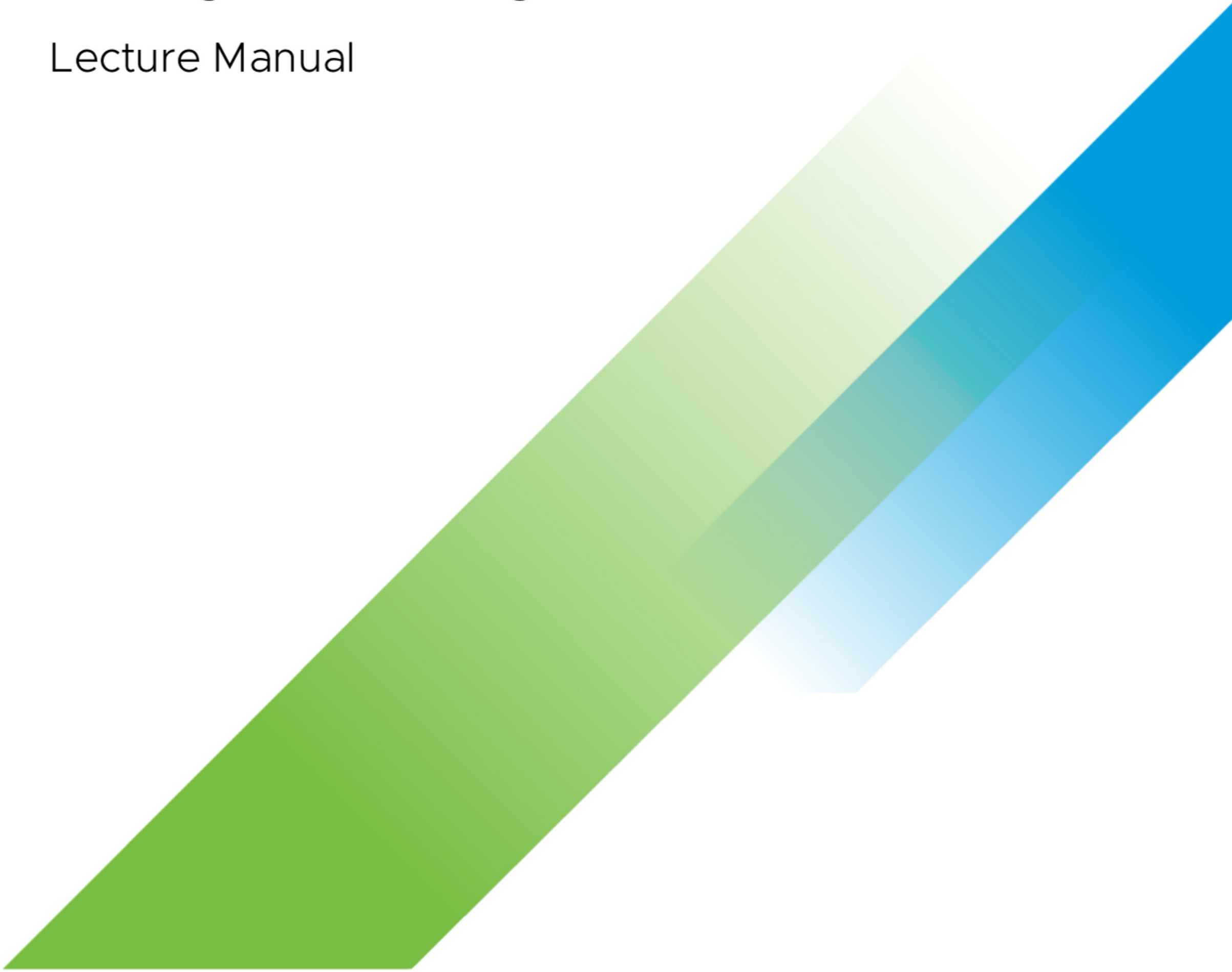
azarpara.vahid@gmail.com

VMware Aria Automation: Install, Configure, Manage [V8.10]

Lecture Manual



VMware® Education Services
VMware, Inc.
www.vmware.com/education

mcse2012.blogfa.com

azarpara.vahid@gmail.com

VMware Aria Automation: Install, Configure, Manage [V8.10]

Lecture Manual

Part Number EDU-EN-VAAICM810-LEC (17-MAR-2023)

Copyright © 2023 VMware, Inc. All rights reserved. This manual and its accompanying materials are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware vSphere® with VMware Tanzu®, VMware vSphere® Distributed Switch™, VMware vSphere® Distributed Resource Scheduler™, VMware vSphere® 2015, VMware vSphere®, VMware vSAN™, VMware vRealize® Suite Lifecycle Manager™, VMware vRealize® Suite, VMware vRealize® Orchestrator™, VMware vRealize® Operations Manager™, VMware vRealize® Operations Manager™ for Horizon®, VMware vRealize® Operations™ Enterprise, VMware vRealize® Operations™, VMware vRealize® Operations™ Standard, VMware vRealize® Operations™ Advanced, VMware vRealize® Network Insight™, VMware vRealize® Log Insight™ for vCenter™, VMware vRealize® Log Insight™, VMware vRealize® Cloud Universal™, VMware vRealize® Cloud Subscription Manager™, VMware vRealize® Automation Cloud™, VMware vRealize® Automation Cloud™ Standard Plus, VMware vRealize® Automation™ , VMware vRealize®, VMware vCloud Suite® Subscription, VMware vCenter Server®, VMware vCenter®, VMware vSphere® vApp(s)™, VMware Workspace ONE® Verify, VMware Workspace ONE® Access™, VMware View®, VMware Horizon® View™, VMware Verify™, VMware Tanzu®, VMware Tanzu® Enterprise, VMware Tanzu® Community, VMware Tanzu® Basic, VMware Tanzu® Standard, VMware Skyline™, VMware Horizon® 7, VMware Horizon® 7, VMware Horizon® 7 on VMware Cloud™ on AWS, VMware® Enterprise PKS, VMware Customer Connect™, VMware Code™, VMware Cloud™ on AWS, VMware Cloud Templates™, VMware Cloud Foundation™ SDDC Manager™, VMware Cloud Foundation™, VMware Cloud Foundation™ for Amazon EC2, VMware Cloud Foundation™ for Remote Office Branch Office, VMware Cloud Director™, VMware Cloud Director™ service, VMware Cloud Director™ on Dell Technologies Cloud Platform, VMware Cloud™ on AWS GovCloud (US), VMware Cloud™ on AWS Outposts, VMware Aria Universal Suite™, VMware Aria Suite Lifecycle™, VMware Aria Suite™, VMware Aria Operations™ for Networks, VMware Aria Operations™ for Logs, VMware Aria Operations™, VMware Aria Migration™, VMware Aria Hub Subscription™, VMware Aria Hub™, VMware Aria Cost™ powered by CloudHealth®, VMware Aria Automation™ for Secure Hosts, VMware Aria Automation™ for Secure Clouds, VMware Aria Automation Templates™, VMware Aria Automation Pipelines™, VMware Aria Automation Orchestrator™, VMware Aria Automation Consumption™, VMware Aria Automation Config™, VMware Aria Automation Assembler™, VMware Aria Automation™, VMware Aria™, VMware vSphere® Distributed Switch™, VMware Tanzu® Kubernetes Grid™ Service, VMware Tanzu® Kubernetes Grid™ Integrated Edition, VMware Service Catalog™, VMware Service Broker™, VMware vRealize® Automation SaltStack® SecOps, VMware vRealize® Automation SaltStack® Config, VMware RabbitMQ®, Project Photon OS™, VMware Photon™, VMware NSX-T™ Data Center, VMware NSX-T™, VMware NSX® Manager™, VMware NSX® Edge™, VMware NSX® Controller™, VMware NSX Cloud™,

www.vmware.com/education

mcse2012.blogfa.com

VMware NSX® API™, VMware NSX®, VMware NSX® Professional, VMware NSX® for Remote Office Branch Office, VMware NSX® for Desktop, VMware NSX® Enterprise Plus, VMware Migration Manager™, VMware Lab Connect™, VMware Go™, VMware ESXi™, VMware Pivotal Labs® Continuous Delivery™, CloudHealth® Secure State™, CloudHealth® Secure State™ Standard, CloudHealth® Secure State™ Enterprise, CloudHealth® by VMware, CloudHealth® by VMware Enterprise, CloudHealth® by VMware Standard, CloudHealth® by VMware Basic, CloudHealth®, and VMware Cloud Assembly™ are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

The training material is provided "as is," and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This material is designed to be used for reference purposes in conjunction with a training course.

The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended. These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted or modified without the express written approval of VMware, Inc.

Contents

Module 1 Course Introduction 1

1-2 Course Introduction 1

1-3 Importance 1

1-4 Learner Objectives (1) 1

1-5 Learner Objectives (2) 1

1-6 Course Outline 2

1-7 VMware Aria Naming (1) 3

1-8 VMware Aria Naming (2) 4

1-9 Typographical Conventions 5

1-10 References 6

1-11 VMware Online Resources 7

1-12 VMware Learning Overview 8

1-13 VMware Certification Overview 9

1-14 VMware Credentials Overview 10

Module 2 VMware Aria Automation Overview and Architecture 11

2-2 Importance 11

2-3 Module Lessons 11

2-4 Lesson 1: VMware Aria Automation Overview 12

2-5 Learner Objectives 12

2-6 Introduction to VMware Aria Automation 13

2-7 VMware Aria Automation Key Components 14

2-8 About VMware Aria Automation Assembler 15

2-9 About VMware Aria Automation Consumption 16

2-10 About VMware Aria Automation Pipelines 17

2-11 About VMware Aria Automation Orchestrator 18

2-12 About VMware Aria Automation Config 19

2-13 About VMware Aria Automation SaaS 20
2-14 Benefits of VMware Cloud Services 21
2-15 VMware Aria Automation: 8.10 Versus SaaS 22
2-16 VMware Aria Universal Suite Licensing Model 23
2-17 Lab 1: Requesting a Service 24
2-18 Review of Learner Objectives 24
2-19 Lesson 2: VMware Aria Automation Architecture 25
2-20 Learner Objectives 25
2-21 VMware Aria Automation Deployment Types 26
2-22 Standard Deployment Architecture 27
2-23 Clustered Deployment Architecture 28
2-24 About VMware Aria Suite Lifecycle 29
2-25 About Workspace ONE Access 31
2-26 VMware Aria Automation Appliance 32
2-27 Role of Kubernetes 33
2-28 VMware Aria Automation Services 34
2-29 Lab 2: Exploring the VMware Aria Automation Architecture 35
2-30 Review of Learner Objectives 35
2-31 Key Points 35

Module 3 Installing VMware Aria Automation 37

3-2 Importance 37
3-3 Lesson 1: Installing VMware Aria Automation 38
3-4 Learner Objectives 38
3-5 Installation Process 39
3-6 Minimum System Resources 40
3-7 VMware Aria Easy Installer: ISO 41
3-8 VMware Aria Easy Installer: Home Page 42
3-9 VMware Aria Easy Installer: Sections 43
3-10 VMware Aria Suite Lifecycle Configuration 45
3-11 Workspace ONE Access Configuration 46
3-12 VMware Aria Automation Configuration 47
3-13 Monitoring Requests 48
3-14 VMware Aria Suite Lifecycle Environments 49
3-15 VMware Aria Automation: Quickstart 50
3-16 Quickstart: Options 51
3-17 VMware Aria Automation Migration 52

3-18 Migrating VMware Aria Automation 7.x to 8.x....54
3-19 Lab 3: (Simulation) Installing VMware Aria Automation 55
3-20 Lab 4: (Simulation) Using VMware Aria Automation Quickstart 55
3-21 Review of Learner Objectives....56
3-22 Key Points 56

Module 4 Authentication and Authorization 57

4-2 Importance 57
4-3 Module Lessons 57
4-4 Lesson 1: Authentication with Workspace ONE Access....58
4-5 Learner Objectives 58
4-6 Authentication and Authorization 59
4-7 Architecture of Workspace ONE Access 60
4-8 About Workspace ONE Access 61
4-9 Directory Integration 62
4-10 Integrating Active Directory 63
4-11 Mapping User Attributes....64
4-12 Synchronizing Groups....65
4-13 Features of Workspace ONE Access....66
4-14 About the VMware Aria Automation Console 68
4-15 VMware Aria Automation: Organizations....69
4-16 VMware Aria Automation: Branding 70
4-17 Lab 5: Integrating Workspace ONE Access with Active Directory....71
4-18 Review of Learner Objectives....71
4-19 Lesson 2: Authorization with VMware Aria Automation Roles 72
4-20 Learner Objectives 72
4-21 Roles in VMware Aria Automation 73
4-22 Organizations and Services 74
4-23 Assigning Roles....75
4-24 Associating Organization and Service Roles 76
4-25 About Organization Roles 77
4-26 Service Roles: VMware Aria Automation Assembler....78
4-27 Service Roles: VMware Aria Automation Consumption....80
4-28 Service Roles: VMware Aria Automation Pipelines....81
4-29 Service Roles: VMware Aria Automation Orchestrator....83
4-30 Service Roles: VMware Aria Automation Config....84
4-31 About VMware Aria Automation Custom Roles....85

4-32 Lab 6: Assigning User Roles 87
4-33 Review of Learner Objectives 87
4-34 Lesson 3: Multitenancy and Virtual Private Zones 88
4-35 Learner Objectives 88
4-36 Multitenancy in VMware Aria Automation 89
4-37 Configuring DNS Records 90
4-38 Creating Multitenancy Certificates 92
4-39 Applying Multitenancy Certificates to Workspace ONE Access (1) 94
4-40 Applying Multitenancy Certificates to Workspace ONE Access (2) 95
4-41 Configuring Multitenancy in Workspace ONE Access 96
4-42 Applying Multitenancy Certificates to VMware Aria Automation (1) 97
4-43 Applying Multitenancy Certificates to VMware Aria Automation (2) 98
4-44 Configuring Multitenancy in VMware Aria Automation 99
4-45 Virtual Private Zones 100
4-46 Lab 7: (Simulation) Configuring Multitenancy and VPZs 101
4-47 Review of Learner Objectives 102
4-48 Key Points 102

Module 5 Basic Initial Configuration 103

5-2 Importance 103
5-3 Lesson 1: Basic Initial Configuration 104
5-4 Learner Objectives 104
5-5 Basic Configuration Roadmap 105
5-6 Guided Setup 106
5-7 Creating Cloud Accounts 107
5-8 Adding a vCenter Cloud Account 108
5-9 Creating a Cloud Zone and Enabling Provisioning 109
5-10 Creating Cloud Zones 110
5-11 Cloud Zones: Selecting Compute Resources 111
5-12 Creating Projects 112
5-13 Project: Adding Users and Groups 113
5-14 Project: Adding Cloud Zones 114
5-15 Creating Flavor Mappings 115
5-16 Creating Image Mappings 116
5-17 Testing the Configuration 117
5-18 Lab 8: Creating a Basic Configuration 119
5-19 Review of Learner Objectives 120

5-20 Key Points 120

Module 6 VMware Aria Automation Templates 121

6-2 Importance 121
6-3 Module Lessons 121
6-4 Lesson 1: Creating a Basic VMware Aria Automation Template 122
6-5 Learner Objectives 122
6-6 Creating a VMware Aria Automation Template 123
6-7 VMware Aria Automation Template Designer 124
6-8 Resources Pane 125
6-9 Design Canvas Pane 127
6-10 Configuration Pane 128
6-11 Testing and Deploying the VMware Aria Automation Template 129
6-12 Renaming Resources 130
6-13 Creating VMs 131
6-14 Lab 9: Creating a Basic VMware Aria Automation Template 133
6-15 Lab 10: Creating a Virtual Machine 133
6-16 Review of Learner Objectives 134
6-17 Lesson 2: Cloud-Agnostic VMware Aria Automation Templates 135
6-18 Learner Objectives 135
6-19 Cloud-Agnostic Versus Platform-Specific Resources 136
6-20 Giving End Users Choice with Inputs 137
6-21 Required Configuration 138
6-22 Capability Tags and Constraint Tags 139
6-23 Resource Grouping 141
6-24 Explicit Links 142
6-25 Implicit Links 143
6-26 Hard Links 144
6-27 Resource Grouping Example 145
6-28 Lab 11: (Simulation) Creating Cloud-Agnostic VMware Aria Automation Templates 146
6-29 Review of Learner Objectives 146
6-30 Lesson 3: Using cloudConfig and cloud-init 147
6-31 Learner Objectives 147
6-32 Use Case: Customizing VMware Aria Automation Templates for Deployment on Any Cloud 148
6-33 About cloudConfig and cloud-init 149

6-34 About cloudbase-init 150
6-35 Creating a vSphere Template That Supports cloud-init 151
6-36 Formatting cloudConfig 152
6-37 cloudConfig Commands 153
6-38 Creating Users in a Virtual Machine After Deployment 154
6-39 Customizing the DNS Host Name of a Virtual Machine After Deployment 155
6-40 Running Commands 156
6-41 Installing Software in a Virtual Machine After Deployment 157
6-42 cloudConfig in Image Mappings 158
6-43 cloudConfig Recommendations in vSphere 159
6-44 cloudConfig Logs and Scripts in a Deployed Machine 160
6-45 Lab 12: Creating a cloudConfig vSphere Template 161
6-46 Lab 13: Enhancing VMware Aria Automation Templates with cloudConfig 161
6-47 Lab 14: (Optional) Enhancing VMware Aria Automation Templates with cloudbase-init 162
6-48 Review of Learner Objectives 163
6-49 Lesson 4: Advanced YAML 164
6-50 Learner Objectives 164
6-51 Use Case: Using YAML to Create Infrastructure as Code 165
6-52 Indentation in YAML 166
6-53 Comments in YAML 167
6-54 Key-Value Pairs in YAML 168
6-55 Lists in YAML 169
6-56 Variables in YAML 170
6-57 User Inputs in YAML 171
6-58 Formatting Text in a VMware Aria Automation Template 172
6-59 Using Escape Characters 174
6-60 Evaluating Expressions in the VMware Aria Automation Template 175
6-61 Conditional Deployment in the VMware Aria Automation Template 176
6-62 Lab 15: Creating an Advanced VMware Aria Automation Template 177
6-63 Review of Learner Objectives 178
6-64 Key Points 178

Module 7 Tags 179
7-2 Importance 179
7-3 Lesson 1: Tags 180
7-4 Learner Objectives 180

7-5 Tags in VMware Aria Automation 181
7-6 Capability Tags 182
7-7 Constraint Tags 183
7-8 Tags in Projects 184
7-9 Hard, Soft, and Not Modifiers 185
7-10 Tagging Strategies 186
7-11 Tagging Implementation 187
7-12 Sequencing of Capability and Constraint Tag Processing 188
7-13 Lab 16: Creating and Using Tags 189
7-14 Lab 17: Using a Filter Tag on a Cloud Zone 189
7-15 Lab 18: Tagging Deployed Virtual Machines in vSphere 190
7-16 Review of Learner Objectives 191
7-17 Key Points 191

Module 8 Storage Configuration 193
8-2 Importance 193
8-3 Lesson 1: Storage Configuration 194
8-4 Learner Objectives 194
8-5 Use Case: Effective Storage Management 195
8-6 vSphere VM Storage Policies 196
8-7 About vSphere Tags 197
8-8 Creating VMware Aria Automation Storage Profiles 198
8-9 Using Preferred VMware Aria Automation Storage Profiles 200
8-10 Storage Constraint Tag on Machines 201
8-11 Storage Policy on a Disk 202
8-12 Order of Precedence 203
8-13 About Volumes 204
8-14 About Standard Disks 205
8-15 About First Class Disks 206
8-16 Storage Limits 208
8-17 Lab 19: Using Storage Profiles 209
8-18 Lab 20: First Class Disks as a Service 210
8-19 Review of Learner Objectives 211
8-20 Key Points 211

Module 9 Integrating NSX with VMware Aria Automation 213
9-2 Importance 213

9-3 Module Lessons 213
9-4 Lesson 1: Introduction to NSX 214
9-5 Learner Objectives 214
9-6 NSX: Introduction 215
9-7 NSX: Workload Objects 216
9-8 NSX: Use Cases 217
9-9 NSX: Architecture 218
9-10 NSX: Capabilities 220
9-11 Network and Security Services 221
9-12 NSX Edge Nodes 222
9-13 NSX Tiered Routing 223
9-14 Review of Learner Objectives 225
9-15 Lesson 2: NSX Integration 226
9-16 Learner Objectives 226
9-17 NSX: Cloud Accounts 227
9-18 Network Profiles 229
9-19 Discovered Networks 230
9-20 Public Network 231
9-21 Network Profile: Existing 232
9-22 Network Profile: Private 234
9-23 Network Profile: Outbound 235
9-24 Network Profile: Routed 237
9-25 Security Groups 238
9-26 Load Balancers 239
9-27 VMware Aria Automation Template with Network and Security Constructs 240
9-28 Day 2 Actions: Networks 241
9-29 Day 2 Actions: Security Groups 242
9-30 Lab 21: Integrating NSX with VMware Aria Automation 244
9-31 Lab 22: Performing Day 2 Network Actions 244
9-32 Review of Learner Objectives 245
9-33 Key Points 245

Module 10 Integration with Public Clouds 247

10-2 Importance 247
10-3 Lesson 1: Integration with Public Clouds 248
10-4 Learner Objectives 248
10-5 Public Cloud Support 249

10-6 Amazon Web Services: Credentials 250
10-7 Amazon Web Services: Cloud Accounts 252
10-8 Amazon Web Services: Simple VMware Aria Automation Template 254
10-9 Microsoft Azure: Credentials 255
10-10 Microsoft Azure: Cloud Account 256
10-11 Microsoft Azure: Simple VMware Aria Automation Template 258
10-12 Google Cloud Platform: Credentials 259
10-13 Google Cloud Platform: Cloud Account 260
10-14 Google Cloud Platform: Simple VMware Aria Automation Template 261
10-15 About VMware Cloud Foundation 262
10-16 VMware Cloud Foundation SDDC Manager Integration 263
10-17 VMware Cloud Foundation: Cloud Account 265
10-18 VMware Cloud Director: Cloud Account 266
10-19 VMware Cloud on AWS 267
10-20 VMware Cloud on AWS: Credentials 268
10-21 VMware Cloud on AWS: Cloud Account 269
10-22 Lab 23: (Simulation) Configuring the VMware Cloud Foundation Account 270
10-23 Lab 24: (Simulation) Configuring Public Cloud Accounts 270
10-24 Review of Learner Objectives 271
10-25 Key Points 271

Module 11 Using VMware Aria Automation Consumption 273

11-2 Importance 273
11-3 Lesson 1: Using VMware Aria Automation Consumption 274
11-4 Learner Objectives 274
11-5 Use Case: VMware Aria Automation Consumption 275
11-6 Self-Service Catalog 276
11-7 Releasing VMware Aria Automation Templates 277
11-8 Accessing VMware Aria Automation Consumption 278
11-9 Content Sources 279
11-10 Policy Definitions 280
11-11 Policy Type: Content Sharing 281
11-12 Content Sharing: Options 282
11-13 Policy Type: Approval Policy 283
11-14 Approval Requests 285
11-15 Policy Type: Lease Policy 286
11-16 Policy Type: Day 2 Actions Policy 288

11-17 Policy Type: Deployment Limit 290
11-18 Policy Type: Resource Quota 291
11-19 Monitoring Deployments 293
11-20 Managing Deployments 294
11-21 Request Forms 295
11-22 Custom Forms 296
11-23 Customizing the Request Form 297
11-24 Lab 25: Configuring the VMware Aria Automation Consumption Catalog 298
11-25 Lab 26: Managing Deployments 298
11-26 Lab 27: Creating Custom Forms 299
11-27 Lab 28: Configuring the VMware Aria Automation Consumption Policies 299
11-28 Lab 29: Using VMware Aria Automation Deployment Limit Policies 300
11-29 Lab 30: Using VMware Aria Automation Resource Quota Policies 300
11-30 Lab 31: Using Multilevel Approvals 300
11-31 Review of Learner Objectives 301
11-32 Key Points 301

Module 12 VMware Aria Automation Extensibility 303

12-2 Importance 303
12-3 Module Lessons 303
12-4 Lesson 1: Introduction to Extensibility 304
12-5 Learner Objectives 304
12-6 Native Functionality in VMware Aria Automation 305
12-7 Overview of Extensibility 306
12-8 VMware Aria Automation Extensibility Proxy 307
12-9 About VMware Aria Automation Orchestrator 308
12-10 ABX Actions 309
12-11 Defining VMware Aria Automation Orchestrator Workflows and ABX Actions 310
12-12 Event Topics in VMware Aria Automation 311
12-13 Descriptions of Event Topics 312
12-14 Subscriptions 314
12-15 Review of Learner Objectives 316
12-16 Lesson 2: VMware Aria Automation Orchestrator Workflows 317
12-17 Learner Objectives 317
12-18 Orchestrator Client 318
12-19 Orchestrator Client: Summary Tab 320
12-20 Orchestrator Client: Inputs/Outputs Tab 322

12-21 Orchestrator Client: Schema Tab 323
12-22 Subscriptions Call Workflows 324
12-23 Lab 32: Using VMware Aria Automation Orchestrator to Set Custom Host Names 325
12-24 Review of Learner Objectives 325
12-25 Lesson 3: ABX Actions 326
12-26 Learner Objectives 326
12-27 Creating an ABX Action 327
12-28 New ABX Action Wizard 328
12-29 ABX Action Settings 329
12-30 ABX Flows, ABX REST Calls, and ABX Scripts 331
12-31 Polyglot Capabilities of ABX 332
12-32 ABX Action Templates 333
12-33 Packaging ABX Actions 334
12-34 Calling ABX Actions 335
12-35 Lab 33: Using ABX to Set Custom Host Names 336
12-36 Review of Learner Objectives 337
12-37 Key Points 337

Module 13 Integration with Kubernetes 339

13-2 Importance 339
13-3 Lesson 1: Integration with Kubernetes 340
13-4 Learner Objectives 340
13-5 Overview of Kubernetes Integration 341
13-6 Introduction to vSphere with Tanzu 342
13-7 vSphere with Tanzu: Virtual Machines 343
13-8 vSphere with Tanzu: Supervisor Clusters 345
13-9 vSphere with Tanzu: Tanzu Kubernetes Cluster 346
13-10 vSphere with Tanzu: Integration 347
13-11 Managing Supervisor Namespaces 348
13-12 Kubernetes Zones 349
13-13 Cluster Plans 350
13-14 VMware Aria Automation Template: On-Demand Namespaces 351
13-15 Kubernetes Resources in VMware Aria Automation Templates 352
13-16 Deploying the Tanzu Kubernetes Cluster 353
13-17 Integrating VMware Tanzu Kubernetes Grid Integrated Edition 354
13-18 Tanzu Kubernetes Grid Integrated Edition: Kubernetes Zone 355

13-19 Kubernetes Cluster Options 356
13-20 Integrating External Kubernetes 357
13-21 Integrating Red Hat OpenShift 358
13-22 Lab 34: Integrating an Existing Kubernetes Cluster with VMware Aria Automation 360
13-23 Review of Learner Objectives 361
13-24 Key Points 361

Module 14 Introduction to VMware Aria Automation Config 363

14-2 Importance 363
14-3 Lesson 1: Introduction to VMware Aria Automation Config 364
14-4 Learner Objectives 364
14-5 Introduction to VMware Aria Automation Config 365
14-6 Salt Masters and Minions 366
14-7 About VMware Aria Automation Config 367
14-8 Communication Between Salt Master and Salt Minion 368
14-9 Communication in VMware Aria Automation Config 370
14-10 VMware Aria Automation Config Installation 371
14-11 VMware Aria Automation Config Integration in VMware Aria Automation 373
14-12 SaltStack Config Resource 374
14-13 Salt Minion Installation 375
14-14 Salt Master Keys 376
14-15 Accepting Minion Keys 377
14-16 Command Structure 378
14-17 About Targeting 379
14-18 About Grains 381
14-19 Salt Modules 382
14-20 Salt States 383
14-21 About Pillars 384
14-22 About Jobs 385
14-23 VMware Aria Automation Config Job Inputs 386
14-24 About Beacons 387
14-25 About Reactors 388
14-26 Reacting to Events with Beacons and Reactors 389
14-27 Remediations with VMware Aria Automation Config for Secure Hosts 390
14-28 Lab 35: Using VMware Aria Automation Config to Build a Web Server 391

14-29 Lab 36: Using VMware Aria Automation Config to Restore a Hacked Web Server 391
14-30 Review of Learner Objectives 392
14-31 Key Points 392

Module 15 Troubleshooting and Integration with VMware Aria Suite . 393

15-2 Importance 393
15-3 Module Lessons 393
15-4 Lesson 1: Troubleshooting VMware Aria Automation 394
15-5 Learner Objectives 394
15-6 Overview of the CLI 395
15-7 Useful vracli Commands 396
15-8 Useful kubectl Commands 397
15-9 Restarting Services 398
15-10 About the deploy.sh Script 399
15-11 Collecting Log Bundles 400
15-12 Log Bundle Structure 401
15-13 Important Logs 402
15-14 Monitoring Requests 403
15-15 Lab 37: Collecting Log Bundles and Investigating Logs 404
15-16 Lab 38: Restarting Services 404
15-17 Review of Learner Objectives 405
15-18 Lesson 2: VMware Aria Suite Integration 406
15-19 Learner Objectives 406
15-20 Overview of VMware Aria Operations for Logs 407
15-21 VMware Aria Operations for Logs: Integration 408
15-22 VMware Aria Operations for Logs: Interactive Analytics 409
15-23 Overview of VMware Aria Operations 411
15-24 Integration in VMware Aria Automation 412
15-25 Integration with VMware Aria Operations 413
15-26 VMware Aria Operations: Integration Benefits 414
15-27 Integration Benefits: Cost Pricing 415
15-28 Integration Benefits: Deployment Monitoring 416
15-29 Integration Benefits: Workload Placement 417
15-30 Review of Learner Objectives 418
15-31 Key Points 418

Module 1

Course Introduction

1-2 Course Introduction

1-3 Importance

You use VMware Aria Automation to create and manage multivendor cloud infrastructures. Using VMware Aria Automation, end users can self-provision virtual machines, applications, and IT services according to policies defined by administrators.

1-4 Learner Objectives (1)

- Install and configure VMware Aria Automation
- Describe the VMware Aria Automation architecture and its use cases in multitenant cloud environments
- Identify the roles of Workspace ONE Access and VMware Aria Suite Lifecycle
- Configure and manage cloud accounts and projects for compute resources
- Configure, customize, and manage VMware Aria Automation Templates
- Configure VMware Aria Automation Consumption for creating a self-service catalog
- Use the self-service portal to request and manage deployments in VMware Aria Automation
- Integrate NSX with VMware Aria Automation

1-5 Learner Objectives (2)

- Describe VMware Aria Automation extensibility
- Use and manage Kubernetes clusters from VMware Aria Automation
- Use VMware Aria Automation Config for software deployment and configuration management
- Identify the key log files and commands to troubleshoot VMware Aria Automation

1-6 Course Outline

1. Course Introduction
2. VMware Aria Automation Overview and Architecture
3. Installing VMware Aria Automation
4. Authentication and Authorization
5. Basic Initial Configuration
6. VMware Aria Automation Templates
7. Tags
8. Storage Configuration
9. Integrating NSX with VMware Aria Automation
10. Integration with Public Clouds
11. Using VMware Aria Automation Consumption
12. VMware Aria Automation Extensibility
13. Integration with Kubernetes
14. Introduction to VMware Aria Automation Config
15. Troubleshooting and Integration with VMware Aria Suite

1-7 VMware Aria Naming (1)

This course uses the new product names, but you might encounter the former names in the user interface. You can use the following tables for reference.

Former Name	New Name
VMware vRealize Automation and VMware vRealize Automation Cloud	VMware Aria Automation
VMware Cloud Assembly	VMware Aria Automation Assembler
VMware Service Broker	VMware Aria Automation Consumption
VMware Code Stream	VMware Aria Automation Pipelines
VMware vRealize Orchestrator	VMware Aria Automation Orchestrator
VMware vRealize Automation SaltStack Config	VMware Aria Automation Config
VMware vRealize Automation SaltStack SecOps	VMware Aria Automation for Secure Hosts
VMware vRealize Automation Cloud Templates	VMware Aria Automation Templates

1-8 VMware Aria Naming (2)

Former Name	New Name
VMware Identity Manager	VMware Workspace ONE Access
VMware vRealize Suite Lifecycle Manager	VMware Aria Suite Lifecycle
CloudHealth Secure State	VMware Aria Automation for Secure Clouds
VMware vRealize Operations/Cloud	VMware Aria Operations
VMware vRealize Log Insight/Cloud	VMware Aria Operations for Logs
VMware vRealize Network Insight/Cloud	VMware Aria Operations for Networks
CloudHealth	VMware Aria Cost powered by CloudHealth
VMware vRealize Cloud Universal	VMware Aria Universal Suite
VMware vRealize Suite	VMware Aria Suite
VMware vRealize Migration Manager	VMware Aria Migration
VMware vRealize Cloud Subscription Manager	VMware Aria Hub Subscription

1-9 Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Use and Examples
`Monospace`	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: • Run the `esxtop` command. • … found in the `/var/log/messages` file.
`Monospace Bold`	Identifies user inputs: • Enter **`ipconfig /release`**.
Boldface	Identifies user interface controls: • Click the **Configuration** tab.
Italic	Identifies book titles: • *vSphere Virtual Machine Administration*
< >	Indicates placeholder variables: • <ESXi_host_name> • … the `Settings/<Your_Name>.txt` file

1-10 References

Title	Location
Installing vRealize Automation with vRealize Easy Installer	https://docs.vmware.com/en/vRealize-Automation/index.html
Using and Managing vRealize Automation Cloud Assembly	https://docs.vmware.com/en/vRealize-Automation/index.html
Using and Managing vRealize Automation Service Broker	https://docs.vmware.com/en/vRealize-Automation/index.html
Using the Embedded vRealize Orchestrator Client	https://docs.vmware.com/en/vRealize-Automation/index.html
vRealize Automation Support Matrix	https://docs.vmware.com/en/vRealize-Automation/8.x/SupportMatrix/GUID-2B9D7C13-8ACC-4428-81CF-B265C01A231C.html
VMware Product Interoperability Matrix	http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php

1-11 VMware Online Resources

Documentation for vRealize Automation 8.10: https://docs.vmware.com/en/vRealize-Automation/index.html

VMware Communities: http://communities.vmware.com

- Start a discussion.
- Access the knowledge base.
- Access documentation, technical papers, and compatibility guides.
- Access communities.
- Access user groups.

VMware Support: http://www.vmware.com/support

VMware Hands-on Labs: http://hol.vmware.com

VMware Learning: http://www.vmware.com/learning

- Access course catalog.
- Access worldwide course schedule.

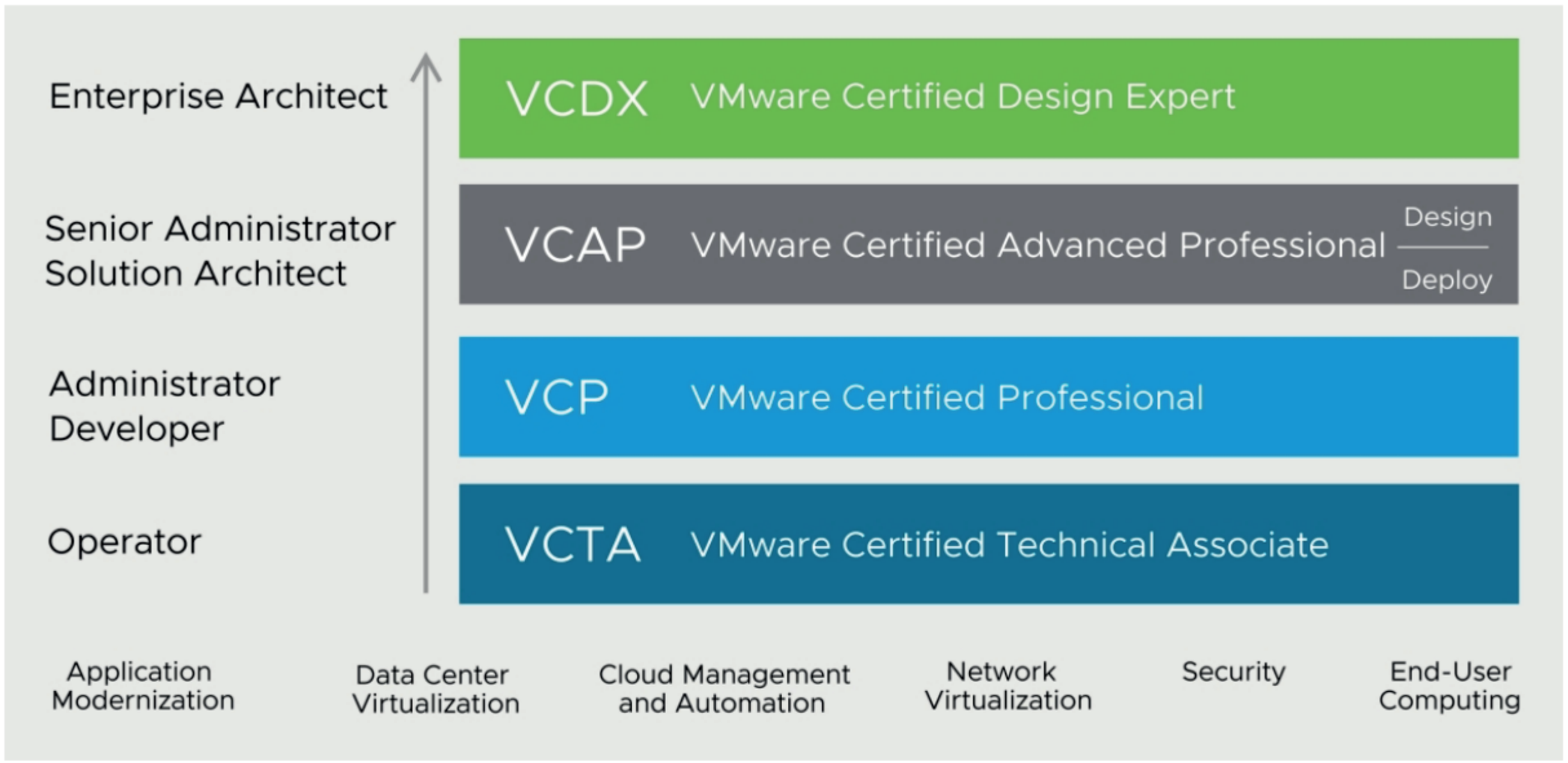
1-12 VMware Learning Overview

You can access the following Education Services:

- VMware Learning Paths:
  - Help you find the course that you need based on the product, your role, and your level of experience
  - Can be accessed at https://vmware.com/learning
- VMware Customer Connect Learning, which is the official source of digital training, includes the following options:
  - On Demand Courses: Self-paced learning that combines lecture modules with hands-on practice labs
  - VMware Lab Connect: Self-paced, technical lab environment where you can practice skills learned during instructor-led training
  - Certification Exam Prep: Comprehensive video-based reviews of exam topics and objectives to help you take your certification exam
- For more information, see https://vmware.com/learning/connect-learning.

1-13 VMware Certification Overview

VMware certifications validate your expertise and recognize your technical knowledge and skills with VMware technology.



VMware certification sets the standards for IT professionals who work with VMware technology. Certifications are grouped into technology tracks. Each track offers one or more levels of certification (up to four levels).

For the complete list of certifications and details about how to attain these certifications, see https://vmware.com/certification.

1-14 VMware Credentials Overview

VMware badges are digital emblems of skills and achievements. Career certifications align to job roles and validate expertise across a solution domain. Certifications can cover multiple products in the same certification.











Specialist certifications and skills badges align to products and verticals and show expanded expertise.





Digital badges have the following features:

- Easy to share in social media (LinkedIn, Twitter, Facebook, blogs, and so on)
- Validate and verify achievement
- Contain metadata with skill tags and accomplishments
- Based on Mozilla's Open Badges standard

For the complete list of digital badges, see http://www.pearsonvue.com/vmware/badging.

Module 2

VMware Aria Automation Overview and Architecture

2-2 Importance

VMware Aria Automation is a cloud management platform with numerous components. To implement VMware Aria Automation successfully, you must understand these components and their architecture.

2-3 Module Lessons

1. VMware Aria Automation Overview
2. VMware Aria Automation Architecture

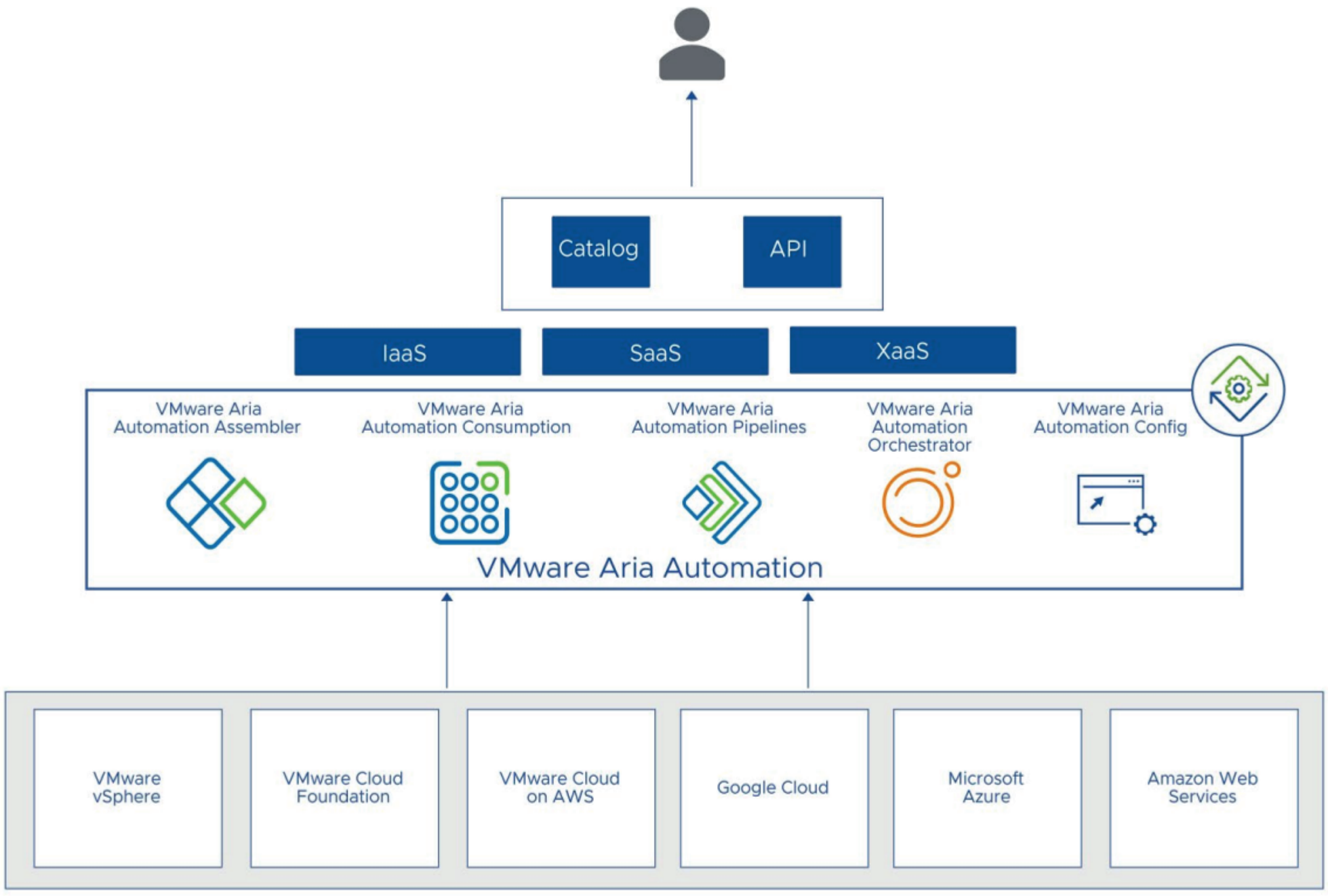
2-4 Lesson 1: VMware Aria Automation Overview

2-5 Learner Objectives

- Describe the purpose of VMware Aria Automation
- Identify the services offered by VMware Aria Automation
- Describe the SaaS version of VMware Aria Automation and identify its benefits
- Explain the VMware Aria Universal Suite licensing model

2-6 Introduction to VMware Aria Automation

The VMware Aria Automation platform automates the delivery of virtual machines, applications, and personalized IT services across a multivendor, multicloud infrastructure.



VMware Aria Automation delivers self-service automation, DevOps for infrastructure, Kubernetes automation, configuration management, and network automation.

You can integrate, streamline, and modernize traditional, cloud-native, and multicloud infrastructures with VMware Aria Automation.

VMware Aria Automation offers a common service catalog for administrators, developers, and business users to request IT services, including infrastructure, applications, and desktops.

2-7 VMware Aria Automation Key Components

VMware Aria Automation has several key components.



VMware Aria Automation has the following key components:

- VMware Aria Automation Assembler
- VMware Aria Automation Consumption
- VMware Aria Automation Pipelines
- VMware Aria Automation Orchestrator
- VMware Aria Automation Config

2-8 About VMware Aria Automation Assembler

VMware Aria Automation Assembler is a cloud-based service used to iteratively create and deploy machines, applications, and services to multiple clouds.



Multiple Cloud Accounts



Kubernetes Integration



Infrastructure as Code
Cloud Templates



Extensibility

The primary purpose of VMware Aria Automation Assembler is to create and deploy VMware Aria Automation Templates.

VMware Aria Automation Templates are the specifications that define the machines, applications, and services that you create on cloud resources through VMware Aria Automation Assembler.

VMware Aria Automation Templates were previously referred to as VMware Cloud Templates or blueprints.

VMware Aria Automation Assembler administrators configure the infrastructure to support the development and deployment of VMware Aria Automation Templates.

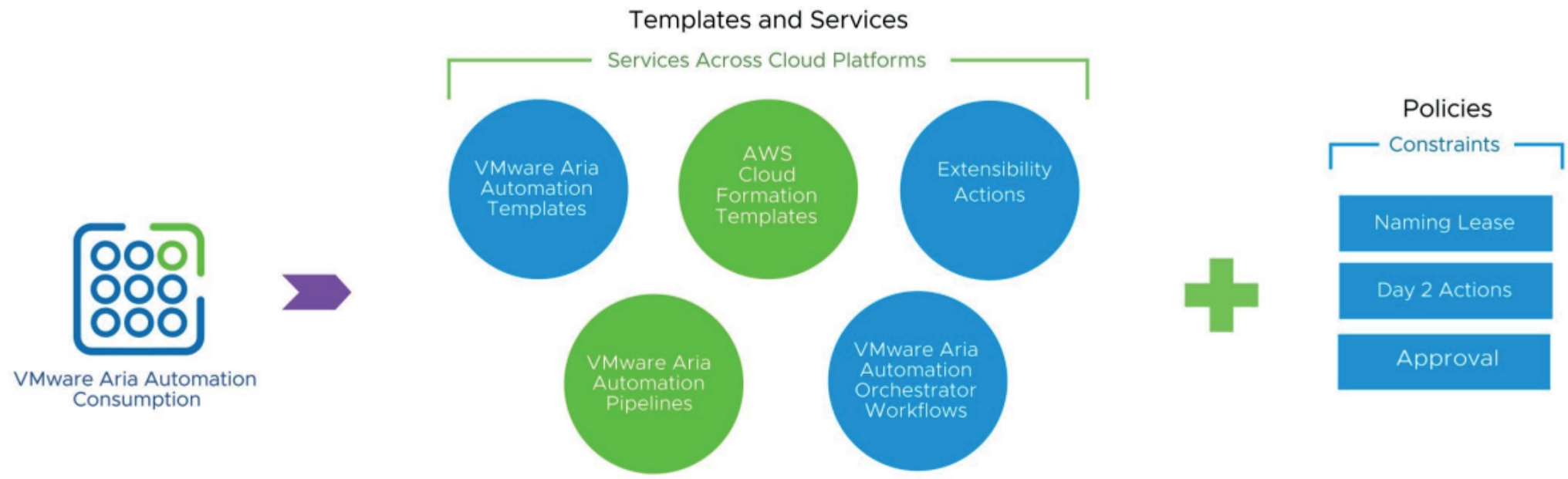
Project members use VMware Aria Automation Assembler to iteratively develop and deploy VMware Aria Automation Templates to a production-ready state.

VMware vCenter, VMware Cloud Foundation, Amazon AWS, Microsoft Azure, and Google Cloud Platform are some of the cloud accounts supported by VMware Aria Automation Assembler.

Users can create VMware Aria Automation Templates as code in YAML format.

2-9 About VMware Aria Automation Consumption

VMware Aria Automation Consumption aggregates services from multiple sources into a single catalog provided to the users. Users use this catalog to request the offered services.



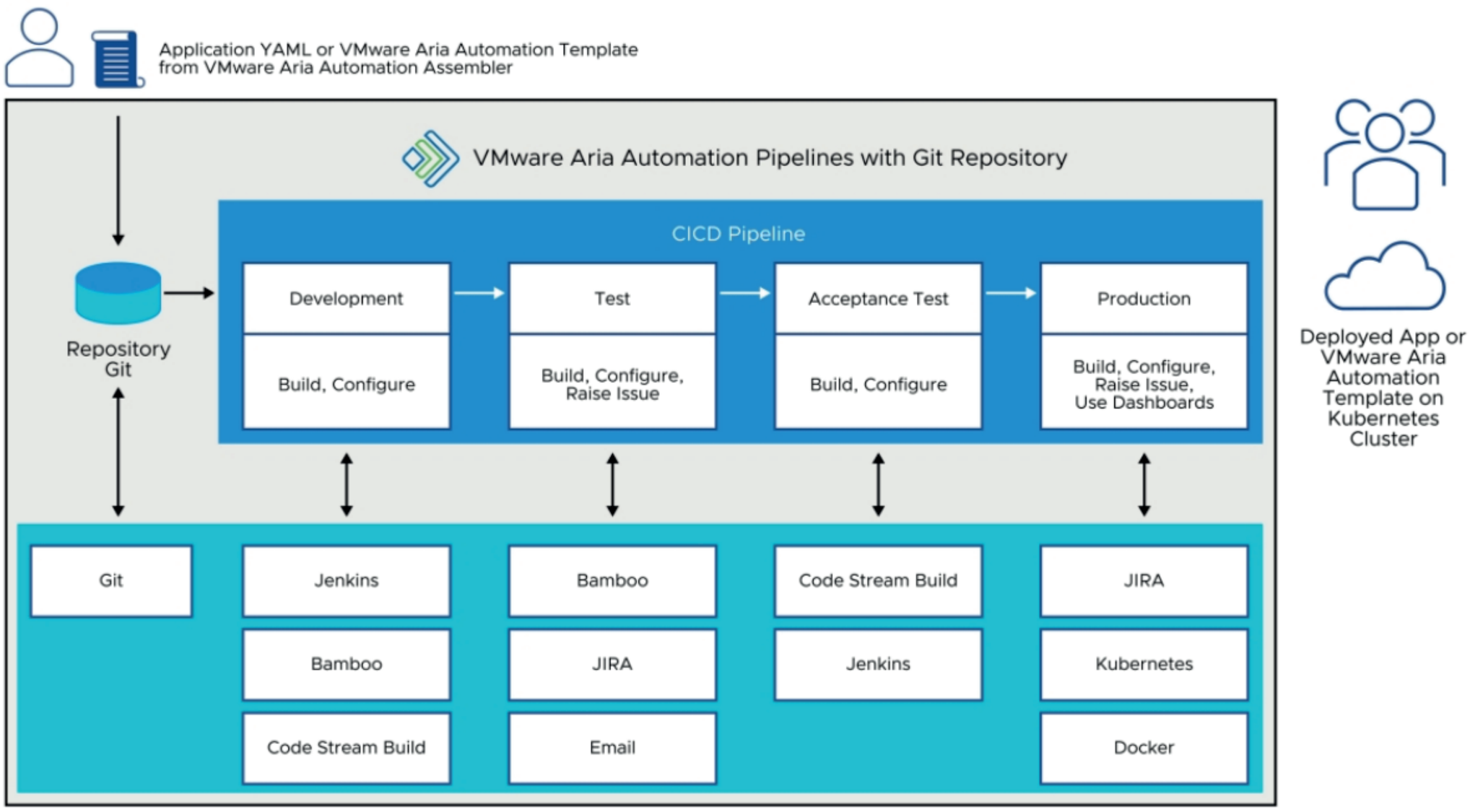
As a cloud administrator, you create one of the following catalog items:

- VMware Aria Automation Templates
- AWS CloudFormation Template
- VMware Aria Automation Pipelines
- Extensibility Action
- VMware Aria Automation Orchestrator Workflows

Users can use this created catalog to request catalog items.

2-10 About VMware Aria Automation Pipelines

VMware Aria Automation Pipelines is a Continuous Integration and Continuous Delivery (CI/CD) tool that you can use to deliver your software rapidly and reliably, with little overhead.



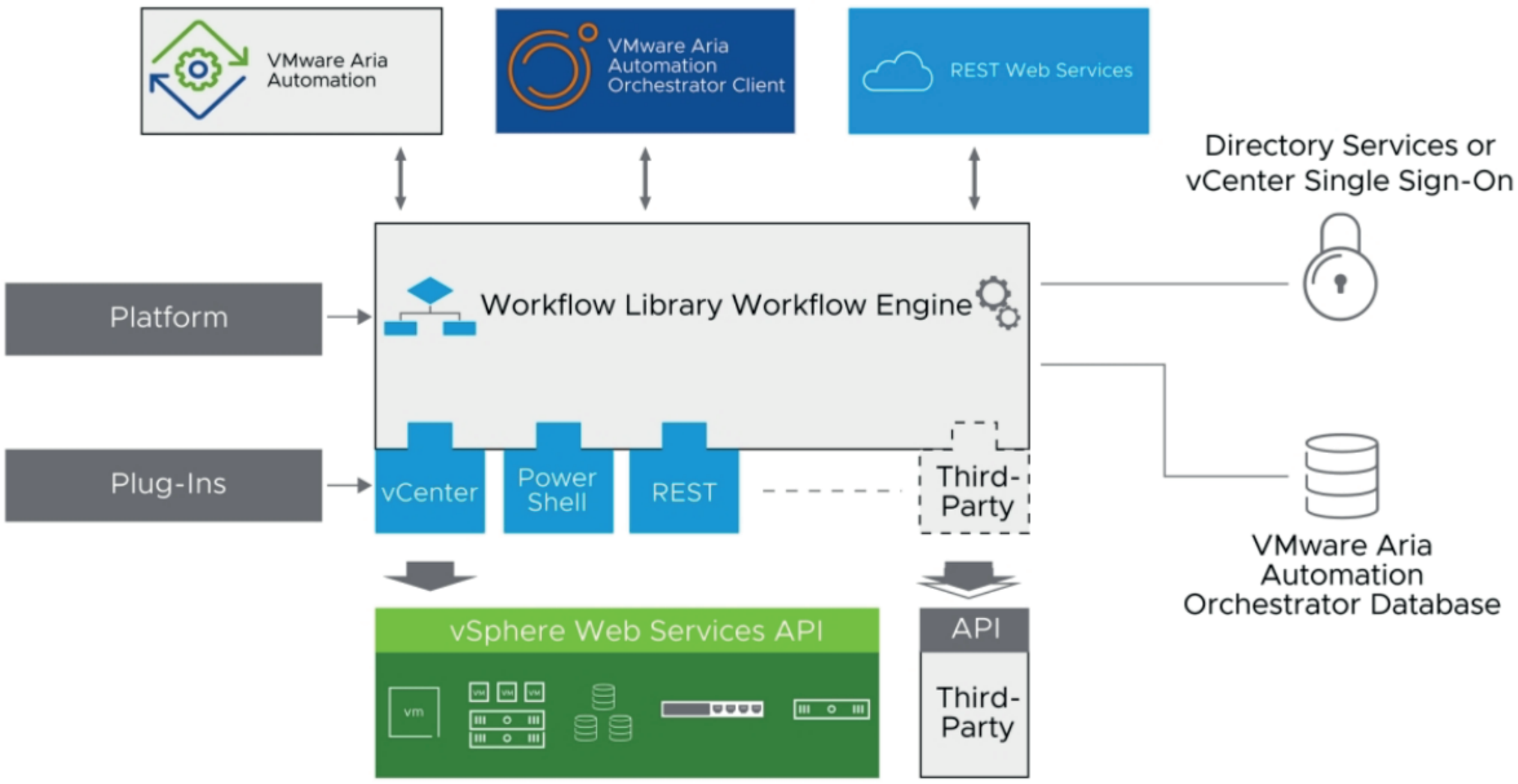
VMware Aria Automation Pipelines supports deploying monolithic legacy applications in addition to Docker and Kubernetes containers running on multiple clouds.

You can create a pipeline that runs actions to build, deploy, test, and release your software. VMware Aria Automation Pipelines runs your software through each stage of the pipeline until it is ready to be released to production.

You can integrate your pipeline with one or more DevOps tools, such as data sources, repositories, or notification systems, which provide data for the pipeline to run.

2-11 About VMware Aria Automation Orchestrator

VMware Aria Automation Orchestrator is a development and process-automation platform that provides an extensive library of workflows in addition to a workflow engine.



VMware Aria Automation Orchestrator uses workflows to simplify and automate complex data center infrastructure processes.

A workflow is a program that describes a sequence of tasks that achieve a specific function.

You can use the VMware Aria Automation Orchestrator prebuilt workflows or easily design new workflows to automate IT processes across VMware and third-party applications.

2-12 About VMware Aria Automation Config

VMware Aria Automation Config is a software configuration automation component in VMware Aria Automation. With VMware Aria Automation Config, you can easily define optimized, compliant software states and enforce them across your environment.



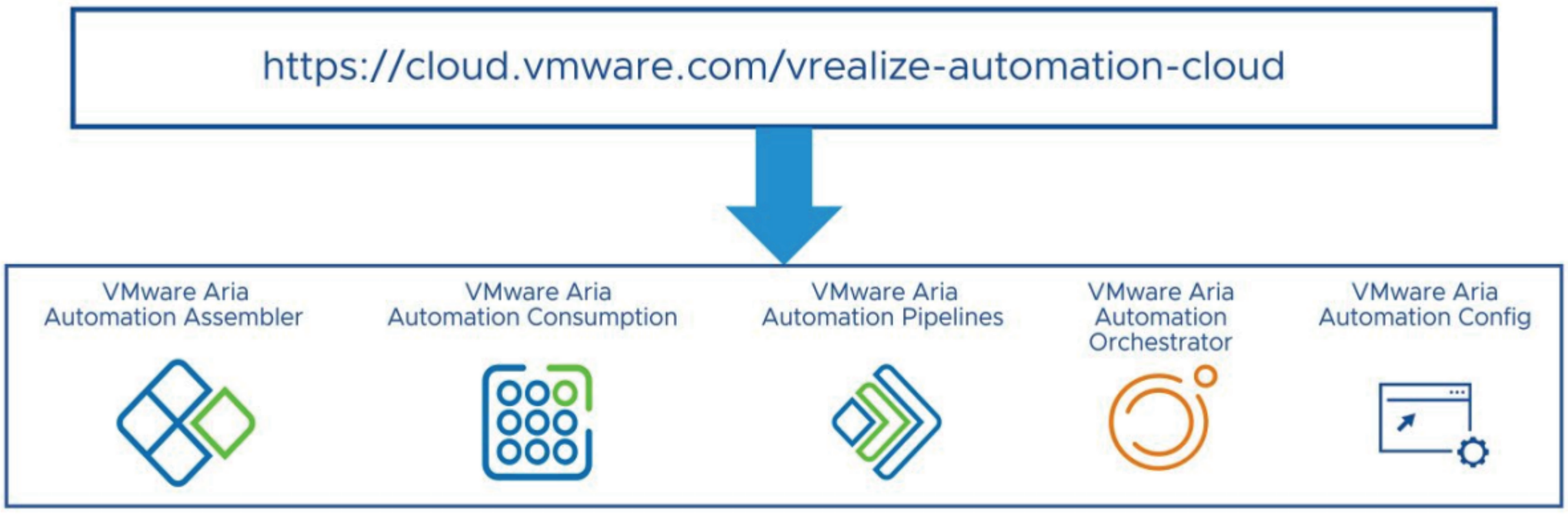
VMware Aria Automation Config is a configuration management tool, which ensures that a desired configuration state is maintained on target systems across multiple clouds. VMware Aria Automation Config is powered by Salt, an open-source automation and configuration management engine sponsored by VMware.

The core concept of VMware Aria Automation Config is remote execution using the server-client model.

VMware Aria Automation Config has two system classes: Salt master and Salt minion. The Salt master is responsible for sending commands to the Salt minions. The Salt master also aggregates and displays the results of commands that are received from the Salt minions. A single Salt master can manage thousands of Salt minions.

2-13 About VMware Aria Automation SaaS

VMware Cloud services offer a web-based software-as-a-service (SaaS) version of VMware Aria Automation.



The VMware Cloud services platform is a web-based application that offers software-as-a-service (SaaS) solutions.

You can log in to VMware Cloud services at https://cloud.vmware.com.

The first time you sign up for VMware Cloud services, you create a cloud service account with your VMware account. If you do not have a VMware account, you create one when you sign up.

2-14 Benefits of VMware Cloud Services

VMware Cloud services introduce numerous benefits and simplify administrative tasks.



VMware Cloud services introduce numerous benefits and simplify administrative tasks:

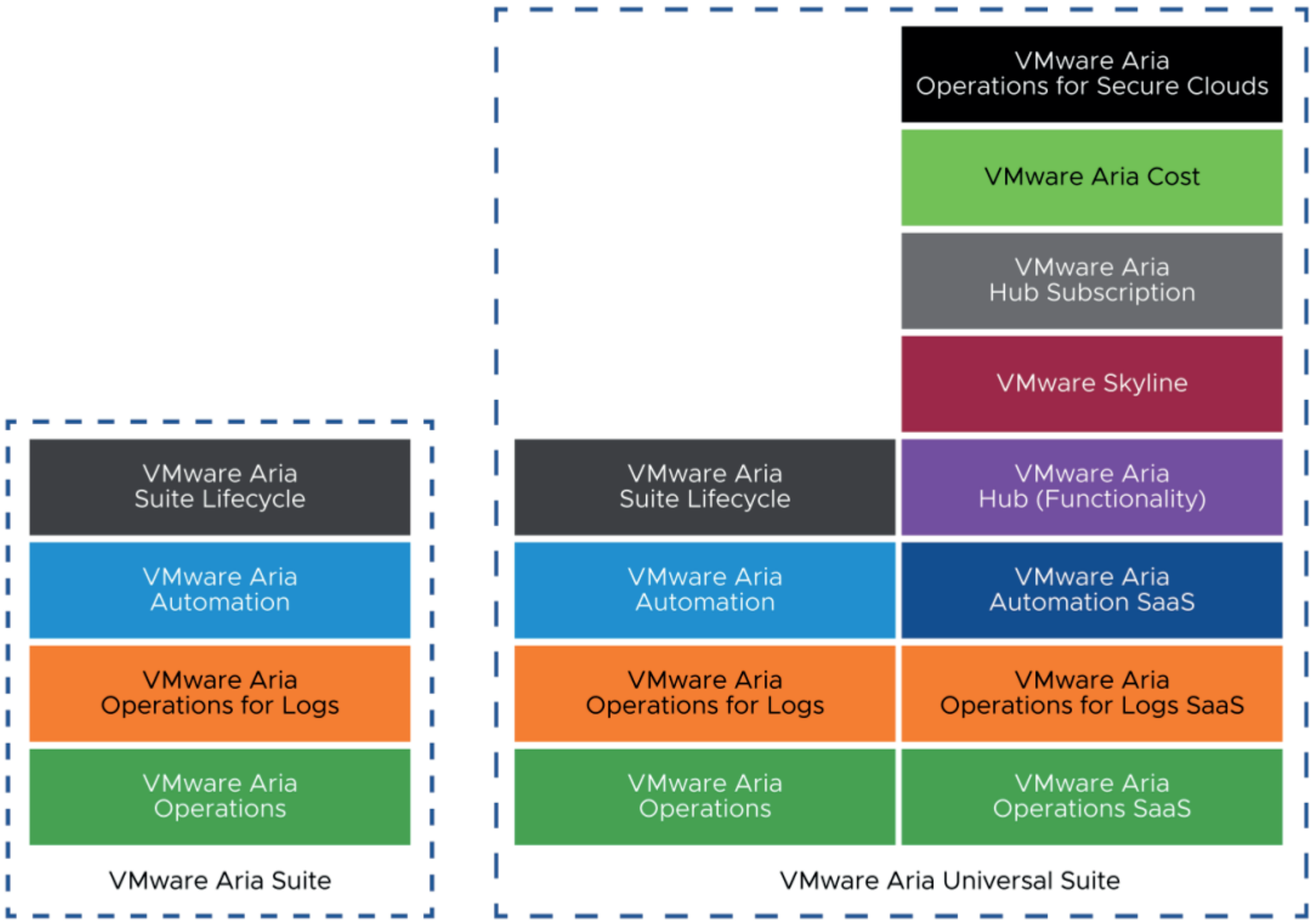
- You can chat with VMware Support 24/7 or create and manage support requests.
- You select the preferred payment method for your organization when you bring VMware Cloud services onboard.
- Your customer profile determines the payment methods available to you. For example, some users can only select a commit contract as their payment method, while others can select VMware funds and credit cards.
- You gain insight across both public and private clouds to know where workloads are deployed and how resources are being used.

2-15 VMware Aria Automation: 8.10 Versus SaaS

VMware Aria Automation 8.10	VMware Aria Automation SaaS
Existing VMware Aria customers	New VMware Aria customers
Does not require rapid scalability	Difficult to deploy and scale on-premises capacity
Cannot use SaaS due to security of compliance requirements	Organizations moving towards SaaS
Dependent on on-premises ecosystem tools (Service Desk, IPAM, load balancers, and so on)	Requires fast time for first provision

2-16 VMware Aria Universal Suite Licensing Model

VMware Aria Universal Suite is a SaaS management suite that combines both on-premises and SaaS capabilities for automation, operations, log analytics, and network visibility into one license.



This new subscription model offers the flexibility to deploy VMware Aria Automation components on-premises or consume VMware Aria services as SaaS interchangeably without the need to repurchase licenses.

Additional VMware Aria functionality is added by providing access to VMware Aria Hub functionalities and integration with VMware Skyline.

VMware Aria Universal Suite is available in four editions. See the pricing and comparison section on the VMware Aria Universal Suite product page at https://www.vmware.com/products/aria-universal-suite.html and see *VMware vRealize Cloud Universal and VMware vCloud Suite Subscription* at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-vrealize-cloud-universal-licensing-whitepaper.pdf.

2-17 Lab 1: Requesting a Service

Request a service from VMware Aria Automation:

1. Request a Service
2. Track Your Request
3. Examine Your Deployment
4. Delete Your Deployment

2-18 Review of Learner Objectives

- Describe the purpose of VMware Aria Automation
- Identify the services offered by VMware Aria Automation
- Describe the SaaS version of VMware Aria Automation and identify its benefits
- Explain the VMware Aria Universal Suite licensing model

2-19 Lesson 2: VMware Aria Automation Architecture

2-20 Learner Objectives

- Explain which components are used in a standard deployment
- Explain which components are used in a clustered deployment
- Identify the components of VMware Aria Automation
- Describe the role of Kubernetes in the VMware Aria Automation appliance

2-21 VMware Aria Automation Deployment Types

You can use one of the following approaches to deploy VMware Aria Automation:

- Standard deployment
- Clustered deployment

You choose your deployment type according to the needs of your business.

2-22 Standard Deployment Architecture

Standard deployments are used primarily for proof-of-concept and small environments. This deployment includes the following components:

- VMware Aria Suite Lifecycle
- Workspace ONE Access
- VMware Aria Automation

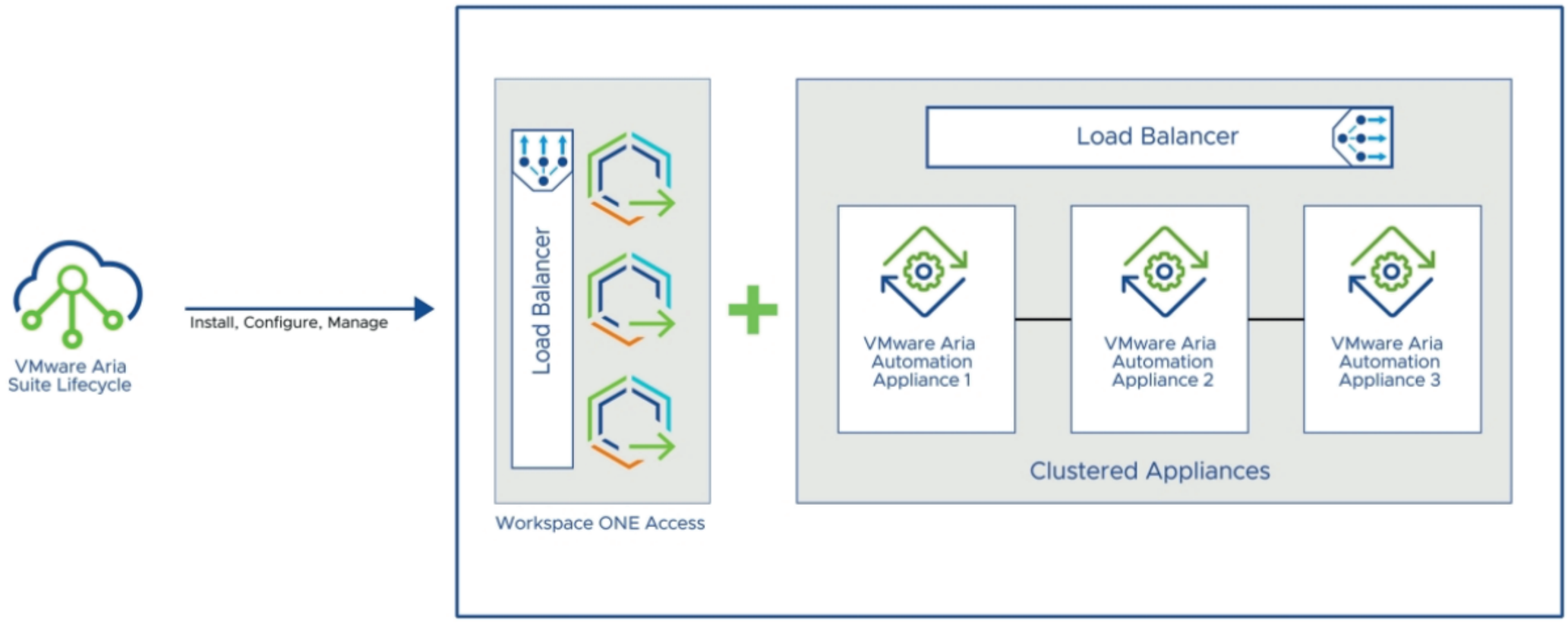


The standard deployment includes three appliances.

VMware Aria Suite Lifecycle is deployed first. It is then used to deploy and manage Workspace ONE Access and VMware Aria Automation.

2-23 Clustered Deployment Architecture

The clustered deployment is used in larger enterprises and has the following architecture.



The clustered deployment includes the following components:

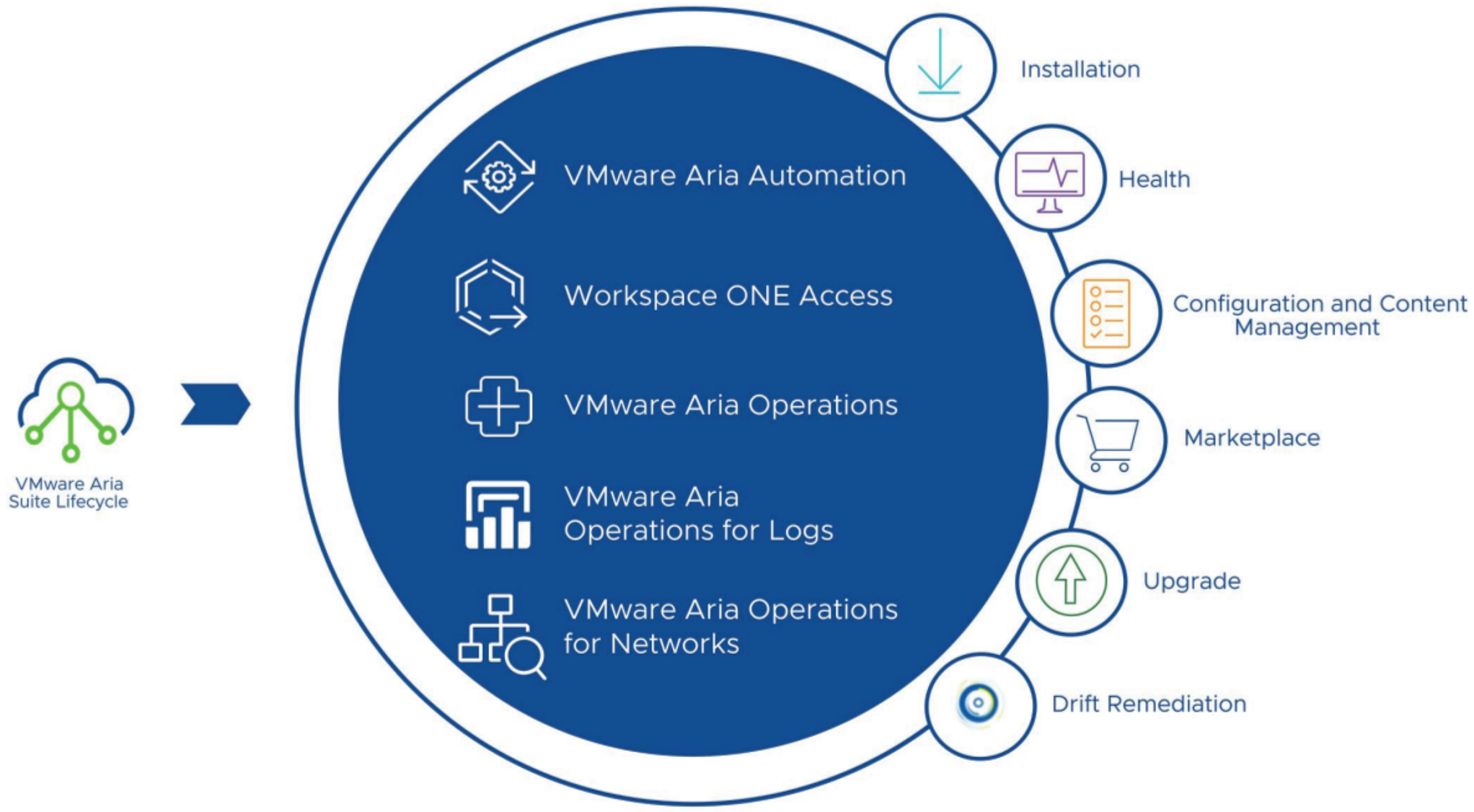
- One VMware Aria Suite Lifecycle appliance
- Three Workspace ONE Access appliances
- Three VMware Aria Automation appliances

A load balancer is required for this deployment.

This deployment achieves high availability and is recommended for production environments.

2-24 About VMware Aria Suite Lifecycle

VMware Aria Suite Lifecycle provides a comprehensive solution to deploy, upgrade, configure, and manage the VMware Aria Suite products.



In a traditional configuration, customers oversee the installation and maintenance of the VMware Aria product portfolio by managing each of the individual product components separately. VMware Aria Suite Lifecycle unifies all suite management tasks into a single console. VMware Aria Suite Lifecycle simplifies installation and configuration management of VMware Aria Suite products.

VMware Aria Suite Lifecycle automates day 0 to day 2 operations of the entire VMware Aria Suite.

VMware Aria Suite Lifecycle automates the following processes from a single platform:

- Installation
- Configuration and content management
- Environment health
- Drift remediation
- Upgrades

As a result, IT management and cloud administration resources can focus on business-critical initiatives, improving time to value, reliability, and consistency.

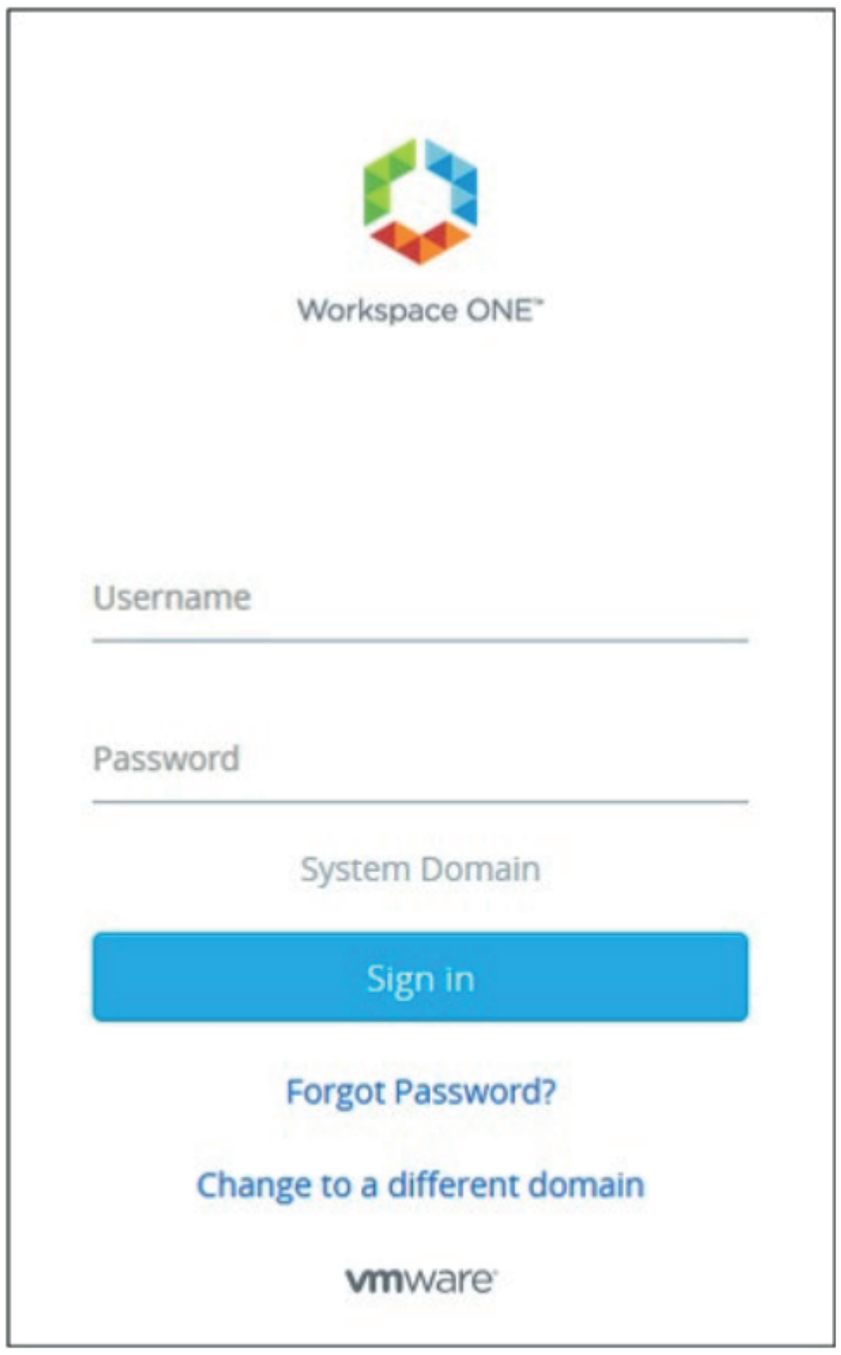
VMware Aria Suite Lifecycle has a locker repository that you can use to secure and manage passwords, certificates, and licenses for the VMware Aria Suite product solutions and integrations.

Through integration with VMware Aria Hub Subscription, VMware Aria Suite Lifecycle supports VMware Aria Universal Suite license usage metering to provide insights about usage and subscription management.

2-25 About Workspace ONE Access

Workspace ONE Access is an identity-as-a-service (IDaaS) solution:

- Workspace ONE Access provides multifactor authentication, conditional access, and single sign-on (SSO) to SaaS, web, and native mobile applications.
- VMware products can use Workspace ONE Access as an enterprise SSO solution.



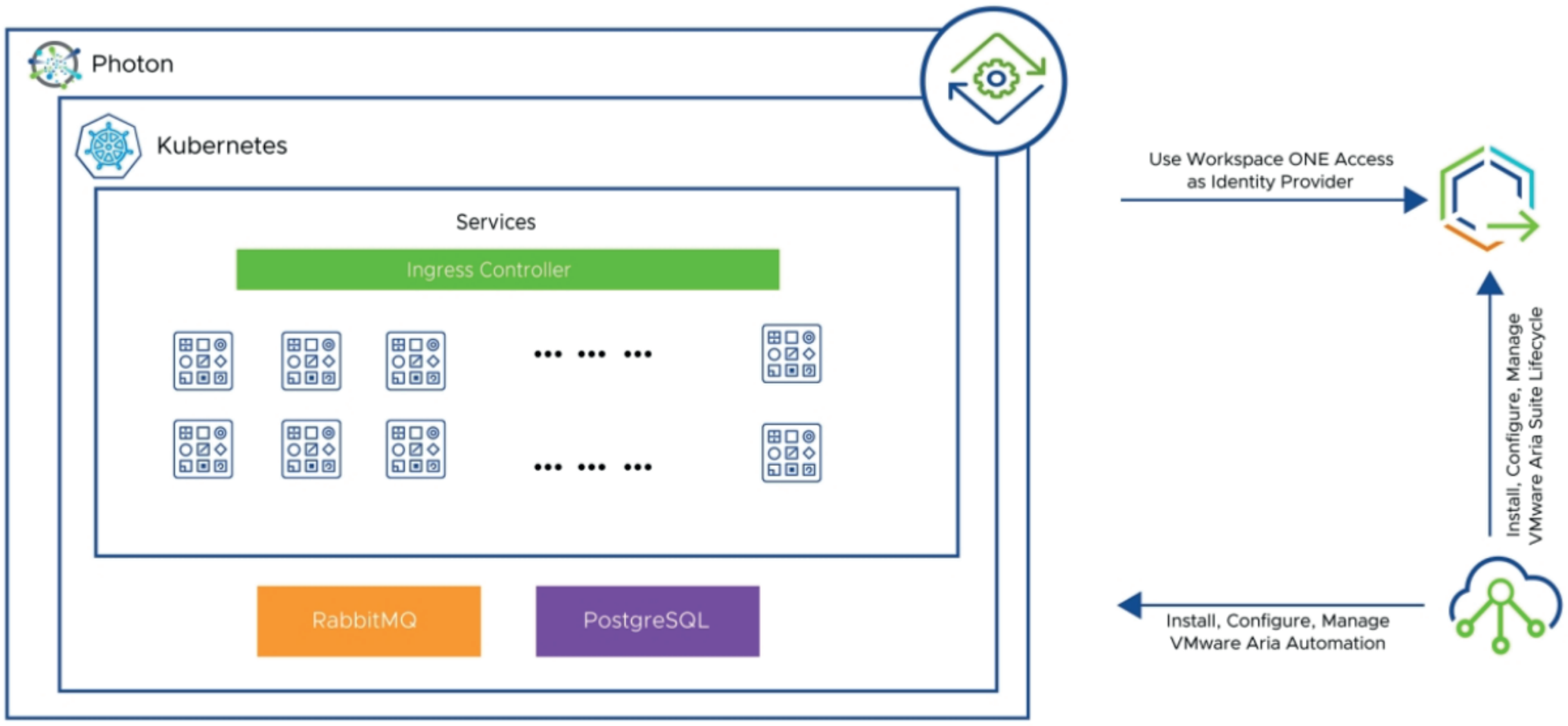
Workspace ONE Access offers the following functions:

- Set up and manage authentication methods and access policies
- Customize a catalog of resources for your organization's applications
- Provide a secure multidevice-managed user with access to resources, including web applications, Citrix-based applications, and VMware Horizon desktop and application pools

Workspace ONE Access was formerly known as VMware Identity Manager.

2-26 VMware Aria Automation Appliance

The VMware Aria Automation appliance is powered by Photon OS. VMware Aria Automation includes native Kubernetes to host containerized services.



The VMware Aria Automation appliance is installed on the Photon OS.

Native Kubernetes is installed on Photon. All the core VMware Aria Automation services run as Kubernetes pods.

A pod is the smallest deployable unit in Kubernetes. The Docker engine hosts the containers in a pod.

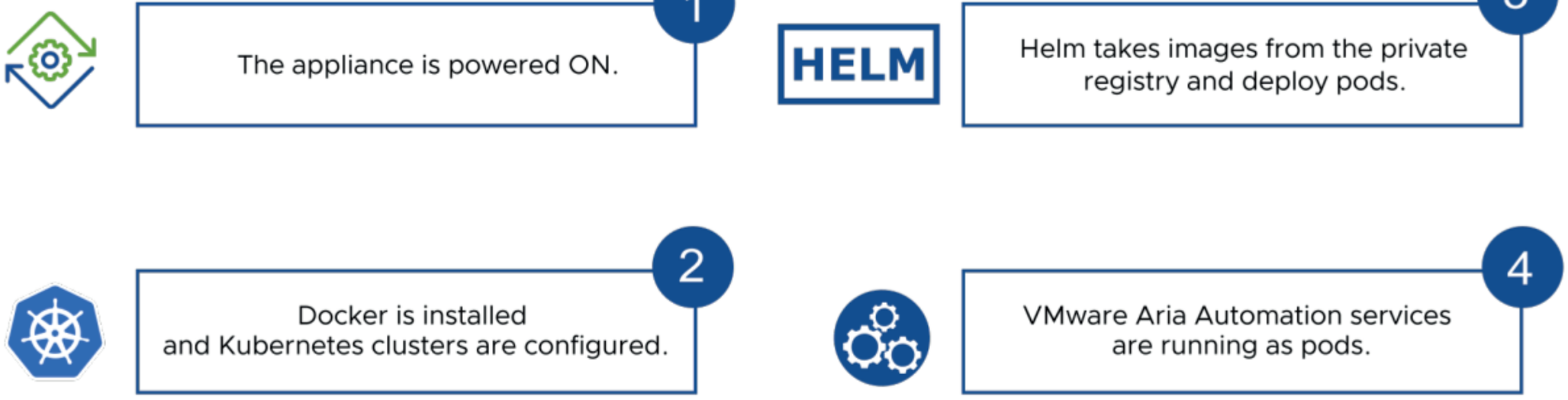
RabbitMQ is the industry-standard message bus used in VMware Aria Automation. RabbitMQ runs as a pod.

PostgreSQL is the default and only supported database for VMware Aria Automation. PostgreSQL runs as a pod and uses a Persistent Volume (PV) to store data.

A PV is a storage resource in the Kubernetes cluster. A PV might represent a host path (`/mnt/data`) or an iSCSI, NFS volume.

2-27 Role of Kubernetes

The VMware Aria Automation appliance services are deployed and managed as pods by using industry-standard Kubernetes.



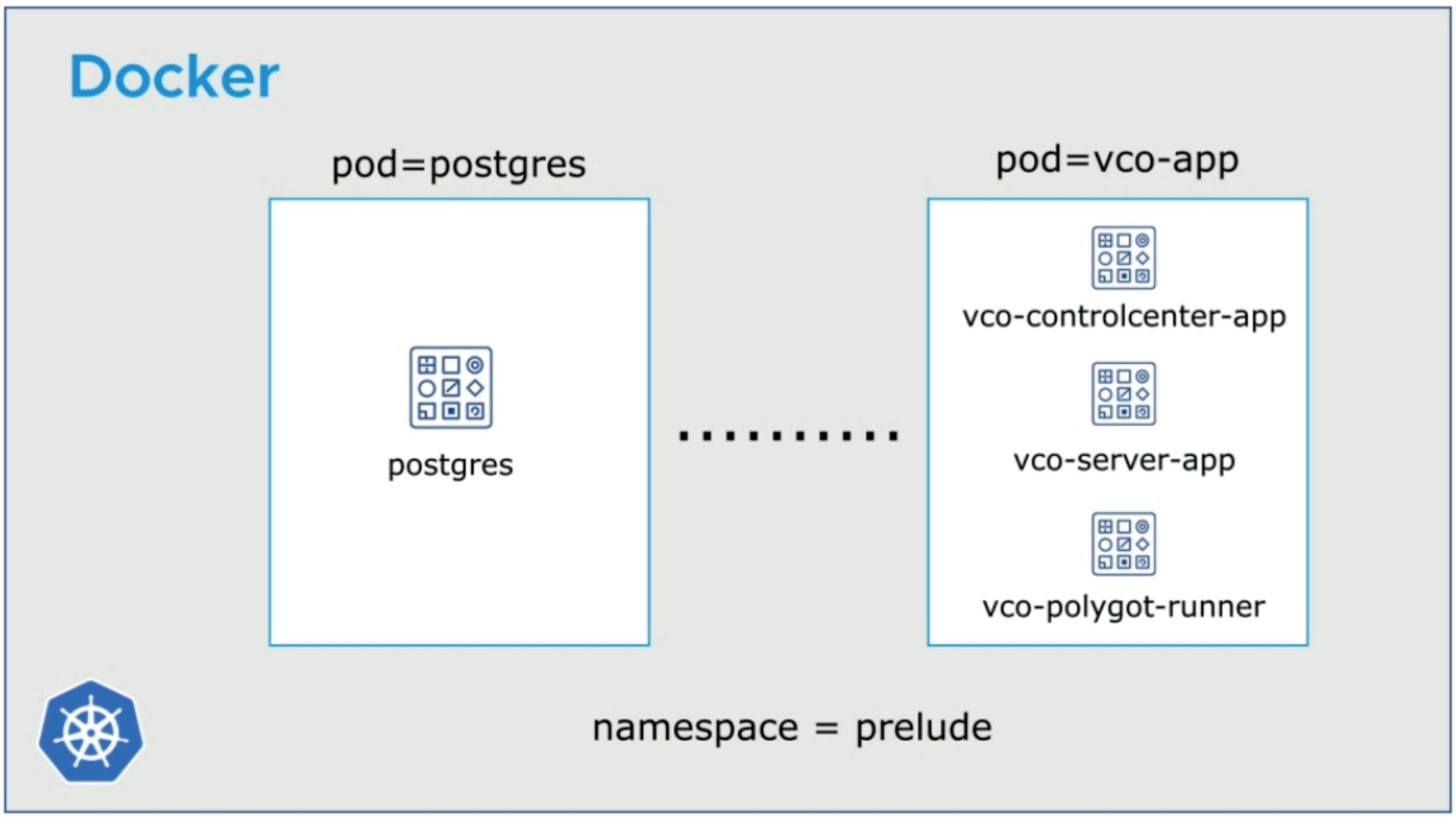
The VMware Aria Automation appliance has the following power-on sequence:

1. The VMware Aria Automation appliance is deployed and powered on for the first time.
2. Docker is installed and Kubernetes clusters are configured during the first boot.
3. Helm takes images that are stored in a private Docker registry on the appliance and deploys Kubernetes services that are running as pods.

   Helm is a package manager for Kubernetes. It is used to package, configure, and deploy applications and services onto Kubernetes clusters. Service configurations are stored in the Kubernetes-native Helm package manager format called charts. A chart describes a service in VMware Aria Automation (containers, number of instances, network settings, persistence, and so on) and is stored in a human-readable text format.
4. VMware Aria Automation services run as Kubernetes pods.

2-28 VMware Aria Automation Services

The VMware Aria Automation services run as Docker containers in Kubernetes pods.



A Kubernetes service is an abstraction that defines a logical set of pods and a policy by which to access them (sometimes this pattern is called a microservice).

Each Kubernetes pod hosts one or more containers.

For example, the VMware Aria Automation Orchestrator service runs as a pod hosting the following key containers:

- Control Center is used to manage the operation of VMware Aria Automation Orchestrator, including plug-ins.
- The vco-server service is the orchestration engine responsible for running workflows.

The databases run as a pod managed by Kubernetes whose data is stored in a persistent storage volume.

Namespaces are used to divide Kubernetes cluster resources between multiple users.

2-29 Lab 2: Exploring the VMware Aria Automation Architecture

Explore the architecture of a standard VMware Aria Automation deployment:

1. Examine VMware Aria Suite Lifecycle
2. Examine Workspace ONE Access
3. Examine VMware Aria Automation Services
4. Examine the VMware Aria Automation Appliance

2-30 Review of Learner Objectives

- Identify the components used in a standard deployment
- Identify the components used in a clustered deployment
- Identify the components of VMware Aria Automation
- Describe the role of Kubernetes in the VMware Aria Automation appliance

2-31 Key Points

- VMware Aria Automation reduces the complexity of provisioning virtual and cloud machines.
- VMware Aria Automation enables a business-relevant self-service cloud infrastructure.
- VMware Aria Automation services run as pods managed by Kubernetes.

Questions?

Module 3

Installing VMware Aria Automation

3-2 Importance

To set up a VMware Aria Automation environment, you must install VMware Aria Suite Lifecycle, Workspace ONE Access, and VMware Aria Automation. Deploying these products separately requires time and effort.

VMware Aria Easy Installer deploys all three components with minimal steps in less time. You can use the Quickstart wizard to easily configure the infrastructure and deploy the first VMware Aria Automation template.

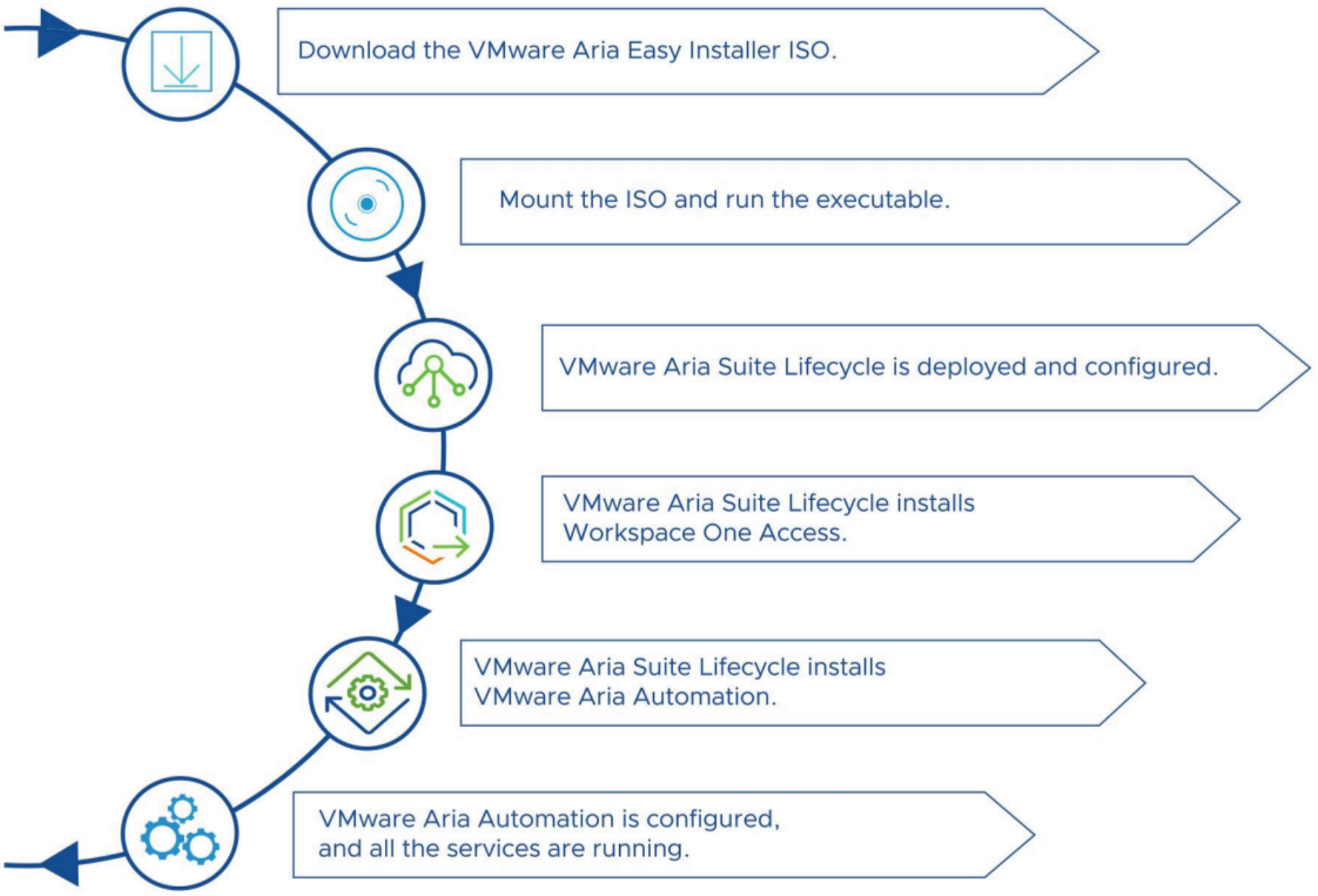
3-3 Lesson 1: Installing VMware Aria Automation

3-4 Learner Objectives

- Describe the VMware Aria Automation installation process
- Use VMware Aria Easy Installer to set up a VMware Aria Automation environment
- Discuss the importance of VMware Aria Migration
- Use the Quickstart wizard to configure the infrastructure and deploy a VMware Aria Automation template

3-5 Installation Process

VMware Aria Easy Installer simplifies the installation and configuration of VMware Aria Suite Lifecycle, Workspace ONE Access, and VMware Aria Automation.



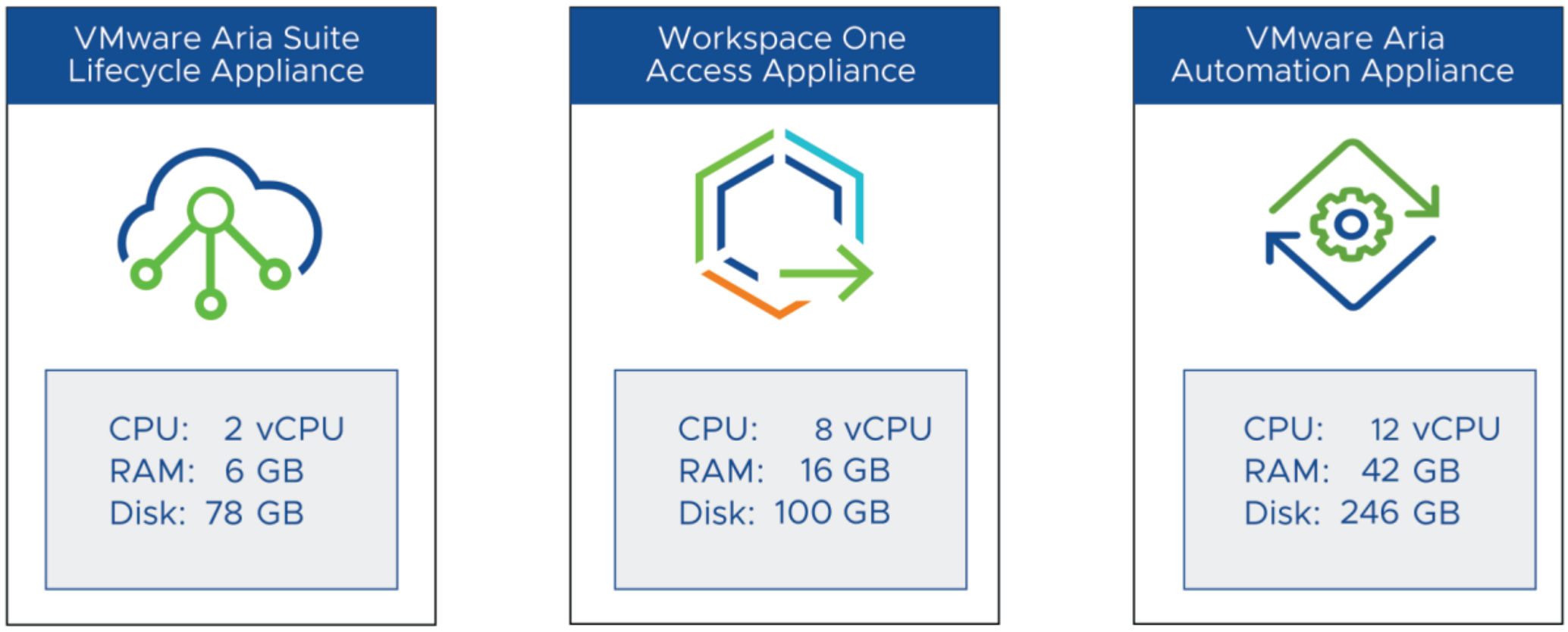
Installing each component consumes much time and effort. VMware Aria Easy Installer simplifies this installation process through a single installation wizard.

The steps in the diagram are high-level steps performed by VMware Aria Easy Installer.

This course covers only the installation of a standard deployment.

3-6 Minimum System Resources

The VMware Aria Suite Lifecycle, Workspace ONE Access, and VMware Aria Automation appliances must meet minimum system resource requirements.



VMware Aria Easy Installer installs the following appliances:

- VMware Aria Suite Lifecycle 8.10.0.6
- Workspace ONE Access 3.3.4
- VMware Aria Automation 8.10

For more information, please see *Installing vRealize Automation with vRealize Easy Installer* at https://docs.vmware.com/en/vRealize-Automation/index.html.

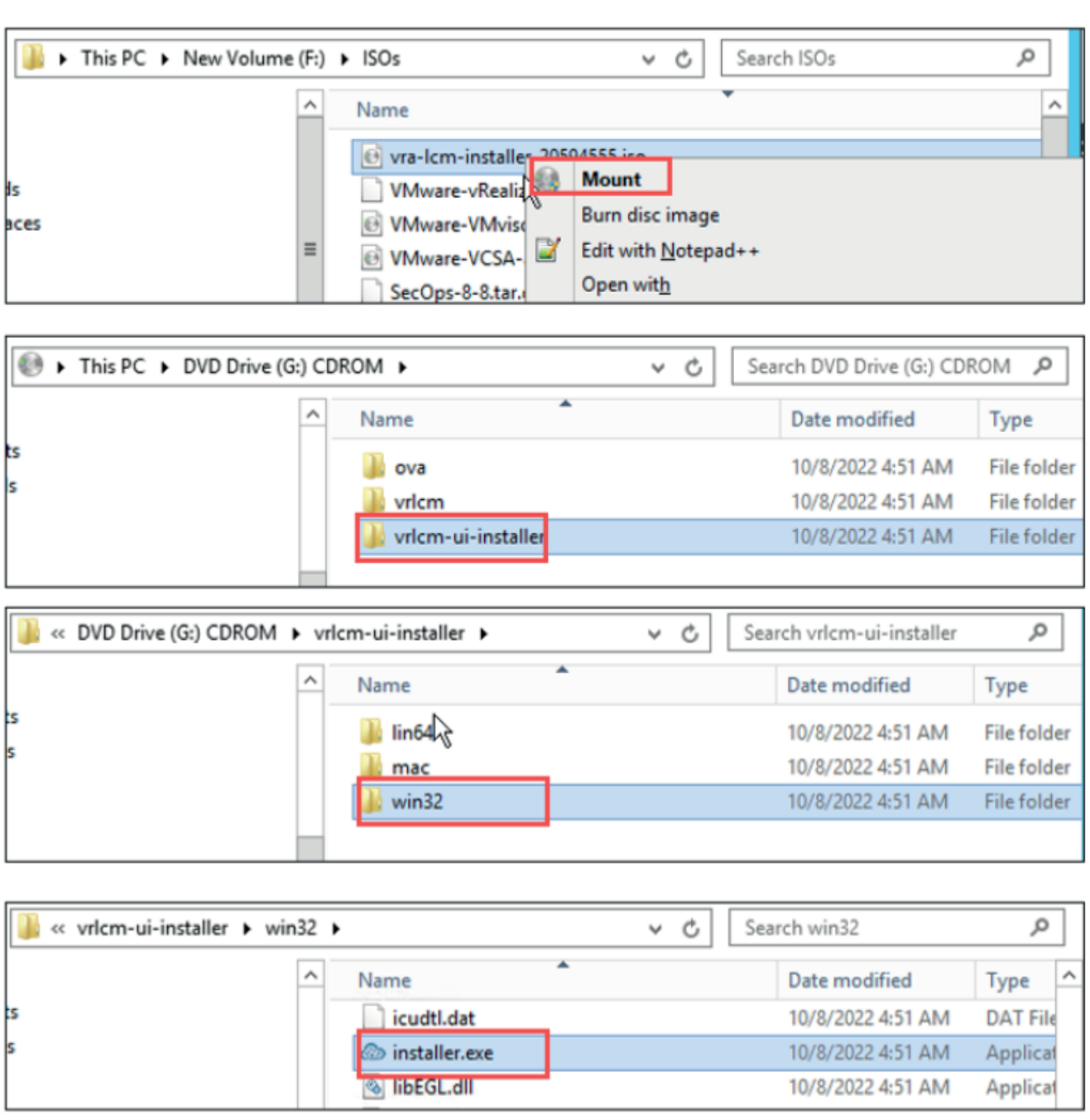
3-7 VMware Aria Easy Installer: ISO

The first step is to download the VMware Aria Easy Installer ISO image and mount it.

Mount the ISO image on any guest OS:

- Linux
- macOS
- Windows

Start the VMware Aria Easy Installer wizard by running the executable file.



Download the easy installer at https://my.vmware.com/web/vmware/downloads/.

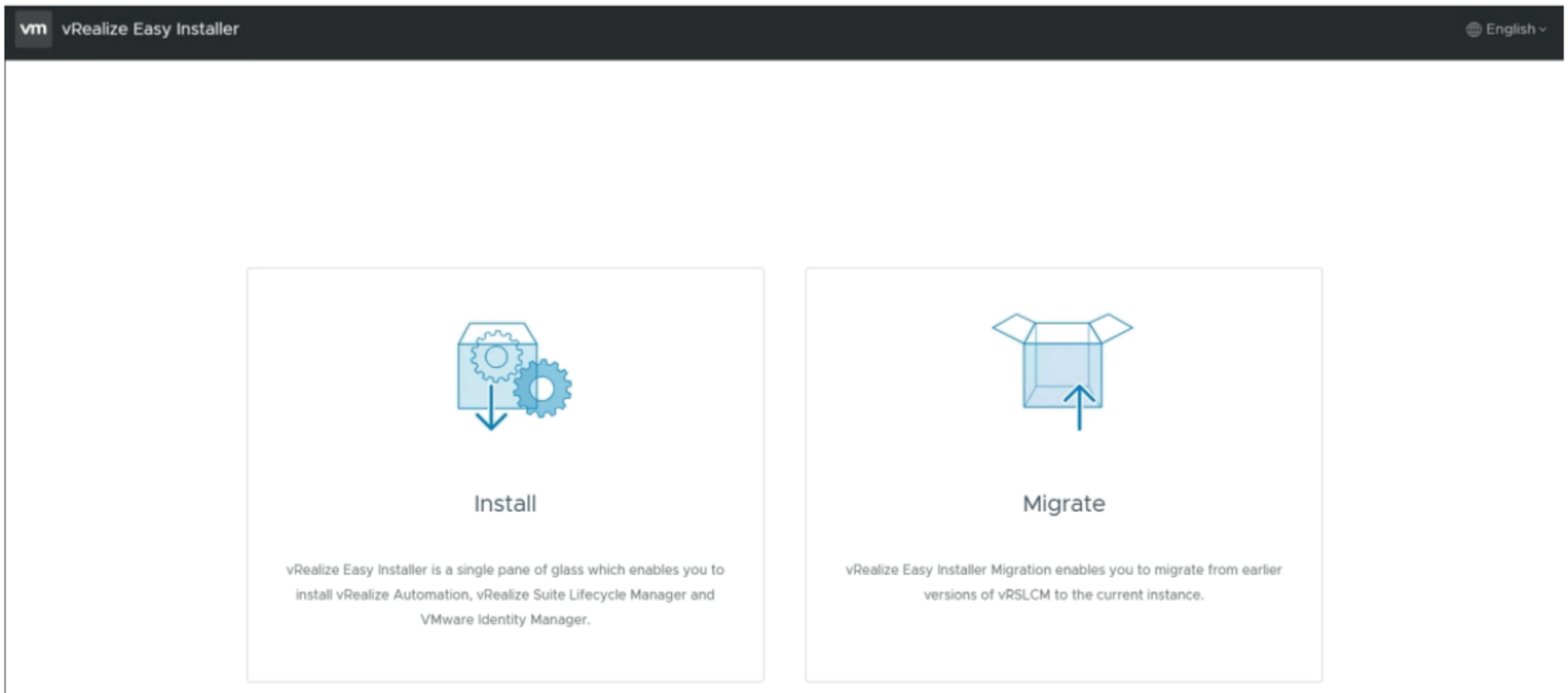
The guest OS that runs VMware Aria Easy Installer must be connected to vCenter.

The screenshot is from a Windows OS.

3-8 VMware Aria Easy Installer: Home Page

The following options are available in the VMware Aria Easy Installer home page:

- **Install**: Installs VMware Aria Suite Lifecycle, Workspace ONE Access, and VMware Aria Automation
- **Migrate**: Migrates data from earlier versions of VMware Aria Suite Lifecycle to the current instance



Direct migration from vRealize Lifecycle Manager 2.1 is supported. The VMware Aria Suite Lifecycle instances on versions earlier to 2.1 must be upgraded to version 2.1 before migration.

The following data can be migrated:

- Data centers and vCenter systems
- All existing environments
- DNS, SNMP, NTP, MyVMware and proxy details
- Workspace ONE Access installation or import
- Blackstone content endpoints

Blackstone content cannot be migrated.

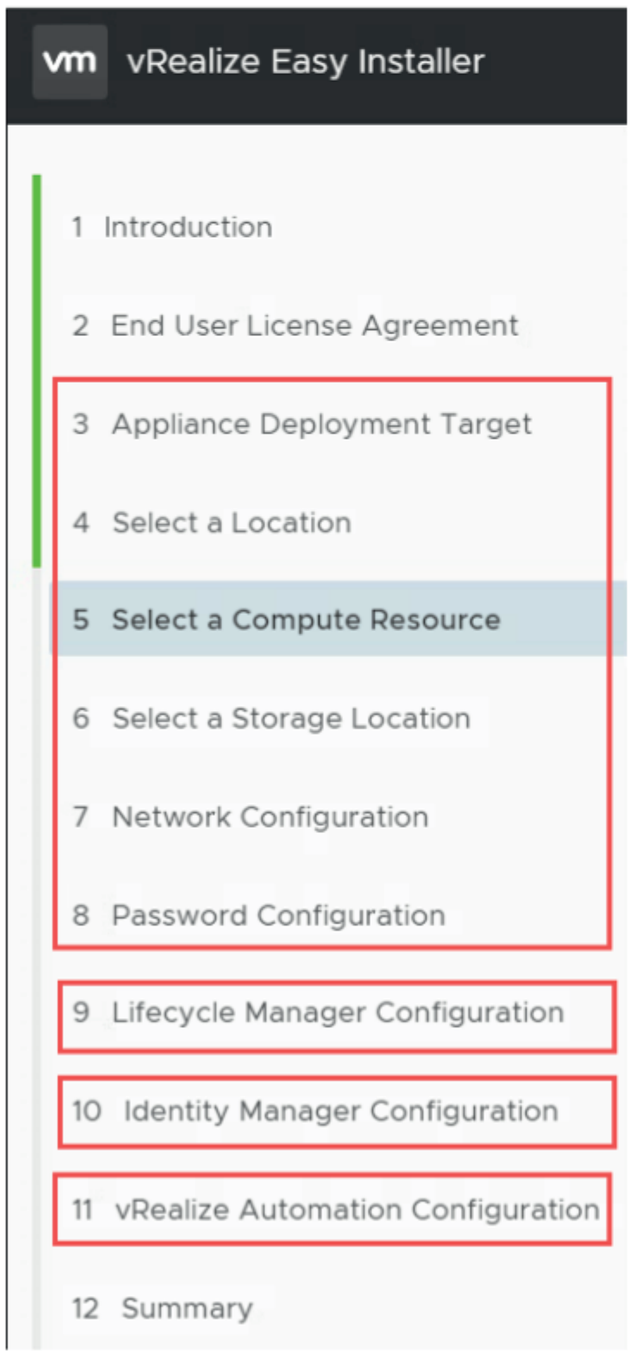
3-9 VMware Aria Easy Installer: Sections

VMware Aria Easy Installer simplifies the installation by splitting the configuration into multiple sections, which can be categorized as follows:

- Common configurations
- Appliance-specific configurations

The common configurations define the following settings:

- Target vCenter system
- Target data center or VM folder
- Target compute resources
- Target datastore
- Common network settings
- Common password



VMware Aria Easy Installer includes the following sections:

- **Appliance Deployment Target**: Specify the vCenter FQDN or IP address with administrator credentials.
- **Select a Location**: Select the data center or folder to place the appliances.
- **Select a Compute Resource**: Select a vSphere cluster.
- **Select a Storage Location**: Select a datastore and enable thin provisioning, if required.
- **Network Configuration**: Configure the target network, network subnet, gateway, DNS servers, domain name, and NTP servers.
- **Password Configuration**: Set passwords for all products.

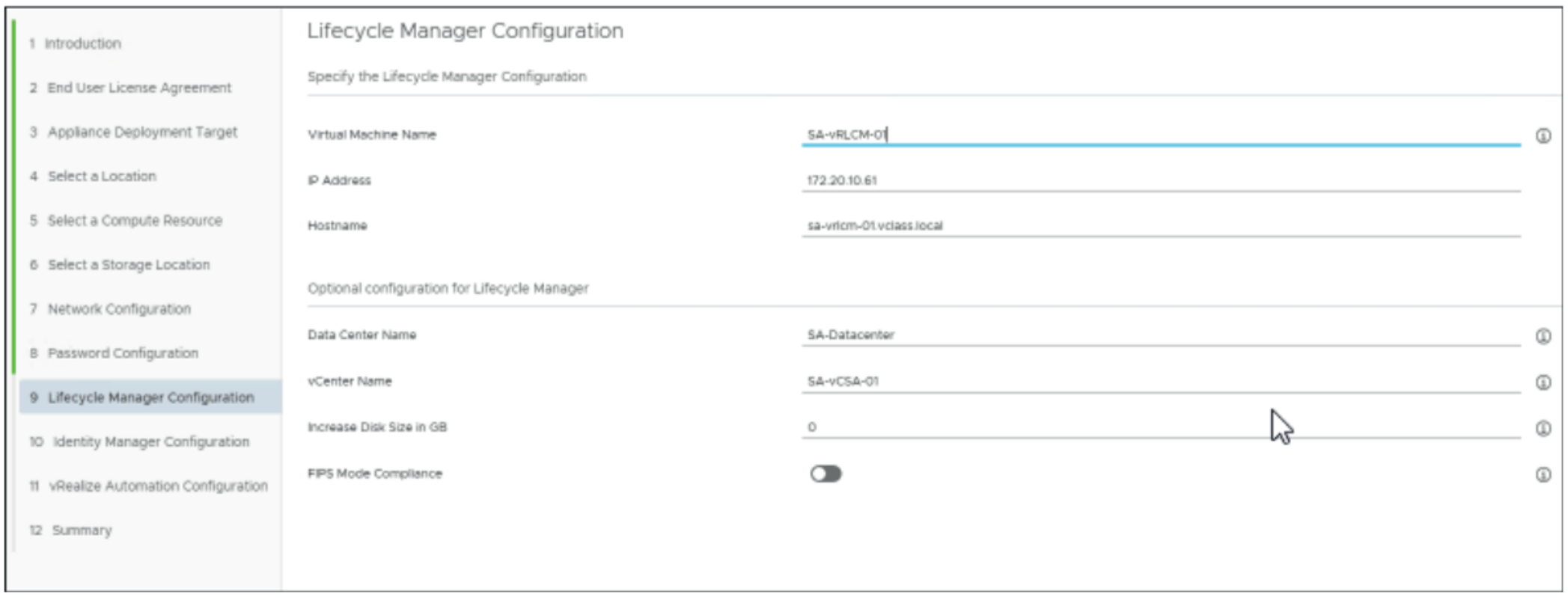
The following passwords are configured:

- VMware Aria Suite Lifecycle root password and administrator password
- Workspace ONE Access administrator password, SSH user password, root password, and password for the default configuration user that is used while integrating products
- VMware Aria Automation root password

The defined password must contain at least one digit, one uppercase character, one lowercase character, and one special character. Special characters include ! @ # $ % ^ &. The minimum length is 8 characters, and the maximum length is 16 characters.

3-10 VMware Aria Suite Lifecycle Configuration

You define the virtual machine name, IP address, and host name for the VMware Aria Suite Lifecycle appliance.



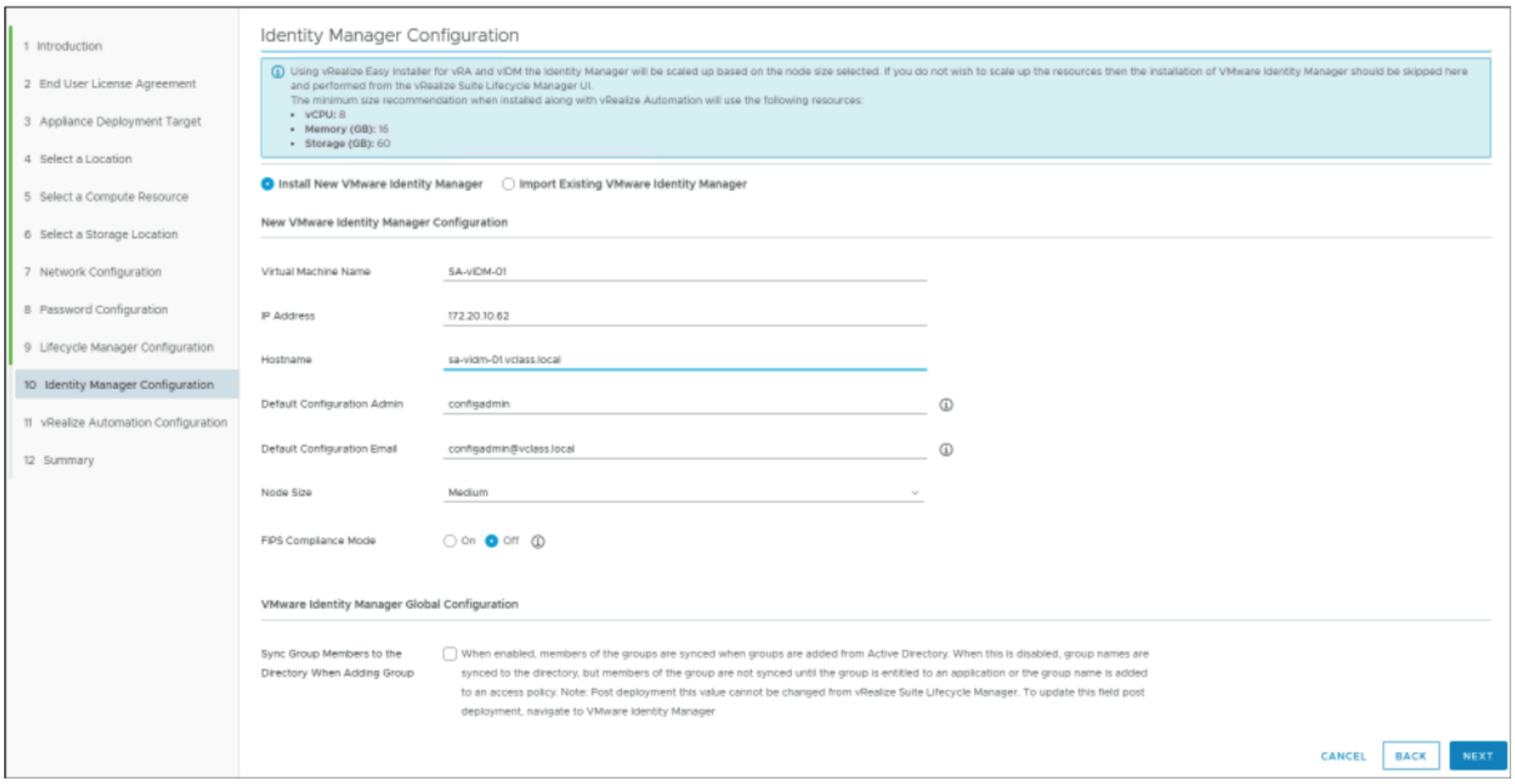
The other configuration settings are as follows:

- **Data Center Name**: Data center name in VMware Aria Suite Lifecycle to group multiple vCenter systems
- **vCenter Name**: Name defined for the target vCenter system used in VMware Aria Suite Lifecycle
- **Increase Disk Size in GB**: Extra disk space defined to increase during installer run
- **FIPS Mode Compliance**: Toggle that activates or deactivates the Federal Information Processing Standards (FIPS) mode

  When FIPS is activated, inbound and outbound network traffic on port 443 uses encryption that is compliant with FIPS.

3-11 Workspace ONE Access Configuration

Define the virtual machine name, IP address, and host name for the Workspace ONE Access appliance.



This step is optional.

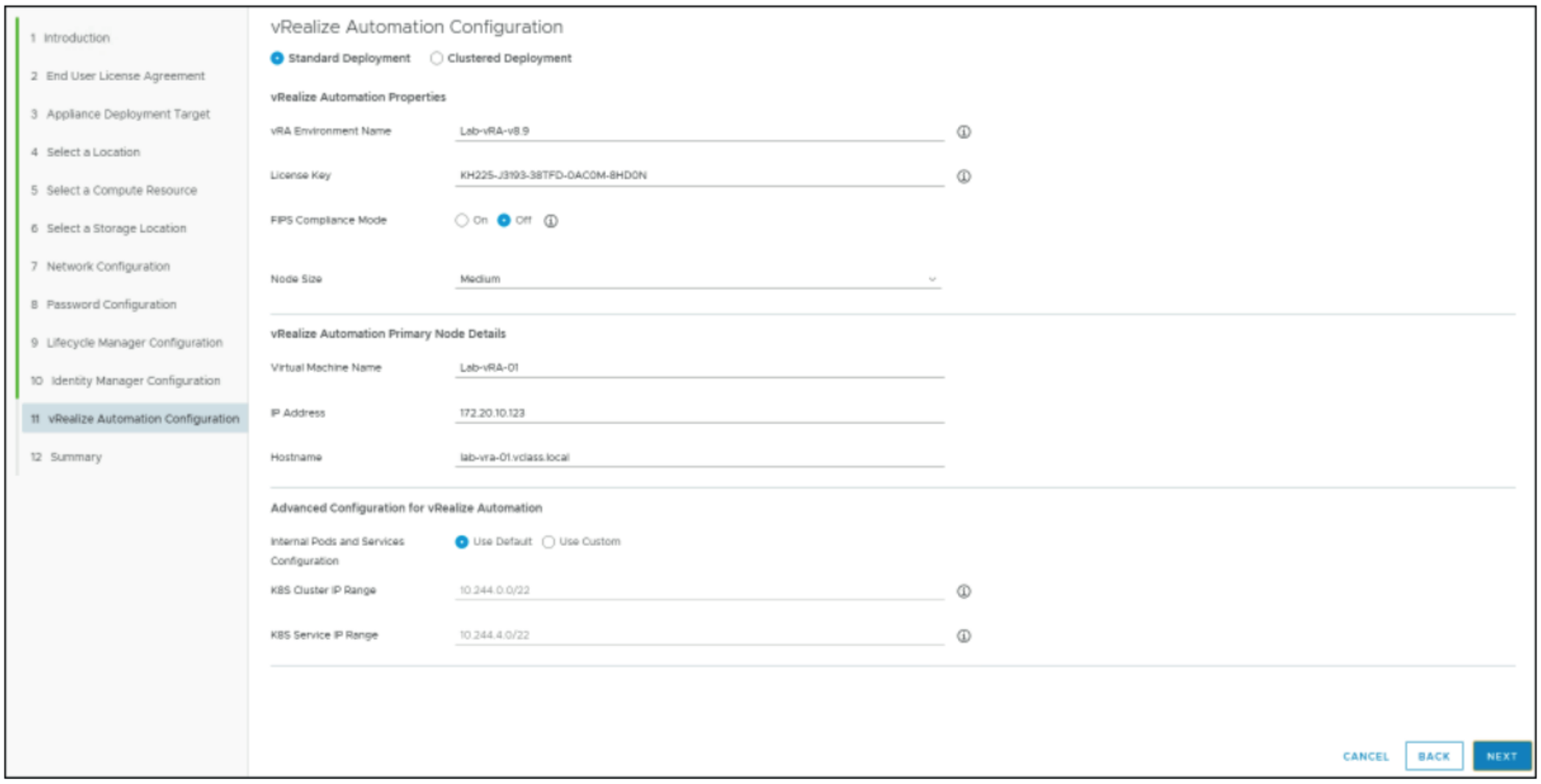
You choose to either install a new Workspace ONE Access appliance or import an existing one.

The other configuration settings are as follows:

- **Default Configuration Admin/Email**: User who integrates products with Workspace ONE Access
- **Node Size**: Medium, Large, Extra Large, and Extra Extra Large
- **Sync Group Members to the Directory When Adding Group**: Check box to decide whether group members are synced when groups are added from Active Directory directly or when the group is linked to an application or access policy

3-12 VMware Aria Automation Configuration

Define the virtual machine name, IP address, and host name for VMware Aria Automation. The license key is specified here.



This step is optional.

You choose between standard and clustered deployments. This course covers only standard deployment.

The other configuration settings are as follows:

- **VMware Aria Automation Environment Name**: Name for the VMware Aria Automation environment in VMware Aria Suite Lifecycle
- **FIPS Mode Compliance**: Toggle that activates or deactivates the FIPS mode

  When FIPS is activated, inbound and outbound network traffic on port 443 uses FIPS-compliant encryption.
- **Node Size**: Medium and Extra Large

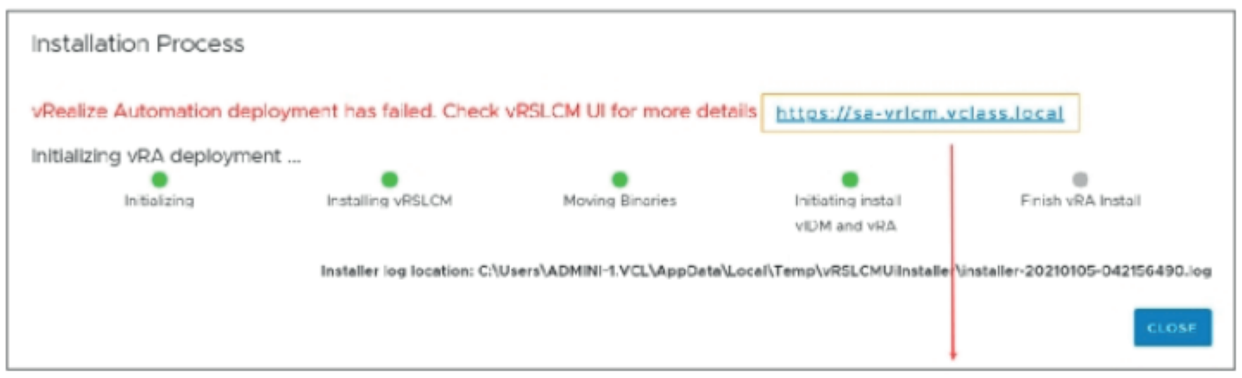
The 10.244.0.0/24 and 10.244.4.0/24 network CIDR ranges are by default reserved for Kubernetes clusters pods and services. Change these default IP address ranges for Kubernetes clusters and services.

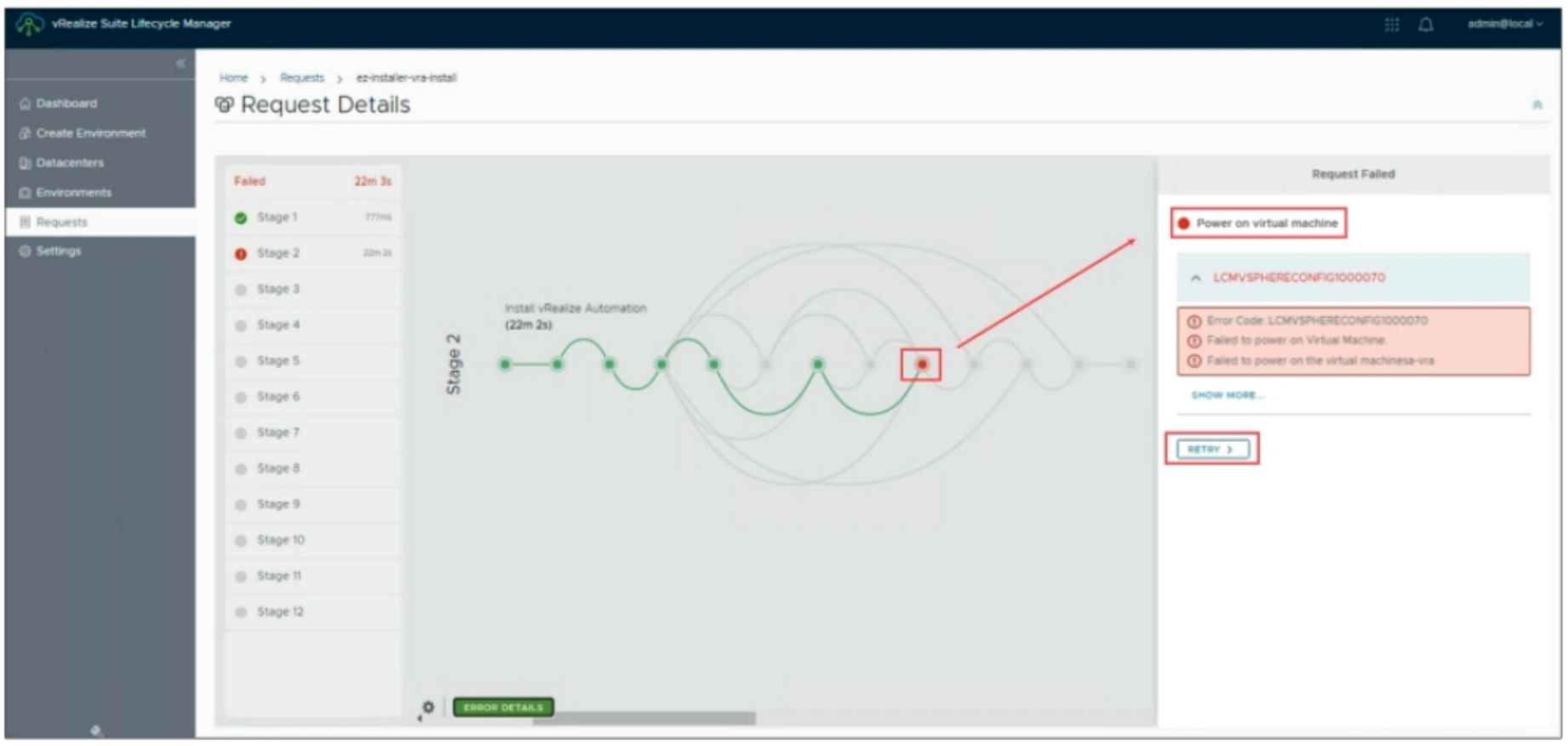
3-13 Monitoring Requests

You can monitor the installation from the VMware Aria Easy Installer wizard. If the installer fails, click the link to log in to VMware Aria Suite Lifecycle.

In the VMware Aria Suite Lifecycle console, select **Requests** in the left navigation pane to display the request details with the overall status of the product installation.

Start troubleshooting the error and click **RETRY** to continue the request.





After VMware Aria Suite Lifecycle is installed and configured, the link to access its interface becomes available. Click the link and log in to VMware Aria Suite Lifecycle to monitor the installation of Workspace ONE Access and VMware Aria Automation.

