

## 构建企业私有云的最佳实践

### 概要

在我们踏入企业私有云开发的最终阶段之际，我们在多个方面确定了最佳实践。这些最佳实践可帮助我们实现云计算的最大业务优势、将解决方案快速引入到我们的企业计算环境中，以及实现我们的业务目标。

英特尔 IT 部门在跨越数年的企业私有云构建方面取得显著的进展。到目前为止，实施云战略已帮助我们实现了 9 百万美元的节约，而且我们预计将在未来 4 年内实现大约 1400 万美元的净现值（NPV）。

现在，大多数英特尔业务团队在我们的私有云中运行应用，享用着在过去所没有的计算能力。我们由于有广泛的自动化能力，实现了自助服务基础设施供应的标准化——在我们的私有云中，80% 的新服务器可在三小时内提供，其中大部分更可在 45 分钟内完成。

我们在基础设施即服务（IaaS）之外积极地扩展使用模式，并制定了相应的蓝图来实施混合云环境，以获更高的灵活程度和效率。在我们踏入企业私有云开发的最终

阶段之际，我们在多个方面确定了最佳实践。这些最佳实践可帮助我们实现云计算的最大业务优势、将解决方案快速引入到我们的企业计算环境中，以及实现我们的业务目标。这些目标包括：

- IT 资产有效使用率达 80%
- 稳定的业务速度提升
- IT 基础设施故障的零业务影响

展望未来，这些最佳实践将有助于持续发挥云计算在英特尔的全部优势。

Sameer Adhikari

英特尔 IT 部门云计算商业智能架构师

Greg Bunce

英特尔 IT 部门自动化设计领队

Winson Chan

英特尔 IT 部门软件工程师

Ajay Chandramouly

英特尔 IT 部门行业参与经理

Das Kamhout

英特尔 IT 部门 IT 云计算领队

Brian McGeough

英特尔 IT 部门托管云设计经理

Jon Slusser, Jr.

英特尔 IT 部门云服务运营经理

Catherine Spence

英特尔 IT 部门企业架构师

Bill Sunderland

英特尔 IT 部门 IT 云计算基础设计

## 目录

|                     |    |
|---------------------|----|
| 概要.....             | 1  |
| 背景.....             | 2  |
| 制定私有云战略.....        | 5  |
| 打造全面的托管云能力.....     | 6  |
| 实现虚拟化普及.....        | 8  |
| 建立端到端状况监控.....      | 10 |
| 提供灵活的容量和可衡量的服务..... | 11 |
| 支持按需自助服务.....       | 12 |
| 成效.....             | 13 |
| 后续工作.....           | 13 |
| 结束语.....            | 14 |

## IT@INTEL

IT@Intel 计划将全球各地的 IT 专业人员及其在我们机构中的同仁紧密联系在一起，共同分享经验教训、方法和战略。我们的目标十分简单：分享英特尔 IT 部门最佳实践，获得业务价值并实现 IT 竞争优势。如欲了解更多信息，请访问 [www.intel.com/cn/IT](http://www.intel.com/cn/IT) 或联系您当地的英特尔代表。

## 背景

作为我们整体数据中心战略的一部分，英特尔 IT 部门正在把我们的数据中心基础设施按业务作垂直式整合和优化来提高业务效率，以满足英特尔各重要业务职能部门的不同需求：设计、办公、制造、企业和服务（DOMES）。如图 1 所示，云计算是办公、企业和服务方面的关键计划。

我们正在积极开展一项跨越数年的项目来实施企业私有云，为我们的办公、企业和服务应用提供支持，例如数据库、文件和 Web 访问。作为云基础设施的标准，我们采用了基于英特尔® 至强® 处理器 5500 系列的服务器和基于英特尔® 至强® 处理器 5600 系列的服务器这一战略性组合。尽管我们的私有云建设还未完成，但我们已经取得了突出的成就，最显著的是由自助服务来提供计算基础设施。

随着 2012 年的来临，我们关注的重点将转移至使用云计算来提供数据和应用平台服务。我们的目标是开发企业私有云来交付高度可靠的计算环境——共享、灵活的多租户基础设施，为通过验证的用户和设备提供高度安全的按需服务和数据。除此之外，我们的战略愿景还包括打造一个可靠的混合云环境，为我们下列的业务战略和目标提供支持：

- IT 资产有效使用率达 80%。我们计划采取全面的虚拟化组合来提高资源使用率，并降低我们的资本和运营支出——由更少数的数据中心内的更大的虚拟机池改进用户之间的共享。我们认为，能让所有业务部门共享所有英特尔资源的能力，有助于实现更高的容量重复使用率。为达到这一目标，我们在合适的时候使用专门的硬件来创建可替代的大型资源池。
- 稳定的业务速度提升。我们希望在企业内实现按需自助服务的标准化。未来，我们预计将对此概念进行扩展——在几分钟内供应虚拟机，以及只需点击一个按钮或者一个 API 呼叫来提供完整的应用环境。此外，我们还期待使用外部云来应对高峰需求，并把资源配备决策的自动化。所有这些措施均可支持更大的资源池，让开发人员可在一天之内将创新理念转化为实际的工作服务。
- IT 基础设施故障的零业务影响。使用针对故障和自动化端到端服务托管云而设计的云感知型应用组合，可以确保我们的服务始终处于运行状态，即便是在基础设施出现故障的情况下也不例外。

### 英特尔数据中心概况

|      |               |
|------|---------------|
| D 设计 | 可扩展的高性能计算解决方案 |
| O 办公 | 企业私有云         |
| M 制造 | 工厂自动化         |
| E 企业 | 企业私有云         |
| S 服务 | 企业私有云         |

图 1. 云计算为办公、企业和服务业务等职能带来显著的优势。

我们的私有云环境为英特尔带来了重要的优势：

- **灵活程度。**我们的新服务器中有 80% 在三小时内提供，其中大部分更是在 45 分钟内完成。而两年前，在传统 IT 环境中供应服务器通常需要长达 90 天的时间。
- **商业智能。**我们根据实际数据来测量系统的使用率和状态，并为英特尔各业务部门提供清晰的数据以帮助他们作资源规划。
- **伸缩力。**我们正处于根据用户需求实现资源动态扩展的最终阶段，这有助于提高基础设施效率，加速响应用户需求。用户目前已经可使用我们的自助式供应门户网站进行纵向扩充，在未来 6 个月内，我们预计可提供更自动化的伸缩力，经由横向扩展和缩减来满足高峰容量需求。
- **经济高效。**由于具有多用户和资源集中功能，私有云可实现更高效的资源使用。我们在云计算方面的投资已经证明

了其价值，而且帮助我们节约了 9 百万美元的现金（不包括非现金业务价值，例如员工效率提升）。在迁移到云计算之前，我们的平均使用率为 8% 左右。而完成迁移后，我们的使用率增加至 40%，而且我们预计随着企业私有云环境部署的完成，可实现进一步的使用率提升。

其它优势还包括：显著减少基础设施占地面积 — 包括服务器、机架、网络端口和 I/O 端口 — 以及增强网络管理和、灾难恢复能力，以及减少温室气体排放和能耗。

英特尔云挑战和解决方案概述

在过去的两年中，云计算行业的成熟度显著提升。市场中出现了许多现成的产品，这些产品在我们刚开始开展私有云计划时还没有存在。因此，我们开发了特定应用来满足我们的云计算需求，并让我们可以重复使用在企业 IT 管理的现有投资。

