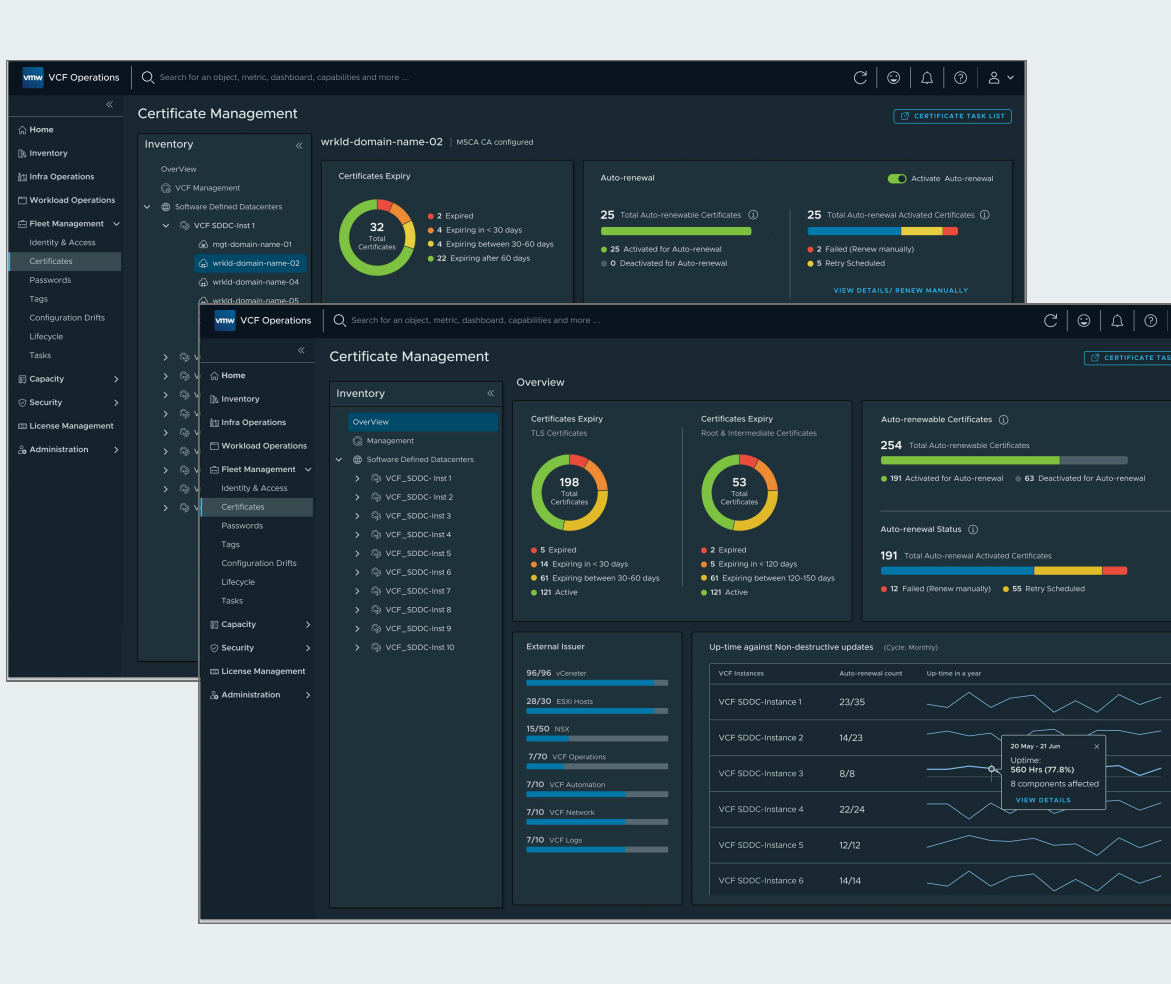
Case Study

Enhancing CX by Feature Integration & Centralizing Ops Management

By Abneet Chauhan
2024-2025


VCF Operations
Certificate Management
Inventory
Overview

Product

VCF Operations

VMware Cloud Foundation (VCF) Operations enables you to run and manage your IT infrastructure with covering many features like monitoring, lifecycle management, workload handling, security, and performance optimization.

User

Vi Admin **SRE**

Infrastructure Admins / SREs responsible for managing the VCF stack, including compute, storage, networking, and cloud management components.

Goal:
To ensure the virtualized IT infrastructure is highly available, secure, scalable, and performing optimally to support business operations.

How It All Started

After Broadcom took over, the product strategy evolved to prioritize enhancement over expansion. The concept of centralized fleet-level management was conceived in response to a combination of operational and strategic drivers.

Integration: One of the Directions

One of the directions proposed by leadership was product and feature integration. There shouldn't be redundancies across products.

AHA Tickets

User feedback on the certificate and password consoles was gathered through various Customer Connect Programs.

Details

Certificate & Password

TLS Certificate & Passwords Management got separated from security work stream and I was assigned for seamless integration of these in vROps.

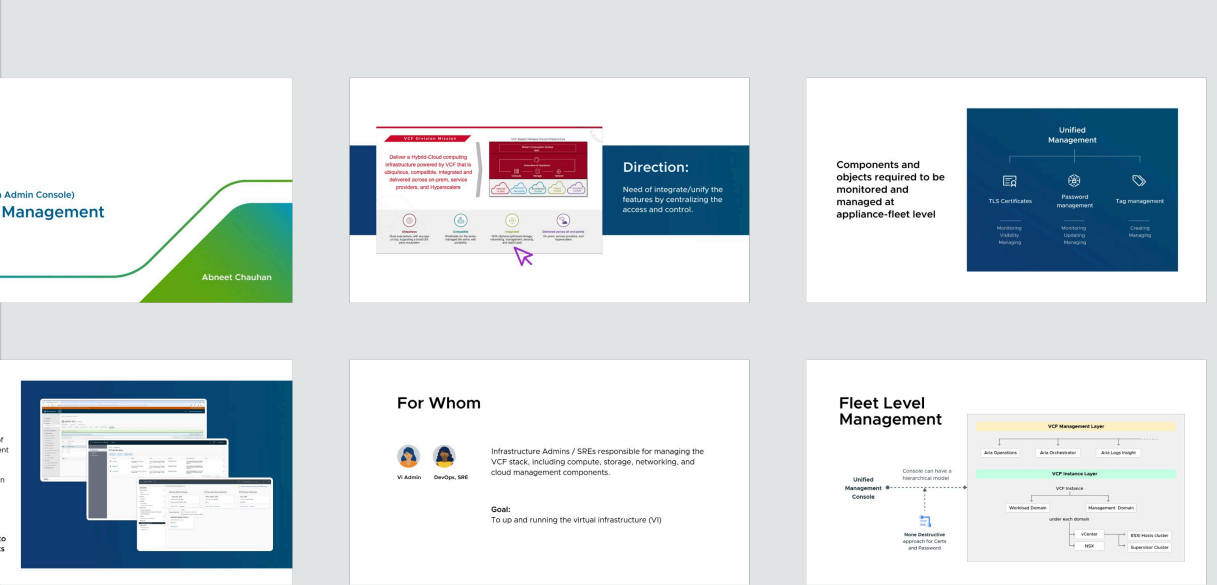
Details

Long-overdue Exp Enhancement

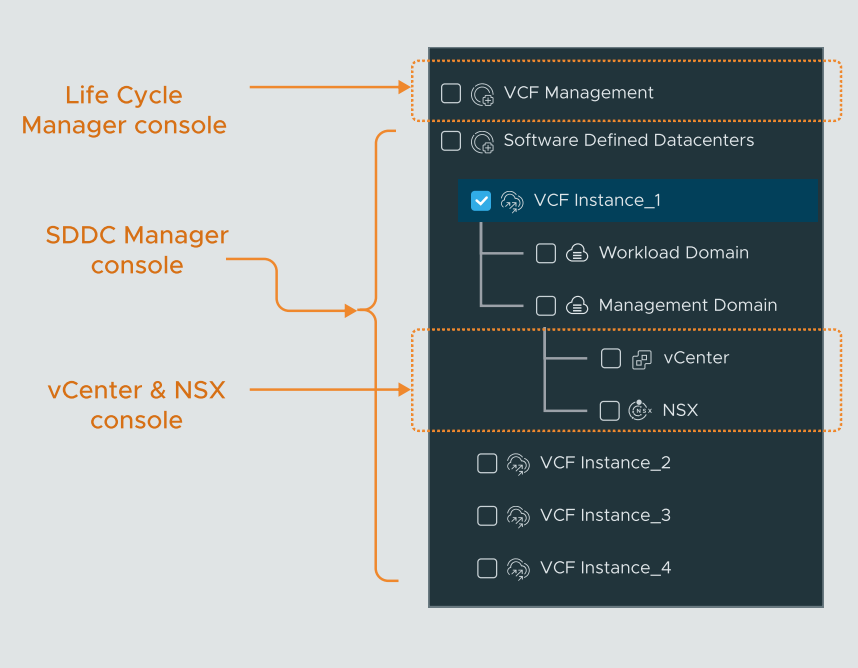
With various Ops features built by separate product teams, a cohesive, use-case-driven experience had been missing and was long overdue.

Pitched To Triad

Presented the idea of fleet-level management for TLS Certificates and Passwords to the Triad Panel— Design, Product Management, and Engineering—If it looks feasible to architects, we can possibly integrate all the consoles in to Ops. And through a combined effort we arrived on a potential solution.


