Beyond High Availability

Designing and Validating Management-Plane Recovery in VMware Cloud Foundation 9.1.x

A framework for recovering the capabilities required to operate a private cloud.

First edition | Version 1.0 | Published October 20, 2026

Zenodo DOI: https://doi.org/10.5281/zenodo.23485597

Reference release: VCF 9.1.1 | Architecture source baseline: VCF 9.1

Paul Bryant | Digital Thought Disruption

Abstract

Applications can remain available while the organization loses the ability to administer infrastructure, investigate incidents, enforce policy, or restore protection. Enterprise recovery planning must establish how management capabilities return, which dependencies must survive, and what evidence supports a return-to-service decision.

This paper develops a capability-oriented assessment framework for VMware Cloud Foundation (VCF) 9.1.x. It connects seven observable capabilities to runtime and recovery dependencies, compares documented recovery models, and shows how to qualify, exercise, and accept a named recovery path. Public vendor sources support product statements; the assessment method and hypothetical examples are proposed by this paper. No laboratory measurements or customer results are reported.

Intended readers: VCF architects, platform owners, operations leads, and recovery planners.

Executive summary

A private cloud can continue serving applications while its operators lose access to the tools needed to investigate an incident, change infrastructure, or restore protection. Management recovery therefore needs its own objectives and acceptance evidence. A running virtual machine, a responding management endpoint, and an administrator able to complete a controlled change establish different outcomes.

VCF 9.1 introduces Management Services and a services runtime for shared functions. Fleet and instance functions can share hosting infrastructure while requiring different recovery procedures. Recovery planning must identify both the scope of each function and the dependencies of its selected recovery path [1].

The framework begins with seven observable capabilities, then maps their normal and recovery dependencies, defines degraded operation, and selects an applicable documented recovery model. An authorized exercise tests the resulting design. The acceptance authority uses the evidence to make a decision for the named failure, baseline, and operating state.

Four evidence dimensions support that decision: vendor documentation, release and topology qualification, observed behavior, and organizational acceptance. The recovery evidence record keeps those dimensions together without treating one as proof of another.

The outcome is a scoped readiness decision and an owned plan to close gaps. The hypothetical Log Management case demonstrates why spare infrastructure and a completed restore task are insufficient: the required fresh event must also become searchable. It remains a planning example, with no executed results. The readiness-decision section defines the decision rules and a practical adoption sequence.

Contents

Executive summary 2
How to use this paper 3
Baseline and evidence boundaries 4
Define what recovered means 5
Map dependencies and failure boundaries 6
Describe degraded operation 10
Establish documented, applicable recovery paths 11
Validate the design in an authorized laboratory 16
Produce a readiness decision 22
Recovery evidence record 25
Laboratory planning worksheet 27
Release and recovery qualification 31
Bounded recovery test library 32
Public source register 33
Component protection and fleet recovery qualification 36

How to use this paper

Begin by defining recovered capabilities, mapping dependencies and failure boundaries, and describing degraded operation. Then compare documented recovery paths, plan an authorized laboratory exercise, and use its evidence to make a readiness decision. The worked Log Management example connects the method to prerequisites, timing, and failed-state capacity.

The supplementary material provides a recovery evidence record, laboratory planning worksheet, release and recovery qualification record, and bounded recovery test library. The public source register records sources and their applicability. Component and fleet qualification notes retain the detailed conditions behind the protection and recovery tables.

Baseline and evidence boundaries

VCF 9.1.1 is the reference release. Broadcom records its general availability on September 3, 2026. The title uses 9.1.x for the architectural subject; component procedures still require release-specific qualification and an inventory of installed builds and deployment history [2].

The VCF 9.1 design distinguishes Management Services in the first VCF instance from services in additional instances. The first combines fleet-level and instance-level functions; additional instances host local functions and can host selected optional services. The dependency-mapping section separates these logical scopes from their hosting infrastructure [3].

The reference release is not a validated compatibility bill of materials. Record source and target builds for Operations, Automation when deployed, Services Runtime, vCenter, NSX, SDDC Manager where relevant, and every protection or external service in the path. KB 449628 documents an Automation-to-Services-Runtime compatibility precheck for VCF 9.1.1.x. It supports recording both versions, not treating every 9.1.x combination as an allowed restore pairing [4].

How statements should be read

Numbered references support vendor-specific statements. Capability definitions, dependency analysis, acceptance criteria, readiness decisions, and laboratory methods are this paper's proposed assessment guidance. Tables distinguish documented conditions from proposed evidence. Hypothetical inputs are not customer facts or test observations.

The platform owner maintains the cross-service readiness view. Service and dependency owners qualify recovery paths and supply evidence; the acceptance authority approves the scoped operating decision. The recovery evidence record defines the supporting responsibilities.

The architectural comparison uses the publisher's VMware Cloud Foundation 9.1.x documentation. Each KB retains its own release scope. The 9.0.x Identity Broker article illustrates an explicit exclusion and supplies no 9.1 recovery instructions [5].

The public source register identifies the consulted editions, access dates, and exact PDF locators. Live topics can change. This assessment framework does not prescribe a universal placement model or component startup sequence. Before execution, resolve the applicable procedure, exact source and target conditions, required artifacts, and current advisories.

Scope and applicability

The framework covers availability failures and operational recoverability of the management plane. It does not establish cyber-clean recovery, forensic preservation, regulatory compliance, or application-data recovery. Suspected compromise requires a separately authorized incident-response and trusted-state recovery process. Technology previews are excluded from production recovery commitments; Broadcom identifies the native GitOps service announced with 9.1.1 as a technology preview [6].

Define what recovered means

Define recovery through an action a named actor must perform. Each acceptance criterion identifies the actor, target, expected result, and evidence. The seven categories below are proposed assessment terms, not vendor service-level definitions. Observe workload behavior alongside management capabilities.

Table 1. Seven capabilities and proposed recovery demonstrations

Capability	Proposed demonstration after recovery	Insufficient evidence on its own
C1 Workload availability	A representative application transaction succeeds from its intended client path.	A VM is powered on or answers a ping.
C2 Administrative access	A fresh authorized session reaches the required endpoint and exercises its intended role.	An existing browser session still works.
C3 Infrastructure management	An approved reversible action changes a designated test object; the resulting state is verified.	Inventory loads or an API accepts a task.
C4 Self-service provisioning	A bounded request obeys required policy, creates the intended resource, and completes cleanup.	A catalog loads or a request enters a queue.
C5 Operational visibility	A fresh event reaches the expected view; its timestamp, source, and required alert delivery are verified.	A dashboard displays historical data.
C6 Security and trust	Intended roles, endpoint trust, and network restrictions hold; an explicitly prohibited test action remains denied.	A privileged user can sign in.
C7 Continued protection	New protection evidence is created and retrievable; its recovery point and required access are identified.	A backup schedule remains configured.

A capability delta is an action unavailable during the named failure that becomes possible after recovery. Each claim should identify this before-and-after observation.

Capabilities can return at different times. An incident statement might accept workload availability and emergency administration while suspending provisioning. Record the permitted state, duration, owner, and restrictions. A successful C7 backup check does not demonstrate a tested restore path.

A read-only query can demonstrate visibility; infrastructure management requires an authorized reversible change and confirmation of its effect. Test permitted and denied actions for security controls, then remove temporary access through the approved process.

Workload availability and management-plane recovery are separate outcomes. A management outage alone does not establish application failure. Observe each through a suitable client path and report its evidence separately.

Recovery objectives and acceptance boundaries

Assign objectives to capabilities. Infrastructure management may be needed to restore services before tenant provisioning resumes; visibility may be needed for diagnosis before historical data returns. The

platform owner and affected service owners set these priorities rather than assigning every appliance the same recovery-time target.

Recovery time objective (RTO) and recovery point objective (RPO) express business tolerance for interruption and lost state. NIST SP 800-34 Rev. 1 provides contingency-planning context for priorities, exercises, and validation. This paper's capability-oriented application is a proposed method, not NIST certification [7].

Define measured intervals before testing. Record injected capability loss, first functional acceptance, completion of the agreed stability interval, and renewed protection separately. Select the milestone that closes the owner's recovery-time objective. Capture detection, decision, prerequisite recovery, restoration, and reconciliation to explain elapsed time. Explicitly record any different business-defined starting event; do not change the clock after testing.

Define the recovered-state boundary. An older configuration can conflict with a recently changed identity, endpoint, or external integration. Acceptance should identify the restored recovery point, consistency checks, and treatment of subsequent changes. A backup schedule alone demonstrates neither the age nor completeness of recoverable state.

A hypothetical capability commitment

Suppose an illustrative commitment requires an infrastructure administrator to regain management of a test cluster within 90 minutes. Acceptance requires a fresh authorized login, current inventory, a reversible change to a designated test object, verification, and cleanup. The owner-selected 90-minute target is hypothetical, not a measured VCF result or universal recommendation.

If fresh login returns at minute 25 but the controlled change, verification, and cleanup finish at minute 110, administrative access returned in 25 minutes and the 90-minute management objective was missed. Stale inventory or an object managed by the wrong endpoint also fails acceptance, even with a responsive UI.

Define a return-to-service condition for normal safeguards. An approved emergency access path or restricted service set may support temporary recovery. Before routine changes resume, address remaining restrictions, audit evidence, backup protection, and ownership of temporary measures. Emergency access does not establish that normal identity integration has recovered.

Map dependencies and failure boundaries

A dependency map asks what must be available for an actor to perform an action during a particular phase. VM placement alone is insufficient. Include the services, data, trust relationships, access paths, and tools required for recovery.

Express each relationship as "A requires B for action X during phase Y." Distinguish normal runtime, authentication, administration, backup, restore, and post-restore reconciliation. Processing existing work may continue without a service needed for configuration or rebuilding state. Phase labels distinguish those dependencies from continuous runtime requirements.

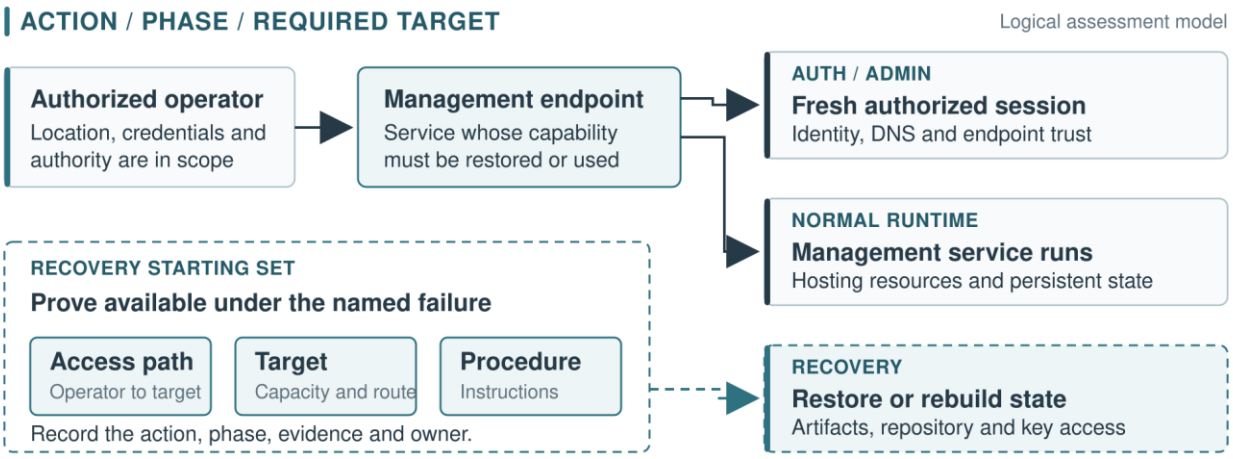


Figure 1. Action- and phase-specific dependency view. Runtime, authentication, and restore prerequisites are distinct; an arrow means that the labeled action requires the target. This is an assessment model, not a deployment topology.