在开发英特尔企业私有云时，我们面临着多种挑战：

- 完整的云基础设施
- 虚拟化的普及
- 端到端的系统状态监控
- 灵活的容量与可衡量的服务
- 按需自助服务

在进入私有云实施和部署的最后阶段时，我们继续针对其中一些挑战开发相应的解决方案。

完整的云基础设施

与供应链管理相似，我们将来自云基础（网络、存储、计算、应用和设施）的数据整合来创建计算基础设施即服务（IaaS）。我们消除了数据孤岛以创建单一的数据仓库，让员工和自动化工具均可使用该数据仓库来进行实时决策制定。我们使用传统数据库技术开发的内部解决方案，针对我们的云环境提供了高度可靠和经济高效的基础设施。

如图 2 所示，我们可以使用完备的数据来预测问题以免导致发生中断，或者在出现问题时进行快速的修复。

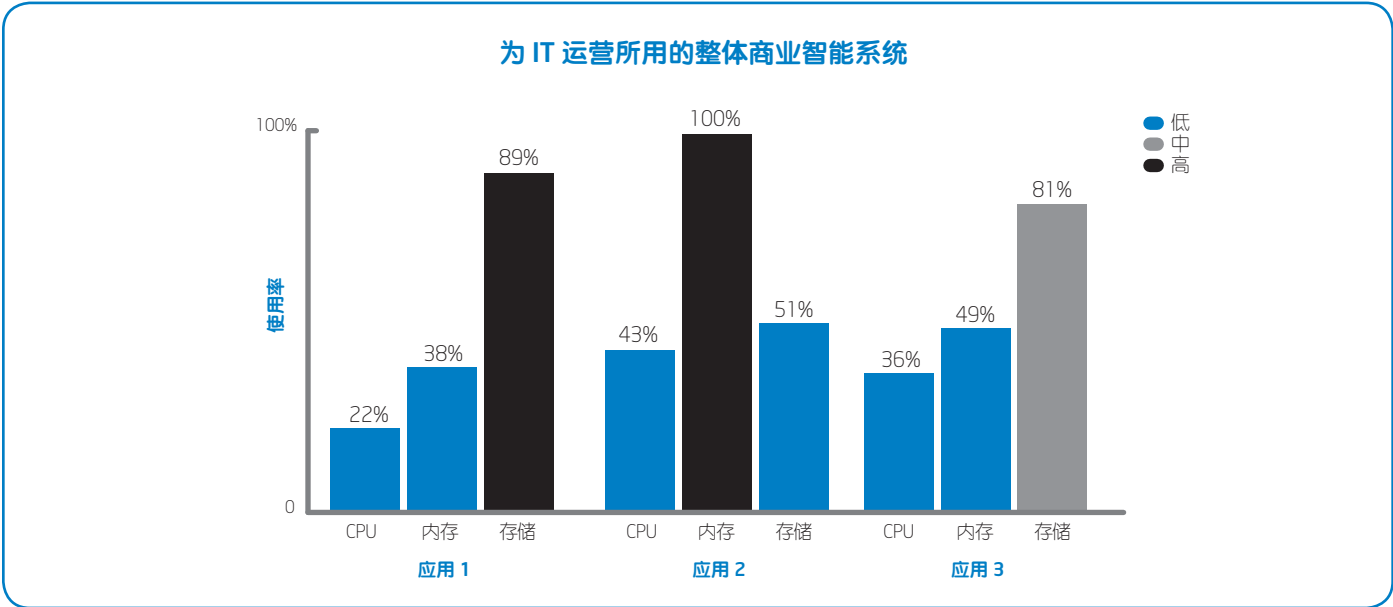


图 2. 我们的集成式数据信息可根据各个应用向我们发送关于 CPU、内存和存储使用率问题的告警。

## 虚拟化普及

当我们决定构建私有云时，已开始部署虚拟化。但是，我们的部署规模相对较小：虚拟化本身没有什么规则，更多的是应对意外情况，例如响应业务部门的特定请求。直到 2009 年底，我们仅完成了约 12% 的办公和企业应用虚拟化。我们的容量和虚拟化能力有限；由于技术限制，我们仅能对较小和要求较低的系统进行虚拟化，而这些系统在整个环境中所占的比例还不到 50%。

此外，由于技术的局限，某些早期虚拟化的工作没有令人满意的效果，因此 IT 管理层在支持完整规模的虚拟化上有所保留。虚拟化进度缓慢的另一个原因是，尽管架构师和工程师已设计出虚拟化解解决方案，但我们的运营团队并未向业务团队积极阐明我们的计划，鼓励他们进行虚拟化。

以下这三个因素可为我们在虚拟化方面的发展提供动力：

- IT 管理人员明确授权，将虚拟化作为优先执行的任务。
- 扩展技术能力，使我们能够扩展虚拟化项目的范围，同时确保服务质量，并不会对实际工作环境造成任何负面影响。
- 我们积极展示了虚拟化能够带来显著的业务价值。

## 端到端的系统状态监控

在英特尔，某些英特尔应用是交由外部供应商托管的，但是过去只有我们的应用开发团队对监控这些外部托管的应用感兴趣。随着我们的私有云的日趋成熟，我们开始在云计算环境中提供服务，因此我们

必须监控这些外部托管的应用，以便衡量总体服务的稳定程度。

对云环境进行端到端的监控，其复杂程度超过了对分布式系统的监控，因为我们必须整合内外部的系统和服务监控。此外，我们还要为运营支持员工定义新的任务，以便将我们的支持服务级别协议（SLA）转化为真正的端到端监控。而且，由于监控涉及多方面的知识领域和支持机构，其中包括设施、网络、存储、计算和应用，我们在 IT 运营团队和内部用户软件开发团队之间建立了共同负责的机制。

为解决这些问题，我们开发了一套工具来定义服务状态模型，并收集来自每个组件级域的监控数据。然后，该工具动态提供服务级别仪表板，帮助 IT 运营支持团队了解服务是否正常运行，还是发生故障或降级的情况。支持团队可根据该仪表板监控此类状态变化。我们整合来自多个监控系统的报告，可以完整了解用户体验和事件的如何严重。

我们执行了一系列概念验证，为数量有限的应用团队提供了新的监控工具。这些概念验证展示了该新功能可以提供更清晰的事件管理记录流程，并大幅度减少了刺耳的警告和人工错误。

这种新的工具提供自动化的一站式事件管理记录流程，可减轻 IT 运营支持团队的负担 — 他们无需浏览数千个无关的事件数据并决定需要记录哪些数据。这样可让团队将精力放在更有效率和要求更苛刻的任务上，例如管理日益复杂的内外部应用和服务部署，且无需增加资源投入。

## 灵活的容量与可衡量的服务

要根据需求快速扩展，就必须能够检测需求增加的情况、了解哪些容量可用于横向扩展并从历史的角度查看该数据，以确定正常和高峰使用率。尽管公共云用户通常认为其可以无限扩展，但事实上，数据中心（甚至一组数据中心）中并没有具备无限扩展能力的组件。我们的私有云的目标是创建一个与无线扩展能力近似的情境来满足业务需求。

我们开发了相应的方法来确定业务部门应用的资源需求并快速提供，而且对服务进行衡量，并时常向业务部门报告相关的使用信息。在总体云解决方案堆栈的其它领域，则包括部署自动化和商业智能工具来支持灵活的响应和可追溯既往的需求来作分析，帮助我们了解每个应用需求的性质。

除了基础层面上的灵活，我们需要为用户从私有云中提供质量最佳服务。将多台虚拟机整合到一台主机带来了严峻的性能/容量管理问题，许多传统的管理解决方案对此无能为力。过度供应虚拟机和基础 I/O、内存或 CPU 的风险会导致服务质量下降。为了应对这一复杂事项，我们在汇集通透的子系统使用情况，并将有关数据视图与在平台和/或基础设施上运行的应用或服务作对照。