You log in to VMware Aria Suite Lifecycle with the following default credentials:

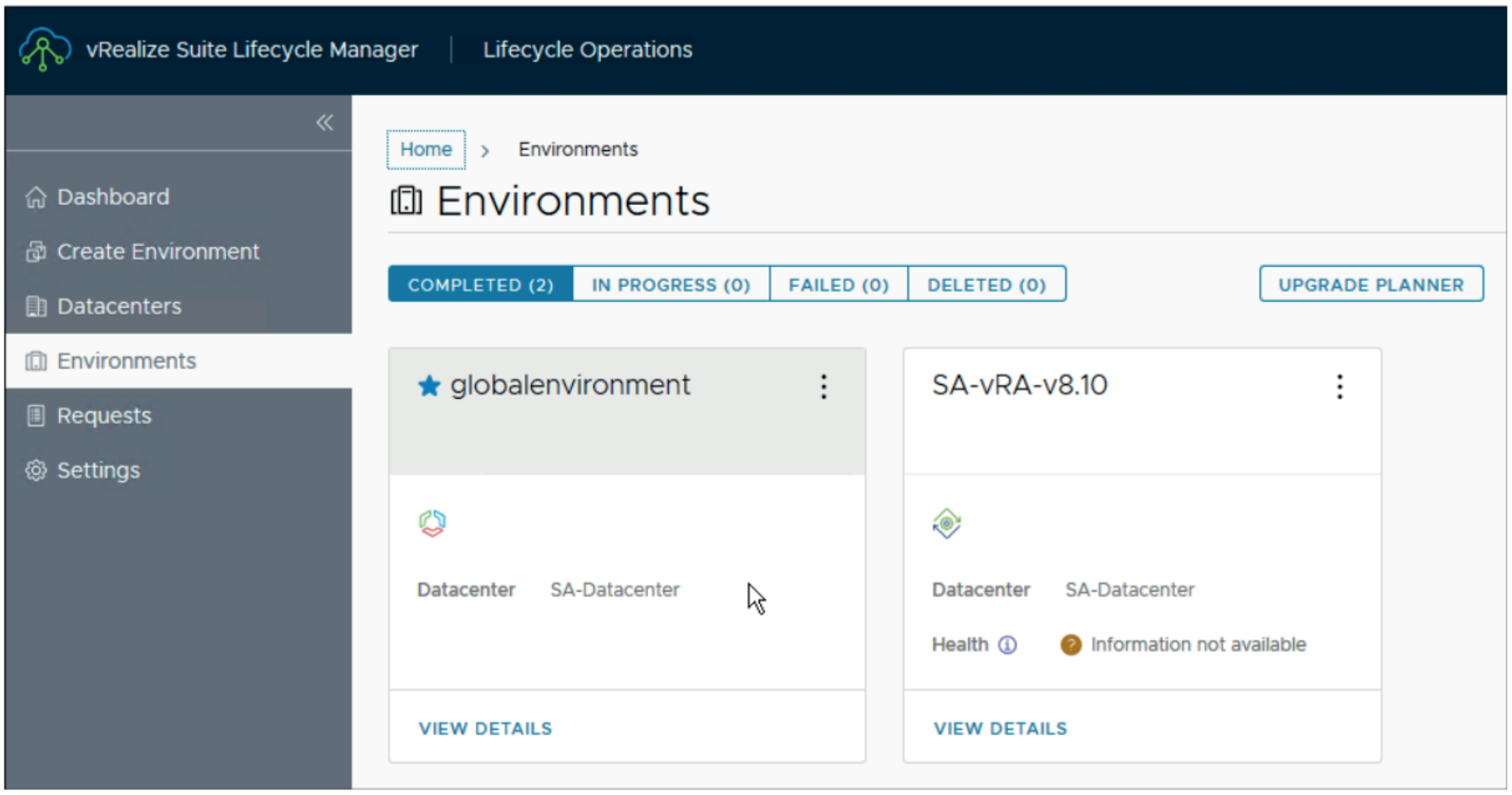
- User name: admin@local
- Password: Specified in VMware Aria Easy Installer

3-14 VMware Aria Suite Lifecycle Environments

An environment is a logical entity that includes one or more VMware Aria products.

VMware Aria Suite Lifecycle creates the following environments:

- Global environment for deploying and managing Workspace ONE Access
- VMware Aria Automation environment

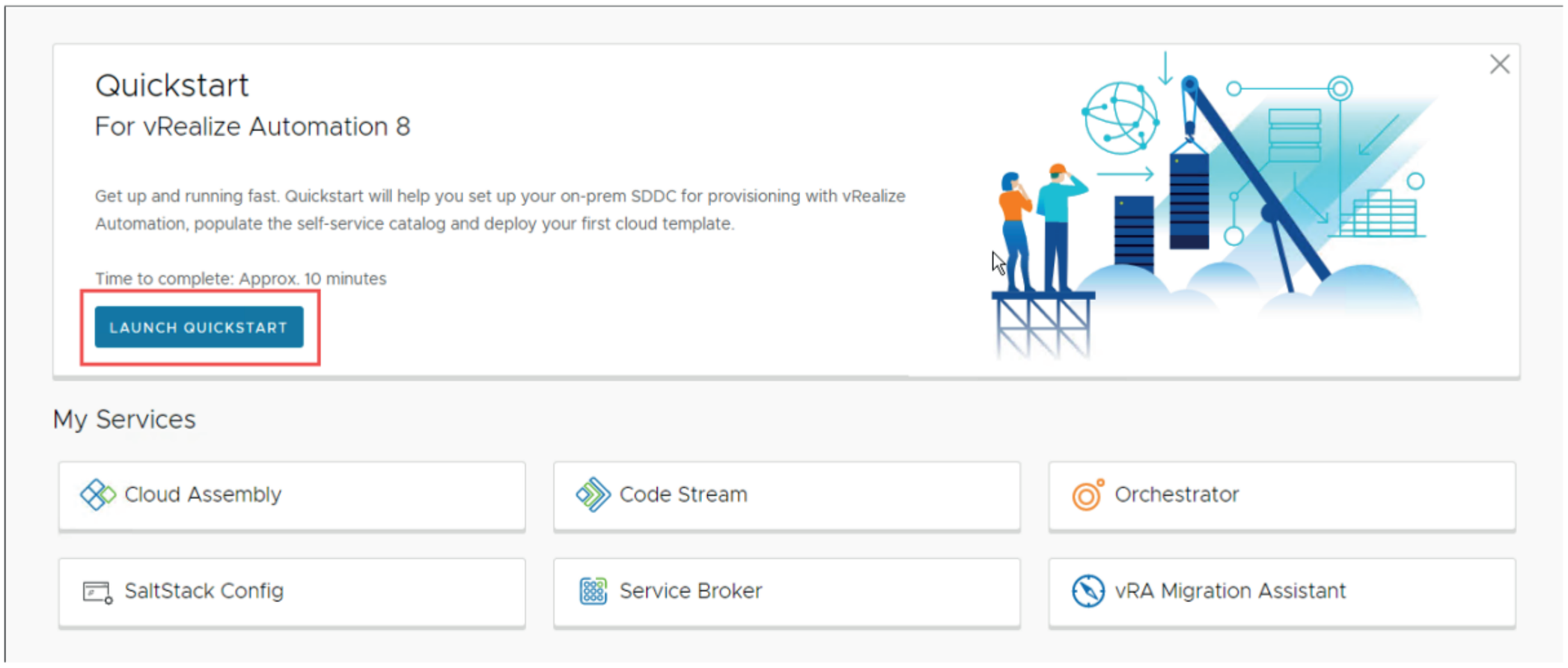


The name of the VMware Aria Automation environment is the name specified in the VMware Aria Easy Installer wizard.

3-15 VMware Aria Automation: Quickstart

After the installation, log in to the VMware Aria Automation console as the Default Configuration Admin user specified during installation.

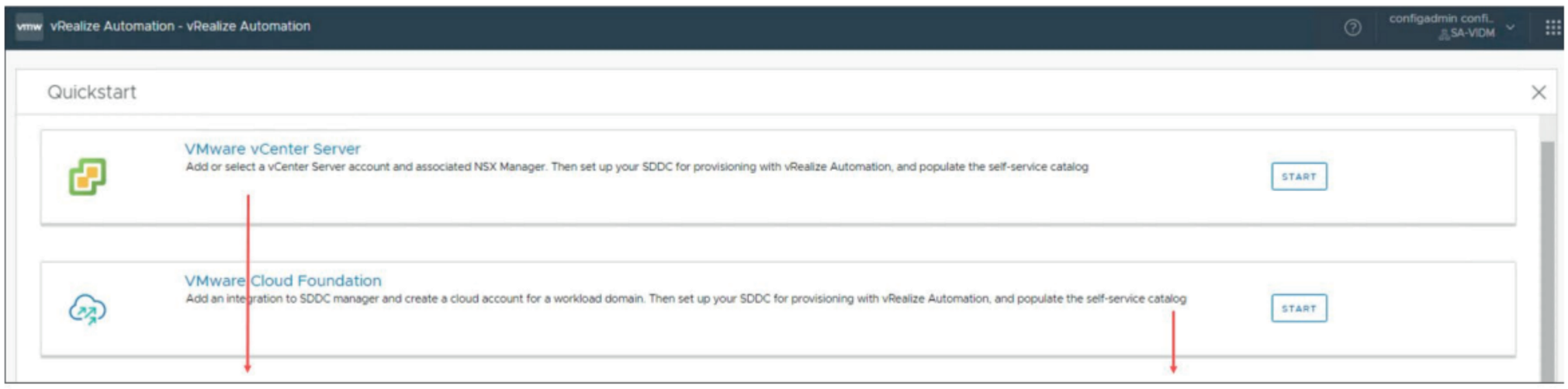
Use the Quickstart wizard to set up an on-premises software-defined data center (SDDC) for provisioning with VMware Aria Automation, populate the self-service catalog, and deploy a VMware Aria Automation template.

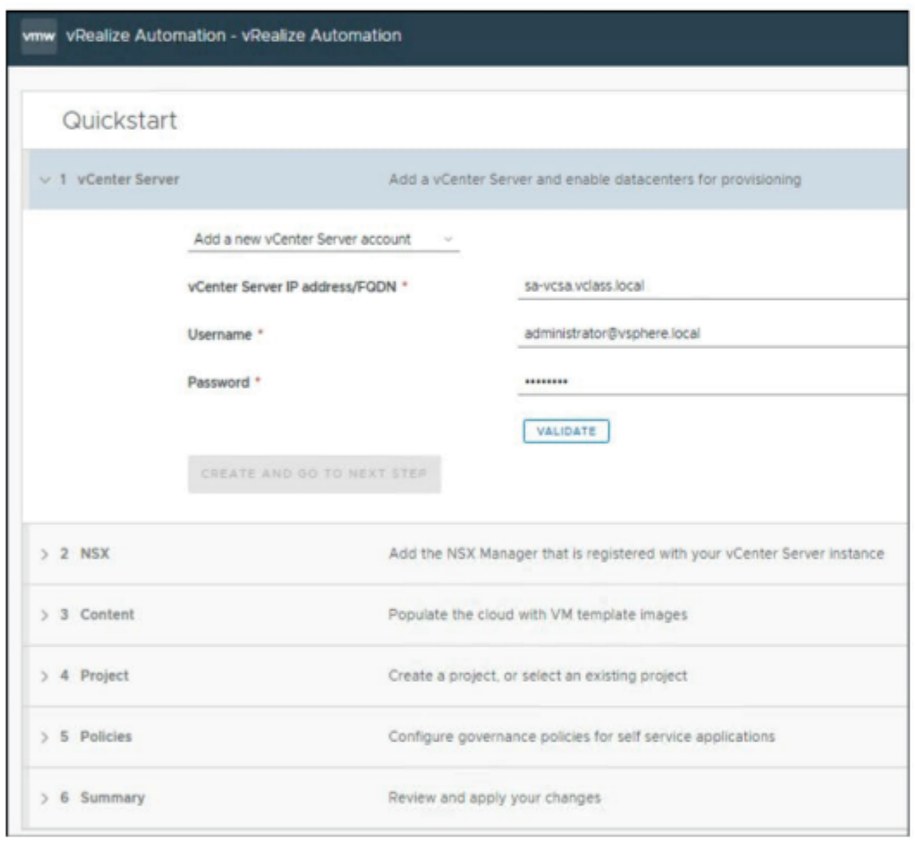


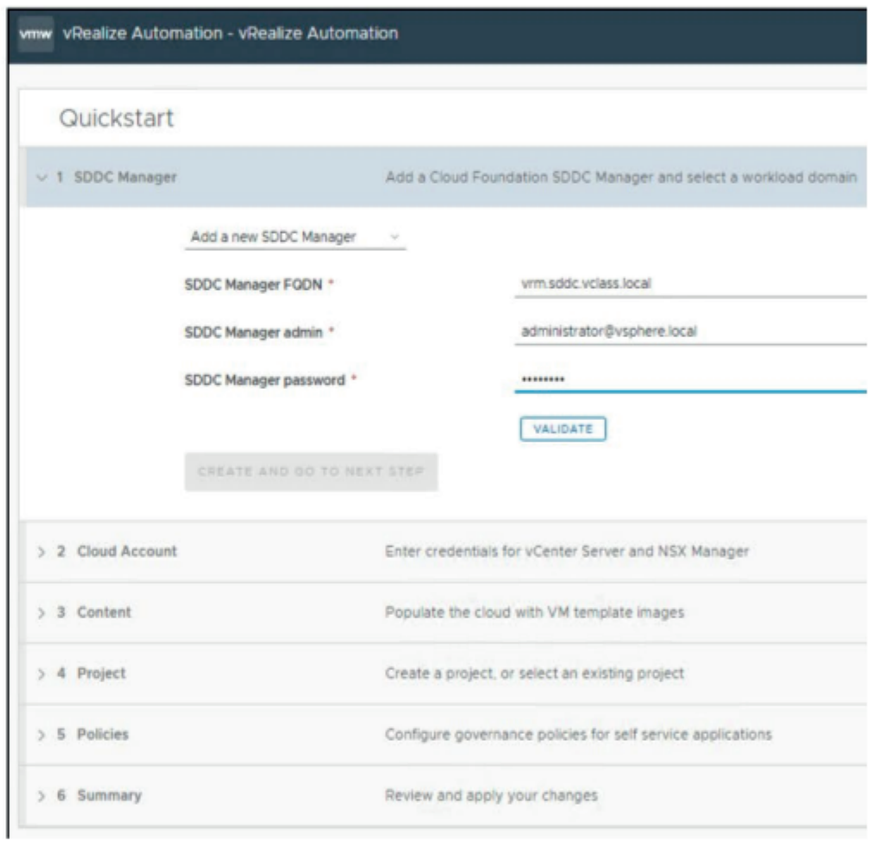
The login URL for the VMware Aria Automation console is https://<VMware_Aria_Automation_FQDN>.

3-16 Quickstart: Options

To set up an on-premises SDDC for provisioning with VMware Aria Automation, you use either vCenter or VMware Cloud Foundation.





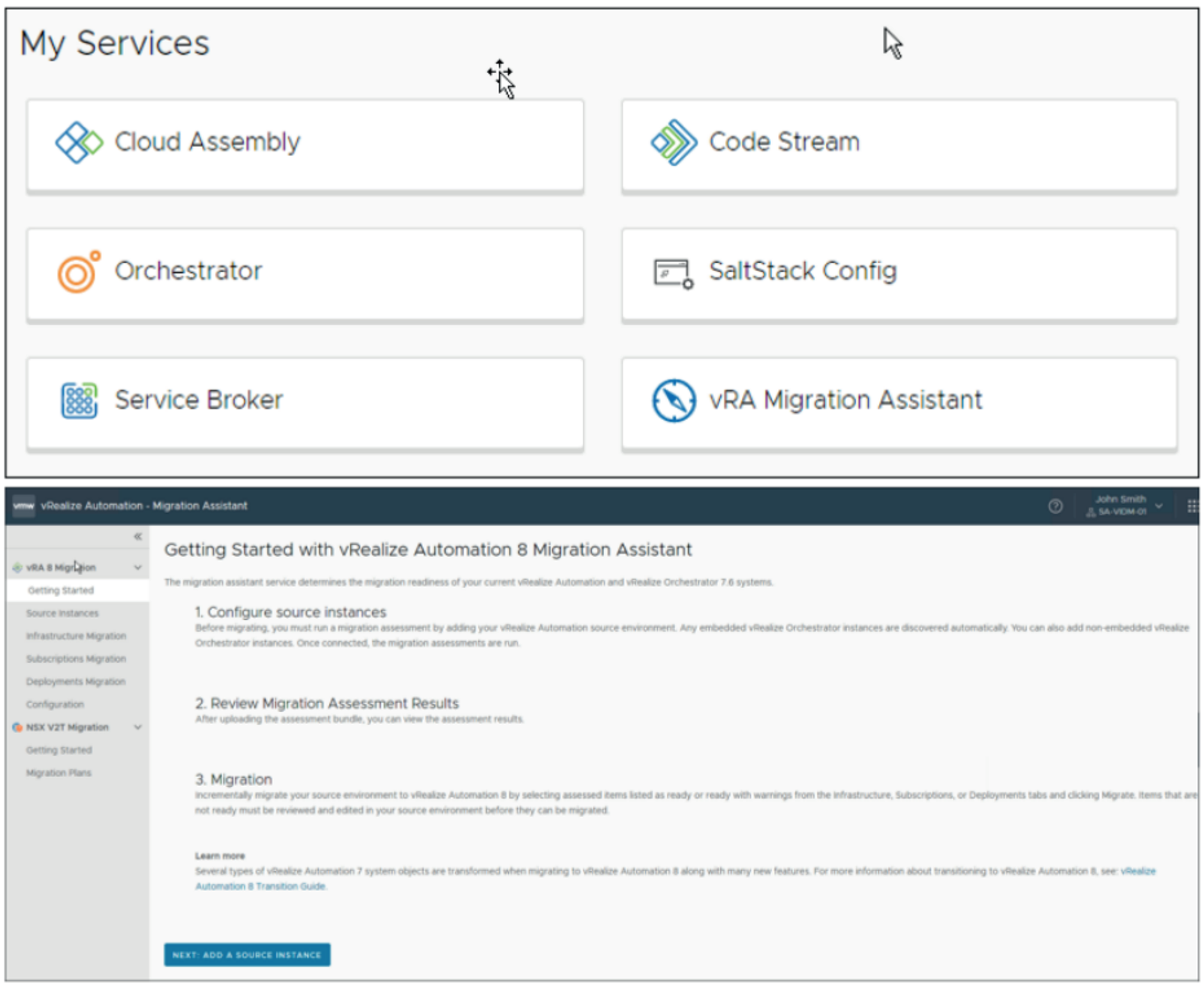


The following options are available in the Quickstart wizard:

- Add or select a vCenter account and an associated NSX Manager instance. You then set up a software-defined data center (SDDC) for provisioning with VMware Aria Automation and populate the self-service catalog.
- Add an integration to SDDC Manager and create a cloud account for a VMware Cloud Foundation workload domain. You then set up an SDDC for provisioning with VMware Aria Automation and populate the self-service catalog.

3-17 VMware Aria Automation Migration

VMware Aria Migration (formerly called vRealize Migration Manager) facilitates the migration from VMware vRealize Automation 7.x to VMware Aria Automation 8.x.



The migration is performed in the following sequence:

- Define a source VMware Aria Automation 7.x instance.
- Perform a migration assessment against the source to determine the migration readiness of the VMware vRealize Automation 7.x source environment. The migration assessment alerts any system object and its dependencies that are not ready for migration and that impacts the migration process.
- After performing a migration assessment, migrate to import content and configuration data from the current VMware vRealize Automation 7.x source environment to VMware Aria Automation 8.x.

VMware Aria Migration aids the migration process in stages:

- Migrate the infrastructure
- Migrate the subscriptions
- Migrate the deployments

You can do incremental migrations. You can also rollback migrations as needed for corrections.

For more information, see the section about migration limitations in *VMware Aria Automation 8 Transition Guide* at https://docs.vmware.com/en/vRealize-Automation/index.html.

3-18 Migrating VMware Aria Automation 7.x to 8.x

You can use one of the following methods to transition from an earlier VMware Aria Automation system to VMware Aria Automation 8.x:

- Create a VMware Aria Automation 8.x system and do not migrate components.
- Migrate a recent version of VMware vRealize Automation 7.4 or later directly to VMware Aria Automation 8.x.
- Upgrade from an earlier version of VMware vRealize Automation 7.x (earlier than 7.4) to VMware vRealize Automation 7.6 and migrate that system to VMware Aria Automation 8.10.

Several types of VMware vRealize Automation 7.x system objects are transformed with many new features when they migrate to VMware Aria Automation 8.x.

3-19 Lab 3: (Simulation) Installing VMware Aria Automation

Use the VMware Aria Easy Installer to install VMware Aria Automation:

1. Install VMware Aria Automation
2. Log In to VMware Aria Automation

3-20 Lab 4: (Simulation) Using VMware Aria Automation Quickstart

Use the Quickstart wizard to set up a software-defined data center:

1. Start the Quickstart Wizard
2. Validate the Configuration

3-21 Review of Learner Objectives

- Describe the VMware Aria Automation installation process
- Use VMware Aria Easy Installer to set up a VMware Aria Automation environment
- Discuss the importance of VMware Aria Migration
- Use the Quickstart wizard to configure the infrastructure and deploy a VMware Aria Automation template

3-22 Key Points

- VMware Aria Easy Installer simplifies and accelerates the VMware Aria Automation installation process.
- The Quickstart wizard helps set up the proof-of-concept environment and deploy the first VMware Aria Automation template with minimal steps.
- VMware Aria Automation Migration facilitates the migration from VMware Aria Automation 7.6 or later to VMware Aria Automation 8.x.

Questions?

Module 4

Authentication and Authorization

4-2 Importance

VMware Aria Automation requires an authentication framework to allow user logins, and it requires an authorization framework to assign user privileges. VMware Aria Automation integrates seamlessly with Workspace ONE Access to provide both authentication and authorization.

4-3 Module Lessons

1. Authentication with Workspace ONE Access
2. Authorization with VMware Aria Automation Roles
3. Multitenancy and Virtual Private Zones

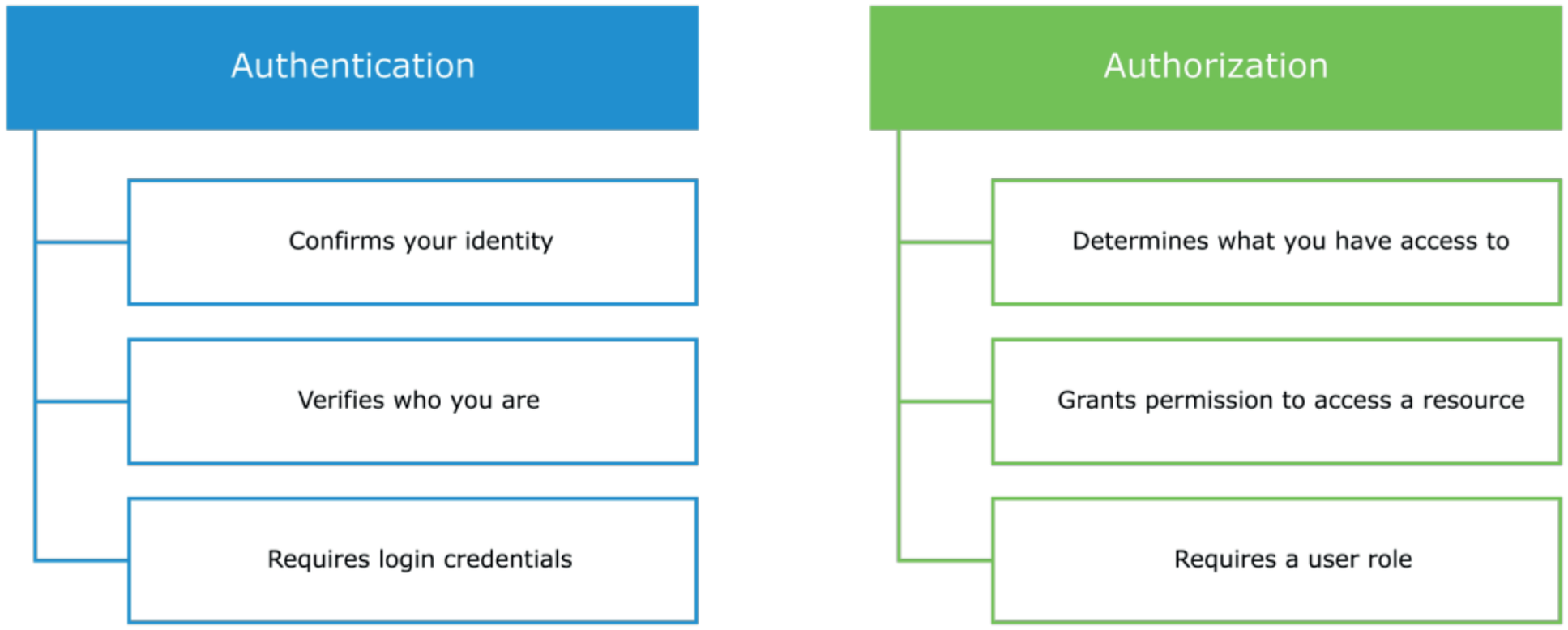
4-4 Lesson 1: Authentication with Workspace ONE Access

4-5 Learner Objectives

- Describe how identity management works in VMware Aria Automation
- Identify the steps involved in integrating Workspace ONE Access with Active Directory
- Outline the features of Workspace ONE Access

4-6 Authentication and Authorization

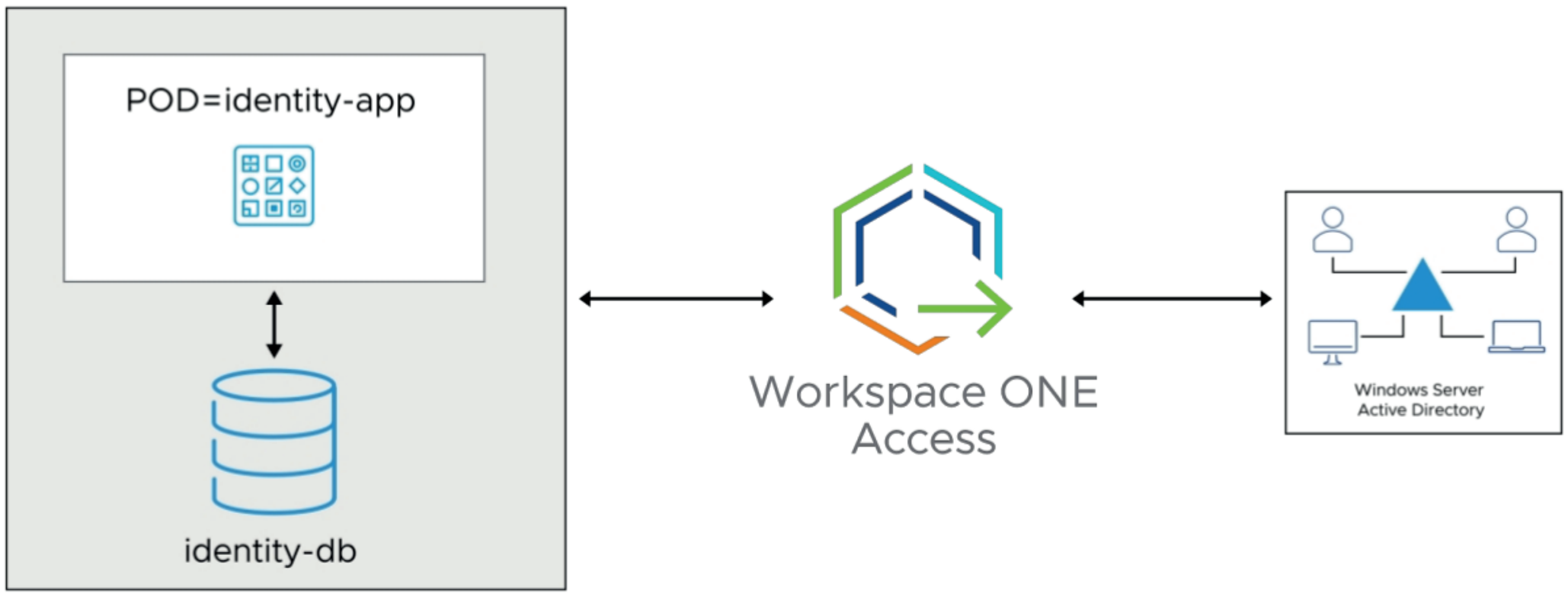
Authentication and authorization are important concepts in the configuration process.



4-7 Architecture of Workspace ONE Access

The identity service runs as a pod in Kubernetes. If a user tries to log in to VMware Aria Automation:

1. The identity service redirects the request to the Workspace ONE Access URL.
2. Workspace ONE Access validates the user credentials with Active Directory.
3. The user can log in to the VMware Aria Automation console.



The identity-db is a dedicated PostgreSQL database for the identity service.

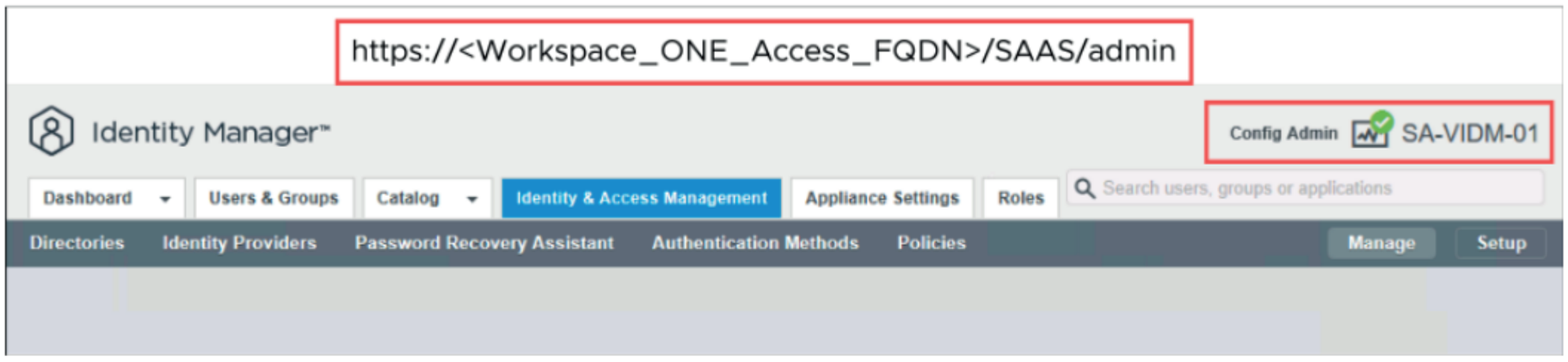
The URL to access the Workspace ONE Access appliance is set as a host name environment variable during installation. All requests to authorize credentials are forwarded to the Workspace ONE Access appliance.

4-8 About Workspace ONE Access

Administrators use Workspace ONE Access to manage user authentication, access policies, and entitle users to resources.

Administrators log in using the default Config Admin user that is specified during installation.

The Config Admin user is assigned the Super Admin role, which has full administrator access in Workspace ONE Access.



Administrators can use access policies to configure features such as mobile single sign-on (SSO), conditional access to applications based on enrollment and compliance status, and multifactor authentication.

VMware products can use Workspace ONE Access as an enterprise SSO solution.

Workspace ONE Access is based on the OAuth 2.0 authorization framework.

Workspace ONE Access was previously known as VMware Identity Manager. Some UI elements might still be labeled as VMware Identity Manager.

4-9 Directory Integration

By integrating the enterprise directory with Workspace ONE Access, you can synchronize users and groups from the enterprise directory to Workspace ONE Access.

The following types of directories are supported:

- Active Directory over LDAP
- Active Directory, Integrated Windows Authentication

Workspace ONE Access supports integration with the following types of directories:

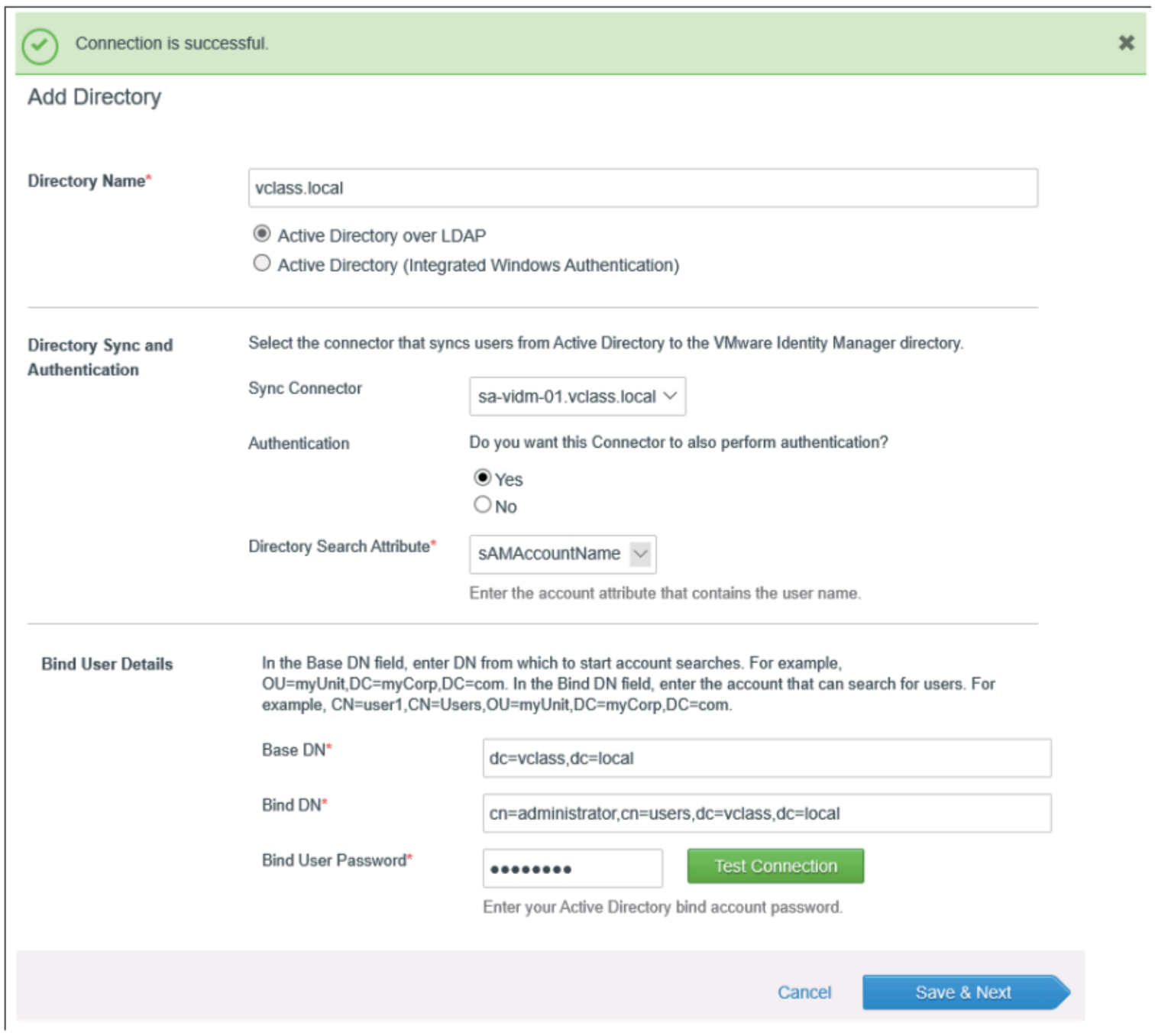
- Active Directory over LDAP:
  - Create this directory type if you plan to connect to a single Active Directory domain environment.
  - For the Active Directory over LDAP directory type, the connector binds to Active Directory with simple bind authentication.
- Active Directory, Integrated Windows Authentication:
  - Create this directory type if you plan to connect to a multidomain or multi-forest Active Directory environment.
  - The connector binds to Active Directory with Integrated Windows Authentication.

The system directory is created by default, and the configadmin user is created in the system directory. You can create multiple local directories. You use the Local User Directory option to create a second local directory.

4-10 Integrating Active Directory

To integrate Workspace ONE Access with Active Directory:

1. In the Workspace ONE Access console, select **Identity & Access Management** > **Directories**.
2. Click **Add Directory**.



You must add the Workspace ONE Access appliance to the domain before you can use the Integrated Windows Authentication option.

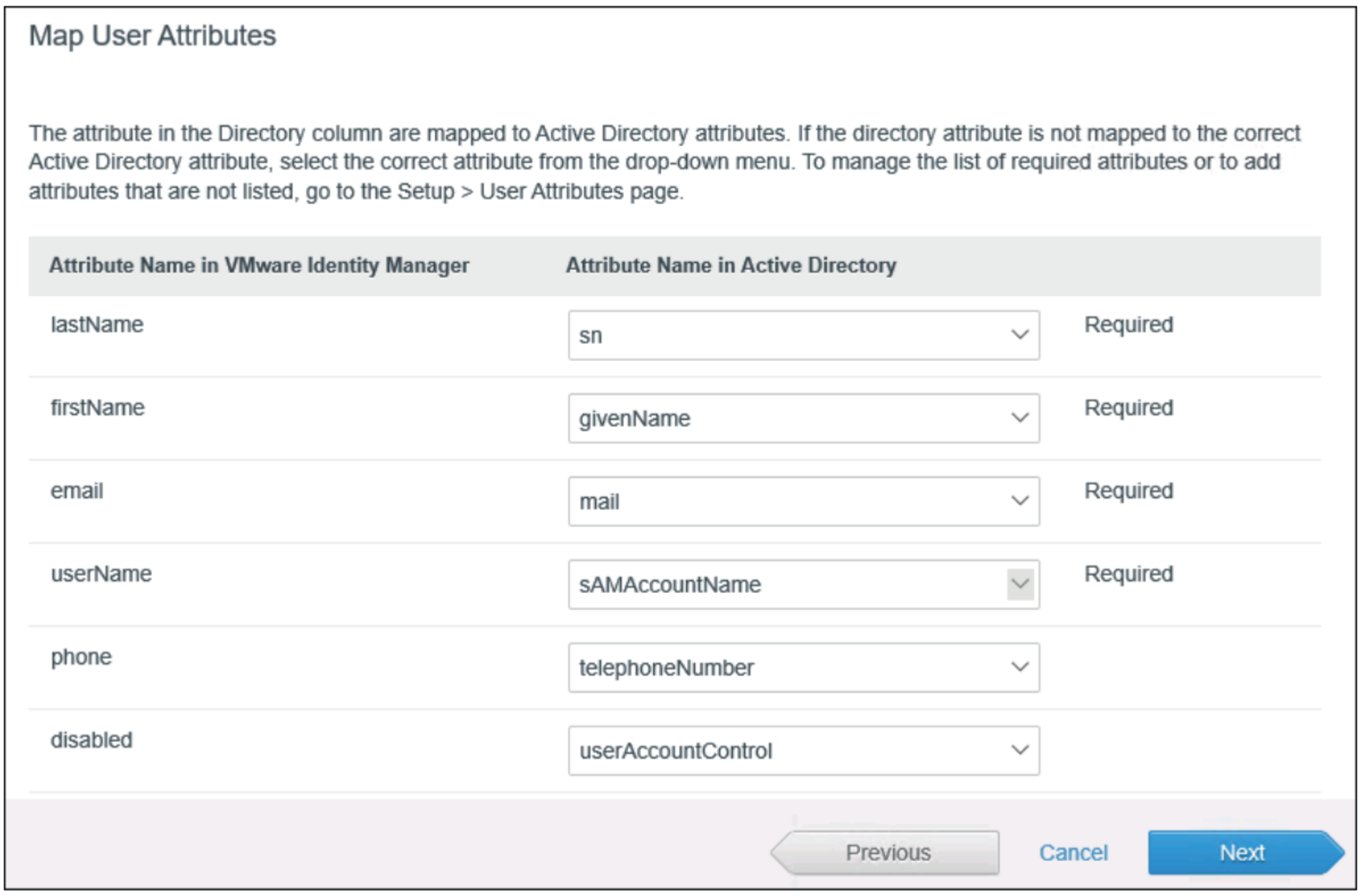
The default sync connector is used to synchronize Active Directory users and groups to Workspace ONE Access. The connector also performs user authentication against Active Directory.

4-11 Mapping User Attributes

You select the attributes that synchronize between Active Directory and Workspace ONE Access.

Some attributes are required, and other attributes are optional.

The required attributes can be modified.

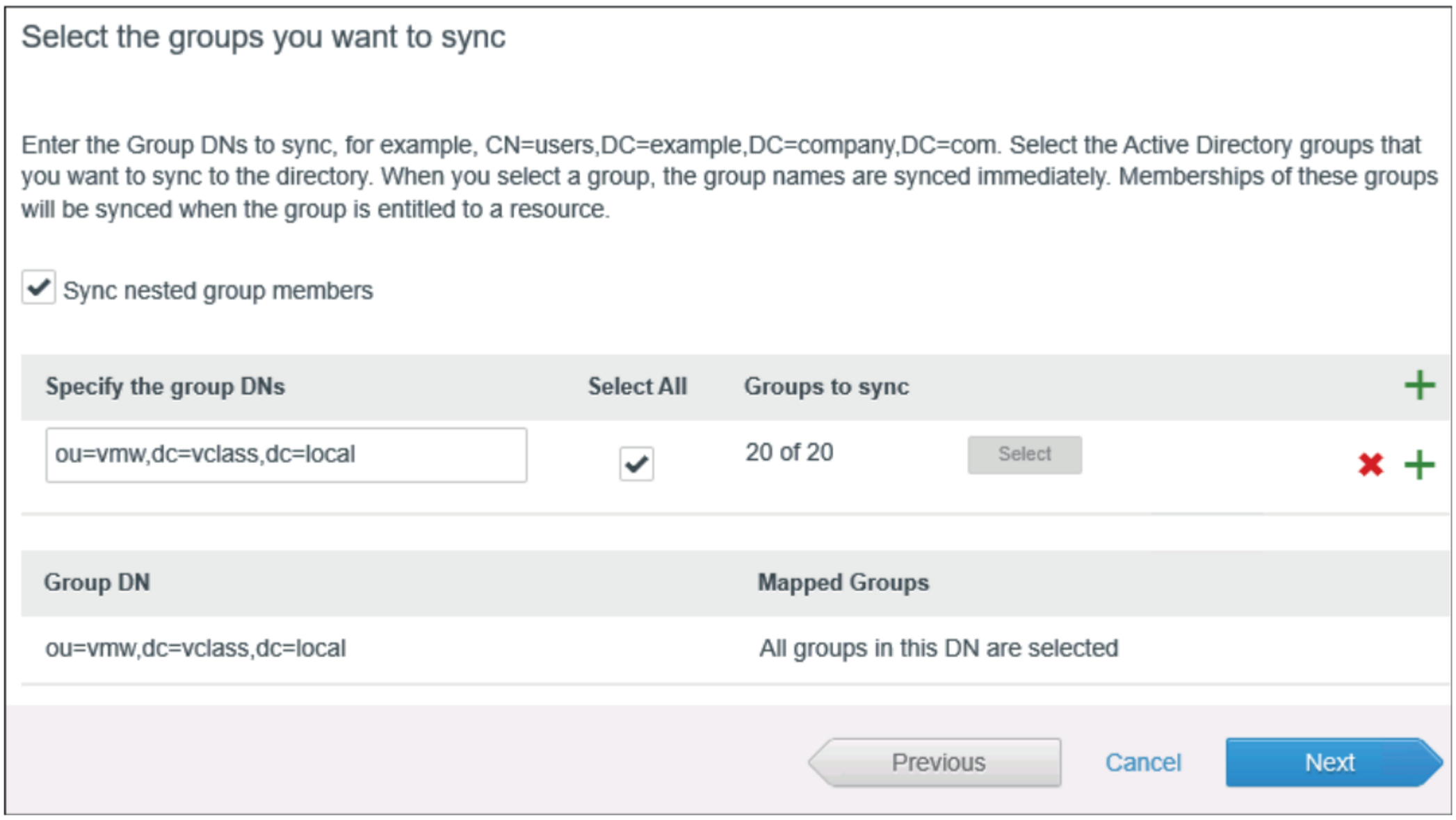


When you configure the User Attributes page before the directory is created, you can change default attributes from Required to Not Required, mark attributes as Required, and add custom attributes. To change the required user attributes, navigate to **Identity & Access Management** > **Setup** > **User Attributes** from the menu bar of the Workspace ONE Access console.

4-12 Synchronizing Groups

You specify the groups that you want to synchronize from Active Directory to Workspace ONE Access.

Click **Next** to synchronize Active Directory users to Workspace ONE Access.



The **Sync nested group members** check box is selected by default. When this check box is selected, all users that belong directly to the selected group and any nested groups are synchronized when the group is entitled.

To use the **Sync nested group members** option, you must select the **Sync Group Members to the Directory When Adding Group** option during the installation process.

If the **Sync nested group members** check box is deselected when you specify a group to sync, all users that belong directly to that group are synced.

After you integrate your enterprise directory and perform the initial sync, you can update the configuration, set up a sync schedule to synchronize on a regular basis, or start a sync at any time.

4-13 Features of Workspace ONE Access

Workspace ONE Access includes the following additional features:

- Access policies
- Support for multiple user authentication methods
- Two-factor authentication
- Password recovery assistant
- Just-in-time (JIT) user provisioning

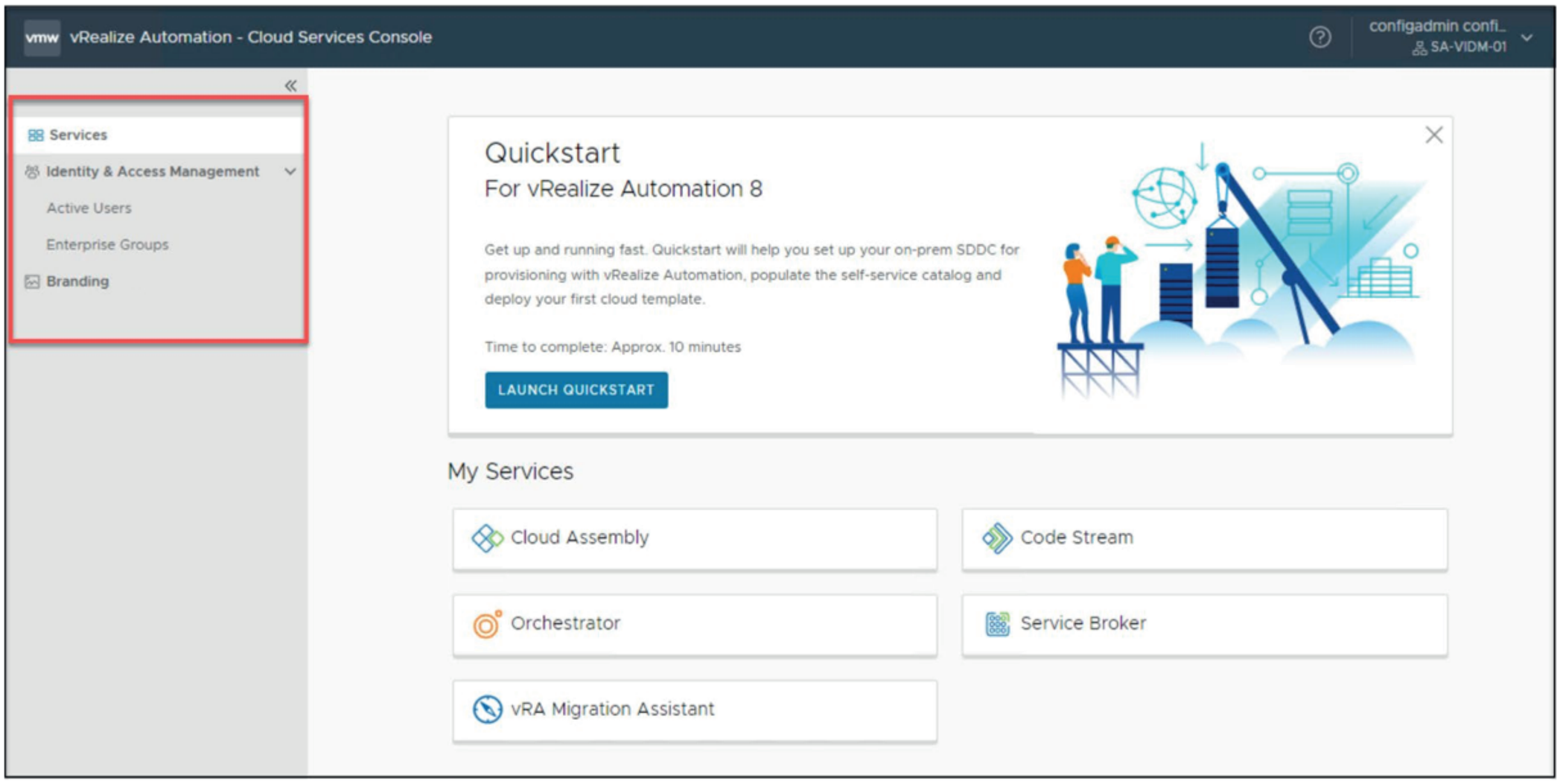
Workspace ONE Access provides several additional features:

- Access policies:
  - Access policies include rules that specify criteria that users must meet to log in to their applications portal and to use their resources.
  - Administrators can use access policies to configure features such as mobile SSO, conditional access to applications based on enrollment and compliance status, and multifactor authentication.
- Workspace ONE Verify:
  - Workspace ONE Verify is a configurable authentication method that can be used as the second authentication method when two-factor authentication is required.
  - The first authentication method is user name and password, and the second authentication method is Workspace ONE Verify.
- Password recovery: Using the password recovery assistant, a custom message can be displayed when the end user clicks **Forgot password** on the login screen.
- Just-in-time (JIT) provisioning:
  - You can use JIT user provisioning to create users in the Workspace ONE Access service dynamically at login time by using SAML assertions sent by a third-party identity provider.
  - You can use the JIT users feature to restrict access to VMware Aria Automation to only users who are intended to log in.
  - The JIT users are only synchronized at first login.
  - JIT user provisioning is available only for third-party identity providers.

- With JIT provisioning, you can add users without synchronizing from Active Directory.
- The JIT feature can be used to provide temporary access to services. An example use case is interns working on a project for an organization. Interns do not require permanent credentials.

4-14 About the VMware Aria Automation Console

You log in to the VMware Aria Automation console as the default configadmin user. This user has full administrative access to all three sections of the console's navigation menu.

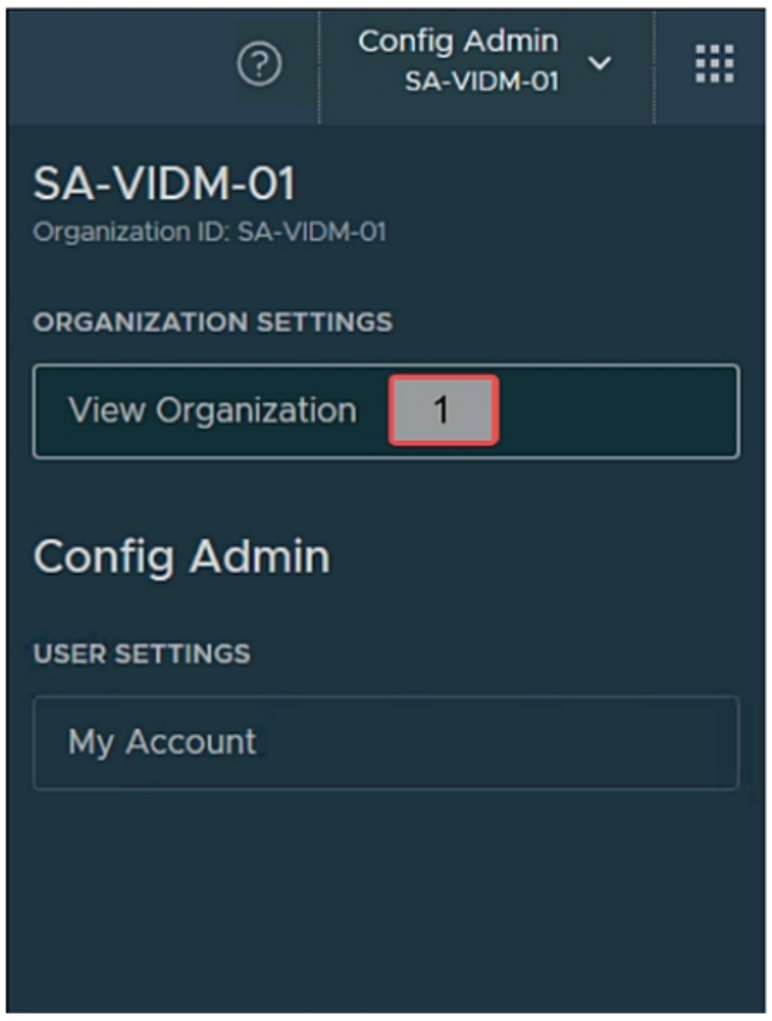


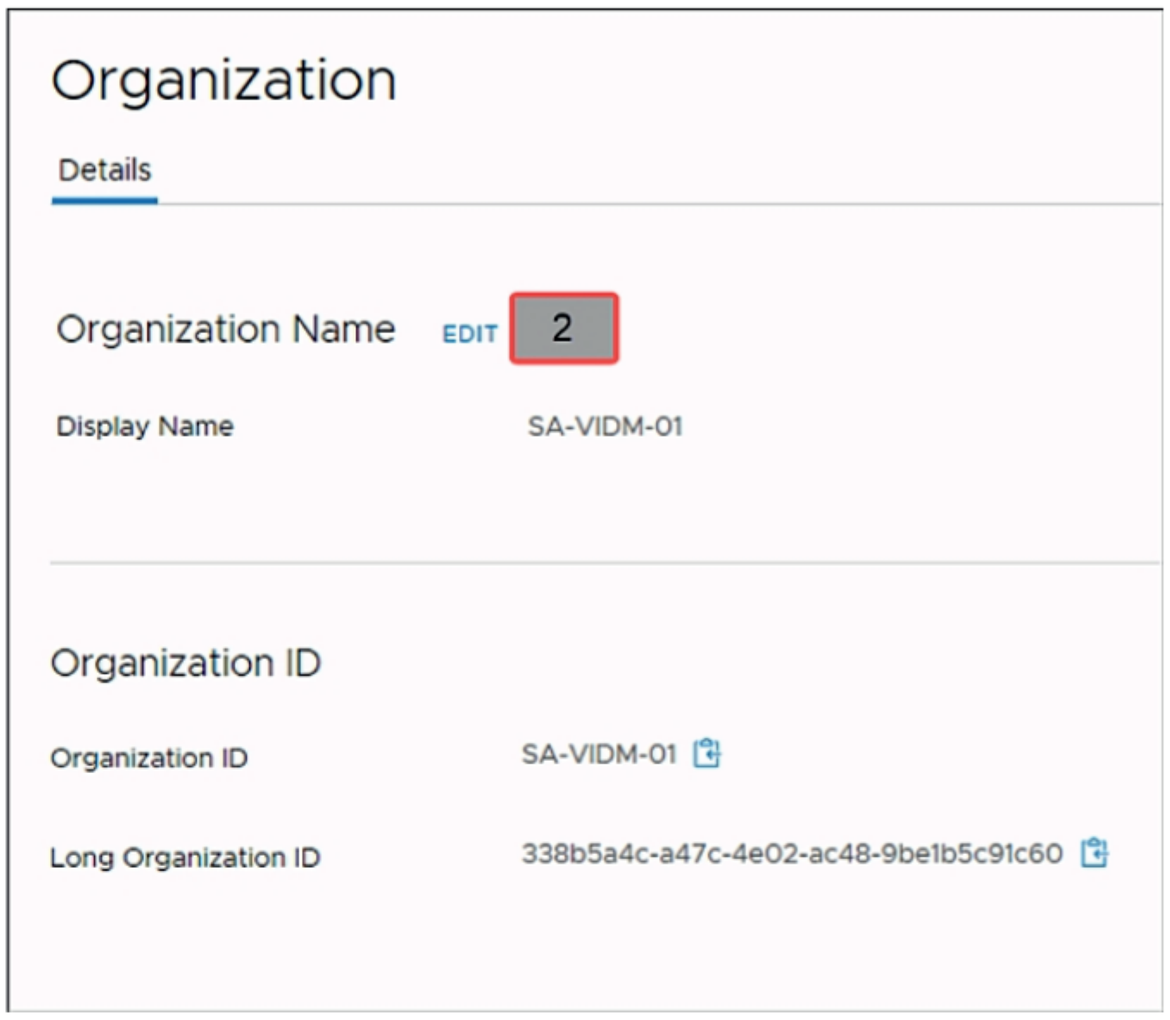
Go to https://<VMware_ Aria_ Automation_ FQDN>/ to log in to VMware Aria Automation.

You log in to VMware Aria Automation for the first time by using the Default Configuration Admin user that is specified during installation.

4-15 VMware Aria Automation: Organizations

By default, an organization is named after the short name assigned to the Workspace ONE Access appliance. However, this organization name is editable.

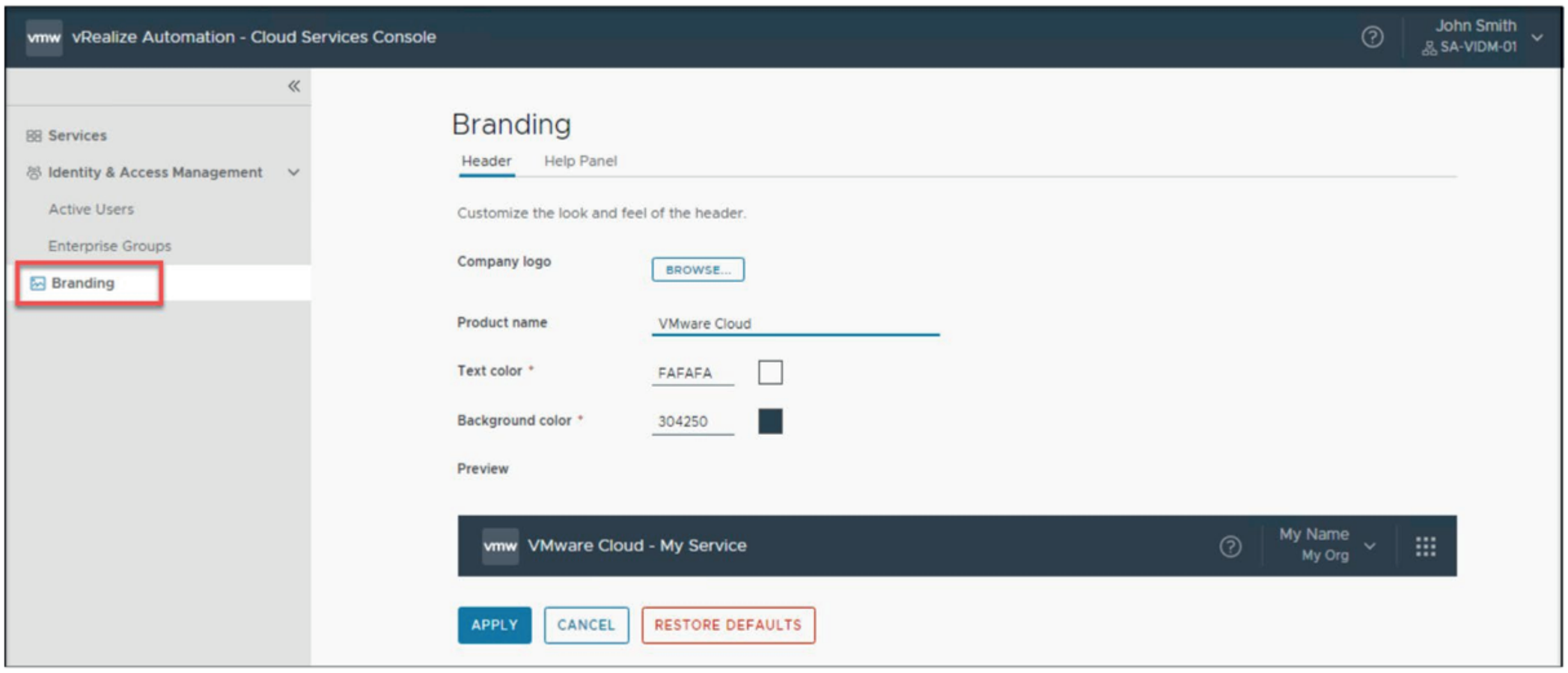




An organization in VMware Aria Automation represents the deployment name. A single VMware Aria Automation deployment can have only one organization.

4-16 VMware Aria Automation: Branding

To customize the default header name and logo in the VMware Aria Automation console, select **Branding** in the left navigation pane.



4-17 Lab 5: Integrating Workspace ONE Access with Active Directory

Integrate Workspace ONE Access with Active Directory and import users:

1. Integrate Workspace ONE Access with Active Directory
2. Manage Directory Synchronization Settings

4-18 Review of Learner Objectives

- Describe how identity management works in VMware Aria Automation
- Identify the steps involved in integrating Workspace ONE Access with Active Directory
- Outline the features of Workspace ONE Access

4-19 Lesson 2: Authorization with VMware Aria Automation Roles

4-20 Learner Objectives

- Identify the user roles available in VMware Aria Automation
- Explain the key tasks performed by each user role

4-21 Roles in VMware Aria Automation

Roles define a set of privileges associated with users. These privileges are tasks that users can perform.

Depending on your responsibilities, you might be assigned one or more roles.

In VMware Aria Automation, roles are broadly categorized as follows:

- Organization roles
- Service roles

Organization roles are defined at the topmost VMware Aria Automation layer.

The following organization roles exist in VMware Aria Automation:

- Organization Owner
- Organization Member

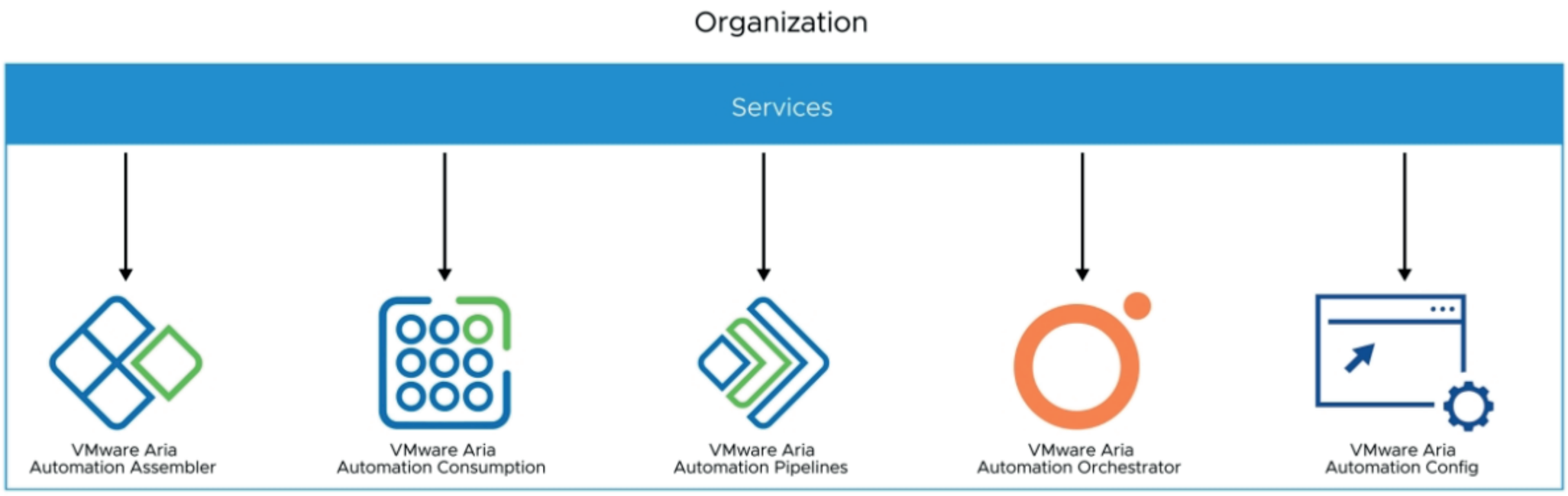
Service roles define user access to individual services offered by VMware Aria Automation.

VMware Aria Automation offers the following service:

- VMware Aria Automation Assembler
- VMware Aria Automation Pipelines
- VMware Aria Automation Orchestrator
- VMware Aria Automation Consumption
- VMware Aria Automation Config

4-22 Organizations and Services

The organization and service user roles determine what the user can view and do in each service. The roles at the organization level are either Organization Owner or Organization Member.



Each service in VMware Aria Automation has more than one role. For example, the VMware Aria Automation Assembler service includes the following roles:

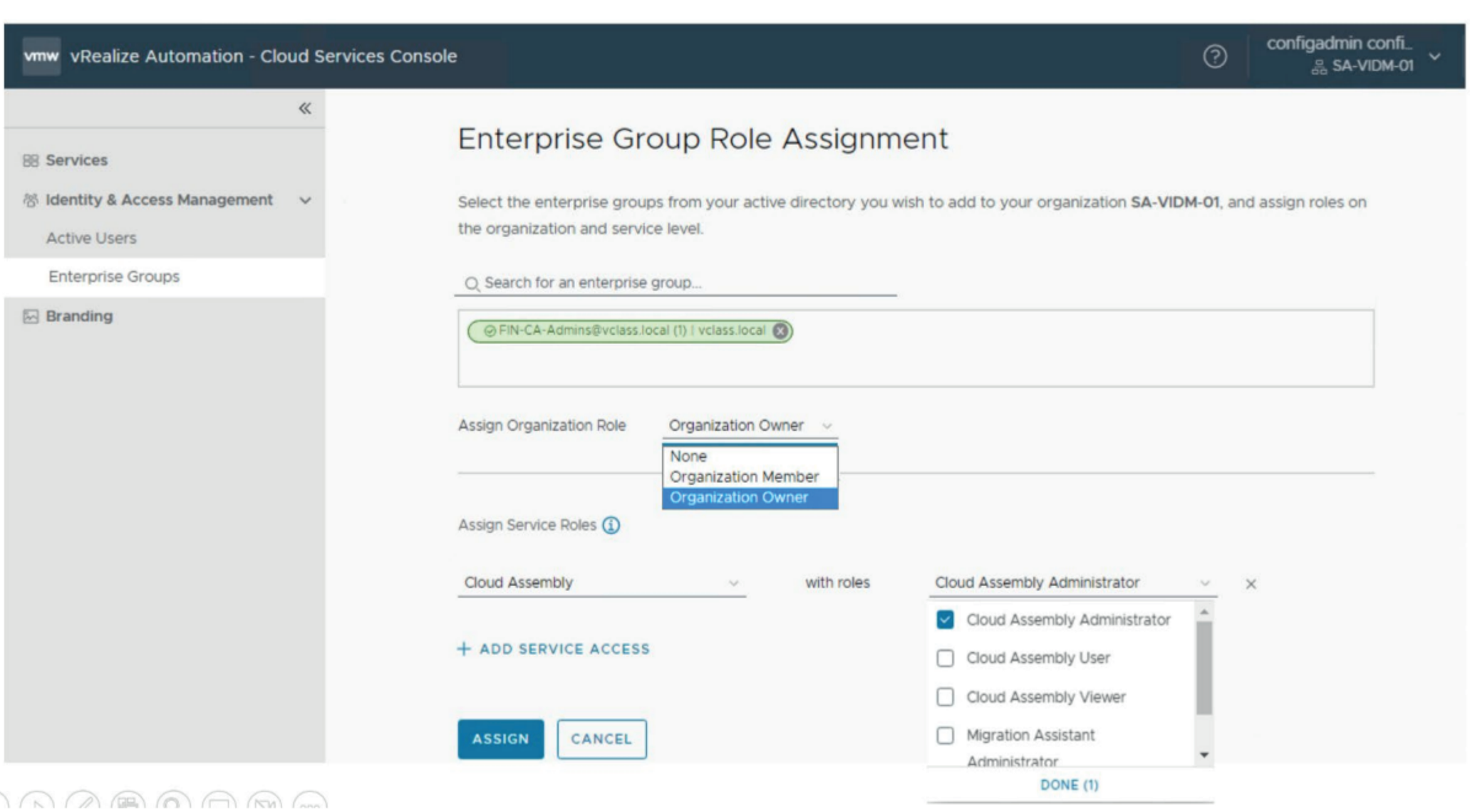
- VMware Aria Automation Assembler Administrator
- VMware Aria Automation Assembler User
- VMware Aria Automation Assembler Viewer

Any user in VMware Aria Automation must be assigned an organization role with an associated service role.

4-23 Assigning Roles

To assign roles in the VMware Aria Automation console:

1. In the navigation pane on the left, select **Identity & Access Management** > **Enterprise Groups**.
2. Click **ASSIGN ROLES** and then select an enterprise group.
3. Select the organization role from the **Assign Organization Role** drop-down menu.
4. Select a service from the **Assign Service Roles** drop-down menu.
5. Select the check box next to the service roles that you want to assign to the user.



In the example, the roles are assigned to the users in the FIN-CA-Admins enterprise group:

1. Organization role: Organization Owner
2. Service: Cloud Assembly
3. Service role: Cloud Assembly Administrator

The service roles change based on the selected service.

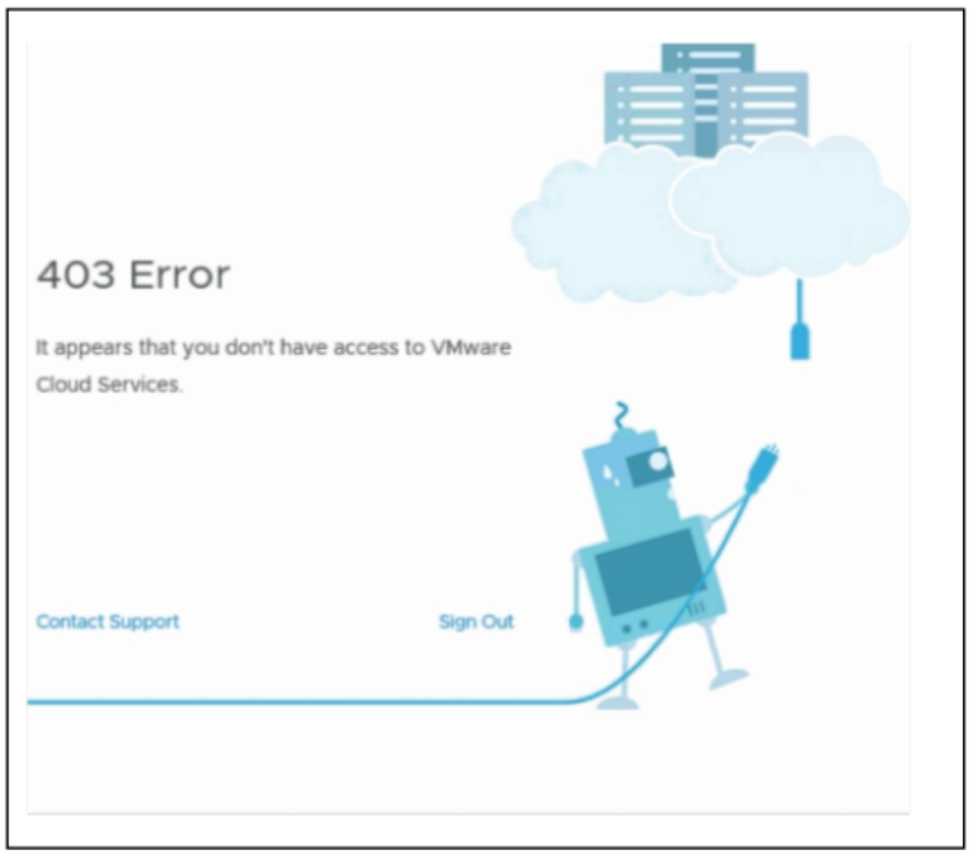
You must also assign roles to a group by selecting **Identity & Access Management** > **Enterprise Groups** in the left navigation pane.

See the chapter about organization and service user roles in *Using and Managing Cloud Assembly* at https://docs.vmware.com/en/vRealize-Automation/index.html.

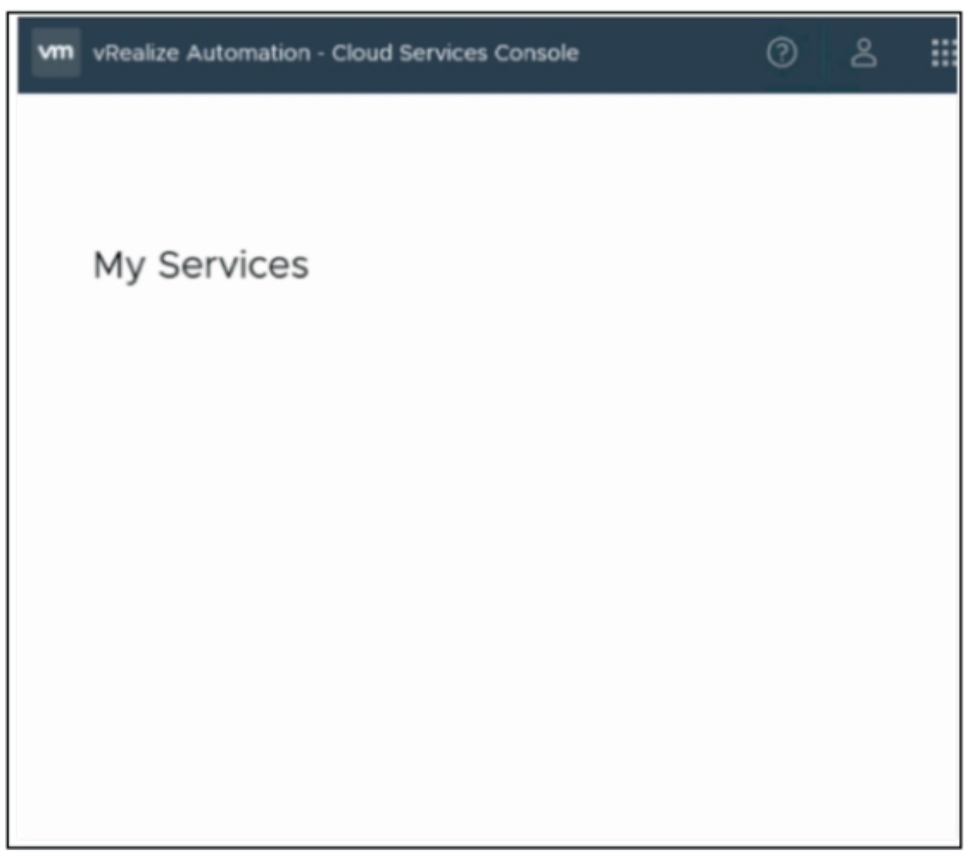
4-24 Associating Organization and Service Roles

You must associate an organization role with a service role.

No Organization Role Assigned

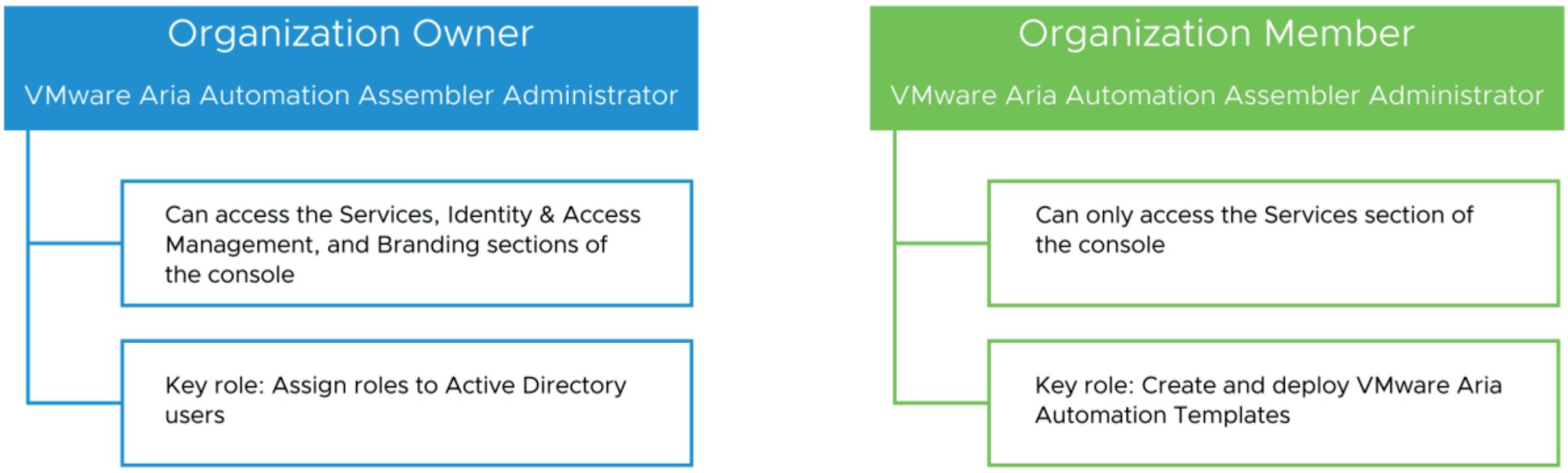


No Service Role Assigned



4-25 About Organization Roles

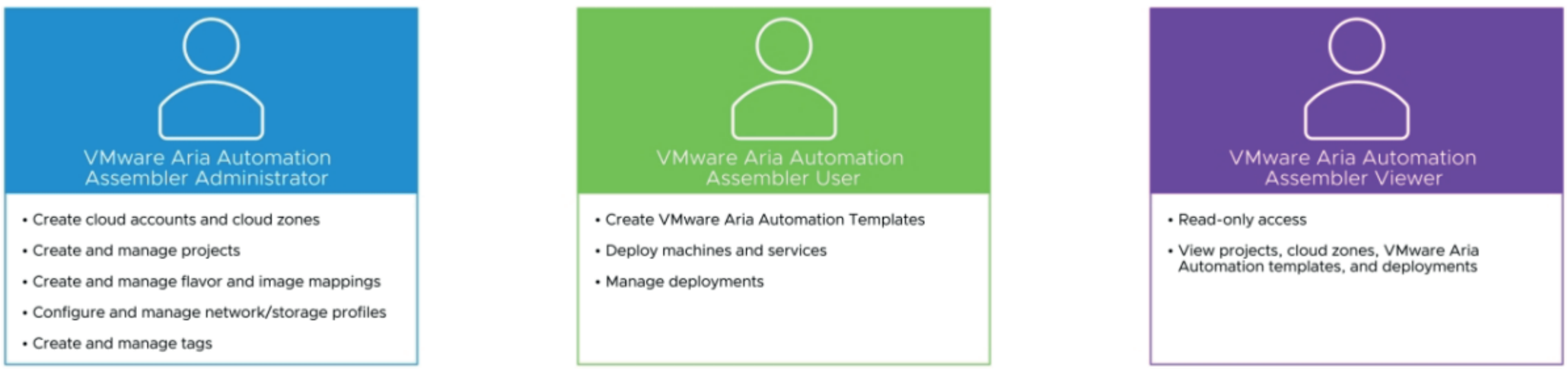
VMware Aria Automation has two levels of organization roles, Organization Owner and Organization Member, with key differences in their levels of access and their responsibilities. For example, a VMware Aria Automation Assembler administrator has unique capabilities as an Organization Owner compared to an Organization Member.



The key responsibility of an organization owner is to assign roles.

4-26 Service Roles: VMware Aria Automation Assembler

The VMware Aria Automation Assembler service has multiple roles, and these roles have different key responsibilities.



VMware Aria Automation Assembler has the following service roles:

- VMware Aria Automation Assembler Administrator:
  - Create cloud accounts and cloud zones
  - Create and manage projects, flavor, image mappings, and tags
  - Configure and manage network profile, and storage profiles
- VMware Aria Automation Assembler User:
  - Create VMware Aria Automation Templates
  - Deploy machines and services
  - Manage deployments
- VMware Aria Automation Assembler Viewer:
  - Read only access role
  - View projects, cloud zones, VMware Aria Automation Templates, and deployments

In addition to its service roles, VMware Aria Automation Assembler has the following project roles that can be assigned on a per-project basis:

- Project administrators: View all provisioned resources, provision new resources, and manage users
- Project members: View their own provisioned resources and work within their projects to design and deploy VMware Aria Automation templates

- Project viewers: View all provisioned resources and perform non-destructive actions, such as downloading VMware Aria Automation templates

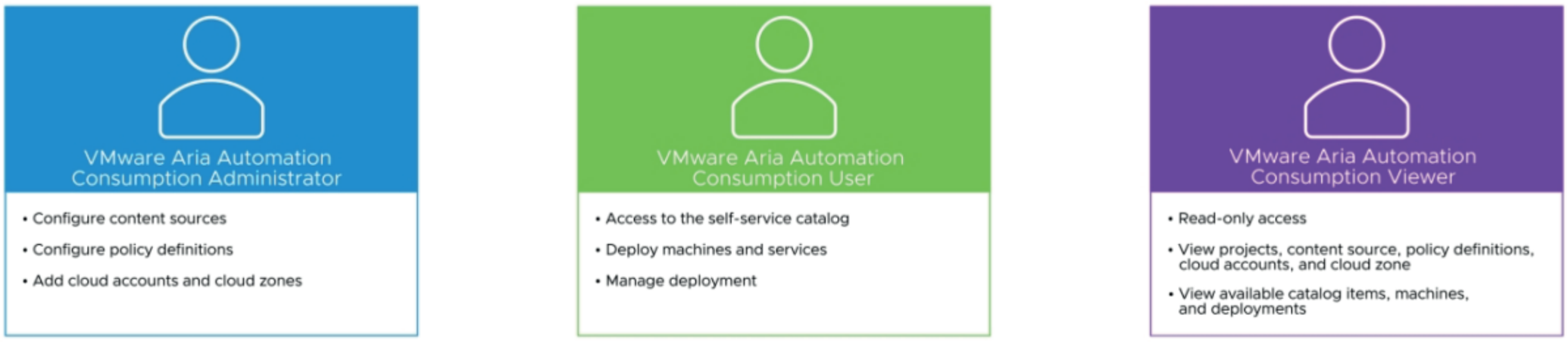
  Project viewers are restricted to read-only access.

- Project supervisors: Approve deployment requests

  To provide project supervisors with context for approvals, you should consider also assigning them project member or viewer roles.

4-27 Service Roles: VMware Aria Automation Consumption

The VMware Aria Automation Consumption service has multiple roles with several key responsibilities.



VMware Aria Automation Consumption has the following service roles:

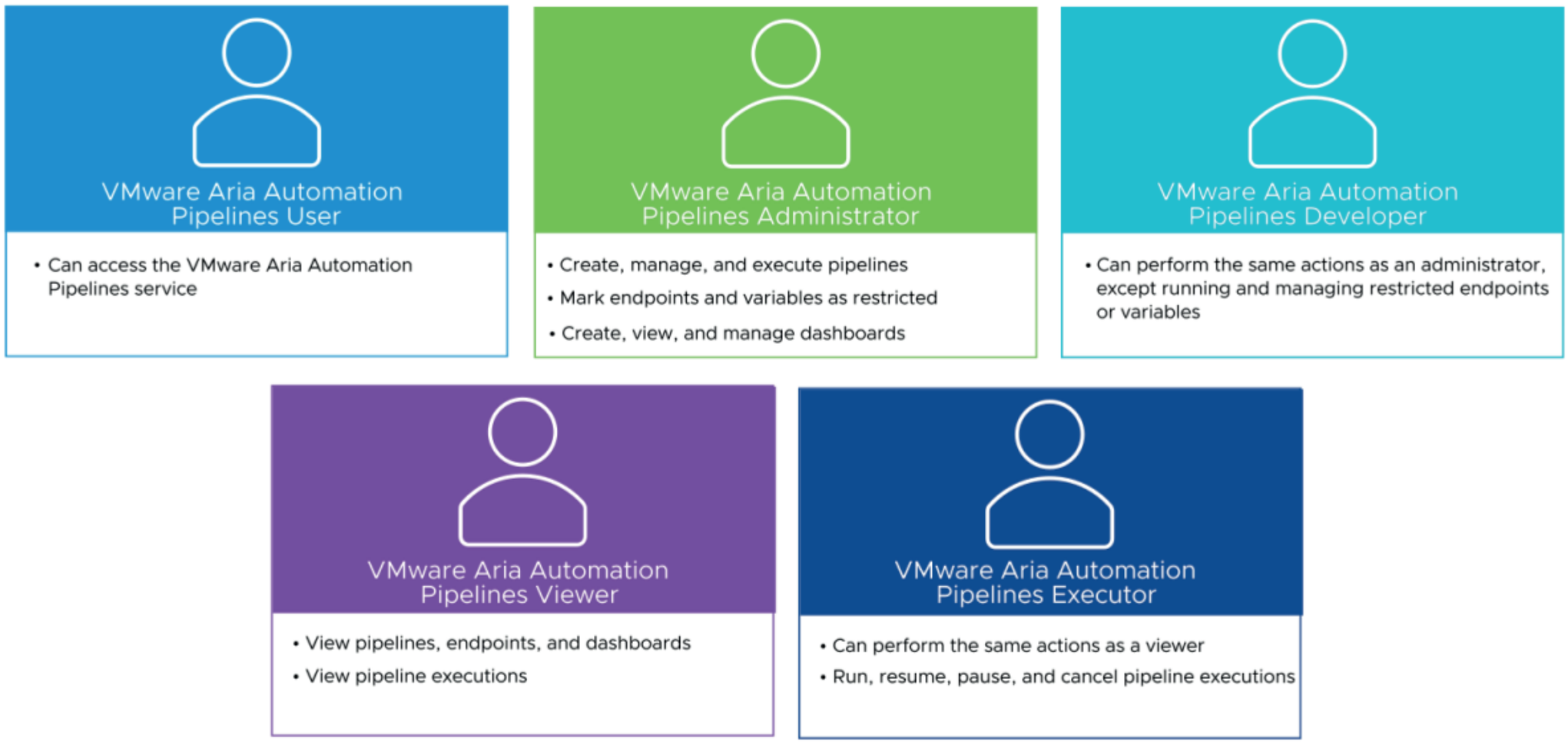
- VMware Aria Automation Consumption Administrator:
  - Configure content sources, and policy definitions
  - Add cloud accounts and cloud zones
- VMware Aria Automation Consumption User:
  - Access to the self-service catalog
  - Deploy machines and services
  - Manage deployments
- VMware Aria Automation Consumption Viewer:
  - Read-only access role
  - View projects, content source, policy definition, cloud accounts, and cloud zones
  - View available catalog items, machines, and deployments

In addition to its service roles, you can define the following VMware Aria Automation Consumption project roles:

- Project administrator
- Project member
- Project viewer
- Project supervisor

4-28 Service Roles: VMware Aria Automation Pipelines

The VMware Aria Automation Pipelines service has several roles with key responsibilities.



VMware Aria Automation Pipelines has the following service roles:

- VMware Aria Automation Pipelines Administrator:
  - Create, manage, and execute pipelines
  - Mark an endpoint or variable as restricted
  - Run pipelines that include restricted endpoints or variables
  - Create, view, and manage dashboards
- VMware Aria Automation Pipelines Developer:
  - Can perform the same actions as an administrator except running and managing restricted endpoints or variables
- VMware Aria Automation Pipelines User:
  - Can access the VMware Aria Automation Pipelines service
- VMware Aria Automation Pipelines Viewer:
  - View pipelines, endpoints, and dashboards
  - View pipeline execution

- VMware Aria Automation Pipelines Executor:
  - Can perform the same actions as a viewer
  - Run, resume, pause, and cancel pipeline execution

In addition to its service roles, you can define the following VMware Aria Automation Pipelines project roles:

- Project administrator
- Project member
- Project viewer

To define a VMware Aria Automation Pipelines project role:

1. In the VMware Aria Automation console, select **Configure** > **Projects** in the navigation pane on the left.
2. Open the target project.
3. Click the **Users** tab.
4. Click **Add Users** or **Add Groups** to add a specific user or group and then select the target project role.
5. Click **ADD**.
6. Click **SAVE**.

4-29 Service Roles: VMware Aria Automation Orchestrator

The VMware Aria Automation Orchestrator service has multiple roles with several key responsibilities.



VMware Aria Automation Orchestrator has the following service roles:

- VMware Aria Automation Orchestrator Administrator:
  - Access to built-in workflows, actions, policies, built-in packages, configurations, and resources
  - Add Git repositories
- VMware Aria Automation Orchestrator Workflow Designer:
  - Create new workflows, actions, and policies
  - Import packages, configurations, and resources
- VMware Aria Automation Orchestrator Viewer:
  - Read-only access role

4-30 Service Roles: VMware Aria Automation Config

The VMware Aria Automation Config service has multiple roles with several key responsibilities.



VMware Aria Automation Config has the following service roles:

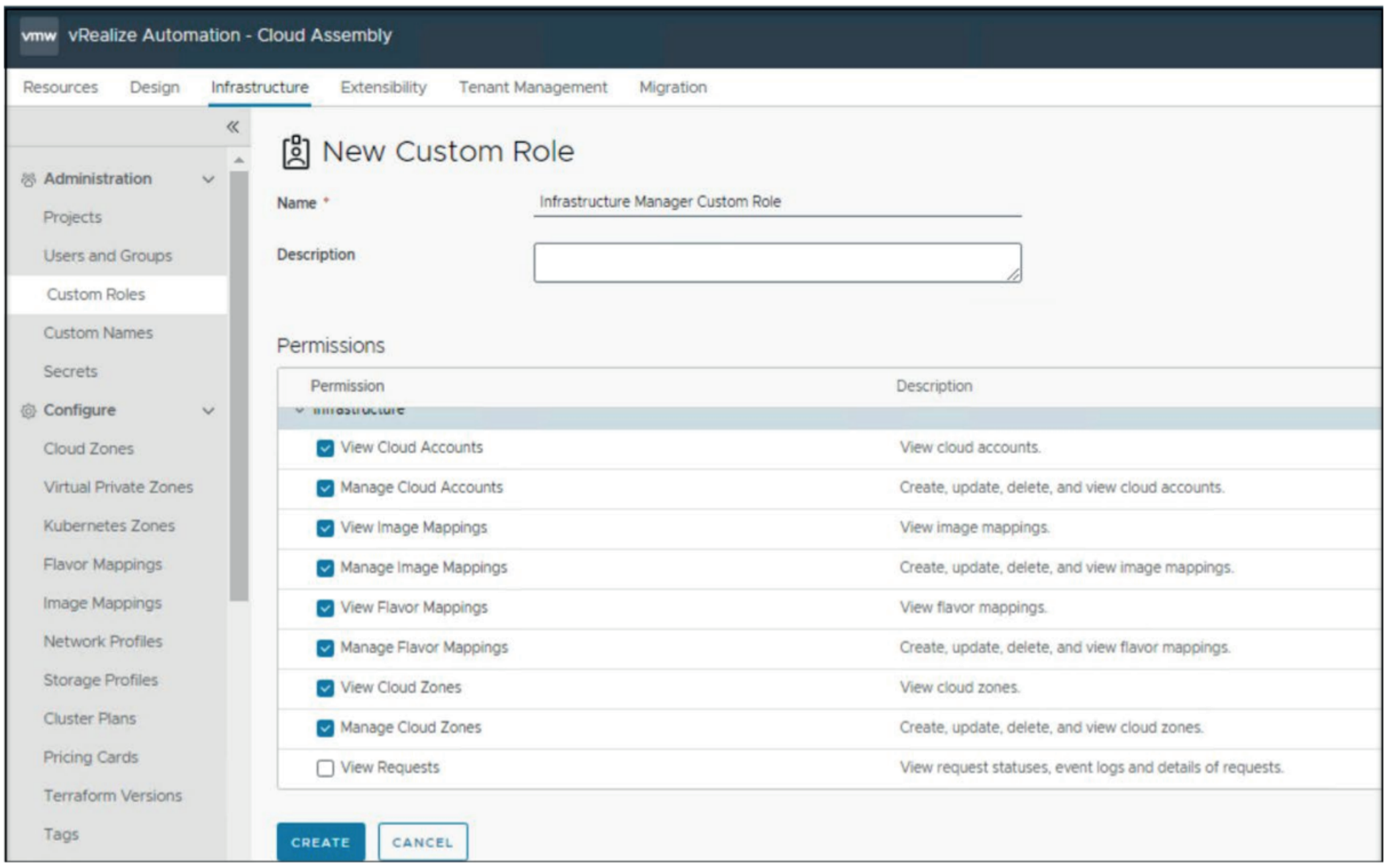
- VMware Aria Automation Config User:
  - This default role is assigned to all new local users and directory-synced users
  - It contains fundamental permissions, such as Read access
  - Generate reports for certain minions and job types
  - Permissions are limited to the role's resource access
- VMware Aria Automation Config Administrator:
  - Configure the Salt master and Salt minions
  - Create and manage resources such as jobs, remote execution module, and targets
  - Permissions are limited to the role's resource access
- VMware Aria Automation Config Superuser:
  - Perform any operation in VMware Aria Automation Config

To access the VMware Aria Automation Config service, the user must also be assigned the VMware Aria Automation Assembler Administrator role.

4-31 About VMware Aria Automation Custom Roles

To create a VMware Aria Automation custom role:

1. In the navigation pane on the left, select **Infrastructure** > **Administration** > **Custom Roles**.
2. Click **NEW CUSTOM ROLE**.
3. Enter a descriptive name for the new custom role in the **Name** text box.
4. Select the check boxes under Permissions to assign specific permissions to the custom role.
5. Click **CREATE**.



Using VMware Aria Automation, you can create custom roles to define granular user roles. A custom role is defined by the VMware Aria Automation Assembler Administrator or the VMware Aria Automation Consumption Administrator for all the services. After defining a custom role, you should assign it to a user or group. The user or group must have at least a Viewer role in the relevant services so that they can access the service.

For information about custom roles, see "Custom User Roles with vRealize Automation" at https://blogs.vmware.com/management/2020/07/custom-roles-with-vrealize-automation.html and see the chapter about custom user roles in *Using and Managing Cloud Assembly* at https://docs.vmware.com/en/vRealize-Automation/index.html.

4-32 Lab 6: Assigning User Roles

Assign various VMware Aria Automation roles to Active Directory users:

1. Assign Roles to Enterprise Groups
2. Create and Assign a Custom Role
3. Verify Organization Roles
4. Verify VMware Aria Automation Assembler Service Roles

4-33 Review of Learner Objectives

- Identify the user roles available in VMware Aria Automation
- Explain the key tasks performed by each user role

4-34 Lesson 3: Multitenancy and Virtual Private Zones

4-35 Learner Objectives

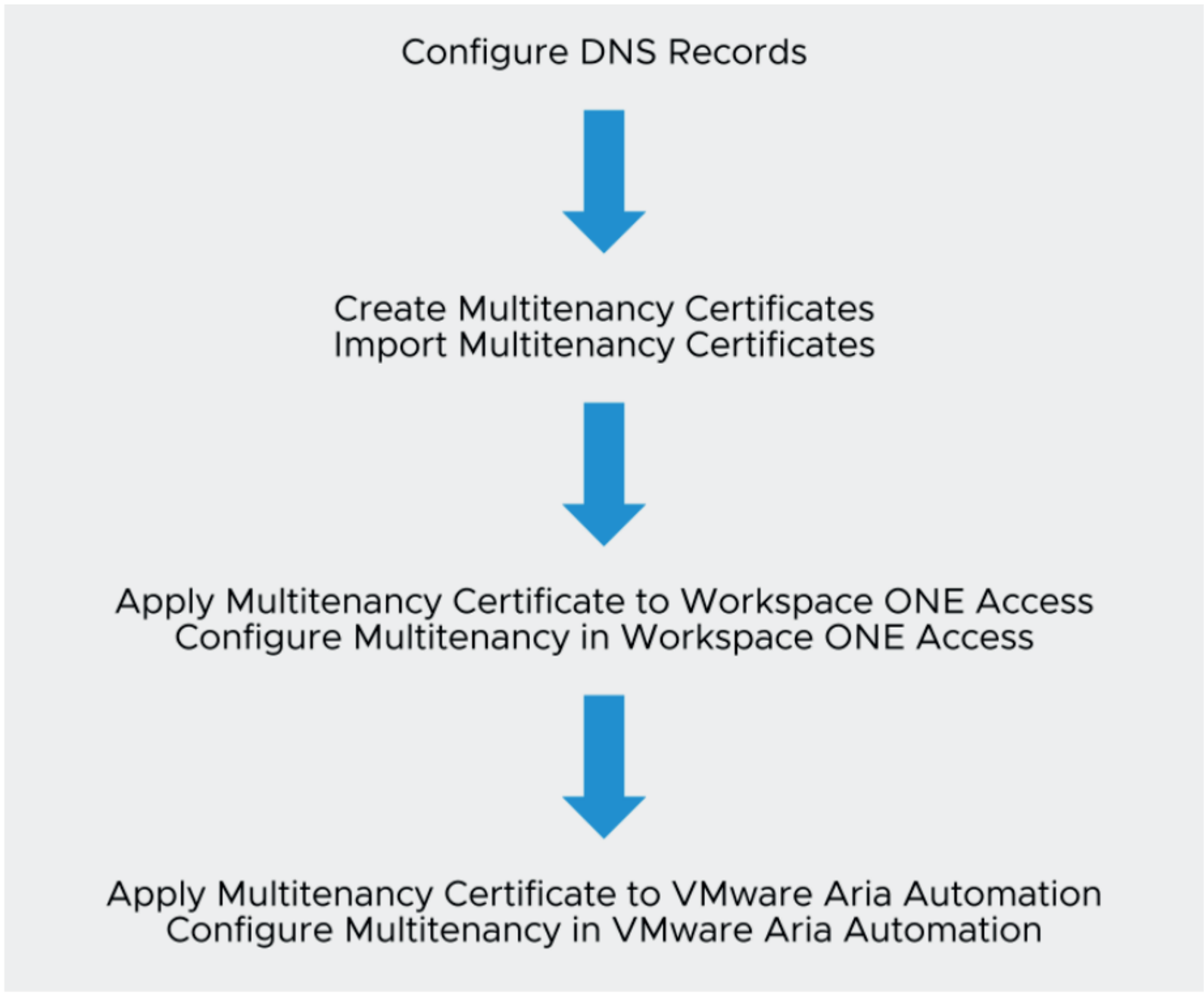
- Create multitenancy certificates
- Enable multitenancy in Workspace ONE Access
- Enable multitenancy in VMware Aria Automation
- Create tenants

4-36 Multitenancy in VMware Aria Automation

With multitenancy, a single instance of VMware Aria Automation can be securely shared by multiple customers (also called tenants).

Tenants can create their own projects, flavor mappings, image mappings, tags, deployments, and so on.

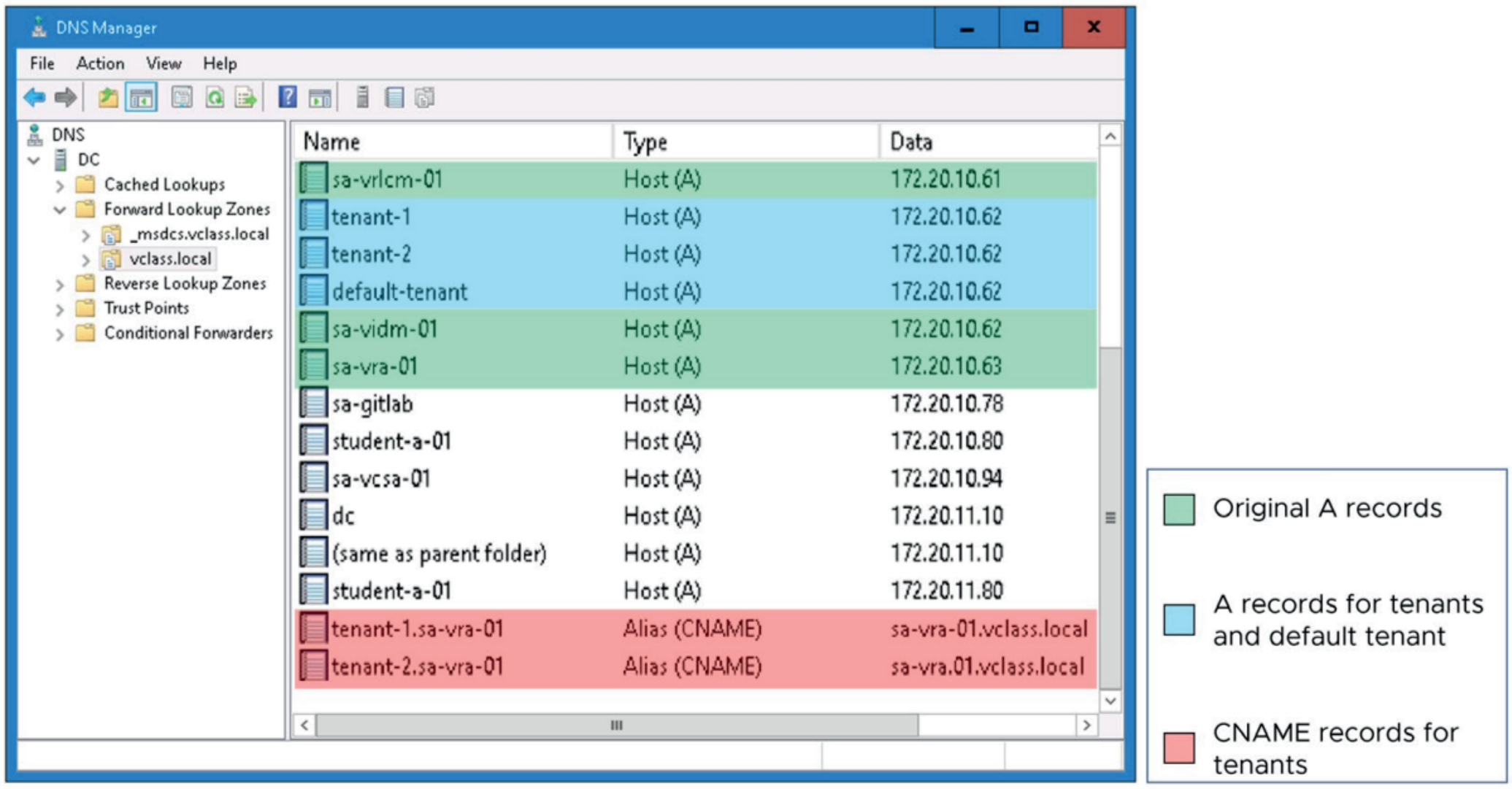
The multitenancy configuration procedure is performed in VMware Aria Suite Lifecycle.



For a detailed explanation of the multitenancy configuration process, see vRealize Automation 8.1 - Multi-Tenancy Setup with vRealize Suite Lifecycle Manager 8.1 at https://www.youtube.com/watch?v=-djlJMHfgos.

4-37 Configuring DNS Records

Multitenancy in VMware Aria Automation requires DNS records.



Configuring multitenancy in VMware Aria Automation requires configuring additional DNS records.

In the example, the machines highlighted in green (sa-vrlcm-01, sa-vidm-01, and sa-vra-01) were deployed when VMware Aria Automation was originally deployed in a single-tenant configuration.

These machines have the following FQDNs:

- The VMware Aria Suite Lifecycle appliance: sa-vrlcm-01.vclass.local
- The Workspace ONE Access appliance: sa-vidm-01.vclass.local
- The VMware Aria Automation appliance: sa-vra-01.vclass.local

In addition to the DNS records for those initial machines, configuring multitenancy requires creating additional DNS A records and CNAME records.

The DNS records for the machines highlighted in blue (default-tenant, tenant-1, and tenant-2) are A records. You must create an A record for the default tenant and a separate A record for each of the other tenants. The IP address for each of these A records must match the IP address of the Workspace ONE Access appliance. In the example, the IP address is 172.20.10.62 to match the IP address of sa-vidm-01.

These machines have the following FQDNs:

- default-tenant.vclass.local
- tenant-1.vclass.local
- tenant-2.vclass.local

The DNS records for the machines highlighted in red (tenant-1.sa-vra-01 and tenant-2.sa-vra-01) are CNAME records. You must create a separate CNAME record for each tenant. The CNAME record for each tenant must point to the FQDN of the VMware Aria Automation appliance. In the example, this CNAME record is sa-vra-01.vclass.local.

These machines have the following FQDNs:

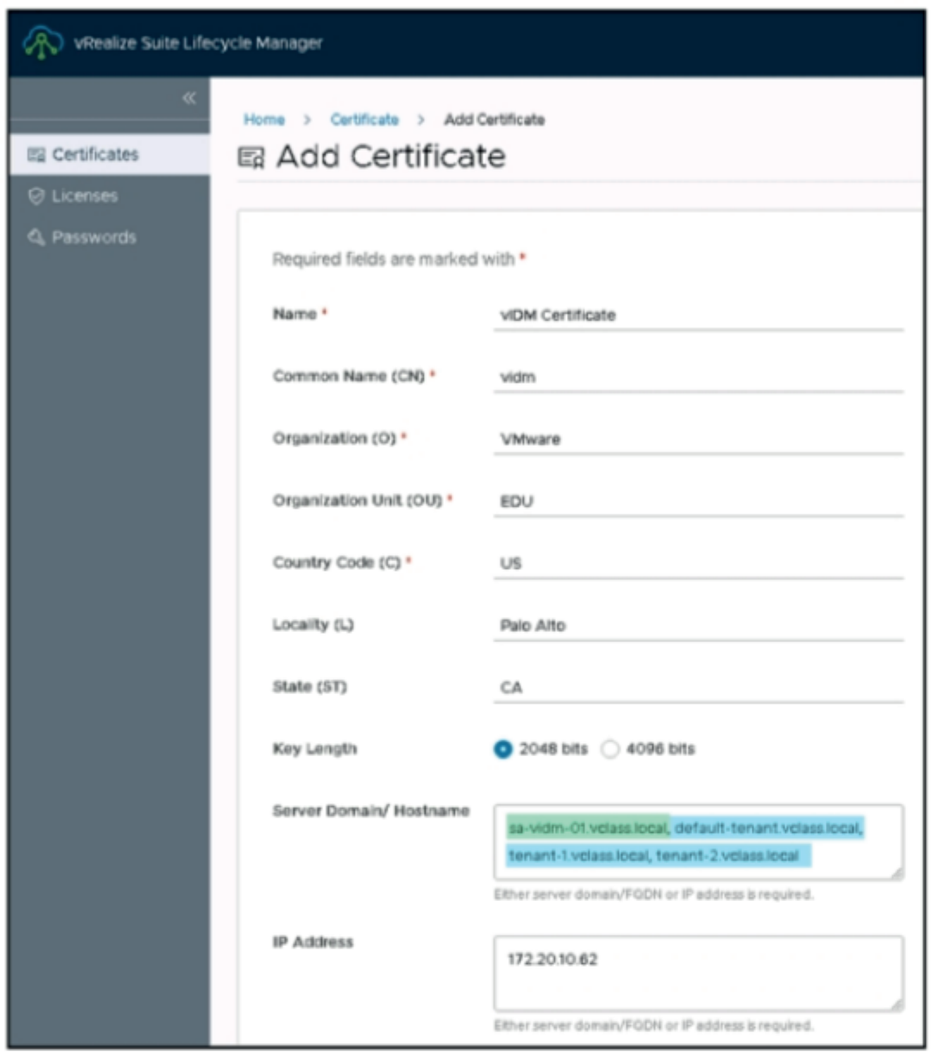
- tenant-1.sa-vra-01.vclass.local
- tenant-2.sa-vra-01.vclass.local

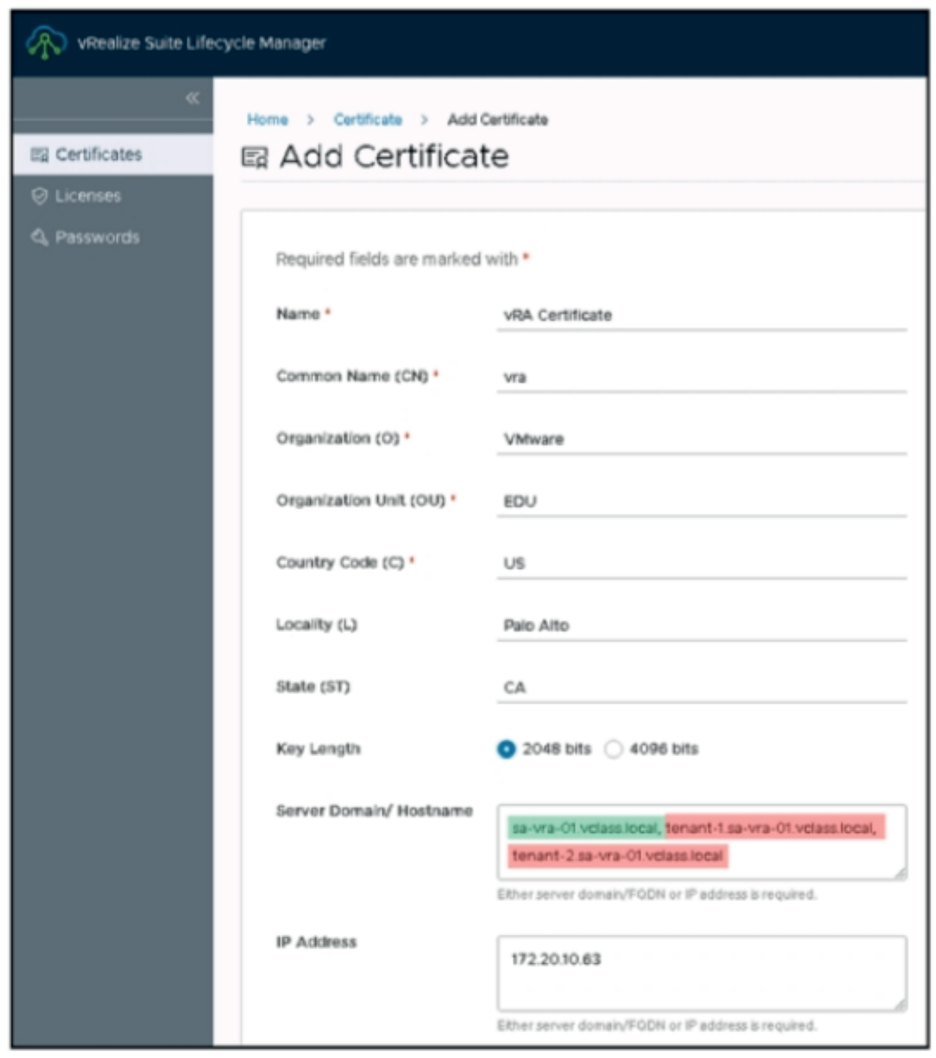
The tenant CNAME records use the name of the VMware Aria Automation appliance as a subdomain. These FQDNs can be lengthy, which is something to consider when naming the VMware Aria Automation appliance.

Do not create a CNAME record for the default tenant.

4-38 Creating Multitenancy Certificates

Generate new Certificate Signing Requests (CSRs) in VMware Aria Suite Lifecycle by selecting **Locker** > **Certificates** > **GENERATE.**





Original A records A records for tenants and default tenant CNAME records for tenants

You must generate separate certificates for Workspace ONE Access and VMware Aria Automation.

In the **Server Domain/Hostname** text box of the Workspace ONE Access certificate, include the following values as a comma-separated list:

- sa-vidm-01.vclass.local: FQDN of the Workspace ONE Access appliance
- default-tenant.vclass.local: FQDN of the default tenant
- tenant-1.vclass.local: FQDN of the first tenant
- tenant-2.vclass.local: FQDN of the second tenant
- FQDNs of additional tenants

The certificate for Workspace ONE Access can optionally include the IP address of the Workspace ONE Access appliance.

In the **Server Domain/Hostname** text box of the VMware Aria Automation certificate, include the following values as a comma-separated list:

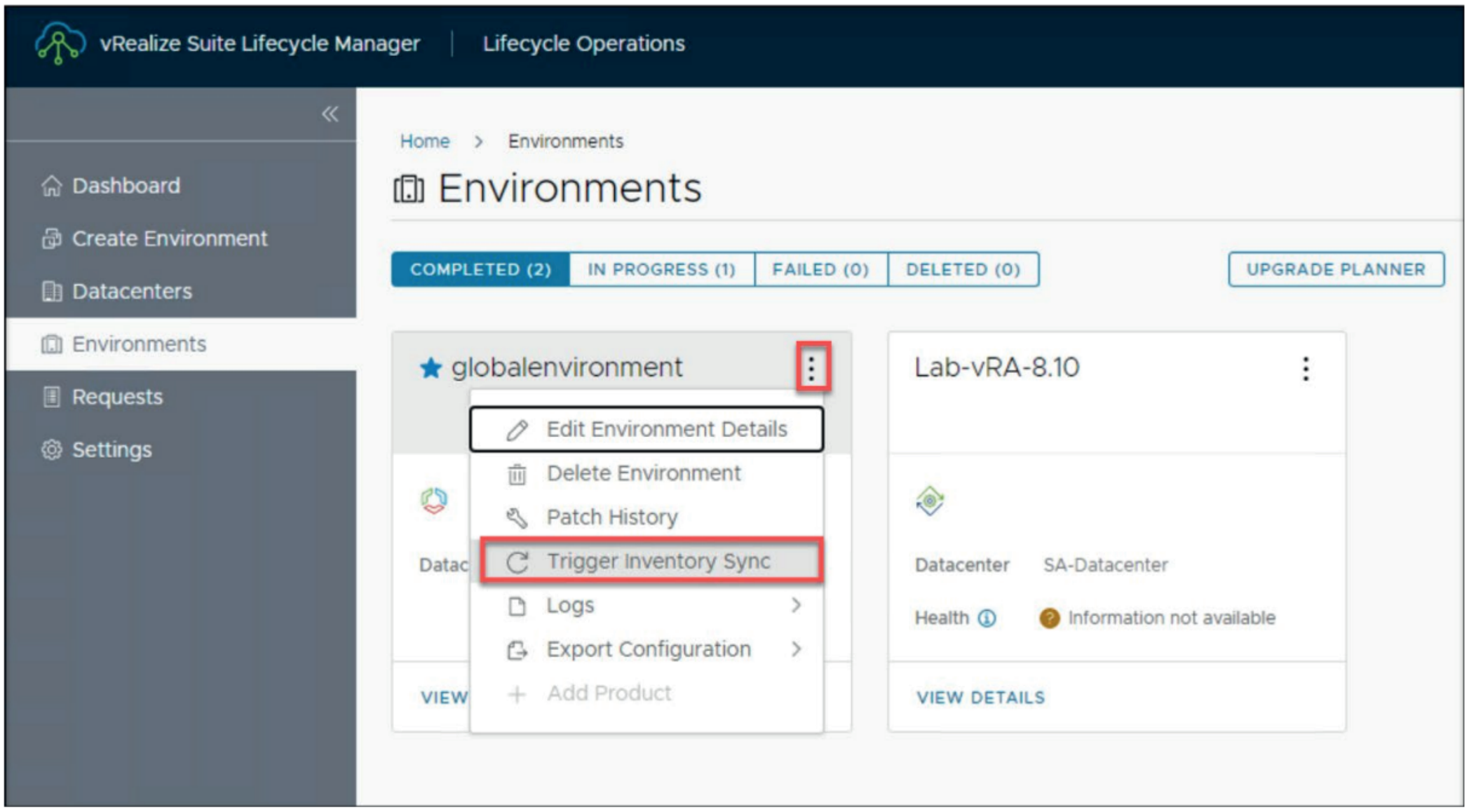
- sa-vra-01.vclass.local: FQDN of the VMware Aria Automation appliance
- tenant-1.sa-vra-01.vclass.local: FQDN of the first tenant
- tenant-2.sa-vra-01.vclass.local: FQDN of the second tenant
- FQDNs of any additional tenants

The certificate for VMware Aria Automation can optionally include the IP address of the VMware Aria Automation appliance.

Using wildcard certificates is possible, but Subject Alternative Name (SAN) certificates are generally preferred for security reasons.

4-39 Applying Multitenancy Certificates to Workspace ONE Access (1)

To start applying the multitenancy certificate to Workspace ONE Access, you trigger an inventory sync.

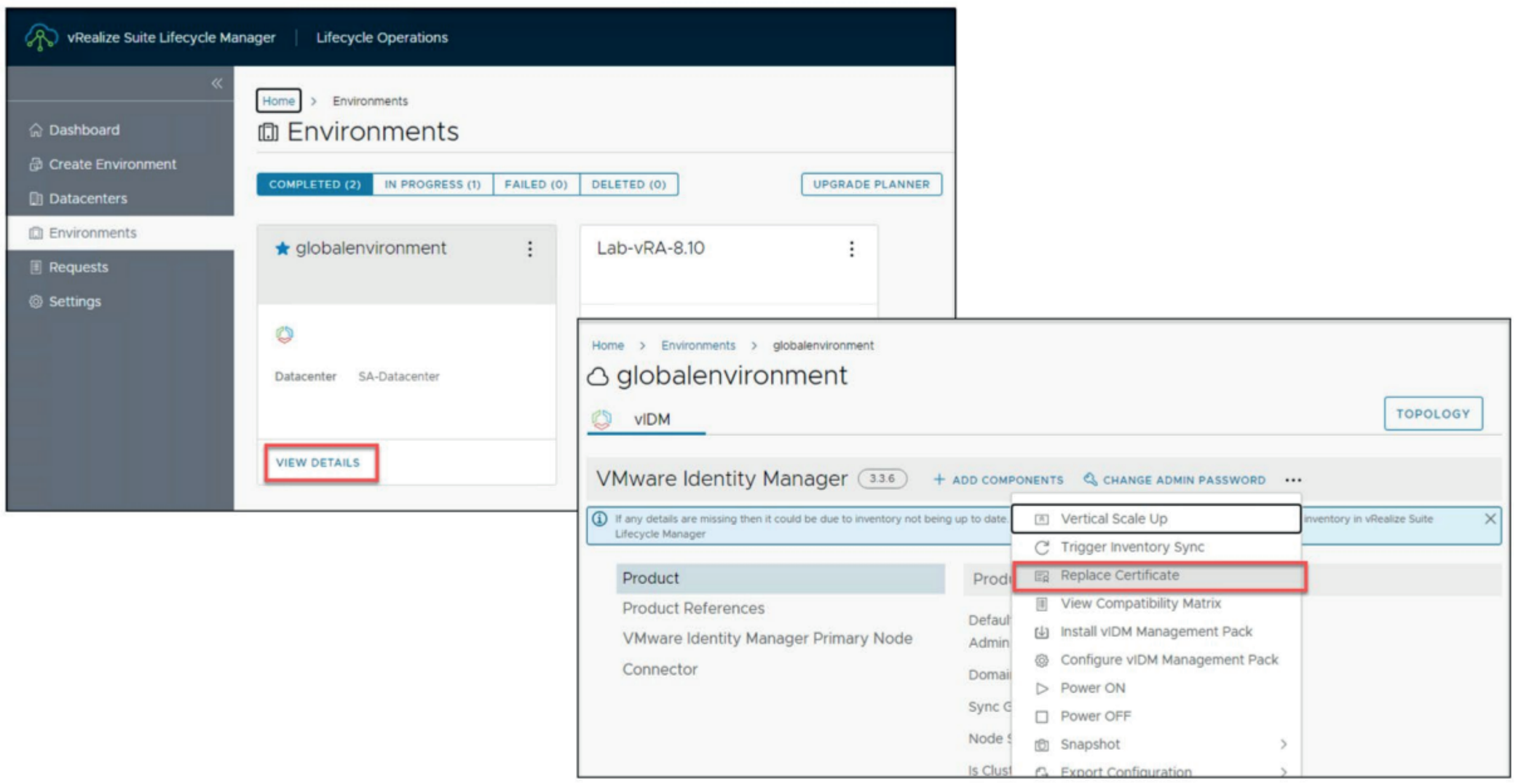


To trigger an inventory sync and start applying multitenancy:

1. Log in to VMware Aria Suite Lifecycle.
2. Select **Lifecycle Operations** > **Environments** in the left navigation pane.
3. Click the vertical ellipsis icon next to globalenvironment and select **Trigger Inventory Sync**.

4-40 Applying Multitenancy Certificates to Workspace ONE Access (2)

After triggering an inventory sync, you replace the single-tenant certificate with the multitenancy certificate.



To replace the single-tenant certificate with the multitenancy certificate that you created:

1. Select **Lifecycle Operations** > **Environments** in the left navigation pane.
2. Under globalenvironment, click **VIEW DETAILS**.
3. Click the vertical ellipsis icon next to VMware Identity Manager and select **Replace Certificate**.

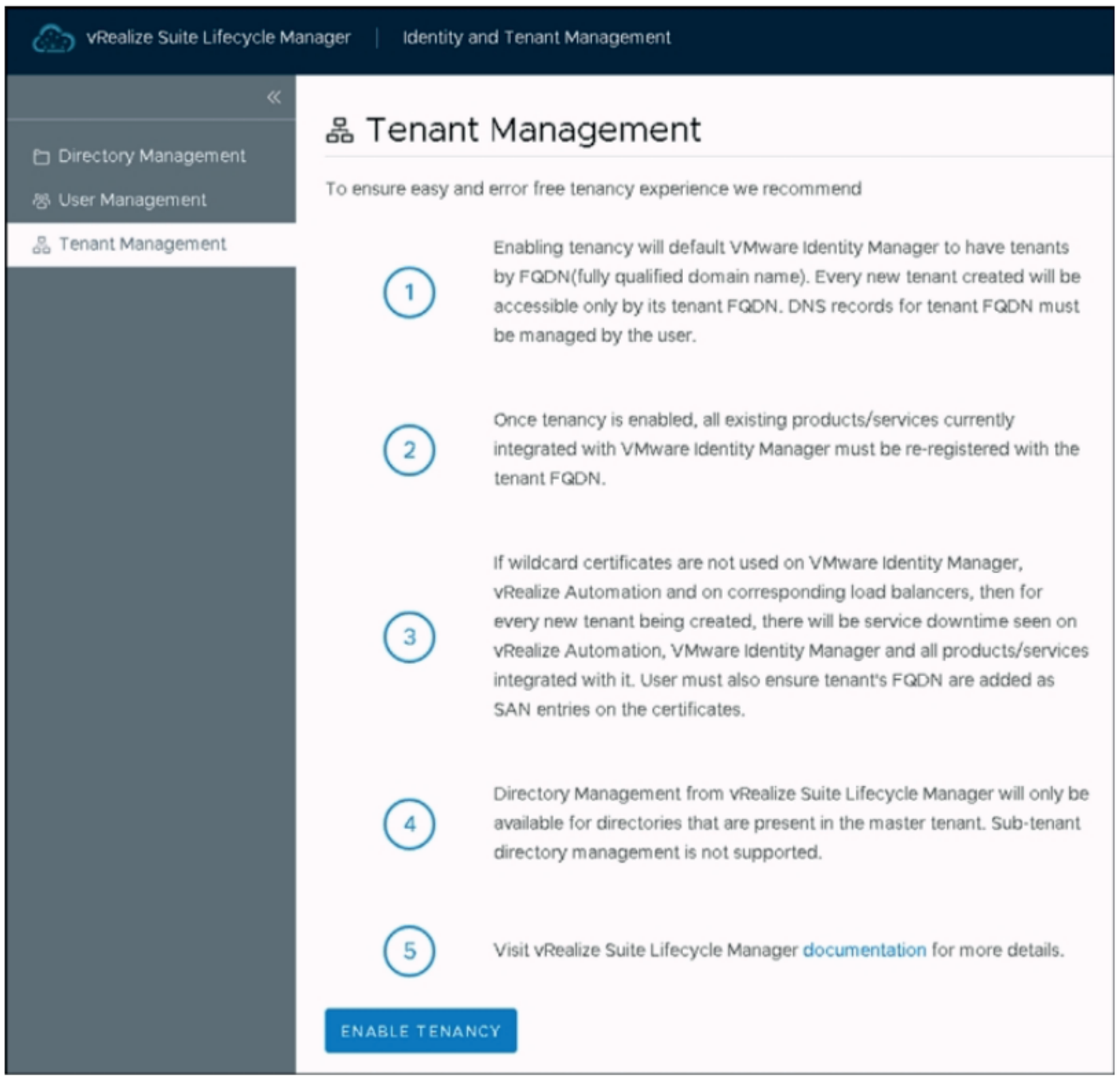
During the process, you are prompted to re-trust the certificate for VMware Aria Automation. Select the check box.

You are prompted to have a snapshot taken. The snapshot is a protective measure that enables you to roll back if the procedure fails.

You are prompted to run a precheck. If errors are found during the precheck, fix these issues. A normal and expected warning appears that the procedure will shut down the product to perform the snapshot. This process causes downtime, so the precheck prompts you to consent to the shutdown.

4-41 Configuring Multitenancy in Workspace ONE Access

To enable multitenancy in Workspace ONE Access, you select **Identity and Tenant Management** > **Tenant Management** in VMware Aria Suite Lifecycle and click **ENABLE TENANCY**.

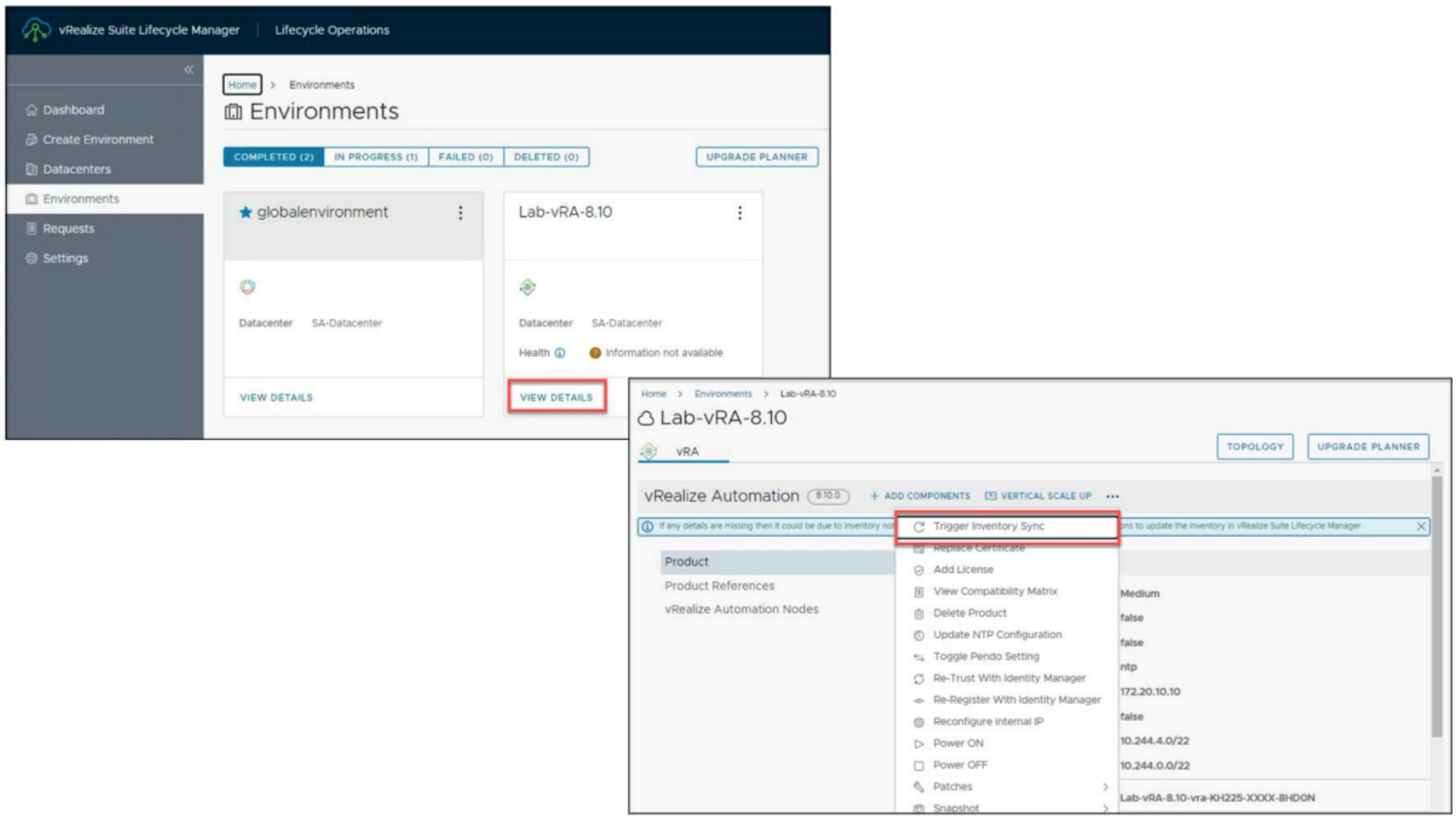


When you use VMware Aria Suite Lifecycle to enable multitenancy in Workspace ONE Access, you are prompted to take a snapshot and perform an inventory sync.

In the **Master Tenant Alias** text box, enter the name of the default tenant, which is also called the provider organization.

4-42 Applying Multitenancy Certificates to VMware Aria Automation (1)

To start applying the multitenancy certificate to VMware Aria Automation, you trigger an inventory sync.

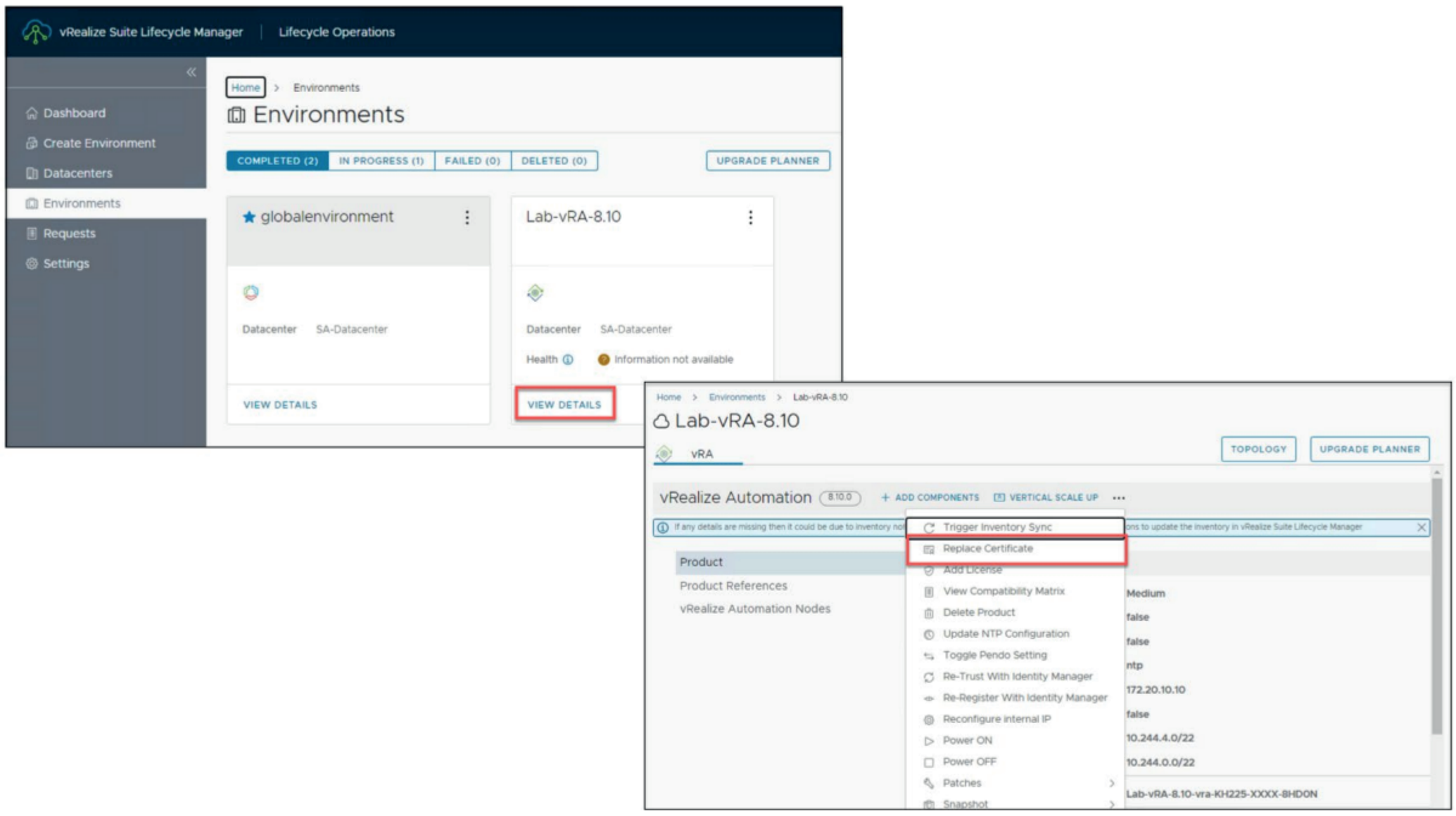


To begin the process of applying the multitenancy certificate to VMware Aria Automation:

1. Log in to VMware Aria Suite Lifecycle.
2. Select **Lifecycle Operations** > **Environments** in the left navigation pane.
3. Click **VIEW DETAILS** under your existing VMware Aria Automation deployment.
4. Click the vertical ellipsis icon next to vRealize Automation and select **Trigger Inventory Sync**.

4-43 Applying Multitenancy Certificates to VMware Aria Automation (2)

After triggering an inventory sync, you replace the single-tenant certificate with the multitenancy certificate.



To replace the single-tenant certificate with the multitenancy certificate that you created:

1. Select **Lifecycle Operations** > **Environments** in the left navigation pane.
2. Click **VIEW DETAILS** under your existing VMware Aria Automation deployment.
3. Click the vertical ellipsis icon next to vRealize Automation and select **Replace Certificate**.

During the process, you are prompted to re-trust the certificate for VMware Aria Automation. Select the check box.