Direction:
For Whom
Fleet Level Management
Customer Benefits
Broadcom Benefits

Consoles mapping to unified inventory model


Life Cycle Manager console
SDDC Manager console
vCenter & NSX console
VCF Management
Software Defined Datacenters
VCF Instance_1
Workload Domain
Management Domain
vCenter
NSX
VCF Instance_2
VCF Instance_3
VCF Instance_4

In order to simplify the journey,
let's focus on one of the items - Certificates.

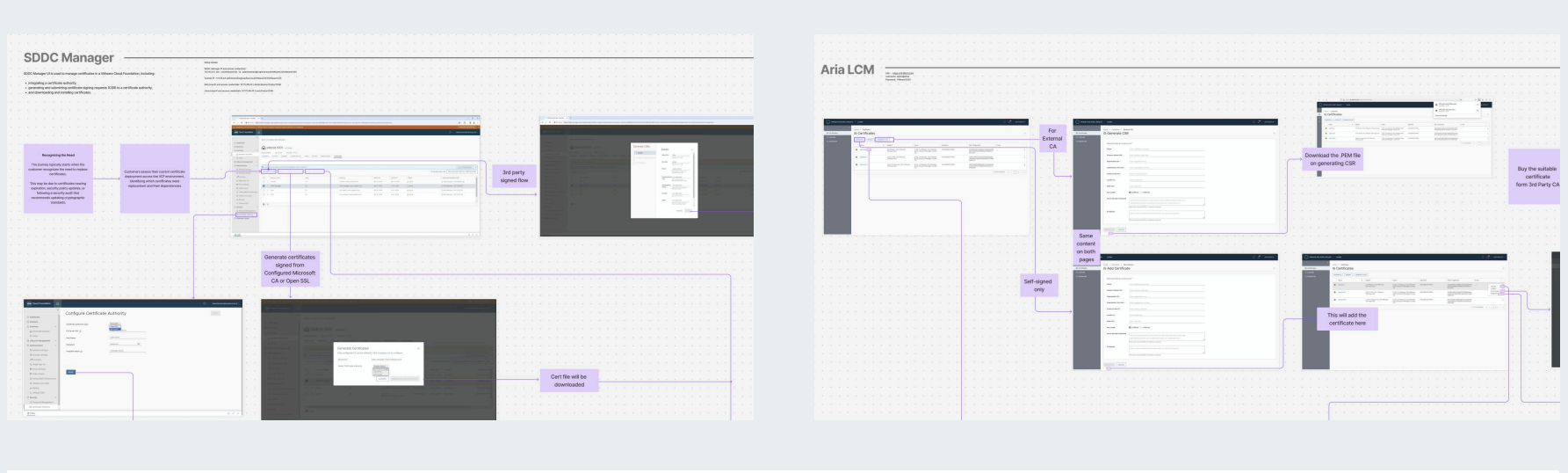
Unified
TLS Certificate Management

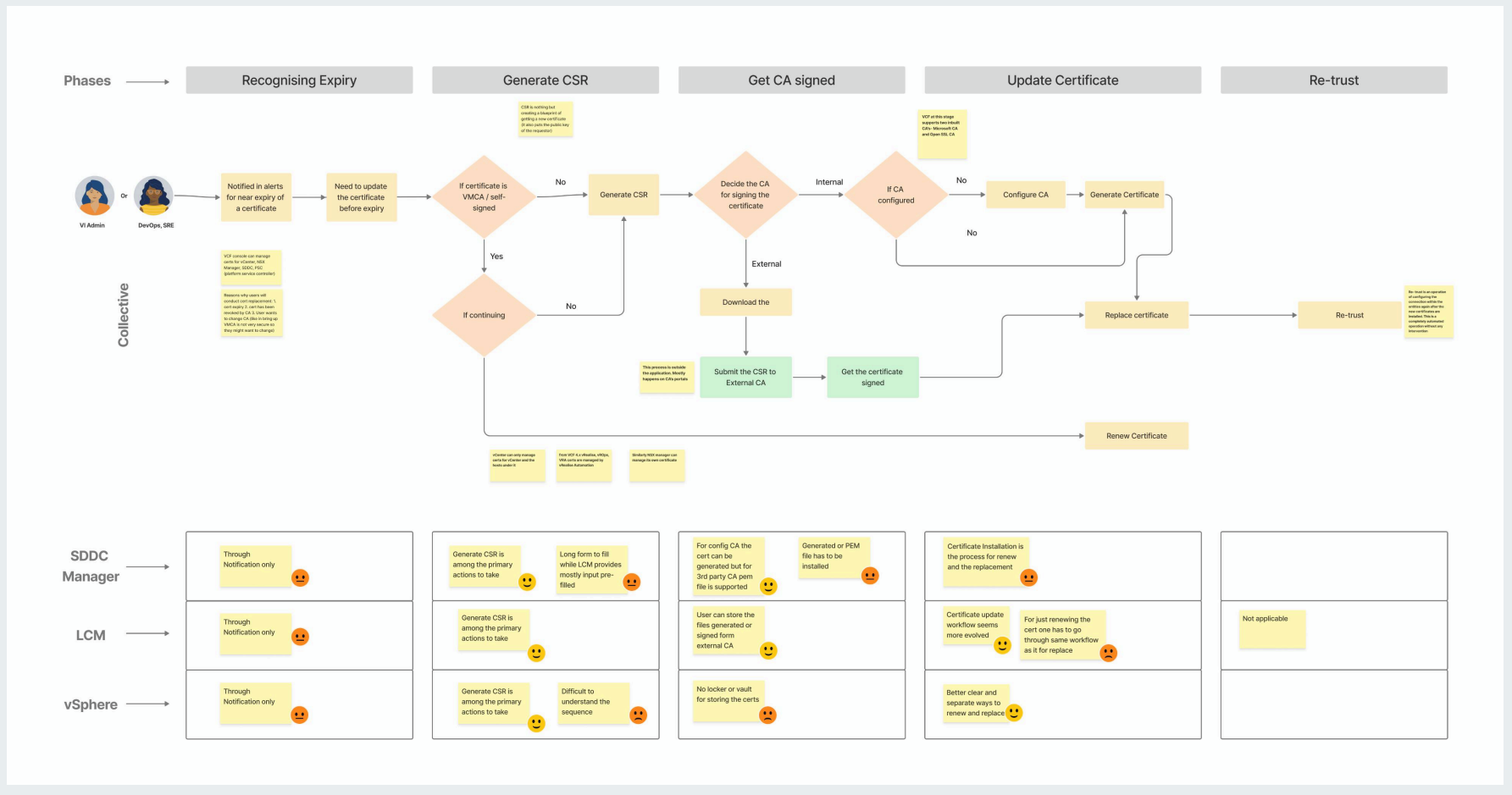
1

Unifying The Workflows

First, I quickly studied the workflows across SDDC Manager, Aria LCM, vSphere Client, and NSX Console to deeply understand the current functionality and key differences.

Next, I mapped out a user journey that could apply across all consoles and analyzed the strengths and gaps within each console at different stages of the journey.

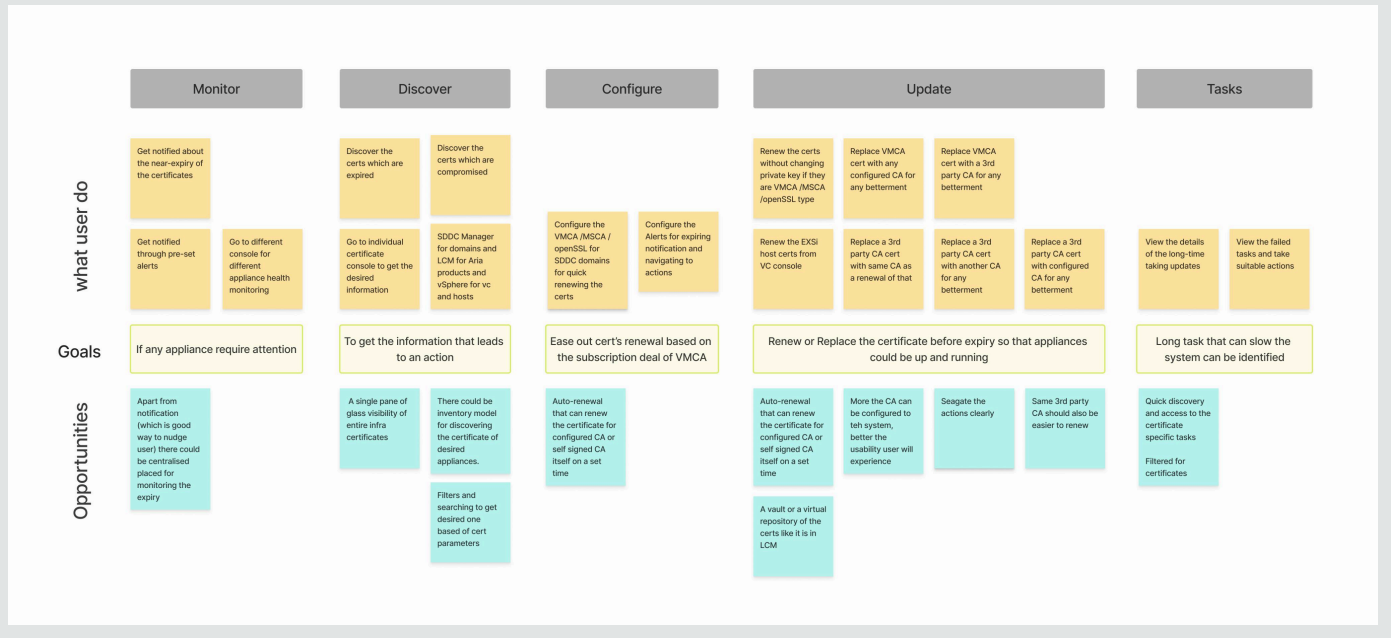

SDDC Manager
Aria LCM


Phases
Recognising Expiry
Generate CSR
Get CA signed
Update Certificate
Re-trust
Collective
Vi Admin
DevOps, SRE
Notified in alerts for near expiry of a certificate
Need to update the certificate before expiry
If certificate is VMCA / self-signed
Yes
No
If continuing
Generate CSR
Decide the CA for signing the certificate
Internal
External
Download the
Submit the CSR to External CA
Get the certificate signed
If CA configured
Configure CA
Generate Certificate
Replace certificate
Re-trust
Renew Certificate
SDDC Manager
LCM
vSphere
Through Notification only
Generate CSR is among the primary actions to take
Long form to fill while LCM provides mostly input pre-filled
Difficult to understand the sequence
For config CA the cert can be generated but for 3rd party CA pem file is supported
Generated or PEM file has to be installed
User can store the files generated or signed form external CA
No locker or vault for storing the certs
Certificate Installation is the process for renew and the replacement
Certificate update workflow seems more evolved
For just renewing the cert one has to go through same workflow as it for replace
Better clear and separate ways to renew and replace
Not applicable