我们用一个例子来说明集成数据如何能帮助改进决策制定。例如，我们发现许多虚拟机在每天下午 4 点都会出现 I/O 延迟问题。我们把相关的数据整合与分析后，发现在许多系统上同时运行的一个进程导致了 I/O 超量的问题。在把数据集成之前，我们将该数据视为一个孤岛，不单止无法

了解该问题有多大，而且，也没有将虚拟机性能与 I/O 的局限关联在一起研究。

### 按需自助服务

为提高效率，云环境应具备自动化能力，让用户能够自行获得计算资源，从而消除手动流程。除了创建该系统所需的后端自动化工作外，我们还需要开发一个简单、直观，而且最重要的是，可按需定制的前端系统。我们尤其不希望用户需要与多个门户进行交互才能自助获得各部分基础设施，例如存储、虚拟机和网络资源。我们希望为所有基础设施服务打造一站式平台。

工作流自动化在企业中实施虚拟化中极为重要。我们调整了业务流程以便在环境中充分使用自动化工具。此外，我们还确定了在哪些情况下，自动化工具不足以解决问题。我们意识到对自动化的依赖程度越高，就越需要一致的流程和基础设施。

尽管我们的设计和制造环境的自动化程度已经达到相当的水平，但我们的企业 IT 环境仍采取手动的方式执行许多任务。我们替换了 IT 运营团队所执行的大量手动流程和职能——这是一项艰巨的工作。此外，我们还在相同的自动化框架中整合了与业务、技术和用户相关的流程。

由于没有可以满足我们所有需求的现成的工作流自动化解决方案，我们只好自己构建。我们构建的解决方案可访问支持其它云解决方案层所需的标准接口，例如状态监控以及按需自助供应。

## 制定私有云战略

**构建英特尔的企业私有云是一项为期多年的复杂流程，我们需要制定一套全面的战略。我们决定采取由内到外的方式来构建我们的云计算，首先关注的是实施私有 IaaS。现在，我们将重点转移至向特定使用案例提供平台即服务（PaaS）和软件即服务（SaaS）。**

我们的云战略有助于推动实现可观的成本效益。我们从高达 20:1 的平均服务器整合率获得了 9 百万美元的节约，预计在未来 4 年内将会实现大约 1400 万美元的净现值（NPV）。

### 首先实施计算 IaaS 来支持企业使用模式

云计算创建了一个分布于多个站点的计算资源池。这可使我们让单独的项目应用使用英特尔的全球计算资源，并提高现有资源的使用率来提供更多的计算容量，同时有效减少硬件添加需求。我们在更新、更强大的高效服务器上创建灵活的计算资源池。在这些资源池内，虚拟化工作负载可以动态分配并在物理服务器之间迁移，而且我们可以根据业务需求，在英特尔核心业务领域合理地划分这些资源池。

### 部署 PaaS 加速应用开发

PaaS 可帮助软件工程师在云环境中构建并托管定制应用。开发人员控制应用和托管配置，同时对底层基础设施进行抽象化处理。平台包含标准软件、中间件、业务 Web 服务、开发工具和自动化，可提供更快的软件制造路径并缩短产品上市时间。

PaaS 环境本身是一个高度灵活和能容纳多用户的按需自助服务环境，而且具备广泛

的辅助功能和资源规划能力。另外，PaaS 可简化创建具备云特征（例如灵活、能容纳多用户以及故障设计等）的应用。软件开发人员使用基于云的环境来创建可在云环境运作的定制应用。

英特尔的 PaaS 部署在企业私有云的 IaaS 之上。PaaS 基于 IaaS 提供的功能而构建，而且能够对这些功能进行扩展。我们关注的是为传统和开源编程语言所用的两种应用堆栈。我们希望在写入到 PaaS 的应用中，能为所有应用层面提供自动化的弹性资源，而且构建的应用和平台较为灵活且不会发生中断。PaaS 对代码进行分区而不是使用专门的服务器虚拟化，可提高计算环境的使用率。我们的最终目标是进一步提高 PaaS 自动化和投资，让业务更为灵活，能将创新理念在一天内转化为实际服务。

### 打造联合云以实现最高的灵活程度和效率

云联盟是尽量增高灵活程度和效率的关键，有助于在企业内不同的 IT 基础设施之间轻松地迁移工作负载和服务——最终实现在私有和公共云环境之间迁移工作负载。为了获得联合云的优势，同时不会造成 IT 工作量过度负重，应用和服务提供商需要针对工作负载、API、工具和数据安全实施相关的标准。增强数据安全以保护数据和知识产权是实现云联盟的关键。英特尔正在通过开放数据中心联盟帮助推动制定必要的企业要求。

我们在使用混合云在进一步扩展以及提高容量方面奠定了基础。我们在多个资源池之间共享容量；在 2012 年，我们计划在数据中心之间共享容量，然后扩展至安全外部云的混合使用模式。

## 打造全面的托管云能力

在我们开始整合云基础之前，需要了解每个主要资源领域相关的数据类型。例如，我们需要了解用户正在使用的容量、需求增长速度，以及性能是否满足他们的期望。

如图 3 所示，对数据进行分类后，我们使用信息技术基础设施库\*（ITIL）标准在云能力堆栈的每个层面当中管理我们的云环境。这些标准提供了我们云环境的整体视图——其中包括物理设备和容器、功能管理、数据集成和分析、工作流自动化以及服务交付。在使用 ITIL 标准之前，我们只能

在孤岛模式下查看数据，这限制了我们对于 IT 资产的了解以及如何作最有效的使用。

### 功能管理层

功能管理层在四个主要方面具有两个主要目的——查看并执行相关操作：配置管理、事件管理、变更管理和容量管理。除了提供跨计算环境的视图外，功能管理层还包括适用于具体设备或容器的措施的列表。例如，相关的措施可能包括在虚拟机中供应新操作系统、更新虚拟机中已经安装的操作系统或安装补丁，或者在虚拟机中更新或安装新应用。

### 数据集成和分析层

数据集成层允许我们集成来自所有容器以及功能管理层的数据。此外，在适当的情况下，它还可以进入工作流自动化和服务交付层。

图 4 显示了我们如何将来自不同功能管理器的容量和性能数据，汇聚到我们的基础设施管理运营数据存储（iMODS）中。如图 4 中顶部的两个框所示，云框架中的其它组件可使用该数据。其目标是对数据进行统一，以便呈现全面的云性能视图。