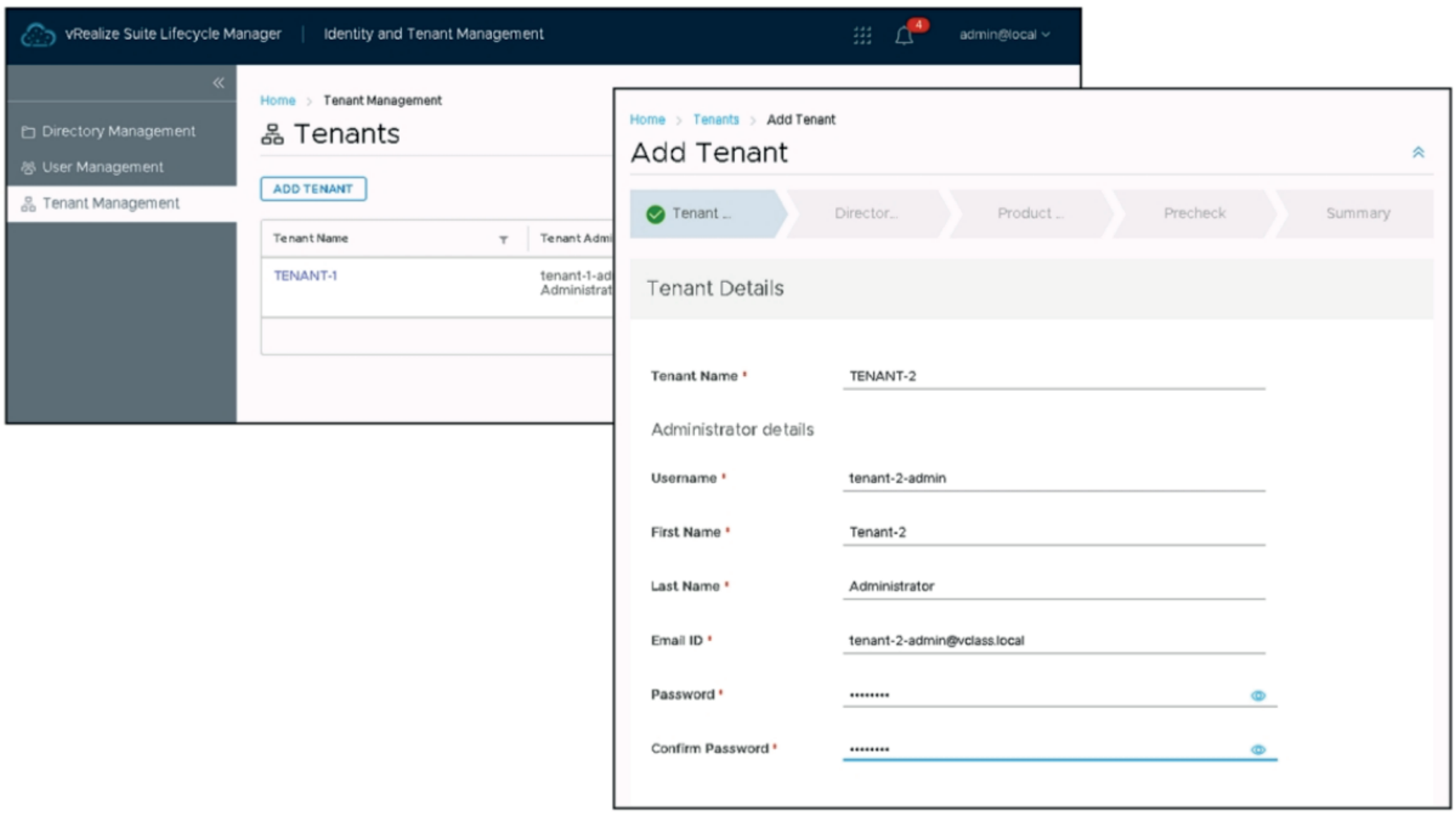
You are prompted to have a snapshot taken. The snapshot is a protective measure that enables you to roll back if the procedure fails.

You are prompted to run a precheck. If errors are found during the precheck, you must fix these issues. A normal and expected warning appears that the procedure will shut down the product to perform the snapshot. This shutdown causes downtime, so the precheck prompts you to consent to the shutdown.

4-44 Configuring Multitenancy in VMware Aria Automation

To create tenants, you select **Identity and Tenant Management** > **Tenant Management** and click **ADD TENANT**.

When prompted, specify the name of the new tenant, the contact information and password, and other details.



You can connect the new tenant to an Active Directory domain if the domain is already configured in the default tenant.

4-45 Virtual Private Zones

A Virtual Private Zone (VPZ) is a type of container of infrastructure capacity and services that can be defined and allocated to a tenant. The settings in each VPZ can only be changed by the Provider administrator.

You can add unique or shared cloud accounts, with associated compute, storage, networking, and tags to each VPZ.

Each component offers the same configuration options that might be available for a single-tenant configuration.

4-46 Lab 7: (Simulation) Configuring Multitenancy and VPZs

Configure VMware Aria Automation to support multiple tenants:

1. Create DNS Records
2. Create SSL Certificates
3. Replace the VMware Aria Automation SSL Certificate
4. Replace the Workspace ONE Access SSL Certificate
5. Enable Multitenancy in Workspace ONE Access
6. Create Tenants
7. Create a Virtual Private Zone
8. Allocate the VPZ to Tenant-1
9. Configure the Tenants

4-47 Review of Learner Objectives

- Create multitenancy certificates
- Enable multitenancy in Workspace ONE Access
- Enable multitenancy in VMware Aria Automation
- Create tenants

4-48 Key Points

- The identity service in the VMware Aria Automation appliance forwards the authentication requests to Workspace ONE Access.
- Workspace ONE Access can be integrated with Active Directory.
- The VMware Aria Automation roles are broadly classified into organization roles and service roles.
- A user must be assigned an organization role with an associated service role.

Questions?

Module 5

Basic Initial Configuration

5-2 Importance

You can configure VMware Aria Automation to start rapidly creating and deploying VMware Aria Automation Templates.

5-3 Lesson 1: Basic Initial Configuration

5-4 Learner Objectives

- Create a vCenter cloud account
- Create cloud zones
- Create projects
- Create flavor mappings
- Create image mappings

5-5 Basic Configuration Roadmap

You configure several items to create and deploy VMware Aria Automation Templates.



Configure VMware Aria Automation to create and deploy VMware Aria Automation Templates.

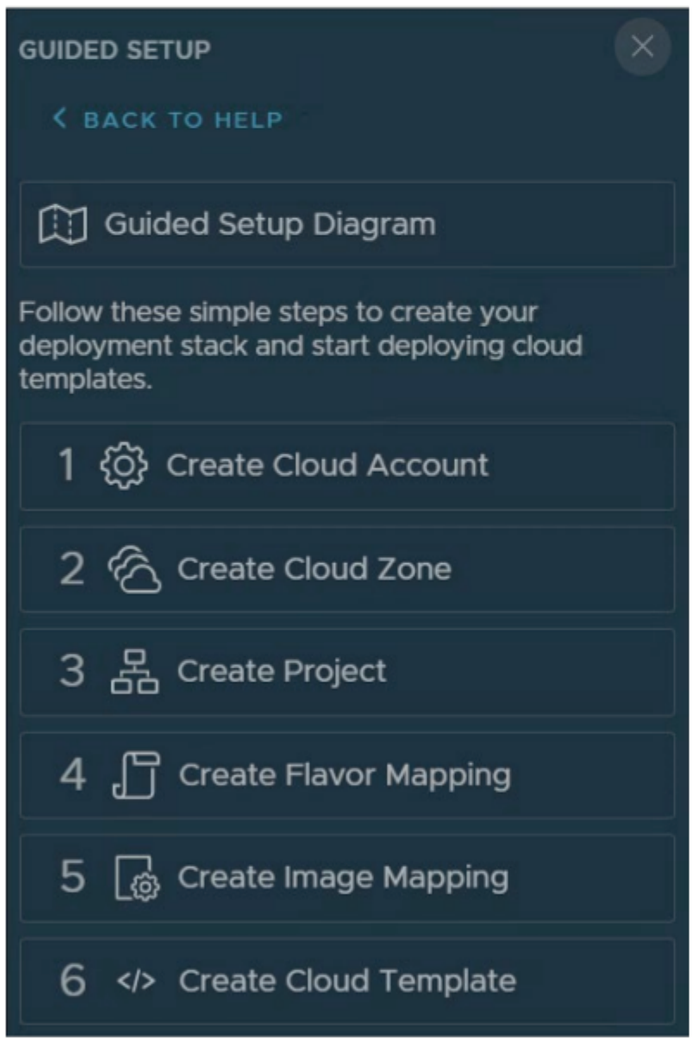
Use the following options to set up a basic configuration:

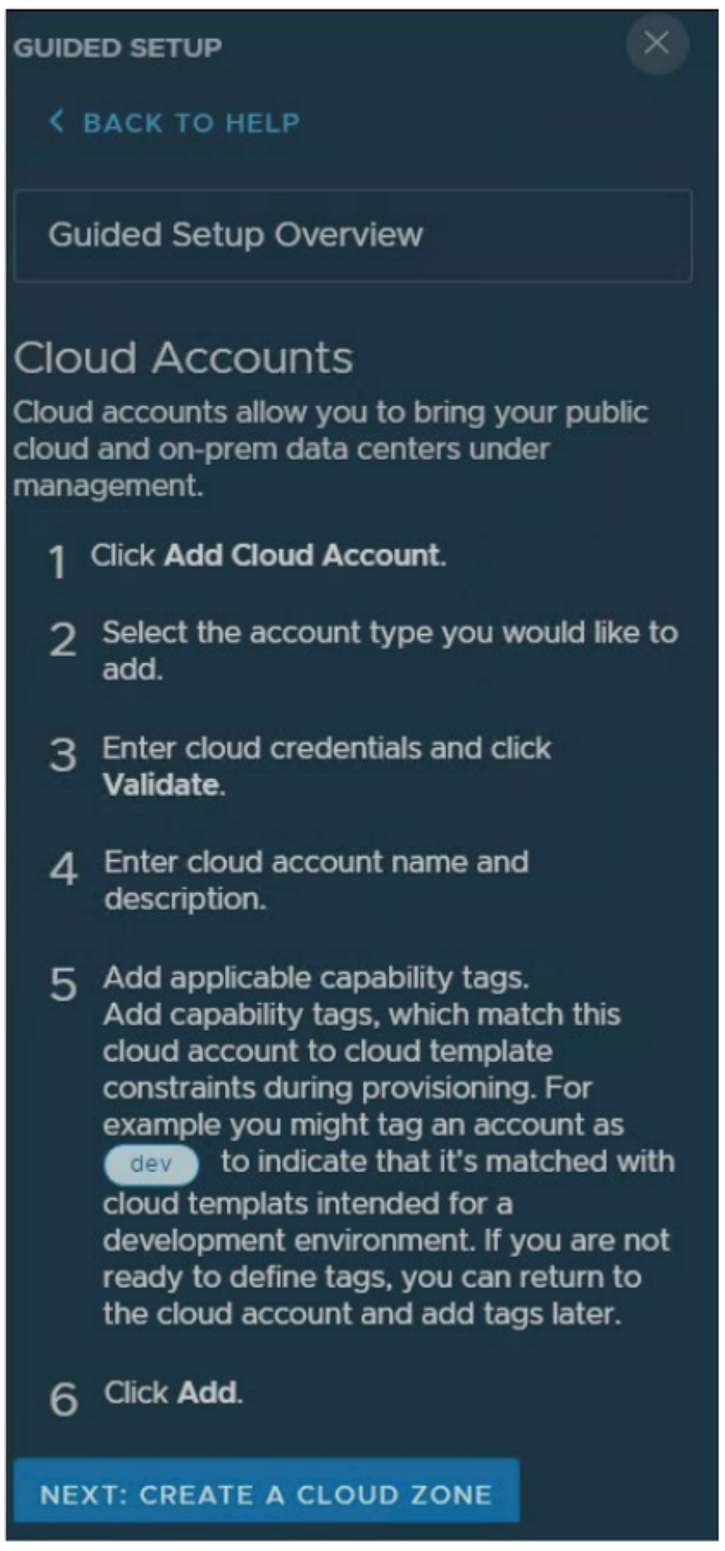
- Cloud account: Connects to resource providers to provision and manage the cloud infrastructure
- Cloud zone: Identifies a set of resources for provisioning within a cloud account
- Project: Defines who can use what resources
- One or more flavors: Groups a set of target deployment sizing's for a specific cloud account/region
- One or more image mappings: Groups a set of predefined target operating system specifications for a specific cloud account/region

5-6 Guided Setup

Click **GUIDED SETUP** in the upper-right corner of the VMware Aria Automation console to see a diagram of the simple configuration process:

- Click each step for detailed instructions.
- This diagram remains open during basic configuration.
- Click the bottom of the menu to proceed to the next step.

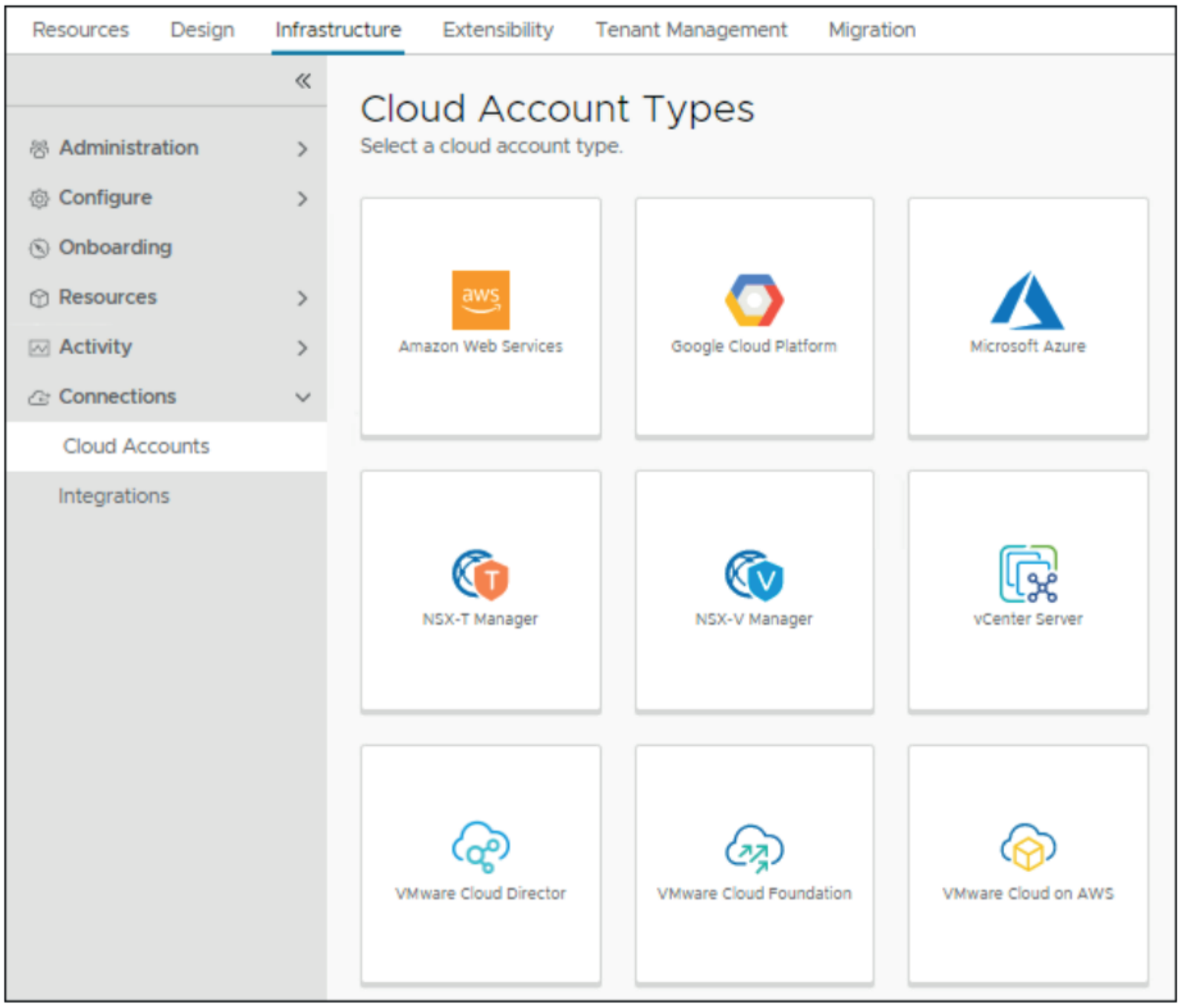




The **GUIDED SETUP** button appears in the upper-right corner of the VMware Aria Automation console. This wizard walks you through the basic setup process with detailed instructions about configuring each step.

5-7 Creating Cloud Accounts

Define resource providers by creating cloud accounts. In the navigation pane on the left, select **Infrastructure** > **Connections** > **Cloud Accounts** and click a resource provider. For example, click **vCenter** to add a vCenter system.

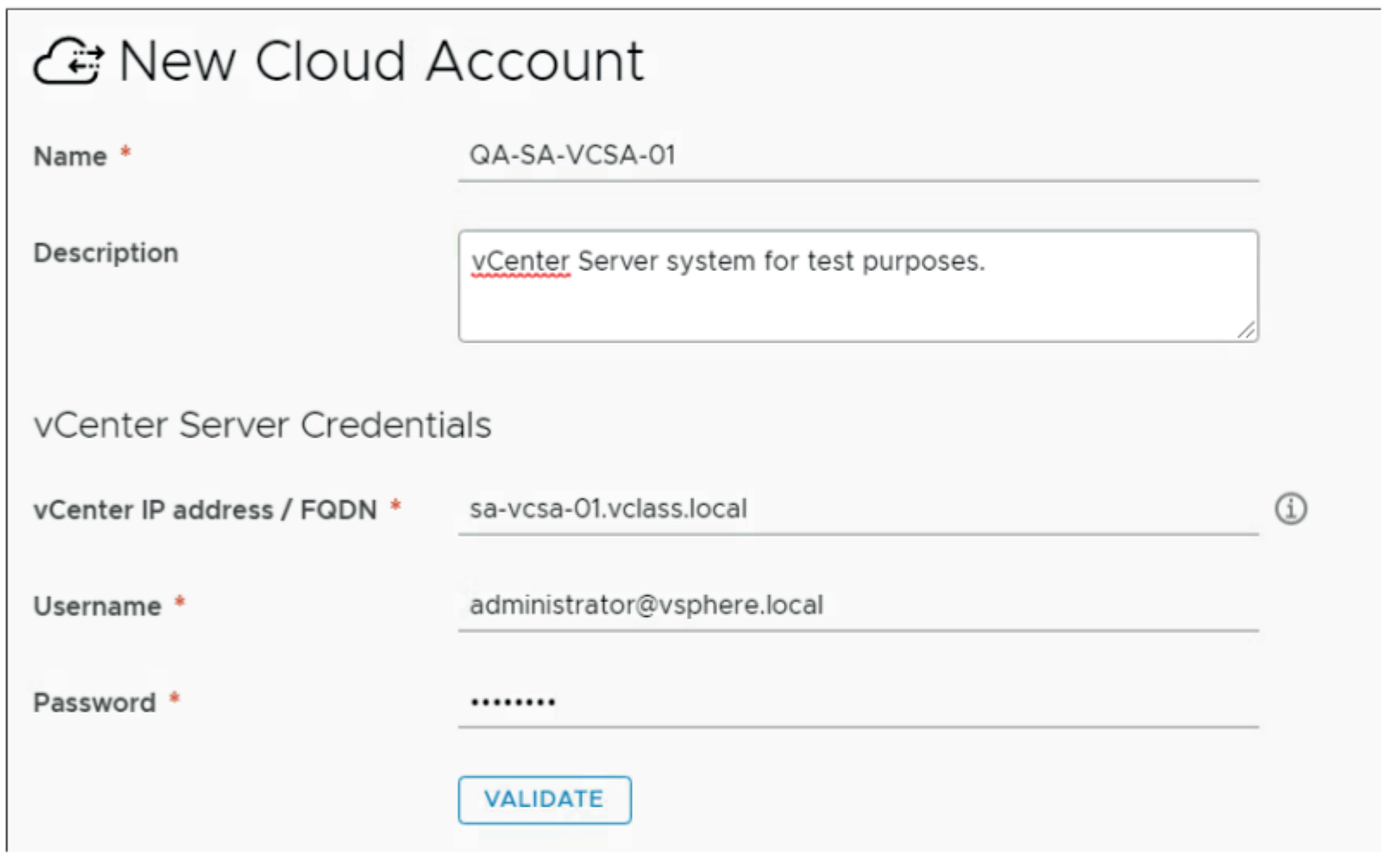


Cloud accounts connect systems to multiple types of resource providers. You can add or create multiple cloud accounts for each type of system.

5-8 Adding a vCenter Cloud Account

To configure a cloud account to connect to vCenter:

1. Enter the cloud account name and description.
2. Enter the FQDN or IP address of the vCenter system.
3. Enter the user name and password.
4. Click **VALIDATE**.

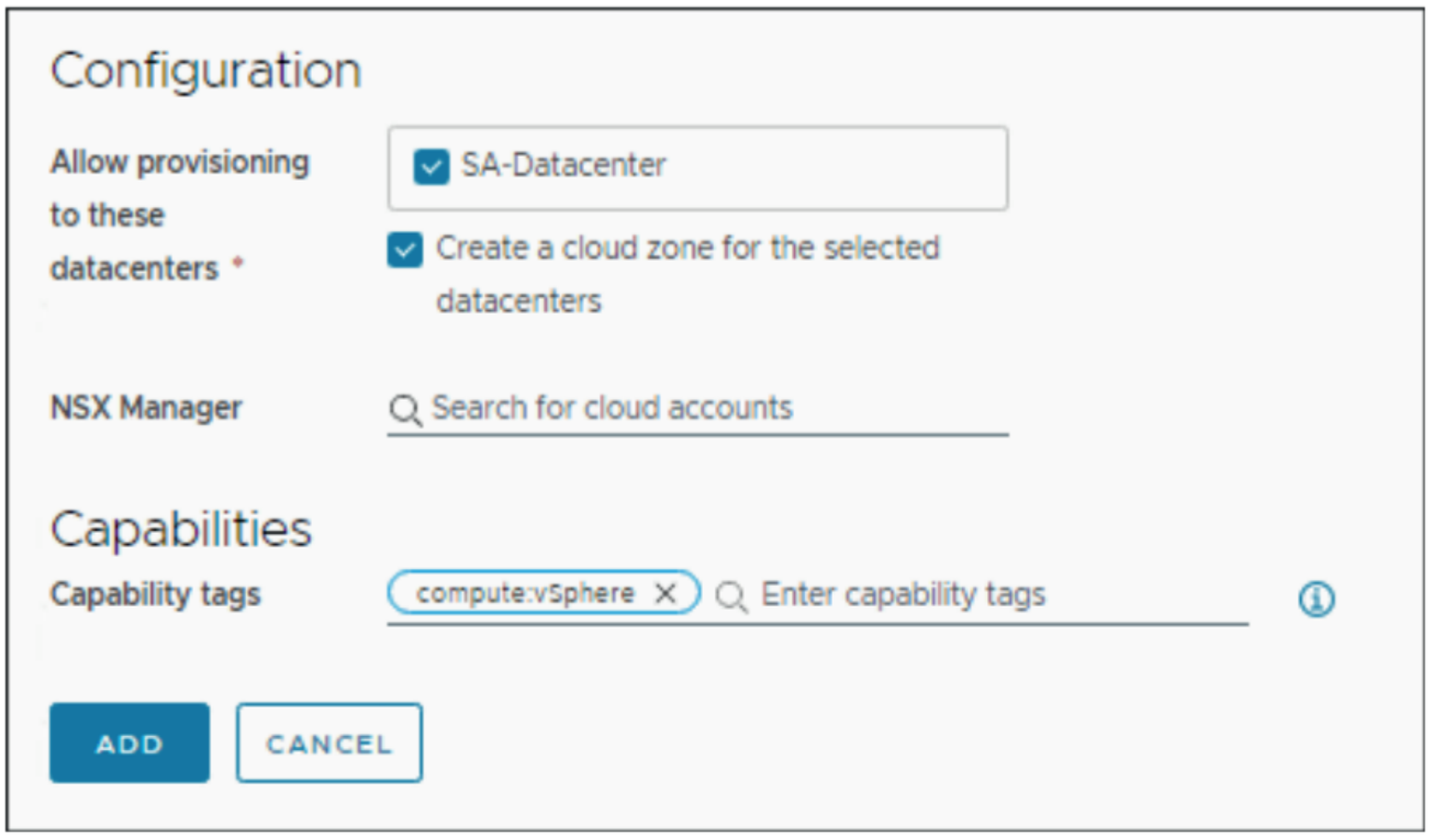


VMware Aria Automation must validate your user name and password. The best practice is to create a service account in vSphere that VMware Aria Automation uses for provisioning.

5-9 Creating a Cloud Zone and Enabling Provisioning

When creating the cloud account, the option is available to automatically create a cloud zone and enable provisioning:

1. Select the data centers to provision.
2. (Optional) Select the **Create a cloud zone for the selected datacenters** check box.



The screenshot is from the lower part of Adding a New Cloud Account page. After validating the connection to a vCenter system, all the data centers that were defined on that vCenter system appear. You must select **Allow Provisioning** on each data center on which you plan to provision VMware Aria Automation Templates.

If you select the **Create a cloud zone for the selected datacenters** check box, then cloud zones are created for those data centers. This method helps speed up the creation of the basic configuration.

If you do not select the **Create a cloud zone for the selected datacenters** check box, you can add a cloud zone later.

You cannot connect to an NSX endpoint currently because no NSX Cloud accounts have been created. You can connect the NSX endpoint to the vCenter cloud account later.

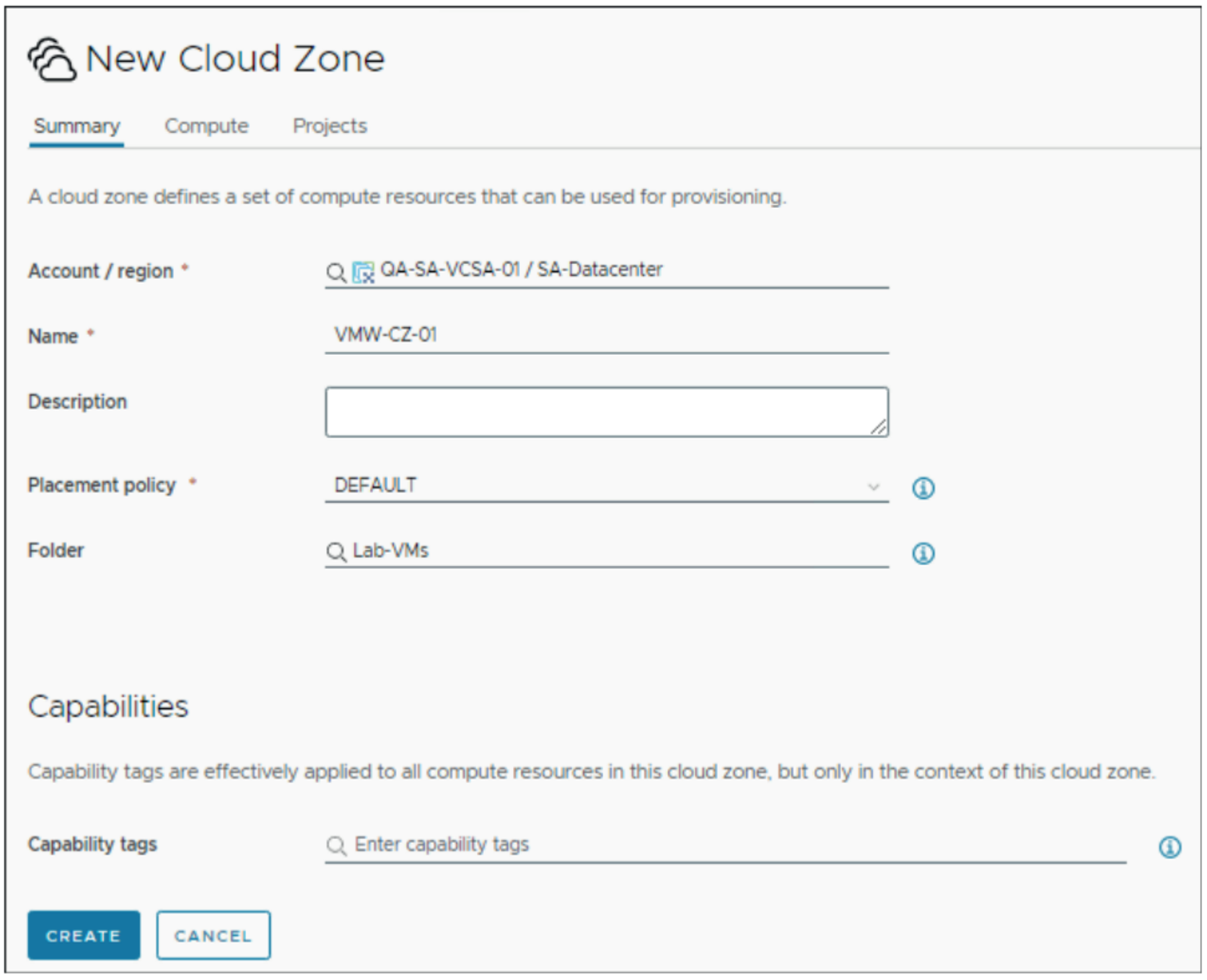
You can also add capability tags now, or you can add them later.

5-10 Creating Cloud Zones

A cloud zone helps to identify subsystems for provisioning within a cloud account. In vSphere, data centers are the provisioning systems.

To create a cloud zone:

1. In the navigation pane on the left, select **Infrastructure** > **Configure** > **Cloud Zones**.
2. Click **NEW CLOUD ZONE**.



The account or region can be selected from previously defined cloud accounts. You can also use placement policies and VM folders in vSphere.

Capability tags help to identify specific systems that are associated with a particular template.

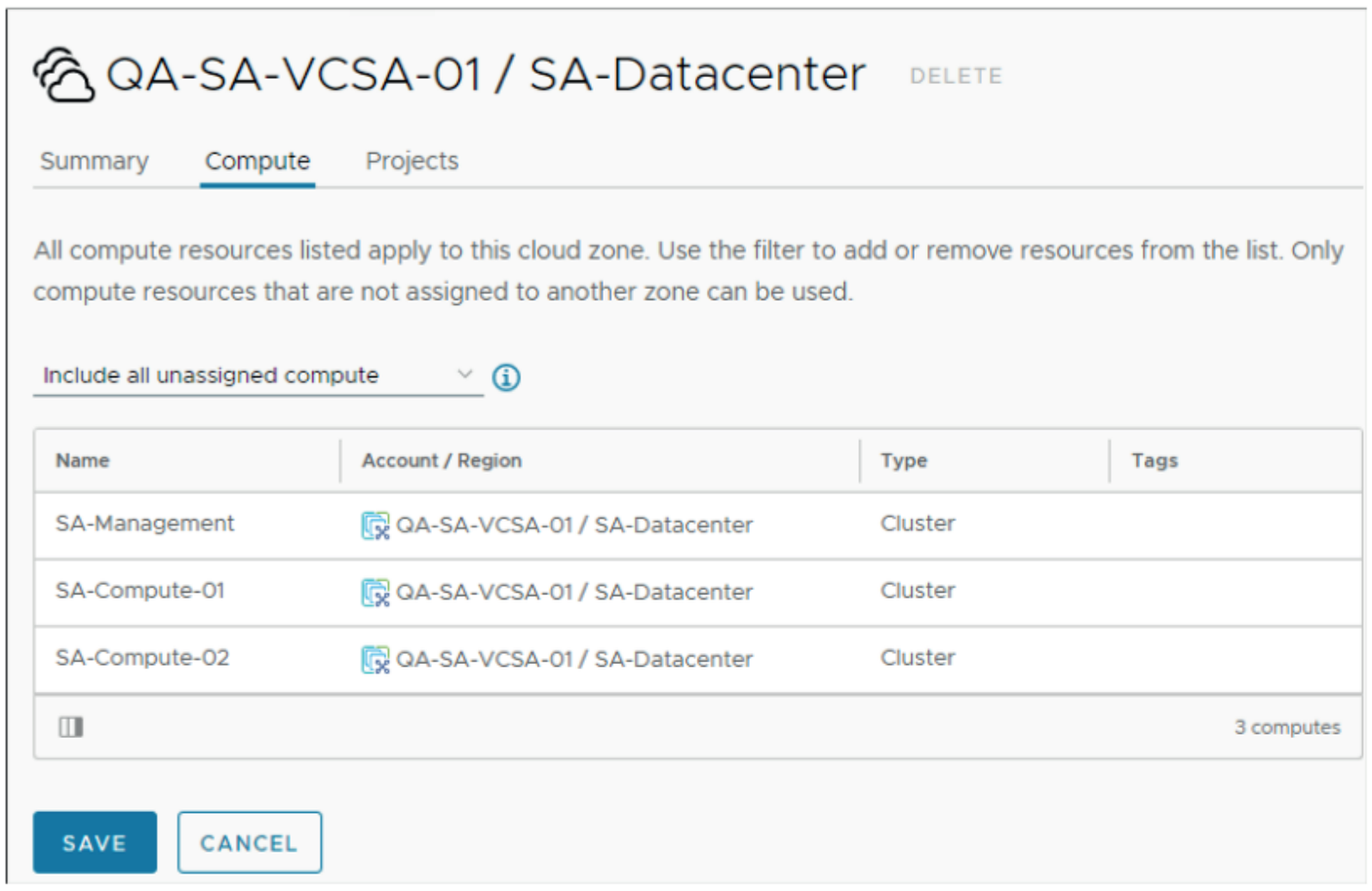
You can select one of the following placement policies:

- **DEFAULT**: Distributes compute resources across clusters and hosts randomly
- **BINPACK**: Places compute resources on the most loaded host that has enough available resources to run the given compute
- **SPREAD**: Provisions compute resources to the cluster or host with the fewest virtual machines

5-11 Cloud Zones: Selecting Compute Resources

On the **Compute** tab, specify the compute resources that the cloud zone can use:

- Select the clusters.
- Select the individual hosts.



You can select one of the following options to specify which clusters and hosts to use as resources:

- **Include all Compute**
- **Manually select compute**
- **Dynamically include compute by tags**

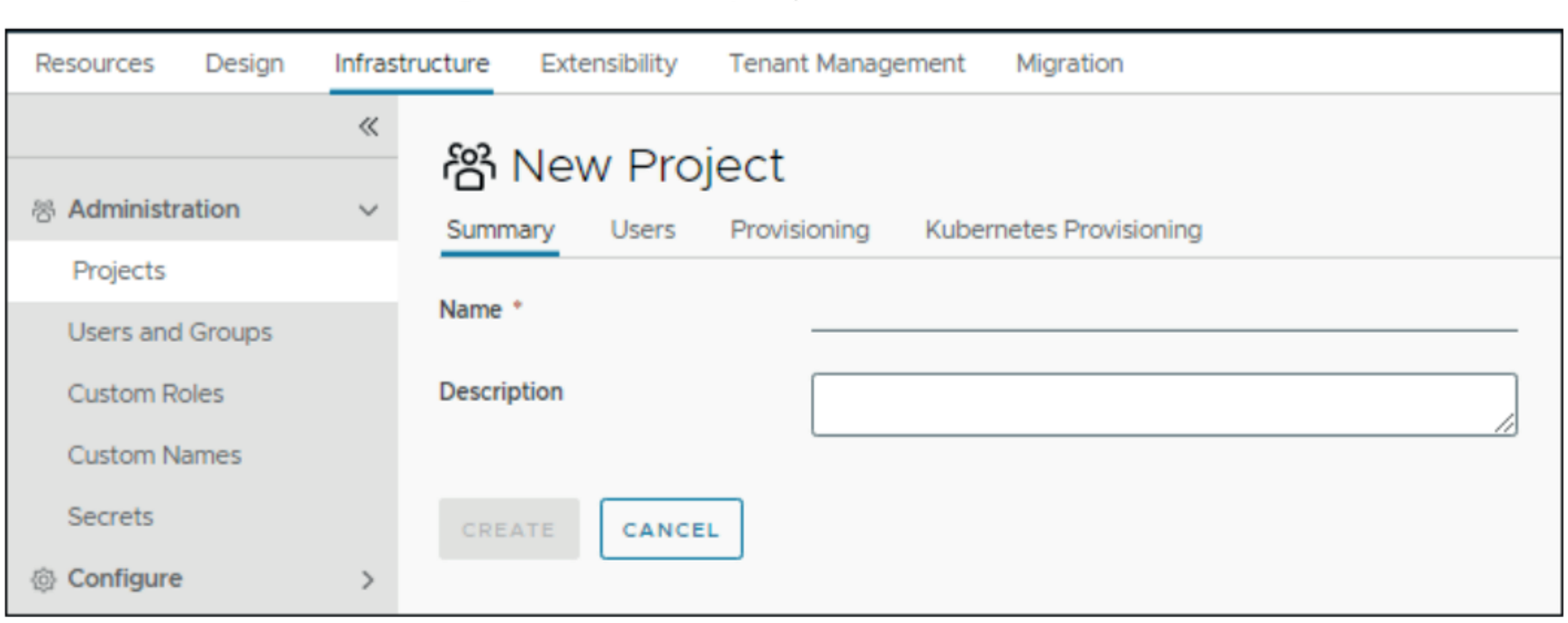
If you select a vSphere DRS cluster, only that cluster is available. If you select individual hosts, you can specify those individual hosts as targets. Cloud zones can be associated with projects at a later stage.

5-12 Creating Projects

Projects organize the VMware Aria Automation system into resources that are associated with users and groups.

To create a project:

1. Select **Infrastructure** > **Administration** > **Projects** and click **New Project**.
2. On the **Users** tab, add users and groups to the project.
3. On the **Provisioning** tab, link the project to cloud zones.



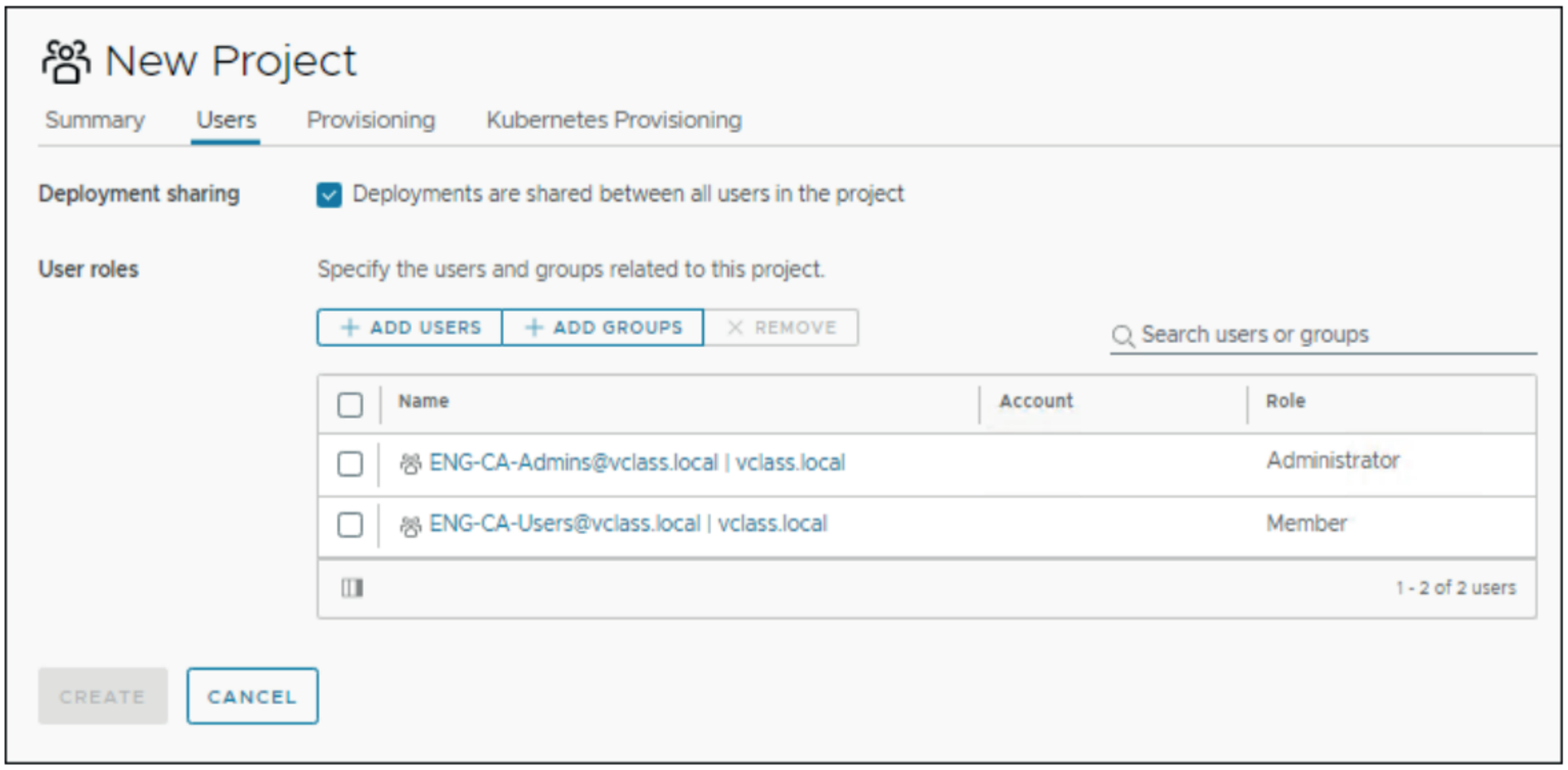
Projects map compute resources to users and groups.

Projects organize and govern which users can use which cloud zones to deploy VMware Aria Automation Templates in your cloud infrastructure.

Anyone who creates and deploys VMware Aria Automation Templates must be a member of at least one project.

5-13 Project: Adding Users and Groups

Add groups and users to the project and assign different roles to them.

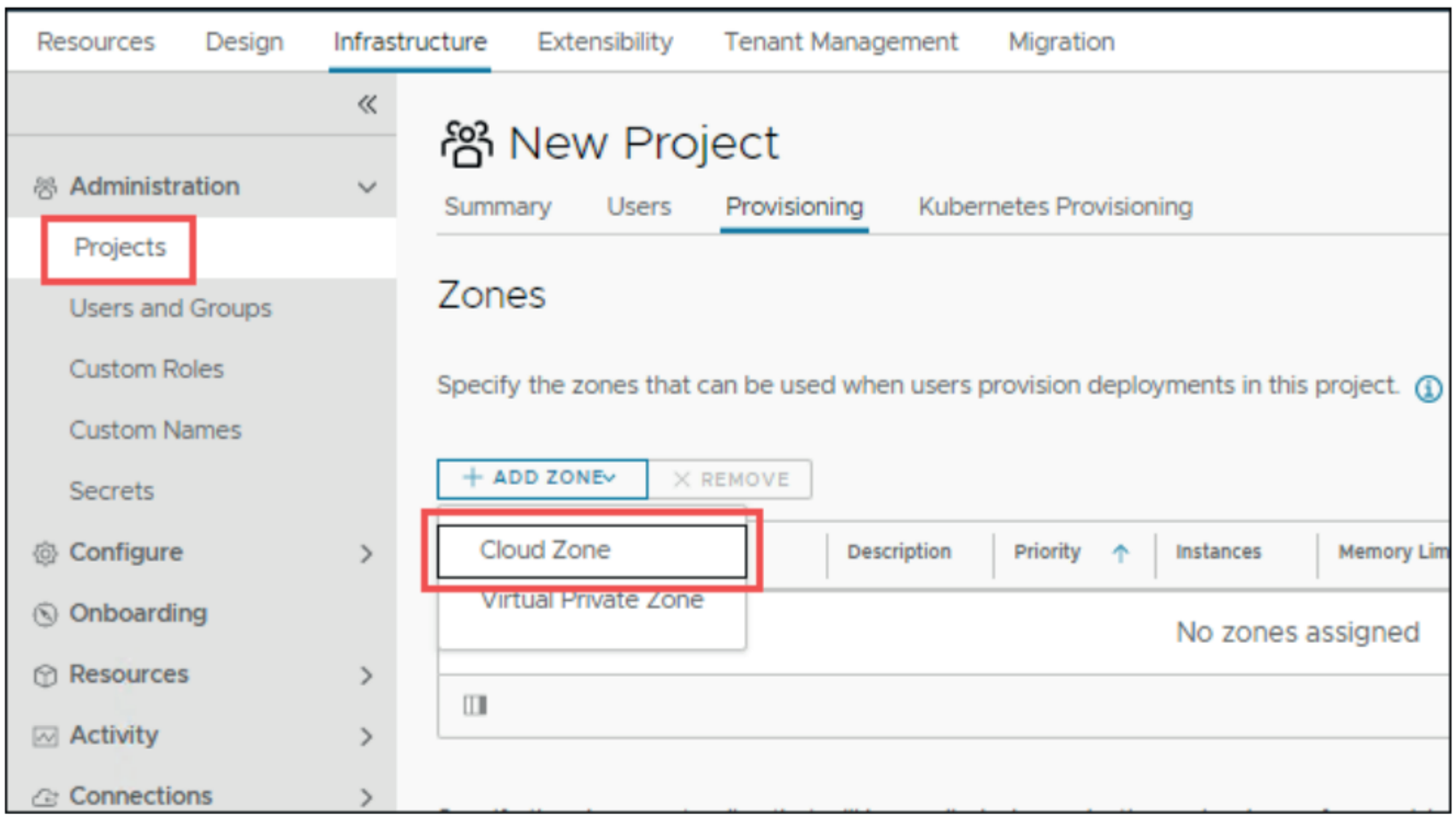


Users and groups are assigned different roles:

- Administrator: Can change the project configuration, add or remove users, and add or remove cloud zones
- Member: Can use the project services and deploy VMware Aria Automation Templates
- Viewer: Can only view VMware Aria Automation Templates and the deployments in this project but cannot deploy VMware Aria Automation Templates
- Supervisor: Can approve policies in Service Broker if a policy is defined with the project supervisor as an approver

5-14 Project: Adding Cloud Zones

On the **Provisioning** tab, add cloud zones to the project.



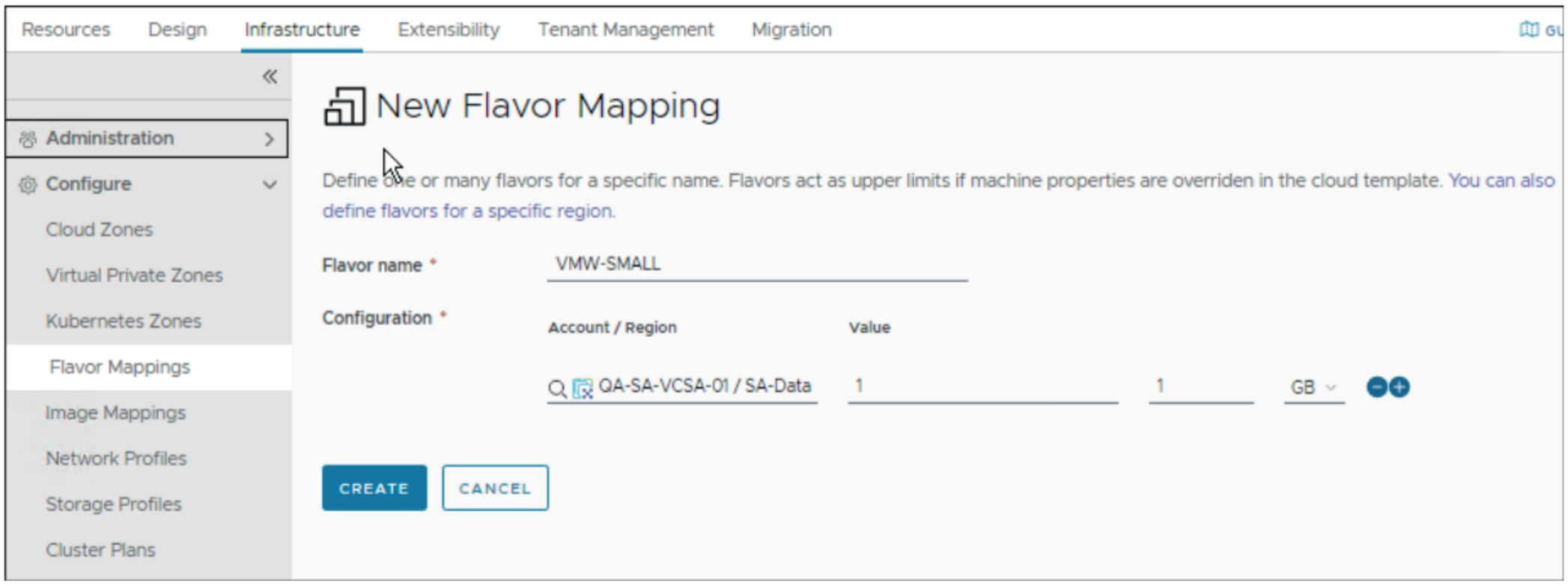


Each project must have at least one cloud zone for resources. You can connect multiple cloud zones to a project. The cloud zones can be of different types: vCenter, Google, Amazon Web Services (AWS), and others.

For each zone, you can set a zone priority and you can limit how many resources the project can use. The possible limits include the number of instances, the number of CPUs, and the amount of memory. For vSphere cloud zones only, you can configure storage limits. The default value of 0 gives you unlimited instances.

5-15 Creating Flavor Mappings

Flavor mappings define virtual machine size limits to create a combination of size configurations. To create a flavor mapping, select **Infrastructure** > **Configure** > **Flavor Mappings**.

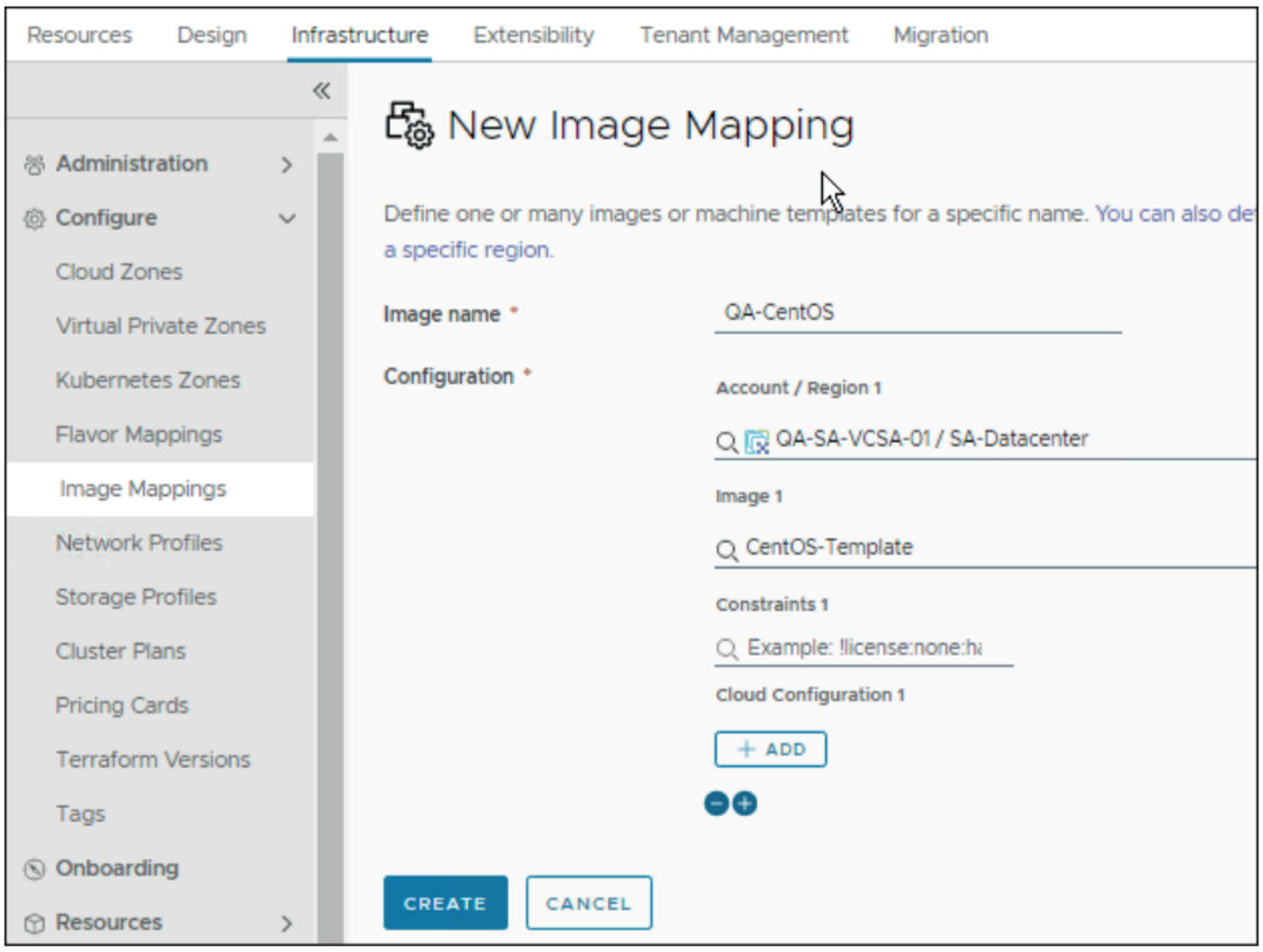


In a flavor mapping, you use natural language to define target deployment sizes for a specific cloud account.

Specify the cloud account that works with the flavor. Set your number of CPUs and the size of the memory. If you click the plus sign (+) icon at the end of the line, you can add multiple cloud accounts that work with the same size flavor.

5-16 Creating Image Mappings

In a vCenter system, the image mapping is a virtual machine template. To create an image mapping, select **Infrastructure** > **Configure** > **Image Mappings**.



In an image mapping, you use natural language to define target deployment images for a specific cloud account.

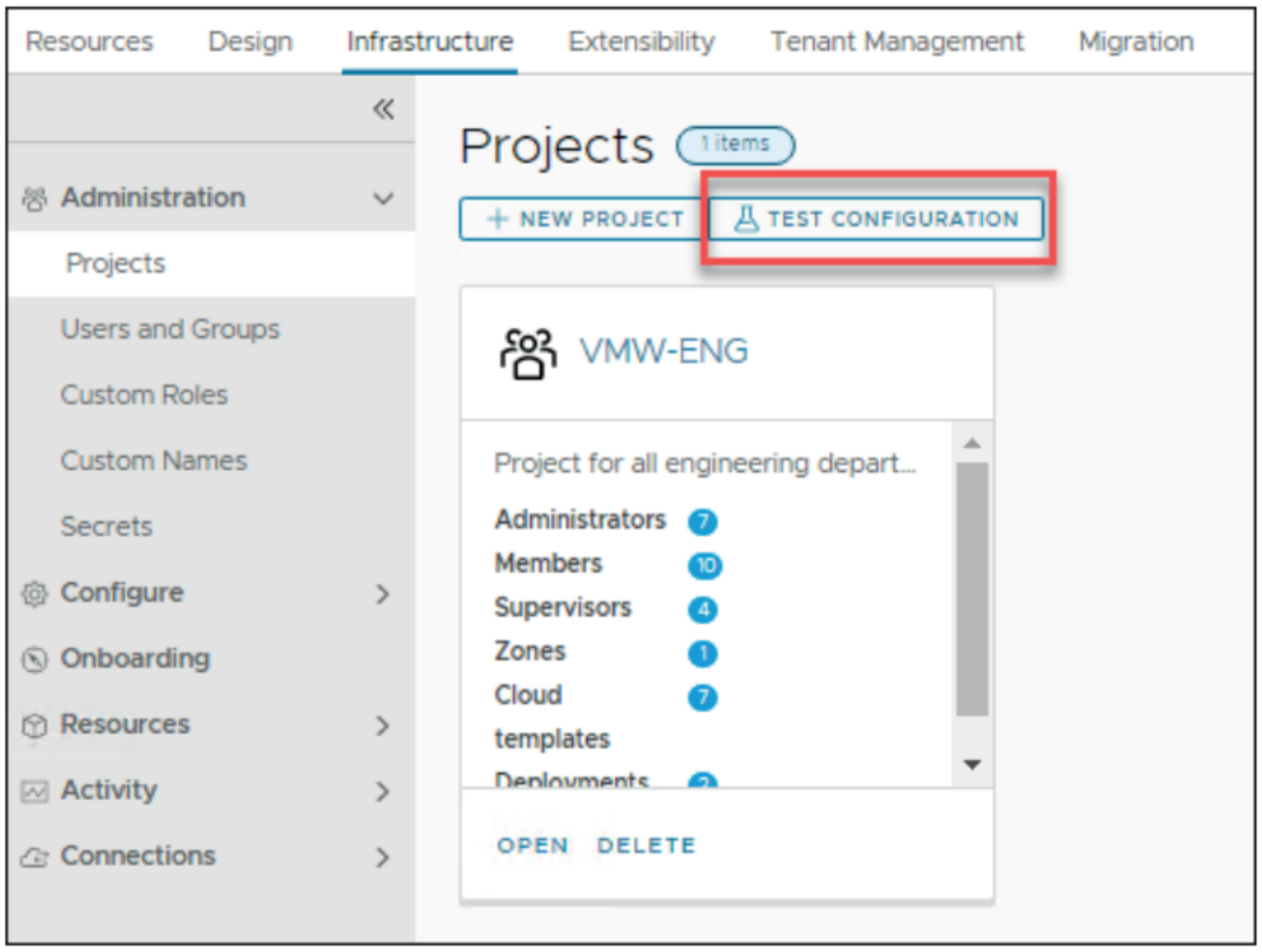
You can map images to any kind of template: predefined web server, predefined database servers, or predefined application system.

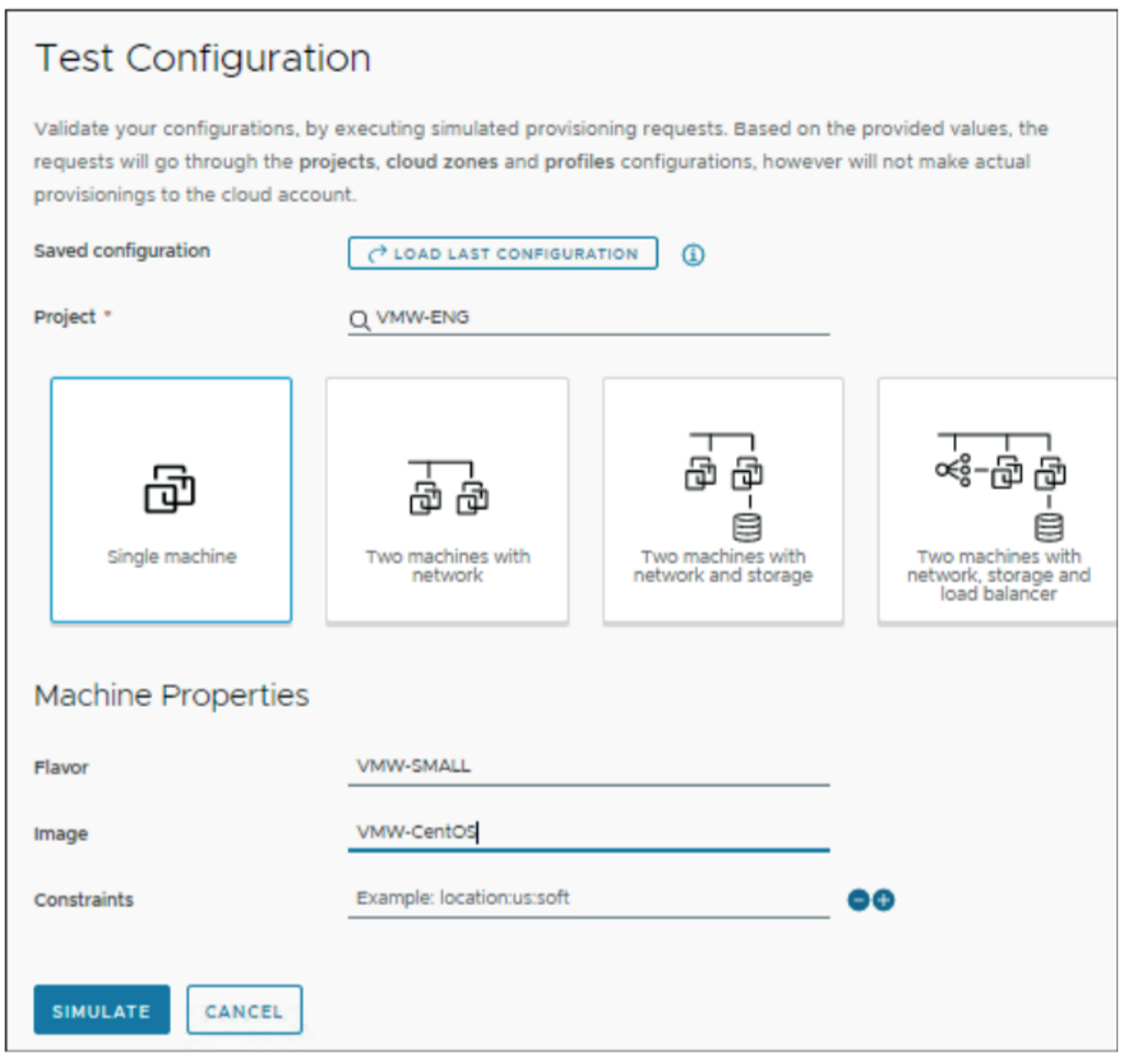
For a vCenter cloud account, the target deployment image is a virtual machine template.

You can map images from multiple cloud accounts to the same image mapping.

5-17 Testing the Configuration

Test the project with the cloud zones assigned to it by running a simulation. To test the configuration, select **Infrastructure** > **Administration** > **Projects** and click **TEST CONFIGURATION**.





The Test Configuration utility runs a simulation against your configuration. VMware Aria Automation Templates or virtual machines are not deployed. You can simulate simple and complex VMware Aria Automation Templates instances and use different flavors and images in your simulation.

You select the type of test that you want to run (**Single machine**, **Two machines with network**, and so on) and then click **SIMULATE**.

5-18 Lab 8: Creating a Basic Configuration

Create a basic VMware Aria Automation configuration:

1. Create a Cloud Account
2. Change a Cloud Zone Configuration
3. (Optional) Add Fin Groups
4. Create a Project
5. Create a Flavor Mapping
6. Create an Image Mapping

5-19 Review of Learner Objectives

- Create a vCenter cloud account
- Create cloud zones
- Create projects
- Create flavor mappings
- Create image mappings

5-20 Key Points

- The design guide allows for a basic rapid configuration of VMware Aria Automation.
- The following components are required for a basic configuration:
  - Cloud account
  - Cloud zone
  - Project
  - Flavor mapping
  - Image mapping

Questions?

Module 6

VMware Aria Automation Templates

6-2 Importance

VMware Aria Automation Templates are specifications that define virtual machines, applications, and services on cloud resources. You can use VMware Aria Automation to create a basic VMware Aria Automation template in minutes after VMware Aria Automation is configured.

Customization is the process of configuring a standard template referenced in an image mapping so that it is better suited to a specific purpose. This process can include running commands after deployment, creating, and editing configuration files, creating user accounts, and installing software.

cloud-init is an industry-standard configuration package that enables you to send configuration instructions to virtual machines as they are being deployed to customize the virtual machines. The VMware implementation of cloud-init is cloudConfig.

6-3 Module Lessons

1. Creating a Basic VMware Aria Automation Template
2. Cloud-Agnostic VMware Aria Automation Templates
3. Using cloudConfig and cloud-init
4. Advanced YAML

6-4 Lesson 1: Creating a Basic VMware Aria Automation Template

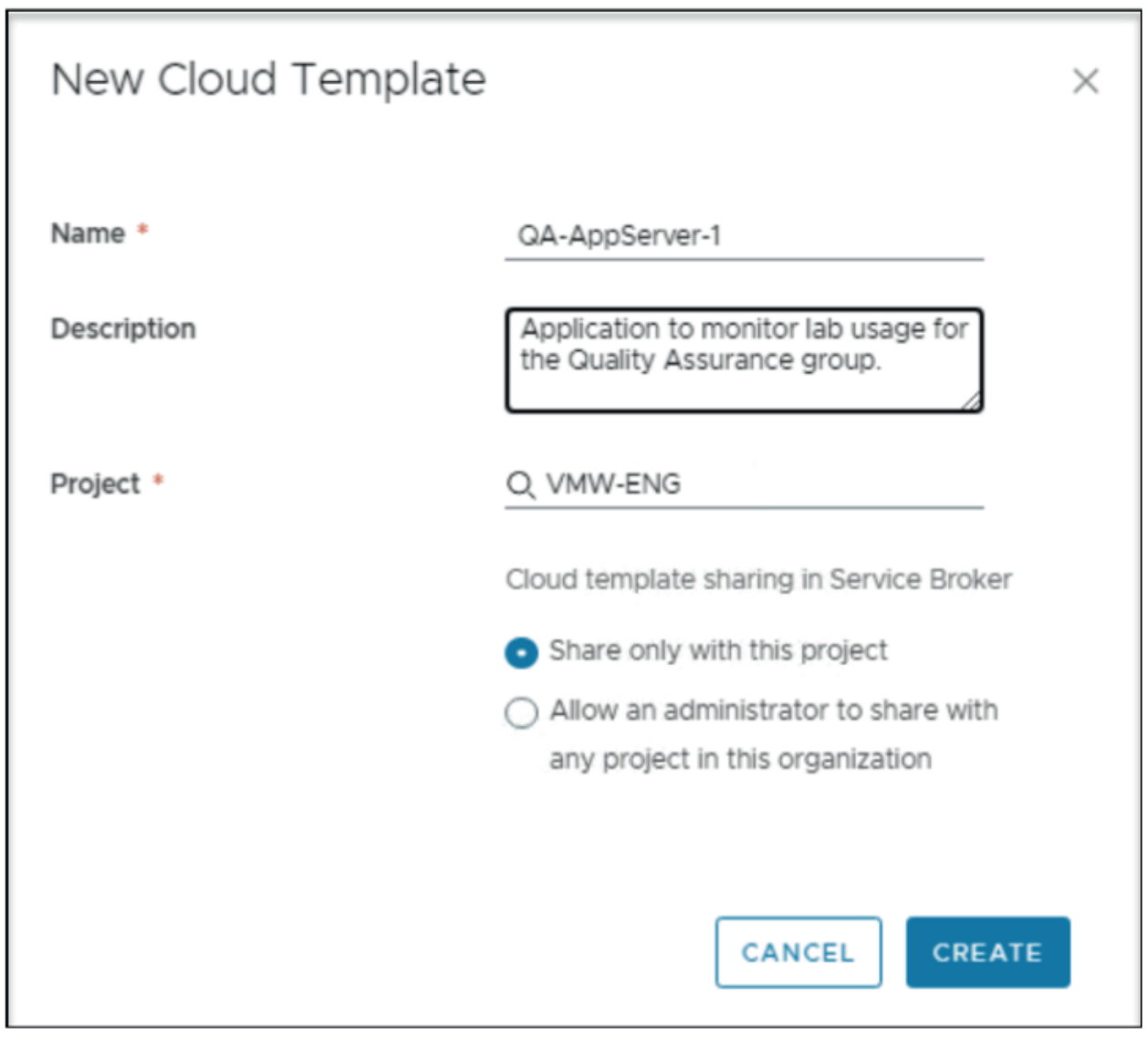
6-5 Learner Objectives

- Create a basic VMware Aria Automation template
- Perform a deployment from a VMware Aria Automation template
- Perform a deployment using the Create VM wizard

6-6 Creating a VMware Aria Automation Template

To create a VMware Aria Automation template:

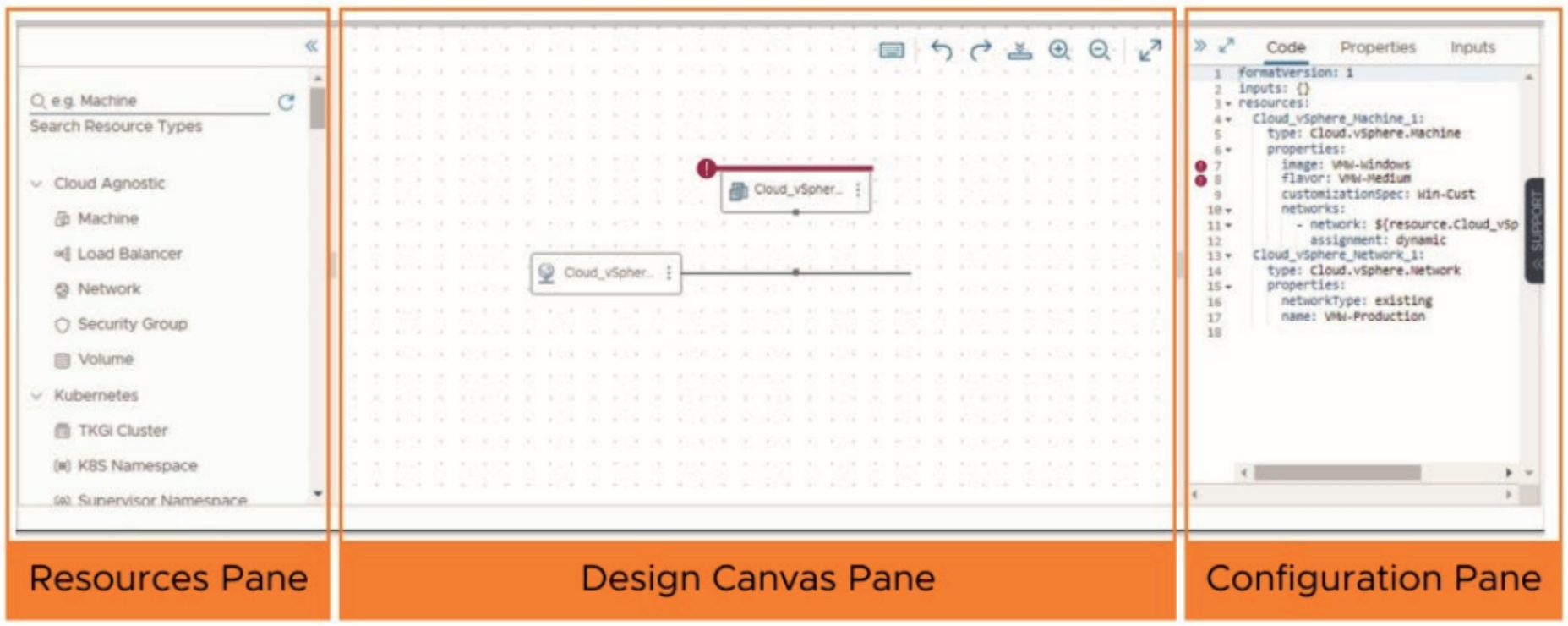
1. Click the **Design** tab.
2. Select **Cloud Templates** in the left navigation pane.
3. Click **NEW FROM**.
4. Select **Blank canvas**.
5. Enter a name and description for the VMware Aria Automation template.
6. Associate the VMware Aria Automation template with a project.
7. Select whether the VMware Aria Automation template is restricted to project members only.
8. Click **CREATE**.



When you create a VMware Aria Automation template, you must select a project and associate the VMware Aria Automation template with the project. A VMware Aria Automation template can be restricted to a single project's user or can be available to users in all projects.

6-7 VMware Aria Automation Template Designer

Use the VMware Aria Automation template designer to automate the deployment of machines and networks.



The VMware Aria Automation template designer can be used to create simple VMware Aria Automation templates such as the basic template in the screenshot. When a user requests a deployment from this VMware Aria Automation template, VMware Aria Automation deploys a single machine and connects it to a single network.

You can use the same VMware Aria Automation template designer to create VMware Aria Automation templates of increasing complexity. You can create VMware Aria Automation templates that deploy multiple machines, connect those machines to multiple networks, add disks to the machines, load balance the machines, and configure the machines.

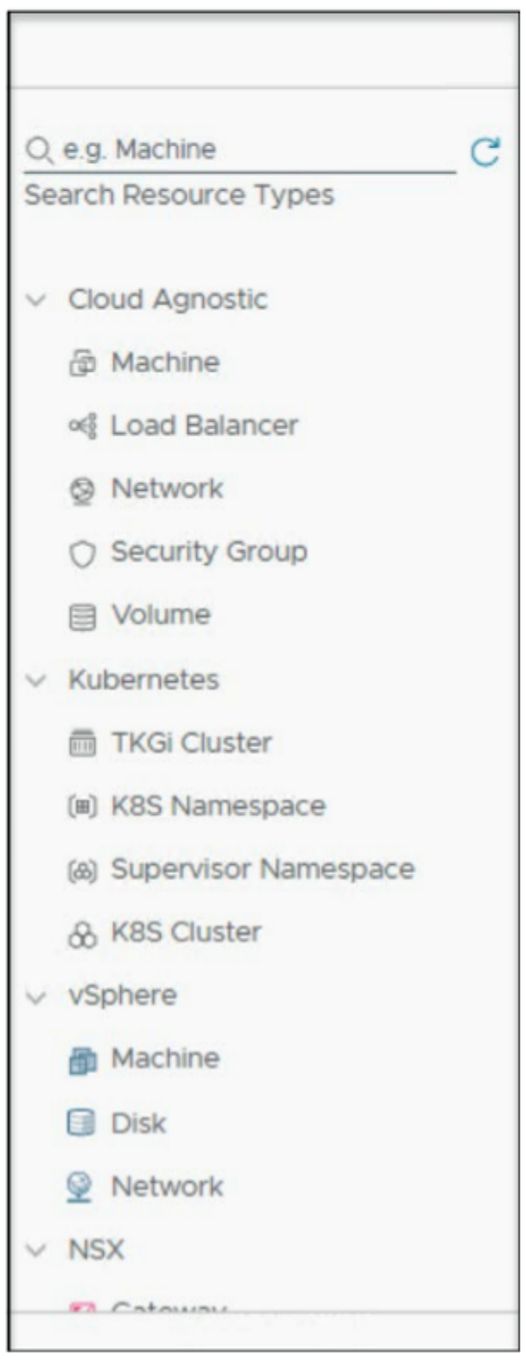
The configuration pane has three tabs that you can use to configure the components that you dragged to the design canvas. When you select a component in the design canvas, the **Code** tab highlights the YAML code that implements the functionality provided by the component and the **Properties** tab enables you to configure the settings of the component. You can define inputs on the **Inputs** tab, which enables the end user to control the configuration of the VMware Aria Automation template deployment.

6-8 Resources Pane

You can select components and drag them to the design canvas from the resources pane.

Resource types are available for the following cloud systems and technologies:

- Cloud-agnostic
- vSphere
- NSX
- Amazon Web Services (AWS)
- Configuration management
- Google Cloud Platform (GCP)
- Kubernetes
- Microsoft Azure
- Terraform

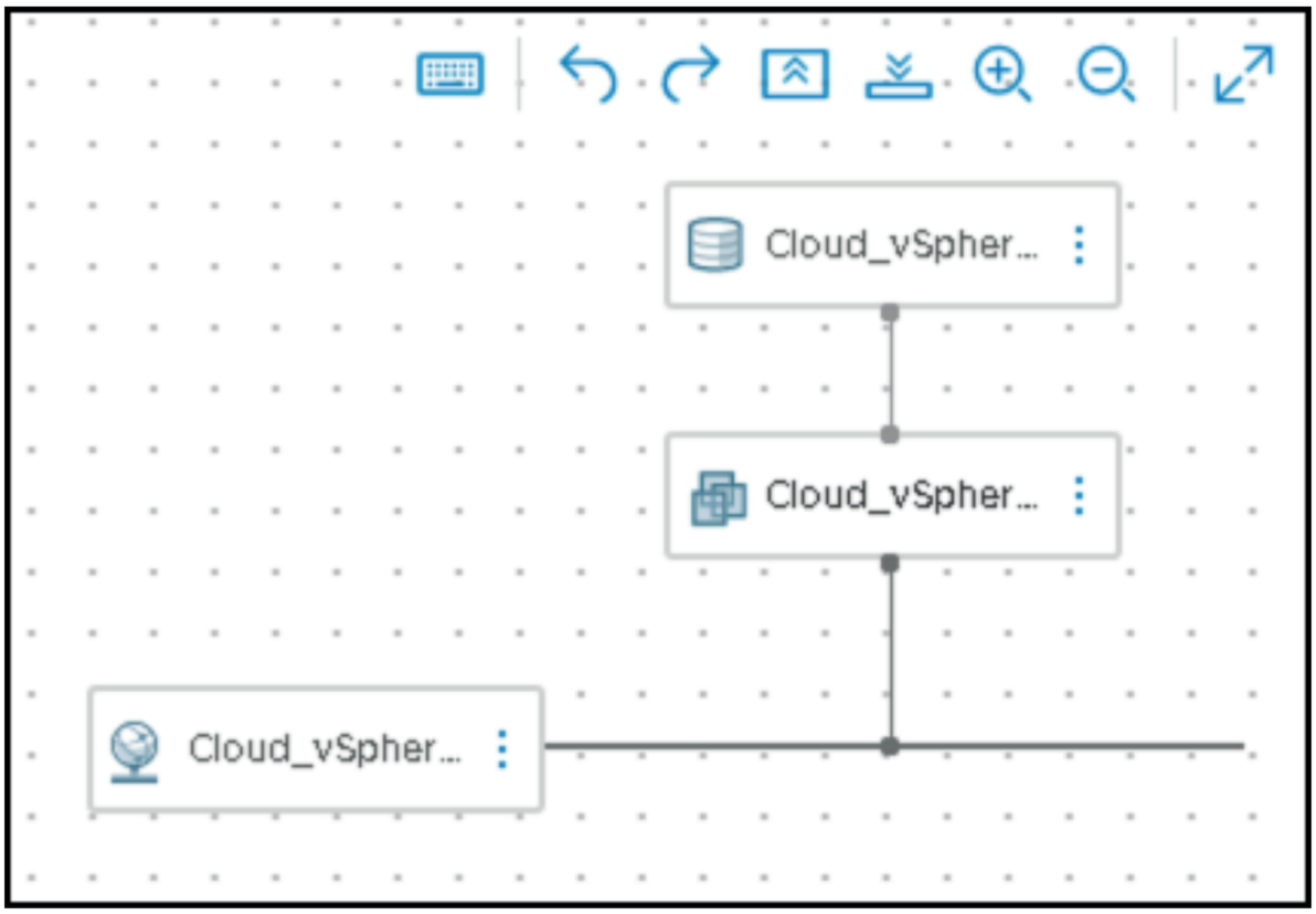


The resources pane includes components that you can drag to the VMware Aria Automation template. These components include machines, networks, NSX components, disks, and volumes. The resources pane includes cloud components for Amazon Web Services (AWS), Microsoft Azure, and Google Compute Platform (GCP). It also includes components for creating Kubernetes clusters, Kubernetes namespaces, and supervisor clusters. Additionally, the resources pane includes components for configuration management technologies such as Ansible, Ansible Tower, Puppet, and Terraform.

6-9 Design Canvas Pane

To assemble the basic components in the design canvas:

1. Select an item in the resources pane and drag it to the design canvas.
2. Connect items, such as virtual machines, networks, and storage.



The design canvas is where you drag components and connect those components to visually design your VMware Aria Automation template. Icons at the top of the design canvas provide useful functions such as delete, duplicate, zoom, undo, redo, and so on. As you drag components to the design canvas, VMware Aria Automation automatically writes the YAML code, which appears in the Configuration pane.

You can connect certain components on the design canvas, such as machines and networks. To connect two components:

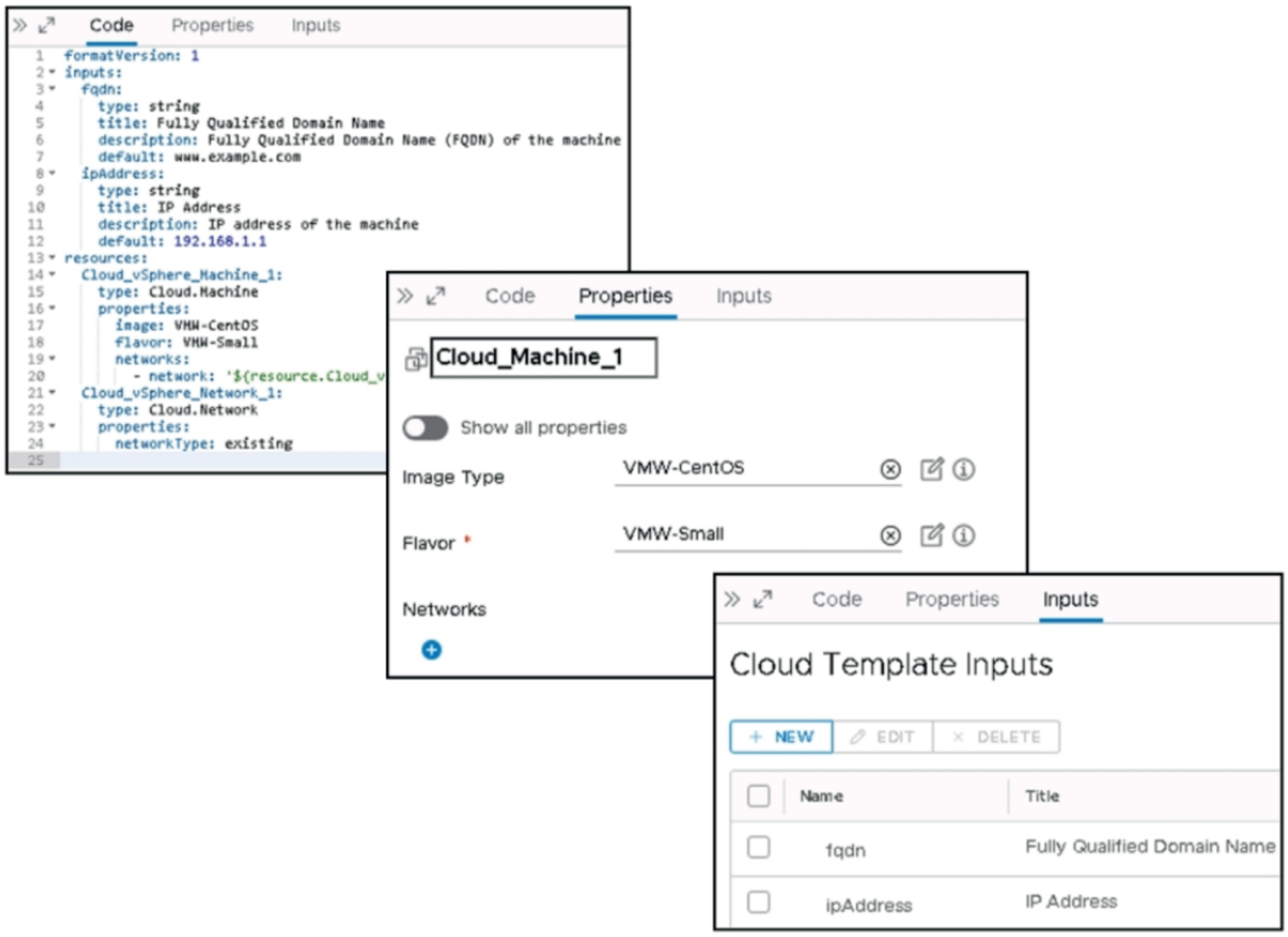
1. Click a component.

   A circle appears on the left of the component graphic.

2. Point to the circle and drag the pointer to the component that you want to connect to.

6-10 Configuration Pane

The configuration pane has three tabs that enable the configuration of components that you drag to the design canvas.

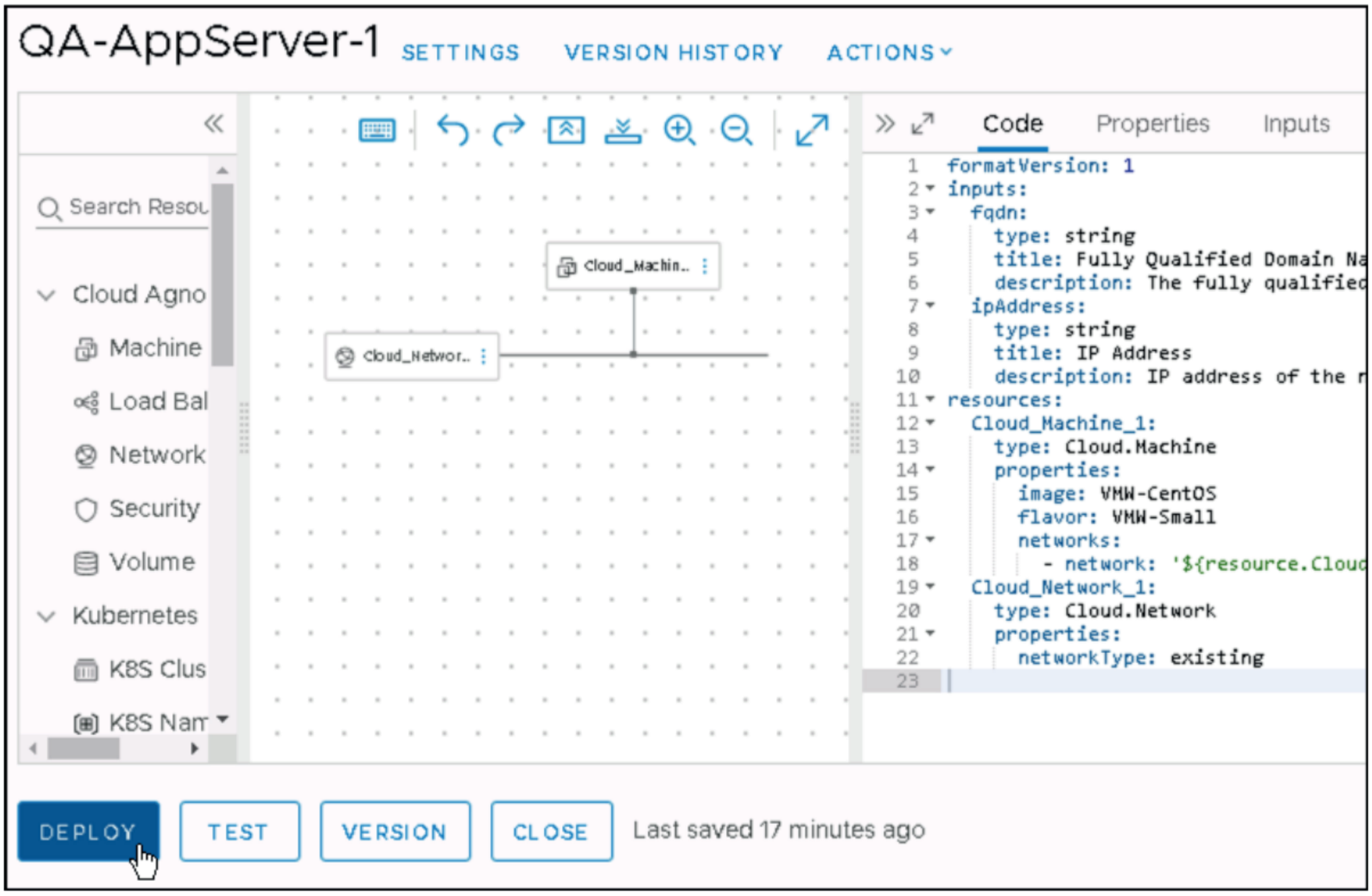


When you select a component in the design canvas, the YAML code that implements the functionality provided by the component is highlighted on the **Code** tab. You configure the settings of the component on the **Properties** tab. On the **Inputs** tab, you can define inputs that enable you to prompt the end user to control aspects of how the VMware Aria Automation template deployment is configured.

The code editor allows you to type, cut, copy, and paste code directly. The code editor supports syntax completion and error checking features.

6-11 Testing and Deploying the VMware Aria Automation Template

Click **TEST** to test the VMware Aria Automation template. Click **DEPLOY** to deploy the VMware Aria Automation template.



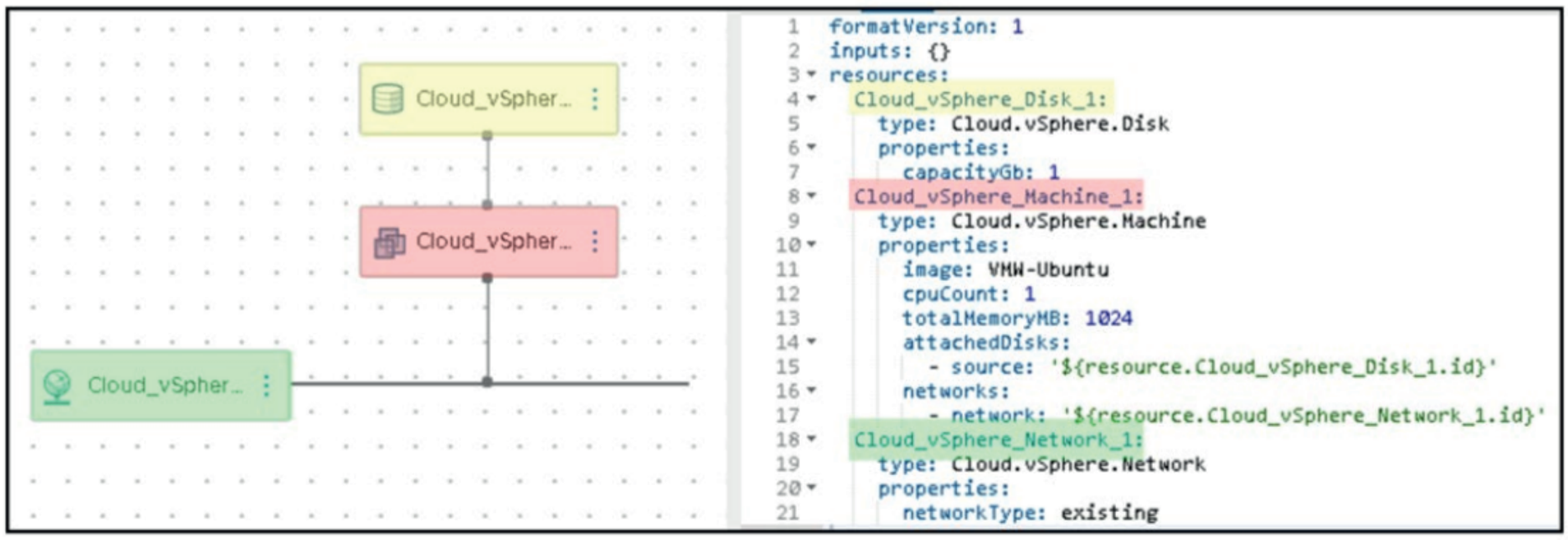
Before performing a deployment from a VMware Aria Automation template, you can click **TEST** to confirm that the YAML code is syntactically valid, and meets the constraints specified with tags.

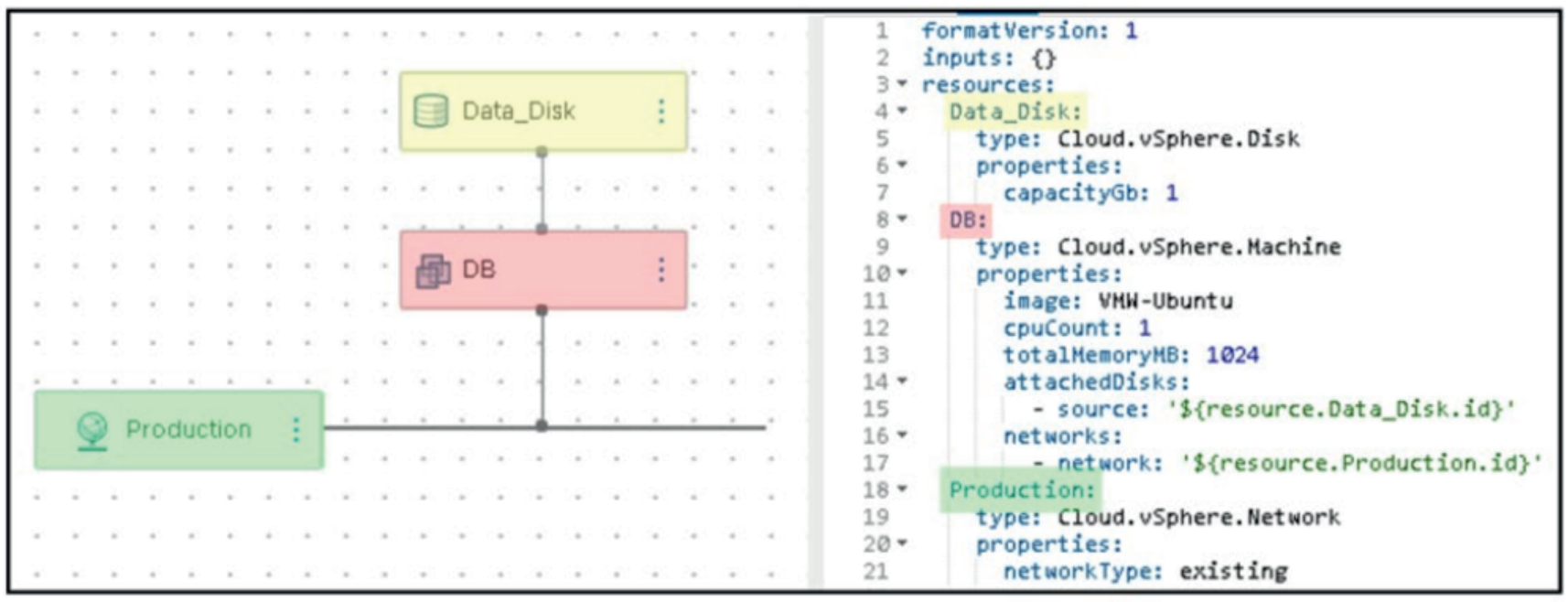
To perform a deployment from a VMware Aria Automation template in the VMware Aria Automation template designer, click **DEPLOY**.

Alternatively, you can click **CLOSE** to return to the **Design** > **Cloud Templates** page, select a VMware Aria Automation template, and click **DEPLOY**.

6-12 Renaming Resources

You can rename resources in the VMware Aria Automation template.



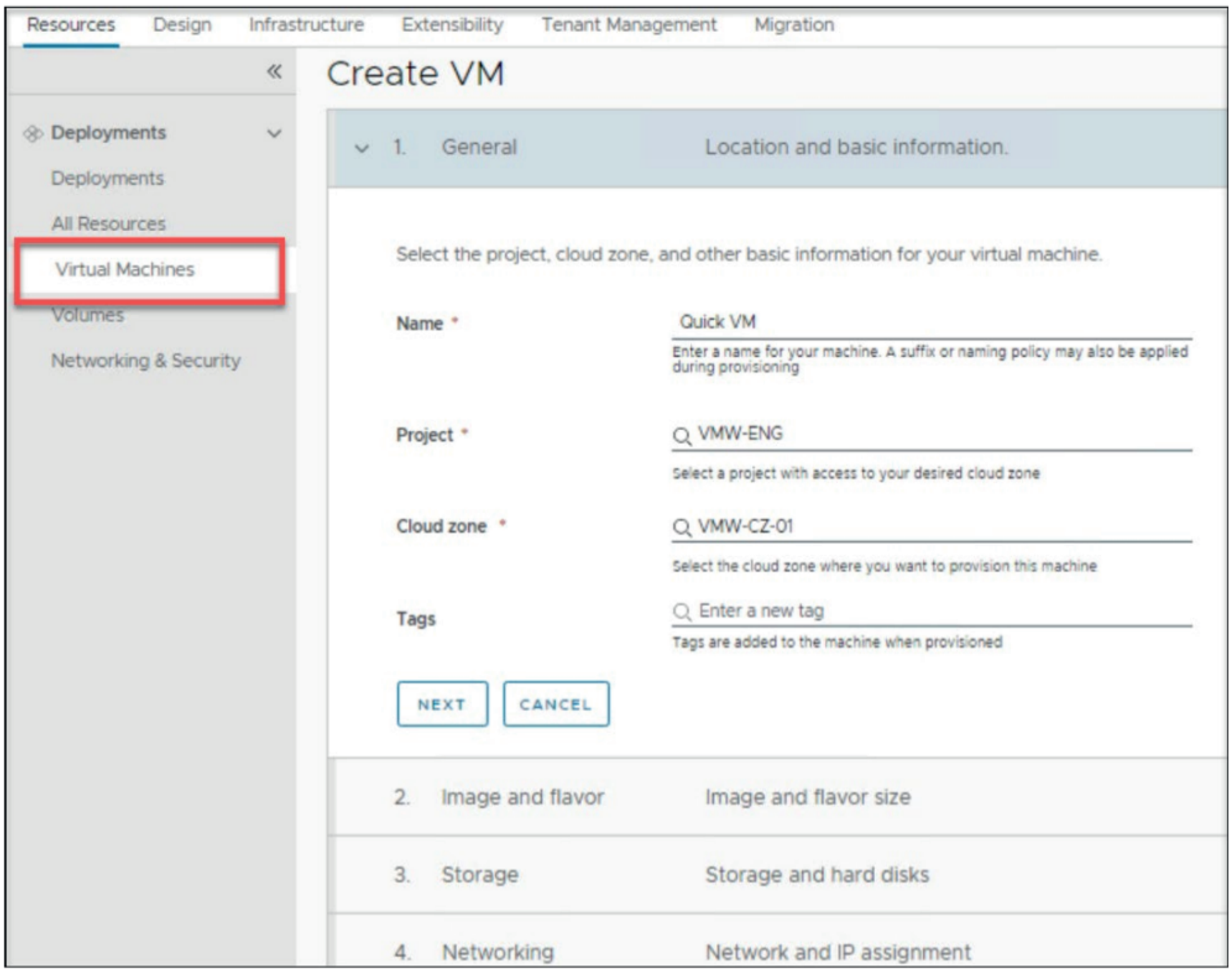


6-13 Creating VMs

To deploy a basic VM independent of the VMware Aria Automation template:

1. Select **Resources** > **Virtual Machines**.
2. Click **NEW VM**.
3. Enter the VM name.
4. Associate the VM to a project and a cloud zone.
5. Click **NEXT**.
6. Select the VM image.

   You can select a local image or provide a URL to a target image.
7. Specify a flavor mapping for your machine.
8. Click **CREATE**.



Deploy a virtual machine independent of the VMware Aria Automation template using the **NEW VM** option available on the **Resources** > **Virtual Machines** page. The wizard guides you through the available tasks to create a virtual machine. The first two tasks are mandatory to create a virtual machine. The storage and networking tasks are optional. In the Storage section, you can add and configure a new storage device. The option to add an existing storage device to the virtual machine is also supported. In the Networking section, the option to add and configure a virtual machine network adapter is supported.

6-14 Lab 9: Creating a Basic VMware Aria Automation Template

Create and deploy a basic VMware Aria Automation template:

1. Create a VMware Aria Automation Template
2. Specify an Image in Your VMware Aria Automation Template
3. Specify a Flavor in Your VMware Aria Automation Template
4. Specify a vSphere Folder in Your VMware Aria Automation Template
5. Add a vSphere Customization Specification to Your VMware Aria Automation Template
6. Add a Network to Your VMware Aria Automation Template
7. Specify a Static IP Address for Your Virtual Machine
8. Test Your VMware Aria Automation Template
9. Deploy Your VMware Aria Automation Template
10. Examine Your Deployment
11. Delete Your Deployment to Save Lab Resources

6-15 Lab 10: Creating a Virtual Machine

Use the Create VM wizard to create and deploy a virtual machine:

1. Specify a Project and Cloud Zone for Your Virtual Machine
2. Specify Your Virtual Machine Image and Flavor
3. Add New Storage to Your Virtual Machine
4. Add a Network to Your Virtual Machine and Specify a Static IP Address
5. Deploy Your Virtual Machine
6. Examine Your Deployment
7. Delete Your Deployment to Save Lab Resources

6-16 Review of Learner Objectives

- Create a basic VMware Aria Automation template
- Perform a deployment from a VMware Aria Automation template
- Perform a deployment using the Create VM wizard

6-17 Lesson 2: Cloud-Agnostic VMware Aria Automation Templates

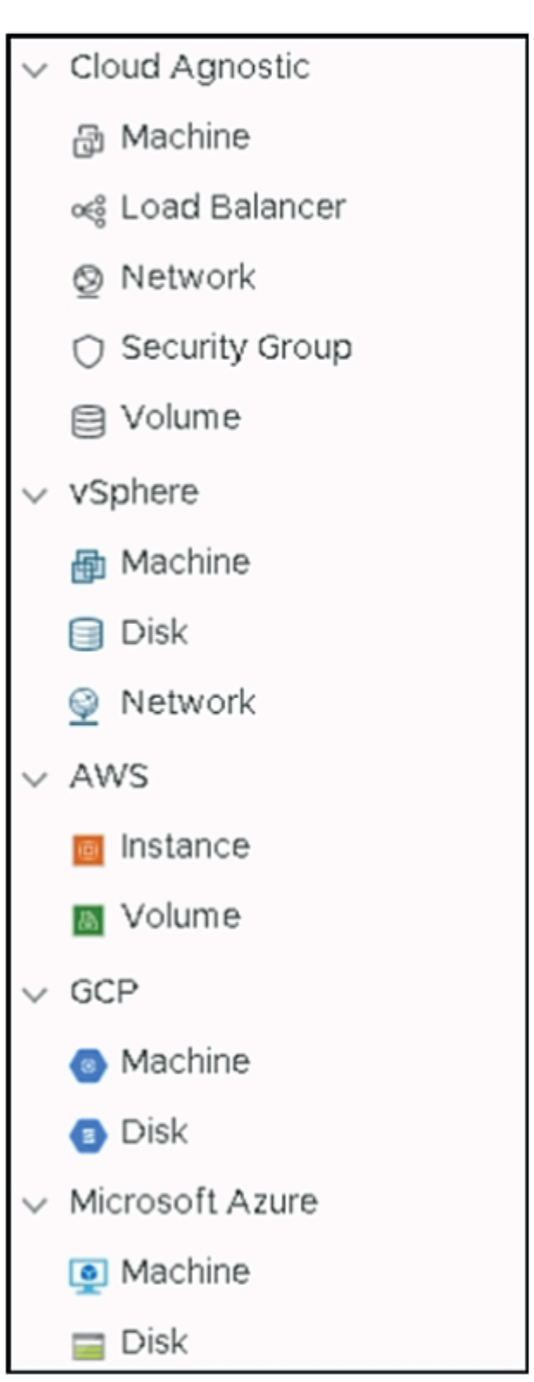
6-18 Learner Objectives

- Explain the difference between cloud-agnostic and platform-specific resources
- Configure VMware Aria Automation to allow cloud-agnostic VMware Aria Automation templates

6-19 Cloud-Agnostic Versus Platform-Specific Resources

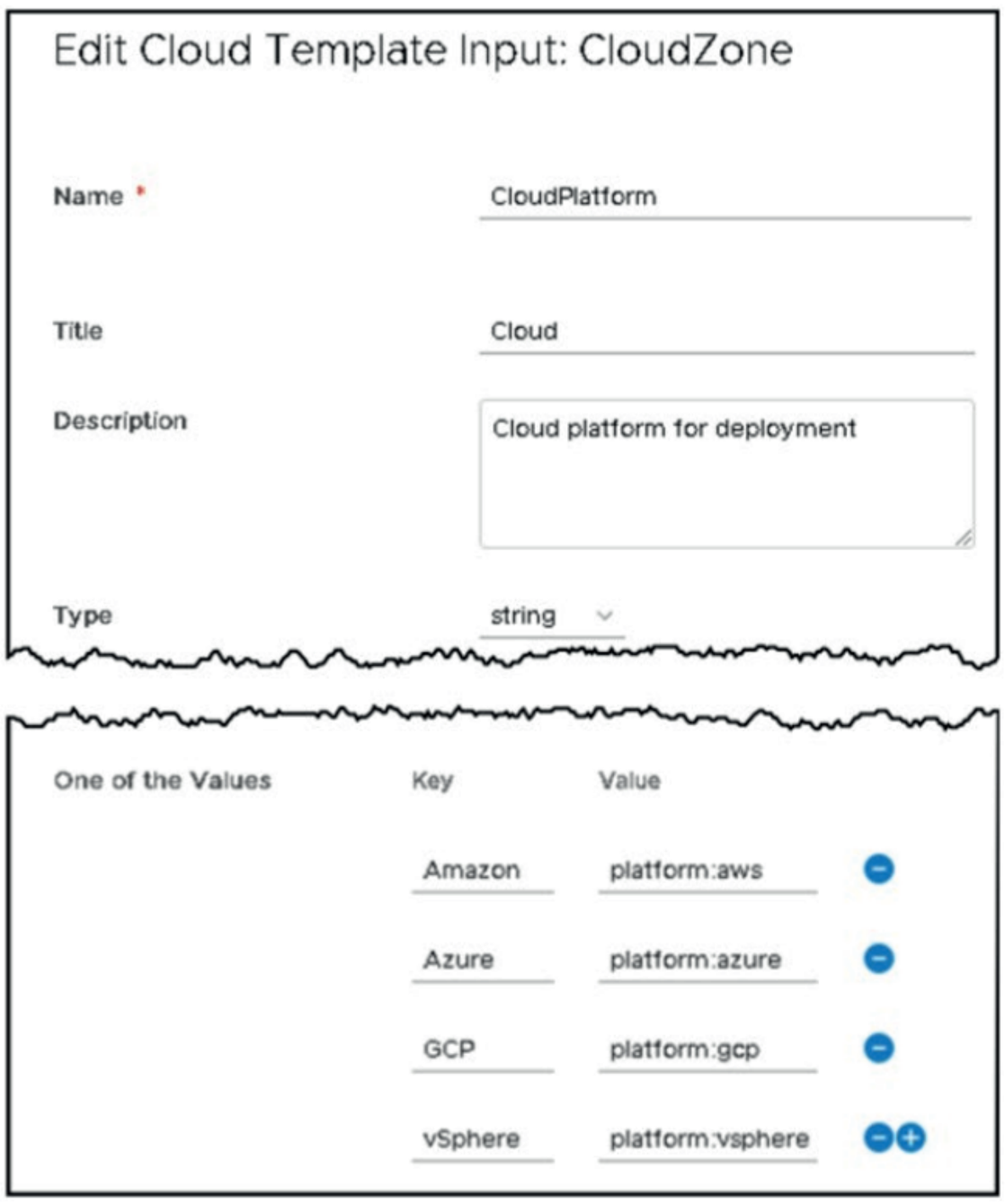
As the names suggest, resources such as **vSphere** > **Machine**, **AWS** > **Volume**, **Azure** > **Machine**, and **GCP** > **Disk** instruct VMware Aria Automation to create resources on specific compute platforms.

The cloud-agnostic counterparts instruct VMware Aria Automation to create resources. You can select the compute platform during deployment rather than hard coding the decision to the VMware Aria Automation template.



6-20 Giving End Users Choice with Inputs

Inputs are optional but useful when you create cloud-agnostic VMware Aria Automation templates because they enable the end user to select the target platform.

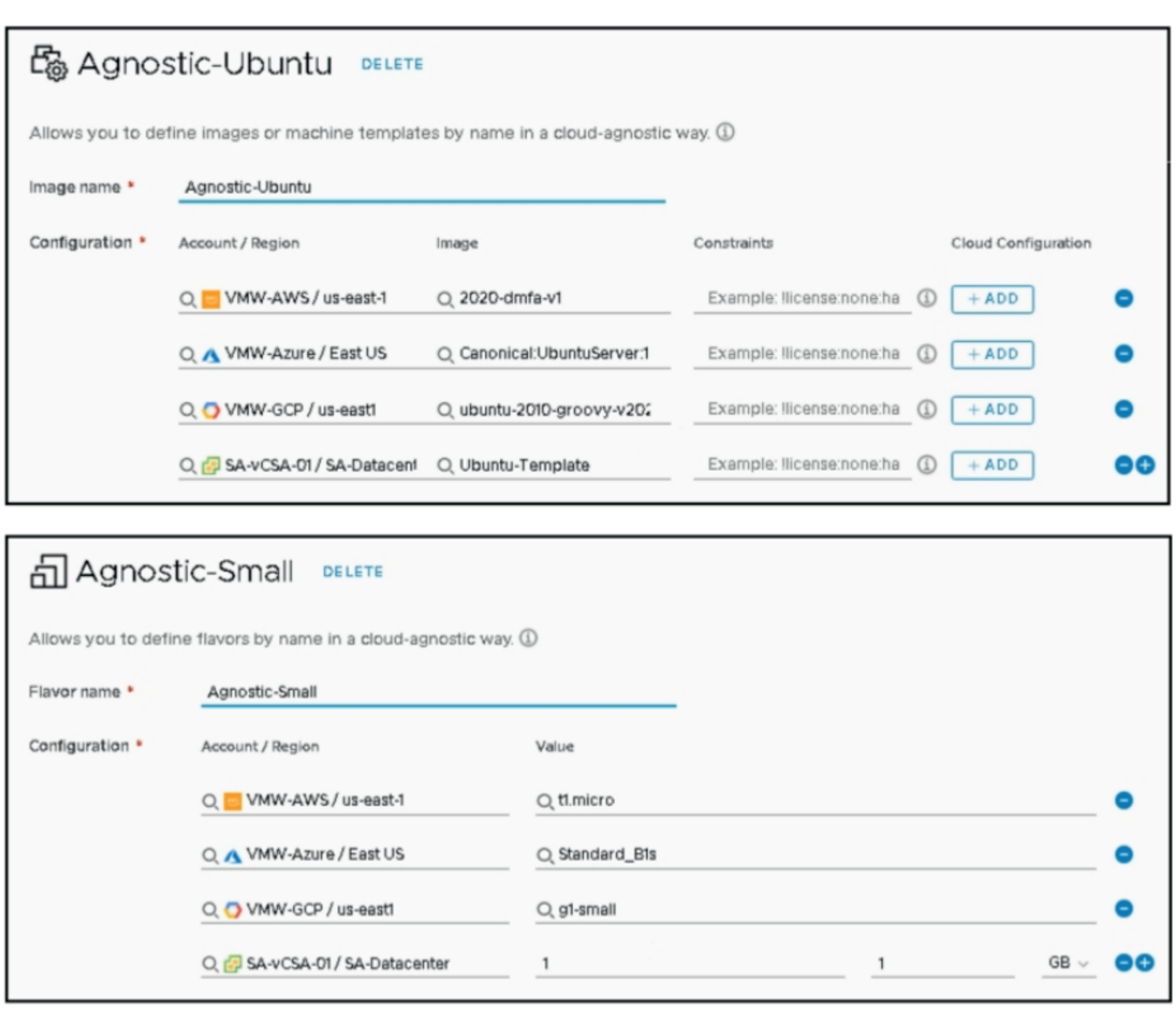



```
inputs:
  Hostname:
    type: string
    title: Hostname
  IpAddress:
    type: string
    title: IP Address
  CloudPlatform:
    type: string
    description: Cloud platform for deployment
    title: Cloud
    oneOf:
      - title: Amazon
        const: 'platform:aws'
      - title: Azure
        const: 'platform:azure'
      - title: GCP
        const: 'platform:gcp'
      - title: vSphere
        const: 'platform:vsphere'
```

6-21 Required Configuration

To use cloud-agnostic resources in a VMware Aria Automation template, configure the following features for each cloud platform:

- Cloud accounts
- Cloud zones
- Flavor mappings
- Image mappings
- Capability tags



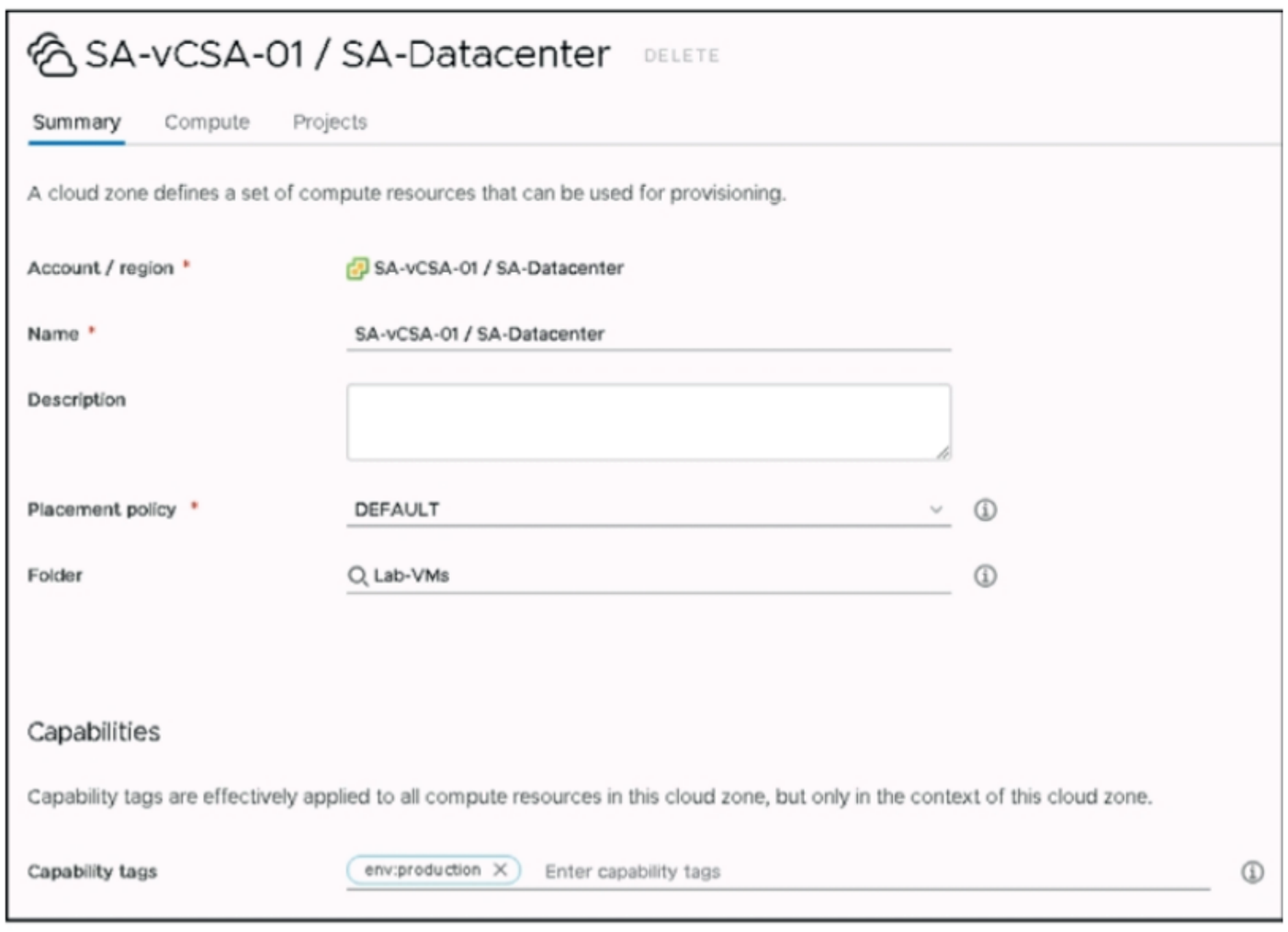
6-22 Capability Tags and Constraint Tags

You can set capability tags on resources such as:

- Cloud accounts
- Cloud zones
- Kubernetes zones
- Network profiles and networks
- Storage profiles and storage
- Compute

You can set constraint tags on:

- VMware Aria Automation Templates
- Image mappings
- Projects





Administrators apply capability tags to resources such as cloud accounts, cloud zones, and network profiles, so that VMware Aria Automation template designers can target the resources that they need to deploy to. VMware Aria Automation template designers apply constraint tags to resources such as machines, networks, disks, and volumes.

For example, in the screenshots, the administrator applied the env:production capability tag, to a cloud zone. In the VMware Aria Automation template, the designer applied the env:production constraint tag to a machine. These tags instruct VMware Aria Automation that the deployment of this machine is constrained to cloud zones that have the matching capability tag.

6-23 Resource Grouping

Administrator can create and use capability tags and constraint tags to tag cloud accounts, cloud zones, Kubernetes zones, network profiles, storage profiles, machines, or networks.

Tagging extensively is not needed due to grouping in VMware Aria Automation deployments.

Grouping relies on links in VMware Aria Automation templates:

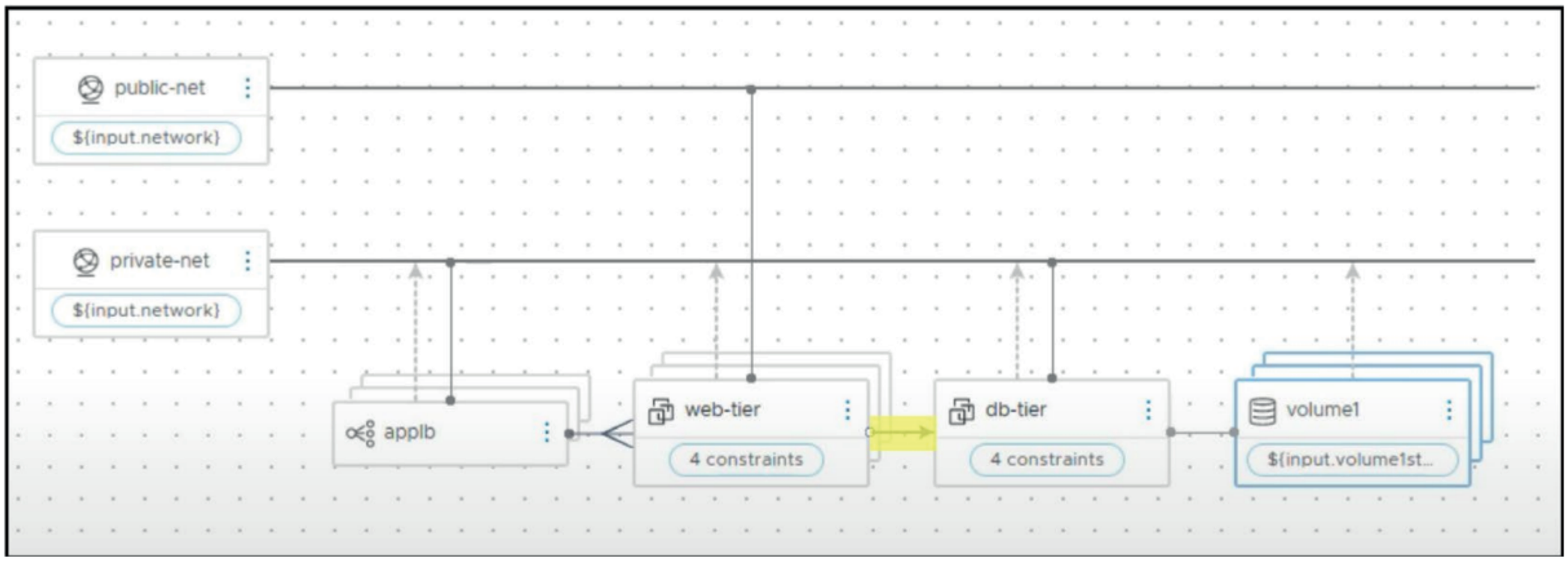
- Explicit links
- Implicit links
- Hard links

For a detailed explanation of links and grouping, see Zero2Hero: Constraint Tags & Placement (Cloud Assembly) at https://www.youtube.com/watch?v=4zNQ33RyQio.

6-24 Explicit Links

Explicit links indicate when one machine depends on another machine.

Explicit links are indicated by a solid arrow. Explicit links indicate dependencies between machines.



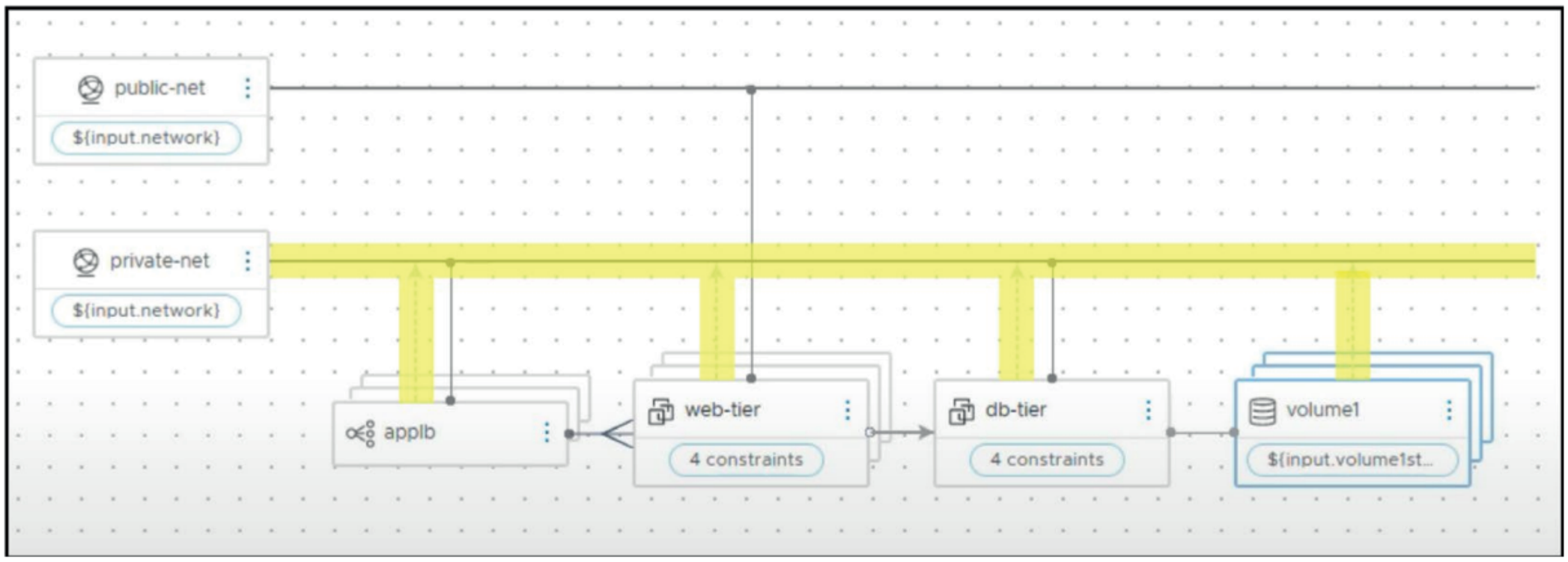
In the example, the arrow indicates that db-tier must be deployed before web-tier can be deployed. The web-tier VM depends on the db-tier VM.

At the deployment time, an explicit dependency sets the build order. To add an explicit dependency, use the design canvas or use the `dependsOn` property in the code editor.

6-25 Implicit Links

Implicit links are created when the YAML code for one resource refers to another resource.

Implicit links are indicated by a dashed arrow.

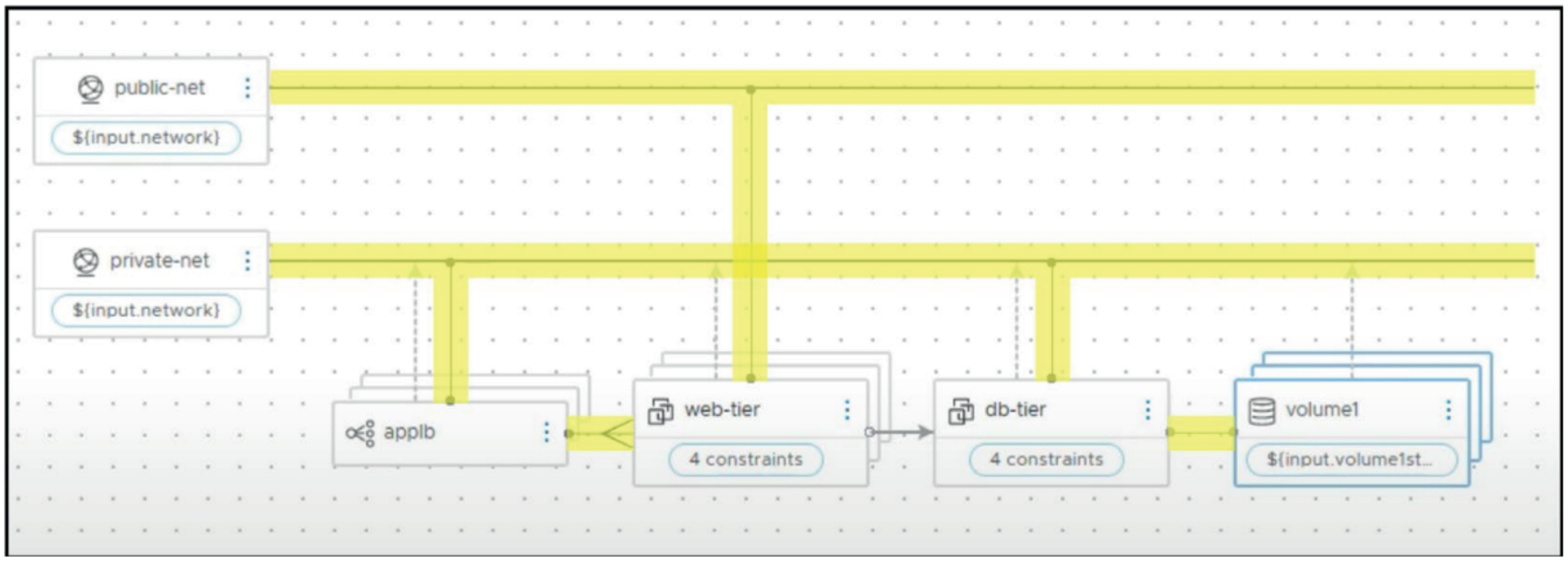


Implicit links are created when somewhere in an object you reference information from another object. For example, volume1 in the screenshot has an implicit link to private-net. The YAML code for volume1 contains a line that begins with `resourceGroupName: '${resource["private-net"]....`

6-26 Hard Links

Hard links indicate connections between resources. Grouping is performed only based on the hard links.

Hard links are indicated by a solid line. Examples of hard links include solid lines connecting machines to networks, solid lines connecting machines to volumes, and solid lines indicating load-balanced connections.

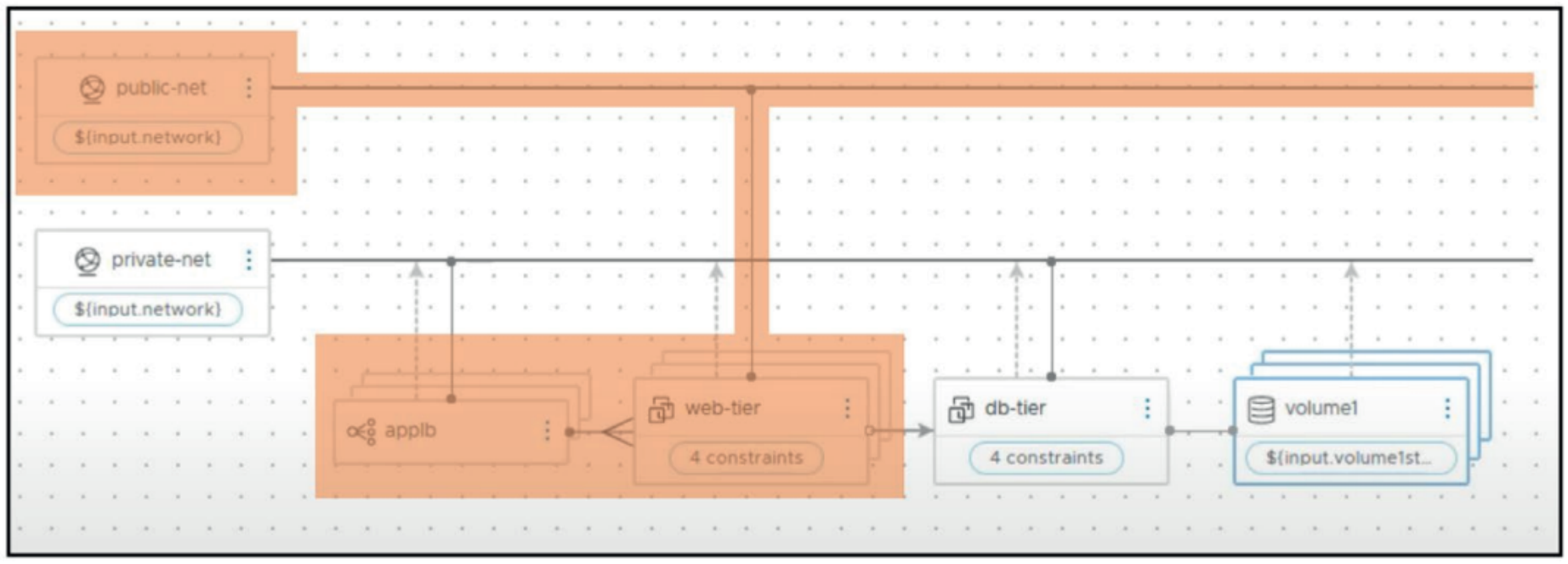


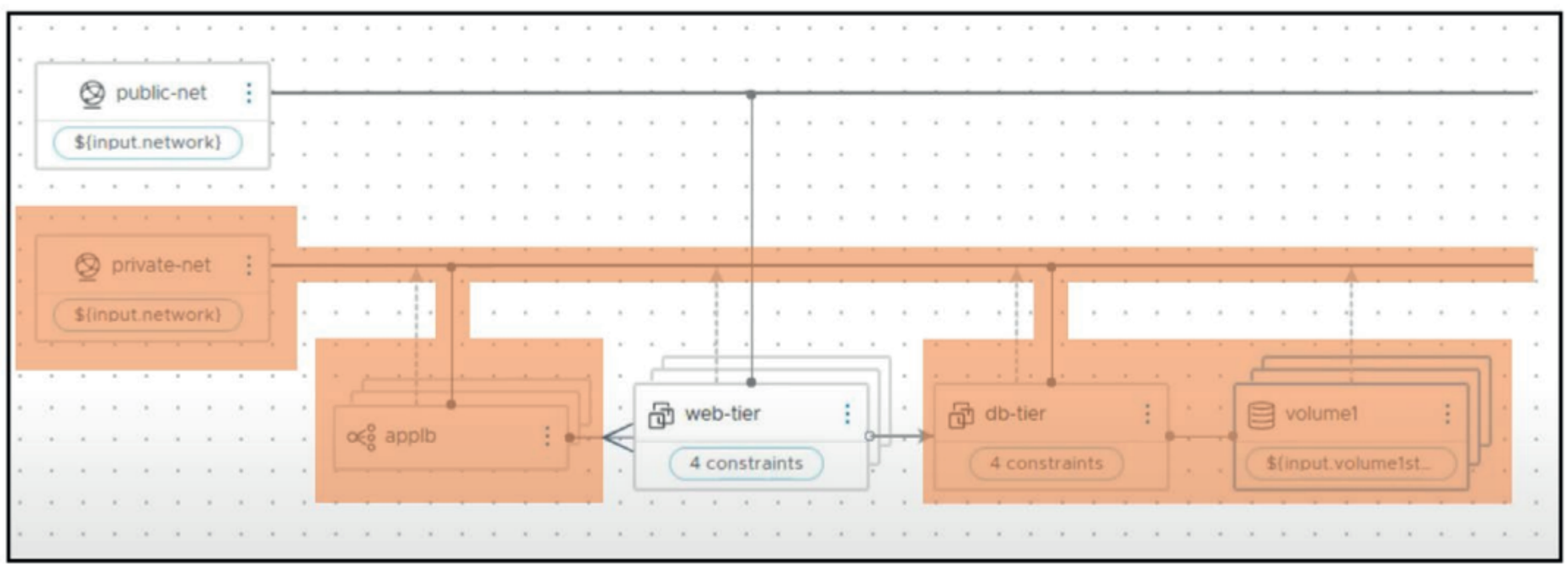
Grouping is performed only based on the hard links. Explicit links and implicit links are not considered during the grouping process.

In the example, a hard link exists between web-tier and public-net. Consequently, VMware Aria Automation determines that these two resources belong to the same resource group. Thus, VMware Aria Automation knows to deploy the web-tier machine and the public-net network on the same cloud platform.

6-27 Resource Grouping Example

Because of the implications of resource grouping, you can reduce the number of resources that must be tagged in VMware Aria Automation to create cloud-agnostic VMware Aria Automation templates.





VMware Aria Automation knows how to deploy all resources from a resource on the same platform.

Because of the implications of resource grouping, you can reduce the number of resources that must be tagged in VMware Aria Automation to create cloud-agnostic VMware Aria Automation templates.

