Part II

Fundamental Technologies and Concepts

A concept is stronger than a fact. – Charlotte Perkins Gilman

Having introduced the field of System Administration in the previous section, we will now focus on a number of important technologies and principles. System Administrators need to approach their job holistically; as discussed, a "system" is comprised of many different interdependent components and the maintenance of the complex whole requires an intricate understanding of each.

In this section, we will look at the (computer) system from the ground up; the chapters have a certain order and the materials in one chapter tend to build upon topics covered in those preceding it. However, as both an instructor or student, you are encouraged to work your way through this book in any order you like. To help you better find the topic that is right for your progress and pace, let us briefly summarize the chapters in this part.

To begin our presentation of fundamental concepts and technologies, we start with an overview of storage models, discuss the benefits, drawbacks, and properties of local storage devices, network storage, and even further abstracted cloud storage models. As if building a new machine, we start out at a fairly low level by understanding the physical disk structure and partitions. Next, we review the traditional UFS in some detail in order to illustrate general file system concepts.

Next, in Chapter 5, we cover software installation concepts. We divide the overall chapter into different sections, focusing on firmware, BIOS and operating system installation, system software, and the concept of the basic operating system (versus a kernel all by itself), and finally third party applications. We present different package management solutions, including binary- and source-based approaches and discuss patch management, softwarr upgrades, and security audits.

Once we understand how software is installed and maintained on our systems, we will spend some time examining how to configure our systems for their different tasks and how to use centralized systems to ensure consistency across multiple and diverse environments. In Chapter 7, we will review the fundamental requirements a configuration management system has to meet, discuss architectural decisions and pay particular attention to their impact on scalability and security. This chapter touches upon a number of interesting aspects including, but not limited to, user management, access control, role definition, local or system-wide customizations, and eventually hints at what

has become known as "Service Orchestration", a concept we will revisit later in Part III in Chapter 12.

Having seen the power of automating system and software deployment and having faced the vast amounts of data collected and processed, we will take a step back and review in detail the basic concepts of automating administrative tasks. In Chapters 8 and 9, we dive into the how, when and why of automation in general. Once again, we will build fundamental knowledge and understanding by reviewing *concepts* rather than explicit code excerpts. We will differentiate between "scripting", "programming" and "software engineering", and focus on the art of writing *simple* tools for use in a System Administrator's daily life. In doing so, we will once again revisit a few topics from earlier in the book and deepen our understanding of (software) documentation and package management.

Following this, we discuss networking in Chapter 10. This chapter can be viewed as being entirely "out of order", as virtually all previous topics in a way require or relate to working with a network. Within the context of System Administration, we being our coverage of this significant topic by traversing the layers of the OSI stack. We include practical and detailed examples of how to analyze network traffic and how packets are transferred from one application to another on the other side of the internet. The discussions will cover both IPv4 and IPv6 equally and include the implications and possible caveats of networking with a dual stack.

The internet architecture and some governing standards bodies will also be covered here. Programs covering these topics in depth in pre-requisites may consider skipping this chapter, even though we believe to approach it from a unique angle, i.e. the System Administrator's point of view.

The last chapter in Part II (Chapter 11) is entitled "System Security". Like the previous chapter, it, too, feels a bit out of order: all previous chapters include specific security related notes and explicitly identify security concerns in any technology discussed, yet this chapter finally takes a step back and discusses security not from an application point of view, but from a general all-encompassing view. That is, we discuss the basic concepts of Risk Assessment and Risk Management, the different threat scenarios one might experience and how to best respond to them. We will cover basics of encryption and how it provides different layers of security via assurance of confidentiality, integrity and authenticity. A second particular focus will be on balancing usability with security as well as the social implications of any instated security policy.

Having built a foundation of core concepts and technologies, we then enter Part III, where we discuss management of complex services by building upon the previous chapters. We will discuss different service architectures (e.g. monolithic vs. microservices), complexity implications and considerations, service orchestration and maintenance in Chapter 12; revisiting certain aspects of different file systems and storage devices, we cover the concepts relating to backups and disaster recovery in Chapter 13. We distinguish between backups for different use cases (prevent temporary data loss, long-term archival of data, file/file system integrity) and help students learn to develop an appropriate disaster recovery plan.

We will analyze the need for large scale system and event logging, which then ties directly into the area of system and network monitoring in Chapter 14. Here we will discuss the Simple Network Monitoring Protocol (SNMP) as well as a few industry standard tools built on this protocol and review how they can be used to measure metrics such as system response time, service availability, uptime, performance and throughput on an enterprise scale.

We will conclude our whirlwind tour across all the diverse areas of System Administration in Part IV, hinting at the fact that we really only have barely scratched the surface in many ways. We will outline major industry trends and developments that we did not have the time or space to include here in Chapter 15, before circling back to the definition of our profession in Chapters 16 and 17, where we elaborate on the legal and ethical obligations and considerations before we take a brief look at what might lie ahead.

As you can tell, each topic is far reaching, and we cannot possibly cover them all in every possible detail. For this reason, we focus not on specific examples but on the basic principles. Instructors should try to choose real-world examples from personal experience to illustrate some of these concepts in class, as we will present some case studies where appropriate. Students, on the other hand, are encouraged to relate the topic to their own experiences and to deepen research based on their interests.