CHAPTER

OVERVIEW 1

Application management provides tremendous benefits by improving the productivity of application users and lines of business.
Wayne Morris, VP, Corporate Marketing, BMC Software, Inc.

Application management has become one of the critical challenges for all large IT organizations today since it is where IT groups often have the most visibility with their business clients.
Theo Forbath, Global VP, Digital Transformation at Cognizant Technology Solutions

INTRODUCTION

In many organizations, applications that were developed 20 or 30 years ago are still in use, and the most recently developed applications can be expected to have a similar longevity. To ensure high performance and productivity, these applications and their related data structures must be systematically monitored, enhanced, renewed, and retired. The question is, "How do we best manage applications in the complex world of mobile and cloud computing?"

In the following pages, we provide the answer to this question through an enlightening discussion focused on the various aspects of application management and its evolving role in mobile and cloud systems. To achieve this, we take a brief look at application management in traditional standalone systems as a necessary starting point, followed by a systematic discussion of the ways in which application management processes, techniques, tools, and standards have changed to successfully manage today's complex application environment. In those chapters where it is appropriate, a list of vendors who offer products in the topic space is provided at the end of each chapter.

CHAPTER 2—EVOLUTION OF APPLICATION MANAGEMENT

Application management is closely coupled to the technologies of application software and the associated networks, systems, and databases. As such, application management is always constrained and at the same time driven by those technologies. It is important to understand the development and **evolution of application management** in order to help the reader better understand and give context to modern application management.

Chapter 2 explains the process through which the management of modern applications, though built on innovations of the past, was revolutionized since the beginning of the 21st century. It also discusses how and why the complexity of the management challenge increased tremendously as applications became componentized and virtualized with the introduction of mobile and cloud computing.

Application Performance Management (APM) in the Digital Enterprise. http://dx.doi.org/10.1016/B978-0-12-804018-8.00001-2

CHAPTER 3—MANAGING TRADITIONAL APPLICATIONS

The primary functions of application management are Fault, Configuration, Accounting, Performance, and Security. Key roles for application management are frontline staff (e.g., system administrator, help desk technician, service desk analyst, etc.), applications specialists (e.g., Tier II or Tier III support, etc.), and application developers. The key objectives of application management are to ensure that applications are available to users and deliver an acceptable level of performance, in accordance with a service-level agreement.

Chapter 3 focuses on how traditional applications created 10–20 years ago were managed. We use this as our starting point to embark on the application management journey since it is a simpler environment than is found with more modern applications, and consequently the role of application management was much less complex than it is in today's distributed environment.

CHAPTER 4—MANAGING APPLICATIONS IN THE CLOUD

Cloud computing is a key enabler of the distributed information technology (IT) environment. The use of public and private cloud environments by organizations around the globe continues to grow at a rapid pace and shows no signs of abating in the near future, and the financial benefits of cloud computing will continue to drive its adoption. However, cloud computing brings unique challenges for managing the applications that run in those environments. Chapter 4 discusses the multifaceted nature of **application management in cloud environments**. It also addresses the user and service provider dimensions that exist in each of the public cloud environments, along with the different capabilities and responsibilities in each instance. In addition, it presents a discussion of IaaS and private cloud environments, the responsibilities of the customer's IT department for active management of the applications, and their power to install the appropriate tools as needed.

CHAPTER 5—MANAGING VIRTUALIZED SYSTEMS

A key concept in the distributed environment is **virtualization,** which can be viewed as a logical abstraction of a physical system that allows multiple physical systems to appear as a single logical system, or as a single physical system that is partitioned to appear as multiple independent logical systems. Chapter 5 addresses the various forms of virtualization, including virtualized desktops, virtualized applications, virtual appliances, network virtualization, storage virtualization, and service virtualization. It will also discuss how virtualization is evolving as an innovative concept designed to enable organizations to gain better control over their IT resources, reduce network equipment costs, and reduce power and space requirements. Also addressed are the benefits and challenges of managing virtual machines.

CHAPTER 6—MANAGING MOBILE COMPUTING

Hardware also enabled the distributed environment. Laptop computers, tablets, and smartphones dramatically changed the ways in which people work, interact with each other, and even how they think. It is not just the mobile devices themselves, but those devices together with the applications that run on them and (usually) network connectivity that provide access to additional application functionality and

additional data. Chapter 6 addresses the new set of management challenges that **mobile applications** bring to application management, particularly in the realm of security. Also addressed is how the role of "bring your own device" (BYOD) simultaneously complicated and simplified the challenges of management mobile applications. BYOD made managing mobile applications more complicated because of the diversity of devices on which applications may run and, alternatively, how BYOD simplified the management challenges since most of the responsibility for managing performance and availability of mobile applications shifted to the user of the device.

