Cisco Cloud Infrastructure

AVINASH SHUKLA, CCIE® NO. 28418
JALPA PATEL, CCIE® NO. 42465
KOMAL PANZADE
HIMANSHU SARDANA

ciscopress.com

FREE SAMPLE CHAPTER

Cisco Cloud Infrastructure: Application, Security, and Data Center Architecture

Avinash Shukla, CCIE No. 28418
Jalpa Patel, CCIE No. 42465
Komal Panzade
Himanshu Sardana

Cisco Press

Cisco Cloud Infrastructure: Application, Security, and Data Center Architecture

Avinash Shukla, Jalpa Patel, Komal Panzade, Himanshu Sardana

Published by:
Cisco Press

ScoutAutomatedPrintCode

Library of Congress Cataloging-in-Publication Number: 2022920878

ISBN-13: 978-0-13-769012-1
ISBN-10: 0-13-769012-6

Warning and Disclaimer

This book is designed to provide information about Cisco Cloud Infrastructure for various Cisco Products, existing Cisco technologies in the "Data Center, Security, and Applications" domain which are available in the On-Prem environment and how the technology has evolved to fit in a Hybrid Cloud model, which facilitates the management and operation of On-Prem deployments and provides integration with Public Cloud. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

Special Sales

Feedback Information

Editor-in-Chief: Mark Taub

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Project Editor: Mandie Frank

Copy Editor: Bart Reed

Technical Editors: Manuel Velasco, Atul Khanna

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Erika Millen

Proofreader: Donna E. Mulder

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Credits

Chapter 2, 3, 6, Logo of Google Cloud: Google

Chapter 2, 3, 8, Logo of Azure: Microsoft Corporation

Chapter 2, 3, 8, Logo of AWS: Amazon, Inc

Chapter 2, Logo of Alibaba: Alibaba

Chapter 3, Logo of VMware: VMware, Inc

Chapter 3, Logo of Windows Hyper V: Microsoft Corporation

Chapter 3, Logo of Red Hat: Red Hat, Inc

Chapter 3, Logo of F5: F5, Inc

Chapter 3, Logo of Citrix Systems: Citrix Systems, Inc

Chapter 3, Logo of Dell: Dell, Inc

Chapter 3, Logo of Brocade: Broadcom

Chapter 3, Logo of IBM: IBM

Chapter 3, Logo of Netapp: NetApp

Chapter 3, Logo of Pure Storage: Pure Storage, Inc

Chapter 3, Logo of Hitachi: Hitachi, Ltd

Chapter 6, Logo of OneDrive: Microsoft Corporation

Chapter 6, Logo of SharePoint: Microsoft Corporation

Chapter 6, Logo of Box: Box

Chapter 6, Logo of DropBox: DropBox

About the Authors

Avinash Shukla (CCIE No. 28418), Senior Leader in Cisco's US Customer Experience (CX) Organization, has 14 years of experience in Cisco CX roles spanning Professional and Technical Services, and extensive expertise in collaboration and data center technologies. He now leads a team of engineers working on Cisco Data Center Technology (Cisco Unified Computing Systems, Hyperconverged Infrastructure, Virtualization, and data center automation). He holds a B.Tech in ECE from IIIT, Hyderabad and has won numerous Cisco awards for customer focus, and has delivered many technical trainings for Cisco partners and customers.

Jalpa Patel (CCIE No. 42465) is a multidisciplinary technologist and a passionate leader with a strong track record of successful engineering executions and game-changing business achievements defining, building, and growing new products. Her domain knowledge of Data Center hardware infrastructure is focused on Compute, Networking, Storage, and Accelerators. Patel holds an MS degree in Telecommunication Networks from NYU, a BS degree from Government Engineering College, Gujarat, India, and an Advanced Program Management Certificate from Stanford.

Komal Panzade is a Senior Technical Consulting Engineer in Cisco's Customer Experience (CX) organization and has 6 years of experience working on different Data Center Technologies like Compute, Storage, and Virtualization. She currently works in the Hyperconverged Infrastructure (HCI) domain focusing on Distributed Systems and Automation. She is a Certified Kubernetes Administrator and helps Cisco customers with efficient management of their infrastructure using Cisco's SaaS platform called Intersight. Komal holds a Bachelor of Technology degree in Information Technology from Amity University, Noida, India.

Himanshu Sardana (CCNP, VCP, CKA), is a Senior Technical Consulting Engineer in Cisco's Customer Experience (CX) Org. He started his professional journey with Cisco and now has 6 years of experience in Data Center Compute and Storage space. His current area of focus is on Cisco's Hyperconverged business (Hyperflex) and Intersight, helping with high escalations and creating tools like Hypercheck to make customer interactions with Cisco Products better. He holds a BS degree in Computer Science from Chitkara University, Punjab, India.

About the Technical Reviewers

Manuel Velasco (CCIE No. 49401) is a Customer Success Specialist, in the Customer Experience group at Cisco Systems. In his previous role, he worked as TAC engineer at Cisco supporting multiple data center technologies, including Cisco Unified Computing System and Virtualization, Cisco Application Centric Infrastructure (ACI), and Cisco Hyperflex. He has over 11 years of experience in the data center technologies. Manuel holds a B.S. degree in Computer Engineering from CalPoly San Luis Obispo.

Atul Khanna (CCIE No. 35540) is working as Personalized Support Manager in Twilio Inc. Before joining Twilio, he was Data Center Networking Manager with Cisco Customer Experience Center Americas. He has extensive experience in directing and leading strategies to provide optimal technical services to Cisco Customers, with more than 12 years of experience at Cisco in enterprise support, network operations, manage/cloud services, data center networking, compute, and virtualization. Atul was a senior technical consulting engineer supporting Hyperflex solutions in Richardson, Texas; he facilitated Advanced Services (AS) team members for successful new customer deployments and upgrades; and he cultivated relationships with Cisco Partners and customers to meet organizational demands. He also presented a technical webinar for cloud services platform 2100. He attended Cisco Live in 2015 and 2018, interacting with Cisco customers and partners at the TAC booth. Atul lives with his wife and son in Frisco, Texas.

Dedications

Avinash Shukla: I would like to dedicate this book to my lil' baby girl Avira who was born during the time of writing the book, my son Aryav, my nieces Riddhi and Siddhi, my lovely wife Neelima, my sister Anubha, and my parents Kanak and Anil, for their unconditional love and support. Without their support, none of this would have been possible. I would also like to dedicate this book to one of my earliest inspirations while growing up, my beloved Bade Papa, Aravind Kumar Shukla (RIP). Lastly, I would like to thank everyone in my big extended family for their motivation and encouragement. All of you have inspired me in many ways and helped me in my professional endeavors.

Jalpa Patel: I would like to dedicate this book to my parents, Minaxi and Babubhai Patel, for their blessings and faith in me; and to Jigisha, Falguni, and Harish, for their guidance and encouragement. I also would like to dedicate this book to my brother, Hardik, and his wife, Dharmistha, who have been a great support to me throughout the complete process of writing of this book. Finally, thank you to Raj and Samaira for their love and inspiration.

Acknowledgments

We would like to thank and acknowledge several people who have helped us directly or indirectly with the necessary skills that enabled us to write this book.

This book couldn't have been possible without the support of many people in the CiscoPress team. A thank you goes to James Manly, Eleanor Bru, and everybody else at CiscoPress for believing in us and supporting us throughout this journey.

Also, much research for this book was done by sifting through heaps of design guides, specifications, and videos so many thanks to all of the technology professionals.

Finally, we would like to thank our technical reviewers Manuel Velasco, Vibhor Amrodia, and Atul Khanna, for their patience, commitment, and support in the adventure of writing this book.

Contents at a Glance

Introduction xxiii

Part 1 Cisco Data Center Networking and Infrastructure

Chapter 1 Cisco Data Center Orchestration 1

Chapter 2 Cisco Data Center Analytics and Insights 41

Chapter 3 Cisco Data Center Solutions for Hybrid Cloud 81

Part 2 Cisco Applications and Workload Management

Chapter 4 Application, Analytics, and Workload Performance Management with AppDynamics 129

Chapter 5 Management 201

Chapter 6 Cisco Cloud Webex Applications 239

Chapter 7 Internet of Things (IoT) 287

Part 3 Cisco Cloud Security

Chapter 8 Cisco Cloud Security 313

Index 361

Reader Services

Register your copy at www.ciscopress.com/title/ISBN for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780137690121 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Contents

Introduction xxiii

Part 1 Cisco Data Center Networking and Infrastructure

Chapter 1 Cisco Data Center Orchestration 1

IT Challenges and Data Center Solutions 2

Cisco Nexus Dashboard 4

Features and Benefits 6

Hardware vs. Software Stack 11

Cisco Data Center Networking (DCN) Licensing 11

Available Form Factors 12

Cisco Nexus Dashboard Orchestrator 14

Common Use Cases 15

Large-Scale Data Center Deployment 15

Data Center Interconnectivity 16

Cisco NDO Multidomain Integrations 16

Hybrid Cloud and Multicloud 18

Service Provider/5G Telco 18

Functions Provided by the Nexus Dashboard Orchestrator 19

Deployment of Cisco Nexus Dashboard Orchestrator 21

Add ACI/DCNM Sites 22

Manage Sites Using Cisco Nexus Dashboard Orchestrator 24

Cisco Nexus Dashboard Fabric Controller 25

Cisco NDFC Benefits and Features 27

Benefits 27

Features 28

Platform Support Information 34

Server Requirements 34

Third-party Applications and Cloud-based Services 34

Cisco Nexus Dashboard Open Ecosystem with Splunk 36

Cisco Nexus Dashboard Open Ecosystem with ServiceNow 37

Summary 39

References/Additional Reading 40

Chapter 2 Cisco Data Center Analytics and Insights 41

Cisco Nexus Dashboard Insights 41

Cisco Nexus Dashboard Insights Licensing 45

Key Components of Cisco Nexus Dashboard Insights 46

Browsing Cisco Nexus Dashboard Insights 50
Resources 50
Environmental 52
Statistics 53
Flows 54
Endpoints 56
Applications 56
Event Analytics 57
Diagnostics, Impact, Recommendation 58
Advisories 60
Firmware Update Analysis 60
Pre-Change Analysis 62
Cisco Nexus Dashboard Insights Features and Benefits 63
Cisco Nexus Insights Cloud Connector 66
Cisco Nexus Dashboard Data Broker 68
Automated SPAN Configuration in Production Network 70
Cisco Application Centric Infrastructure (ACI) Integration 71
Cisco DNA Center Integration 72
Scalable Traffic Monitoring with Cisco Nexus Dashboard Data Broker Inline Option 72
Cisco Nexus Dashboard Data Broker Access Mechanisms 73
Cisco Meraki MX 74
Meraki Virtual MX Appliances for Public and Private Clouds 77
Features and Functionality of the vMX Appliance 77
vMX Setup for Microsoft Azure 78
vMX Setup for Google Cloud Platform 78
vMX Setup for Alibaba Cloud 79
Summary 79
References/Additional Reading 79

Chapter 3 Cisco Data Center Solutions for Hybrid Cloud 81
Cisco Cloud Application Centric Infrastructure (Cisco Cloud ACI) 82
Challenges in Hybrid Cloud Environments 82
High-Level Architecture of Cisco Cloud ACI on AWS 85
Cisco ACI Nexus Dashboard Orchestrator 86
Cisco Cloud APIC on AWS 86
Cisco Cloud APIC's First Time Setup Wizard 88
Registering a Cisco ACI Cloud Site in NDO 89

Deploying a Multitier Application in a Hybrid Scenario 89
Cisco UCS Director 92
Infrastructure Configuration and Management 94
Cisco UCS Management Through Cisco UCS Director 95
Cisco UCS Management Tasks You Can Perform in Cisco UCS Director 95
Configuration and Administration 95
Monitoring and Reporting 95
Orchestration and Automation 97
Infrastructure as a Service 97
Secure Multitenancy 102
Rapid Application Deployment 102
Self-Service Portal 103
Cisco Workload Optimization Manager 103
Create More Effective Teams 105
Optimize Your Multicloud Environment 106
Optimize Public Cloud Costs 106
Optimize Hyperconverged Workloads 107
Ensure Application Performance 107
Cisco Workload Optimization Main Features 108
Target Integration 109
View Your Global Environment 110
Automate Actions 111
Plan for the Future 112
Set Policies and Service Level Agreements 114
Cisco Intersight Workload Optimizer 115
Cisco Hyperflex – Intersight 116
Deployment Options 117
Benefits of Using Cisco Intersight 118
Hyperconverged Infrastructure (HCI): Hyperflex 119
Deploying Hyperflex Anywhere with Intersight 122
Cisco Intersight Workload Engine at a Glance 125
Benefits 126
Key Features 126
Summary 127
References/Additional Reading 127

Part 2 Cisco Applications and Workload Management

Chapter 4 Application, Analytics, and Workload Performance Management with AppDynamics 129

What Is AppDynamics? 129
AppDynamics Concepts 130
User Interface 130
Application Performance Monitoring 130
Infrastructure Visibility with Database Visibility 131
End User Monitoring for Client Experience 132
Business iQ and Analytics for Business Impact 132
Use Metrics 132
Baselines and Thresholds 133
Health Rules, Policies, and Actions 134
Infrastructure Monitoring 134
Integrate and Extend AppDynamics 135
Deployment Planning Guide 135
Deployment Models 136
Installation Overview 136
Platform Components and Tools 136
On-Premises Deployment Architecture 137
Platform Components 138
Platform Connections 138
Data Storage Location 140
SaaS Deployment Architecture 140
Application Monitoring 142
Overview of Application Monitoring 142
Business Transactions 143
Business Applications 144
Nodes 144
Tiers 144
Entities 145
Historical and Live Entity Data 145
Anchor Metrics for Entities 145
Liveness Status 145
How the Controller Displays Live Entities 146
Backends 146

Integration with Other AppDynamics Modules 146
Application Monitoring and Infrastructure Visibility 147
Application Monitoring and Browser Real User Monitoring 148
Application Monitoring and Database Visibility 148
Application Monitoring and Analytics 148
Application Security Monitoring 148
Supported APM Agents 149
Cisco Secure Application Components 149
Cisco Secure Application Architecture 150
Monitor Application Security Using Cisco Secure Application 151
Select Scope for the Dashboard 152
Navigate to AppDynamics Application or Tier Flow Map 153
View Data Using Search Filter 153
End User Monitoring 154
Overview of End User Monitoring 155
Understand End User Activity 156
View EUM Data 157
On-Premises EUM Deployments 157
Access the SaaS EUM Server 158
How EUM Works with Other AppDynamics Products 158
EUM and Application Performance Monitoring 158
EUM and Application Analytics 158
Experience Journey Map 159
Experience Journey Map UI 159
Browser Monitoring 163
Overview of the Controller UI for Browser Monitoring 163
Browser App Dashboard 163
Resource Performance Dashboard 165
IoT Monitoring 168
Mobile Real User Monitoring 169
Database Visibility 169
Infrastructure Visibility 171
Overview of Infrastructure Visibility 171
Network Visibility 172
Drill Down to the Root Cause 173
Network Visibility Metrics 174

Server Visibility 176
Using the Server Visibility UI 176
Basic Machine Metrics 177
Java and .NET Infrastructure Monitoring 177
Infrastructure Visibility Strategies 177
Analytics 178
Overview of Analytics 179
Analytics Home Page 179
Monitoring Cloud Applications 180
Docker 180
Monitor Containers with Docker Visibility 181
Enable Container Monitoring 182
Container Monitoring Setup 183
View Container Details 183
View Container Metrics Using the Metric Browser 185
Kubernetes 186
Using Docker Visibility with Kubernetes 186
Container Visibility with Kubernetes 186
Enable Container Visibility 188
Register the Container ID as the Host ID 188
Instrument Applications with Kubernetes 189
Deploy the Machine Agent on Kubernetes 189
ClusterRole Configuration 190
Network Visibility with Kubernetes 193
Cloud Monitoring with AppDynamics Cloud 196
Cloud Infrastructure Monitoring 197
AWS Cloud Infrastructure Observability 197
Azure Cloud Infrastructure Observability 198
Summary 198
References/Additional Reading 199

Chapter 5 Management 201
IT Challenges and Workload Management Solutions 202
Business Impact 202
Cisco Intersight Workload Optimizer 204
CWOM-to-IWO Migration 205
Optimize Hybrid Cloud Infrastructure with IWO 206
How Intersight Workload Optimizer Works 209

Understanding the Market and Virtual Currency 210
Risk Index 212
Understanding Intersight Workload Optimizer Supply Chain 212
Supply Chain Terminology 212
Working with Intersight Workload Optimizer 214
Claiming AWS Targets 214
Claiming Azure Targets 214
Cisco Container Platform 215
Cisco Container Platform Architecture Overview 218
Components of Cisco Container Platform 219
Sample Deployment Topology 219
Administering Clusters on vSphere 221
Administering Amazon EKS Clusters Using CCP Control Plane 224
Licensing and Updates 226
Connected Model 226
Registering CCP Using a Registration Token 226
Upgrading Cisco Container Platform 227
Cisco Intersight Kubernetes Service 228
Benefits of IKS 229
Common Use Case 229
Deploying Consistent, Production-Grade Kubernetes Anywhere 230
How It Works 230
IKS Release Model 232
Deploy Kubernetes from Intersight 232
Step 1: Configure Policies 232
Step 2: Configure Profile 234
Summary 238
References/Additional Reading 238

Chapter 6 Cisco Cloud Webex Application 239
Cisco Webex Features 239
Webex Cloud Calling 241
Webex Security Model 243
Webex Meetings 244
Customize Your Audio and Video Preferences 245
Start Your First Meeting 246
Upcoming Meetings 247
Webex Meetings Security Update 248

Webex Messaging 249
Send a Message 250
Read and Respond to Messages 251
Organize Your Messages 251
Webex | App Security 253
Webex Application Polling 254
Poll in Webex Meetings or Webex Webinars 255
Polls in Slido 256
Webex Events 259
Schedule Webex Webinars 260
Register for a Meeting or Webinar 260
Join a Webinar 261
Webex | Record a Meeting 262
Share Content in Meetings, Webinars, and Events 263
Sharing Multiple Applications 264
Webex Integrations 265
Integrations 265
Bots 266
Support 266
Add Bots and Integrations 266
Remove an Integration 267
Remove a Bot 268
Cisco Webex Cloud Service Architecture 268
Webex Teams Security Features and Deployment Practices 269
Internet Access for Cloud-Based Services 269
Reducing Traffic to the Webex Cloud by Deploying Video Mesh Nodes 270
Webex Teams Inspection Capabilities 272
Webex Team Data Protection 273
Webex Teams Apps – Data at Rest Protection 276
Webex Teams App for Web – Data Storage 277
Webex Team Indexing Service 277
KMS On-Premises 279
Webex Team Single Sign-On 281
Multifactor Authentication 282
IdP and MDM/MAM with Webex Teams 282

Webex Teams Proximity and Device Pairing 282
Proximity for Cloud-Registered Webex Devices 283
Proximity for On-Premises Registered Webex Devices 284
Other Webex Device Discovery Mechanisms 285
Summary 286
References/Additional Reading 286

Chapter 7 Internet of Things (IoT) 287
How Do OT and IT Differ? 288
IoT Challenges 289
Cisco Kinetic Platform 289
Why Cisco Kinetic 291
Understanding Cisco Kinetic Platform 292
Cisco Kinetic – Gateway Management Module 292
Cisco Kinetic – Data Control Module 294
Cisco Kinetic – Edge & Fog Processing Module 296
Introduction to Cisco IoT 297
Edge Device Manager 298
Supported Device Interfaces for Onboarding 300
Onboarding Devices 301
Onboarding IR devices 301
SIM Card Activation and Seamless Device Onboarding 304
SDO Architecture 304
Secure Equipment Access 305
Summary Steps 305
Edge Intelligence 305
Edge to Multicloud Data Flow 306
Overview of Configuration Lifecycle Management in EI 307
Enable and Manage EI Agents 307
Asset Management Workflow 308
Add Data Destinations 309
Add an MQTT Server Destination 309
Deploy Data Rules 310
Deploy Data Logic 310
Licensing 311
Summary 311

Part 3 Cisco Cloud Security

Chapter 8 Cisco Cloud Security 313

Shadow IT Challenge 313

Cisco Cloudlock 314

User Security 315

Data Security 316

Identify Sensitive Data in Cloud Environments 316

Mitigate Increased Risk of Data Exposure in Cloud Applications 316

Mitigate Risk Through Automated Responses 317

App Security 317

Enabling Cloudlock via WSA (11.5) 318

The Evolution of Cloud Security Service 322

DNS-Layer Security 322

Secure Web Gateway 323

Firewall 323

Cloud Access Security Broker 323

Interactive Threat Intelligence 323

Integration with SD-WAN 324

Leveraging Umbrella Log Files for Shadow IT Visibility 324

Dashboard for Visibility and Trends 324

Overview and Trending Information 324

Application Details 325

Optimization 325

Application Blocking 326

Enabling Healthy and Efficient Cloud Adoption 327

Cisco Umbrella 328

Benefits 329

Deployment Options 333

Umbrella Integrations 333

Umbrella Packages 336

Cisco Secure Cloud Analytics 337

Understanding Secure Cloud Analytics 339

How Secure Cloud Analytics Works 341

Deployment 341

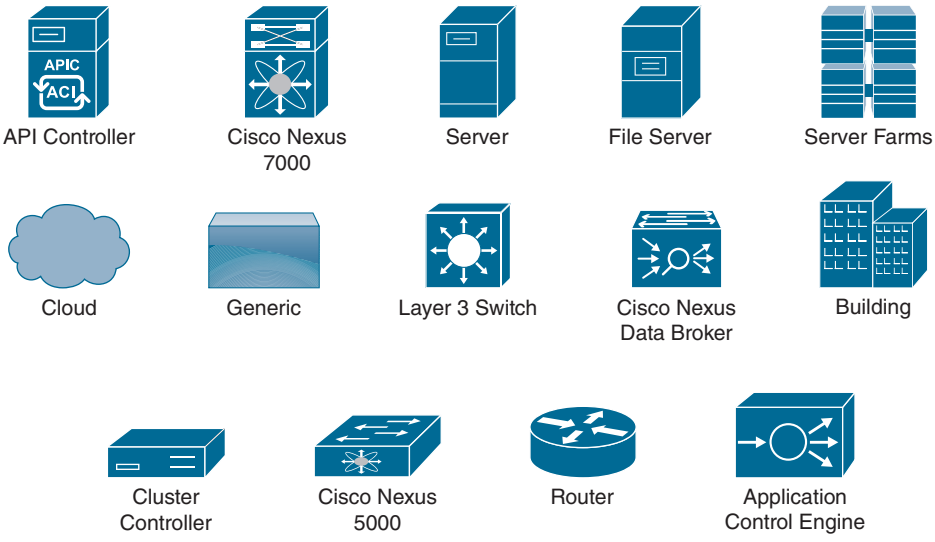
Dynamic Entity Modeling 341

Alerts and Analysis 342

Public Cloud Monitoring Configuration for Amazon Web Services 343
Public Cloud Monitoring Configuration for Google Cloud Platform 344
Single GCP Project Configuration 344
Multiple GCP Project Configuration 344
Public Cloud Monitoring Configuration for Microsoft Azure 345
Watchlist Configuration 346
Configuring the AWS CloudTrail Event Watchlist 346
Configuring the GCP Logging Watchlist 347
Configuring the Azure Activity Log Watchlist 347
Dashboard Overview 347
Cisco Duo Security 348
Multifactor Authentication from Duo 349
Types of 2FA 351
Duo Device Trust Monitor 351
Enforce Adaptive Policies 356
Secure Access for Every User 357
Secure VPN-Less Remote Access for Any Environment 358
Simple, Secure Single Sign-On 358
Summary 360

Index 361

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in Cisco's Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Note This book covers multiple operating systems, and a differentiation of icons and router names indicates the appropriate OS that is being referenced. IOS and IOS XE use router names like **R1** and **R2** and are referenced by the IOS router icon. IOS XR routers will use router names like **XR1** and **XR2** are referenced by the IOS XR router icon.

Introduction

Almost every company is adopting hybrid cloud solutions as it provides decreased hosting costs, agility and scalability, and faster deployment ability and security. Using a hybrid cloud might be an investment upfront, but it will provide plenty of cost saving benefits down the road. For example, businesses that use public cloud without a hybrid might have a difficult and expensive time migrating information if they decide to make changes to their internal systems. Furthermore, because a hybrid cloud is scalable, it makes handling changes in business goals cheaper down the line. Only hybrid cloud technology can provide a blend of benefits that come from public and private servers. With a hybrid cloud, for instance, you can enjoy the scalability of a public cloud environment without forfeiting all control to a third party. In fact, with every hybrid cloud situation being different, a unique solution will have to be applied to each hybrid system in order to fulfill specific requirements. Because a hybrid cloud is designed around your organization's needs, it can be optimized with speed in mind. For example, because this system isn't entirely public, your IT staff will be able to minimize latency, which will make data transfers quicker and easier. The overall level of customization available for hybrid cloud also ensures your organization is agile enough to handle the needs of customers or clients. Not only does it connect old systems to new ones, but the hybrid cloud also allows businesses to create an overarching structure that meets the unique needs of a specific enterprise.

As we see an increasing trend in deployment of hybrid cloud with on-prem solutions, the book will be useful to both small-scale customers and large-scale data centers. It can be considered as one book for all who deal with Cisco Cloud Solutions on a daily basis. External references are provided wherever applicable, but readers are expected to be familiar with cloud-specific technologies, infrastructure concepts, networking connectivity, and security policies of the customer installation. Readers can gain knowledge about the benefits of cloud solutions, how to manage, operate, and integrate existing infrastructure in a hybrid/multicloud environment with minimum changes and leverage insights from the cloud for their business decisions.

Cisco doesn't have a public cloud offering like AWS but has many products that complement and facilitate cloud integration and use of hybrid cloud. The attempt of this book is to fill the gap where a user can find a one-stop book that details all such products and architecture and provides insights on how they can co-exist in a hybrid cloud environment.

The book helps IT professionals, CIOs, and IT managers in their decision to move into a hybrid cloud deployment vs. an on-prem deployment. It describes in detail and from a technical and business aspect the possible solutions and offerings from Cisco. The book also describes products such as the Cisco Nexus Dashboard, which facilitate the orchestration and insights about your deployment.

Last but not least, the book covers best practices and guidelines to make readers aware of known caveats prior to specific deployment, the do's and don'ts while designing complex hybrid cloud networks, how and why to design in a certain way for maximum efficiency.

Goals and Methods

CIOs and IT professionals who want to simplify their IT and networking environment are now challenged with the decision of whether to move fully into the cloud, build their own data centers, or go with hybrid solution. Making such decisions depends on a lot of factors that include the scale and complexity of their existing setup, the level of control over their own resources, security, availability of IT and networking resources, level of expertise, overall fixed and recurring costs, and so on.

As cloud is a new buzzword in industry and multiple vendors are introducing products that offer various infrastructure solutions and are challenging the existing network design, all the new technologies are getting confusing to IT professionals who are trying to move into next-generation architectures while maintaining a current setup that is generating revenue. This book will walk the reader through and provide a reference guide to understand and independently implement cloud solutions for Cisco Network, Compute, Storage, Application, and Security.

