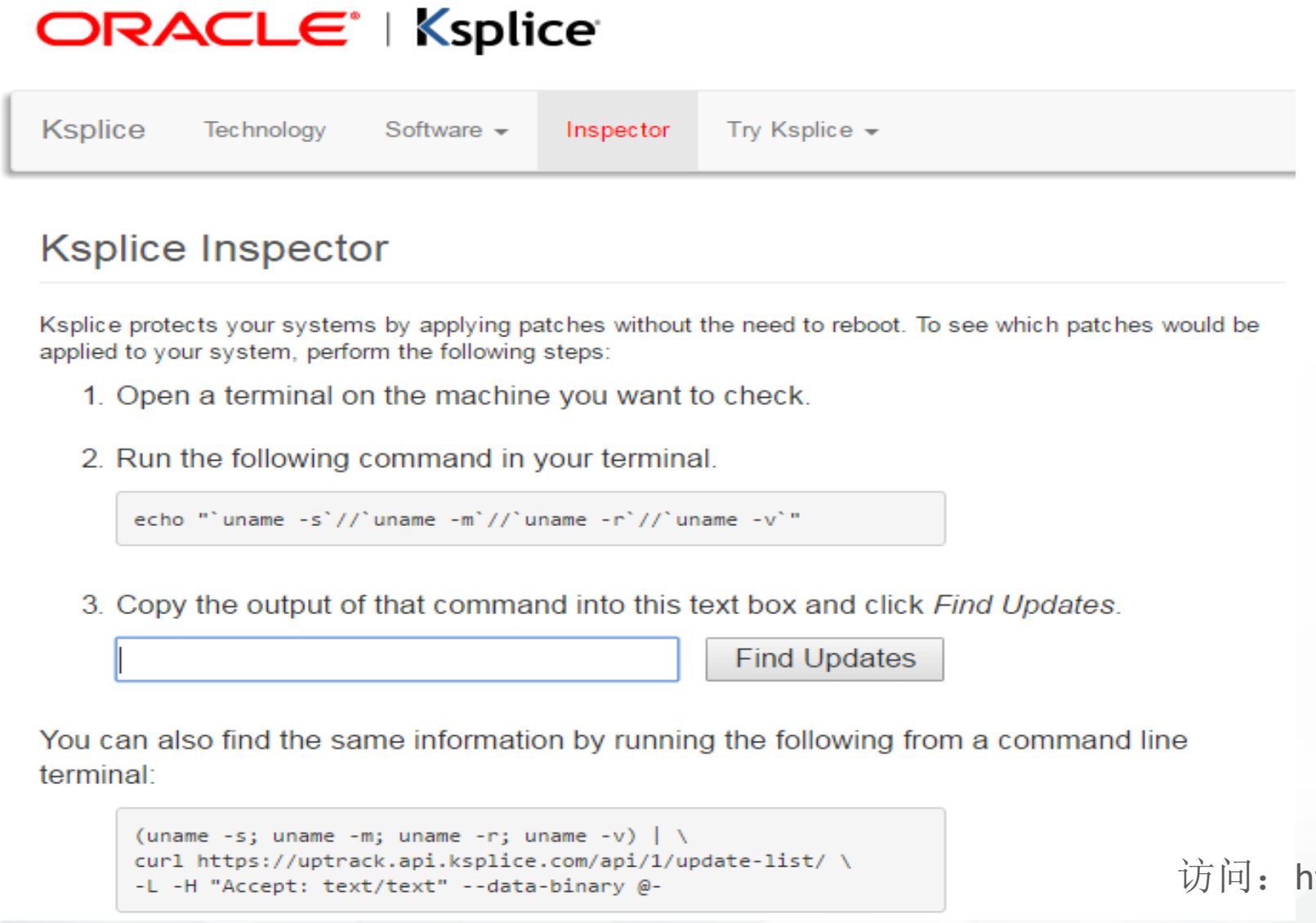
Inspector
Review the updates available for your kernel

Try Ksplice
See how you can start using Ksplice for free today

Legacy Customers
Find information relevant to Ksplice Legacy customers

Reboots are a thing of the past!

Ksplice Inspector



访问：http://ksplice.oracle.com/inspector

Sign In/Register for Account Help

Ksplice Technology Software Inspector Try Ksplice Legacy Customers Quick Links

Try Oracle Ksplice

Oracle Ksplice improves the security of your Linux systems while reducing the administrative burden. To see how Oracle Ksplice can improve *your* environment, try it today. There are three ways you can try Oracle Ksplice:

Oracle Linux Premier Support

Oracle Linux Premier Support customers already have access to all of the benefits of Oracle Ksplice. Click the button above to learn about all of the benefits of Premier Support.

30 Day Trial for Oracle Linux and RHEL

Red Hat Enterprise Linux and Oracle Linux users can try Oracle Ksplice for 30 days for free. Experience the peace of mind that comes from rebootless updates.

