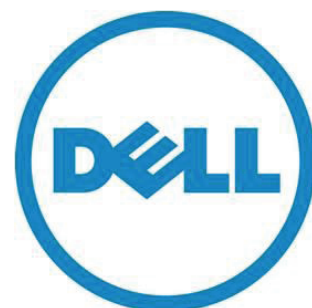


# 英特尔云构建器指南：英特尔平台上的云设计和部署

---

使用 Enomaly ECP™ HAE 和 Dell™ PowerEdge™ 服务器，增强云平台安全性

英特尔 | 戴尔



本白皮书仅供参考，可能包含排版错误和技术上的不准确性。本文内容按原样提供，不含任何形式的明示或暗示保证。

本文档中提供的信息与英特尔®产品相关。本文档并未以默许或以其他方式明确或隐含地授予任何知识产权的许可。除非英特尔在此类产品的销售条款和条件中另有说明，否则，英特尔不以任何方式承担与销售和/或使用英特尔产品相关的任何法律责任，并且英特尔不提供任何明示或默示担保，包括对特定目的的适用性、适销性或者不侵犯任何专利、版权或其他知识产权的法律责任或担保。除非与英特尔达成书面协议，否则英特尔产品并不旨在或意图用于英特尔产品的故障会造成人员伤亡情况的任何应用。

英特尔处理器编号并非性能指标。处理器编号可区分每个处理器系列中的不同处理器的特性，但不能区分不同系列处理器的特性。有关详情，请参见[www.intel.com/products/processor\\_number](http://www.intel.com/products/processor_number) for details。

英特尔可能随时更改规格和产品说明，恕不另行通知。设计人员不得依据任何特性或指导的缺失或特征，并且对于因未来对其进行更改而产生的任何冲突或不兼容概不负责。此处提供的信息如有更改，恕不另行通知。请勿依靠此信息来最终确定设计。

本文档中说明的产品可能包含设计缺陷或错误（收录在勘误表中），这些缺陷或错误可能导致产品偏离已发布的规格。可致函索取最新勘误表。请与您当地的英特尔销售机构或经销商联系，获得最新的规格后再提交产品订单。您可以致电1-800-548-4725，或访问英特尔网站[www.intel.com](http://www.intel.com)，获得具有订单编号并在本文档（或其他英特尔资料）中引用的文档的副本。

英特尔®虚拟化技术要求计算机系统配备支持该技术的英特尔®处理器、BIOS、虚拟机监视器(VMM)。功能、性能或其他益处可能会因硬件和软件配置而有所差异。软件应用程序可能无法与所有操作系统兼容。请咨询您的PC制造商。有关详情，请访问<http://www.intel.com/go/virtualization>。

© 2011 Dell Inc.保留所有权利。未经Dell Inc.的明确书面许可，严禁以任何方式复制本材料。有关详细信息，请联系戴尔。

Dell、Dell徽标、戴尔徽章和PowerEdge是Dell Inc.的商标。Intel和Xeon是Intel Corporation在美国和其他国家和地区的商标。本文中可能使用的其他商标和商品名称是指拥有这些商标和名称的实体或其产品。Dell Inc.对不属于自己的商标和商品名称不拥有任何专有权益。

2011年5月

## 目录

|                                             |    |
|---------------------------------------------|----|
| 受众与目标 .....                                 | 5  |
| 执行摘要 .....                                  | 5  |
| 简介 .....                                    | 5  |
| 概述 .....                                    | 5  |
| 潜在的云安全性风险 .....                             | 5  |
| 应对云安全性风险 .....                              | 6  |
| 英特尔 TXT 概述 .....                            | 7  |
| 英特尔 TXT 如何发挥作用 .....                        | 7  |
| 英特尔 TXT 的特性 .....                           | 7  |
| 典型的英特尔 TXT 使用情景 .....                       | 8  |
| Enomaly ECP HAE 技术概述 .....                  | 9  |
| 远程认证 .....                                  | 9  |
| 运营：正在使用中的 Enomaly ECP HAE .....             | 11 |
| 测试台蓝图概述 .....                               | 12 |
| 测试台硬件说明 .....                               | 12 |
| 安装和配置 .....                                 | 13 |
| 初始 BIOS 更改 .....                            | 13 |
| 软件安装、配置和功能验证 .....                          | 13 |
| 验证系统功能的前提条件 .....                           | 16 |
| 英特尔 TXT 使用案例 .....                          | 18 |
| 使用案例 1：攻击导致引导环境被修改 .....                    | 18 |
| 使用案例 2：验证向受信任主机重新分发受信任 VM .....             | 19 |
| 使用案例 3：验证受信任 VM 向非受信任主机的意外迁移是否会被标记为违规 ..... | 20 |
| 使用案例 4：验证 VM 向非受信任主机的手动迁移是否会被标记为违规 .....    | 21 |
| 注意事项 .....                                  | 22 |
| 网络技术体系结构 .....                              | 22 |
| 存储体系结构 .....                                | 22 |
| 硬件考虑因素 .....                                | 22 |
| 总结 .....                                    | 23 |
| 词汇表 .....                                   | 23 |

## 图

|                                                    |    |
|----------------------------------------------------|----|
| 图 1. 英特尔 TXT 保护虚拟服务器环境 .....                       | 8  |
| 图 2. 在 TPM 中创建 MLE 和存储值 .....                      | 10 |
| 图 3. 安全传输 TPM 信息以验证 Enomaly ECP HAE 环境 .....       | 10 |
| 图 4. 平台可信度通过验证（绿色屏幕） .....                         | 11 |
| 图 5. 检测到平台可信度违规（红色屏幕） .....                        | 12 |
| 图 6. 建议的处理器 BIOS 设置 .....                          | 14 |
| 图 7. 建议的操作系统和 I/OAT BIOS 设置 .....                  | 14 |
| 图 8. 设置 Enomaly ECP Agent .....                    | 15 |
| 图 9. 建议的安装后 BIOS 设置 .....                          | 16 |
| 图 10. 两个正在运行的虚拟机 .....                             | 17 |
| 图 11. 为两个 VM 验证 TPM 功能 .....                       | 18 |
| 图 12. 在服务器 B 上运行的 VM 不受信任 .....                    | 18 |
| 图 13. Mozilla Firefox 插件程序显示服务器 B 上的 VM 不受信任 ..... | 19 |

图 14. 服务器故障：VM 迁移至另一受信任主机（服务器 A） .....20

图 15. Enomaly ECP 发起的 VM 向非受信任主机的迁移被标记为非受信任 .....21

图 16. 强制 VM 向不受信任的主机上迁移：VM 被标记为不受信任 .....22

## 受众与目标

本文的目标受众是负责设计、部署和验证云基础架构（无论是公共云还是专用云）的云服务提供商、企业IT管理员和安全性管理员。本参考体系结构（或称“本文”）简要说明使用Dell PowerEdge™服务器和Enomaly Elastic Computing Platform™ High Assurance Edition (ECP HAE)的专用云设置。使用本文中的内容（其中包括详细的内容和屏幕截图），可显著降低构建和运营您首个云计算基础架构的学习难度。

由于云计算市场刚刚形成，缺少正式的标准，不应期望将本文中讲述的体系结构按原样使用。相反，应对此处提供的解决方案加以调整，来满足各种组织的需求，尤其是因为公共部门和私人部门对公共云和专用云的安全性要求可能大不相同。本书可用作这一旅程的起点。

## 执行摘要

云计算是相对较新的IT服务交付模式，可为其用户提供成本和可扩展性方面的巨大益处。但是，关于安全性的顾虑经常会限制企业对此新模式的使用。

本文提供技术和体系结构解决方案，此解决方案旨在解决因云计算而产生的一些主要安全性顾虑。本文中概述的参考体系结构基于在Dell PowerEdge R710服务器（该服务器采用英特尔®至强®处理器5600系列，并支持英特尔®可信执行技术2<sup>1</sup>[英特尔®TXT]）上运行的Enomaly Elastic Computing Platform High Assurance Edition<sup>2</sup> (ECP HAE)，描述了一个能够提供有力的保护来抵御安全性风险的云环境。

## 简介

### 概述

云计算可实现提取物理计算资源池，从而可以将计算以虚拟服务的形式按需消耗，并具有动态可扩展性、高资源利用率和多租户等特性。此方法对于各种规模的公司（从受运行数据中心不断增加的成本影响的中小型企业[SMB]，到需要高峰计算能力和迅速周转以处理客户需求高峰的大型企业）有着巨大的吸引力。

对于大多数企业而言，在云采用的早期阶段，基于云的解决方案通常是而非关键应用程序和系统（测试和开发活动、Web前端等等）评估和部署的。但是，随着企业用户认识到了云计算的益处，并希望进一步使用它，他们经常会开始考虑针对更接近企业核心的应用程序和数据使用云解决方案，而这经常会意味着应用程序和数据要遵守强制实施紧密的控制的特定安全性和隐私要求。

在这一点上，关于云计算的安全性顾虑浮上了水面。Forrester Research、The Brookings Institute、International Data Corporation (IDC)和其他调查公司进行了无数的研究和调查，结果表明对于云中安全性的担忧是限制企业使用云的一个最重要因素。