6-28 Lab 11: (Simulation) Creating Cloud-Agnostic VMware Aria Automation Templates

Create a cloud-agnostic VMware Aria Automation template that enables the end user to deploy machines to different public cloud platforms:

1. Create a Cloud-Agnostic VMware Aria Automation Template
2. Deploy a Machine to vSphere
3. Deploy a Machine to Google GCP
4. Deploy a Machine to Microsoft Azure
5. Deploy a Machine to Amazon AWS
6. Examine the Tagging Configuration
7. Examine the Cloud Accounts
8. Examine the Cloud Zones
9. Examine the Flavor Mappings
10. Examine the Image Mappings
11. Examine the Network Profiles

6-29 Review of Learner Objectives

- Explain the difference between cloud-agnostic and platform-specific resources
- Configure VMware Aria Automation to allow cloud-agnostic VMware Aria Automation templates

6-30 Lesson 3: Using cloudConfig and cloud-init

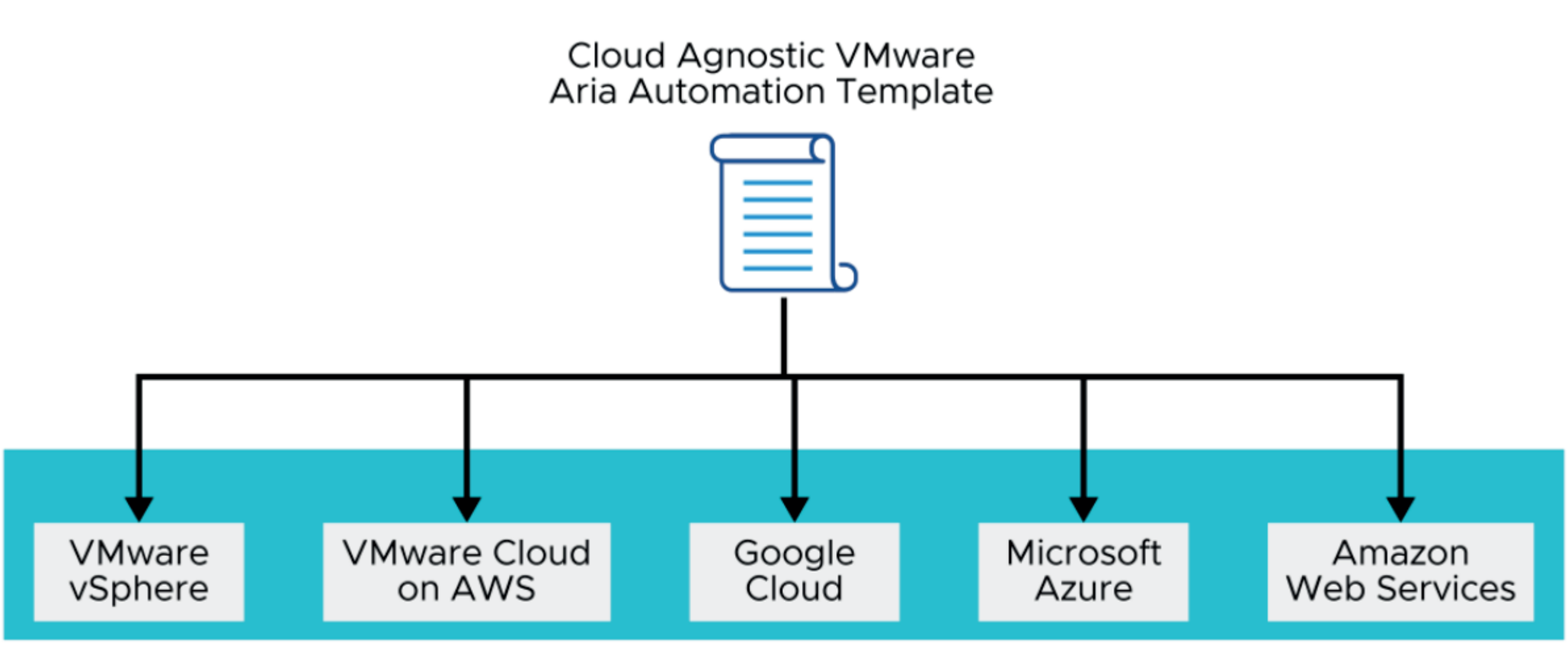
6-31 Learner Objectives

- Describe cloudConfig and cloud-init
- Create a vSphere virtual machine template that supports cloud-init
- Customize a host name in a virtual machine after deployment by using cloudConfig
- Create users in a virtual machine after deployment by using cloudConfig
- Run commands in a virtual machine after deployment by using cloudConfig
- Install software packages in a virtual machine after deployment by using cloudConfig
- Customize a host name in a virtual machine after deployment by using cloudbase-init
- Run commands in a virtual machine after deployment by using cloudbase-init

6-32 Use Case: Customizing VMware Aria Automation Templates for Deployment on Any Cloud

cloudConfig and cloud-init allow you to customize a single VMware Aria Automation template so that it can be deployed and run on any cloud:

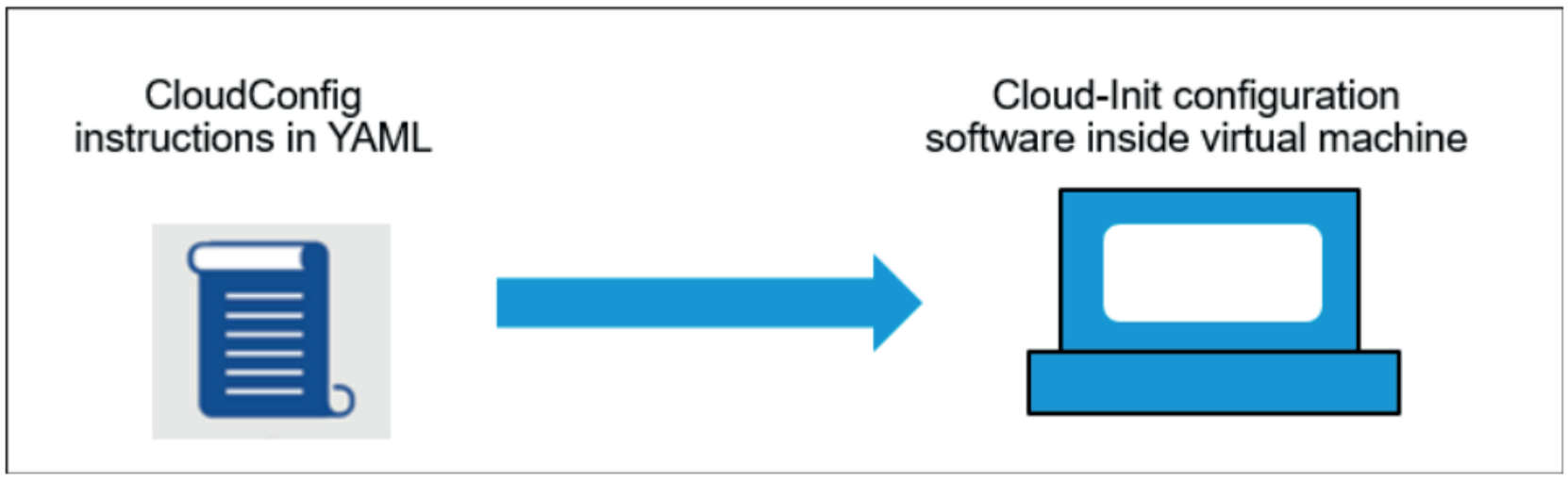
- Several commands work on all the supported operating systems.
- Combine YAML with cloudConfig to customize a single VMware Aria Automation template allowing different commands to run on different cloud deployments.



6-33 About cloudConfig and cloud-init

cloudConfig sends instructions to cloud-init:

- cloud-init is an industry-standard software package that allows customization.
- cloudConfig is the VMware Aria Automation template YAML code that sends instructions to cloud-init.



cloud-init is a set of Python scripts that initialize cloud instances of Linux machines. The cloud-init scripts configure SSH keys and run commands to customize the machine without user interaction.

A special software package called cloudbase-init is available. The package is the Windows equivalent of cloud-init.

cloud-init is available by default in Ubuntu 18 and Photon 3. You must install cloud-init on CentOS, and earlier versions of Photon or Ubuntu.

Cloud-init commands are not supported across all the operating systems.

cloudConfig sends instructions through the CD-ROM drive on the virtual machine template.

For information about cloud-init, see the Canonical website at https://cloud-init.io/.

Output from cloud-init is available in the `/var/log/cloud-init-output.log` file after the virtual machine is deployed.

6-34 About cloudbase-init

cloudbase-init is a special software package. This package is the Windows equivalent of cloud-init.

cloudbase-init supports different `userdata` content:

- PowerShell
- Bash
- Python
- cloudConfig
- Multi-part content

```
minionID: ${input.Hostname}
cloudConfig: |
  #cloud-config
  write_files:
    content: Cloudbase-init test
    path: C:\test.txt
  set_hostname: ${input.Hostname}
networks:
  - network: ${resource.Cloud_Network_1.id}
```

You must carefully format `cloudbase-init` in YAML. The line following `cloudConfig: |` defines the user data type. For example, in the screenshot you are using `cloudConfig userdata` and the line following the pipe must begin with `#cloud-config`. You can then proceed using the `cloudbase-init cloudConfig` supported directives.

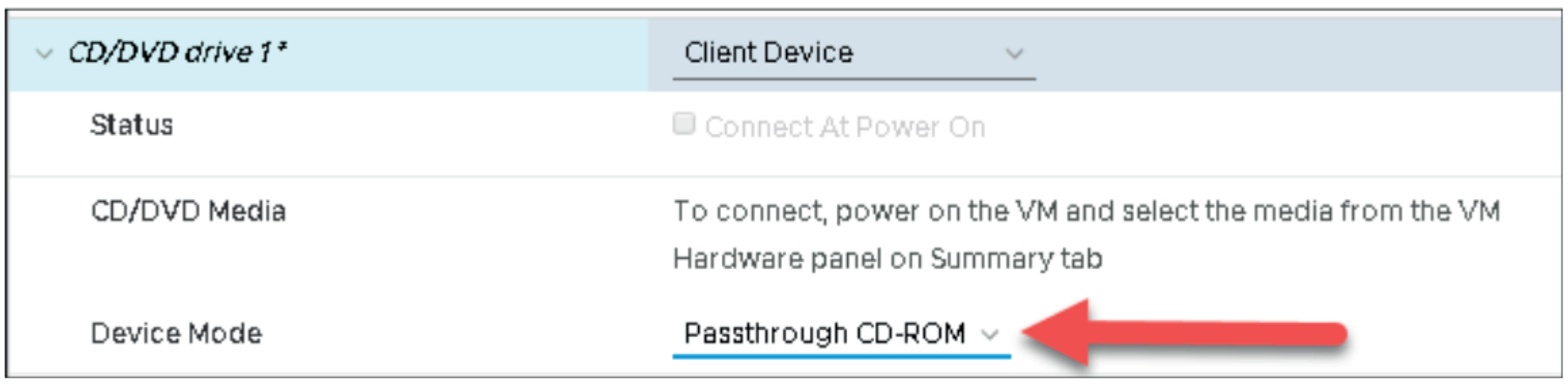
See the cloudbase-init technical documentation at https://cloudbase-init.readthedocs.io/en/latest/index.html.

6-35 Creating a vSphere Template That Supports cloud-init

To create a vSphere template that supports cloud-init:

1. Install cloud-init.
   - Use `yum` to install cloud-init in CentOS.
   - Use `apt-get` to install cloud-init in Ubuntu.

   Each operating system has unique configuration requirements.
2. Verify that you set the CD-ROM on the virtual machine template to the passthrough mode.
3. End your configuration with the `cloud-init clean` command.



The procedure for creating the CentOS and Ubuntu templates in vSphere is complex. You are guided through the complete procedure during the lab.

After you complete the configuration, enter the `cloud-init clean` command. After you enter this command, you must not modify your template virtual machine. Instead, you must shutdown the virtual machine and convert it into a template.

6-36 Formatting cloudConfig

When you use cloudConfig in YAML, you must consider case sensitivity and format:

- The `cloudConfig:` section must line up under other parts of machine properties (`image`, `flavor`, `networks`, and so on).
- The cloudConfig directive begins with a lowercase c and has an uppercase C in the middle.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: VMW-Ubuntu-Cloud
      flavor: VMW-Small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: dynamic
      cloudConfig: |
        users:
          - name: ${input.user}
            sudo: ['ALL=(ALL) NOPASSWD:ALL']
            groups: sudo
            shell: '/bin/bash'
        runcmd:
          - mkdir -p /root/test
          - hostnamectl set-hostname ${input.hostname1}
```

The pipe character (**|**) must occur after the cloudConfig directive. All commands after the pipe character are sent to the virtual machine cloud-init software package after the image is deployed. These commands are run only on the first boot.

In many cloudConfig examples, the line following `cloudConfig: |` begins with `#cloud-config`. In YAML, a comment starts with #. Adding a line with `#cloud-config` immediately after `cloudConfig: |` is not required.

You must enter the pipe character (**|**) after you add two spaces after the colon (:) in cloudConfig.

The next line after `cloudConfig: |` must be indented two spaces, followed by cloudConfig directives, such as `users`, `runcmd`, `hostname`, and so on.

After the directive (`users`, `runcmd`, and so on), the next line must begin with two spaces followed by a hyphen and a space.

6-37 cloudConfig Commands

The following commands are available in cloudConfig:

- `users:`
- `hostname:`
- `runcmd:`
- `packages:`

```
cloudConfig: |
  users:
    - name: ${input.user}
      sudo: ['ALL=(ALL) NOPASSWD:ALL']
      groups: sudo
      shell: '/bin/bash'
  runcmd:
    - mkdir -p /root/test
    - hostnamectl set-hostname ${input.hostname1}
    - PASS=${input.password}
    - USER=${input.user}
    - echo $USER:$PASS | /usr/sbin/chpasswd
    - sed -i "s/PasswordAuthentication no/PasswordAuthentication yes/g" /etc/ssh/sshd_config
    - service ssh reload
    - yum update
```

6-38 Creating Users in a Virtual Machine After Deployment

Create local users in the virtual machine by using the `users` directive:

1. Specify the name of the user.
2. Configure `sudo`.
3. Add the user to groups.
4. Specify the shell.

```
cloudConfig: |
  users:
    - name: ${input.user}
      sudo: ['ALL=(ALL) NOPASSWD:ALL']
      groups: sudo
      shell: '/bin/bash'
```

The `sudo` configuration command creates the `/etc/sudoers.d/dont-prompt-<Your_Username>-for-sudo-password` file. The user is not prompted for a password when running the `sudo` command.

You can use the `groups:` command to create groups and add local users to the created groups.

You cannot set the password of a user in the `users:` directive of cloudConfig. However, you can set the password with `runcmd:` after the user is created.

6-39 Customizing the DNS Host Name of a Virtual Machine After Deployment

Use one of the following methods to customize host DNS names:

- cloudConfig `hostname` directive
- Linux `hostnamectl` command

```
Cloud_Machine_1:
  type: Cloud.Machine
  properties:
    image: VMW-Ubuntu-Cloud
    flavor: VMW-Small
    cloudConfig: |
      hostname: ${input.hostname1}
```

```
Cloud_Machine_1:
  type: Cloud.Machine
  properties:
    image: VMW-Ubuntu-Cloud
    flavor: VMW-Small
    cloudConfig: |
      runcmd:
        - hostnamectl set-hostname ${input.hostname1}
```

The `hostname` directive in cloudConfig sets the host name. This directive is not supported in all the operating systems.

If you pass the Linux `hostnamectl` command as a `runcmd` command, the hostname is set in all the Linux operating systems.

6-40 Running Commands

Use the `runcmd:` directive to run commands in the virtual machine after deployment.

```
runcmd:
  - mkdir -p /root/test
  - hostnamectl set-hostname ${input.hostname1}
  - PASS=${input.password}
  - USER=${input.user}
  - echo $USER:$PASS | /usr/sbin/chpasswd
  - sed -i "s/PasswordAuthentication no/PasswordAuthentication yes/g" /etc/ssh/sshd_config
  - service ssh reload
```

You can use `runcmd` in YAML:

- You must begin with `runcmd:`.
- You must begin the next line with a hyphen (-), followed by a space, and followed by the command.
- Most commands that you can run interactively, can also be run in `runcmd`.
- You can edit files with the sed editor.
- Commands must be self-contained. You cannot provide user input to a `runcmd` command.

Maximizing the size of your YAML editor can help you enter long commands.

6-41 Installing Software in a Virtual Machine After Deployment

The `packages:` directive installs the software:

- The virtual machine must have access to a local repository or to the Internet to use the `packages:` directive.
- The `packages:` directive works on different versions of Linux. Although Ubuntu uses `apt-get` to install software and CentOS uses `yum` to install software, cloud-init can use the `packages:` directive on both operating systems.
- Including a directive before `packages:` updates your repositories in the virtual machine.

```
formatVersion: 1
inputs:
  hostname1:
    type: string
    title: Enter your hostname
    description: This will be the internal DNS hostname of the machine
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: VMW-Ubuntu-Cloud
      flavor: VMW-Small
      cloudConfig: |
        runcmd:
          - mkdir -p /root/test
          - hostnamectl set-hostname ${input.hostname1}
        package_update: true
        package_upgrade: true
        packages:
          - apache2
          - vim
          - uget
          - emacs25
          - thunderbird
```

To update your package repository, use the `package_update: true` directive.

The `package_update` and `package_upgrade` directives must occur before you use the `packages:` directive.

Not all packages are available for every operating system.

A package might have a different name for different operating systems.

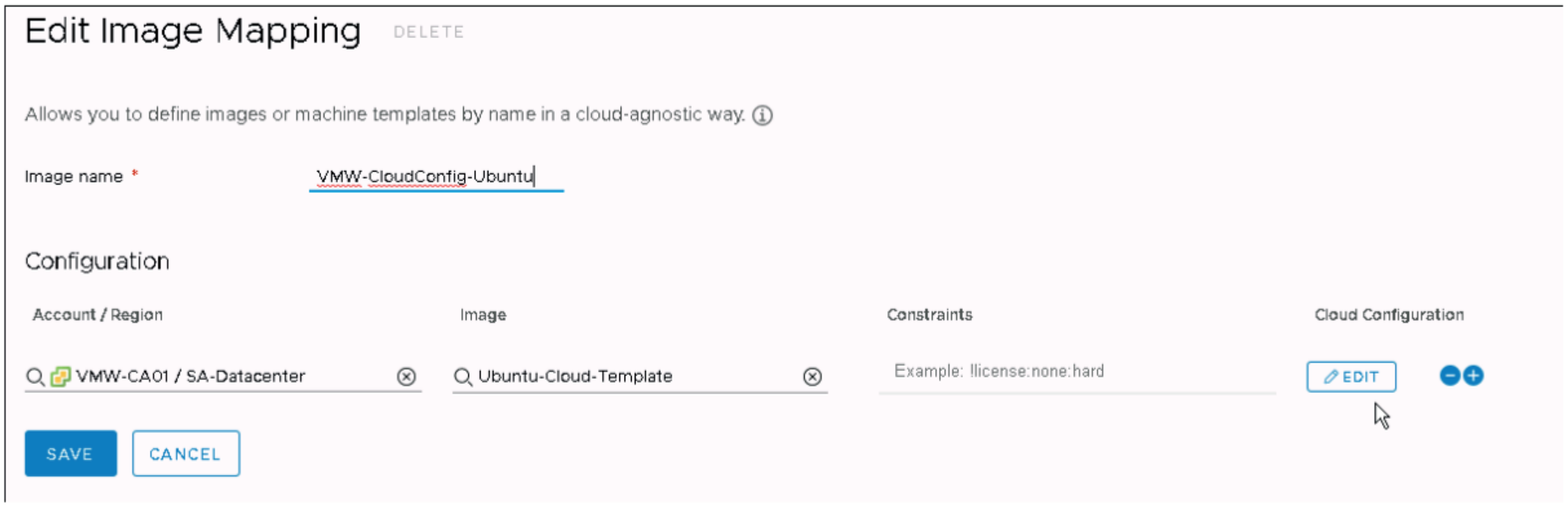
Some operating systems might have certain packages already installed by default.

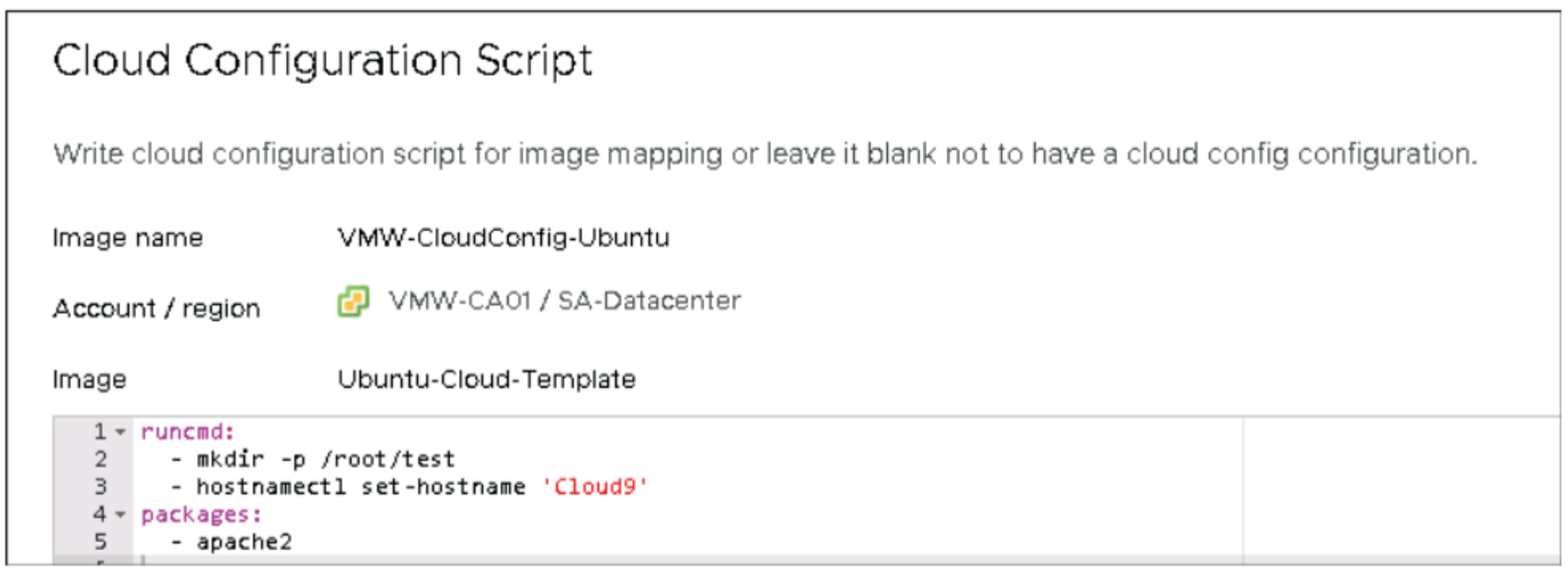
You can use YAML coding to allow the same VMware Aria Automation template to deploy virtual machines for different operating systems. A decision statement can be used based on the operating system that is deployed to select the packages that are installed.

6-42 cloudConfig in Image Mappings

Add cloudConfig commands to an image mapping:

- Enter only cloudConfig commands.
- Image commands are not interactive.
- Image mapping commands take precedence over VMware Aria Automation template commands.





You can add cloudConfig scripts to an image mapping.

These commands must be noninteractive. You cannot enter any inputs.

Enter only the commands that might follow `cloudConfig:` in a YAML VMware Aria Automation template, using the same spacing and formatting that you use for commands in the VMware Aria Automation template.

If you have cloudConfig commands in both an image mapping and a VMware Aria Automation template, the commands are combined to a single list of commands.

If a conflict occurs between the cloudConfig commands in an image mapping and the cloudConfig commands in a VMware Aria Automation template, the directives in the image mapping take precedence.

6-43 cloudConfig Recommendations in vSphere

Follow these recommendations when you use cloudConfig for vSphere deployments:

- The virtual machine that is deployed must have a DHCP IP address.
- Do not combine a vSphere customization specification with a VMware Aria Automation template that uses cloudConfig.

cloudConfig uses the network during its configuration operations.

The virtual machine template must have a live connection to the network before you run the configuration commands.

In general, this restriction forces networking to be DHCP only. You can use a static IP address with a workaround. For more information, see the following references:

- https://docs.vmware.com/en/vRealize-Automation/8.10/Using-and-Managing-Cloud-Assembly/GUID-70EA052D-FABF-4CE5-875D-9B52FED08AA3.html
- https://vnuggets.com/2020/01/29/vra-with-cloud-init-and-static-networking/
- https://vmwarelab.org/2020/02/14/vsphere-customization-with-cloud-init-while-using-vrealize-automation-8-or-cloud/

Do not combine cloudConfig with a vSphere customization specification. cloudConfig is not designed to be compatible with the vSphere customization specification and results are unpredictable. The most common result is that the networking is not properly configured.

6-44 cloudConfig Logs and Scripts in a Deployed Machine

The following files in a deployed machine have key troubleshooting information:

- Output log file: `/var/log/cloud-init-output.log`
- Main log file: `/var/log/cloud-init.log`
- Main cloudConfig scripts directory: `/var/lib/cloud/instance/scripts`
- Main cloudConfig script: `/var/lib/cloud/instance/user-data.txt`
- Runcmd script file: `/var/lib/cloud/instance/scripts/runcmd`

You can also examine the actual commands sent to cloudConfig by VMware Aria Automation:

1. Open the deployment in VMware Aria Automation.
2. Click **History**.
3. Click **ProvisioningDiagram**.
4. Use the slider to turn on the **Dev mode** toggle.
5. Click **EXPORT**.
6. Click **Save** to save the JSON file.

   You must use a JSON viewer (such as Notepad++ with a JSON plug-in installed) to read the file.
7. Search for cloudConfig.



6-45 Lab 12: Creating a cloudConfig vSphere Template

Use cloudbase-init in YAML coding to run commands and install software in a virtual machine:

1. Create a Virtual Machine
2. Power On and Configure Your Virtual Machine
3. Create a vSphere Template That Supports cloud-init
4. Use the VMware Aria Automation Template to Test the vSphere Template
5. Delete Your Deployments to Save Lab Resources

6-46 Lab 13: Enhancing VMware Aria Automation Templates with cloudConfig

Use cloudConfig in YAML coding to run commands and install software in a virtual machine:

1. Import a VMware Aria Automation Template
2. Add cloudConfig Code to Run Commands and Install Software
3. Deploy and Test Your VMware Aria Automation Template
4. Delete Your Deployment to Save Lab Resources

6-47 Lab 14: (Optional) Enhancing VMware Aria Automation Templates with cloudbase-init

Use cloudbase-init in YAML coding to run commands and install software in a virtual machine:

1. Use cloudConfig to Copy and Modify a cloudbase-init VMware Aria Automation Template
2. Examine Your Deployment
3. (Optional) Import a Multipart cloudbase-init VMware Aria Automation Template
4. (Optional) Review and Deploy Your VMware Aria Automation Template
5. (Optional) Examine Your Second Deployment
6. Delete Your Deployments to Save Lab Resources

6-48 Review of Learner Objectives

- Describe cloudConfig and cloud-init
- Create a vSphere virtual machine template that supports cloud-init
- Customize a host name in a virtual machine after deployment by using cloudConfig
- Create users in a virtual machine after deployment by using cloudConfig
- Run commands in a virtual machine after deployment by using cloudConfig
- Install software packages in a virtual machine after deployment by using cloudConfig
- Customize a host name in a virtual machine after deployment by using cloudbase-init
- Run commands in a virtual machine after deployment by using cloudbase-init

6-49 Lesson 4: Advanced YAML

6-50 Learner Objectives

- Add comments to the VMware Aria Automation template YAML code
- Create lists in the VMware Aria Automation template YAML code
- Use variables in the VMware Aria Automation template YAML code
- Configure user input in the VMware Aria Automation template YAML code
- Concatenate text in the VMware Aria Automation template YAML code
- Evaluate expressions in the VMware Aria Automation template YAML code
- Deploy components conditionally in the VMware Aria Automation template YAML code

6-51 Use Case: Using YAML to Create Infrastructure as Code

YAML is a flexible, easy-to-use language for quickly configuring and managing infrastructure as code.

```yaml
formatVersion: 1
#This section of the YAML code provides user inputs
inputs:
  SelectFlavor:
    type: string
    enum:
      - VMW-Small
      - VMW-Medium
      - VMW-Large
#This section of the YAML code controls resources
resources:
#This is a cloud agnostic machine
 Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ''
      flavor: ''
#This is the first virual machine
 Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: VMW-CentOS
      flavor: '${input.SelectFlavor}'
      customizationSpec: Lin-Cust
      networks:
        - network: '${resource.Cloud_vSphere_Network_1.id}'
          assignment: static
```

Infrastructure as code is the process of provisioning infrastructure (machines, networks, load balancers, and storage) through code rather than manually configuring physical hardware or using configuration tools.

In software, the same source code always generates the same binary code. Infrastructure as code creates the same infrastructure every time that it is deployed.

In VMware Aria Automation, you use the YAML language to manage infrastructure as code.

6-52 Indentation in YAML

Unlike many computer programming languages, YAML is sensitive to indentation:

- In YAML, indentation denotes nested blocks.
- All items in a nested block must be indented equally.
- Use spaces to indent. Tabs are not allowed.
- The YAML editor in VMware Aria Automation draws vertical lines to show where spaces are used to indent code.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: VMW-CentOS
      flavor: VMW-Small
      customizationSpec: Lin-Cust
      networks:
        - network: '${resource.Cloud_vSphere_Network_1.id}'
          assignment: static
  Cloud_vSphere_Network_1:
    type: Cloud.vSphere.Network
```

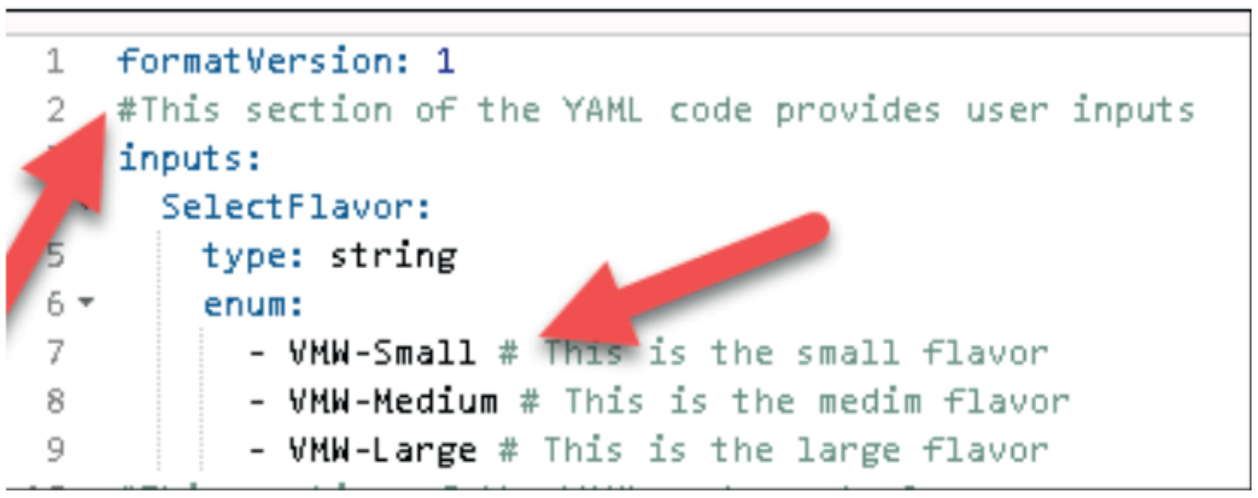
You can use any number of spaces to indent a section. Subsections that are at the same level must have the same number of spaces.

If you have the same type of items in the code that are indented with different number of spaces, the YAML editor displays a syntax error. In the example, all items under `properties` (`image`, `customizationSpec`, and `networks`) must be indented with the same number of spaces.

6-53 Comments in YAML

As VMware Aria Automation templates become more complicated, include comments for documentation:

- A # symbol anywhere in the YAML code makes everything following the # to be treated as a comment.
- A # symbol at the beginning of a line makes the entire line a comment.
- A # symbol at the end of a line adds a comment about that specific line.
- A # symbol that is enclosed by single or double quotation marks is not treated as a comment.



If you place a # symbol in single or double quotation marks, it is not as a comment. For example, in `image: 'VMW-CentOS#'`, the YAML code looks for an image named VMW-CentOS#.

To use this comment correctly, change the line to `image:'VMW-CentOS' #<write_comment_here>`.

6-54 Key-Value Pairs in YAML

YAML stores data in a map that contains keys and values:

- The format is `<KEY>: <VALUE>`.
- The value can be enclosed in single quotes.
- When using several key-value pairs, their order in the YAML code does not matter.

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
    name: VMW-Production
    networkCidr: 172.20.11.0/24
```

YAML stores data in a map of key-value pairs.

Each pair must always have a colon (:) between the key and the value.

The order of the key-value pair does not matter. You can have `flavor: <flavor_name>` followed by `image: <image_name>` or `image: <image_name>` followed by `flavor: <flavor_name>`.

The YAML editor guides you about the possible key-value pairs at a specific point in the YAML code.

Examples of key-value pairs:

- `image: <image-name>`
- `flavor: <flavor_name>`
- `type: <any type, depending on where you are in the code>`

6-55 Lists in YAML

Lists are used to store a collection of values in order:

- Lists begin with a key followed by a colon (:).
- Each list item starts with a hyphen (-).
- All list items in a list must be indented equally.

```
enum:
  - VMW-Small # T
  - VMW-Medium #
  - VMW-Large # T
```

```
networks:
  - network: '${resource.Cloud_vSp
    assignment: static
    assignPublicIpAddress: true
  - network: '${resource.Cloud_vSp
    assignment: static
    assignPublicIpAddress: false
  -
ud_v
ype:
ropel
 net
```

address: string

assignIPv6Address: boolean

Lists are useful when you define variables or inputs.

6-56 Variables in YAML

Variables in YAML start with the $ character:

- Variables can be used to reference other components in the YAML code.
- Variables can also be used with user inputs.

```
resources:
  #This is the first virual machine
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: VMW-CentOS
      flavor: '${input.SelectFlavor}'
      customizationSpec: Lin-Cust
      networks:
        - network: '${resource.Cloud_vSphere_Network_1.id}'
          assignment: static
  Cloud_vSphere_Network_1:
    type: Cloud.vSphere.Network
    properties:
      networkType: existing
      name: VMW-Production
      networkCidr: 172.20.11.0/24
```

Variables can also be used with user inputs. When referenced, these variable names start with the `input.` text.

The first part of the variable name (for example, `resource.`) describes the part of the YAML code that the variable comes from.

If you connect two objects in the design canvas, a variable that points to the connected object is added automatically in the YAML code to the object that is connected to it. These variables always end with the `.id` text.

6-57 User Inputs in YAML

User inputs enable the user to select options from a list of choices:

- The list is defined in YAML.
- Assign the variable to any name you like.
- Define the list as a type of `string` and delineate the list items under `enum`.
- Use the variable anywhere in the YAML code:
  - Begin the variable with `'${input.`
  - End with the variable name and a right brace, for example, `'${input.SelectFlavor}'`.

```
3  inputs:
4    SelectFlavor:
5      type: string
6      enum:
7        - VMW-Small # This is the small flavor
8        - VMW-Medium # This is the medim flavor
9        - VMW-Large # This is the large flavor
10 #This section of the YAML code controls resources
11 resources:
12   #This is the first virual machine
13   Cloud_vSphere_Machine_1:
14     type: Cloud.vSphere.Machine
15     properties:
16       image: VMW-CentOS
17       flavor: '${input.SelectFlavor}'
```

When you define an input variable, it appears in the `inputs` section (plural). When you reference the variable, it is singular `${input.<variable_name>}`.

6-58 Formatting Text in a VMware Aria Automation Template

To create a user-friendly input on your choice list, you might want to concatenate the text or change the case.

```
inputs:
  SelectCloud:
    type: string
    enum:
      - AWS
      - GCP
      - Azur
      - vSphere
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      constraints:
        - tag: ${'cloud:""' + to_lower(input.SelectCloud)}
      image: VMW-CentOS
      flavor: VMW-Small
```

Capability Tags

cloud:aws
cloud:gcp
cloud:azure
cloud:vsphere

In the example, a user input was created that enables the user to choose between multiple cloud platforms. But these choices might not match the capability tags that were defined. YAML code addresses this issue.

The YAML takes the input, adds the word `cloud:` before it, and switches all the input to lowercase.

The concatenated text gives the exact name of a capability tag that you previously created in VMware Aria Automation.

The YAML code includes `'${''cloud:""''`. The part of the code has a single quote, `${cloud`, a colon (`:`), two double quotes, and one single quote. The colon (`:`) is a special character in YAML. To use a colon in a string, two double quotes must follow the colon. The `:""` code allows the colon (`:`) to be used in a string. The two double quotes are like an escape character.

As an alternative to this approach, using `oneOf` instead of `enum` provides an easier solution. In the drop-down menu defined by an `enum`, each entry in the list is a single value such as AWS. Because that value does not match the hypothetical capability tags, the earlier example converted the value that the user selects to precisely match a capability tag. When defining a drop-down menu using `oneOf`, each entry in the list is a pair. Each pair consists of a value

that the user is shown in the drop-down menu and a value that is returned to VMware Aria Automation. For example:

```
oneOf:
- title: AWS
const: 'cloud:aws'
- title: Azure
const: 'cloud:azure'
- title: GCP
const: 'cloud:gcp'
- title: vSphere
const: 'cloud:vsphere'
```

6-59 Using Escape Characters

Configuration files often require the following special characters:

- The standard escape character in YAML is the backslash (\).
- You can escape a single quote (') by enclosing it in a pair of double quotes.
- You can escape a colon (:) by following it with two double quotes.

Example escaping the dollar sign:

```
- echo "\$cfg['Servers'][\$i]['compress'] = 'FALSE';"  >> /root/my_phpmyadmin-host.conf
- echo "\$cfg['Servers'][\$i]['auth_type']= 'config';" >> /root/my_phpmyadmin-host.conf
- echo "\$cfg['Servers'][\$i]['user']     = '$USER';"  >> /root/my_phpmyadmin-host.conf
- echo "\$cfg['Servers'][\$i]['password'] = '$PASS';"  >> /root/my_phpmyadmin-host.conf
```

Example escaping the colon:

```
- echo "network:"" "     >> /etc/netplan/50-cloud-init.yaml
- echo "  version:"" 2"  >> /etc/netplan/50-cloud-init.yaml
- echo "  ethernets:"" " >> /etc/netplan/50-cloud-init.yaml
- echo "    ens160:"" "  >> /etc/netplan/50-cloud-init.yaml
```

A single colon in YAML is a special character and requires a special escape character. To use a colon in a string, two double quotation marks must follow the colon. The `:""` code allows the colon (`:`) to be used in a string. The two double quotations act as an escape character.

6-60 Evaluating Expressions in the VMware Aria Automation Template

Set values based on the evaluation of an expression.

```
  SelectCloud:
    type: string
    enum:
      - AWS
      - GCP
      - Azure
      - vSphere
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      constraints:
        - tag: '${input.SelectCloud}'
      folderName: '${input.SelectCloud == "vSphere" ? "Production_VMs" : ""}'
```

In the example, YAML evaluates the value of the `SelectCloud` input variable.

The == expression tests the value of the variable to see if it equals what follows. On the slide, if `SelectCloud` is equal to <some_value>, then <perform_some_action>. The == expression is the syntax equivalent of is equal to.

The ? expression is the equivalent to a `Then` clause in an If-Then-Else expression.

If `SelectCloud` is equal to `vSphere`, the `folderName` property is set to `Production_VMs`.

If `SelectCloud` is not equal to `vSphere`, the `folderName` property is set to a blank.

Several other conditional expressions are available:

- Equality operators are == (equal to) and != (not equal to).
- Logical operators are && (and) || (or) and ! (not).
- Relational operators are < (less than) > (greater than) <= (less than or equal to) and >= (greater than or equal to).

Conditional expressions always use the pattern: `conditional-expression ? true-answer : false-answer`

For more information about the VMware Aria Automation Assembler expressions syntax, see *Using and Managing Cloud Assembly* https://docs.vmware.com/en/vRealize-Automation/index.html.

6-61 Conditional Deployment in the VMware Aria Automation Template

Deploy an object only if specific values are set.

```
formatVersion: 1
inputs:
  DeploymentMode:
    title: How to deploy
    type: string
    enum:
      - Single
      - Cluster
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.Machine
    properties:
      count: '${input.DeploymentMode == "Cluster" ? 3 : 1}'
      image: VMW-CentOS
      flavor: VMW-Small
  Cloud_LoadBalancer_1:
    type: Cloud.LoadBalancer
    properties:
      count: '${input.DeploymentMode == "Cluster" ? 1 : 0}'
```

In the example, the user is prompted whether to perform a clustered deployment or to deploy a single machine. The user's response is stored in the `DeploymentMode` input variable.

If `DeploymentMode` is set to `Cluster`, three machines and one load balancer are deployed.

If `DeploymentMode` is set to `Single`, one machine and zero load balancers are deployed.

6-62 Lab 15: Creating an Advanced VMware Aria Automation Template

Use advanced YAML coding in a VMware Aria Automation template:

1. Copy and Modify a VMware Aria Automation Template
2. Add a Constraint to Your VMware Aria Automation Template
3. Add a Conditional Disk Deployment to Your VMware Aria Automation Template
4. Deploy the VMware Aria Automation Template
5. Examine Your Deployment
6. Delete Your Deployment to Save Lab Resources

6-63 Review of Learner Objectives

- Add comments to the VMware Aria Automation template YAML code
- Create lists in the VMware Aria Automation template YAML code
- Use variables in the VMware Aria Automation template YAML code
- Configure user input in the VMware Aria Automation template YAML code
- Concatenate text in the VMware Aria Automation template YAML code
- Evaluate expressions in the VMware Aria Automation template YAML code
- Deploy components conditionally in the VMware Aria Automation template YAML code

6-64 Key Points

- VMware Aria Automation Templates enable the automation of deployments.
- cloudConfig provides a cross-platform method of enhancing deployed machines.
- Cloud-agnostic resources enable VMware Aria Automation Templates to deploy resources such as machines, networks, and disks across public cloud platforms.
- YAML is the language used by VMware Aria Automation to power VMware Aria Automation Templates.

Questions?

Module 7

Tags

7-2 Importance

Tags are labels that can be added to items and resources so that they can be managed and categorized. In VMware Aria Automation Assembler, tags are used to determine the compute, storage, and network resources that a project can use.

Based on the tags defined, VMware Aria Automation matches the capabilities and constraints for VMware Aria Automation Templates and projects and then provisions resources accordingly. Additionally, tags can be used to search and filter resources based on a specific criterion.

7-3 Lesson 1: Tags

7-4 Learner Objectives

- Describe the relationship between capability tags and constraint tags
- Explain how tags are used in VMware Aria Automation
- Create tags by setting keys and values
- Understand tagging strategies and implementation

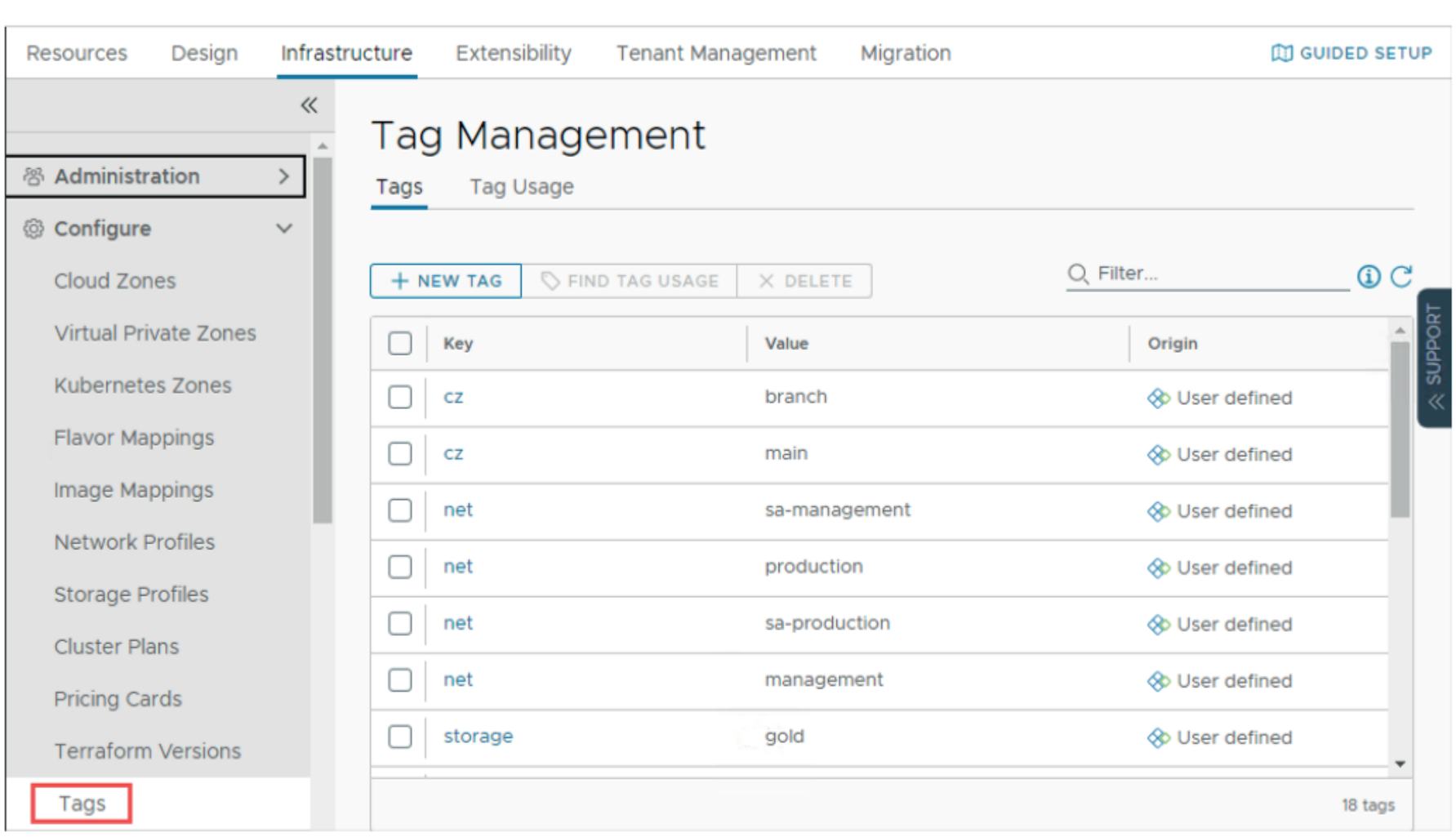
7-5 Tags in VMware Aria Automation

To access tags in the VMware Aria Automation console, select **Infrastructure** > **Configure** > **Tags** in the left navigation pane.

Tags are labels that are applied to resources. They can be of the form `key` or `key:value`.

Based on their functionality, tags can be defined as:

- Capability tags
- Constraint tags
- Resource tags



Tags are typically either external or internal:

- External tags: Defined in the cloud accounts (public and private clouds)
- Internal tags: Defined in VMware Aria Automation Assembler

Tags drive the placement of deployments by matching capabilities and constraints.

Tags match capabilities and constraints for VMware Aria Automation Templates and projects in relation to compute, network, and extensibility resources.

While a single value can be defined for a tag, the best practice to use name-value pairs in the format `name:value`.

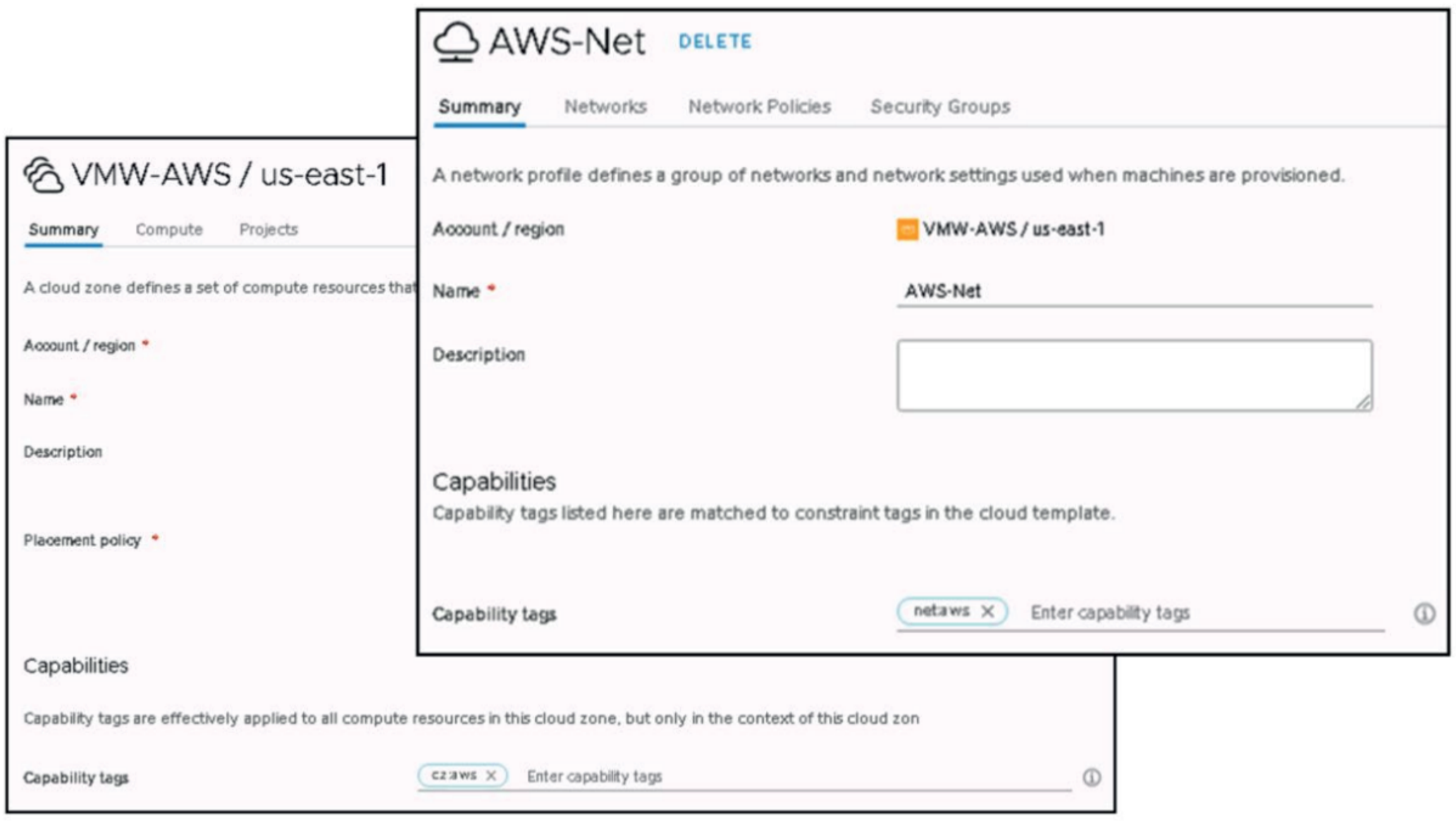
Tags defined in the vSphere environment and external cloud providers are automatically discovered and imported into VMware Aria Automation.

7-6 Capability Tags

Capability tags define deployment capabilities based on infrastructure resources.

Capability tags can be applied to the following types of resources:

- Cloud accounts
- Integrations
- Cloud zones
- Virtual private zones
- Kubernetes zones
- Network profiles
- Storage profiles



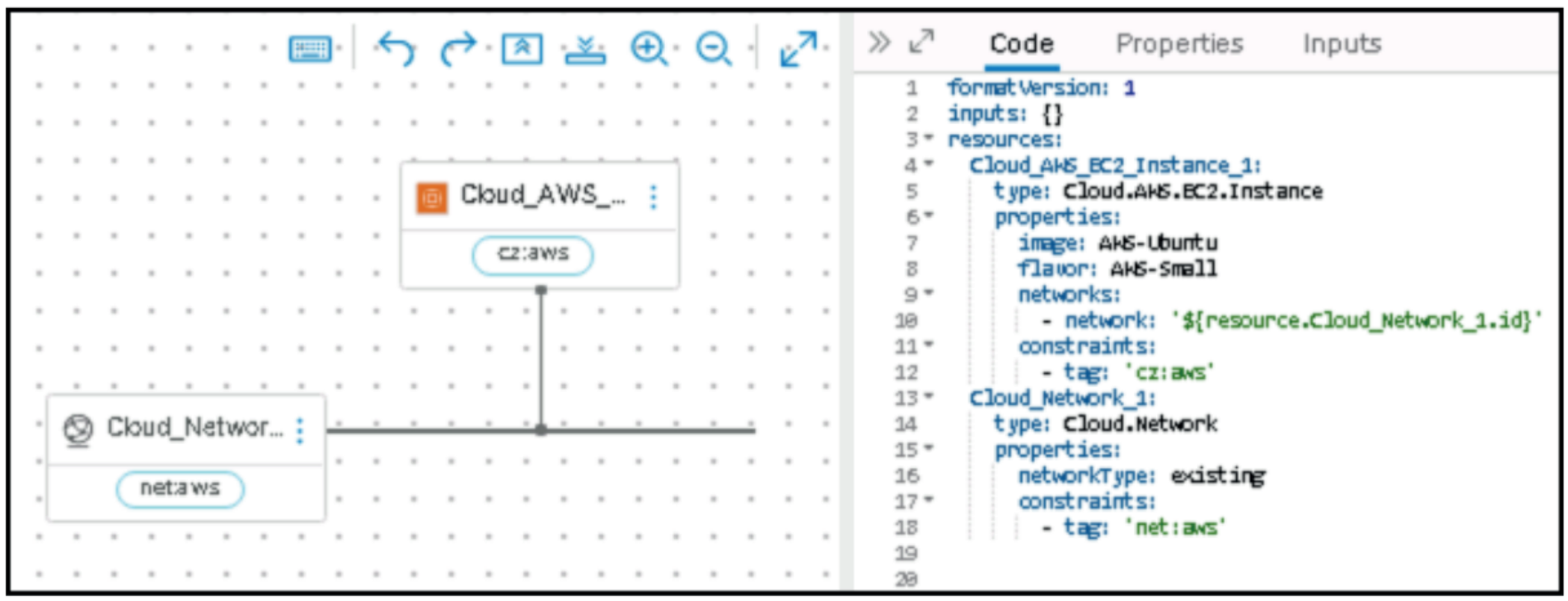
Capability tags are used for labeling resources within the cloud.

7-7 Constraint Tags

Constraint tags governs how VMware Aria Automation selects resources to use during deployments.

Constraint tags can be applied to the following types of resources:

- VMware Aria Automation Templates
- Image mappings
- Projects



Constraint tags are used for controlling access to resources.

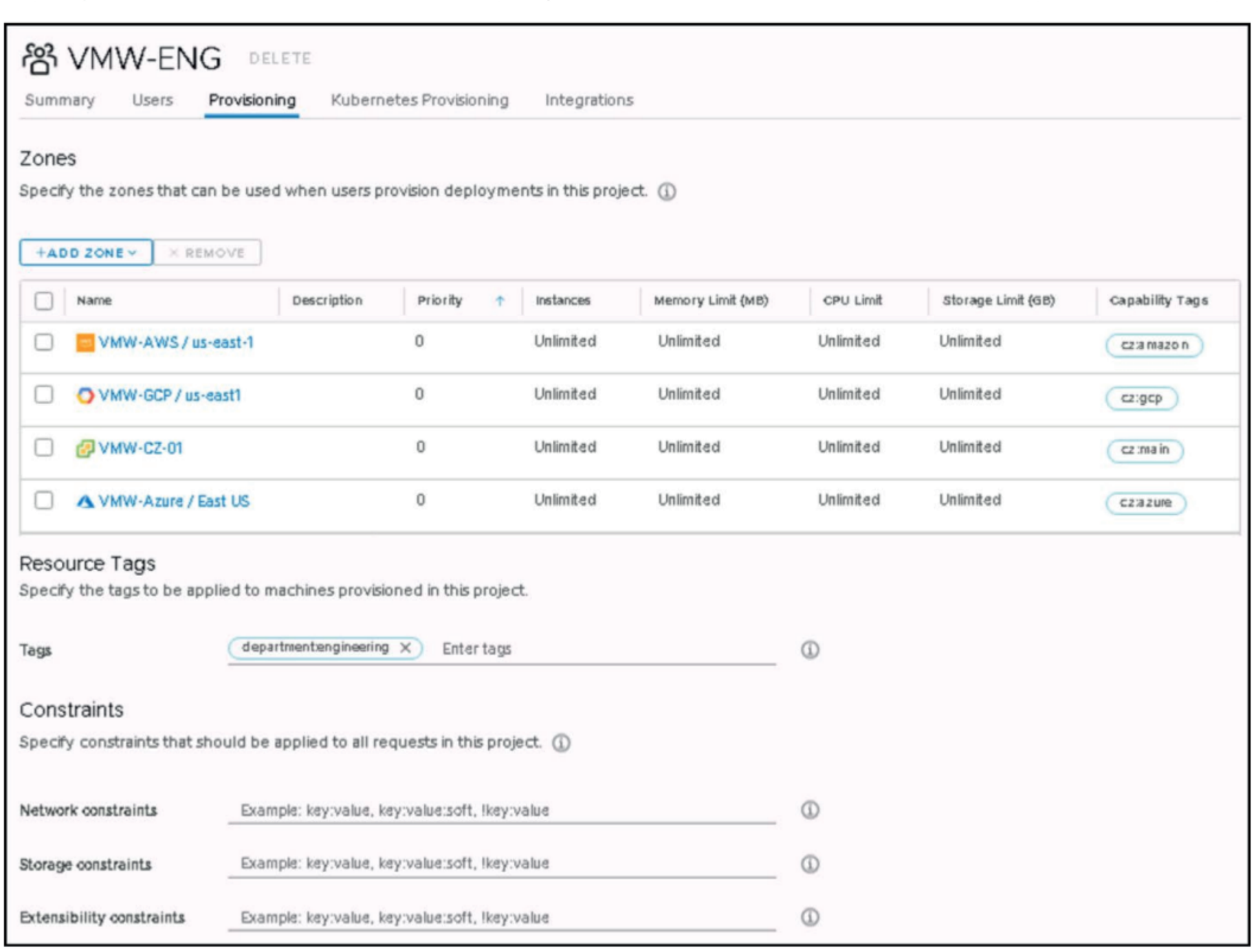
They are used to define the resources that are available for provisioning or to redirect provisioning to specific resources that are available for deployments.

7-8 Tags in Projects

Network constraints, storage constraints, and extensibility constraints can be specified on a project.

Project constraint tags take precedence over VMware Aria Automation Templates constraint tags.

In addition to constraint tags, resource tags can be added to the resources deployed during the provisioning process. Along with any machine-specific tags, the resource tags defined in a project are added to all the deployed machine resources that are part of that project.



If the same constraint is specified in both the project and the VMware Aria Automation template, then the constraint specified in the project takes precedence. For example, if the network constraint is set to `location:boston` in the project and the network constraint set in VMware Aria Automation Templates is `location:london`, then the project constraint takes precedence. As a result, the constraint is `location:boston`.

Resource tags result in machines deployed from VMware Aria Automation Templates instance being tagged in the compute platform. For example, if the machine being deployed by VMware Aria Automation is a vSphere VM, then the VM is tagged using the tagging mechanism built into vSphere.

7-9 Hard, Soft, and Not Modifiers

The following modifiers can be added to the `<key:value>` tags:

- `<key:value>:hard`
- `<key:value>:soft`
- `!<key:value>`

The `hard` modifier indicates that the constraint tag is a requirement. If the constraint cannot be satisfied, then deployment fails. The `key:value` tag is synonymous with the `key:value:hard` tag.

The `soft` modifier indicates that the constraint tag is a preference. If VMware Aria Automation can find a resource that satisfies the constraint tag, then VMware Aria Automation uses that resource. If VMware Aria Automation cannot find a resource that satisfies the constraint tag, then the deployment can continue using another resource even though it does not satisfy the constraint tag.

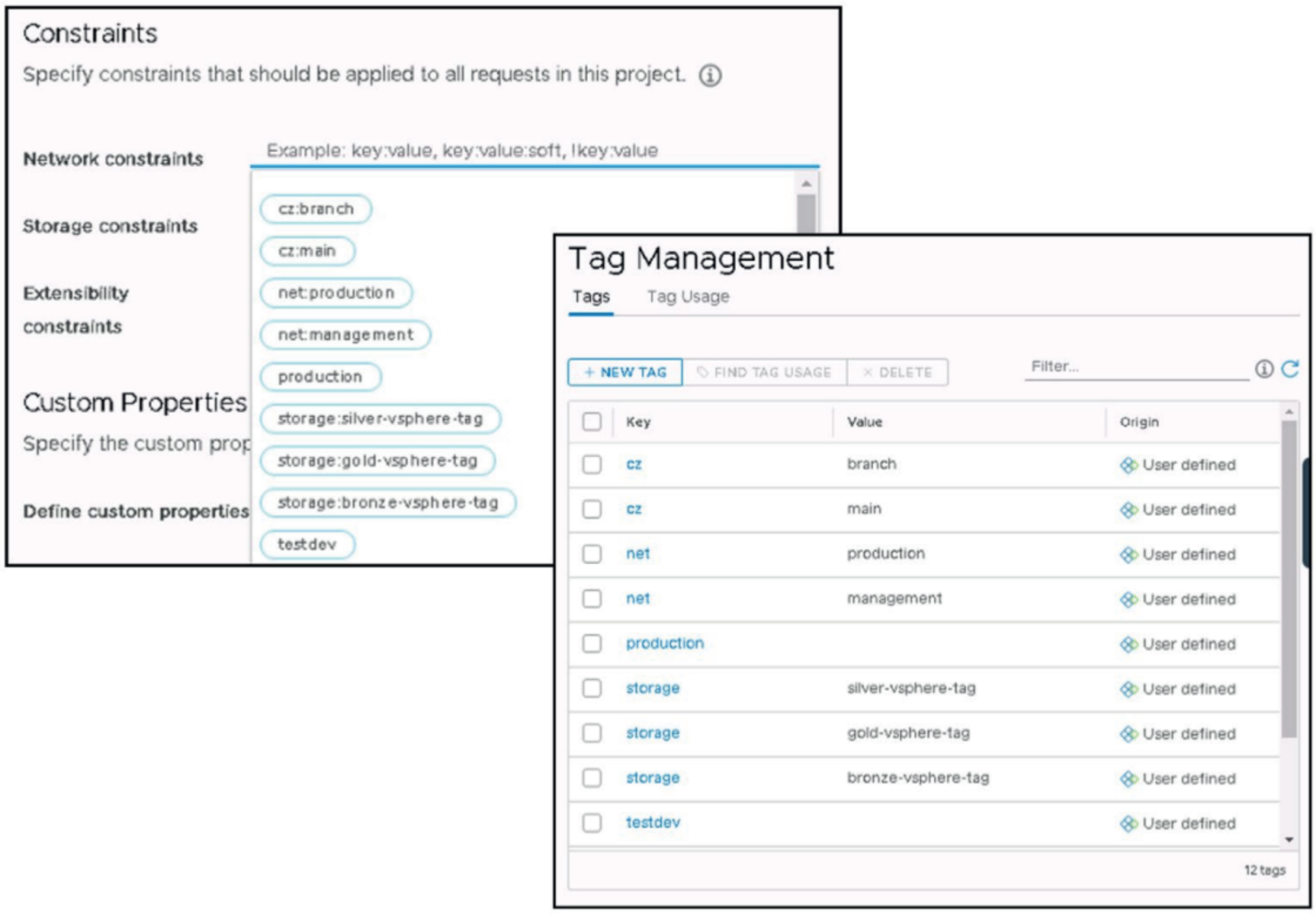
The `!` modifier negates the constraint tag. You use `!` with the `<key:value>` tag (with or without the `hard` or `soft` modifiers) to avoid deploying to resources with a matching tag.

7-10 Tagging Strategies

Developing tagging strategies based on specific use cases helps to optimize VMware Aria Automation Assembler capabilities and reduce potential misunderstanding.

Follow these suggestions while developing a tagging strategy:

- Tag enough to be useful, but do not tag excessively.
- Resource grouping can reduce the amount of tagging required.
- Use `<key:value>` style tags rather than `<key>` style tags.
- Perform a business requirements analysis and base the tagging strategy on those requirements.



7-11 Tagging Implementation

The following considerations can be helpful when implementing a tagging strategy:

- Plan the number of environments to be deployed and create a tag for each environment.
- Create cloud zones and network profile capability tags to support the deployment.
- Consider the different deployment regions or locations. Create tags at the profile level that represent each of these different regions or locations.
- Consider the different storage options that are available for deployments. These storage options should be represented by tags.
- Consider the networking options and create tags to accommodate all applicable options.

7-12 Sequencing of Capability and Constraint Tag Processing

The following high-level operations summarize the sequence for processing capability and constraint tags:

- The cloud zones are filtered by several criteria, including availability and profiles. Tags in profiles for the zone are matched.
- The remaining cloud zones are filtered by hard constraints using cloud zone and compute capability tags.
- Cloud zones are chosen based on provisioning priority. If more than one cloud zone has the same provisioning priority, they are sorted by matching soft constraints using a combination of cloud zones and compute capabilities.
- After a cloud zone is selected, a host is selected by matching a series of hard and soft constraints as defined in VMware Aria Automation Templates.

7-13 Lab 16: Creating and Using Tags

Create tags and use them in a blueprint:

1. Create Tags
2. Examine the VMW-CZ-01 Cloud Zone
3. Create a Project
4. Copy and Modify a VMware Aria Automation Template
5. Deploy a Machine into the Production Environment
6. Deploy a Machine into the Test/Dev Environment
7. Examine Deployments
8. Delete Your Deployments to Save Lab Resources

7-14 Lab 17: Using a Filter Tag on a Cloud Zone

Apply a filter tag to a cloud zone to restrict where VMware Aria Automation deploys machines:

1. Examine the vSphere Cloud Account
2. Modify the VMW-CZ-01 Cloud Zone
3. Examine a Project
4. Deploy a Machine into the Production Environment
5. Examine the Deployment
6. Remove the Filter Tag from VMW-CZ-01
7. Delete Your Deployment to Save Lab Resources

7-15 Lab 18: Tagging Deployed Virtual Machines in vSphere

Tag machines that are deployed by VMware Aria Automation with a tag that is visible in vSphere:

1. Create a Project
2. Copy and Deploy a VMware Aria Automation Template
3. Examine the Deployment
4. Delete Your Deployment to Save Lab Resources

7-16 Review of Learner Objectives

- Describe the relationship between capability tags and constraint tags
- Explain how tags are used in VMware Aria Automation
- Create tags by setting keys and values
- Understand tagging strategies and implementation

7-17 Key Points

- Tags can be used to manage, categorize, and match resources.
- Storage can be managed with VMware Aria Automation storage profiles.

Questions?

Module 8

Storage Configuration

8-2 Importance

Storage is one of the most critical resources to consider when planning your environment. Incorrect storage configurations can easily destabilize an environment. Dividing storage into storage tiers and managing storage with storage profiles and tags maximizes the return on storage investment.

8-3 Lesson 1: Storage Configuration

8-4 Learner Objectives

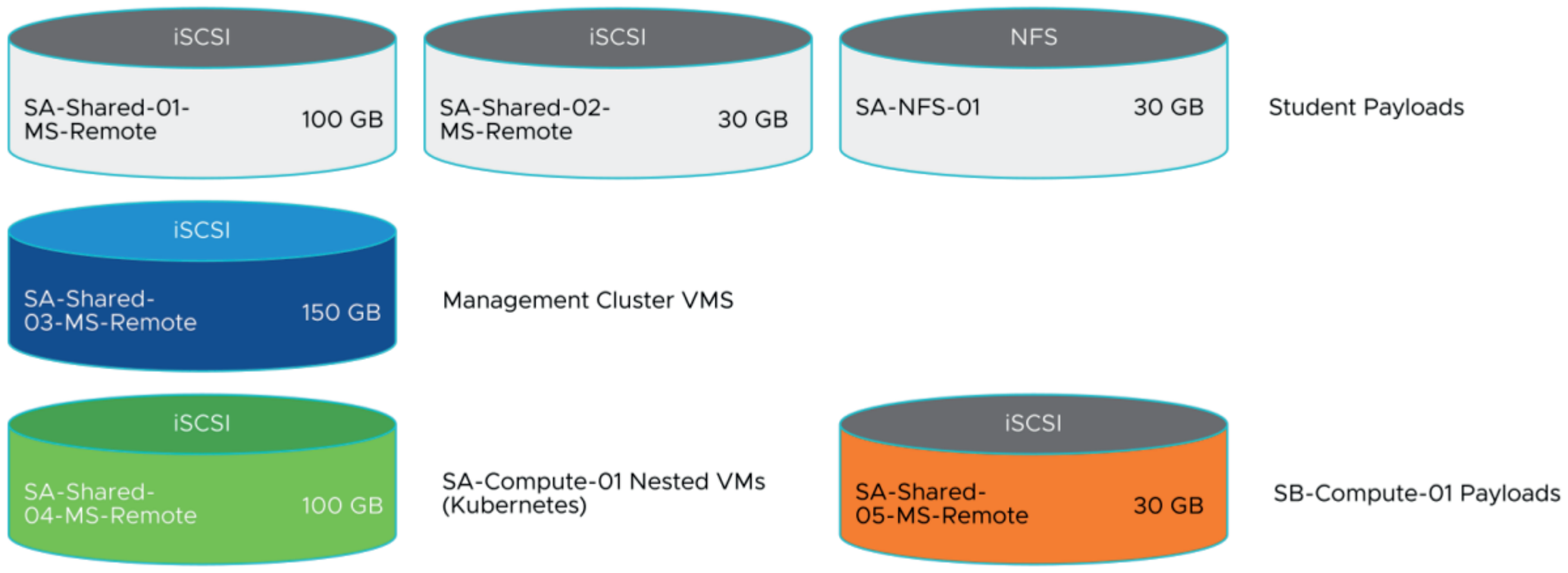
- Create a VMware Aria Automation storage profile
- Use a VMware Aria Automation storage profile in VMware Aria Automation Templates
- Describe volumes
- Explain how to deploy a first class disk using VMware Aria Automation Templates

8-5 Use Case: Effective Storage Management

Storage management is a key part of resource management.

Unlike CPUs and memory, storage is not homogenous. Different types of storage are available with different capabilities:

- Some storage is more expensive than others.
- Some storage systems are fast, such as SSDs.
- Some storage arrays have a small amount of free space.
- Some storage arrays have different IOPS characteristics.
- Some storage systems, such as NFS, have unique characteristics.

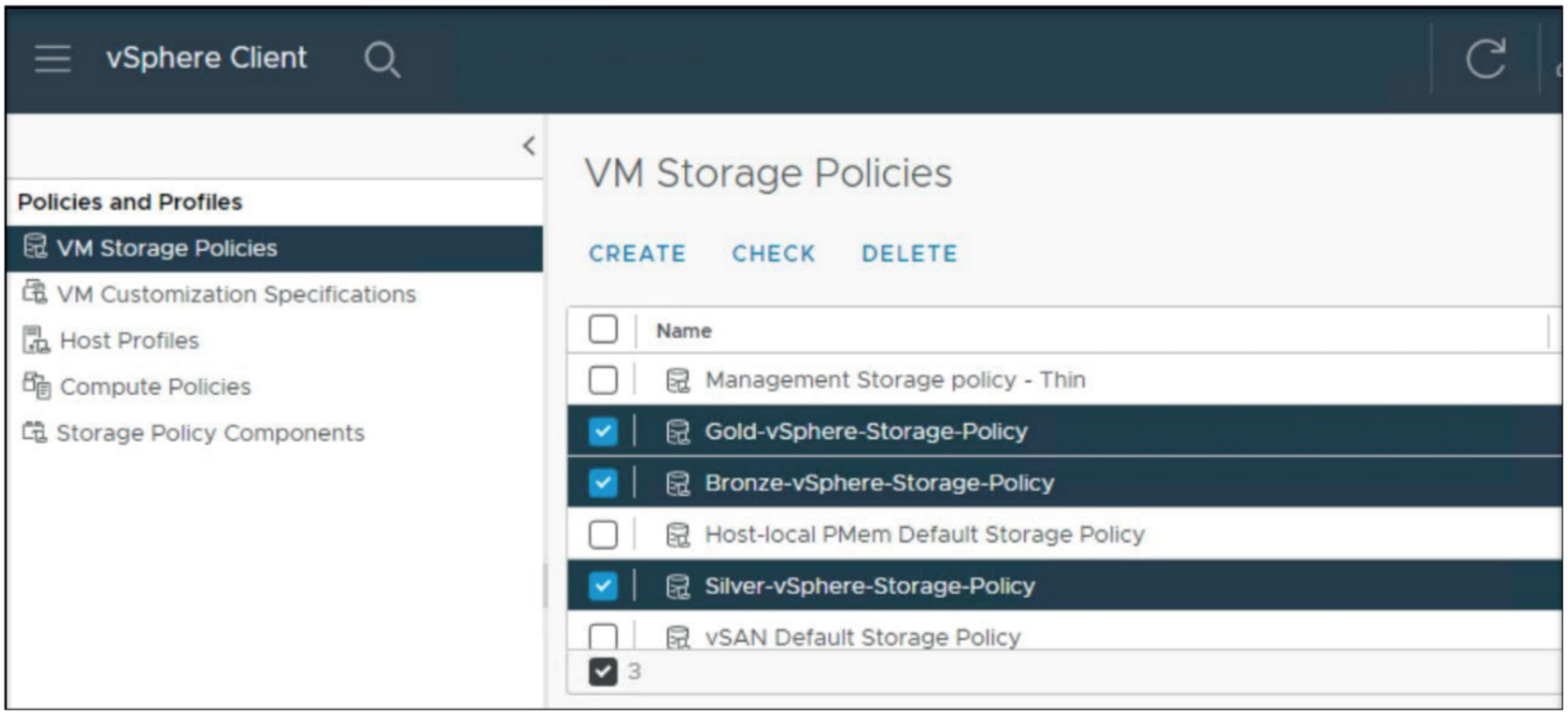


Storage is available in multiple types, and each type has different capabilities. VMware Aria Automation uses storage profiles to help you manage different types of storage.

8-6 vSphere VM Storage Policies

vSphere VM storage policies can be used to define your storage:

- Storage policies can be based on host-based rules, vSAN rules, or tags.
- After a VM storage policy is defined, it must be assigned to compatible storage.
- An easy method is to create tags in vSphere, assign the tags to datastores, and then create tag-based VM storage policies.



VMware Aria Automation storage profiles can directly interface with vSphere VM storage policies. You can also use VMware Aria Automation storage profiles on other cloud accounts.

The screenshot includes three vSphere VM storage policies: Gold-vSphere-Storage-Policy, Silver-vSphere-Storage-Policy, and Bronze-vSphere-Storage-Policy.

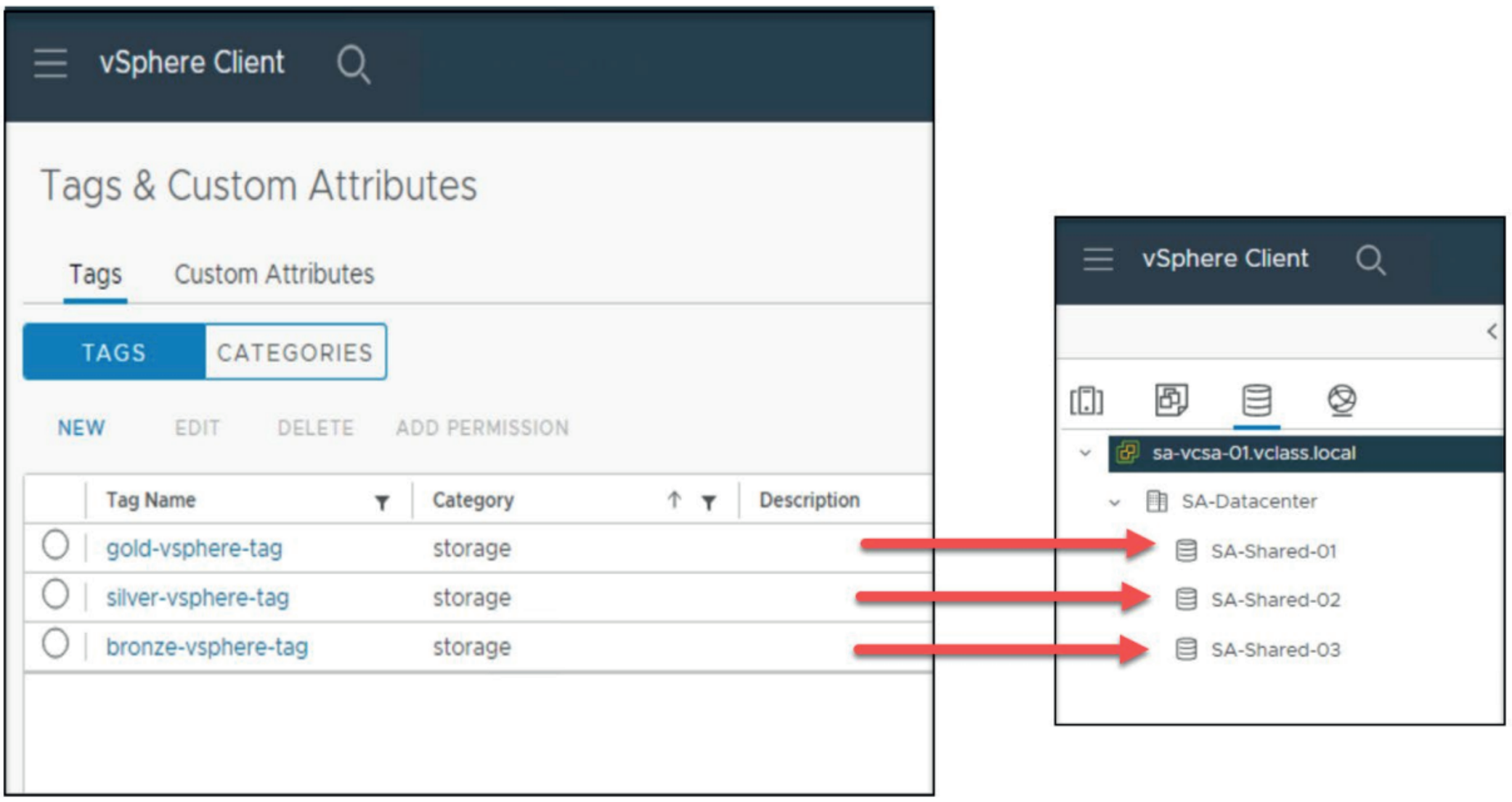
These vSphere VM storage policy names are verbose for real-world scenarios. These names were intentionally selected for this course to clarify where the tags are defined. These VM storage policies are defined in vSphere, not VMware Aria Automation.

Most VM storage policies are tied to characteristics of the storage.

8-7 About vSphere Tags

vSphere VM storage policies can use vSphere tags.

Like tagging in VMware Aria Automation, you can use vSphere tags to label objects in your vSphere inventory, such as datastores.



Although VMware Aria Automation tags and vSphere tags are similar in many ways, you must recognize that these tags are separate mechanisms that operate independently of each other.

The VMware Aria Automation tags and vSphere tags differ in their terminology. With Aria Automation tags, you set a key and a value. With vSphere tags, you set a category and a tag. A vSphere tag category is analogous to a VMware Aria Automation tag key, and a vSphere tag is analogous to a VMware Aria Automation tag value.

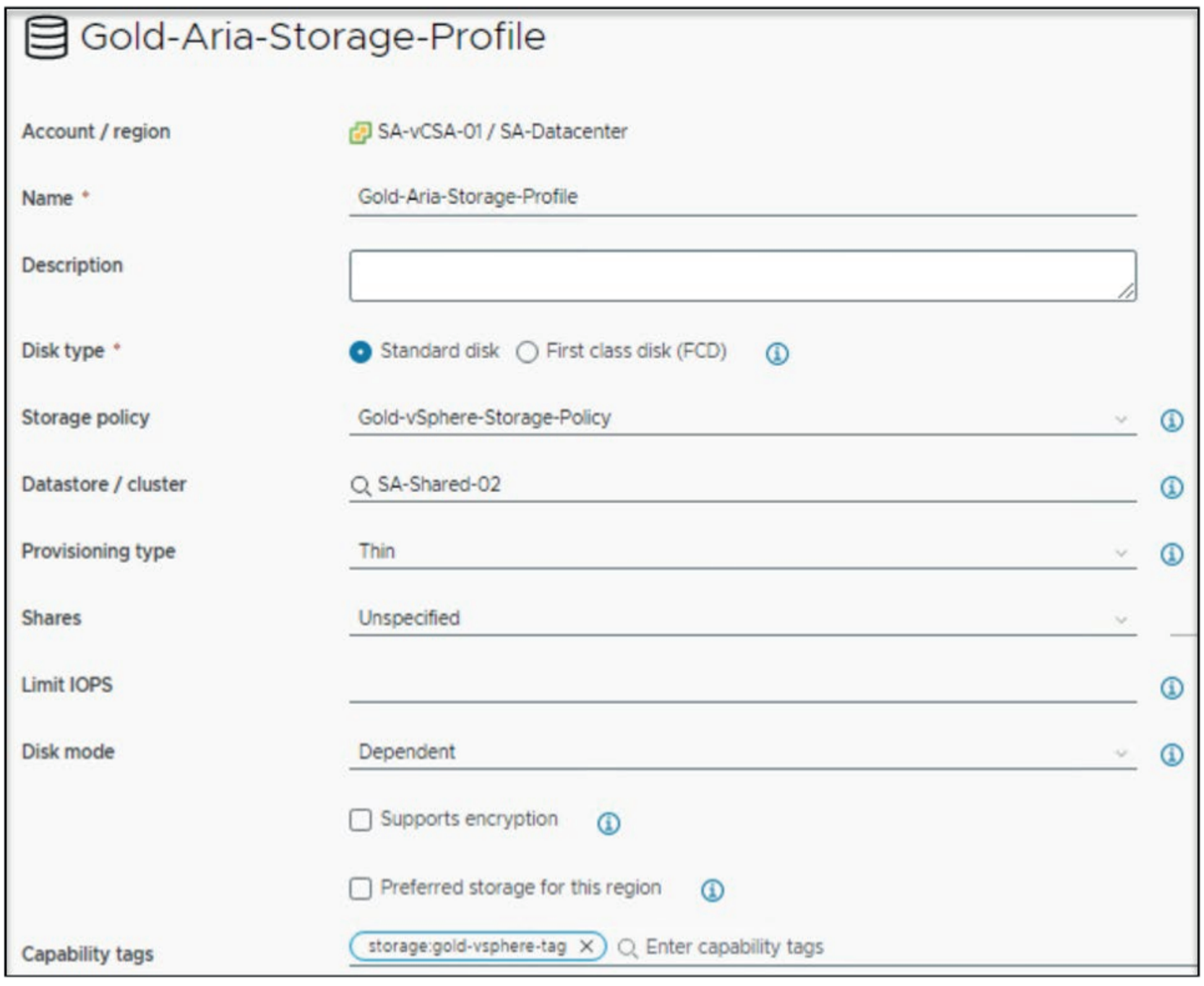
The screenshot includes three vSphere tags that were created: gold-vsphere-tag, silver-vsphere-tag, and bronze-vsphere-tag. One tag was applied to each of the datastores called SA-Shared-01, SA-Shared-02, and SA-Shared-03.

These vSphere tag names (gold-vsphere-tag, silver-vsphere-tag, and bronze-vsphere-tag) are verbose for real-world scenarios. These names were intentionally selected for this course to clarify where the tags are defined. These tags are defined in vSphere, not VMware Aria Automation.

8-8 Creating VMware Aria Automation Storage Profiles

To create a storage profile in VMware Aria Automation that is related to a vSphere VM storage policy:

1. Select **Infrastructure** > **Configure** > **Storage Profiles**.
2. Click **NEW STORAGE PROFILE**.
3. Select your cloud account/region.
4. Enter a name and description for your storage profile.
5. Configure the storage profile.
   a.. Next to Disk type, select **Standard disk** or **First class disk (FCD)**.
   b.. Select the vSphere VM storage policy from the **Storage policy** drop-down menu.
   c.. Create or attach a capability tag.
6. Click **CREATE**.



The screenshot includes a VMware Aria Automation storage profile called Gold-vRA-Storage-Profile.

The VMware Aria Automation storage profile name Gold-Aria-Storage-Profile is verbose for real world-scenarios. This name was intentionally selected for this course to clarify where the VMware Aria Automation storage policy is defined. This storage profile is defined in VMware Aria Automation, not vSphere.

In the screenshot, **Storage policy** is set to point to a VM storage policy called Gold-vSphere-Storage-Policy. This VM storage policy is defined in vSphere.

In the screenshot, **Capability tags** is set to storage:gold-vsphere-tag. This tag is defined in vSphere. The example uses a vSphere tag, but you are not limited to using tags defined in vSphere.

VMware Aria Automation automatically detects all VM Storage profiles and tags that you define in vSphere. A data collection is scheduled to run every ten minutes. If a VM storage policy or a tag that you defined in vSphere does not appear in VMware Aria Automation, wait for the next data collection. To view when the last data collection occurred, select **Infrastructure** > **Connections** > **Cloud Accounts**, open your vCenter Server cloud account, and examine the **Status** section.

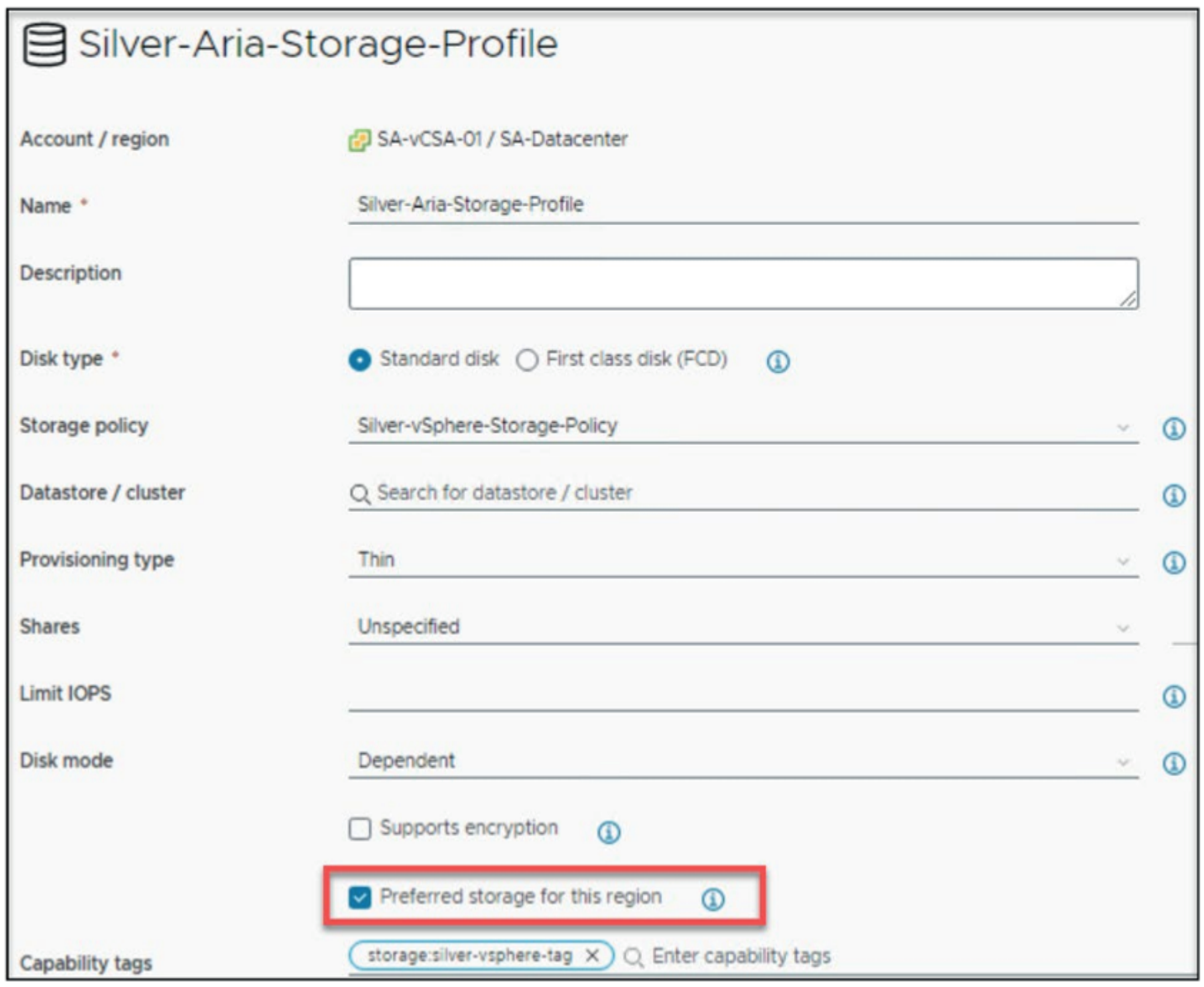
The default storage in Aria Automaton is the storage profile that is marked as Preferred Storage If you do not set a disk constrain or set a storage policy in a VMware Aria Automation template, then the default storage policy is used.

8-9 Using Preferred VMware Aria Automation Storage Profiles

For each cloud account, you can define multiple storage profiles. Only one storage profile can be marked as the preferred storage profile for that region.

To mark a storage profile as the preferred storage profile:

1. In the VMware Aria Automation console, select **Infrastructure** > **Configure** > **Storage Profiles** in the left navigation pane.
2. Click **BROWSE** on the catalog card for your cloud account/region.
3. Click the storage profile that you want to set as the default for that cloud account.
4. Scroll down and select the **Preferred storage for this region** check box.
5. Click **SAVE**.

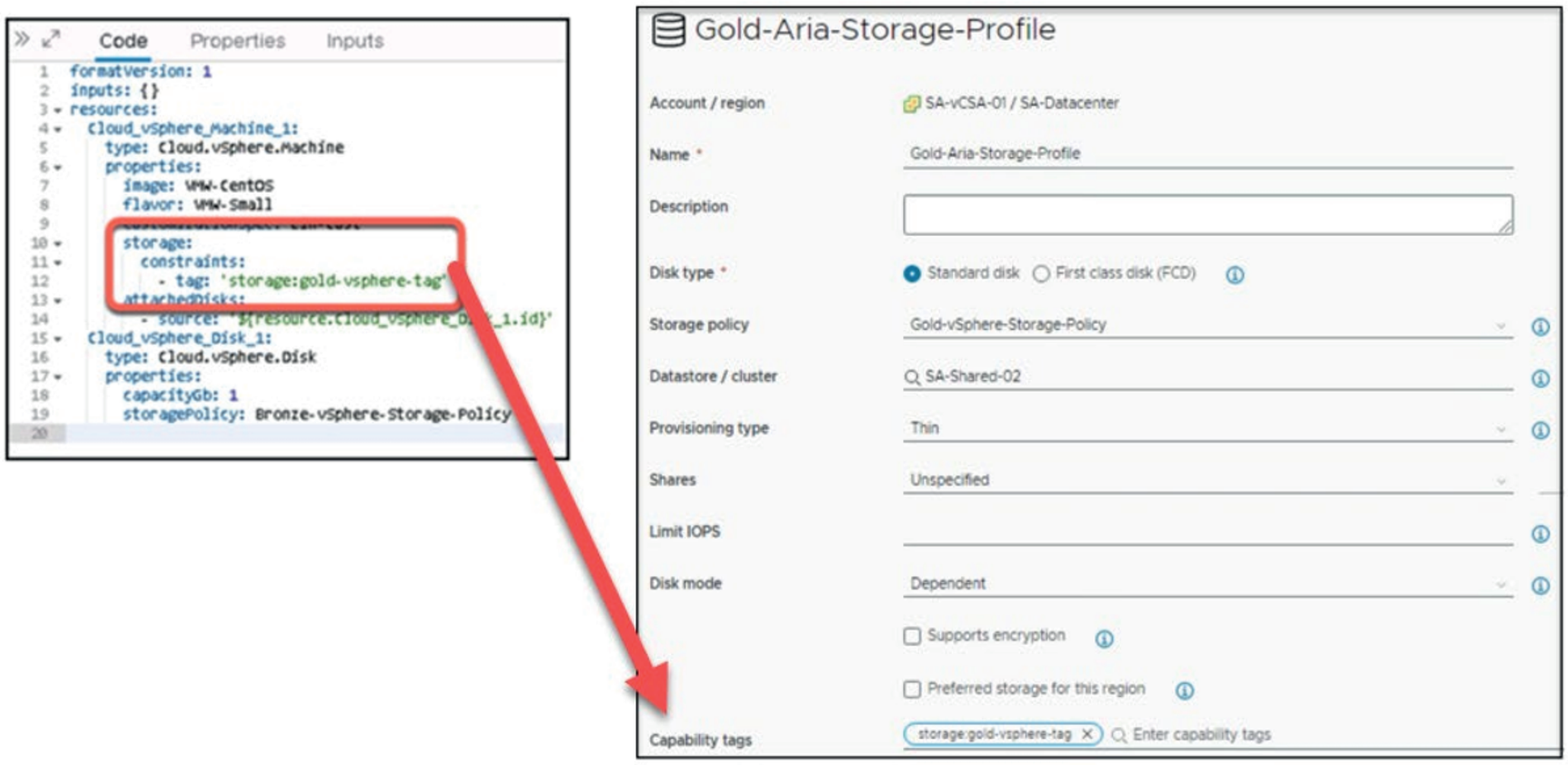


When possible, VMware Aria Automation uses the storage profile that is marked as the preferred storage for the region.

The preferred storage profile is overridden by a storage constraint tag on a machine in a VMware Aria Automation template. Another way of overriding the preferred storage profile is by specifying the `storagePolicy` property on a disk in VMware Aria Automation Templates.

8-10 Storage Constraint Tag on Machines

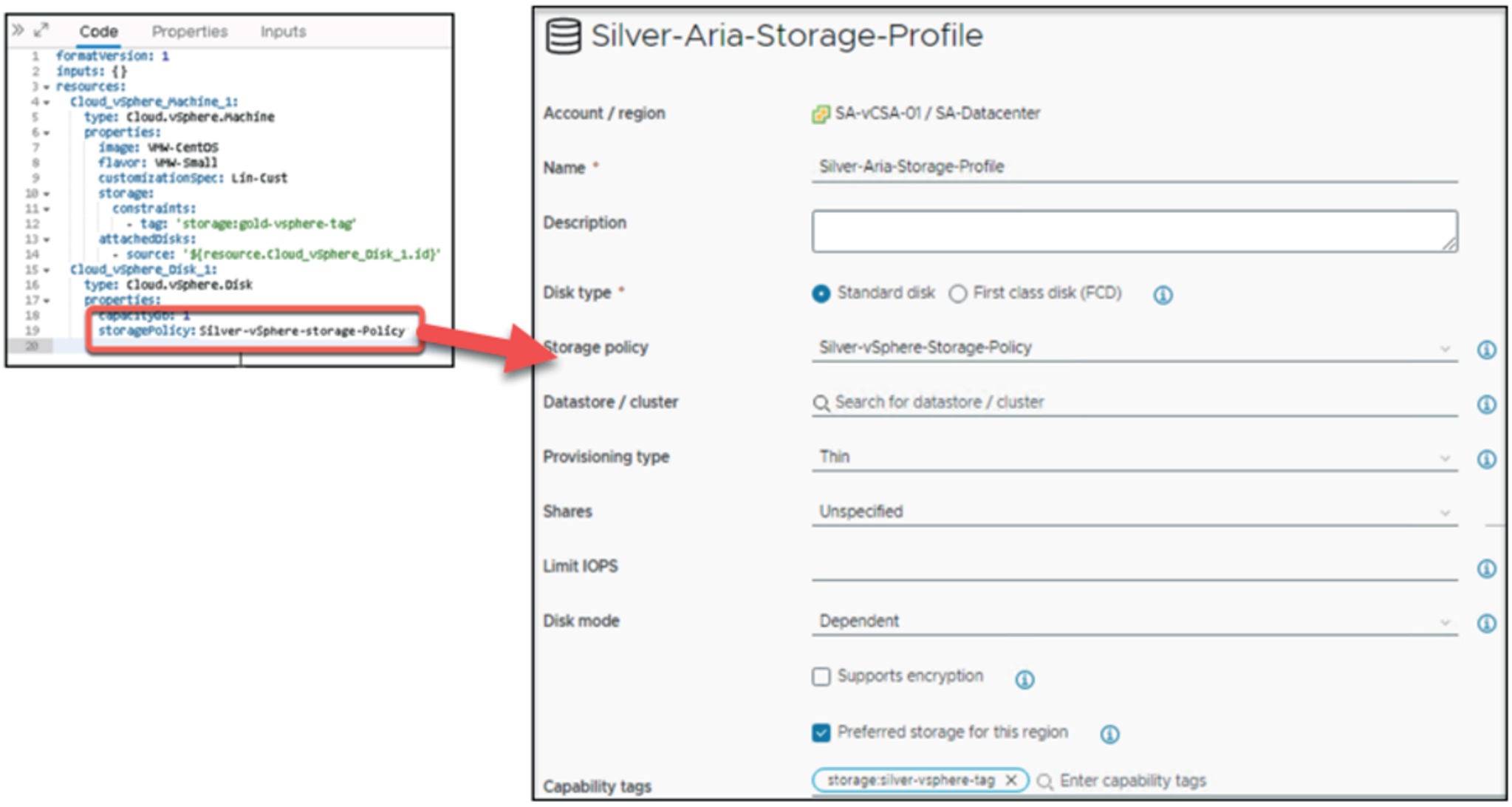
You can use a storage constraint tag to specify the storage location for the disk of a machine.



If you specify a storage location by setting a storage constraint tag on a machine, then the base disk and all the other disks are placed on that storage. However, you can override the storage location of the secondary disks by specifying the `storagePolicy` property.

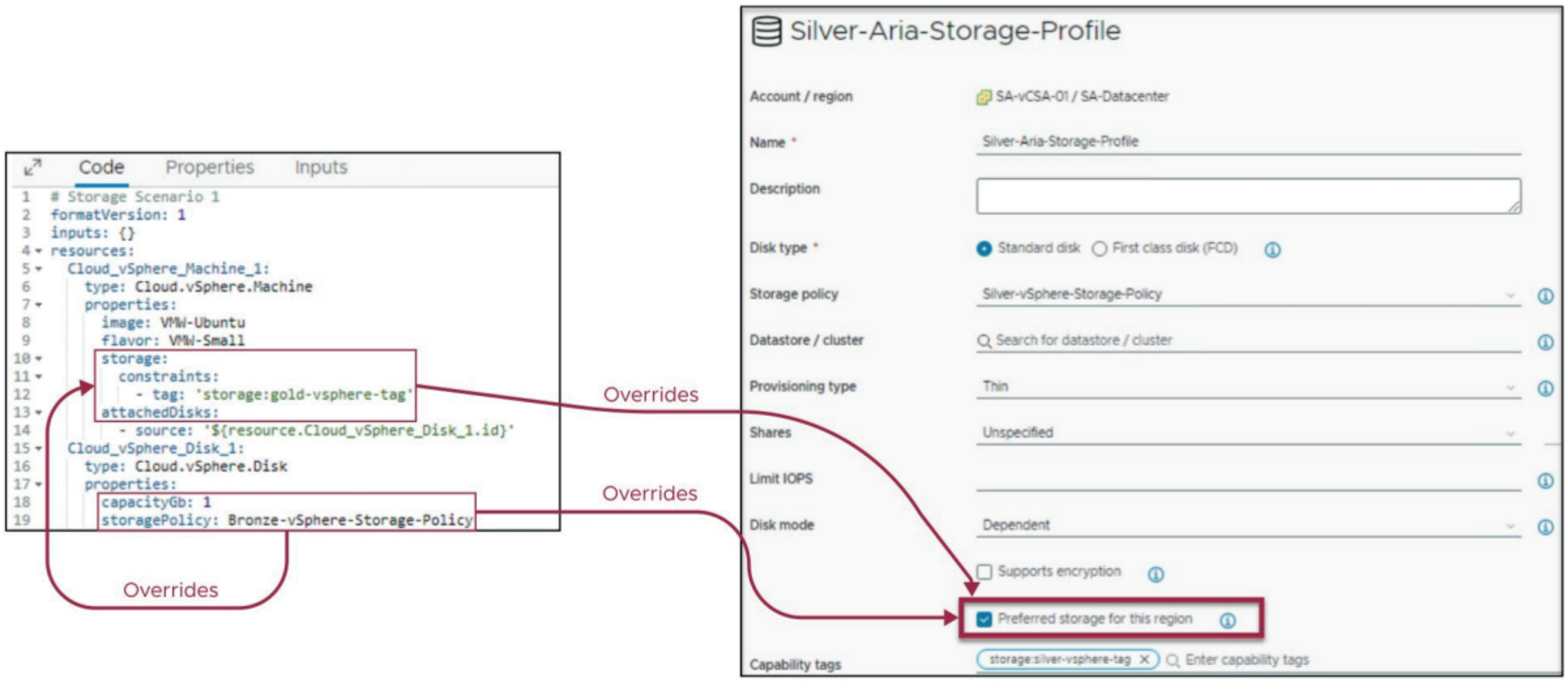
8-11 Storage Policy on a Disk

You can specify the storage location per disk by setting `storagePolicy` or constraints on a disk resource.



8-12 Order of Precedence

You must understand how different techniques for specifying storage locations relate to one another in terms of the order of precedence. You can use multiple techniques to specify storage locations. However, certain techniques override others in order of precedence.



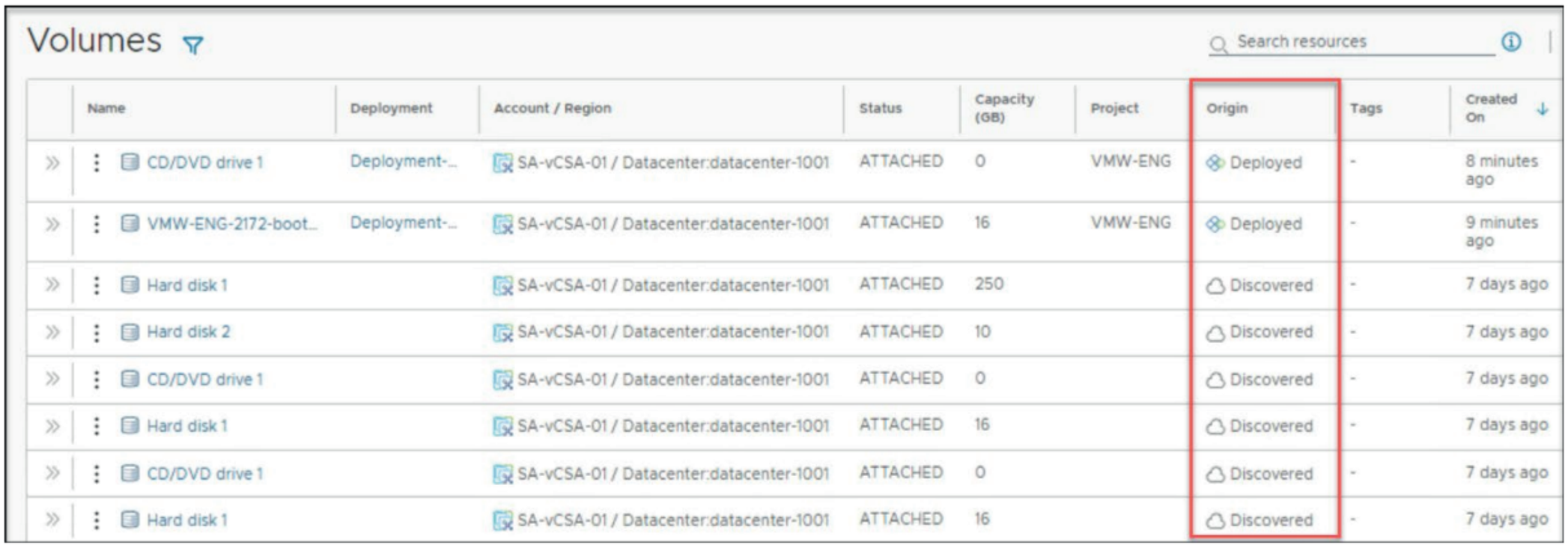
A `storagePolicy` property on a disk overrides a storage constraint tag on a machine.

A storage constraint tag on a machine overrides the preferred VMware Aria Automation storage profile.

A `storagePolicy` property on a disk overrides the preferred VMware Aria Automation storage profile.

8-13 About Volumes

A volume is a logical drive that was either discovered through data collection on cloud accounts or is deployed with workloads that were provisioned by VMware Aria Automation Assembler. A volume is another item in VMware Aria Automation storage management.

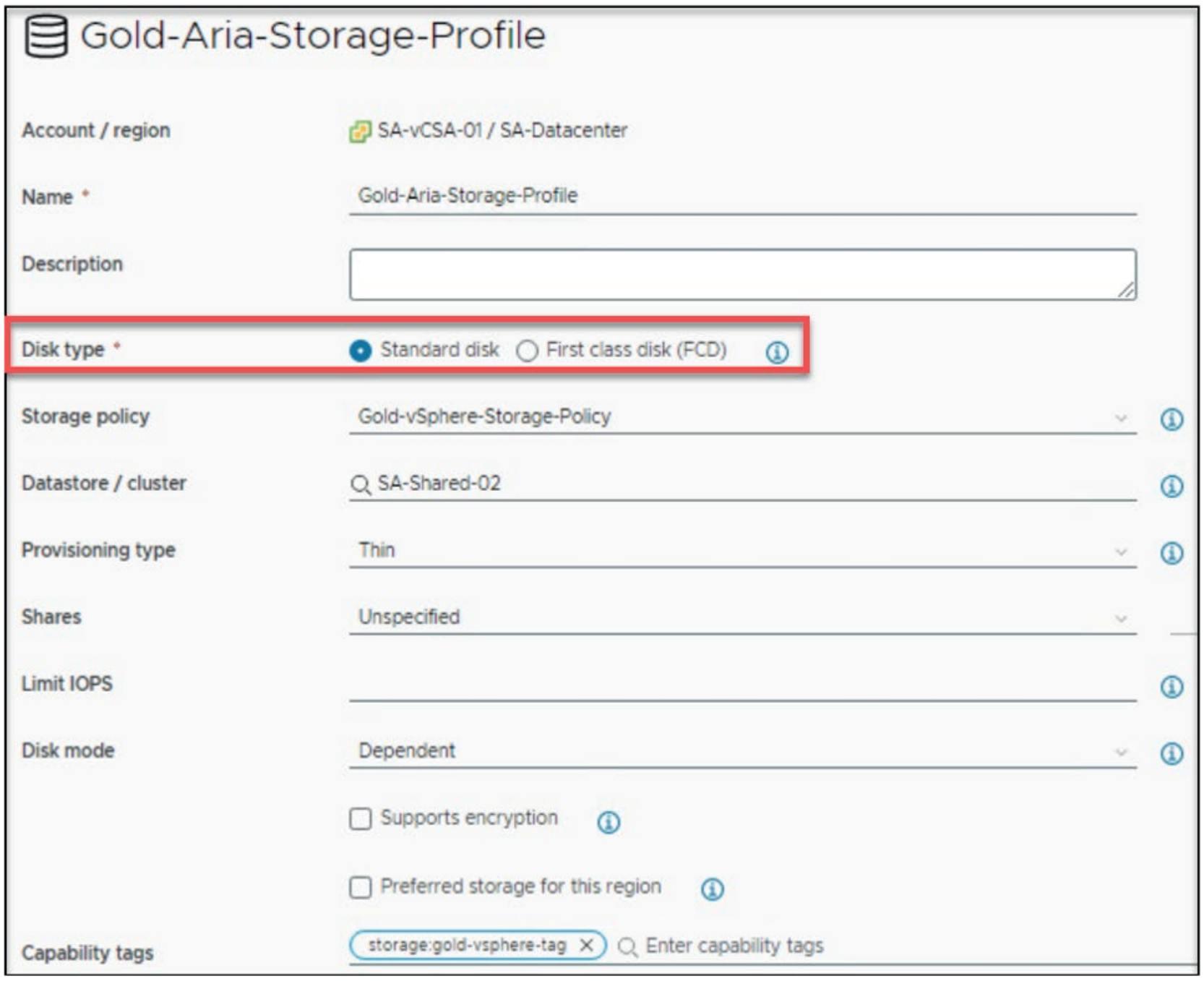


You can see a list of all volumes by selecting **Resources** > **Deployments** > **Volumes** in the VMware Aria Automation console.

8-14 About Standard Disks

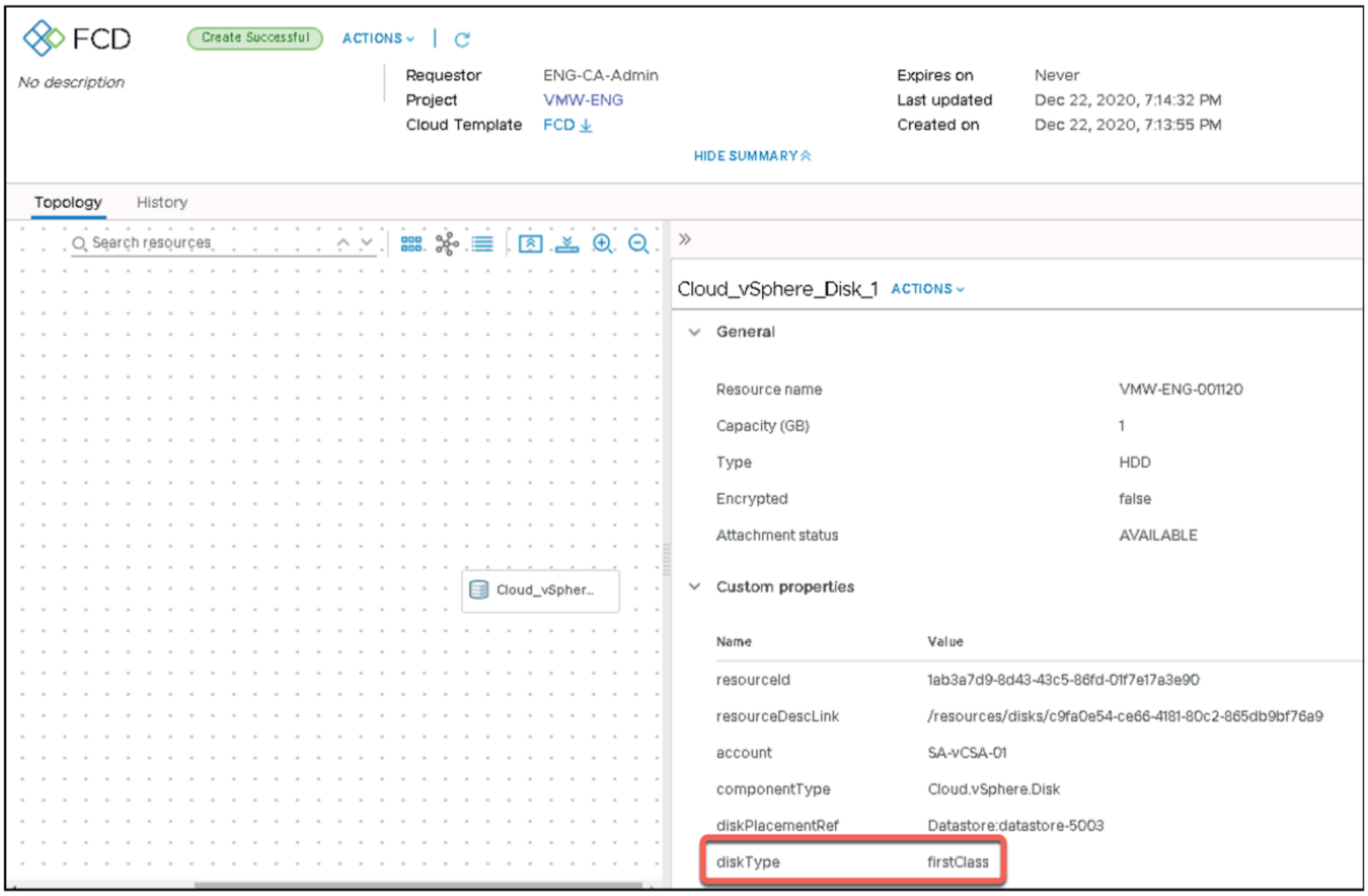
VMware Aria Automation storage profiles support standard disks and first class disks (FCDs).

Standard disks are dependent on the machine in which they exist. If you delete the machine, the standard disk is also deleted.



8-15 About First Class Disks

FCDs are independent of a specific machine. If you delete a VM with an FCD attached to it, the VM and all its standard disks are deleted, but the FCDs are not deleted.



First class disks (FCDs) are also known by other names:

- Improved Virtual Disks
- Enhanced Virtual Disks
- Managed Virtual Disks

If you take a snapshot of a VM, the snapshot captures the state of all (non-independent) standard disks. Conversely, you can take snapshots of individual FCDs independent of any VM to which the FCD is attached.

FCDs can be used for various use cases:

- Provide persistent storage to containers
- Enable testing using data generated on a production VM without working with (and potentially compromising) the production data

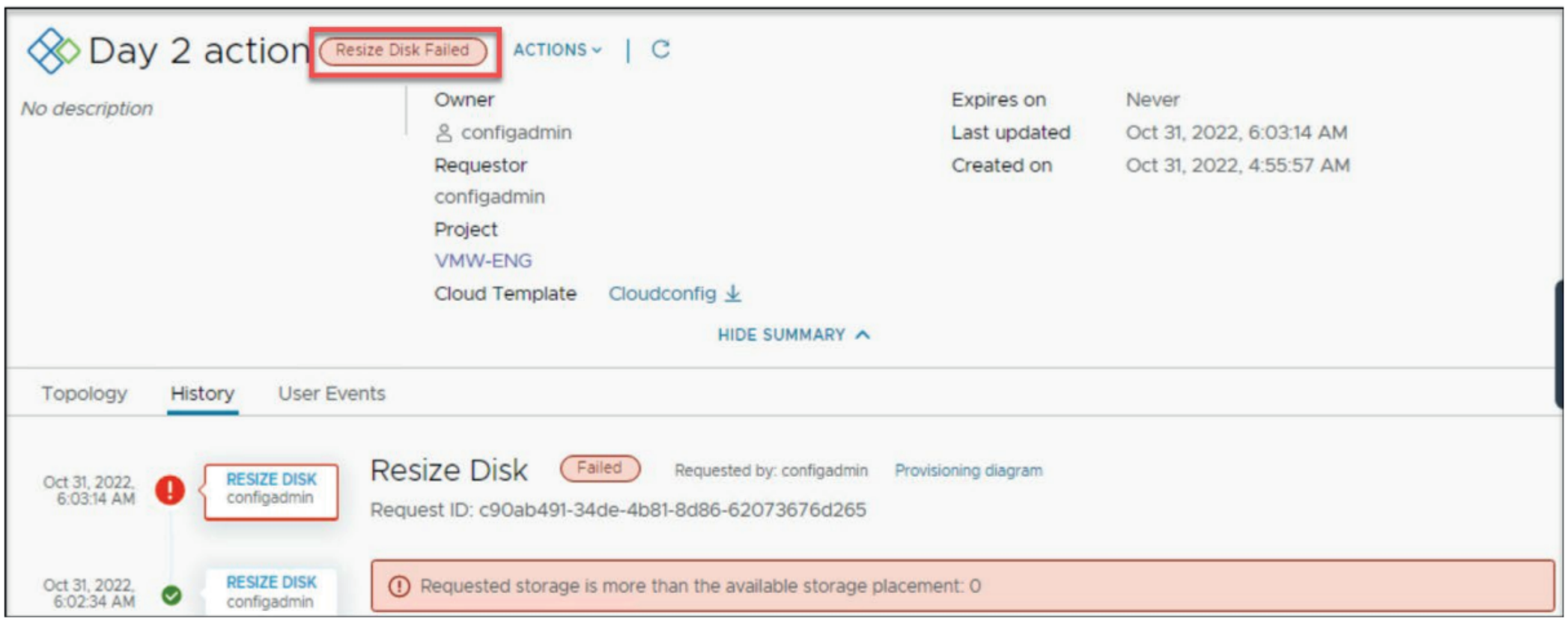
You create a production VM, attach an FCD to the VM, and put production data into the FCD. When you want to perform testing, you can take a snapshot of the FCD, create another FCD from that snapshot, attach the duplicate FCD to a Test/Dev VM, and safely perform your testing using the Test/Dev VM.

For now, FCDs are available for vSphere VMs only.

The VMware Aria Automation REST API provides numerous operations that can be performed on FCDs. For information about creating and using an FCD with the REST API, see *vRealize Automation 8.10 API Programming Guide* at https://developer.vmware.com/docs/16548/vrealize-automation-8-10-api-programming-guide.

8-16 Storage Limits

When you deploy a VMware Aria Automation template that includes any type of disks, or when you run a relevant day 2 action, the cloud zone storage limits that you configured for each project are evaluated. Your deployment fails if the disk size request exceeds those limits. The storage limits are applied to FCDs, so FCDs are now evaluated against the storage limit set by the user.



For more information about the capabilities and limitations of FCDs, see the section about what can you do with FCD storage in *Using and Managing Cloud Assembly* at https://docs.vmware.com/en/vRealize-Automation/index.html.

8-17 Lab 19: Using Storage Profiles

Explore storage configuration in VMware Aria Automation:

1. Explore the Current Storage Configuration in VMware Aria Automation
2. Explore the Current Storage Configuration in vSphere
3. Investigate Storage Scenario 1
4. Investigate Storage Scenario 2
5. Investigate Storage Scenario 3
6. (Optional) Investigate Storage Scenario 4

8-18 Lab 20: First Class Disks as a Service

Create a VMware Aria Automation template to deploy a first class disk as a service:

1. Deploy a Standard Disk
2. Change the Preferred Storage Profile
3. Create a VMware Aria Automation Template That Deploys a First Class Disk
4. Deploy a First Class Disk from the VMware Aria Automation Template
5. Attach the First Class Disk to a Production VM
6. Use the First Class Disk in CentOS in the Production VM
7. Attach the First Class Disk to a Test/Dev VM
8. Use the First Class Disk in CentOS in the Test/Dev VM
9. Delete the First Class Disk
10. Change the Preferred Storage Profile to the Silver Aria Automation Storage Profile

8-19 Review of Learner Objectives

- Create a VMware Aria Automation storage profile
- Use a VMware Aria Automation storage profile in VMware Aria Automation Templates
- Describe volumes
- Explain how to deploy a first class disk using VMware Aria Automation Templates

8-20 Key Points

- Tags can be used to manage, categorize, and match storage resources.
- Storage can be managed with VMware Aria Automation storage profiles.
- VMware Aria Automation supports standard disks and first class disks.

Questions?

Module 9

Integrating NSX with VMware Aria Automation

9-2 Importance

Integrating NSX with VMware Aria Automation enables access to improved networking capabilities. Using NSX, you can design systems with advanced networking and security features that deliver high-quality services and applications.

9-3 Module Lessons

1. Introduction to NSX
2. NSX Integration

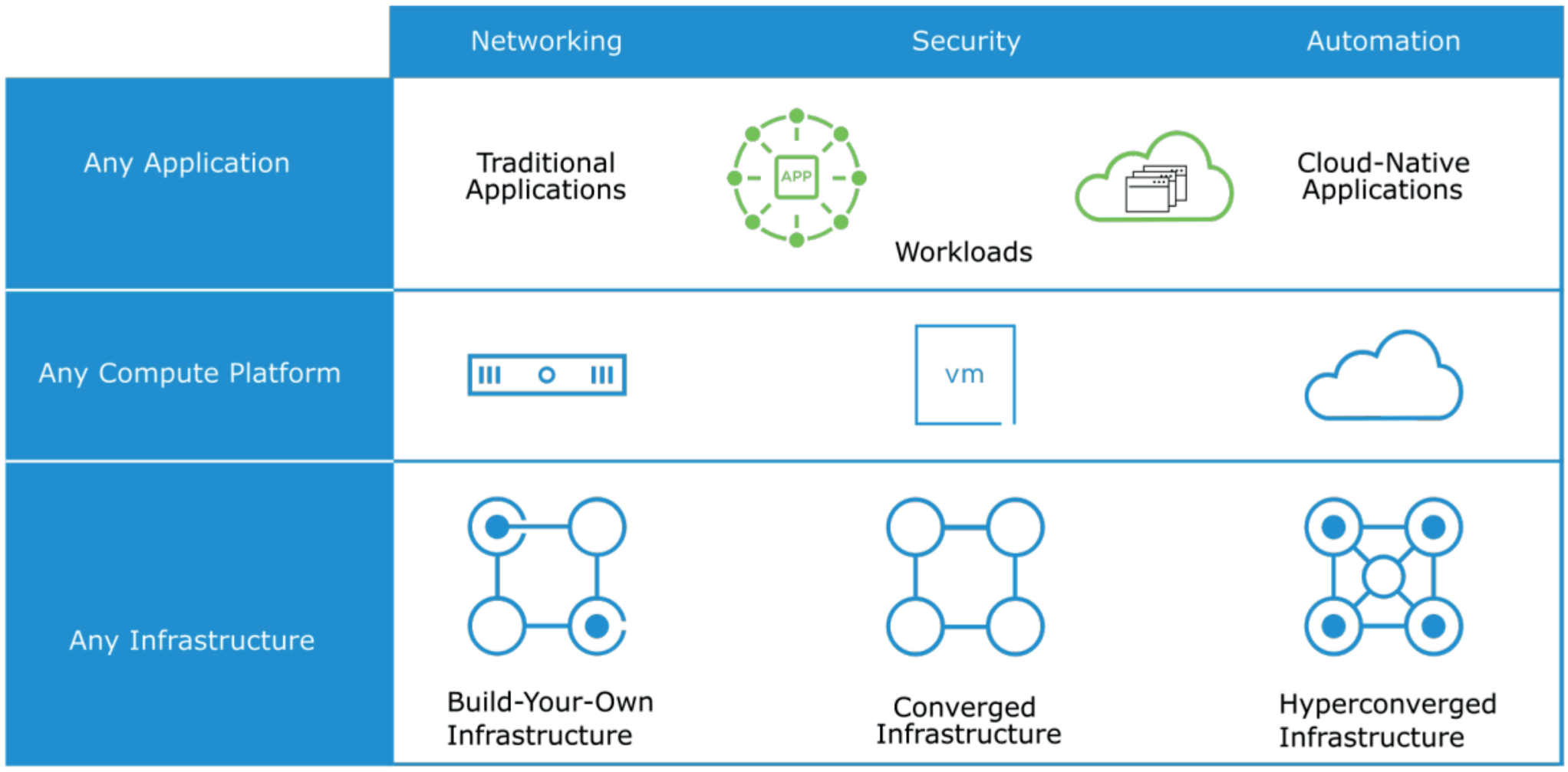
9-4 Lesson 1: Introduction to NSX

9-5 Learner Objectives

- Describe how NSX works
- List the capabilities and use cases of NSX
- Describe the NSX architecture and components

9-6 NSX: Introduction

NSX provides consistent networking and security across the entire IT environment. NSX runs on any infrastructure, any platform, and any application.



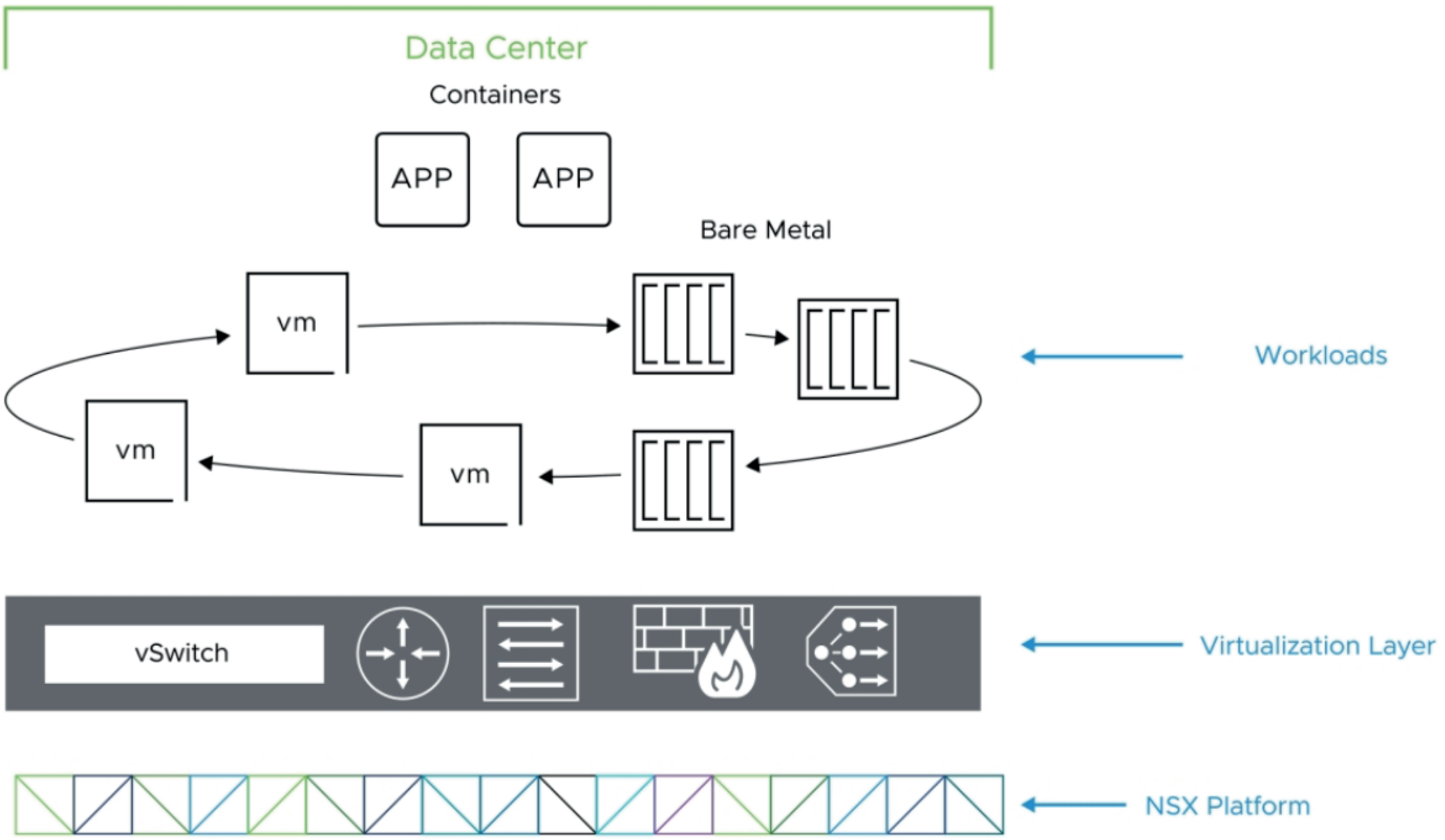
NSX is the next-generation product that provides a scalable network virtualization and micro-segmentation platform for cloud environments, container deployments, and native workloads running in public cloud environments.

NSX focuses on providing networking, security, automation, and operational simplicity for emerging application frameworks and architectures that have heterogeneous endpoint environments and technology stacks.

NSX supports cloud-native applications, bare-metal workloads, ESXi hypervisors, public clouds, and multiple clouds.

9-7 NSX: Workload Objects

You can provision and manage networks independent of the underlying hardware, similar to the operational model of VMs. NSX reproduces the entire network model in software.



You can provision and manage networks independent of the underlying hardware, similar to the operational model of VMs. NSX reproduces the entire network model in software. NSX enables network topologies, from simple to complex multitier networks, to be created and provisioned in seconds.

Data center operators can achieve levels of agility, security, and economics that were previously unreachable when the data center network was tied solely to physical hardware components.

NSX provides a complete set of logical networking and security capabilities and services, including logical switching, routing, firewalling, load balancing, VPN, and monitoring.

These services are provisioned in virtual networks through cloud management platforms that use NSX APIs.

Virtual networks are deployed in a nondisruptive way over any existing networking hardware and can extend across data centers, public and private clouds, container platforms, and bare-metal servers.

9-8 NSX: Use Cases

You can use NSX for the following purposes:

- Security
- Multicloud networking
- Automation
- Cloud-native applications

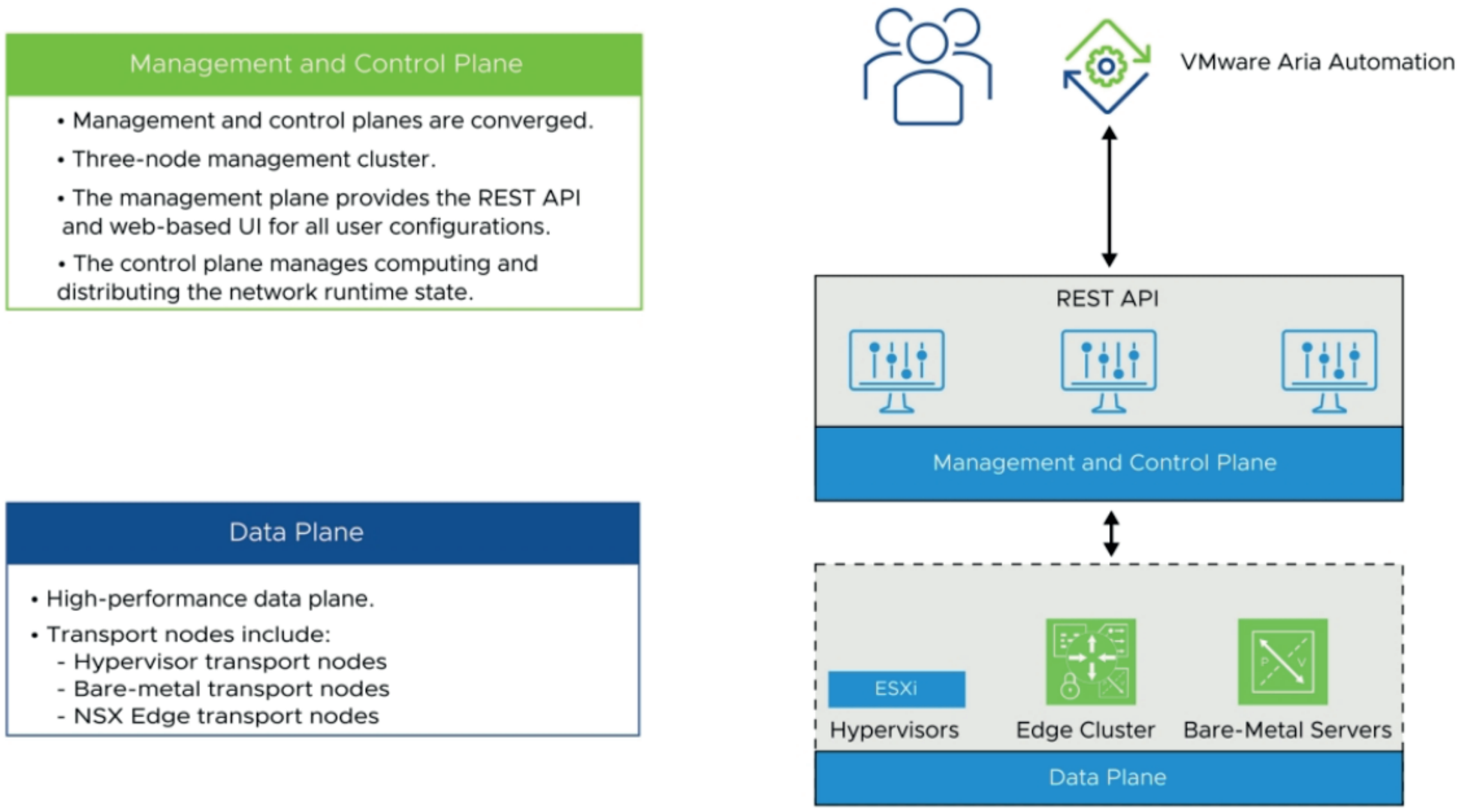


You can use NSX for the following purposes:

- Security: Delivers application-centric security at the workload level to prevent the lateral spread of threats
- Multicloud networking: Brings networking and security consistency across varied sites and streamlines multicloud operations
- Automation: Enables faster deployment through automation by reducing manual, error-prone tasks
- Cloud-native applications: Enables native networking and security for containerized workloads across application frameworks

9-9 NSX: Architecture

The three main elements of NSX architecture are the management, control, and data planes. The separation of the architecture into these planes enables it to expand and scale without affecting workloads.



The three main elements of NSX architecture are the management, control, and data planes. The separation of the architecture into these planes enables it to expand and scale without affecting workloads. Each plane has its own components:

- Management plane: The management plane is designed with advanced clustering technology, which enables the platform to process large-scale concurrent API requests. NSX Manager provides the REST API and a web-based UI interface entry point for all user configurations.
- Control plane: The control plane includes a three-node controller cluster, which is responsible for computing and distributing the runtime virtual networking and security state of the NSX environment.
  - The control plane is separated to a central control plane and a local control plane. This separation significantly simplifies the work of the central control plane and enables the platform to extend and scale for various endpoints.
  - With NSX 2.4 and later, the management plane and control plane have converged.
  - Each manager node in NSX is an appliance with converged functions, including manager, control, and policy.

- Data plane: The data plane includes a group of ESXi hosts, bare-metal servers and NSX Edge nodes.
  - The group of servers and edge devices prepared for NSX are called transport nodes.
  - Transport nodes are responsible for the distributed forwarding of network traffic.
  - The ESXi hosts managed by VMware vCenter use vSphere Distributed Switch (VDS) for the traffic forwarding.

All operations are performed from the management plane. These operations include create, read, update, and delete (CRUD).

9-10 NSX: Capabilities



Any Compute

- ESXi Hypervisor
- VM
- Container
- Bare Metal



Distributed Services

- Distributed routing and firewall services on ESXi



Scale

- Clustered management and control plane
- Multitenant Edge

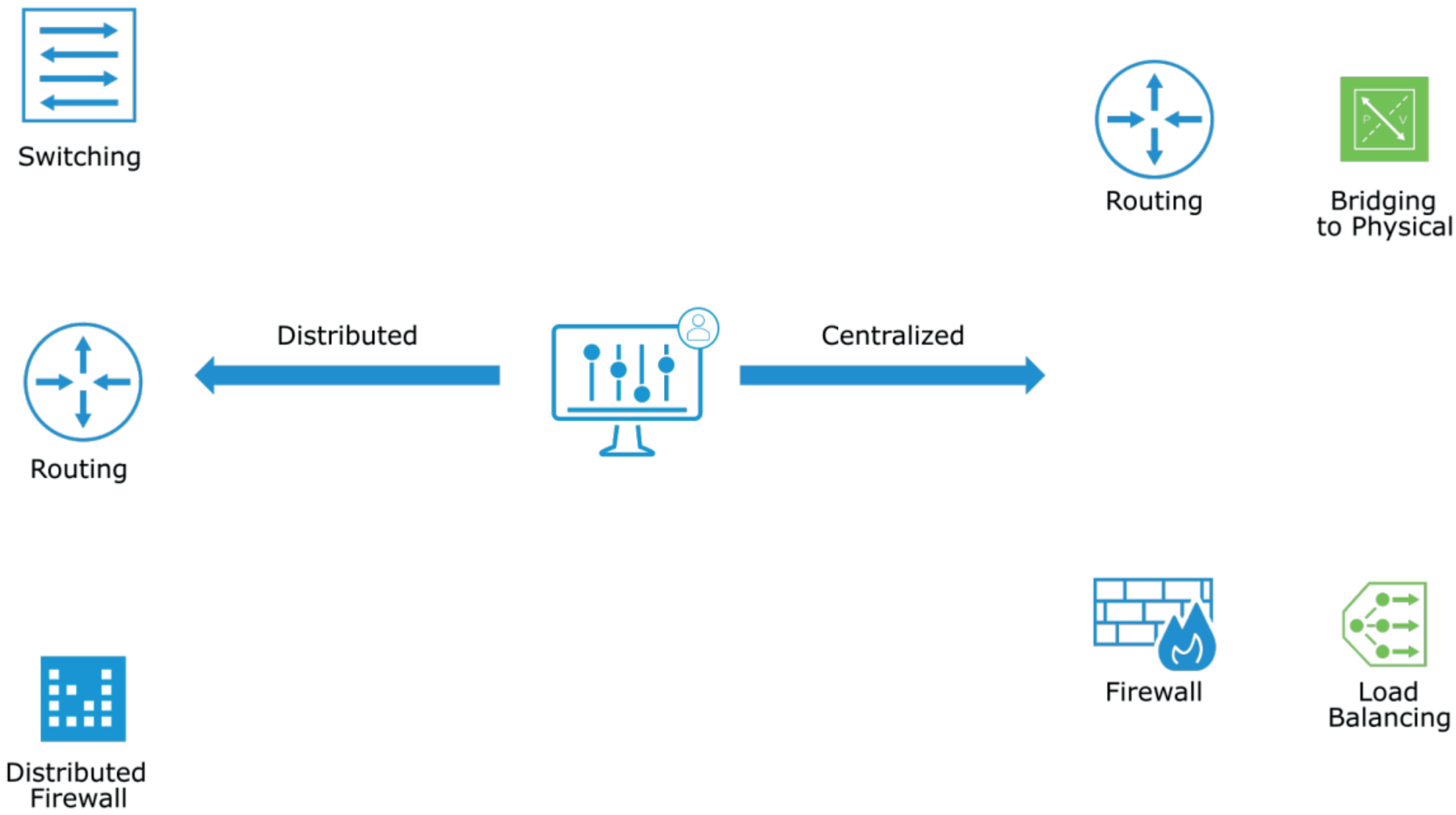


Availability

- Management and control plane HA
- Edge HA

9-11 Network and Security Services

Some components in NSX are distributed, and some components are centralized.



The distributed services in NSX run on hypervisors and are used for east-west traffic, for example, network traffic between two ESXi hosts.

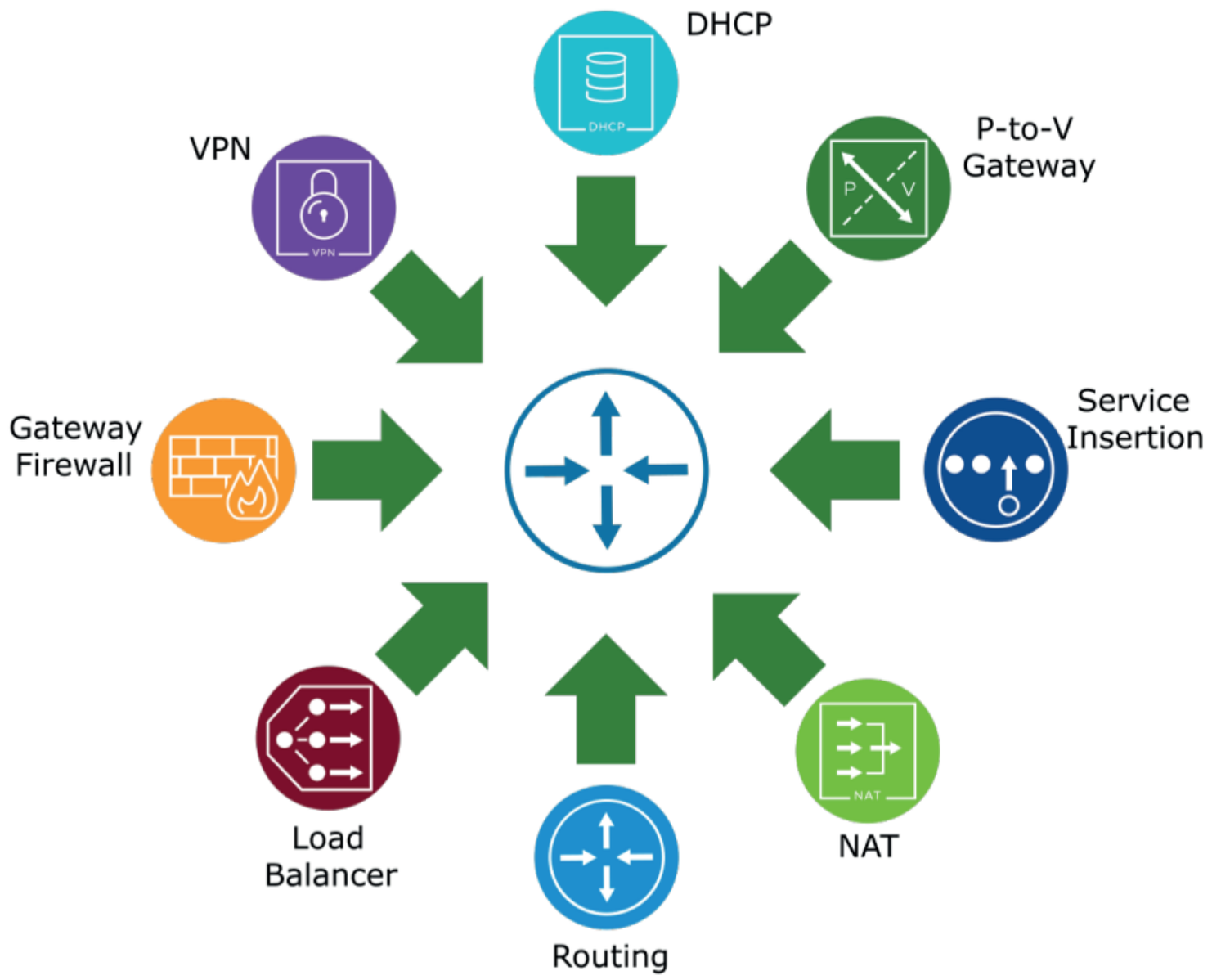
Centralized services cannot be distributed and require an NSX Edge node. Centralized services are used for north-south traffic. For example, a VM on an ESXi host tries to communicate with the external web server external to the data center.

9-12 NSX Edge Nodes

The NSX Edge nodes are service appliances dedicated to running centralized network services that cannot be distributed to the hypervisors.

Features of NSX Edge nodes:

- Connectivity to the physical infrastructure (Tier-0 gateway uplink)
- NAT
- DHCP server
- Edge firewall
- Load balancer



NSX Edge is a component with the functional goal to provide computational power to deliver the IP address routing and the IP address services functions.

The NSX Edge cluster provides high availability in active-active and active-passive modes.

The NSX Edge node supports the following form factors:

- VM on an ESXi host
- Bare-metal node

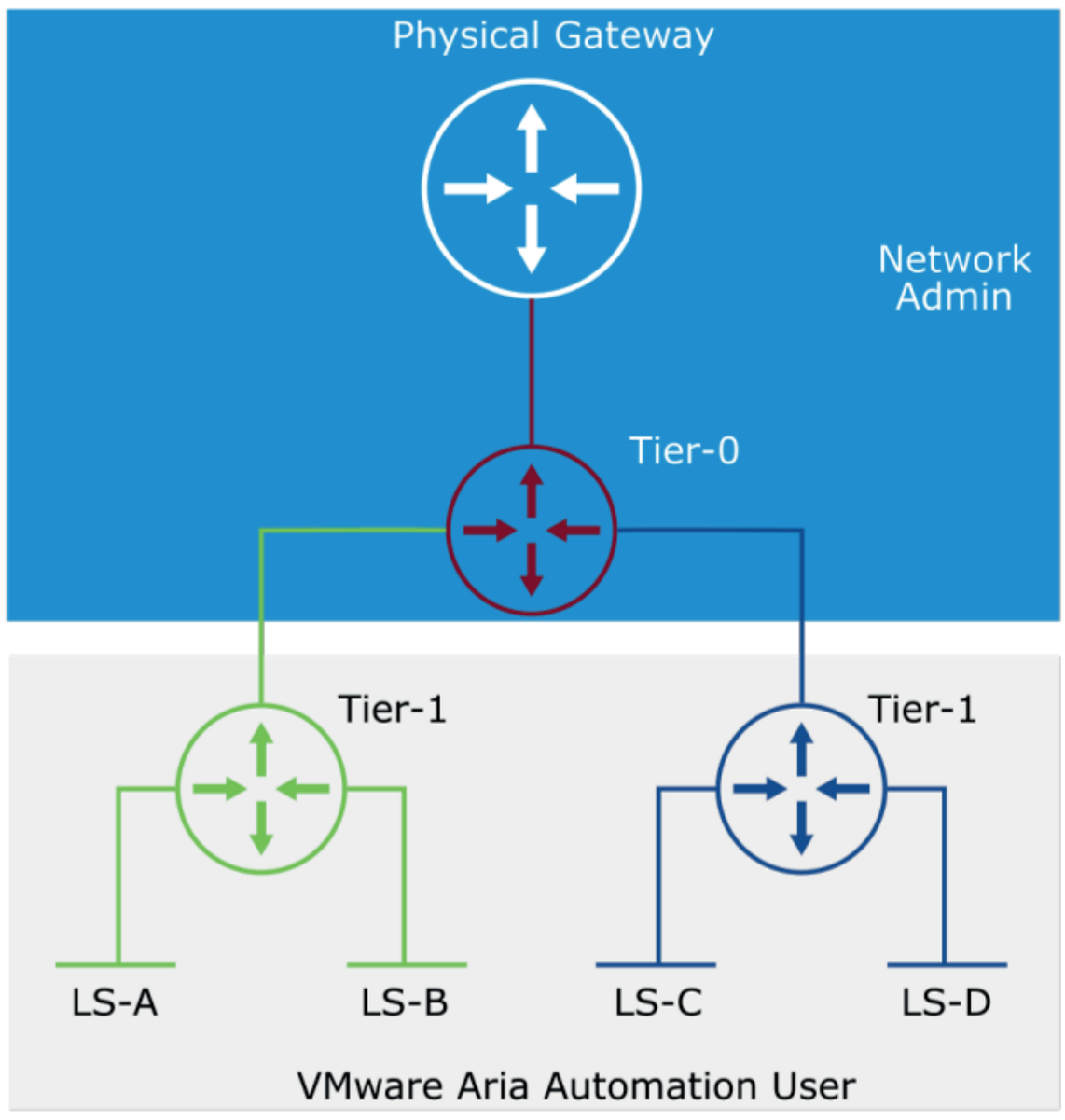
9-13 NSX Tiered Routing

Tier-0 gateway:

- Created and configured by the NSX administrator
- Offers north-south gateway service to the physical network
- Supports dynamic routing (BGP and OSPF)
- Requires an NSX Edge cluster

Tier-1 gateway:

- Is created on demand by VMware Aria Automation
- Offers east-west gateway service
- Is connected to the Tier-0 gateway
- Requires an NSX Edge cluster, only if centralized services are used



The Tier-0 logical gateway is a top-tier gateway. The Tier-0 logical gateway supports static routing and dynamic routing (BGP and OSPF) with physical gateways.

Tier-1 gateways are provisioned on demand when a user from VMware Aria Automation requests a catalog item that includes outbound or routed network profiles.

When VMware Aria Automation is used with NSX, the Tier-0 gateway must be deployed as a prerequisite for north-south traffic.

The Tier-1 logical gateway cannot connect to the physical gateway directly. It has to connect to a Tier-0 logical gateway to provide north-south connectivity to the subnets attached to it:

- The NSX Controller instances are responsible for advertising routes between Tier-1 and Tier-0 gateways.
- No routing protocol or control VM is required.
- BGP and OSPF dynamic routing protocols are supported between the Tier-0 gateway and the physical gateway.

9-14 Review of Learner Objectives

- Describe how NSX works
- List the capabilities and use cases of NSX
- Describe the NSX architecture and components

9-15 Lesson 2: NSX Integration

9-16 Learner Objectives

- Integrate NSX with VMware Aria Automation
- List the supported network profiles in VMware Aria Automation
- Identify the network and security options that are available in the design canvas
- Use NSX components to design a multitier application with VMware Aria Automation templates

9-17 NSX: Cloud Accounts

To integrate NSX with VMware Aria Automation, create a cloud account:

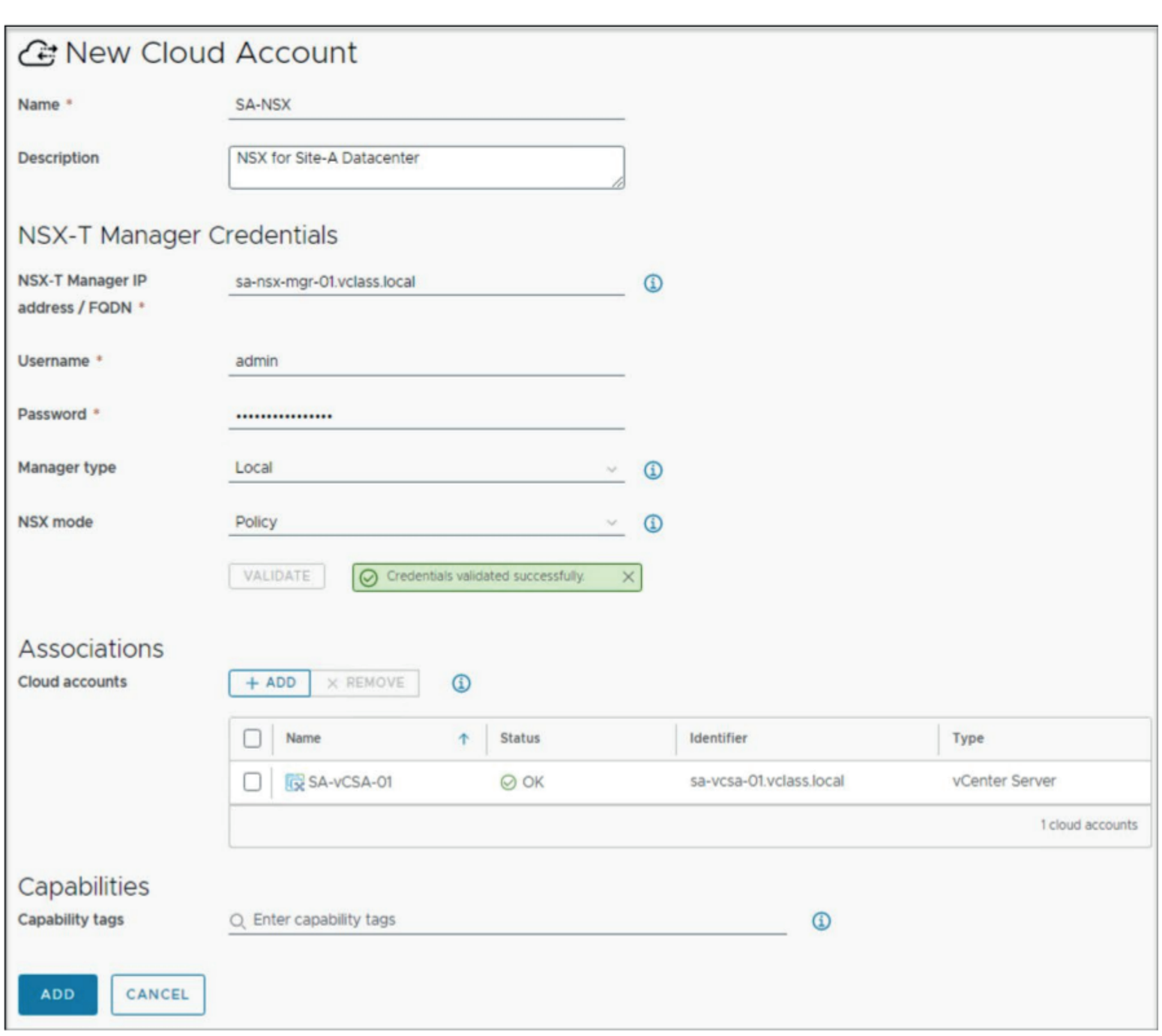
1 Log in to the VMware Aria Automation console as a VMware Aria Automation Assembler Administrator.

2 Select **Infrastructure** > **Connections** > **Cloud Accounts**.

3 From the **ADD CLOUD ACCOUNT** drop-down menu, select **NSX-T Manager**.

4 Select **NSX Mode** and **Manger type**.

5 Associate the vCenter instances.



If you want to add tags to support a tagging strategy, enter the capability tags.

An NSX cloud account can be associated to one or more VMware vCenter cloud accounts from the NSX policy manager console.

For the Manager type, you can select:

- **Local**: The option defines a traditional NSX cloud account that can be associated to one or more vSphere cloud accounts.
- **Global**: The Global setting refers to the NSX federation capabilities, including global network segments. Only NSX cloud accounts with the Global setting support NSX federation.

For the NSX mode, you can select from:

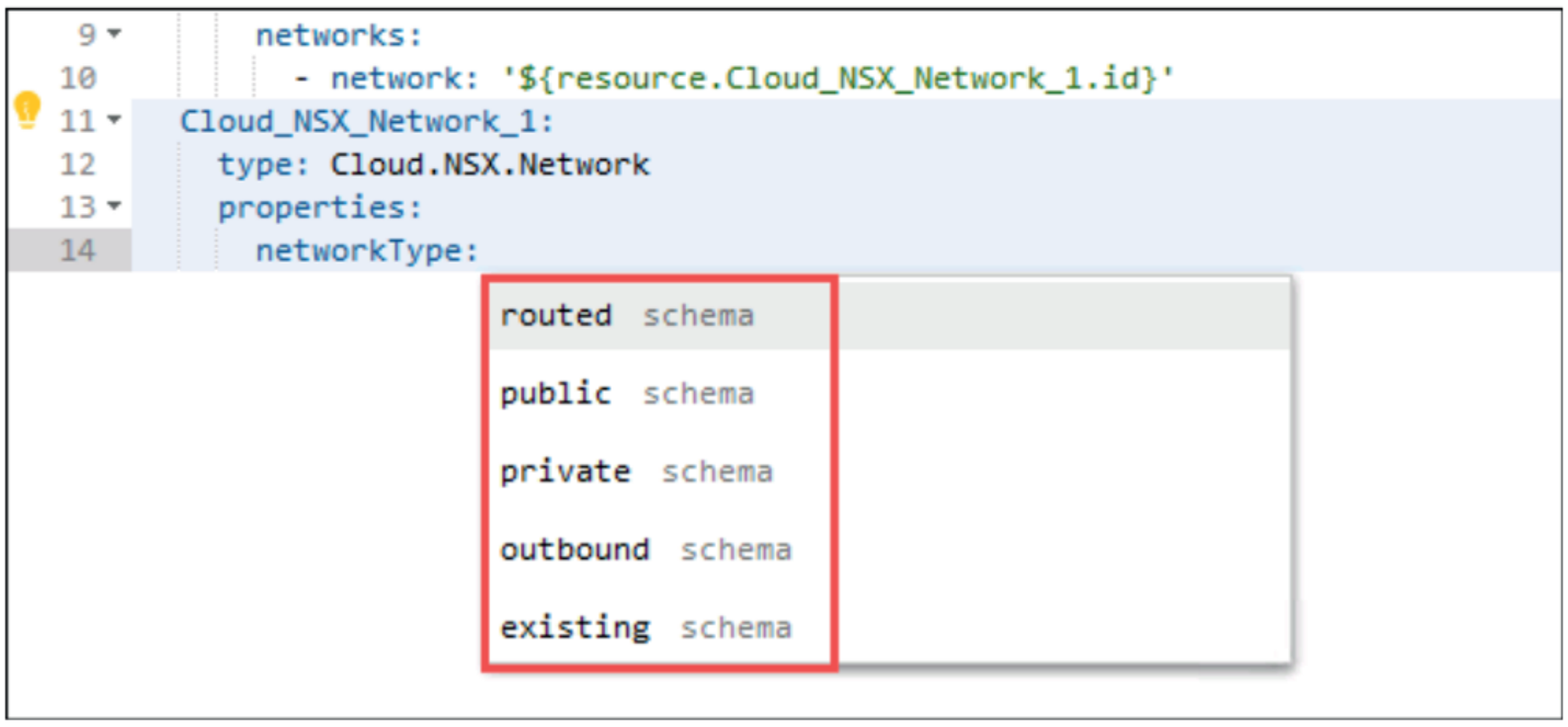
- **Policy** (default): Supported with NSX v3.0 and later. The option is recommended for greenfield environment, and it enables VMware Aria Automation to use the additional capabilities available in the NSX Policy API.
- **Manager** (to be deprecated): Existing NSX endpoints or cloud accounts that are upgraded from an earlier version of VMware Aria Automation that did not provide a Policy option are treated as Manager mode NSX cloud accounts.

For more information about NSX modes, see the section on creating Create an NSX-T cloud account in vRealize Automation in *Using and Managing Cloud Assembly* at https://docs.vmware.com/en/vRealize-Automation/index.html.

9-18 Network Profiles

Network profiles control placement decisions to select a network during virtual machine provisioning. They also control the level of isolation for a deployed workload:

- Network profiles use the default IP Address Management (IPAM) in VMware Aria Automation.
- Network profiles are used in VMware Aria Automation templates.
- You can create the following network types:
  - Routed
  - Public
  - Private
  - Outbound
  - Existing



Network profiles configure network interfaces when VMs are provisioned. They also specify the configuration of the NSX Edge devices that must be created when multiple machines are provisioned.

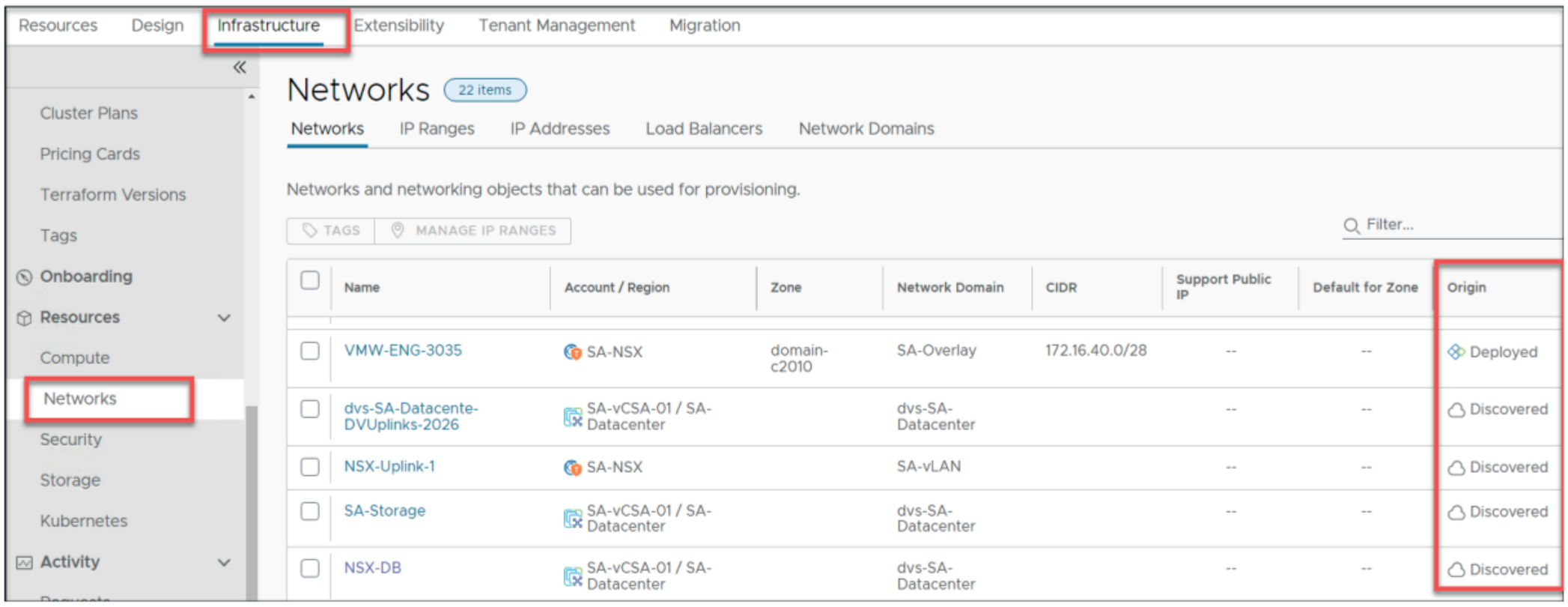
Network profiles are created on the **Infrastructure** tab. Network profiles use the `networkType` property in the VMware Aria Automation template.

Network profiles also support third-party IP Address Management (IPAM) providers, such as Infoblox.

When you configure a network profile for IPAM, the provisioned machines can obtain the IP address data, and related information such as DNS and gateway, from the configured IPAM solution.

9-19 Discovered Networks

Networks are discovered from vSphere and associated NSX cloud accounts. Click a network to define its attributes.

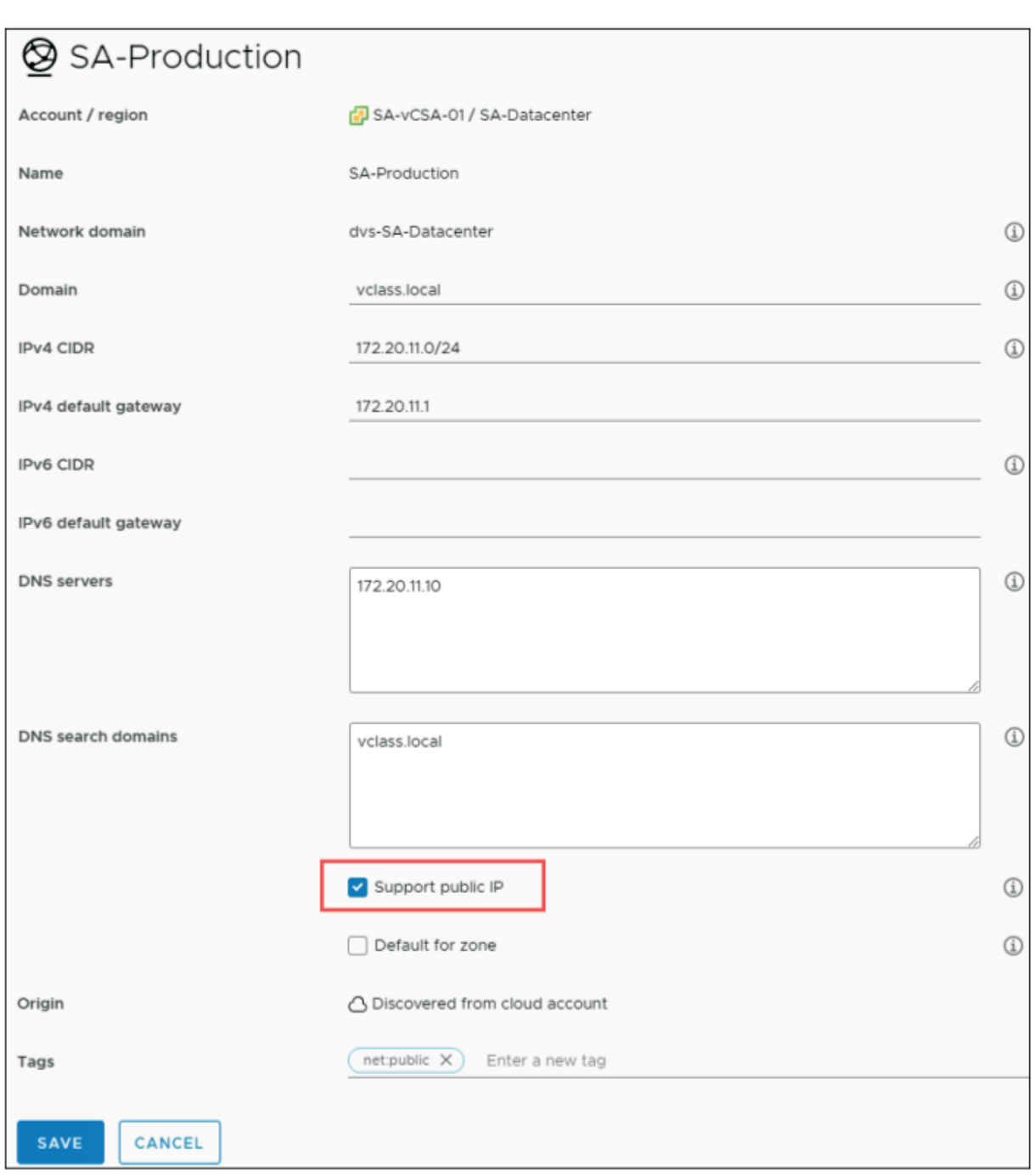


You can define CIDR, default gateway, and DNS servers for the networks. Networks can be set as default for the zone and enable support for the public IP address (external network).

9-20 Public Network

Configure one of the vSphere or NSX port groups as public:

- Use case: Allow direct external access.
- Select the **Support public IP** check box.
- This configuration is used to match `networkType: public` in the VMware Aria Automation template.
- The VM is connected directly to the public network.
- Public networks are also used when other network profiles need external access.



Network components in the VMware Aria Automation template that have the **network type: public** property are matched to networks that are flagged as public.

Select the **Default for zone** check box to flag the network as a default network for the cloud zone. During the VMware Aria Automation template deployment, default networks are preferred over other networks.

9-21 Network Profile: Existing

Use case: Use the existing discovered networks to deploy VMware Aria Automation templates.

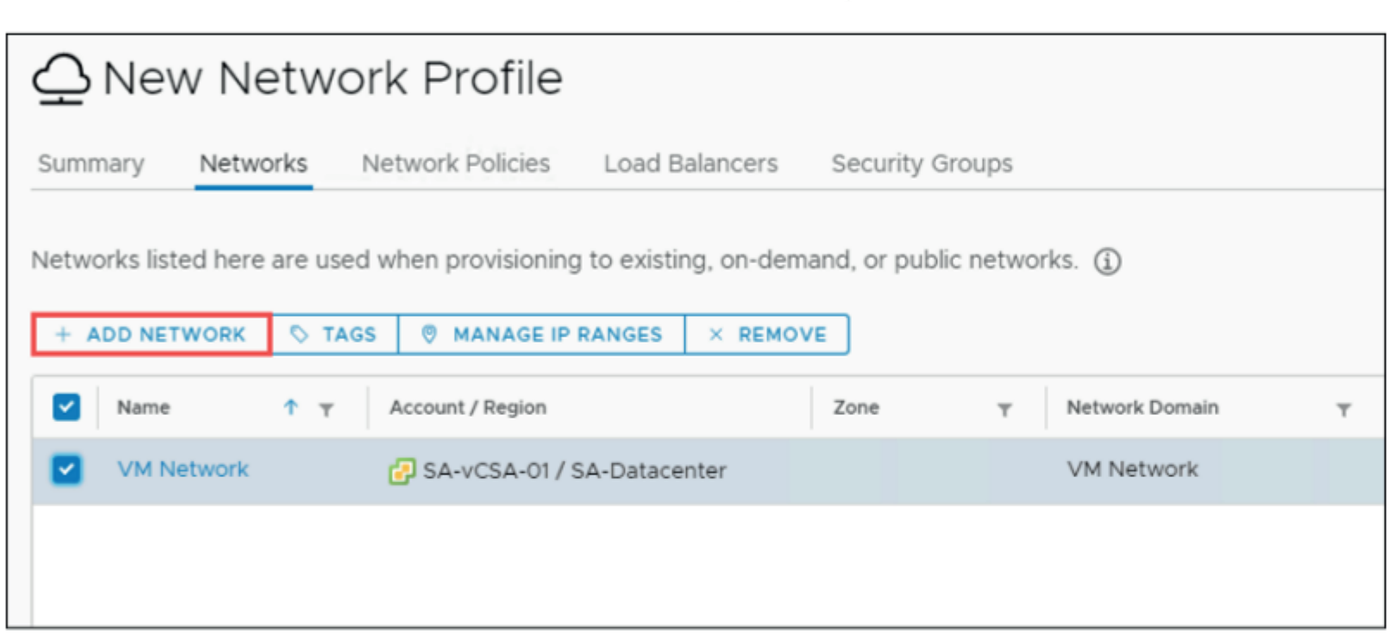
To create a network profile:

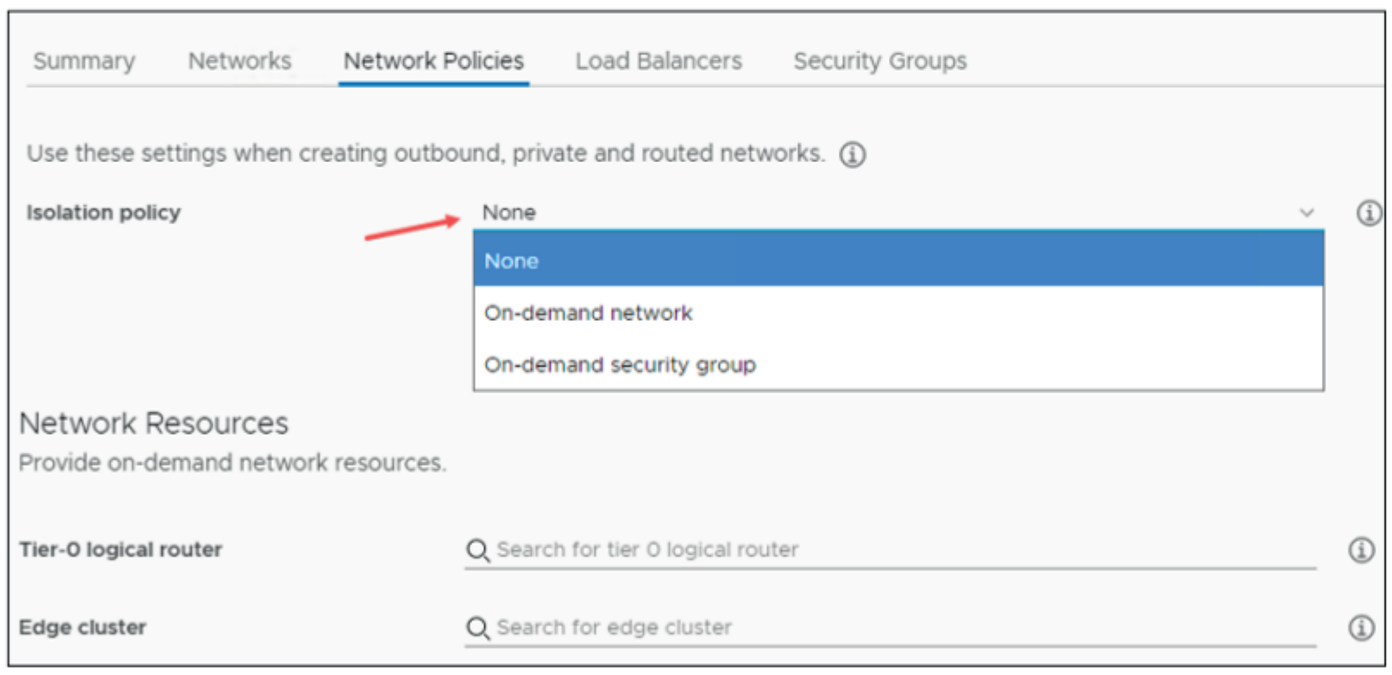
1 Navigate to **Infrastructure** > **Configure** > **Network Profiles**.

2 Click **New Network Profile**.

3 Click the **Networks** tab to add an existing network.

4 Select **None** as the isolation policy.





For example, you can add a vSphere port group or an NSX segment that VMware Aria Automation has already discovered.

The networks defined on the **Networks** tab are used to match `networkType: existing` in the VMware Aria Automation template.

The networks marked to support the public IP can also be listed on the **Networks** tab to match `networkType: public` in the VMware Aria Automation template.

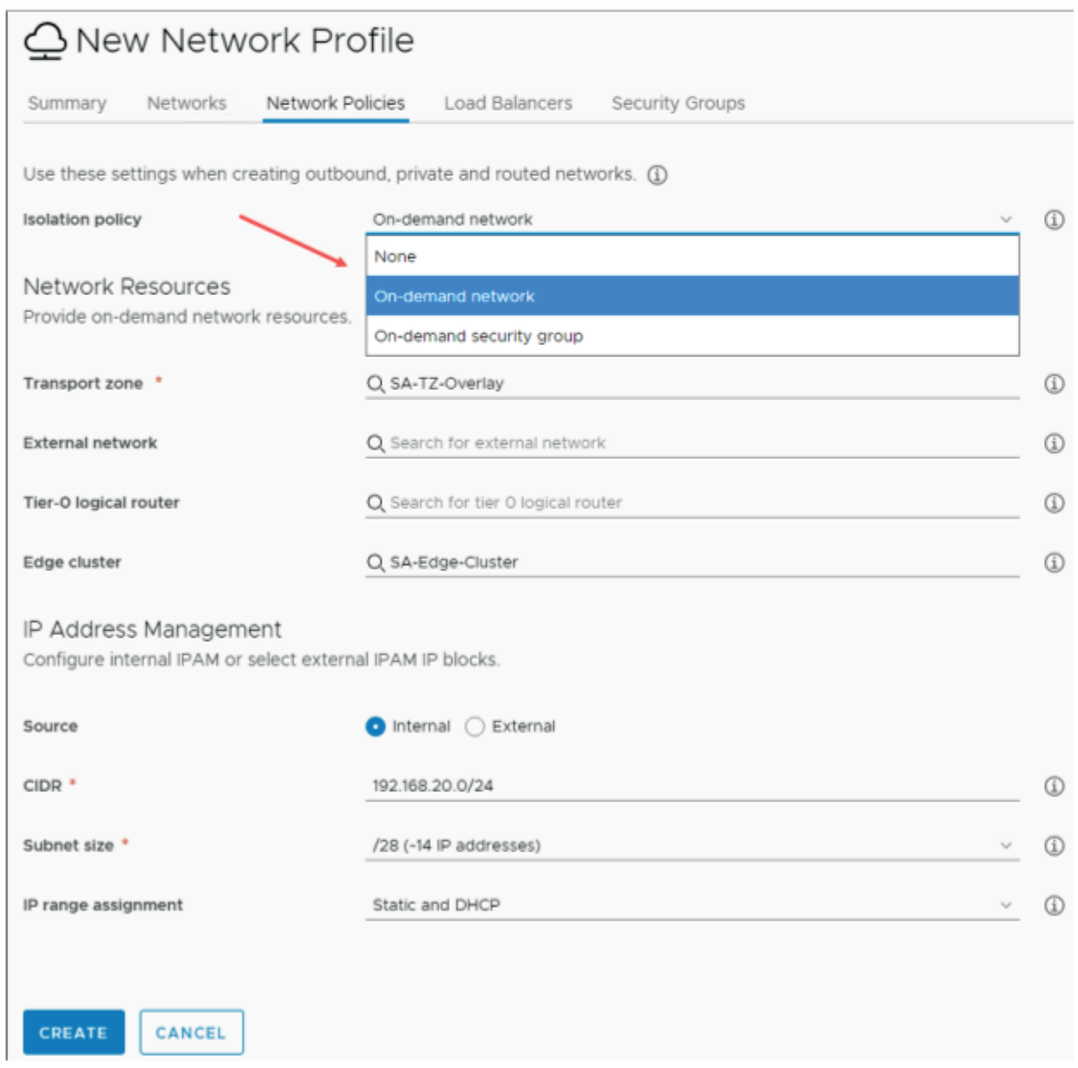
Creating a network profile for existing or public network profile types is not mandatory. The VMware Aria Automation template can select from the discovered networks. If no tags are specified to select an existing or public network, the default network created for the cloud zone is used.

9-22 Network Profile: Private

Use case: Isolate provisioned VMs from external access.

A private network profile can be created in one of the following ways:

1. Select the **On-demand network** policy:
   - Do not specify any existing networks.
   - Do not specify an external network and Tier-0 gateway.
2. Select the **On-demand security group** policy:
   - Define an existing network that is discovered or deployed by NSX in the **Networks** tab.
   - vSphere networks are not supported.



A private network profile can be created in one of the following ways:

- Create an on-demand network: In NSX, a DHCP server and pool are created. A Tier-1 gateway is not deployed and security groups are not created.
- Create an on-demand security group: An on-demand security group is created with three associated firewall rules. The associated rules include inbound and outbound reject rules, and a third rule that allows intra-VM communication for members of that security group.

Private networks do not allow any external access.

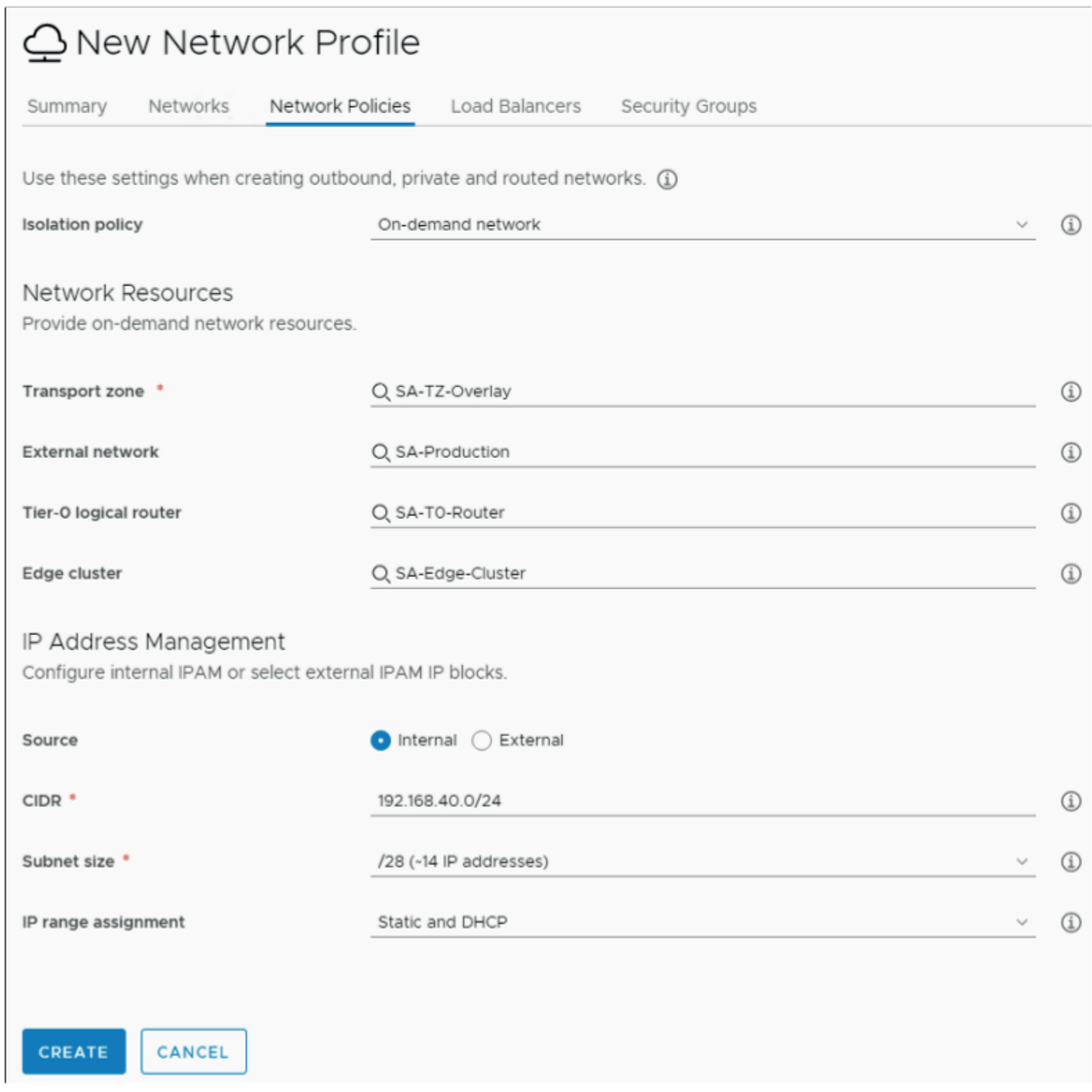
9-23 Network Profile: Outbound

Outbound network profiles are on-demand networks that are created during provisioning. An outbound network profile defines internal and external networks that use a translation table for mutual communication.

Use case: Single public IP addresses shared across internal networks that need external connectivity.

Deploying one VM with an outbound network profile:

- Creates one logical switch
- Creates one DHCP server
- Creates one Tier-1 gateway
- Connects a Tier-1 gateway to a Tier-0 gateway
- Creates a one-to-many SNAT rule



You must select an external network. The deployed on-demand outbound network is allocated a static IP from the external network for the outbound access (SNAT) rule. NSX routes are not advertised.

The CIDR value specifies the network address range to use during provisioning to create subnets.

The subnet size is the size of the on-demand network that is created for each isolated network in a deployment that uses this profile.

One-to-Many: One external IP address is shared among all machines on the network:

- An internal machine can have either DHCP or static IP addresses.
- Every machine can access the external network, but no machine is accessible from the external network.
- The SNAT rule is configured to enable VMs to communicate externally.

Outbound networks allow one way access to upstream networks.

9-24 Network Profile: Routed

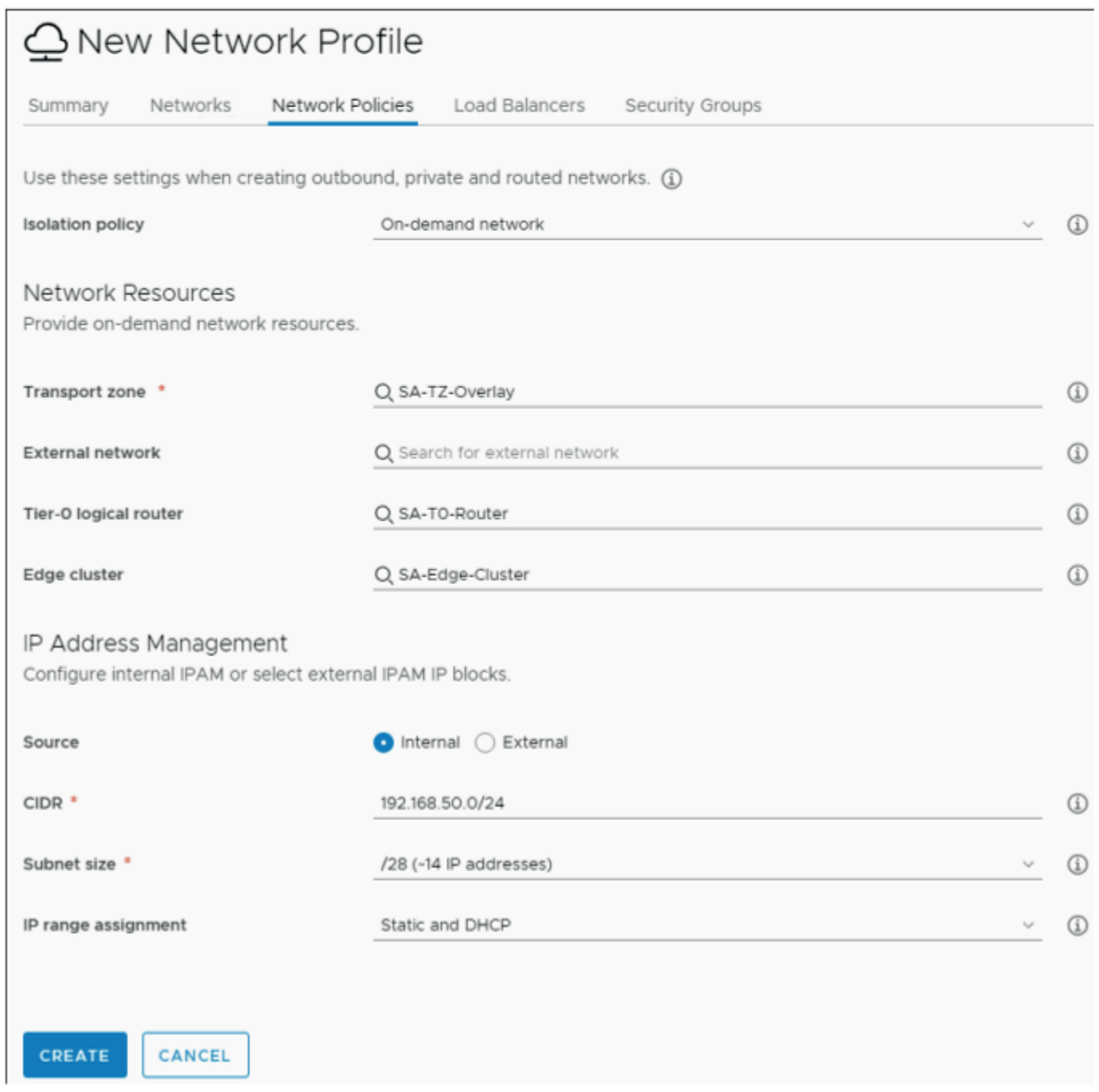
Routed network profiles are on-demand networks created during provisioning. Routed network profiles must use a routed gateway to access external networks.

Network profile configuration for routed profiles is the same as an outbound profile. But you do not define the external network.

Use case: End-to-end routable access with unique IP addresses.

Deploying one VM with routed network profile:

- Creates one logical switch
- Creates one DHCP server
- Creates one Tier-1 gateway
- Connects a Tier-1 gateway to a Tier-0 gateway
- Advertises NSX routes



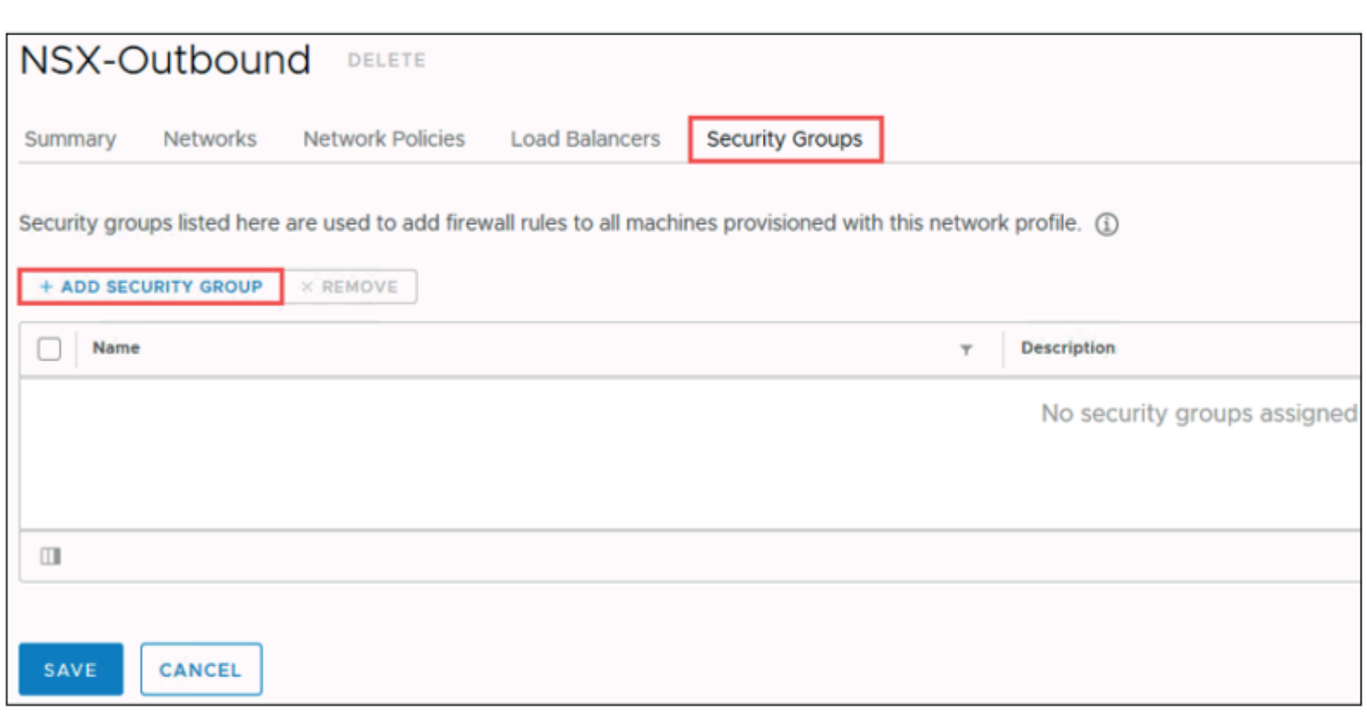
Changing `networkType` to `routed` in the VMware Aria Automation template network properties deploys routed networks.

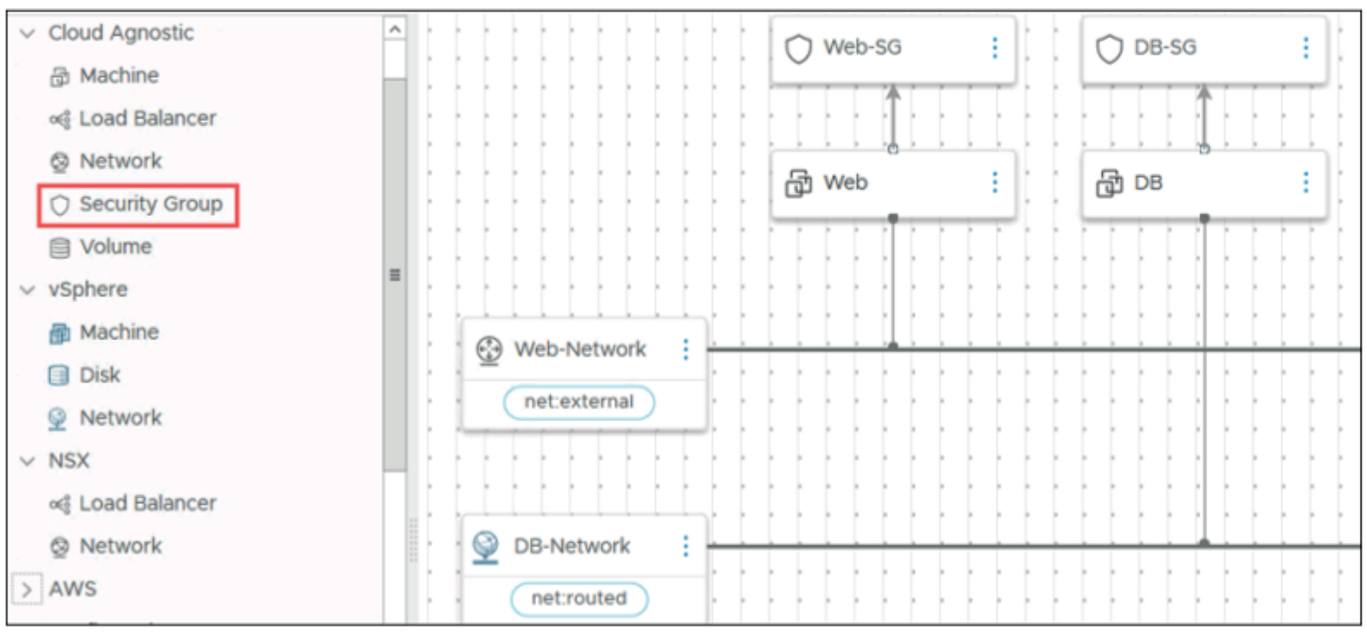
NAT rules are not created. The VM can communicate to the external network. The VM can also be reached from the external network. End-to-end routable communication is enabled.

9-25 Security Groups

Existing security groups can be associated with a VM in the following ways:

- Network profile:
  - Assign a common security group to set a minimum-security baseline.
  - Security groups added to the network profile are applied to all the VMs in a deployment that use the network profile.
- VMware Aria Automation template design canvas:
  - More detailed or specific security groups.
  - Each VM can be assigned an individual security group.





Security groups are available in **Infrastructure** > **Resources** > **Security**. This view enables you to view all the discovered security groups.

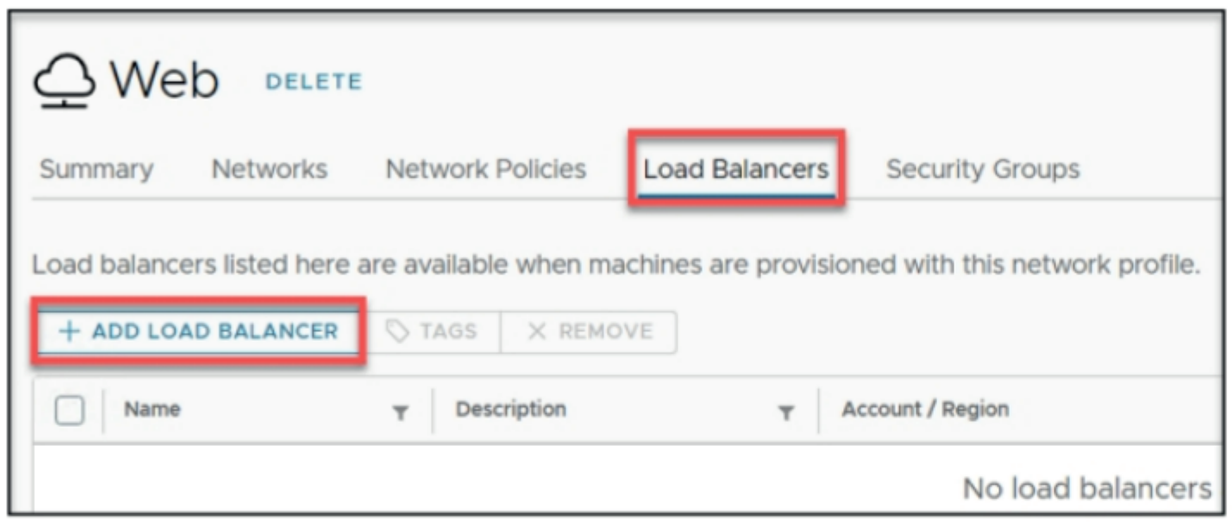
You can add multiple security groups to one network profile. Click **ADD SECURITY GROUP** to add security groups.

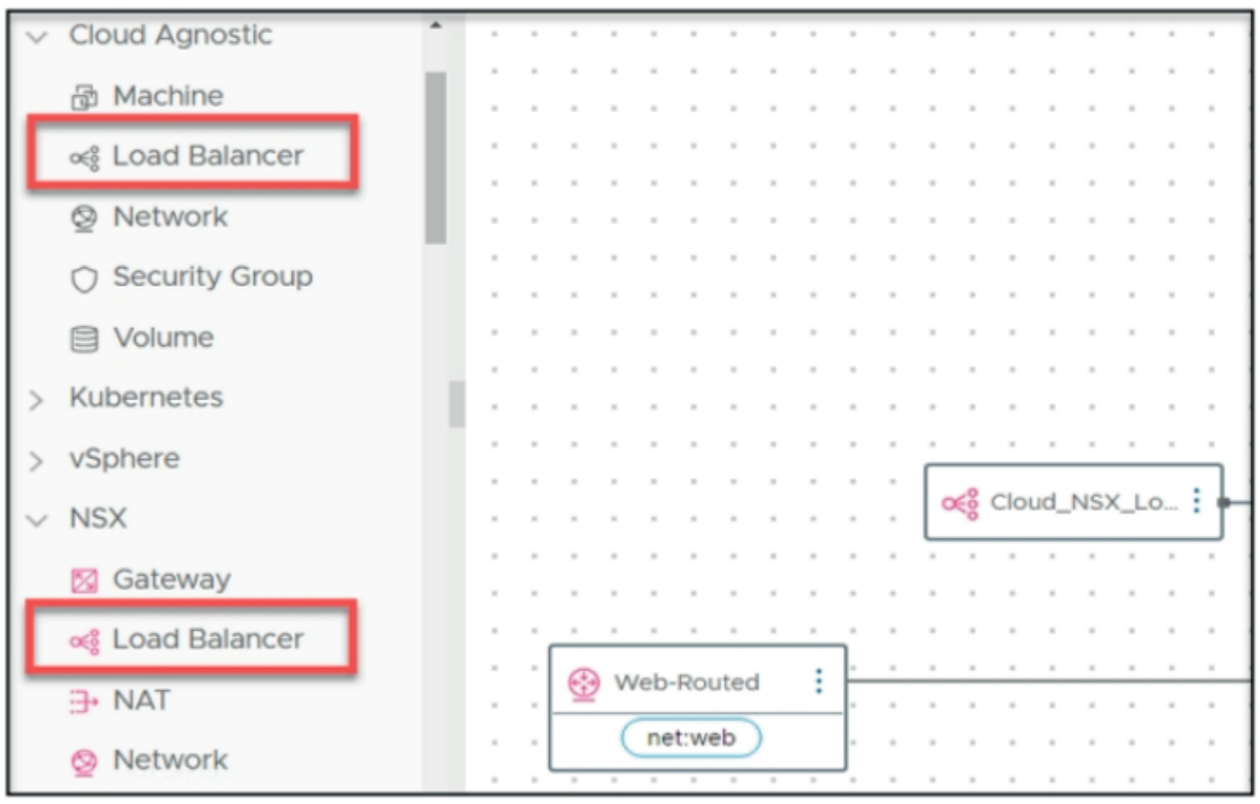
You can use the Security Group component in the VMware Aria Automation template to associate security groups directly to the VM network.

9-26 Load Balancers

Load balancers in VMware Aria Automation are available in the following ways:

- Add an existing load balancer to a network profile.
- Deploy an on-demand load balancer from a VMware Aria Automation template.



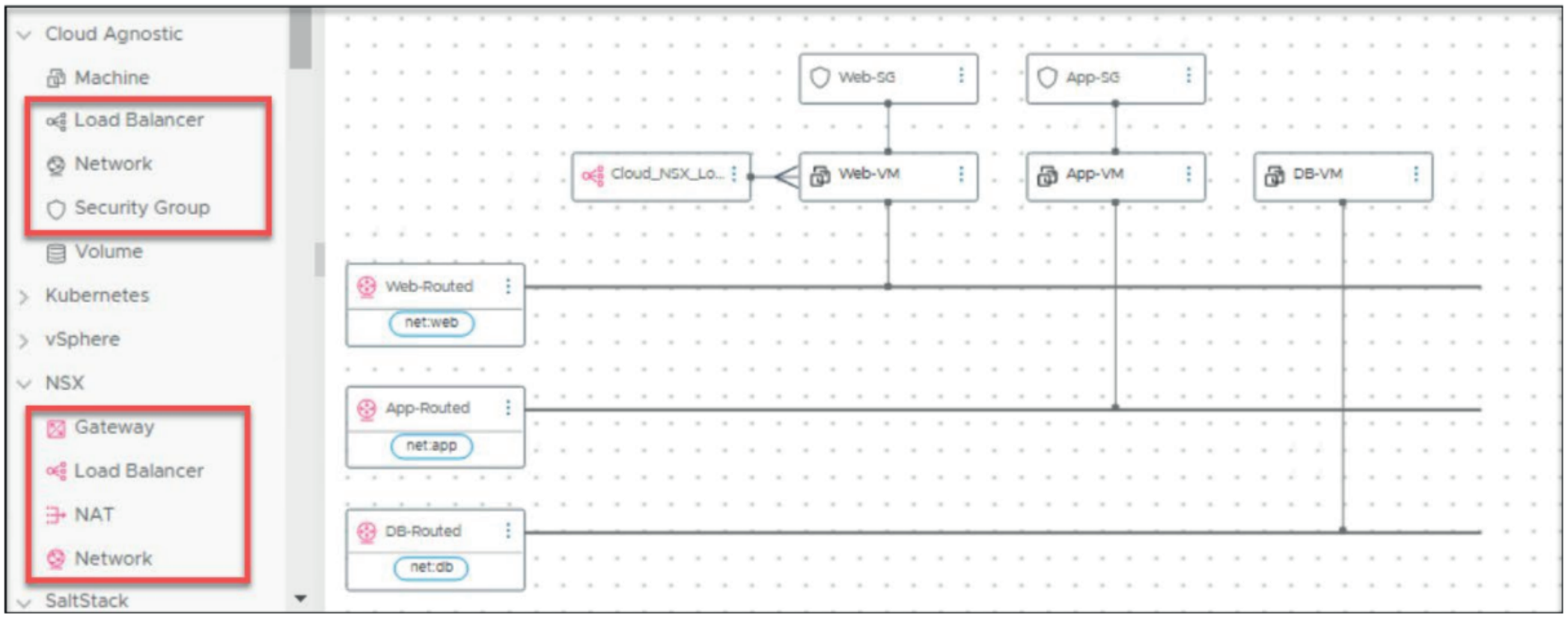


All load balancers that are discovered or deployed can be viewed in the **Resources** > **Deployments** > **Networking & Security** > **Load Balancers** tab.

You can add a cloud-agnostic load balancer or NSX load balancer to the design canvas based on your environment.

9-27 VMware Aria Automation Template with Network and Security Constructs

You can select components from the list of available network and security components to design a simple or complex VMware Aria Automation template.



The key difference between networking components available in cloud-agnostic network and NSX is the supported features. For example:

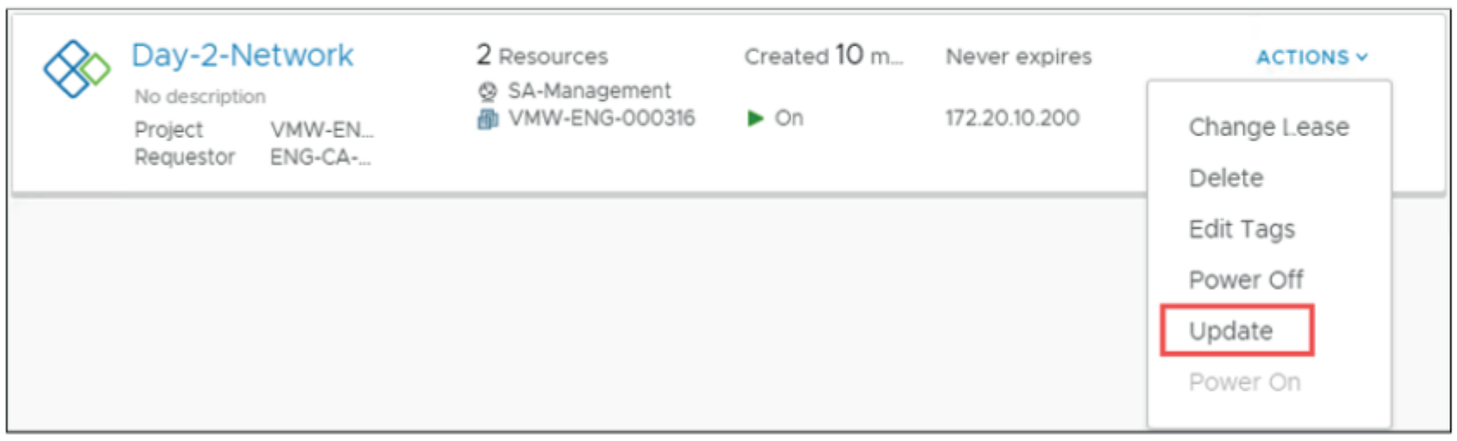
- Cloud-agnostic network does not support routed network profiles.
- Cloud-agnostic load balancer does not support UDP.

9-28 Day 2 Actions: Networks

A VMware Aria Automation template can be designed to support day 2 actions for managing networks after the deployment.

Code Properties Inputs