Record each relationship's action, phase, scope, evidence, and owner. Documentation can establish product requirements; configuration inspection can identify actual endpoints; tests can demonstrate consequences of loss. Inferred relationships remain provisional until their practical consequences are established.

Define the recovery starting set: access, artifacts, infrastructure, and information that must survive to begin the procedure. Include the operator. A guide behind failed identity services may be inaccessible; an available API is insufficient without the jump host, credentials, name resolution, or route. Verify the complete authorized path from the operator's actual recovery location.

Protect dependency records and procedure references in a location reachable through the recovery path, and prove operator access during testing. A second copy on the same unavailable storage provides no independent path.

Logical fleet and instance boundaries

In the VCF 9.1 design, fleet lifecycle coordinates lifecycle work; instance-local SDDC lifecycle performs local tasks. Record actual deployment scope for Identity Broker, Software Depot, and real-time metrics because their placement options cannot be inferred from a generic fleet diagram [3].

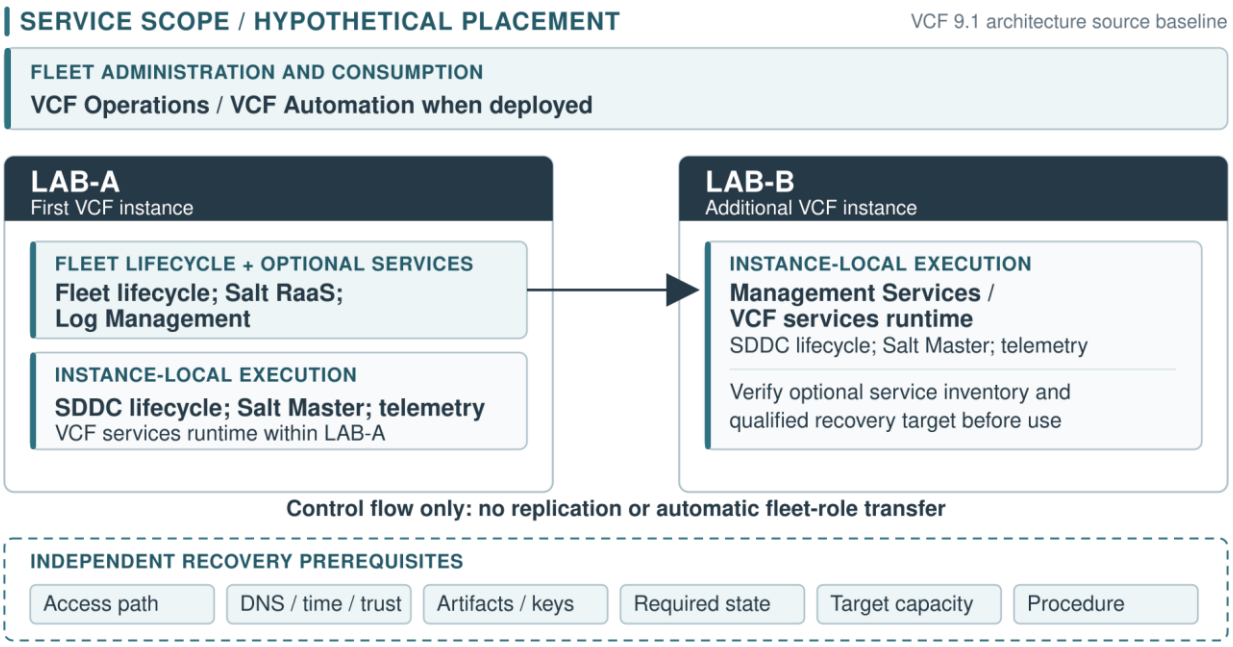


Figure 2. Logical VCF 9.1 service scope with hypothetical LAB-A and LAB-B placement. Lifecycle control flow is not replication or automatic failover. The independent resources and exact recovery target require separate qualification [3].

Distributing local lifecycle execution across instances does not replace a lost fleet function. The recovery target must meet the component-specific conditions in the qualification notes, and external prerequisites must remain reachable through the operator's recovery path.

Capture infrastructure and access dependencies

Start with services implementing the required capabilities and follow their dependencies outward. Replace labels such as "network available" with actual boundaries: administrator to recovery endpoint, restored component to backup repository, and restored component to identity provider are separate paths.

Infrastructure placement and storage

For vCenter, NSX, Management Services, and other in-scope components, record hosting compute, storage, and network resources and their controlling administrative plane. Verify that plane's reachability under the assumed failure. Prove spare recovery capacity, installation-media access, and target-specific constraints before relying on them during an incident.

Include persistent service data and recovery backups in storage dependencies. Demonstrate repository access from the recovery target; access from the normal management node is insufficient. If encryption requires a key, include its authorized access mechanism in the recovery graph and keep secret values out of the evidence matrix.

Identity and trust

Identify the authentication route and fresh-session permissions for each recovery action; an existing browser session can conceal identity failure. For documented, authorized emergency access, record the account type, endpoint, custody, and audit requirements, then validate that route under the intended failure. An account from another release may not exist or have equivalent authority on 9.1.1.

Record name resolution, time synchronization, certificate trust, endpoint names, and external certificate or key services used by the path. Verify required client-server relationships after recovery. A claim that "DNS is redundant" must include the recovery host's resolvers, routing, and required records.

Backup and lifecycle access

Backup protection has its own dependencies. For VCF Operations 9.1.1 and VCF services runtime 9.1.1, KB 443787 identifies SFTP reachability, credentials, capacity, and component health among checks for missing recent runtime backups. Its completion check is a successful manual backup, which does not establish subsequent restore success [8].

Test artifact retrieval and usability separately from backup-task completion. Identify compatible deployment media and recovery tools, access and authorization during an outage, and the owner responsible for acquisition failures.

Separate failure scope from service scope

A single-node test with surviving peers, storage, and networking cannot substantiate recovery from loss of an entire services cluster, management domain, or site. State the failure boundary and surviving dependencies before interpreting results.

Table 2. Failure boundaries and the limits of narrower tests

Failure boundary	Conditions that must be stated	What a narrower test leaves open
Process or service	Named service; node and supporting services remain available.	Loss of the host, persisted state, or recovery interface.
Node or host	Failed member; surviving capacity and shared dependencies.	Cluster-wide loss, common storage, or common network failure.
Cluster or management domain	All included services and remaining external dependencies.	Independent recovery of shared identity, networking, or a second instance.
Network partition	Direction, endpoints, protocols, and duration of isolation.	Total service loss, alternate routing, and conflicting active writers.
Site or shared external service	Lost power, storage, routes, identity, or repository access as applicable.	Recovery when supposedly independent resources share the same cause.

A service can participate in several failure boundaries. A locally hosted fleet function may have broader administrative consequences; establish these per capability and consumer. Shared placement suggests a possible common-cause failure, while shared naming alone proves none.

Find and resolve recovery cycles

In a hypothetical cycle, recovering A requires B, while recovering B requires an operation exposed only through A. The assessment must identify an applicable starting path from the surviving state; changing an arrow's direction does not resolve the cycle.

Candidate starting paths include a documented lower-level interface, an independently available target, or an authorized access route that survives the failure. Qualify each against the product procedure and actual starting state. Without an applicable path, mark the dependency unresolved and the scenario not ready.

Verify every prerequisite from the operator's starting position. An alternate endpoint sharing the failed resolver, credential store, or storage device may preserve the cycle rather than provide an independent path.

Describe degraded operation

A degraded-operation matrix distinguishes continued processing from administration and recovery. Identify what continues, what stops, what becomes harder to diagnose, and which recovery actions remain available. The entries below are hypotheses to investigate, not VCF behavior guarantees.

Table 3. Questions to ask during degraded operation

Hypothetical failure	Capability questions	Candidate surviving actions to verify
Normal identity route unavailable	Do existing sessions differ from fresh logins? Which APIs require new authentication?	A documented and authorized recovery login at the required endpoint.
Management endpoint unavailable	Do representative workloads continue? Which changes, inventory queries, or tasks fail?	An applicable lower-level management or recovery interface.
Logging service unavailable	Is fresh ingestion lost, delayed, or buffered? Is historical search still available?	Independent observations at test sources and recovery components.
Backup repository unreachable	Do current services continue? Can a new backup complete or an existing backup be retrieved?	A documented repository recovery or alternate-copy path.
Management network partition	Which endpoint pairs fail in each direction? Do views of state disagree?	A verified access path from the designated recovery location.
Shared runtime resource pressure	Which services and actions degrade? Is the control interface still usable?	Component-specific diagnosis and an applicable restoration path.

KB 443784 covers component-specific effects of node disk pressure in VCF Operations 9.1.1 and VCF services runtime 9.1.1. It supports evaluating resource pressure without implying a uniform service outage pattern. Identify the affected resource and observe the required capabilities [9].

Measure representative application behavior from a suitable client separately from management behavior. An appliance status page does not establish workload continuity. Record workload placement, traffic paths, dependencies, and test duration to bound the observation.

Choose the observation interval for the failure mechanism. Short tests can miss session expiry, full buffers, or capacity exhaustion. Disclose longer-duration behavior that remains untested.

Two public examples of recovery boundaries

Identity Broker and release applicability

KB 436356 describes Identity Broker recovery to a different management domain for VCF Operations 9.0.x and explicitly excludes 9.1. Component names alone therefore cannot establish that a procedure applies to a newer release [5].

For 9.1.1, start with the documented VCF 9.1 recovery models, then qualify the executable identity procedure and target separately. Do not borrow the older KB's deployment steps, account assumptions, or target behavior. A documented design pattern is distinct from a qualified procedure.

Proposed acceptance uses a fresh session, exercises the required authorized role, and verifies that an intentionally unprivileged test identity cannot perform the protected action. This tests the intended access model, not merely restored access. These are this paper's functional tests, not steps from the excluded KB.