In this book we are covering Cisco Cloud Infrastructure for various Cisco Products. This book will cover existing Cisco technologies in the "Data Center, Security, and Applications" domain that are available in the on-prem environment and how the technology has evolved to fit in a hybrid cloud model that facilitates the management and operation of on-prem deployments and provides integration with public cloud. This gives you the tools to ask the right questions when you embark on the transformation of your data center into private and hybrid clouds.

Who Should Read This Book?

We see an increase in hybrid cloud adoption, which requires planning, designing, and execution strategy of on-prem and public cloud setups. In general IT professionals are divided in their areas of expertise. Individuals are spread into focus areas that overlap:

- Orchestration
- Analytics
- Cloud integration
- Virtualization
- Storage networking
- Security
- Software applications
- Automation
- DevOPs

Cisco is taking a network-centric approach to multi-cloud and hybrid deployments. Cisco has partnerships with Azure and AWS and has expanded a relationship with Google Cloud. Add in AppDynamics, which specializes in application and container management, and Cisco has the various parts to address hybrid and multi-cloud deployments. In addition, Cisco is a key hyper-converged infrastructure player and its servers and networking gear are staples in data centers. The audience of this book is the sum of all solution architects, deployment engineers, systems engineers, networking engineers, software virtualization engineers, network management engineers, sales engineers, field consultants, professional services, partner engineering, customers deploying the Cisco Cloud Solutions, and anyone who would like to know about Cisco's presence in cloud space. Also as the book touches on the business aspects of pros and cons of moving from private clouds to public clouds, IT managers and CIOs will benefit from understanding the impact of cloud solutions on the transformation of their data centers and the speed of deploying highly available applications.

How This Book Is Organized

For those who are familiar with the authors' writing style from previous books such as "Implementing Cisco HyperFlex Solutions," the authors put a big emphasis on easy reading and making the difficult look easy. The book goes through a smooth progression of the topics and a lot of the basic concepts are laid out in advance so you do not miss a beat and feel comfortable progressing through the chapters. It is recommended to go through the chapters in order to get the full benefit of the book.

Orchestration, analytics, management, security, and automation are not easy topics and are getting more complex every day. Boundaries between system administrators, networking engineers, and software engineers are getting blurred day by day and expectations are increasing to be an expert in all dimensions by a single individual.

The authors have put a lot of effort into putting you on the right track and giving you the launch pad into tackling cloud infrastructure. Their many years of experience in both the vendor and system integration track and across the different technology areas make this difficult topic sound simple. The advantages you see from this book follow:

- An easy reading style with no marketing fluff or heavy technical jargon
- Progression through the chapters from easy to advanced
- Comprehensive coverage of the topic at both a technical and business level
- First book to address Cisco cloud solutions in detail under one umbrella to bridge the technology gap between the different IT departments
- Beneficial to IT professionals trying to evaluate whether to move into the hybrid cloud solution

- Beneficial to IT management, CIO, and CTO evaluating various cloud applications
- Coverage of the latest cloud offerings by Cisco
- Discusses Automation and Orchestration solutions
- Compares and contrasts different implementations objectively and with vendor neutrality

Book Structure

The book is organized into three parts.

PART 1—Cisco Data Center Networking and Infrastructure

Chapter 1—Cisco Data Center Orchestration: This chapter talks about Cisco's data center orchestration software that uses the automation of tasks to implement processes, such as deploying new servers. Automation solutions that orchestrate data center operations enable an agile DevOps approach for continual improvements to applications running in the data center. Data center orchestration systems automate the configuration of L2-L7 network services, compute and storage for physical, virtual, and hybrid networks. New applications can be quickly deployed.

Chapter 2—Cisco Data Center Analytics and Insights: This chapter talks about Cisco's API-driven monitoring and assurance solutions that provide essential insights as well as add to an expansive and increasingly onerous toolset. These network insight solutions are bringing the ability to see the big picture, and if something goes wrong, they show exactly where to look instead of poking around and hoping to get lucky. This helps prepare companies to progressively transition from reactive to proactive and eventually predictive IT operations.

Chapter 3—Cisco Data Center Solutions for Hybrid Cloud: This chapter talks about the various hybrid cloud management platforms like ACI, UCS Director, CWOM, and Intersight that are provided by Cisco and offer flexible consumption for on-premises infrastructure in order to optimize workloads across clouds, on-premises data centers, labs, and co-location facilities for scale, performance, and agility with great value.

PART 2—Cisco Applications and Workload Management

Chapter 4—Application, Analytics, and Workload Performance Management with AppDynamics: This chapter describes Cisco's AppDynamics solution, cloud migration, and various monitoring such as Application Security Monitoring, End User monitoring and Browser monitoring. It also covers database and infrastructure visibility and cloud platforms.

Chapter 5—Management: This chapter describes the challenges that the IT teams face in managing the modern workloads and gives you various systematic Workload Management Solutions such as Intersight Workload Optimization Manager, Cisco Container Platform, and Cisco Intersight Kubernetes Service (IKS).

Chapter 6—Cisco Cloud Webex Applications: Collaboration is a key component of any IT solution and Cisco Webex provides an ideal platform for staying connected and collaborating with individuals, teams, and meetings to move projects forward faster. This chapter describes Cisco Webex Features and Cisco Webex Cloud Service Architecture in detail.

Chapter 7—Internet of Things (IoT): This chapter describes how well we can combine the Operational Technology hardware with IT and come up with amazing IoT solutions, which Cisco currently offers. These solutions can really help you get the best insights and increase efficiency.

PART 3—Cisco Cloud Security

Chapter 8— Cisco Cloud Security: This chapter talks about all the Cisco Cloud Security solutions like Cloudlock, Umbrella, Cloud Analytics, and Duo using which one can adopt the cloud with confidence and protect users, data, and applications, anywhere they are. Unlike traditional perimeter solutions, Cisco Cloud Security blocks threats over all ports and protocols for comprehensive coverage. Cisco Cloud Security also uses API-based integrations so that the existing security investments can be amplified.

This page intentionally left blank

Chapter 5

Management

Cisco has been working for over three years to bring the industry-leading Application Resource Management (ARM) capability to Cisco customers. It started with Cisco Workload Optimization Manager (CWOM). CWOM is powered by Turbonomic, and it enables Cisco customers to continuously resource applications to perform at the lowest cost while adhering to policies irrespective of where the application is hosted (that is, on the premises or in the cloud, containers, or VMs). In January 2020, Cisco announced Intersight Workload Optimizer (IWO), which is the integration of CWOM and Intersight. With IWO, application and infrastructure teams can now speak the same language to ensure that applications are automatically and continuously resourced to perform.

Alongside the Intersight Workload Optimizer, Cisco offers Intersight Kubernetes Service (IKS), which is a fully curated, lightweight container management platform for delivering multicloud production-grade upstream Kubernetes. It simplifies the process of provisioning, securing, scaling, and managing virtualized Kubernetes clusters by providing end-to-end automation, including the integration of networking, load balancers, native dashboards, and storage provider interfaces.

This chapter will cover the following topics:

- IT challenges and workload management solutions
- Intersight Workload Optimization Manager
- Cisco Container Platform
- Cisco Intersight Kubernetes Service

IT Challenges and Workload Management Solutions

Managing application resources in a dynamic, hybrid cloud world is increasingly complex, and IT teams are struggling. With application components running on the premises and in public clouds, end users can suffer outages or experience slow application performance because IT teams simply lack visibility to see how things are connected and how to manage their dynamic environment at scale.

With more people accessing your business through a digital experience, application performance is more critical than ever. Managing workload placement and resources across your ever-changing IT environment is a complex, time-consuming task that has big implications on user experience and costs.

Cisco Intersight Workload Optimizer (CWOM) discovers how all the parts of your hybrid world are connected and then automates these day-to-day operations for you. Supporting more than 50 common platforms and public clouds, it provides real-time, full-stack visibility across your applications and infrastructure. Now you can harness the power of data to continuously monitor supply and demand, match workloads and resources in the most efficient way, and ensure that governance rules are always enforced. The result? Better application performance, reduced cost, faster troubleshooting, and more peace of mind.

Business Impact

Unchecked complexity can result in the following:

- **Underutilized on-premises infrastructure:** To ensure application performance, IT teams often allocate resources modeled to peak-load estimates and/or set conservative utilization limits.
- **Public cloud overprovisioning and cost overruns:** When planning and placing workloads in public clouds, IT teams routinely overprovision computing instance sizes as a hedge to ensure application performance.
- **Wasted time:** IT teams end up chasing alerts and meeting in war rooms to unravel problems instead of supporting innovation.

Figure 5-1 illustrates why managing hybrid cloud resources to ensure application performance and control costs is a complex problem.

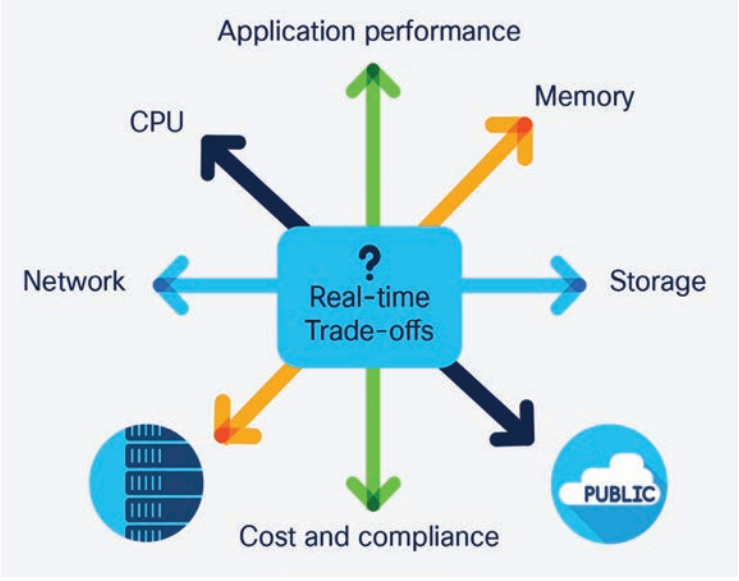


Figure 5-1 *Hybrid cloud resources for ensuring performance and cost*

The following are some of the challenges of workload management in a hybrid cloud:

- Siloed teams with different toolsets managing different layers of the stack and multiple types of resources
- Flying blind without a unified view of the complex interdependencies between layers of infrastructure and applications across on-premises and public cloud environments
- Separating the signal from the noise and prioritizing the constant flow of alerts coming from separate tools
- Lack of visibility into underutilized capacity in public clouds and cost overruns from unmanaged spikes in utilization

To deal with all this complexity, the only choice is to automate resource management and workload placement operations. But how? To optimize effectively, you need a way to collect and track streams of telemetry data from dozens, hundreds, perhaps thousands of sources. You need a way to correlate and continuously analyze all of this data to understand how everything fits together and what's important, as well as how to decide what to do from moment to moment as things continue to change. New tooling is required to connect all the dots and give you the insight you need to stay ahead of demand, stay ahead of problems, and respond to new projects with confidence. What if you could create a unified view of your environment and continuously ensure that applications get the resources they need to perform, all while increasing efficiency and lowering costs?

Cisco Intersight Workload Optimizer

Cisco Intersight Workload Optimizer is a real-time decision engine that ensures the health of applications across your on-premises and public cloud environments while lowering costs. The intelligent software continuously analyzes workload demand, resource consumption, resource costs, and policy constraints to determine an optimal balance. Cisco IWO is an artificial intelligence for IT operations (AIOps) toolset that makes recommendations for operators and can trigger workload placement and resource allocations in your data center and the public cloud, thus fully automating real-time optimization.

With Cisco IWO, infrastructure and operations teams are armed with visibility, insights, and actions that ensure service level agreements (SLAs) are met while improving the bottom line. Also, application and DevOps teams get comprehensive situational awareness so they can deliver high-performing and continuously available applications.

Benefits of using Cisco Intersight Workload Optimizer:

- Radically simplify application resource management with a single tool that dynamically optimizes resources in real time to ensure application performance.
- Continuously optimize critical IT resources, resulting in more efficient use of existing infrastructure and lower operational costs on the premises and in the cloud.
- Take the guesswork out of planning for the future with the ability to quickly model what-if scenarios based on the real-time environment.

Figure 5-2 illustrates how IWO ensures application performance with continuous visibility, deep insights, and informed actions.

Figure 5-2 *Application performance with continuous visibility, deep insights, and informed actions*

CWOM-to-IWO Migration

In June 2019, Turbonomic and CWOM became inaugural members of the Integration Partner Program (IPP), which takes the technology partnership to another level by helping joint customers maximize the value of their AppDynamics and CWOM investment. The extended integration and partnership delivers on the vision of AIOps, where software is making dynamic resourcing decisions and automating actions to ensure that applications are always performing, enabling positive business outcomes and improved user experiences. Organizations across the world are investing heavily in developing new applications and innovating faster to deliver better, more simplified user experiences. The partnership and the combination of AppDynamics and CWOM ensure that applications are architected and written well and are continuously resourced for performance.

As a full-stack, real-time decision engine, Intersight Workload Optimizer revolutionizes how teams manage application resources across their multicloud landscape, significantly simplifying operations. It delivers unprecedented levels of visibility, insights, and automated actions, as customers look to prevent application performance issues.

Figure 5-3 provides a very high-level view of IWO application management.

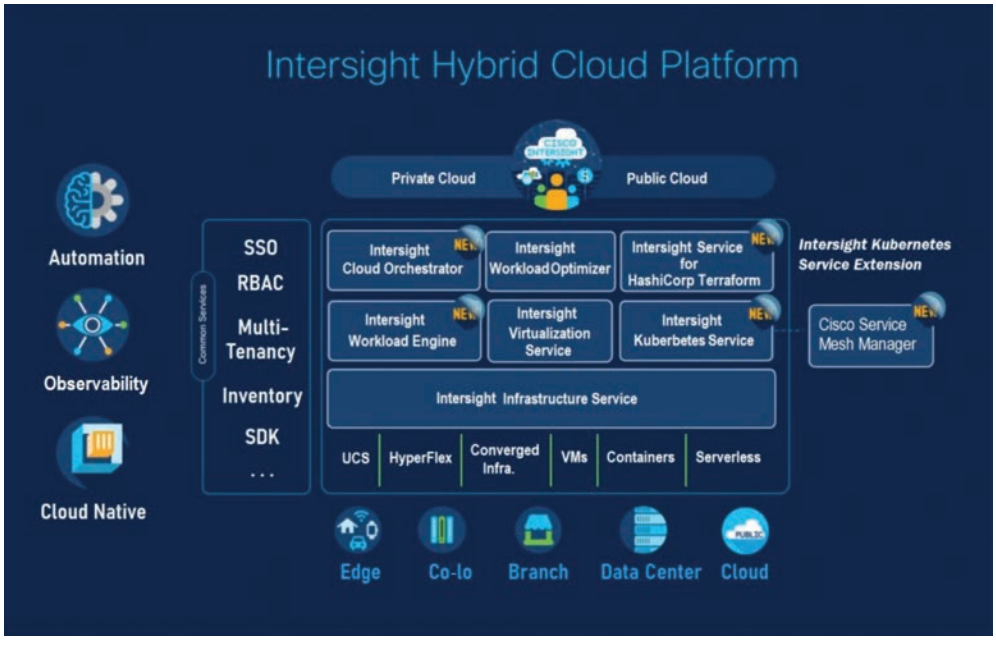


Figure 5-3 *Very high-level view of IWO application management*

Simply put, IWO provides the following customer benefits:

- It bridges the gap between application and IT teams to ensure application performance.

- It eliminates application resourcing as a source of application delay, meaning applications can perform and continuously deliver services.
- It helps IT departments stop overspending and delivers a modern application hosting platform to end users.
- It enables high-value application and IT teams to focus on strategy and innovation without jeopardizing applications.

IWO expands Intersight capabilities. All in one place, Intersight customers can manage the health of the infrastructure and how well that infrastructure is utilized to ensure application performance. Additionally, Intersight customers can monitor and manage application resources on third-party infrastructure, public cloud, and container environments.

Optimize Hybrid Cloud Infrastructure with IWO

Application resource management is a top-down, application-driven approach that continuously analyzes applications' resource needs and generates fully automatable actions to ensure applications always get what they need to perform. It runs 24/7/365 and scales with the largest, most complex environments.

To perform application resource management, Intersight Workload Optimizer represents your environment holistically as a supply chain of resource buyers and sellers, all working together to meet application demand. By empowering buyers (VMs, instances, containers, and services) with a budget to seek the resources that applications need to perform and empowering sellers to price their available resources (CPU, memory, storage, network) based on utilization in real time, IWO keeps your environment within the desired state, with operating conditions that achieve the following conflicting goals at the same time:

- **Ensured application performance:** Prevent bottlenecks, upsize containers/VMs, prioritize workload, and reduce storage latency
- **Efficient use of resources:** Consolidate workloads to reduce infrastructure usage to the minimum, downsize containers, prevent sprawl, and use the most economical cloud offerings

IWO is a containerized, microservices-architected application running in a Kubernetes environment (or within a VM) on your network or a public cloud VPC (Virtual Private Cloud). You assign services running on your network to be IWO targets. IWO discovers the entities (physical devices, virtual components, and software components) that each target manages and then performs analysis, anticipates risks to performance or efficiency, and recommends actions you can take to avoid problems before they occur.

Intelligent, proactive workload optimization simplifies and automates operations. With many tools, the focus is on monitoring and alerting users after a problem has occurred. Cisco IWO is a proactive tool that is designed to avoid application performance issues in the first place. It continuously analyzes workload performance, costs, and compliance

rules and makes recommendations on what specific actions to take to avoid issues before they happen, thus radically simplifying and improving day-to-day operations.

While some tools provide visibility into applications or visibility into an individual tier of physical or virtual infrastructure, Cisco IWO bridges all these layers with a single tool. It creates a dynamic dependency graph that visualizes the connections between application elements and infrastructure throughout the layers of the stack, all the way down to component resources within servers, networking, and storage. Figure 5-4 shows how Cisco IWO analyzes telemetry data across your hybrid cloud environment to optimize resources and reduce cost.

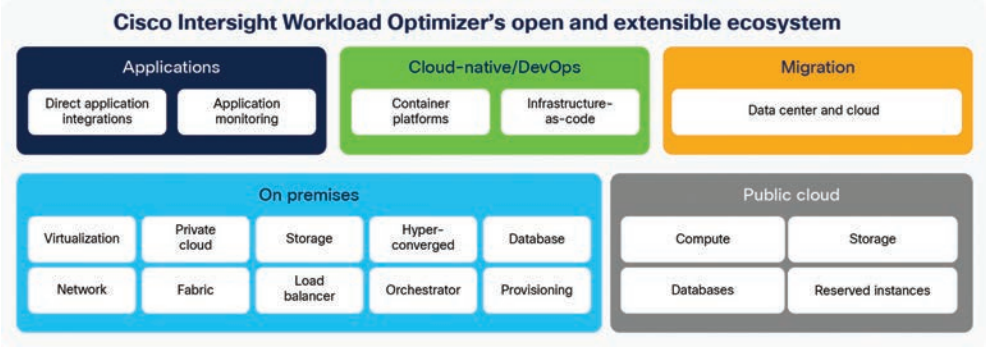


Figure 5-4 *Cisco IWO analyzes telemetry data across your hybrid cloud environment to optimize resources and reduce cost*

Cisco IWO can optimize workloads in any infrastructure, any environment, and any cloud, and it works with the industry's top platforms, including VMware vSphere, Microsoft Hyper-V, Citrix XenServer, and OpenStack. It automatically manages compute, storage, and network resources across these platforms, both on the premises and in the cloud. It analyzes telemetry data from a broad ecosystem of data center and cloud technologies, with agentless support for over 50 targets across a range of hypervisors, compute platforms (including Cisco UCS and HyperFlex), container platforms, public clouds, and more. Cisco IWO correlates these telemetry sources into a holistic view to deliver intelligent recommendations and trigger actions, including where to place workloads and how to size and scale resources.

Cisco Intersight is a cloud operations platform that delivers intelligent visualization, optimization, and orchestration for applications and infrastructure across public cloud and on-premises environments. It provides an essential control point for customers to get more value from hybrid cloud investments.

The Cisco IWO service extends these capabilities with hybrid cloud application resource management and support for a broad third-party ecosystem. With this powerful solution, you can have confidence that your applications have continuous access to the IT resources they need to perform, at the lowest cost, whether they reside on the premises or in a public cloud.

The combination of Cisco IWO and AppDynamics can break down siloes between IT teams. This integration provides a single source of truth for application and infrastructure teams to work together more effectively, avoiding finger pointing and late-night war rooms.

AppDynamics discovers and maps your business application topology and how it uses IT resources. Cisco IWO correlates this data with your infrastructure stacks to create a dynamic dependency graph of your hybrid IT environment. It analyzes supply and demand and drives workload placement and resource allocation actions in your IT environment to help ensure that application components get the computing, storage, and network resources they need. Together, these intelligent tools replace sizing guesswork with real-time analytics and modeling so that you know how much infrastructure is needed to allow your applications and business to keep pace with demand.

If you have workloads running on the premises and in public clouds, your IT teams need to make complex, on-going decisions about where to locate workloads and how to size resources in order to ensure performance and minimize cost.

Figuring out what workloads should run where is nearly impossible if you lack clear visibility into available resources and associated costs. And for workloads that run in the cloud, how do you determine what cloud instance or tier is the best fit at the lowest cost? Cloud costs can become volatile, and you can get lost in a myriad of sizing, placement, and pricing decisions that can have very expensive consequences. Cisco IWO can help in the following ways:

- Manage resource allocation and workload placement in all your infrastructure environments, giving you full-stack visibility in a single pane of glass for supply and demand across your combined on-premises and cloud estate.
- Optimize cloud costs with automated selection of instances, reserved instances (RIs), relational databases, and storage tiers based on workload consumption and optimal costs.
- Dynamically scale, delete, and purchase the right cloud resources to ensure performance at the lowest cost.
- Extend on-premises resources by continuously optimizing workload placement and cutting overprovisioning based on utilization trends.
- De-risk migrations to and from the cloud with a data-driven scenario modeling engine.

In increasingly competitive markets, more organizations are adopting containerized deployment options to deliver business-differentiating applications quickly. Kubernetes has become the de facto standard for container orchestration and helps to build, deliver, and scale applications faster. For IT teams, Kubernetes has introduced new layers of complexity with interdependencies and fluctuating demand that make it nearly impossible to effectively manage modern IT at scale.

Cisco IWO simplifies Kubernetes deployments and optimizes performance and cost in real time for on-going operations in the following ways:

- **Container rightsizing:** Scale container limits/requests up or down based on application demand.
- **Pod "move"/rescheduling:** Reschedule pods while maintaining service availability to avoid resource fragmentation and/or contention on the node.
- **Cluster scaling:** When Cisco IWO sees that pods have too little (or too much) capacity in a cluster, it will give the recommendation to spin up another node (or to suspend nodes).
- **Container planning:** Model what-if scenarios based on your real-time environment. With a few clicks, you can determine how much headroom you have in your clusters or simulate adding or removing Kubernetes pods.

How Intersight Workload Optimizer Works

To keep your infrastructure in the desired state, IWO performs application resource management. This is an ongoing process that solves the problem of ensuring application performance while simultaneously achieving the most efficient use of resources and respecting environment constraints to comply to business rules. This is not a simple problem to solve. Application resource management has to consider many different resources and how they are used in relation to each other, in addition to numerous control points for each resource. As you grow your infrastructure, the factors for each decision increase exponentially. On top of that, the environment is constantly changing—to stay in the desired state, you are constantly trying to hit a moving target. To perform application resource management, IWO models the environment as a market made up of buyers and sellers. These buyers and sellers make up a supply chain that represents tiers of entities in your inventory. This supply chain represents the flow of resources from the data center, through the physical tiers of your environment, into the virtual tier and out to the cloud. By managing relationships between these buyers and sellers, IWO provides closed-loop management of resources, from the data center through to the application.

IWO uses virtual currency to give a budget to buyers and assign cost to resources. This virtual currency assigns value across all tiers of your environment, making it possible to compare the cost of application transactions with the cost of space on a disk or physical space in a data center. The price that a seller charges for a resource changes according to the seller's supply. As demand increases, prices increase. As prices change, buyers and sellers react. Buyers are free to look for other sellers that offer a better price, and sellers can duplicate themselves (open new storefronts) to meet increasing demand. IWO uses its Economic Scheduling Engine to analyze the market and make these decisions. The effect is an invisible hand that dynamically guides your IT infrastructure to the optimal use of resources. To get the most out of IWO, you should understand how it models your environment, the kind of analysis it performs, and the desired state it works to achieve. Figure 5-5 illustrates the desired state graph for infrastructure management.

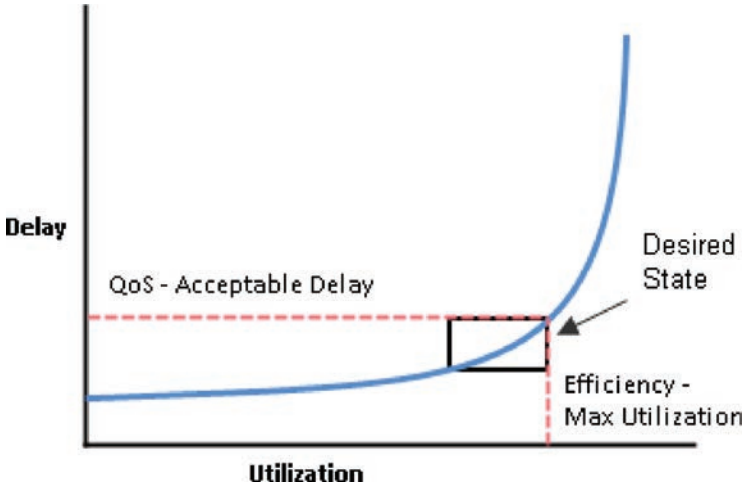


Figure 5-5 *Desired state graph for infrastructure management*

The goal of application resource management is to ensure performance while maintaining efficient use of resources. When performance and efficiency are both maintained, the environment is in the desired state. You can measure performance as a function of delay, where zero delay gives the ideal quality of service (QoS) for a given service. Efficient use of resources is a function of utilization, where 100% utilization of a resource is the ideal for the most efficient utilization.

If you plot delay and utilization, the result is a curve that shows a correlation between utilization and delay. Up to a point, as you increase utilization, the increase in delay is slight. There comes a point on the curve where a slight increase in utilization results in an unacceptable increase in delay. On the other hand, there is a point in the curve where a reduction in utilization doesn't yield a meaningful increase in QoS. The desired state lies within these points on the curve.

You could set a threshold to post an alert whenever the upper limit is crossed. In that case, you would never react to a problem until delay has already become unacceptable. To avoid that late reaction, you could set the threshold to post an alert before the upper limit is crossed. In that case, you guarantee QoS at the cost of over-provisioning—you increase operating costs and never achieve efficient utilization.

Instead of responding after a threshold is crossed, IWO analyzes the operating conditions and constantly recommends actions to keep the entire environment within the desired state. If you execute these actions (or let IWO execute them for you), the environment will maintain operating conditions that ensure performance for your customers, while ensuring the lowest possible cost thanks to efficient utilization of your resources.

Understanding the Market and Virtual Currency

To perform application resource management, IWO models the environment as a market and then uses market analysis to manage resource supply and demand. For example,

bottlenecks form when local workload demand exceeds the local capacity—in other words, when demand exceeds supply. By modeling the environment as a market, IWO can use economic solutions to efficiently redistribute the demand or increase the supply.