2

Finding Opportunities

After the above exercise, I held a quick workshop with TAMs and CSMs to identify what customers need beyond centralized management and drafted key opportunity areas.



	Monitor	Discover	Configure	Update	Tasks
what user do	Get notified about the near-expiry of the certificates Get notified through pre-set alerts Go to different console for different appliance health monitoring	Discover the certs which are expired Discover the certs which are compromised Go to individual certificate console to get the desired information SDDC Manager for domains and LCM for Aria products and vSphere for vc and hosts	Configure the VMCA /MSCA / openSSL for SDDC domains for quick renewing the certs Configure the Alerts for expiring notification and navigating to actions	Renew the certs without changing private key if they are VMCA /MSCA /openSSL type Replace VMCA cert with any configured CA for any betterment Replace VMCA cert with a 3rd party CA for any betterment Renew the EXSI host certs from VC console Replace a 3rd party CA cert with same CA as a renewal of that Replace a 3rd party CA cert with another CA for any betterment Replace a 3rd party CA cert with configured CA for any betterment	View the details of the long-time taking updates View the failed tasks and take suitable actions
Goals	If any appliance require attention	To get the information that leads to an action	Ease out cert's renewal based on the subscription deal of VMCA	Renew or Replace the certificate before expiry so that appliances could be up and running	Long task that can slow the system can be identified
Opportunities	Apart from notification (which is good way to nudge user) there could be centralised placed for monitoring the expiry	A single pane of glass visibility of entire infra certificates There could be inventory model for discovering the certificate of desired appliances. Filters and searching to get desired one based of cert parameters	Auto-renewal that can renew the certificate for configured CA or self signed CA itself on a set time	Auto-renewal that can renew the certificate for configured CA or self signed CA itself on a set time More the CA can be configured to teh system, better the usability user will experience Seagate the actions clearly Same 3rd party CA should also be easier to renew A vault or a virtual repository of the certs like it is in LCM	Quick discovery and access to the certificate specific tasks Filtered for certificates

Centralised place for monitoring cert-expiry

Certificate vaults for external CA

Renewal automation

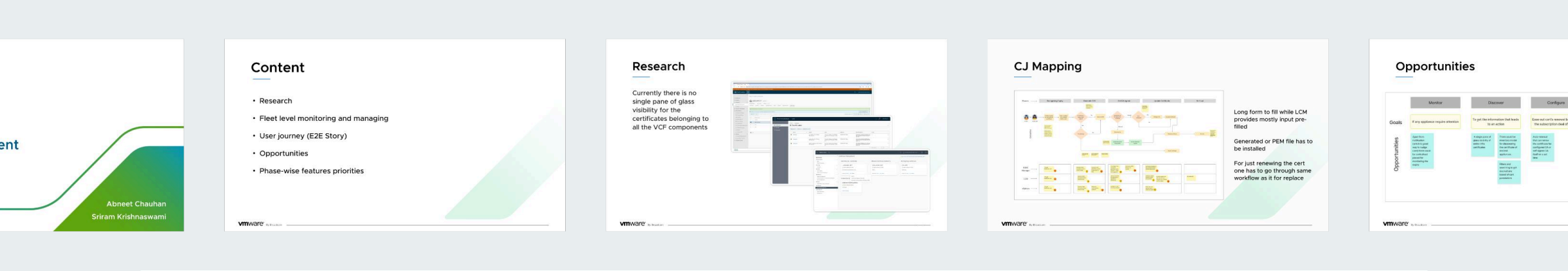
More CAs could be configured for automation

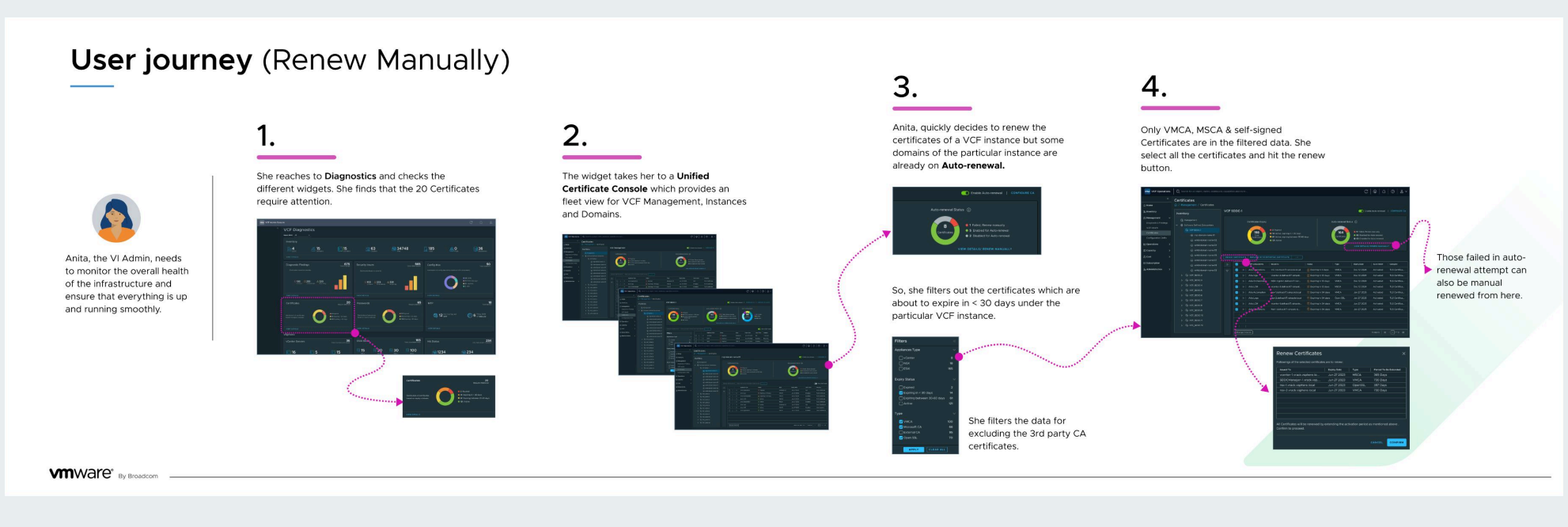
Non- Destructive Certificate Update (NDC)

3

Concept Share-Out

I with assigned PM worked on the quick ideation and put together the E2E Experience for the Unified Certificate Management. This was shared with the entire Ops-Management work-stream team.


Abneet Chauhan
Sriram Krishnaswami
Content
Research
Fleet level monitoring and managing
User journey (E2E Story)
Opportunities
Phase-wise features priorities
Research
Currently there is no single pane of glass visibility for the certificates belonging to all the VCF components
CJ Mapping
Long form to fill while LCM provides mostly input pre-filled
Generated or PEM file has to be installed
For just renewing the cert one has to go through same workflow as it for replace
Opportunities



User journey (Renew Manually)

Anita, the VI Admin, needs to monitor the overall health of the infrastructure and ensure that everything is up and running smoothly.

1. She reaches to **Diagnostics** and checks the different widgets. She finds that the 20 Certificates require attention.

2. The widget takes her to a **Unified Certificate Console** which provides an fleet view for VCF Management, Instances and Domains.