Log Management and useful function

KB 436904 describes VCF 9.1 Log Management reconciliation after restoration to a new or rebuilt Management Services cluster. It requires previously configured NFS storage access where applicable and checks completion through new searchable logs. Bundle and verification-artifact locations remain placeholders in the inspected public article [10].

In a proposed test, generate a uniquely identifiable, harmless event after restoration from a designated laboratory source. Find it through the normal investigation path and correlate source identity and timestamps. This demonstrates useful function beyond task completion. Check historical search and post-recovery ingestion separately when both are required.

The test covers only its named sources, paths, and observation interval. Fleet-wide ingestion, historical completeness, and sustained throughput require broader evidence. The worked E02 planning example develops the complete planning decision.

Establish documented, applicable recovery paths

Select the recovery mechanism for the failed capability before writing a procedure. The mechanisms below have different state assumptions and therefore need different evidence. A design can combine them, but it should identify where one mechanism ends and another begins.

Table 4. Recovery mechanisms require different evidence

Mechanism	State assumption to establish	Evidence required for the selected path
High availability or restart	Sufficient surviving infrastructure and recoverable service state remain.	Applicable behavior, surviving dependencies, and functional continuation or restoration.
Backup and restore	A usable protected state exists and can be applied to an allowed target.	Backup identity, integrity, required secrets, compatible target, restored state, and reconciliation.
Failover	An alternate service or site can take the intended role with an acceptable state.	Applicable failover procedure, activation conditions, prevention of conflicting control, and return path.
Rebuild or redeployment	Required configuration and integrations can be re-established.	Installation media, exact configuration inputs, identity and trust restoration, state-loss boundary, and acceptance.

Recovery scope and mechanism are separate decisions. A component restore, a same-site instance recovery, and recovery of fleet functions in another instance solve different problems. The VCF design blueprints below make those distinctions explicit. Restored fleet administration does not, by itself, recover the failed site's local infrastructure or business applications.

Qualify a recovery path against the official procedure, release, topology, protection method, source state, and target restrictions. Preserve requirements for coordinated recovery, source isolation, credentials, and integration repair. A plausible command sequence is insufficient.

Mark the documentation applicable only when vendor guidance and environment evidence establish those conditions. Missing authoritative evidence means needs validation; a documented exclusion means explicitly excluded.

Documented VCF recovery models

Table 5 paraphrases the VCF 9.1 design blueprints. Its first two columns describe documented models; the decision questions are this paper's guidance. These models do not by themselves qualify a 9.1 procedure for an installed 9.1.1 build.

Table 5. VCF recovery models and the decisions they support

Documented model	Recovery boundary and conditions	Architectural decision question
Component Backup and Restore [11], [12]	Selected management components in a management or workload domain; component-specific file-based and image-based protection.	Which state is protected, and can the individual service be recovered without rebuilding its hosting instance?
Instance Backup and Restore [13]	Recovery of the failed VCF instance in the same site. The operational preparation guidance requires the failed environment's IP address, network, storage, appliance-size details, exact builds, and file-based backups from the same backup window. An isolated test is therefore an assessment requirement, not a vendor-stated alternate restore target [13], [14].	Can the same-site foundation, exact media, backups, required identities, and captured environment details be re-established without colliding with an active source?
Fleet Disaster Recovery [15]	Recovery of designated fleet functions in another VCF instance or location. Different components use different recovery methods.	Which shared capabilities must move, what must already exist at the destination, and which source resources remain unrecovered?

Protect the state required by the selected model

Table 6 summarizes the documented protection methods. The component qualification notes retain the detailed conditions and proposed acceptance checks. A backup method alone establishes neither an allowed target nor an executable, build-qualified restore path [11], [12].

Table 6. Component protection methods and qualification priorities

Component or service	Protection starting point and detailed qualification
vCenter Server	File-based or image-based; the design recommends file-based backup [11], [12]. Detailed qualification.
SDDC Manager	File-based or image-based; the instance-recovery guide uses file-based backup. The 9.1.1-and-later file-based instance-recovery path requires separate credential protection [11], [12], [14]. Detailed qualification.
NSX Manager and NSX Edge	Manager file-based backup includes Edge configuration, but not Edge VM binaries. Lost Edges require redeployment; Manager or Edge snapshot and cold-clone restores are unsupported [12], [16]. Detailed qualification.
VCF Operations	Coordinated image-based protection of all nodes. Offline backup is recommended; online backup must not use file-system quiescing. Avoid the dynamic-threshold window [11], [12]. Detailed qualification.
VCF Operations for Networks	Image-based protection [11], [12]. Detailed qualification.

Component or service	Protection starting point and detailed qualification
VCF services runtime and Management Services components	Separate file-based protection applies to the runtime and named services. Log Management backup excludes log data; three services are captured only by scheduled backup [12]. Detailed qualification.
VCF License Server	The design directs new deployment and licensing reconfiguration. Use the release-specific deployment task [11], [12], [17]. Detailed qualification.
VCF Automation	File-based protection [11], [12]. Detailed qualification.

In VCF 9.1, the operational backup guidance configures an SFTP destination and component schedules for Automation and Management Services. It also requires safe custody of the encryption passphrase for restoration. Confirm the artifacts and component results actually produced; neither a runtime inventory entry nor a schedule proves that all required service state is recoverable [18].

Recover fleet functions by component

The fleet blueprint assigns different methods and target conditions to different components (Table 7). The fleet-recovery qualification notes retain the detailed constraints. These conditions apply to that documented model [15].

Table 7. Fleet recovery methods and destination conditions

Fleet component	Recovery method and target	Functional evidence
VCF Operations; VCF Operations for Networks	VCF Protection and Recovery replication with recovery plans, or image-based restore. Both methods require IP mobility [15].	Qualify mobility, network controls, consistency, failover, and failback. Verify collection, object association, and alerts separately for each product. Detailed qualification.
VCF Operations, Continuous Availability alternative	One cluster across two fault domains, with a witness in a third location. One-domain loss is tolerated in a degraded state; an inter-site partition requires manual return and resynchronization, and both-zone loss requires restoration from backup [15], [19].	Qualify placement, failed-state capacity, connectivity, latency, and resynchronization. Demonstrate the named failure and retain a separately qualified backup path. This alternative is documented only for VCF Operations. Detailed qualification.
VCF Automation	Deploy a new instance at the recovery site and restore its backup. This method has no IP-mobility requirement [15].	Verify authorized tenant access and a governed disposable request, including policy, resulting resources, and cleanup. Detailed qualification.
Management Services fleet components: Identity Broker, fleet lifecycle, Software Depot, Salt RaaS, Log Management	Restore individual components onto the recovery site's existing Management Services instance. No IP mobility is required; Identity Broker and Software Depot must be absent from that target [15].	Validate each function and its consumers through fresh access, a bounded lifecycle or configuration transaction, or fresh log ingestion. Detailed qualification.

Reserve a qualified destination, including its service inventory. Do not remove an existing Identity Broker or Software Depot to force a target fit without an independently authorized design and applicable procedure.

A method without an IP-mobility requirement still needs DNS, routing, certificates, endpoint reconciliation, and authorized access.

The fleet model recovers specified fleet functions; it is not a blanket relocation plan for vCenter, NSX, ESXi, or applications. Record fleet administration, failed-instance infrastructure recovery, and business-application recovery separately. The instance blueprint's same-site model and the fleet blueprint's recovery-site model must not be interchanged [13], [15].

Prove prerequisites before sequencing recovery

Derive the recovery sequence from the surviving state and dependencies under the named failure. Identify the first authorized operation, then establish prerequisites for each subsequent operation. Preserve component-specific ordering from the applicable guidance. A generic rule such as "identity first" can fail when identity recovery depends on a management interface or host that is unavailable.

The execution record identifies the procedure revision or access date, exact source and target versions, backup or deployment artifacts, access, network and storage prerequisites, and expected state after each material transition. Mark dependencies that must already exist and link those recovered earlier to their own recovery records.

Verify the recovery target

Qualify the target's builds, service inventory, endpoint identity, permitted addressing changes, data and artifact access, operator access, and failed-state capacity. Include licensing and software acquisition. A new cluster or site is not automatically an allowed target.

Before replacing an active service, identify the authoritative instance and follow the selected procedure's isolation or shutdown requirements. Include evidence that the old and recovered instances cannot perform prohibited conflicting operations. The framework prescribes no universal fencing command.

Preserve state relationships

Component and consumer backups may represent different times. Identify shared objects and relationships that require consistency and the documented restoration or reconciliation method. Compare object identity, registrations, role mappings, or a controlled transaction across the relationship; matching names alone is insufficient.

Record post-backup changes and whether each test change should survive, be lost, or be reconstructed. Derive that expectation from the protection model and procedure.

Reconcile and protect the recovered state

Restored consumers may retain obsolete addresses, credentials, certificates, or registrations. Verify both sides of each relationship through the selected procedure and a bounded transaction. Reconcile interrupted tasks with actual infrastructure before retrying; a failed console task may still have created an object requiring cleanup.

Broadcom KB 443506 covers supporting fleet failover and failback scripts for VCF 9.1.0.x and 9.1.1. Its listed tasks include component registration, Identity Broker instance association, and virtual IP updates. It limits use to the TechDocs procedures that reference those scripts. This is evidence of context-specific reconciliation, not authority to use the scripts for arbitrary relocation [20].

Make renewed protection an acceptance milestone

Measure renewed protection separately from first functional acceptance. Verify the new artifact or replication state, recoverable point, retrieval and key access, and owner. A service can pass an immediate capability test while remaining unprotected against the next incident.

Repository behavior also needs evidence. In VCF 9.0 and 9.1, NSX retention values are not natively enforced, so backups can accumulate until an external job or manual process removes them. Broadcom documents nsx_backup_cleaner.py; validate its retention period, minimum-count behavior, execution status, retained restore points, and repository capacity [21].

Treat failback as a separate controlled change

The recovery environment may accumulate newer configuration and credentials. Before reconnection, identify authoritative state and establish the applicable transfer or reprotection method, target prerequisites, dependency order, and acceptance tests. Retain source isolation until authorized reconnection. Powering on an old appliance does not reconcile its state.

A stop condition requires reassessment. Before an irreversible action, establish the next applicable option, such as a documented retry, another qualified recovery point, or redeployment. Suspected compromise requires incident-response direction before reconnection.