IWO uses two sets of abstraction to model the environment:

- **Modeling the physical and virtual IT stack as a service supply chain:** The supply chain models your environment as a set of managed entities. These include applications, VMs, hosts, storage, containers, availability zones (cloud), and data centers. Every entity is a buyer, a seller, or both. A host machine buys physical space, power, and cooling from a data center. The host sells resources such as CPU cycles and memory to VMs. In turn, VMs buy host services and then sell their resources (VMem and VCPU) to containers, which then sell resources to applications.
- **Using virtual currency to represent delay or QoS degradation, and to manage the supply and demand of services along the modeled supply chain:** The system uses virtual currency to value these buy/sell transactions. Each managed entity has a running budget. The entity adds to its budget by providing resources to consumers, and the entity draws from its budget to pay for the resources it consumes. The price of a resource is driven by its utilization—the more demand for a resource, the higher its price.

Figure 5-6 illustrates the IWO abstraction model.

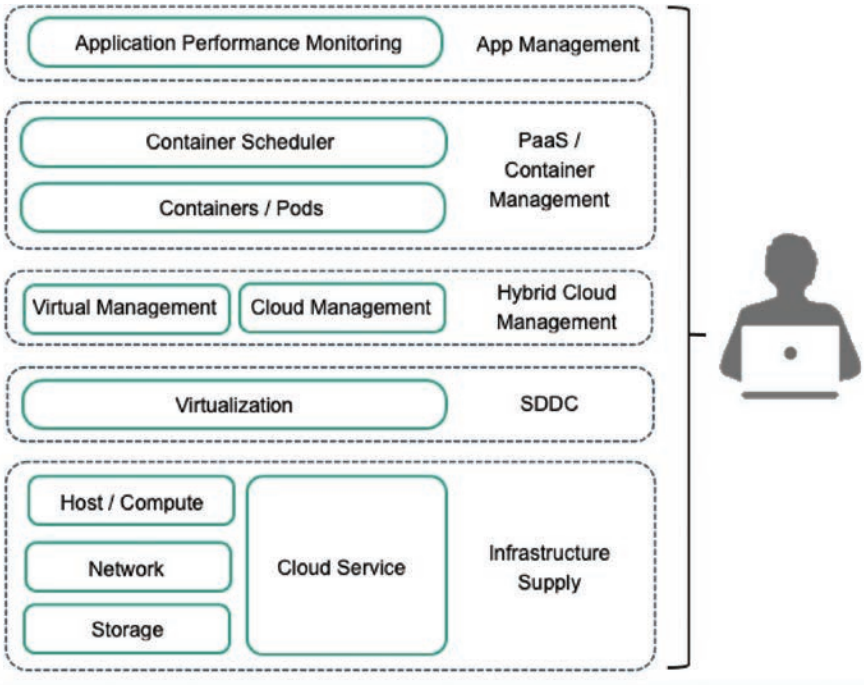


Figure 5-6 *IWO abstraction model*

These abstractions open the whole spectrum of the environment to a single mode of analysis—market analysis. Resources and services can be priced to reflect changes in supply and demand, and pricing can drive resource allocation decisions. For example, a bottleneck (excess demand over supply) results in rising prices for the given resource. Applications competing for the same resource can lower their costs by shifting their workloads to other resource suppliers. As a result, utilization for that resource evens out across the environment and the bottleneck is resolved.

Risk Index

Intersight Workload Optimizer tracks prices for resources in terms of the Risk Index (RI). The higher this index for a resource, the more heavily the resource is utilized, the greater the delay for consumers of that resource, and the greater the risk to your QoS. IWO constantly works to keep the RI within acceptable bounds.

You can think of the RI as the cost for a resource, and IWO works to keep the cost at a competitive level. This is not simply a matter of responding to threshold conditions. IWO analyzes the full range of buyer/seller relationships, and each buyer constantly seeks out the most economical transaction available.

This last point is crucial to understanding IWO. The virtual environment is dynamic, with constant changes to workload that correspond with the varying requests your customers make of your applications and services. By examining each buyer/seller relationship, IWO arrives at the optimal workload distribution for the current state of the environment. In this way, it constantly drives your environment toward the desired state.

Understanding Intersight Workload Optimizer Supply Chain

Intersight Workload Optimizer models your environment as a market of buyers and sellers. It discovers different types of entities in your environment via the targets you have added, and it then maps these entities to the supply chain to manage the workloads they support. For example, for a hypervisor target, IWO discovers VMs, the hosts and datastores that provide resources to the VMs, and the applications that use VM resources. For a Kubernetes target, it discovers services, namespaces, containers, container pods, and nodes. The entities in your environment form a chain of supply and demand, where some entities provide resources while others consume the supplied resources. IWO stitches these entities together, for example, by connecting the discovered Kubernetes nodes with the discovered VMs in vCenter.

Supply Chain Terminology

Cisco introduces specific terms to express IT resources and utilization in relation to supply and demand. The terms shown in Table 5-1 are largely intuitive, but you should understand how they relate to the issues and activities that are common for IT management.

Table 5-1 *The Supply Chain Terminologies Used in IWO*

Term	Definition
Commodity	This is the basic building block of IWO supply and demand. All the resources that IWO monitors are commodities. For example, the CPU capacity and memory that a host can provide are commodities. IWO can also represent clusters and segments as commodities. When the user interface (UI) shows "commodities," it's showing the resources a service provides. When the interface shows "commodities bought," it's showing what that service consumes.
Composed of	This refers to the resources or commodities that make up the given service. For example, in the UI you might see that a certain VM is *composed of* commodities, such as one or more physical CPUs, an Ethernet interface, and physical memory. Contrast "composed of" with "consumes," where consumption refers to the commodities the VM has bought. Also contrast "composed of" with the commodities a service offers for sale. A host might include four CPUs in its composition, but it offers CPU cycles as a single commodity.
Consumes	This refers to the services and commodities a service has bought. A service *consumes* other commodities. For example, a VM consumes the commodities offered by a host, and an application consumes commodities from one or more VMs. In the UI, you can explore the services that provide the commodities the current service consumes.
Entity	This refers to a buyer or seller in the market. For example, a VM or a datastores is an entity.
Environment	This refers to the totality of data center, network, host, storage, VM, and application resources that you are monitoring.
Inventory	This is the list of all entities in your environment.
Risk Index	This is a measure of the risk to quality of service (QoS) that a consumer will experience. The higher the Risk Index (RI) on a provider, the more risk to QoS for any consumer of that provider's services. For example, a host provides resources to one or more VMs. The higher the RI on the provider, the more likely that the VMs will experience QoS degradation. In most cases, for optimal operation, the RI on a provider should not go into double digits.

Working with Intersight Workload Optimizer

The public cloud provides compute, storage, and other resources on demand. By adding an AWS Billing Target (AWS) or Microsoft Enterprise Agreement (Azure) to use custom pricing and discover reserved instances, you enable IWO to use that richer pricing information to calculate workload size and RI coverage for your Azure environment. You can run all of your infrastructure on a public cloud, or you can set up a hybrid environment where you burst workload to the public cloud as needed. IWO can analyze the performance of applications running on the public cloud and then provision more instances as demand requires. For a hybrid environment, IWO can provision copies of your application VMs on the public cloud to satisfy spikes in demand, and as demand falls off, it can suspend those VMs if they're no longer needed. With public cloud targets, you can use IWO to perform the following tasks:

- Scale VMs and databases
- Change storage tiers
- Purchase VM reservations
- Locate the most efficient workload placement within the hybrid environment while ensuring performance
- Detect unused storage volumes

Claiming AWS Targets

For IWO to manage an AWS account, you provide the credentials via the Access Key that you use to access that account. (For information about getting an Access Key for an AWS account, see the Amazon Web Services documentation.)

To add an AWS target, specify the following:

- **Custom Target Name**: The display name that will be used to identify the target in the Target List. This is for display in the UI only; it does not need to match any internal name.
- **Access Key**: Provide the Access Key for the account you want to manage.
- **Access Key Secret**: Provide the Access Key Secret for the account you want to manage.

Claiming Azure Targets

Microsoft Azure is Microsoft's infrastructure platform for the public cloud. You gain access to this infrastructure through a service principal target. To specify an Azure target, you provide the credentials for the subscription and IWO discovers the resources available to you through that service principal. Through Azure service principal targets, IWO automatically discovers the subscriptions to which the service principal has been granted

access in the Azure portal. This, in turn, creates a derived target for each subscription that inherits the authorization provided by the service principal (for example, contributor). You cannot directly modify a derived target, but IWO validates the target and discovers its inventory as it does with any other target.

To claim an Azure service principal target, you must meet the following requirements:

- Set up your Azure service principal subscription to grant IWO the access it needs. To set up the Azure subscription, you must access the Administrator or Co-Administrator Azure Portal (portal.azure.com). Note that this access is only required for the initial setup. IWO does not require this access for regular operation.
- Claim the target with the credentials that result from the subscription setup (Tenant ID, Client ID, and so on).
- Azure Resource Manager Intersight Workload Optimizer requires the Azure Resource Manager deployment and management service. This provides the management layer that IWO uses to discover and manage entities in your Azure environment.

Cisco Container Platform

Setting up, deploying, and managing multiple containers for multiple micro-sized services gets tedious—and difficult to manage across multiple public and private clouds. IT Ops has wound up doing much of this extra work, which makes it difficult for them to stay on top of the countless other tasks they're already charged with performing. If containers are going to truly be useful at scale, we have to find a way to make them easier to manage.

The following are the requirements in managing container environments:

- The ability to easily manage multiple clusters
- Simple installation and maintenance
- Networking and security consistency
- Seamless application deployment, both on the premises and in public clouds
- Persistent storage

That's where Cisco Container Platform (CCP) comes in, which is a fully curated, lightweight container management platform for production-grade environments, powered by Kubernetes, and delivered with Cisco enterprise-class support. It reduces the complexity of configuring, deploying, securing, scaling, and managing containers via automation, coupled with Cisco's best practices for security and networking. CCP is built with an open architecture using open source components, so you're not locked in to any single vendor. It works across both on-premises and public cloud environments. And because it's optimized with Cisco HyperFlex, this preconfigured, integrated solution sets up in minutes.

The following are the benefits of CCP:

- **Reduced risk:** CCP is a full-stack solution built and tested on Cisco HyperFlex and ACI Networking, with Cisco providing automated updates and enterprise-class support for the entire stack. CCP is built to handle production workloads.
- **Greater efficiency:** CCP provides your IT Ops team with a turnkey, preconfigured solution that automates repetitive tasks and removes pressure on them to update people, processes, and skill sets in-house. It provides developers with flexibility and speed to be innovative and respond to market requirements more quickly.
- **Remarkable flexibility:** CCP gives you choices when it comes to deployment—from hyperconverged infrastructure to VMs and bare metal. Also, because it's based on open source components, you're free from vendor lock-in.

Figure 5-7 provides a holistic overview of CCP.

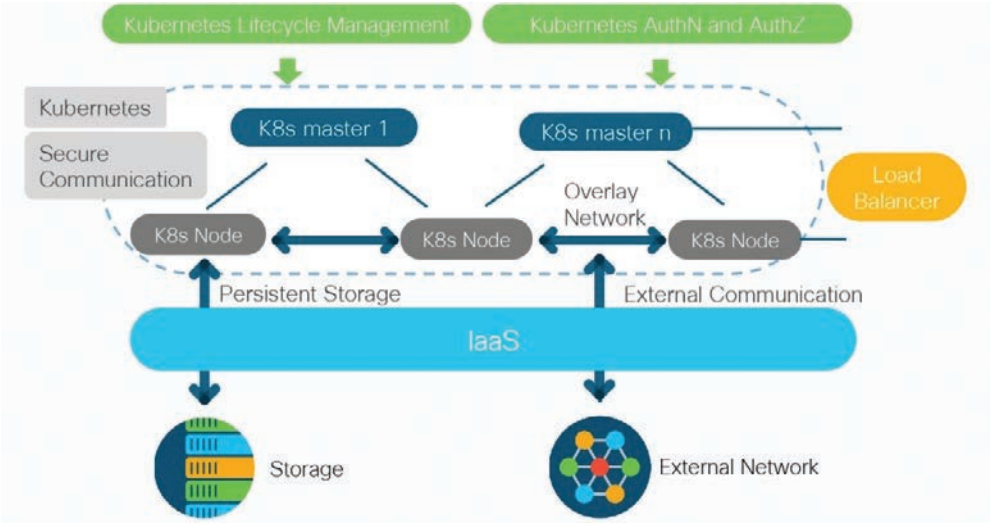


Figure 5-7 *Holistic overview of CCP*

Cisco Container Platform ushers all of the tangible benefits of container orchestration into the technology domain of the enterprise. Based on upstream Kubernetes, CCP presents a UI for self-service deployment and management of container clusters. These clusters consume private cloud resources based on established authentication profiles, which can be bound to existing RBAC models. The advantage to disparate organizational teams is the flexibility to consistently and efficiently deploy clusters into IaaS resources, a feat not easily accomplished and scaled when utilizing script-based frameworks. Teams can discriminately manage their cluster resources, including responding to conditions requiring a scale-out or scale-in event, without fear of disrupting another team's assets.

CCP boasts an innately open architecture composed of well-established open source components—a framework embraced by DevOps teams aiming their innovation toward cloud-neutral work streams.

CCP deploys easily into an existing infrastructure, whether it be of a virtual or bare-metal nature, to become the turnkey container management platform in the enterprise. CCP incorporates ubiquitous monitoring and policy-based security and provides essential services such as load balancing and logging. The platform can provide applications an extension into network management, application performance monitoring, analytics, and logging. CCP offers an API layer that is compatible with Google Cloud Platform and Google Kubernetes Engine, so transitioning applications potentially from the private cloud to the public cloud fits perfectly into orchestration schemes. The case could be made for containerized workloads residing in the private cloud on CCP to consume services brokered by Google Cloud Platform, and vice versa. For environments with a Cisco Application Centric Infrastructure (ACI), Contiv, a CCP component, will secure the containers in a logical policy-based context. Those environments with Cisco HyperFlex (HX) can leverage the inherent benefits provided by HX storage and provide persistent volumes to the containers in the form of FlexVolumes. CCP normalizes the operational experience of managing a Kubernetes environment by providing a curated production quality solution integrated with best-of-breed open source projects. Figure 5-8 illustrates the CCP feature set.

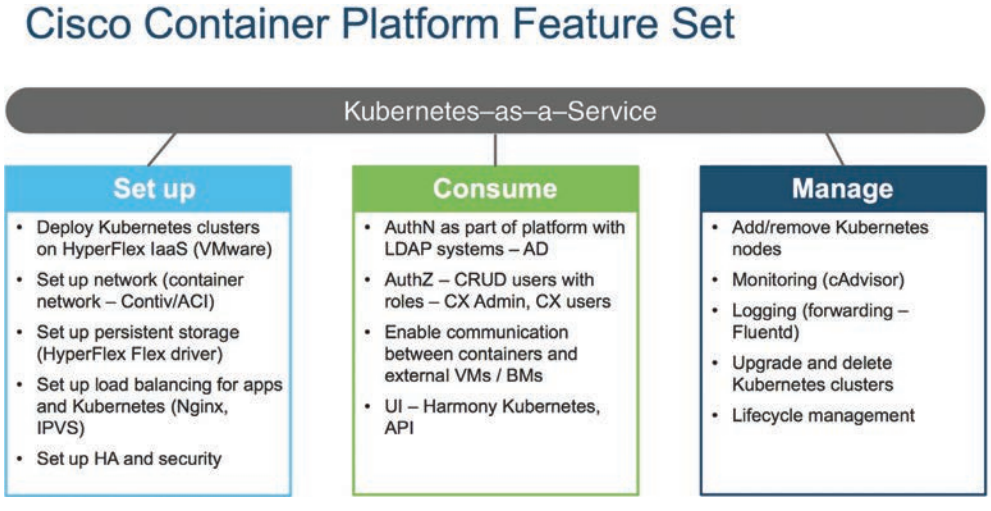


Figure 5-8 *CCP feature set*

The following are some CCP use cases:

- **Simple GUI-driven menu system to deploy clusters:** You don't have to know the technical details of Kubernetes to deploy a cluster. Just fill in the questions, and CCP will do the work.

- **The ability to deploy Kubernetes clusters in air-gapped sites:** CCP tenant images contain all the necessary binaries and don't need Internet access to function.
- **Choice of networking solutions:** Use Cisco's ACI plug-in, an industry standard Calico network, or if scaling is your priority, choose Contiv with VPP. All work seamlessly with CCP.
- **Automated monthly updates:** Bug fixes, feature enhancements, and CVE remedies are pushed automatically every month—not only for Kubernetes, but also for the underlying operating system (OS).
- **Built-in visibility and monitoring:** CCP lets you see what's going on inside clusters to stay on top of usage patterns and address potential problems before they negatively impact the business.
- **Preconfigured persistent volume storage:** Dynamic provisioning using HyperFlex storage as the default. No additional drivers need to be installed. Just set it and forget it.
- **Deploy EKS clusters using CCP control plane:** CCP allows you to use a single pane of glass for deploying on-premises and Amazon clusters, plus it leverages Amazon Authentication for both.
- **Pre-integrated Istio:** It's ready to deploy and use without additional administration.

Cisco Container Platform Architecture Overview

At the bottom of the stack is Level 1, the Networking layer, which can consist of Nexus switches, Application Policy Infrastructure Controllers (APICs), and Fabric Interconnects (FIs).

Level 2 is the Compute layer, which consists of HyperFlex, UCS, or third-party servers that provide virtualized compute resources through VMware and distributed storage resources.

Level 3 is the Hypervisor layer, which is implemented using HyperFlex or VMware.

Level 4 consists of the CCP control plane and data plane (or tenant clusters). In Figure 5-9, the left side shows the CCP control plane, which runs on four control-plane VMs, and the right side shows the tenant clusters. These tenant clusters are preconfigured to support persistent volumes using the vSphere Cloud Provider and Container Storage Interface (CSI) plug-in. Figure 5-9 provides an overview of the CCP architecture.

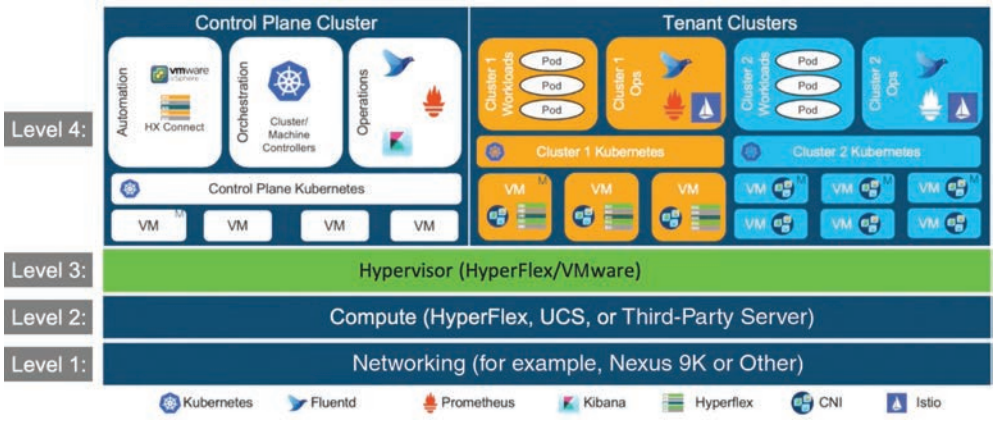


Figure 5-9 *Container Platform Architecture Overview*

Components of Cisco Container Platform

Table 5-2 lists the components of CCP.

Table 5-2 *Components of CCP*

Function	Component
Operating System	Ubuntu
Orchestration	Kubernetes
IaaS	vSphere
Infrastructure	HyperFlex, UCS
Container Network Interface (CNI)	ACI, Contiv, Calico
SDN	ACI
Container Storage	HyperFlex Container Storage Interface (CSI) plug-in
Load Balancing	NGINX, Envoy
Service Mesh	Istio, Envoy
Monitoring	Prometheus, Grafana
Logging	Elasticsearch, Fluentd, and Kibana (EFK) stack
Container Runtime	Docker CE

Sample Deployment Topology

This section describes a sample deployment topology of the CCP and illustrates the network topology requirements at a conceptual level.

In this case, it is expected that the vSphere-based cluster is set up, provisioned, and fully functional for virtualization and virtual machine (VM) functionality before any installation of CCP. You can refer to the standard VMware documentation for details on vSphere installation. Figure 5-10 provides an example of a vSphere cluster on which CCP is to be deployed.

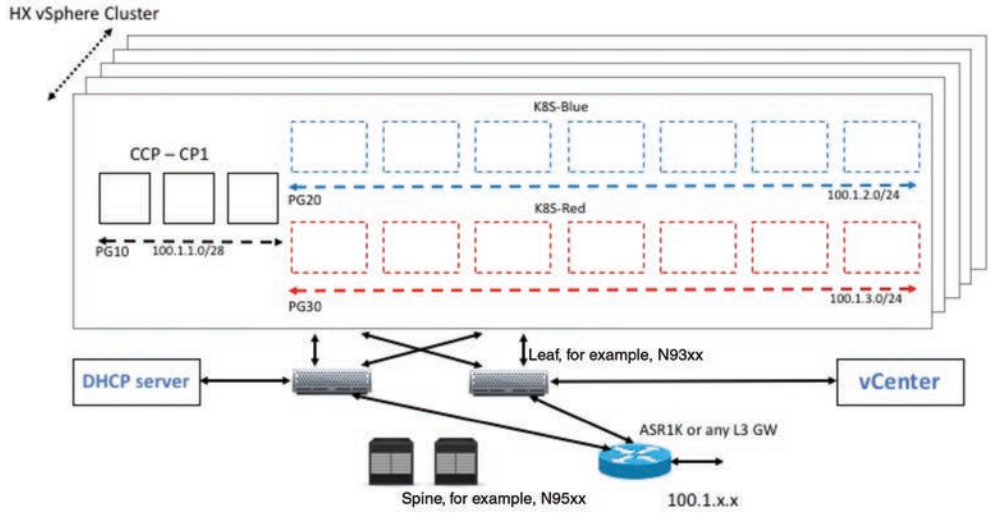


Figure 5-10 *vSphere cluster on which CCP is to be deployed*

Once the vSphere cluster is ready to provision VMs, the admin then provisions one or more VMware port groups (for example, PG10, PG20, and PG30 in the figure) on which virtual machines will subsequently be provisioned as container cluster nodes. Basic L2 switching with VMware vswitch functionality can be used to implement these port groups. IP subnets should be set aside for use on these port groups, and the VLANs used to implement these port groups should be terminated on an external L3 gateway (such as the ASR1K shown in the figure). The control-plane cluster and tenant-plane Kubernetes clusters of CCP can then be provisioned on these port groups.

All provisioned Kubernetes clusters may choose to use a single shared port group, or separate port groups may be provisioned (one per Kubernetes cluster), depending on the isolation needs of the deployment. Layer 3 network isolation may be used between these different port groups as long as the following conditions are met:

- There is L3 IP address connectivity among the port group that is used for the control-plane cluster and the tenant cluster port groups
- The IP address of the vCenter server is accessible from the control-plane cluster
- A DHCP server is provisioned for assigning IP addresses to the installer and upgrade VMs, and it must be accessible from the control-plane port group cluster of the cluster

The simplest functional topology would be to use a single shared port group for all clusters with a single IP subnet to be used to assign IP addresses for all container cluster VMs. This IP subnet can be used to assign one IP per cluster VM and up to four virtual IP addresses per Kubernetes cluster, but would not be used to assign individual Kubernetes pod IP addresses. Hence, a reasonable capacity planning estimate for the size of this IP subnet is as follows:

(The expected total number of container cluster VMs across all clusters) + 3 × (the total number of expected Kubernetes clusters)

Administering Clusters on vSphere

You can create, upgrade, modify, or delete vSphere on-premises Kubernetes clusters using the CCP web interface. CCP supports v2 and v3 clusters on vSphere. The v2 clusters use a single master node for their control plane, whereas the v3 clusters can use one or three master nodes for their control plane. The multimaster approach of v3 clusters is the preferred cluster type, as this approach ensures high availability for the control plane. The following steps show you how to administer clusters on vSphere:

Step 1. In the left pane, click **Clusters** and then click the **vSphere** tab.

Step 2. Click **NEW CLUSTER**.

Step 3. In the **BASIC INFORMATION** screen:

- **a.** From the **INFRASTRUCTURE PROVIDER** drop-down list, choose the provider related to your Kubernetes cluster.

  For more information, see **Adding vSphere Provider Profile**.

- **b.** In the **KUBERNETES CLUSTER NAME** field, enter a name for your Kubernetes tenant cluster.

- **c.** In the **DESCRIPTION** field, enter a description for your cluster.

- **d.** In the **KUBERNETES VERSION** drop-down list, choose the version of Kubernetes that you want to use for creating the cluster.

- **e.** If you are using ACI, specify the ACI profile.

  For more information, see **Adding ACI Profile**.

- **f.** Click **NEXT**.

Step 4. In the **PROVIDER SETTINGS** screen:

- **a.** From the **DATA CENTER** drop-down list, choose the data center that you want to use.

- **b.** From the **CLUSTERS** drop-down list, choose a cluster.

Note Ensure that DRS and HA are enabled on the cluster that you choose. For more information on enabling DRS and HA on clusters, see *Cisco Container Platform Installation Guide*.

c. From the **DATASTORE** drop-down list, choose a datastore.

Note Ensure that the datastore is accessible to the hosts in the cluster.

d. From the **VM TEMPLATE** drop-down list, choose a VM template.

e. From the **NETWORK** drop-down list, choose a network.

Note Ensure that you select a subnet with an adequate number of free IP addresses. For more information, see **Managing Networks**. The selected network must have access to vCenter.

For v2 clusters that use HyperFlex systems:

- The selected network must have access to the HypexFlex Connect server to support HyperFlex Storage Provisioners.
- For HyperFlex Local Network, select **k8-priv-iscsivm-network** to enable HyperFlex Storage Provisioners.

f. From the **RESOURCE POOL** drop-down list, choose a resource pool.

g. Click **NEXT**.

Step 5. In the **NODE CONFIGURATION** screen:

a. From the **GPU TYPE** drop-down list, choose a GPU type.

Note GPU configuration applies only if you have GPUs in your HyperFlex cluster.

b. For v3 clusters, under **MASTER**, choose the number of master nodes as well as their VCPU and memory configurations.

Note You may skip this step for v2 clusters. You can configure the number of master nodes only for v3 clusters.

c. Under **WORKER**, choose the number of worker nodes as well as their VCPU and memory configurations.

d. In the **SSH USER** field, enter the SSH username.

e. In the **SSH KEY** field, enter the SSH public key that you want to use for creating the cluster.

Note Ensure that you use the Ed25519 or ECDSA format for the public key. Because RSA and DSA are less-secure formats, Cisco prevents the use of these formats.

f. In the **ROUTABLE CIDR** field, enter the IP addresses for the pod subnet in the CIDR notation.

g. From the **SUBNET** drop-down list, choose the subnet that you want to use for this cluster.

h. In the **POD CIDR** field, enter the IP addresses for the pod subnet in the CIDR notation.

i. In the **DOCKER HTTP PROXY** field, enter a proxy for the Docker.

j. In the **DOCKER HTTPS PROXY** field, enter an HTTPS proxy for the Docker.

k. In the **DOCKER BRIDGE IP** field, enter a valid CIDR to override the default Docker bridge.