CHAPTER 7—MANAGING WEB-BASED APPLICATIONS

Internally hosted, cloud-hosted, or software as a service **web-based applications** compose a significant and growing majority of today's business applications and are transforming the ways in which enterprise-class applications are built, deployed, consumed, and managed. There are differing opinions as to whether web applications are easier to develop and require less management than traditional desktop applications. Regardless of the position taken on this debate, most people would agree it is impossible for any organization to prosper without implementing, executing, monitoring, and ultimately retiring dozens of web applications across many different platforms. The challenge is to determine the best way to achieve these goals while expending minimum effort, time, and money to manage them throughout their lifecycle. Chapter 7 discusses the management of web-based applications throughout the system development lifecycle with a particular emphasis on skills, concepts, principles, and challenges related to their development, maintenance, and operations. Finally, protection of corporate and customer data in a web-based environment is discussed, and a set of web application security management principles are recommended.

CHAPTER 8—APPLICATION MANAGEMENT SECURITY

Applications are at the heart of an organization's security. If compromised, they can become an avenue to exploiting or destroying valuable organizational assets. The initial development of an application is where critical decisions must be made. Correct decisions then lead to the creation of much more secure applications and less vulnerability for organizational assets.

Chapter 8 explores the need to secure those applications and how to achieve this objective. Topics covered include the need to secure applications and how to accomplish that, and Chapter 8 describes steps that can be taken to prevent problems from arising or minimize the impact if they do arise. In addition, Chapter 8 identifies 25 of the worst application coding errors that can create vulnerabilities and describes steps that can be taken to prevent problems from arising and/or minimizing their impact. Finally, protection of corporate and customer data in a web-based environment is discussed, and a set of web application security management principles are explained.

CHAPTER 9—DISTRIBUTED, TIERED, AND COMPONENTIZED APPLICATION ARCHITECTURES

The definition of "application" is exceedingly broad, defined differently in many different contexts. Often, the only things "applications" have in common are the fact that they are created from code and designed to perform a discrete task or set of tasks.

For example, in the network management space, file transfer protocol (FTP) is considered to be an "application." In the desktop space, Microsoft Word and Virtual Private Network (VPN) software are considered to be "applications." On a mobile device, an application could be either a tiny native "app" running on the device *or* a traditional web application running on a mobile browser. A mobile "app" and a massive enterprise resource planning (ERP) system consisting of hundreds of modules and thousands of functions are both examples of "applications."

This diversity can be extremely confusing to potential application performance management (APM) buyers. It can be time-consuming to navigate the sea of potential vendors and solutions in search of the one single product that best meets the buyer's needs.

Chapter 9 discusses the management challenges inherent in complex **distributed and componentized application architectures.** Tiered/distributed applications, services built over service-oriented architectures (SOA), hybrid applications executing across on-premise and public cloud, and even complex web applications can be grouped into this category. All traverse multiple infrastructure elements, software components, network segments, platforms, and often data centers/locations during end-to-end execution.

The growth of this level of heterogeneity means that cross-functional skills, instrumentation/insight from multiple vantage points, and collaborative processes and tools are the new normal. For IT organizations already grappling with support costs and expertise shortfalls, the impact can be overwhelming. Automated toolsets are virtually the only way to ensure the quality of complex applications while also mitigating the support costs and workforce effort required to manage massively complex application systems.

CHAPTER 10—DEVOPS AND CONTINUOUS DELIVERY

DevOps and continuous delivery are separate but related IT practices that are neither institutionalized by standards nor uniformly defined and understood. They differ, for example, from IT service management (ITSM) practices, which are now well-defined across the industry and provide a common language and framework, enabling cross-functional IT practitioners to collaborate more effectively.

From the tools perspective, both of these terms are often defined by vendors as "whatever we have that may fit into these 'hot topic' categories." They are likewise defined differently by industry thought leaders and by DevOps and continuous delivery zealots, all of whom cast a somewhat different flavor to their definitions based on their personal experience and that of the companies with which they have worked or consulted.

Chapter 10 explores these two topics separately and together, lending a generic twist to the definitions and descriptions of these concepts. The history and underlying drivers for both DevOps and continuous delivery are discussed, along with how and why they captured center stage in recent years, and the implications for both IT and business stakeholders are described.

CHAPTER 11—MANAGING APPLICATION PROGRAMMING INTERFACES AND CONNECTED SYSTEMS

We live in a world of massively **interconnected applications** and supply chains. In recent years, the use of **application programming interfaces (APIs)** has largely replaced technologies such as electronic data interchange (EDI) and custom-written programs for the development of new system

integrations. APIs are now the de facto industry standard for integrating data and functionality across diverse application ecosystems.