每个功能管理器都是一个与其它管理器不相关的孤岛——因此数据统一将在提取、转化和加载层带来挑战。

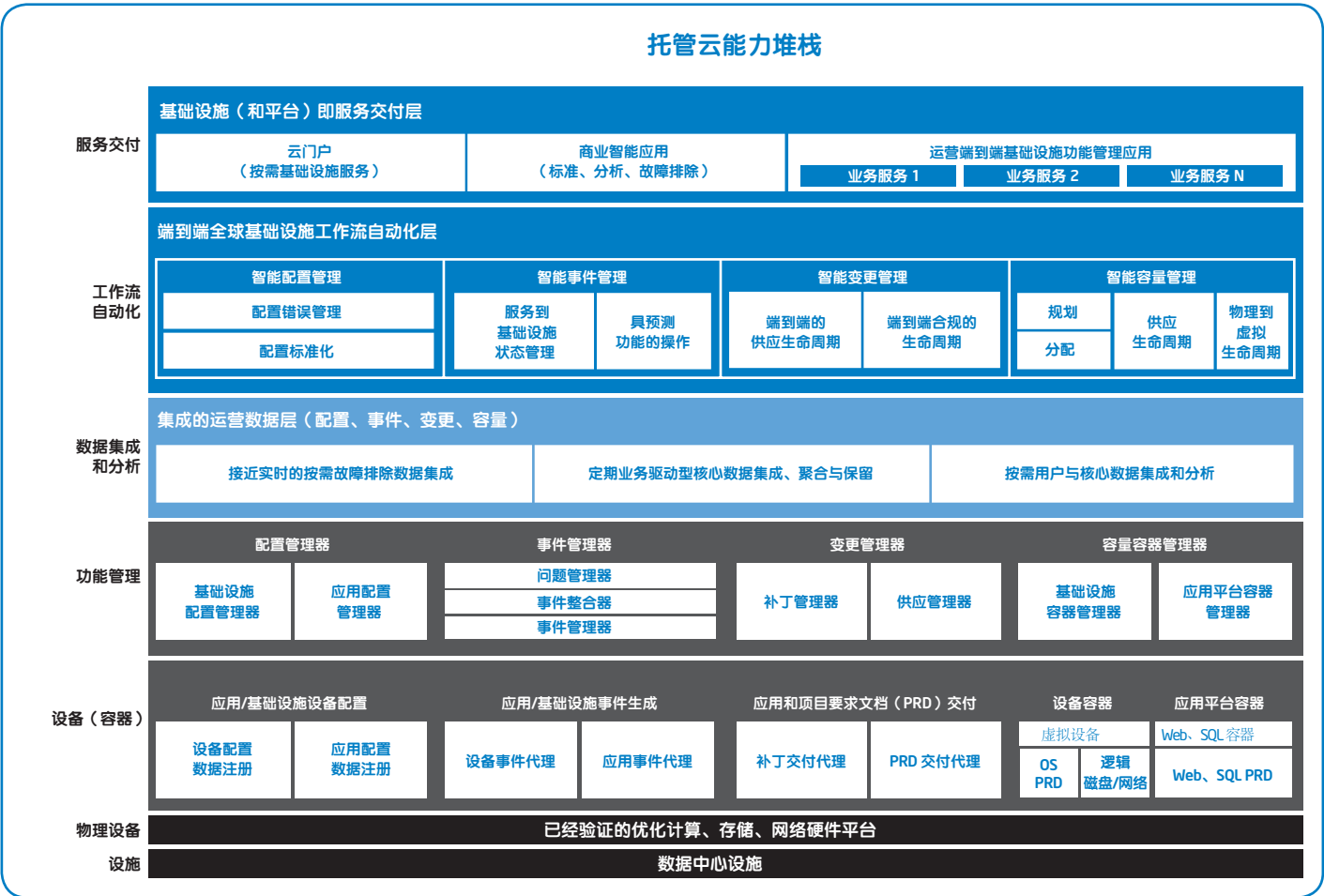


图 3. 信息技术基础设施库\*（ITIL）标准提供了我们的整个云解决方案堆栈的整体视图。

我们解决了某些集成关键数据的挑战，同时开发了集成层。

- 集成容量和性能数据。我们需要集成容量和性能数据集，以便全面了解运营容量。例如，存储区域网络（SAN）上可能还有可用空间，但是 I/O 标准可能会限制使用该空间。
- 唯一的实体标识符（entity identifier）。尽管用户可能会考虑使用“C:”作为服务器上一块硬盘的唯一名称，而存储管理器或虚拟机管理器不使用该标识符。此外，随着时间的推移，一个服务器名称还可以重复用于不同的设备。因此，按服务器名称收集的数据并不一定与同一的设备相关。

- 一致的端到端数据视图。我们必须集成来自不同系统的数据。例如，为了确保“虚拟机 - 文件系统 - 虚拟机磁盘文件 - 虚拟存储容器 - 物理逻辑单元号（LUN）- SAN 机柜”这一链条正常工作，我们需要在链条上协调所有各种性能和容量数据。

工作流自动化层

更稳定和可扩展的按需云计算基础设施需要同样健全的自动化能力，以便与预期的灵活程度和效率级别匹配，进而实现虚拟机的快速供应和取消供应。对于我们的私有云自动化来说，我们设计了一个模块化的可扩展框架，如表 1 所示，将多个云计算领域的整合简化。

表 1. 工作流自动化注意事项

|                                                  |
|--------------------------------------------------|
| 复杂的业务逻辑                                          |
| ▪ 状态管理，包括从非活动状态恢复以应对系统故障的能力                      |
| 轻松的工作流设计和部署                                      |
| ▪ 进度追踪                                           |
| 提供用于系统整合的工具                                      |
| ▪ 回传运行时生成的数据                                     |
| 工作流实例管理                                          |
| ▪ 支持长时间交易                                        |
| 异步编程设计模式，具备处理事件和回调的能力                            |
| ▪ 异构和分散系统之间的大幅度整合，其中包括配置管理数据库、虚拟机管理、网络管理、监控和补丁应用 |

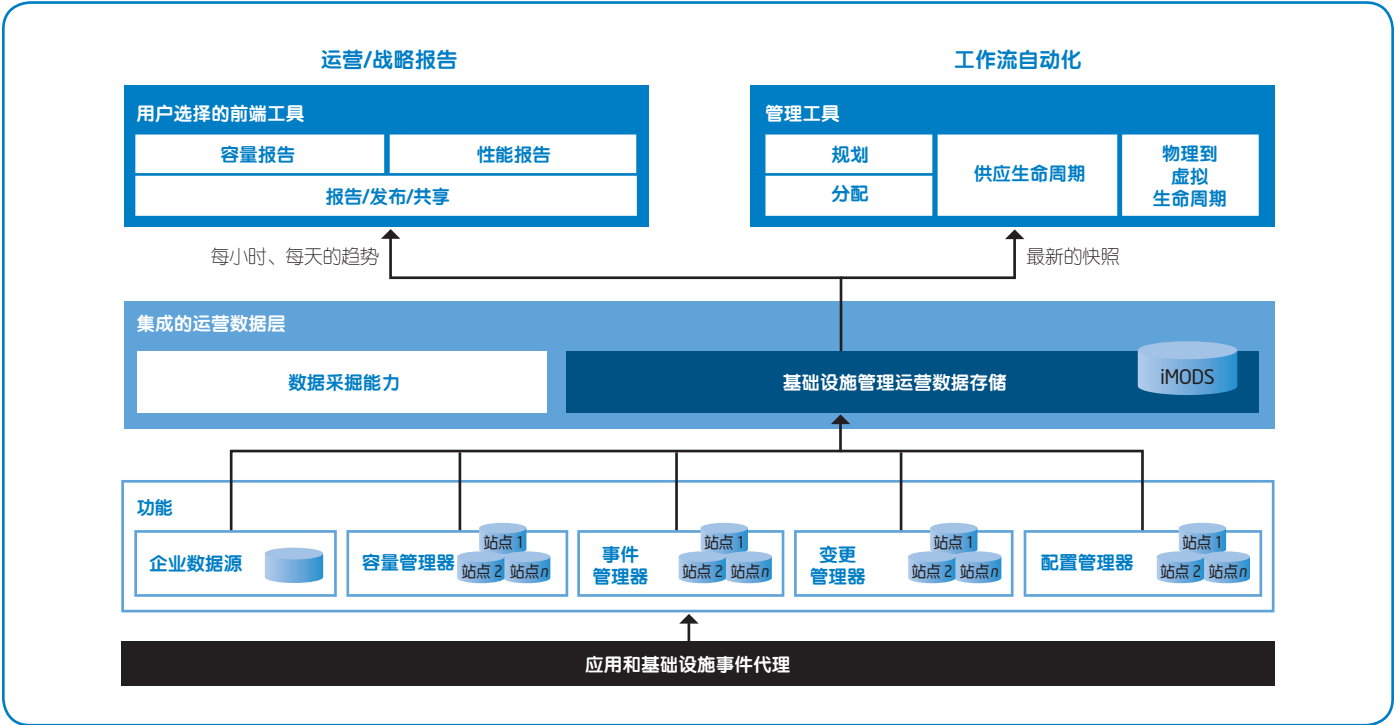


图 4. 基础设施管理运营数据存储（iMODS）可统一来自所有功能管理器的数据，因此可供最终用户和管理工具使用。

随着行业的成熟，自动化框架的模块化性质允许我们使用可满足业务与技术需求的解决方案来取代相关组件。我们在开发工作流自动化框架时，评估了手动流程中的每个步骤，简化现有的流程并将其标准化。我们确定了那些步骤可经标准化后而能稳定地重复操作、果断地取消了不再需要的步骤、探索不同的流程方法，并持续扩大自动化的实施范围。