Note If you want to install the HX-CSI add-on, ensure that you set the CIDR network prefix of the **DOCKER BRIDGE IP** field to **/24**.

l. Under **DOCKER NO PROXY**, click **ADD NO PROXY** and then specify a comma-separated list of hosts that you want to exclude from proxying.

m. In the **VM USERNAME** field, enter the VM username that you want to use as the login for the VM.

n. Under **NTP POOLS**, click **ADD POOL** to add a pool.

o. Under **NTP SERVERS**, click **ADD SERVER** to add an NTP server.

p. Under **ROOT CA REGISTRIES**, click **ADD REGISTRY** to add a root CA certificate to allow tenant clusters to securely connect to additional services.

q. Under **INSECURE REGISTRIES**, click **ADD REGISTRY** to add Docker registries created with unsigned certificates.

r. For v2 clusters, under **ISTIO**, use the toggle button to enable or disable Istio.

s. Click **NEXT**.

Step 6. For v2 clusters, to integrate Harbor with CCP:

> **Note** Harbor is currently not available for v3 clusters.

a. In the **Harbor Registry** screen, click the toggle button to enable Harbor.

b. In the **PASSWORD** field, enter a password for the Harbor server administrator.

c. In the **REGISTRY** field, enter the size of the registry in gigabits.

d. Click NEXT.

Step 7. In the **Summary** screen, verify the configuration and then click **FINISH**.

Administering Amazon EKS Clusters Using CCP Control Plane

Before you begin, make sure you have done the following:

- Added your Amazon provider profile.
- Added the required AMI files to your account.
- Created an AWS IAM role for the CCP usage to create AWS EKS clusters.

Here is the procedure for administering Amazon EKS clusters using the CCP control plane:

Step 1. In the left pane, click **Clusters** and then click the **AWS** tab.

Step 2. Click **NEW CLUSTER**.

Step 3. In the **Basic Information** screen, enter the following information:

a. From the **INFRASTUCTURE PROVIDER** drop-down list, choose the provider related to the appropriate Amazon account.

b. From the **AWS REGION** drop-down list, choose an appropriate AWS region.

> **Note** Not all regions support EKS. Ensure that you select a supported region. Currently, CCP supports the ap-northeast-1, ap-northeast-2, ap-southeast-1, ap-southeast-2, eu-central-1, eu-north-1, eu-west-1, eu-west-2, eu-west-3, us-east-1, us-east-2, and us-west-2 regions.

c. In the **KUBERNETES CLUSTER NAME** field, enter a name for your cluster.

d. Click NEXT.

Step 4. In the **Node Configuration** screen, specify the following information:

a. From the **INSTANCE TYPE** drop-down list, choose an instance type for your cluster.

b. From the **MACHINE IMAGE** drop-down list, choose an appropriate CCP Amazon Machine Image (AMI) file.

c. In the **WORKER COUNT** field, enter an appropriate number of worker nodes.

d. In the **SSH PUBLIC KEY** drop-down field, choose an appropriate authentication key.

This field is optional. It is needed if you want to ssh to the worker nodes for troubleshooting purposes. Ensure that you use the Ed25519 or ECDSA format for the public key.

Note Because RSA and DSA are less-secure formats, Cisco prevents the use of these formats.

e. In the **IAM ACCESS ROLE ARN** field, enter the Amazon Resource Name (ARN) information.

Note By default, the AWS credentials specified at the time of Amazon EKS cluster creation (that is, the credentials configured in the Infrastructure Provider) are mapped to the Kubernetes cluster-admin ClusterRole. A default ClusterRoleBinding binds the credentials to the system:masters group, thereby granting superuser access to the holders of the IAM identity. The **IAM ACCESS ROLE ARN** field allows you to specify the ARN of an additional AWS IAM role or IAM user who is also granted administrative control of the cluster.

f. Click **NEXT**.

Step 5. In the **VPC Configuration** screen, specify the following information:

a. In the **SUBNET CIDR** field, enter a value of the overall subnet CIDR for your cluster.

b. In the **PUBLIC SUBNET CIDR** field, enter values for your cluster on separate lines.

c. In the **PRIVATE SUBNET CIDR** field, enter values for your cluster on separate lines.

Step 6. In the **Summary** screen, review the cluster information and then click **FINISH**.

Cluster creation can take up to 20 minutes. You can monitor the cluster creation status on the **Clusters** screen.

Note If you receive the "Could not get token: AccessDenied" error message, this indicates that the AWS account is not a trusted entity for the Role ARN.

Licensing and Updates

You need to configure Cisco Smart Software Licensing on the Cisco Smart Software Manager (Cisco SSM) to easily procure, deploy, and manage licenses for your CCP instance. The number of licenses required depends on the number of VMs necessary for your deployment scenario.

Cisco SSM enables you to manage your Cisco Smart Software Licenses from one centralized website. With Cisco SSM, you can organize and view your licenses in groups called "virtual accounts." You can also use Cisco SSM to transfer the licenses between virtual accounts, as needed.

You can access Cisco SSM from the Cisco Software Central home page, under the Smart Licensing area. CCP is initially available for a 90-day evaluation period, after which you need to register the product.

Connected Model

In a connected deployment model, the license usage information is directly sent over the Internet or through an HTTP proxy server to Cisco SSM.

For a higher degree of security, you can opt to use a partially connected deployment model, where the license usage information is sent from CCP to a locally installed VM-based satellite server (Cisco SSM satellite). Cisco SSM satellite synchronizes with Cisco SSM on a daily basis.

Registering CCP Using a Registration Token

You need to register your CCP instance with Cisco SSM or Cisco SSM satellite before the 90-day evaluation period expires. The following is the procedure for registering CCP using a registration token, and Figure 5-11 shows the workflow for this procedure.

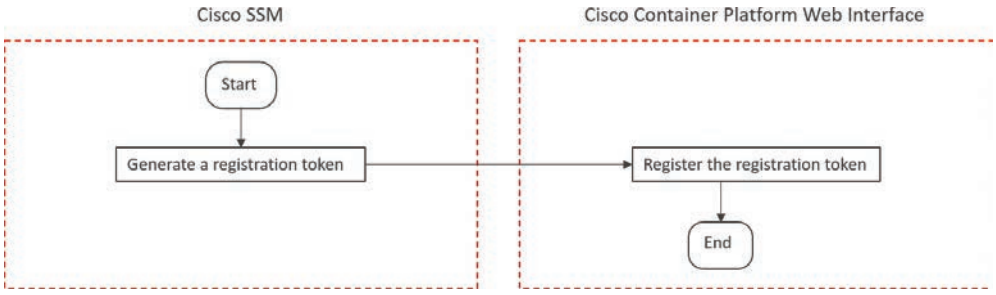


Figure 5-11 *Registering CCP using a registration token*

Step 1. Perform these steps on Cisco SSM or Cisco SSM satellite to generate a registration token:

a. Go to **Inventory** > *Choose Your Virtual Account* > **General** and then click **New Token**.

b. If you want to enable higher levels of encryption for the products registered using the registration token, check the **Allow Export-Controlled functionality on the products registered with this token** check box.

Note This option is available only if you are compliant with the Export-Controlled functionality.

c. Download or copy the token.

Step 2. Perform these steps in the CCP web interface to register the registration token and complete the license registration process:

a. In the left pane, click **Licensing**.

b. In the license notification, click **Register**.

The Smart Software Licensing Product Registration dialog box appears.

c. In the **Product Instance Registration Token** field, enter, copy and paste, or upload the registration token that you generated in Step 1.

d. Click **REGISTER** to complete the registration process.

Upgrading Cisco Container Platform

Upgrading CCP and upgrading tenant clusters are independent operations. You must upgrade CCP to allow tenant clusters to upgrade. Specifically, tenant clusters cannot be upgraded to a higher version than the control plane. For example, if the control plane is at version 1.10, the tenant cluster cannot be upgraded to the 1.11 version.

Upgrading CCP is a three-step process:

You can update the size of a single IP address pool during an upgrade. However, we recommend that you plan ahead for the free IP address requirement by ensuring that the free IP addresses are available in the control-plane cluster prior to the upgrade.

If you are upgrading from a CCP version, you must do the following:

- Ensure that at least five IP addresses are available (3.1.x or earlier).
- Ensure that at least three IP addresses are available (3.2 or later).
- Upgrade the CCP tenant base VM.
- Deploy/upgrade the VM.
- Upgrade the CCP control plane.

To get the latest step-by-step upgrade procedure, you can refer to the CCP upgrade guide.

Cisco Intersight Kubernetes Service

Cisco Intersight Kubernetes Service (IKS) effectively expands CCP's functionality to benefit from Intersight's native infrastructure management capabilities, further simplifying building and managing Kubernetes environments. IKS is a SaaS offering, taking away the hassle of installing, hosting, and managing a container management solution. For organizations with specific requirements, it also offers two additional deployment options (with a virtual appliance). So, let's take a look at how IKS can make our lives easier. Figure 5-12 provides an overview of Intersight Cloud management.

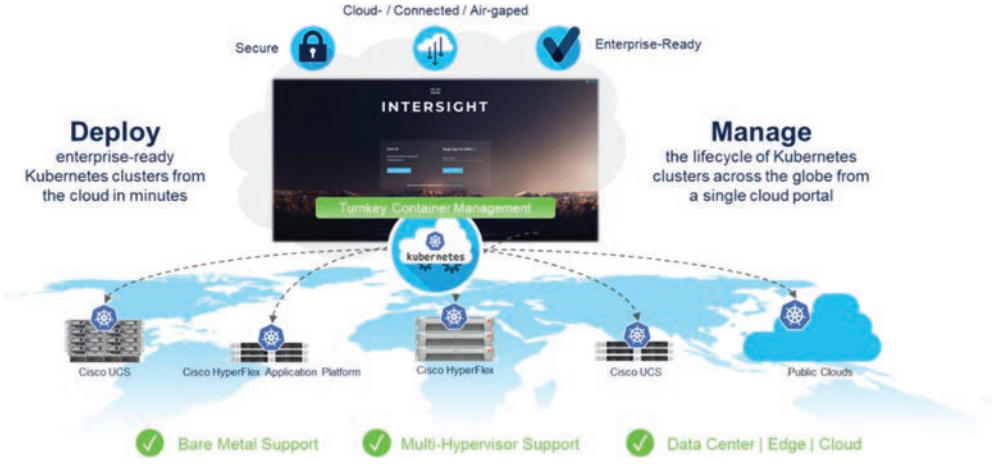


Figure 5-12 *Intersight Cloud management*

Benefits of IKS

The following are the benefits of using IKS:

- Simplify Kubernetes Day 0 to Day N operations and increase application agility with a turnkey SaaS platform that makes it easy to deploy and manage clusters across data centers, the edge, and public clouds.
- Reduce risk, lower cost, improve governance, and take multicloud control on a security-hardened platform, with enhanced availability, native integrations with AWS, Azure, and Google Cloud, and end-to-end industry-leading Cisco TAC support.
- Get more value from your investments with a flexible, extensible Kubernetes platform that supports multiple delivery options, hypervisors, storage, and bare-metal configurations.
- Automate and simplify with self-service built-in add-ons and optimizations such as AI/ML frameworks, service mesh, networking, monitoring, logging, and persistent object storage.

Common Use Case

A good example comes from the retail sector: an IT admin needs to quickly create and configure hundreds of edge locations for the company's retail branches to perform AI/ML processing and a few core ones in privately owned or co-located data centers. The reason it makes sense for processing or storing large chunks of data at the edge is the cost of shipping the data back to the core DC or to a public cloud (and latency to a certain extent).

Creating those Kubernetes clusters would require firmware upgrades as well as OS and hypervisor installations before the IT admin can even get to the container layer. With Cisco Intersight providing a comprehensive, common orchestration and management layer—from server and fabric management to hyperconverged infrastructure management to Kubernetes—creating a container environment from scratch can be literally done with just a few clicks. Figure 5-13 illustrates a high-level architecture of IKS.

IT admins can use either the IKS GUI or its APIs, or they can integrate with an Infrastructure as Code plan (such as HashiCorp's Terraform) to quickly deploy a Kubernetes environment on a variety of platforms—VMware ESXi hypervisors or Cisco HyperFlex—thus enabling significant savings and efficiency without the need of virtualization.

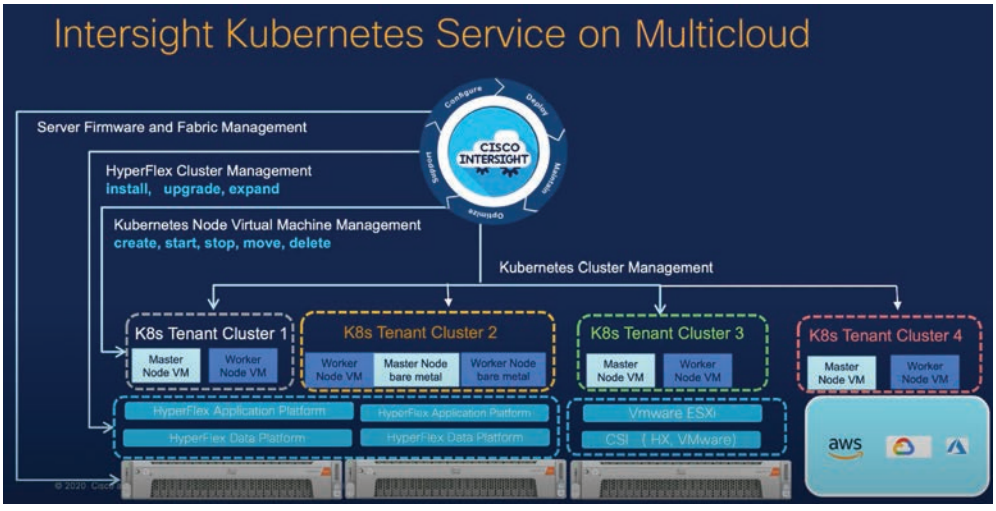


Figure 5-13 *Architecture of IKS*

Deploying Consistent, Production-Grade Kubernetes Anywhere

Few open source projects have been as widely and rapidly adopted as Kubernetes (K8s), the de facto container orchestration platform. With Kubernetes, development teams can deploy, manage, and scale their containerized applications with ease, making innovations more accessible to their continuous delivery pipelines. However, Kubernetes comes with operational challenges, because it requires time and technical expertise to install and configure. Multiple open source packages need to be combined on top of a heterogeneous infrastructure, across on-premises data centers, edge locations, and, of course, public clouds. Installing Kubernetes and the different software components required, creating clusters, configuring storage, networking, and security, optimizing for AI/ML, and other manual tasks can slow down the pace of development and can result in teams spending hours debugging. In addition, maintaining all these moving parts (for example, upgrading, updating, and patching critical security bugs) requires ongoing significant human capital investment.

The solution? Cisco Intersight Kubernetes Service (IKS), a turnkey SaaS solution for managing consistent, production-grade Kubernetes anywhere.

How It Works

Cisco Intersight Kubernetes Service (IKS) is a fully curated, lightweight container management platform for delivering multicloud, production-grade, upstream Kubernetes. Part of the modular SaaS Cisco Intersight offerings (with an air-gapped on-premises option also available), IKS simplifies the process of provisioning, securing, scaling, and managing

virtualized or bare-metal Kubernetes clusters by providing end-to-end automation, including the integration of networking, load balancers, native dashboards, and storage provider interfaces. It also works with all the popular public cloud–managed K8s offerings, integrating with common identity access with AWS Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS) and Google Cloud Google Kubernetes Engine (GKE). IKS is ideal for AI/ML development and data scientists looking for delivering GPU-enabled clusters, and Kubeflow support with a few clicks. It also offers enhanced availability features, such as multimaster (tenant) and self-healing (operator model).

IKS is easy to install in minutes and can be deployed on top of VMware ESXi hypervisors, Cisco HyperFlex Application Platform (HXAP) hypervisors, and/or directly on Cisco HyperFlex Application Platform bare-metal servers, enabling significant savings and efficiency without the need of virtualization. In addition, with HXAP leveraging container-native virtualization capabilities, you can run virtual machines (VMs), VM-based containers, and bare-metal containers on the same platform! Cisco Intersight also offers native integrations with Cisco HyperFlex (HX) for enterprise-class storage capabilities (for example, persistent volume claims and public cloud-like object storage) and Cisco Application Centric Infrastructure (Cisco ACI) for networking, in addition to the industry- standard Container Storage Interface and Container Network Interface (for example, Calico).

Intersight Kubernetes Service integrates seamlessly with the other Cisco Intersight SaaS offerings to deliver a powerful, comprehensive cloud operations platform to easily and quickly deploy, optimize, and lifecycle-manage end-to-end infrastructure, workloads, and applications. Figure 5-14 illustrates the benefits of IKS.

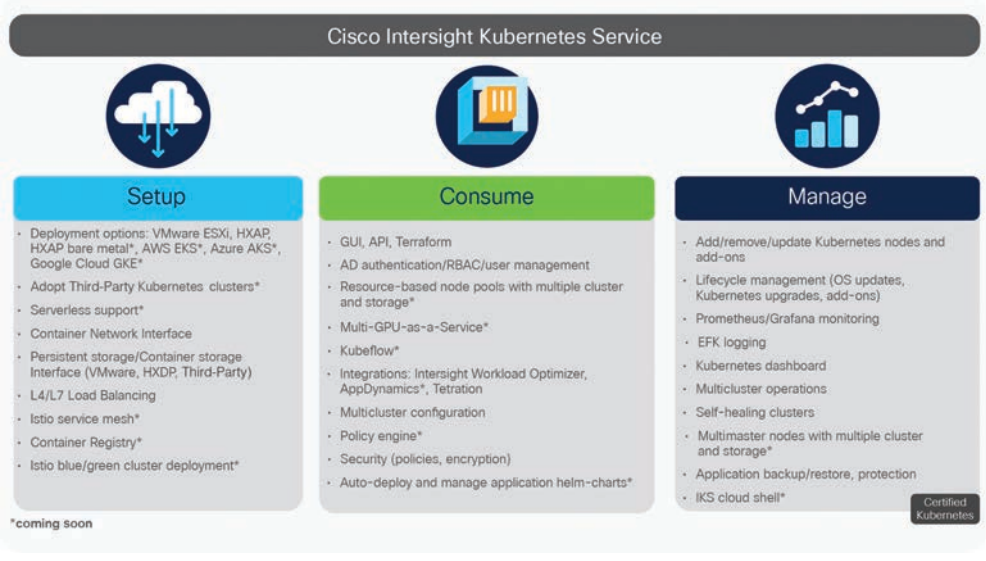


Figure 5-14 *Benefits of IKS*

IKS Release Model

IKS software follows a continuous-delivery release model that delivers features and maintenance releases. This approach enables Cisco to introduce stable and feature-rich software releases in a reliable and frequent manner that aligns with Kubernetes supported releases.

Intersight Kubernetes Service Release and Support Model:

- The IKS team supports releases from N-1 versions of Kubernetes. The team will not fully support/make available IKS versions older than N-1.
- IKS follows a fix-forward model that requires release upgrades to fix issues. Release patches are not necessary with this model.
- Tenant images are versioned according to which version of Kubernetes they contain.

Deploy Kubernetes from Intersight

The Intersight policies allow simplified deployments, as they abstract the configuration into reusable templates. The following sections outline the steps involved in deploying Kubernetes from Intersight.

Step 1: Configure Policies

All policies are created under the **Configure > Polices & Configure > Pools** section on Intersight. You can see the path of the policy at the top of each of the following figures.

1. The IP Pool will be used for IP addresses on your Control and Worker nodes virtual machines, when launched on the ESXi host. Figure 5-15 illustrates the IPv4 Pool details for policy configuration.

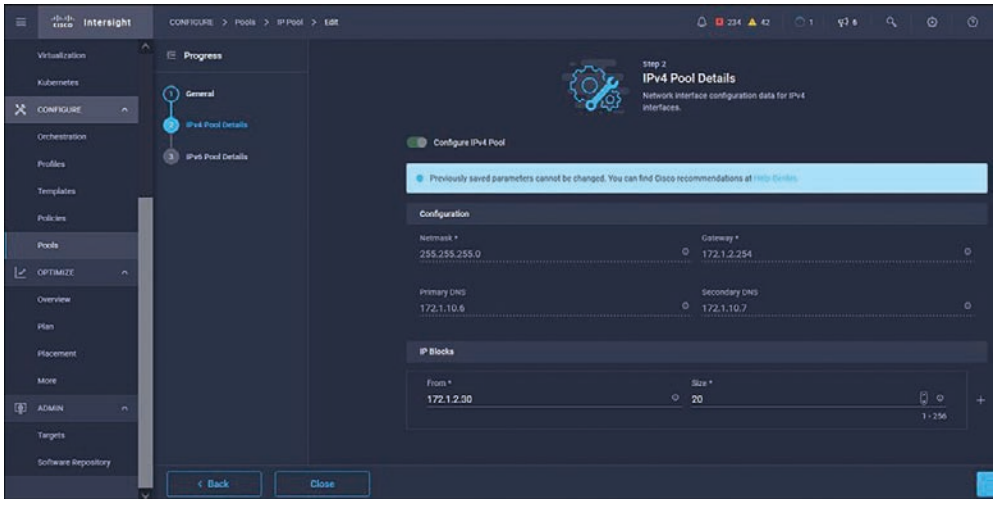


Figure 5-15 *IPv4 Pool details for policy configuration*

2. The Pod and Services Network CIDR is defined for internal networking within the Kubernetes cluster. Figure 5-16 illustrates the CIDR network to be used for the pods and services.

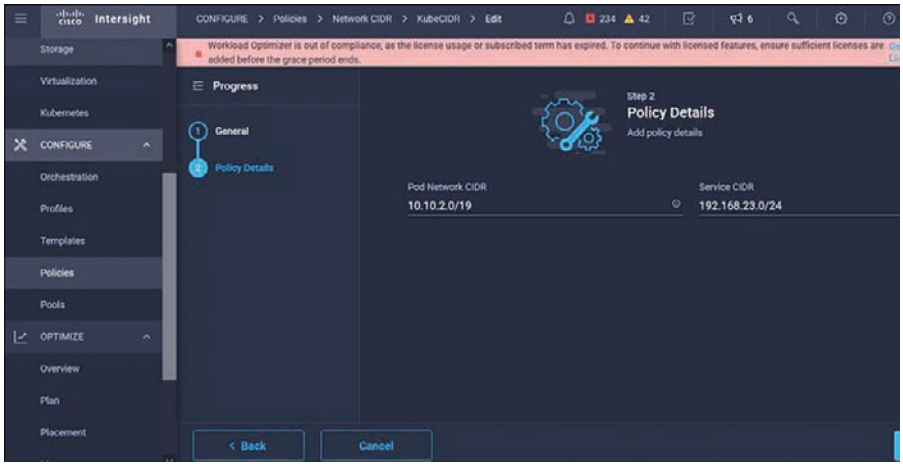


Figure 5-16 *CIDR network to be used for the pods and services*

3. The DNS and NTP configuration policy defines your NTP and DNS configuration (see Figure 5-17).

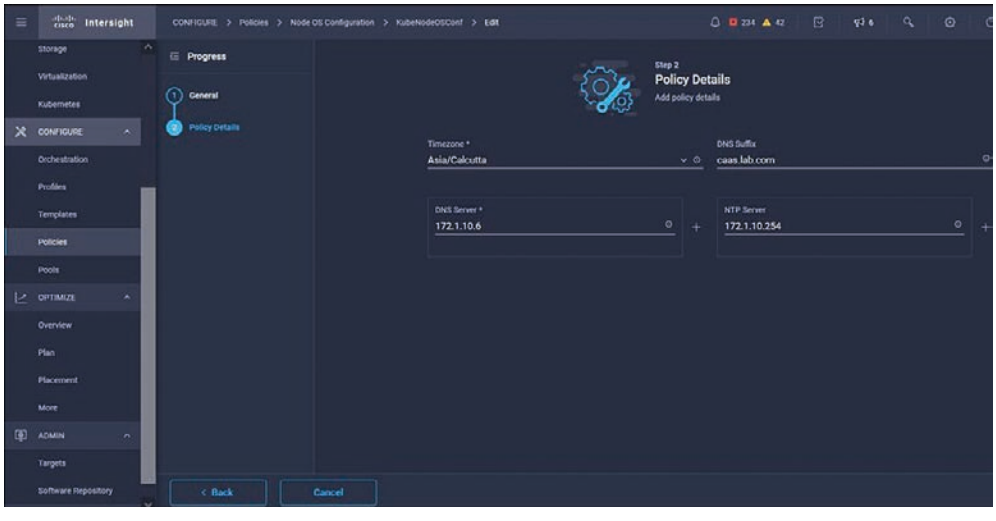


Figure 5-17 *DNS and NTP configuration policy*

4. You can define the proxy configuration policy for your Docker container runtime. Figure 5-18 illustrates this policy.

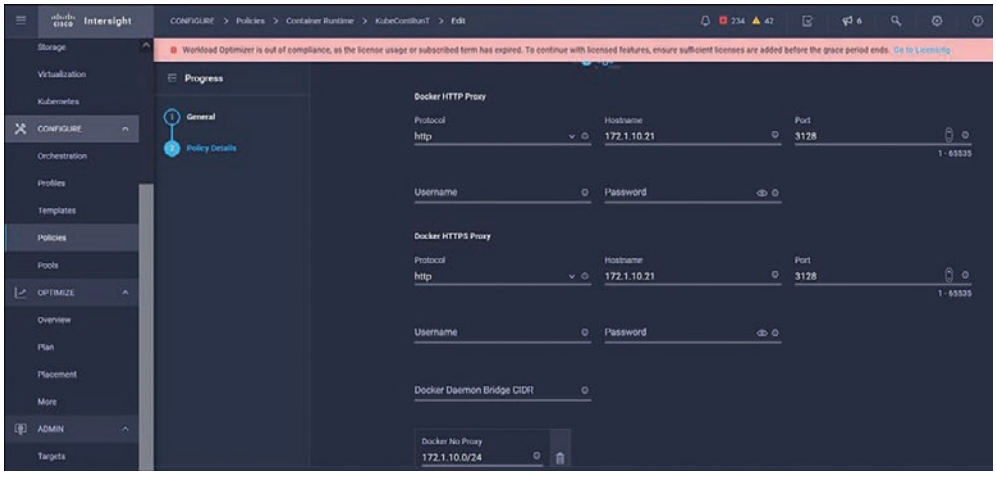


Figure 5-18 *Policy for configuring a proxy for Docker*

5. In the master and worker node VM policy, you define the configuration needed on the virtual machines deployed as Master and Worker nodes (see Figure 5-19).

