大型运维环境实施安全加固经验谈

2006-8-5
Coolc
Email: eanalysis AT gmail.com
Homepage:blog.xfocus.net/coolc

前言

安全加固在安全甚至运维领域，已经是一个大家都不再感到陌生的名字了。相当多的安全甚至集成公司，都会再项目工程中提供此类服务。Coolc 从事工作以来，也大大小小的实施了相当多次的安全加固工作，最近完成了一个大型运维环境的加固工作，积累了一些经验，现在记录下来与大家分享。

因为所属工作的原因，coolc 不会透露具体的操作的技术细节，这点还希望大家能见谅，但是 Coolc 会更多的阐述记录在项目操作中框架性思维和理念，同大家分享我的收获和经验。

背景

本次项目之所能称之为大型项目，主要是基于如下几个特点。

- 涉及的主机众多，总体主机数量在万台以上。
- 涉及业务情况复杂、数量众多，其中重点大业务有数百个，而旗下子业务更为种类繁多。
- 业务多为在线业务，对于中断的容忍度很低。
- 涉及部门多，光运维层面的部门会涉及 10 余个左右，横向沟通成本较大。

内容

困难

- 选用何种层面的加固技术，是系统层？应用配置层？IDS 配合 iptables 联动？抑或是 kernel patch？
- 涉及的主机多为在线业务，如何保证平滑切换。
- 横跨多个部门，如何协调各个部门的人力资源具有相当难度。
- 安全加固本身是叫好不叫座的东西，在完成项目后如何体现安全加固的效果？
- 在自身进行了大量技术考量后，如何向技术部门验证你的说法，得到一线运维部门的支持？

思路

1. 争取运维线的上下层支持和理解。
2. 充分准备，数据支撑，取得认可。

3. 自动化部署，减轻工作量和误操作。
4. 充分考虑回退和规避运维风险。
5. 以点带面，分步骤部署。

准备阶段

安全加固项目的准备阶段主要的工作内容为，

- 确定项目组成和成员的职责
- 内容宣讲，介绍加固项目的工作内容。
- 了解安全需求，打消存在的顾虑，争取配合和支持。
- 对加固内容进行测试，后续工程中需要配合工具和文档进行准备。

人员准备

人员准备可讲的东西不多，从这次操作中较多的体会是，项目组中最好能配备一个具有编写脚本能力的人，减小大规模主机部属时碰到的巨大工作量。其次，人员不在于多，PM 的沟通能力要很强，具有较强的破冰和应变能力。项目组能够阶段性引入实施部门的 Teamleader ，在实施时会极大地提高执行力。

宣讲和破冰

在安全项目中，最常见的问题就是实施方和相关的配合人员，因关注点不同而导致的分歧。项目中安全人员关注的是如何按时完成项目，保证自身的安全项目内容得以实现。而参与实施配合得人员关注点主要集中在。

- 加固是否会影响业务系统的正常运行。
- 加固是否会带来业务上的中断。
- 加固是否会给系统带来性能上的影响。
- 加固实施是否会带来大量的工作量和挤占大量的时间。
- 加固后运维工作是否会在操作上十分不便。
- 加固后的主机是否会会在安全上和现有水平相比，有很大提升。

此时整个项目的主要矛盾是相关人员对加固没有了解，不清楚项目可能会带来哪些“利”、“弊。

因此需要通过会议等方式，向各个部门的 Leader ，骨干进行加固方面的知识介绍和内容宣讲。

首先，为了验证自身说法的科学性，前期测试需要通过数据证明各种影响的具体数值，并给出目前的数值进行比较。根据数据同运维线沟通，商讨性能等指标容忍基线。

其次，项目在设计时要充分考虑业务中断、性能的影响。本次操作中 Coolc，在初始设计上规避重起等可能造成中断的行为，并出具了性能评估报告，比较图谱等进行性能影响验

证。为了使报告具有说服力，应尽量争取将被实施部门提供样机（或选取明星部门的主机），以便采集数据得到较大范围的认可。

再次，Coolc 在本次加固项目中，实施采取自动化脚步、程序的模式进行。事先设置好加固项的配置文件后，执行安装脚本自动化部署，尽量避免部署所带来的时间和人力成本(Windows 下安装应用程序亦是此类思想)。

同时此类自动化部署，十分有利于在短时间内批量部署大规模主机。 **而且脚本应具有很强的回退功能，能通过执行脚步达到完全回退的目的。（当然回退功能的自保护能力应该很强 :)）**

同时，提供一份加固影响表，将每项加固内容可能带来的影响进行描述，并且在实施中时时更新此表，并同步收集故障案例，作为培训资料。

最后，加固效果的验证本身存在一定的困难，前期可以采用制作演示录像，PPT 讲解等方式，后期进行培训时，可以构建一些演练环境进行展示。

总结一下，此阶段主要是对加固框架内容进行修正，同时向各个部门传导加固意识，打消顾虑，寻求领导层支持和理解，也为后面的大规模实施打下基础。

实施和尝试

经过前一阶段的准备和沟通，基本达成了如下效果。

- 各个部门在部门领导和骨干级知晓了解了安全加固的内容。
- 对安全加固内容的安全提升有了认可。
- 对于安全加固方面可能造成的影响有了一定认识。
- 熟悉安全加固项目中的项目组成员和每个成员的职责。
- **清楚地知悉安全加固不会带来很大工作量。并且是必须要操作的一个安全工程项目。**

