

RCCMD v5

Multi-Cluster Control & Intelligente RZ-Orchestrierung



Maximierung der Uptime durch strukturelle Effizienz. Wir sind stolz auf unsere Lösung.



Inhaltsverzeichnis

Vorwort	4
Anwendungen	5
RCCMD v5: Multi-Cluster Control & Intelligente RZ-Orchestrierung	5
Das zentrale Paradigma unserer neuen Version	5
Alle Neuerungen im Überblick.....	6
Übersicht: RCCMD v4 vs RCCMD v5	6
Die 7 Säulen der RCCMD v5 Architektur	7
1. Architektur, Identity Management & Dynamisches Blueprinting	7
Harmonisierte Authentifizierung.....	7
Neu: Dynamisches Blueprinting	7
Direkte Interaktion	8
Infrastruktur-Selbstschutz	8
2. Dynamische Ressourcensteuerung & Maximierte USV-Effizienz	8
Synchronisation vs. Migration	8
Ressourcenschonung	8
USV-Optimierung.....	8
3. Prävention von Cluster-Konflikten & Kontrollierte Cluster-Isolation („Cluster-Sterilisierung“)	8
RCCMD in der Praxis: Die DRS Endlos-Schleife	9
4. Spezial-Szenarien: Storage (SAN/NAS) und Netzwerkstörungen	10
Schutz für Shared Storage:	10
Reaktion auf Faserbruch	10
RCCMD in der Praxis: Wenn das Netzwerk uns verlässt	11
5. Multi-Site-Management und redundante RZ-Steuerung	11
Die Infrastruktur im Wandel.....	11
Redundanzgruppen-Skalierung:	11
Parallel-Redundanz	12
Cluster-übergreifende Kontrolle	12
RCCMD in der Praxis: Wenn mehrere USV-Anlagen absichern.....	12
6. Sicherheit, Simulation & Intelligente Trigger-Logik	13
Principle of Least Privilege (RBAC)	13
Auditierung & Dry-Run Modus	13
Dynamische Auslösekriterien	13



7. Intuitive Verwaltung & Transparenz	13
Schnelle und intuitiv gestaltete Einrichtung	13
Drag'n'Drop Zuweisung.....	13
Visualisierte Infrastruktur-Gesundheit	13
RCCMD in der Praxis: Komplexe Shutdown-Kontrolle intuitiv umgesetzt.....	14
Fazit: Ein zukunftssicheres Resilienz-Konzept.....	16



Vorwort

RCCMD gehört seit vielen Jahren zu den etablierten Lösungen für das sichere Herunterfahren und die kontrollierte Steuerung von IT-Infrastrukturen im Notfall. Ein wesentlicher Grund dafür ist unser grundlegender Anspruch:

Leistungsfähige Technologie zu fairen und transparenten Lizenzbedingungen

Über viele Jahre hinweg enthielt das RCCMD Standardpaket eine gemeinsame Lizenz für Windows-, Linux-, Unix- und VMware-Umgebungen. Für den überwiegenden Teil unserer Kunden war genau dies eine einfache, wirtschaftliche und langfristig planbare Lösung.

In den vergangenen Jahren haben sich beide, die Anforderungen moderner VMware-Infrastrukturen und die Sichtweise auf Lizenzmodelle am Markt grundlegend verändert. Während viele Hersteller inzwischen ausschließlich abonnementbasierte Modelle für exklusive Nutzungsrechte an der Software setzen, verfolgen wir weiterhin das Ziel, unseren Kunden eine langfristig kalkulierbare Alternative anzubieten.

Aus diesem Grund haben wir uns entschieden, die VMware-Plattform künftig als eigenständigen Produktbereich zu behandeln, da die technischen Anforderungen hochverfügbarer, verteilter VMware-Umgebungen sich heute deutlich von klassischen Shutdown-Szenarien unterscheiden.

Moderne Infrastruktursysteme erfordern eine speziell ausgelegte Architektur.

Mit RCCMD v5 stellen wir deshalb nicht einfach eine Weiterentwicklung bestehender Funktionen vor, sondern eine vollständige Neuentwicklung für moderne VMware-Infrastrukturen.

Ab dem 1. September 2026 wird RCCMD für VMware ausschließlich als RCCMD v5 unter einer eigenen Artikelnummer und in einem separaten Lizenzpaket angeboten.

Der Support für RCCMD v4 wird für VMware-7-Umgebungen noch bis Ende 2026 fortgeführt. Für VMware 8 empfehlen wir bereits den Einsatz von RCCMD v5. Für zukünftige VMware-Versionen wird RCCMD v5 die zentrale Plattform für einen sicheren und kontrollierten Shutdown-Betrieb darstellen.