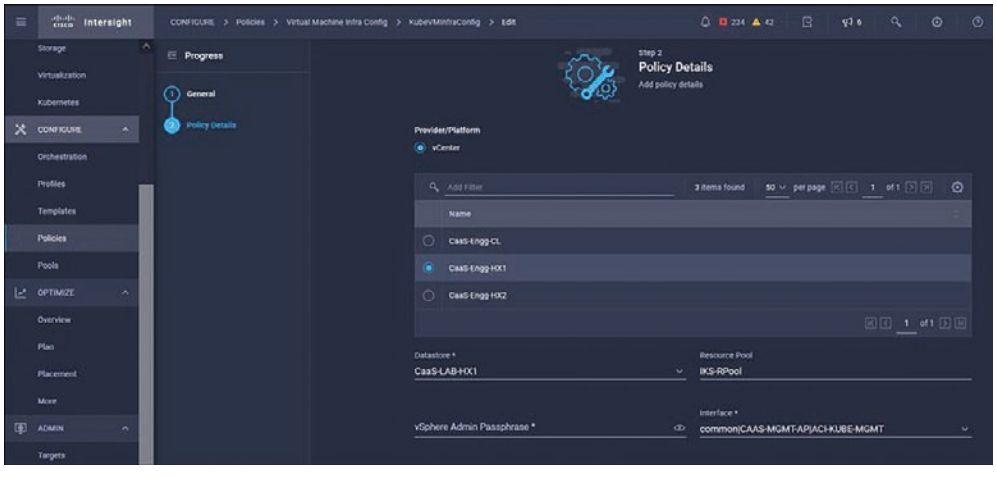


Figure 5-19 *Master and worker node VM policy*

Step 2: Configure Profile

Once we have created the preceding policies, you would then bind them into a profile that you can then deploy.

Deploying the configuration using policies and profiles abstracts the configuration layer so that it can be repeatedly deployed quickly.

1. You can copy this profile and create a new one with modifications on the underlying policies within minutes, to one or more Kubernetes clusters, in a fraction of the time needed for the manual process. Figure 5-20 illustrates the name and tag configuration in the profile.

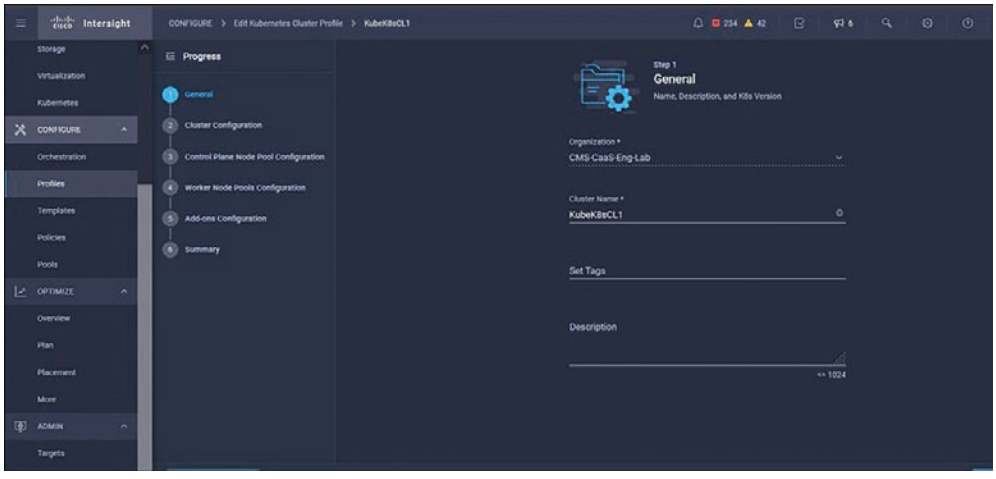


Figure 5-20 *Name and tag configuration in the profile*

2. Set the Pool, Node OS, and Network CIDR policies. You also need to configure a user ID and SSH key (public). Its corresponding private key would be used to ssh into the Master and Worker nodes. Figure 5-21 illustrates the created policies being referred to in the profile.

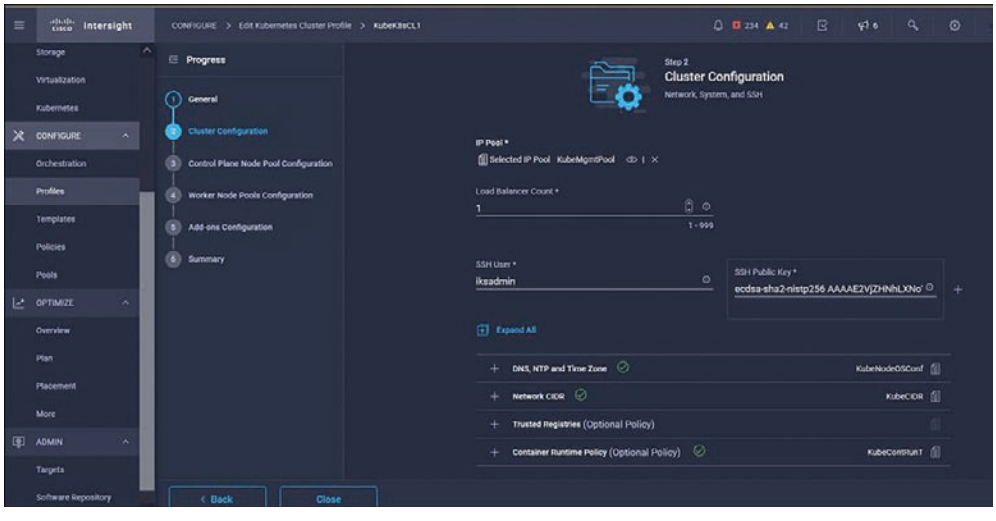


Figure 5-21 *Created policies being referred to in the profile*

3. Configure the control plane. You can define how many Master nodes you would need on the control plane. Figure 5-22 illustrates the K8s cluster configuration and number of Master nodes.

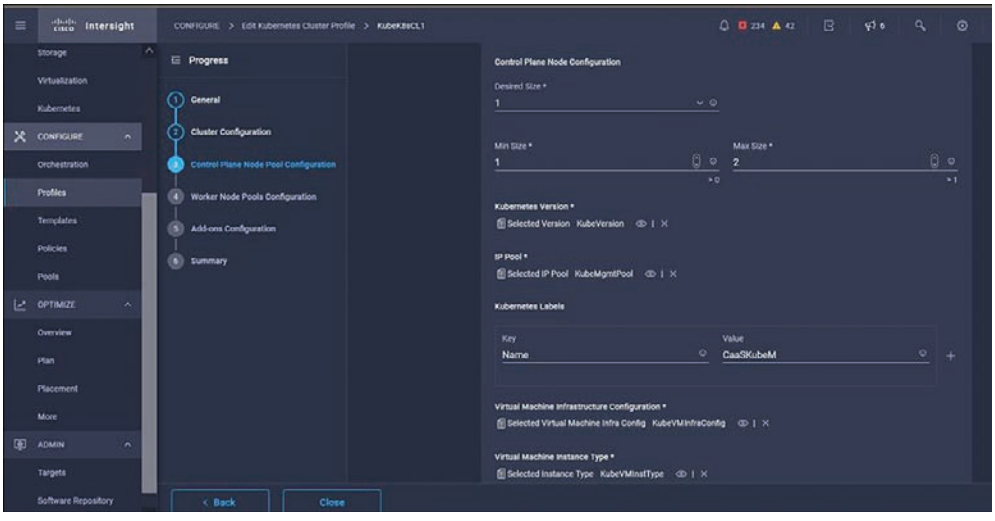


Figure 5-22 *Cluster configuration and number of Master nodes*

4. Configure the Worker nodes. Depending on the application requirements, you can scale up or scale down your Worker nodes. Figure 5-23 illustrates the K8s cluster configuration and number of Worker nodes.

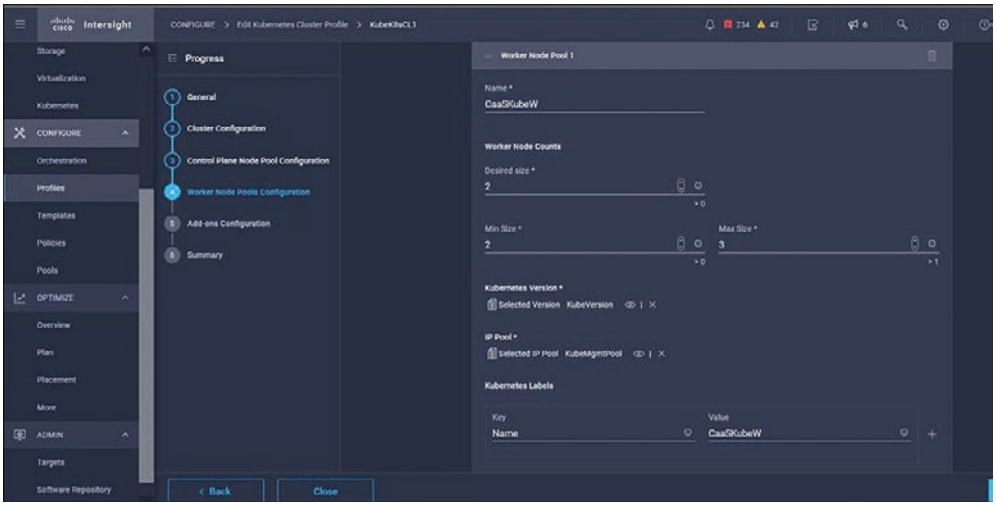


Figure 5-23 *Cluster configuration and number of Worker nodes*

5. Configure add-ons. As of now, you can automatically deploy Kubernetes Dashboard and Graffana with Prometheus monitoring. In the future, you can add more add-ons, which you can automatically deploy using IKS. Figure 5-24 illustrates the K8s cluster add-ons configuration.

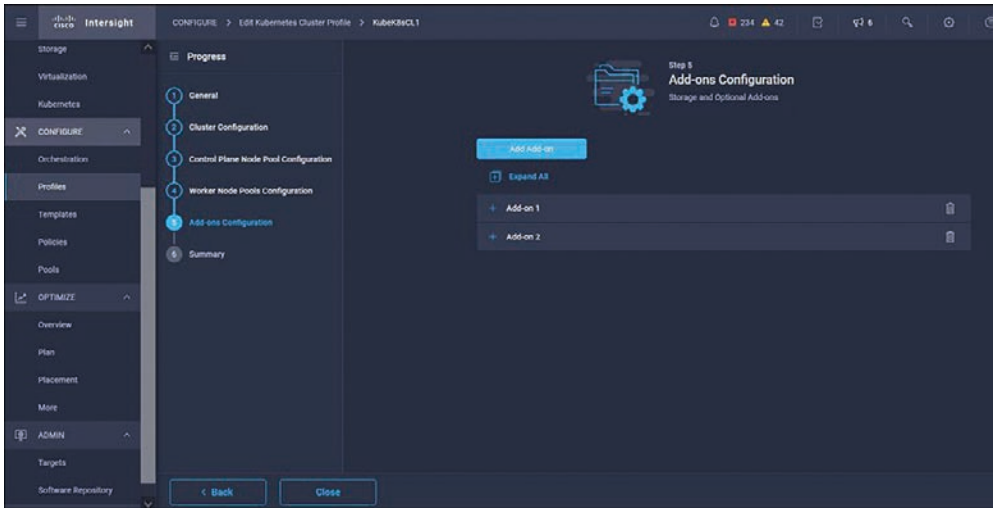


Figure 5-24 *Cluster add-ons configuration*

6. Check the **Summary** and click **Deploy**.

   Figure 5-25 illustrates the K8s cluster **Summary and Deployment** screen.

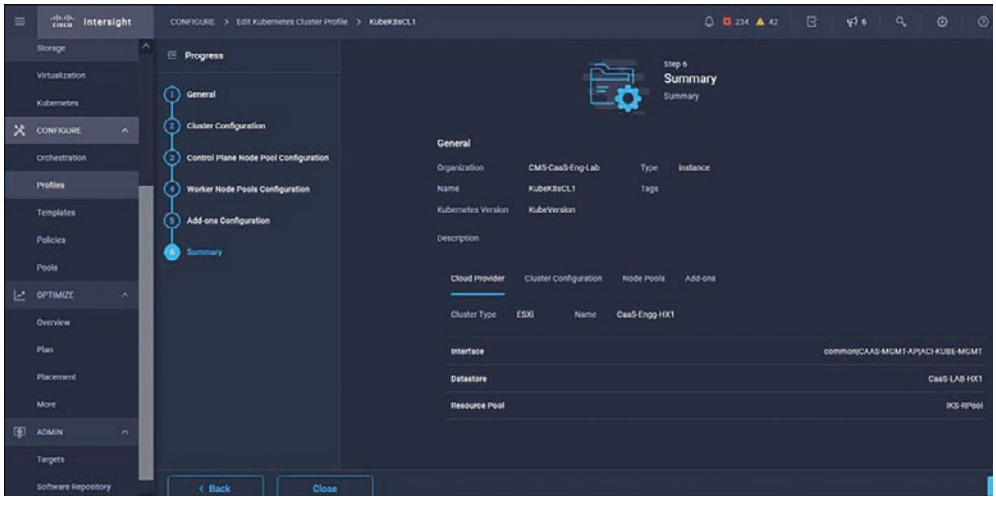


Figure 5-25 *Cluster Summary and Deployment screen*

Summary

Containers are the latest—and arguably one of the most powerful—technologies to emerge over the past few years to change the way we develop, deploy, and manage applications. The days of the massive software release are quickly becoming a thing of the past. In their place are continuous development and upgrade cycles that are allowing a lot more innovation and quicker time to market, with a lot less disruption—for customers and IT organizations alike.

With these new Cisco solutions, you can deploy, monitor, optimize, and auto-scale your applications.

References/Additional Reading

cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight-workload-optimizer/solution-overview-c22-744342.html

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/intersight/217640-configure-deployment-of-kubernetes-clust.html

https://blogs.cisco.com/cloud/ciscocontainerplatform

https://www.cisco.com/c/dam/global/en_uk/products/cloud-systems-management/pdfs/cisco-container-platform-at-a-glance.pdf

https://blogs.cisco.com/cloud/saas-based-kubernetes-lifecycle-management-an-introduction-to-intersight-kubernetes-service?ccid=cc001268

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/at-a-glance-c45-744332.html

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/intersight/217640-configure-deployment-of-kubernetes-clust.html

Index

Numbers

2FA (two-factor authentication), 349–351

5G telco, 18

A

ACI (Application Centric Infrastructure)

ACI Multi-Site, 15

ACI/DNCM sites, adding, 22–24

Cisco NDO (Nexus Dashboard Orchestrator), 86. *See also* NDO (Nexus Dashboard Orchestrator)

Cisco Nexus Dashboard Data Broker integration, 71

Cisco UCS Director integration, 97–103

rapid application deployment, 102–103

secure multitenancy, 102

self-service portal, 102–103

Cloud ACI (Application Centric Infrastructure), 82–91

capabilities of, 83–84

Cisco ACI NDO (Nexus Dashboard Orchestrator), 86

Cisco APIC (Application Policy Infrastructure Controller), 84

Cisco Cloud APIC, 83–84, 86–91

high-level architecture of, 85

hybrid cloud environment challenges, 82–84

EPGs (endpoint groups), 51, 84, 87–88

multitier support, 66

actions, AppDynamics

automation of, 111–112

overview of, 134

activation

of Slido polls, 257–258

of Slido quizzes, 258

adaptive policies, Cisco Duo Security, 356–357

Add Data Destination command, 309

addresses, MAC, 51

Admin Console menu, Sites command, 23

Administrator Designated model, Duo Security Trust Monitor, 353
Advanced Encryption Standard (AES), 253
Advanced Malware Protection (AMP), 74, 337
advisories, Cisco Nexus Dashboard Insights, 48, 60, 65
AES (Advanced Encryption Standard), 253
agents
AppDynamics, 149
NET agent, 149, 177
Java agent, 149, 150, 177
Machine Agent, 147–148, 176–178, 181–183
AppDynamics APM (Application Performance Monitoring), 177
database, 132
EI (Edge Intelligence), 307–308
JavaScript, 148
AI (artificial intelligence)
in Cisco Webex, 240
in Event Analytics, 57
AKS (Azure Kubernetes Service), 230–231
alerts
analysis of. *See* Cisco Nexus Dashboard Insights
Cisco Cloudlock, 318
Cisco Secure Cloud Analytics, 342–343
algorithms
Event Analytics, 57
SHA (Secure Hash Algorithm), 253
Alibaba Cloud, 74, 79
Amazon EBS (Elastic Block Store), 87
Amazon EC2 (Elastic Compute Cloud), 87
Amazon Web Services. *See* AWS (Amazon Web Services)
.ami form factor, 12
AMP (Advanced Malware Protection), 74, 337
Analytics, AppDynamics, 178–180
EUM (End User Monitoring) with, 158–159
Home page, 179–180
overview of, 138, 178–179
analytics and insights. *See also* AppDynamics
Cisco Meraki MX, 74–79
features and benefits of, 75–76
overview of, 74–75
vMX (virtual MX) appliances, 77–79
Cisco Nexus Dashboard Data Broker, 68–73
Cisco ACI (Application Centric Infrastructure) integration, 71
Cisco DNA Center integration, 72
Inline option, 72–73
modes of, 68
monitoring out-of-band and inline network traffic with, 68–69
overview of, 68
scalable traffic monitoring with, 72–73
SPAN Automation-enabled networks, 70
Cisco Nexus Dashboard Insights, 41, 48
advantages of, 42–43
advisories, 60, 65
Analyze Alerts view, 46
Anomalies view, 46–47

AppDynamics. See AppDynamics
application statistics, 56–57
change management, 64
Cisco ACI multitier support, 66
Cisco TAC Assist, 66
Connectivity Analysis, 49–50
custom dashboards, 65
Delta Analysis, 48–49, 64
design of, 41–42
diagnostics and impact, 58–59
email notification support, 43, 66
endpoint analytics, 56, 65
environmental data, 52–53, 65
Event Analytics, 57–58
features and benefits of, 63–66
Firmware Update Analysis, 60–61
flow analytics, 54–55, 64, 66
Kafka messaging support, 43, 66
key components of, 43–45, 46–50
licensing, 45–46
offline analysis, 66
One View capability, 10, 44, 63, 64
one-click remediation, 64
Pre-Change Analysis, 62–63, 64
product usage telemetry, 66
PSIRTs/bugs, 48, 60, 66
recommendations, 58–59
resource utilization, 50–51, 65
statistical data, 53–54, 65
topology view, 65
upgrade assist, 64
Cisco Nexus Insights Cloud Connector, 66–68
Analyze Alerts view, Cisco Nexus Dashboard Insights, 46
anchor metrics, for entities, 145
Android mobile applications, monitoring, 169
Anomalies view, Cisco Nexus Dashboard Insights, 46–47
anomaly detection and analysis
with Cisco Cloudlock, 318
with Cisco Nexus Dashboard Insights, 46–47, 65
AnyConnect, 76, 335–336
APIC (Application Policy Infrastructure Controller)
Cisco Cloud APIC, 83–84, 86–91
First Time Setup Wizard, 88
key functionalities of, 86–88
multitier application deployment, 89
registering Cisco Cloud APIC in NDO, 89
overview of, 83, 84
APIs (application programming interfaces)
Cisco UCS Director, 94
REST, 43, 71, 97
Webex Teams, 275–276
APM (Application Performance Monitoring), 129, 142–154. *See also* AppDynamics
agents, 149
application security monitoring with Cisco Secure Application, 148–154
AppDynamics flow map, 153
Cisco Secure Application architecture, 150–151

Cisco Secure Application components, 149–150
dashboard, 151–152, 154
overview of, 148–149
search filter, 153–154
supported APM agents, 149
tier flow map, 153
backends, 146
business applications, 144
business transactions, 143–144
Database Visibility, 148
entities, 145–146
anchor metrics for, 145
historical, 145
live, 145–146
EUM (End User Monitoring) with, 148, 158
Infrastructure Visibility, 131–132, 134, 147–148, 171–172
Network Visibility, 147, 172–175, 193–196
overview of, 171–172
Server Visibility, 138, 176–178
Log Analytics, 148
nodes, 144
overview of, 130, 142–143
tiers, 144–145
Transaction Analytics, 148
appd-cluster-reader role, 190–192
AppDynamics, 47, 56, 65, 107–108
actions, 134
agents, 149
NET agent, 149, 177
Java agent, 149, 150, 177
Machine Agent, 147–148, 176–178, 181–183
Analytics, 178–180
EUM (End User Monitoring) with, 158–159
Home page, 179–180
overview of, 138, 178–179
APM (Application Performance Monitoring), 142–154
agents, 149
application security monitoring with Cisco Secure Application, 148–154
backends, 146
business applications, 144
business transactions, 143–144
entities, 145–146
EUM (End User Monitoring) with, 148, 158
Log Analytics, 148
nodes, 144
overview of, 142–143
tiers, 144–145
Transaction Analytics, 148
AppDynamics Cloud, 196–198
AWS cloud infrastructure observability, 197–198
Azure cloud infrastructure observability, 198
overview of, 196–197
AppDynamics Controller, 149
application performance monitoring with, 130
baselines and thresholds, 133
browser monitoring
Browser Application Dashboard, 163–164
Browser RUM (Real User Monitoring), 163
Browser Synthetic Monitoring, 163

Resource Performance Dashboard, 165–168
Business iQ, 132
Cisco IWO (Intersight Workload Optimizer) and, 208
cloud application monitoring, 180–196
Docker, 180–185
Kubernetes, 186–196
cloud infrastructure monitoring, 196–198
AWS cloud infrastructure observability, 197–198
Azure cloud infrastructure observability, 198
overview of, 196–197
CWOM (Cisco Workload Optimization Manager)and, 107–108
Database Visibility, 131–132, 148, 169–170
capabilities of, 169
overview of, 138
supported databases, 169–170
supported operating systems, 170
definition of, 129
deployment of, 135–141
deployment models, 136
on-premises deployment architecture, 137–140
overview of, 135–136
platform components and tools, 136–137
requirements for, 136
SaaS deployment architecture, 140–141
EUM (End User Monitoring), 132, 154–169
APM (Application Performance Monitoring) with, 158
Application Analytics, 158–159
browser monitoring, 163–168
capabilities of, 148, 156–157
data storage locations, 140
Experience Journey Map with, 159–162
IoT (Internet of Things) monitoring, 168–169
Mobile RUM (Real User Monitoring), 169
on-premises deployments, 157–163
on-premises installation, 138
overview of, 154–156
platform connections, 139
SaaS EUM Server, accessing, 158
viewing data in, 157
Experience Journey Map, 159–162
accessing, 159
end user events, 160–161
Experience Journey Map dashboard, 159–160
overview of, 159
refresh loops, 162
requirements for, 159
traffic segments, 161–162
extensions, 135
health rules, 134
Infrastructure Visibility, 131–132, 134, 147–148, 171–172
Network Visibility, 147, 172–175, 193–196
overview of, 171–172
Server Visibility, 138, 176–178
integration of, 135

Machine Agent, 147–148, 176–178, 181–183
policies, 134
Security Events widget, 149, 151
tenants, 130
UI (user interface), 130
use metrics, 132–133

AppDynamics Controller, 149

AppDynamics flow map, 153

Application Centric Infrastructure. ***See*** **ACI (Application Centric Infrastructure)**

application container templates, 97–102

Application Performance Monitoring. ***See*** **APM (Application Performance Monitoring)**

Application Policy Infrastructure Controller. ***See*** **APIC (Application Policy Infrastructure Controller)**

application polling, Cisco Webex, 254–259
overview of, 254
in Slido, 256–259
poll activation/deactivation, 257–258
poll creation, 257
poll types, 256–257
quiz activation/deactivation, 258
survey creation, 259
in Webex meetings/webinars, 255–256

Application Resource Management (ARM), 201

application security monitoring with Cisco Secure Application, 148–154
AppDynamics flow map, 153
Cisco Secure Application architecture, 150–151
Cisco Secure Application components, 149–150
dashboard, 151–152, 154
overview of, 148–149
search filter, 153–154
supported APM agents, 149
tier flow map, 153

application-level reports, Cisco Cloudlock, 325

applications. ***See also*** **ACI (Application Centric Infrastructure); APIC (Application Policy Infrastructure Controller); AppDynamics;** ***individual apps***
ARM (Application Resource Management), 201
blocking with Cisco Cloudlock, 326–327
business, 144
Cisco Nexus Dashboard Insights, 56–57
governance with Cisco Cloudlock, 318
monitoring with APM (Application Performance Monitoring). *See* APM (Application Performance Monitoring)
monitoring with Cisco Secure Application, 148–154
AppDynamics flow map, 153
Cisco Secure Application architecture, 150–151
Cisco Secure Application components, 149–150
dashboard, 151–152, 154
overview of, 148–149
search filter, 153–154

supported APM agents, 149
tier flow map, 153
polling with Cisco Webex, 254–259
overview of, 254
in Slido, 256–259
in Webex meetings/webinars, 255–256
rapid application deployment, 102–103
security with Cisco Cloudlock, 317–318
sharing in Cisco Webex events, 263–264
Applications page, Cisco Secure Application dashboard, 154
approval, Cisco UCS Director, 96
AppSec, 148–154
ARM (Application Resource Management), 201
artificial intelligence. *See* AI (artificial intelligence)
asset management, EI (Edge Intelligence), 308–309
Attack Pattern model, Duo Security Trust Monitor, 353
Attacks page, Cisco Secure Application dashboard, 154
audio preferences, Cisco Webex, 245
audit logs, 58
authentication
Cisco Duo Security, 349–351
multifactor, 7, 349–351
Webex Teams, 282
automation
of actions, 111–112
Cisco NDFC (Nexus Dashboard Fabric Controller), 26
Cisco UCS Director, 97
AWS (Amazon Web Services), 74
.ami form factor, 12
Cisco Cloud APIC (Application Policy Infrastructure Controller) on, 86–91
First Time Setup Wizard, 88
key functionalities, 86–88
multitier application deployment, 89
registering Cisco Cloud APIC in NDO, 89
cloud infrastructure observability, 197–198
CloudTrail Event Watchlist, 346
EKS (Elastic Kubernetes Service), 224–226, 229, 230–231
Marketplace, vMX offer on, 79
public cloud monitoring configuration for, 343–344
targets, claiming, 214
Azure, 74
AKS (Azure Kubernetes Service), 230–231
Azure Activity Log Watchlist, 347
cloud infrastructure observability, 198
Microsoft Azure (.arm) form factor, 12
public cloud monitoring configuration for, 345–346
vMX (virtual MX) appliance configuration for, 78

B

backends, 146
baselines, AppDynamics, 133
BDs (bridge domains), 51, 87–88

BGP (Border Gateway Protocol), Cisco Nexus Dashboard Insights, 47
blocking applications, with Cisco Cloudlock, 326–327
Border Gateway Protocol (BGP), Cisco Nexus Dashboard Insights, 47
bots, Cisco Webex, 266–268
adding, 266–267
removing, 268
support, 266
bridge domains (BDs), 51, 87–88
bridge-domain subnets, 87–88
bring-your-own-license (BYOL), 87
Browser Application Dashboard, 163–164
Geo tab, 164
Overview tab, 163–164
browser monitoring, 163–168
Browser Application Dashboard, 163–164
Geo tab, 164
Overview tab, 163–164
Browser RUM (Real User Monitoring), 163
Browser Synthetic Monitoring, 163
Resource Performance Dashboard, 165–168
capabilities of, 165
maximizing effectiveness of, 168
Overview tab, 166
Resources tab, 167–168
Violations tab, 166–167
Browser RUM (Real User Monitoring), 163
Browser Synthetic Monitoring, 163
budget management, CWOM (Cisco Workload Optimization Manager) settings, 115
business applications, 144
Business iQ, 132
business transactions, 143–144
BYOL (bring-your-own-license), 87