The growth of public cloud, mobile devices, containers, microservices, and Internet of Things (IoT) has accelerated the need for software integration. Industry standards such as representational state transfer (REST), simple object access protocol (SOAP), and hypertext transfer protocol/secure (HTTP/S) facilitated the process.

APIs built over these protocols simplify and, to some degree, standardize the integration process. They reduce the need for the "bespoke" integrations of the past—which were required to support exotic protocols and proprietary operational systems. In short, APIs became the standard currency of exchange connecting applications, devices, and companies.

There are two sides to the API coin: "providing" and "consuming" APIs. Growing numbers of companies are consuming APIs to access data and functionality exposed by other entities. A large number of companies are acting as API providers, exposing their systems to those of customers, partners, and suppliers. Many companies are doing both, and some are monetizing access to data or internal systems as part of revenue generation. Both business-to-business (B2B) and business-to-consumer (B2C) interactions are supported by API connections, and usage grows on a daily basis.

The speed and breadth with which standards-based APIs have proliferated are affecing APM in a big way. Applications relying on APIs to provide data or functions necessary to complete a transaction—an Internet sale, for example—can be slowed or stalled by many of the same factors as tiered, distributed transactions. At the same time, APIs are supported by new protocols, connection methodologies, and architectures that are largely unsupported by many traditional APM solutions.

Chapter 11 points out that while APIs are the new standard of B2B and B2C interchanges, they also introduce new management challenges that many companies are not equipped to address.

CHAPTER 12—APPLICATION PERFORMANCE MANAGEMENT AND USER EXPERIENCE MANAGEMENT

The term **"application performance management" (APM)** is defined differently by virtually every vendor delivering any sort of performance-related toolset. Whether the tool monitors data centers, containers, virtual ecosystems, or networks, APM is the new hot topic, and nearly every enterprise management vendor wants to hop on that bandwagon.

Closely related to APM, **user experience management (UEM)** is a complementary discipline, often with a different set of drivers and always supported by a variety of diverse data collection methodologies. UEM is often viewed as a subset of APM, and the two are particularly valuable when the metrics delivered by each are consolidated, correlated, and analyzed in context with one another.

Although the loose definitions of these terms can be confusing, the reality is that the application performance product family must be versatile enough to accommodate a wide variety of application types and architectures. Since the applications themselves often execute across heterogenous and geographically separated infrastructure elements, the monitoring infrastructure supporting them must be equally diverse and distributed.

It is also true that by its nature, application performance "management" (versus simple "monitoring") requires a level of root-cause analysis functionality. From this perspective, multiple instrumentation points and perspectives supporting insights into application execution all contribute to building an end-to-end perspective.

Chapter 12 explores the various facets of APM and UEM. We also examine the types of products that deliver the multidimensional visibility necessary to manage complex applications, as well as the performance metrics required to support sophisticated modern users. Two models—a "semantic cube" focusing on product capabilities supporting the full spectrum of IT service management and an "application management semantic model" focusing specifically on instrumentation supporting the APM discipline round out the chapter content.

CHAPTER 13—MANAGING CONTAINERIZED APPLICATIONS

Containerized applications represent a major shift in the evolution of IT. Building on the tenets of virtualization, containerization is often referred to as "lightweight virtualization" because of its ability to run applications on a variety of hosts, reduce memory requirements, increase ease of migration and use of applications, enable faster deployment, and back up and free up server capacity.

Chapter 13 explores the history and underlying concepts of containerized applications and container-based virtualization, explores their relationship to virtualization, describes the areas of computing that benefit most from using container-based virtualization, and evaluates how containerized applications can be managed by various categories of IT personnel to provide the greatest value. Finally, we discuss containerization management challenges and the creation of the Open Container Project, a move spearheaded by many of the largest technology organizations to develop a containerization industry standard.

CHAPTER 14—APPLICATION MANAGEMENT IN THE SOFTWARE-DEFINED DATA CENTER

In the past decade, data centers evolved into mission-critical assets whose availability, performance, power, efficiency, security continuity, and overall effectiveness must be guaranteed to avoid critical downtime and revenue losses. The planning, design, implementation, operation and control, maintenance, evolution, and eventual disposal at the end of the data center's useful life consist of a set of complex processes. Managing these processes was difficult, and data center managers had to use a plethora of IT tools and techniques to achieve optimal integration, interoperability, security, reliability, serviceability, manageability, controllability, scalability, security, virtualization, energy efficiency, and overall performance to effectively deploy and operate their data centers. As organizations transitioned to a cloud-based infrastructure, data centers became virtualized. In turn, virtualization led to the emergence of the **software-defined data center (SDDC)** that facilitates the integration of the various infrastructure silos, optimizes resource usage and balances workloads, and maximizes operational efficiency through dynamic workload distribution and network provisioning.