由于这些顾虑，当今拥有需要遵守特定安全性和隐私要求的应用程序的组织通常在固定的硬件基础架构上运行这些工作负载，而非在云环境中运行，即放弃云计算的益处而寻求更高的安全性。

---

<sup>1</sup> Enomaly Elastic Computing Platform High Assurance Edition: <http://www.enomaly.com/484.0.html>

<sup>2</sup> 英特尔可信执行技术 (TXT): <http://www.intel.com/technology/malwarereduction/index.htm>

本文讲述一个本问题的解决方案，它可为云平台用户提供可靠的证据，证明其云环境未受损害。此解决方案基于Enomaly ECP HAE。它通过基于硬件的独特机制，使用包括英特尔TXT、Dell PowerEdge服务器、带可信平台模块(TPM)的安全存储等技术，提供持续的安全性保证和平台可信性证明。

此解决方案使专用云环境能够满足最严格的企业安全性要求，并使服务提供商组织能够提供具备卓越价值主张、高度差异化的云环境。它经常使服务提供商能够满足客户安全性要求，而这些要求是使用其他技术的竞争提供商无法满足的。

## 潜在的云安全性风险

虽然云计算是一个新兴的领域，但是主要益处已得到企业IT组织的深刻理解。各种研究指出，安全性担忧是采用的最大障碍。这些担忧不仅仅出于对新事物的恐惧，还有着广泛的基础。在传统的数据中心环境中，管理员必须了解服务器硬件是否值得信任。企业依靠服务器硬件来运行安全性软件，并且他们保护其网络，却不担忧其服务器本身是否值得信任。但是，云的情况却不同。执行客户工作负载的虚拟服务器基于软件（虚拟机管理程序），而非基于硬件。对于黑客而言，软件是比硬件更容易攻击的目标，因此不能盲目地信任虚拟服务器。

换种方式说，对于大多数企业，云计算代表着他们首次考虑使用与外部机构同步共享且虚拟化的任何形式的基础架构。这些因素的全新组合带来了以前从未存在过的新的安全性风险。由于环境是共享的，恶意元素（由黑客控制的VM、恶意软件，或者由意图不良的系统管理员添加到环境中的元素）可以与用户工作负载一起在云中运行。由于环境是虚拟化的，所以存在着对客户VM进行全部控制的软件层（虚拟机管理程序以及控制它的云管理层）。因此，如果软件层受到黑客或恶意软件的侵害，则黑客或恶意软件现在就完全控制了用户工作负载。在这种情况下，用户对于保护自己无计可施，甚至都检测不到这种安全性被破坏的情况。

尝试通过人工审计来解决这一问题极为困难，而且成本高昂，足以抵消通过云获得的规模经济而产生的成本节约。另一方面，自动化、纯基于软件的解决方案无法向云用户保证云环境未被黑客攻击或未被篡改。如果云软件堆栈仅仅实施自我检查来检测未经授权的更改，并向用户报告结果，则没有什么来阻止同一软件的黑客版本继续报告一切正常的自我检查结果。

## 应对云安全性风险

为了成功地解决这些难题，并向云用户保证其云环境未受黑客攻击或未被篡改，需要一种自动化、高度可扩展的机制，这种机制基于不会被黑客或意图不良的系统管理员访问并进行修改的可信任层的根。此外，您应当有一组机制用于可靠地访问此受信任的根环境，然后使用它来验证堆栈的更高层的可信度。本文讲述这样一个解决方案，它基于英特尔TXT、Enomaly ECP HAE和Dell PowerEdge服务器，通过对分布式云环境实施英特尔TXT来实现。

由于这一解决方案实现了对于云的更高层次的信任，限制关键和非关键计算系统迁移到云中的一个重要因素得以解除。英特尔TXT和Enomaly ECP HAE提供云可信度的可靠证明，从而帮助您在云中构建完全分层的安全性自信，这种自信源自像传统的非虚拟化数据中心一样可信任的基础环境。通过这种方法，基础架构即服务(IaaS)云服务能够满足公共部门和私营企业的安全性，无论是在公共云还是专用云部署方案中。

本书说明英特尔TXT和Enomaly ECP HAE技术及其使用，并概述一系列测试案例来验证此解决方案提供的保护。其中使用了一个简单但有代表性的测试台环境，该环境中主要包括两台基于英特尔至强处理器5600系列、配备了英特尔TXT和TPM的Dell PowerEdge R710服务器。

## 英特尔TXT概述

英特尔TXT是一套高度通用的平台级硬件扩展，它提供用于创建可信平台的构建块。这些扩展内置在英特尔硅产品中，可通过实施运行时保护（例如防病毒软件），在物理和虚拟基础架构中应对不断增加且不断演变的安全性威胁。

源于硬件的安全性可增强敏感信息的机密性和完整性使之不受基于软件的攻击，保护敏感数据而不牺牲平台的用途，并通过测量和保护功能来提供平台级解决方案的更高的安全性。英特尔TXT提供一般用途的安全计算环境，该环境能够运行多种操作系统和应用程序。当与英特尔®虚拟化技术（英特尔®VT）<sup>3</sup>结合使用时，英特尔TXT可提供源自于硬件的信任，出于这种信任，您可以为执行环境打造安全性链。

英特尔TXT的主要目标是为软件提供在较大系统中定义安全、隔离的执行空间的能力。对于此执行空间的控制不允许任何未经授权的软件观测或与正在那里执行的操作进行交互。系统中一次可以存在多个这种执行空间，各个空间具备由处理器、芯片组、操作系统内核或虚拟机管理程序管理的专用资源。

构成这一功能的基础的体系结构包括以下一些系统组件中的特性：

- 处理器：处理器为标准分区以及一个或多个受保护分区提供同步支持。标准分区相当于不支持英特尔TXT的系统上的传统执行环境。它允许传统应用程序正常执行而不被修改。受保护分区提供对于内存和其他系统资源的强化访问，以便将执行与其他流程相隔离。在大多数情况下，应用程序的一部分可以在标准分区上执行，而另一部分可以在受保护分区上执行。
- 芯片组：通过芯片组的扩展，以及帮助确保保护数据的数据访问机制的各种增强功能，实施内存保护政策。芯片组还提供到TPM的接口。
- TPM：TPM设备（受信任计算组[TCG] TPM规范，版本1.2）是一种基于硬件的机制，它存储加密密钥、平台测量值以及平台中与英特尔TXT相关的其他数据。它还为认证流程提供硬件支持以确认英特尔TXT环境的成功调用。

## 英特尔TXT如何发挥作用

英特尔TXT通过创建经衡量的启动环境（MLE，该环境支持将启动环境的所有关键元素与已知良好的源进行精确比较）来发挥作用。英特尔TXT为每个经批准的支持启动的组件创建独特的密码标识符，然后提供基于硬件的机制，根据预期已知的良好启动顺序来评估各个组件。这样，当有异常事件发生（例如组件受到损害或启动环境中存在恶意软件，从而导致与批准的代码不匹配）时它便可检测到。MLE在本质上是一种洁净状态、经密码验证的环境，它作为英特尔TXT功能的一部分实施、由处理器扩展创建，这确保没有恶意代码（无论在BIOS、引导加载程序或其他位置中）能够影响它。

## 英特尔TXT的特性

英特尔TXT支持以下特性：

- 经验证的启动：基于硬件的信任链，可实现将MLE启动至已知的良好状态。对于MLE的任何未经授权的更改都可通过密码测量值检测到。
- 启动控制政策(LCP)：一个政策引擎，用于创建和实施已知良好的可执行代码的强制实施清单。
- 秘密保护：一种硬件协议的方法，可删除在不恰当的MLE关闭后遗留的数据，从而保护数据不受内存窥探软件和重置攻击的损害。
- 认证：保证受信任的环境被正确调用。它还能够为受保护空间中运行的软件提供测量值。认证使本地或远程用户或系统能够使用平台测量值凭证，以完成信任验证流程并支持合规性和审计活动。