在此基础上，**整个项目的主要矛盾点已经由对项目不了解，工作量可能的负担，转变为了安全加固是否给运维带来风险。**

1. 针对主要矛盾上的变化，整个项目调整进入实施和尝试阶段。在此阶段 ，主要工作从各个部门抽取主机，进行初步的加固试运行。试运行的主要目的是：

2. 验证稳定性，因为此阶段运维人员重点关注稳定性，所以从项目组侧应保证，实施的加固大多数情况下，确实可以保证技术层面的稳定；如果一旦出现问题，响应时间解决问题的态度要到位；选取主机要具有代表性和一定的数量，这样在数据上才会有说服力和验证效果。

3. 进行项目磨合，此时是熟悉配合人员的最好阶段，同时也为项目组提供了后期部署的演练机会。因为此阶段时间压力小，因此应尽可能多的让项目组组员熟悉各个环节(让每个成员都可以互为备份)，并对操作流程进行演练修正。

4. 试验主机的选取，Coolc 采用的方式为典型主机选取方法，一般会选取如下类型的主机：
   - 典型角色，选取的主机在业务架构上是典型角色，如一个游戏中，前台的应用服务器，Cache 服务器，DB 等，各抽取一台。
   - 负载特征明显，系统负载上有较多代表性的主机，如高 IO 访问量的主机，高并发

session 主机，高 CPU 占用，高内存占用的主机。

- 充分尊重运维人员的意见，抽取试验的目的，最终还是为了通过在有代表性主机的试运行，能提前发现隐患，避免可能的问题。因此抽取何种主机方面，熟悉实际环境的运维人员的意见十分值得参考。
- 架构上冗余，考虑到试运行可能带来的风险，选取主机应尽量选取架构上提供冗余支持的主机，不要在可能出现单点故障的主机上实施。

如果在试验阶段出现大型事故，那么此项目推行的难度将会几何级上升，因此此阶段一定要慎重，同时 PM 要具有在基层消化小型问题的能力，避免一般性问题因人为因素被放大升级。

总结，此阶段主要是通过沟通，争取一小批具有代表性的主机参加试运行，观察实际运行效果，安全人员对试验情况进行跟踪，对发现的问题进行修正。同时锻炼队伍，准备下一阶段的大规模部署

全面展开

通过前一阶段的工作，基本可以到达如下效果

- 业务部门领导到技术层对于整个加固的稳定性有了初步认可。
- 参与配合的实际运维人员对于操作方法、流程和人员有了熟悉和操作经验。
- 加固项目在加固内容上可能存在的问题和不兼容基本被消化。
- 加固项目组内技术人员得到锻炼，能应付一般突发情况，并对各个部门的业务结构、人员组成结构相当的认识和了解。

此阶段**主要矛盾也有对于加固内容的稳定性的担心，逐渐转化为对工程操作方法不了解，以及担心在后续工作中可能碰到未知问题，所造成的不安。**

因此该阶段的重点为。

- 同运维部门 Leader 和骨干共同回顾前期的项目进度和成果。
- **同运维部门骨干和部门领导确认回退方案，认可回退方案的可靠性和可行性。**（这点是重中之重。

  举例：

  当加固后，运维中出现故障，是否为安全加固导致，往往会带来很多争论和工作量，尤其是如果因为此类故障，导致对加固稳定性的质疑，将直接影响整个工程的进度。如果能够双方认可回退方案，一旦出现问题，运维部门执行回退后，即可迅速定位是否是“加固造成的影响”，便于双方进行排障。
- **同运维部门就项目中的人员分工、操作内容、时间等进行落实，并进行备忘。**
- **对新装主机加固纳入装机流程，保证后续上架主机全部闭合为“加固主机”。**
- 对相关运维技术人员进行培训，重点在于回退技术的反复演练。并让运维部门领导了解到此技术，在部门内进行强化。
- 向运维技术人员表明态度，并做出行动，加固相关支持的将以持续性的姿态进行，不会在加固完结后终止。