Unser Ziel war dabei nicht, bestehende Konzepte lediglich anzupassen:

Wir wollten die Möglichkeiten moderner Shutdown- und Orchestrierungssoftware konsequent neu „denken“, ohne unsere gewohnte Linie zu verlassen. Das Ergebnis ist eine Lösung, die deutlich über klassische Shutdown-Funktionen hinausgeht und die besonderen Anforderungen verteilter, hochverfügbarer VMware-Infrastrukturen berücksichtigt. Während Hersteller wie APC oder Eaton jährlich lediglich noch mit neuen oder stetig teureren Lizenzmodellen die „theoretische Genehmigung zur Nutzung von Softwaremodulen“ unserer Meinung nach am Markt vorbei entwickeln, bringen wir unsere professionelle Software weiterhin als Lifetime Lizenz auf den Markt.

Wo genau liegt der Unterschied zwischen der bisherigen RCCMD V4 für VMware und der neuen RCCMD V5 erklären wir auf den nächsten Seiten.



Anwendungen

RCCMD v5: Multi-Cluster Control & Intelligente RZ-Orchestrierung

Seit vielen Jahren begleiten wir als Team IT-Verantwortliche durch die wachsenden Herausforderungen hochverfügbarer Rechenzentren. Aus dieser engen, vertrauensvollen Zusammenarbeit wissen wir: Moderne, verteilte VMware-Infrastrukturen benötigen weit mehr als einfache, statische Shutdown-Befehle. Ein proaktives Risikomanagement erfordert heute zwingend eine Abkehr von isolierten, reaktiven Skript-Lösungen.

Wir sind stolz darauf, Ihnen mit RCCMD v5 eine Architektur zu präsentieren, die sich dynamisch in die Systemumgebung einfügt, anstatt als starre Insellösung zu operieren, wie es in der Vergangenheit noch oft der Fall war.

Unsere Entwickler haben die Softwarearchitektur von Grund auf neu konzipiert, um den strengen normativen Sicherheits- und Automatisierungsanforderungen moderner IT-Infrastrukturen vollumfänglich gerecht zu werden.

Der primäre Vorteil liegt für Sie in der intuitiven Automatisierung und der spürbaren Entlastung im administrativen Alltag:

Das zentrale Paradigma unserer neuen Version

„Maximierung der Uptime durch strukturelle Effizienz. RCCMD v5 koordiniert die verfügbaren Rechen-, Storage- und Netzwerkressourcen so, dass Redundanzen gezielt genutzt und ungeplante Abschaltungen möglichst vermieden werden.“

Dies führt als direkte Konsequenz dazu, dass Ihre bestehenden USV-Anlagen – völlig unabhängig von der verwendeten Batterie-Chemie (wie Blei, Natrium oder Lithium) – die gewonnene Laufzeit signifikant besser nutzen können, um das System länger aktiv und verfügbar zu halten.



Alle Neuerungen im Überblick

Das zentrale Paradigma unserer neuen Version lautet: **Maximierung der Uptime durch strukturelle Effizienz.** RCCMD v5 koordiniert die verfügbaren Rechen-, Storage- und Netzwerkressourcen so, dass vor allem **ungeplante Abschaltungen möglichst vermieden werden.**

Dies führt als direkte Konsequenz dazu, dass Ihre bestehenden USV-Anlagen – völlig unabhängig von der verwendeten Batterie-Chemie (wie Blei, Natrium oder Lithium) – die gewonnene Laufzeit signifikant besser nutzen können, um das System länger aktiv und verfügbar zu halten.

Übersicht: RCCMD v4 vs RCCMD v5

Traditionelles USV-Management (RCCMD v4)	RCCMD v5 Orchestrierung
Starre, manuelle Skripte und Listenpflege	Dynamisches Onboarding durch vCenter-Inventory
Dezentrale Logins auf jedem ESXi-Host notwendig	Zentralisierte Authentifizierung (vCenter, Active Domain) mit sicherem Fallback
Gefahr von Boot-Loops durch DRS-Konflikte im Notfall	Prävention von Boot Loops durch temporäre Cluster-Sterilisierung und vCLS Retreat Mode

RCCMD v5 ist nicht nur eine allgemeine „Funktionserweiterung“, sondern ist eine komplette Neuentwicklung, welche Funktionen bietet, um die Anforderungen moderner Infrastrukturen transparent und anforderungsgerecht zu bedienen:

- ✓ Keine statischen Host-Listen mehr
- ✓ Zentrale Authentifizierung
- ✓ Multi-Site-Unterstützung
- ✓ DRS- und vCLS-Integration
- ✓ Intelligente Trigger-Logik
- ✓ Deutlich geringerer Pflegeaufwand
- ✓ Intuitive und zentrale Übersicht des Gesamtsystem im Notfall