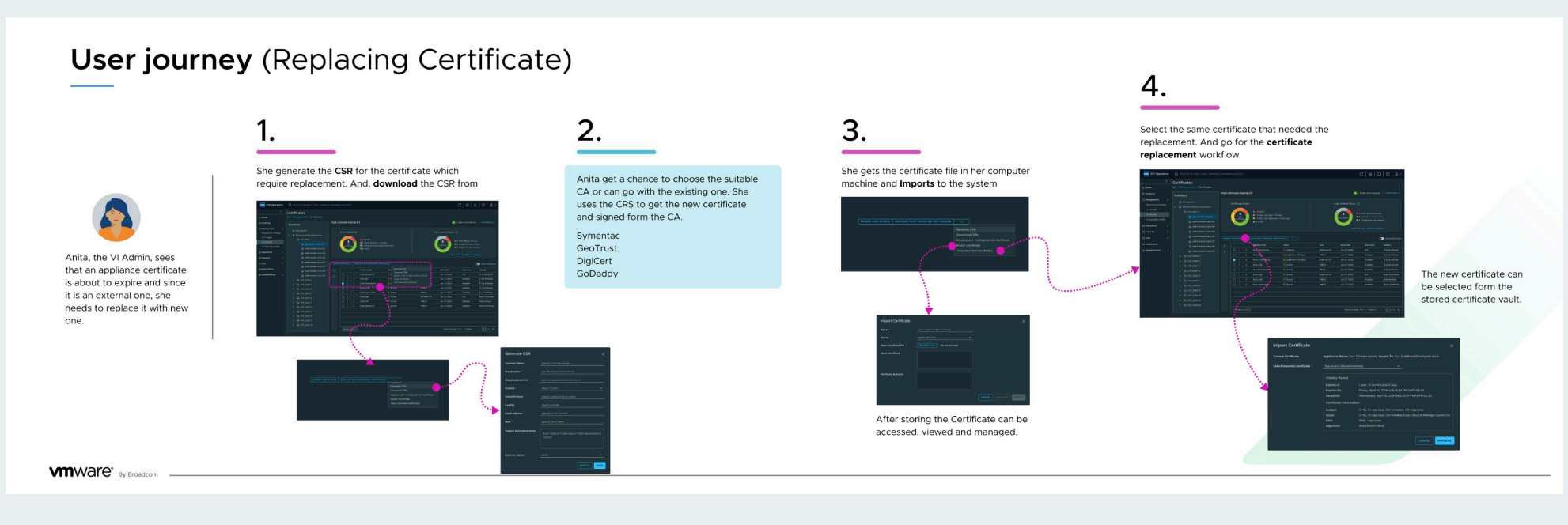
3. Anita, quickly decides to renew the certificates of a VCF instance but some domains of the particular instance are already on **Auto-renewal.**

So, she filters out the certificates which are about to expire in < 30 days under the particular VCF instance.

She filters the data for excluding the 3rd party CA certificates.

4. Only VMCA, MSCA & self-signed Certificates are in the filtered data. She select all the certificates and hit the renew button.

Those failed in auto-renewal attempt can also be manual renewed from here.



User journey (Replacing Certificate)

Anita, the VI Admin, sees that an appliance certificate is about to expire and since it is an external one, she needs to replace it with new one.

1. She generate the **CSR** for the certificate which require replacement. And, **download** the CSR from

2. Anita get a chance to choose the suitable CA or can go with the existing one. She uses the CRS to get the new certificate and signed from the CA.
Symentac
GeoTrust
DigiCert
GoDaddy

3. She gets the certificate file in her computer machine and **Imports** to the system

After storing the Certificate can be accessed, viewed and managed.

4. Select the same certificate that needed the replacement. And go for the **certificate replacement** workflow

The new certificate can be selected form the stored certificate vault.

Versioning

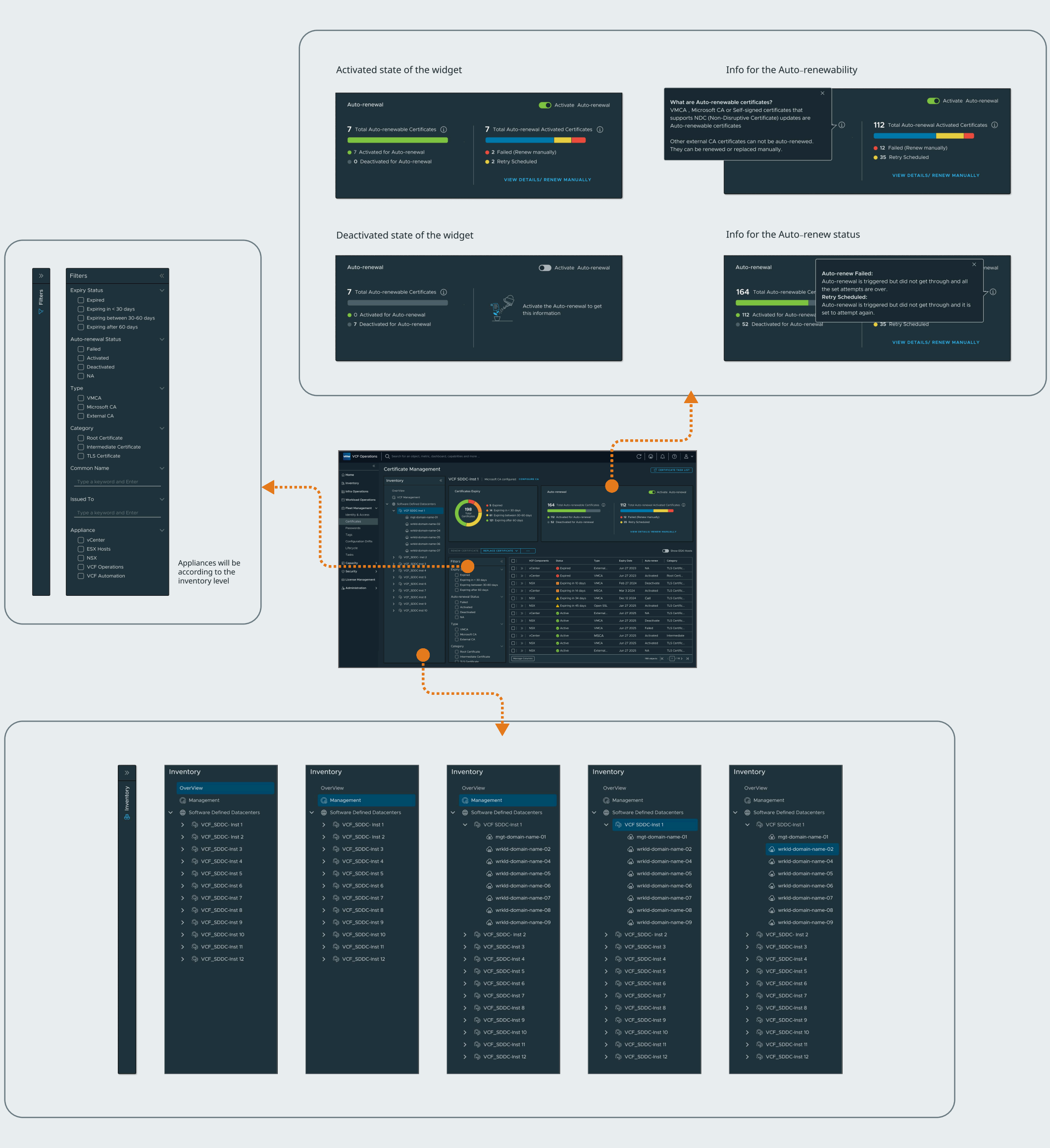
VCF 7.0	VCF 9.0	Beyound
Visibility only Monitoring will still happen from respective application consoles	Visibility of entire certificate Fleet Fleet level Monitoring Auto-renewal Replacement for 3rd party Import Feature CA configuration	Capability expansion of Auto-renewal Capability expansion of CA configuration Feedback based improvement