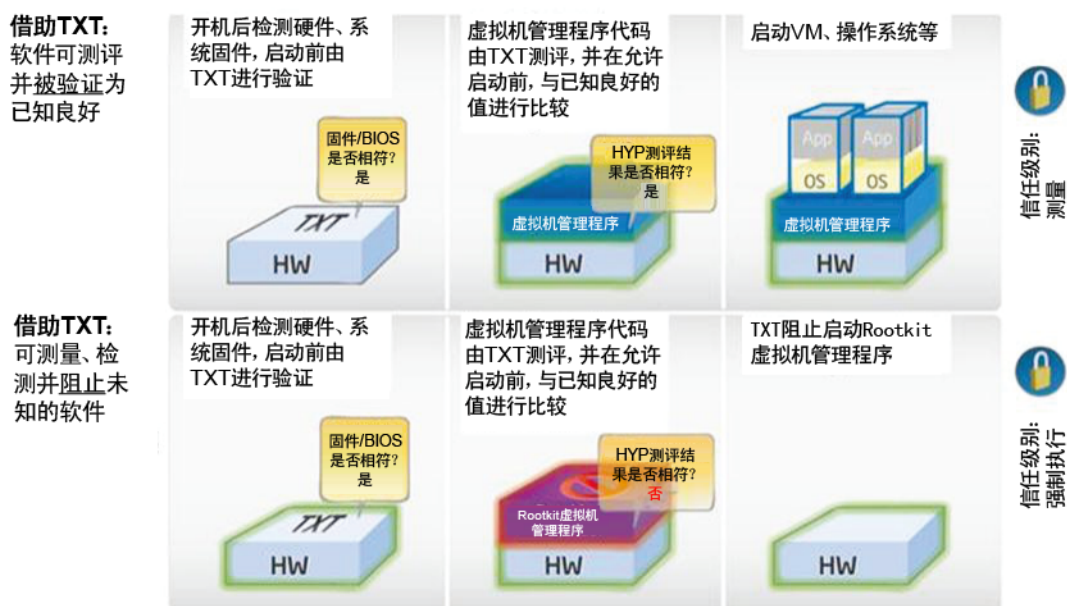
---

<sup>3</sup> 英特尔虚拟化技术：<http://www.intel.com/technology/virtualization/>

## 典型的英特尔TXT使用情景

图1演示了英特尔TXT启动流程的两种不同情景。在第一个情景中，MLE匹配期望的已经良好的配置，允许虚拟机管理程序启动。在第二个情景中，系统受到了rootkit虚拟机管理程序（它尝试在虚拟机管理程序下安装自身以获得对系统的控制）的侵害。在这种情况下，MLE哈希值与已知良好的测量值不匹配，则英特尔TXT将根据LCP放弃启动。

图1. 英特尔TXT保护虚拟服务器环境



这种增强的控制和保护对于独立的服务器有益，此概念可用作构建块，并在应用至数据中心级别时变得更加强大。由于固有的在共享基础架构上进行物理硬件提取和多租户移动，云计算实施比传统的以边界为导向的安全性方法要求更高。英特尔TXT通过提供平台可信度保证，并能够报告此信息以供管理基础架构使用，帮助填补这一安全性差距。

例如，考虑VM实时迁移的情况。这一由政策驱动的特性使云服务提供商能够将VM从一个节点迁移到另一节点，甚至是迁移至其他国家的数据中心，从安全性角度来看，这大幅地增加了风险。英特尔TXT通过帮助创建计算资源的可信池，帮助解决这一问题。在这种模式下，通过英特尔TXT衡量启动流程进行过可信度验证的服务器可被标记并分组至可信主机的池中。然后将创建一条政策，限制受信任的VM只能迁移至同一受信任池中或在其他受信任池中迁移。同理，在非受信任的主机中创建的VM将被阻止在受信任池中运行。这样，IT经理或服务提供商获得了其他工具和控制点集，以便为关键应用程序提供更好、更安全的环境。

## Enomaly ECP HAE技术概述

Enomaly ECP™ HAE扩展了Enomaly ECP服务提供商版(SPE)的功能，使电信和服务提供商能够为客户提供比以前的IaaS产品中安全性级别更高的云计算服务。通过Enomaly ECP HAE平台，客户可以将应用程序部署至服务提供商的云中，并确保其数据的机密性和完整性不受损害。

通过满足这一客户需求，服务提供商可以提供具备卓越价值主张的高度差异化的云环境，此外还可将自己定位为唯一能够满足客户安全性要求的云提供商。

此外，因为Enomaly ECP HAE提供能够确保正确地运行其他分层的安全性解决方案（否则，这些解决方案需要在非受信任的虚拟服务器上执行，并且自身会因此而受到怀疑）的可信任基础，Enomaly ECP HAE使云提供商能够构建完全符合特定于部门或特定于行业的要求的云平台。

Enomaly ECP HAE利用特定英特尔处理器和芯片组中的硬件安全性机制，从而使用英特尔TXT来提供对于云的可信度的持续验证。与当今可用的任何云计算服务不同，基于Enomaly ECP HAE的云能够向其用户可靠地证明它未受黑客的攻击和损害。此部分提供Enomaly ECP HAE的概述，并说明它如何操作。

### 远程认证

Enomaly ECP HAE平台使用名为远程认证的机制，确保保护和验证虚拟机管理程序环境的身份，使得该平台能够证明它是可靠的并且未经更改。将使用基于硬件的机制来生成认证证书，此证书记录关于云环境及其配置的精细信息。云服务的用户然后可以使用Enomaly ECP HAE Trust Agent软件来验证认证，核实该平台的可信度与可靠性。

对于服务提供商的云环境中的每台服务器，Enomaly ECP HAE平台在系统启动时引导加载程序运行后立即设置MLE。

在MLE中操作后，Enomaly ECP HAE平台加载并执行虚拟机管理程序并连接根文件系统。加载这些组件时，Enomaly ECP HAE采纳这些组件参数的密码安全的测量值并将其存储于TPM中。在TPM中存储的信息不会被篡改，因此稍后可以依靠这些比较来向用户保证该环境在运行时未曾以任何方式更改。

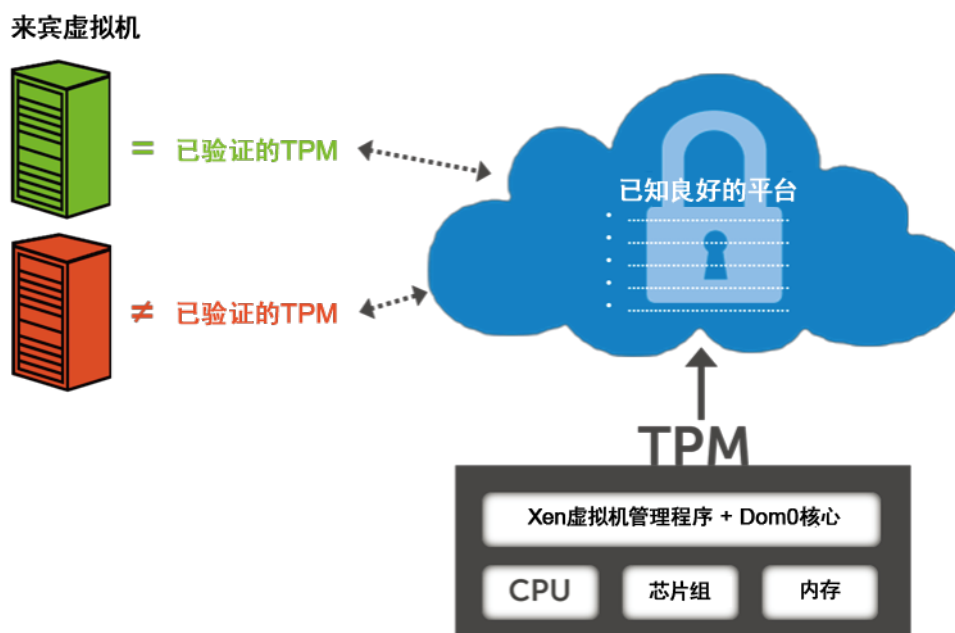
图2. 在TPM中创建MLE和存储值



当用户在云中配置VM并且此VM被配置到Enomaly ECP HAE节点时，相应的TPM值将被检索并与环境在运行时提供的值比较。这可确保在选择的设备上运行经验证的虚拟机管理程序软件堆栈。

Enomaly ECP HAE Protected Boundary包括Xen®虚拟机管理程序、Dom0内核以及服务提供商的云中各个服务器的相关硬件。针对Enomaly ECP HAE配置了服务器时，将捕获并存储这些环境的安全引导时测量值。

图3. 安全传输TPM信息以验证Enomaly ECP HAE环境



为了建立云平台的可信度，当客户配置了新VM时，环境在运行时提供的测量值会与存储的TPM测量值进行比较，以确保实际使用的是有效的Enomaly ECP HAE服务器。这些TPM测量值将安全地传输至用户的设备，在此它们将针对已知良好的平台的清单进行验证。

Enomaly ECP HAE全面地验证虚拟机管理程序平台以及相关的一切。因此，Enomaly ECP HAE可以检测到环境的任何受损情况或未经授权的修改，无论这些行为是有意为之还是无意间造成的。这可针对虚拟机管理程序受损害或被篡改进行保护，这种情况源自各种事件，例如受到与客户信任的VM一起运行的恶意VM的攻击。