Die 7 Säulen der RCCMD v5 Architektur

1. Architektur, Identity Management & Dynamisches Blueprinting

Eine fehlerresistente VMware-Infrastruktur erfordert, dass IT-Administratoren nicht durch manuelle Listenpflege oder dezentrale Logins gebunden werden. Hier haben wir massiv angesetzt:

Dynamisches Onboarding: Anstatt Hosts manuell in statischen Shutdown-Skripten zu hinterlegen, liest RCCMD v5 dynamisch den Verzeichnisbaum des vCenters aus. Neue oder an andere Standorte verschobene Hosts werden automatisch erkannt und der korrekten Shutdowngruppe zugeordnet.

Harmonisierte Authentifizierung

Ein lokaler Login auf jedem ESXi-Host ist nicht mehr zwingend erforderlich. Die Software ermöglicht eine zentralisierte Authentifizierung über vCenter, Active Directory oder Shared User. Fällt das vCenter aus, greift die Appliance auf lokale hostbasierte Zugangsdaten als zusätzliche Fallback-Ebene zurück.

Neu: Dynamisches Blueprinting

Sobald ein Shutdownsignal im Netzwerk registriert wird, erstellt RCCMD v5 in Echtzeit eine dedizierte Netzwerkkarte (Blueprint). Anhand dieser Blaupause wird evaluiert, ob ein vCenter

The screenshot displays the 'VMware Settings' window, specifically the 'Groups & Inventory' tab. It shows the configuration for shutdown groups and their inventory. The 'Shutdown Sender (Redundancy Groups) - Hamburg' section lists two groups: 'Hamburg' and 'Düsseldorf', each with a 'Redundancy Level: 0'. The 'Hamburg' group lists several hosts and clusters, including 'DC-01' and 'Cluster-01-01' through 'Cluster-01-04'. The 'Düsseldorf' group lists 'DC-02' and 'Cluster-02-01' through 'Cluster-02-04'. The 'vCenter Inventory' section shows a list of clusters and hosts with status indicators (HA, DRS, vSAN) and a 'Refresh' button.

Abb.: Sobald eine USV ein RCCMD - Shutdown Signal sendet, erstellt RCCMD in Echtzeit eine interne Netzwerkkarte, und wägt im Anschluss ab, wie weiter vorgegangen werden muss oder kann. Gut zu erkennen: RCCMD liefert nicht nur Standortbezogen eine Übersicht über die zugewiesenen Hosts, die zu einer USV oder Redundanzgruppe gehören, sondern auch einen praktischen Überblick über den Gesundheitszustand aller bekannten Cluster, DataCenter und Hosts im Netzwerk mit praktischen Farbcode - Grün: Die Hosts arbeiten innerhalb der gesetzten Betriebsparameter Gelb: Das zuständige vCenter meldet eine Warnung zum Betriebszustand - Rot: Dieses System hat einen verifizierten Fehler – Grau: „Deaktivierter Dienst“ Die Statusmeldungen werden mit komfortablen „OnMouseOver“ direkt angezeigt.

Administratoren können sich in Notfallsituationen sofort einen Systemweiten Überblick verschaffen, ohne Vmware-Spezifische Systemlogs auszuwerten.



partnerschaftlich mit anderen Clustern verknüpft ist oder als isoliertes System agiert. Diese Entscheidung passiert innerhalb weniger Millisekunden innerhalb von RCCMD

Direkte Interaktion

Anders als die Vorgängerversion kann RCCMD v5 durch dieses Blueprinting den USV-Zustand anderer Cluster-Nodes oder Datacenter proaktiv abfragen und so ggfls. einen Shutdown vermeiden.

Infrastruktur-Selbstschutz

RCCMD v5 kann nun seine eigene exponierte Lage im Netzwerk zu erkennen. Im Ernstfall stellt das RCCMD System ein priorisiertes Migrationsverhalten für seine eigene Instanz sicher, sodass die Infrastruktursteuerung von RCCMD auch während kritischer Migrationsphasen verfügbar bleibt.

2. Dynamische Ressourcensteuerung & Maximierte USV-Effizienz

Es ist RCCMD ein besonderes Anliegen, dass ein geordneter Notfallprozess vorhandene Kapazitäten intelligent nutzt. **Ein kompletter Shutdown darf normativ immer nur die letzte Option bei absolutem Ressourcenmangel sein.**

Synchronisation vs. Migration

Das VMware-System unterscheidet präzise zwischen einer regulären „VM-Migration“ und einem „Failover“. RCCMD v5 identifiziert bestehende Hochverfügbarkeits- und Replikationskonzepte und analysiert, ob diese synchron oder asynchron laufen.