Free Desktop Edition

Oracle provides free Ksplice updates for desktop users of Ubuntu and Fedora. Install Ksplice on your desktop Linux system and get the protection of regular updates without interfering with your day-to-day work.

http://ksplice.oracle.com/try/

客户角度 -美联航如何确保服务的连续性

使用Oracle Linux运行容器

ORACLE Linux

- 适用于Docker的Oracle Container Runtime
  - 包括由Oracle构建和维护的Docker Engine二进制文件
  - 支持btrfs和overlay2作为Docker文件系统
  - 需要Oracle Linux 7和UEK版本4
- 用于Kubernetes的Oracle容器服务
  - 基于上游Kubernetes 1.9.1
  - 提供RPM包和Docker容器
  - 包括Oracle提供的安装脚本，以简化Oracle Linux 7上的安装/配置
  - 需要Oracle Linux 7, UEK 版本4和Oracle Container Runtime for Docker

支持在Docker容器中部署的Oracle软件

- Oracle Linux
  - 6 and 7 及精简版本
- MySQL Community Server
- MySQL Enterprise Server
- NoSQL
- Oracle Database

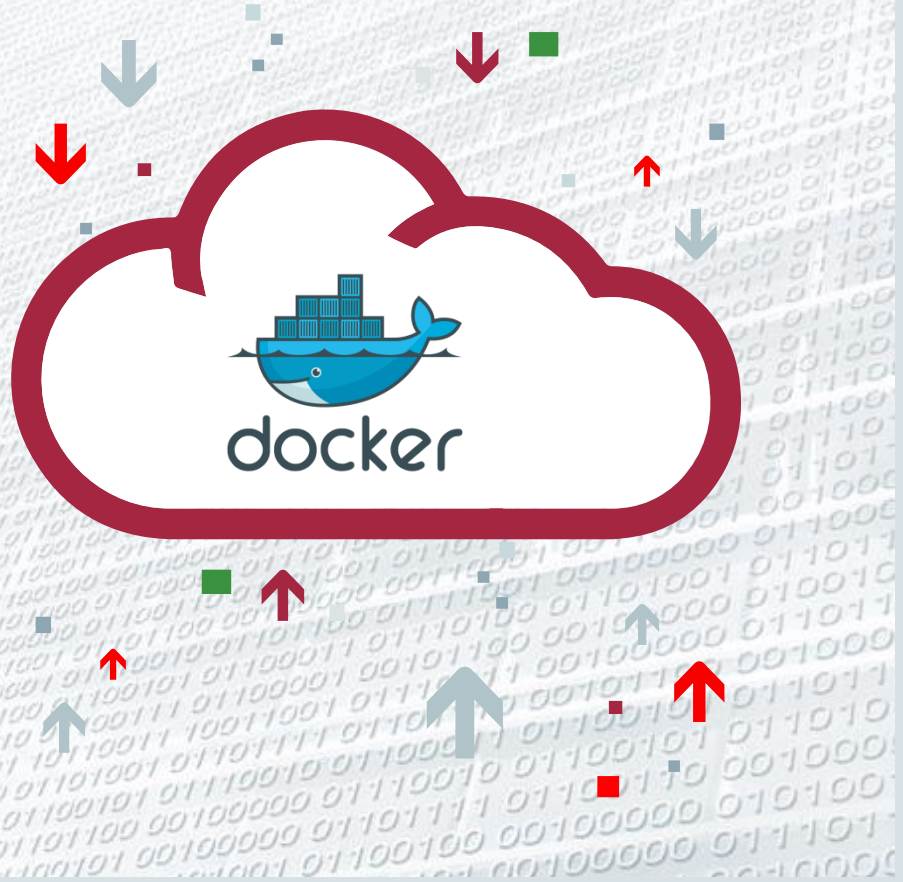
- WebLogic Server/FMW Infrastructure
- Coherence
- Tuxedo
- HTTP Server
- Business Intelligence Platform
- GoldenGate
- SOA Suite

Oracle软件产品的Dockerfiles

- Oracle在GitHub上发布基础产品和示例Dockerfiles
  - https://github.com/oracle/docker-images
- Dockerfiles可以按原样使用或根据客户要求进行修改
- 任何人都可以通过拉取(pull)请求提交更新/修复/增强功能
- 用作Oracle Container Registry和Docker Store上提供的预建图像的源代码

Oracle容器注册表

- 为Oracle产品提供Oracle经过测试和认证的预先构建的Docker和其他容器映像
  - 公开访问
    - https://container-registry.oracle.com
  - 为Oracle云基础架构客户镜像
    - https://container-registry-phx.oracle.com
    - https://container-registry-ash.oracle.com
    - https://container-registry-fra.oracle.com



在Oracle云中使用Oracle Linux

ORACLE Linux

云就绪，集成

- 方便访问及更新Oracle Linux软件
- 快捷访问Oracle容器注册表和yum服务器
- 零停机时间使用云中预先安装的Ksplice操作系统内核和用户空间更新
- 全面的容器和容器管理支持
- Oracle Linux存储设备提供了一种在云中构建NFS和Samba共享存储的简单方法

增强开发者平台

- 通过本地yum服务器可以更快更轻松地部署Oracle Cloud开发人员工具，例如Terraform，SDK和CLI
- 轻松访问Linux开发人员并在本地Oracle LInux yum服务器中预览软件频道
- 成千上万的EPEL软件包由Oracle为安全性和合规性而构建和签署
- 软件集合库(SCL)支持包括安装最新版本的Python，PHP，NodeJS，nginx等

经济有效

- Oracle云上免费提供Oracle Linux支持
- 充分利用其24 x7最佳的支持服务和工具
- 无需预算Oracle云的操作系统支持费用
- 使用Oracle Linux作为全面且广泛测试的云基础架构堆栈的一部分

ORACLE Cloud Infrastructure

下一步行动

链接与资源

- 阅读有关打击网络犯罪的内容
  - NIST
    - https://csrc.nist.gov/
    - https://nccoe.nist.gov/
  - 国际信息系统安全认证协会
    - https://www.isc2.org/
- 访问 - Oracle Linux 安全网站和资源页面
  - https://oracle.com/Linux/Security
  - https://www.oracle.com/linux/resources.html
- 观看
  - 美国联合航空公司谈论安全和应用程序可用性问题
- 了解有关 Ksplice 的更多信息
  - https://ksplice.oracle.com
- 联系我们
  - Twitter.com/oraclelinux, facebook.com/oraclelinux
- 下载 – edelivery.oracle.com/linux

集成云

应用程序和平台服务


ORACLE®