通过保护云提供商的基础架构的低层次部分的安全，Enomaly ECP HAE确保维护VM间的隔离。

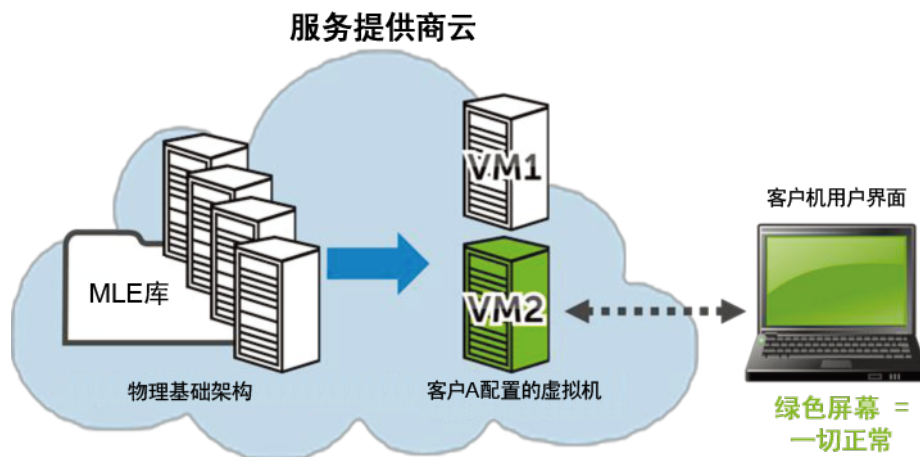
## 运营：正在使用中的Enomaly ECP HAE

Enomaly ECP HAE平台使远程云用户能够建立对云提供商的平台信任。本部分说明这一流程。

以下简化的示例使用Enomaly Desktop Trust Agent。除了Desktop Trust Agent，Enomaly ECP HAE还提供command-line interface (CLI) Trust Agent，以及一个简单的API，通过该API，用户可以自动使用Enomaly ECP HAE云安全性检查，并将其与安全性信息和事件管理(SIEM)系统集成。在典型的使用情况下，Enomaly ECP HAE的用户将结合使用Desktop Trust Agent与CLI Trust Agent和/或Enomaly ECP HAE API集成。

图4显示客户机访问由Enomaly ECP HAE验证过的平台。客户机使用Desktop Trust Agent，此软件使用专利技术来验证云提供商软件环境的可信度。在本情况下，由于客户机连接至经批准Enomaly ECP HAE平台，Desktop Trust Agent显示一条主动通知（由绿色屏幕表示），声明该平台是安全的，可以使用。

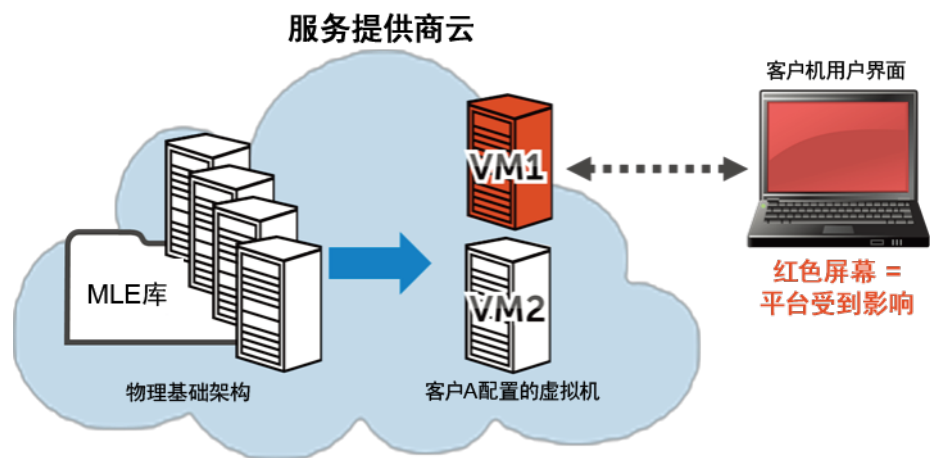
图4. 平台可信度通过验证（绿色屏幕）



另一方面，考虑一下如果云提供商的虚拟机管理程序软件环境被篡改，则会发生什么情况。这种情况可能会由于各种原因而发生：例如云提供商的心有不满的雇员可能会从云提供商的客户处窃取秘密，或者被竞争对手收买的恶意内部人员可以试图窥探云用户的VM。类似地，虚拟机管理程序本身可能会有被黑客探测到的漏洞，用以控制云中的其他VM，从而使攻击者能够篡改云提供商的虚拟机管理程序环境。由于虚拟机管理程序是云计算基础架构中最关键的组件，其可信度的任何损失都意味着直接的灾难性安全性违规。

图5显示了当Enomaly ECP HAE Desktop Trust Agent用于连接被篡改的平台、或者连接至任意组件被非信任的软件所替换的环境中时，会发生什么。Enomaly ECP HAE Trust Agent检测到这种情况，并以红色警告屏幕通知用户。这种红色警告屏幕由Desktop Trust Agent在用户的桌面上本地生成，不会被避开。

图5. 检测到平台可信度违规（红色屏幕）



无论未经批准的平台是因意外还是恶意造成的，Enomaly ECP HAE平台提供对于虚拟机管理程序环境（用户的VM在此环境中运行）的密码安全的可信度检测。

## 测试台蓝图概述

我们的测试台中使用的以下硬件体系结构是云数据中心的典型设计，但因为简单性的原因，规模较小：

- 两台高效Dell PowerEdge R710机架式服务器（基于英特尔至强处理器5600系列）
- 扁平的2层网络
- 本地存储
- 使用虚拟化整合工作负载并提高资源利用率

使用高度自动化的灵活构建块作为云部署的基础，可实现资本支出(CapEx)与运营支出(OpEx)的轻松平衡。

## 测试台硬件说明

表1说明测试台使用的硬件配置。

表1. 测试台配置

| 系统                                                                     | 处理器配置               | 其他信息                                                                                                                                                                     |
|------------------------------------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2个Enomaly ECP™ HAE主机<br>服务器A: 192.168.101.130<br>服务器B: 192.168.101.140 | 英特尔®至强®处理器<br>X5667 | 平台: Dell PowerEdge™ R710机架式服务器<br>外形规格: 2U机架式<br>处理器: 英特尔至强处理器X5667, 3.06 GHz, 2路 x 6个核心 = 12个核心<br>内存: 24 GB RAM<br>存储: 300 GB硬盘<br>软件: CentOS 5.5 x64, Enomaly ECP HAE |
| 网络: Cisco Nexus 5010<br>S2410-01-10GE-24CP                             | 不适用                 | 英特尔®82576千兆位以太网控制器网络连接                                                                                                                                                   |

戴尔支持了从全球《财富》500强公司到小型企业等上千家客户环境的虚拟化。许多戴尔系统都可用于此目的，但Dell PowerEdge R710基于灵感来自于客户的特定设计考虑，并在设计时谨记虚拟化与可扩展性。它采用2U机箱，提供高达12 TB的内部存储、最大288 GB的1333 MHz内存，以及在SD卡或内置USB中的嵌入式虚拟机管理程序。可配置性极高的Dell PowerEdge R710提供可促进快速部署的特性。额外的通用可扩展固件接口(UEFI)提供对于物理服务器和虚拟服务器的强大的管理功能。Dell PowerEdge R710为安全灵活的云基础架构提供了坚实的基础。

## 安装和配置

本部分说明Enomaly ECP HAE的安装和配置过程。

### 初始BIOS更改

- 英特尔TXT设置为“Enabled”（启用）
- TPM状态设置为“Enabled and Activated”（启用并激活）
- 在BIOS中设置了有效的密码

### 软件安装、配置和功能验证

#### **第1步：操作系统安装**

在本书发布时，Enomaly ECP HAE在CentOS 5.5和Red Hat® Enterprise Linux® 5.5上享有正式支持。此特定测试台使用CentOS 5.5。安装该操作系统的要求如下：