我们的工作流自动化流程让用户自助获得具备完整功能的虚拟机，并根据规格要求来配置计算、网络和存储资源，包括配置设备身份、访问控制和管理功能，例如补丁、监控和备份——亦即是在托管企业环境中供应虚拟机的所有先决条件。

我们的开发团队在自动化的早期实施阶段中获得了丰富的经验和专业知识，这为部署更全面的自动化框架铺平了道路。新框架将包括发布管理、负载均衡器、防火墙以及更复杂的虚拟机集合等。

## 服务交付层

在我们的私有云基础层的顶部，我们采用服务交付门户解决方案来提供整个解决方案堆栈，该门户依赖于来自下方各层的数据源。服务交付层可以根据各用户的职责来控制他们执行的任务。例如，工程师可以从云门户提出计算、存储和网络资源的申请，而 IT 运营经理则可以使用不同的商业智能工具，根据用户要求的资源来衡量实际的使用情况，并检查有关的故障。

## 实现虚拟化普及

**对于在高度复杂的企业中运行的大量应用工作负载来说，虚拟化是打造云环境的第一步，也是合理及具有重要实际意义的一步。虚拟化为多用户和资源集中奠定了基础，因此支持计算和内存资源的共享，并有助于提升使用率。**

在 2010 年，我们的办公和企业环境中的虚拟化服务器数量增加了三倍，虚拟化比率达到了 42%。在 2011 年，我们的虚拟化比率约为 60%，我们的目标是 75%。正由于有多个技术障碍使我们不能对好几类应用实施虚拟化，为实现此目标，我们针对这些技术障碍开发了相应的解决方案。

## 建立可重复运作的标准化流程

为了加快虚拟化步伐，我们致力于创建可重复使用的标准化流程——模拟工厂生产线，让 IT 运营团队帮助业务团队创造其所需的计算服务，以高效、可预测的方式快速实现大量服务器的虚拟化。我们将其称为“虚拟化工厂”。<sup>1</sup>

英特尔 IT 部门的虚拟化工厂包括 7 个明确定义的步骤，这些步骤涵盖了整个虚拟化流程：

- **识别。**识别可实施虚拟化的服务器，并与服务器和应用负责人联系来确定其是否适用。
- **创造需求。**在业务部门中传达虚拟化的优势并创造需求。

- **调度安排与容量管理。**安排转换时间并保留硬件容量。
- **转换。**执行物理到虚拟的转换。
- **测试与调试。**完成虚拟化后帮助用户执行相关的测试和调试。
- **标准化配置管理。**将所有管理和系统管理功能准确地传输到虚拟服务器。
- **生命周期结束。**从环境中移除物理服务器。

## 系统化地确定和解决技术与业务限制因素

为了实现 75% 的应用虚拟化目标，我们需要消除技术限制，以便能够以安全的方式对关键业务和外部应用实施虚拟化。

在识别步骤中，我们发现由于缺乏技术解决方案，应用无法进行虚拟化。我们将详细情况转达给英特尔 IT 工程团队，并由后者开发相应的解决方案。

在 2010 年，我们解决了技术障碍，并对办公和企业环境中的大多数服务器实施了虚拟化。我们能够支持关键任务特性，例如集群、数据库镜像以及 Web 负载均衡器，内存超过 16 GB 的大型虚拟机，以及供外部使用的应用服务器实施虚拟化。

在 2011 年，我们的重点是攻克更多的技术堡垒，例如应用数据安全、存储复制、备份和恢复限制、内存超过 48 GB 的超大型虚拟机，以及符合 Sarbanes-Oxley 的相关规定。

为了加快虚拟化进程，我们还需要帮助业务部门创造需求，并让他们相信，我们可以在对实际工作环境不会带来负面影响的情况下对应用进行虚拟化。我们开展了广泛的内部推广活动，使业务团队了解我们的计划和私有云的优势。此外，我们还与业务团队建立了紧密的合作关系来加速虚拟化流程。

使用专用的虚拟局域网来隔离应用

为了使虚拟化环境达到与物理环境相似的隔离水平，我们需要在主机上运行的应用之间进行隔离。在每台虚拟化主机上，我们为每个应用提供专用的虚拟局域网

(PVLAN) 来实现应用隔离。<sup>2</sup> 采用这种方式提供的应用网络隔离，与我们在传统的非虚拟化计算环境中提供的保护类似。应用之间的所有通信都要通过防火墙或其它网关，即便共享相同主机的应用也不例外。因此，网络分段有助于防止将影响从一台虚拟机扩展至相同或不同主机上的其它虚拟机。

部署安全的登录区

如图 5 所示，我们在虚拟环境的安全隔离区 (DMZ) 和安全的内部区域 (SIZ) 登录区中部署虚拟化主机。这些区域与我们传统的物理办公和企业环境中的安全区类似。

支持外部应用的虚拟机主机位于 DMZ 中。每个 DMZ 登录区包含一个通过防火墙与互联网隔离的子网，而且它还经由一组单独的防火墙与内部网隔离。

支持安全的内部应用的虚拟机主机位于 SIZ 中。每个 SIZ 登录区包含一个通过一组单独的防火墙与内部网隔离的子网。此外，SIZ 登录区可能还托管其它系统，例如与 DMZ 中的应用进行通信的管理服务器。