Recovery assessment sequence

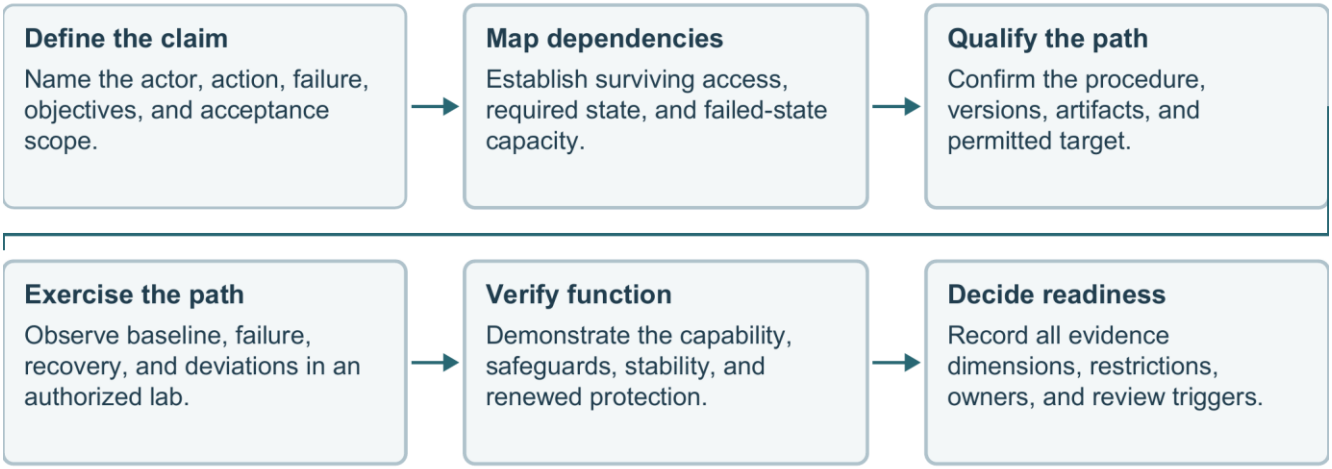


Figure 3. Proposed recovery assessment sequence. Each stage produces evidence for the named capability. Failed prerequisites or acceptance conditions require reassessment; this is not a universal component startup order.

Make the recovery evidence matrix the decision record

Create one evidence record per service, failure boundary, and recovery path. Node loss, state corruption, management-domain loss, and site loss require distinct claims even when they share source references.

The central observation is the capability delta: what action becomes possible after recovery that could not be demonstrated during failure? Reference observations from both phases. If an action continued during failure, record continuity and choose a different observation to demonstrate recovery.

Table 8 contains planning records. The worked E02 planning example develops prerequisites, test design, and a justified not-ready decision.

Table 8. Illustrative recovery evidence matrix

ID / service	Named failure and capability delta	Documented starting point and evidence to close
E01 / Identity Broker	Normal authentication unavailable; a fresh authorized session and required role action return.	Management Services protection and fleet-target conditions. Qualify the 9.1.1 procedure and target, then record C2 and C6 observations [11], [15].
E02 / Log Management	Original hosting cluster unavailable; a new post-recovery event becomes searchable.	Management Services protection plus the scoped reconciliation advisory. Close exact-build and target qualification, authenticated package acquisition, backup and secret access, and any configured NFS dependency required for restart; then run the proposed C5 fresh-ingestion test in the worked E02 planning example. Historical recovery requires separate evidence when included [10], [11], [12].
E03 / vCenter	Specified management service lost; a reversible change succeeds and its state is verified.	Select the documented backup method and actual component restore procedure. Qualify target identity, builds, consumer relationships, and C3 [11].
E04 / NSX management	Named management path unavailable; the authorized change and intended effect return.	File-based NSX management protection. Qualify the component procedure and separately record C1, C3, and C6 as selected [11].
E05 / Services Runtime backup	Repository unreachable; fresh protection can again be created and retrieved.	Scoped backup-dependency advisory. Demonstrate C7 after repository recovery; record backup restoration separately [8].

The recovery evidence record includes the four evidence dimensions, capacity, renewed protection, failback, owners, and closure evidence. Link executable steps to a controlled runbook rather than duplicating vendor instructions in the matrix.

Validate the design in an authorized laboratory

A laboratory exercise tests a claim under controlled conditions. It should reproduce the dependencies relevant to that claim and deliberately document the differences from production. A smaller environment can answer a precise question, but it cannot establish all consequences of a larger topology or the time needed to recover it.

Establish the experiment before causing the failure

The experiment owner records authorization, the exact builds, the services and data in scope, and permission to retain or publish results. Use isolated test identities, disposable objects, and non-sensitive event content. Confirm the recovery artifacts and an authorized access route before starting. Record how to stop the injection and recover the laboratory if the normal path fails.

Define the failure precisely enough for another operator to reproduce it. "Turn off management" is not a sufficient instruction. The approved test procedure should identify the node, process, route, resource, or service being affected, the method of injection, its duration, and the dependencies intentionally left available. Failure injection itself must be appropriate for the product and environment; the framework does not authorize arbitrary destructive experiments.

Observe each phase independently

First, collect a baseline showing the relevant capabilities work. Then introduce the agreed failure and verify that the intended boundary was actually affected. Record both failed and continuing actions. Use observations from a location that is not dependent solely on the service being tested, otherwise loss of telemetry may be mistaken for loss of the underlying workload.

Execute the selected recovery procedure from the operator's declared starting position. Record prerequisite repairs, waiting periods, retries, errors, and any deviation. A successful result that depended on an undeclared administrator session, manually supplied artifact, or surviving service should be recorded with that dependency rather than presented as an autonomous recovery.

After the restore task or failover action completes, perform the acceptance tests. Verify current function, relevant restored state, intended authorization, and consumer integration. Continue observations for the agreed interval. Capture failures even if a later retry succeeds, so the result distinguishes transient recovery from stable operation.

The experiment ends with cleanup and confirmation of the laboratory's intended final state. Restore approved test settings, remove disposable objects, account for temporary access, and verify any required backup protection. If the procedure cannot return to the original state, record the rebuild or other approved recovery path before the experiment starts.

Design tests that answer distinct questions

Test A Restore authorized administrative access

The hypothetical claim is that an administrator can regain a specified management capability when the normal identity route is unavailable. The preconditions are an applicable documented recovery route, approved credentials, a named endpoint, and verified access from the designated recovery workstation. No account behavior from the 9.0.x Identity Broker KB is assumed for 9.1.1.

Establish baseline fresh logins with the permitted and intentionally unprivileged test identities. Introduce the approved identity-path failure and repeat the login attempts in new sessions. Record existing-session behavior separately. Recover through the selected route, then demonstrate the required role and the expected denial for the unprivileged identity. If only emergency access works, accept that specific capability and leave normal identity integration open.

Stop if the experiment affects an unauthorized identity domain, loses the only viable recovery path, or produces access outside the approved test scope. Rollback means withdrawing the injection and following the pre-established identity recovery procedure. It does not mean disabling security controls until a login succeeds.

Test B Restore useful logging

The hypothetical claim is that the required logging path works after the selected restore procedure. Establish a baseline event from the designated source and record its event identifier, generation time, arrival time, and searchable representation. Prepare the applicable recovery artifacts and any required external storage before introducing the approved failure.

Generate separate, distinguishable events before the failure, during the failure, and after recovery. Search for each according to the intended retention and delivery expectations. The post-recovery event demonstrates fresh function. The other events help distinguish lost history, delayed delivery, and restored ingestion. A missing during-failure event should be reported against the actual protection or buffering expectation, not automatically called a failed restore.

Stop if the experiment reaches unintended data, storage, or tenants. Return through the selected recovery or rebuild path and retain the minimum evidence needed to explain the result. Do not invent a replacement script when the vendor's required artifact cannot be obtained.

These exercises answer distinct questions. The worked E02 plan below shows how the logging criteria are used to make a design decision. The laboratory planning worksheet records observations; the bounded recovery test library extends coverage while retaining each capability's required demonstration.

Worked planning example: E02 Log Management recovery

E02 is a hypothetical planning assessment. It shows how an architectural recovery model becomes a decision about prerequisites, test scope, and required evidence. No actual builds, customer environment, measured durations, or executed results are supplied.

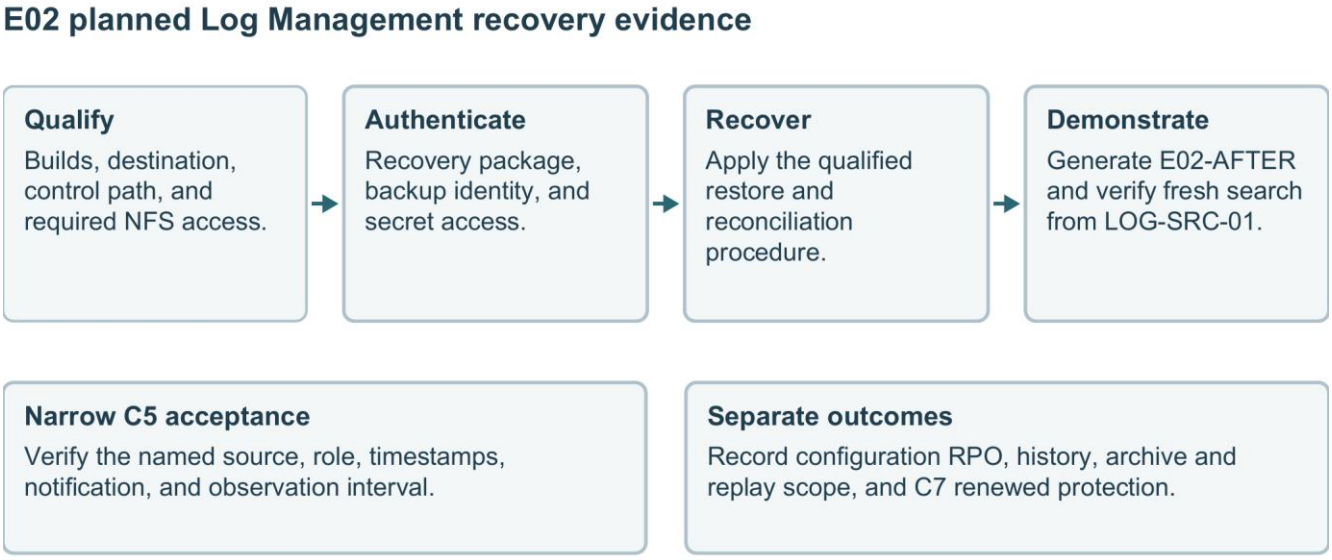
Claim, failure, and operator starting position

The claim is that an investigator can regain fresh log search after the original Management Services cluster, LAB-MS-A, becomes unavailable and Log Management is restored onto a qualified new or rebuilt cluster, LAB-MS-B. The assessment references VCF 9.1.1; KB 436904 is scoped to VCF 9.1, so exact-build applicability remains open. This component claim does not establish full-instance or site recovery [10].