- 必须启用IPv4支持，必须禁用IPv6支持
- 建议为所有服务器使用静态IP地址
- 在设置时必须指定域名

#### **第2步：Enomaly ECP HAE安装**

安装Enomaly ECP HAE之前，务必适当地配置服务器上的BIOS，以便使TPM可供配置。建议的BIOS设置如图6和图7所示。

图6. 建议的处理器BIOS设置

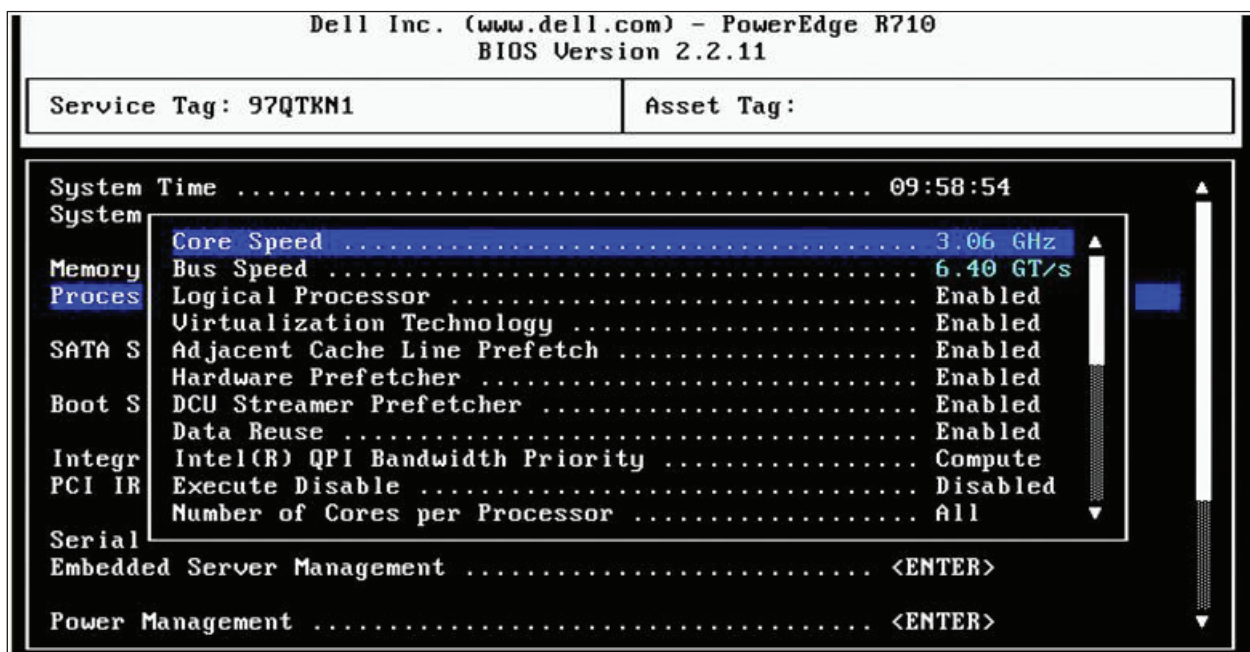
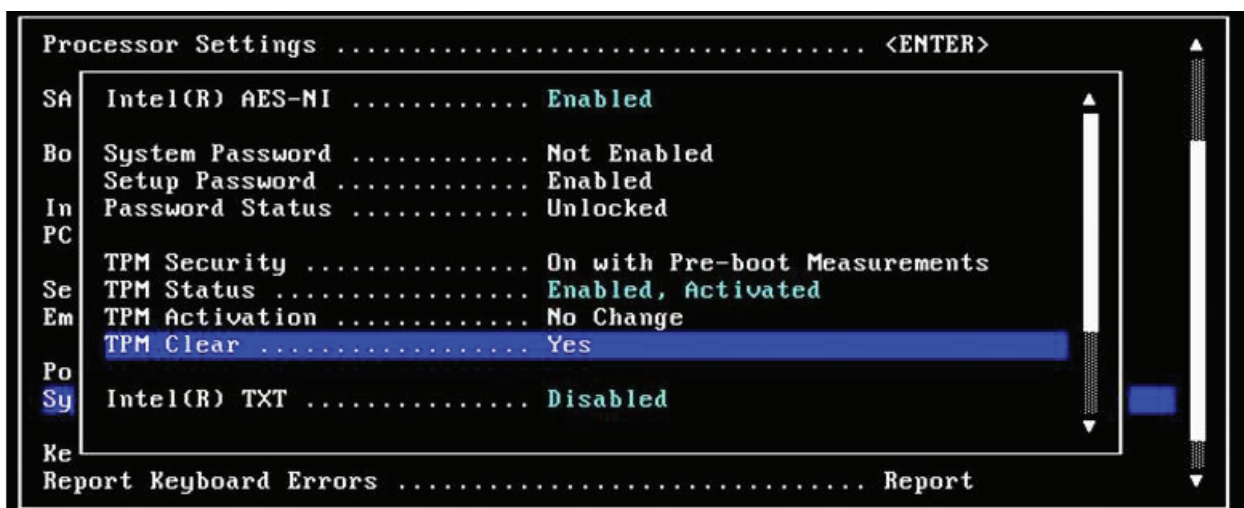


图7. 建议的操作系统和I/OAT BIOS设置



最后，重置TPM并在设置的第一部分中禁用英特尔TXT。完成这些配置更改后，将服务器完全关闭并重新启动。

Enomaly ECP HAE包括三项服务：

- Enomaly ECP Web Interface (ecp)
- Enomaly ECP Manager (ecpmanager)
- Enomaly ECP Agent (ecpagent)

默认情况下，Manager安装脚本会在同一主机上安装Enomaly ECP Web Interface和Enomaly ECP Manager。

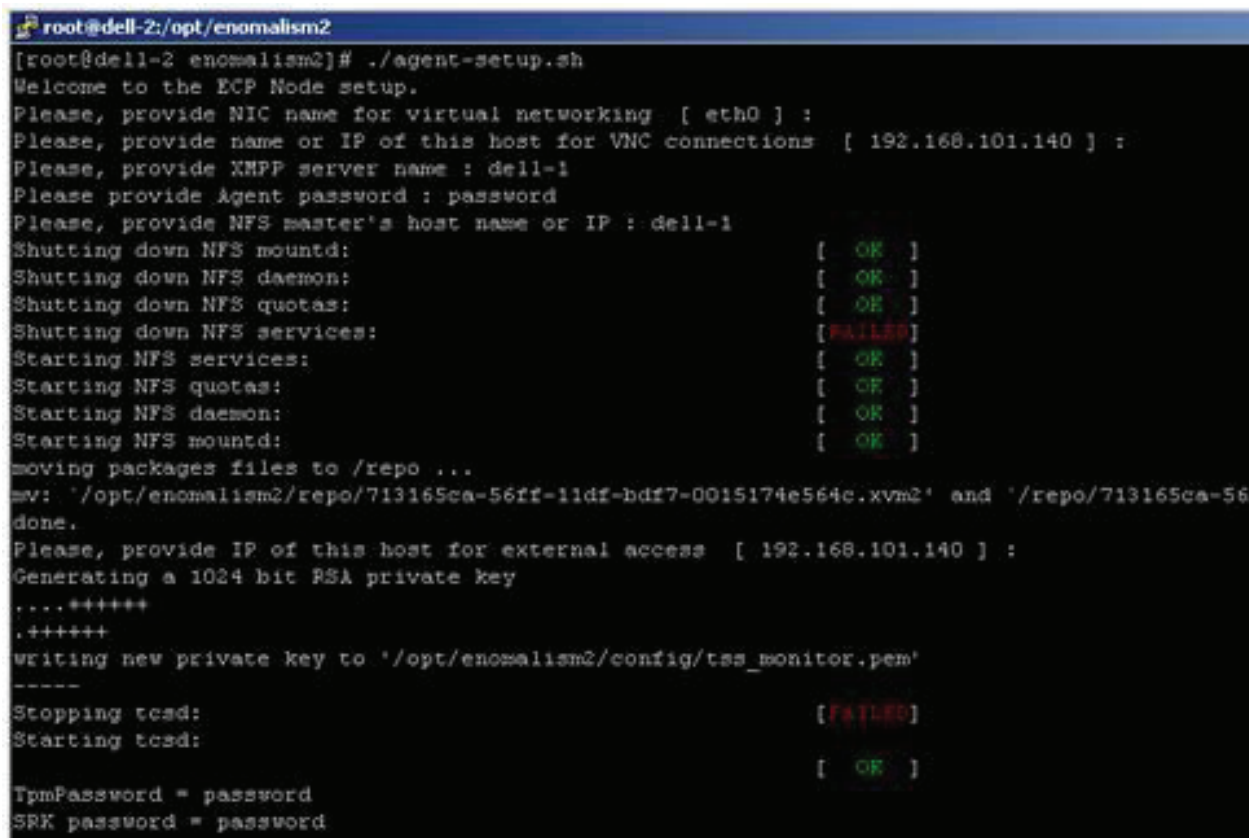
### 第3步：Enomaly ECP HAE配置

Enomaly ECP HAE安装流程在Enomaly ECP HAE安装说明文件的第1.3部分中详述，本参考体系结构中不再赘述。

### 第4步：Enomaly ECP Agent安装

除了Enomaly ECP HAE安装说明文件的第1.3部分中详述配置步骤外，还需要有TPM配置步骤。此代理安装的结果如图8所示。通常在停止尚未运行的服务时会出现失败，但在设置过程中，这是正常的。