这些安全区域可防止已成功的网络攻击在虚拟环境中的扩散。由于采用这个模式，如果要在环境中造成大规模的影响，则必须对多个虚拟机和登录区进行攻击。

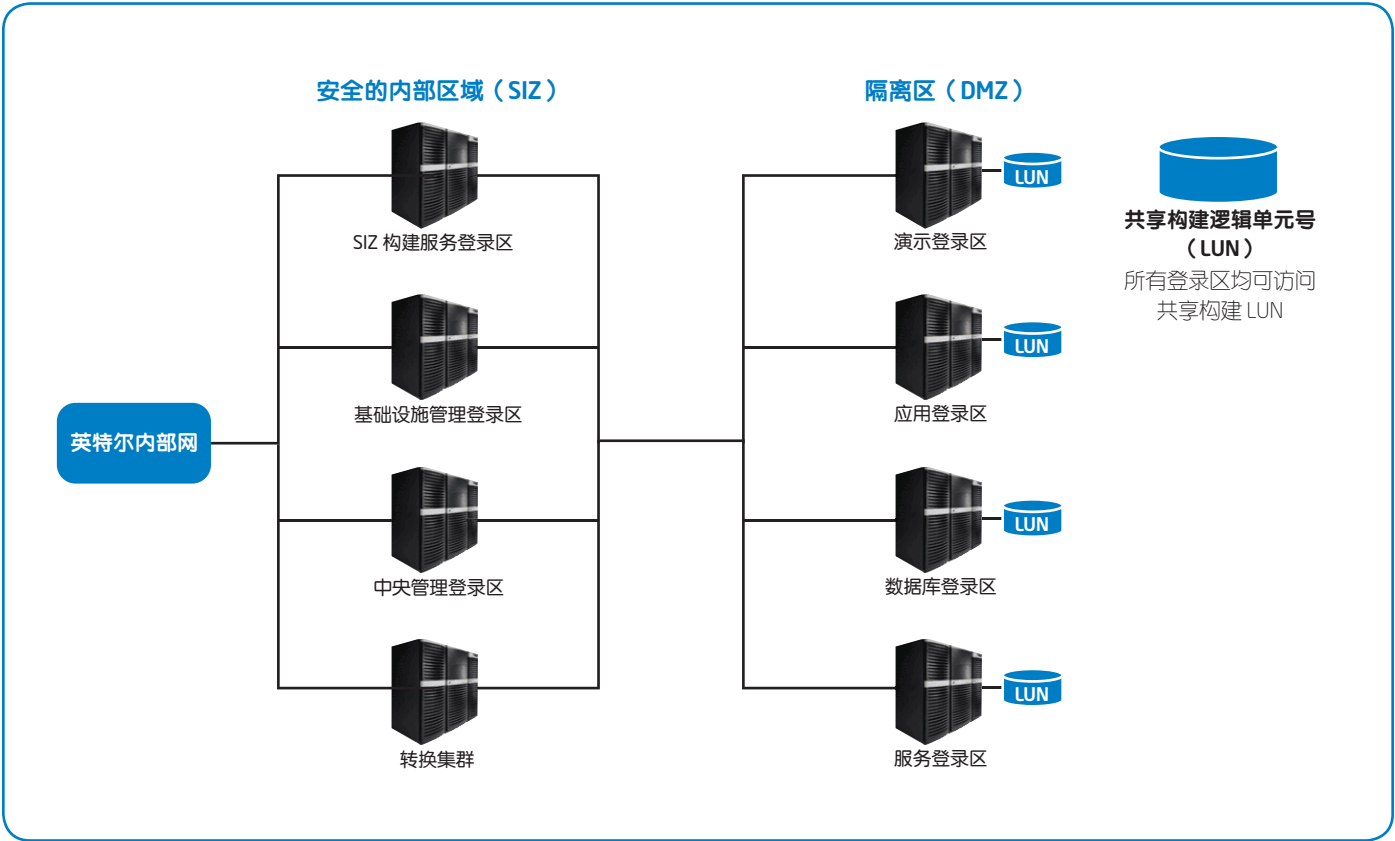


图 5. 隔离区 (DMZ) 和安全内部区域 (SIZ) 可防止已成功的网络攻击在虚拟环境中的扩散。

## 建立端到端状况监控

在英特尔 IT 部门，伴随其它业务领域的快速扩展，我们所需支持的服务的复杂程度与数量也日益提高。由于这种情况，我们希望能更有效地监控服务状况（包括防火墙内外部），而不是以增加员工人数来满足服务需求。我们认为端到端状况监控是企业云环境管理的最关键要素之一。

当出现复杂的组件和应用问题时，端到端状况监控支持快速做出响应，因而可以提高用户满意度并节省成本。能在问题变得复杂或普遍之前就将其解决的话，解决成本也通常较低。此外，端到端状况监控还可让基础设施更为稳定，从而转化为更高的生产力。

我们采用了以下的最佳实践后，告警-工作单比率（alert-to-ticket ratio）改善了 50%，并减少了 IT 运营支持团队每周达 100 个小时的工作时间。随着继续加强我们的工作流自动化和分析能力，我们预计能进一步提高运营效率。

### 自动化虚拟基础设施提供管理功能

使用自动化虚拟基础设施来增强管理，是实现状况监控服务以应对不断变化的业务方向作出动态响应的基础。我们建立了一套自动化框架，能够在服务生命周期中管理下列过程：

- **供应。**我们把新操作系统的快速部署、监控负载以支持安置管理，和集成把多款供应工具的响应全自动化。
- **软件和配置分发。**在此部分，我们打包软件以实现快速部署、管理维修及重新配置响应，并在部署服务组件时，配置管理功能。
- **数据和工作处理。**在此部分，我们把多项相关事务的功能整合，包括从事件到服务的模型中任何关联的影响、检测可触发自动响应的状态变化，并限制对列表中的服务事件作手动响应。
- **第二阶段：**对事件/问题作相应和解决，避免问题发生的智慧功能和自我修复。在该阶段，我们将专注于以下方面：
  - 采取有效、高度自动化的行动来快速恢复服务。
  - 提供持续的服务质量监控，并采取行动以确保较可靠的服务。
  - 对有可能发生的问题和事件进行预测分析。
  - 采取主动和自动化的行动来避免重大影响，并支持有效的修复响应。

### 使用分阶段方法实施监控

实施端到端状况监控是一项复杂的任务，会影响许多 IT 流程。因此，我们采用了分阶段办法，并对每阶段设立明确的目标、里程碑和成功指标。我们从少数几个关键 IT 管理服务开始，例如供外部大众使用的企业应用，而不是从一开始就试图监控所有的服务。

- **第一阶段：**事件降噪和状况监控。在此阶段中，我们侧重于开发一套具备明确角色和职责的事件管理流程、实现工作单创建自动化、开发服务状况模型和事件识别流程，并支持组件级别和服务级别的事件处理。该模型让我们及早检测出应用的问题症状、正确诊断原因，并在故障不可收拾之前把应用修复。

### 包括所有关键要素

随着我们继续为私有云建立端到端状况监控系统，必须考虑以下各点：

- **IT 服务管理。**启用、改善并尽量提供支持英特尔业务的 IT 服务。
- **服务影响管理。**监控和管理关键业务服务的性能和稳定程度，以及密切注意各服务在运作上的关系
- **应用管理。**分析如何从英特尔的企业资源规划（ERP）、客户关系管理（CRM）和其它应用中获得最大的收益。
- **IT 运营、数据库和基础设施管理。**针对成功的业务服务可靠程度监控建立坚实的基础，其中包括可与第三方企业管理技术互操作的开放式解决方案。

## 提供灵活的容量和可衡量的服务

可衡量的服务是云计算的关键属性。为了帮助我们实现有效使用率达 80% 的目标，我们建立了专门的系统以监控和优化资源。此外，我们还实施了流程改进措施，以提高自动化程度并消除对提高效率和灵活程度会有阻碍的手工操作。

在实施私有云之前，我们遇到了几个与容量相关的问题：

- 低资源使用率和失衡的容量限制
- 对资本投资有效使用的问责不足
- 手工操作妨碍了效率和灵活程度的提升
- 在性能问题方面，由于缺乏可供参考的数据和解决办法，因而造成服务中断

容量规划和管理的自动化可提高生产力并缩短上市时间（TTM）以及提高资源使用率、成本效益和系统的预测。此外，由于与分配、使用和成本有关的数据较为明朗，使用户提出合理的资源要求。我们采用下列定义：

- **容量规划。**在合适的时间以合适的数量及合适的价格提供 IT 基础设施，并确定如何最有效地使用它。
- **容量管理。**针对与服务和资源相关的容量和性能问题，提供一个关注和管理的点。

如图 6 所示，我们的容量管理模型是环形的，从预测、规划和预算开始。然后，我们基于这些步骤的结果来采购资源。我们还对预测人员提供反馈，这种协调步骤可以帮助他们从我们的工作中得到数据资料，并在未来作更准确的预测。