4

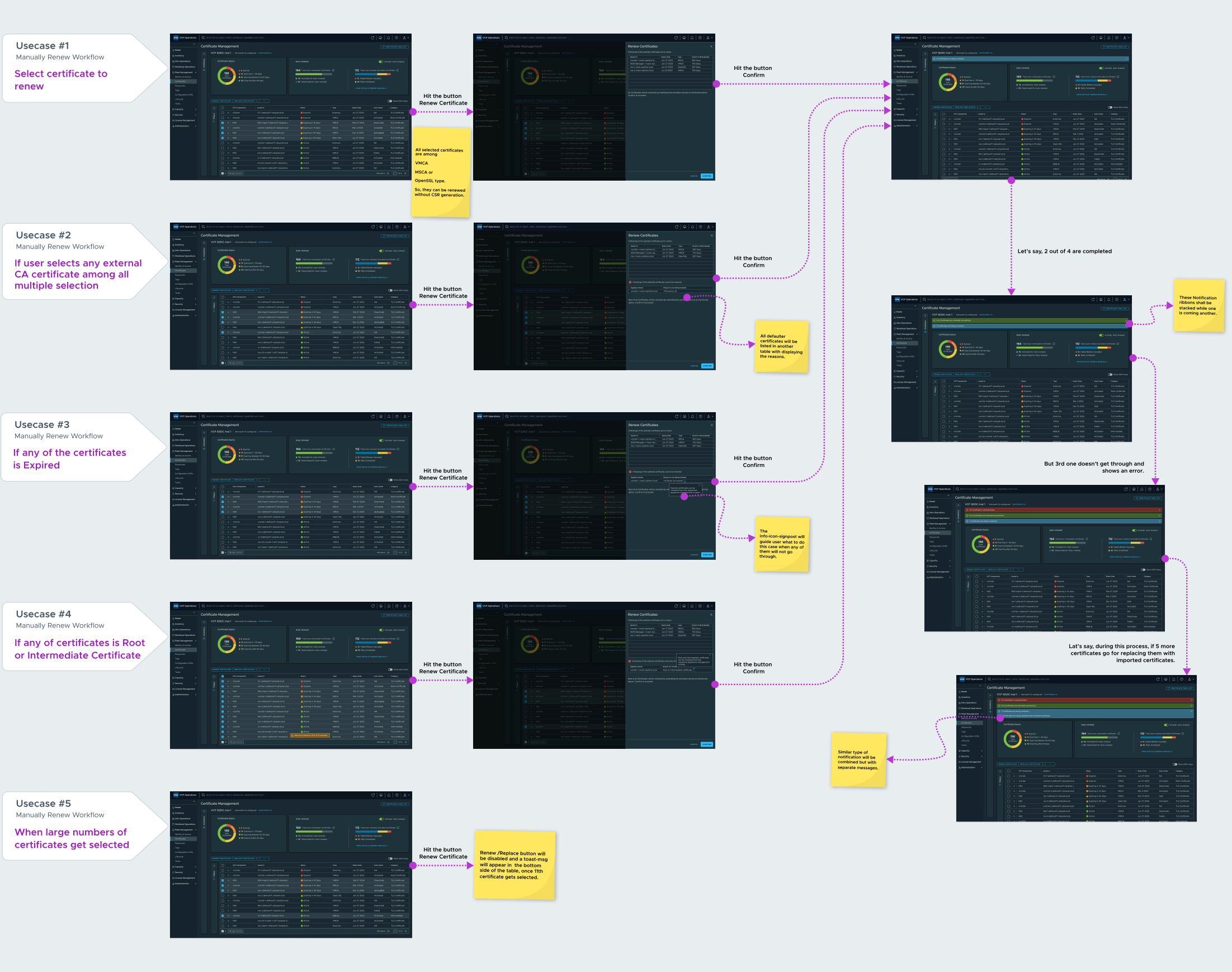
The Production Ready Design

Following the positive response and constructive feedback, I refined the design for production, which was finalized after multiple iterations. While I primarily used existing UI components and patterns from the CLARITY design system, I also designed and established several new patterns by identifying their broader applicability.

Different states of the widgets

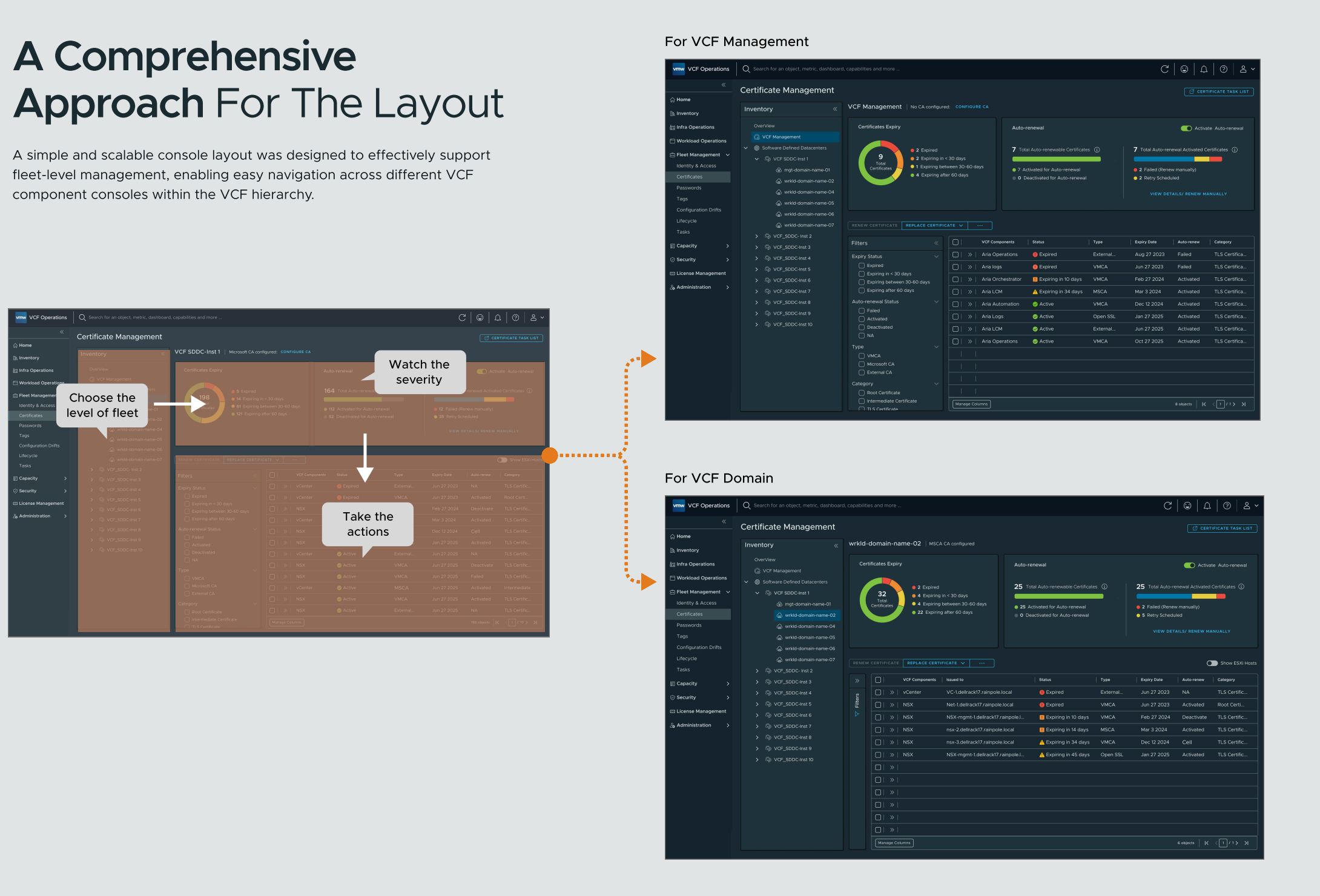

Activated state of the widget
Info for the Auto-renewability
Deactivated state of the widget
Info for the Auto-renew status
Filters
Appliances will be according to the inventory level
Inventory

Workflow: **Manually renew**


Usecase #1
Manually Renew Workflow
Select certificate to renew
Usecase #2
Manually Renew Workflow
If user selects any external CA certificate among all multiple selection
Usecase #3
Manually Renew Workflow
If any of the certificates is Expired
Usecase #4
Manually Renew Workflow
If any of certificates is Root or Intermediate Certificate
Usecase #5
Manually Renew Workflow
When large numbers of certificates get selected
Hit the button Renew Certificate
Hit the button Confirm
Let's say, 2 out of 4 are completed
But 3rd one doesn't get through and shows an error.

A Comprehensive Approach For The Layout

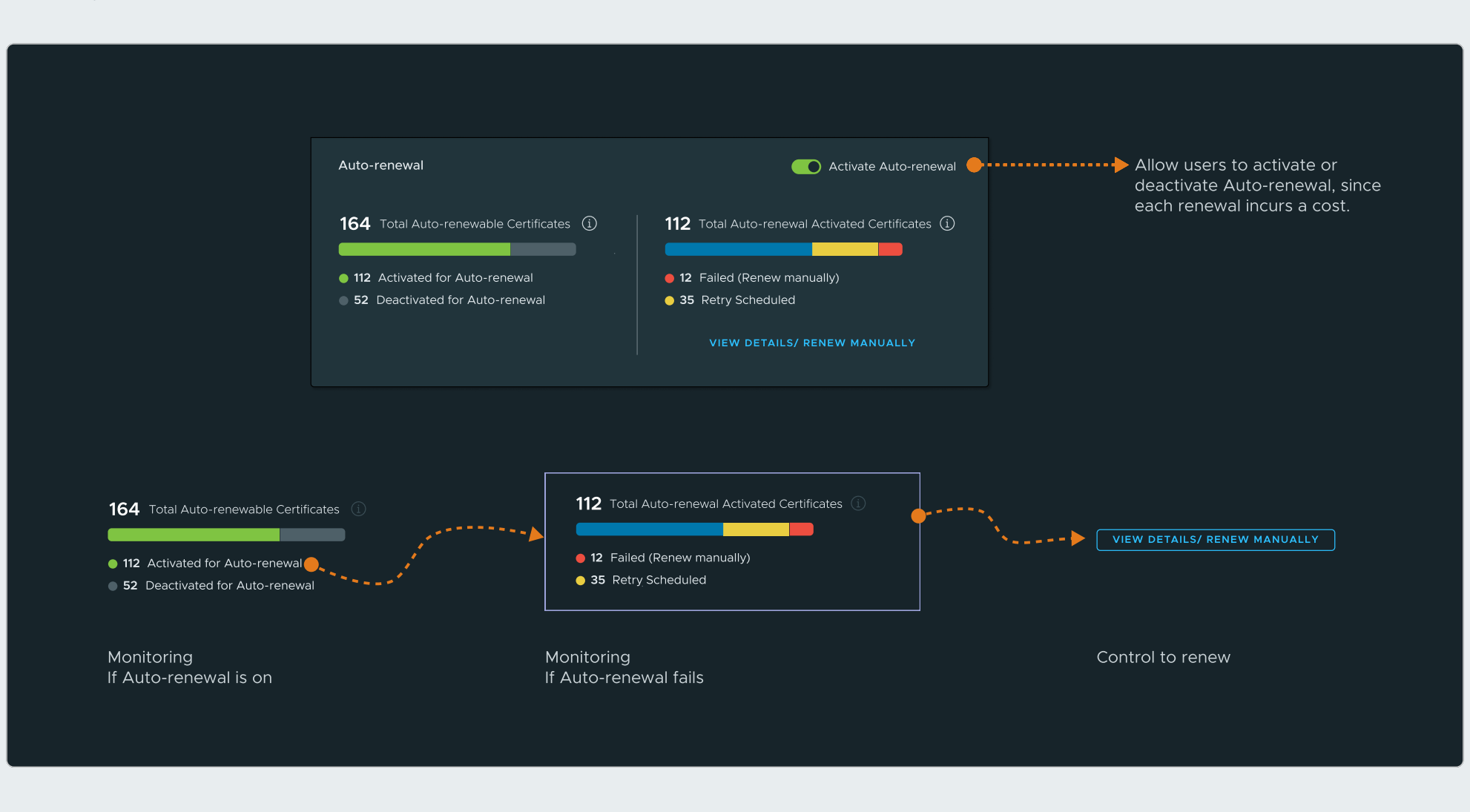
A simple and scalable console layout was designed to effectively support fleet-level management, enabling easy navigation across different VCF component consoles within the VCF hierarchy.