Table 9. E02 inputs and their evidence class

Input class	Scenario input	Decision consequence
Surviving services	The authorized operator starts from RECOVERY-WS. Operations access, laboratory infrastructure, DNS, time, and identity survive independently or are recovered under separate records.	These are assumed prerequisites, not results proved by the Log Management exercise.
Backup, storage, and source	SFTP-01 holds the selected component backup; its identifier and recoverable point are unqualified. NFS-01 is a previously configured path. LOG-SRC-01 supplies test events.	Qualify the backup and builds. If restart requires NFS-01, qualify its role, protocol, export, permissions, capacity, and runtime-network path. Indexed history and external archives remain separate.
Execution blockers	The backup is reachable, but the authenticated recovery package has not been acquired. NFS-01 is unreachable from LAB-MS-B; its restart requirement is unresolved.	Obtain the package and determine whether NFS is required. When required, prove target access to the supported configured export before injection.
Unconfirmed environment	Source and target Log Management, Services Runtime, and Operations builds; backup metadata; target topology; and configured NFS details.	Complete the release and recovery qualification record before selecting the executable procedure. No exact combination is qualified in this example.
Owner decisions	Configuration RPO; indexed-history coverage; external archive retrieval or import; E02-DURING treatment; permitted gaps; delayed delivery or replay.	Mark each included, excluded, or awaiting a decision. A fresh-ingestion result establishes none of these separately scoped outcomes.
Illustrative objectives	Fresh-event search within 90 minutes of capability loss; acceptance events searchable within two minutes; a further 15-minute observation interval.	Planning assumptions only. The service owner selects actual targets and the acceptance authority approves them. These are not vendor limits or measurements.

The NFS path is conditional. For the VCF Operations for Logs 9.1 scope in KB 418135, configured external storage supports NFS v3, not NFS v4; traffic originates from Management Services runtime VMs. Qualify the path's archive, export, or import role, export, write access, capacity, reachability, and actual source and target builds. When required at restart, it is an execution prerequisite even if historical recovery is excluded. Indexed service state, optional external storage, and the component backup have separate evidence paths [10], [22], [23].



Hypothetical planning flow. E02 remains not ready; no exercise result or approval is represented.

Figure 4. Planned E02 evidence flow, with no executed result. Required NFS access must be resolved before restart when the selected procedure needs it. Fresh C5 ingestion, historical-data acceptance, and renewed protection remain separate outcomes. Arrows indicate assessment flow, not replication or automatic failover.

Prerequisites and the recovery design decision

KB 436904 describes reconciliation, but its recovery-bundle, detached-signature, and public-key locations remain placeholders. The link to KB 142814 gives generic portal instructions. Obtain release-matched artifacts from an authoritative Broadcom source or Support and validate the publisher key and signature. Management Services control-plane access and the previously configured NFS path, when applicable, are also required [10].

The service owner qualifies builds, package applicability, and adopted history criteria. The storage owner qualifies the NFS role, protocol, export, permissions, capacity, and runtime-network path; the platform owner qualifies LAB-MS-B and the control path. The protection owner supplies backup and secret-access references. Close applicable prerequisites before authorizing the experiment. An unsourced script, empty replacement share, or removal of a target service is not an accepted workaround.

E02 remains not ready, so failure injection is postponed. In an incident, preserve available state and seek applicable recovery direction. The unreachable NFS path blocks execution only when required by the recovered configuration. Unresolved artifacts and exact-build applicability are evidence gaps, not proof that the product is universally unsupported.

Proposed execution after the prerequisites close

Table 10. E02 proposed sequence and evidence

Phase	Planned action and evidence	Acceptance or stop condition
Baseline	Generate E02-BEFORE from LOG-SRC-01. Preserve its identifier, source timestamp, successful search, agreed role, and notification path.	Verify the starting capability. Stop before injection if access, artifacts, required storage, backup, secrets, or target qualification is incomplete.
Failure observation	Inject only the authorized LAB-MS-A failure. Generate E02-DURING and record generation and search results independently.	E02-BEFORE tests historical-query continuity. Searchable E02-DURING establishes fresh-ingestion continuity. Do not assume buffering or later delivery.
Recovery and reconciliation	Use the qualified procedure and verified package. Retain backup identity, task state, actions, prerequisite repairs, and deviations.	Stop for untrusted artifacts, unreachable required data, conflicting authoritative instances, or impact outside the lab boundary.
Narrow C5 acceptance	Generate E02-AFTER after recovery. Verify event identifier, source, generation and search timestamps, content, intended role, notification, and observation interval.	A pass establishes only the named fresh-ingestion and search claim. It does not establish RPO, history, archive handling, E02-DURING delivery, or replay.
Broader return to service	For adopted scope, verify configuration RPO, indexed-history interval, E02-BEFORE and E02-DURING, gaps, delay or replay, authorization, notification, and archive retrieval or import.	Record separate results. Mark items outside the narrow C5 scope explicitly excluded or awaiting an owner decision. C5 alone does not close broader acceptance.
Protection and final state	Create fresh protection through the selected supported method. Verify its identity, recoverable point, retrieval, and key access. Remove disposable content where permitted and close temporary access.	C7 demonstrates the newly protected state; restoring that new backup is a separate test. If the qualified return path is unavailable, retain the approved isolated state and escalate.

The capability delta is a fresh post-recovery event becoming searchable when that action was unavailable during failure. Record history, archives, during-failure delivery, alert routing, authorization, and renewed protection separately. Restored configuration and reachable NFS alone do not establish historical search.

Completed planning disposition

Table 11. E02 planning assessment and operational disposition

Evidence dimension	E02 planning assessment
Vendor documentation	A VCF 9.1 design model and Log Management advisory are identified. Exact 9.1.1 execution conditions remain unqualified.
Release and topology qualification	Not completed. Actual builds, target suitability, backup metadata, and package applicability are not supplied.
Observed behavior	Not run. Event identifiers and timing targets describe the proposed exercise.
Organizational acceptance	Not sought or represented. Named roles do not establish approval.

Evidence dimension	E02 planning assessment
Operational disposition	Not ready for the named scenario. Execution prerequisites remain open and C5 is unobserved and unaccepted. Broader configuration, history, archive, E02-DURING, and replay boundaries require explicit owner decisions.
Closure evidence	Dated build and target qualification; authenticated artifact, backup, and secret access; required NFS evidence; then distinct narrow C5 and adopted return-to-service results from Table 10. Record acceptance separately.

The immediate work is to qualify the destination and make the documented path executable. Additional recovery compute does not close the missing artifact, access, or qualification evidence.

How the decision could change

The following continuation is conditional. If exact-build and target qualification confirms an applicable path, the authenticated artifacts and secrets are accessible, and any required NFS dependency is proven from LAB-MS-B, the plan could proceed to an authorized exercise. Those prerequisites alone would not make E02 ready.

A future exercise that demonstrates E02-AFTER ingestion and search from LOG-SRC-01, with the adopted role, notification, timing, stability, and safeguards, could support the narrow C5 claim only after all four evidence dimensions are complete and the acceptance authority records its decision. Historical coverage, archive handling, E02-DURING delivery, replay, and C7 must retain their own results. A restricted decision would require an independently qualified, demonstrated, and accepted narrower scope; an unmet mandatory condition would keep the affected claim not ready. No such results or approval are asserted here.

Interpret observations and timing correctly

Preserve the failure, method, build, prerequisites, observations, and limits of each result. A successful node-restart test does not establish management-domain or site recovery.

Record capability loss, detection, authorization, prerequisite recovery, restore completion, reconciliation, first functional acceptance, stability completion, and renewed protection. Report functional recovery and renewed protection separately, with clock sources and timestamp uncertainty.

A synthetic timing example

The following values are illustrative arithmetic, not laboratory measurements. A test loses a required capability at minute 0. Detection and the decision to recover take 8 minutes. Prerequisite recovery takes another 12 minutes, the restore task takes 25 minutes, and reconciliation and functional acceptance take 10 minutes. The first functional acceptance is therefore at minute 55: 8 + 12 + 25 + 10. A further 15-minute successful observation interval ends at minute 70. If verified renewed protection is established at minute 85, report that separate 85-minute interval and the 30 minutes after first functional acceptance during which renewed protection was not yet established.

Under an objective defined as first successful functional acceptance, the result would be 55 minutes. Under an objective requiring completion of the stability interval, it would be 70 minutes. Reporting the 25-minute restore-task duration as total capability recovery would omit material work. When tasks overlap, use the actual timeline and the dependency path that controls completion; do not simply add every task duration.

Record the selected backup and verified recoverable point, deliberate post-backup changes, and state recovered, missing, duplicated, or reconciled. Job frequency and a backup-file timestamp alone do not establish the recovered application's consistent state.

Include assisted and failed attempts. An artifact supplied outside the planned path is a dependency. If a failed attempt changes state, explain the next attempt's starting condition and which evidence remains comparable.

Evaluate capacity in the failed state

Identify the chain controlling elapsed recovery time, including access, media staging, prerequisite recovery, restoration, reconciliation, and acceptance. Use observed durations when available; label unmeasured inputs as assumptions. Include waits for authorization, repositories, and qualified operators.

Parallel restoration saves elapsed time only when tasks are independent and shared resources sustain their combined demand. Higher concurrency can instead queue work at repositories, storage, networks, or endpoints. Reassess the controlling path and measure contention when concurrency changes.

Account for all demands on surviving resources

For each resource, compare surviving usable capacity with continuing demand, recovery execution, permitted overlap, and operating reserve. Evaluate CPU, memory, storage space, storage performance, and network throughput separately. Do not add unlike units or treat configured vCPUs as measured CPU demand.

Table 12. Demand on surviving resources

Demand	Evidence to collect in the named failed state
Continuing services	Demand from the recovery platform and workloads that must remain active.
Recovery execution	Restore throughput, write load, network traffic, and management-task load at the proposed concurrency.
Temporary overlap	Resources for staged media, isolated test copies, old and replacement components, and intermediate artifacts where the procedure permits them.
Operating reserve	Remaining headroom for the stated additional failure, maintenance, or rebuilding condition required by the design.

The owner selects reserve requirements using measurements and applicable guidance; this framework sets no universal percentage. State whether usable storage reflects the protection policy and whether rebuilding competes with restore work. Operator and approval availability can constrain the timeline even when hardware has spare capacity.

Test demand on the surviving topology. Pre-failure capacity or a smaller laboratory does not establish production recovery margin. Record those differences, and include the resources and time needed for renewed protection and the return path.

Produce a readiness decision

Evaluate each recovery claim through four independent evidence dimensions: vendor documentation, release and topology qualification, observed behavior, and organizational acceptance. Table 13 identifies the record required for each dimension.

Table 13. Four independent evidence dimensions

Evidence dimension	Required record
Vendor documentation	Applicable procedure, release scope, prerequisites, exclusions, and unresolved authoritative clarification.
Release and topology qualification	Actual source and target builds, deployment model, partner or hardware conditions, and exact check inputs and results.
Observed behavior	Test boundary, date, observations, capability results, timing, deviations, and stability evidence.
Organizational acceptance	Acceptance authority, accepted capability, service objective, residual restrictions, and expiry or review trigger.

Record a status and its conditions for every dimension. For documentation, use applicable, explicitly excluded, or needs validation. For observed behavior, use not run, passed, failed, inconclusive, or no longer representative. A successful observation does not establish that the procedure applies to the environment.