Chapter 14 describes the innovative concept of SDDC and discusses the managerial implications of its potential impact, risks, and benefits. The need for new IT management approaches is examined, new approaches are presented, and ways to implement the new approaches are recommended. Finally, challenges to transitioning to the SDCC are identified and solutions offered.

CHAPTER 15—APPLICATION MANAGEMENT IN THE INTERNET OF THINGS

The **Internet of Things (IoT)** is an explosion in progress that promises to change the lives of nearly every human being. IoT is only possible because of advances in technology that have allowed miniaturization of components and drastic reduction in power requirements.

In Chapter 15, the remote application that resides on or in close proximity to the IoT system that collects data from associated sensors, and the IoT component that receives data that was captured by the remote application, are explained and discussed. The importance of security in the management of IoT is of particular interest since IoT systems are frequently unattended and may not be physically secured.

CHAPTER 16—THE CASE FOR STANDARDS

As industry leaders recognize the importance of developing standardized technologies to instrument IoT-related applications and in response to customer demands for increased efficiency and effectiveness in application manageability, several organizations have stepped up to develop **standards** to guide deployment and management of software and hardware components. These organizations, made up of industry leaders, recognize the importance of developing standardized technologies to instrument applications. They include the Internet Engineering Task Force (IETF), Desktop Management Task Force (DMTF), Institute of Electronic Engineers (IEEE), Tivoli, ASL-BiSL Foundation, and the International Organization of Standards (ISO).

Chapter 16 discusses the various industry and government organization standards and explains the standards developed by these influential organizations vis-à-vis the different aspects of the application management lifecycle. Finally, the pros and cons of using standards to facilitate the management of applications are presented and discussed. The primary utility of this chapter is that it presents a timeline of the development of application management standards and an overview of the many standards that were published over the past 25-plus years in a single, concise resource.

CHAPTER 17—LOOKING AHEAD

As organizations in the future continue to leverage mobile and cloud computing to enable users to connect on a 24/7 basis to applications and data centers through a wide range of devices, the professionals who build and manage them will face an increasing application performance gap.

As a result, in the next several years, considerable changes will occur in how applications are managed. For example, digital transformation will emerge as an important business strategy. Organizations that embrace the next wave of innovative opportunities to digitally transform applications and free themselves of outdated legacy business models will be the big winners in application lifecycle management.

In Chapter 17, digital transformation and other important future developments in application management are presented and discussed, including expected changes in the nature of applications, evolution of software-defined everything, importance of advanced predictive analytics, need for integrated

dynamic policy rules, heightened levels of security, autonomics and cognitive computing, and the increased development and impact of standards.

To address topics that are tangential, yet relevant to application management, we have provided three appendices to explain the configuration management database, service-level management, and the NIST definition report.

APPENDICES

APPENDIX A—SERVICE-LEVEL MANAGEMENT

While **service-level management (SLM)** is not specifically about application, applications are generally central to SLM and the associated service-level agreements (SLAs). Ultimately, SLM is about setting realistic expectations for the clients and holding the service provider (IT) accountable for meeting those expectations—expectations that were mutually agreed on.

Appendix A provides the reader with an overview of the SLM process, its components, and how they integrate with application management.

APPENDIX B—CONFIGURATION MANAGEMENT DATABASE

There are a multitude of views as to what a **configuration management database (CMDB)** really is. Some define the CMDB and the configuration management system (CMS) by the strict IT Infrastructure Library (ITIL) definitions, while others rely on one of the many descriptions put forth by vendors of CMDB-related products. A CMDB is a repository that acts as a data warehouse for IT installations. It holds data relating to a collection of IT assets [commonly referred to as configuration items (CIs)], as well as to descriptive relationships between such assets. When populated, the repository provides a means of understanding.

While a CMDB does contain CIs about servers and devices in the infrastructure, it is not limited to those. A CMDB may also contain information about applications, middleware, documentation, people, processes, service providers, and other relevant information in addition to the basic infrastructure components.

Appendix B examines ITIL processes and associated CMDB-related technologies that are the foundations of the CMDB.

APPENDIX C—NIST DEFINITION REPORT

The NIST definition of cloud computing characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies.

Appendix C present the NIST definition, which is a baseline for discussion from “what is cloud computing” to “how best to use cloud computing.” The service and deployment models defined in the NIST definition forms a single taxonomy designed to better inform system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.

SUMMARY

Application management has become increasingly complex during the past 20 years. The various chapters of this book are packed with valuable information and insights into best practices in application management in the digital enterprise. The overviews provided in this chapter assist the reader in targeting the areas that interest them most.