C

CaaS (containers as a service), 125–127
calendar, starting Cisco Webex Meetings from, 247
Calico. *See* HX (HyperFlex)
calls, Webex, 241–243
AI (artificial intelligence) in, 240
Cloud Calling, 241–243
Cloud Service Architecture, 268–269
Events, 259–264
features and benefits of, 239–240
integrations, 265–268
Meetings, 244–250
Messaging, 249–253
Polling, 254–259
security model, 243–244
Webex Assistant, 240
Webex Teams
for cloud-registered Webex devices, 283–284
data protection, 273–281
for on-premises registered Webex devices, 284–285
proximity and device pairing, 282–285
security and deployment, 269–273
single sign-on, 281–282

SSO (single sign-on), 281–282
with Wi-Fi, 285
capacity planning, with Cisco Nexus Dashboard Insights, 42
CASBs (cloud access security brokers), 314, 323, 328–329, 337. ***See also*** **Cisco Cloudlock**
Cisco Meraki MX, 76
Cisco Umbrella, 331
CCP (Cisco Container Platform), 213, 215–228
architecture of, 218–219
cluster administration on AWS EKS (Elastic Kubernetes Service), 224–226
cluster administration on vSphere, 221–224
components of, 219
deployment of, 219–221
licensing, 226
overview of, 215–218
registering with registration tokens, 226–227
upgrading, 227–228
use cases, 217–218
Centralized mode, Cisco Nexus Dashboard Data Broker, 68
change management, with Nexus Dashboard Insights, 44, 64
CIP (Common Industrial Protocol), 289
Cisco ACI (Application Centric Infrastructure)
ACI Multi-Site, 15
ACI/DNCM sites, adding, 22–24
Cisco NDO (Nexus Dashboard Orchestrator). *See* NDO (Nexus Dashboard Orchestrator)
Cisco Nexus Dashboard Data Broker integration, 71
Cisco UCS Director integration, 97–103
rapid application deployment, 102–103
secure multitenancy, 102
self-service portal, 102–103
Cloud ACI (Application Centric Infrastructure), 82–91
capabilities of, 83–84
Cisco ACI NDO (Nexus Dashboard Orchestrator), 86
Cisco APIC (Application Policy Infrastructure Controller), 84
Cisco Cloud APIC, 83–84, 86–91
high-level architecture of, 85
hybrid cloud environment challenges, 82–84
Cloud Nexus Dashboard Orchestrator, 86
EPGs (endpoint groups), 51, 84, 87–88
multitier support, 66
Cisco ACI mode, Cisco Nexus Dashboard Data Broker, 68
Cisco AMP (Advanced Malware Protection), 74, 337
Cisco APIC (Application Policy Infrastructure Controller)
Cisco Cloud APIC, 83–84, 86–91
First Time Setup Wizard, 88
key functionalities of, 86–88
multitier application deployment, 89
registering Cisco Cloud APIC in NDO, 89
overview of, 83, 84

Cisco Cloud ACI (Application Centric Infrastructure), 82–91
capabilities of, 83–84
Cisco ACI NDO (Nexus Dashboard Orchestrator), 86
Cisco Cloud APIC, 83–84, 86–91
First Time Setup Wizard, 88
key functionalities of, 86–88
multitier application deployment, 89–91
registering Cisco Cloud APIC in NDO, 89
high-level architecture of, 85
hybrid cloud environment challenges, 82–84
Cisco Cloud APIC (Application Policy Infrastructure Controller), 83–84, 86–91
First Time Setup Wizard, 88
key functionalities of, 86–88
multitier application deployment, 89
registering Cisco Cloud APIC in NDO, 89
Cisco Cloud Security
Cisco Cloudlock, 314–328
app security, 317–318
CASB (cloud access security broker), 323
dashboard, 324
data security, 316–317
DNS-layer security, 322
enabling via WSA, 318–321
evolution of, 322–325
firewalls, 323
interactive threat intelligence, 323
log files for shadow IT visibility, 324
overview and trending information, 324
overview of, 314–315
SDWAN integration, 324
secure web gateway, 323
timeline of, 322
user security, 315–316
Cisco Duo Security, 348–359
adaptive policies in, 356–357
Duo Network Gateway, 358
MFA (multifactor authentication), 349–351
overview of, 348–349
secure user access in, 357–359
Trust Monitor, 351–355
Cisco Secure Cloud Analytics, 337–348
alerts and analysis, 342–343
benefits of, 337–339
business advantages of, 340–341
dashboard, 347–348
deployment of, 341
dynamic entity modeling, 341–342
overview of, 339–341
public cloud monitoring configuration, 342–346
watchlist configuration, 346–347
Cisco Umbrella, 328–337
benefits of, 329–332
deployment of, 333
integrations, 333–336
overview of, 328–329
packages, 336–337
overview of, 313
shadow IT challenge, 313–314

Cisco Cloudlock, 314–328
app security, 317–318
application blocking, 326–327
application-level reports, 325
Composite Risk Score, 327–328
dashboard, 317
data security, 316–317
risk mitigation, 316–317
sensitive information, 316
enabling via WSA, 318–321
evolution of, 322–325
CASB (cloud access security broker), 323
dashboard, 324
DNS-layer security, 322
firewalls, 323
interactive threat intelligence, 323
log files for shadow IT visibility, 324
overview and trending information, 324
SDWAN integration, 324
secure web gateway, 323
timeline of, 322
optimization, 325–326
overview of, 314–315
UEBA (User and Entity Behavior Analytics), 316
use cases, 318
user security, 315–316
Cisco Container Platform. *See* CCP (Cisco Container Platform)
Cisco Data Center Network Manager (DCNM), 15. *See also* Cisco NDFC (Nexus Dashboard Fabric Controller)
Cisco data center orchestration. *See* data center orchestration
Cisco DCM (Data Control Module), 292, 294–296
Cisco DCN (Data Center Networking) licensing, 11–12, 45–46
Cisco DCNM (Data Center Network Manager), 15, 83
Cisco DNA Center, 72
Cisco Duo Security, 348–359
adaptive policies in, 356–357
Cisco Umbrella integration with, 335–336
Duo Network Gateway, 358
MFA (multifactor authentication), 349–351
overview of, 348–349
secure user access in, 357–359
remote access enablement, 357–358
SSO (single sign-on), 358–359
VPN-less remote access, 358
Trust Monitor, 351–355
models, 353
risk profiles, 353–355
telemetry, 352–353
Cisco Edge Intelligence Solution, 297
Cisco EFM (Edge and Fog Processing Module), 292, 296
Cisco ENFV (Enterprise Network Functions Virtualization), 75
Cisco GMM (Gateway Management Module), 292–294
Cisco HyperFlex Application Platform (HXAP), 231
Cisco HyperFlex (HX), 116–127, 229, 231
deployment of, 122–124
HXAP (HyperFlex Application Platform), 231
HXDP (Hyperflex Data Platform), 125

key functionalities of, 119–120
systems architecture of, 120
Cisco Intersight
benefits of, 118–119
Cisco Intersight Workload Optimizer, 115, 204–215
AppDynamics and, 208
AWS (Amazon Web Services) targets, claiming, 214
benefits of, 204
capabilities of, 214
CWOM-to-IWO migration, 205–206
Economic Scheduling Engine, 209
how it works, 209–210
hybrid cloud optimization with, 206–209
market and virtual currency, 210–212
risk index, 212
supply chain, 212
Cisco IWE (Intersight Workload Engine), 125–127
benefits of, 126
full stack integration, 125
key features of, 126–127
overview of, 125
deployment options, 117–118
HyperFlex, 116–127, 229, 231
deployment of, 122–124
HXAP (HyperFlex Application Platform), 231
HXDP (Hyperflex Data Platform), 125
key functionalities of, 119–120
systems architecture of, 120
IKS (Intersight Kubernetes Service), 125–127, 228–237
login page, 116
MaaS (Management as a Service), 117
overview of, 116–117
Cisco IoT Solution
EDM (Edge Device Manager), 298–305
IR device onboarding, 301–304
SDO (Secure Device Onboarding) architecture, 304
SEA (Secure Equipment Access), 305
seamless device onboarding, 304
SIM card activation, 304
summary steps, 305
supported device interfaces for onboarding, 300
EI (Edge Intelligence), 305–308
agent management, 307–308
asset management, 308–309
configuration lifecycle management in, 307
data destinations, adding, 309–310
edge-to-multicloud data flow, 306
licensing, 311
overview of, 305–306
overview of, 298
Cisco IWE (Intersight Workload Engine), 125–127
benefits of, 126
full stack integration, 125
key features of, 126–127
overview of, 125

Cisco IWO (Intersight Workload Optimizer), 204–215
AppDynamics and, 208
AWS (Amazon Web Services) targets, claiming, 214
benefits of, 204
capabilities of, 214
CWOM-to-IWO migration, 205–206
Economic Scheduling Engine, 209
how it works, 209–210
hybrid cloud optimization with, 206–209
market and virtual currency, 210–212
risk index, 212
supply chain, 212
Cisco Kinetic platform, 289–296
benefits of, 291–292
DCM (Data Control Module), 292, 294–296
EFM (Edge and Fog Processing Module), 292, 296
features of, 291–292
GMM (Gateway Management Module), 292–294
key functions of, 291
overview of, 289–296
Cisco Meraki MX, 74–79
features and benefits of, 75–76
overview of, 74–75
vMX (virtual MX) appliances, 77–79
configuration for Alibaba Cloud, 79
configuration for GCP (Google Cloud Platform), 78
configuration for Microsoft Azure, 78
features and functionality of, 77–79
Cisco NDFC (Nexus Dashboard Fabric Controller), 5–6, 25–33
benefits of, 27
Cisco NDFC app, 28
comprehensive management with, 25–26
DIRL (dynamic ingress rate limiting), 32–33
fabric builder for IPFM, 31
Fabric Discovery capability, 29
fabric topology view, 29
feature manager, 29
image management, 30–31
multitenancy VRF, 31
non-Nexus platform support, 31
optics information for SAN interfaces, 33
programmable reports, 31
RBAC (role-based access control), 31
SAN Insights, 31–32
SAN zoning interface, 33
SLP (Smart Licensing Policy), 31
topology view, 28
Cisco NDO (Nexus Dashboard Orchestrator), 5, 14–25
for Cisco ACI Multi-Site, 15
for Cisco DCNM Multi-Site, 15
common use cases for, 15–18
Cisco NDO multidomain integrations, 16
data center interconnectivity, 16
hybrid cloud and multicloud, 18
large-scale data center deployment, 15
service provider/5G telco, 18
deployment of, 21–24

ACI/DNCM sites, adding, 22–24
Cisco NDO app on Nexus Dashboard, 22
services communication with APIC nodes, 21
site management, 24–25
functions provided by, 19–21, 84
overview of, 14–15
site management with, 24–25
Cisco Network Function Virtualization Infrastructure Software (NFVIS), 74
Cisco Nexus Dashboard. ***See also*** **Cisco Nexus Dashboard Insights**
Cisco DCN licensing, 11–12, 45–46
Cisco Nexus Dashboard Orchestrator, 5, 14–25
for Cisco ACI Multi-Site, 15
for Cisco DCNM Multi-Site, 15
Cisco NDO app, 22
common use cases for, 15–18
deployment of, 21–24
functions provided by, 19–21
multidomain integrations, 16
overview of, 14–15
registering Cisco Cloud APIC in, 89
site management with, 24–25
common infrastructure services, 10
components of, 4–5
Data Broker service, 5, 68–73
Cisco ACI (Application Centric Infrastructure) integration, 71
Cisco DNA Center integration, 72
Inline option, 72–73
modes of, 68
monitoring out-of-band and inline network traffic with, 68–69
overview of, 68
scalable traffic monitoring with, 72–73
SPAN Automation-enabled networks, 70
feature and benefits of, 6–10
form factors, 12–13
GUI (graphical user interface), 6
hardware versus software stack, 11
NDFC (Nexus Dashboard Fabric Controller), 5–6, 25–33
benefits of, 27
Cisco NDFC app, 28
comprehensive management with, 25–26
DIRL (dynamic ingress rate limiting), 32–33
fabric builder for IPFM, 31
Fabric Discovery capability, 29
fabric topology view, 29
feature manager, 29
image management, 30–31
multitenancy VRF, 31
non-Nexus platform support, 31
optics information for SAN interfaces, 33
programmable reports, 31
RBAC (role-based access control), 31
SAN Insights, 31–32
SAN zoning interface, 33
SLP (Smart Licensing Policy), 31
topology view, 28
One View capability, 7, 44
overview of, 4–5

personas, 8–9
platform support information, 33–34
programmable infrastructure, 10
server requirements, 34
SSO (single sign-on), 7, 8
third-party applications, 5–6, 34–38
HashiCorp Terraform, 35
Red Hat Ansible, 35
ServiceNow, 35, 37–38
Splunk, 35–37
Cisco Nexus Dashboard Insights, 5, 41, 43, 65
advantages of, 42–43
advisories, 48, 60, 65
Analyze Alerts view, 46
Anomalies view, 46–47
AppDynamics. *See* AppDynamics
application statistics, 56–57
change management, 64
Cisco ACI multitier support, 66
Cisco TAC Assist, 66
Cloud Connector, 66–68
Connectivity Analysis, 49–50
custom dashboards, 65
Delta Analysis, 48–49, 64
design of, 41–42
diagnostics and impact, 58–59
email notification support, 43, 66
endpoint analytics, 47, 56, 65
environmental data, 52–53, 65
Event Analytics, 57–58
features and benefits of, 63–66
Firmware Update Analysis, 60–61
flow analytics, 54–55, 64, 66
Kafka messaging support, 43, 66
key components of, 43–45, 46–50
licensing, 45–46
offline analysis, 66
One View capability, 7, 10, 44, 63, 64
one-click remediation, 64
Pre-Change Analysis, 62–63, 64
product usage telemetry, 66
PSIRTs/bugs, 48, 60, 66
recommendations, 58–59
resource utilization, 50–51, 65
statistical data, 53–54, 65
topology view, 65
upgrade assist, 64
Cisco Nexus Dashboard Insights, hybrid site support, 63
Cisco Secure Application, 148–154
AppDynamics flow map, 153
architecture, 150–151
components of, 149–150
dashboard, 151–152, 154
overview of, 148–149
search filter, 153–154
supported APM agents, 149
tier flow map, 153
Cisco Secure Cloud Analytics, 337–348
alerts and analysis, 342–343
benefits of, 337–339
business advantages of, 340–341
dashboard, 347–348
deployment of, 341
dynamic entity modeling, 341–342
overview of, 339–341
public cloud monitoring configuration
for AWS (Amazon Web Services), 343–344
for GCP (Google Cloud Platform), 344–345
for Microsoft Azure, 345–346

watchlist configuration, 346–347
AWS CloudTrail Event Watchlist, 346
Azure Activity Log Watchlist, 347
overview of, 346
Cisco TAC (Technical Assistance Center), 66, 118, 125
Cisco Talos, 75
Cisco TelePresence Video Communication Server, 282–284
Cisco Tetration, 107
Cisco UCS (Unified Computing System) Director, 92–103
application container templates, 97–102
automation, 97
Cisco ACI integration, 97–103
rapid application deployment, 102–103
secure multitenancy, 102
self-service portal, 102–103
Cisco UCS management through, 95–96
configuration/administration, 95
monitoring/reporting, 95
components of, 95–97
End User Portal, 97–102
IaaS (Infrastructure as a Service), 97–102
infrastructure configuration and management, 94
key functionalities of, 92–93
orchestration, 95–97
components, 95–96
workflows, 97–102
policies, 97–102
servers, 11
system overview, 93
Cisco Umbrella, 328–337
benefits of, 329–332
CASB (cloud access security broker), 331
DNS-layer security, 329
firewalls, 331
interactive threat intelligence, 332
SD-WAN integration, 332
secure web gateway, 330
deployment of, 333
DNS-layer security, 329, 336, 337
evolution of, 322–325
CASB (cloud access security broker), 323
dashboard, 324
DNS-layer security, 322
firewalls, 323
interactive threat intelligence, 323
log files for shadow IT visibility, 324
overview and trending information, 324
SDWAN integration, 324
secure web gateway, 323
timeline of, 322
integrations, 333–336
Cisco Duo, 335–336
SD-WAN, 334–335
SecureX, 334–335
overview of, 328–329
packages, 336–337
Cisco Unified CM, 282–284
Cisco Validated Design (CVD) templates, 298

Cisco Webex
AI (artificial intelligence) in, 240
Cloud Calling, 241–243
Cloud Service Architecture, 268–269
Events, 259–264
joining, 261–262
overview of, 259
recording, 262–263
registering for, 260–261
scheduling, 260
sharing content in, 263–264
sharing multiple applications in, 264
features and benefits of, 239–240
integrations, 265–268
adding, 266–267
bots, 266–268
overview of, 265–266
removing, 267
support, 266
Meetings, 244–250
audio/video preferences, 245
joining, 261–262
overview of, 244
polling in, 255–256
recording, 262–263
security features for, 248–249
starting meetings in, 246–247
upcoming meetings, viewing, 247
Messaging, 249–253
organizing messages in, 251
overview of, 249
reading/responding to messages in, 251
security features, 253
sending messages in, 250
Polling, 254–259
overview of, 254
in Slido, 256–259
in Webex meetings/webinars, 255–256
security model, 243–244
Webex Assistant, 240
Webex Teams
for cloud-registered Webex devices, 283–284
data protection, 273–281
increasing effectiveness of, 105–106
for on-premises registered Webex devices, 284–285
proximity and device pairing, 282–285
security and deployment, 269–273
single sign-on, 281–282
SSO (single sign-on), 281–282
with Wi-Fi, 285
Cisco Workload Optimization Manager. ***See*** **CWOM (Cisco Workload Optimization Manager)**
Citrix XenServer, 105–106
claiming AWS (Amazon Web Services) targets, 214
client VPN, 74
cloud access security brokers. ***See*** **CASBs (cloud access security brokers)**
Cloud ACI (Application Centric Infrastructure), 82–91
on AWS (Amazon Web Services), 85
capabilities of, 83–84
Cisco ACI NDO (Nexus Dashboard Orchestrator), 86

Cisco APIC (Application Policy Infrastructure Controller), 84
Cisco Cloud APIC, 83–84, 86–91
First Time Setup Wizard, 88
key functionalities of, 86–88
multitier application deployment, 89
registering Cisco Cloud APIC in NDO, 89
high-level architecture of, 85
hybrid cloud environment challenges, 82–84
cloud application monitoring, 180–196
Docker, 180–185
container metrics, viewing, 183–185
container monitoring configuration, 183
container monitoring deployment, 181–182
Metric Browser, 183–185
overview of, 180
Kubernetes, 186–196
AppDynamics Machine Agent deployment on, 189–190
ClusterRole configuration, 190–192
container IDs, registering as host IDs, 188–189
Container Visibility with, 186–188
Docker Visibility with, 186
instrumenting applications with, 189
Network Visibility with, 193–196
overview of, 186
Cloud Calling, Webex, 241–243
Cloud Foundry, 105–106
cloud infrastructure monitoring, 196–198
AWS cloud infrastructure observability, 197–198
Azure cloud infrastructure observability, 198
overview of, 196–197
Cloud Security. *See* Cisco Cloud Security
Cloud Service Architecture, Cisco Webex, 268–269
Cloudlock, 314–328
app security, 317–318
application blocking, 326–327
application-level reports, 325
Composite Risk Score, 327–328
dashboard, 317
data security, 316–317
risk mitigation, 316–317
sensitive information, 316
enabling via WSA, 318–321
evolution of, 322–325
CASB (cloud access security broker), 323
dashboard, 324
DNS-layer security, 322
firewalls, 323
interactive threat intelligence, 323
log files for shadow IT visibility, 324
overview and trending information, 324
SDWAN integration, 324
secure web gateway, 323
timeline of, 322
optimization, 325–326

overview of, 314–315
UEBA (User and Entity Behavior Analytics), 316
use cases, 318
user security, 315–316
cloud-registered Webex devices, proximity for, 282–285
CloudTrail, 343, 346
Cloupia Script, 97
cluster administration
on AWS EKS (Elastic Kubernetes Service), 224–226
on vSphere, 221–224
ClusterRole configuration, 190–192
cmdlets, PowerShell, 97
CNC (computer numerical control), 288
collaboration solutions. *See* Cisco Webex
commodities, definition of, 213
Common Industrial Protocol (CIP), 289
common infrastructure services, Cisco Nexus Dashboard, 10
communication compliance, Cisco Nexus Dashboard Insights, 64
compliance assurance, with Nexus Dashboard Insights, 44, 47
Composite Risk Score, Cisco Cloudlock, 327–328
Compounding Risk model, Duo Security Trust Monitor, 353
computer numerical control (CNC), 288
configuration change management, 44
configuration compliance, 64
configuration resource utilization, 51
Connectivity Analysis, Cisco Nexus Dashboard Insights, 49–50
consumption, definition of, 213
container IDs, registering as host IDs, 188–189
containers
CCP (Cisco Container Platform)
cluster administration on AWS EKS (Elastic Kubernetes Service), 224–226
cluster administration on vSphere, 221–224
components of, 219
deployment of, 219–221
licensing, 226
overview of, 215–218
registering with registration tokens, 226–227
upgrading, 227–228
use cases, 217–218
Docker, 180–185
container metrics, viewing, 183–185
container monitoring deployment, 181–182
container monitoring setup, 183
Docker Store, 183
images, creating, 194
Kubernetes with, 186
Metric Browser, 185
overview of, 180
Trusted Registry, 194
Kubernetes, 105–106, 186–196
AKS (Azure Kubernetes Service), 230–231
AppDynamics Machine Agent deployment on, 189–190
Cisco IKS (Intersight Kubernetes Service), 125–127

ClusterRole configuration, 190–192
container IDs, registering as host IDs, 188–189
Container Visibility with, 186–188
GKE (Google Kubernetes Engine), 230–231
IKS (Intersight Kubernetes Service), 125–127, 228–237
instrumenting applications with, 189
Network Visibility with, 193–196
overview of, 186
containers as a service (CaaS), 125–127
content filtering, 74
continuous compliance assurance, 44
contracts, 87–88
controllers, AppDynamics, 149
Cordova-based mobile applications, monitoring, 169
CORS (Cross-Origin Resource Sharing) domains, 168
costs, performance cost optimization, 106
CRC errors, 47, 54
Cross-Origin Resource Sharing (CORS) domains, 168
currency, virtual, 210–212
custom dashboards, Cisco Nexus Dashboard Insights, 65
customization, Cisco Webex, 245
CVD (Cisco Validated Design) templates, 298
CWOM (Cisco Workload Optimization Manager), 103–115, 201
action automation, 111–112
AppDynamics and, 107–108
application performance, 107–108
Cisco Intersight Workload Optimizer, 115
global environment view, 110
hyperconverged workloads, 107
increasing team effectiveness with, 105–106
key functionalities of, 103–104
multicloud environment optimization, 106
performance cost optimization, 106
plan types, 112–114
policies, 114–115
SLAs (service level agreements), 114–115
target integration, 109–110

D

D2Ops Solution Suite, 11
DaemonSet, 188, 193, 193
dashboards
Browser Application, 163–164
Geo tab, 164
Overview tab, 163–164
Cisco Cloud Security, 324
Cisco Cloudlock, 317
Cisco Duo Security Trust Monitor, 351–355
Cisco Secure Application, 151–152, 154
Cisco Secure Cloud Analytics, 347–348
Experience Journey Map, 159–160
Resource Performance, 165–168
data at rest, Cisco Webex, 276–277

Data Broker service (Cisco Nexus Dashboard), 5, 68–73
Cisco ACI (Application Centric Infrastructure) integration, 71
Cisco DNA Center integration, 72
Inline option, 72–73
modes of, 68
monitoring out-of-band and inline network traffic with, 68–69
overview of, 68
scalable traffic monitoring with, 72–73
SPAN Automation-enabled networks, 70
data center analytics. *See* network insight solutions
data center interconnectivity, 16
Data Center Network Manager (DCNM), 15, 83. *See also* Cisco NDFC (Nexus Dashboard Fabric Controller)
Data Center Networking (DCN) licensing, 11–12, 45–46
data center orchestration. *See also* Cisco Nexus Dashboard
IT challenges, data center solutions for, 2–4
platform support information, 33–34
server requirements, 34
third-party applications, 34–38
HashiCorp Terraform, 35
Red Hat Ansible, 35
ServiceNow, 35, 37–38
Splunk, 35–37
Data Control Module (DCM), 292, 294–296
data destinations, adding with EI (Edge Intelligence), 309–310
data logic deployment, 310
data rule deployment, 310
MQTT server destinations, 309
Data Destinations command, 309
data leakage, Cisco Cloudlock, 316
data logic deployment, EI (Edge Intelligence), 310
data loss prevention (DLP), 76, 316
data protection, Webex Teams, 273–281
data at rest, 276–277
data storage, 277
indexing service, 277–279
KMS (Key Management Server), 279–281
overview of, 273–276
data rule deployment, EI (Edge Intelligence), 310
data storage
Cisco Webex, 277
on-premises AppDynamics deployment architecture, 140
database agents, 132
Database Visibility, AppDynamics, 131–132, 148, 169–170
capabilities of, 169
overview of, 138
supported databases, 169–170
supported operating systems, 170
databases, SQLite, 276
DCM (Data Control Module), 292, 294–296
DCN (Data Center Networking) licensing, 11–12, 45–46
DCNM (Data Center Network Manager), 15, 83. *See also* Cisco NDFC (Nexus Dashboard Fabric Controller)
deactivating
Slido polls, 257–258
Slido quizzes, 258

Deliver phase, edge-to-multicloud lifecycle, 306
Delta Analysis, Cisco Nexus Dashboard Insights, 48–49, 64
Deployed status, 310
deployment
AppDynamics, 135–141
deployment models, 136
Machine Agent on Kubernates, 189–190
on-premises deployment architecture, 137–140
overview of, 135–136
platform components and tools, 136–137
requirements for, 136
SaaS deployment architecture, 140–141
CCP (Cisco Container Platform), 219–221
Cisco Intersight, 117–118
Cisco Nexus Dashboard Orchestrator, 21–24
ACI/DNCM sites, adding, 22–24
Cisco NDO app on Nexus Dashboard, 22
services communication with APIC nodes, 21
site management, 24–25
Cisco Secure Cloud Analytics, 341
Cisco Umbrella, 333
Docker container monitoring, 181–182
EI (Edge Intelligence)
data logic, 310
data rules, 310
Hyperflex, 122–124
IKS (Intersight Kubernetes Service), 230, 232–237
policies, 232–234
profiles, 234–237
rapid application deployment, 102–103
Webex Teams, 269–273
Internet access for cloud-based services, 269–270
overview of, 269
Video Mesh Nodes, 270–271
Webex Teams inspection capabilities, 272–273
Deployment Pending status, 310
destinations. *See* data destinations, adding with EI (Edge Intelligence)
device fingerprinting, 282
device onboarding, Cisco IoT
IR devices, 301–304
SDO (Secure Device Onboarding) architecture, 304
SEA (Secure Equipment Access), 305
seamless device onboarding, 304
SIM card activation, 304
summary steps, 305
supported device interfaces for onboarding, 300
device pairing, proximity and, 282–285
cloud-registered Webex devices, 283–284
on-premises registered Webex devices, 284–285
with Wi-Fi, 285
DIA (direct Internet access), 328–329
diagnostics, Cisco Nexus Dashboard Insights, 58–59
direct Internet access (DIA), 328–329