```yaml
formatVersion: 1
inputs:
  network:
    type: string
    enum:
      - test
      - production
    title: Select a network
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: 'VMW-PhotonOS'
      cpuCount: 1
      totalMemoryMB: 1024
      networks:
        - network: '${resource.Cloud_Network_1.id}'
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
    constraints:
      - tag: '${"net:" + input.network}'
```





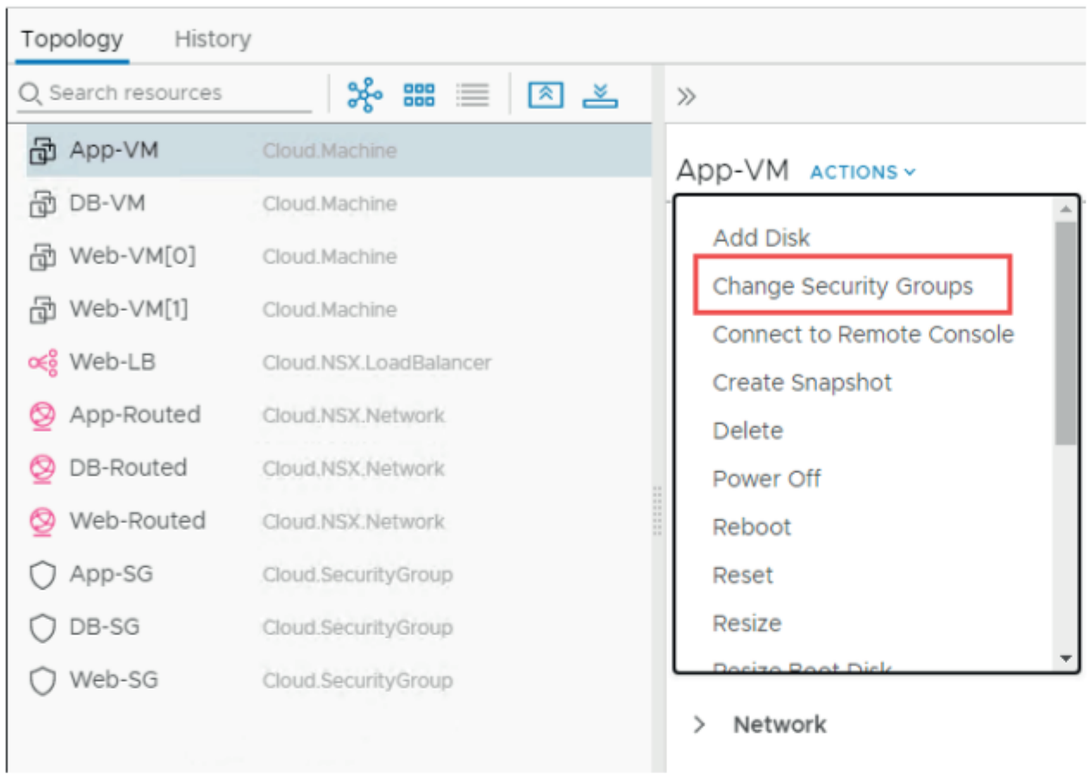
Network day 2 actions are supported with Cloud.vSphere.Machine resources. This method works for cloud-agnostic machines that are deployed to vSphere.

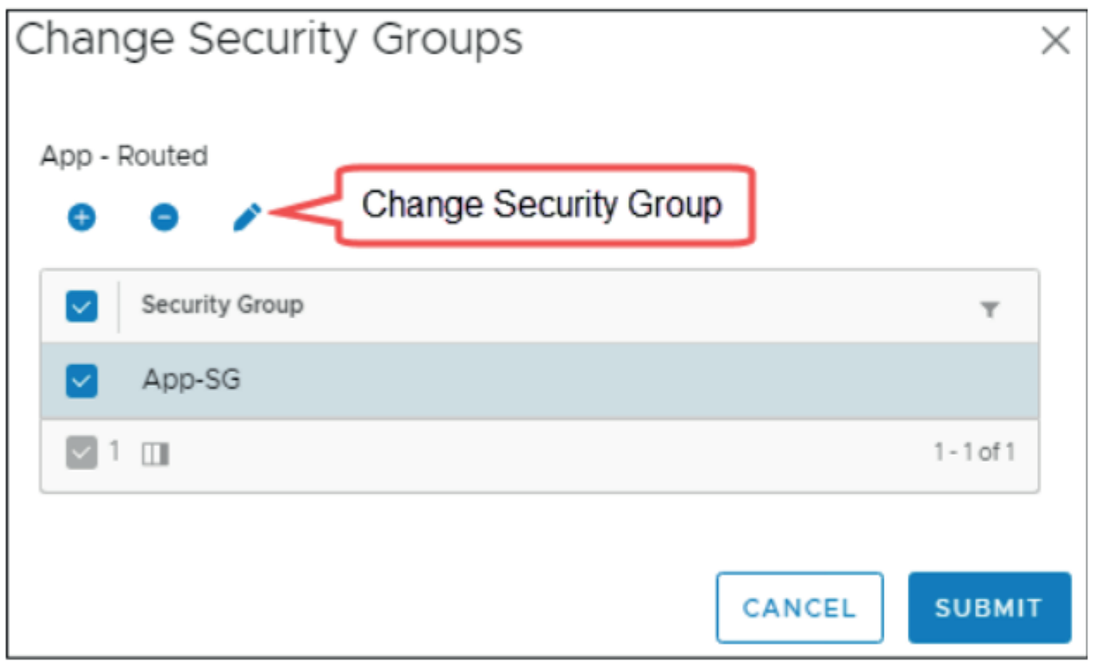
Update deployment constraints on the machine NIC to move it from one existing network to another existing network in the same network profile.

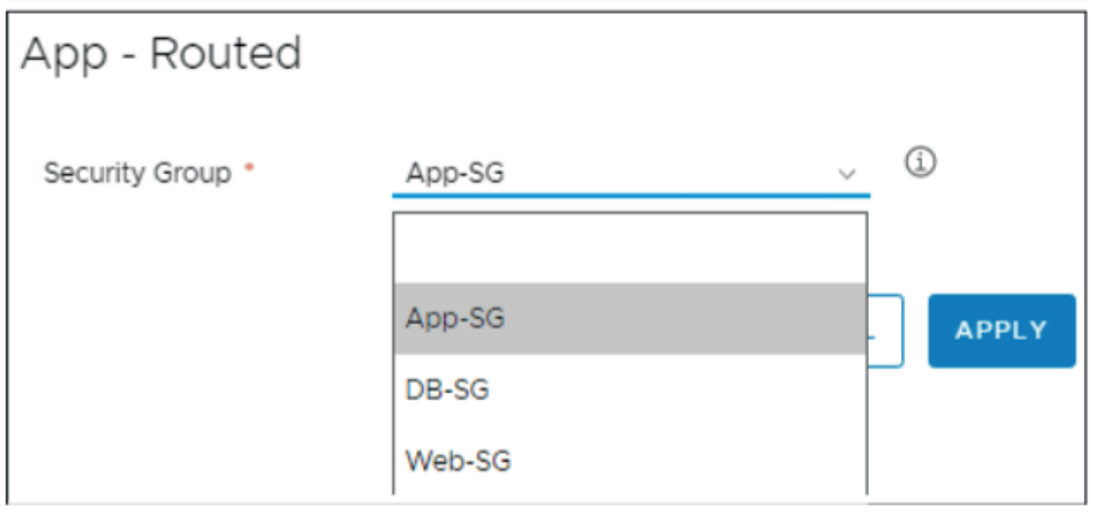
A machine can be moved between static networks or between dynamic networks.

9-29 Day 2 Actions: Security Groups

Security groups can be associated and dissociated with VMs in a deployment.







The day 2 action is supported for a security group that is associated with a single machine only and not for a multimachine cluster. This change applies to existing and on-demand security groups only and does not affect security groups applied as part of the network profiles.

You can perform the following actions:

- Add a security group to the VM. The security group must be present at the deployment.
- Remove a security group associated with a VM (the security group is disassociated but not deleted).
- Delete a security group (only applicable to on-demand security groups).

9-30 Lab 21: Integrating NSX with VMware Aria Automation

Integrate NSX and create a multitier VMware Aria Automation template with NSX network components:

1. Create an NSX Cloud Account
2. Create Network Profiles
3. Import and Validate the NSX 3-Tier VMware Aria Automation Template
4. Deploy the NSX 3-Tier VMware Aria Automation Template
5. Examine the NSX 3-Tier Deployment
6. Clean Up to Save Lab Resources

9-31 Lab 22: Performing Day 2 Network Actions

Edit the deployment to change one existing network to another existing network in the same network profile:

1. Create a Network Profile
2. Create a VMware Aria Automation Template
3. Deploy the VMware Aria Automation Template
4. Change the Existing Network
5. Clean Up to Save Lab Resources

9-32 Review of Learner Objectives

- Integrate NSX with VMware Aria Automation
- List the supported network profiles in VMware Aria Automation
- Identify the network and security options that are available in the design canvas
- Use NSX components to design a multitier application with VMware Aria Automation templates

9-33 Key Points

- VMware Aria Automation can be integrated with NSX.
- NSX integration offers advanced networking and security features, including logical networks, security groups, and load balancer.
- VMware Aria Automation supports various network profiles that you can use based on the use case.
- A simple or complex VMware Aria Automation template can be designed by using the NSX networking and security constructs available in the design canvas.
- Users can perform day 2 actions for networks and security groups in the deployment.

Questions?

Module 10

Integration with Public Clouds

10-2 Importance

VMware Aria Automation supports native integration with public cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, VMware Cloud Foundation, and VMware Cloud on AWS. Creating cloud accounts in VMware Aria Automation allows you to integrate with public cloud platforms and deploy services.

10-3 Lesson 1: Integration with Public Clouds

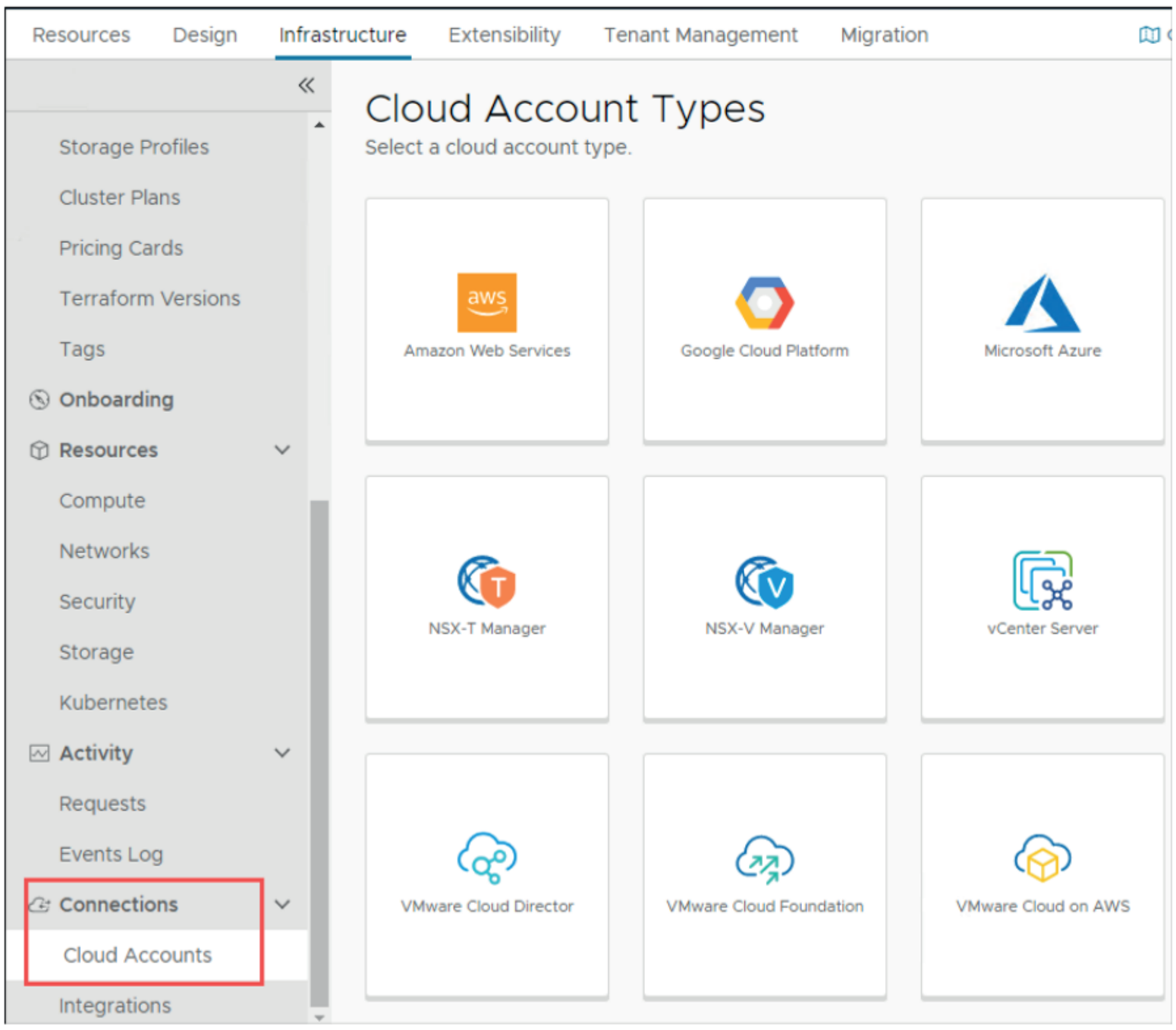
10-4 Learner Objectives

- Describe the public cloud accounts supported by VMware Aria Automation
- Create an AWS public cloud account
- Create a Microsoft Azure public cloud account
- Create a Google Cloud Platform public cloud account
- Create a VMware Cloud Foundation public cloud account
- Create a VMware Cloud Director public cloud account
- Create a VMware Cloud on AWS public cloud account

10-5 Public Cloud Support

VMware Aria Automation includes native support for adding public cloud accounts:

- AWS
- Microsoft Azure
- Google Cloud Platform
- VMware Cloud Foundation
- VMware Cloud on AWS
- VMware Cloud Director



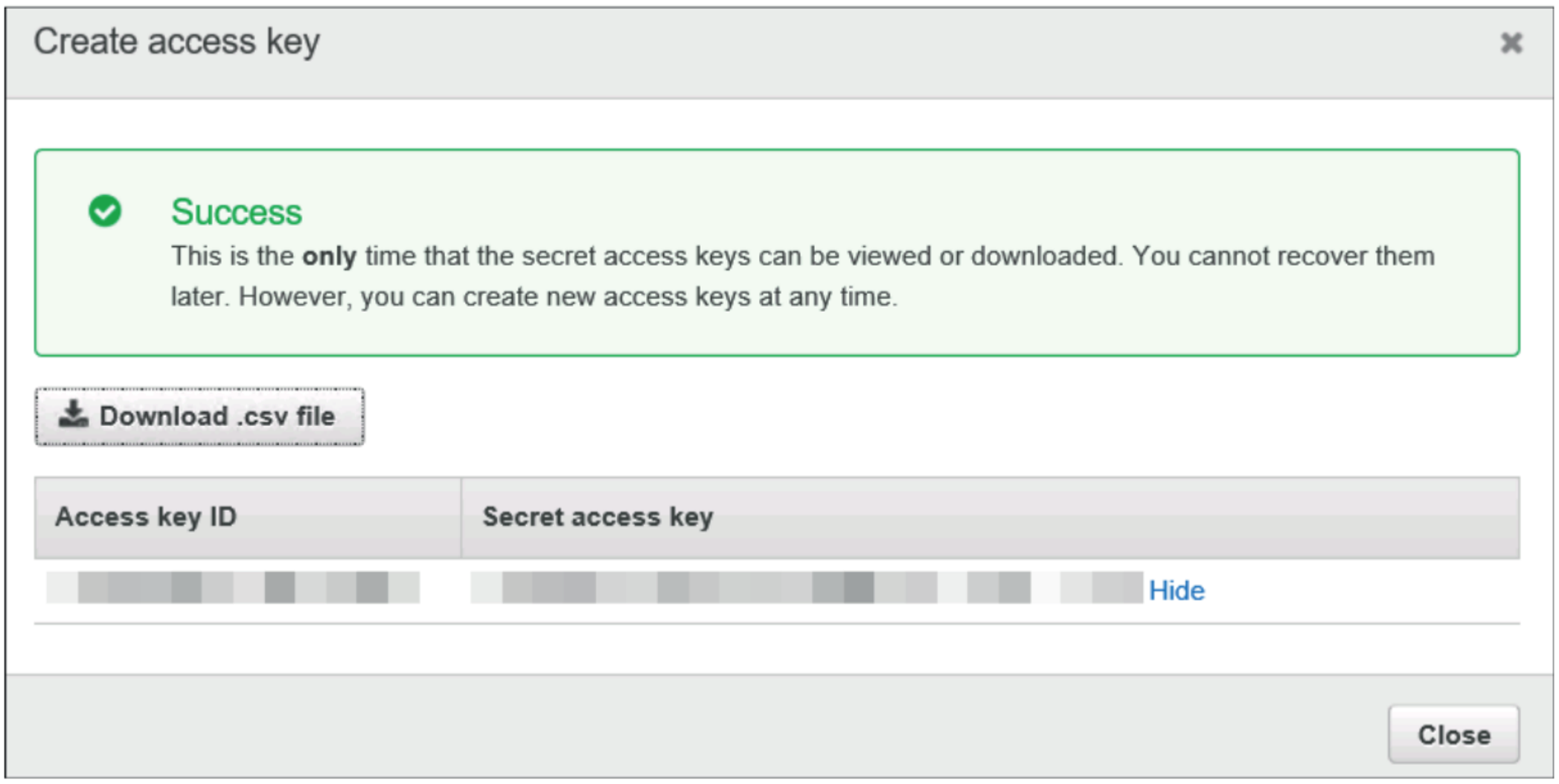
10-6 Amazon Web Services: Credentials

An Amazon Web Services cloud account requires the following credentials:

- Access key ID
- Secret access key

To create an access key:

1. Log in to the Amazon Web Services console using a power user account with read and write privileges.
2. Select **Identity and Access Management (IAM)** > **Users** > **Security Credentials**.
3. Click **Create access key**.



Access keys are long-term credentials for an Identity and Access Management (IAM) user or the Amazon Web Services (AWS) account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or by using the AWS SDK).

Access keys consist of the following parts:

- Access key ID of 20 digits, for example, AKIAIOSFODNN7EXAMPLE
- Secret access key, for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. You must manage your access keys as securely as your user name and password.

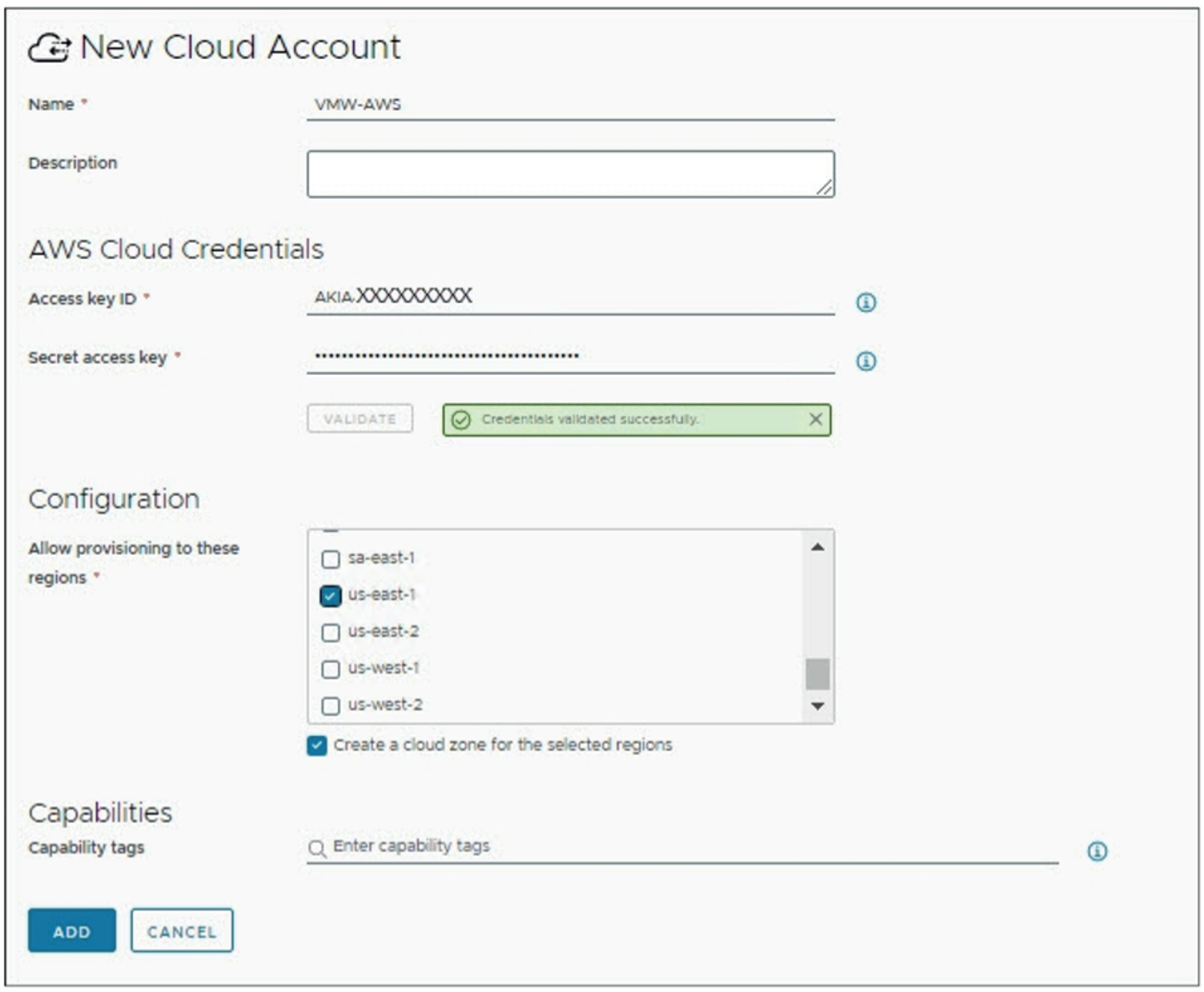
When you create an access key pair, save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must delete the access key and create it again.

As a security best practice, you must regularly rotate (change) IAM user access keys. If your administrator granted you the necessary permissions, you can rotate your own access keys.

10-7 Amazon Web Services: Cloud Accounts

To create an AWS cloud account:

1. Log in to the VMware Aria Automation console as an administrator and select **Infrastructure** > **Connections** > **Cloud Accounts**.
2. Click **ADD CLOUD ACCOUNT** and click **Amazon Web Services**.
3. On the New Cloud Account page, configure the AWS cloud account details.
   - Name
   - Access key ID
   - Secret access key
4. Click **VALIDATE** and select the AWS regions to deploy services.
5. Click **ADD**.



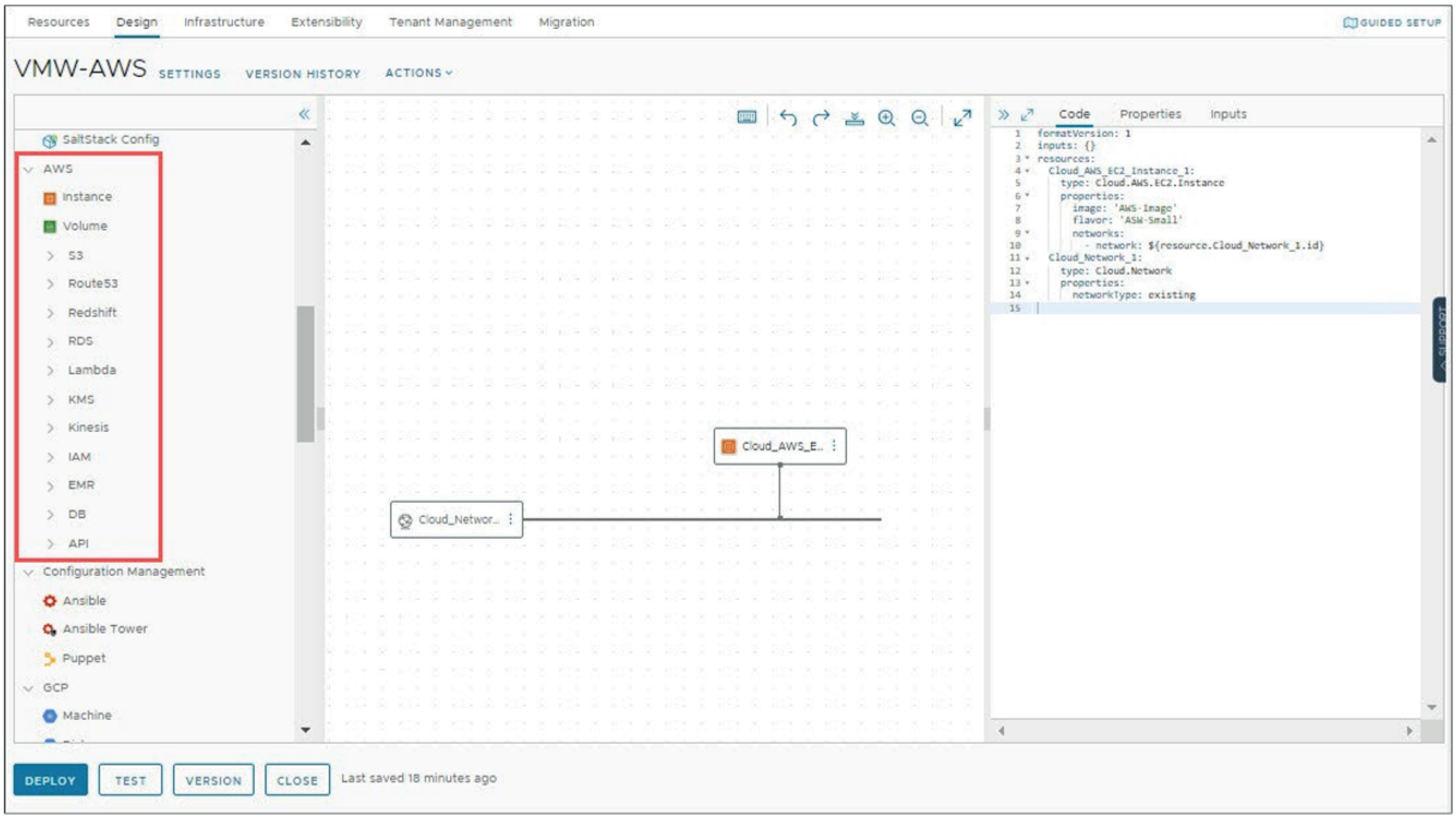
You enter the access key ID and secret access key that are acquired from the AWS console. Enter an appropriate name and description for this cloud account.

If the credentials are validated successfully, an extra option is available to select AWS regions. Services requested by VMware Aria Automation are deployed to these regions. Cloud zones and projects can manage these regions.

After the cloud account is created, the data collection process starts immediately to gather resources from AWS. Resources include images, flavors, machines, networks, security objects, and volumes.

10-8 Amazon Web Services: Simple VMware Aria Automation Template

To create a VMware Aria Automation template, you drag components from the AWS section in the left pane to the design canvas. Deployed resources are hosted on AWS.



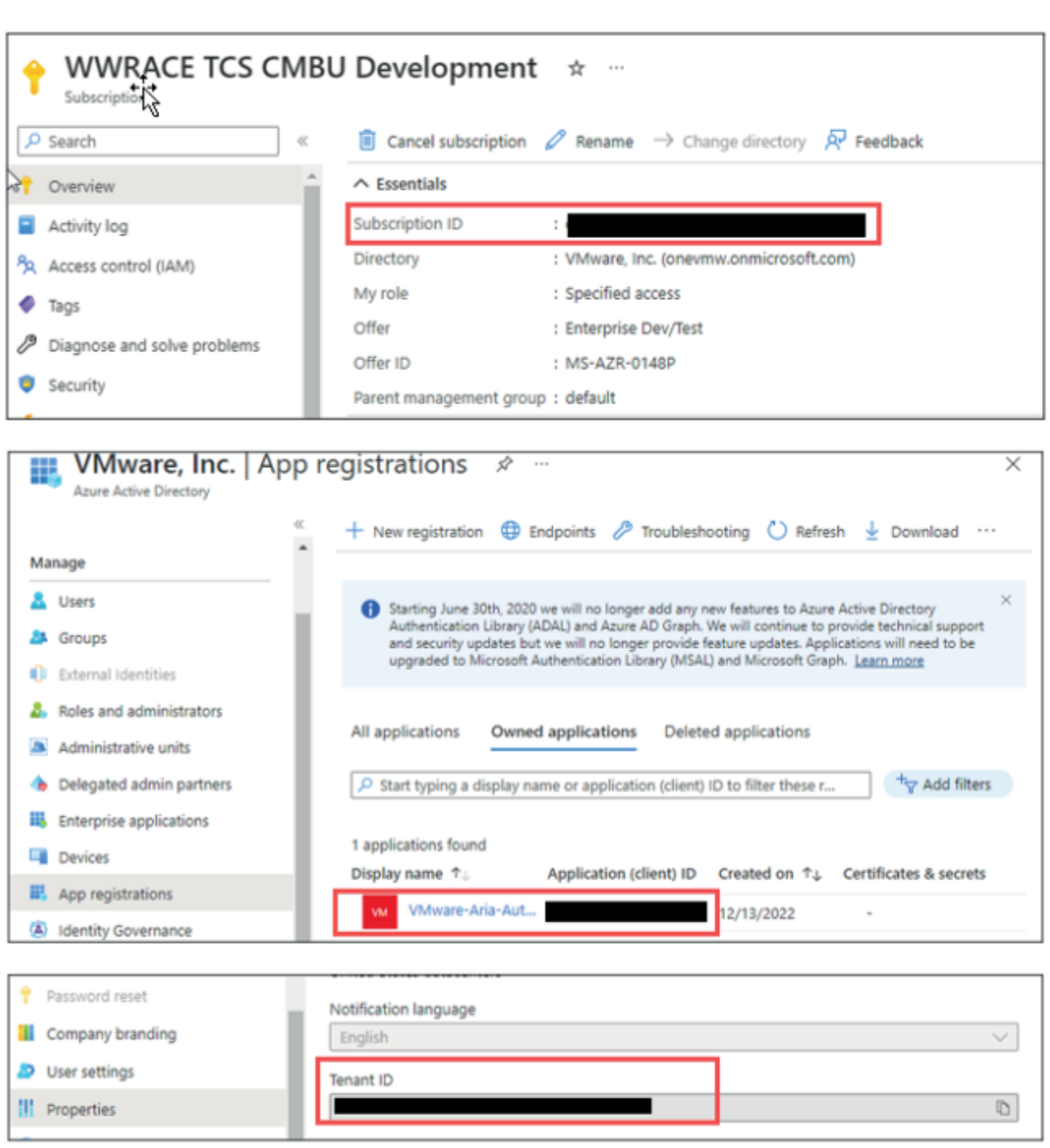
In the example, an Amazon instance and cloud network are dragged to the design canvas.

For details about the AWS services, see the AWS documentation at https://docs.aws.amazon.com.

10-9 Microsoft Azure: Credentials

You log in to the Microsoft Azure console as an organization owner to gather the following information:

- Subscription ID
- Tenant ID
- Client application ID
- Client application secret key





The subscription ID allows you to access to your Microsoft Azure subscriptions.

The tenant ID is the authorization endpoint for the Active Directory applications that you create in your Microsoft Azure account.

The client application ID provides access to Active Directory in your Microsoft Azure individual account.

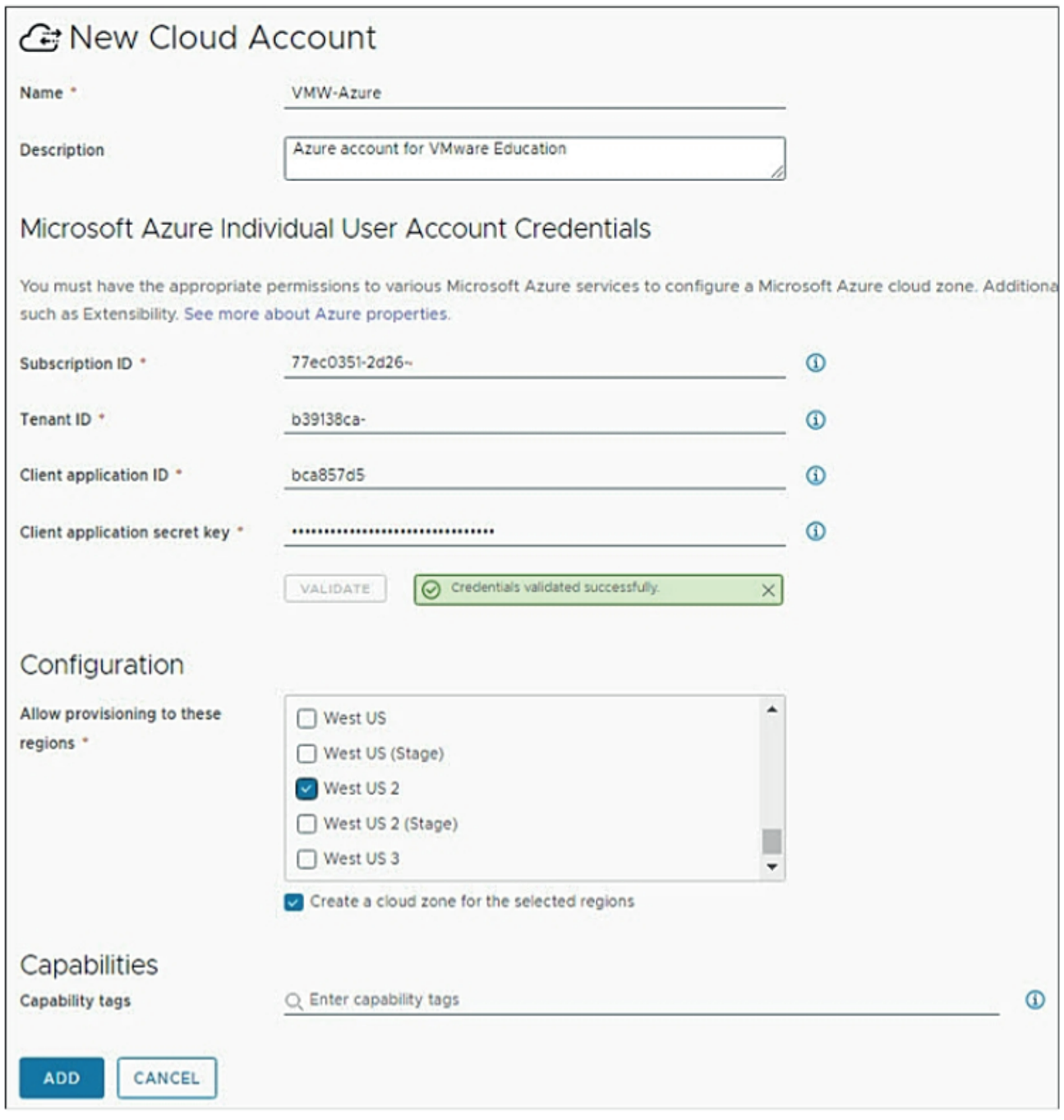
The client application secret key is the unique secret key generated to pair with your client application ID. The secret key can be generated by clicking the display name.

For more information about creating an Active Directory application, see "Creating a service principal" at https://learn.microsoft.com/en-us/azure/purview/create-service-principal-azure.

10-10 Microsoft Azure: Cloud Account

To create a Microsoft Azure cloud account:

1. Log in to the VMware Aria Automation console as an administrator and select **Infrastructure** > **Connections** > **Cloud Accounts**.
2. Click **ADD CLOUD ACCOUNT** and then click **Microsoft Azure**.
3. On the New Cloud Account page, configure the Microsoft Azure cloud account details.
   - Subscription ID
   - Tenant ID
   - Client application ID
   - Client application secret key
   - Name
4. Click **VALIDATE** and select the Microsoft Azure regions to deploy services.
5. Click **ADD**.



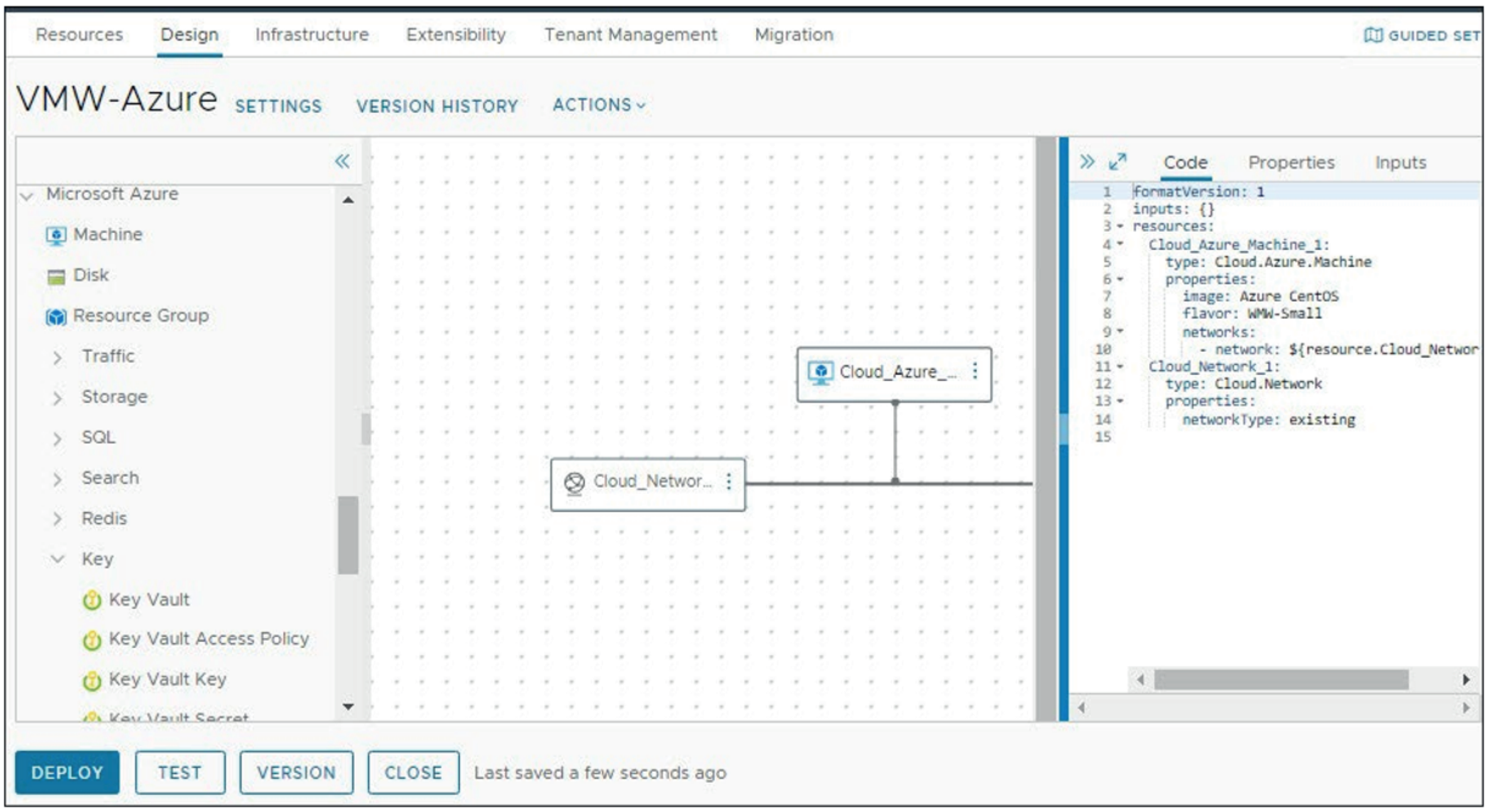
Enter the subscription ID, tenant ID, client application ID, and client application secret key that are acquired from the Microsoft Azure console. Enter an appropriate name and description for this cloud account.

If the credentials are validated successfully, an extra option is available to select Microsoft Azure regions. Services requested by VMware Aria Automation are deployed to these regions. Cloud zones and projects can manage these regions.

After the cloud account is created, the data collection process starts immediately to gather resources from Microsoft Azure. The resources include, images, flavors, machines, networks, security objects, and volumes.

10-11 Microsoft Azure: Simple VMware Aria Automation Template

To create a VMware Aria Automation template, you drag components from the Microsoft Azure section in the left pane to the design canvas. Deployed resources are hosted on Microsoft Azure.



In the example, a Microsoft Azure instance and cloud network are dragged to the design canvas.

For details about the Microsoft Azure services, see the Microsoft Azure documentation at https://docs.microsoft.com/en-us/azure/.

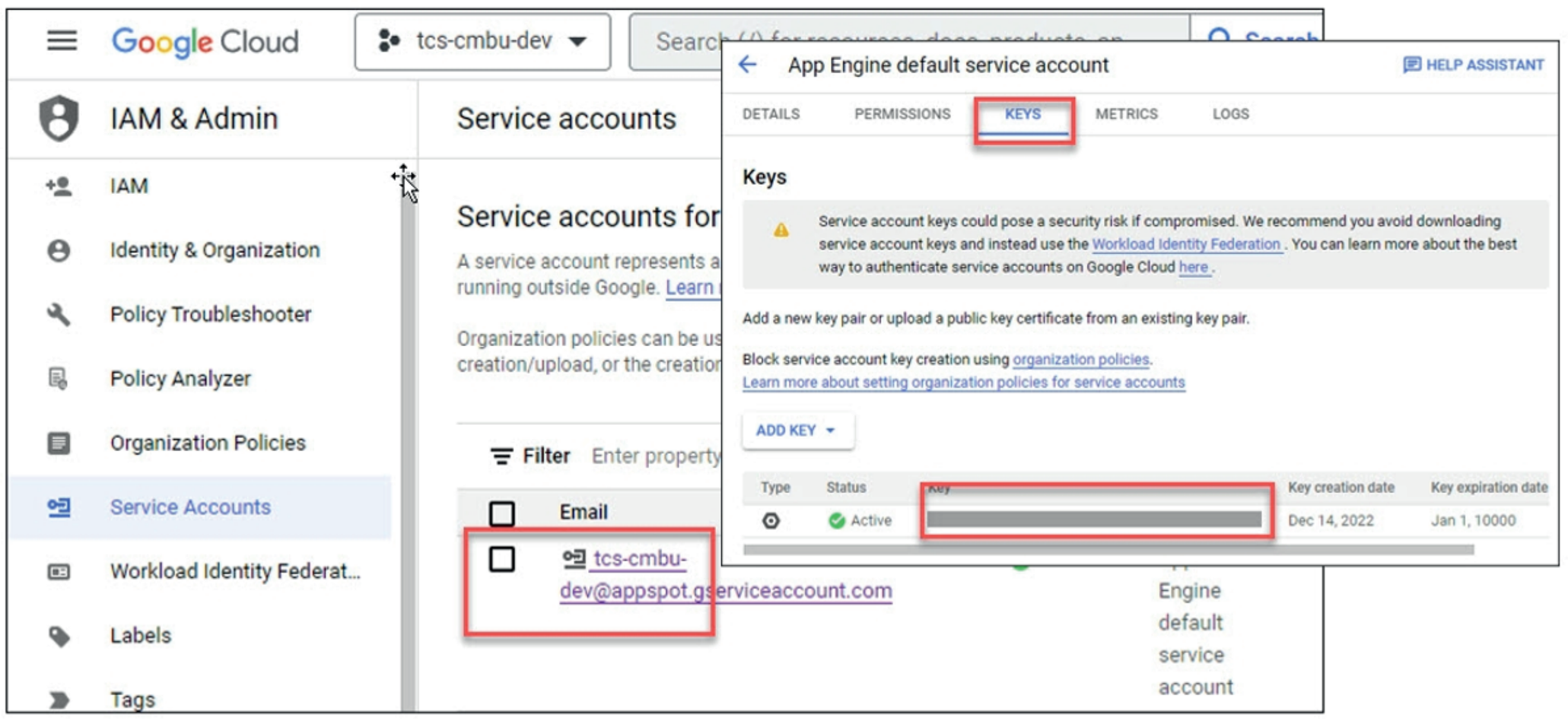
10-12 Google Cloud Platform: Credentials

A Google Cloud Platform account requires the following credentials:

- Project ID
- Private key ID
- Private key
- Client email

To generate the private key ID and private key:

1. Log in to the Google Cloud Platform console as the organization owner.
2. Select **IAM & admin** > **Service accounts** in the left navigation pane and then click the service account.
3. Click the **KEYS** tab and click **ADD KEY** to download the JSON file or copy the key from the key column.



The project ID is available on the Google Cloud Platform console dashboard.

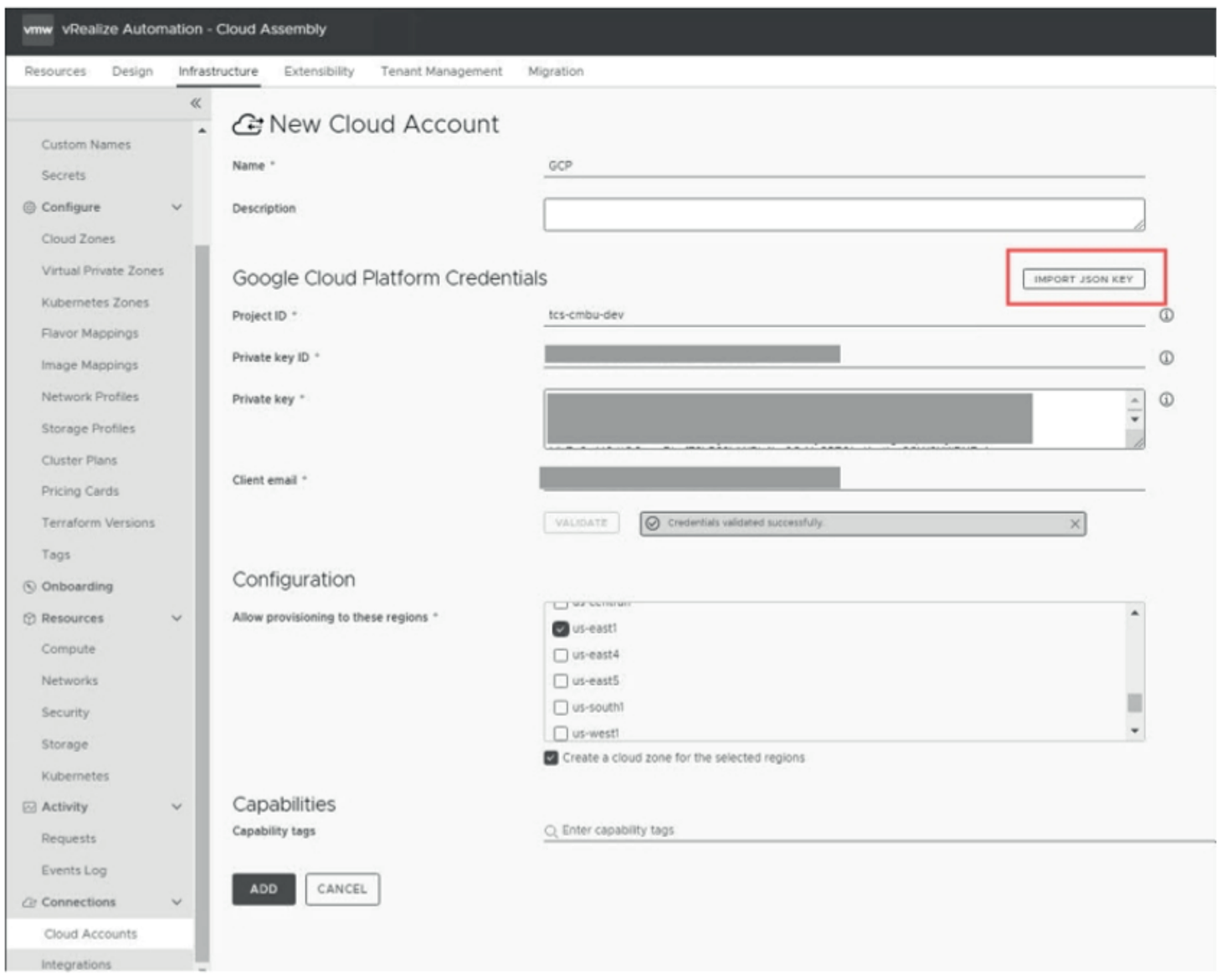
Clicking **CREATE KEY** downloads a JSON file that includes all the required attributes, including the project ID, private key ID, private key, and client email. Store the file securely because this key cannot be recovered if lost. You can generate a new file.

10-13 Google Cloud Platform: Cloud Account

To create a Google Cloud Platform cloud account:

1. Log in to the VMware Aria Automation console as an administrator and select **Infrastructure** > **Connections** > **Cloud Accounts**.
2. Click **ADD CLOUD ACCOUNT** and then click **Google Cloud Platform**.
3. On the New Cloud Account page, configure the Google Cloud Platform cloud account details.
   - Project ID
   - Private key ID
   - Private key
   - Client email
4. Click **VALIDATE** and select the Google Cloud Platform regions to deploy services.

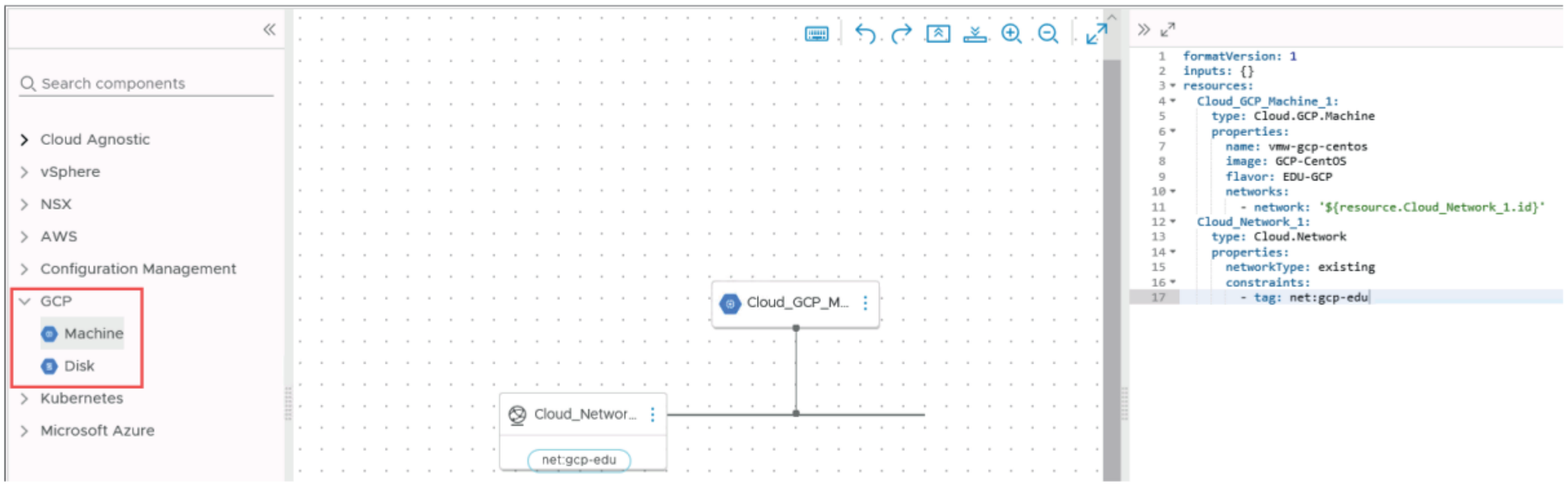
   Alternatively, you can click **IMPORT JSON KEY** to autofill the required fields.



You can obtain the credentials in JSON format from the Google Cloud Platform console. The JSON file includes project ID, private key ID, private key, and client email. All these details are autofilled when you import the JSON file for creating the Google Cloud Platform cloud account.

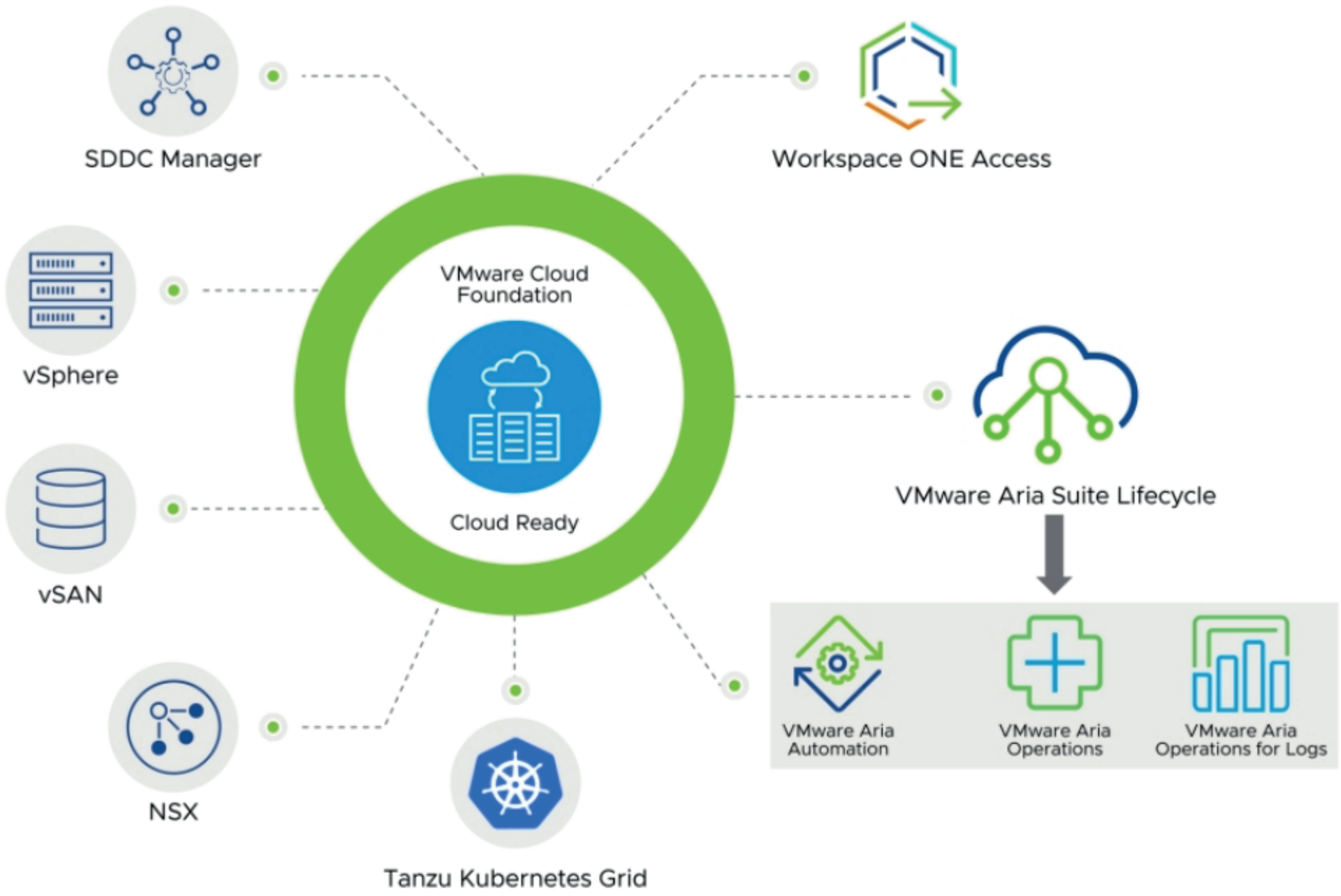
10-14 Google Cloud Platform: Simple VMware Aria Automation Template

You drag components from the GCP section in the left pane to the design canvas to use these objects in VMware Aria Automation template.



10-15 About VMware Cloud Foundation

VMware Cloud Foundation delivers a natively integrated software-defined data center stack that includes core infrastructure virtualization, vSphere, vSAN, and NSX.



VMware Cloud Foundation also provides the following capabilities:

- Automated deployment and configuration of the VMware Cloud Foundation software components
- Life cycle management
- Support for traditional and new (cloud-native) workloads
- Path to the hybrid cloud

VMware Cloud Foundation SDDC Manager automates the entire system life cycle (from configuration and provisioning to upgrades and patching) and simplifies day-to-day management and operations.

VMware Cloud Foundation supports automated deployment of VMware Aria Suite Lifecycle. You can then deploy and manage the life cycle of the VMware Aria Suite of products (VMware Aria Operations for Logs, VMware Aria Automation, and VMware Aria Operations) through VMware Aria Suite Lifecycle.

VMware Cloud Foundation 4.0.x provides a standardized and configured infrastructure for vSphere with Tanzu.

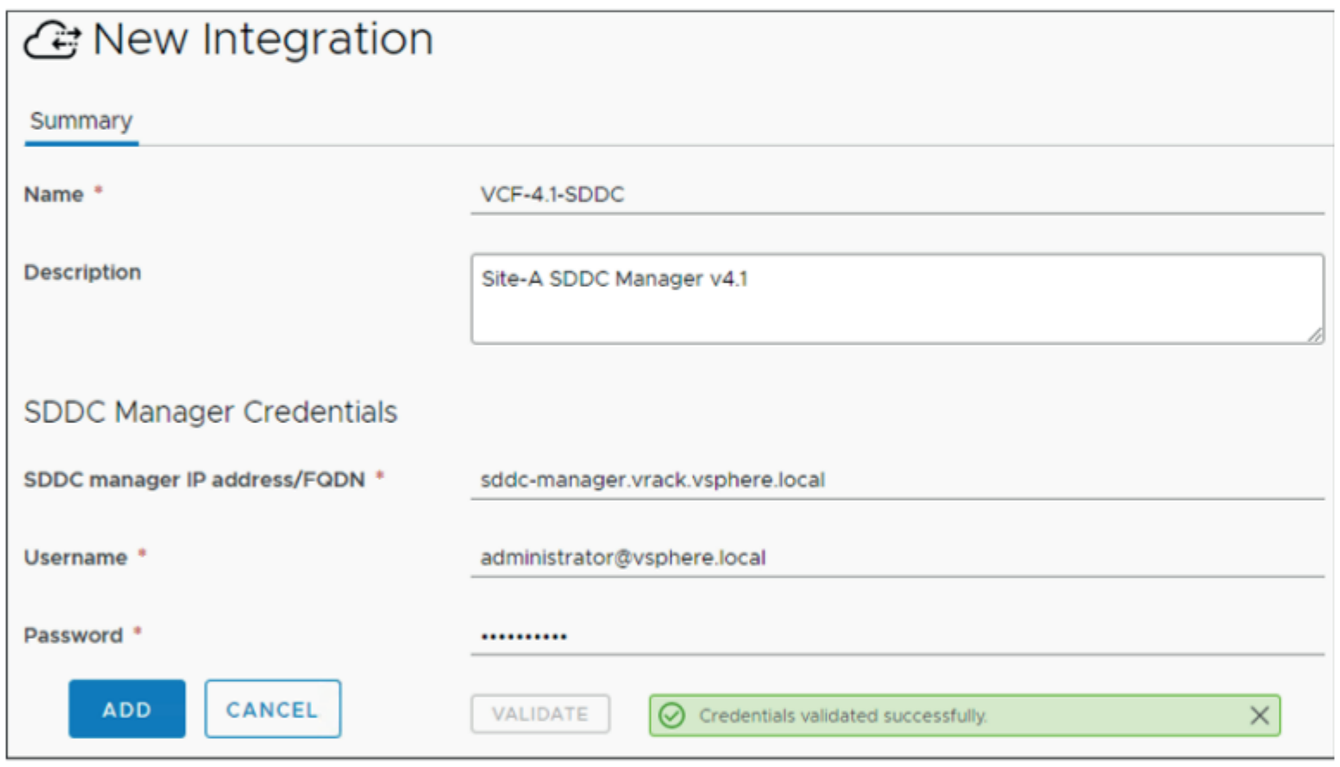
10-16 VMware Cloud Foundation SDDC Manager Integration

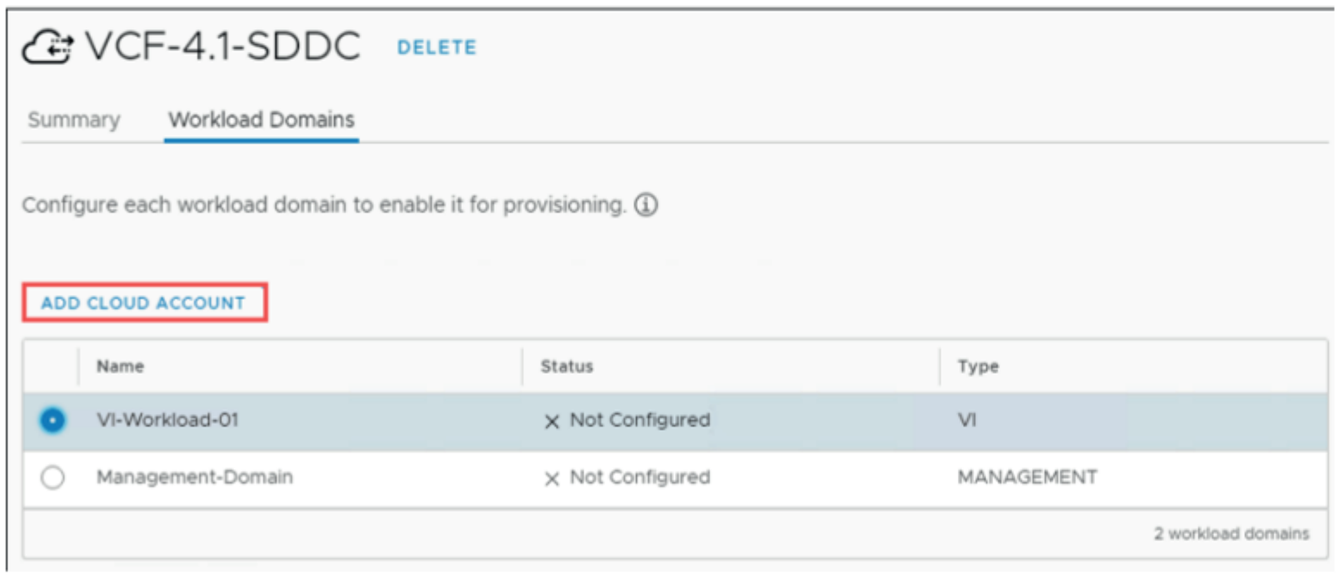
Before creating a VMware Cloud Foundation cloud account, you must integrate VMware Aria Automation with VMware Cloud Foundation SDDC Manager:

1. Select **Infrastructure** > **Connections** > **Integrations** in the VMware Aria Automation console.
2. Click **ADD INTEGRATION**.
3. Select **SDDC Manager**.

Edit the SDDC Manager integration:

1. Select the workload domain.
2. Click **ADD CLOUD ACCOUNT**.





You use SDDC Manager to perform administration tasks on your VMware Cloud Foundation system. SDDC Manager provides the user interface for your single point of control for managing and monitoring your VMware Cloud Foundation system and for provisioning virtual environments.

Clicking **ADD** on the **Summary** tab retrieves the workload and management domains hosted on VMware Cloud Foundation.

VMware Aria Automation supports integration only with SDDC Manager 4.1 and later.

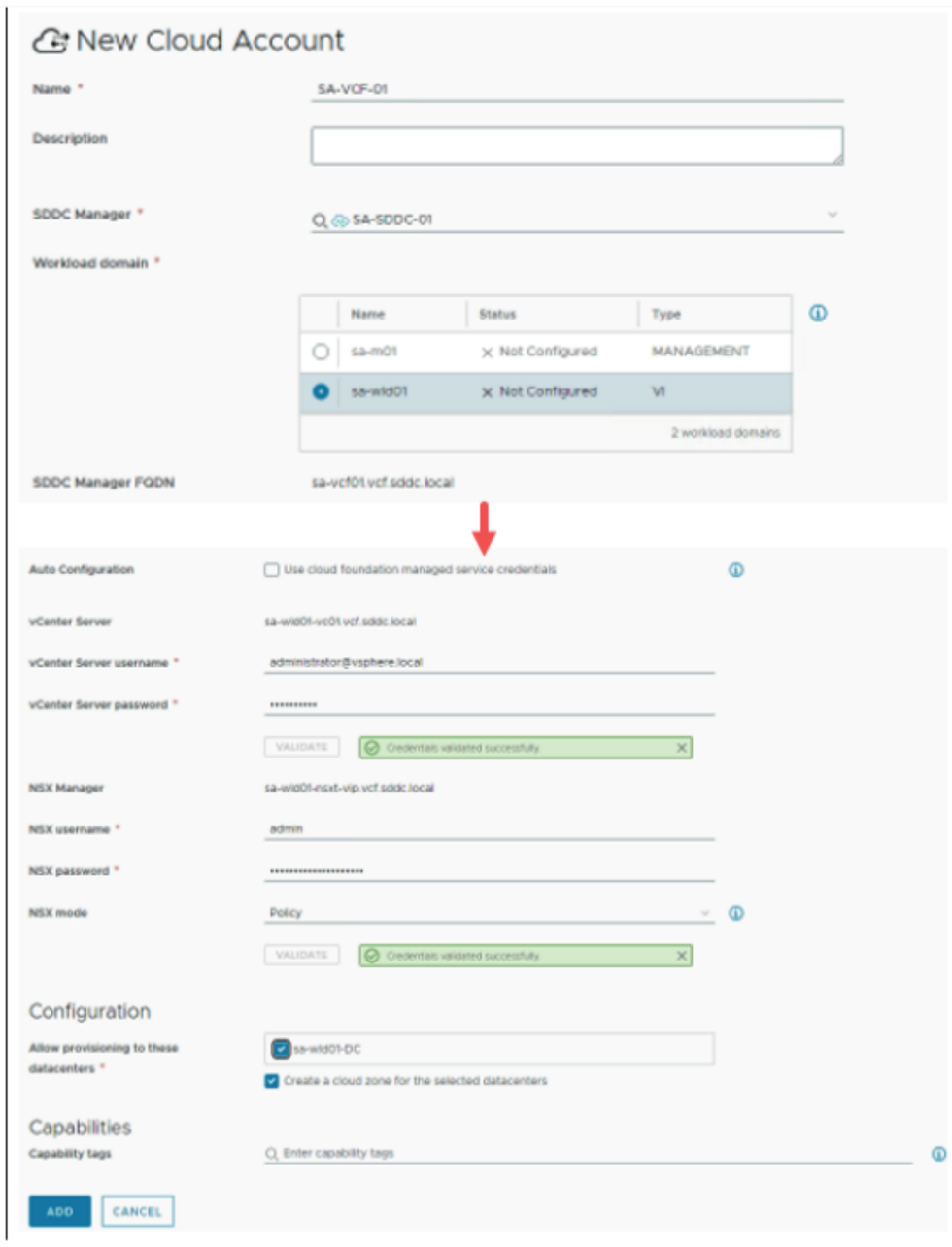
The management domain is created by default during the VMware Cloud Foundation installation. The VMware Cloud Foundation software stack is deployed on the management domain.

Each configured workload domain is added as a cloud account. Cloud accounts are used in VMware Aria Automation to configure the provisioning infrastructure. To create the cloud accounts, the workload domain must be active.

10-17 VMware Cloud Foundation: Cloud Account

The selected workload domain is used to create the VMware Cloud Foundation cloud account:

- Configure one cloud account per workload domain.
- Create service credentials or use the existing credentials.
- Configure cloud zone and image or flavor mappings.
- Resources are deployed on the workload domain.



Auto Configuration: Service credentials are automatically created on the vCenter system. These service credentials are used to validate the cloud account. Certificates are automatically accepted.

The administrator credentials are used for NSX.

After you create the cloud account, you can configure the workload cluster and NSX.

You configure image or flavor mappings and create a VMware Aria Automation template in the same way as a vSphere cloud account. The resources are deployed on the workload domain defined in the cloud account.

10-18 VMware Cloud Director: Cloud Account

To integrate VMware Cloud Director with VMware Aria Automation:

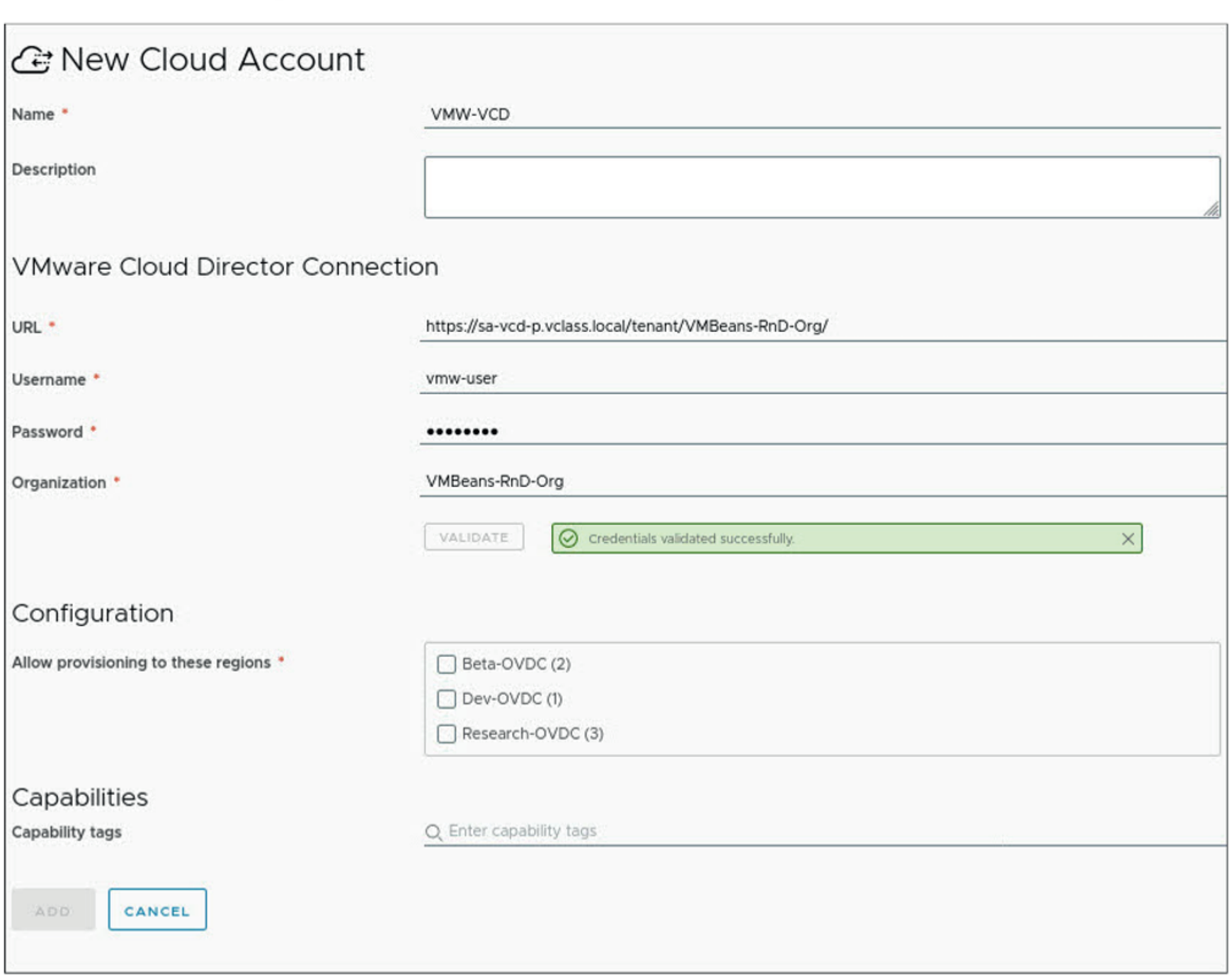
1 Log in to the VMware Aria Automation console as an administrator and select **Infrastructure** > **Connections** > **Cloud Accounts**.

2 Click **ADD CLOUD ACCOUNT** and then click **VMware Cloud Director**.

3 Enter the URL and credentials to use to connect to the VMware Cloud Director server.

4 Fill in the account details and validate.

5 Select the regions and create the cloud account.



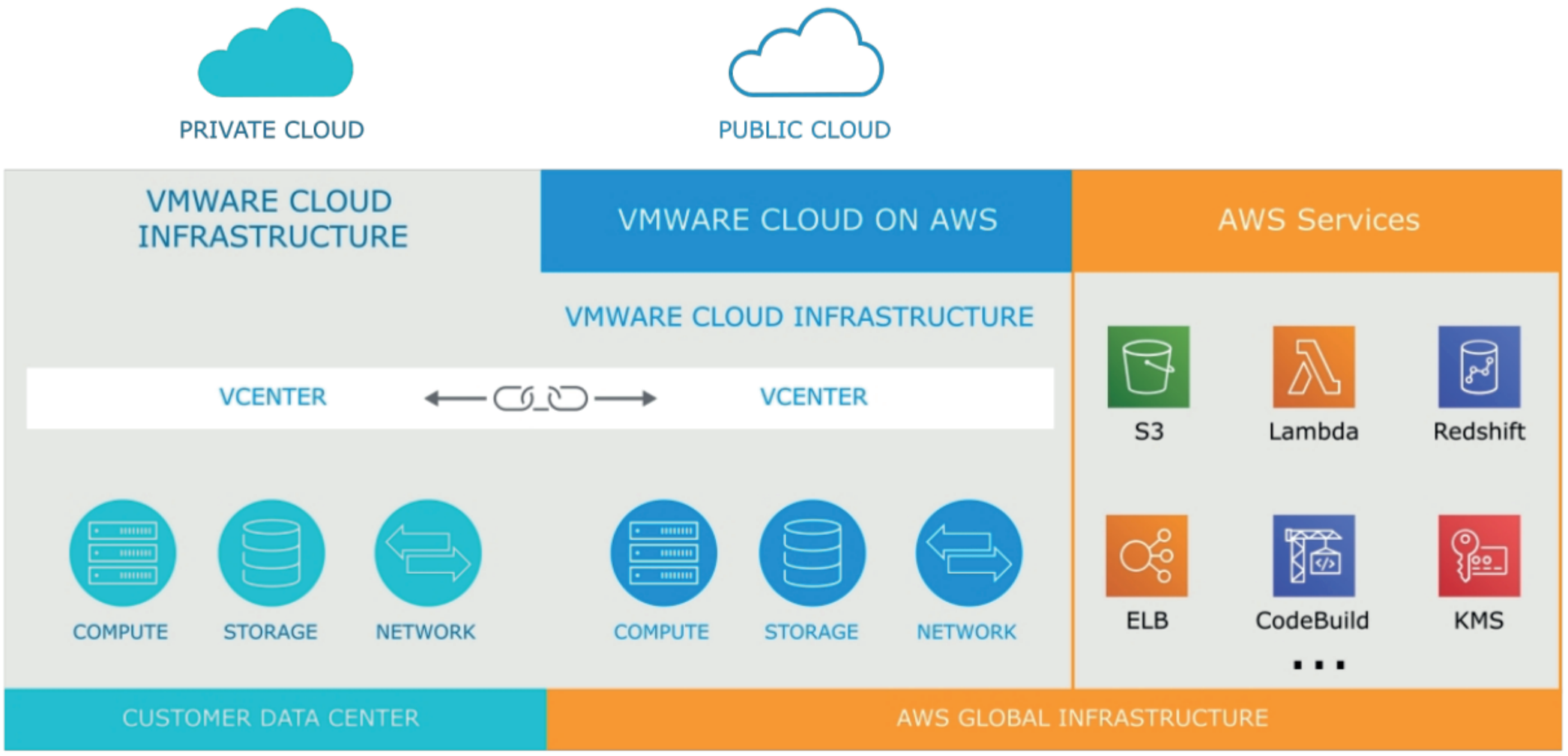
Integration with VCD allows you to map VCD components with VMware Aria Automation for provisioning and management of resources.

In VMware Cloud Director, an organization contains users, the vApps, and the resources the vApps use.

You configure image or flavor mappings and create a cloud template in the same way as any cloud account. The resources are deployed on the organization defined in the cloud account.

10-19 VMware Cloud on AWS

VMware Cloud on AWS brings enterprise-class VMware SDDC software to the AWS cloud with optimized access to AWS services.



VMware Cloud on AWS is an integrated cloud offering jointly developed by AWS and VMware. You can deliver a highly scalable and secure service by migrating and extending your on-premises environments based on vSphere to the AWS cloud running on Amazon Elastic Compute Cloud (Amazon EC2).

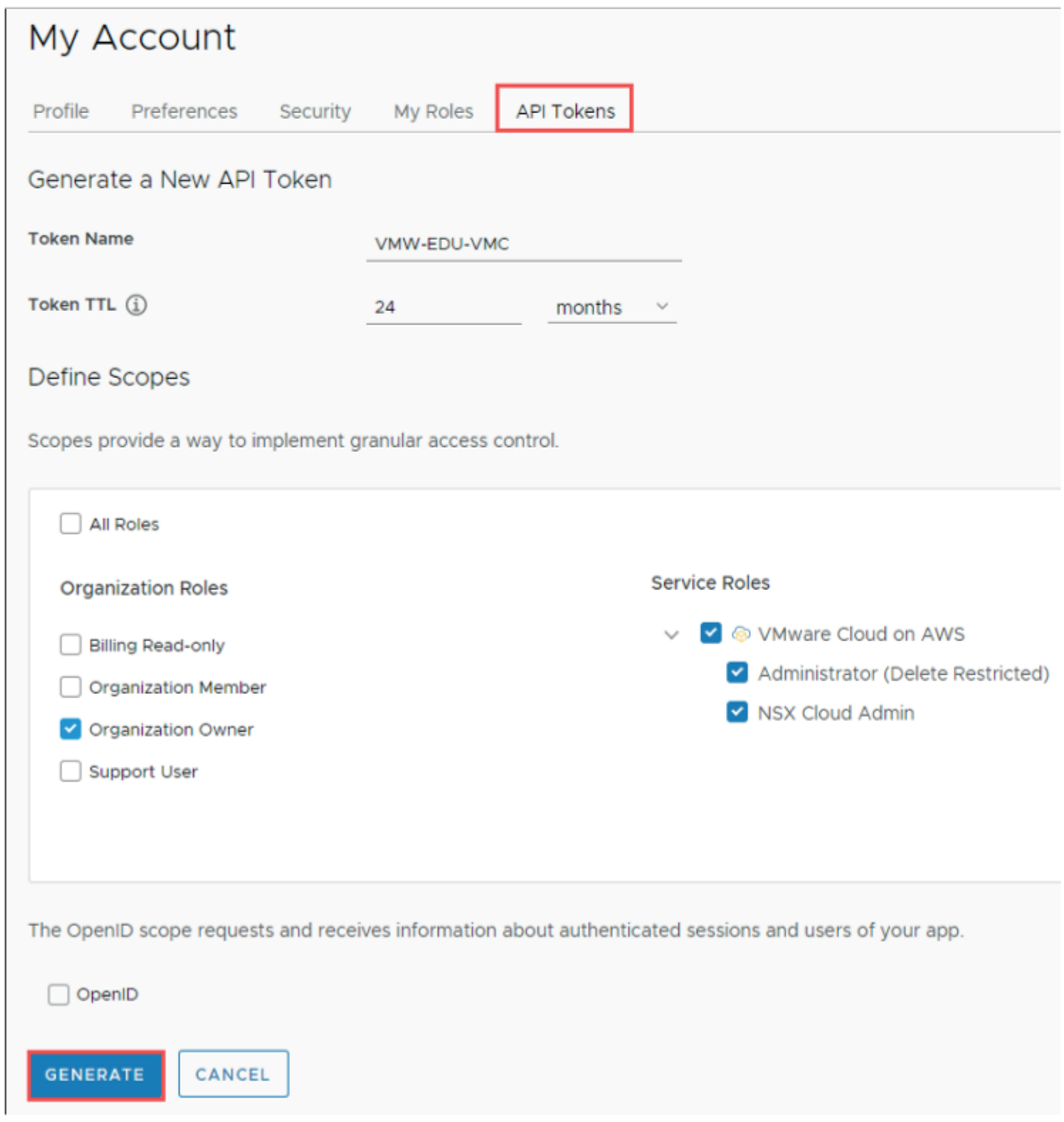
With the same architecture and operational experience on-premises and in the cloud, you can quickly derive business value from the VMware and AWS hybrid cloud experience.

10-20 VMware Cloud on AWS: Credentials

The VMware Cloud on AWS cloud account requires an API token.

To generate an API token:

1. On the VMware Cloud Services toolbar, click your user name and select **My Account** > **API Tokens**.
2. Enter the token name.
3. Specify the lifespan of the token.
4. Define scopes for the token.
5. Click **GENERATE**.



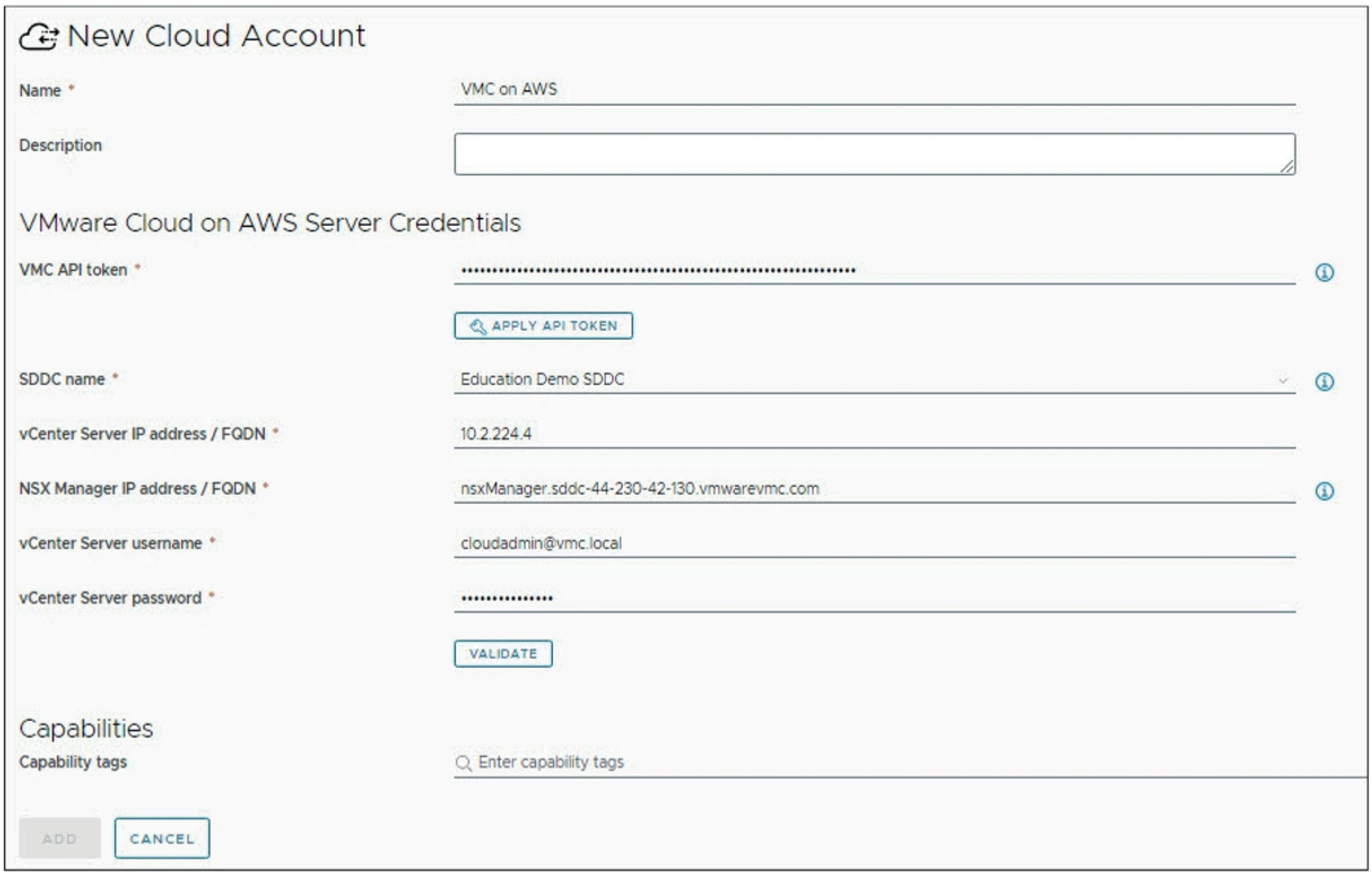
You use API tokens to authenticate yourself when you make authorized API connections.

For security reasons, only the token name is displayed after you generate the token. The token credentials are not displayed. You can reuse the token by copying the credentials from this page. You can regenerate a token at any time.

10-21 VMware Cloud on AWS: Cloud Account

To create a VMware Cloud on AWS cloud account:

1. Log in to the VMware Aria Automation console as an administrator and select **Infrastructure** > **Connections** > **Cloud Accounts**.
2. Click **ADD CLOUD ACCOUNT** and then click **VMware Cloud on AWS**.
3. Enter the VMC API token and then click **APPLY API TOKEN**.
4. Select the appropriate SDDC from the drop-down menu.
5. Enter the vCenter Server credentials for the selected SDDC.
6. Click **VALIDATE**.



If the specified API token is validated, all the SDDCs from VMware Cloud on AWS are acquired. Selecting the appropriate SDDC autofills the vCenter IP address and the NSX Manager IP address.

Configure image or flavor mappings and create a cloud template in the same way as a vSphere cloud account. The resources are deployed on the SDDC defined in the cloud account.

10-22 Lab 23: (Simulation) Configuring the VMware Cloud Foundation Account

Create a VMware Cloud Foundation cloud account and deploy a VMware Aria Automation template:

1. Create an SDDC Integration
2. Create a VMware Cloud Foundation Cloud Account
3. Add an Image Mapping
4. Create a Flavor Mapping
5. Add a Network Profile
6. Add a Storage Profile
7. Create a Project
8. Create and Deploy a VMware Aria Automation Template
9. Verify Your Deployment

10-23 Lab 24: (Simulation) Configuring Public Cloud Accounts

Create a public cloud account and deploy a VMware Aria Automation template:

1. Create a Public Cloud Account
2. Create a Project and Add a Cloud Zone
3. Create a Flavor Mapping
4. Create an Image Mapping
5. Create a VMware Aria Automation Template
6. Deploy the Resource

10-24 Review of Learner Objectives

- Describe the public cloud accounts supported by VMware Aria Automation
- Create an AWS public cloud account
- Create a Microsoft Azure public cloud account
- Create a Google Cloud Platform public cloud account
- Create a VMware Cloud Foundation public cloud account
- Create a VMware Cloud Director public cloud account
- Create a VMware Cloud on AWS public cloud account

10-25 Key Points

- VMware Aria Automation natively supports AWS, Microsoft Azure, Google Cloud Platform, VMware Cloud Foundation, and VMware Cloud on AWS public cloud accounts.
- Various credentials are required for the different public cloud accounts. These credentials must be acquired from the administration consoles of each public cloud account.

Questions?

Module 11

Using VMware Aria Automation Consumption

11-2 Importance

Using VMware Aria Automation Assembler, you can create VMware Aria Automation templates and deploy services from VMware Aria Automation templates. Administrators can use VMware Aria Automation Consumption to create a catalog of services and enforce governance to users who use resources from the self-service catalog.

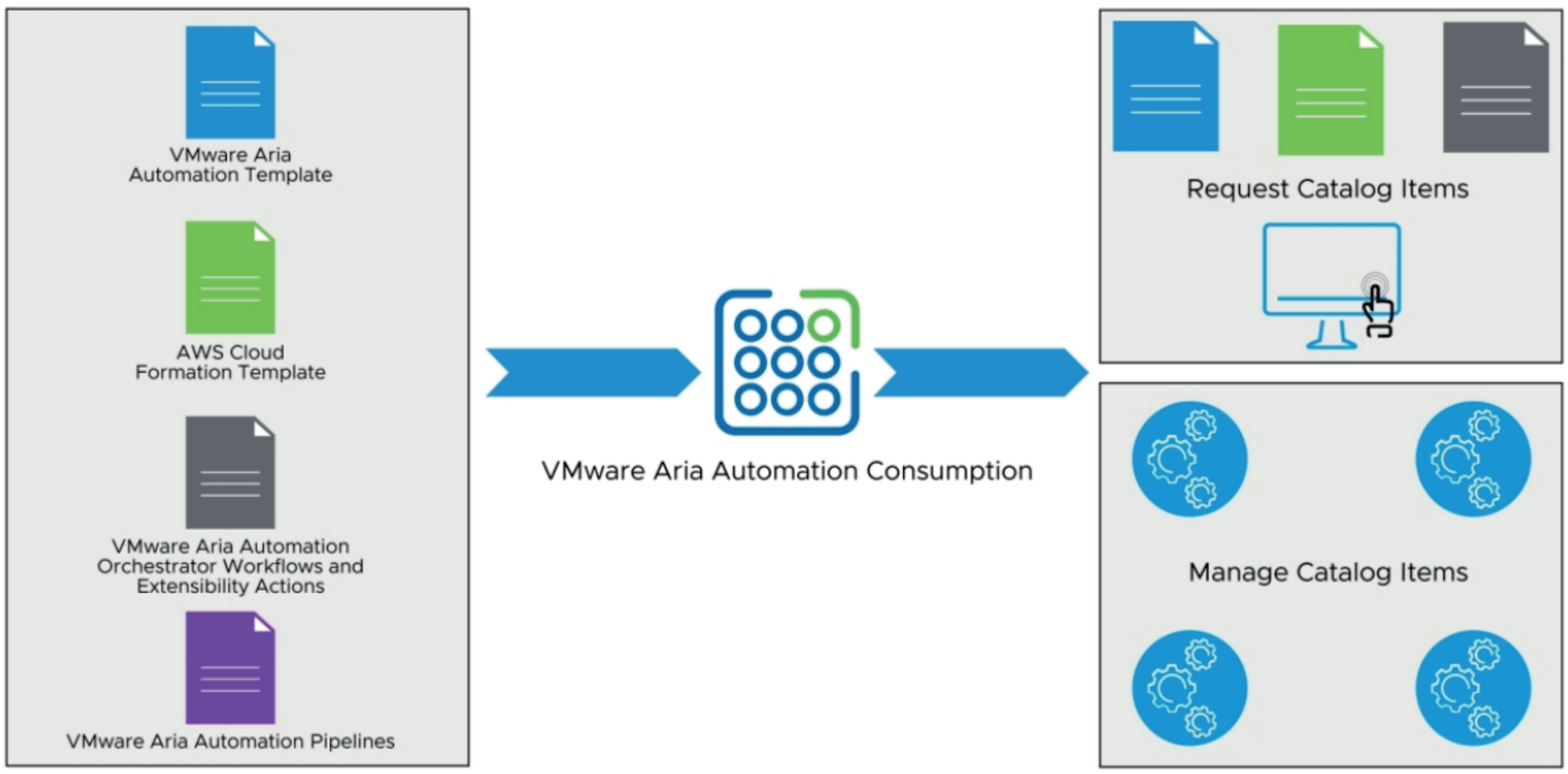
11-3 Lesson 1: Using VMware Aria Automation Consumption

11-4 Learner Objectives

- Explain the purpose of Using VMware Aria Automation Consumption
- List the supported content sources
- Explain the process for creating catalog items
- Request catalog items from the self-service catalog
- Monitor and manage the catalog items
- Describe the policy types
- Configure a custom form for a VMware Aria Automation template

11-5 Use Case: VMware Aria Automation Consumption

VMware Aria Automation Consumption offers a single console to request and manage the catalog items from various platforms.



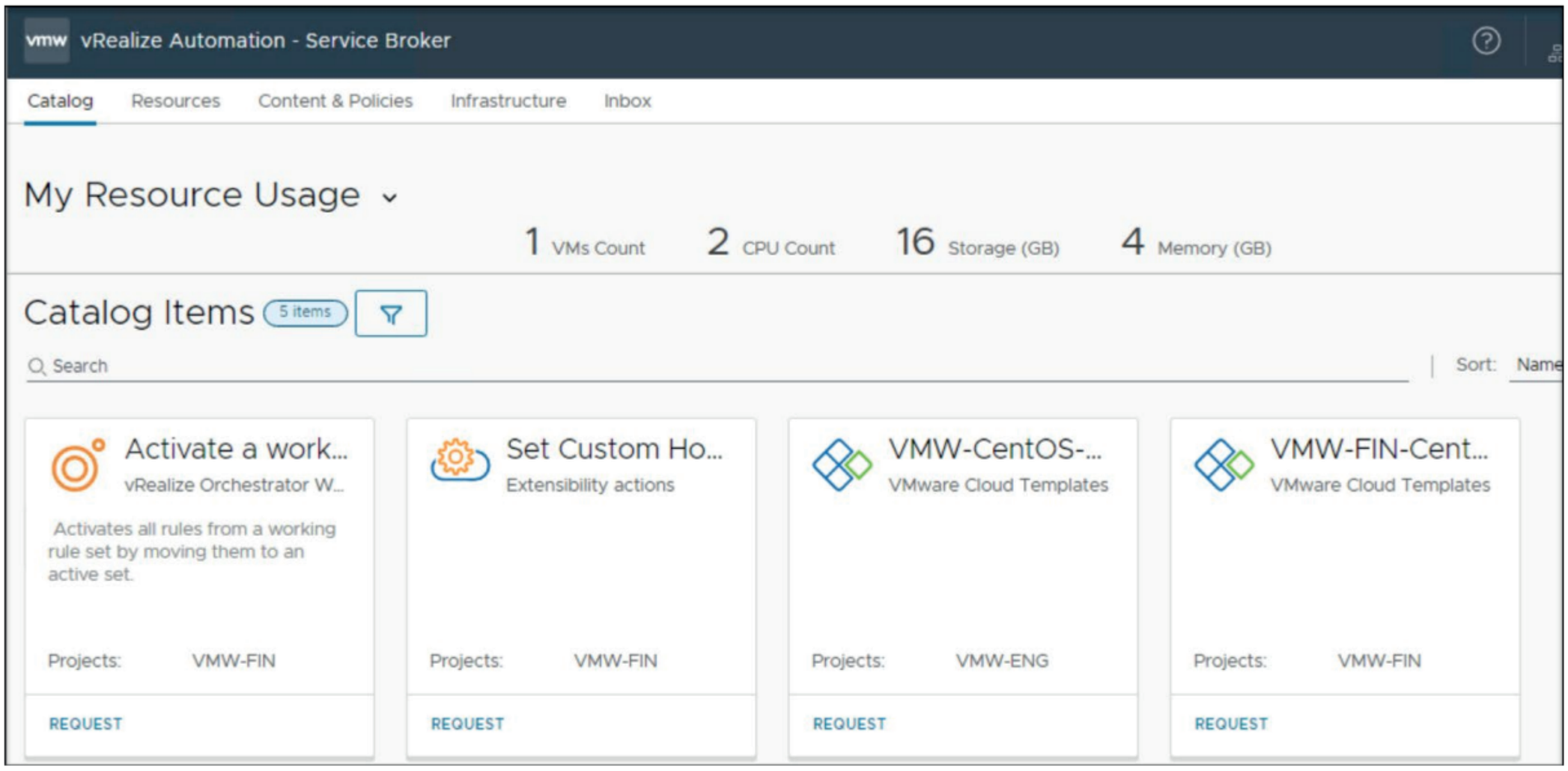
A VMware Aria Automation Assembler user can create VMware Aria Automation templates. You use VMware Aria Automation Consumption to ensure that the users can request, use, and manage catalog items.

As an organization administrator, you create catalog items by importing the templates from various supported sources that your users can deploy to cloud vendor regions.

As a user, you can request and monitor the provisioning process. After deployment, you manage the deployed catalog items throughout the deployment life cycle.

11-6 Self-Service Catalog

VMware Aria Automation templates that are released to VMware Aria Automation Consumption are available in the self-service catalog. Members of the configured project can deploy services from the **Catalog** tab.



Catalog items can include VMware Aria Automation templates, vRealize Orchestrator workflows, extensibility actions, Amazon CloudFormation templates, VMware Aria Automation pipelines, and other deployable templates. A catalog item is the specification for one or more machines, networks, and other components that you deploy to a cloud vendor.

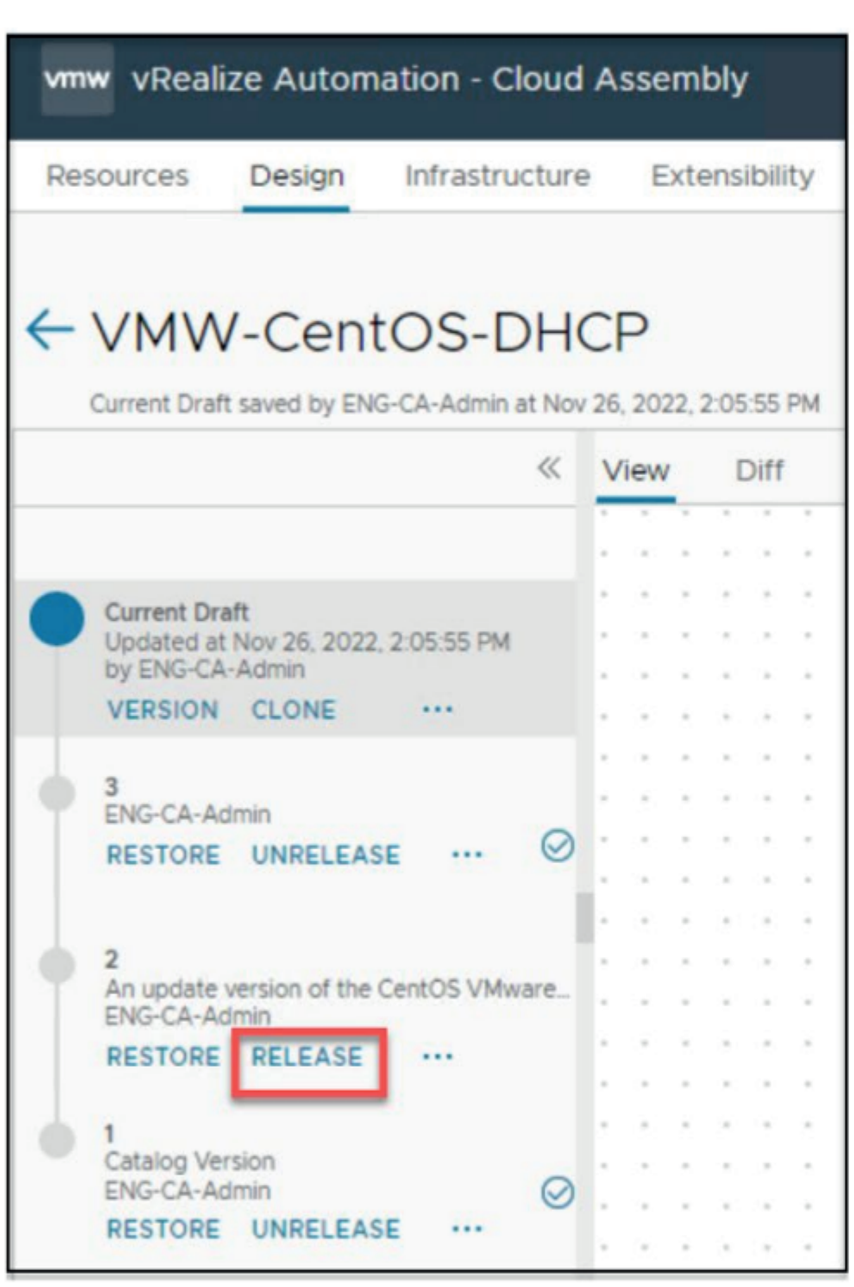
Your cloud administrator determines your access to different items and where you can deploy them.

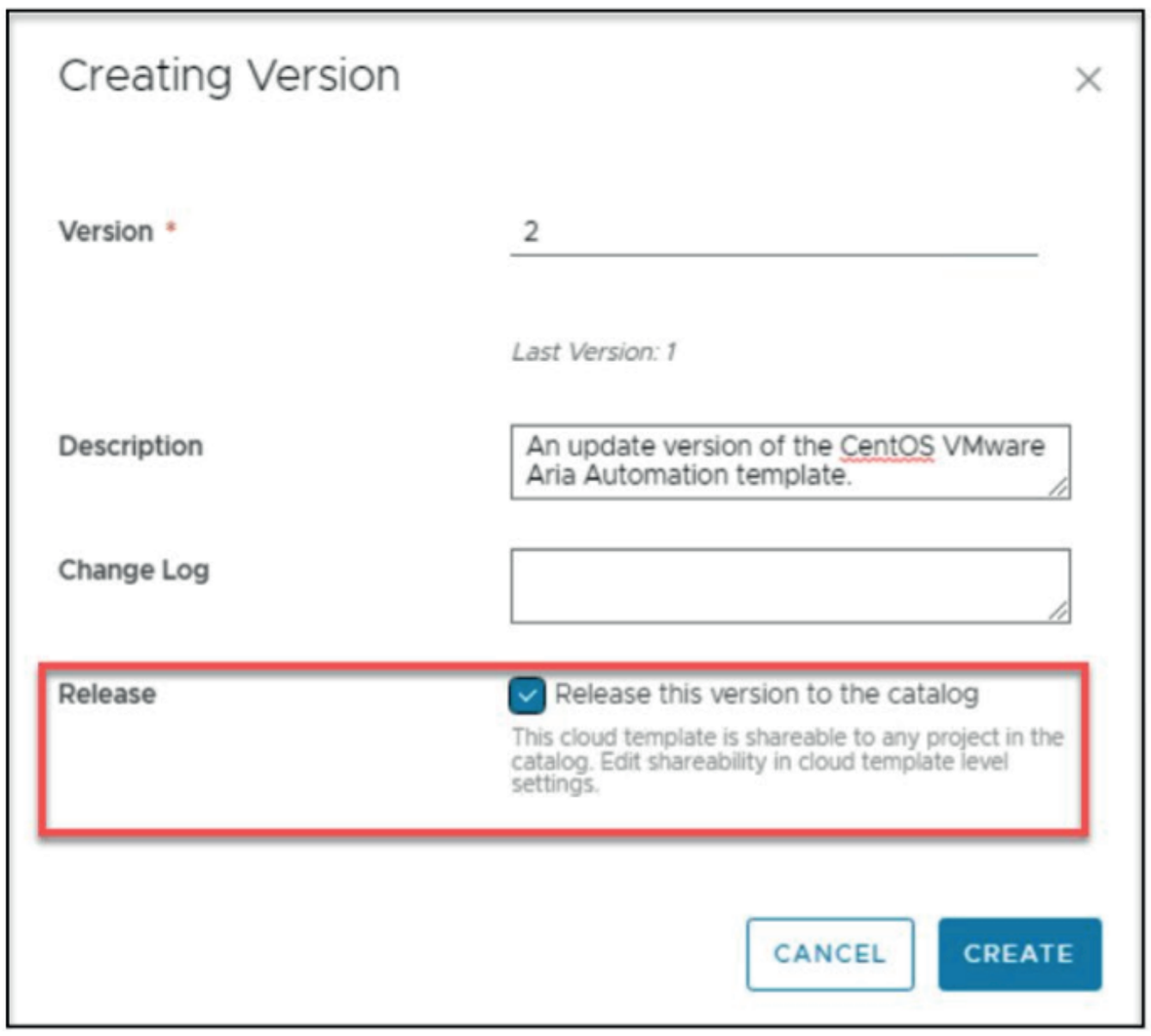
11-7 Releasing VMware Aria Automation Templates

VMware Aria Automation templates must be released for import to VMware Aria Automation Consumption.

Select **VERSION HISTORY** and click **RELEASE** to release an older version of a VMware Aria Automation template.

Alternatively, click **VERSION** and select the **Release this version to the catalog** check box to release the current draft.



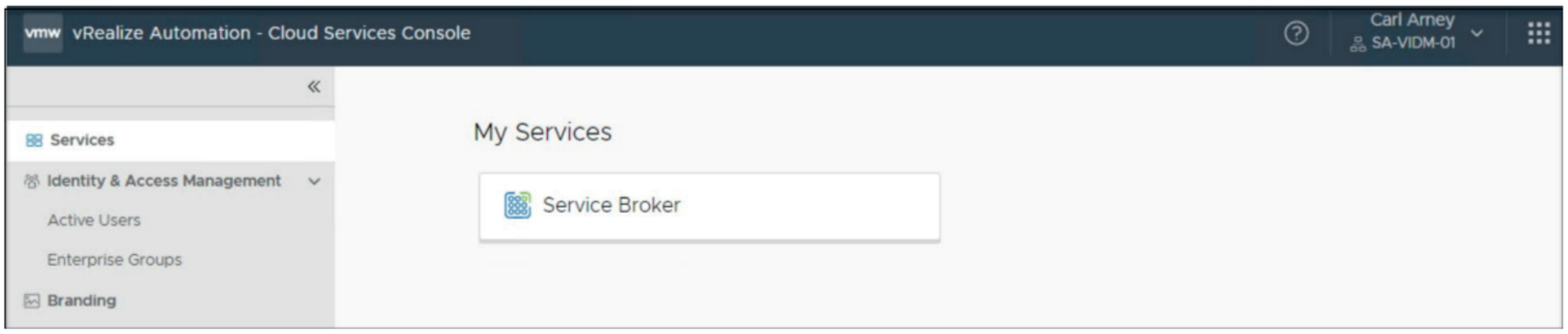


Released VMware Aria Automation templates have a check box, and you can use **UNRELEASE** to remove a VMware Aria Automation template from the VMware Aria Automation Consumption service catalog.

You can release the VMware Aria Automation template only if it is versioned.

11-8 Accessing VMware Aria Automation Consumption

Log in to the VMware Aria Automation console as a user with one of the assigned VMware Aria Automation Consumption roles. Based on the assigned role, a user can access VMware Aria Automation Consumption features.



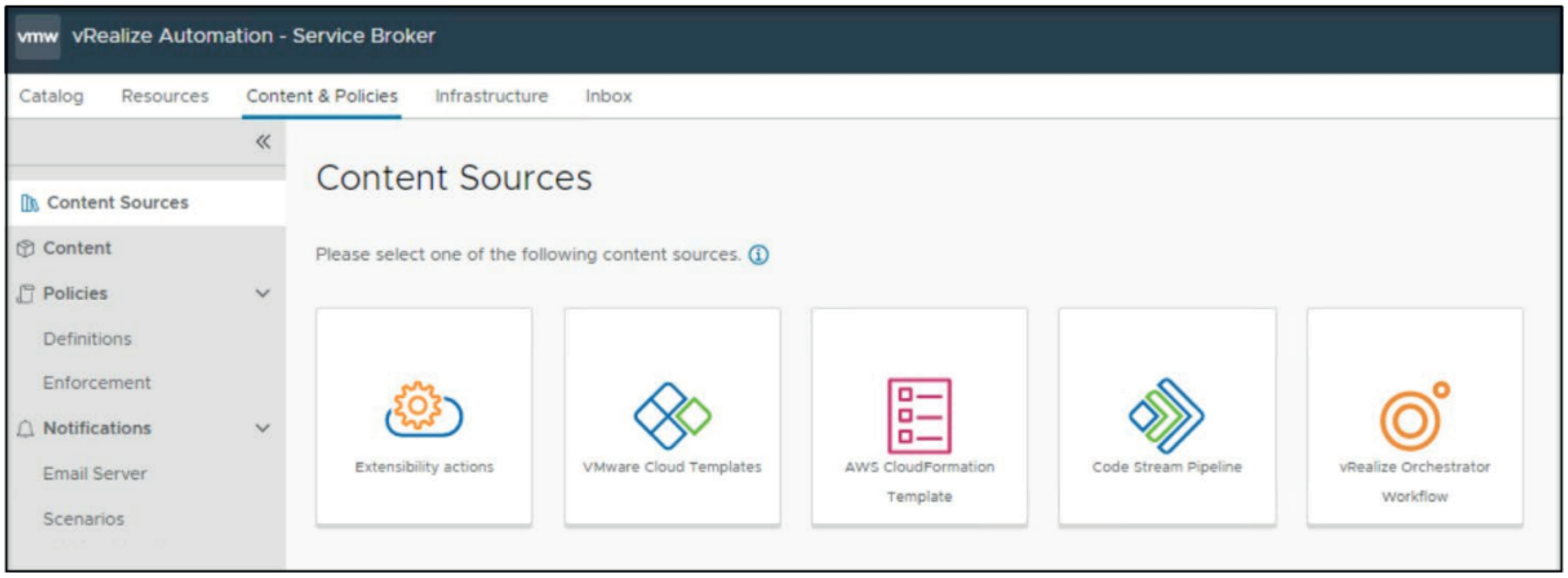
One of the VMware Aria Automation Consumption roles must be assigned to view VMware Aria Automation Consumption in the My Services list.

11-9 Content Sources

A content source defines the origin of importing the VMware Aria Automation templates to a Service Catalog.

Only the released VMware Aria Automation templates from the selected project are imported.

The imported VMware Aria Automation templates appear under the Content section in the left pane.



After you add the content source, templates are refreshed every six hours. Changes to templates in your external sources are reflected in the catalog after a refresh.

If you add a new template or change a template, and must see the changes before a standard refresh, you can edit the content sources and click **Save and Import**.

When you delete a content source, the imported items are deleted from the catalog. The VMware Aria Automation templates remain intact.

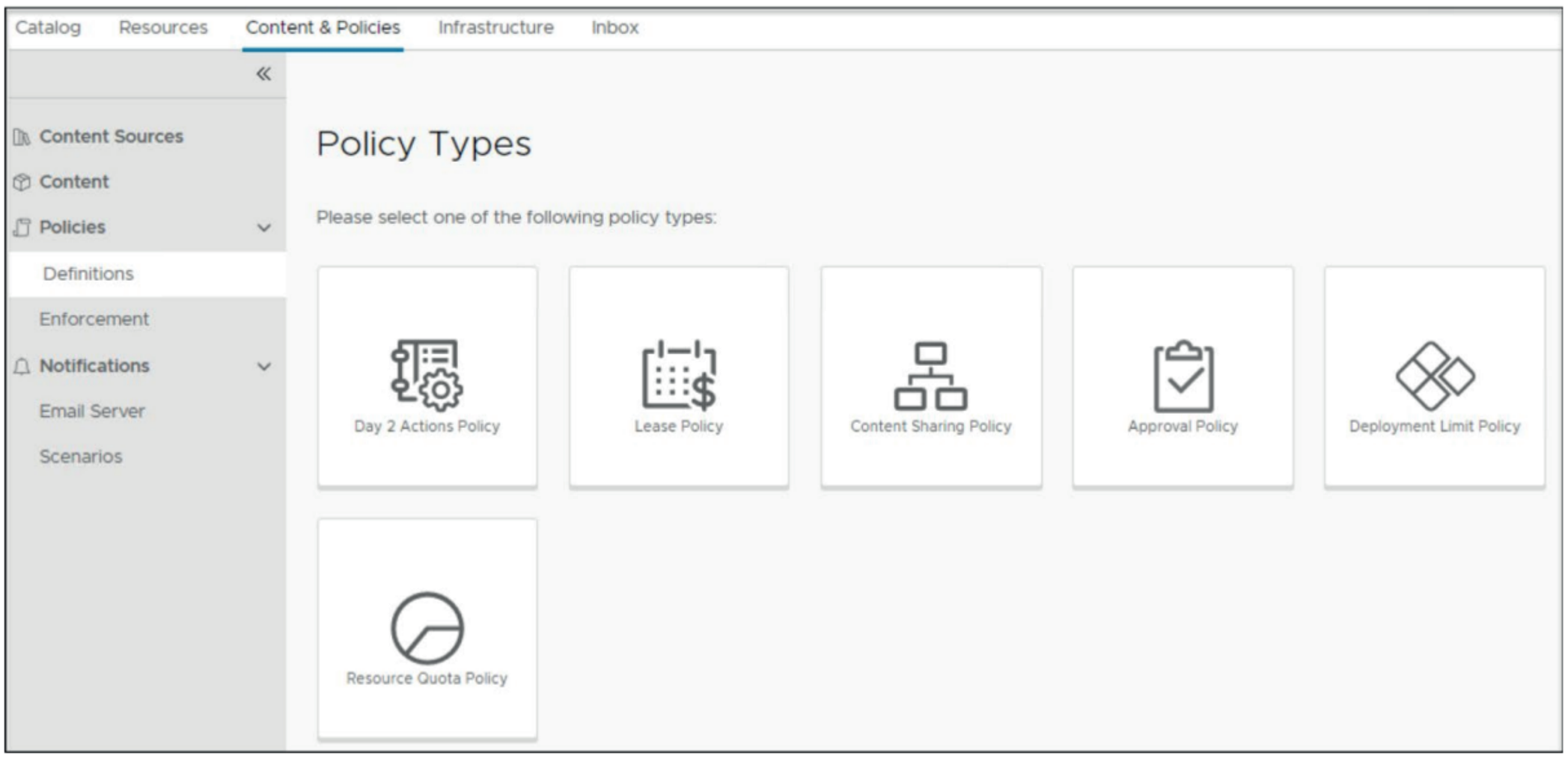
11-10 Policy Definitions

Policies are a set of rules or parameters that are applied to enable governance and process your deployments.

Click the **Content & Policies** tab and navigate to **Policies** > **Definitions**.

The following policy types are available:

- Day-2 Actions Policy
- Lease Policy
- Content Sharing Policy
- Approval Policy
- Deployment Limit Policy
- Resource Quota Policy



The policy that you create is applied to new deployments and to current deployments. If you create a policy, wait for VMware Aria Automation Consumption to evaluate, and process the policy.

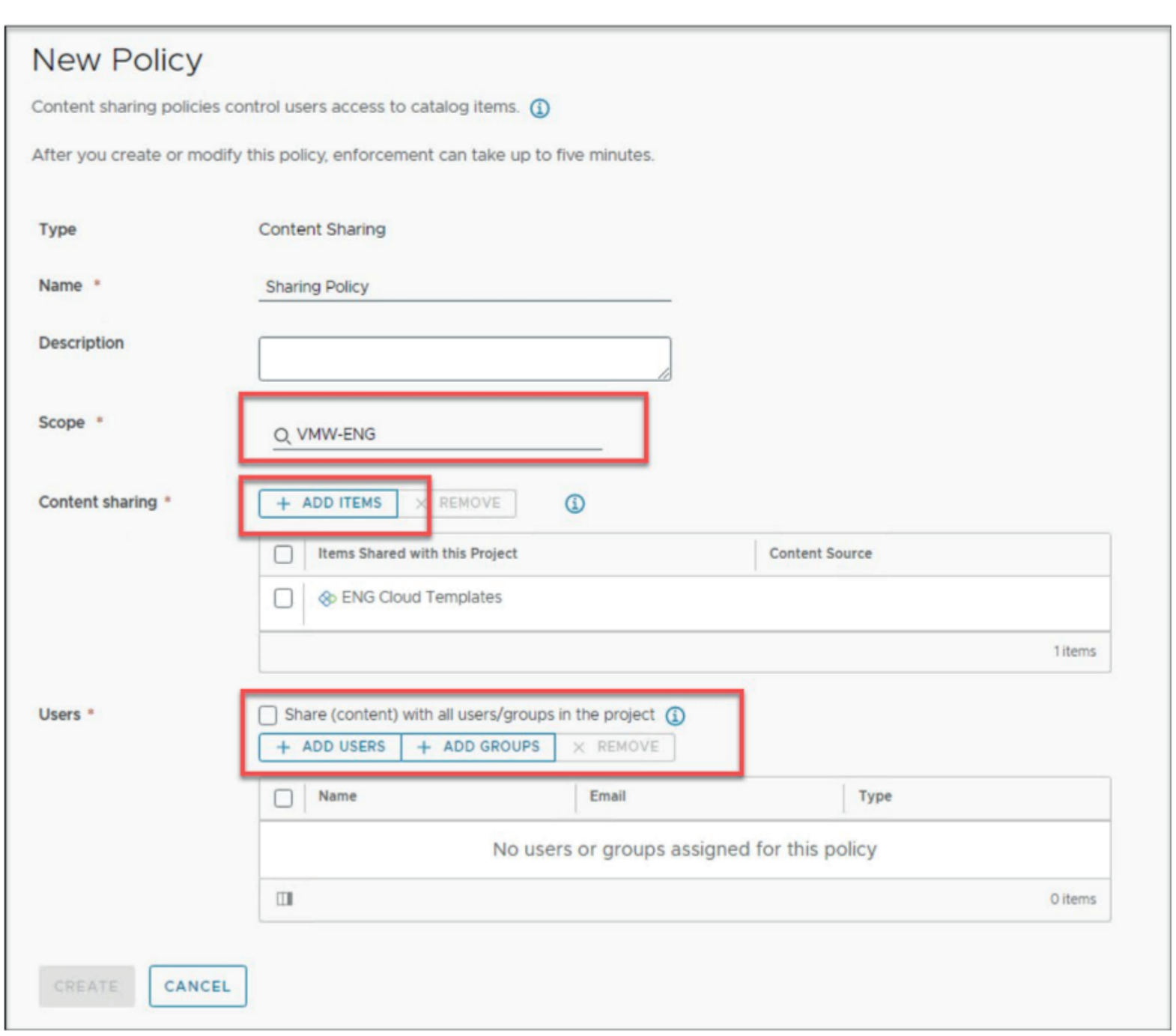
11-11 Policy Type: Content Sharing

Create a content sharing policy to make the imported VMware Aria Automation templates available to project members.

Select the project whose VMware Aria Automation templates must be shared.

Click **ADD ITEMS** and select the released VMware Aria Automation templates.

Select the users who can view and request the VMware Aria Automation templates as catalog items.



Select the project, select the content, and select the members you want to share.

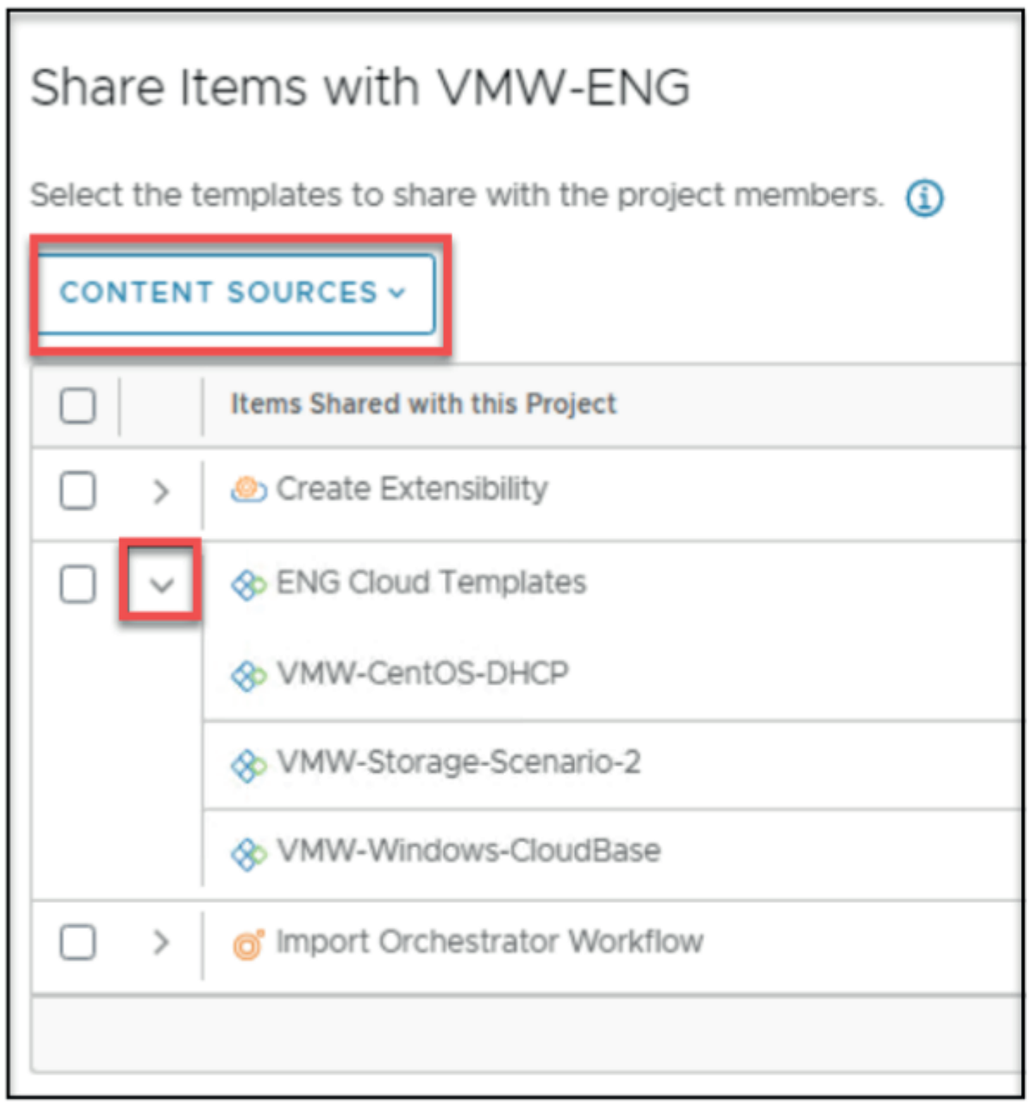
Selected users can deploy the shared templates from the catalog.

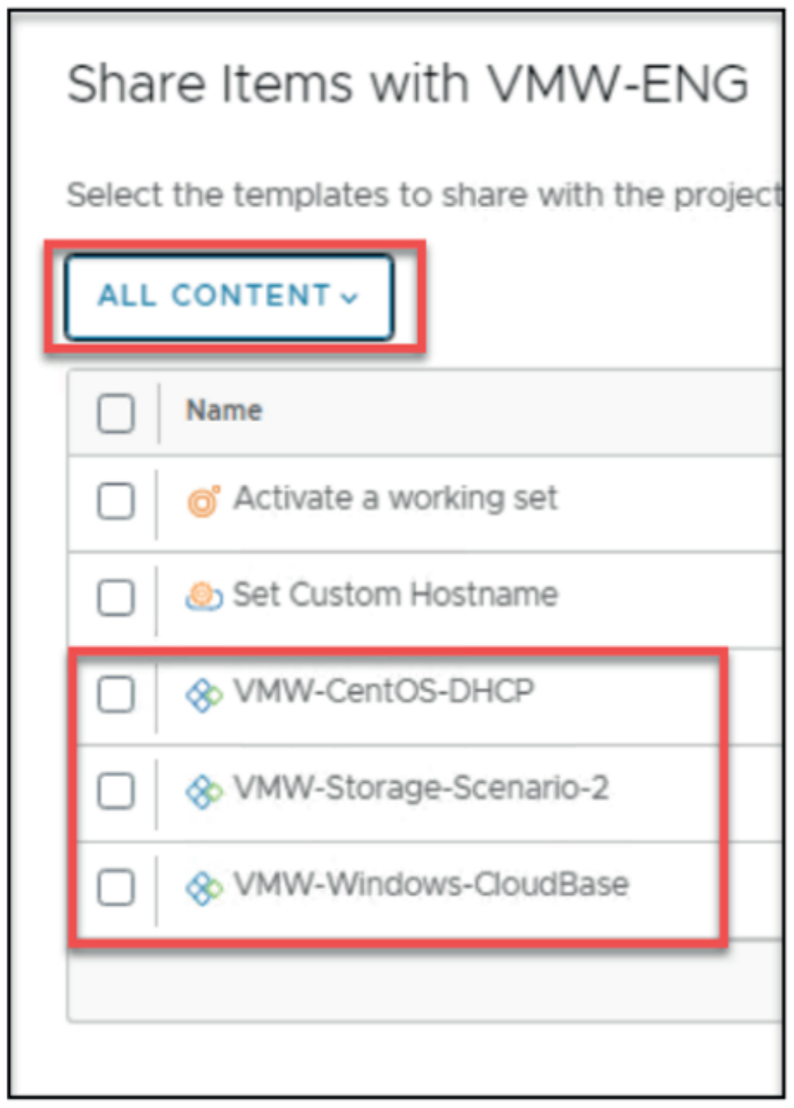
Select the **share (content) with all users/groups in the project** check box to share the content with all project members.

11-12 Content Sharing: Options

VMware Aria Automation templates can be shared in the following ways:

- **Content Sources**: Dynamic method of sharing content. If new VMware Aria Automation templates are added to the content source, they are available in the catalog for members of this project.
- **All Content**: Static method of sharing content. If new templates are added to the content source, you add them individually to make them available in the catalog.





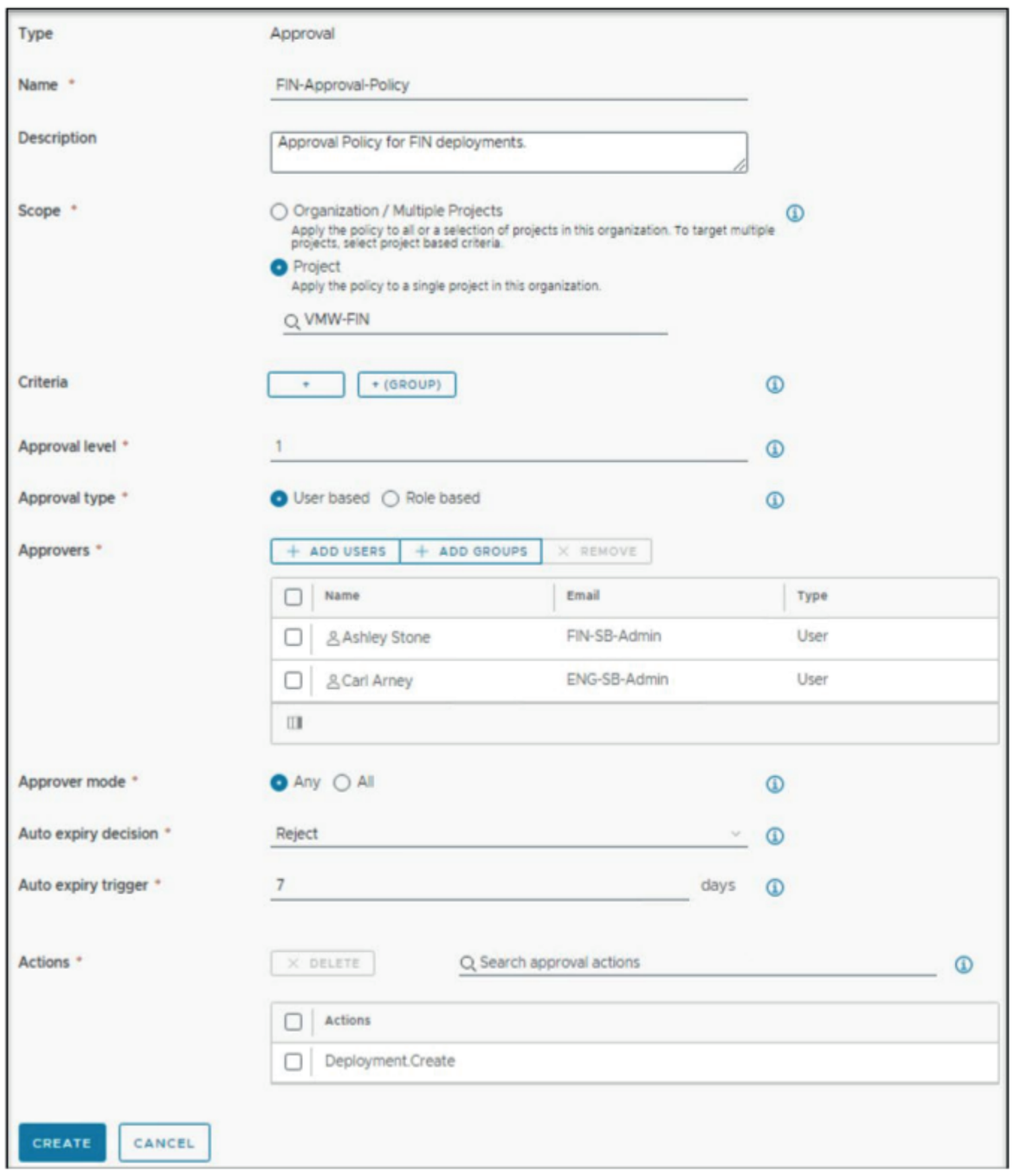
If you share VMware Aria Automation templates, the content list includes VMware Aria Automation templates that are associated with the selected project. The content list might also include VMware Aria Automation templates that are explicitly shared with other projects in your organization.

11-13 Policy Type: Approval Policy

Configure an approval policy to have governance and control over deployment requests and Day-2 action requests.

Use cases:

- Approve a deployment that consumes large resource.
- Approve the Day-2 action of a deployment that users use.



The VMware Aria Automation Consumption administrator is responsible for configuring an approval policy. Policies are applied to resources that are used by catalog users.

Scope: The scope determines if the policy is applicable to all deployments in the organization or only to deployments in a selected project.

Criteria: If you want to further refine when the policy is applied in the selected scope, you add a policy criterion. The policy criteria are a logical expression. For example, if you set the scope to organization and you want to apply a policy to all the deployments except the deployments named pipeline test, you enter the **name not equal "pipeline test"** criteria. If a deployment is named pipeline prod, the policy is applied. If it is named pipeline test, the policy is not applied. You can create one criterion or a group of criteria.

Approval level: Determines if multilevel approval is used. Enter a level value between **1** to **99** to prioritize policies. Approval policies are evaluated in an ascending level order. If the first level of approval is rejected, the request is rejected. If the first level of approval is accepted, the second level of approval is evaluated and so on.

Approver mode:

- **Any**: Only one approver must approve the request before it is processed.
- **All**: All approvers must respond with the same response before the request is processed. If one approver rejects the request, the request is denied, and the user is notified.

Approval type: Choose whether you want to assign the approval role to specific users or based upon assigned roles.

Approvers: Add the name or email address for each approver. The approval request is sent to all approvers at the same time.

An approver, who might not be a regular VMware Aria Automation Consumption or VMware Aria Automation Assembler user, must have one of the following combination of roles:

- Organization member and VMware Aria Automation Consumption user
- Organization member and the Manage Approvals custom role

The roles provide the minimum level of permissions and still allow you to approve or reject a request.

Auto expiry decision: Automatically approve or reject a request after the number of days specified in the Auto expiry trigger field.

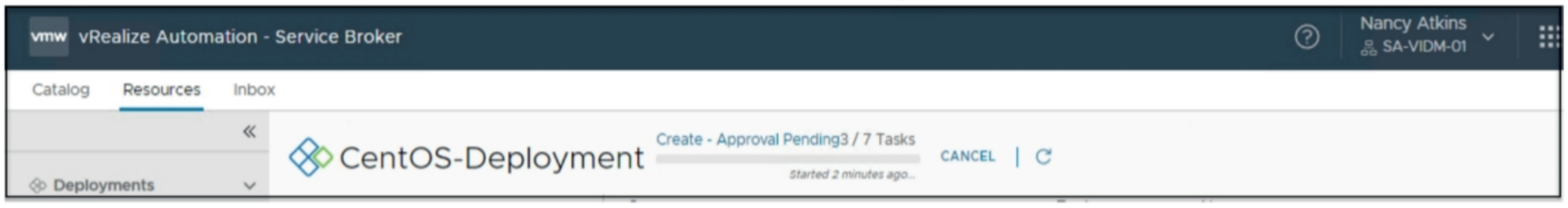
- **Approve**: The request is approved if an approver does not respond in the specified time.
- **Reject**: The request is denied if an approver does not respond in the specified time.

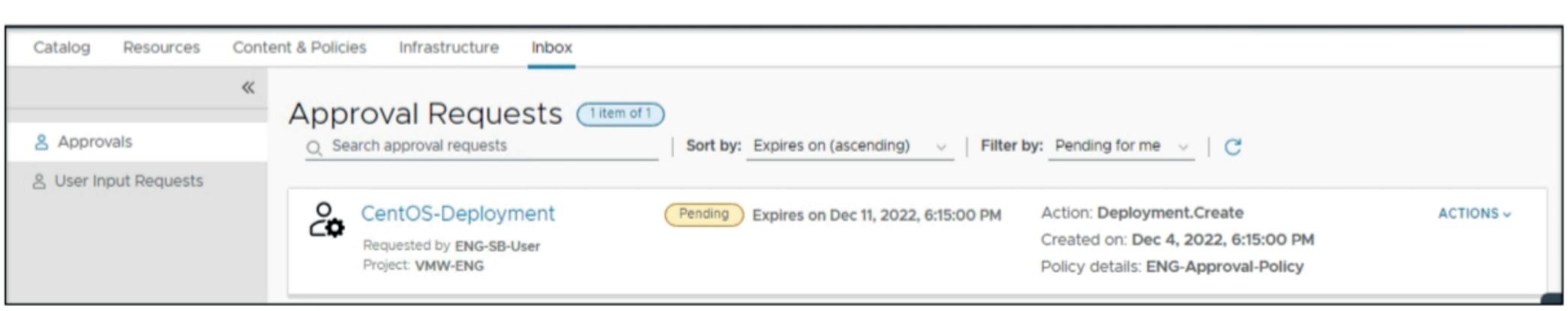
Auto expiry trigger: The number of days the approvers must respond before the Auto expiry decision is triggered. The value should be in the range of 1 through 7 days.

Actions: Select one or more actions to which the policy applies. The actions include deployments and component level Day-2 actions.

11-14 Approval Requests

When a deployment or Day-2 action request from a catalog user matches the approval policy criteria, the request is sent to approvers.





The catalog user must wait for the approvers to approve their requests. Users can monitor the approval request from the **Inbox** > **Approval** tab.

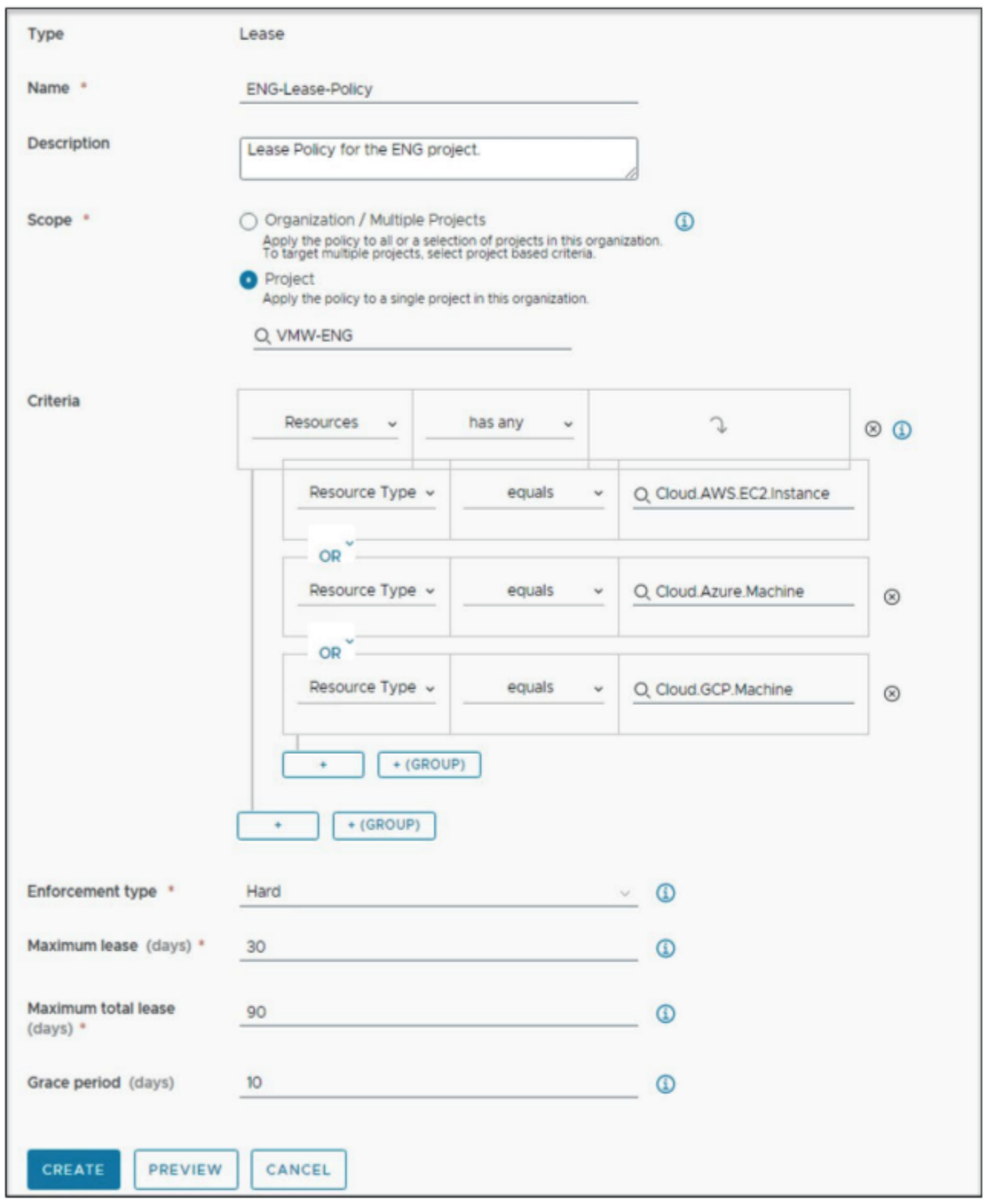
All approvers receive a notification with the approval details. The approver must log in to Service Broker and use the **Inbox** >**Approvals** tab to accept or reject a request.

The catalog user receives an email notification when the approver responds to a request.

11-15 Policy Type: Lease Policy

The lease policy enables administrators to control the time in which deployments are available to users.

If no lease policies are defined, the deployments never expire.



When a lease policy is created or updated, it continuously evaluates the deployments in the background to ensure that they comply with the defined leases.

Enforcement type: Enforcement is hard or soft. Hard policies are ranked higher than soft policies. Hard policies override soft policies. If a conflict occurs between a soft lease policy applied to an organization and a soft lease policy applied to a project, the project lease policy takes precedence because it is more specific.

Maximum lease (days): The maximum number of days that a deployment can be active initially at the deployment time or when users extend a lease, for example, 30 days.

Maximum total lease (days): The combined total number of days that the deployment can be active, including lease renewals. The cumulative renewal value cannot exceed the maximum total lease. For example, the deployment is shut down after 30 days and an email is sent to the user. If the user does not extend the lease, the deployment is destroyed after the grace period is finished.

If the user extends the lease for 30 more days, and another 30 days, for a combined total of 90 days, the maximum lease time is reached at day 90, and the deployment is shut down.

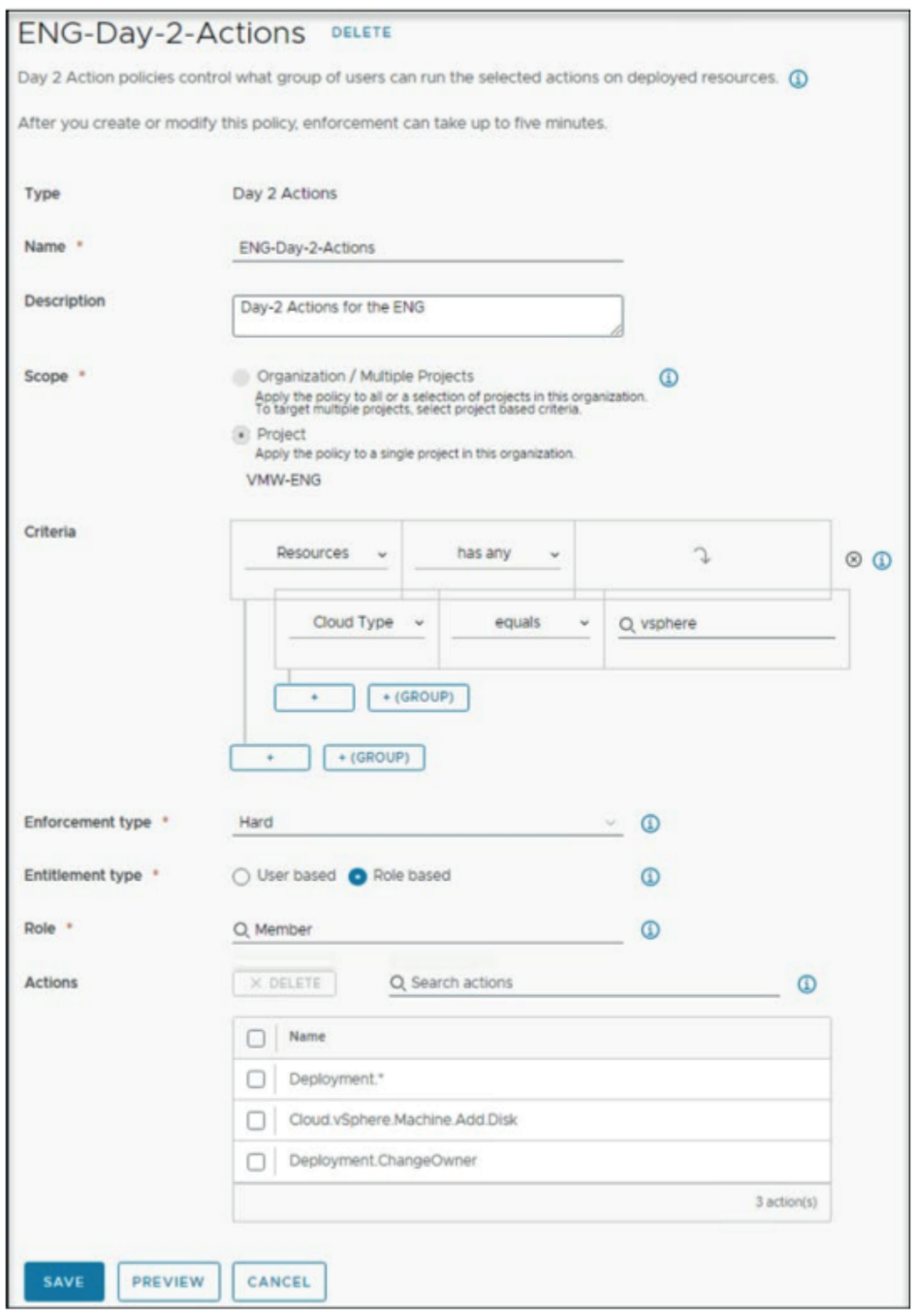
Grace period (days): The number of days after a lease expires before it is destroyed. The grace period allows users to extend the lease for another block of time that does not exceed the Total Lease value, for example, 10 Days.

The grace period is not included in the total lease days.

11-16 Policy Type: Day 2 Actions Policy

Day 2 action policies enable the administrator to control changes that users can make to deployments and their component resources.

If no day 2 action policies are defined, no governance is applied, and all users have access to all the actions.



For the **Entitlement type**, you can choose between the following options:

- **User based**: You can entitle specific users to run day 2 actions.
- **Role based**: You can entitle users to run actions based on roles. To grant certain action privileges to a role, you can create a policy for that role.
  - **Administrator**: Enables the project administrators associated with the deployment to run the selected actions. Administrators can run any action that their project members run.
  - **Member**: Enables the project members associated with the deployment to run the selected actions.

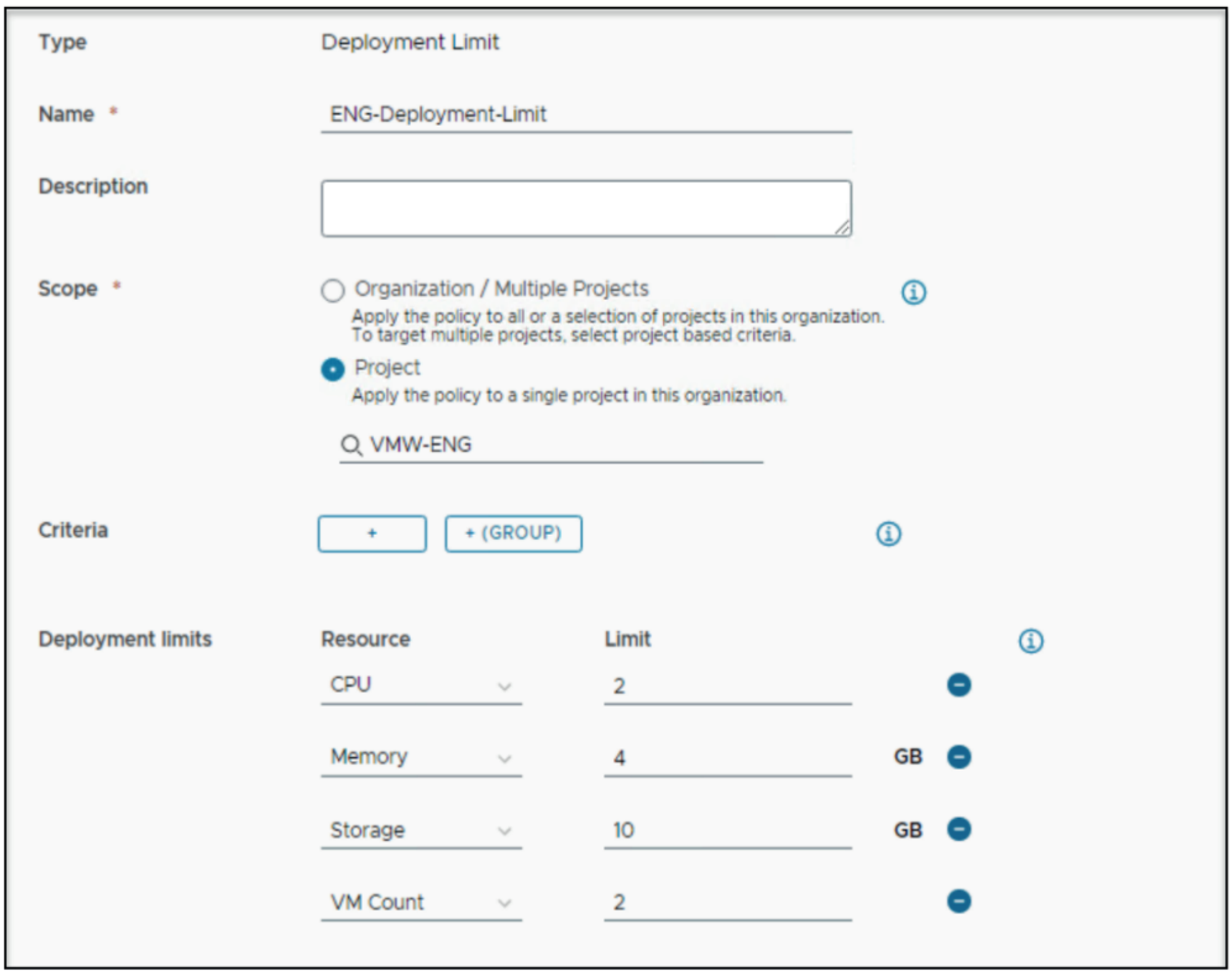
- **Infrastructure Administrator:** Enables the project infrastructure administrators associated with the deployment to run the selected actions. This role is built in and cannot be assigned to users through the UI.
- **Custom Role**: If you have one or more custom roles defined, you can select a named role in the list. The users assigned to the role can run the selected actions on the deployments in their projects.

Actions: Actions are cloud specific. When you enable users to make changes, consider the cloud accounts the entitled users deploy and verify that you select all the cloud-specific versions of the actions. For example, if you want to allow changes to an AWS instance, add the Cloud.AWS.EC2.Instance.Resize action to enable users to resize AWS instances.

11-17 Policy Type: Deployment Limit

Deployment limit policies enable the administrator to control the resources used by the users per deployment.

Using deployment limit policies, administrators can define the maximum total memory, CPU count, storage, and number of virtual machines per deployment.



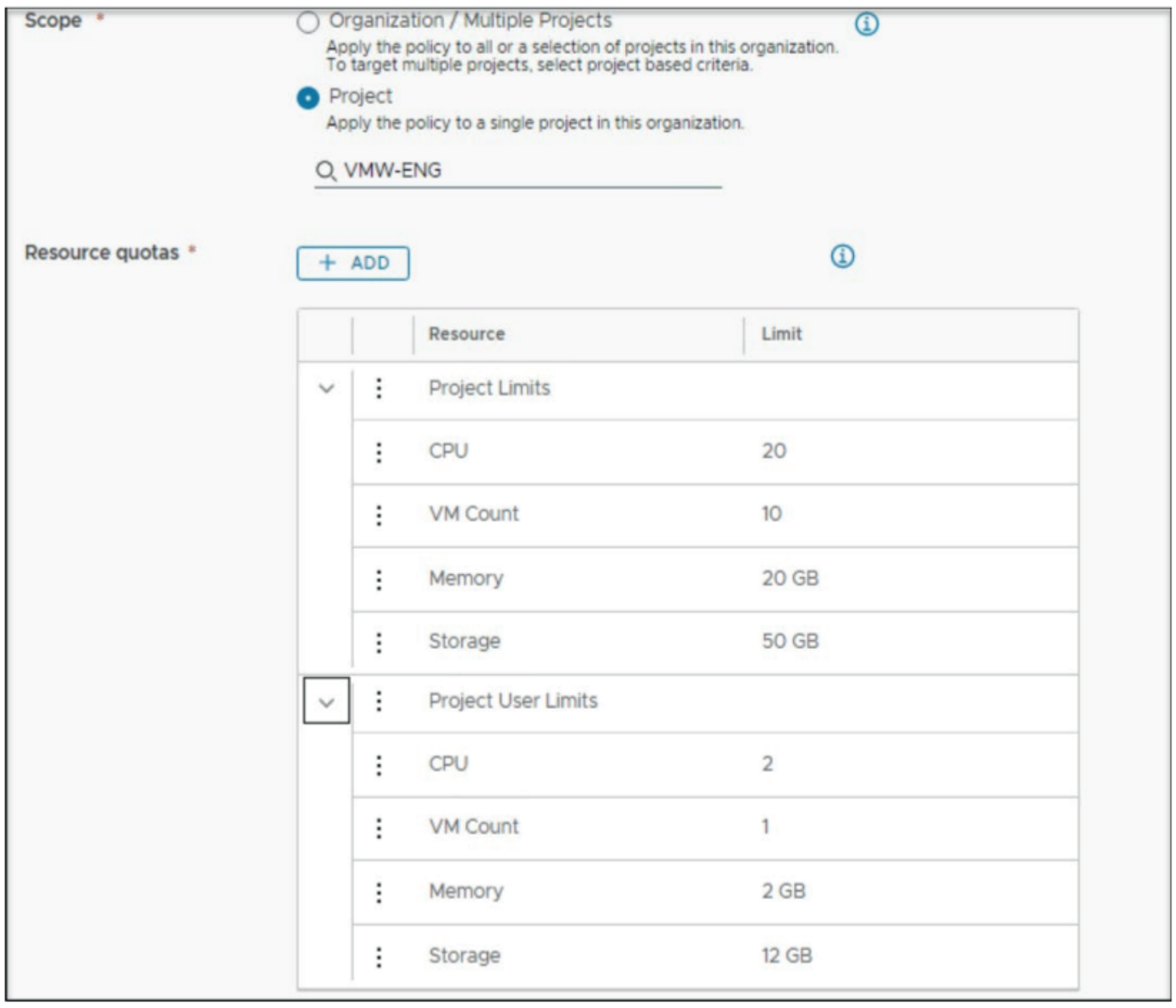
If multiple deployment policies are defined for a deployment, the deployment is evaluated against the lowest limit value for each resource.

Deployment limit policies are evaluated before resource quota policies and approval policies.

11-18 Policy Type: Resource Quota

Configure resource quota policies to have governance and control over the resources used by the users, projects, or the organization.

If no resource quota policies are defined, the users can use all the available resources. Resource quota policies limit the use of the CPU, memory, storage, and number of VMs.



You can define the resource quota policies at various levels:

- Organization: Limits the resource consumption for the whole organization
- Organization User: Limits each organization user resource consumption
- Projects: Limits the resource consumption for a specific project or group of projects
- Projects User: Limits each project user resource consumption

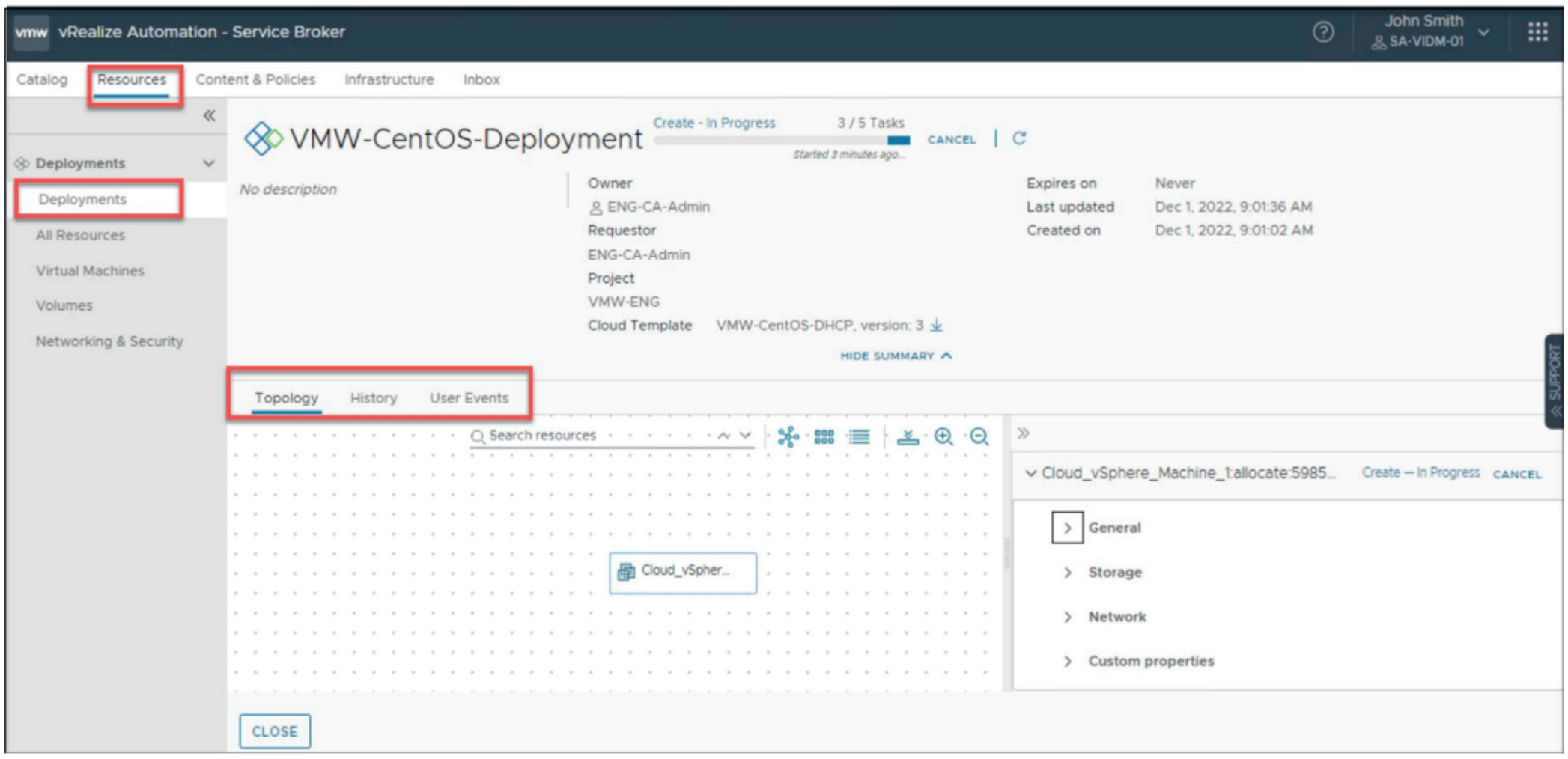
You can define multiple resource quota policies on different scops to provide control over the resource consumption.

In the screenshot example, a resource quota policy is defined for the ENG project and the ENG project users. The example shows the number of VMs that can be deployed by the ENG project is 10 in which each ENG project user can only deploy one machine. A user VM can use only up to 12 GB storage. The project has up to 50 GB storage that can be used by different deployments. The policy allows up to 20 GB of memory to be used by the ENG project while each project user is allowed up to 2 GB of memory consumption.

For more information about configuring and using policies, see the section about setting up policies in *Using and Managing Service Broker* at https://docs.vmware.com/en/vRealize-Automation/index.html.

11-19 Monitoring Deployments

Requests can be monitored on the **Resources** > **Deployments** tab. Click the requested item to view the deployment details.



You have the following tabs to navigate:

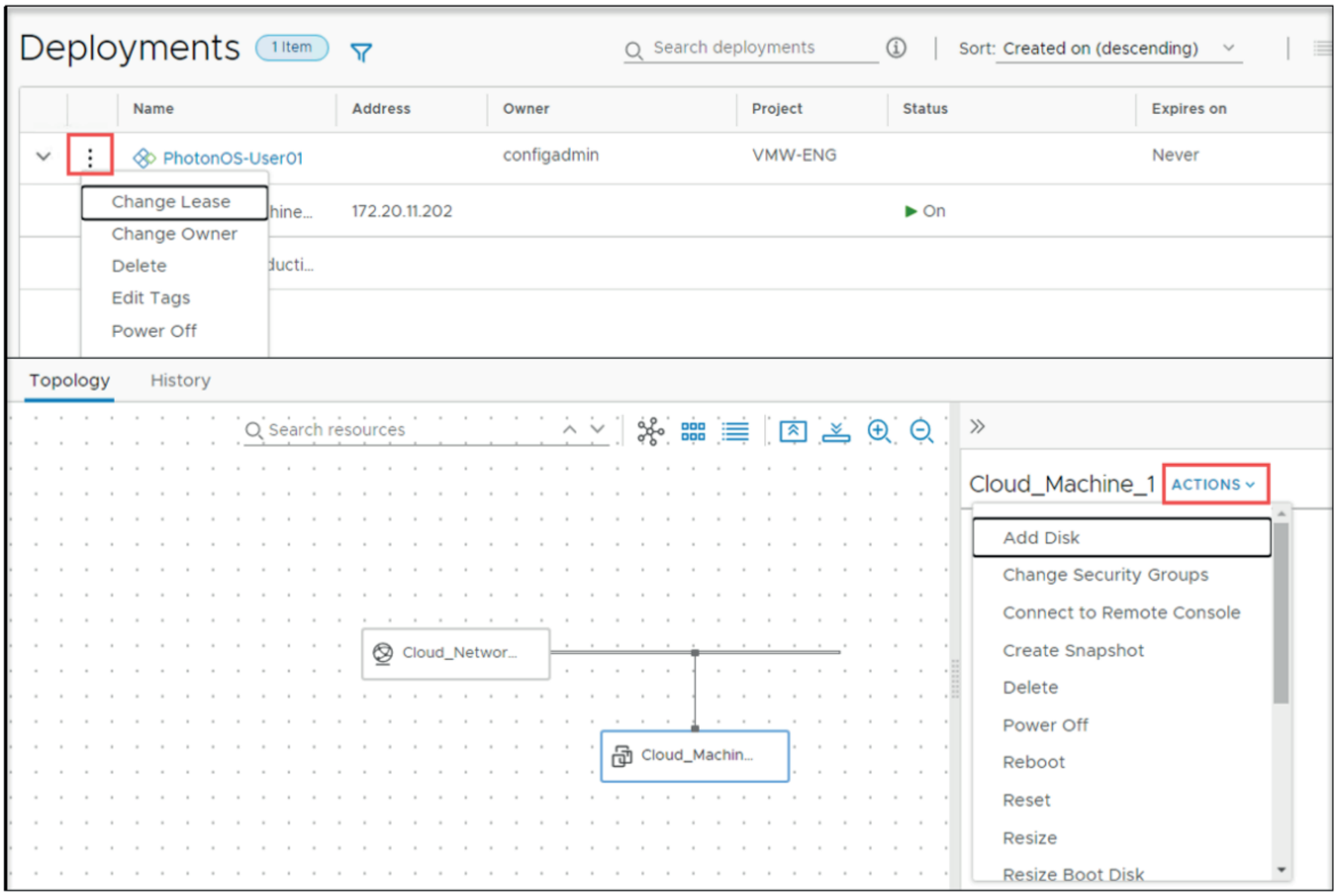
- **Topology**: To visualize the deployment structure and resources.
- **History**: Provisioning events and any events related to actions that you run after the requested item is deployed. If the provisioning process fails, the **History** tab events help you to troubleshoot failures.
- **User Events:** To visualize the user's inputs.

Additionally, the **Monitor, Alert** and **Optimize** tabs are available when integrated with VMware Aria Operations.

11-20 Managing Deployments

A VMware Aria Automation Consumption user can manage the deployments based on the policies defined by the VMware Aria Automation Consumption administrator.

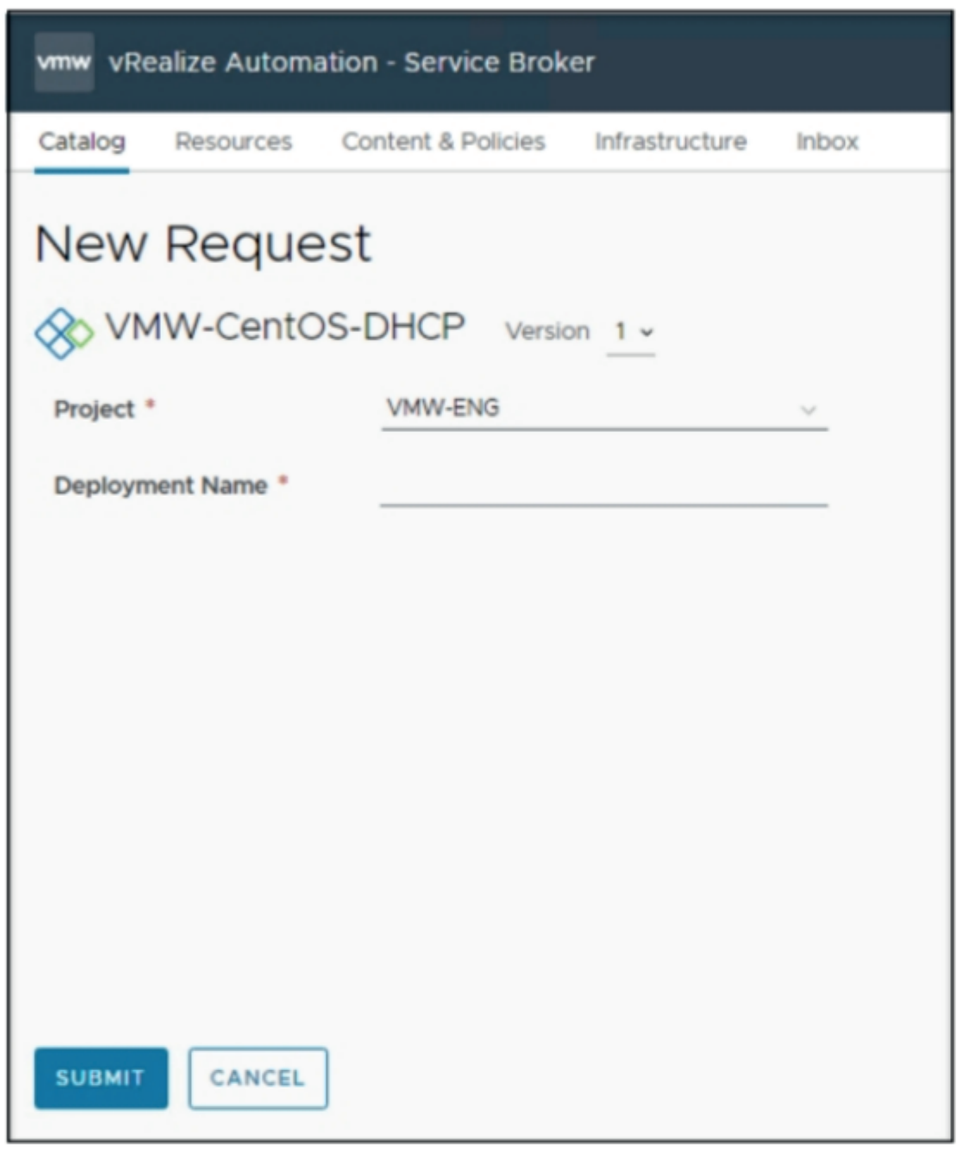
Select **Resources** > **Deployment** and select the object (VM in this example). Click **ACTIONS** to manage the object.

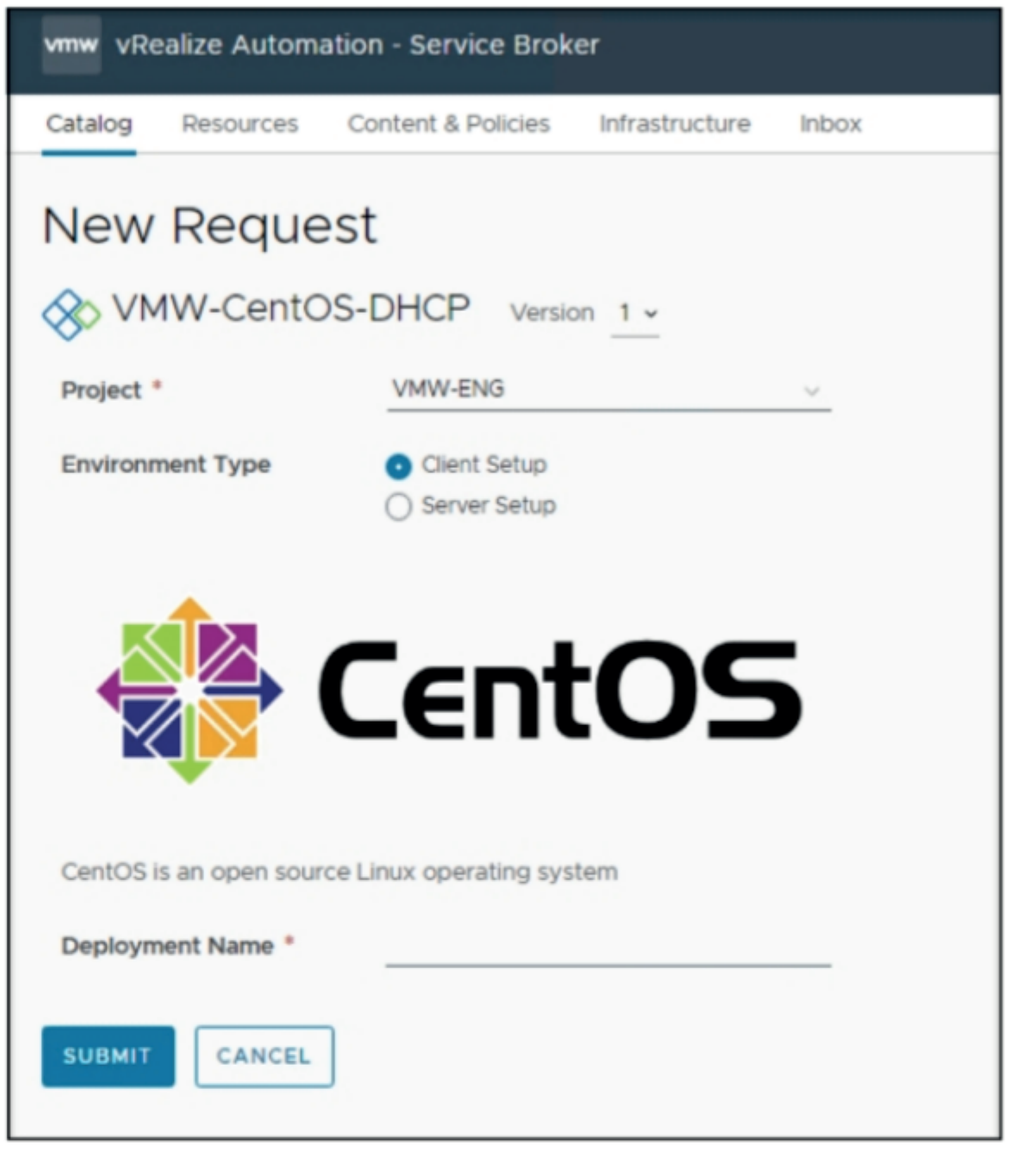


The options available for a VMware Aria Automation Consumption user to manage the deployment and its objects depend on the policies defined by the VMware Aria Automation Consumption administrator.

11-21 Request Forms

VMware Aria Automation Consumption offers the default form with minimal options. Administrators can use the Custom Form feature to customize the request form.

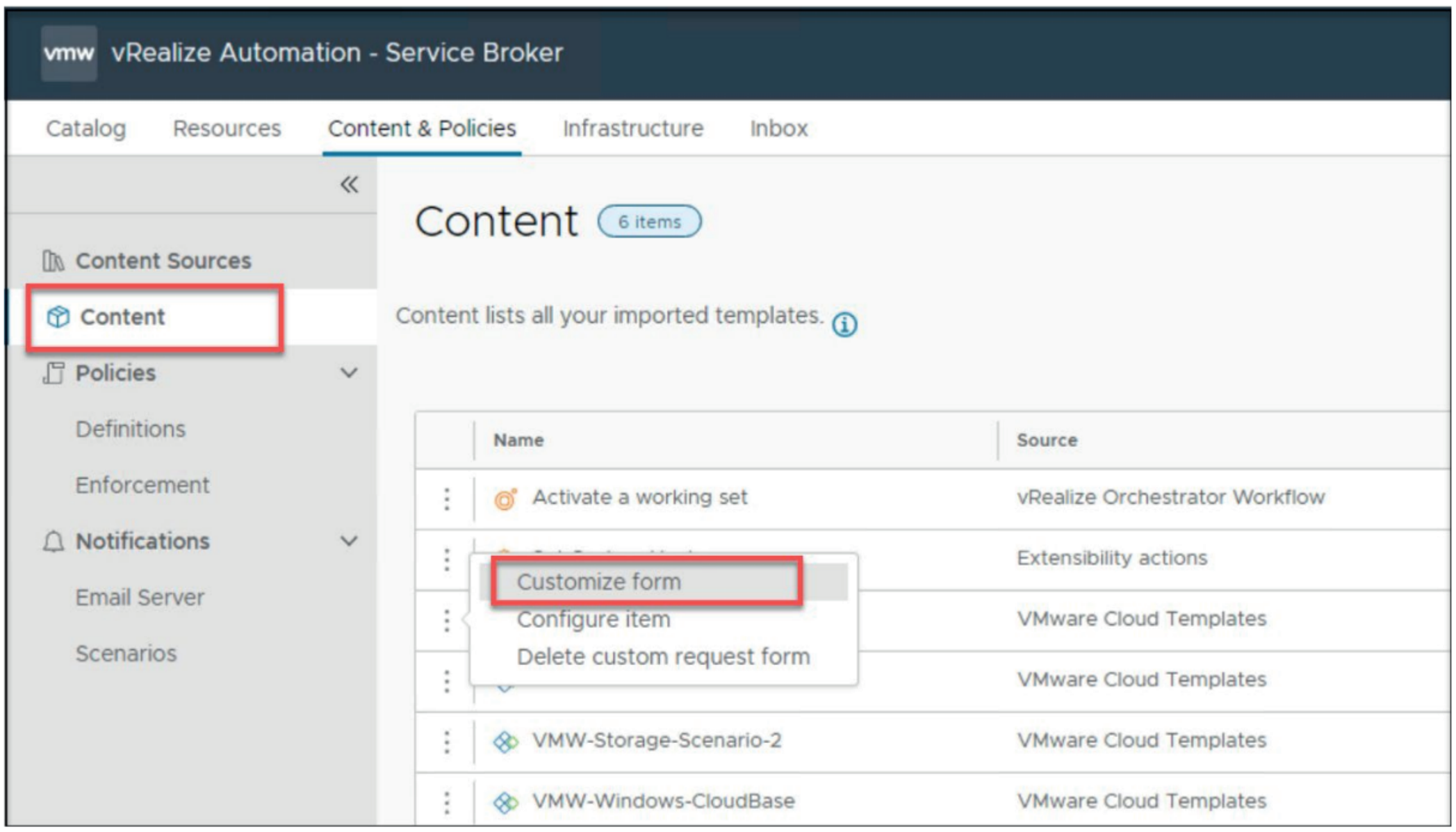




11-22 Custom Forms

VMware Aria Automation Consumption offers the Custom Form feature to customize the input parameters that are available to a user during the request.

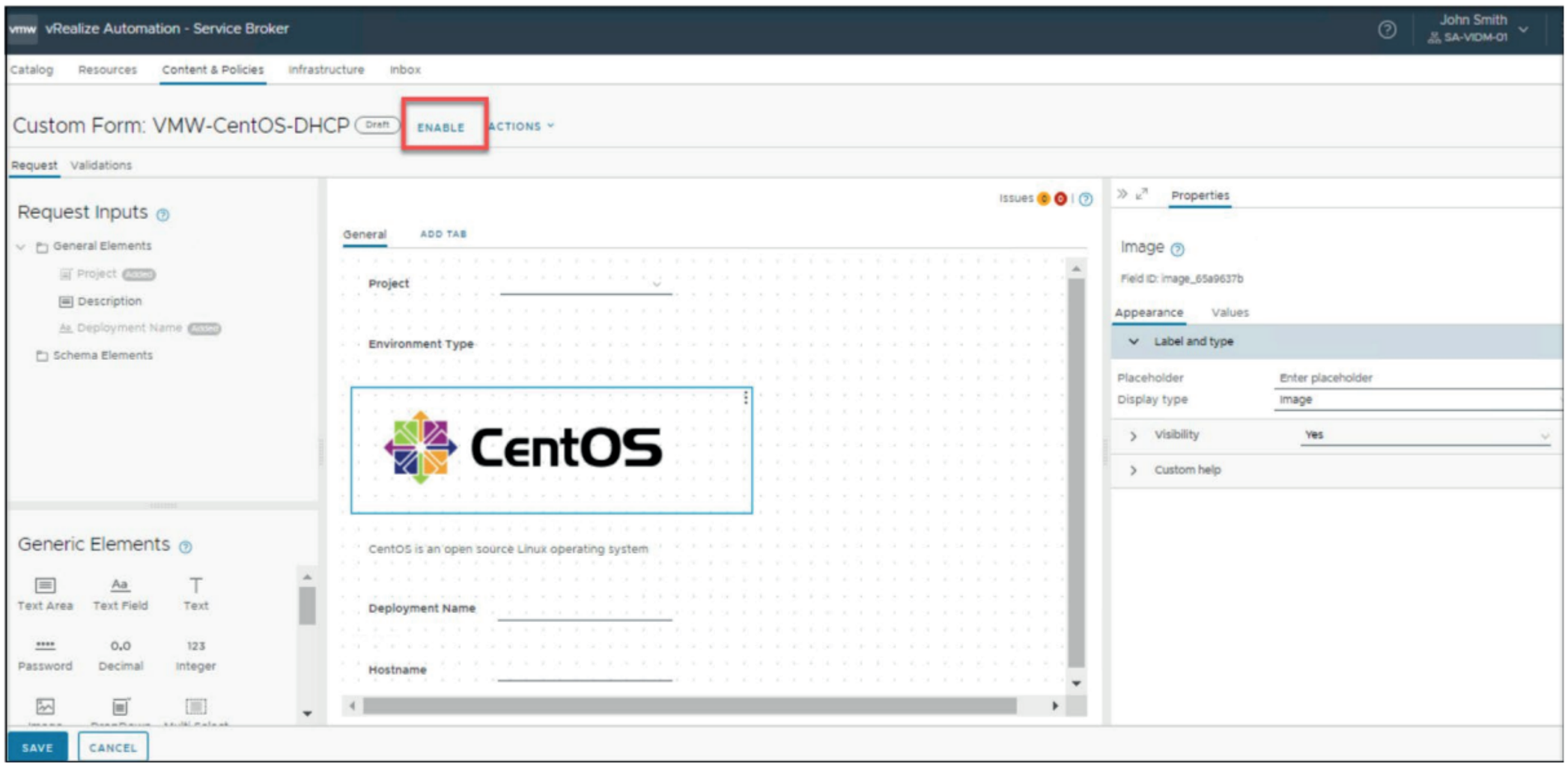
Log in as the VMware Aria Automation Consumption administrator, navigate to **Content & Policies** > **Content**, and click **Customize form**.



To customize the standard form, click **Customize form**.

11-23 Customizing the Request Form

Drag elements to the design canvas and use the properties pane to configure each element. Activate the custom form to update the new request form.



The custom form design canvas has the following broad categories:

- Elements: Drag various elements to the design canvas.
- Design canvas: Overview of items in the request form. You can change the order of listed items.
- Properties: The properties text box in VMware Aria Automation Consumption determine the look of the fields and the default values that are presented to the user. You can also use the properties to define rules that verify that you provide a valid entry when you request the item from the self-service catalog. You configure each field individually.

  You can select the field and edit the following properties:

  — **Appearance**: You use the Appearance properties to determine whether the field appears on the form and the label and custom help are available to your catalog users.

  — **Values**: You use the Values properties to provide any default values.

  — **Constraints**: You use the Constraint properties to verify that the requesting user provides valid values in the request form.

In the example, the Hostname input is defined in the VMware Aria Automation template inputs.

11-24 Lab 25: Configuring the VMware Aria Automation Consumption Catalog

Use VMware Aria Automation Consumption to configure the self-service catalog:

1. Import VMware Aria Automation Templates from VMware Aria Automation Assembler
2. Share VMware Aria Automation Templates with Project Users
3. Validate the VMware Aria Automation Consumption Catalog

11-25 Lab 26: Managing Deployments

Use VMware Aria Automation Consumption to configure the self-service catalog:

1. Deploy a VM from the Self-Service Catalog and Monitor the Deployment
2. Modify the Virtual Machine Resource Settings
3. Create and Delete Snapshots
4. Delete Your Deployment to Save Lab Resources

11-26 Lab 27: Creating Custom Forms

Use custom forms to deploy machines with properties:

1. Review the Standard Request Form
2. Create a Custom Form
3. Validate the Custom Form

11-27 Lab 28: Configuring the VMware Aria Automation Consumption Policies

Use VMware Aria Automation Consumption to configure the self-service catalog:

1. Create an Approval Policy
2. Create a Day-2 Actions Policy
3. Create a Lease Policy
4. Review the Configured Policies in Action
5. Review the Configured Day 2 Policies in Action
6. Delete Your Deployment to Save Lab Resources

11-28 Lab 29: Using VMware Aria Automation Deployment Limit Policies

Use VMware Aria Automation Consumption to configure the self-service catalog:

1. Create a Deployment Limit Policy
2. Review the Configured Policies in Action
3. Delete Your Deployments to Save Lab Resources

11-29 Lab 30: Using VMware Aria Automation Resource Quota Policies

Use VMware Aria Automation Consumption to configure and use the Resource Quota policies:

1. Create a Resource Quota Policy
2. Review the Configured Policies in Action
3. Delete Your Deployments to Save Lab Resources

11-30 Lab 31: Using Multilevel Approvals

Use VMware Aria Automation Consumption to configure multilevel approvals:

1. Create a Level 1 Approval Policy
2. Create a Level 2 Approval Policy
3. Create a Level 3 Approval Policy
4. Review the Configured Policies in Action
5. Clean Up to Save Lab Resources

11-31 Review of Learner Objectives

- Explain the purpose of Using VMware Aria Automation Consumption
- List the supported content sources
- Explain the process for creating catalog items
- Request catalog items from the self-service catalog
- Monitor and manage the catalog items
- Describe the policy types
- Configure a custom form for a VMware Aria Automation template

11-32 Key Points

- VMware Aria Automation Assembler does not offer a self-service catalog.
- You can use VMware Aria Automation Consumption to configure a self-service catalog for a project or entire organization.
- Released VMware Aria Automation templates can be imported into VMware Aria Automation Consumption from various sources.
- The Approval, Lease, Deployment Limit, Resource Quota, and Day-2 Action policies can be applied for governance.
- The standard request form can be customized by using the Custom Forms feature.

Questions?

Module 12

VMware Aria Automation Extensibility

12-2 Importance

The built-in capabilities of VMware Aria Automation are extensive.

However, extensibility techniques can extend the capabilities of VMware Aria Automation beyond what comes built in. In addition, these extensibility techniques tightly integrate VMware Aria Automation with systems in the IT infrastructure, such as IP address management systems, configuration management databases, and more.

12-3 Module Lessons

1. Introduction to Extensibility
2. VMware Aria Orchestrator Workflows
3. ABX Actions

12-4 Lesson 1: Introduction to Extensibility

12-5 Learner Objectives

- Describe the use cases for extensibility
- Differentiate VMware Aria Automation Orchestrator workflows from ABX actions
- Evaluate the event topics to trigger a VMware Aria Automation Orchestrator workflow or ABX action

12-6 Native Functionality in VMware Aria Automation

VMware Aria Automation is a multicloud management platform with several built-in capabilities:

- Deploys machines into VMware platforms, such as vSphere and VMware Cloud on AWS
- Deploys machines into third-party public clouds, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform
- Deploys machines controlled by configuration management tools, such as Aria Automation Config, Terraform, Ansible, Ansible Tower, and Puppet
- Deploys disks, networks, load balancers, and other services

12-7 Overview of Extensibility

Extensibility is a collection of techniques that extend the built-in capabilities of VMware Aria Automation. Each extensibility technique can use VMware Aria Automation Orchestrator workflows or ABX actions.

Life cycle extensibility options:

- Implementing DNS record changes
- IPAM solutions
- Adding users and domain registration
- Executing PowerShell scripts
- Interoperability with third-party tools, such as ServiceNow
- Installation of software
- Actions for everyday operations, such as backups

Anything-as-a-service (XaaS) extensibility options:

- Create custom actions
- Create services to be requested from the catalog

12-8 VMware Aria Automation Extensibility Proxy

With the VMware Aria Automation extensibility proxy, you can manage geographically dispersed data centers from a single VMware Aria Automation instance. Instead of deploying a dedicated instance for each vCenter server, you use a vSphere agent within a specified VMware Aria Automation extensibility proxy to act as a vCenter server proxy.

The steps for setting up and using the VMware Aria Automation extensibility proxy are as follows:

1. Deploy a VMware Aria Automation extensibility proxy to one or more vCenter servers on one or more data centers.
2. Configure VMware Aria Automation to support remote vSphere servers with the help of a VMware Aria Automation extensibility proxy.
3. Connect the VMware Aria Automation extensibility proxy to the remote VMware Aria Automation instance.
4. Create or edit a vCenter cloud account in VMware Aria Automation and associate it to the VMware Aria Automation extensibility proxy in the specified data center to access the remote vCenter server.

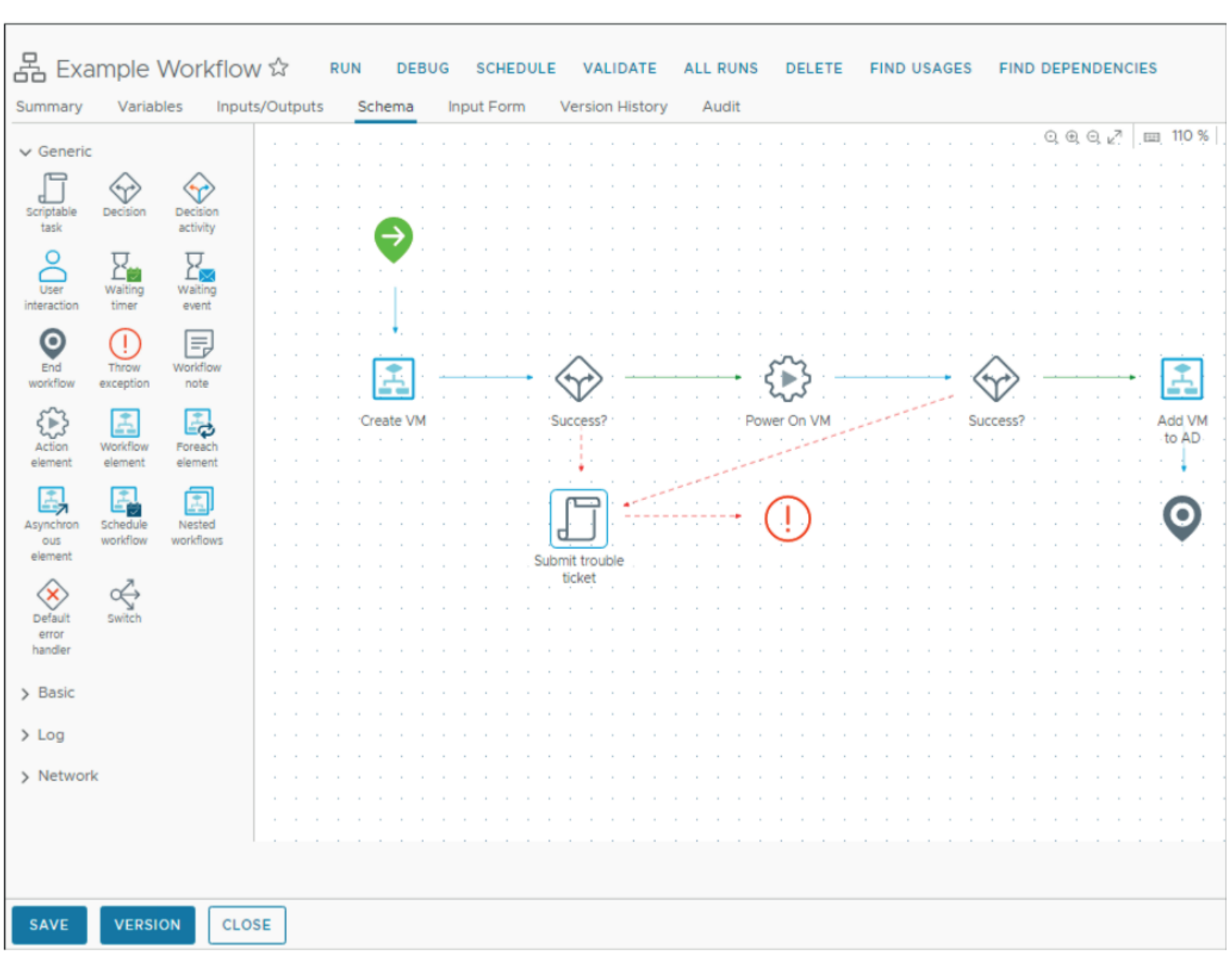
For more information about configuring a VMware Aria Automation extensibility proxy, see the chapter about setting up integrations that use a cloud proxy in *Using and Managing Cloud Assembly* at https://docs.vmware.com/en/vRealize-Automation/index.html.

12-9 About VMware Aria Automation Orchestrator

VMware Aria Automation Orchestrator uses workflows to automate hardware and software systems throughout the IT infrastructure.

VMware Aria Automation Orchestrator workflows are created using a visual drag-and-drop programming approach.

VMware Aria Automation Orchestrator supplies hundreds of built-in workflows, and additional workflows can be added by installing plug-ins.



VMware Aria Automation Orchestrator is included with VMware Aria Automation.

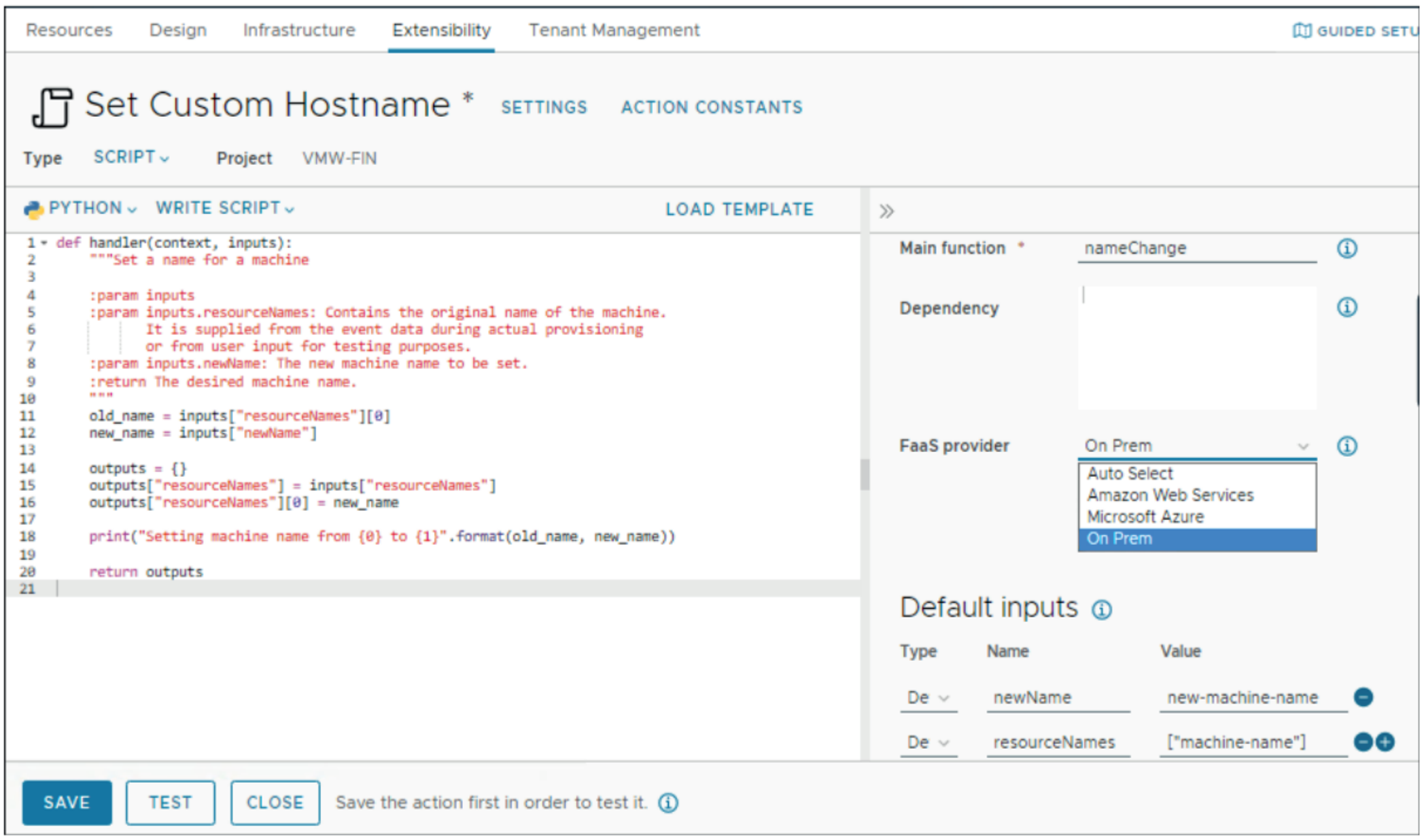
VMware Aria Automation Orchestrator includes numerous preinstalled plug-ins.

In addition, you can add code to VMware Aria Automation Orchestrator workflows to customize workflow behavior. This code can be written in Node.js, PowerShell, or Python.

12-10 ABX Actions

Action Based Extensibility (ABX) actions provide multicloud function-as-a-service (FaaS) features to extend the capabilities of VMware Aria Automation and to integrate with the IT infrastructure.

ABX actions can be written in Node.js, PowerShell, or Python.

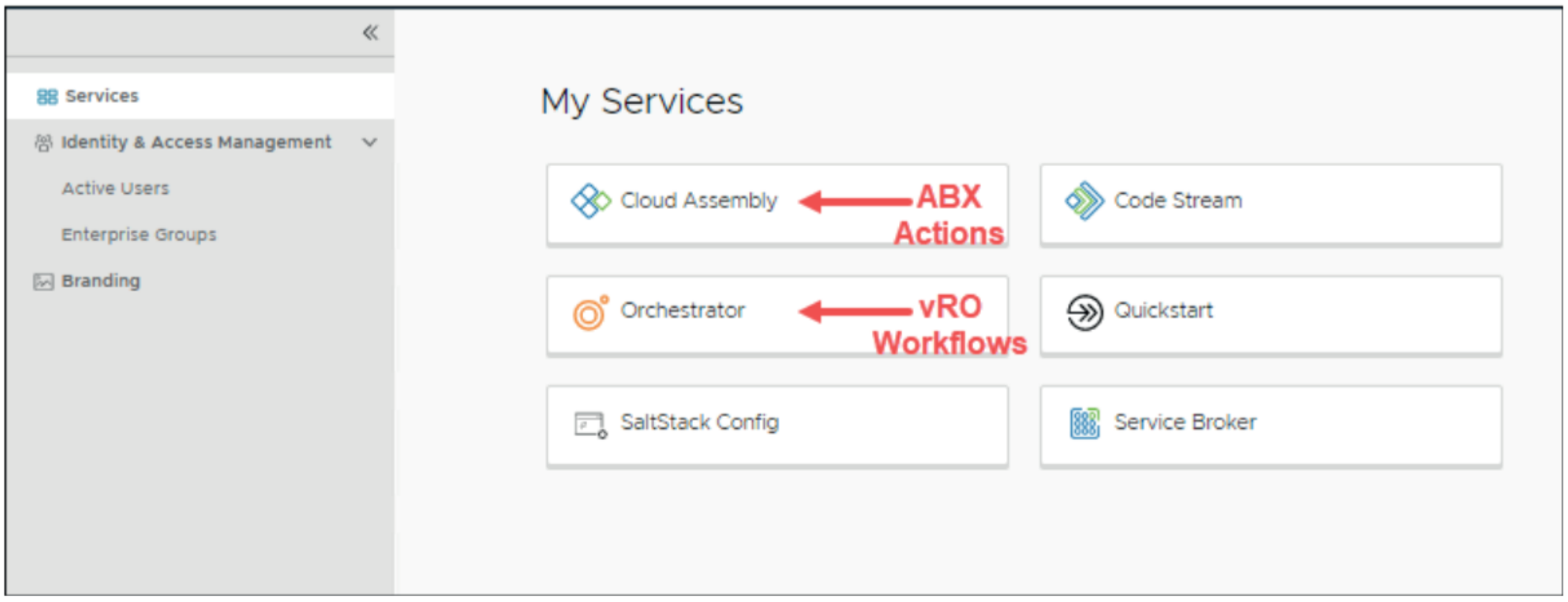


ABX actions in VMware Aria Automation are similar to AWS Lambda. Both platforms provide function-as-a-service (FaaS) capabilities, but ABX actions are multicloud. In VMware Aria Automation, you can run your ABX action on your on-premises vSphere environment on Amazon Web Services (AWS) or on Microsoft Azure.

The example screenshot shows an ABX action written in Python code. This Python code enables VMware Aria Automation to configure a custom host name that is selected by the end user. This custom host name is used instead of the default host name normally used by VMware Aria Automation.

12-11 Defining VMware Aria Automation Orchestrator Workflows and ABX Actions

VMware Aria Automation Orchestrator workflows and ABX actions are defined in different locations in the VMware Aria Automation user interface.



You define VMware Aria Automation Orchestrator workflows in VMware Aria Automation Orchestrator). In the Cloud Services Console, select **Orchestrator** > **Library** > **Workflows** in the left navigation pane.

You define ABX actions in VMware Aria Automation Assembler. From the Cloud Services Console, select **Cloud Assembly** > **Extensibility** > **Library** > **Actions**.

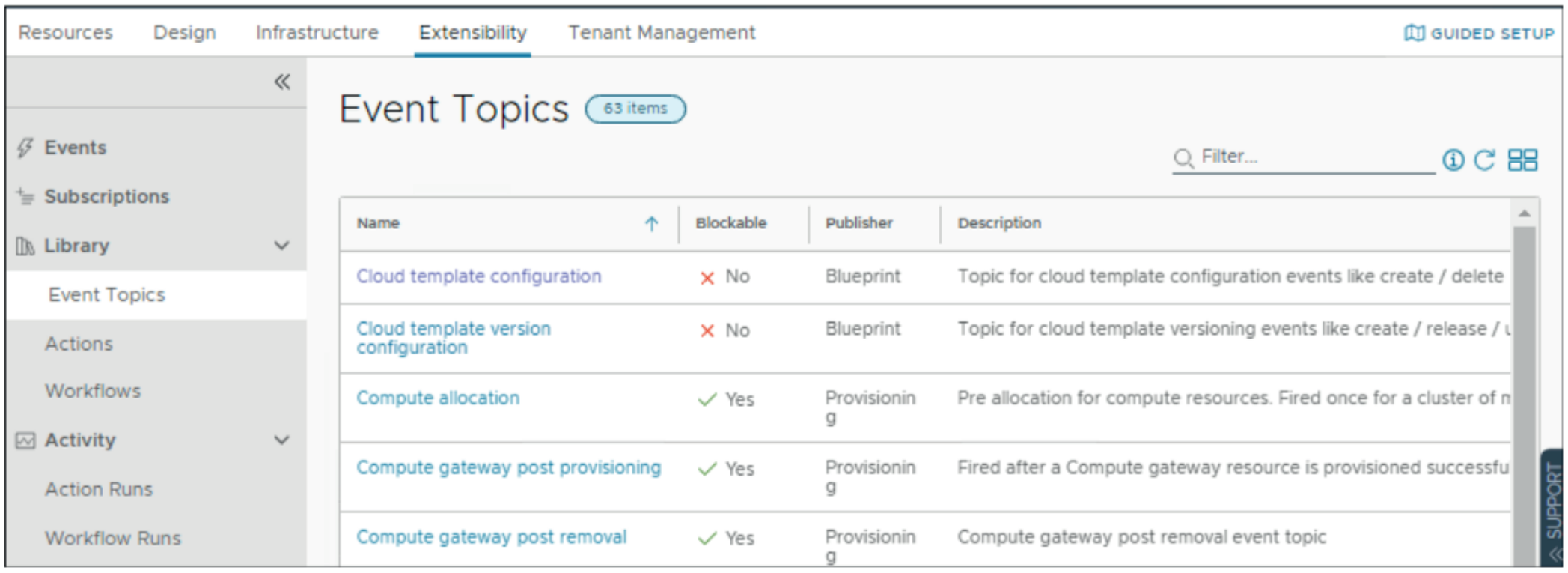
After defining VMware Aria Automation Orchestrator workflows and ABX actions, use both for extensibility operations in Cloud Assembly and Service Broker.

One way of using VMware Aria Automation Orchestrator workflows and ABX actions for extensibility in Cloud Assembly is by creating an event subscription. From the Cloud Services Console, select **Cloud Assembly** > **Extensibility** > **Subscriptions**.

You configure Service Broker to enable users to call VMware Aria Automation Orchestrator workflows and ABX actions from the catalog. For VMware Aria Automation Orchestrator workflows and ABX actions to be available for use in Service Broker, you must create a content source for each. From the Cloud Services Console, select **Service Broker** > **Content & Policies** > **Content Sources**. This ability to call ABX actions and VMware Aria Automation Orchestrator workflows from the catalog enables end users to execute Day 2 actions on objects to which they have access.

12-12 Event Topics in VMware Aria Automation

VMware Aria Automation has many predefined event topics. Each event topic is linked to specific times during the deployment life cycle.



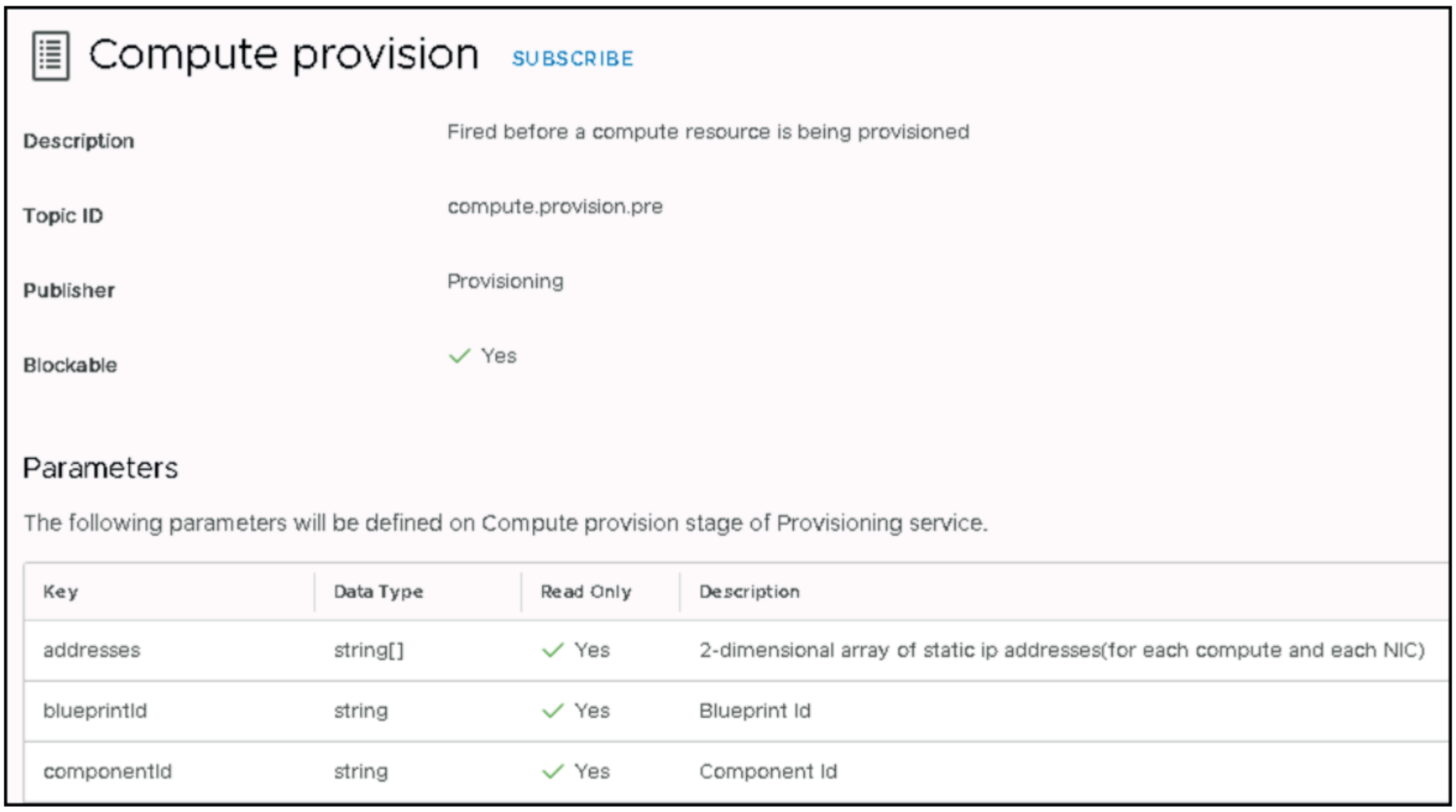
Event topics are defined by VMware Aria Automation. Event topics trigger when particular events occur in VMware Aria Automation, such as when a machine is provisioned, when a cloud template is modified, and so on. By configuring a subscription, you can instruct VMware Aria Automation to invoke a specific VMware Aria Automation Orchestrator workflow or ABX action when a particular event topic triggers.

When you want a VMware Aria Automation Orchestrator workflow or ABX action to run and complete before some other event occurs, you can block this event. While creating your subscription, you can choose for VMware Aria Automation to invoke a VMware Aria Automation Orchestrator workflow or ABX action synchronously (blocking) or asynchronously (nonblocking). If a particular event topic is not blockable, then you do not have that choice. Non-blockable event topics in a subscription always result in the specified VMware Aria Automation Orchestrator workflow or ABX action being called asynchronously.

Each event topic is defined by a publisher, such as Blueprint, Provisioning, Kubernetes, and so on. The publisher is the subsystem in VMware Aria Automation that defines and monitors event topics.

12-13 Descriptions of Event Topics

Each event topic displays a list of parameters details when opened from the event topics list.



Compute provision SUBSCRIBE

Description	Fired before a compute resource is being provisioned
Topic ID	compute.provision.pre
Publisher	Provisioning
Blockable	✓ Yes

Parameters

The following parameters will be defined on Compute provision stage of Provisioning service.

Key	Data Type	Read Only	Description
addresses	string[]	✓ Yes	2-dimensional array of static ip addresses(for each compute and each NIC)
blueprintId	string	✓ Yes	Blueprint Id
componentId	string	✓ Yes	Component Id

All the event topics defined by VMware Aria Automation are listed in Cloud Assembly. In the Cloud Services Console, select **Extensibility** > **Library** > **Event Topics**. When you click an event topic on that page, VMware Aria Automation opens a page with details on the specific event topic.

This page lists both the name of the event topic and its topic ID. In the example in the screenshot, the name of the event topic is Compute provision and the topic ID is compute.provision.pre. The former is a readable name which is the main way event topics are listed in the VMware Aria Automation UI. The event topic ID uses a dotted notation for the same event topic. The topic ID is useful to understand when writing VMware Aria Automation Orchestrator workflows or ABX actions.

The bottom of this page lists the parameters of the event topic. Each event topic sends a payload of information from the VMware Aria Automation event broker service to the VMware Aria Automation Orchestrator workflow or ABX action that you specify in your subscription. Different event topics define this payload differently, but some examples of information contained in the payload are as follows:

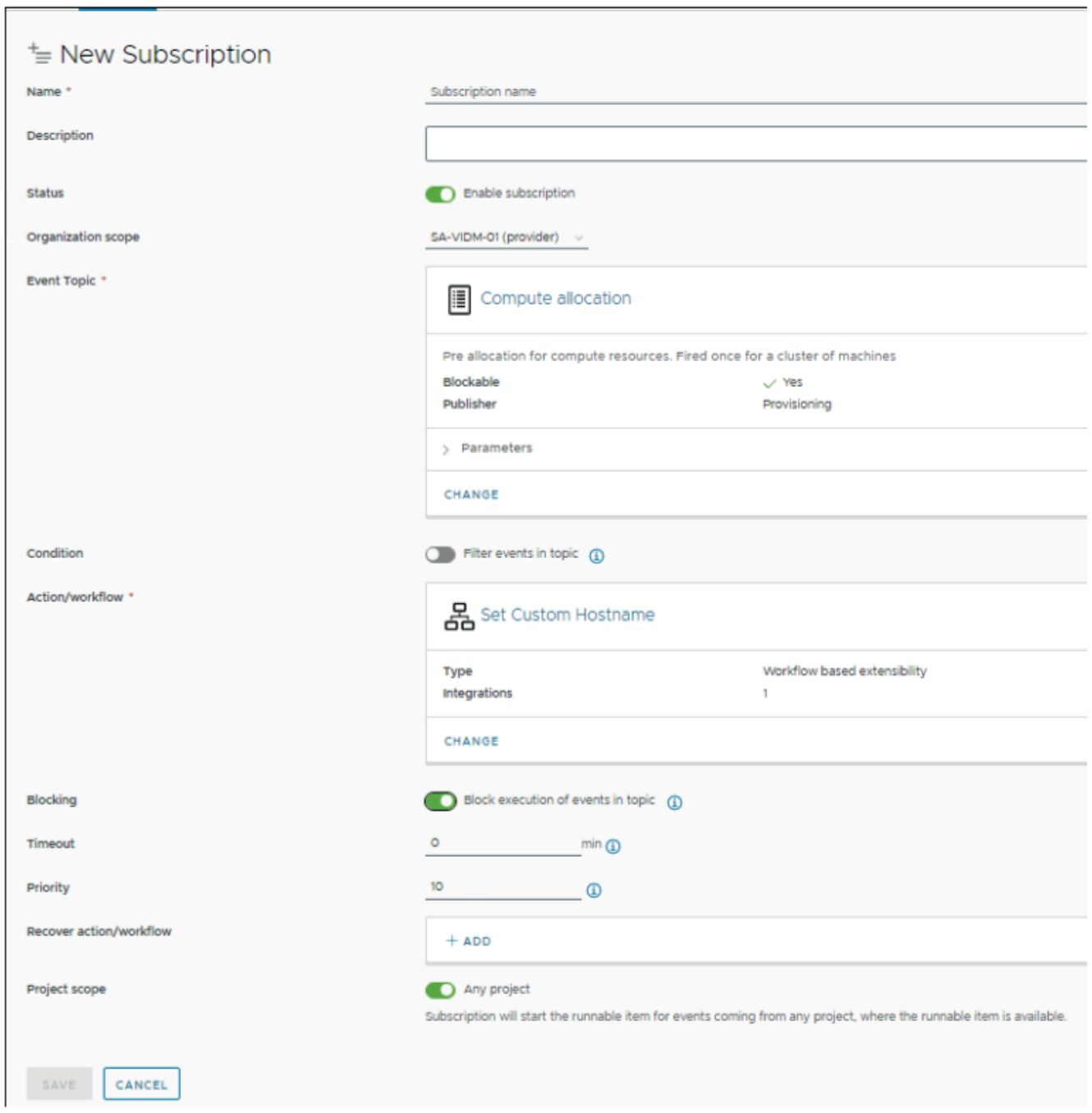
- Array of the IP addresses that VMware Aria Automation is assigning to the NICs in the machines being deployed
- ID of the cloud template being deployed

- Project to which the end user belongs
- Custom properties defined in the cloud template

The communication is bidirectional between the event broker service in VMware Aria Automation and the VMware Aria Automation Orchestrator workflow (or ABX action) called. VMware Aria Automation not only sends a payload to VMware Aria Automation Orchestrator (or ABX), but VMware Aria Automation Orchestrator (or ABX) can send a payload back to VMware Aria Automation. The screenshot indicates that some parameters are read-only. Your VMware Aria Automation Orchestrator workflow or ABX action can see the data stored in that parameter, but your VMware Aria Automation Orchestrator workflow or ABX action cannot change that value.

12-14 Subscriptions

Subscriptions are used to specify that when a particular event topic triggers, VMware Aria Automation should invoke a specific VMware Aria Automation Orchestrator workflow or ABX action.



The New Subscription wizard can be used to create subscriptions that invoke VMware Aria Automation Orchestrator workflows and ABX actions.

When creating a subscription, you begin by giving it a name and a description.

You use the **Status** toggle to enable or disable the subscription.

Event Topic is used to specify exactly one type of event that VMware Aria Automation should look for.

The **Condition** toggle provides a code editor that you can use to specify the exact conditions that must be satisfied for VMware Aria Automation to invoke the VMware Aria Automation Orchestrator workflow or ABX action. Examples of conditions include a specific cloud template that is being deployed, a machine with a specific name that is being deployed, and so on. If you specify a condition in a subscription, then both the event topic must trigger and the condition must be met for VMware Aria Automation to invoke the VMware Aria Automation Orchestrator workflow or ABX action.

Action/workflow is used to specify which VMware Aria Automation Orchestrator workflow or which ABX action that you want VMware Aria Automation to invoke.

The **Blocking** toggle allows you to indicate whether you want VMware Aria Automation to call the VMware Aria Automation Orchestrator workflow or ABX action synchronously (blocking) or asynchronously (nonblocking).

If you specify blocking, you can specify how long the VMware Aria Automation Orchestrator workflow or ABX action waits for the action or workflow to complete before it times out and allows the other events to continue.

Recover action/workflow is used to specify a VMware Aria Automation Orchestrator workflow or ABX action to call if the VMware Aria Automation Orchestrator workflow or ABX action for the subscription fails. This other VMware Aria Automation Orchestrator workflow or ABX action is designed to gracefully address failures.

Subscription scope is used to control whether the subscription is limited to a single project or applicable to all projects.

12-15 Review of Learner Objectives

- Describe the use cases for extensibility
- Differentiate VMware Aria Automation Orchestrator workflows from ABX actions
- Evaluate the event topics to trigger a VMware Aria Automation Orchestrator workflow or ABX action

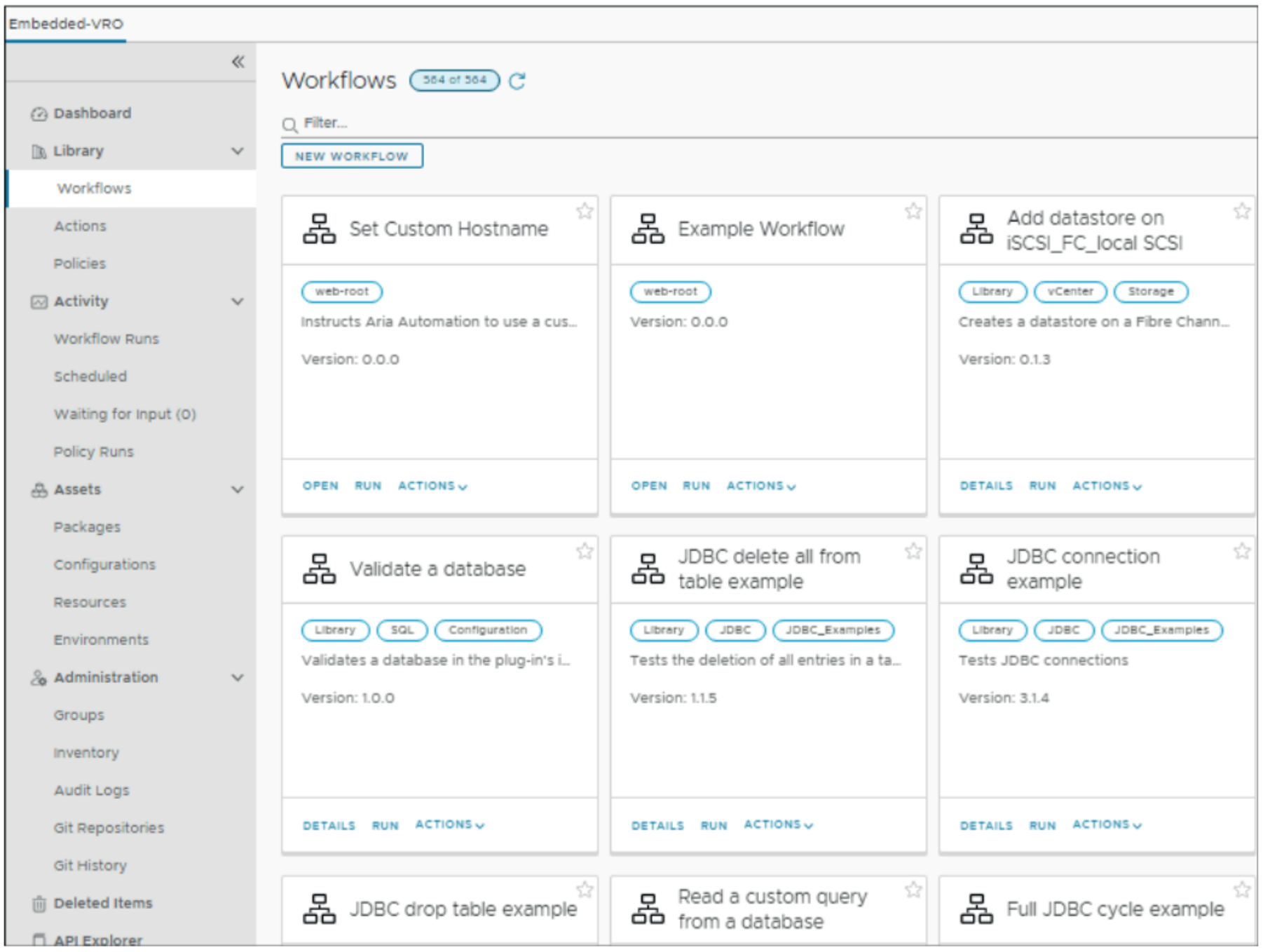
12-16 Lesson 2: VMware Aria Automation Orchestrator Workflows

12-17 Learner Objectives

- Demonstrate how to start the Orchestrator Client
- Describe the schema of a VMware Aria Automation Orchestrator workflow
- Create a subscription that calls a VMware Aria Automation Orchestrator workflow

12-18 Orchestrator Client

The Orchestrator Client is used for developing, executing, debugging, managing, and monitoring VMware Aria Automation Orchestrator workflows.



The Orchestrator Client includes the following features:

- You can create, run, and debug workflows on the **Library** > **Workflows** page.
- You can create VMware Aria Automation Orchestrator actions on the **Library** > **Actions** page. VMware Aria Automation Orchestrator actions are reusable snippets of code that can be called from any workflow. These VMware Aria Automation Orchestrator actions are similar to functions in other programming environments. VMware Aria Automation Orchestrator has hundreds of built-in VMware Aria Automation Orchestrator actions, and you can easily create your own custom actions.

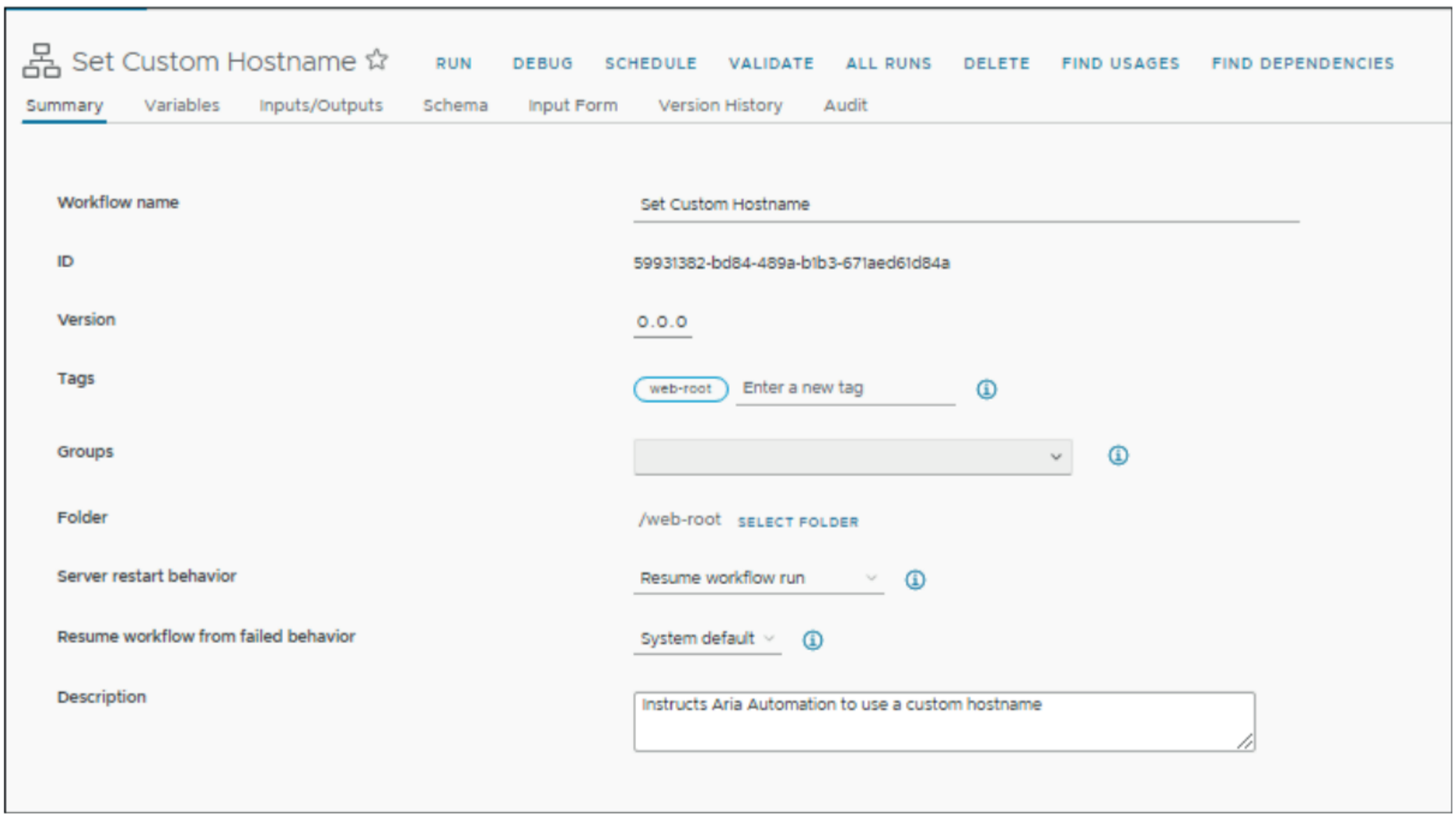
  VMware Aria Automation Orchestrator actions and ABX actions are unrelated.
- You can monitor running workflows on the **Activity** > **Workflow Runs** page. Additionally, a record of workflow runs is maintained so that historical information is available about workflows that ran in your environment.
- You can import packages created by VMware, third-party developers, and other VMware Aria Automation Orchestrator environments on the **Assets** > **Packages** page. You can

also easily create your own packages. Each package contains a collection of VMware Aria Automation Orchestrator workflows, VMware Aria Automation Orchestrator actions, configuration elements, and resources.

- You can explore all objects managed by the plug-ins installed in VMware Aria Automation Orchestrator on the **Administration** > **Inventory** page.
- To see the details of the hundreds of data types provided by VMware Aria Automation Orchestrator, selecting **API Explorer** in the left navigation pane.

12-19 Orchestrator Client: Summary Tab

On the **Summary** tab, you set the general properties of a workflow, such as the workflow name, its version number, and its description.



You specify the name of the VMware Aria Automation Orchestrator workflow in the **Workflow name** text box. When you first create a workflow, a pop-up window gives you the chance to specify the name of the workflow. After creating the workflow, you cannot change the workflow from the main screen. Instead, you must change a workflow's name on the **Summary** tab in the **Workflow name** text box.

ID is a read-only text field that reports the workflow ID (unrelated to a workflow run ID). Workflow IDs are handy when using the VMware Aria Automation Orchestrator REST API to invoke workflows external to the Orchestrator Client.

You can create multiple versions of a workflow in the **Versions** text box. This mechanism enables you to compare versions side by side and revert to other versions.

The **Tags** text box enables you to organize workflows. Tags allow you to label your workflows. You can use these tags for performing searches for workflows.

Groups is used to control access to workflows. Groups and roles are more effective when you license VMware Aria Automation Orchestrator with a VMware Aria Automation license than with a vSphere license.

Folder provides another way to organize your workflows. With folders, you can organize workflows hierarchically like files in a filesystem. You can use tags and folders together.

Server restart behavior is used to control how VMware Aria Automation Orchestrator handles running workflows if the VMware Aria Automation Orchestrator server stops unexpectedly. The default behavior is that when the server is restored, VMware Aria Automation Orchestrator automatically resumes (not restarts) workflows from where they were. VMware Aria Automation Orchestrator uses checkpointing to make this possible. You can optionally disable this feature on an individual workflow basis.

Resume workflow from failed behavior is similar to the **Server restart behavior** setting:

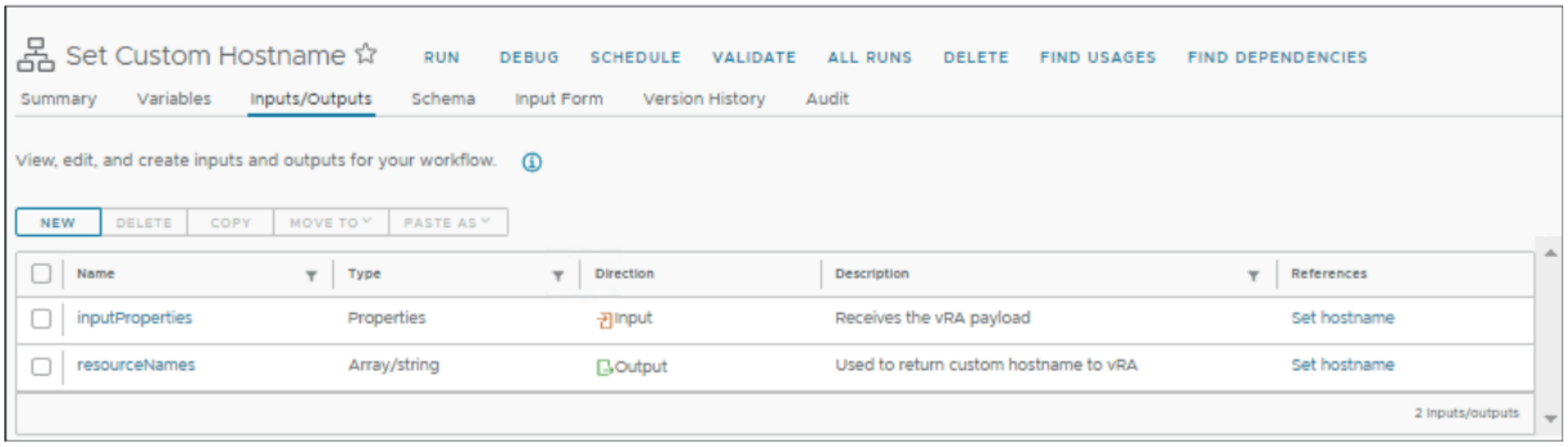
- The **Server restart behavior** drop-down menu specifies what to do if the VMware Aria Automation Orchestrator server goes down unexpectedly. In contrast, Resume workflow from failed behavior is concerned with what to do if the VMware Aria Automation Orchestrator workflow fails.
- By default, if a workflow fails, then the VMware Aria Automation Orchestrator server terminates the workflow. But with **Resume workflow from failed behavior**, you can instruct the VMware Aria Automation Orchestrator server to pause a failed workflow, giving you a chance to address the cause of the failure and resume the workflow.
- This option is useful in situations when failure is caused an infrastructure issue, for example, a storage array that runs out of space. You can add additional space to the storage array and then resume the workflow.

The **Description** text box is where you can describe the functionality that your workflow provides. When you provide a description for your workflows, other VMware Aria Automation Orchestrator developers can quickly and easily understand each workflow's purpose without having to open and study it in detail.

12-20 Orchestrator Client: Inputs/Outputs Tab

You use inputs to prompt whoever (or whatever) is calling a workflow for information.

You use outputs to pass information back to whoever (or whatever) is calling a workflow.



With inputs, you can allow the user calling your workflow to feed information into the workflow.

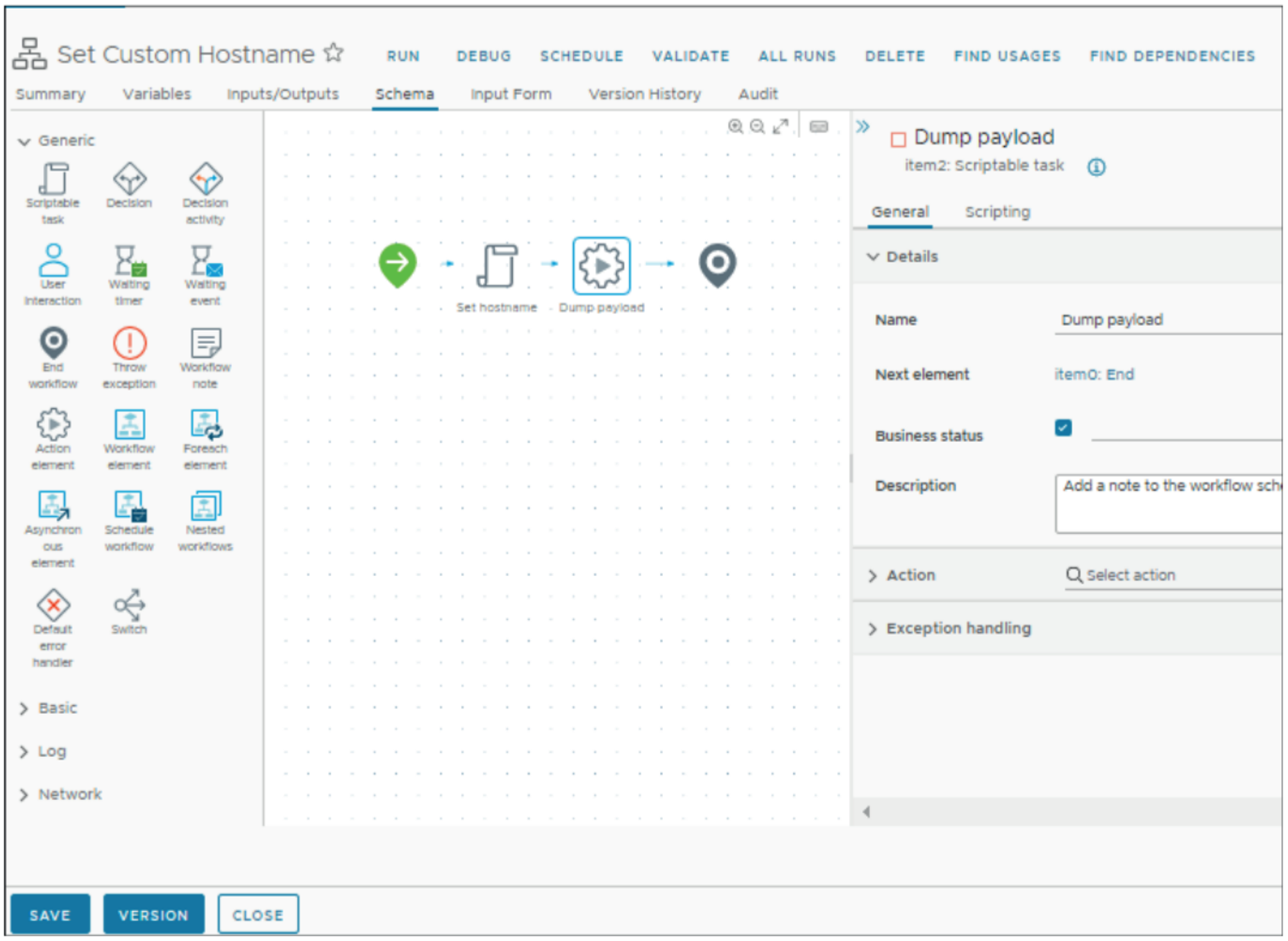
With outputs, you can pass information from the workflow back to the user.

Each input and each output can be assigned a different type, such as string, number, Boolean, and so on. You can use the API Explorer to look up all the data types defined by VMware Aria Automation Orchestrator and the plug-ins.

You should specify a description for every input and every output so that other VMware Aria Automation Orchestrator developers can quickly and easily understand their purposes.

12-21 Orchestrator Client: Schema Tab

On the **Schema** tab, you define the logic that controls the behavior of a workflow.



The left pane of the **Schema** tab includes all the schema elements that you can build into your workflow. These elements include actions, decisions, multiple schema elements to call other workflows, and more.

The middle pane of the **Schema** tab includes the design canvas to which you drag the schema elements from the left pane.

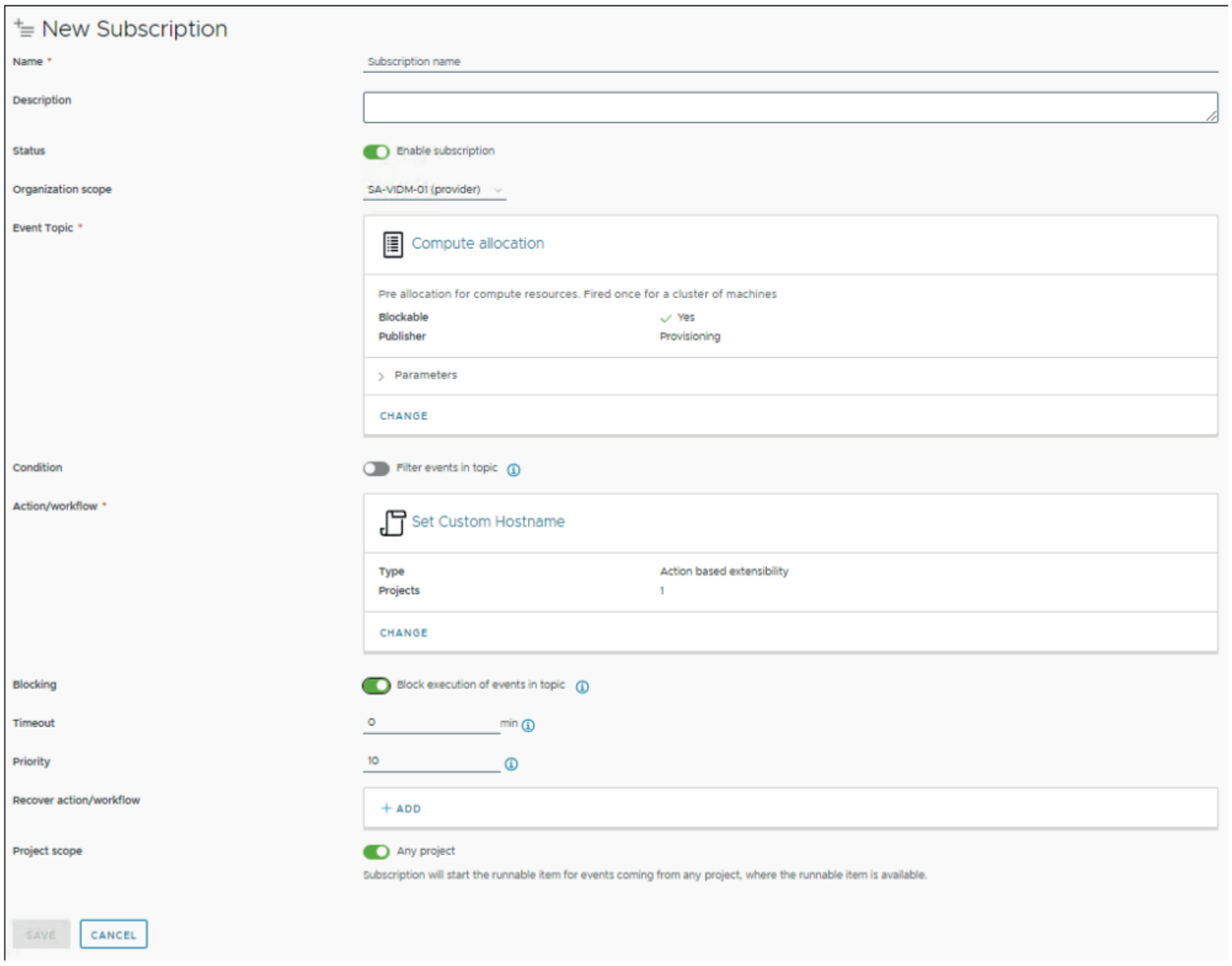
In right pane of the **Schema** tab, you configure the schema elements that you dragged to the design canvas.

12-22 Subscriptions Call Workflows

You can call a VMware Aria Automation Orchestrator workflow by calling it from a subscription.

You can also call a VMware Aria Automation Orchestrator workflow in the following ways:

- Creating a custom resource
- Creating a catalog item in Service Broker



You can call your VMware Aria Automation Orchestrator workflow from a subscription.

You can also create a custom resource that calls your VMware Aria Automation Orchestrator workflow. By creating a custom resource, you can create another component that you can drag to your cloud template. For example, a new Active Director user can create another Active Directory user at the same time that a virtual machine is deployed.

Another way of calling your VMware Aria Automation Orchestrator workflow is to set it up as a catalog item in Service Broker.

12-23 Lab 32: Using VMware Aria Automation Orchestrator to Set Custom Host Names

Set a custom host name on a machine deployed from a VMware Aria Automation Templates:

1. Create a VMware Aria Automation Template
2. Create a VMware Aria Automation Orchestrator Workflow
3. Create a Subscription
4. Deploy Your VMware Aria Automation Template
5. Delete Your Deployment to Save Lab Resources

12-24 Review of Learner Objectives

- Demonstrate how to start the Orchestrator Client
- Describe the schema of a VMware Aria Automation Orchestrator workflow
- Create a subscription that calls a VMware Aria Automation Orchestrator workflow

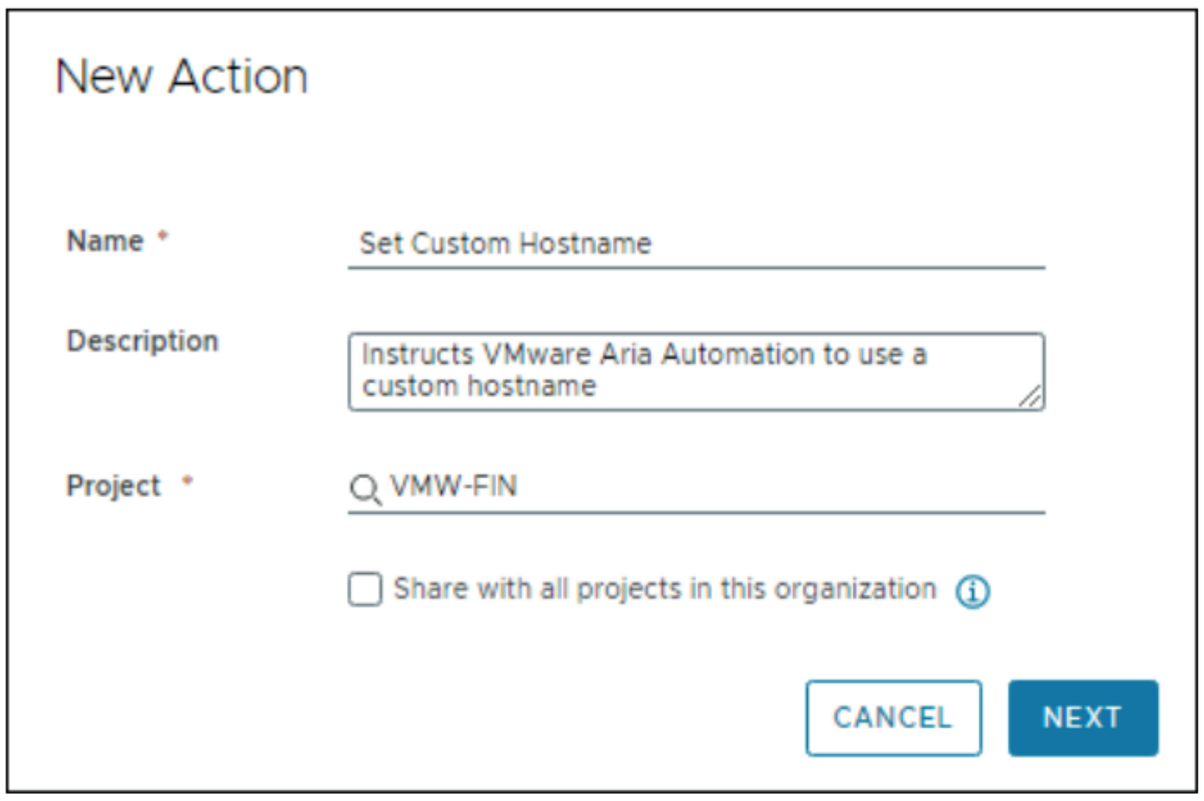
12-25 Lesson 3: ABX Actions

12-26 Learner Objectives

- Create an ABX action
- Use the polyglot capability of ABX
- Specify the entry point of an ABX action

12-27 Creating an ABX Action

To create an ABX action, select **Extensibility** > **Library** > **Actions** in VMware Aria Automation Assembler and click **NEW ACTION**.



You must first select a name for the ABX action. You are likely to create numerous ABX actions, so selecting a clear name for each action is a best practice.

You should also enter a description to help you (and other developers) quickly understand the purpose of each ABX action.

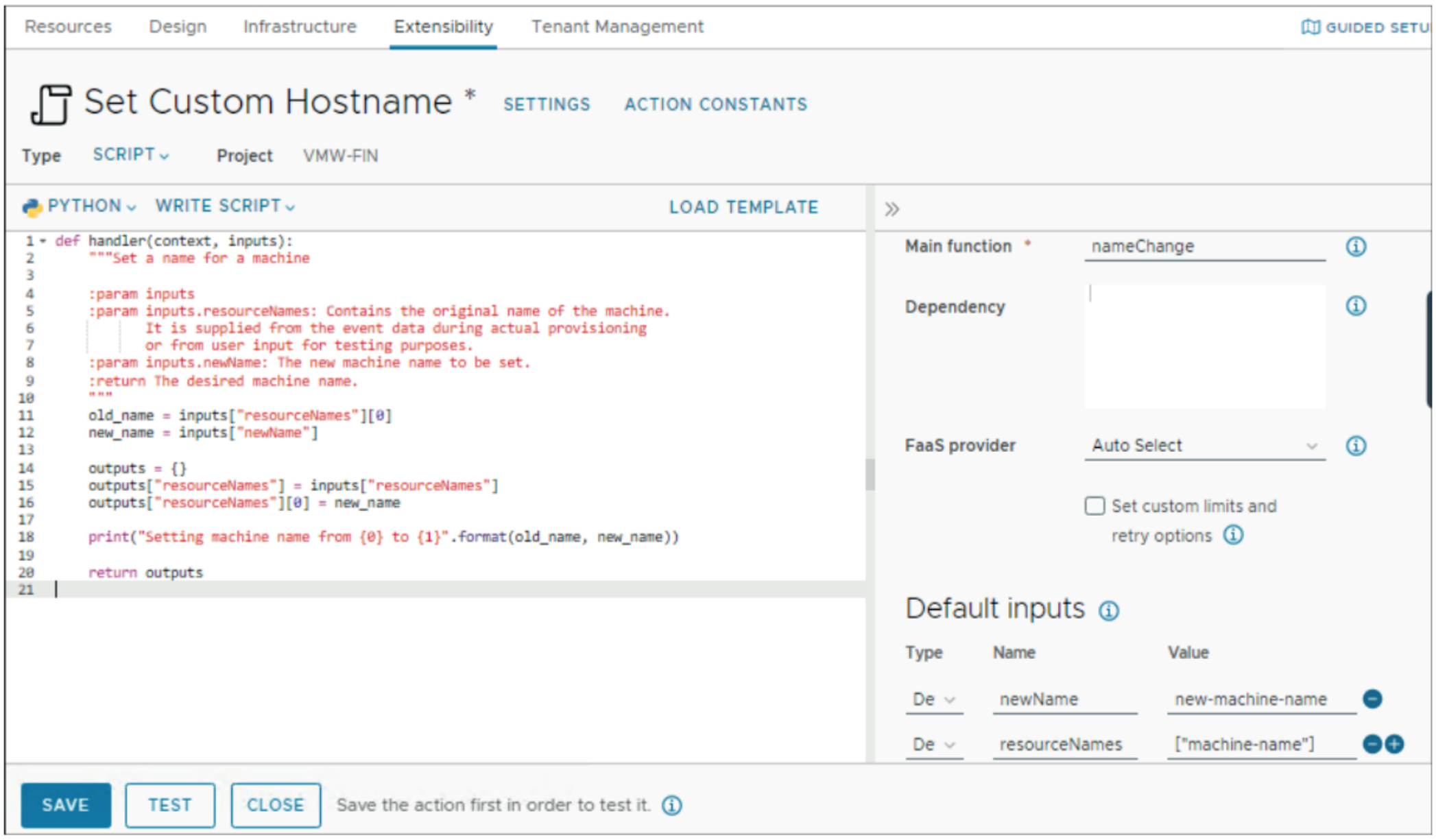
Like cloud templates, when you create an ABX action, you associate it with a specify project.

Optionally, you can share the ABX action across projects.

12-28 New ABX Action Wizard

In the New ABX Action wizard, enter the code that implements the ABX action functionality in the left pane.

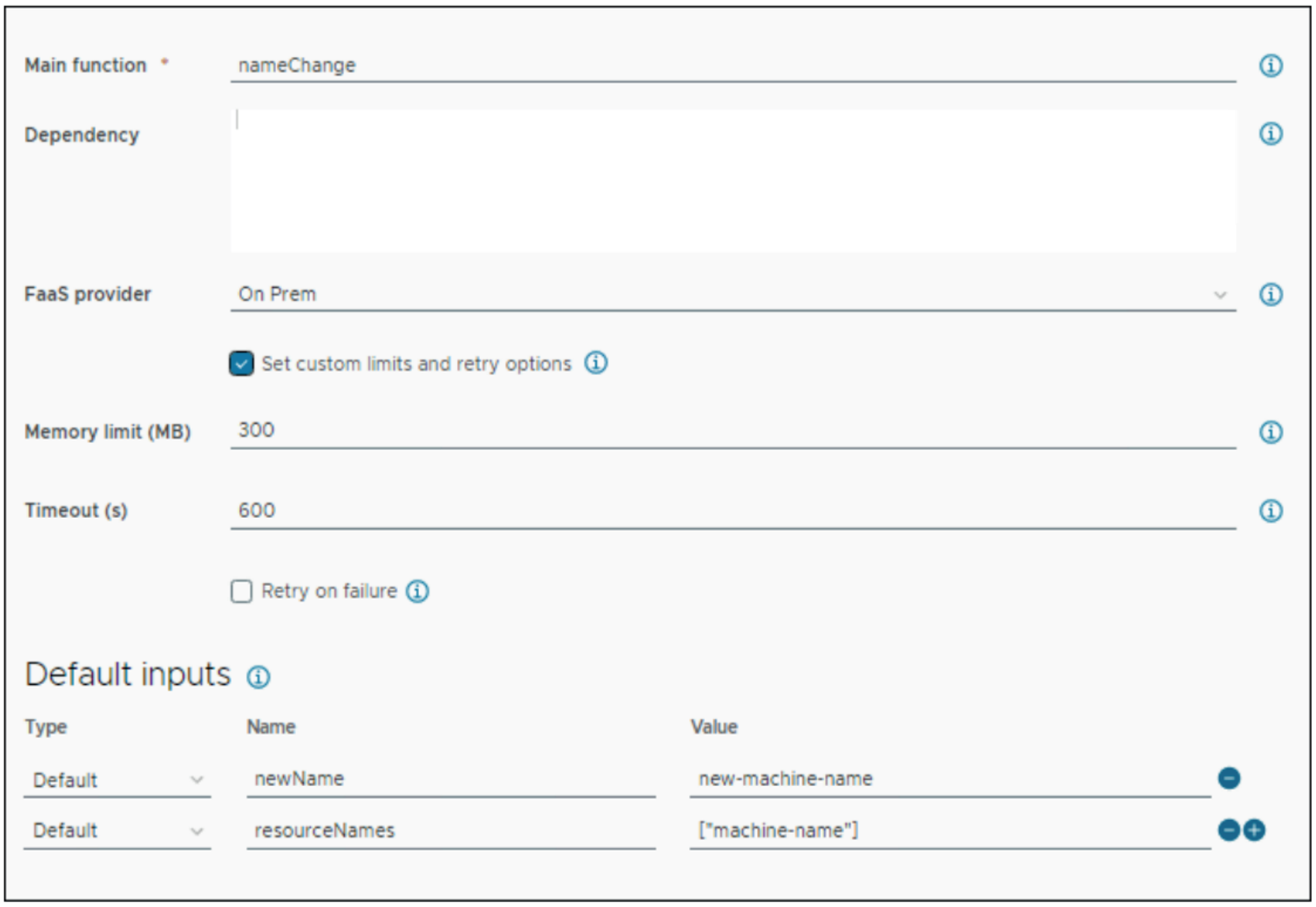
You configure the settings that control the ABX action behavior in the right pane of the wizard.



The code that implements the ABX action can be written in Node.js, PowerShell, or Python.

12-29 ABX Action Settings

You configure numerous settings that control the behavior of the ABX action in the right pane of the New ABX Action wizard.



The default value in the **Main function** text box is **`handler`**. You can change the name of your function by entering a different value in the **Main function** text box. A specific use case for changing the **Main function** value is if your ABX action includes multiple functions. Only one of these functions is the entry point to your ABX action, so you must set the value in the **Main function** text box to indicate the name of the entry point function.

The **Default inputs** option is useful when your ABX action is not being invoked by the event broker service. If your ABX action is being invoked by the event broker service, then the event broker sends a payload to your ABX action. If you click **TEST** to test your ABX action, then your ABX action is not being called by the event broker, and therefore your ABX action does not receive the payload. This outcome can cause an error in the ABX action test even when the ABX action is coded correctly. In general, ABX actions are designed based on the assumption that they receive the payload from the event broker service. To make testing possible, you can set **Default inputs** to pass the sort of values that you expect the payload to include. If you set **Default inputs** and your ABX action is called by the event broker service, then values included in the payload override the default inputs.

VMware Aria Automation runs your ABX script code in a container. If your code depends on libraries or packages not included in the container, you can specify the needed content by setting a value in the **Dependency** text box.

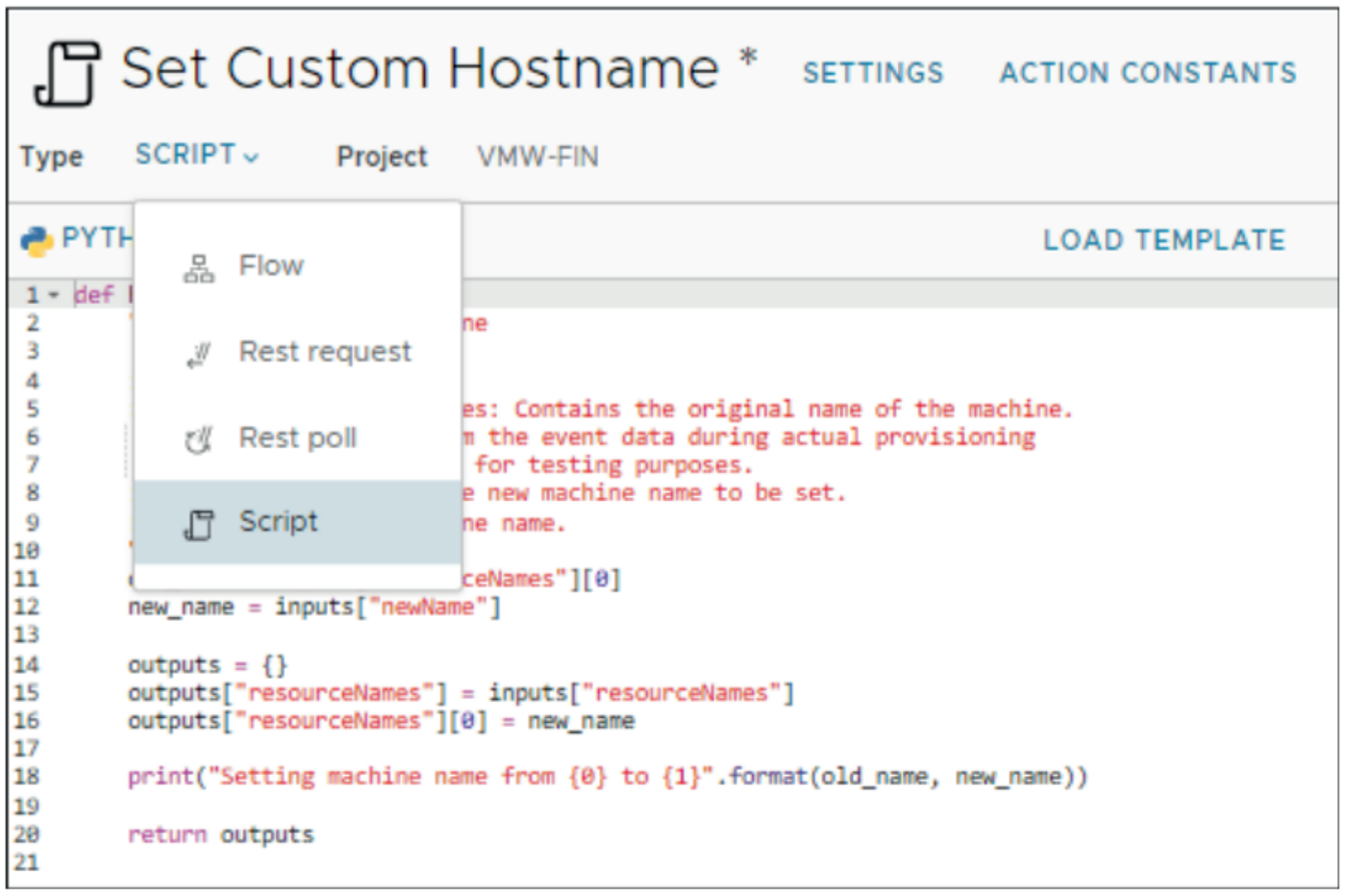
The **FaaS provider** drop-down menu is used to specify where you want your ABX action script to run. Choices include **AWS**, **Azure**, and **On Prem**. **On Prem** refers to a non-cloud system, for example, a local vSphere system.

When you select the **Set custom limits and retry options** check box, you can set a memory limit and timeout on the execution of your ABX script. These quotas are useful in situations in which you are charged by the FaaS provider based on your ABX action's CPU and memory consumption. **Memory limit (MB)** and **Timeout (s)** are used to set the quotas in megabytes and seconds, respectively.

By selecting the **Retry on failure** check box, you can instruct VMware Aria Automation to retry your ABX action if your ABX action fails.

12-30 ABX Flows, ABX REST Calls, and ABX Scripts

In addition to ABX action scripts, VMware Aria Automation also creates ABX REST calls and ABX flows.



The **Script** option creates an ABX action that calls a written code. This code can be written in Node.js, PowerShell, or Python.

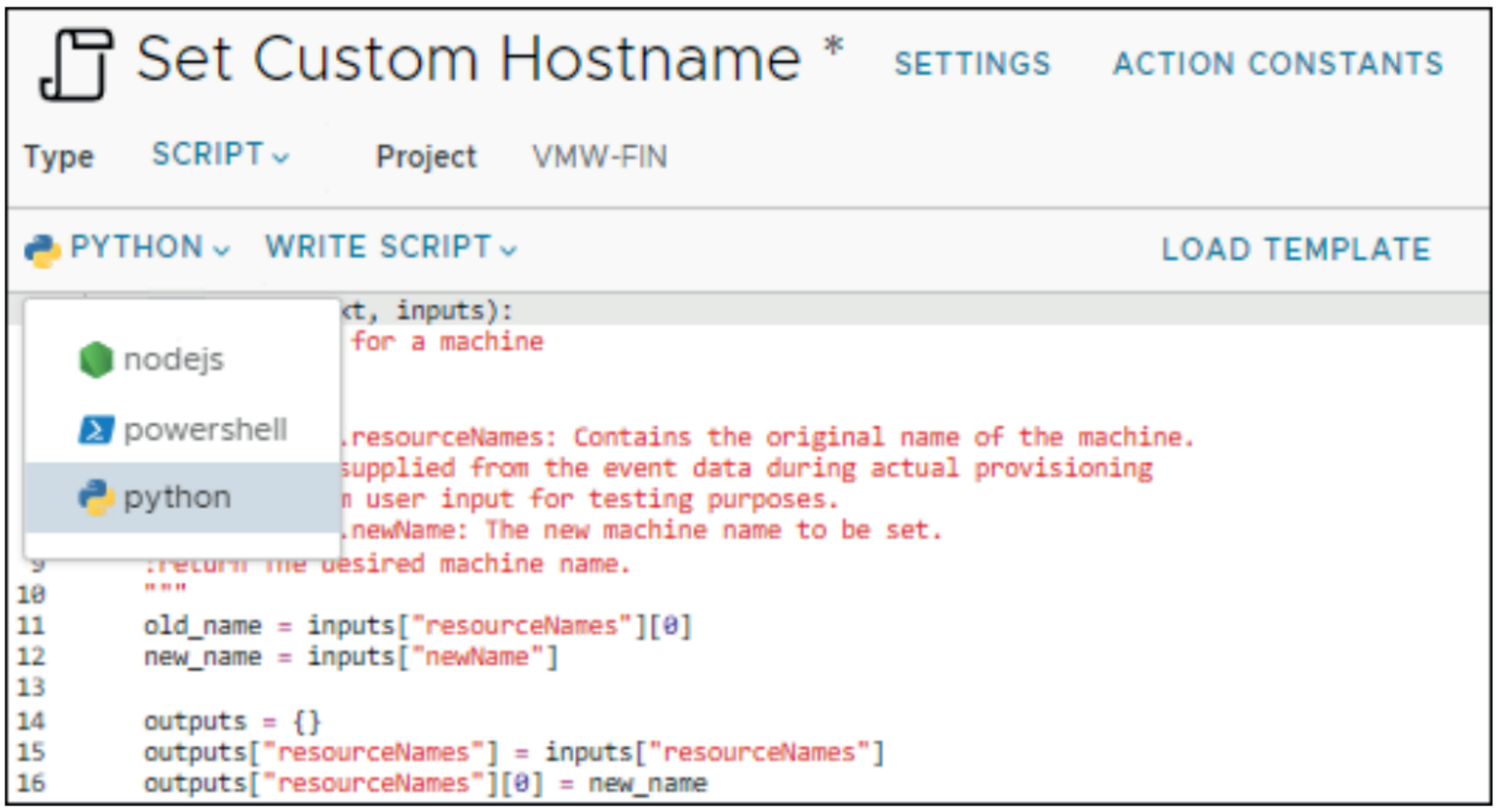
You use **REST request** and **REST poll** to invoke a REpresentational State Transfer (REST) operation once or periodically, respectively. Numerous VMware products and third-party products support REST operations.

A flow is like a VMware Aria Automation Orchestrator workflow. With the **Flow** option, you can string together multiple ABX actions that run in a sequence that you define.

12-31 Polyglot Capabilities of ABX

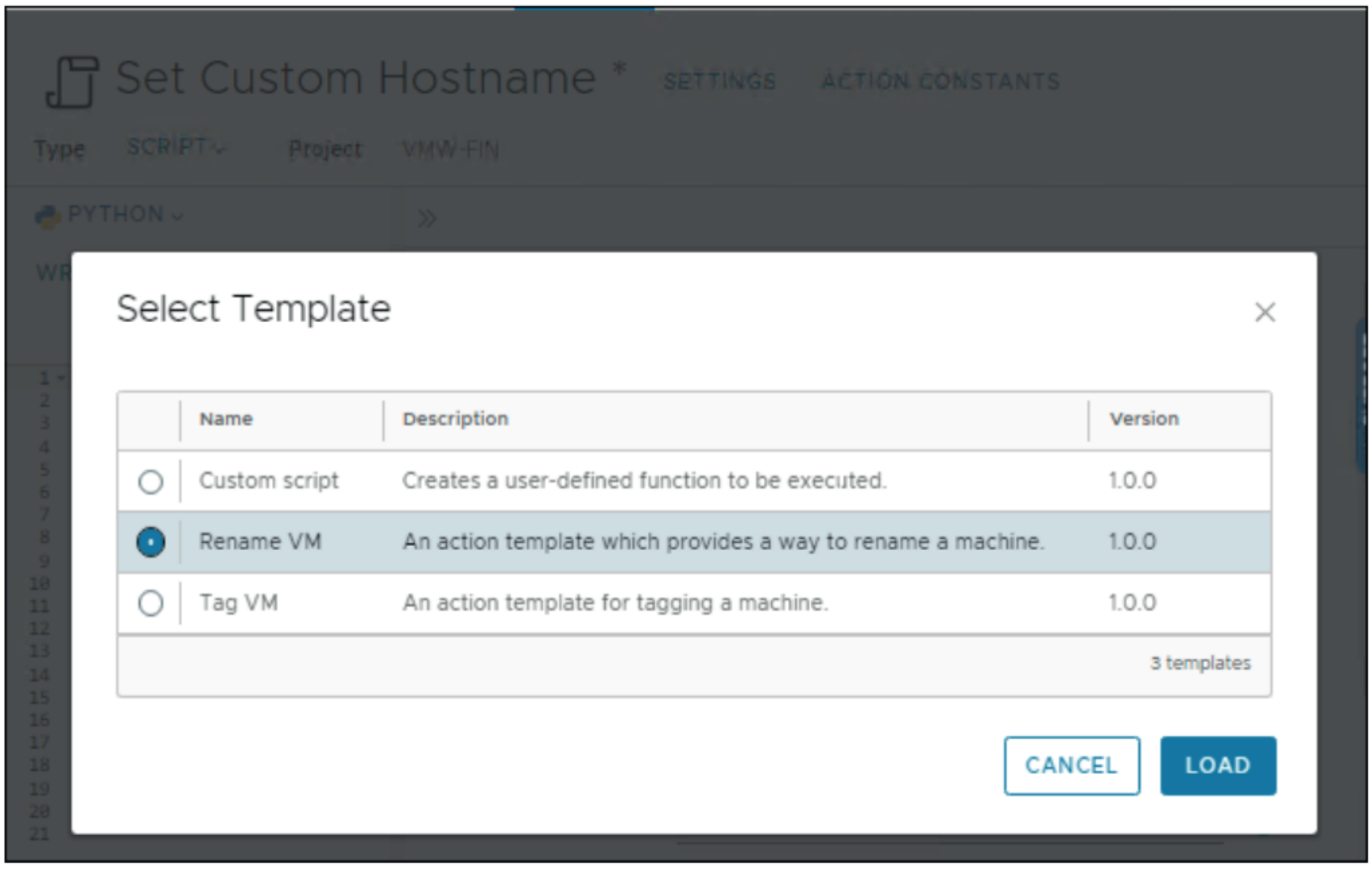
The ABX action script code can be written in multiple languages:

- Node.js
- PowerShell
- Python



12-32 ABX Action Templates

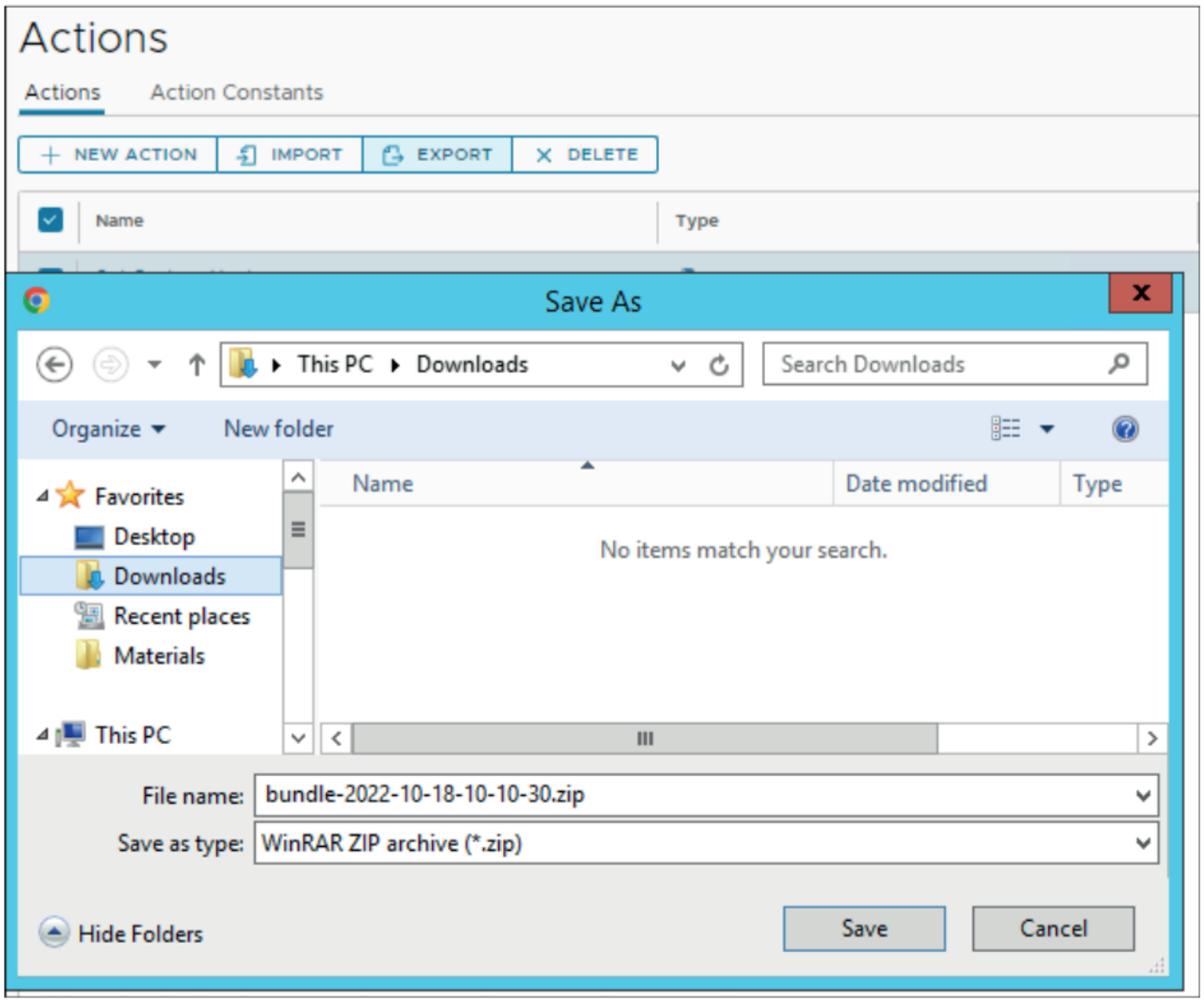
Templates accelerate the development of ABX actions.



Rather than writing entirely new ABX action code, you can base your ABX action on one of the templates provided by VMware Aria Automation.

12-33 Packaging ABX Actions

ABX actions can be imported and exported between VMware Aria Automation environments.

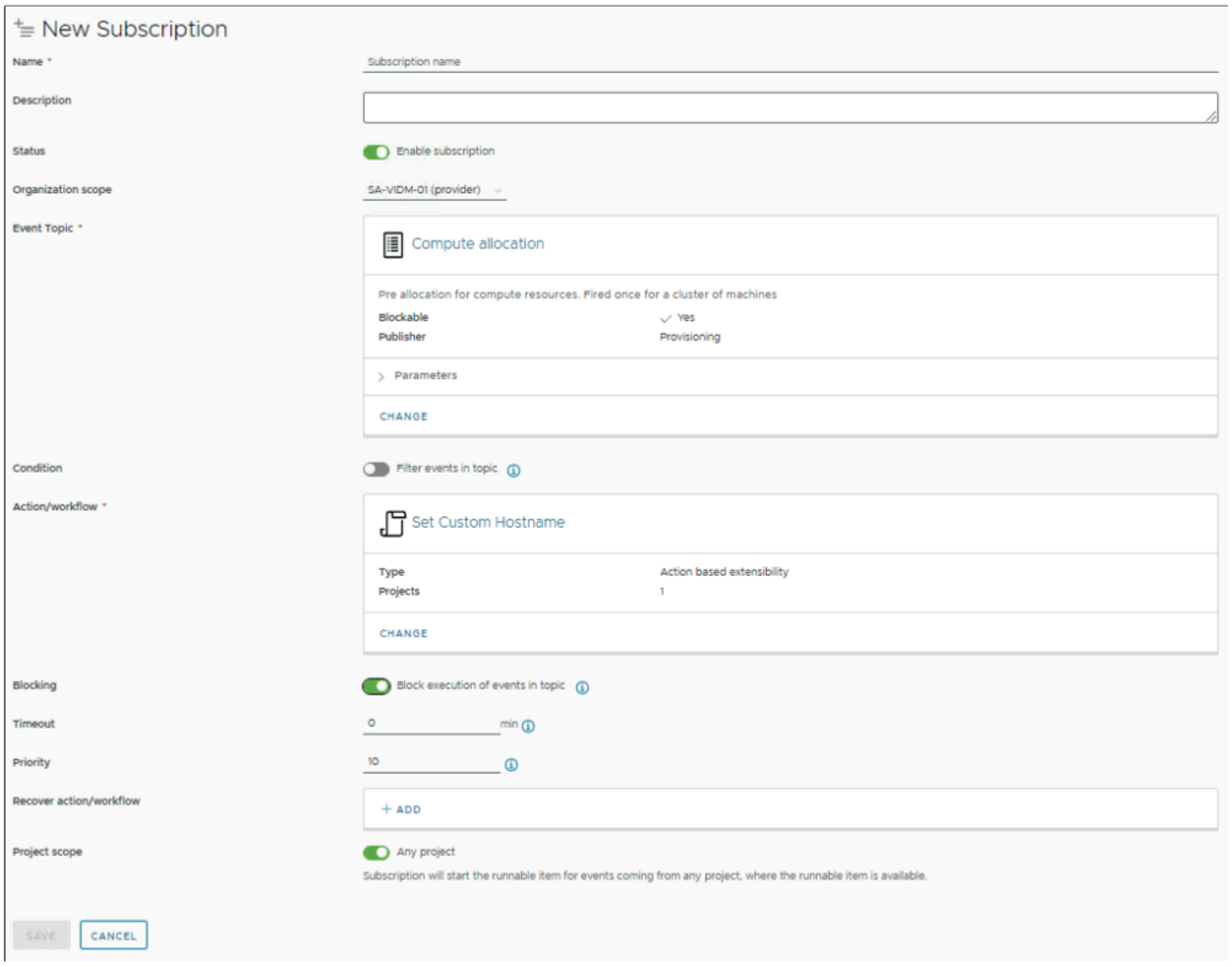


12-34 Calling ABX Actions

One way to call an ABX action is from a subscription.

You can also call ABX actions in the following ways:

- Creating a "custom resource"
- Creating a catalog item in Service Broker



One way to call your ABX action is from a subscription, but this is not the only way.

You can also create a custom resource that calls your ABX action. By creating a custom resource, you can create another component that you can drag into your cloud template.

A third way of calling your ABX action is to set it up as a catalog item in Service Broker.

12-35 Lab 33: Using ABX to Set Custom Host Names

Set a custom host name on a machine deployed from a VMware Aria Automation template:

1. Create a VMware Aria Automation Templates
2. Create an ABX Action
3. Create a Subscription
4. Deploy Your VMware Aria Automation Template
5. Delete Your Deployment to Save Lab Resources

12-36 Review of Learner Objectives

- Create an ABX action
- Use the polyglot capability of ABX
- Specify the entry point of an ABX action

12-37 Key Points

- Extensibility techniques provide the ability to extend the capabilities of VMware Aria Automation.
- VMware Aria Orchestrator workflows automate IT infrastructure processes.
- ABX actions provide an additional method for automation.

Questions?

Module 13

Integration with Kubernetes

13-2 Importance

Modern applications running as microservices are more suited to run on the Kubernetes platform. VMware Aria Automation supports integration with several Kubernetes platforms to automate the deployment and management of Kubernetes components.

13-3 Lesson 1: Integration with Kubernetes

13-4 Learner Objectives

- List the various Kubernetes integration options available in VMware Aria Automation
- Describe vSphere with Tanzu components
- Explain how to integrate VMware Aria Automation with external Kubernetes
- Create a VMware Aria Automation template with Kubernetes components

13-5 Overview of Kubernetes Integration

Using VMware Aria Automation, administrators can monitor, manage, and obtain an overview of multiple Kubernetes clusters at once.

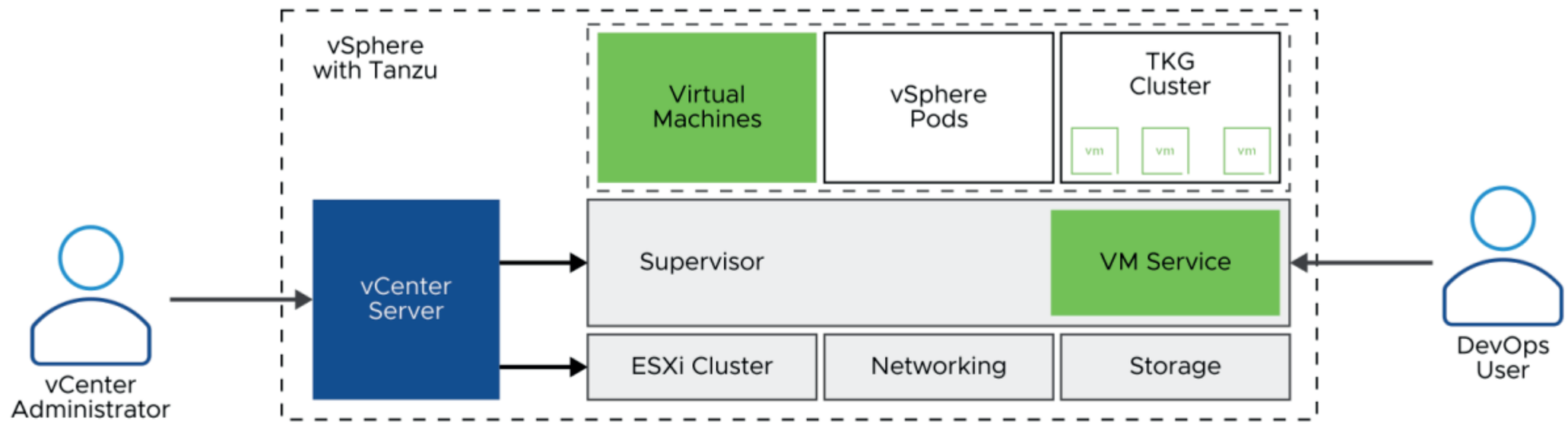
The following Kubernetes integration options are supported:

- vSphere with Tanzu
- Tanzu Kubernetes Grid Integrated Edition
- External Kubernetes
- Red Hat OpenShift

VMware Aria Automation supports the integration with VMware vSphere with Tanzu. In version 7.x, this is also known as Tanzu Kubernetes Grid Service.

13-6 Introduction to vSphere with Tanzu

vSphere with Tanzu transforms vSphere into a native Kubernetes platform.



When vSphere with Tanzu is enabled, a supervisor cluster is created.

The supervisor cluster runs on an SDDC layer and uses the following components:

- ESXi for compute
- NSX for networking
- vSAN or other shared storage solution as the shared storage for vSphere pods, Tanzu Kubernetes clusters, and VMs that run in the supervisor cluster

After a supervisor cluster is created, you can create namespaces in the supervisor cluster called supervisor namespaces.

As of version vSphere 7.x, supervisor namespaces are now referred to as vSphere namespaces. However, the VMware Aria Automaton UI and documentation for version 8.10 is not updated to reflect the new name. This course uses the term supervisor namespaces.

DevOps engineers can run Kubernetes workloads and deploy containers directly on the supervisor cluster. These containers run in vSphere pods. vSphere pods are Kubernetes pods that run directly in the ESXi hypervisor. Each pod can consist of multiple containers.

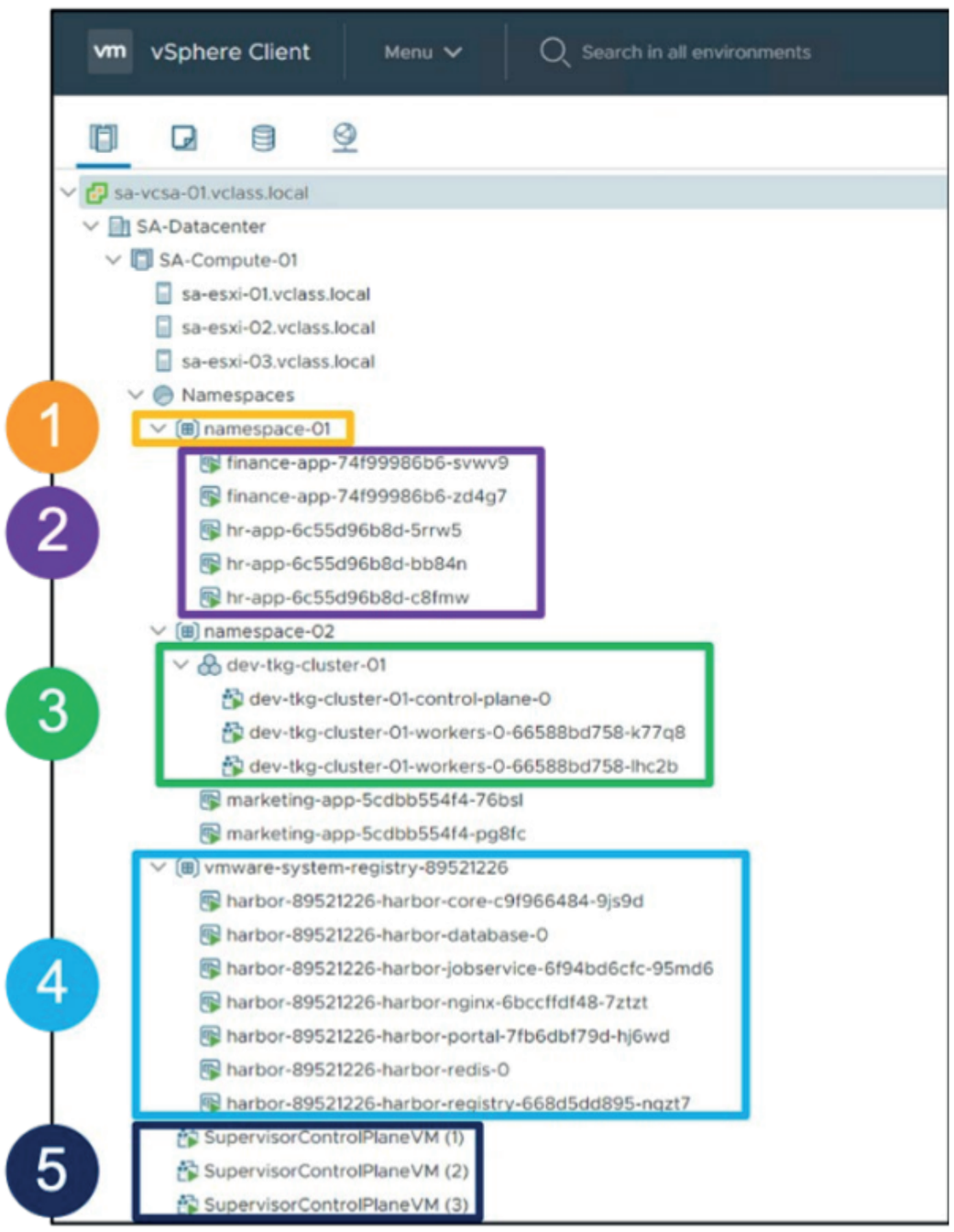
13-7 vSphere with Tanzu: Virtual Machines

To run container-based workloads natively on vSphere, you enable Workload Management:

- A three-node supervisor cluster is deployed.
- Manually create a supervisor namespace on the supervisor cluster.
- (Optional) Deploy a Tanzu Kubernetes cluster.

The following objects are visible in the Hosts and Clusters view:

1. Supervisor namespaces
2. vSphere pods
3. Tanzu Kubernetes clusters
4. Harbor registry
5. Supervisor clusters



Select between creating the supervisor cluster with the vSphere networking stack or with NSX as the networking solution. vSphere pods are only supported on supervisors that use NSX as their networking stack. They are not supported on supervisors that are configured with the VDS networking stack.

You can enable Workload Management with the 60-day free trial license, after that a valid Tanzu Edition license is required to use the product after the 60-days trial.

The following objects are visible in the Hosts and Clusters view:

- Supervisor namespaces: You create a supervisor namespace on a supervisor cluster and configure it with resource quota, storage policy, and user permissions. You associate it with a content library for fetching the latest Tanzu Kubernetes cluster files, if you are using a subscribed content library, or local images for local content libraries.
- vSphere pod: A vSphere pod is a VM with a small footprint that runs one or more Linux containers. The vSphere pods are running directly on the ESXi hosts, managed by the supervisor cluster. vSphere Pods are only supported on supervisor clusters that use NSX as their networking solution.
- Tanzu Kubernetes cluster: Log in to the supervisor cluster namespace and use the content library files to deploy a Tanzu Kubernetes cluster. Access to the Tanzu Kubernetes clusters can be granted to a developer. The developer can manage the Tanzu Kubernetes cluster as a normal Kubernetes cluster using the kubectl commands.
- Harbor registry: Use images that are stored in the harbor registry to deploy vSphere pods in namespaces on the supervisor cluster.
- Supervisor Cluster: A Kubernetes cluster that manages vSphere pods and Tanzu Kubernetes clusters.

Starting from vSphere 8, the Tanzu Kubernetes clusters are called Tanzu Kubernetes Grid clusters.

See the sections about enabling workload management with vSphere networking and NSX networking in *vSphere with Tanzu Configuration and Management* at https://docs.vmware.com/en/VMware-vSphere/index.html.

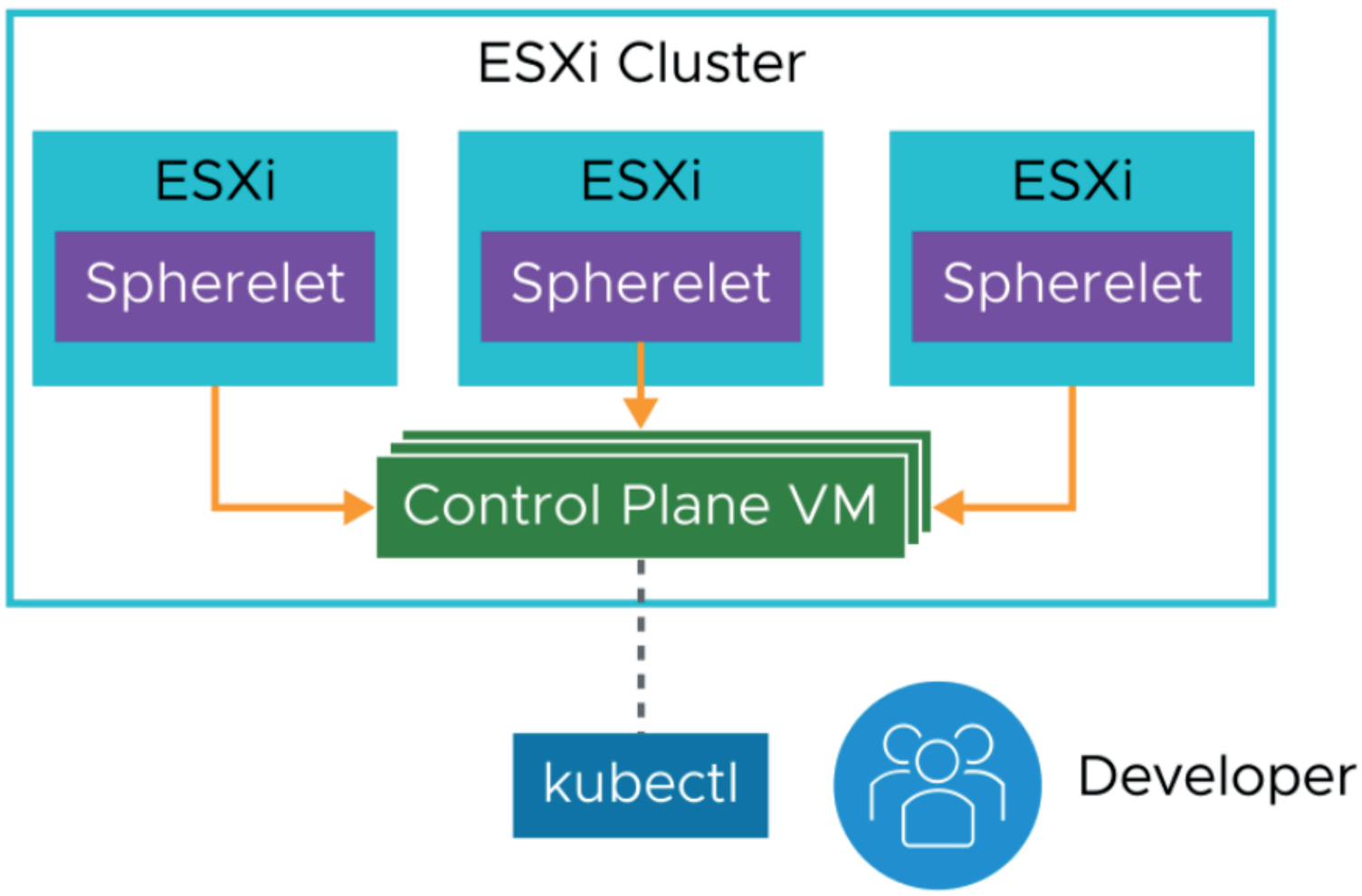
See the section about configuring and managing a supervisor cluster in *vSphere with Tanzu Configuration and Management* at https://docs.vmware.com/en/VMware-vSphere/index.html.

See the section about working with Kubernetes in VMware Aria Automation in *Using and Managing Cloud Assembly* at https://docs.vmware.com/en/vRealize-Automation/index.html.

13-8 vSphere with Tanzu: Supervisor Clusters

The supervisor cluster includes a set of control plane VMs that provide API access to the supervisor cluster.

The control plane VM serves as an endpoint for Kubernetes users to manage their namespaces using the familiar kubectl CLI.



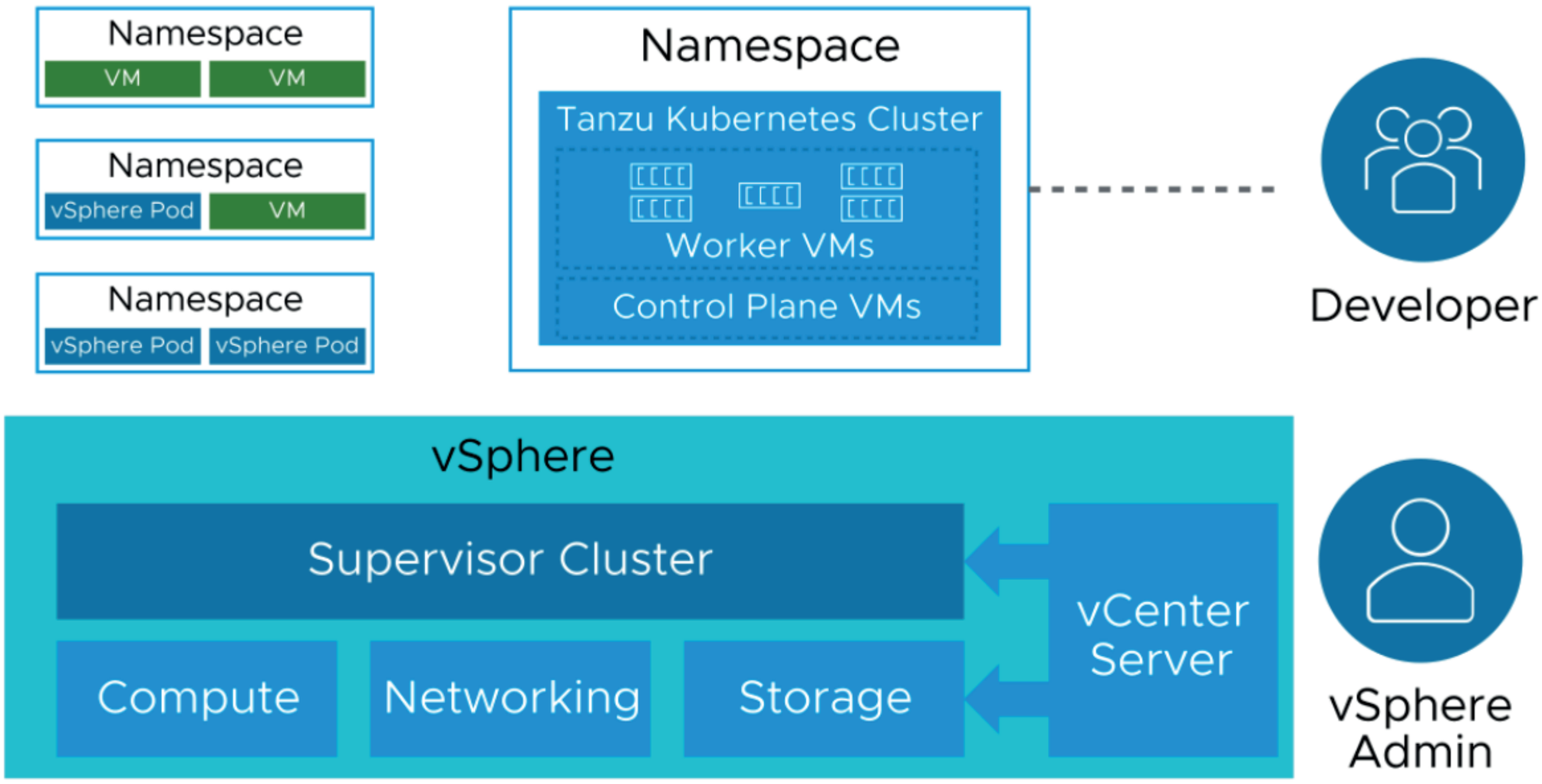
The three control plane VMs are load balanced by a load balancer that has its own virtual IP address. Additionally, a floating IP address is assigned to one of the VMs.

An additional process called Spherelet is started on each host. The Spherelet process is based on the Kubernetes kubelet. Spherelet is ported natively to ESXi and allows the ESXi host to become part of the Kubernetes cluster.

The supervisor cluster provides the management layer by which Tanzu Kubernetes clusters are built. Tanzu Kubernetes Grid Service is a custom controller manager with a set of controllers that is part of the supervisor cluster. Tanzu Kubernetes Grid Service provisions Tanzu Kubernetes clusters.

13-9 vSphere with Tanzu: Tanzu Kubernetes Cluster

Tanzu Kubernetes clusters are built by the supervisor cluster. Administrators can use Tanzu Kubernetes Grid Service to provision and operate Tanzu Kubernetes clusters on the supervisor cluster.

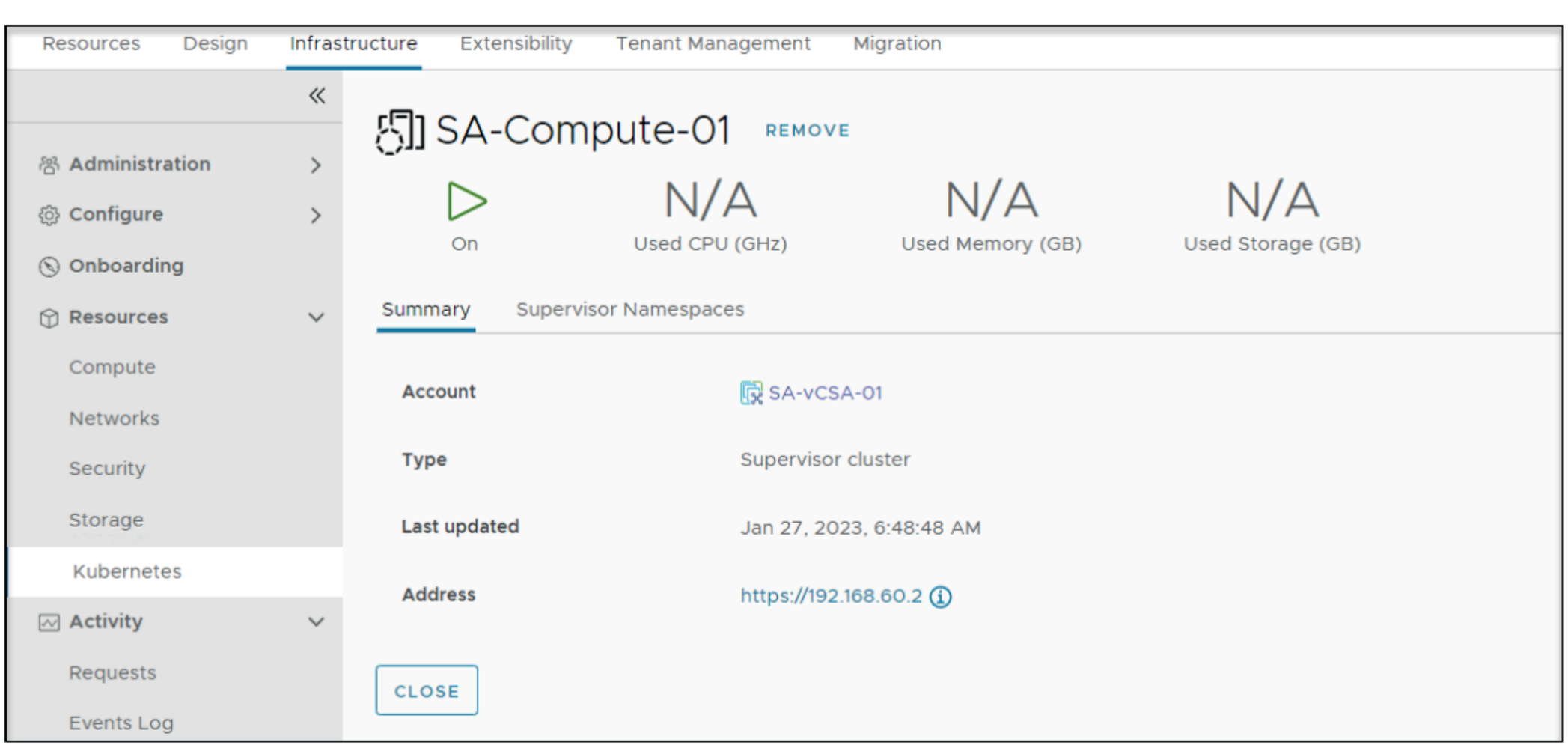


Running a Tanzu Kubernetes cluster can be compared to running traditional Kubernetes clusters by using VMs and a container host OS. Tanzu Kubernetes Grid Service, which runs in the supervisor control VMs, automates the deployment of such a cluster. To summarize, a Tanzu Kubernetes cluster runs inside VMs provisioned on the ESXi host and consists of a control plane and workload nodes. vSphere pods run inside the ESXi hypervisor and accommodate application containers.

13-10 vSphere with Tanzu: Integration

After enabling vSphere with Tanzu, the supervisor cluster can be integrated with VMware Aria Automation:

1. Click the **Infrastructure** tab.
2. Navigate to **Resources** > **Kubernetes**.
3. Click the **Supervisor Clusters** tab.
4. Click **ADD SUPERVISOR CLUSTER**.



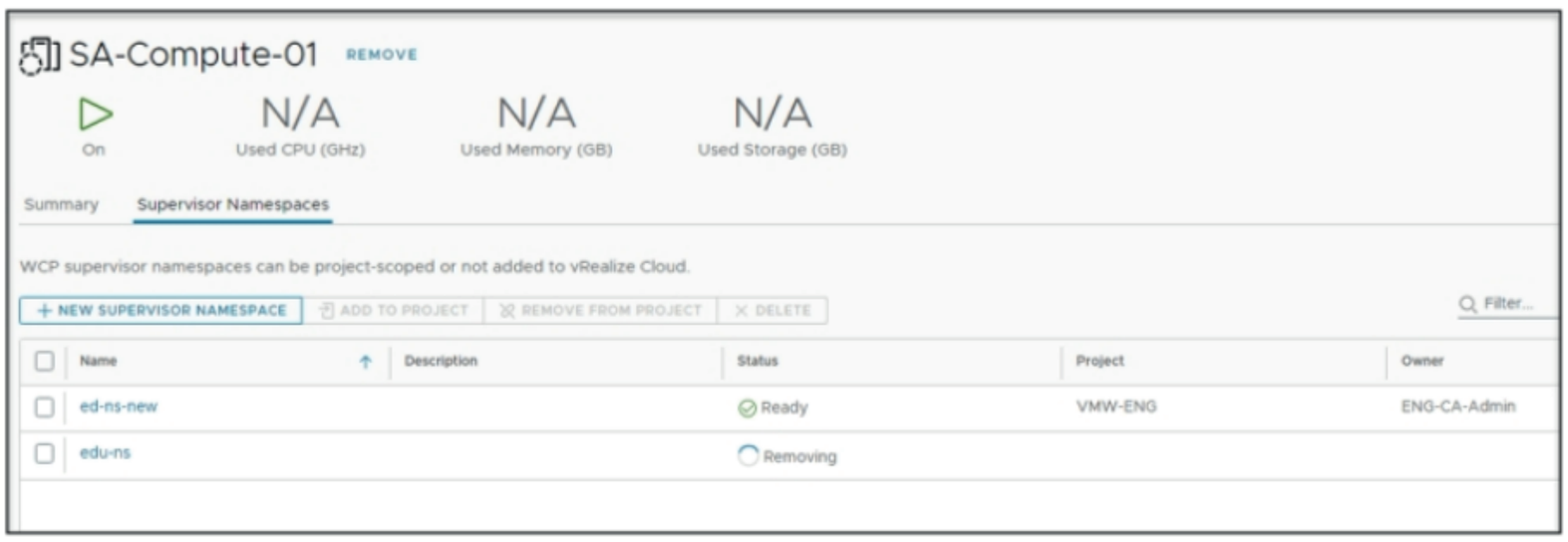
vSphere cloud accounts with Workload Management enabled can be used as managed Kubernetes providers. These accounts also offer at least one supervisor cluster and namespace.

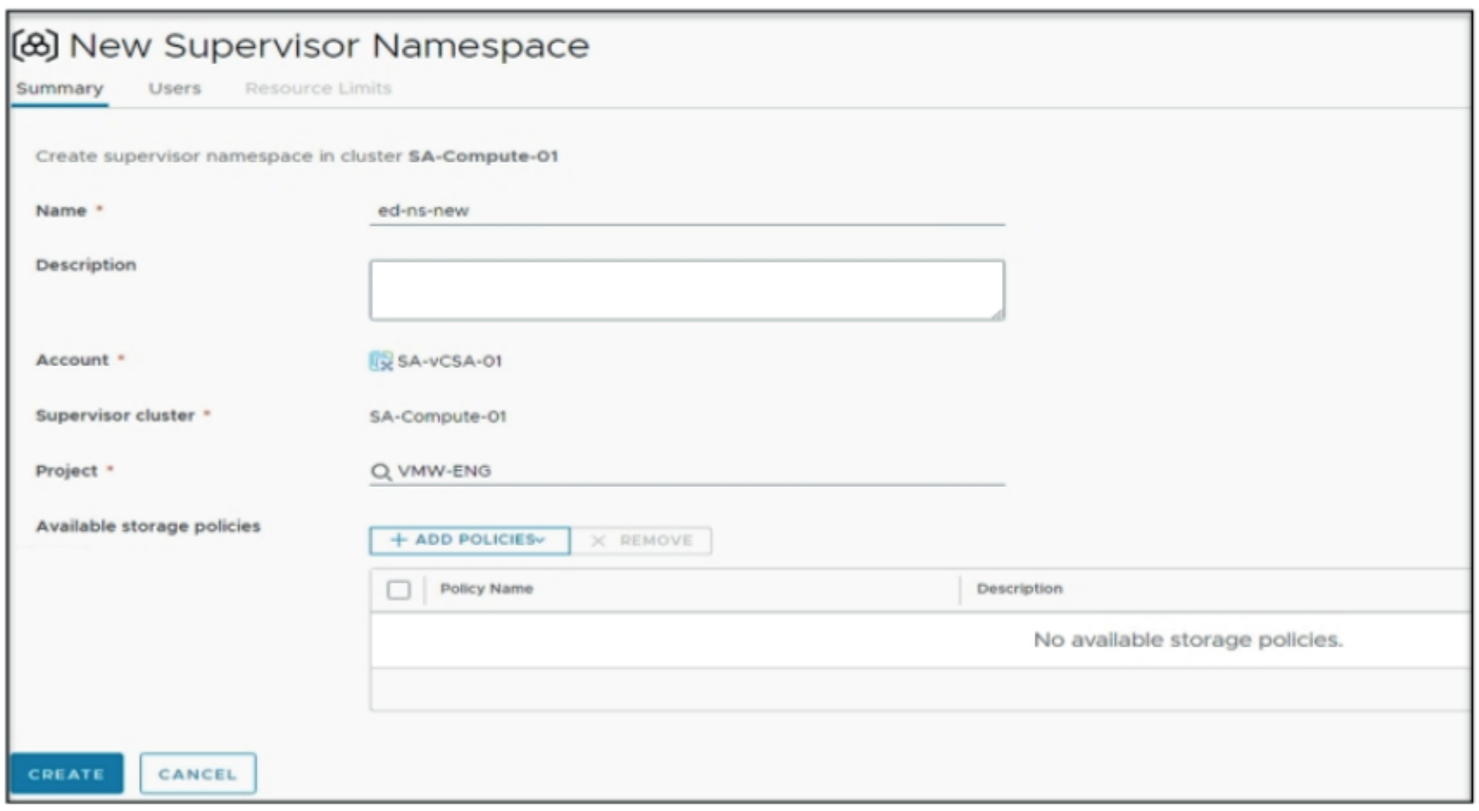
For information about vSphere with Tanzu, see *vSphere with Tanzu Configuration and Management* at https://docs.vmware.com/en/VMware-vSphere/index.html.

13-11 Managing Supervisor Namespaces

After integrating the supervisor cluster with VMware Aria Automation, the administrator can perform the following actions:

- Manage existing supervisor namespaces
- Create supervisor namespaces
- Use the supervisor namespace to deploy vSphere pods or Tanzu Kubernetes clusters





In the example, edu-ns is an existing supervisor namespace created in vSphere. You can add an existing supervisor namespace to the VMware Aria Automation project. All the project users can edit the existing namespace. You can remove the existing supervisor namespace using VMware Aria Automation.

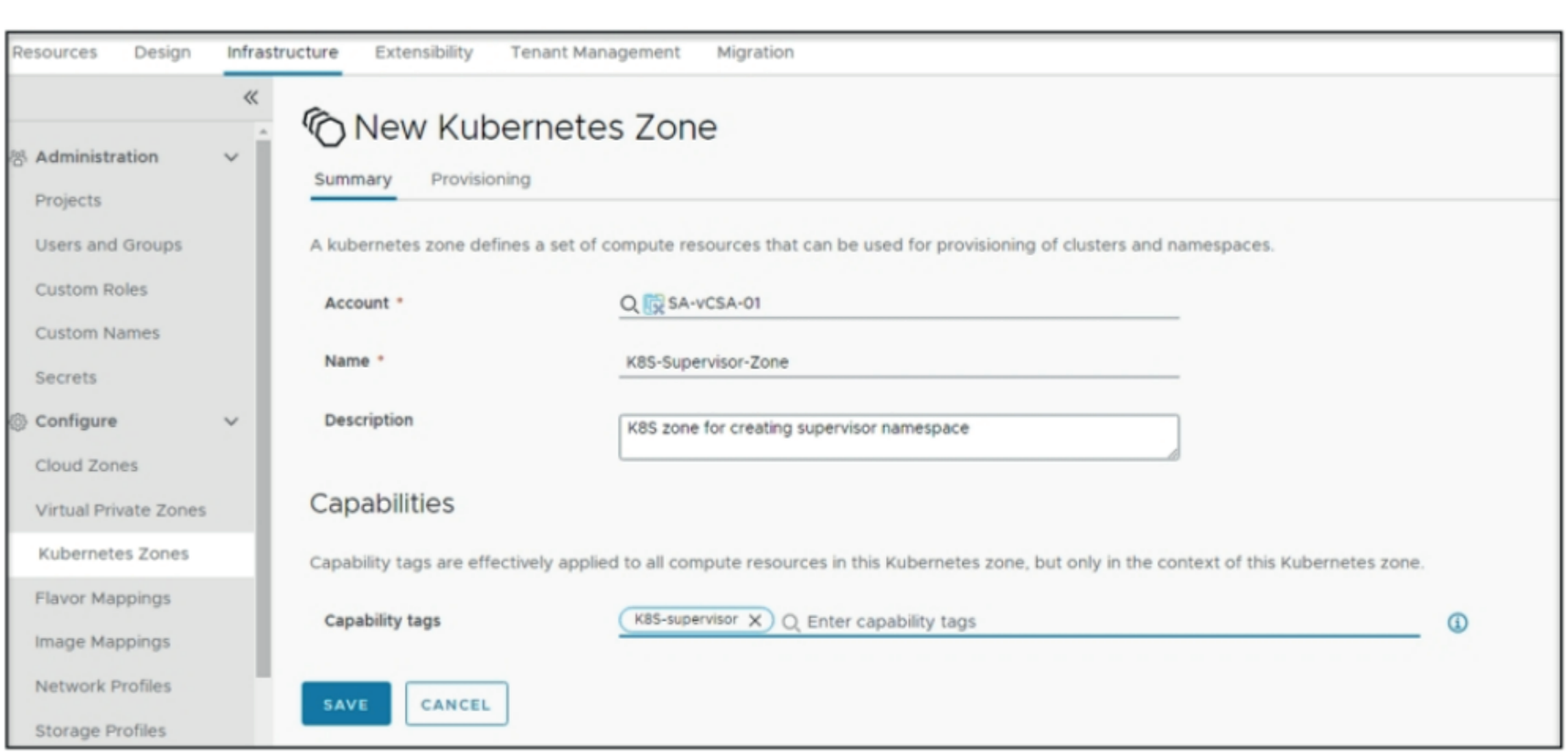
You can also create a supervisor namespace from VMware Aria Automation. All the project users can edit the new namespace.

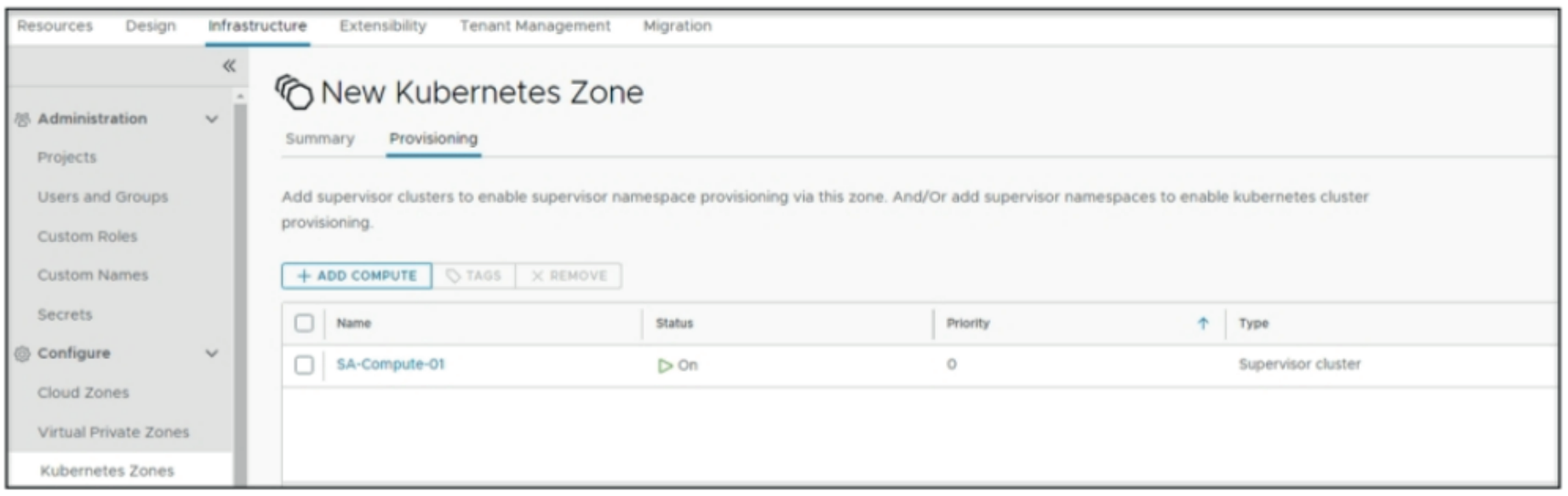
The new supervisor namespace created from VMware Aria Automation can be used to deploy vSphere pods or Tanzu Kubernetes clusters.

13-12 Kubernetes Zones

Create a Kubernetes zone with a Supervisor Cluster for creating namespaces on demand:

1. Click the **Infrastructure** tab.
2. In the navigation pane on the left, select **Configure** > **Kubernetes Zones.**
3. Click **NEW KUBERNETES ZONE**.
4. Specify the details on the **Summary** tab.
5. Select the supervisor cluster on the **Provisioning** tab.
6. Associate the Kubernetes zone with a project.





To create a Kubernetes zone for the supervisor cluster:

1. Select the vCenter system on the **Summary** tab.
2. Select the vSphere cluster where you enabled vSphere with Tanzu on the **Provisioning** tab.

Edit a VMware Aria Automation project and click the **Kubernetes Provisioning** tab to associate the Kubernetes zone with the project.

13-13 Cluster Plans

You create a cluster plan to use with vSphere with Tanzu Kubernetes deployments in VMware Aria Automation. A cluster plan functions as a configuration template for provisioning Tanzu Kubernetes cluster instances on a particular vSphere cloud account instance:

1. Select **Infrastructure** > **Configure** > **Cluster Plan**.
2. Click **New Cluster Plan**.
3. Select an account on which to apply the cluster plan.
4. Enter a Name, and **Description** for the cluster plan.
5. Select the Kubernetes version that is applicable to this cluster plan.
6. Configure the **Control plane** and **Workers** settings.
7. Under the Additional Settings section, select the default PVC storage class to use with this cluster.
8. Configure the behavior regarding usage of storage classes and network settings.
9. Click **CREATE**.

To create a cluster plan, you must first perform the following actions:

1. Access to the vSphere 7.x cloud account with Tanzu enabled and one or more vSphere namespaces.
2. All supervisor clusters on the registered vSphere cloud account that are eligible for provisioning of Tanzu Clusters must be added as managed entities on the VMware Aria Automation Assembler.

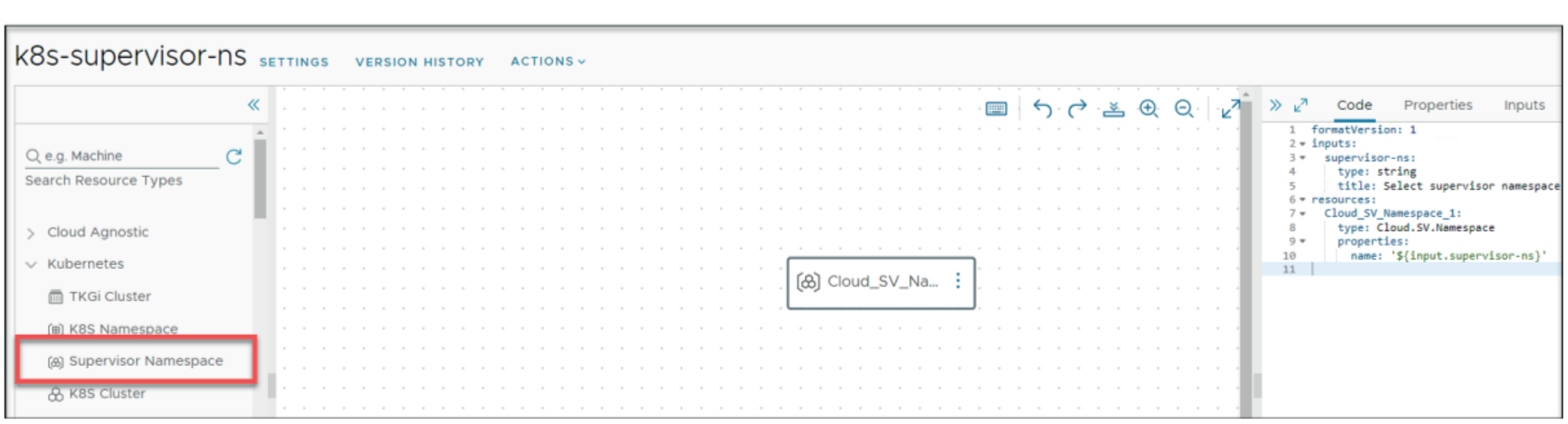
Tanzu Kubernetes Grid Integrated Edition does not require a VMware Aria Automation Assembler cluster plan.

13-14 VMware Aria Automation Template: On-Demand Namespaces

You create a VMware Aria Automation template to deploy supervisor namespaces on demand:

1. Drag the **Kubernetes Supervisor Namespace** resource to the design canvas.
2. Configure `inputs:` in the YAML section.

The VMware Aria Automation template can be made available in the VMware Aria Automation Consumption catalog.



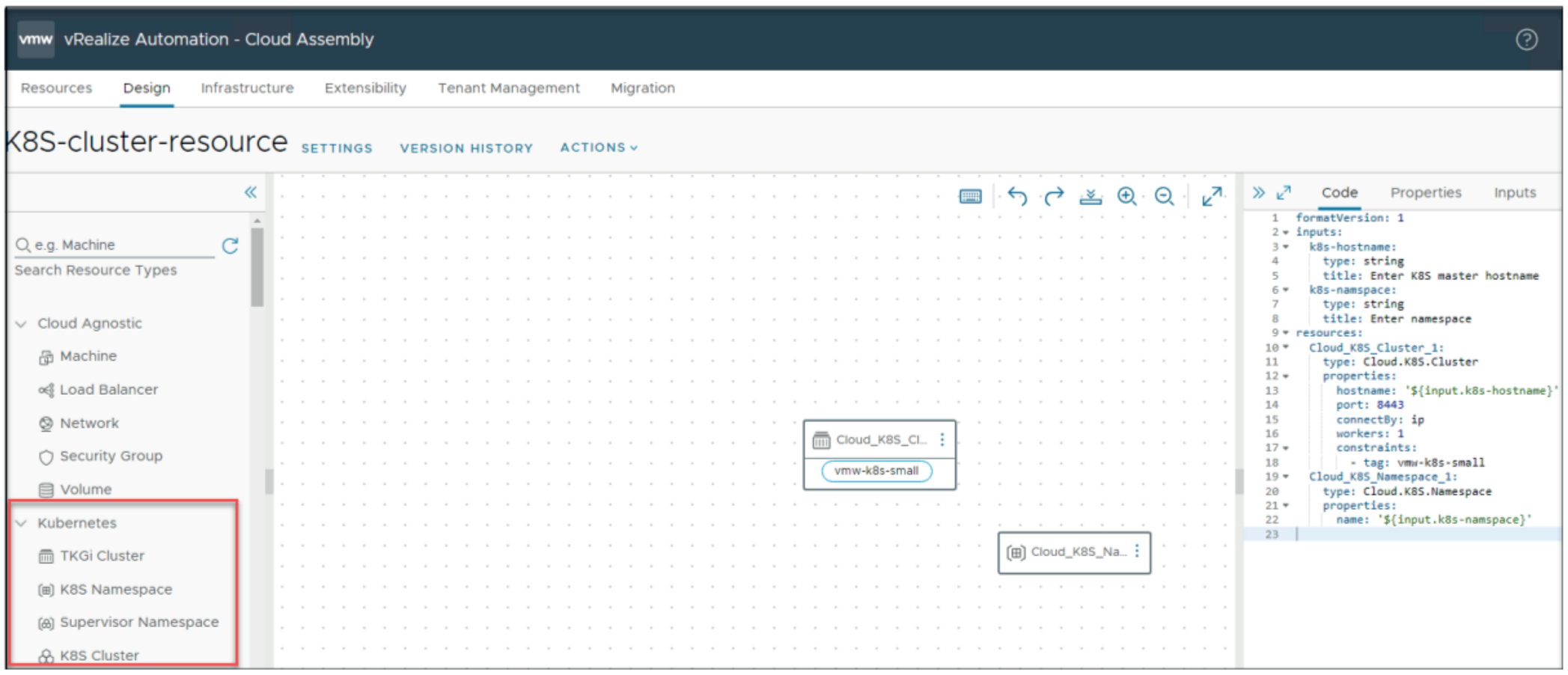
At the time of creating the VMware Aria Automation template, select the project with a Kubernetes zone assigned.

Configure the input for the users to enter their namespaces when requested.

You can version the VMware Aria Automation template and release it to the VMware Aria Automation Consumption catalog. The catalog item can be made available for the business users.

13-15 Kubernetes Resources in VMware Aria Automation Templates

You create a VMware Aria Automation template to deploy an on-demand Kubernetes cluster, Tanzu Kubernetes Grid Integrated Edition cluster, and namespace.

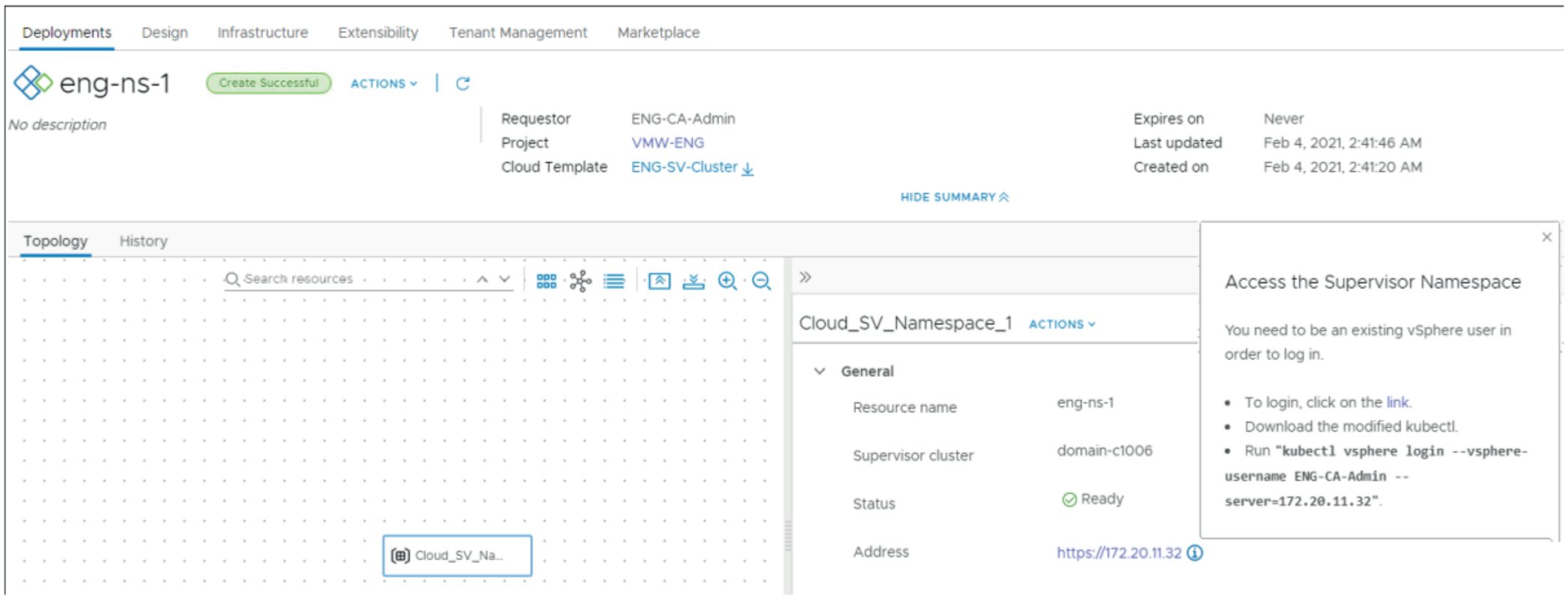


Kubernetes components are available to use with VMware Aria Automation Templates. When adding Kubernetes components to a VMware Aria Automation template, you choose between adding clusters or enabling users to create namespaces in various configurations. Typically, this choice depends on your access control requirements, your Kubernetes component configurations, and your deployment requirements.

Administrators can set up a VMware Aria Automation template with variables so that users can input the desired cluster host name or namespace when requesting a deployment. Tags can also be used to select a zone and a Tanzu Kubernetes Grid Integrated Edition plan during the resource allocation phase of cluster deployment.

13-16 Deploying the Tanzu Kubernetes Cluster

The steps to log in to the on-demand supervisor namespace can be accessed from the deployment. The Tanzu Kubernetes cluster can also be deployed on the requested on-demand namespace.



Users can use `kubectl` to log in to the Tanzu Kubernetes cluster.

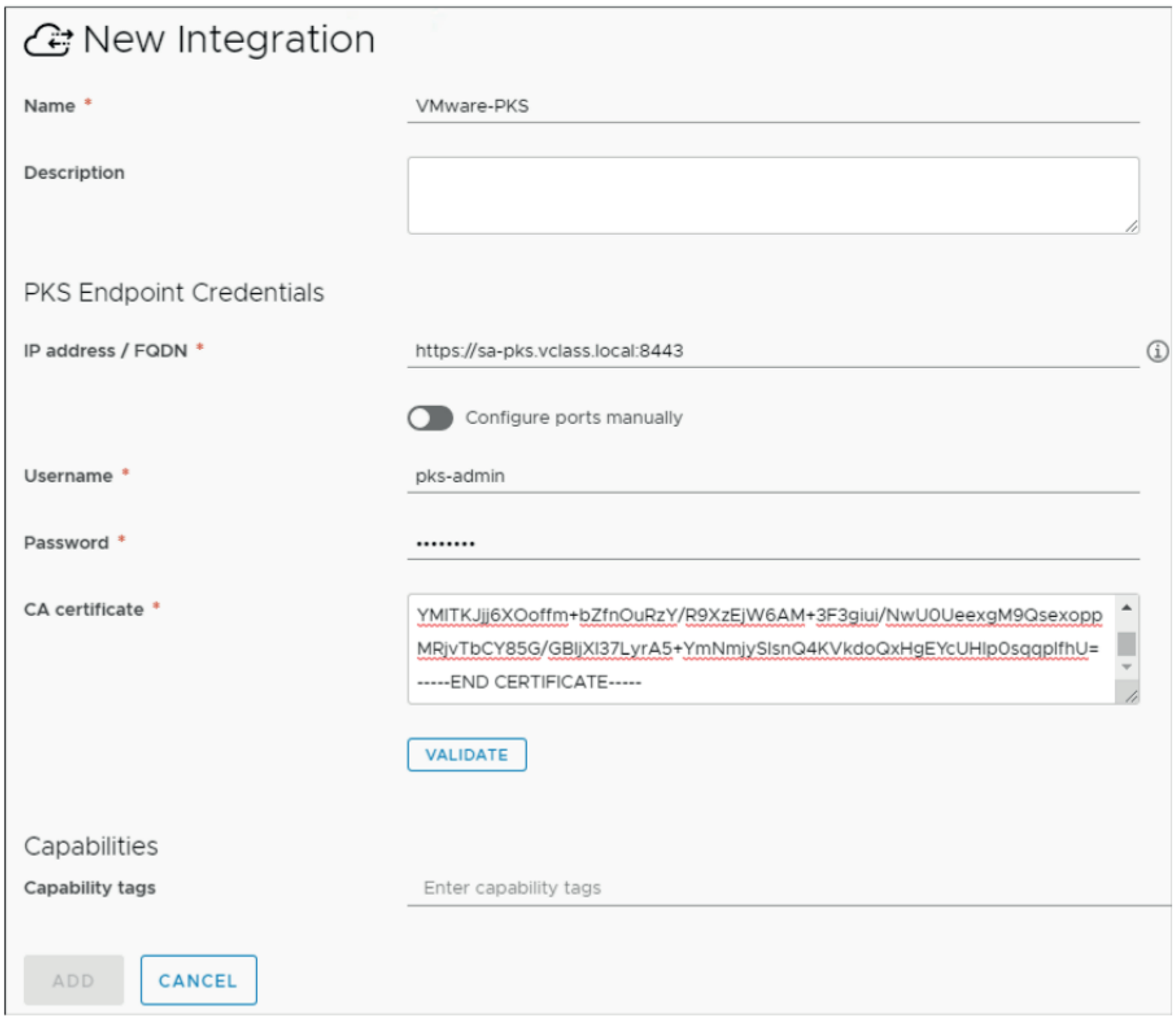
Users can deploy pods and services in the same way as on any Kubernetes cluster.

13-17 Integrating VMware Tanzu Kubernetes Grid Integrated Edition

Tanzu Kubernetes Grid Integrated Edition (formerly called VMware Enterprise PKS) simplifies the deployment and management of Kubernetes clusters so that you can run and manage containers at scale on private and public clouds.

To create a Tanzu Kubernetes Grid Integrated Edition integration:

1. Click the **Infrastructure** tab.
2. In the navigation pane on the left, select **Connections** > **Integrations**.
3. Click **ADD INTEGRATION**.
4. Select **VMware Enterprise PKS**.



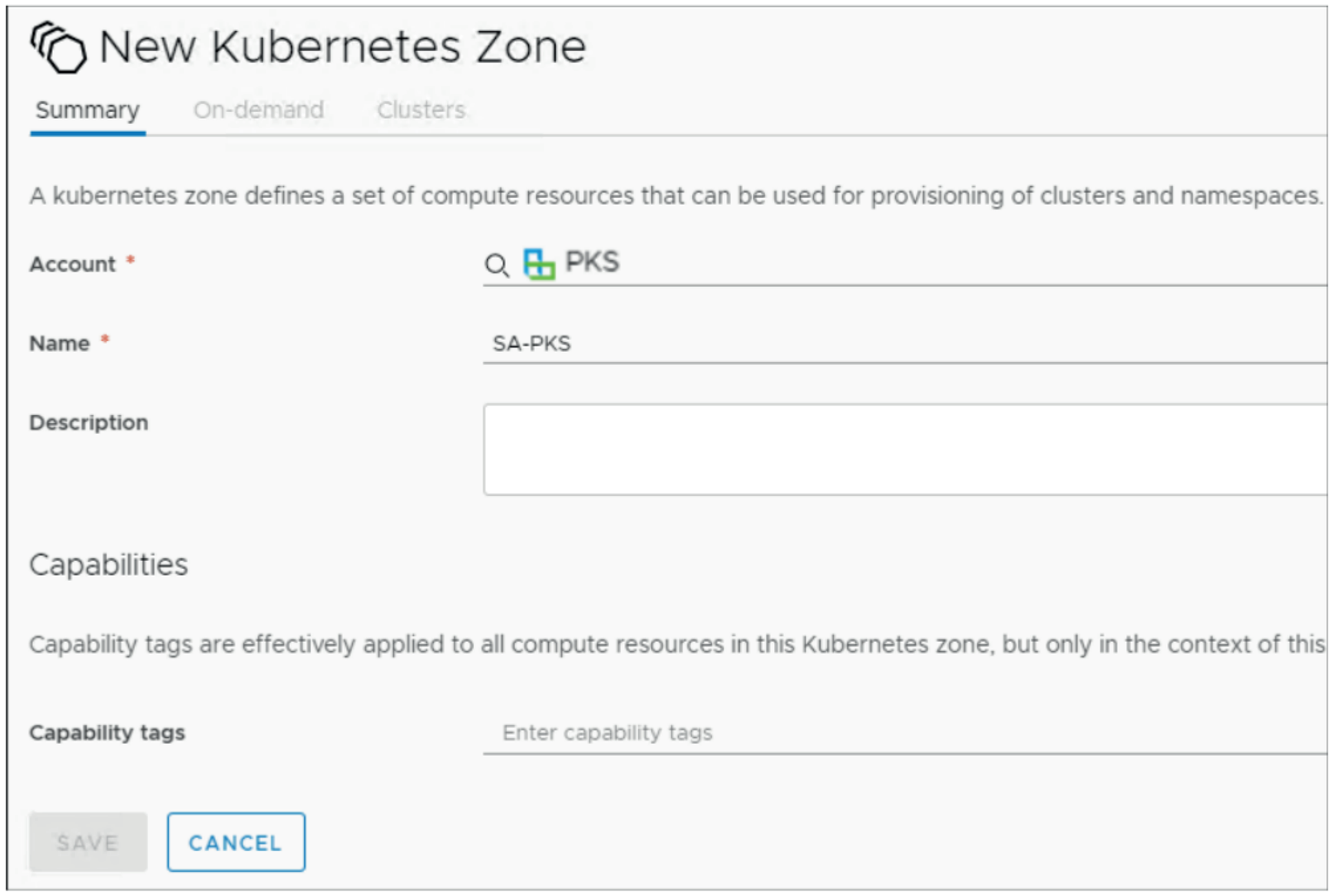
Tanzu Kubernetes Grid Integrated Edition includes critical production capabilities, such as high availability, autoscaling, health checks, self-healing, and rolling upgrades for Kubernetes clusters.

13-18 Tanzu Kubernetes Grid Integrated Edition: Kubernetes Zone

Kubernetes zones enable cloud administrators to define policy-based placement of Kubernetes clusters and namespaces.

To create a Kubernetes zone:

1. Click the **Infrastructure** tab.
2. In the navigation pane on the left, select **Configure** > **Kubernetes Zones**.
3. Click **NEW Kubernetes Zone**.



When creating a Kubernetes zone for Tanzu Kubernetes Grid Integrated Edition, the administrator can assign multiple resources to the zone. These resources dictate what properties can be set for the newly provisioned clusters and are referred to as Tanzu Kubernetes Grid Integrated Edition plans.

On the **On-demand** tab, select one or more plan and assign priorities to them. You can define the number of workers, masters, available CPUs, and other configuration settings in a plan.

You must associate the Kubernetes zone with a project before creating a VMware Aria Automation template.

13-19 Kubernetes Cluster Options

The option that you select to integrate VMware Aria Automation with Kubernetes depends on the platform and use case.

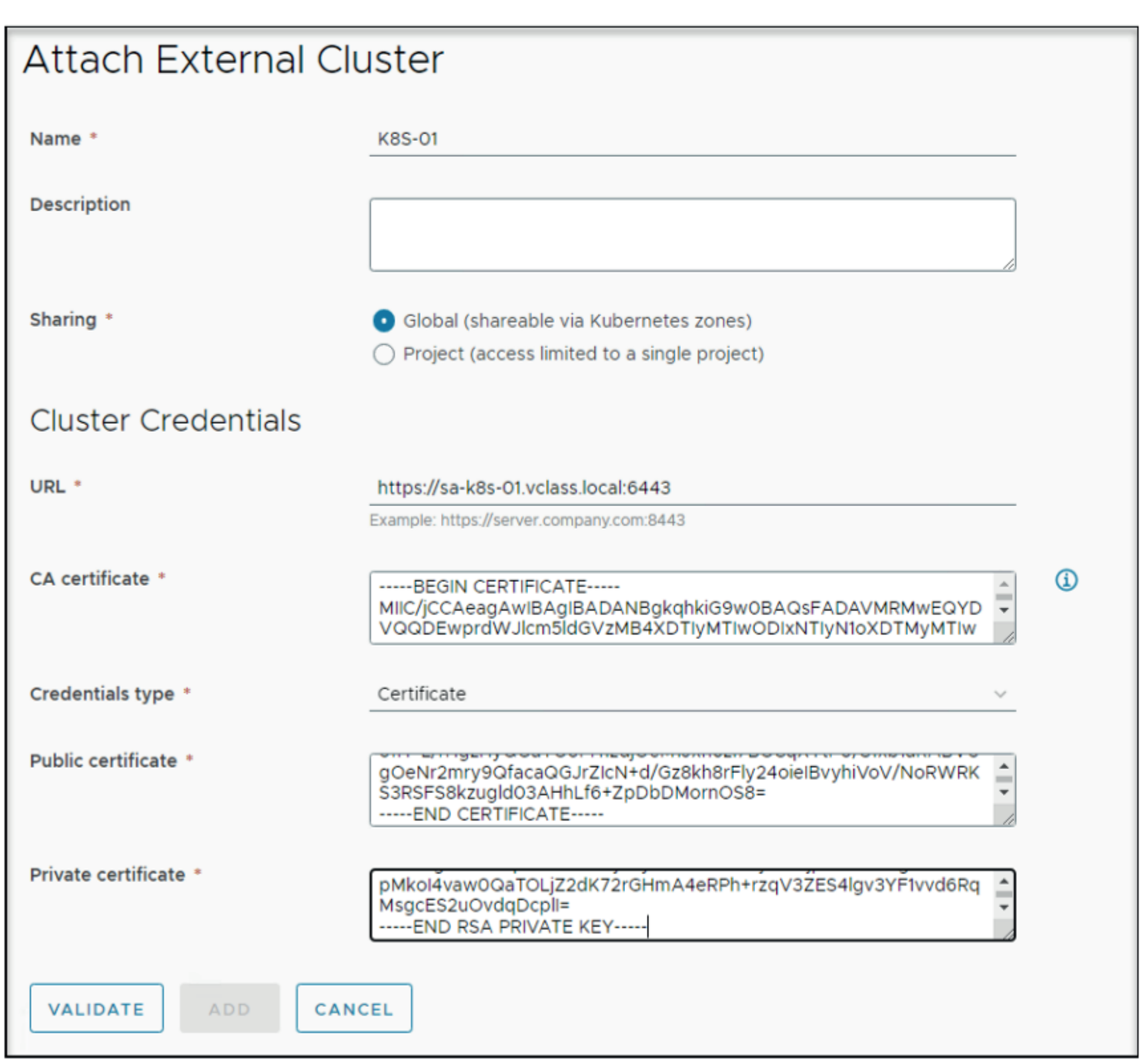
Integration Option	Description	Details
Deploy Cluster	Add new clusters to VMware Aria Automation Assembler.	You can deploy an on-demand Tanzu Kubernetes cluster on a vSphere with Tanzu enabled cloud account using cluster plans. You can also deploy an on-demand Kubernetes cluster to an integrated Tanzu Kubernetes Grid Integrated Edition cloud account.
Add from cloud account	Configure an existing cluster to work with your project.	Specify the Tanzu Kubernetes Grid Integrated Edition or the vSphere with Tanzu enabled cloud account, the (supervisor) cluster to use, the project, and the sharing scope.
Attach external cluster	Add an external Kubernetes cluster, which might not be associated with Tanzu Kubernetes Grid Integrated Edition, to VMware Aria Automation Assembler.	Connect to an external Kubernetes cluster.

13-20 Integrating External Kubernetes

An existing external Kubernetes cluster can be imported into VMware Aria Automation. You cannot deploy a new external Kubernetes cluster from VMware Aria Automation.

To add an existing Kubernetes cluster:

1. Click the **Infrastructure** tab.
2. In the left navigation pane, select **Resources** > **Kubernetes**.
3. Select **ADD EXTERNAL**.



After an external Kubernetes cluster is imported into VMware Aria Automation, you can perform the following tasks:

- Create a namespace
- Add an existing namespace

You can create a Kubernetes zone and associate it with a project. VMware Aria Automation Templates can also be created to request on-demand namespaces on the external Kubernetes cluster.

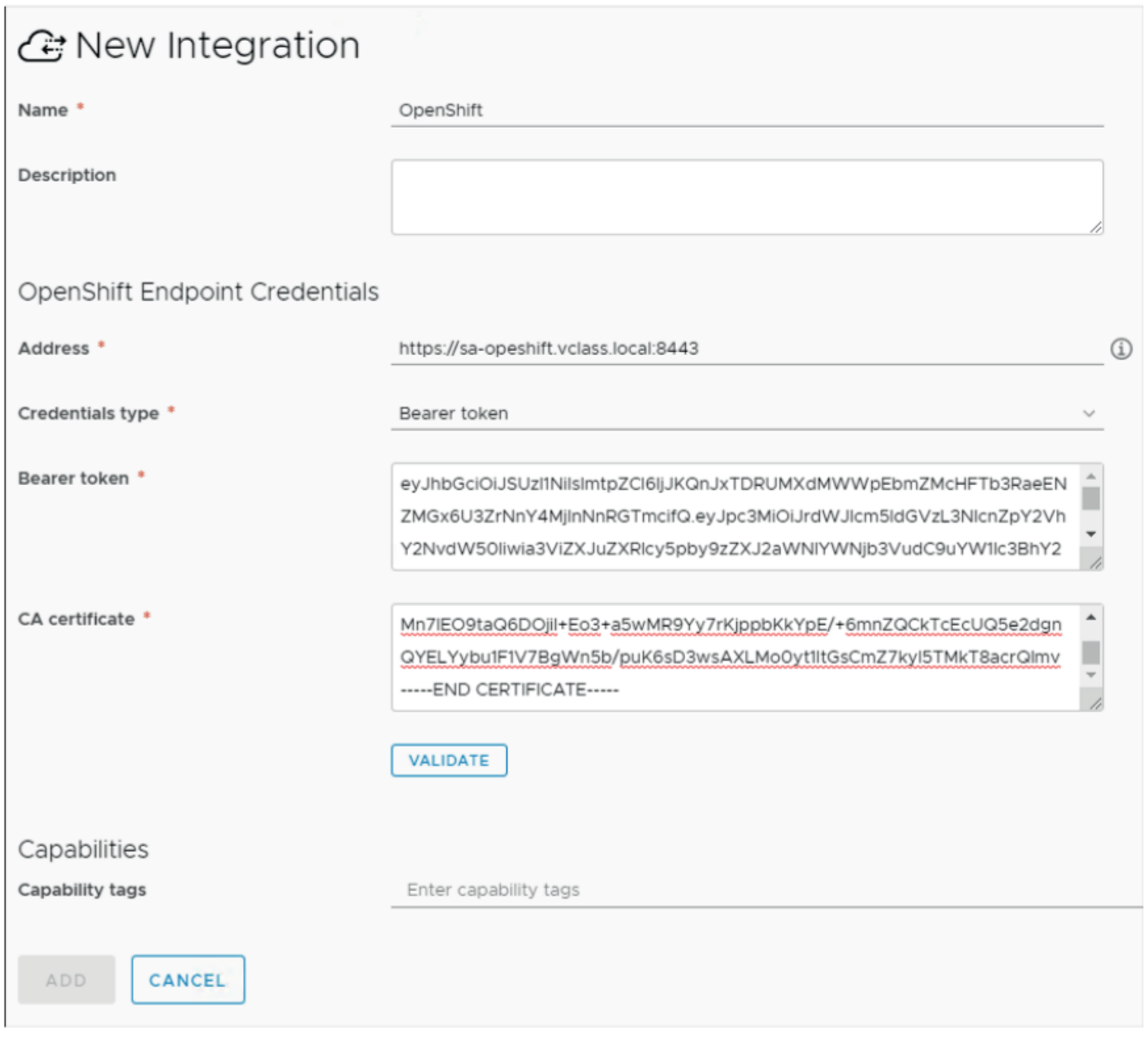
13-21 Integrating Red Hat OpenShift

Red Hat OpenShift is an enterprise Kubernetes application platform built on the Red Hat Enterprise Linux (RHEL) operating system.

To add an existing Red Hat OpenShift integration:

1. Click the **Infrastructure** tab.
2. In the left navigation pane, select **Connections** > **Integrations**.
3. Click **ADD INTEGRATION**.
4. Select **Red Hat OpenShift**.
5. Enter the name of the OpenShift integration.
6. Enter the address and location for the OpenShift server.

   If the OpenShift server is located on a private cloud, you must configure a cloud proxy to access it. Click **New Cloud Proxy**.
7. Select the appropriate credential type and enter the credentials.



For more information about the RedHat OpenShift integration, see "Cloud Assembly Now Supports Red Hat OpenShift Integration" at https://blogs.vmware.com/management/2019/11/ca-supports-os.html.

Create Kubernetes zones and associate them with a project. You can also configure Kubernetes namespaces.

13-22 Lab 34: Integrating an Existing Kubernetes Cluster with VMware Aria Automation

Integrate external Kubernetes with VMware Aria Automation:

1. Integrate the Kubernetes Cluster with VMware Aria Automation Assembler
2. Create a New Namespace Using VMware Aria Automation
3. Create an On-Demand Namespace Using VMware Aria Automation Templates
4. Delete Your Deployment to Save Lab Resources

13-23 Review of Learner Objectives

- List the various Kubernetes integration options available in VMware Aria Automation
- Describe vSphere with Tanzu components
- Explain how to integrate VMware Aria Automation with external Kubernetes
- Create a VMware Aria Automation template with Kubernetes components

13-24 Key Points

- VMware Aria Automation supports integration with multiple Kubernetes platforms.
- VMware Aria Automation can be integrated with vSphere with Tanzu for requesting on-demand supervisor namespaces.
- External Kubernetes clusters can be added to VMware Aria Automation to create and manage namespaces.
- Tanzu Kubernetes Grid Integrated Edition can be integrated to deploy an on-demand Kubernetes cluster by using a VMware Aria Automation template.

Questions?

Module 14

Introduction to VMware Aria Automation Config

14-2 Importance

VMware Aria Automation Config (formerly known as SaltStack Config) is a configuration management tool. VMware Aria Automation Config can manage the configurations of the deployed systems in an environment. You create reusable configuration templates called states and apply Salt states to the managed system to configure them. VMware Aria Automation Config uses beacons and reactors to monitor different activities on managed systems and then respond to them.

14-3 Lesson 1: Introduction to VMware Aria Automation Config

14-4 Learner Objectives

- Describe VMware Aria Automation Config, Salt minion, and Salt master
- Describe the VMware Aria Automation Config installation process
- Use VMware Aria Automation Config for configuration management
- Describe the Salt command structure and targeting criteria
- Describe grains, Salt states, pillars, beacons, and reactors

14-5 Introduction to VMware Aria Automation Config

VMware Aria Automation Config simplifies and automates common tasks and procedures that must be performed on a regular basis.

VMware Aria Automation Config is a configuration management system that defines the applications, files, and other settings that must exist on target systems.

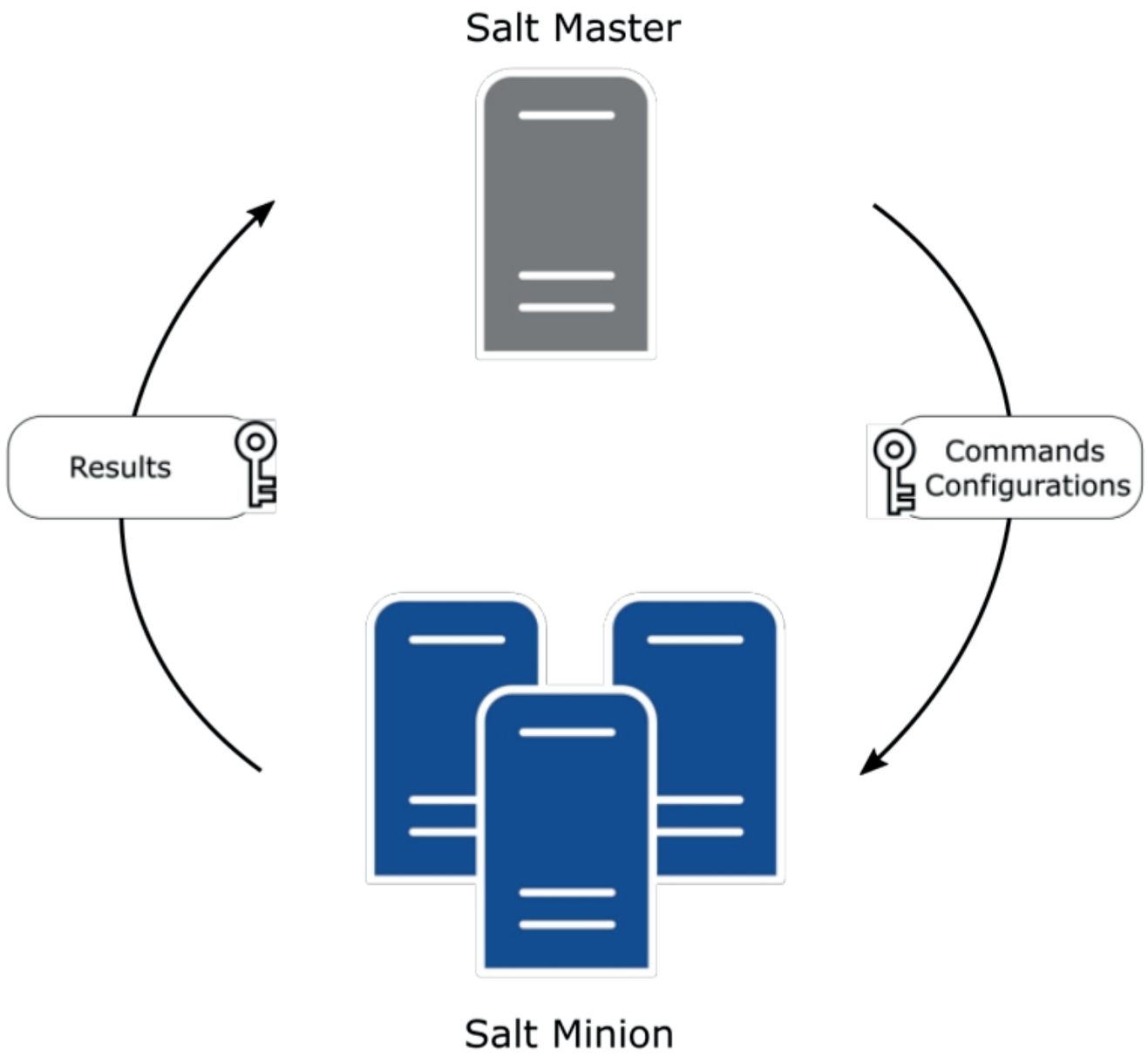
The target systems are evaluated against their respective defined configuration and necessary changes are made.

You can use VMware Aria Automation Config for data-driven orchestration, remote execution for any infrastructure, and configuration management for any application stack.

14-6 Salt Masters and Minions

VMware Aria Automation Config has the following classes of systems:

- Salt master: This central management system runs the Salt master service. The service sends commands and configurations to the Salt minions.
- Salt minion: The Salt master controls this management system. It runs the Salt minion service, which receives commands and configuration from the Salt master and runs them.



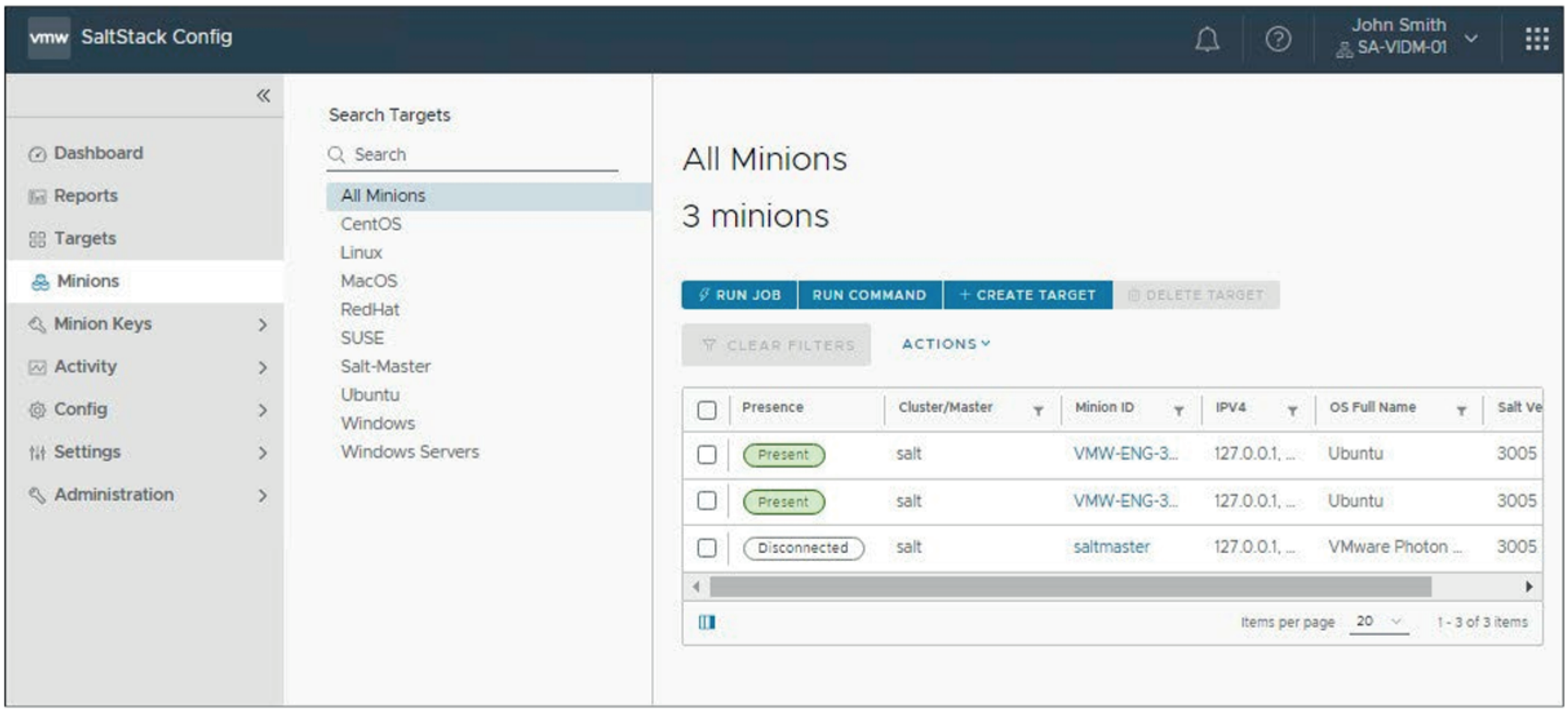
Salt uses a server-agent communication model. The server component is the Salt master, and the agent is the Salt minion.

The Salt master is responsible for providing commands to Salt minions, which run the tasks specified in the commands. The minions send the resulting data back to the Salt master. The Salt master aggregates and displays the results received from the Salt minions.

The Salt minions can also run agentless using salt-ssh.

14-7 About VMware Aria Automation Config

VMware Aria Automation Config provides an intuitive user interface to perform complex functions such as configuration management and orchestration.



With VMware Aria Automation Config, you can spend less time and fewer resources running routine functions.

VMware Aria Automation Config includes the following features:

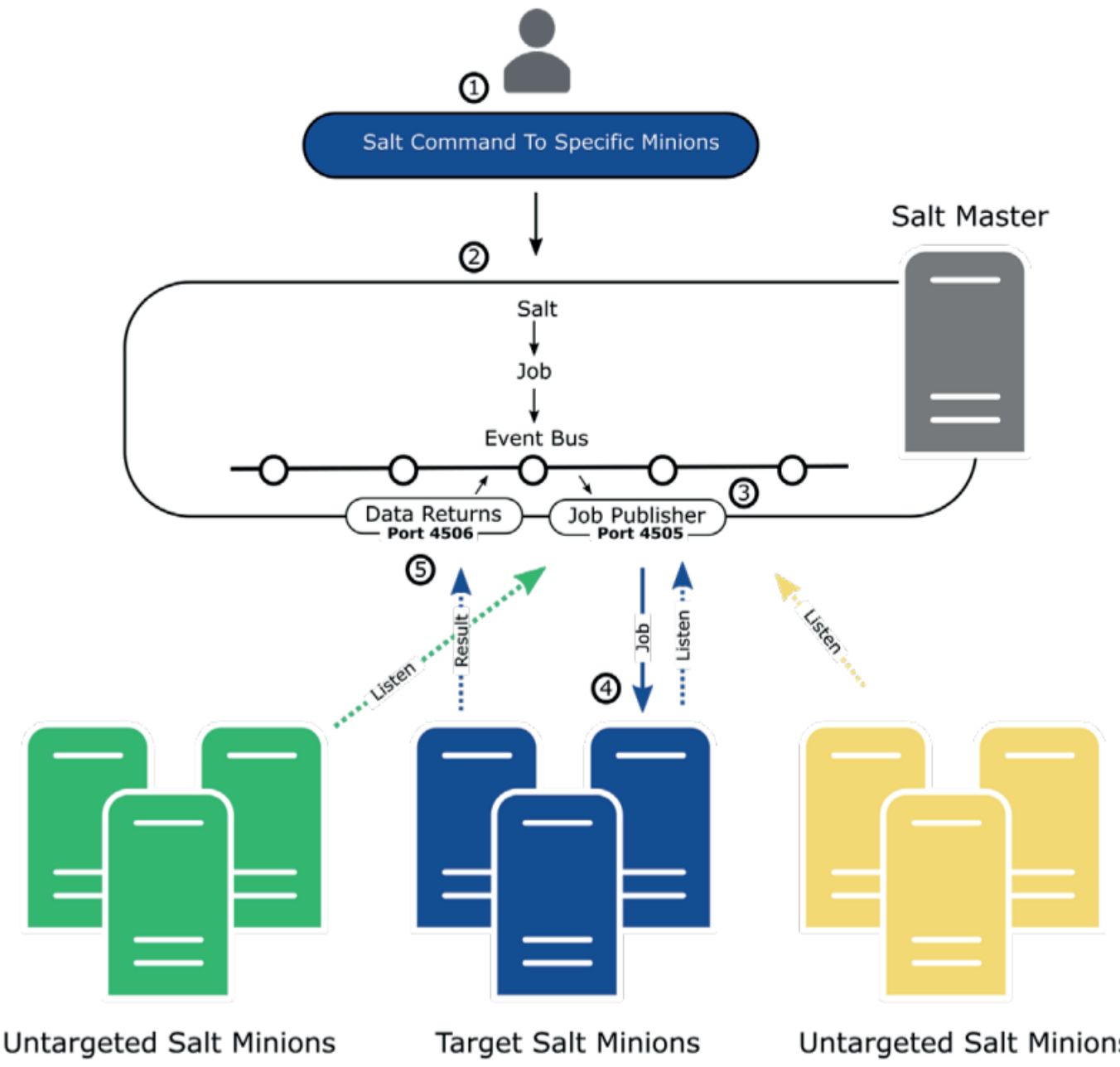
- Web-based user interface
- Role-based access control
- Multimaster support
- Central job and event cache
- Scheduling UI
- LDAP and Active Directory integration
- Reporting
- Enterprise API (eAPI)

14-8 Communication Between Salt Master and Salt Minion

The Salt master uses a publish-subscribe pattern to communicate with Salt minions.

The following ports are used:

- Port 4505: All Salt minions establish a persistent connection to this publisher port on which they listen for messages. Salt minions execute the message published if they are the targeted minions.
- Port 4506: Salt minions use this port to send job results to the Salt master and to securely request files and minion-specific data values from the Salt master.



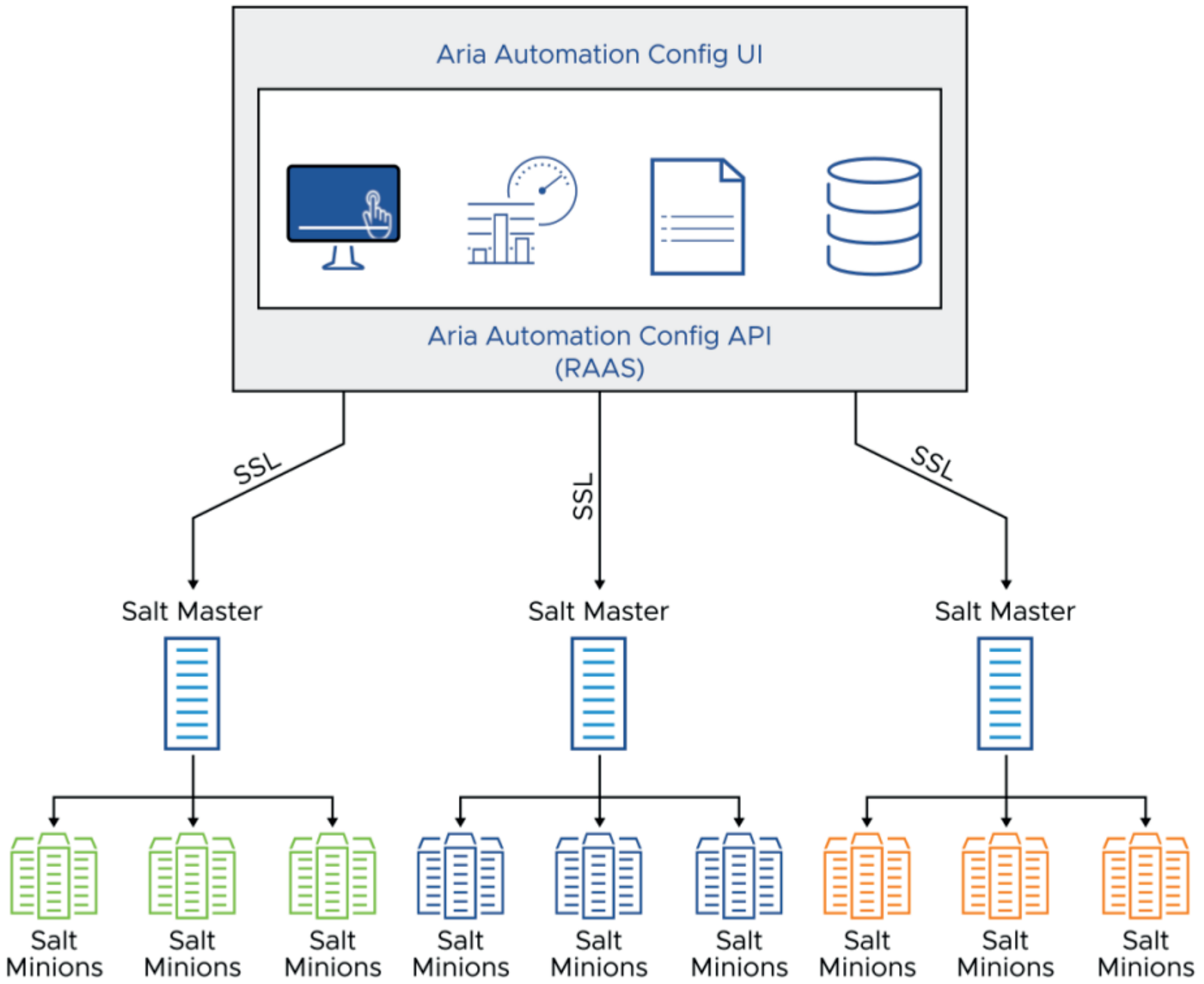
The following communication occurs:

1. A user runs a Salt command on the defined target Salt minions.
2. The Salt master takes this defined command and publishes it on port 4505.
3. Communication from the Salt master is a lightweight set of instructions with the following message: If a Salt minion with these properties exists, run the command with these arguments. All Salt minions receive commands simultaneously.

4. Salt minions determine whether they match the target properties when the command is received. If the Salt minion matches the target properties, it runs the command. Otherwise, it ignores the command.
5. The results from the targeted Salt minions are returned to the Salt master on port 4506.

14-9 Communication in VMware Aria Automation Config

When a job is executed in VMware Aria Automation Config user interface, this job passes through the VMware Aria Automation Config RAAS API toward the respective Salt master.

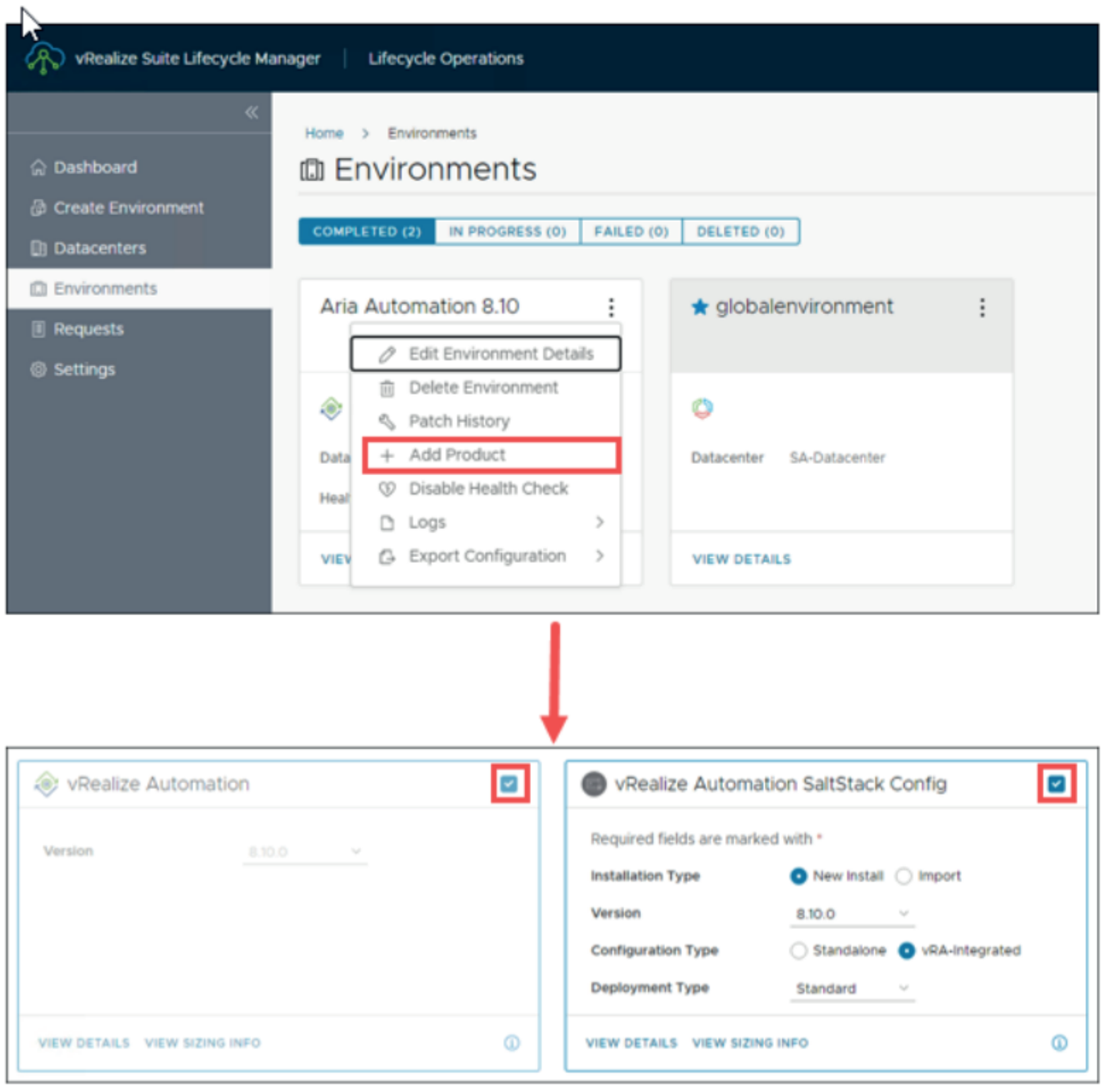


14-10 VMware Aria Automation Config Installation

You install VMware Aria Automation Config from VMware Aria Suite Lifecycle. Navigate to **Lifecycle Operations** > **Environments** and select **Add Product** in the VMware Aria Automation environment.

To install VMware Aria Automation Config, VMware Aria Automation must be installed in the environment.

VMware Aria Automation Config installation requires enabling multitenancy in VMware Aria Suite Lifecycle because VMware Aria Automation Config is integrated with a VMware Aria Automation tenant.



VMware Aria Automation Config appliance has the following minimum resource requirements:

- 8 CPUs
- 16 GB RAM
- 40 GB disk space

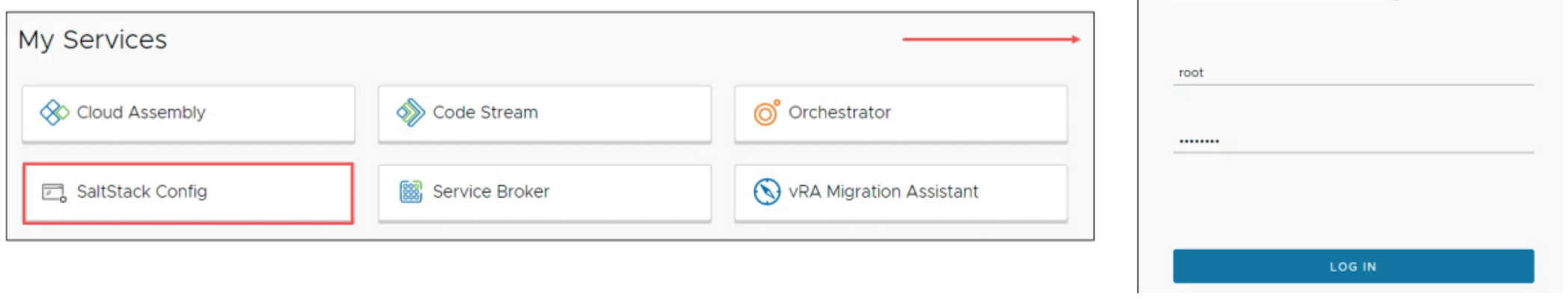
If the environment does not appear after the installation, run the following command:

```
echo -n | openssl s_client -connect sa-vra-01.vclass.local:443
-showcerts | tac | sed -ne '1,/-BEGIN CERTIFICATE-/p' | tac |
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' | tee -a
/etc/pki/tls/certs/ca-bundle.crt && sed -i.bak
'/ExecStart\=/iEnvironment=REQUESTS_CA_BUNDLE=/etc/pki/tls/cer
ts/ca-bundle.crt' /usr/lib/systemd/system/raas.service &&
systemctl daemon-reload && systemctl stop raas && rm
/var/log/raas/raas && systemctl start raas && echo -e
'Starting RaaS Service and tailing the log to see if errors
persist. \n Please Wait' && sleep 10 && echo -e 'Relaunch the
web browser and navigate to the vRASSC login page and monitor
this screen for further errors.\n CTRL+C to exit the tail' &&
tail -f /var/log/raas/raas
```

14-11 VMware Aria Automation Config Integration in VMware Aria Automation

After installing VMware Aria Automation Config, a new **SaltStack Config** service appears under My Services in the VMware Aria Automation Service Console of the tenant.

After clicking the **SaltStack Config** service, log in to VMware Aria Automation Config.



The vssc_ sa-vidm-01 integration is created in Aria Automation Assembler with VMware Aria Automation Config. The integration appears under **Infrastructure** > **Connections** > **Integrations**. Open the integration and set the running environment.

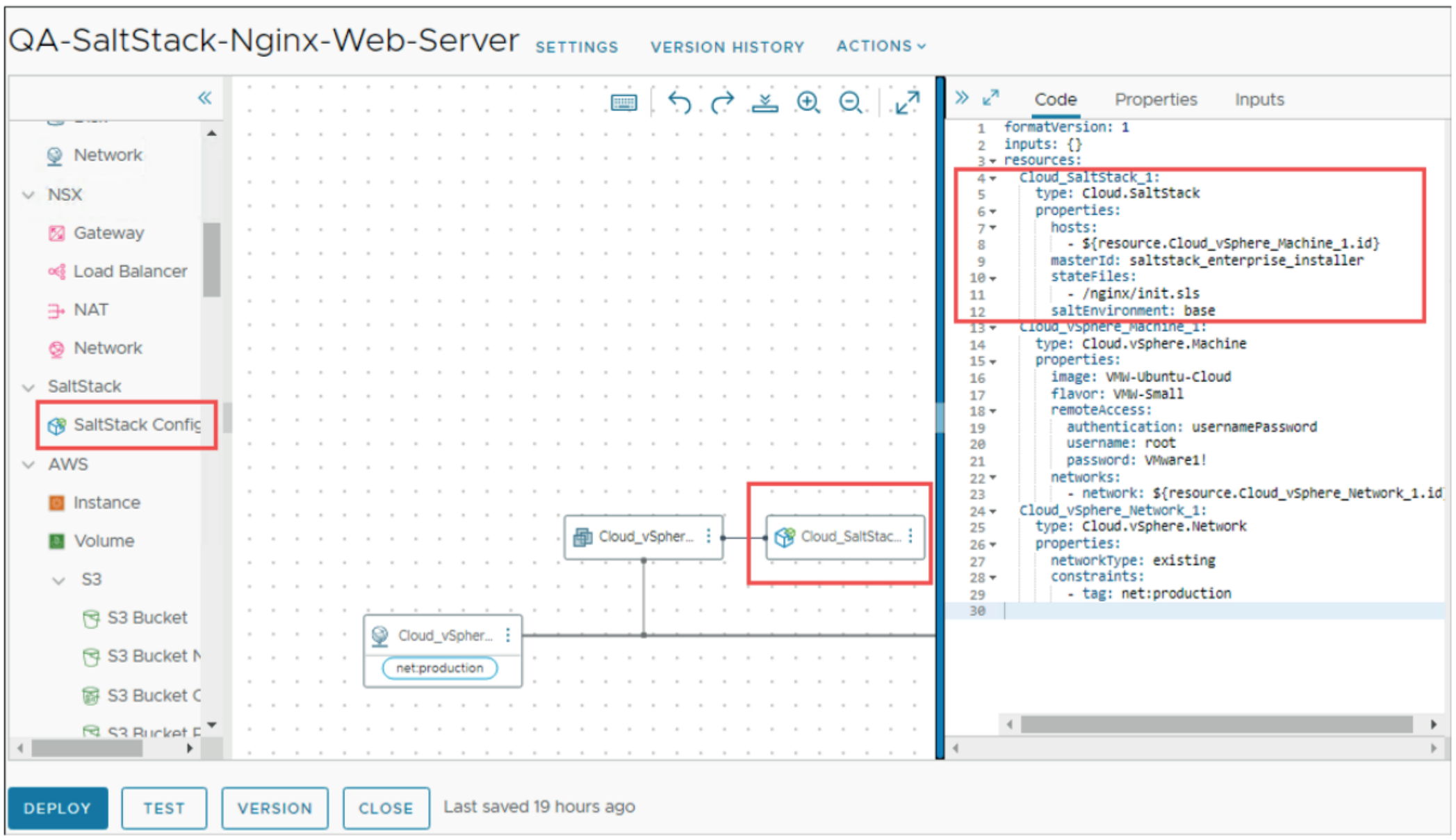
14-12 SaltStack Config Resource

SaltStack Config Resource adds properties to the YAML that installs the Salt minion when deploying the template.

The primary properties to be added are remote access details for the machine to be deployed and configuration properties for SaltStack Config Resource.

To use SaltStack Config Resource:

1. Go to Cloud Assemble and select **Design** > **Cloud Templates**.
2. Click any existing template or **Create New from Blank Canvas**.
3. Drag SaltStack Config Resource to the canvas.
4. Connect it to the machine that you want to deploy the minion and configure.



14-13 Salt Minion Installation

Install Salt minion on the managed systems.

Use cloudConfig in VMware Aria Automation to run the following commands on the Linux VMware Aria Templates deployments:

- `curl -L https://bootstrap.saltstack.com -o install_salt.sh`
- `sudo sh install_salt.sh -A <Salt_master_IP_address>`

VMware Aria Automation Config manages these deployments.

Code Properties Inputs