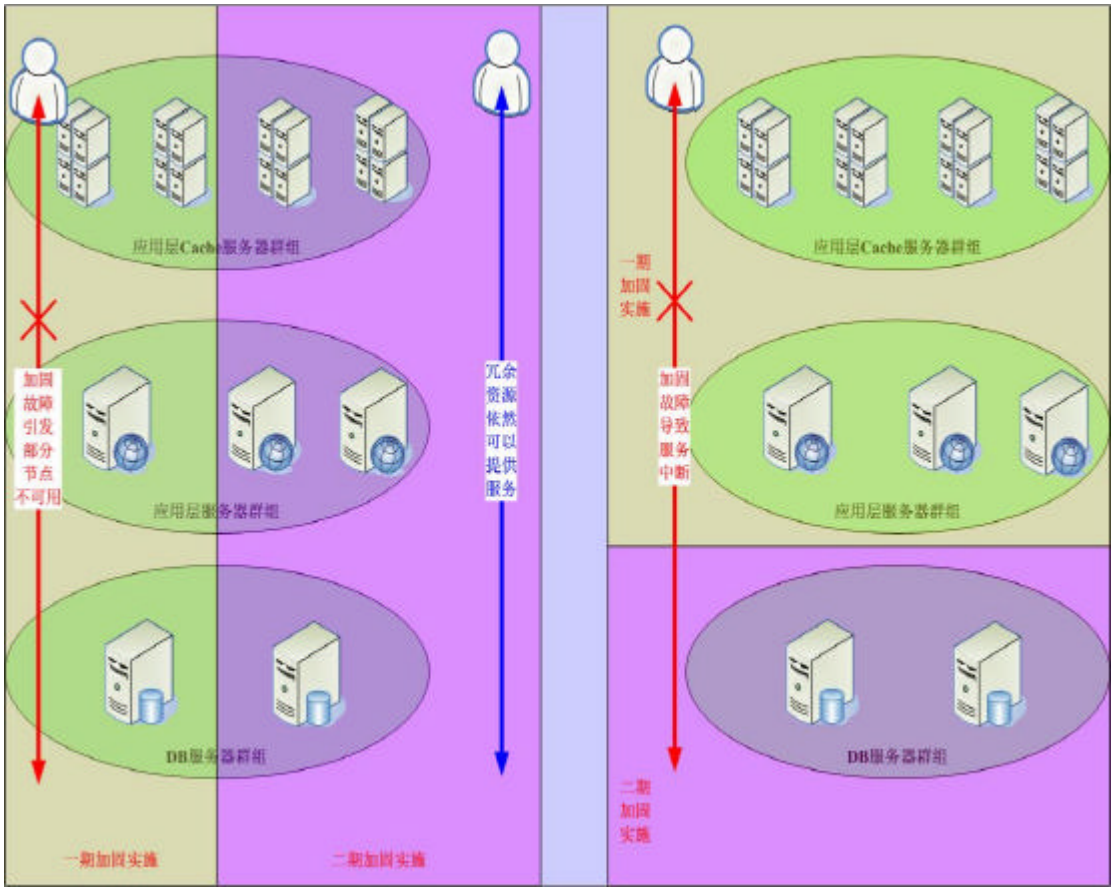
- **组织“ 实战演练 ”，通过搭建模拟环境，让一线人员有机会操作实际工具，增加其操作和动手能力。**

重点关注

因为此阶段将会完成整个实施过程的 95%以上的加固工作，因此在部署时的技巧十分重要，部署实的几个大原则为：

- **阶梯式部署，部署之初应该采取逐步递增的方式，如分 5 个阶段，在 3 个月内部署 3000 台主机，可以采取如下步骤** 1% ---9% ---10%---30%---50%。
- **选取角色考虑，在部署时应充分利用业务的冗余特性，尽量避免按照业务角色分类、分组，在一次部署时，选取单一角色的主机进行部署。如图所示，右图的方式，如果部署时出现故障，那么整个业务都将受到影响，对用户提供的服务不得不中断。**

因此不应该以业务系统为单位进行部署，而应该纵向切片进行部署，这样如果出现故障，即便部分节点不可用，但是由于同一角色服务器被分批次部署，提供了冗余，服务提供商依然可以为用户提供持续服务，如左图所示。



- **每完成一个阶段，如** 50% **，**80%**应该时时输出加固阶段性报告，对具体实施人员和相关部门** Leader **进行通告和知会。**
- **此阶段应该注意收集加固效果体现的案例，作为阶段性报告输出和结项报告素材。**

项目收尾完结

项目进入到此阶段，大部分主机完成加固，主要矛盾基本消失，主要工作集中在：

- **主要是对剩余主机做好加固收尾工作，不残留未加固主机，如果有特殊情况，需要进行文档备案。**
- **整理项目资料，文档 、代码等进行封闭，不再进行改动，保存归档并进行备份。**
- **酬谢相关配合** Leader **和技术人员。**
- **发出结项报告，对于整个项目进行回顾，总结案例、加固成效和问题。**
- **作为持续性安全工程，提出下一阶段的构想蓝图。**

总结

曾经同朋友开玩笑说，通过此次项目的操作，Coolc 也许是加固主机最多的人之一了，当然在实际操作中涉及了更多的是 PM 的角色，主要是筹划、设计、推动等工作偏多，总结了一些项目操作的经验，从内容上看，此项目也许只能视为中小型项目，但从主机数目看，此项目绝对可以视为大型安全项目，因此 Coolc 觉得其中积累的一些经验，应该还是有一定的成色，不妨写出来与大家分享。

项目中涉及的具体内容、技术细节、代码工具以及数字等数据，因为涉及敏感信息，不方便提供，还请大家原谅。如果大家有什么希望同 Coolc 讨论的，欢迎同我 Email 联系，谢谢。

附录