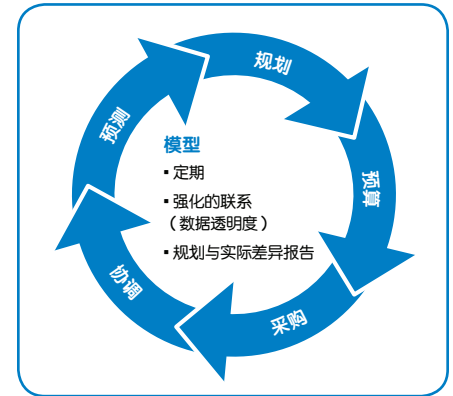


图 6. 我们用于提供灵活的容量和可测量的服务的模型包括向预测人员提供数据，以便他们在未来能作更佳决策。

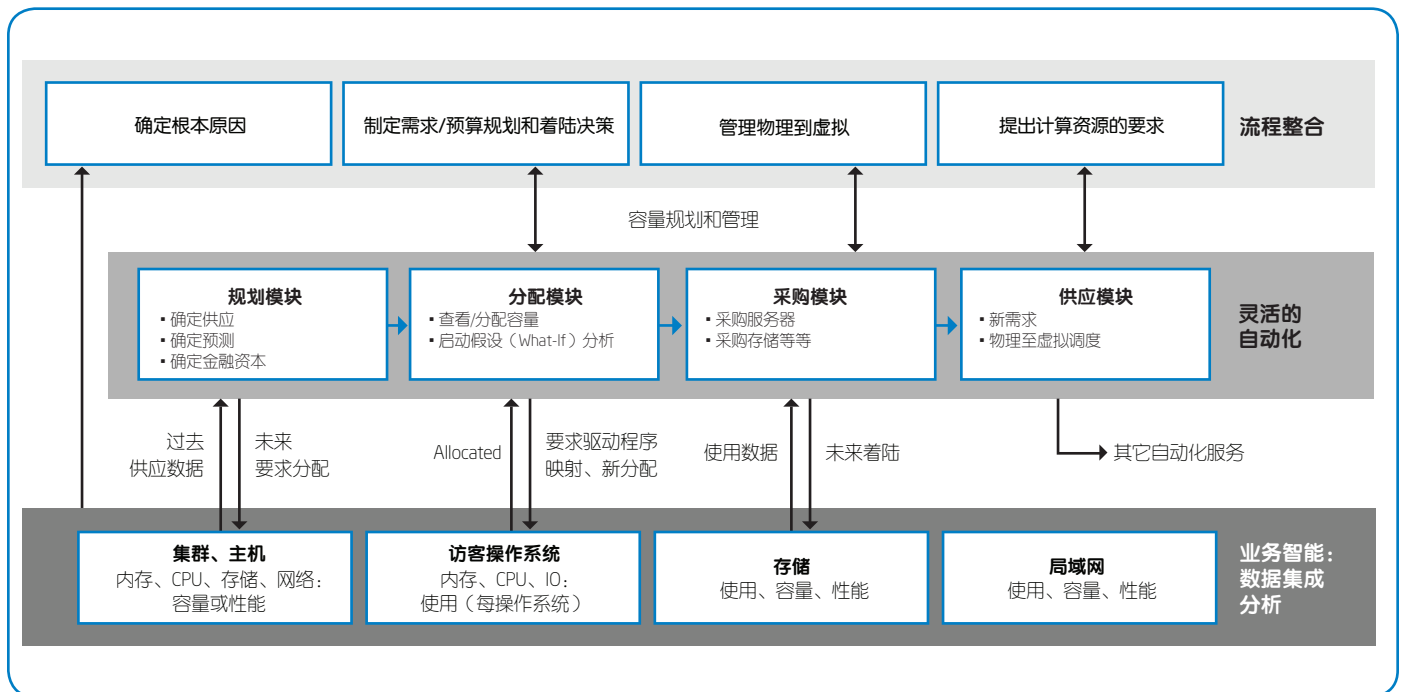


图 7. 我们的容量管理基础设施使用业务智能、工作流自动化和整合流程。

我们也定义了两类使用案例：

- “临时的”需求，即没有作预测，而用户要求使用少量按需容量。
- 预测到需求，让用户能使用更大的容量以满足更大规模的需求。

## 建立容量管理基础设施

图 7 描述了我们的容量管理基础设施，包括三个主要的层：

- 提供数据集成分析的业务智能应用基础。
- 自动化工作流层，执行规划、分配、采购和供应任务。
- 一套流程整合，可确定容量问题、帮助决策并根据需求信号申请计算资源。

## 定义容量规划的关键性能指标

我们使用以下关键性能指标（KPI）来评估容量规划流程运作情况以及可以改进的部分：

- 不在预算之内的采购—容量规划偏差的数量以及无规划容量的总支出。
- 容量事件的数量。
- 由各阶段之间的变化来衡量，改善规划及实际中的偏差。
- 在运作中有多少时间我们无法横向扩展以满足需求（因为太小的缓冲区）。

## 使用现有的供应链专业知识以支持云容量方法

供应链管理的许多概念与我们的私有云环境相关联：

- 了解库存缓冲并尽量降低其水平，在没有浪费的情况下满足实际需求。
- 了解所有与成功扩展相关的供应资源。我们分析存储、网络 IP 范围、计算、内存以及监测环境容量，以确定何时能接近最大使用、多久可对它们完成补充、哪些是关键供应路径的组成部分以及哪些需要双源备份等等。
- 了解需求，例如确定其在性质上是否呈周期循环或是纯粹的线性增长。对于优化供需比例来说，识别下降的趋势和原因也非常重要。

随着我们开发容量管理流程和基础设施，我们亦获得进一步的供应链管理智识。

---

## 支持按需自助服务

**按需自助服务是云计划成功的一个关键性标准；但是，如果缺少基础业务逻辑、控制和透明度，不受限制的按需企业私有云便会过量分配容量，因而快速超过其容量限制。**

我们将之前从自动化工作获得的经验和能力应用在设计计算环境中，开发了一个按

需自助服务门户，这代表了数据中心灵活度的巨大飞跃。我们制定一个包括授权、配额、透明的可衡量服务和数据驱动型业务逻辑在内的托管自动化框架，创建一个真正的企业私有云，提供一个以用户为主导，能提高业务灵活程度与速度的自助服务门户。目前，办公室和企业环境中 80% 的应用就是采用我们的自助服务门户提出新服务器供应的请求。

我们采取按需自助服务供应，将新基础设施服务的部署时间从 90 天减到不足 3 小时。许多申请在 45 分钟内就能得到供应。我们将继续在整个企业中加强并扩展该解决方案，力争在短短几分钟内完成供应。这是帮助我们迈向最终目标的第一步。我们的目标是每当英特尔的工程师有创新想法展开工作时，可以让他们在一天内获得适合的计算基础设施。

## 现有企业的自动化和业务流程转换

要达到目标使 80% 的企业计算环境在 3 小时内获得虚拟机供应，便需要业务流程高度的自动化，当用户自助获取 IT 服务供应时不会增加 IT 运营负担，或影响共享基础设施上的其它用户环境。

业务流程转换是实现按需自助服务优势的最大障碍，太多手动控制阻碍了变更以及灵活程度的提升。控制点和重复检查的数量以及团队之间的工作交接使这一流程极

为繁琐，而且无法跟上业务需求的变化。我们记录业务流程、汲取宝贵的经验教训并重复最佳实践，能够从现有流程迁移到全新的自助服务模式。

我们自助服务功能的核心是可接收服务请求和作响应的 web 服务、跟踪这些服务的状态和进度的数据块、满足请求的调度程序，以及具备完成这些任务所需的工作流的协调引擎。

### 不断尝试加速或扩展云产品

工作流自动化是云计算的一个极其重要的组成部分，也是一个快速发展的专业领域。因此，我们需要了解最新的产品和技术信息。

云环境正快速发展成熟，与我们在网格计算中使用多年的功能日趋接近。我们希望到本文出版时，会有更多的新创出现，与及现有解决方案会有显著的改进，让云的自动化变得更可行和更可用。