图8. 设置Enomaly ECP Agent



```
root@dell-2:/opt/enomalism2# ./agent-setup.sh
Welcome to the ECP Node setup.
Please, provide NIC name for virtual networking [ eth0 ] :
Please, provide name or IP of this host for VNC connections [ 192.168.101.140 ] :
Please, provide XMPP server name : dell-1
Please provide Agent password : password
Please, provide NFS master's host name or IP : dell-1
Shutting down NFS mountd: [ OK ]
Shutting down NFS daemon: [ OK ]
Shutting down NFS quotas: [ OK ]
Shutting down NFS services: [ FAILED ]
Starting NFS services: [ OK ]
Starting NFS quotas: [ OK ]
Starting NFS daemon: [ OK ]
Starting NFS mountd: [ OK ]
moving packages files to /repo ...
mv: '/opt/enomalism2/repo/713165ca-56ff-11df-bdf7-0015174e564c.xvm2' and '/repo/713165ca-56ff-11df-bdf7-0015174e564c.xvm2'
done.
Please, provide IP of this host for external access [ 192.168.101.140 ] :
Generating a 1024 bit RSA private key
.....+++++
.+++++
writing new private key to '/opt/enomalism2/config/tss_monitor.pem'
-----
Stopping tssd: [ FAILED ]
Starting tssd: [ OK ]

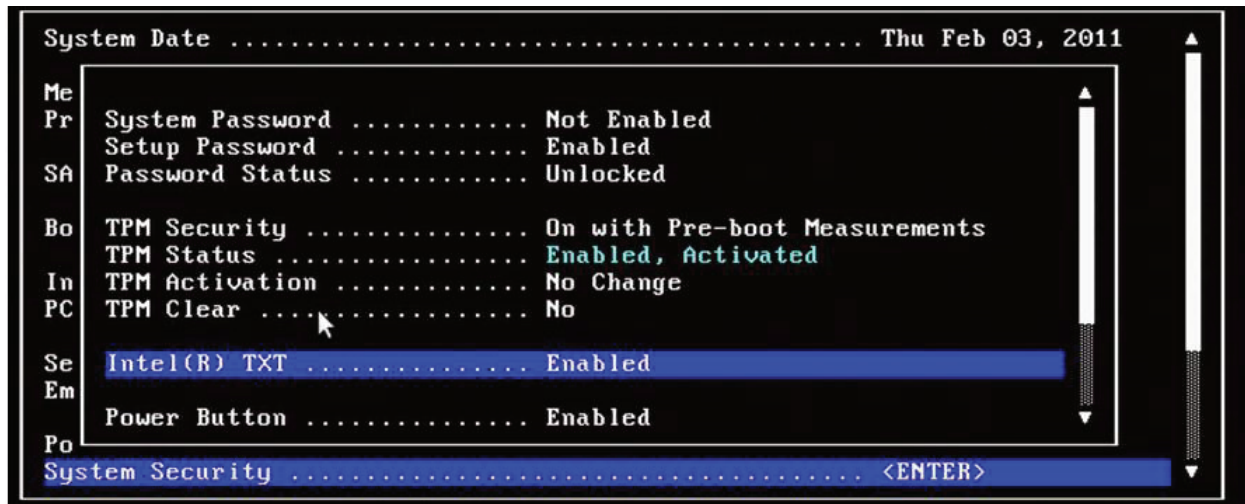
TpmPassword = password
SRK password = password
```

### 第5步：安装后

完成安装后，重新引导系统并重新启用英特尔TXT。重新引导至BIOS并确保满足以下要求：

- 英特尔TXT设置为“Enabled”（启用）
- 以预引导测量值启用TPM
- 保存了设置
- 系统经过了关机后重新启动这一过程

图9. 建议的安装后BIOS设置



服务器现在应引导至受信任、启用了测量值的引导环境。

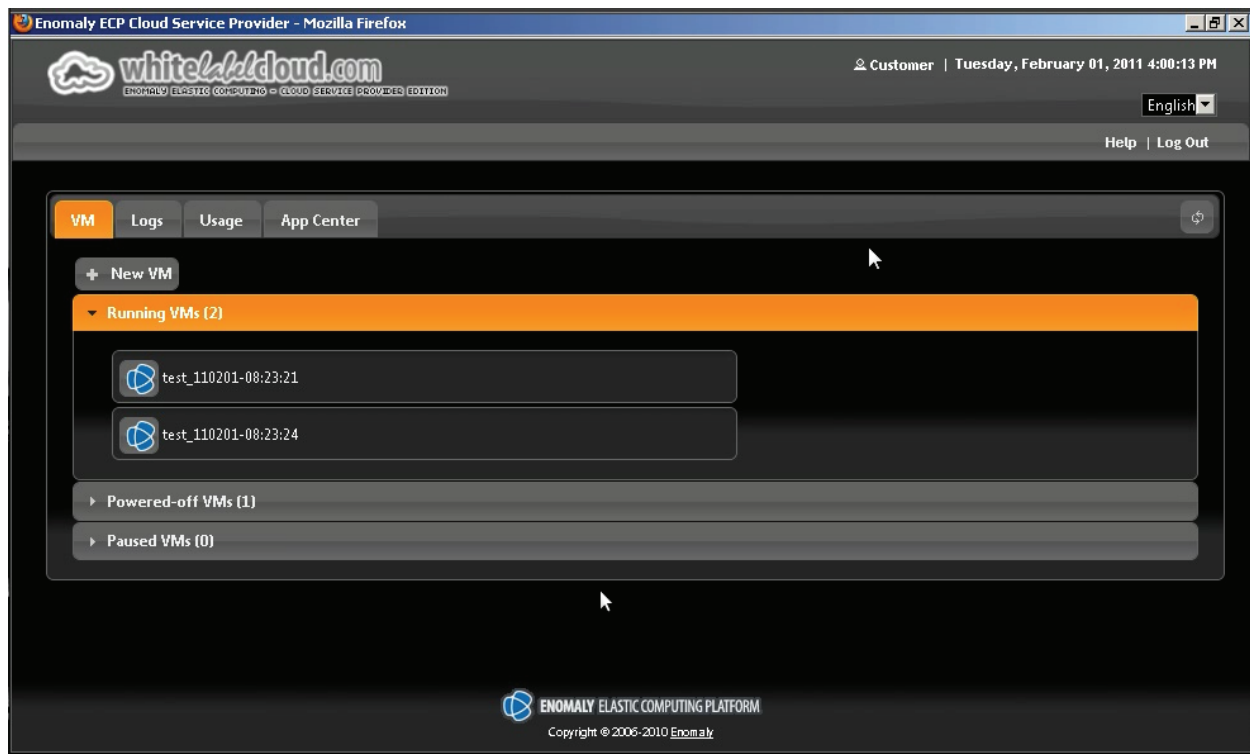
## 验证系统功能的前提条件

### 创建两个Enomaly ECP HAE VM

此时，创建了两个虚拟机以供使用。如需创建VM的详细信息，请参见英特尔云构建器Enomaly ECP SPE参考体系结构。<sup>4</sup> 图10显示了这两个VM。

<sup>4</sup> 英特尔®云构建器指南到基于英特尔®至强®处理器的平台上的云设计和部署：Enomaly Elastic Computing Platform™，服务提供商版：<http://software.intel.com/file/31968>

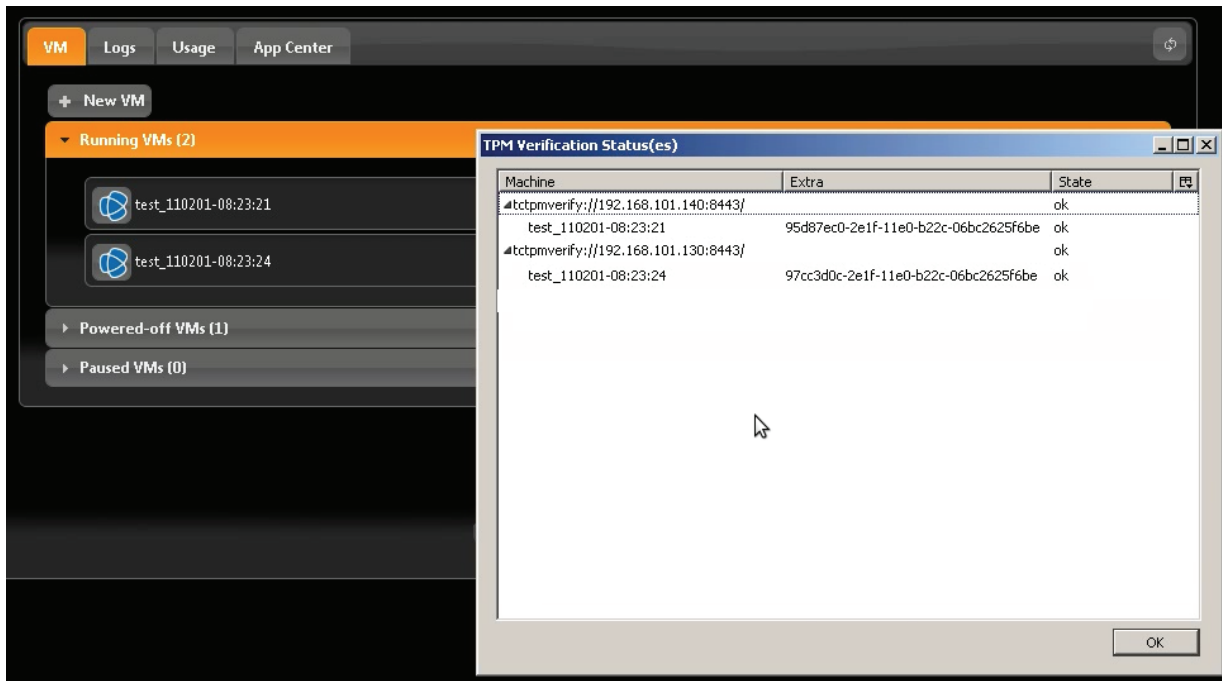
图10. 两个正在运行的虚拟机



#### 为正在运行的VM验证TPM功能

Enomaly ECP HAE提供可用于验证VM的受信任状态的代理。这些代理以多种形式提供，其中包括 Mozilla® Firefox®浏览器扩展。本测试使用Firefox扩展来监控TPM的状态，并因此监控正在运行的VM的状态。01显示两个VM都值得信任。Firefox扩展显示这两个VM在两个不同的物理主机上运行（服务器A：192.168.101.130；服务器B：192.168.101.140）。