Choose the level of fleet
Watch the severity
Take the actions
For VCF Management
For VCF Domain

Facilitating **Human Agency & Control**

Auto-renewal is a process that removes the need for users to actively manage certificate updates—the system handles renewals automatically before expiration. However, users should still have control over:

1. Activating or deactivating the auto-renewal feature
2. Manually renewing a certificate if auto-renewal fails


Auto-renewal
Activate Auto-renewal
164 Total Auto-renewable Certificates
112 Activated for Auto-renewal
52 Deactivated for Auto-renewal
112 Total Auto-renewal Activated Certificates
12 Failed (Renew manually)
35 Retry Scheduled
VIEW DETAILS/ RENEW MANUALLY

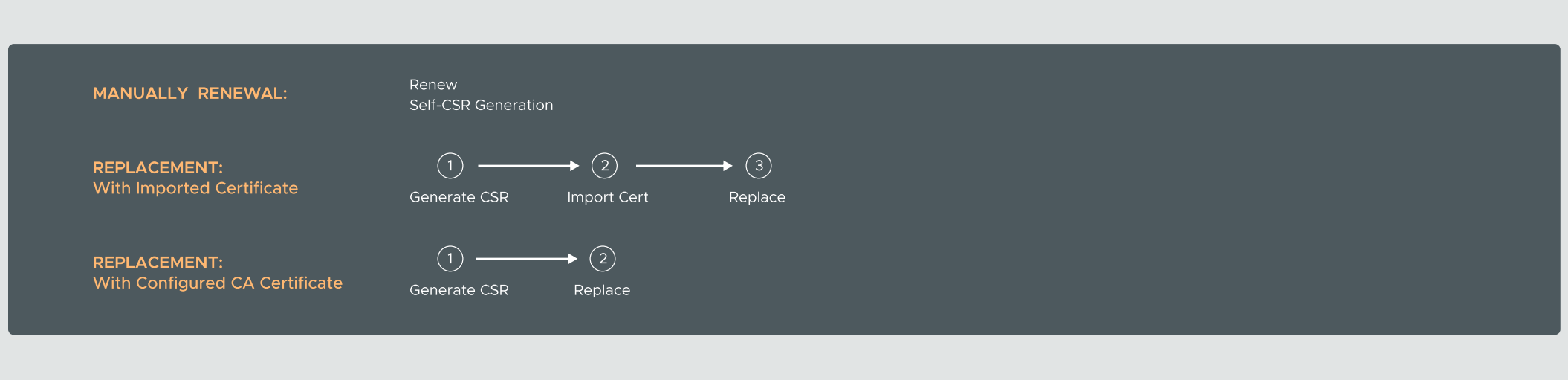
Allow users to activate or deactivate Auto-renewal, since each renewal incurs a cost.

Monitoring
If Auto-renewal is on

Monitoring
If Auto-renewal fails

Control to renew

Intuitive Interface, **Guided Actions**



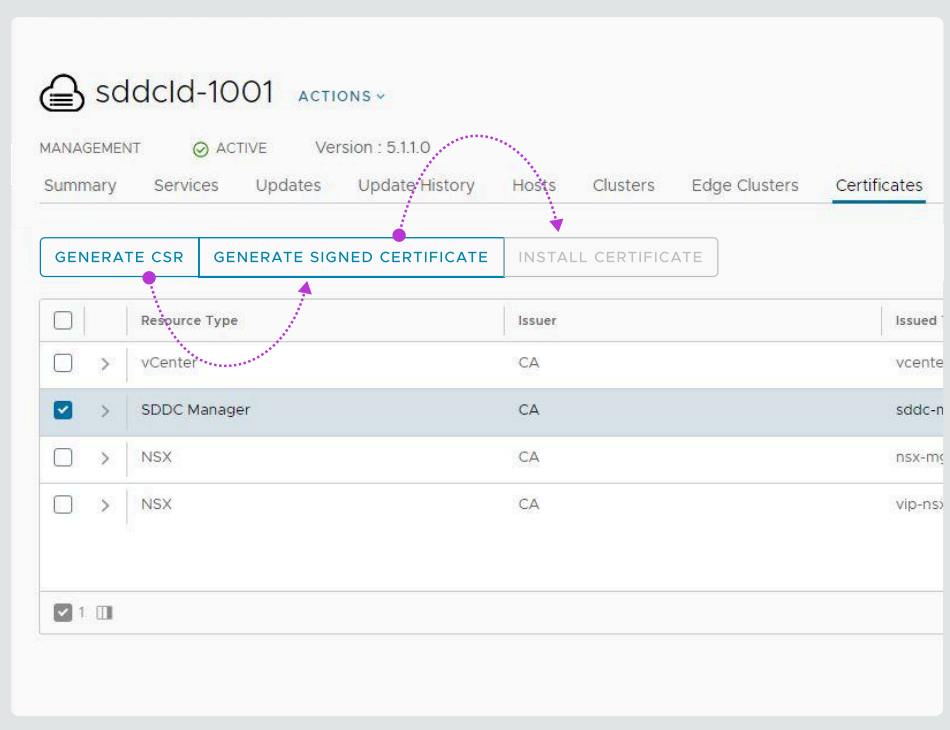
MANUALLY RENEWAL: Renew
Self-CSR Generation

REPLACEMENT:
With Imported Certificate
1 Generate CSR → 2 Import Cert → 3 Replace

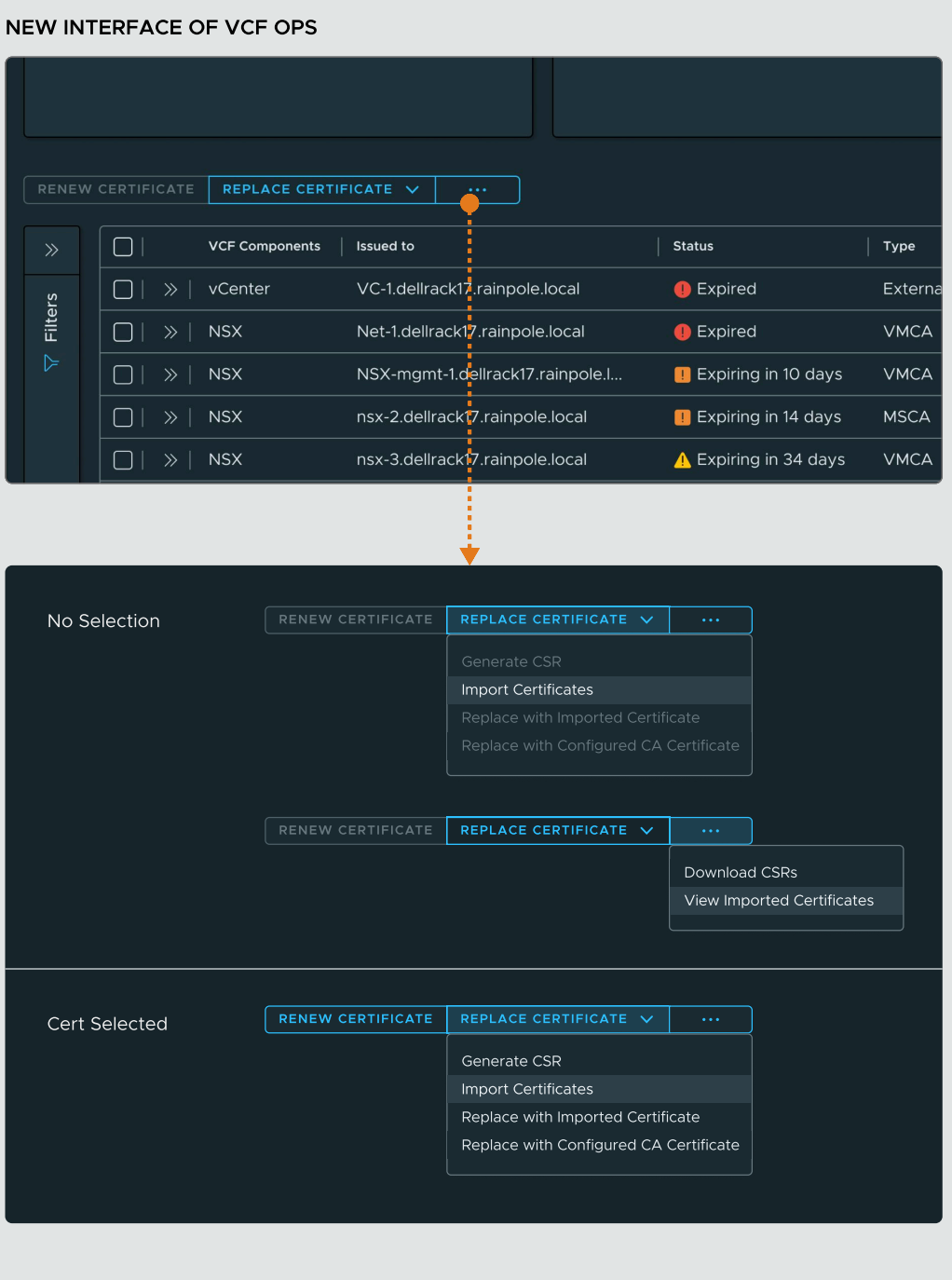
REPLACEMENT:
With Configured CA Certificate
1 Generate CSR → 2 Replace