### 使用分阶段方法，反复扩展功能

分阶段项目实施可帮助我们构建最佳的解决方案，然后将这些解决方案扩展到一个新水平。表 2 展示了自助服务供应的发展蓝图。

我们的战略是分阶段推进自动化，对相关的功能和新架构先进行验证，然后再在业务中推广。在第一阶段，我们仅推出了

在虚拟开发环境的自助服务，何 IT 运营用的可衡量服务。供运营用的自动化允许 IT 部门供应虚拟机，同时在进行广泛扩展之前，先对业务流程和产品的成熟度进行验证。在第二阶段，我们将自助服务扩展到实际工作环境用的虚拟服务器，并为用户提供服务数据作衡量参考。目前，我们 80% 的虚拟机请求都是由用户使用门户来提出申请。

### 成效

随着英特尔扩展为消费者和企业提供的新服务以创造收入来源，并帮助推动英特尔® 处理器的市场需求，英特尔 IT 部门采用提供增值解决方案以及可扩展的按需托管容量来支持这一战略。

此外：

- 我们的云包括 40% 的企业实际工作负载 — 不只是开发环境。
- 我们支持在工程设计、人力资源、企业资源规划（ERP）、财务等方面的实际业务应用。
- 我们已经在支持供面企业外的用户使用的关键任务应用。
- 目前我们的办公室和企业环境超过 60% 都已实现虚拟化 — 与 2010 年相比增加了 3 倍。

- 大约 80% 的云服务请求都来自自助服务门户而不是手动服务。

### 后续工作

目前，我们正将云价值扩展到英特尔的更多部门，并正进一步加快交付新服务。为了快速扩展容量，以支持英特尔的服务能满足不可预测的需求高峰，我们针对基于 Web 的应用添加了快速、灵活的扩展能力。

我们已奠定了基础，准备好使用混合云以进一步提高这种扩展能力性并提供突发容量。今年，我们已在多个资源池间共享容量；在 2012 年，我们计划在数据中心间共享容量，然后扩展到安全的外部云作混合使用。

此外，我们打算完成中期目标，包括：

- **防故障设计。**当端到端服务中的特定组件出现故障时，自动化修复可解决 95% 的问题。此外，节点和组件将可自动化部署与管理，不会因 IT 基础设施停机造成任何业务影响。
- **扩展我们的云产品。**我们可将“基础设施即服务”（IaaS）学到的经验运用到提供“软件即服务”（SaaS），从而获得更大的成本和效率优势。

表 2. 英特尔按需自助服务供应开发

| 2009                                                                                   | 2010                                                                                         | 2011                                                                                                                                      | 2012                                                                                                                  |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>▪ 英特尔设计电网自动化</li><li>▪ 为开发用户所用的自助服务自动化</li></ul> | <ul style="list-style-type: none"><li>▪ 为内部企业员工用户所用的自助服务自动化</li><li>▪ 内部环境的管理功能自动化</li></ul> | <ul style="list-style-type: none"><li>▪ 为管理员所用的控制区（DMZ）环境自动化</li><li>▪ 虚拟机收集、快速扩展（弹性和灵活程度）</li><li>▪ 为有限的非 IT 用户所用 DMZ 的自助服务自动化</li></ul> | <ul style="list-style-type: none"><li>▪ 端到端云服务监控</li><li>▪ 为各种业务需求所用的 DMZ 自助服务自动化</li><li>▪ 平台即服务（PaaS）自助服务</li></ul> |

- **增强自助服务门户**以便包括控制面板功能。将来，我们的用户提出单个请求便能定义和管理多层应用和服务基础设施。此外，我们希望扩展现有的门户功能，以便支持供应、监控、配置、修补与备份。同时，将会提供在用户 SLA 中的供应和管理服务数据。
- **扩展自动化。**自动化和业务逻辑将基于业务需求、信息安全类别、工作负载特性与可用的容量来决定什么类型的服务是恰当的。服务地点的选择也将自动化—公共云、私有云或混合云。随着应用生命周期中需求的不变化，工作负载将被动态地迁移到更高性能的基础设施中然后返回。如果有需要，所有组件和节点也将可以即刻动态地添加或删除。用户将可以了解关键服务等级目标，例如稳定靠程度、性能和配置规则。
- **使用内部托管和互联网托管监控解决方案的组合。**按着 PoC 的成果，我们打算把所有服务区域集成的端到端状况监控功能作整合，目标是不论服务托管在哪里，都要能处理自动修复。

## 结束语

**虽然我们的私有云工作还未完成，但已经取得了显著的成绩，特别在自助服务供应提供计算基础设施方面：**

- 办公室、企业和服务约 60% 的计算环境实现虚拟化，目标为 75%。
- 服务器供应时间从 90 天减少到 3 小时。目标是进一步减少到几分钟内。
- 办公室和企业环境中 80% 的服务器供应请求由自助服务按需处理。

这些结果支持我们向业务目标迈进—实现 IT 资产 80% 的有效使用率、持续的业务速度提升，以及消除 IT 基础设施停机带来的业务影响。

踏入 2012 年后，我们的工作重点要转移到采用云计算来提供数据和应用平台服务上。在过去两年中，我们已经确定了在几项领域中的最佳做法来帮助我们尽量获得云计算带来的商业优势。我们将继续应用这些最佳实践来完成开发我们的企业私有云，为有权限的用户提供一个稳定和具有高度数据安全服务的计算环境，并可按需提供数据，同时也可从共享、灵活、多用户的基础设施中提供设备。此外，这些最佳实践也可帮助我们的战略目标，就是健全的混合云。

## 缩写词

|       |                |
|-------|----------------|
| CRM   | 客户关系管理         |
| DMZ   | 隔离区            |
| DOMES | 设计、办公、制造、企业和服务 |
| ERP   | 企业资源规划         |
| IaaS  | 基础设施即服务        |
| iMODS | 基础设施管理操作数据存储   |
| ITIL  | 信息技术基础设施库*     |
| KPI   | 关键性能指标         |
| LUN   | 逻辑单元号          |
| NPV   | 净现值            |
| PaaS  | 平台即服务          |
| PoC   | 概念验证           |
| PRD   | 项目要求文档         |
| PVLAN | 专用虚拟 LAN       |
| SaaS  | 软件即服务          |
| SAN   | 存储域网络          |
| SIZ   | 安全内部区          |
| SLA   | 服务级别协议         |
| TTM   | 上市时间           |
| VM    | 虚拟机            |

**如欲了解更多有关英特尔 IT 部门的最佳实践，请访问：[www.intel.com/cn/it](http://www.intel.com/cn/it)**

<sup>1</sup> 欲了解更多信息，请参阅“采用工厂运作原则，加速企业计算虚拟化”。英特尔公司，2011 年 2 月。

<sup>2</sup> 欲了解更多信息，请参阅“应对信息安全的挑战，实现虚拟化普及”，英特尔公司，2011 年 11 月。

<sup>3</sup> 欲了解更多信息，请参阅“在英特尔 IT 私有云内实施按需服务”。英特尔公司，2010 年 10 月

本白皮书仅用于参考目的。本文以概不保证方式提供，英特尔不做任何形式的保证，包括对适销性、不侵权性，以及适用于特定用途的担保，或任何由建议、规范或范例所产生的任何其它担保。英特尔不承担因使用

本规范相关信息所产生的任何责任，包括对侵犯任何专利、版权或其它知识产权的责任。本文不代表英特尔公司或其它机构向任何人明确或隐含地授予任何知识产权。

英特尔、英特尔标识、Xeon 和至强是英特尔公司在美国和其它国家（地区）的商标。

\* 文中涉及的其他名称及商标属于各自所有者资产。

版权所有 © 2010 英特尔公司。保留所有权利。

♻️ 请注意环保 1211/ABC/KC/PDF 326182-001 CN