图11. 为两个VM验证TPM功能



## 英特尔TXT使用案例

在本参考体系结构的测试阶段，运行使用案例来模拟典型的数据中心的安全攻击。

### 使用案例1：攻击导致引导环境被修改

本使用案例将服务器B引导至没有Enomaly ECP HAE或受信任引导哈希值的CentOS内核，以便模拟由恶意的管理员或攻击者发起的攻击（例如内核更换或修改）。如图12所示，Enomaly ECP HAE Web UI门户使用红色锁图标提供明确的指示，表明在服务器B上运行的VM不受信任。

图12. 在服务器B上运行的VM不受信任

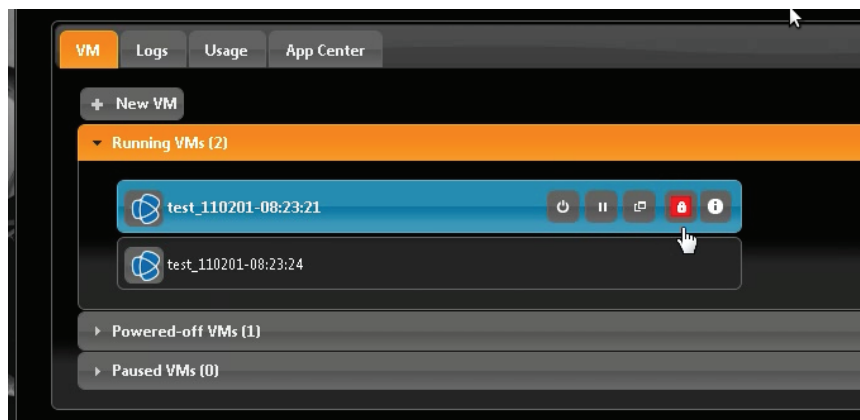
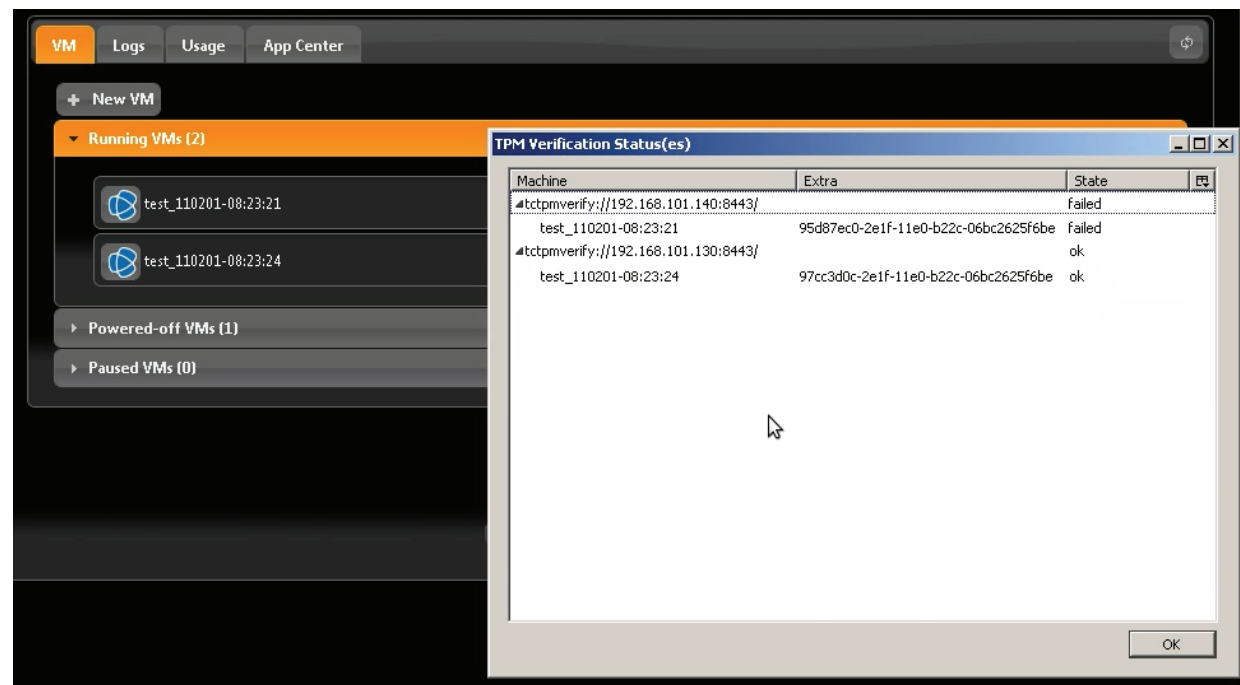


图13使用Firefox浏览器插件程序显示两个VM的状态。 其中一个VM（在服务器B上运行的那一个）未通过TPM检查；而在服务器A上运行的VM是在受信任主机上运行，而且运行时测量值与TPM哈希值匹配。