```
1  formatVersion: 1
2  inputs:
3    hostname1:
4      type: string
5      title: Enter your hostname
6      description: This wil be the internal DNS hostname of the machine
7    ipaddress:
8      type: string
9      title: Enter your IP address
10     description: This will be the IP address
11 resources:
12   Cloud_Machine_1:
13     type: Cloud.Machine
14     properties:
15       image: VMW-Ubuntu-Salt
16       flavor: VMW-Small
17       cloudConfig: |
18         runcmd:
19         - curl -L https://bootstrap.saltstack.com -o install_salt.sh
20         - sudo sh install_salt.sh -A 172.20.10.39
21       networks:
22         - network: '${resource.Cloud_Network_1.id}'
23   Cloud_Network_1:
24     type: Cloud.Network
25     properties:
26       networkType: existing
27       constraints:
28         - tag: 'net:production'
```

The `curl -L https://bootstrap.saltstack.com -o install_salt.sh` command downloads a script that is used to install Salt minion on the system.

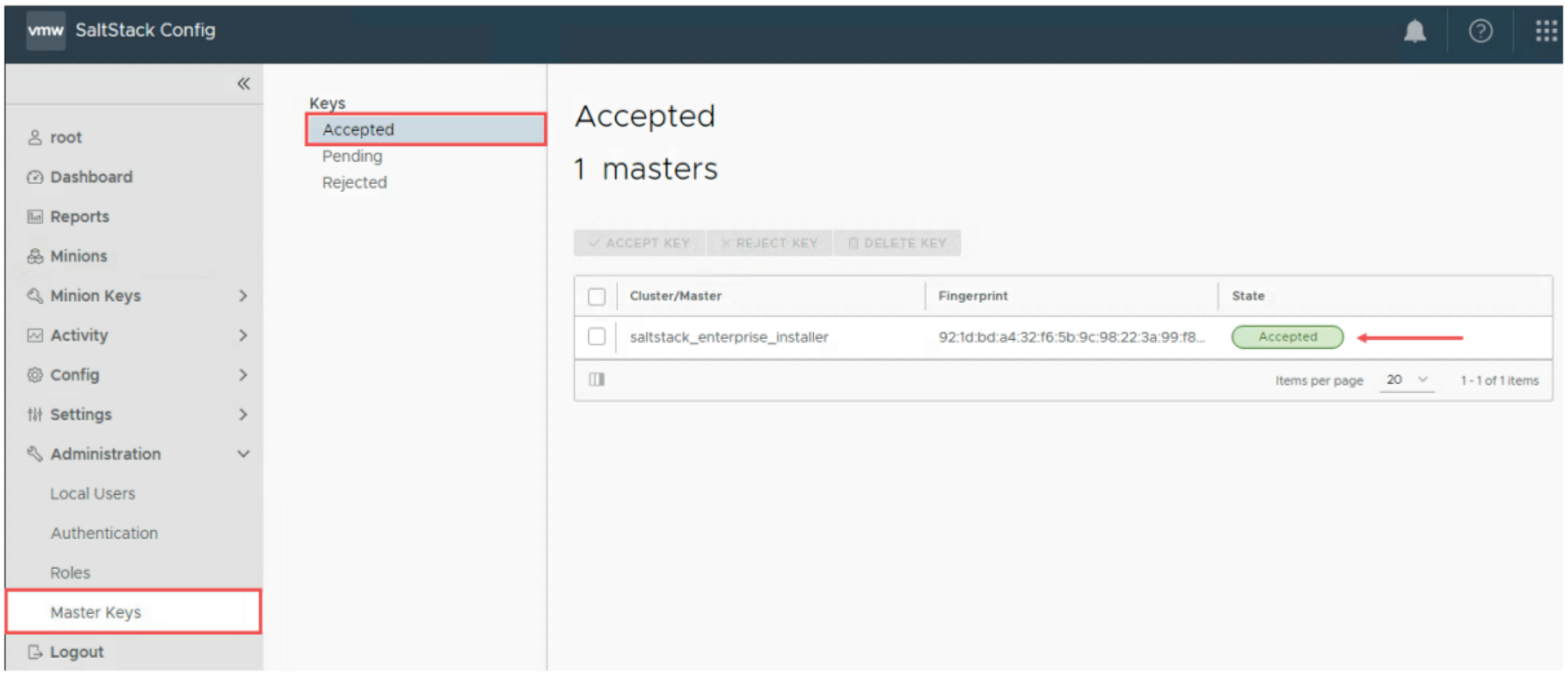
The `sudo sh install_salt.sh -A <Salt_master_IP_address>` command runs the script to install Salt minion on the system and specify the Salt master IP address, which is 172.20.10.39 in the screenshot.

VMware Aria Automation Config manages a minion with the saltmaster minion ID. VMware Aria Automation Config runs as Salt master and Salt minion simultaneously.

14-14 Salt Master Keys

The VMware Aria Automation Config appliance is also a Salt master and a Salt minion.

The master key is automatically accepted after the installation. To view the accepted master keys, select **Administration** > **Master Keys** > **Accepted**.



If a new Salt master is connected to VMware Aria Automation Config, accept its key from **Administration** > **Master Keys** > **Pending**. Select the key and click **ACCEPT KEY**.

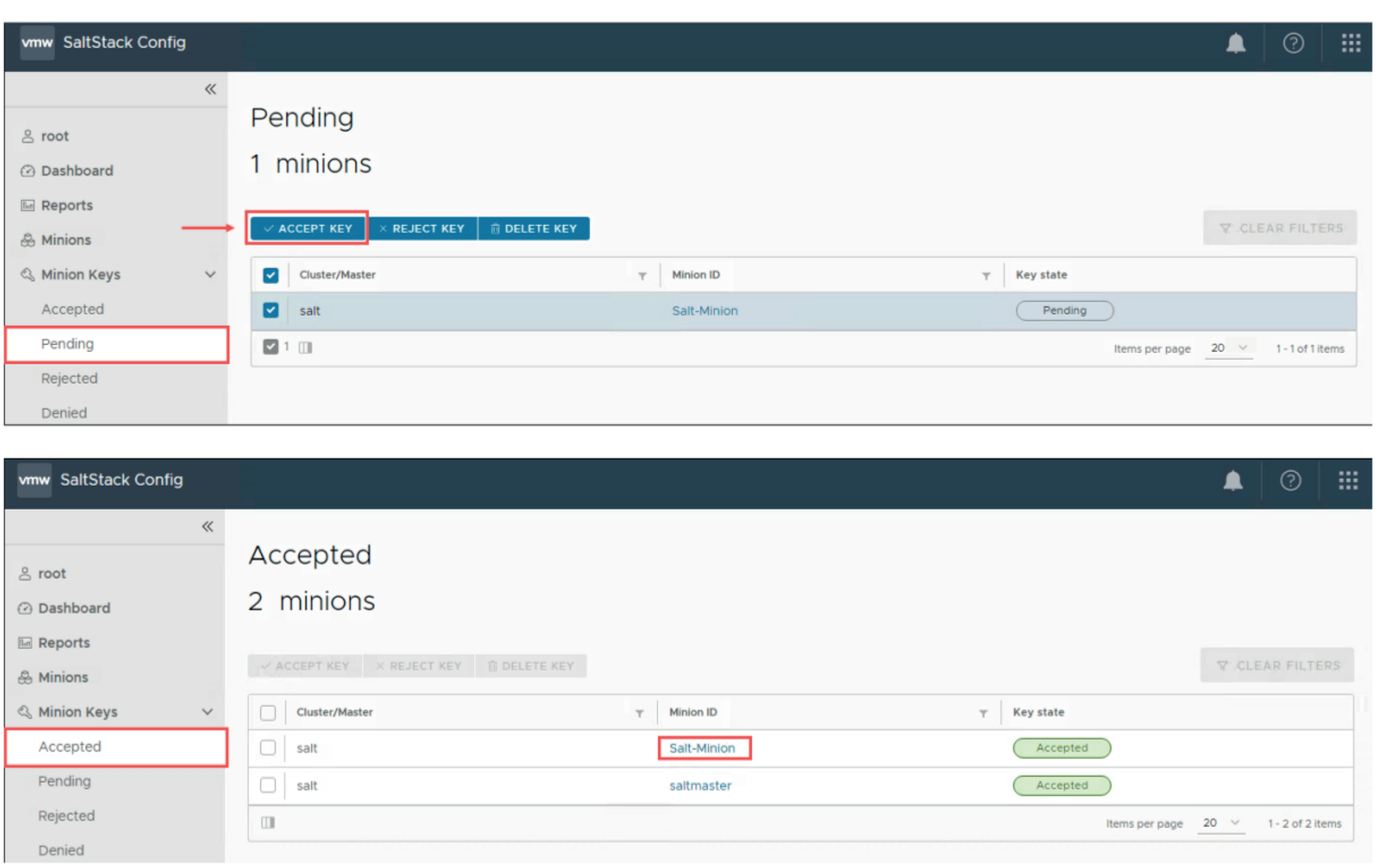
14-15 Accepting Minion Keys

If the Salt minion is deployed from a template using the SaltStack Config resource, the minion key is automatically accepted.

When the Salt minion starts for the first time, it sends its key to the Salt master.

The Salt master does not manage the Salt minion until the Salt minion's key is accepted.

To accept the Salt minion key, navigate to **Minion Keys** > **Pending**, select the key, and click **ACCEPT KEY**.



The Salt minion does not run any commands until its key is accepted.

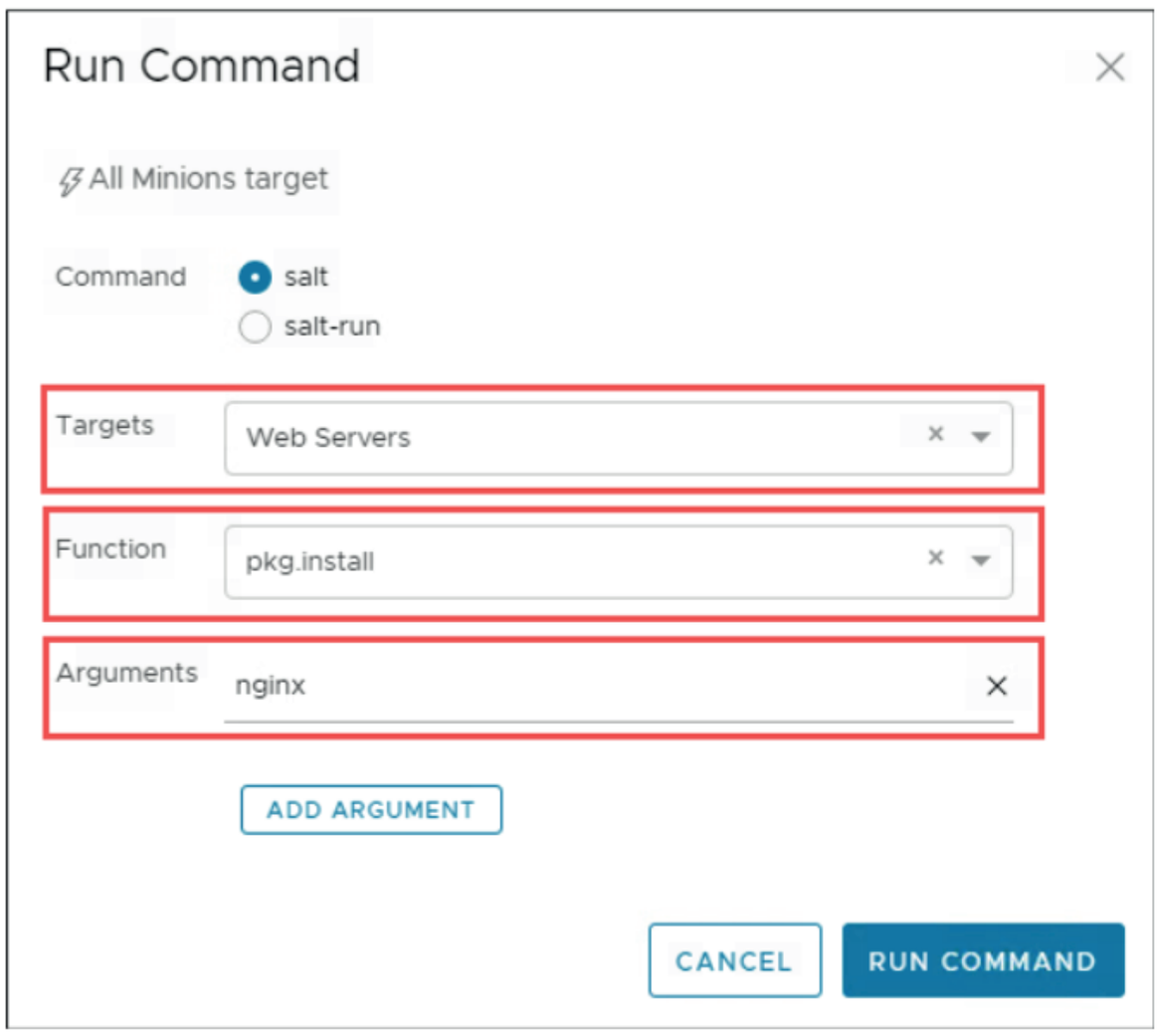
To check all accepted Salt minion keys, navigate to **Minion Keys** > **Accepted**.

14-16 Command Structure

Salt commands have a well-defined structure with the following main components:

- Target specification
- Module and function to call
- Function arguments

To run a command, navigate to **Minions** and click **RUN COMMAND**.



After installing VMware Aria Automation Config and accepting Salt minion keys, run the Salt commands.

All responses from the command runs are returned by the Salt minions so that command failures and successes are identifiable.

The following command types are available:

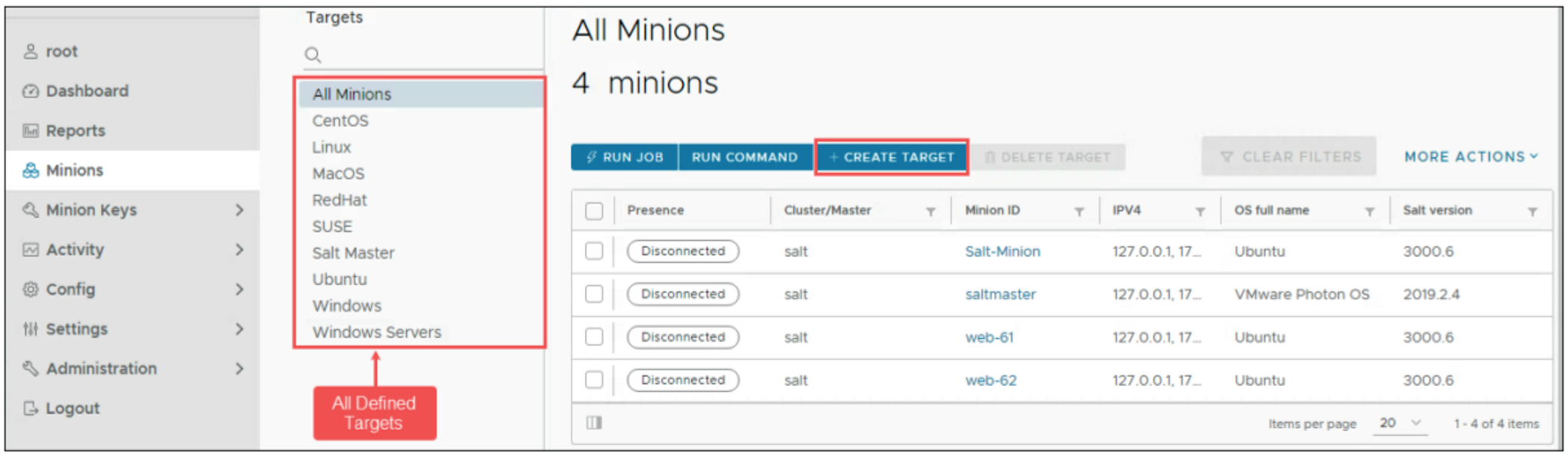
- salt: Runs one of a subset of available modules on the target Salt minions.
- salt-run: Runs one of a subset of available modules directly on the Salt master.

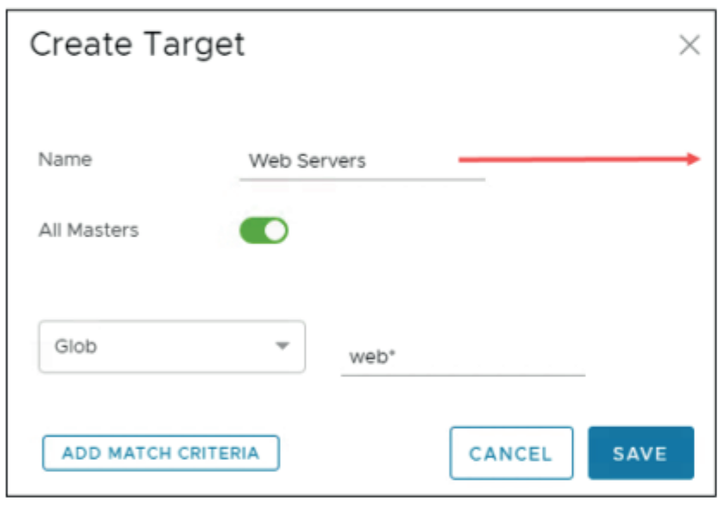
The screenshot shows a command that calls an install function with the nginx argument on the Web Servers as a target. After you run the command, all the Salt minions in the target Web Sever install the Nginx package.

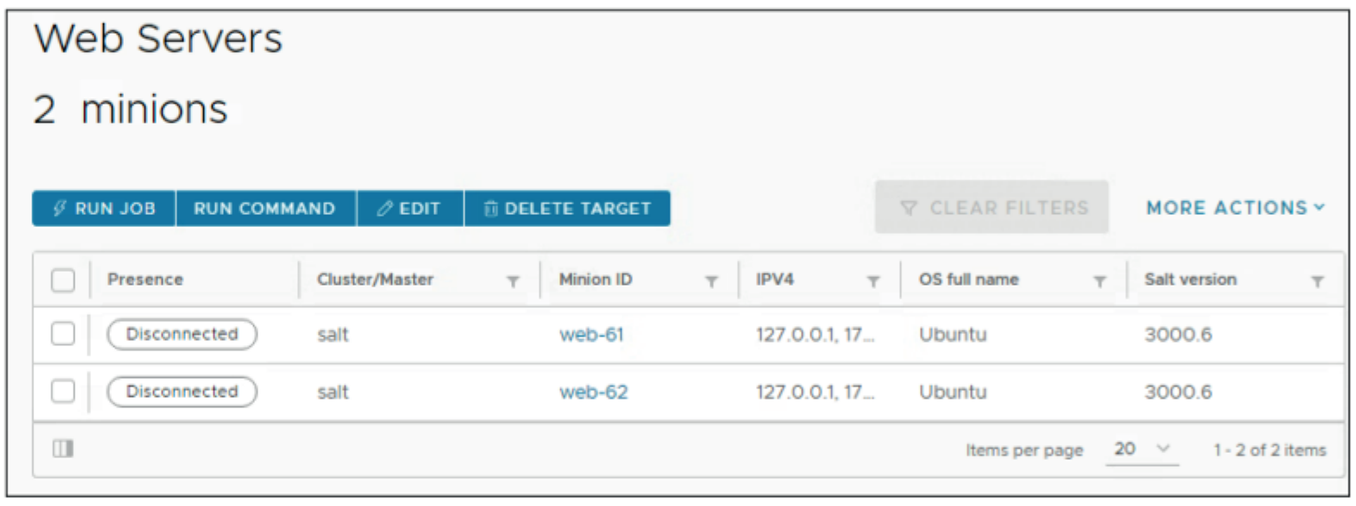
14-17 About Targeting

Use targeting to select the target Salt minions when running commands, apply configurations, and performing tasks in VMware Aria Automation Config that involve a Salt minion.

To create a target, navigate to **Minions** and click **CREATE TARGET**. You can then define the targeting criteria and click **SAVE.**







The following targeting methods are available:

- Grains: Collects static information from the Salt minions
- Glob: Matches one or more Salt minion IDs by using a wildcard matching
- List: Defines a list of Salt minion IDs
- Compound: Allows for many matchers to determine the target

  For more information about compound targeting, see the SaltStack website at https://docs.saltproject.io/en/latest/topics/targeting/compound.html.

The simplest way to target is using the Salt minion ID. By default, the minion ID is by default the minion host name.

The wildcard matching in Glob targeting can be as follows:

- Zero or more characters (*)
- Single character match (?)

- Range, for example, [1-5]
- List, for example, [1,2,4]

Predefined targets are available in VMware Aria Automation Config. These targets match the target by their operating systems.

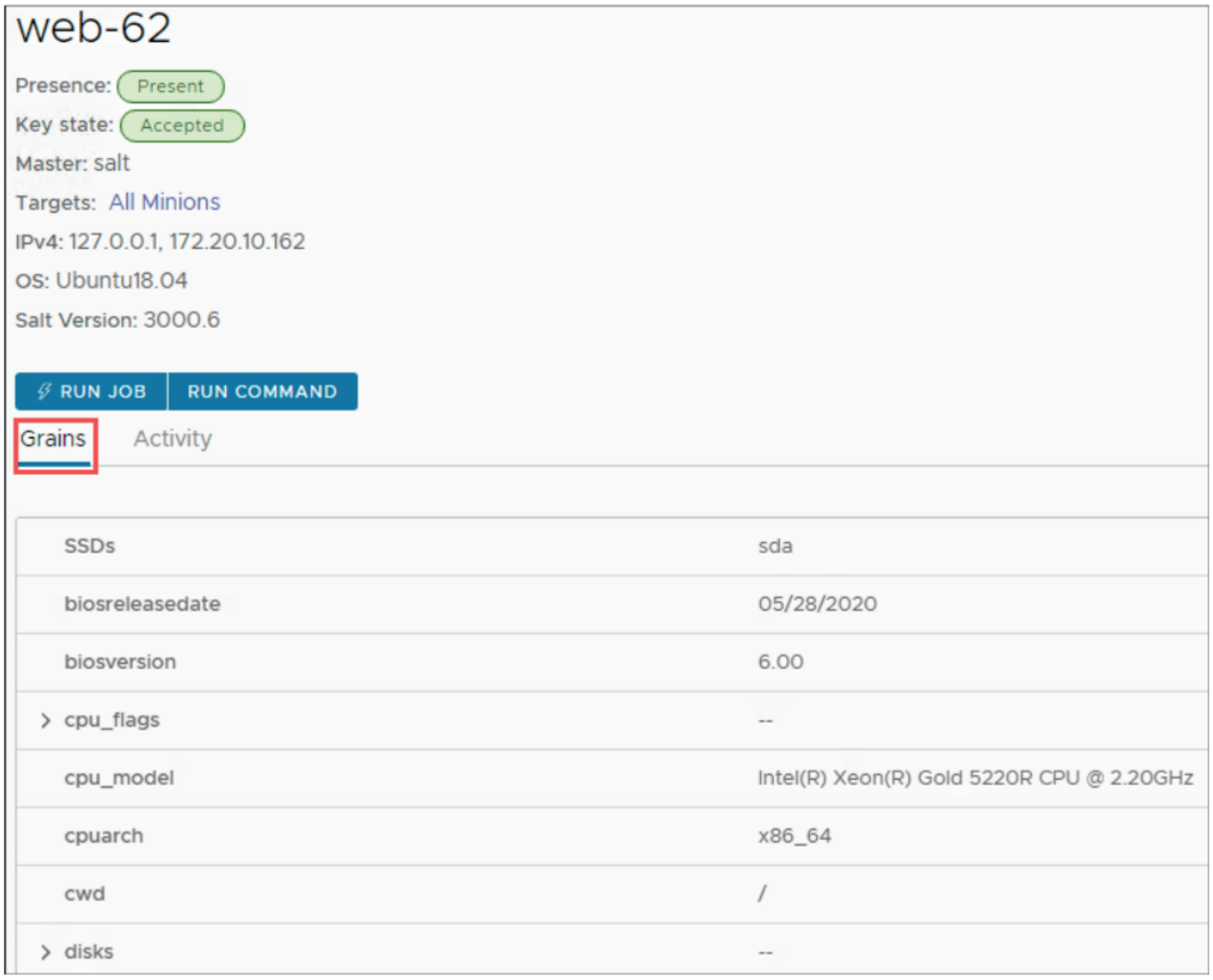
The screenshot shows the steps for creating a new target. Glob targeting is used. The Web Server target contains all the Salt minions whose minion ID starts with web.

14-18 About Grains

Grains are static pieces of information that SaltStack collects from Salt minions.

Grains consist of system properties, such as the operating system, domain name, IP address, kernel, OS type, memory, and so on.

To view the grains for a specific Salt minion, navigate to **Minions**, and click the Salt minion. All the grains collected for this Salt minion appear on the **Grains** tab.



Grains target Salt minions.

Add grains to a Salt minion. These grains are called custom grains.

For more information, see the SaltStack website at https://docs.saltproject.io/en/latest/topics/grains/index.html.

14-19 Salt Modules

A Salt module is a group of functions that manage an application (such as MySQL and Docker) or a system component (such as a disk and a file) or interact with an external system.

Running a Salt command calls a function in a module that performs a specific task.

Common modules include:

- pkg: Package management
- service: Managing services/daemons
- cp: File management
- user and group: Managing users and groups
- network: Network management
- cmd: Run a command

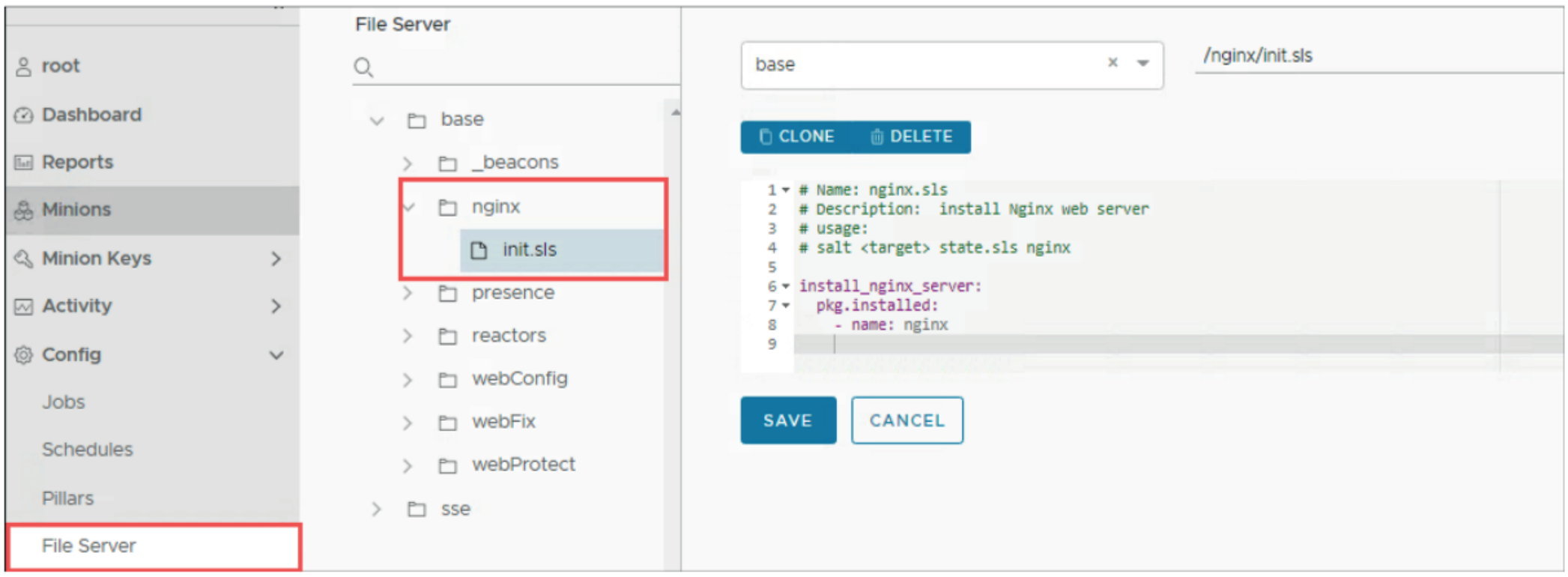
Modules are named in the salt.subsystem.module format. For more information about Salt modules, see the SaltStack website at https://docs.saltproject.io/en/latest/ref/index.html.

14-20 Salt States

VMware Aria Automation configuration management creates a reusable configuration template that describes the elements required to put a system component or application into a known configuration. This configuration template is the Salt state.

Create and save state files in File Server, which is under the **Config** tab.

The main use of the Salt file server is to present files for use in the Salt state system.



Salt uses the term state because the configuration management system defines the state for a system.

Salt states can restart services, copy entire directories, use variables, and so on.

Use the Salt file server for general file transfer from the Salt master to the Salt minions.

A state file is a file with an SLS extension that contains one or more state declarations. For example, the `init.sls` file in the `nginx` directory describes the nginx state in the screenshot.

Salt states are written in the YAML format.

The state in the screenshot calls the function installed in the `pkg` module to install nginx on the target minions.

Commands in state files are run by default from top to bottom.

14-21 About Pillars

You can store sensitive data specific to each Salt minion can be stored in pillars.

Information transferred through a pillar is presented only to the Salt minions that are targeted.

Pillar data is compiled using targeting to determine the data that is sent to each minion.

For more information about pillars, see the SaltStack website at https://docs.saltproject.io/en/latest/topics/tutorials/pillar.html.

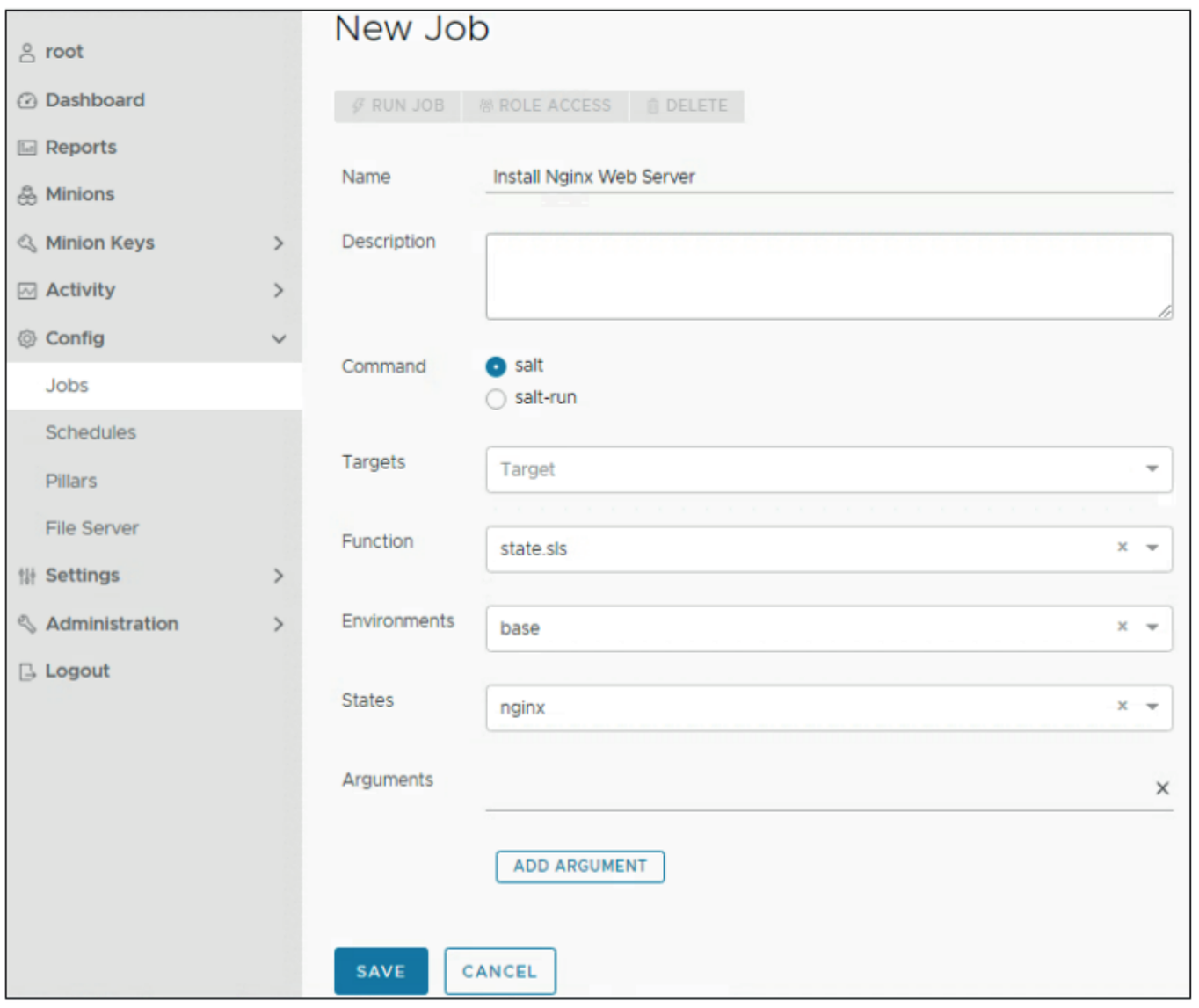
14-22 About Jobs

Jobs run salt commands or apply salt states to the target Salt minions.

The following items are defined when creating a job:

- Name
- Command
- Target
- Function
- Argument

To create a job, select **Config** > **Jobs** in the navigation pane and click **CREATE JOB**.



The screenshot shows the Install Nginx Web Server job. This job runs the `state.sls` function, which applies a defined Salt state on the target Salt minions. The Salt state defined in this job is the nginx state.

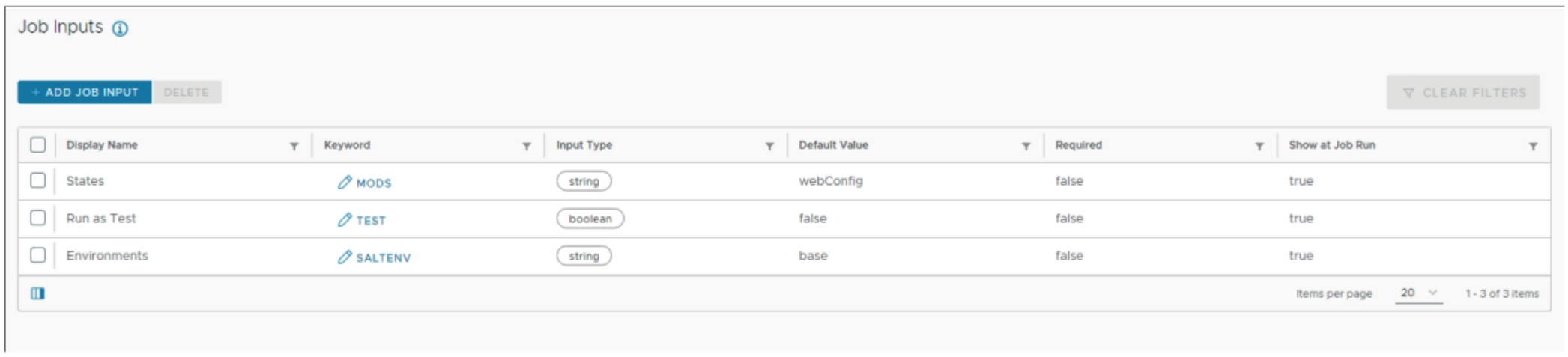
You can define targets directly in the job or leave the option blank and select targets when you run the job.

Environment is a state tree directory containing a set of state files to configure systems. Base is the default environment in SaltStack.

14-23 VMware Aria Automation Config Job Inputs

VMware Aria Automation Config job inputs provide the following features:

- Adds inputs and input types to a job
- Defines static input values or allows users to manipulate values during a job run
- Provides more flexibility about how jobs are configured when they are executed



To access job inputs, select **Config** > **Jobs** in VMware Aria Automation Config.

Administrators can create detailed and custom jobs and then allow users with different skill sets to run jobs against the infrastructure.

Administrators can use job inputs to configure the mandatory and optional job inputs that users can input during runtime. This process helps reduce the number of job creation requests.

14-24 About Beacons

Beacons enable the Salt minion to monitor and raise events for processes that are not related to Salt.

The beacon system allows the Salt minion to connect to system processes and continually monitor these processes.

When the monitored activity occurs in a system process, an event is sent on the Salt event bus.