Then assign one operational disposition for the named capabilities, baseline, failure boundary, and operating state: ready for the named scenario, ready with restrictions, or not ready for the named scenario. Table 14 defines these decisions.

Both ready dispositions require complete evidence in all four dimensions for the exact approved scope. A narrower claim must independently satisfy those requirements. Neither organizational approval nor a successful test can override a vendor exclusion. Risk acceptance records residual-risk ownership; it cannot establish vendor support, complete missing qualification, or replace a required test.

Table 14. Operational disposition is separate from evidence status

Operational disposition	Decision rule	Restriction boundary
Ready for the named scenario	The documented method is applicable; the exact environment is qualified; mandatory capabilities and objectives are demonstrated; safeguards and acceptance are recorded.	Valid only for the named baseline, failure boundary, capabilities, and observation period.
Ready with restrictions	A separately scoped, narrower claim independently satisfies all four evidence dimensions and is accepted by the acceptance authority.	Record restrictions, compensating measures, expiry, and excluded capabilities. Do not use this label to waive a vendor exclusion or an untested required path.
Not ready for the named scenario	A required path, qualification, prerequisite, objective, capability result, or acceptance remains missing, contradicted, or failed.	Preserve any successful observations, but do not promote them into the broader unproven claim.

Apply the decision to E02

E02 remains not ready. Its execution prerequisites are unresolved, no recovery test is represented, and acceptance has not been sought. The worked E02 planning example records the blockers, narrow C5 claim, and broader return-to-service boundaries. Assigned owners must close execution prerequisites before the experiment begins.

Keep the decision current

Revisit affected records after relevant version, placement, network, identity, backup-location, or procedure changes. Identify altered dependencies and acceptance criteria, refresh the affected release and recovery qualification records, and retest affected claims. Preserve earlier results with their original scope; they remain evidence only for those conditions.

Table 15 assigns responsibilities for maintaining readiness. The acceptance authority must cover the affected service commitment and temporary restrictions. Record vendor and partner escalations separately. Give each open item an accountable owner, required closure evidence, a checkpoint, and a review trigger.

Table 15. Ownership keeps evidence current

Stage	Primary responsibility	Readiness evidence
Design and prepare	Platform and service owners record scope, documented recovery models, independent access, protection artifacts, and destination conditions.	Dependency map and protection configuration exist; every recovery prerequisite has an owner. Deployment completion is not recovery acceptance.
Qualify and exercise	Service and dependency owners qualify the path. The experiment owner governs scope and evidence; the operator runs the exercise; the acceptance authority approves the disposition.	Version and topology evidence, observations, objectives, safeguards, and disposition are recorded together.
Maintain readiness	Service owners reassess changed records and exercise affected failure boundaries at an approved cadence.	Current procedure and artifact access, fresh protection, retained observations, and explicit retest triggers.

Scope adjacent services explicitly

Include AI services, VMware vSphere Kubernetes Service (VKS), HCX, or consolidation only when they depend on an in-scope capability. Record the action, versions, and supporting evidence; qualify any extension of the recovery claim.

Distinguish a running transaction from provisioning or repair. For HCX, name the migration or management operation being assessed. For consolidation, assess shared dependencies and a qualified recovery target against the named failure and required capabilities. These boundaries define the assessment; they do not establish release-specific recovery behavior.

Conclusion and practical adoption

Management-plane recovery is demonstrated when the required operator can perform the agreed action through the recovered environment, with the necessary safeguards and evidence. The framework turns that outcome into a scoped decision that owners can maintain as the platform changes.

1. Start with one business-critical recovery scenario. Name the service, failure boundary, required capabilities, objectives, acceptance authority, and accountable owners. Use the recovery evidence record to document the claim.
2. Qualify the recovery path and close its execution prerequisites. Map the dependencies, confirm the applicable procedure and exact environment, and use the laboratory planning worksheet to plan an authorized exercise.
3. Record the exercise evidence, make the scoped readiness decision, and assign closure work and retest triggers. Expand to other scenarios using the same evidence standard; carry forward only the results that apply to each new scope.

Recovery evidence record

Use one record per service, failure boundary, and recovery path. Store secret values in the authorized credential system and record access references only. The worked E02 planning example illustrates the assessment; the schema below supports adoption with actual environment evidence.

Table 16. Recovery evidence record: claim and dependencies

Field	Required entry
Record and claim	Unique ID; service; actor; capability being claimed.
Exact baseline	Product release; component builds; deployment form and history; runtime role; source and target versions; qualification-record reference.
Failure boundary	Failed resources or paths; cause modeled; duration; dependencies intentionally surviving.
Scope	Affected fleet, instance, domain, cluster, tenant, or endpoint; named exclusions.
Capability during failure	Actions attempted; successes and failures; timestamps; evidence locations.
Recovery mechanism	Restart or HA, restore, failover, rebuild, or an explicitly described combination.
Applicable procedure	Official source and exact section; version scope; access date; controlled runbook reference. Do not mark an inaccessible procedure verified.
Protection and artifacts	Protection method; backup ID and recoverable point; media and tool versions; integrity evidence.
Target restrictions	Allowed placement and versions; target service inventory; endpoint identity; addressing; capacity and documented constraints.
Prerequisites	Identity, DNS, time, certificates, routes, storage, keys, repository, tools, and operator access relevant to this path.
Dependency evidence	Owner, phase, source, availability, and linked recovery record; failed-state capacity and recovery concurrency evidence.
Procedure transitions	Starting state; material actions; expected resulting state; authoritative instance and consumer handling.
Post-recovery capability delta	The action now possible; test input; expected output; evidence; scope and stability interval.
State validation	Required history or configuration; expected searchable interval and permitted gaps when historical data is in scope; cross-component consistency; post-backup changes; discrepancies.

Record the following outcome and acceptance fields alongside the claim and dependency fields. Together they form one evidence record.

Table 17. Recovery evidence record: outcome and acceptance

Field	Required entry
Objectives and timing	RTO/RPO definitions and targets; failure, task, capability, stability, and renewed-protection timestamps.
Authorization and stop conditions	Approved scope; operator; stop triggers; applicable rollback or forward-recovery path.
Vendor documentation	Applicable, explicitly excluded, or needs validation; exact source conditions and missing clarification.
Release and topology qualification	Qualification-record reference; exact inputs, result, conditions, date, and owner.
Observed behavior	Not run, passed, failed, inconclusive, or no longer representative; observations, deviations, and evidence.
Organizational acceptance	Acceptance authority; accepted capability or unresolved condition; restrictions and expiry.
Renewed protection and return	Artifact or replication evidence; recoverable point; authoritative state; failback procedure and acceptance reference.
Operational disposition	Ready, ready with restrictions, or not ready for the named scenario; scope, reason, and acceptance authority.
Closure and review	Accountable owner; required evidence; closure date; review or invalidation trigger.

Responsibilities

The service owner owns the recovery claim and procedure. Dependency owners supply identity, network, storage, protection, and other prerequisite evidence. The experiment owner governs authorized test scope and the evidence record; the operator executes the exercise. An accountable owner closes a named gap and is distinct from the acceptance authority unless local governance explicitly combines them. The acceptance authority approves the disposition and residual restrictions. The platform owner maintains the cross-service view.

Applying the record to E02

Use the worked E02 planning example as a structure, replacing its assumptions with actual builds, backups, storage paths, operators, procedures, and criteria. Keep execution prerequisites separate from fresh C5 acceptance and broader return-to-service evidence.

For E02, preserve distinct E02-BEFORE, E02-DURING, and E02-AFTER events. Record generation and search results, source identity, timestamps, and required notification. A historical query does not establish fresh ingestion; do not assume buffering or eventual delivery.

Record the component-state recovery point, searchable history interval, permitted gaps, external archive handling, delayed delivery, and replay expectations separately. Mark each as included, excluded, or awaiting an owner decision. A configured NFS path required at restart remains an execution prerequisite regardless of historical-recovery scope.

Record all four evidence statuses before assigning readiness. Not run, not qualified, and acceptance not sought are valid planning states; they cannot support a ready claim requiring those results. Never convert an absent result into a pass.

Laboratory planning worksheet

Experiment ID: _____ Experiment owner: _____

Date and approved window: _____ Operator: _____

Claim and scope

Capability, actor, action, and target to demonstrate:

_____

_____

Exact release, component builds, source and target placement, and scenario boundary:

_____

_____

Applicable procedure, public source, section, access date, and runbook reference:

_____

_____

Preconditions

Table 18. Evidence required before failure injection

Item to establish	Evidence reference or remaining gap
Authorization, publishable-result permission if needed, and isolated test data	
Baseline functional test and designated disposable objects	
Applicable backup or rebuild artifacts, integrity checks, and recovery point	
Operator access under the assumed failure, including required credential access	
Recovery target, capacity, storage, network, naming, time, and trust prerequisites	
Independent observation path and timestamp convention	
Prevention of conflicting active control where required by the procedure	

Injection and acceptance

Approved failure method, affected boundary, surviving dependencies, and duration:

Expected failed and continuing actions; post-recovery test and stability interval:

Stop conditions, rollback or rebuild procedure, and operator responsible:

Laboratory observation and decision worksheet

Experiment ID: _____ Evidence location: _____

Table 19. Laboratory observation timeline

Phase	Time and observation	Evidence reference
Baseline		
Failure introduced and verified		
Capability loss or continuity observed		
Recovery authorized and started		
Prerequisites restored		
Restore or failover task completed		
Reconciliation completed		
Functional acceptance first passed		
Stability interval completed		
Renewed protection verified		
Cleanup and final-state verification		

Interpret the result

What can be demonstrated after recovery that could not be demonstrated during failure?

_____

_____

_____

_____

Recovered state, missing or delayed data, restored relationships, and authorization results:

_____

_____

_____

_____

Assistance, deviations, failed attempts, and limits on extrapolating this result:

_____

_____

_____

_____

Record the decision

Observed result: _____ Documentation applicability: _____

Qualification record: _____ Acceptance authority: _____

Operational disposition and exact scope: _____

Unresolved condition, accountable owner, evidence needed, and closure date:

_____

_____

_____

Return-path reference, accepted restriction, and review trigger:

_____

_____

_____

Release and recovery qualification

Qualify each recovery claim independently. The paper's release label does not establish a deployment pairing. Complete source and target inventories, including dependencies that remain unchanged, before selecting an executable procedure.

Table 20. Source and target inventory

Inventory field	Information to record
Platform and runtime	VCF release/build; Management Services runtime and hosted service versions; fleet or instance role; SDDC Manager where present.
Infrastructure	vCenter Server, ESXi, NSX, and storage versions/builds; service placement; source and target identities; network and storage assumptions.
Operational services	Operations node membership and availability configuration; collectors; Log Management; Automation; relevant integrations and their releases.
Deployment history	Initial deployment or upgrade; previous releases; migrations, restore history and unresolved changes that affect the selected path.
Protection and partners	Backup, replication and recovery products/builds; plug-ins; backup format and age; repository, catalog, encryption and retention dependencies.
Hardware and external services	Relevant server/device models, drivers and firmware; identity, DNS, time, certificates, keys and privileged-access systems; owners and recovery access.