DIRL (dynamic ingress rate limiting), 32–33
DLP (data loss prevention), 76, 316
DNCM sites, adding, 22–24
DNS Security Advantage package, Cisco Umbrella, 337
DNS Security Essential package, Cisco Umbrella, 336
DNS-layer security
Cisco Cloud Security, 322
Cisco Umbrella, 329, 336, 337
Docker, 180–185
container metrics, viewing, 183–185
container monitoring deployment, 181–182
container monitoring setup, 183
Docker Store, 183
images, creating, 194
Kubernetes with, 186
Metric Browser, 185
overview of, 180
Trusted Registry, 194
DOM anomalies, 47
Duo Network Gateway, 358
Duo Security, 348–359
adaptive policies in, 356–357
Cisco Umbrella integration with, 335–336
Duo Network Gateway, 358
MFA (multifactor authentication), 349–351
overview of, 348–349
secure user access in, 357–359
remote access enablement, 357–358
SSO (single sign-on), 358–359
VPN-less remote access, 358
Trust Monitor, 351–355
models, 353
risk profiles, 353–355
telemetry, 352–353
dynamic entity modeling, Cisco Secure Cloud Analytics, 341
dynamic ingress rate limiting (DIRL), 32–33

E

EBS (Elastic Block Store), 87
EC2 (Elastic Compute Cloud), 87
ECHDE (Elliptic Curve Diffie-Hellman Ephemeral), 279
ECM (Enterprise Content Management), Webex Teams API for, 275–276
Economic Scheduling Engine, 209
eCVD templates, 298, 302
Edge and Fog Processing Module (EFM), 292, 296
Edge Device Manager. *See* EDM (Edge Device Manager), device onboarding with
Edge Intelligence. *See* EI (Edge Intelligence)
edge security, 328
edge-to-multicloud data flow, 306
EDM (Edge Device Manager), device onboarding with, 298–305
IR devices, 301–304
SDO (Secure Device Onboarding) architecture, 304
SEA (Secure Equipment Access), 305
seamless device onboarding, 304
SIM card activation, 304
summary steps, 305

supported device interfaces for onboarding, 300
EFM (Edge and Fog Processing Module), 292, 296
EI (Edge Intelligence), 305–308
agent management, 307–308
asset management, 308–309
configuration lifecycle management in, 307
data destinations, adding, 309–310
data logic deployment, 310
data rule deployment, 310
MQTT server destinations, 309
edge-to-multicloud data flow, 306
licensing, 311
overview of, 297, 305–306
EKS (Elastic Kubernetes Service), 230–231
Elastic Block Store (EBS), 87
Elastic Compute Cloud (EC2), 87
Elastic Kubernetes Service (EKS), 230–231
Elliptic Curve Diffie-Hellman Ephemeral (ECHDE), 279
email notification support, Cisco Nexus Dashboard Insights, 43, 66
Embedded mode, Cisco Nexus Dashboard Data Broker, 68
encryption, Cisco Webex
Messaging, 253
Webex Teams data protection, 275–281
end user events, in Experience Journey Map, 160–161
End User Monitoring. *See* EUM (End User Monitoring)
End User Portal, Cisco UCS Director, 97
end-of-life (EOL) announcements, 48, 60
end-of-sales (EOS) announcements, 48, 60
endpoint groups (EPGs), 51, 84, 87–88
ENFV (Enterprise Network Functions Virtualization), 75
Enterprise Content Management (ECM), Webex Teams API for, 275–276
entities
APM (Application Performance Monitoring), 145–146
anchor metrics for, 145
historical, 145
live, 145–146
definition of, 213
environment, definition of, 213
environmental data, Cisco Nexus Dashboard Insights, 46, 52–53, 65
EOL (end-of-life) announcements, 48, 60
EOS (end-of-sales) announcements, 48, 60
EPGs (endpoint groups), 51, 84, 87–88
Error status, 310
ESXi hypervisors, 229, 231
EUM (End User Monitoring), 132, 154–169
APM (Application Performance Monitoring) with, 158
Application Analytics with, 158–159
browser monitoring, 163–168
Browser Application Dashboard, 163–164
Browser RUM (Real User Monitoring), 163

Browser Synthetic Monitoring, 163
Resource Performance Dashboard, 165–168
capabilities of, 148, 156–157
data storage locations, 140
Experience Journey Map with, 159–162
accessing, 159
end user events, 160–161
Experience Journey Map dashboard, 159–160
overview of, 159
refresh loops, 162
requirements for, 159
traffic segments, 161–162
IoT (Internet of Things) monitoring, 168–169
on-premises deployments, 157–163
on-premises installation, 138
overview of, 154–156
platform connections, 139
SaaS EUM Server, accessing, 158
viewing data in, 157
Event Analytics, Cisco Nexus Dashboard Insights, 57–58
Events, Cisco Webex, 259–264
joining, 261–262
overview of, 259
recording, 262–263
registering for, 260–261
scheduling, 260
sharing content in, 263–264
sharing multiple applications in, 264
Experience Journey Map, EUM (End User Monitoring) with, 159–162
accessing, 159
end user events, 160–161
Experience Journey Map dashboard, 159–160
overview of, 159
refresh loops, 162
requirements for, 159
traffic segments, 161–162
Explorer, Cisco Nexus Dashboard Insights, 64
extensions, AppDynamics, 135
External users, Cisco Webex, 249
Extract phase, edge-to-multicloud lifecycle, 306

F

fabric builder for IPFM, 31
Fabric Controller. *See* NDFC (Nexus Dashboard Fabric Controller)
Fabric Discovery capability, Cisco NDFC (Nexus Dashboard Fabric Controller), 29
fabric topology view, Cisco NDFC (Nexus Dashboard Fabric Controller), 29
Fallback Signaling Cipher Suite Value (SCSV), 274
faults, 58
feature manager, Cisco NDFC (Nexus Dashboard Fabric Controller), 29
FIDO (Fast IDentity Online) Alliance, 351
firewalls
Cisco Cloud Security, 323
Cisco Umbrella, 331
Firmware Update Analysis, 60–61
First Time Setup Wizard, Cisco Cloud APIC, 88
flagging Cisco Webex messages, 251

flow
flow analytics, 54–55, 64
flow drop, 47
flow maps
AppDynamic, 153
tier, 153
Flow State Validator, Cisco Nexus Dashboard Insights, 66
Flow Table Events (FTE), 47
Flutter mobile applications, monitoring, 169
form factors
Cisco Nexus Dashboard, 12–13
OT (operational technology), 289
FTE (Flow Table Events), 47

G

Gateway Management Module (GMM), 292–294
gateways
Duo Network Gateway, 358
GMM (Gateway Management Module), 292–294
secure web gateway, 323, 330
SIG (secure Internet gateway), 328
GCP (Google Cloud Platform)
public cloud monitoring configuration for, 344–345
multiple projects, 344–345
single project, 344
vMX (virtual MX) appliance configuration for, 78
Geo tab, Browser Application Dashboard, 164
GKE (Google Kubernetes Engine), 230–231
global environment view, CWOM (Cisco Workload Optimization Manager)
action automation, 111–112
Cisco Intersight Workload Optimizer, 115
global environment view, 110
plan types, 112–114
policies, 114–115
SLAs (service level agreements), 114–115
GMM (Gateway Management Module), 292–294
Google Cloud Google Kubernetes Engine (GKE), 230–231
Google Cloud Platform, 74
Google Kubernetes Engine (GKE), 230–231
Govern phase, edge-to-multicloud lifecycle, 306
Graph API, 276
graphical user interface (GUI), Cisco Nexus Dashboard, 6
groups
CWOM (Cisco Workload Optimization Manager) settings, 115
endpoint, 51, 84, 87–88
security, 84, 87–88
AWS (Amazon Web Services), 87–88
rules, 84
GUI (graphical user interface), Cisco Nexus Dashboard, 6

H

hardening OT (operational technology), 289

hardware resource utilization, Cisco Nexus Dashboard Insights, 51
hardware stack, Cisco Nexus Dashboard, 11
HashiCorp Terraform, 35, 229
HCI (hyperconverged infrastructure), Hyperflex
deployment of, 122–124
key functionalities of, 119–120
systems architecture of, 120
HDS (Hybrid Data Security) services, 279
health rules, AppDynamics, 134
historical entity data, 145
HMAC-based one-time password (HOTP), 282
Home page
AppDynamics Analytics, 179–180
Cisco Secure Application dashboard, 154
host IDs, registering container IDs as, 188–189
HOTP (HMAC-based one-time password), 282
HTTPS (Secure Hypertext Transfer Protocol), 253, 272–273
HX (HyperFlex), 116–127, 229, 231
deployment of, 122–124
HXAP (HyperFlex Application Platform), 231
HXDP (Hyperflex Data Platform), 125
key functionalities of, 119–120
systems architecture of, 120
HXAP (HyperFlex Application Platform), 231
HXDP (Hyperflex Data Platform), 125

hybrid cloud solutions
Cisco Cloud ACI (Application Centric Infrastructure), 82–91
capabilities of, 83–84
Cisco ACI NDO (Nexus Dashboard Orchestrator), 86
Cisco APIC (Application Policy Infrastructure Controller), 84
Cisco Cloud APIC, 83–84, 86–91
high-level architecture of, 85
hybrid cloud environment challenges, 82–84
Cisco HyperFlex, 116–127, 229, 231
deployment of, 122–124
HXAP (HyperFlex Application Platform), 231
HXDP (Hyperflex Data Platform), 125
key functionalities of, 119–120
systems architecture of, 120
Cisco Intersight
benefits of, 118–119
Cisco IWE (Intersight Workload Engine), 125–127
deployment options, 117–118
login page, 116
MaaS (Management as a Service), 117
overview of, 116–117
Cisco Nexus Dashboard Orchestrator for, 18
Cisco UCS Director, 92–103
application container templates, 97–102
automation, 97
Cisco ACI integration, 97–103

Cisco UCS management through, 95–96
components of, 95–97
End User Portal, 97–102
IaaS (Infrastructure as a Service), 97–102
infrastructure configuration and management, 94
key functionalities of, 92–93
orchestration, 95–97
orchestration workflows, 97–102
policies, 97–102
system overview, 93
CWOM (Cisco Workload Optimization Manager), 103–115
action automation, 111–112
AppDynamics and, 107–108
application performance, 107–108
Cisco Intersight Workload Optimizer, 115
global environment view, 110
hyperconverged workloads, 107
increasing team effectiveness with, 105–106
key functionalities of, 103–104
multicloud environment optimization, 106
performance cost optimization, 106
plan types, 112–114
policies, 114–115
SLAs (service level agreements), 114–115
target integration, 109–110
optimization with IWO (Intersight Workload Optimizer), 206–209
Hybrid Data Security (HDS) services, 279
hyperconverged infrastructure (HCI). *See* HX (HyperFlex)
hyperconverged workloads, optimization of, 107
HyperFlex. *See* HX (HyperFlex)
Hyper-V, 94, 105–106
hypervisors
Cisco UCS Director support for, 94
HXAP (Cisco HyperFlex Application Platform), 231
HXAP (HyperFlex Application Platform), 231
VMware ESXi, 229, 231

I

IaaS (Infrastructure as a Service), 97–102
IAM (Identity and Access Management), 343
IBM Watson, 309
IBN (intent-based networking) strategy, 3
ICS (industrial control systems), 288
Identity and Access Management (IAM), 343
IdPs (identity providers), 282, 335–336
IDSs (intrusion detection systems), 72
IGMP flaps, Cisco Nexus Dashboard Insights, 47
IKS (Intersight Kubernetes Service), 125–127, 201, 228–237
benefits of, 229
deployment of, 230, 232–237
policies, 232–234
profiles, 234–237

how it works, 230–231
overview of, 228
release model, 232
use cases, 229
image management
Cisco NDFC (Nexus Dashboard Fabric Controller), 30–31
Docker, 194
indexing service, Cisco Webex, 277–279
industrial control systems (ICS), 288
information technology (IT), operational technology versus, 288–289
Infrastructure as a Service. *See* IaaS (Infrastructure as a Service)
Infrastructure menu commands, Sites, 25
Infrastructure Visibility, AppDynamics, 131–132, 134, 147–148, 171–172
Network Visibility, 172–175
agent-based approach of, 173
capabilities of, 173–174
with Kubernetes, 193–196
metrics, 174–175
overview of, 172–173
overview of, 171–172
Server Visibility, 138, 176–178
basic machine metrics, 177
functionality of, 176
infrastructure visibility strategies, 177–178
Java and .NET infrastructure monitoring, 177
UI (user interface), 176
strategies for, 177–178
Inline option, Cisco Nexus Dashboard Data Broker integration, 72–73
input/output, Cisco UCS Director, 96
insights. *See* network insight solutions
inspection, Webex Teams, 272–273
installation. *See* deployment
instrumenting applications, with Kubernetes, 189
Integrated Services Router (ISR), 333
integrations
Cisco Umbrella, 333–336
Cisco Duo, 335–336
SD-WAN, 334–335
SecureX, 334–335
Cisco Webex, 265–268
adding, 266–267
bots, 266–268
overview of, 265–266
removing, 267
support, 266
Webex Teams, 281–282
Intel Xeon Scalable processors, 120
intent-based networking (IBN) strategy, 3
interactive threat intelligence
Cisco Cloudlock, 323
Cisco Umbrella, 332
interfaces
Cisco Nexus Dashboard Insights, 47
EDM (Edge Device Manager) support for, 300
interface drops, 47
Internal users, Cisco Webex, 249
Internet access
for cloud-based services, 269–270
DIA (direct Internet access), 328–329
Internet of Things. *See* IoT (Internet of Things)
Intersight. *See* Cisco Intersight

Intersight Kubernetes Service. ***See*** **IKS (Intersight Kubernetes Service)**
Intersight Workload Engine. ***See*** **IWE (Intersight Workload Engine)**
Intersight Workload Optimizer. ***See*** **IWO (Intersight Workload Optimizer)**
intrusion detection systems (IDSs), 72
intrusion prevention systems (IPSs), 72
inventory, definition of, 213
iOS mobile applications, monitoring, 169
IoT (Internet of Things)
challenges of, 289
Cisco Edge Intelligence Solution, 297
Cisco IoT Solution
EDM (Edge Device Manager), 298–305
IR device onboarding, 300
overview of, 298
Cisco Kinetic platform, 289–296
benefits of, 291–292
DCM (Data Control Module), 292, 294–296
EFM (Edge and Fog Processing Module), 292, 296
features of, 291–292
GMM (Gateway Management Module), 292–294
key functions of, 291
overview of, 289–296
IT (information technology), 288–289
monitoring, 168–169
OT (operational technology), 288–289
overview of, 287–288
IP (Internet Protocol) connectivity, 85
IPFM (IP Fabric for Media), 25–26, 31
IPSs (intrusion prevention systems), 72
IR devices, onboarding with Edge Device Manager, 301–304
.iso form factor, 12
ISR (Integrated Services Router), 333
IT (information technology)
challenges of
data center solutions for, 2–4
management, 202–203
ITOM (IT operations management) tools, 94
OT (operational technology) versus, 288–289
ITOM (IT operations management) tools, 94
IWE (Intersight Workload Engine), 125–127
benefits of, 126
full stack integration, 125
key features of, 126–127
overview of, 125
IWO (Intersight Workload Optimizer), 201, 204–215
AppDynamics and, 208
AWS (Amazon Web Services) targets, claiming, 214
benefits of, 204
capabilities of, 214
CWOM-to-IWO migration, 205–206
Economic Scheduling Engine, 209
how it works, 209–210
hybrid cloud optimization with, 206–209
market and virtual currency, 210–212
risk index, 212
supply chain, 212

J

Java AppDynamics agent, 149, 150, 177
Java infrastructure monitoring, 177
JavaScript Agent, 148
joining Cisco Webex webinars, 261–262
JVM Crash Guard, 177

K

Kafka messaging support, 43, 66
Key Management Server (KMS), 274, 279–281
key performance indicators (KPIs), 148
Kinetic platform, 289–296
benefits of, 291–292
DCM (Data Control Module), 292, 294–296
EFM (Edge and Fog Processing Module), 292, 296
features of, 291–292
GMM (Gateway Management Module), 292–294
key functions of, 291
overview of, 289–296
KMS (Key Management Server), 274, 279–281
Known Signal model, Duo Security Trust Monitor, 353
KPIs (key performance indicators), 148
Kubernetes, 105–106, 186–196
AKS (Azure Kubernetes Service), 230–231
AppDynamics Machine Agent deployment on, 189–190
ClusterRole configuration, 190–192
container IDs, registering as host IDs, 188–189
Container Visibility with, 186–188
Docker Visibility with, 186
GKE (Google Kubernetes Engine), 230–231
IKS (Intersight Kubernetes Service), 125–127, 228–237
benefits of, 229
deployment of, 230, 232–237
how it works, 230–231
overview of, 228
release model, 232
use cases, 229
instrumenting applications with, 189
Kubernetes Snapshot Extension, 190
Network Visibility with, 193–196
overview of, 186
Kubernetes Snapshot Extension, 190

L

languages, Cloupia Script, 97
large-scale data center deployment, 15
latency statistics, 47, 55
leaks
data, 316
memory, 46
Libraries page, Cisco Secure Application dashboard, 154
licensing
CCP (Cisco Container Platform), 226
Cisco Data Center Networking, 11–12
Cisco NDFC (Nexus Dashboard Fabric Controller), 31

Cisco Nexus Dashboard Insights, 45–46
CWOM (Cisco Workload Optimization Manager) settings, 115
EI (Edge Intelligence), 311
license-entitlement information, 68
live entity data, 145–146
LLDP flaps, Cisco Nexus Dashboard Insights, 47
load balancing, Cisco Meraki MX, 76
locked meetings, Cisco Webex, 248–249
Log Analytics, 148
log files, Cisco Cloud Security, 324
Log in with Webex command (Slido), 256
logic, data, EI (Edge Intelligence), 310
login page, Cisco Intersight, 116
logs, audit, 58

M

MaaS (Management as a Service), 117
MAC addresses, 51
Machine Agent, 147–148, 176–178, 181–183
machine learning (ML)
Cisco Meraki MX, 74
Event Analytics, 57
machine metrics, AppDynamics Server Visibility, 177
maintenance, CWOM (Cisco Workload Optimization Manager) settings, 115
MAM (mobile application management), 282
management
CCP (Cisco Container Platform), 213, 215–228
architecture overview, 218–219
cluster administration on AWS EKS (Elastic Kubernetes Service), 224–226
cluster administration on vSphere, 221–224
components of, 219
deployment of, 219–221
licensing, 226
overview of, 215–218
registering with registration tokens, 226–227
upgrading, 227–228
use cases, 217–218
Cisco IKS (Intersight Kubernetes Service), 228–237
Cisco IWO (Intersight Workload Optimizer), 204–215
AppDynamics and, 208
AWS (Amazon Web Services) targets, claiming, 214
benefits of, 204
capabilities of, 214
CWOM-to-IWO migration, 205–206
Economic Scheduling Engine, 209
how it works, 209–210
hybrid cloud optimization with, 206–209
market and virtual currency, 210–212
risk index, 212
supply chain, 212–213

CWOM (Cisco Workload Optimization Manager), 201
IKS (Intersight Kubernetes Service), 201
benefits of, 229
deployment of, 230, 232–237
how it works, 230–231
overview of, 228
release model, 232
use cases, 229
IT challenges, 202–203
IWO (Intersight Workload Optimizer). *See* IWO (Intersight Workload Optimizer)
overview of, 201
Management as a Service (MaaS), 117
man-in-the-middle (MITM) attacks, 350
maps
Experience Journey Map, 159–162
accessing, 159
end user events, 160–161
Experience Journey Map dashboard, 159–160
overview of, 159
refresh loops, 162
requirements for, 159
traffic segments, 161–162
flow maps
AppDynamic, 153
tier, 153
market, Cisco IWO (Intersight Workload Optimizer), 210–212
MDM (mobile device management), 282
mean time to resolution (MTTR), 42, 48–49
Meetings, Cisco Webex, 244–250
audio/video preferences, 245
joining, 261–262
overview of, 244–250
polling in, 255–256
recording, 262–263
security features for, 248–249
starting meetings in, 246–247
from calendar, 247
from a space, 246
upcoming meetings, viewing, 247
memory leaks, 46
memory spikes, 46
Meraki MR, 333
Meraki MX
features and benefits of, 75–76
overview of, 74–75
vMX (virtual MX) appliances, 77–79
configuration for Alibaba Cloud, 79
configuration for GCP (Google Cloud Platform), 78
configuration for Microsoft Azure, 78
features and functionality of, 77–79
messages, Cisco Webex
organizing, 251
reading/responding to, 251
security features, 253
sending, 250
Messaging, Cisco Webex, 249–253
organizing messages in, 251
overview of, 249
reading/responding to messages in, 251
security features, 253
sending messages in, 250

Metric Browser, Docker, 185
metrics. *See* AppDynamics
MFA (multifactor authentication)
Cisco Duo Security, 349–351
Cisco Nexus Dashboard, 7
Webex Teams, 282
microburst detection, 47, 59, 64
Microsoft Azure, 74
AKS (Azure Kubernetes Service), 230–231
Azure Activity Log Watchlist, 347
cloud infrastructure observability, 198
Microsoft Azure (.arm) form factor, 12
public cloud monitoring configuration for, 345–346
vMX (virtual MX) appliance configuration for, 78
Microsoft Hyper-V, 94, 105–106
migration, CWOM-to-IWO, 205–206
MITM (man-in-the-middle) attacks, 350
ML (machine learning)
Cisco Meraki MX, 74
Event Analytics, 57
mobile application management (MAM), 282
mobile device management (MDM), 282
Mobile RUM (Real User Monitoring), 169
Modbus, 289, 306
models
AppDynamics deployment, 136
Cisco Duo Security Trust Monitor, 353
modules, Kinetic platform
DCM (Data Control Module), 292, 294–296
EFM (Edge and Fog Processing Module), 292, 296
GMM (Gateway Management Module), 292–294
monitoring. *See also* AppDynamics
with APM (Application Performance Monitoring), 142–154
agents, 149, 177
application security monitoring with Cisco Secure Application, 148–154
backends, 146
business applications, 144
business transactions, 143–144
Database Visibility, 148
entities, 145–146
EUM (End User Monitoring) and, 148
Infrastructure Visibility, 131–132, 134, 147–148, 171–172
Log Analytics, 148
nodes, 144
overview of, 142–143
tiers, 144–145
Transaction Analytics, 148
with Cisco NDFC (Nexus Dashboard Fabric Controller), 26
with Cisco UCS Director, 95
cloud applications, 180–196
Docker, 180–185
Kubernetes, 186–196
cloud infrastructure, 196–198
AWS cloud infrastructure observability, 197–198

Azure cloud infrastructure observability, 198
overview of, 196–197
with EUM (End User Monitoring), 132, 154–169
APM (Application Performance Monitoring), 158
Application Analytics, 158–159
browser monitoring, 163–168
capabilities of, 148, 156–157
data storage locations, 140
Experience Journey Map with, 159–162
IoT (Internet of Things) monitoring, 168–169
Mobile RUM (Real User Monitoring), 169
on-premises deployments, 157–163
on-premises installation, 138
overview of, 154–156
platform connections, 139
SaaS EUM Server, accessing, 158
viewing data in, 157
infrastructure, 134
public cloud monitoring configuration
for AWS (Amazon Web Services), 343–344
for GCP (Google Cloud Platform), 344–345
for Microsoft Azure, 345–346
traffic flows, 147–148, 161–162
MQTT (MQ Telemetry Transport), 306, 309
MSO (Multi-Site Orchestrator), 84. *See also* Orchestrator service (Cisco Nexus Dashboard)
MTTR (mean time to resolution), 42, 48–49
multicast control plane, 65
multicloud environments
Cisco Nexus Dashboard Orchestrator for, 18
optimization of, 106
multifactor authentication. *See* MFA (multifactor authentication)
Multi-Site Orchestrator (MSO), 84. *See also* Orchestrator service (Cisco Nexus Dashboard)
multisite support, Cisco Nexus Dashboard Insights, 63
multitenancy
secure, 102
VRF (virtual routing and forwarding), 31
multitier application deployment, Cisco Cloud ACI (Application Centric Infrastructure), 89

N

NAE (Network Assurance Engine), 43
NDDB (Nexus Dashboard Data Broker). *See* Data Broker service (Cisco Nexus Dashboard)
NDFC (Nexus Dashboard Fabric Controller), 5–6
benefits of, 27
Cisco NDFC app, 28
comprehensive management with, 25–26
DIRL (dynamic ingress rate limiting), 32–33
fabric builder for IPFM, 31
Fabric Discovery capability, 29
fabric topology view, 29

feature manager, 29
image management, 30–31
multitenancy VRF, 31
non-Nexus platform support, 31
optics information for SAN interfaces, 33
programmable reports, 31
RBAC (role-based access control), 31
SAN Insights, 31–32
SAN zoning interface, 33
SLP (Smart Licensing Policy), 31
topology view, 28
NDO (Nexus Dashboard Orchestrator), 5, 14–25, 86
for Cisco ACI Multi-Site, 15
for Cisco DCNM Multi-Site, 15
common use cases for, 15–18
Cisco NDO multidomain integrations, 16
data center interconnectivity, 16
hybrid cloud and multicloud, 18
large-scale data center deployment, 15
service provider/5G telco, 18
deployment of, 21–24
ACI/DNCM sites, adding, 22–24
Cisco NDO app on Nexus Dashboard, 22
services communication with APIC nodes, 21
site management, 24–25
functions provided by, 19–21, 84
multidomain integrations, 16
overview of, 14–15
registering Cisco Cloud APIC in, 89
site management with, 24–25
.NET AppDynamics agent, 149, 177
.NET infrastructure monitoring, 177
NetFlow Collector, 64
Network Assurance Engine (NAE), 43
Network Function Virtualization Infrastructure Software (NFVIS), 74
network insight solutions
Cisco Meraki MX, 74–79
features and benefits of, 75–76
overview of, 74–75
vMX (virtual MX) appliances, 77–79
Cisco Nexus Dashboard Data Broker, 68–73
Cisco ACI (Application Centric Infrastructure) integration, 71
Cisco DNA Center integration, 72
Inline option, 72–73
modes of, 68
monitoring out-of-band and inline network traffic with, 68–69
overview of, 68
scalable traffic monitoring with, 72–73
SPAN Automation-enabled networks, 70
Cisco Nexus Dashboard Insights, 41
advantages of, 42–43
advisories, 48, 60, 65
Analyze Alerts view, 46
Anomalies view, 46–47