OLD INTERFACE OF SDDC:

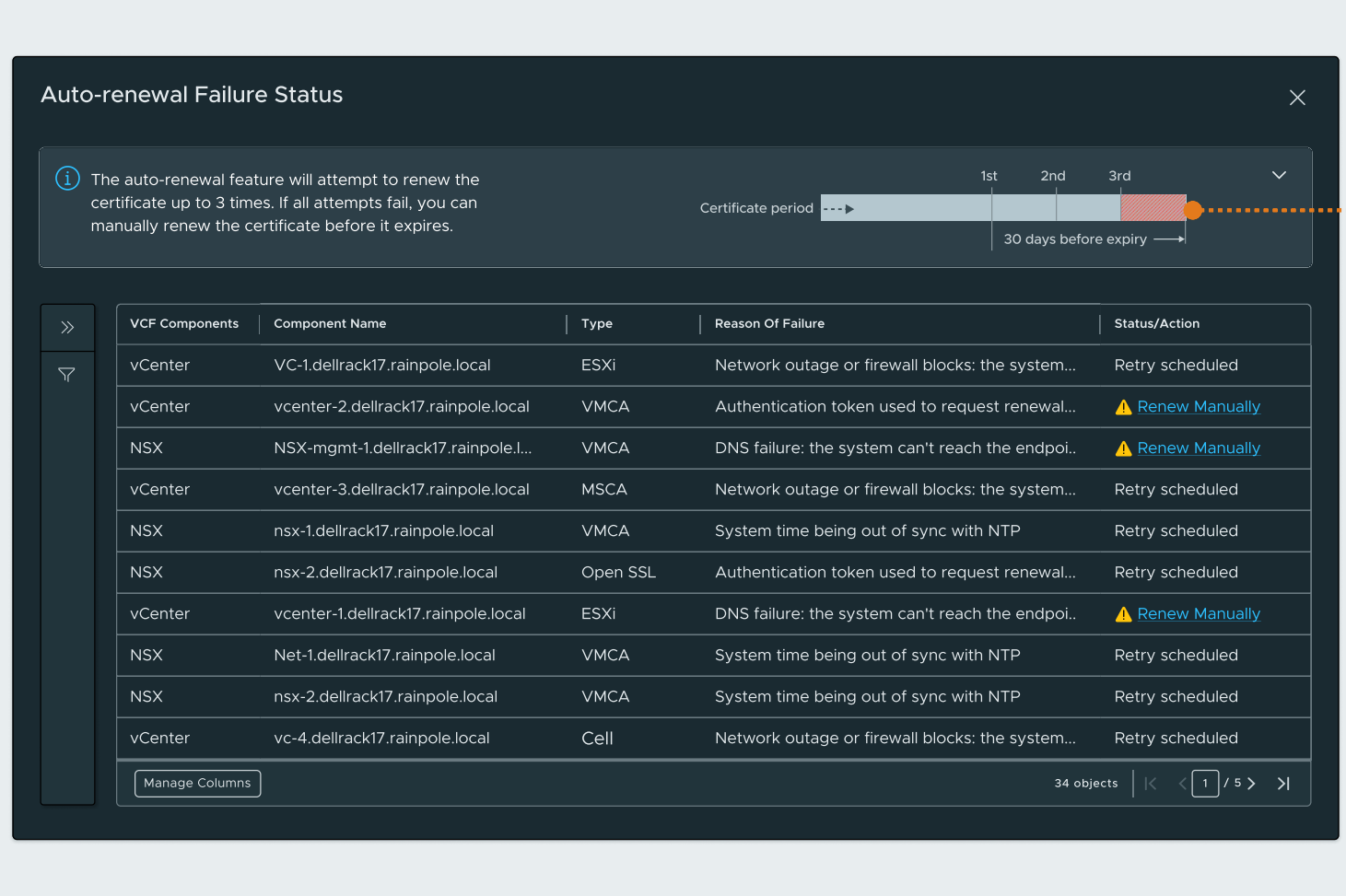
Enabling buttons sequentially works for certificate updates, but it fails a common scenario: if a user generates a CSR for vCenter (activating the first button), then returns days later to replace an SDDC certificate, the second button is enabled even though no new CSR has been generated.


sddcld-1001
ACTIONS
Summary
Services
Updates
Update History
Hosts
Clusters
Edge Clusters
Certificates
GENERATE CSR
GENERATE SIGNED CERTIFICATE
INSTALL CERTIFICATE
Resource Type
Issuer
vCenter
SDDC Manager
NSX
CA

NEW INTERFACE OF VCF OPS


RENEW CERTIFICATE
REPLACE CERTIFICATE
VCF Components
Issued to
Status
Type
No Selection
Cert Selected
Generate CSR
Import Certificates
Replace with Imported Certificate
Replace with Configured CA Certificate
Download CSRs
View Imported Certificates

VCF Components	Component Name	Type	Status
vCenter	VC-1.dellrack17.rainpole.local	Externa	Expired
NSX	Net-1.dellrack17.rainpole.local	VMCA	Expired
NSX	NSX-mgmt-1.dellrack17.rainpole.l...	VMCA	Expiring in 10 days
NSX	nsx-2.dellrack17.rainpole.local	MSCA	Expiring in 14 days
NSX	nsx-3.dellrack17.rainpole.local	VMCA	Expiring in 34 days



Auto-renewal Failure Status

The auto-renewal feature will attempt to renew the certificate up to 3 times. If all attempts fail, you can manually renew the certificate before it expires.

Certificate period 1st 2nd 3rd 30 days before expiry

VCF Components	Component Name	Type	Reason Of Failure	Status/Action
vCenter	VC-1.dellrack17.rainpole.local	ESXi	Network outage or firewall blocks: the system...	Retry scheduled
vCenter	vcenter-2.dellrack17.rainpole.local	VMCA	Authentication token used to request renewal...	⚠ Renew Manually
NSX	NSX-mgmt-1.dellrack17.rainpole.l...	VMCA	DNS failure: the system can't reach the endpoi...	⚠ Renew Manually
vCenter	vcenter-3.dellrack17.rainpole.local	MSCA	Network outage or firewall blocks: the system...	Retry scheduled
NSX	nsx-1.dellrack17.rainpole.local	VMCA	System time being out of sync with NTP	Retry scheduled
NSX	nsx-2.dellrack17.rainpole.local	Open SSL	Authentication token used to request renewal...	Retry scheduled
vCenter	vcenter-1.dellrack17.rainpole.local	ESXi	DNS failure: the system can't reach the endpoi...	⚠ Renew Manually
NSX	Net-1.dellrack17.rainpole.local	VMCA	System time being out of sync with NTP	Retry scheduled
NSX	nsx-2.dellrack17.rainpole.local	VMCA	System time being out of sync with NTP	Retry scheduled
vCenter	vc-4.dellrack17.rainpole.local	Cell	Network outage or firewall blocks: the system...	Retry scheduled

Manage Columns 34 objects 1 / 5

The auto-renewal feature makes its first attempt to renew a certificate 30 days before expiry. If that attempt fails for any reason, it tries again 10 days later.

While it may seem obvious from distinct statuses for auto-renewal attempts versus manual-renewal, a simple graphic here helps customers make more informed decisions and take action more confidently.