Create one qualification record per consequential question. A general compatibility statement cannot close a different question about a restore destination, recovery artifact or required sequence.

Table 21. Reproducible qualification record

Qualification field	Entry to complete
Exact question	State the pairing, permitted destination, recovery method, upgrade history or prerequisite being assessed.
Authoritative source	Canonical official URL and section, applicable release, or partner requirement; retain the supporting evidence.
Selected inputs	All products, versions/builds, topology options, and device combinations used in the check. For a configured Log Management NFS path, include the protocol, archive, export, or import role, server and export identity, required permissions and capacity, network origin of the Management Services runtime, and source and target builds.
Result and conditions	Actual returned result, exclusions, prerequisites, and unresolved conflicts. Distinguish an unavailable source from an explicit exclusion. For the NFS path, record export visibility, required write access, capacity, reachability from the Management Services runtime network, whether the same configured path is available from the target cluster, and any source or target build-scope gap.
Date and owner	Access/check date; evidence location; accountable owner; trigger for reassessment.
Disposition	Applicable within recorded conditions, excluded, or unresolved; link the affected recovery evidence record.

Broadcom distinguishes software interoperability and upgrade-path checks in its matrix guidance [24]. Hardware qualification uses separate server and I/O-device criteria [25]. Record these results independently. This worksheet contains no qualified pairing or hardware result; refresh affected checks when the baseline or destination changes.

Bounded recovery test library

These proposed exercises inherit the authorization, isolation, preconditions, stop rules, and recovery requirements defined for laboratory validation. Select the failure boundary and exact baseline before execution. A tabletop discussion or prerequisite check is not an executed capability-recovery test.

Table 22. Bounded recovery test library

Exercise	Capability IDs	Proposed acceptance evidence
T01. Identity interruption	C2, C6	Use a fresh authorized session through the approved path; verify its intended role and denial of a prohibited action. Record emergency access use and closure.
T02. Infrastructure control	C1, C3	Record representative workload transactions during the failure. After recovery, complete an authorized reversible change on a disposable object, verify the changed state, reverse it, and verify cleanup.
T03. Monitoring recovery	C5	A fresh controlled state change produces current collection data and the expected alert or monitor result. Verify source identity, timestamps, and required notification delivery.
T04. Management Services recovery	C3, C6	Verify the selected service, inventory ownership, and permissions; reconcile interrupted tasks. Execute a permitted reversible management change on a disposable object, verify the result, reverse it, and confirm expected denial for an unprivileged identity.
T05. Log ingestion recovery	C5	Generate a unique event after recovery and find it through the intended search path. Correlate source and timestamps and verify the required test notification. Record history and delayed delivery separately.
T06. Provisioning recovery	C4, C6	A bounded request follows intended approval and policy rules, creates the correct disposable object, and completes cleanup. Confirm the prohibited request or action is denied.
T07. Repository or recovery-key unavailability	C7	Restore authorized access to the repository or recovery key through the qualified alternate path, then complete and retrieve a new backup. If the injected failure also blocks administrative authentication, assess C2 in a separate linked record.
T08. Recovery destination	C2, C3, C6	Compare destination inventory and registrations with the qualified plan. Authenticate freshly, execute and reverse a permitted change on the intended disposable object, and verify trust and expected access denial.
T09. Network and trust recovery	C1, C3, C6	Verify representative application transactions, required existing and new flows, denial of a prohibited flow, and endpoint trust. Execute a bounded reversible management change through the recovered route and verify cleanup.
T10. Protection and return	C3, C7	Use the separately qualified return path. After return, verify an authorized reversible management change and renewed protection, its recoverable point, and retrieval/key access. Record restoration of that new protection separately.

Mappings identify candidate coverage. Apply every selected capability's acceptance criterion in Table 1, including the reversible change required for C3. Record unmet criteria, timing, and limitations alongside successes. Component, instance, and fleet results remain separate.

Public source register

Each entry retains its recorded inspection date, September 22 or October 19, 2026. References follow first-use order and identify source scope, sections, and relevant restrictions. The consulted PDF edition is identified at the end of this register. Figures are newly drawn conceptual views; no vendor diagram, screenshot, or recovery script is reproduced.

VCF 9.1 documentation | VCF 9.1.1 release notes | Canonical publisher PDF

[1] S. Pareek and V. Kondeti, "Modernizing Infrastructure: VMware Cloud Foundation 9.0.x to 9.1 Upgrade Guide," VMware by Broadcom, July 28, 2026.

VCF 9.1; section "What's New." Architectural transition only, not a disaster-recovery runbook. Accessed September 22, 2026.

[2] Broadcom, "Correlating VMware Cloud Foundation version with the versions of its constituent products," KB 314608.

Section "Supported VCF 9.X Releases," 9.1.1 row. The release date does not establish an installed bill of materials. Publication/revision date not stated in the inspected article. Accessed September 22, 2026.

[3] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Design, "VCF Management Services Component Detailed Design," pp. 1976-1979, tables 611-614.

The online topic and October 19, 2026 canonical publisher PDF identify the first and additional VCF instance models. Accessed October 19, 2026.

[4] Broadcom, "VCF Automation upgrade precheck fails with 'Target VCF Automation 9.1.#.#.###### requires VCF services runtime version 9.1.#.#.######'," KB 449628.

VCF 9.1.1.x; Environment, Cause, and Resolution. Establishes a version-coupling precheck, not every permitted restoration combination. Publication/revision date not stated. Accessed September 22, 2026.

[5] Broadcom, "Restore and failover of VCF Identity Broker (vIDB) to a different Management Domain in VCF Operations 9.0.x," KB 436356.

Operations 9.0.x; Environment and opening Resolution restriction. Explicitly not for Operations 9.1. Used as a release-exclusion example only. Publication/revision date not stated. Accessed September 22, 2026.

[6] R. Walsworth, "Announcing General Availability of VMware Cloud Foundation 9.1.1," VMware by Broadcom, September 3, 2026.

VCF 9.1.1; "New GitOps Service [Tech Preview]: Argo CD, Native in VCF." Supports the preview-scope boundary, not production recovery qualification. Accessed September 22, 2026.

[7] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, Contingency Planning Guide for Federal Information Systems, NIST SP 800-34 Rev. 1, May 2010, updated November 11, 2010.

Sections 3.2, 3.5, and 4.4: business impact analysis, testing, training, and exercises, and reconstitution. General contingency-planning context; not VCF guidance or evidence of compliance. Accessed September 22, 2026.

[8] Broadcom, "[9.1.1] VCF services runtime is missing recent successful backup," KB 443787.

VCF Operations 9.1.1 and VCF services runtime 9.1.1; Cause and Resolution. Backup dependencies and backup-task completion, not proof of restoration. Publication/revision date not stated. Accessed September 22, 2026.

[9] Broadcom, "[9.1.1] VCF Management Services Node Resource Usage Approaching Capacity," KB 443784.

VCF Operations 9.1.1 and VCF services runtime 9.1.1; Issue/Introduction and Environment. Component-specific impacts of disk pressure. Publication/revision date not stated. Accessed September 22, 2026.

[10] Broadcom, "Log Management does not come back online after restoring it to a new management services cluster," KB 436904.

VCF 9.1; prerequisites, Resolution, and Additional Information. A previously configured NFS path must be accessible from the new or rebuilt cluster. The public article's bundle, detached-signature, and public-key entries remain placeholders; KB 142814 is generic portal guidance, not an artifact locator. Execution requires release-matched artifacts from an authoritative Broadcom source or Support and successful publisher-key and signature validation. Accessed October 19, 2026.

[11] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Design, "VCF Component Backup and Restore," canonical PDF pp. 1612-1617; Figure 214, pp. 1614-1615; tables 466-468.

Architecture and design methods and recommendations, VCF Operations image-backup precautions, and the License Server deploy-and-reconfigure starting point. Design evidence is not patch-qualified execution guidance. PDF created October 19, 2026. Accessed October 19, 2026.

[12] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Fleet Management, "Component Backup and Restore of VMware Cloud Foundation," canonical PDF pp. 4270-4271; section "Backup Methods for VMware Cloud Foundation."

Current operational per-component backup matrix and caveats, including separate Management Services protection, the Log Management log-data exclusion, and scheduled-backup conditions for named services. The live topic was last updated October 19, 2026. Accessed October 19, 2026.

[13] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Design, "VCF Instance Backup and Restore," canonical PDF pp. 1617-1622, tables 469-472.

The design topic describes same-site instance recovery. Operational source and target inputs are documented separately in [14]. Isolated restoration is an assessment constraint, not a vendor-stated alternate destination. PDF created October 19, 2026. Accessed October 19, 2026.

[14] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Fleet Management, "VCF Instance Backup and Restore" and "On-Demand Backup of SDDC Manager Credential Store."

VCF Instance Backup and Restore | Back up the SDDC Manager credential store

VCF 9.1.x; 'Backup Methods for VMware Cloud Foundation,' PDF p. 4271; 'VCF Components to Back Up,' pp. 4333-4334; 'Preparing for Restore of the VCF Instance,' table 1158, p. 4338; 'Management Domain Restore Plan,' pp. 4338-4339; and the credential-store task, p. 4281. Establishes the file-based scope used by the instance-recovery guide, the VCF 9.1.1-and-later credential-database exclusion, conditional mandatory API export, secure JSON storage, at-least-daily automation recommendation, and recovery input. Accessed October 19, 2026.

[15] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Design, "VCF Fleet Disaster Recovery," canonical PDF pp. 1622-1629; recovery-method matrix p. 1623 and target-component footnote p. 1624.

Component-specific methods, IP-mobility conditions, destination-service restrictions, and the Continuous Availability alternative for VCF Operations. Design evidence is not patch-level execution qualification. PDF created October 19, 2026. Accessed October 19, 2026.

[16] Broadcom, "NSX Edges are in Failed or Unknown state after NSX restore from backup," KB 411895.

VMware NSX; Cause and Resolution. Establishes that NSX backup captures configuration and state rather than Edge VM binaries, that lost Edge nodes require redeployment, and that cold-clone or snapshot-based restores of NSX Manager and Edge VMs are unsupported. Publication/revision date not stated in the inspected article. Accessed September 22, 2026.

[17] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Fleet Management and Licensing, License Server redeployment, deployment, registration, and license-management tasks.