AppDynamics, 47, 56, 65
application statistics, 56–57
change management, 64
Cisco ACI multitier support, 66
Cisco TAC Assist, 66
Connectivity Analysis, 49–50
custom dashboards, 65
Delta Analysis, 48–49, 64
design of, 41–42
diagnostics and impact, 58–59
email notification support, 43, 66
endpoint analytics, 56, 65
environmental data, 52–53, 65
Event Analytics, 57–58
features and benefits of, 63–66
Firmware Update Analysis, 60–61
flow analytics, 54–55, 64, 66
Kafka messaging support, 43, 66
key components of, 43–45, 46–50
licensing, 45–46
offline analysis, 66
One View capability, 10, 44, 63, 64
one-click remediation, 64
Pre-Change Analysis, 62–63, 64
product usage telemetry, 66
PSIRTs/bugs, 48, 60, 66
recommendations, 58–59
resource utilization, 50–51, 65
statistical data, 53–54, 65
topology view, 65
upgrade assist, 64
Cisco Nexus Insights Cloud Connector, 66–68
importance of, 41
network interfaces, OT (operational technology), 289
network software upgrades, 45
network TAP, 69
network telemetry, 43
Network Visibility, AppDynamics, 147, 172–175, 193–196
agent-based approach of, 173
capabilities of, 173–175
overview of, 172–173
Nexus Dashboard. *See* Cisco Nexus Dashboard
Nexus Dashboard Data Broker (NDDB). *See* Data Broker service (Cisco Nexus Dashboard)
Nexus Dashboard Fabric Controller. *See* Cisco NDFC (Nexus Dashboard Fabric Controller)
Nexus Dashboard Insights. *See* Cisco Nexus Dashboard Insights
Nexus Dashboard mode, Cisco Nexus Dashboard Data Broker, 68
Nexus Data Broker. *See* Data Broker service (Cisco Nexus Dashboard)
NI (Nexus Insights). *See* Cisco Nexus Dashboard Insights
nodes
APM (Application Performance Monitoring), 144
reloads, 46
Video Mesh Nodes, 270–271
non-Nexus platform support, Cisco NDFC (Nexus Dashboard Fabric Controller), 31
Novelty model, Duo Security Trust Monitor, 353

O

OAuth (Open Authorization), 253, 351
offline analysis, Cisco Nexus Dashboard Insights, 66
OIFs, 54
onboarding devices, Cisco IoT Solution
IR devices, 301–304
SDO (Secure Device Onboarding) architecture, 304
SEA (Secure Equipment Access), 305
seamless device onboarding, 304
SIM card activation, 304
summary steps, 305
supported device interfaces for onboarding, 300
One View capability, Nexus Dashboard, 10, 44, 63, 64
one-click remediation, Cisco Nexus Dashboard Insights, 64
on-premises AppDynamics deployment architecture, 137–140
data storage locations, 140
EUM (End User Monitoring), 157–163
overview of, 137–138
platform components, 138
platform connections, 138–140
OPC Unified Architecture (OPC-UA), 306
Open Authentication (OAuth), 351
Open Authorization (OAuth), 253
Open Virtual Appliance (OVA), 118
OpenShift, 105–106, 188–190
OpenStack, 105–106
operating systems, Database Visibility support for, 170
Operational expenditure (OpEx) optimization, 4
operational resource utilization, Cisco Nexus Dashboard Insights, 51
operational technology (OT), 288–289
OpEx (operational expenditure) optimization, 4
optics information for SAN interfaces, 33
optimization
Cisco Cloudlock, 325–326
CWOM (Cisco Workload Optimization Manager), 103–115
action automation, 111–112
AppDynamics and, 107–108
application performance, 107–108
Cisco Intersight Workload Optimizer, 115
global environment view, 110
hyperconverged workloads, 107
increasing team effectiveness with, 105–106
key functionalities of, 103–104
multicloud environment optimization, 106
performance cost optimization, 106
plan types, 112–114
policies, 114–115
SLAs (service level agreements), 114–115
target integration, 109–110
hybrid cloud infrastructure, 206–209
multicloud environment, 106

orchestration. *See* data center orchestration
Orchestrator service (Cisco Nexus Dashboard), 5, 14–25
for Cisco ACI Multi-Site, 15
for Cisco DCNM Multi-Site, 15
Cisco NDO app, 22
common use cases for, 15–18
deployment of, 21–24
functions provided by, 19–21
multidomain integrations, 16
overview of, 14–15
registering Cisco Cloud APIC in, 89
site management with, 24–25
organizing Cisco Webex messages, 251
OT (operational technology), 288–289
output, Cisco UCS Director, 96
OVA (Open Virtual Appliance), 118
.ova form factor, 12
Overview tab
Browser Application Dashboard, 163–164
Resource Performance Dashboard, 166

P

packages, Cisco Umbrella, 336–337
pairing, proximity and, 282–285
cloud-registered Webex devices, 283–284
on-premises registered Webex devices, 284–285
with Wi-Fi, 285
passwords
HMAC-based one-time password (HOTP), 282
TOTP (time-based one-time password), 282
performance cost optimization, 106
Performance Impacting Events (PIE) metric, 174
personal identification numbers (PINs), 285
Personal Rooms, Cisco Webex, 248–249
personas, Cisco Nexus Dashboard, 8–9
PIE (Performance Impacting Events) metric, 174
PIM (Privileged Identity Management), 47
PINs (personal identification numbers), 285
plan types, CWOM (Cisco Workload Optimization Manager), 112–114
platform components
AppDynamics, 136–137
on-premises AppDynamics deployment architecture, 138
platform connections, on-premises AppDynamics deployment architecture, 138–140
PLCs (programmable logic controllers), 288
policies
AppDynamics, 134
Cisco ACI (Application Centric Infrastructure), 87–88
Cisco Duo Security, 356–357
Cisco IKS (Intersight Kubernetes Service), 232–234
Cisco Secure Application dashboard, 154
Cisco UCS Director, 97–102
CWOM (Cisco Workload Optimization Manager), 114–115

Polling, Cisco Webex, 254–259
overview of, 254
in Slido, 256–259
poll activation/deactivation, 257–258
poll creation, 257
poll types, 256–257
quiz activation/deactivation, 258
survey creation, 259
in Webex meetings/webinars, 255–256
ports, TCP (Transmission Control Protocol), 147–148, 193
power failure, 46
PowerShell cmdlets, 97
Pre-Change Analysis, 62–63, 64
preferences, Cisco Webex, 245
Premier licenses
Cisco DCN (Cisco Data Center Networking), 11
Cisco Nexus Dashboard Insights, 45–46
private cloud monitoring, 341. ***See also*** **Cisco Secure Cloud Analytics**
Privileged Identity Management (PIM), 47
process crashes, 46
product usage telemetry, Cisco Nexus Dashboard Insights, 66
profiles
Duo Trust Monitor, 353–355
IKS (Intersight Kubernetes Service), 234–237
Profinet, 289
programmable infrastructure, Cisco Nexus Dashboard, 10
programmable logic controllers (PLCs), 288
programmable reports, Cisco NDFC (Nexus Dashboard Fabric Controller), 31
protocols, OT (operational technology) support for, 289. ***See also*** *individual protocols*
provisioning, with GMM (Gateway Management Module), 294
proximity and device pairing, 282–285
for cloud-registered Webex devices, 283–284
for on-premises registered Webex devices, 284–285
with Wi-Fi, 285
PSIRTs/bugs, 48, 60, 66
PSTN (Public Switched Telephone Network) access, 239
public cloud monitoring configuration, 341
for AWS (Amazon Web Services), 343–344
for GCP (Google Cloud Platform), 344–345
multiple projects, 344–345
single project, 344
for Microsoft Azure, 345–346
Public Switched Telephone Network (PSTN) access, 239
push-based 2FA (two-factor authentication), 351

Q

QoE (quality of experience) analytics, 74, 75
QoS (quality of service)
Cisco IWO (Intersight Workload Optimizer), 210
secure multitenancy, 102

quality of experience (QoE) analytics, 74
quality of service (QoS), 102, 210

R

rapid application deployment, 102–103
rapid endpoint movement, 47
Rarity model, Duo Security Trust Monitor, 353
RBAC (role-based access control), 31
React Native mobile applications, monitoring, 169
reading Cisco Webex messages, 251
Real User Monitoring (RUM)
Browser, 163
Mobile, 169
recording Cisco Webex events, 262–263
Red Hat
Ansible, 35
KVM, 94
OpenShift, 105–106, 188–190
refresh loops, in Experience Journey Map, 162
registration
of CCP (Cisco Container Platform), 226–227
for Cisco Webex events, 260–261
registration tokens, 226–227
release model, IKS (Intersight Kubernetes Service), 232
remote access enablement, in Cisco Duo Security, 357–358
reports/reporting
Cisco Cloudlock, 318, 325
Cisco UCS Director, 95
programmable, 31
reserved instance (RI) calculations, 105–106
Resource Performance Dashboard, 165–168
capabilities of, 165
maximizing effectiveness of, 168
Overview tab, 166
Resources tab, 167–168
Violations tab, 166–167
Resource Timing Metrics, 168
resource utilization, Cisco Nexus Dashboard Insights, 50–51, 65
Resources tab, Resource Performance Dashboard, 167–168
responding to Cisco Webex messages, 251
rest, data at, 276–277
REST APIs, 43, 71, 97
Return Materials Authorizations (RMAs), 118
RI (reserved instance) calculations, 105–106
risk management
Cisco Cloudlock, 316–317
Cisco Cloudlock Composite Risk Score, 327–328
Cisco IWO (Intersight Workload Optimizer) risk index, 212
Cisco Nexus Dashboard Insights, 42–43
RI (risk index), 212
risk profiles, Duo Trust Monitor, 353–355
RMAs (Return Materials Authorizations), 118
rogue endpoints, 47
role-based access control. *See* RBAC (role-based access control)
rollback, Cisco UCS Director, 96

routing, Cisco Nexus Dashboard Insights, 47
RSA, 253
rules, 84
AppDynamics health rules, 134
EI (Edge Intelligence), 310
RUM (Real User Monitoring)
Browser, 163
Mobile, 169

S

SaaS (Software as a Service)
AppDynamics deployment architecture, 140–141
Cisco Intersight
benefits of, 118–119
Cisco Intersight Workload Optimizer, 115
Cisco IWE (Intersight Workload Engine), 125–127
deployment options, 117–118
Hyperflex, 119–124
login page, 116
MaaS (Management as a Service), 117
overview of, 116–117
Cisco Meraki MX tenant restrictions, 76
EUM (End User Monitoring) Server, 158
SAG Cumulocity, 309
SAML (Security Assertion Markup Language), 253, 335–336
SAN Insights, NDFC (Nexus Dashboard Fabric Controller), 31–32
SANs (storage-area networks)
SAN Insights, 31–32
SAN interfaces, 33
zoning interface for, 33
SASE (secure access service edge), 328
SCADA (supervisory control and data acquisition), 288
scalable traffic monitoring, 72–73
scheduling Cisco Webex webinars, 260
schemas, definition of, 20
scope, Cisco Secure Application dashboard, 152
SCSV (Fallback Signaling Cipher Suite Value), 274
SDO (Secure Device Onboarding) architecture, 304
SD-WAN integration
Cisco Cloud Security, 324
Cisco Meraki MX, 75
Cisco Umbrella, 332
Cisco Umbrella integration with, 334–335
SEA (Secure Equipment Access), 305
seamless device onboarding, 304
search filter, Cisco Secure Application, 153–154
secure access service edge (SASE), 328
Secure Cloud Analytics, 337–348
alerts and analysis, 342–343
benefits of, 337–339
business advantages of, 340–341
dashboard, 347–348
deployment of, 341
dynamic entity modeling, 341–342
overview of, 339–341

public cloud monitoring configuration
for AWS (Amazon Web Services), 343–344
for GCP (Google Cloud Platform), 344–345
for Microsoft Azure, 345–346
watchlist configuration, 346–347
AWS CloudTrail Event Watchlist, 346
Azure Activity Log Watchlist, 347
overview of, 346
Secure Device Onboarding (SDO) architecture, 304
Secure Equipment Access (SEA), 305
Secure Hash Algorithm (SHA), 253
Secure Hypertext Transfer Protocol (HTTPS), 253, 272–273
secure Internet gateway (SIG), 328, 337. ***See also*** **Cisco Umbrella**
secure multitenancy, 102
Secure Real-Time Transport Protocol (SRTP), 253, 268
Secure Sockets Layer (SSL), 272–273
secure web gateway
Cisco Cloud Security, 323
Cisco Umbrella, 330
SecureX, Cisco Umbrella integration with, 334–335
security
Cisco Cloudlock
app security, 317–318
application blocking, 326–327
application-level reports, 325
Composite Risk Score, 327–328
dashboard, 317
data security, 316–317
enabling via WSA, 318–321
evolution of, 322–325
optimization, 325–326
UEBA (User and Entity Behavior Analytics), 316
user security, 315–316
Cisco Umbrella
benefits of, 329–332
deployment of, 333
evolution of, 322–325
integrations, 333–336
overview of, 328–329
packages, 336–337
Cisco Webex
Meetings, 248–249
Messaging, 253
security model, 243–244
Webex Teams, 269–273, 275–281
cloud. *See* Cisco Cloud Security
policies, 87–88
security groups, 84
AWS (Amazon Web Services), 87–88
rules, 84
Security Assertion Markup Language (SAML), 253, 335–336
Security Events widget, 149, 151
security groups, 84
AWS (Amazon Web Services), 87–88
rules, 84
security operations center (SOC), 334
self-service portal, Cisco UCS Director, 102–103
sending Cisco Webex messages, 250
sensitive information, Cisco Cloudlock, 316

Server Visibility, AppDynamics, 176–178
basic machine metrics, 177
functionality of, 176
infrastructure visibility strategies, 177–178
Java and .NET infrastructure monitoring, 177
overview of, 138
UI (user interface), 176
servers
Cisco data center orchestration, 34
Cisco UCS (Unified Computing System) servers, 11
EUM (End User Monitoring), 158
service level agreements (SLAs), 2
service providers, 18
service requests (SRs), 49, 96
service-level agreements. *See* SLAs (service level agreements)
ServiceNow, 35, 37–38
SHA (Secure Hash Algorithm), 253
shadow IT challenge, 313–314
Share Content command (Cisco Webex), 264
sharing content in Cisco Webex events, 263–264
SIG (secure Internet gateway), 328, 337. *See also* Cisco Umbrella
SIM cards, activating, 304
single sign-on. *See* SSO (single sign-on)
site management, Cisco Nexus Dashboard Orchestrator, 24–25
Sites command (Admin Console menu), 23
Sites command (Infrastructure menu), 25
site-to-site Auto VPN, 74
SLAs (service level agreements), 2, 114–115
Slido, polling in, 256–259
poll activation/deactivation, 257–258
poll creation, 257
poll types, 256–257
quiz activation/deactivation, 258
survey creation, 259
SLP (Smart Licensing Policy), 31
SMS 2FA (two-factor authentication), 351
Snapshot-based network assurance, 45–46
SNORT-based intrusion detection, 74, 76
SOC (security operations center), 334
Software as a Service. *See* SaaS (Software as a Service)
software upgrades, with Nexus Dashboard Insights, 45
spaces, starting Cisco Webex Meetings from, 246
SPAN (Switched Port Analyzer), 69, 70, 72
Splunk, 35–37
SQLite, 276
SRs (service requests), 49, 96
SRTP (Secure Real-Time Transport Protocol), 253, 268
SSL (Secure Sockets Layer), 272–273
SSO (single sign-on)
Cisco Duo Security, 358–359
Cisco Nexus Dashboard, 7, 8
Webex Teams, 281–282
IdPs, 282
integration guides, 281–282

MAM (mobile application management), 282
MDM (mobile device management), 282
multifactor authentication, 282
starting Cisco Webex Meetings, 246–247
from calendar, 247
from a space, 246
statistical data, Cisco Nexus Dashboard Insights, 53–54, 65
storage, data, 277
storage-area networks. *See* SANs (storage-area networks)
subnets, bridge-domain, 87–88
supervisory control and data acquisition (SCADA), 288
supply chain, Cisco IWO (Intersight Workload Optimizer), 212
supported device interfaces for onboarding
EDM (Edge Device Manager)
SDO (Secure Device Onboarding) architecture, 304
SEA (Secure Equipment Access), 305
seamless device onboarding, 304
SIM card activation, 304
summary steps, 305
supported device interfaces for onboarding, 300
EI (Edge Intelligence), 305–308
agent management, 307–308
asset management, 308–309
configuration lifecycle management in, 307
data destinations, adding, 309–310
edge-to-multicloud data flow, 306
licensing, 311
overview of, 305–306
surveys, Slido, 259
Switched Port Analyzer (SPAN), 69, 70, 72
synthetic monitoring, browser, 163

T

TAC (Technical Assistance Center), 66, 118, 125
Talos, 75
TAP (Test Access Point), 69, 72
targets
AWS (Amazon Web Services), claiming, 214
CWOM (Cisco Workload Optimization Manager), 109–110
tasks, Cisco UCS Director, 96
TCAM (Ternary Content-Addressable Memory), 51, 64
TCO (total cost of ownership), 117
TCP (Transmission Control Protocol) ports, 147–148, 193
Teams, Webex
data protection, 273–281
data at rest, 276–277
data storage, 276–277
indexing service, 277–279
KMS (Key Management Server), 279–281
overview of, 273–276
increasing effectiveness of, 105–106
proximity and device pairing, 282–285
for cloud-registered Webex devices, 283–284

for on-premises registered Webex devices, 284–285
with Wi-Fi, 285
security and deployment, 269–273
Internet access for cloud-based services, 269–270
overview of, 269
Video Mesh Nodes, 270–271
Webex Teams inspection capabilities, 272–273
single sign-on, 281–282
IdPs, 282
integration guides, 281–282
MAM (mobile application management), 282
MDM (mobile device management), 282
multifactor authentication, 282
Technical Assistance Center (TAC), 66, 118, 125
templates
Cisco UCS Director, 97–102
CVD (Cisco Validated Design), 298
CWOM (Cisco Workload Optimization Manager) settings, 115
eCVD, 298, 302
tenants, 87–88, 130
Ternary Content-Addressable Memory (TCAM), 51, 64
Terraform, 229
Test Access Point (TAP), 69, 72
Tetration, 107
third-party applications
Cisco data center orchestration, 34–38
HashiCorp Terraform, 35
Red Hat Ansible, 35
ServiceNow, 35, 37–38
Splunk, 35–37
Cisco Nexus Dashboard, 5–6
threat intelligence
Cisco Cloudlock, 323
Cisco Umbrella, 332
three-tier application deployment, Cisco ACI (Application Centric Infrastructure), 89–91
thresholds, AppDynamics, 133
tiers, 144–145
tier flow map, 153
Tier Metric Correlator, 147
Time Series Database, Cisco Nexus Dashboard Insights, 64
time series-based latency statistics, 55
time-based one time password (TOTP), 351
time-based one-time password (TOTP), 282
Timing-Allow-Origin HTTP header, 168
TLS (Transport Layer Security)
inspection for Webex Teams, 272–273
SCSV (Fallback Signaling Cipher Suite Value), 274
topology view
Cisco NDFC (Nexus Dashboard Fabric Controller), 28
Cisco Nexus Dashboard Insights, 65
total cost of ownership (TCO), 117
TOTP (time-based one-time password), 282, 351
traffic flows
flow analytics, 54–55, 64
flow drop, 47

flow maps
AppDynamic, 153
tier, 153
traffic segments, in Experience Journey Map, 161–162
Transaction Analytics, 148
transactions, business, 143–144
Transform phase, edge-to-multicloud lifecycle, 306
Transmission Control Protocol. *See* TCP (Transmission Control Protocol) ports
Transport Layer Security (TLS)
inspection for Webex Teams, 272–273
SCSV (Fallback Signaling Cipher Suite Value), 274
troubleshooting. *See* network insight solutions
Trust Monitor, Cisco Duo Security, 351–355
models, 353
risk profiles, 353–355
telemetry, 352–353
Trusted Registry, Docker, 194
tunnels, VXLAN (Virtual Extensible LAN), 102
Turbonomic, 201

U

UCS (Unified Computing System) Director, 92–103
application container templates, 97–102
automation, 97
Cisco ACI integration, 97–103
rapid application deployment, 102–103
secure multitenancy, 102
self-service portal, 102–103
Cisco UCS management through, 95–96
configuration/administration, 95
monitoring/reporting, 95
components of, 95–97
End User Portal, 97–102
IaaS (Infrastructure as a Service), 97–102
infrastructure configuration and management, 94
key functionalities of, 92–93
orchestration, 95–97
components, 95–96
workflows, 97–102
policies, 97–102
servers, 11
system overview, 93
UCS (Unified Computing System) servers, 11
UDP (User Datagram Protocol), 269
UEBA (User and Entity Behavior Analytics), 316
UIs (user interfaces), AppDynamics, 130, 176
ultrasonic signaling, 284
Umbrella, 328–337
benefits of, 329–332
CASB (cloud access security broker), 331
DNS-layer security, 329
firewalls, 331
interactive threat intelligence, 332
SD-WAN integration, 332
secure web gateway, 330

deployment of, 333
DNS-layer security, 329, 336, 337
evolution of, 322–325
CASB (cloud access security broker), 323
dashboard, 324
DNS-layer security, 322
firewalls, 323
interactive threat intelligence, 323
log files for shadow IT visibility, 324
overview and trending information, 324
SDWAN integration, 324
secure web gateway, 323
timeline of, 322
integrations, 333–336
Cisco Duo, 335–336
SD-WAN, 334–335
SecureX, 334–335
overview of, 328–329
packages, 336–337
unified application, Cisco Nexus Dashboard Insights, 63
Unified Computing System Director. ***See*** **UCS (Unified Computing System) Director**
Unified Computing System servers, 11
unified operations platform, Cisco Nexus Dashboard as, 8
Unverified users, Cisco Webex, 249
upcoming meetings, viewing in Cisco Webex, 247
updates, CWOM (Cisco Workload Optimization Manager) settings, 115
upgrades
CCP (Cisco Container Platform), 227–228
Cisco Nexus Dashboard Insights upgrade assist, 64
use cases
CCP (Cisco Container Platform), 217–218
Cisco Cloudlock, 318
Cisco Nexus Dashboard Orchestrator, 15–18
Cisco NDO multidomain integrations, 16
data center interconnectivity, 16
hybrid cloud and multicloud, 18
large-scale data center deployment, 15
service provider/5G telco, 18
IKS (Intersight Kubernetes Service), 229
use metrics, AppDynamics, 132–133
User and Entity Behavior Analytics (UEBA), 316
User Datagram Protocol (UDP), 269
user interfaces (UIs), AppDynamics, 130, 176
users
AppDynamics EUM (End User Monitoring), 132
AWS (Amazon Web Services) user accounts, 87–88

Cisco Cloudlock, 315–316
Cisco Duo Security user access, 357–359
remote access enablement, 357–358
VPN-less remote access, 358
Cisco Webex
External, 249
Internal, 249
Unverified, 249
CWOM (Cisco Workload Optimization Manager) settings, 115
EUM (End User Monitoring), 132, 154–169
APM (Application Performance Monitoring) with, 158
Application Analytics with, 158–159
browser monitoring, 163–168
capabilities of, 148, 156–157
data storage locations, 140
Experience Journey Map with, 159–162
IoT (Internet of Things) monitoring, 168–169
Mobile RUM (Real User Monitoring), 169
on-premises deployments, 157–163
on-premises installation, 138
overview of, 154–156
platform connections, 139
SaaS EUM Server, accessing, 158
viewing data in, 157
UX (user experience), 4

V

validation, workflow, 96
vCPUs (virtual CPUs), 211
VCS (Video Communication Server), 282–284
versioning, workflow, 96
Video Communication Server (VCS), 282–284
Video Mesh Nodes, 270–271
video preferences, Cisco Webex, 245
Violations tab, Resource Performance Dashboard, 166–167
Viptela, 333, 337
virtual currency, 210–212
Virtual Extensible LAN (VXLAN), 102
virtual machine scale sets (VMSSs), 198
virtual machines (VMs), 231
virtual MX appliances. ***See*** **vMX (virtual MX) appliances**
virtual private clouds (VPCs), 84, 87–88, 343
visualization, with Cisco NDFC (Nexus Dashboard Fabric Controller), 26
VLANs (virtual LANs), 51
VMem, 211
VMs (virtual machines), 231
VMSSs (virtual machine scale sets), 198
VMware
ESX (.ova) form factor, 12
ESXi hypervisors, 229
OVA (Open Virtual Appliance), 118
vSphere, 94, 105–106

vMX (virtual MX) appliances, 77–79
configuration for Alibaba Cloud, 79
configuration for GCP (Google Cloud Platform), 78
configuration for Microsoft Azure, 78
features and functionality of, 77–79
VPCs (virtual private clouds), 84, 87–88, 343
VPN-less remote access, Cisco Duo Security, 358
VPNs (virtual private networks), 74
VRF (virtual routing and forwarding), 51
vSphere, cluster administration on, 221–224
Vulnerabilities page, Cisco Secure Application dashboard, 154
Vulnerability search filter, Cisco Secure Application, 153–154
VXLAN (Virtual Extensible LAN), 102

W

W3C, 351
watchlists, configuration, 346–347
AWS CloudTrail Event Watchlist, 346
Azure Activity Log Watchlist, 347
overview of, 346
Watson, 309
web search filtering, 74
WebAuthn, 351
Webex
Cloud Calling, 241–243
Cloud Service Architecture, 268–269
Events, 259–264
joining, 261–262
overview of, 259
recording, 262–263
registering for, 260–261
scheduling, 260
sharing content in, 263–264
sharing multiple applications in, 264
features and benefits of, 239–240
integrations, 265–268
adding, 266–267
bots, 266–268
overview of, 265–266
removing, 267
support, 266
Meetings, 244–250
audio/video preferences, 245
joining, 261–262
overview of, 244–250
polling in, 255–256
recording, 262–263
security features for, 248–249
starting meetings in, 246–247
upcoming meetings, viewing, 247
Messaging, 249–253
organizing messages in, 251
overview of, 249
reading/responding to messages in, 251
security features, 253
sending messages in, 250

Polling, 254–259
overview of, 254
in Slido, 256–259
in Webex meetings/webinars, 255–256
security model, 243–244
Webex Assistant, 240
Webex Teams
for cloud-registered Webex devices, 283–284
data protection, 273–281
increasing effectiveness of, 105–106
for on-premises registered Webex devices, 284–285
proximity and device pairing, 282–285
security and deployment, 269–273
single sign-on, 281–282
SSO (single sign-on), 281–282
with Wi-Fi, 285
webinars, 259–264
joining, 261–262
overview of, 259
polling in, 255–256
recording, 262–263
registering for, 260–261
scheduling, 260
sharing content in, 263–264
sharing multiple applications in, 264
WiFi, Webex and, 285
wireless LAN controllers, 333
wizards, Cisco Cloud APIC First Time Setup Wizard, 88
workflows, Cisco UCS Director, 96
validation, 96
versioning, 96
workload optimization. *See also* AppDynamics
Cisco IWE (Intersight Workload Engine), 125–127
benefits of, 126
full stack integration, 125
key features of, 126–127
overview of, 125
CWOM (Cisco Workload Optimization Manager), 103–115
action automation, 111–112
AppDynamics and, 107–108
application performance, 107–108
Cisco Intersight Workload Optimizer, 115
global environment view, 110
hyperconverged workloads, 107
increasing team effectiveness with, 105–106
key functionalities of, 103–104
multicloud environment optimization, 106
performance cost optimization, 106
plan types, 112–114
policies, 114–115

SLAs (service level agreements), 114–115
target integration, 109–110
WSA, enabling Cisco Cloudlock with, 318–321

X

Xamarin mobile applications, monitoring, 169
XenServer, 105–106
Xeon Scalable processors, 120

Y-Z

Zero Touch Deployment. *See* ZTD (Zero Touch Deployment)
zoning interface, SANs, 33
ZTD (Zero Touch Deployment)
EDM (Edge Device Manager), 299
GMM (Gateway Management Module), 298