```
#Beacon to watch for the index.html file modifications
beacons:
  inotify:
    - files:
        /var/www/demo/index.html:
          mask:
            - modify
    - disable_during_state_run: True
```

Salt beacons can monitor many system activities:

- File system changes
- Service status
- Shell activity, such as user logins
- Network and disk usage

Beacons configurations are enabled by placing a `beacons:` top-level block in the `/etc/salt/minion` file or any file in `/etc/salt/minion.d/`, for example, `/etc/salt/minion.d/beacons.conf`.

The screenshot shows a `beacons.conf` file. This configuration defines a beacon that triggers an event on the Salt event bus if the `/var/www/demo/index.html` file is modified on the Salt minion.

14-25 About Reactors

Reactors enable the Salt master to trigger actions in response to any event.

Reactors watch the event bus for event tags that match a given pattern and run one or more commands in response.

```
#Reactor file which contains all the reaction to any beacon

reactor:
  - 'salt/beacon/*/inotify//var/www/demo/index.html':
    - salt://reactors/applyFix.sls
```

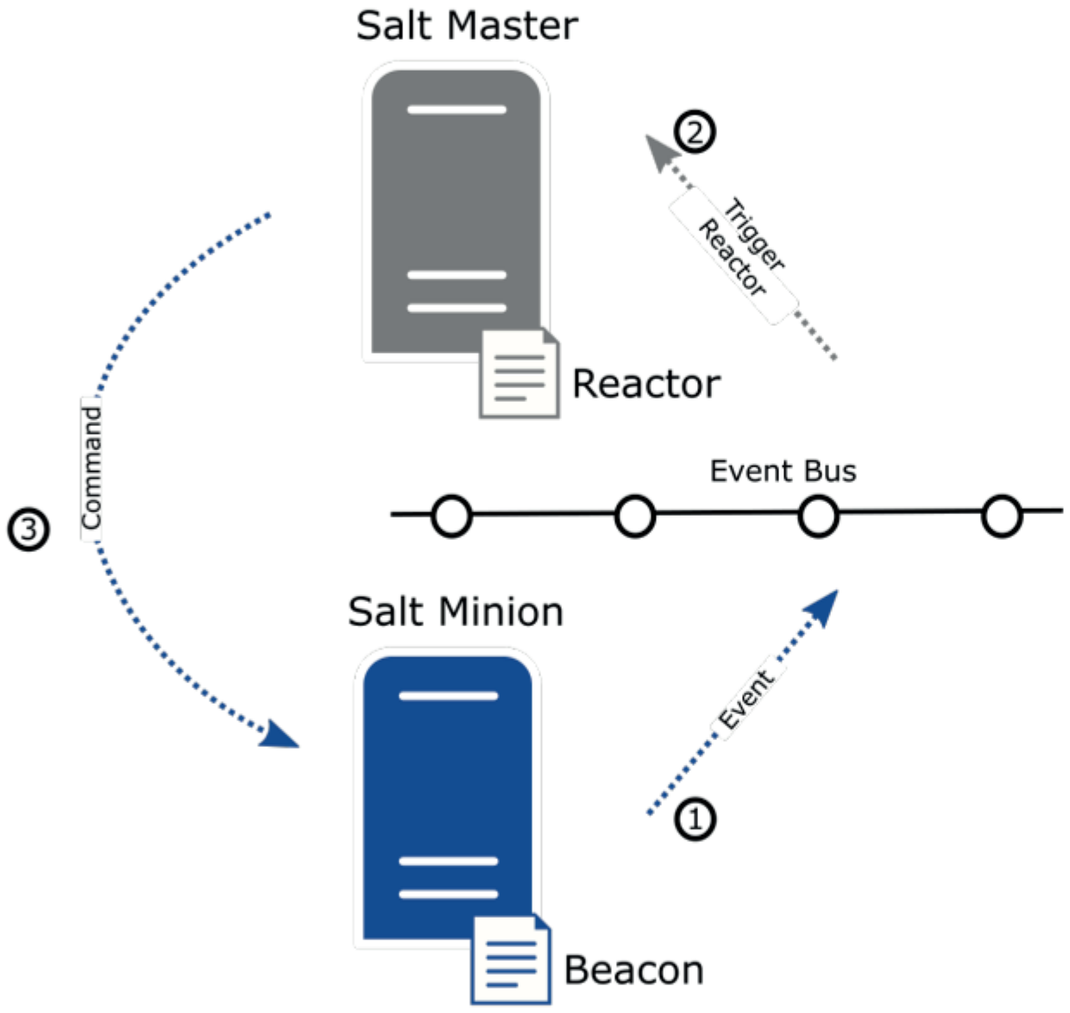
Reactor configurations are enabled by placing a `reactor:` top-level block in `/etc/salt/master` file or defining it in a separate `reactor.conf` file in the `/etc/salt/master.d/` directory.

The screenshot shows a `reactor.conf` file. This configuration defines a reactor that runs the `applyFix.sls` state file when the event tag matches `salt/beacon/*/inotify//var/www/demo/index.html`. A Salt beacon triggers the event with this tag.

14-26 Reacting to Events with Beacons and Reactors

Beacons and reactors work together to provide orchestration:

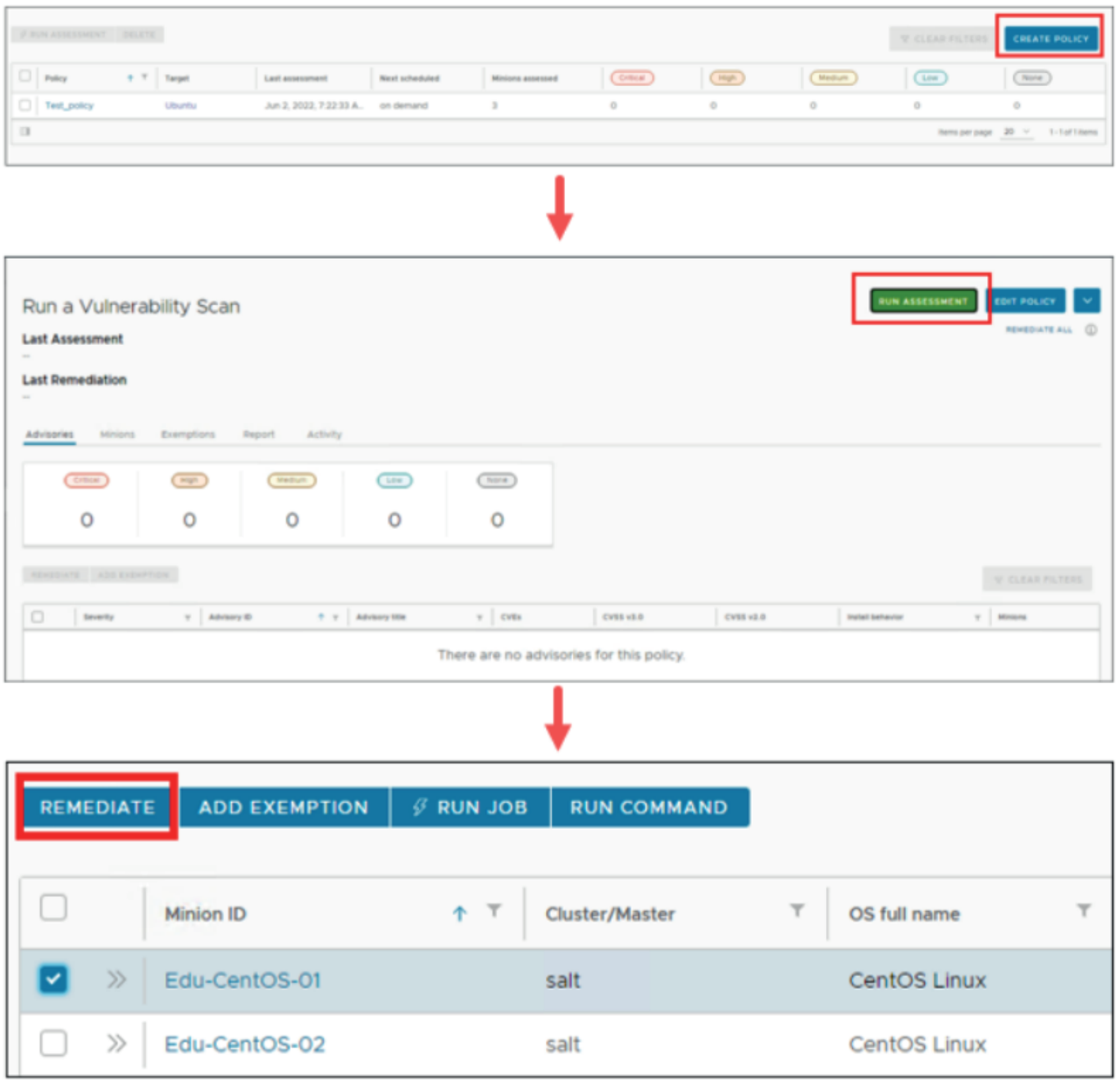
1. Beacons monitor activities. When the monitored activity occurs, they trigger events.
2. The triggered events fire the respective reactors.
3. Reactors respond to the triggered events by sending commands and states for the Salt minions to apply.



14-27 Remediations with VMware Aria Automation Config for Secure Hosts

VMware Aria Automation Config for Secure Hosts (formerly known as VMware vRealize Automation SaltStack SecOps) offers automated compliance and vulnerability detection and remediation for your environment assets:

- VMware Aria Automation Config for Secure Hosts can define a policy that targets minions for an assessment.
- Following an assessment, VMware Aria Automation Config for Secure Hosts can either remediate specific advisories, checks, or remediate all of them at once.



The UI shows how to remediate vulnerabilities on the **Vulnerability** tab. You can perform similar operations on the **Compliance** tab in VMware Aria Automation Config to remediate checks.

14-28 Lab 35: Using VMware Aria Automation Config to Build a Web Server

Use VMware Aria Automation Config to configure a Salt minion:

1. Set the Running Environment
2. Create a VMware Aria Automation Template to Deploy a Salt Minion and Install Nginx
3. Verify the Deployment

14-29 Lab 36: Using VMware Aria Automation Config to Restore a Hacked Web Server

Use VMware Aria Automation Config to orchestrate jobs:

1. Hack the Web Server from VMware Aria Automation Config
2. Restore the Web Server from VMware Aria Automation Config
3. Send the Beacon Configuration File to a New Salt Minion
4. Test the VMware Aria Automation Config Web Server Fix Orchestration
5. Delete Your Deployment to Save Lab Resources

14-30 Review of Learner Objectives

- Describe VMware Aria Automation Config, Salt minion, and Salt master
- Describe the VMware Aria Automation Config installation process
- Use VMware Aria Automation Config for configuration management
- Describe the Salt command structure and targeting criteria
- Describe grains, Salt states, pillars, beacons, and reactors

14-31 Key Points

- VMware Aria Automation Config manages systems configuration in an uncomplicated way.
- Use VMware Aria Suite Lifecycle to install VMware Aria Automation Config.
- VMware Aria Automation Config provides orchestration to different activities through beacons and reactors.

Questions?

Module 15

Troubleshooting and Integration with VMware Aria Suite

15-2 Importance

To monitor and troubleshoot the many components of VMware Aria Automation, you must understand CLI functions and logs. You can also access additional features and capabilities by integrating VMware Aria Suite products. Integration with VMware Aria Suite products provides more features and capabilities.

15-3 Module Lessons

1. Troubleshooting VMware Aria Automation
2. VMware Aria Suite Integration

15-4 Lesson 1: Troubleshooting VMware Aria Automation

15-5 Learner Objectives

- Demonstrate how to monitor and troubleshoot VMware Aria Automation with CLI commands
- Explain how to collect a log bundle
- Identify the key logs location
- Describe the process of monitoring requests in the UI

15-6 Overview of the CLI

The CLI is a text-based function of VMware Aria Automation. The CLI includes Kubernetes and VMware Aria Automation commands.

You can run the following command sets:

- `vracli`: Used for administering and troubleshooting the VMware Aria Automation appliance infrastructure.

  The custom-built `vracli` command set is used for initial configuration, cluster management, databases, certificates, log bundle generation, and other such actions.

- `kubectl`: Used to manage Kubernetes services, pods, and container-level functions in the environment

  The `kubectl` command is the primary command set used after installation.

15-7 Useful vracli Commands

The `vracli` set includes different commands to monitor, configure, and gather information about the VMware Aria Automation infrastructure.

Command	Usage
`vracli status deploy`	Confirms that the deployment is successful
`vracli status`	Gives an overview of the entire VMware Aria Automation cluster infrastructure and database
`vracli service status`	Shows detailed information about each service and its memory and disk usage
`vracli vidm`	Displays or changes the Workspace ONE Access configuration
`vracli vrli`	Checks the existing configuration of VMware Aria Operations for Logs
`vracli log-bundle`	Creates a log bundle in the current working directory
`vracli proxy set --<hostname>`	Configures an internet proxy server
`vracli proxy show`	Shows the proxy configuration

You run the `vracli -h` or `vracli` commands to access the help menu.

The help menu provides information about all commands that can be used in this command set.

For easier access, all commands can be autocompleted by pressing the Tab key.

15-8 Useful kubectl Commands

The `kubectl` command set is the primary means of managing Kubernetes services and pods.

Command	Usage
`kubectl get namespaces`	Shows all the available namespaces
`kubectl get pods -n <namespace>`	Gives information about the pods in a given namespace
`kubectl get services -n <namespace>`	Gives information about the services in a given namespace
`kubectl describe pod <pod name> -n <namespace>`	Gives a detailed breakdown of startup parameters and processes of an individual pod
`kubectl logs <pod name> -n <namespace>`	Checks the logs for a specific service pod in a given namespace

You run the `kubectl -h` or `kubectl` commands to access the help menu.

Replace `-n <namespace>` with `-A` to view the items in all namespaces.

15-9 Restarting Services

If a particular service fails, restarting the service can resolve the issue.

To restart a service, you delete and redeploy the service by running the `kubectl delete pods -n <namespace> <pod name>` command.

```
tenant-management-ui-app-86748d6fd-dvncw        1/1     Running   0          32d
terraform-service-app-78fc6d9bdb-29j9f          2/2     Running   6          32d
user-profile-service-app-59b4cd54d7-gpsfq       1/1     Running   7          32d
vco-app-575db9d9cb-29bkb                        3/3     Running   0          15m
root@sa-vra-01 [ ~ ]# kubectl delete pods -n prelude vco-app-575db9d9cb-29bkb
pod "vco-app-575db9d9cb-29bkb" deleted
```



```
tenant-management-ui-app-86748d6fd-dvncw        1/1     Running   0          32d
terraform-service-app-78fc6d9bdb-29j9f          2/2     Running   6          32d
user-profile-service-app-59b4cd54d7-gpsfq       1/1     Running   7          32d
vco-app-575db9d9cb-9k6k9                        0/3     Init:1/2  0          50s
```

The `kubectl delete` command does not require a full system restart and can fix most services.

The screenshot shows the process of restarting the vco-app service in the prelude namespace.

To query running services pods and their statuses in the prelude namespace, run the `kubectl get pods -n prelude -w` command. Adding `-w` to the end of the command follows changes in the environment similar to a tailing log.

Running the `kubectl describe <pod name> -n <namespace>` command warns about service dependencies if another service is required to operate.

15-10 About the deploy.sh Script

Running the `/opt/scripts/deploy.sh` script forces all the services to rebuild.

The `deploy.sh` script retrieves all images from the helm registry and redeploys the VMware Aria Automation services based on the configuration files.

The information in the PostgreSQL database remains intact, and the service pods are reconfigured.

You must run the `/opt/scripts/deploy.sh --onlyClean` script before running the `deploy.sh` script.

```
root@lab-vra-01 [ ~ ]# /opt/scripts/deploy.sh --onlyClean
+ trap on_exit EXIT
+ export -f wait_deploy_health
+ log_stage 'Waiting for deploy healthcheck'
+ set +x

========================
[2022-10-26 09:02:36.849+0000] Waiting for deploy healthcheck
========================

root@lab-vra-01 [ ~ ]# /opt/scripts/deploy.sh
+ trap on_exit EXIT
+ export -f wait_deploy_health
+ log_stage 'Waiting for deploy healthcheck'
+ set +x

========================
[2022-10-26 09:05:43.486+0000] Waiting for deploy healthcheck
========================

+ timeout 300s bash -c wait_deploy_health
Running check eth0-ip

Running check non-default-hostname

Running check node-name

Running check single-aptr

Running check nodes-ready

Running check nodes-count

Running check fips

+ source /opt/scripts/helm_utils.sh


Prelude has been deployed successfully

root@lab-vra-01 [ ~ ]#
```

Using snapshots or creating a backup with an online VMware Aria Automation system causes issues because the database is not stored locally and data can be lost as a result.

To stop the services cleanly, run the `/opt/scripts/deploy.sh --onlyClean` script before taking a backup or a snapshot of the VMware Aria Automation appliance. You then run the `/opt/scripts/deploy.sh` script after the operation finishes to ensure services health and data integrity.

To shut down the VMware Aria Automation services on all cluster nodes, you run the `/opt/scripts/deploy.sh --shutdown` command.

15-11 Collecting Log Bundles

Collect the complete VMware Aria Automation environment logs as one bundle.

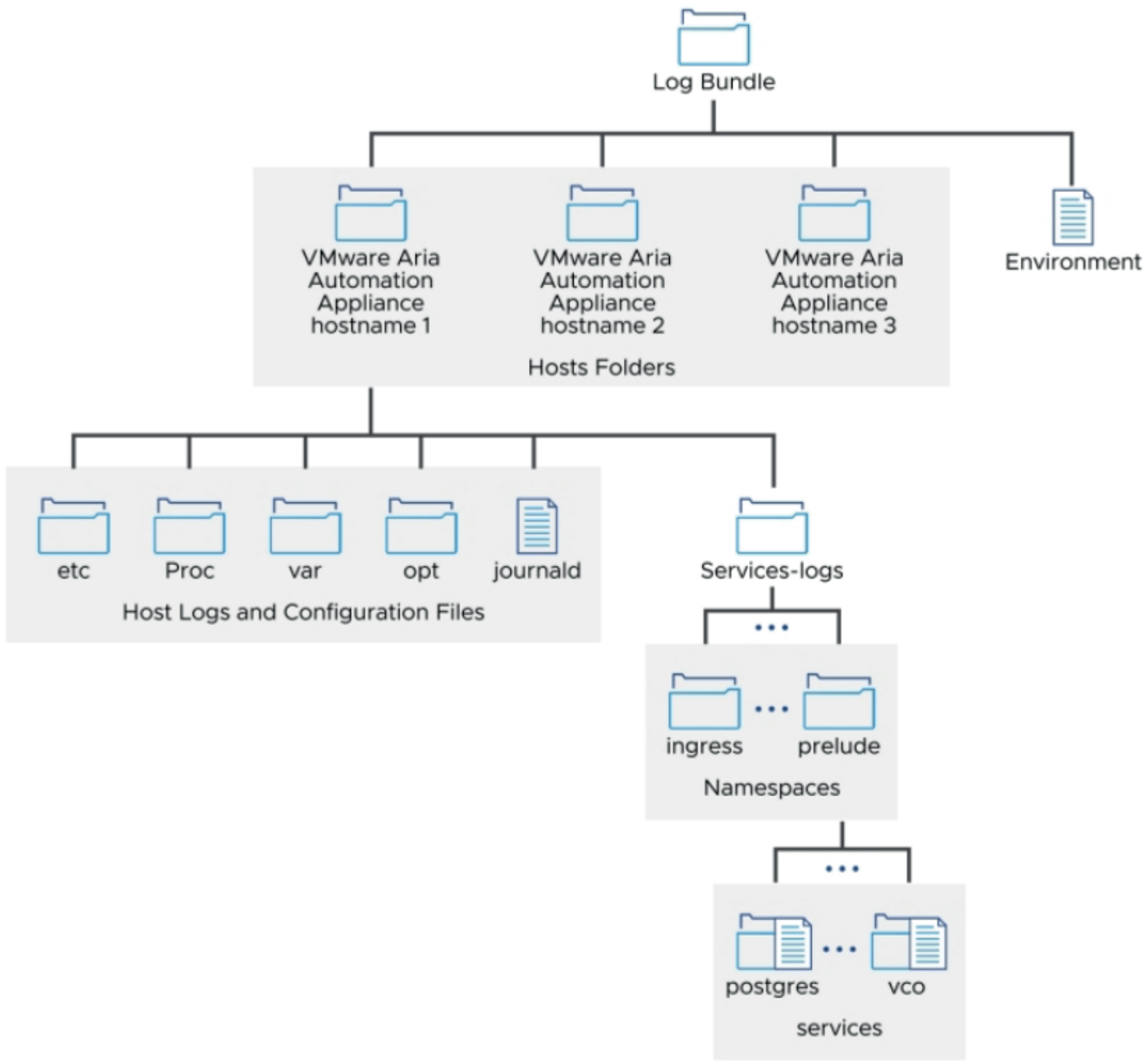
To create a log bundle, use SSH to connect to the VMware Aria Automation appliance and run the `vracli log-bundle` command.

In a clustered deployment, running the `vracli log-bundle` command on one node pulls logs from all nodes in the environment.

```
root@lab-vra-01 [ ~ ]# vracli log-bundle
2022-10-26 09:27:16,101 [INFO] Use temporary directory /home/root/.log-bundle-20221026T092716lxiz9dwc
2022-10-26 09:27:16,102 [INFO] Generation of log bundle /home/root/log-bundle-20221026T092716.tar started
2022-10-26 09:27:16,126 [INFO] Getting endpoints for log collection
2022-10-26 09:27:16,151 [INFO] Log collection endpoints are [command-executor-166k4]
2022-10-26 09:27:16,152 [INFO] Building bundle contents for local node
2022-10-26 09:27:17,642 [INFO] Collecting node logs from local node...
2022-10-26 09:27:17,657 [INFO] Collecting an environment file...
2022-10-26 09:27:19,305 [WARNING] Subprocess completed with warnings on local node. Exit code: [0]. Stderr: [Some of the f
ar: /services-logs/metrics/system/file-logs/current.bin: file changed as we read it
]
]
2022-10-26 09:27:24,376 [INFO] Assembling log bundle...
2022-10-26 09:27:25,466 [INFO] Assembly of log-bundle-20221026T092716.tar completed successfully.
CompletedProcess(args=['/usr/bin/bash', '/opt/scripts/merge_log_bundle_parts.sh', '--source', '/home/root/.log-bundle-2022
dle-20221026T092716.tar'], returncode=0, stdout='Appending extra file environment...\nConcatenating bundle part local-node
6T092716.log...\n', stderr='')
2022-10-26 09:27:25,466 [INFO] assembly script stdout> Appending extra file environment...
2022-10-26 09:27:25,467 [INFO] assembly script stdout> Concatenating bundle part local-node-logs.tar...
2022-10-26 09:27:25,467 [INFO] assembly script stdout> Appending extra file log-bundle-20221026T092716.log...
2022-10-26 09:27:25,467 [INFO] Generation of log bundle /home/root/log-bundle-20221026T092716.tar completed successfully
2022-10-26 09:27:25,467 [INFO] The log bundle /home/root/log-bundle-20221026T092716.tar is now available.
```

15-12 Log Bundle Structure

The log bundle is a timestamped TAR file. The name of the bundle matches the `log-bundle-<date>T<time>.tar` format.



The log bundle consists of the following content:

- Environment file: The environment file contains the output of various Kubernetes commands. It supplies information about current resource usage per node and per pod. It also contains cluster information and descriptions of all available Kubernetes entities.
- Host logs and configuration: The configuration of each host (for example, its `/etc` directory) and the host-specific logs (for example, `journald`) are collected in one directory for each cluster node or host. The name of the directory matches the host name of the node.
- Services logs: Logs of the running Kubernetes services are available in the `<host_name>/services-logs/<namespace>/<app_name>/<container_name>.log` file.

  An example filename is `my-host-01/services-logs/prelude/vco-app/vco-server-app.log`.

15-13 Important Logs

The table includes key logs and their locations in the log bundle for troubleshooting the VMware Aria Automation appliances and services.

Log Location in Bundle	Description
`/services-logs/ingress/traefik/ingress-ctl-traefik.log`	Reverse proxy system used to capture the communication to and from the system
`/services-logs/kube-system/etcd/etcd.log`	Access log for the `/etcd` database
`/var/log/auth.log`	Authentication logs for the core system
`/var/log/deploy.log`	Logs of problems that occurred during the deployment of the virtual appliance
`<host_name>/services-logs/<namespace>/<app_name>/file-logs/<container_name>.log`	Access logs for Kubernetes services

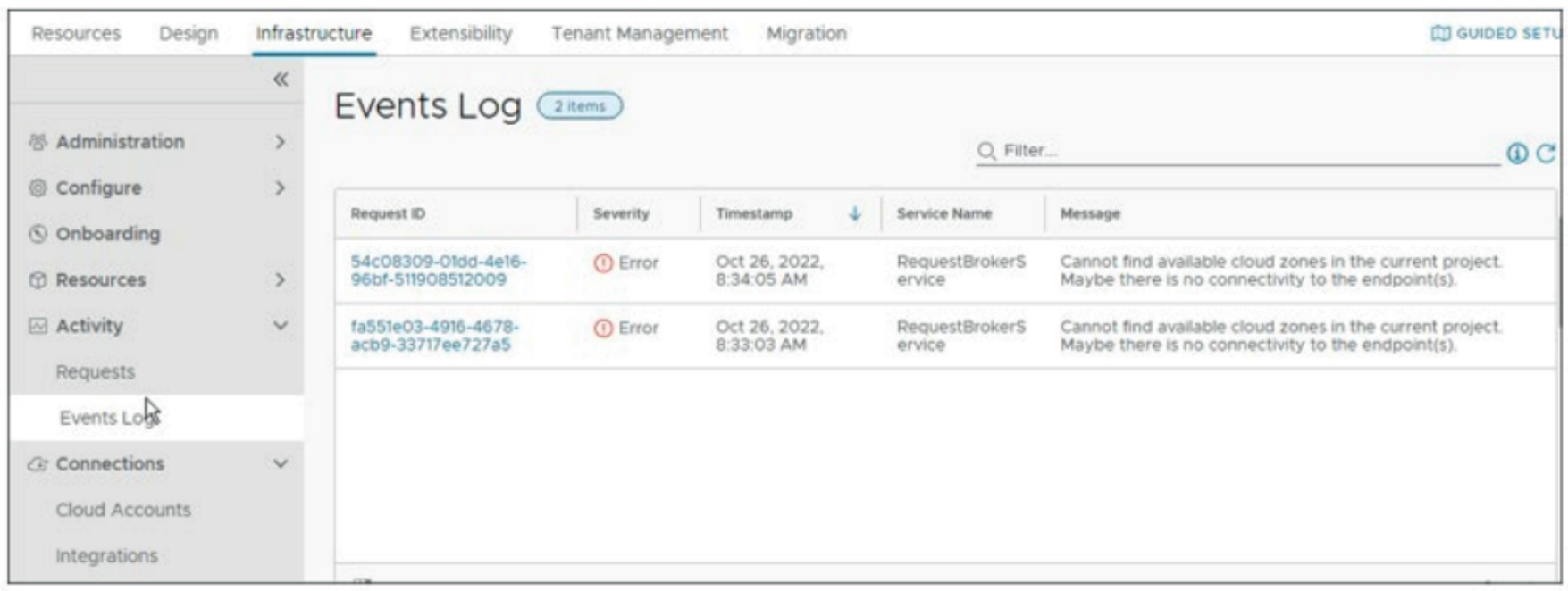
`kubectl -n prelude logs <pod_name> -n <namespace>.`

The `auth.log` and `deploy.log` files are present on the appliance in the `/var/log/` directory. To check other logs that are present on the appliance, you can run the `kubectl logs <pod_name> -n <namespace>` command.

15-14 Monitoring Requests

To monitor requests through the VMware Aria Automation console, you select **Infrastructure** > **Activity** > **Requests** in the navigation pane on the left.





The Requests page displays the status of service requests. If a failure occurs, you can start troubleshooting by viewing the failed request error in Events Log.

15-15 Lab 37: Collecting Log Bundles and Investigating Logs

Create a log bundle and monitor live logs in SSH:

1. Collect a Log Bundle
2. Investigate the Log Bundle
3. Use the kubectl Command to Investigate Logs

15-16 Lab 38: Restarting Services

Restart a service:

1. Check a Service Pod for Dependencies
2. Replace the Service Pod

15-17 Review of Learner Objectives

- Demonstrate how to monitor and troubleshoot VMware Aria Automation with CLI commands
- Explain how to collect a log bundle
- Identify the key logs location
- Describe the process of monitoring requests in the UI

15-18 Lesson 2: VMware Aria Suite Integration

15-19 Learner Objectives

- Describe VMware Aria Operations for Logs and its integration with VMware Aria Automation
- Describe VMware Aria Operations and its integration with VMware Aria Automation

15-20 Overview of VMware Aria Operations for Logs

VMware Aria Operations for Logs provides intelligent log management for infrastructure and applications in any environment.

This highly scalable log management solution delivers intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility across physical, virtual, and cloud environments.



VMware Aria Operations for Logs offers the following benefits:

- Adds structure to unstructured log data
- Provides rich dashboards
- Delivers innovative indexing and machine-learning-based intelligent grouping

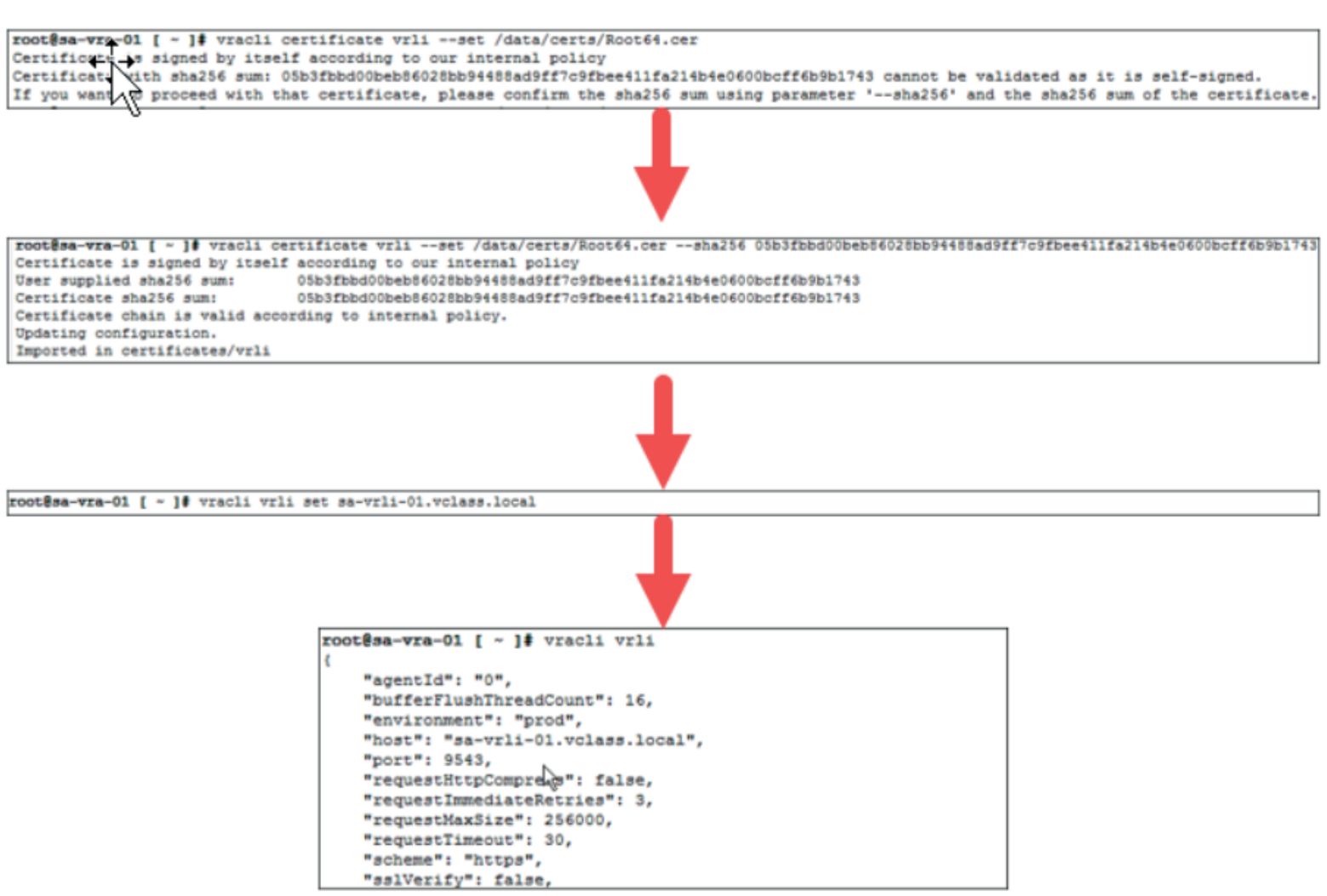
These features result in faster troubleshooting and provide solutions to the challenges of logs management.

15-21 VMware Aria Operations for Logs: Integration

You can forward logs from VMware Aria Automation to VMware Aria Operations for Logs to take advantage of robust log analysis and report generation.

This integration is configured from an SSH session by running the `vracli` command set:

```
vracli vrli set <option>
<VMware_Aria_Operations_for_Logs_FQDN>
```



VMware Aria Automation is bundled with a Fluentd-based logging agent. This agent collects and stores logs so that they can be included in a log bundle and examined later. Using the VMware Aria Operations for Logs REST API, you can configure this agent to forward a copy of the logs to a VMware Aria Operations for Logs server.

Port 9543 and https are used by default for sending the logs, but a different host scheme and port can be used.

To configure http and a specific port, run the following `vracli` command:

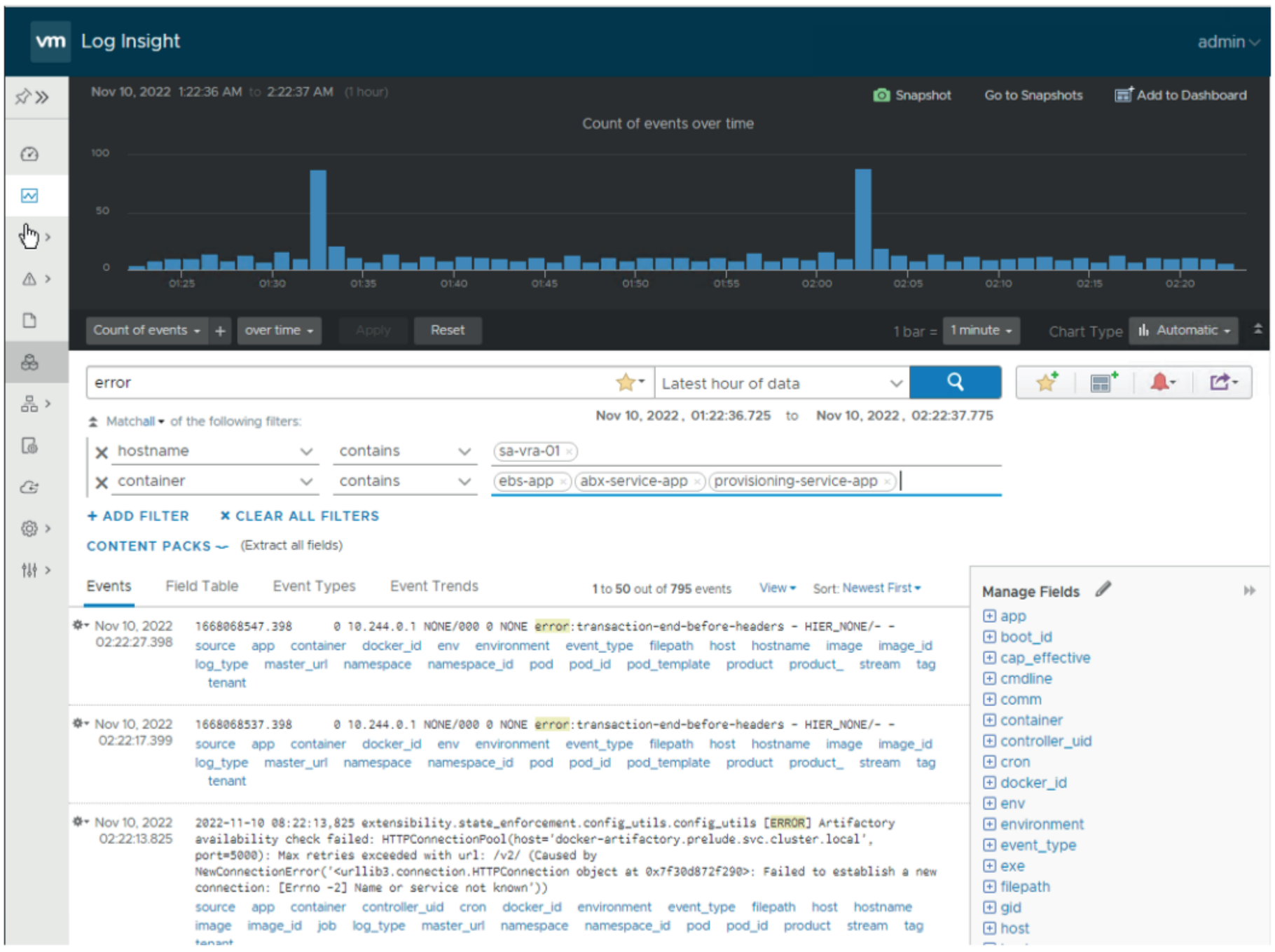
```
vracli vrli set
http://<VMware_Aria_Operations_for_logs_FQDN>:<port>
```

You can check the existing configuration of VMware Aria Operations for Logs by running the `vracli vrli` command.

15-22 VMware Aria Operations for Logs: Interactive Analytics

The Interactive Analytics feature in VMware Aria Operations for Logs provides excellent diagnostic information for troubleshooting VMware Aria Automation.

Using various automatically built tags, administrators can set up log reviews live over more than one container, service, or endpoint.



Multiple options are available for an enhanced log analysis:

- A timeframe can be specific for logs being analyzed. The available options are the previous hour, the previous 6 hours, and a custom time range.
- Tags can be selected on the right under fields, or by clicking **ADD FILTER**. You can add more than one container service to look at multiple logs at once in the primary events window. Select any or all options.
- Adding text examples with an error allows the filtering of base text for rapid selections.

Selections can be saved as dashboards for rapid views and overviews of an environment.

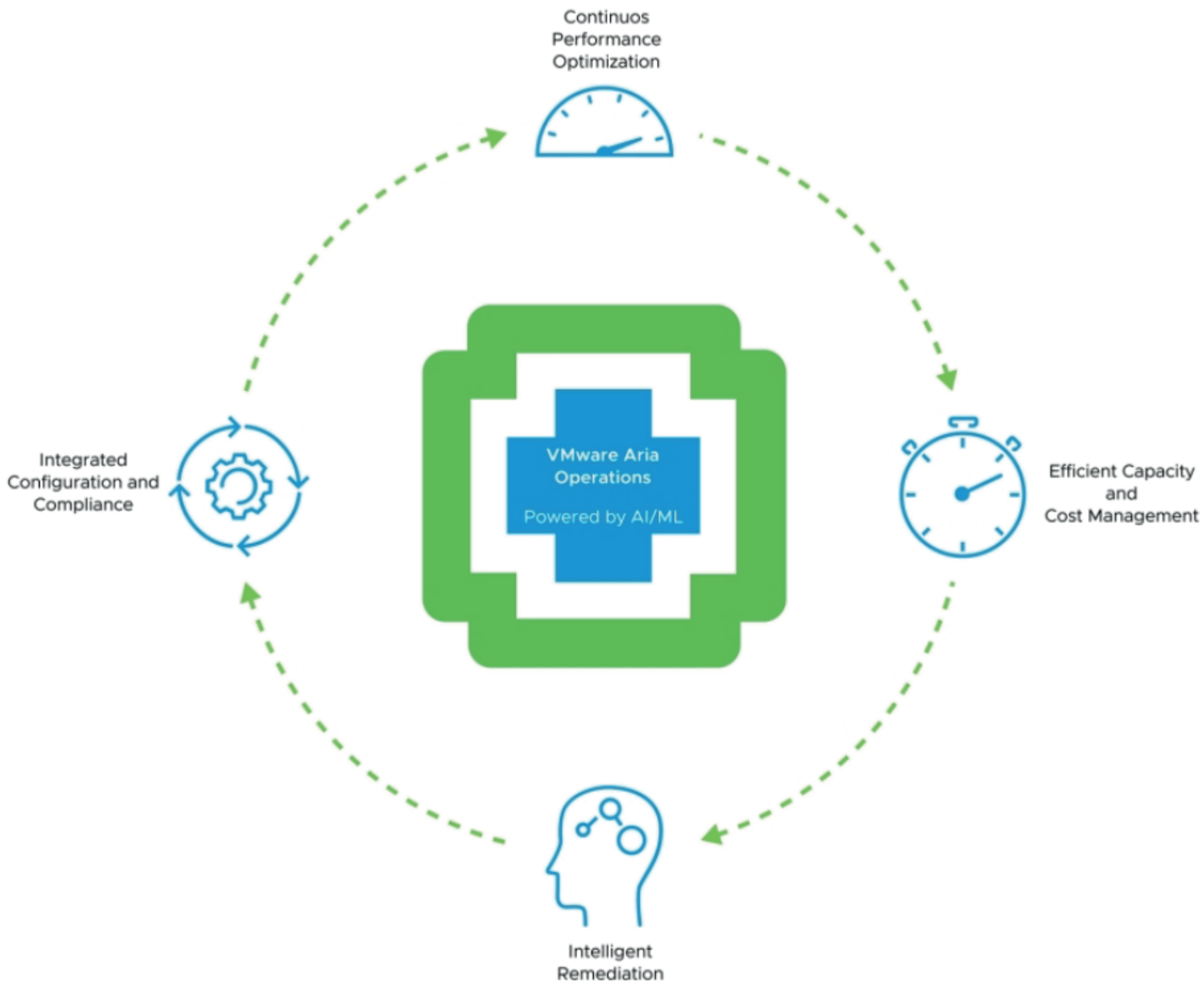
Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs.

To download content packs, log in to VMware Aria Operations for Logs and select **Content Packs** in the left pane. Download the VMware vRA 8.3+ Content Pack.

The VMware Aria Automation content pack is not mandatory for the integration.

15-23 Overview of VMware Aria Operations

VMware Aria Operations delivers self-driving IT operations management for private, hybrid, and multicloud environments in a unified AI-powered platform.



The expansion of data centers to public clouds adds more complexity in IT operations, which results in the need for simplifying and automating operations.

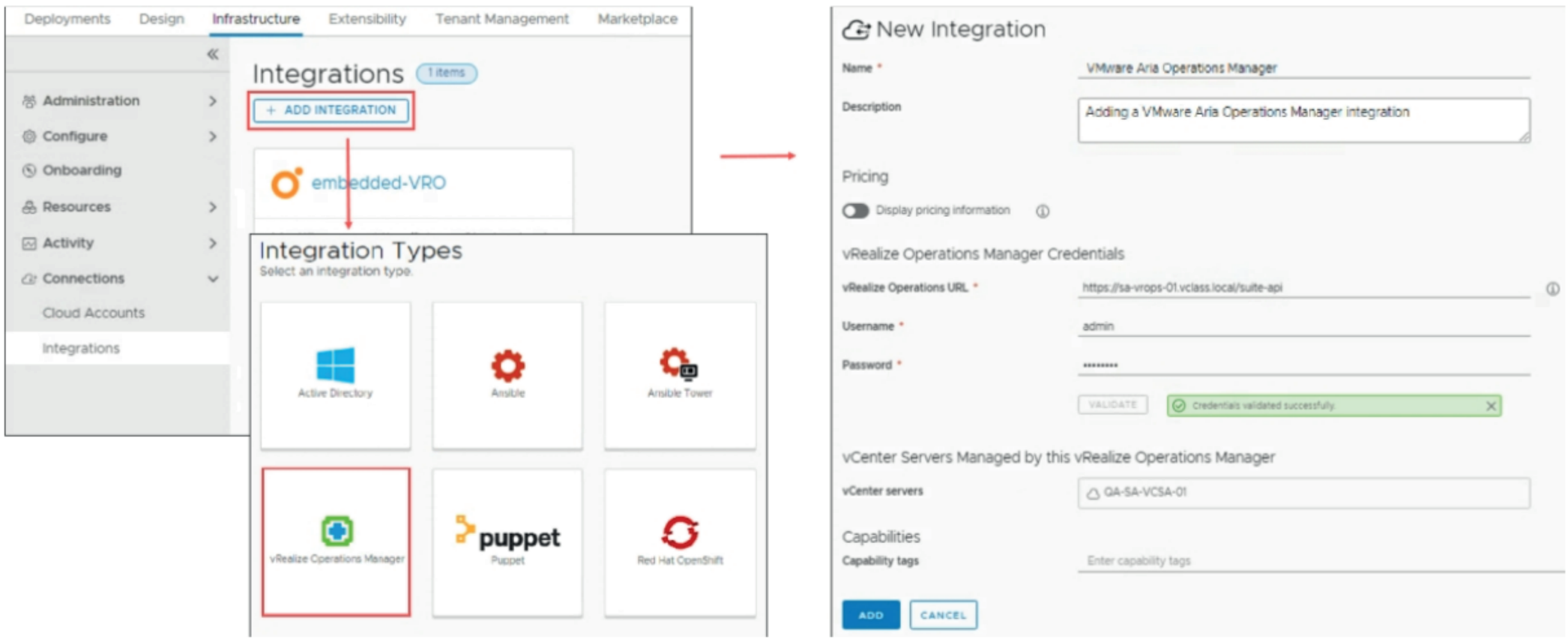
VMware Aria Operations delivers intelligent operations management platform to optimize, plan, and scale VMware Cloud. This includes on-premises private cloud or VMware SDDC in multiple public clouds (VMware Cloud on AWS).

Powered by artificial intelligence, VMware Aria Operations provides a unified operations platform that delivers continuous performance optimization, efficient capacity and cost management, proactive planning, app-aware intelligent remediation, and integrated compliance.

15-24 Integration in VMware Aria Automation

To integrate VMware Aria Automation with VMware Aria Operations, select **Infrastructure** > **Connections** > **Integrations** in the VMware Aria Automation console.

Click **ADD INTEGRATION** and then click **vRealize Operations Manager** to configure this integration.

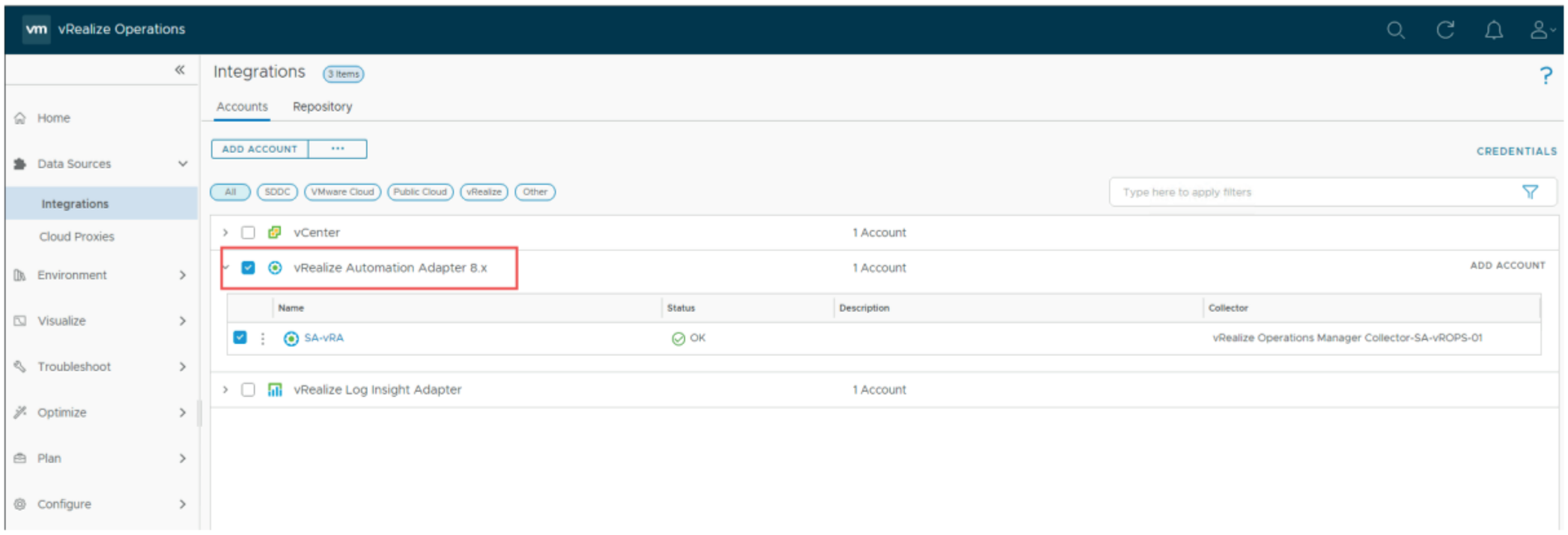


To add the integration in VMware Aria Automation, enter the VMware Aria Operations URL (https://<VMware_Aria_Operations_IP_address_or_FQDN>/suite-api), user name, and password.

After entering the values, click **VALIDATE**.

15-25 Integration with VMware Aria Operations

To integrate VMware Aria Operations with VMware Aria Automation, select **Data Sources** > **Integrations** in the VMware Aria Operations console.



15-26 VMware Aria Operations: Integration Benefits

The integration between VMware Aria Automation and VMware Aria Operations is a two-way integration.

Each integration provides separate functionalities, so both products must be integrated to work with each other.

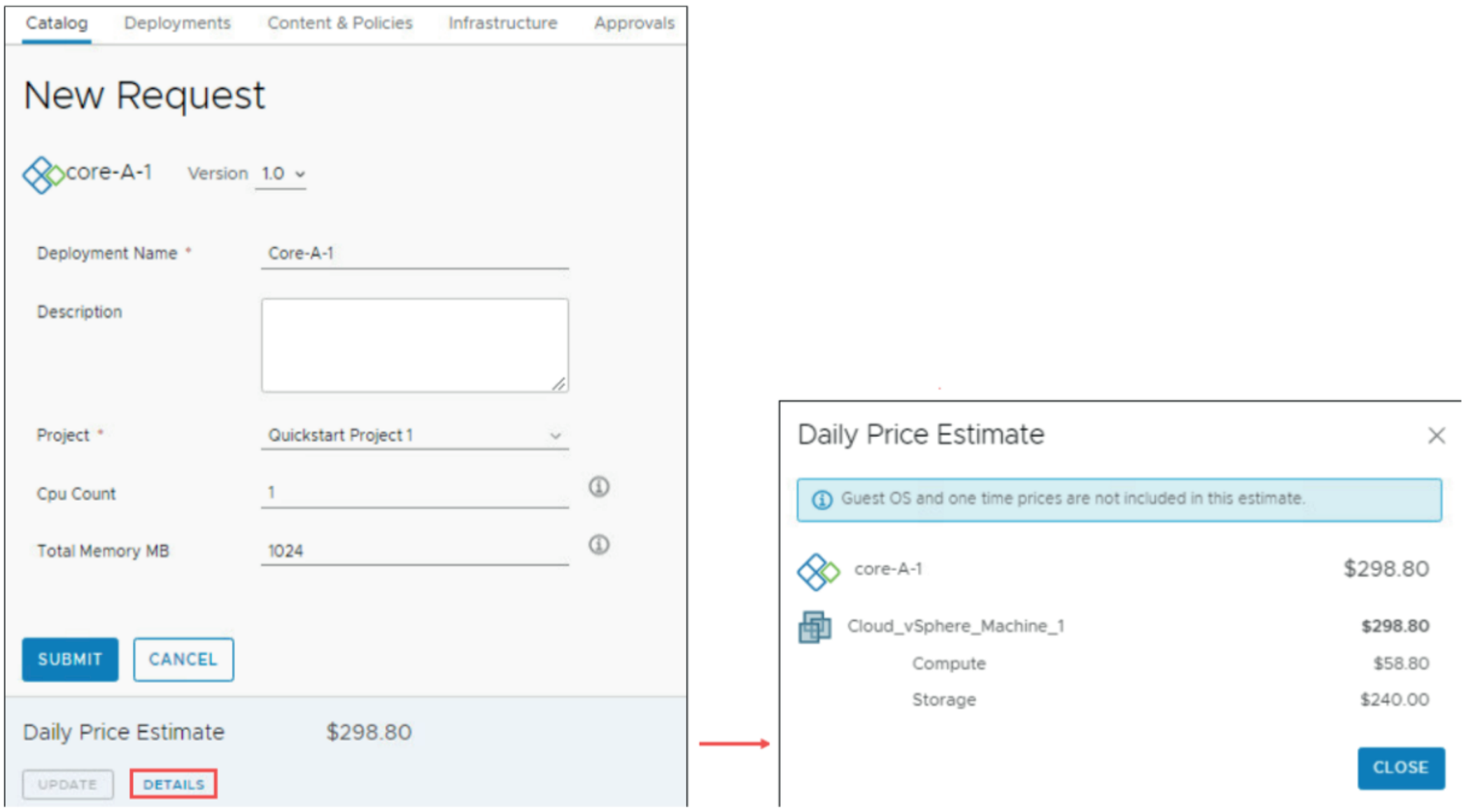
VMware Aria Automation can work together with VMware Aria Operations to display pricing, provide deployment health and virtual machine metrics, and perform advanced workload placement.

15-27 Integration Benefits: Cost Pricing

When integrated with VMware Aria Operations, users can see the associated costs of deployments that they request.

Users can better determine whether they want to request the deployments based on the estimated daily cost.

Users can understand the costing details by viewing compute, storage, and additional charges.



VMware Aria Operations integrates pricing into its analytics.

Integrating with VMware Aria Operations makes these cost pricing data available to VMware Aria Automation.

15-28 Integration Benefits: Deployment Monitoring

VMware Aria Automation retrieves VMware Aria Operations metrics about deployments.

To access deployment monitoring, click a deployment and click the **Monitor** tab.

To see the metrics of a particular virtual machine, select from the collapsible list of components in the left navigation pane.



The **Metrics** tab appears only after configuring the integration with VMware Aria Operations.

Metrics are not cached. VMware Aria Operations provides the metrics directly, and the metrics might take a few moments to load.

Only metrics for virtual machines are shown.

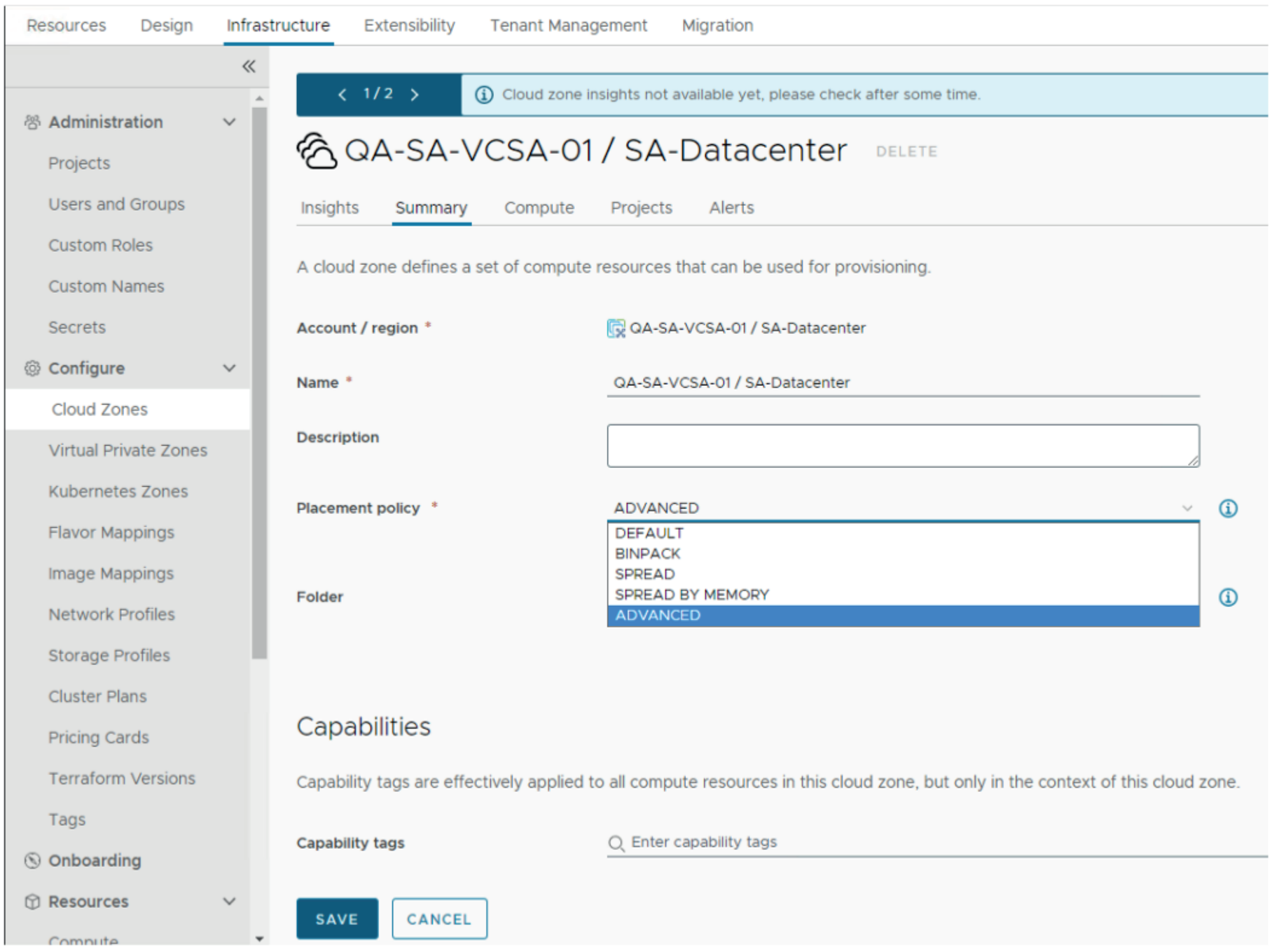
Metrics appear as timeline graphs that show highs and lows for the following measures:

- CPU
- Memory
- Storage
- Network speed

15-29 Integration Benefits: Workload Placement

After integrating with VMware Aria Operations, a new Advanced placement policy appears under the Cloud Zones configuration in VMware Aria Automation.

This Advanced placement policy places workloads based on VMware Aria Operations recommendations.



VMware Aria Operations considers operational intent for an optimal placement.

Operational intent can take past workloads and hypothetical future predictions into account.

15-30 Review of Learner Objectives

- Describe VMware Aria Operations for Logs and its integration with VMware Aria Automation
- Describe VMware Aria Operations and its integration with VMware Aria Automation

15-31 Key Points

- The VMware Aria Automation logs are accessed through the CLI.
- Access key logs in the log bundle for troubleshooting.
- Many functions can be controlled and modified through the CLI because the system is based on Kubernetes.
- Integration with VMware Aria Operations displays pricing, provides deployment health and virtual machine metrics.
- Integration with VMware Aria Operations for Logs supports log analysis and report generation.

Questions?