Redeploy License Server | Deploy License Server 9.1.1 | Register with Business Services Console | Add or import licenses | Update usage and license files

VCF 9.1.x; redeploy p. 4429; deploy 9.1.1 pp. 4228-4231; Business Services Console registration pp. 2684-2685; license add/import pp. 2688-2689; usage and license-file updates pp. 2694-2698. Establishes release-specific redeployment, unique time-bound registration-key and VCF Operations connection requirements, Business Services Console registration, license addition or import, and connected or disconnected workflows. Accessed October 19, 2026.

[18] VMware by Broadcom, VMware Cloud Foundation 9.1, Fleet Management, "Configure an External SFTP Server for VCF Management Services and VCF Automation Backups" and "Configure File-Based Backup Schedule for VCF Management Services and VCF Automation."

Configure the SFTP destination | Configure component backup schedules

The online topics identify SFTP configuration, safe passphrase custody, and per-component scheduling. Current PDF pp. 4272-4273 and schedule beginning p. 4276. Actual component results must be inspected. Accessed October 19, 2026.

[19] VMware by Broadcom, VMware Cloud Foundation 9.1.x, Design, "Continuous Availability VCF Operations Model," pp. 2018-2026, table 660, and Deployment, "Configure VCF Operations Cluster for Continuous Availability," pp. 2539-2542, tables 966-967.

Continuous Availability design | Configure the Continuous Availability cluster

Design prerequisites, latency and placement, one-fault-domain behavior, partition handling, and the whole-deployment loss boundary. Accessed October 19, 2026.

[20] Broadcom, "Supporting Scripts for VCF Fleet Disaster Recovery Failover and Failback," KB 443506.

VCF 9.1.0.x and 9.1.1; Issue/Introduction, Environment, and Resolution. Scripts are restricted to the TechDocs contexts referencing them. Publication/revision date not stated. Accessed September 22, 2026.

[21] Broadcom, "NSX Backup Retention Settings in SDDC Manager Not Applied in VCF 9.0 and 9.1," KB 442696, and VMware by Broadcom, VMware Cloud Foundation 9.1, "Remove Old Backups."

NSX retention advisory | Remove old backups

VCF 9.0 and 9.1; retention values are not natively enforced, and current TechDocs p. 3843 documents the backup-cleaner control. No retention period is prescribed by this paper. Accessed October 19, 2026.

[22] Broadcom, "VCF Operations Log Management service instances remain offline for longer than expected," KB 424379.

VCF Operations Log Management 9.1; Cause and Resolution. Service state resides in persistent volumes; the article distinguishes optional external NFS paths used for archive, export, or import. Accessed October 19, 2026.

[23] Broadcom, "VCF Operations for Logs: Services Not Running and NFS Mount Inaccessible," KB 418135.

VCF Operations for Logs 9.1; Environment, Cause, and Resolution. For this scope, external storage supports NFS v3 and not NFS v4. A configured archive, export, or import mount can prevent affected pods from starting when inaccessible. External-storage traffic originates from the Management Services runtime VMs; qualify export visibility, write access, capacity, network reachability, and actual source and target builds. Accessed October 19, 2026.

[24] Broadcom, "Using the VMware Product Interoperability Matrixes," KB 343230.

Resolution: interoperability and upgrade-path checks. Explains the resource; no pairing is matrix-validated by this whitepaper. Accessed October 19, 2026.

[25] Broadcom, "Checking ESXi Host Compatibility before Upgrade Using the Broadcom Compatibility Guide," KB 381824.

Resolution and Additional Information: server and I/O-device qualification. No hardware, driver, or firmware combination is validated by this whitepaper. Accessed October 19, 2026.

Source edition and applicability

PDF locators refer to the canonical publisher edition titled VMware Cloud Foundation 9.1.x, created October 19, 2026, containing 9,189 pages and downloaded October 19, 2026. SHA-256: 42f90ae154fa2e76996453aa592e24673da3658f4d5400c059da0ee2d94b362f. Live topics remain mutable. These sources establish the cited design and backup guidance, but do not certify a complete 9.1.1 command sequence, product pairing, hardware combination, or recovery-time result. Add current component procedures and exact environment qualification to the adopted record.

This is an independent technical paper. Product names identify the subject matter and do not imply endorsement or validation by Broadcom. No customer architecture, contractual commitment, or executed laboratory result is represented.

Component protection and fleet recovery qualification

This appendix expands Tables 6 and 7. Documented methods and restrictions retain their source references; qualification and acceptance criteria are this paper's proposed assessment guidance. A listed backup method does not establish an allowed recovery target or a build-qualified procedure [11], [12], [15].

vCenter Server

The design blueprint and operational matrix list file-based or image-based protection for vCenter Server; the design recommends file-based backup [11], [12].

Record the selected method, backup identity and recovery point, encryption-passphrase access when applicable, source and target builds, target restrictions, and consumer registrations. Execute the applicable restore procedure and verify fresh administrative access, a reversible management action, and renewed protection.

SDDC Manager and credential protection

The operational matrix lists file-based or image-based protection, while the instance-recovery guide uses file-based backup [11], [12], [14]. For VCF 9.1.1 and later, that guide directs regular Credentials API backup because the credentials database is no longer included in the SDDC Manager backup. The linked task makes API backup mandatory when no external password vault is available, directs secure storage of the JSON, and recommends external automation at least daily. Restore preparation requires the latest Credentials API backup [14].

Record the installed release and build and the selected backup method. For the documented 9.1.1-or-later file-based instance-recovery path, preserve the latest Credentials API export or a verified external-vault recovery path containing the required material. Demonstrate independent authorized access from the recovery starting set. When the SDDC Manager backup is encrypted, preserve its backup passphrase through an independently accessible path. The documented credential-database exclusion must not be extended to image-based protection without method-specific evidence.

NSX Manager and NSX Edge

NSX Manager uses file-based backup. Edge configuration held by NSX Manager is included, but Edge VM binaries are not. Lost Edge nodes must be redeployed through the applicable VCF or NSX recovery workflow. VM snapshots and cold-clone restores of NSX Manager or Edge appliances are unsupported [12], [16].

Qualify Manager restoration and Edge redeployment separately. Verify Manager and Edge cluster health, policy, routing adjacencies, representative forwarding, and the authorized management action.

VCF Operations image protection

VCF Operations uses image-based protection, with all cluster nodes backed up at the same time. Broadcom recommends taking the cluster offline. If an online backup is necessary, do not enable file-system quiescing. Avoid the dynamic-threshold calculation window, which begins at 2 a.m. by default [11], [12].

Record one coordinated recovery point for all nodes, the offline or online condition, the quiescing setting, backup timing, and image consistency. After restore, verify fresh collection, object association, required alerts, authorized access, and renewed protection.

VCF Operations for Networks image protection

VCF Operations for Networks uses image-based protection [11], [12].

Qualify its product-specific image backup and restore procedure, cluster scope, source and target builds, and integrations. Verify fresh collection, topology and object association, required alerts, and renewed protection. Do not apply the VCF Operations quiescing or 2 a.m. precautions without product-specific evidence.

Services runtime and separate Management Services artifacts

The current operational matrix lists VCF services runtime as file-based. SDDC lifecycle, fleet lifecycle, Software Depot, Identity Broker, Salt RaaS, Salt Master, and Log Management each have separate file-based protection. Log Management backup excludes log data. Telemetry, Real-Time Metrics, and Real-Time Metrics Store are file-based and are captured only as part of a scheduled backup [12].

Inventory and test each required component and artifact separately. Do not infer full hosted-service or log-data recovery from a runtime backup. For services with the scheduled-backup caveat, verify the actual scheduled output. Demonstrate the fresh login, logging, or management transaction required by each claimed capability.

VCF License Server redeployment and licensing access

The design component-protection matrix records License Server as None and directs deployment of a new server and licensing reconfiguration; the current operational backup matrix does not list the License Server [11], [12]. The instance-recovery task uses the applicable VCF 9.1.0 or 9.1.1 deployment task. For 9.1.1, deployment requires a unique, time-bound registration key from VCF Operations. Deploy the server into a vCenter instance connected to that VCF Operations instance; standalone ESX deployment is not permitted. The server then connects to Operations and must be registered with the VCF Business Services Console. Licenses must be added or imported before assignment [17].

Prove access to the release-specific OVA, required administrative and portal privileges, DNS and network prerequisites, protected use of the registration key, connection to VCF Operations, Business Services Console registration, and the required license assignment. For disconnected mode, test the documented registration and license-file exchanges plus the separate usage-file and license-file update workflow. Do not infer exact-build matching, a grace period, or a continued-operation guarantee.

VCF Automation component protection

VCF Automation uses file-based protection [11], [12].

Qualify VCF Automation and VCF services runtime versions separately. Demonstrate policy-governed provisioning, resulting resource state, and cleanup.

Fleet recovery of Operations and Operations for Networks

The fleet blueprint permits VCF Protection and Recovery replication and recovery plans or restoration from image-based backup for VCF Operations and VCF Operations for Networks. These are separate methods and both require IP mobility [15].

Record and qualify the selected mobility mechanism, routing and DNS controls, image or replication consistency, and failover and failback procedures. Verify fresh collection, object association, and alerts independently for each product. These conditions apply to the documented fleet model.

VCF Operations Continuous Availability alternative

In the documented VCF design model, Continuous Availability for VCF Operations uses one analytics cluster split evenly across two fault domains in two VCF instances in separate availability zones, with paired analytics nodes and a witness in a third location [15], [19].

Qualify routable L2/L3 connectivity, firewall and certificate settings, less than 10 ms inter-node latency with brief peaks to 20 ms over 20 seconds, and up to 30 ms from the witness to cluster nodes.

The model tolerates loss of one fault domain and runs degraded. An inter-site partition requires manual return and resynchronization of the offline fault domain; loss of both zones requires restore from backup. The cited fleet blueprint documents this alternative for VCF Operations only [15], [19].

Demonstrate the named single-fault-domain failure and degraded-state operating boundaries. Record node placement, witness independence, failed-state capacity, network and latency evidence, and manual resynchronization. Maintain a separately qualified backup recovery path for loss of the complete deployment.

Fleet recovery of VCF Automation

The fleet blueprint directs deployment of a new VCF Automation instance at the recovery site followed by restoration of its backup. The blueprint does not require IP mobility for this method [15].

Verify authorized tenant access and a governed disposable request, including policy checks, resource verification, and cleanup.

Fleet recovery of Management Services components

For Identity Broker, fleet lifecycle, Software Depot, Salt RaaS, and Log Management, the fleet blueprint restores individual components onto the recovery site's existing Management Services instance. No IP mobility is required by this method. Identity Broker and Software Depot must not already exist on that target instance [15].

Validate each recovered function and its consumers. Establish fresh authorized access, a bounded lifecycle or configuration transaction, or fresh log ingestion as applicable. Reserve a qualified destination, including its service inventory. Do not remove an existing target Identity Broker or Software Depot to force a fit without an independently authorized design and the applicable procedure. The absence of an IP-mobility requirement does not remove requirements for DNS, routing, certificates, endpoint reconciliation, or authorized access.