New Book – VMware vCloud Security

Foreword by Harish Chilkoti, Staff Engineer in VMware vShield Networking R&D

What this book covers

Welcome to VMware vCloud Security. In this book, you will learn how to mitigate the security threats on a private cloud running VMware vCloud Director. This book will enable the reader with the knowledge, skills, and abilities to build a highly secured private cloud running VMware vCloud. We will also look at a detailed step-by-step coverage with screenshots, which are usually not available in Cloud Security product manuals.

You will learn how to configure and manage vShield App, which is a hypervisor-based firewall. You will also learn how to use vShield Endpoint, which can help you to strengthen your cloud security by mitigating threats from virus and malware attack.

In the last chapter, you will learn some advanced concepts of cloud assessment for maintaining compliance standards that are available across the world. You will also learn how to run a data security scan and review the violation report that is generated by vShield Data Security and take necessary action to mitigate those risks.

VMware vCloud Security focuses on some critical security risks, such as the application-level firewall and firewall zone, virus and malware attacks on cloud virtual machines, and data security compliance on any VMware vCloud-based private cloud. Security administrators sometimes deploy its components incorrectly, or sometimes cannot see the broader picture and where the vCloud security products fit in. This book is focused on solving those problems using VMware vCloud and the vCloud Networking and Security product suite, which includes vShield App, vShield Endpoint, and vShield Data Security.

You will be introduced to security roles in VMware vCloud Director, integration of LDAP servers with vCloud, and security hardening of vCloud Director. We'll then walk through a hypervisor-based firewall that protects applications from network-based attacks. We'll create access control policies based on logical constructs such as VMware vCenter Server containers and VMware vShield security groups. You'll learn about the architecture of EPSEC and how to implement it. Finally, we will understand how to define data security policies, run scans, and analyze results.

Who this book is for

This book is a valuable addition for technical professionals with Cloud Security administration skills and some amount of VMware vCloud experience, who wish to learn about advanced Cloud Networking and Security products and where they fit and how to configure them as well to mitigate risks in the VMware vCloud based private cloud.

What you will learn from this book

- Install and configure VMware vCloud Director n Understand security hardening of vCloud Director in a nutshell
- Monitor vShield Endpoint health status
- Create a data security policy
- Review the violation reports that are generated by a vShield Data Security scan
- Learn the purpose and operation of vShield Data Security
- Generate a data security policy
- Initiate a data scan
- Handle vShield App Firewall Management n Supervise vShield App Flow

A special thanks to Michael Haines for reviewing it and provide me such a great feedback. Also I want to thank Harish Chilkoti for his tremendous support during the project and Preetam Zare (@techstarts) for his support during the review process.