5

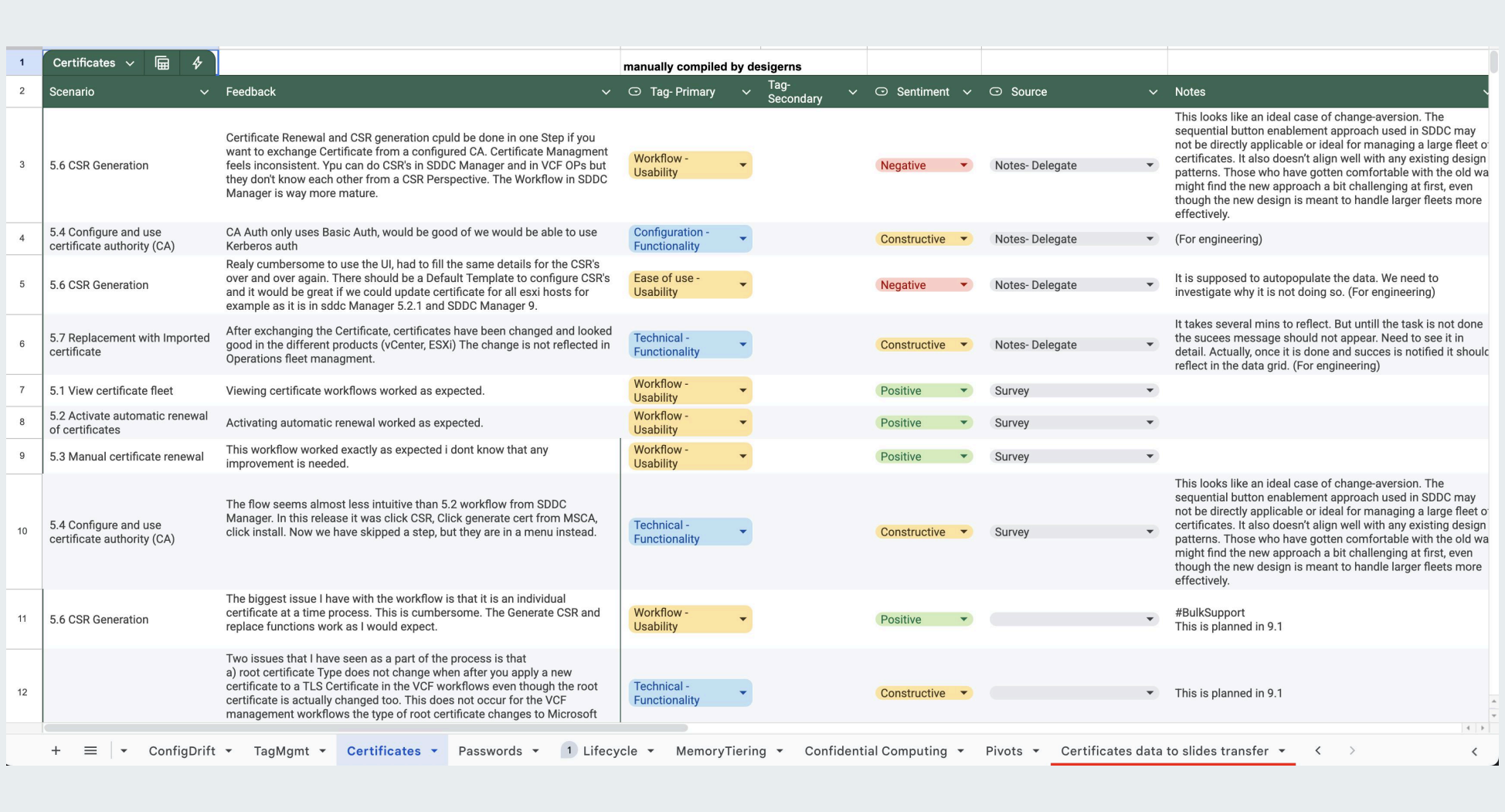
User Feedback From ERP

We conducted an **Early Release Program (ERP)** with a few existing customers to test the design of VCF 9.0. Participants were given access to the interface, and we gathered feedback through group sessions and individual interviews to refine specific areas of the application.

The data indicates that customers appreciated the new integrated design for Certificate and Password Management.

Feedback data says:

25%	Positive feedback
30%	Known issues, already accounted for in the 9.1 release
20%	Engineering implementation issues
15%	Need to go little deeper



Certificates — manually compiled by desigerns

	Scenario	Feedback	Tag-Primary	Tag-Secondary	Sentiment	Source	Notes
3	5.6 CSR Generation	Certificate Renewal and CSR generation cpuld be done in one Step if you want to exchange Certificate from a configured CA. Certificate Managment feels inconsistent. Ypu can do CSR's in SDDC Manager and in VCF OPs but they don't know each other from a CSR Perspective. The Workflow in SDDC Manager is way more mature.	Workflow - Usability		Negative	Notes- Delegate	This looks like an ideal case of change-aversion. The sequential button enablement approach used in SDDC may not be directly applicable or ideal for managing a large fleet of certificates. It also doesn't align well with any existing design patterns. Those who have gotten comfortable with the old way might find the new approach a bit challenging at first, even though the new design is meant to handle larger fleets more effectively.
4	5.4 Configure and use certificate authority (CA)	CA Auth only uses Basic Auth, would be good of we would be able to use Kerberos auth	Configuration - Functionality		Constructive	Notes- Delegate	(For engineering)
5	5.6 CSR Generation	Realy cumbersome to use the UI, had to fill the same details for the CSR's over and over again. There should be a Default Template to configure CSR's and it would be great if we could update certificate for all esxi hosts for example as it is in sddc manager 5.2.1 and SDDC Manager 9.	Ease of use - Usability		Negative	Notes- Delegate	It is supposed to autopopulate the data. We need to investigate why it is not doing so. (For engineering)
6	5.7 Replacement with Imported certificate	After exchanging the Certificate, certificates have been changed and looked good in the different products (vCenter, ESXi) The change is not reflected in Operations fleet managment.	Technical - Functionality		Constructive	Notes- Delegate	It takes several mins to reflect. But untill the task is not done the sucees message should not appear. Need to see it in detail. Actually, once it is done and succes is notified it should reflect in the data grid. (For engineering)
7	5.1 View certificate fleet	Viewing certificate workflows worked as expected.	Workflow - Usability		Positive	Survey	
8	5.2 Activate automatic renewal of certificates	Activating automatic renewal worked as expected.	Workflow - Usability		Positive	Survey	
9	5.3 Manual certificate renewal	This workflow worked exactly as expected i dont know that any improvement is needed.	Workflow - Usability		Positive	Survey	
10	5.4 Configure and use certificate authority (CA)	The flow seems almost less intuitive than 5.2 workflow from SDDC Manager. In this release it was click CSR, Click generate cert from MSCA, click install. Now we have skipped a step, but they are in a menu instead.	Technical - Functionality		Constructive	Survey	This looks like an ideal case of change-aversion. The sequential button enablement approach used in SDDC may not be directly applicable or ideal for managing a large fleet of certificates. It also doesn't align well with any existing design patterns. Those who have gotten comfortable with the old way might find the new approach a bit challenging at first, even though the new design is meant to handle larger fleets more effectively.
11	5.6 CSR Generation	The biggest issue I have with the workflow is that it is an individual certificate at a time process. This is cumbersome. The Generate CSR and replace functions work as I would expect.	Workflow - Usability		Positive		#BulkSupport This is planned in 9.1
12		Two issues that I have seen as a part of the process is that a) root certificate Type does not change when after you apply a new certificate to a TLS Certificate in the VCF workflows even though the root certificate is actually changed too. This does not occur for the VCF management workflows the type of root certificate changes to Microsoft	Technical - Functionality		Constructive		This is planned in 9.1

ConfigDrift · TagMgmt · Certificates · Passwords · Lifecycle · MemoryTiering · Confidential Computing · Pivots · Certificates data to slides transfer

6

Learnings, Refinements & VCF 9.1

These insights helped us fine-tune the design. We made several changes in the design for final GA release, and the remaining refinements are planned for **VCF 9.1 for Certificate & Password Management** with following key learnings:

Auto-renewal is the way to go

Multiple customers have asked to support additional CA-signed certificates in the auto-renewal feature. Since each customer relies on different CAs, they all want their own authorities included for auto-renewal—highlighting a clear need for further automation.

More power to bulk tasks

Due to a technical limitation, bulk actions are currently capped at 15 items per task, which is too low. For environments with many ESXi host certificates, customers must still rely on APIs. We should increase the bulk-action limit to at least 50 items per task.

Simplification

More simplification required in certain areas like 3rd party CA certificate replacement, Policy-driven-control in Password, Certificate Import workflow, etc.

Impact

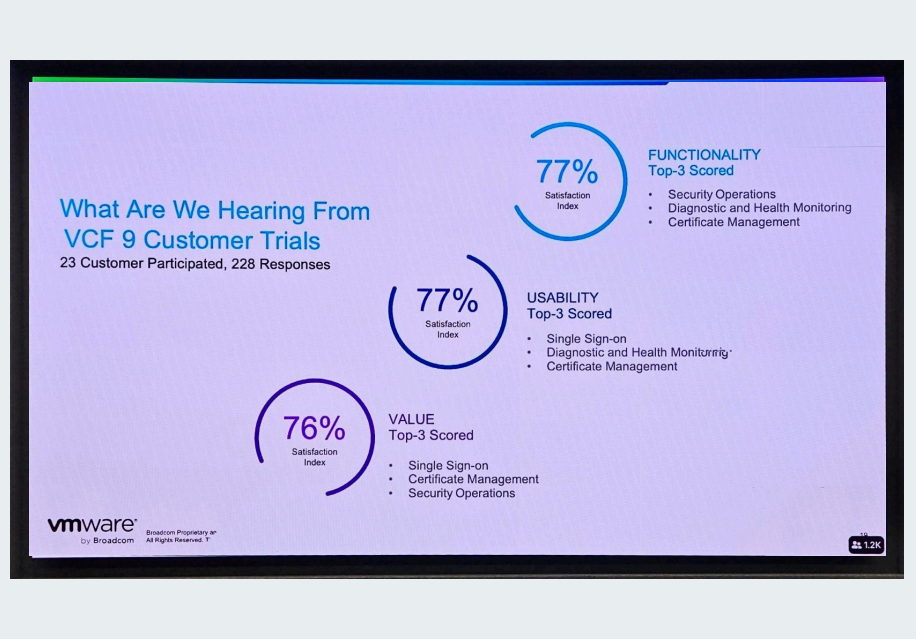
VCF 9.0-GA shipped on June 17 and was very well received—adoption rates have surpassed our expectations. Below are two screenshots from the leadership town-hall presentation, showcasing the design's strong performance on usability, functionality, and overall value satisfaction scores.

Strong Positive Feedback from Trial Customers
Notable Quotes from VCF 9 Customer Trials

FUNCTIONALITY

USABILITY

VALUE



What Are We Hearing From VCF 9 Customer Trials
23 Customer Participated, 228 Responses

77% Satisfaction Index — FUNCTIONALITY Top-3 Scored
- Security Operations
- Diagnostic and Health Monitoring
- Certificate Management

77% Satisfaction Index — USABILITY Top-3 Scored
- Single Sign-on
- Diagnostic and Health Monitoring
- Certificate Management

76% Satisfaction Index — VALUE Top-3 Scored
- Single Sign-on
- Certificate Management
- Security Operations