图13. Mozilla Firefox插件程序显示服务器B上的VM不受信任

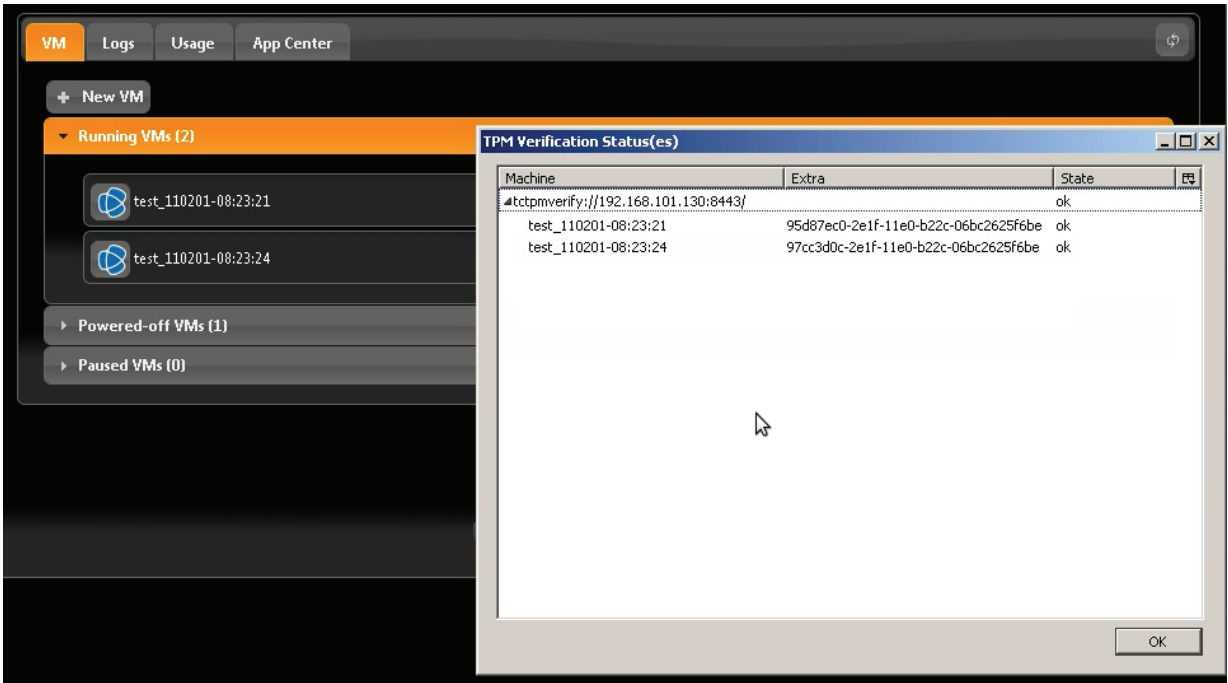


使用案例2：验证向受信任主机重新分发受信任VM

本测试案例验证当遇到灾难性硬件故障时，受信任的VM将向受信任的主机迁移。此硬件故障通过拔出服务器B的电源线来模拟。

如图14所示，先前在服务器B上运行的VM迁移到了服务器A上。两个VM的运行时测量值都与TPM哈希值相匹配，并被标记为受信任。

图14. 服务器故障：VM迁移至另一受信任主机（服务器A）



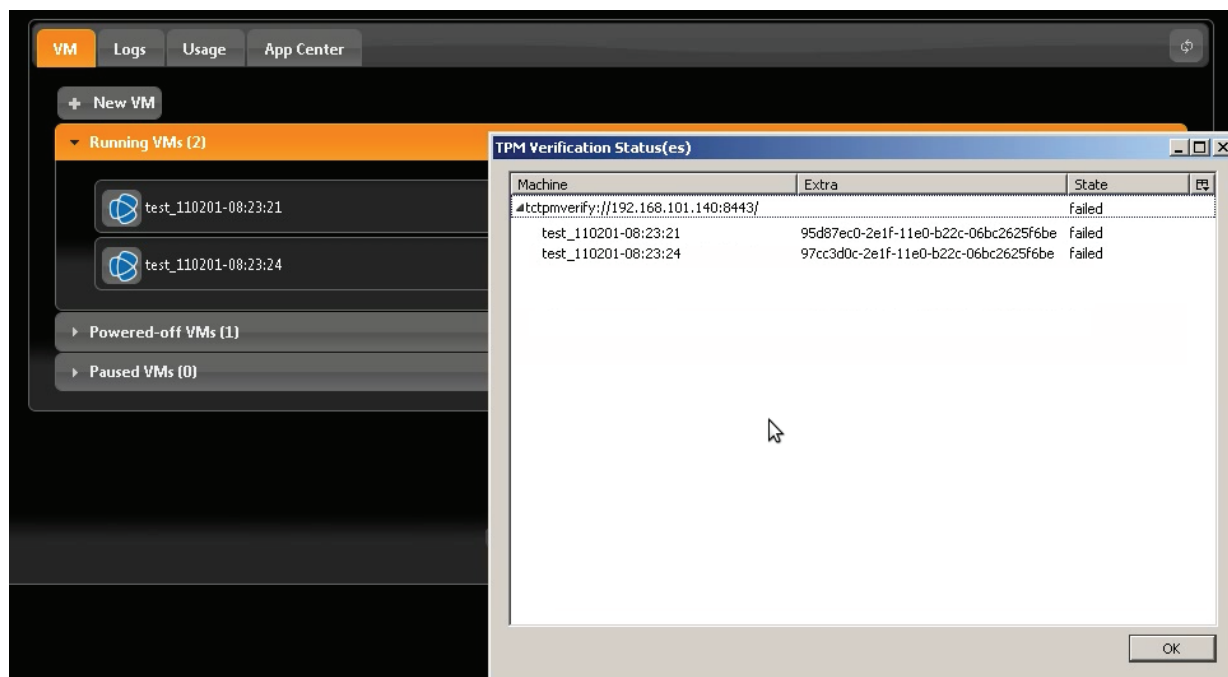
使用案例3：验证受信任VM向非受信任主机的意外迁移是否会被标记为违规

上一个使用案例验证了在意外情况下VM向受信任服务器的迁移。 该服务器未配备支持英特尔TXT（或服务提供商未适当认证的技术）的处理器。 本使用案例确保另一方面，即受信任的VM不会向非受信任的服务器迁移。 这可能在不同的情况下发生，例如攻击者在受信任服务器上运行拒绝服务攻击，以便迫使向非受信任的服务器上再分发。

为了执行此测试，服务器A（上一使用案例中运行两个VM的受信任节点）被关机，而服务器B继续运行没有Enomaly ECP HAE的内核。

图15显示，在服务器B上运行时，两个VM都被标记为非受信任。

图15. Enomaly ECP发起的VM向非受信任主机的迁移被标记为非受信任

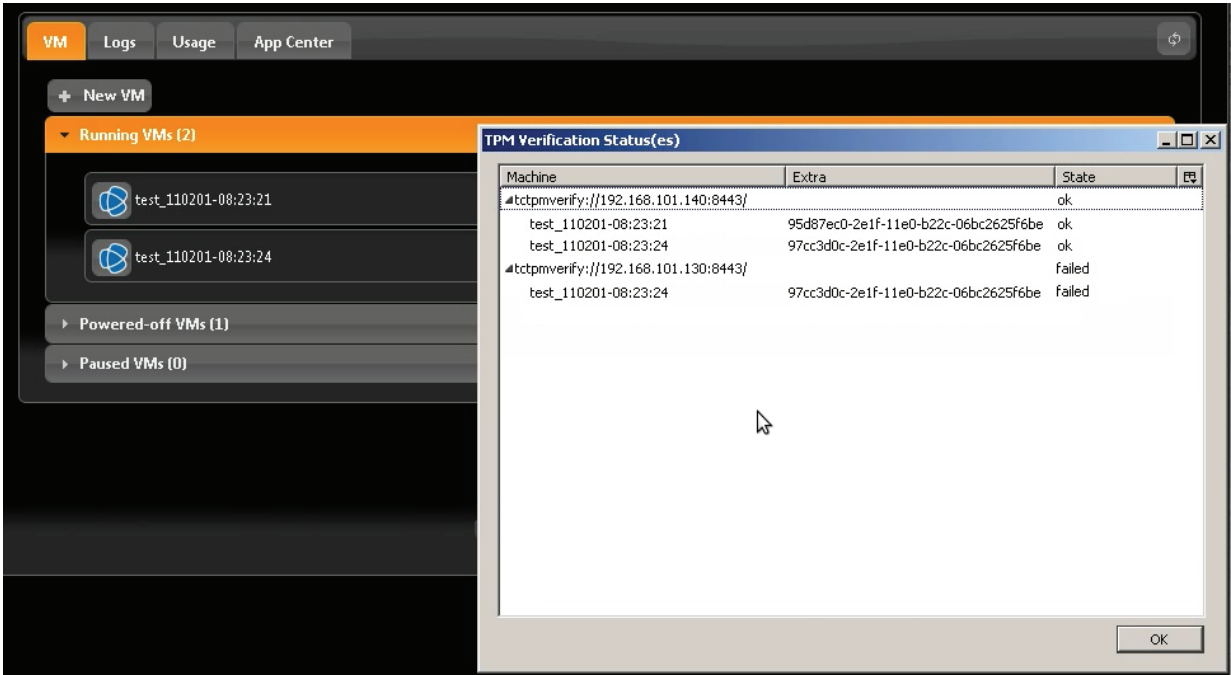


#### 使用案例4：验证VM向非受信任主机的手动迁移是否会被标记为违规

对于本使用案例，我们确保两个受信任的VM都在服务器A上运行，该服务器引导至受信任的Enomaly ECP HAE内核。服务器B引导至没有Enomaly ECP HAE的内核，因此不受信任。

然后使用脚本movevms.py（在Enomaly ECP HAE和Enomaly ECP SPE中都包括）将其中一个VM移动至服务器B。该VM迁移后，Enomaly ECP HAE Web UI门户立即将其标记为不受信任，如图16所示。

图16. 强制VM向不受信任的主机上迁移：VM被标记为不受信任



### 注意事项

云解决方案的可扩展性可能受多个因素的影响，例如选择的网络体系结构、存储实施以及是否使用高性能计算节点。

### 网络技术体系结构

Enomaly ECP HAE支持多种网络体系结构。对于本测试台，使用了扁平的2层拓扑。这一选择能够胜任基本的测试案例。对于生产部署，更高级的技术和体系结构（例如10千兆位以太网和通道绑定）则更为合适。

### 存储体系结构

Enomaly ECP HAE支持一系列存储体系结构。对于本测试台，出于简单性的目的使用了本地存储。对于生产云部署，则应使用某种形式的网络连接存储体系结构。如果打算部署I/O任务量繁重的工作负载，使用固态硬盘(SSD)可帮助提高总体性能和使用寿命，同时降低数据中心级别的总功耗。

### 硬件考虑因素

对于处理器和总体服务器性能及能效的完整讨论超出了本参考体系结构的范围。但是，在云实施中运行的VM的性能和密度可能受到处理器体系结构和提供的特定特性集（例如英特尔®定向I/O虚拟化技术[英特尔®VT-d]）的严重影响。对于一般的生产部署，强烈推荐使用高性能、高能效的服务器，例如基于英特尔至强处理器5600系列的Dell PowerEdge服务器。对于利用英特尔TXT的部署，需要使用基于英特尔至强处理器5600系列的服务器。

## 结论

本书详细说明了一些使用英特尔TXT和Enomaly ECP HAE来打造云中的信任基础的模型。对于旨在支持要求比商品云平台更高信任度的用户工作负载的云部署，此蓝图包括多层安全性的可信云计算基础架构提供了合理的基础。对于公共云服务提供商，本体系结构还消除了提供更安全的公共云体系结构的一个主要障碍，并提供实现差异化的机会，从而为担忧在公共云中运行其应用程序的政府和工业部门提供了接触机会。

## 词汇表

**验证代码模块(ACM)**：特定于平台的代码，经过芯片组的验证并在处理器的隔离环境中执行。此术语也用于表示由ACM支持的可信任环境来执行安全的任务。

**SINIT**：安全的虚拟化；衡量、验证和启动MLE的受信任流程。

**SMX**：较安全的设备扩展；增加到支持英特尔TXT的精选英特尔处理器的功能。

**TCG**：可信计算组；为了推进计算机安全性的行业计划。如需更多信息，请参见 <http://www.trustedcomputinggroup.org>。

**VM**：虚拟机；是像物理设备一样执行程序的计算机的软件实施。

**计算节点**：运行Enomaly ECP HAE并托管VM的服务器。

**经衡量的启动环境(MLE)**：按照GETSEC (SENTER)说明衡量并启动的环境。

**受信任的平台模块(TPM) 1.2**：由TCG定义的硬件设备，可提供一系列由英特尔TXT使用的安全性特性。

**英特尔TXT**：英特尔可信执行技术。

**英特尔VT-d**：定向I/O虚拟化技术；英特尔VT的硬件支持组件，用于管理直接内存访问(DMA)和由I/O设备引起的中断。

**英特尔VT-x**：面向执行环境的虚拟化技术；一组由英特尔VT定义的处理器指令(.vmx)和功能，软件使用它来为虚拟环境提供隔离和保护。