Ressourcenschonung

Liegen durch „vSphere Fault Tolerance“ oder „vSphere Replication“ gespiegelte Datenbestände vor, synchronisiert unser System lediglich den letzten Datenbestand. Dies reduziert den Übertragungsaufwand deutlich und verkürzt die Reaktionszeit insbesondere bei großen virtuellen Maschinen

USV-Optimierung

Durch diese Effizienz reicht oft schon die kurze Haltezeit kostengünstigerer Batterie-Technologien aus, um Rechenzentren sicher herunterzufahren. Die Software respektiert zudem aktiv die individuellen Migrations-Präferenzen, die Sie als Administrator im vCenter festgelegt haben.

3. Prävention von Cluster-Konflikten & Kontrollierte Cluster-Isolation („Cluster-Sterilisierung“)

Aus der Praxis mit RCCMD V4 wissen wir...

Sobald ein physischer Shutdown zwingend eingeleitet werden muss, dürfen VMware-interne Dienste den Prozess unter keinen Umständen blockieren. Bei der Entwicklung von RCCMD v5 wurde genau dieser Aspekt in den Fokus gelegt:

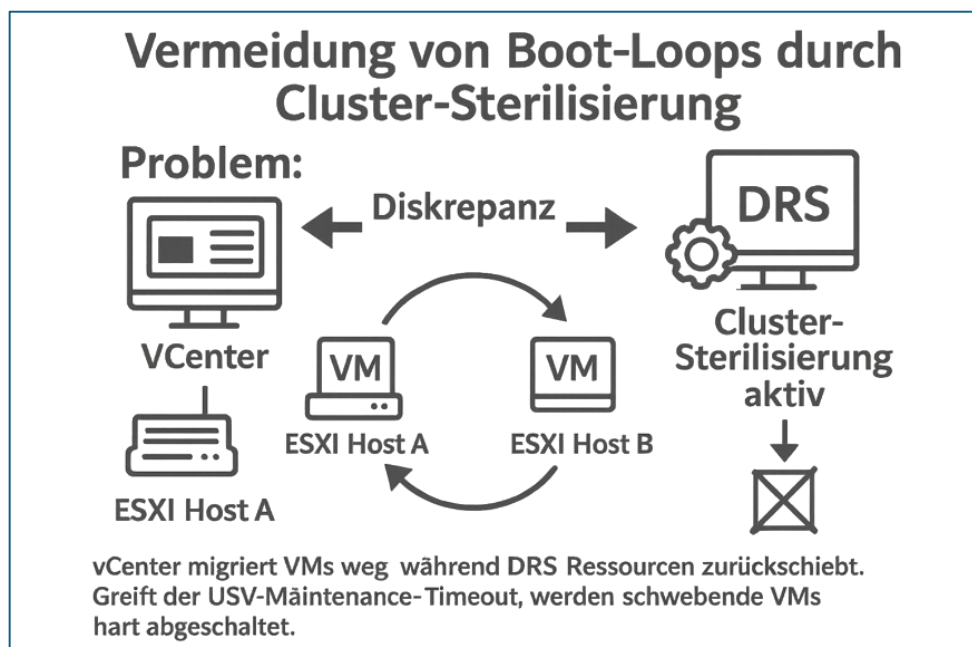
- Verhinderung von Boot-Loops: In hochverfügbaren Umgebungen verschiebt das vCenter im Notfall VMs, während der DRS gleichzeitig freiwerdende Ressourcen erkennt und Daten im Hintergrund zurückschiebt. Diese Endlosschleife zwingt die USV letztlich zu einer harten Abschaltung.
- Cluster-Sterilisierung: RCCMD v5 verhindert diesen Konflikt präventiv. Die HA-Funktion wird im Falle eines notwendigen Shutdowns durch temporäres Blindschalten („Sterilisierung“) vorübergehend deaktiviert. Beim Neustart stellt das System den regulären Betrieb automatisch wieder her.
- Sicherer Retreat Mode & Infrastruktur-Erkennung: RCCMD v5 nutzt das vCenter tiefgreifend, um vCLS, DHCP, DNS sowie virtuelle Switches und Router aktiv zu erkennen. Über ein Kommando versetzt es betroffene System-VMs in den „Retreat Mode“, was die saubere Entfernung aus dem Cluster erzwingt und den physischen Shutdown absichert.
- DRS-Intervention: Während der Shutdown-Phase wird der DRS via API auf den Status „Manual“ gesetzt, um die CPU- und Netzwerklast sofort zu senken und den Vorgang essenziell zu beschleunigen.

RCCMD in der Praxis: Die DRS Endlos-Schleife

Praxisbeispiel – Die DRS-Endlosschleife („The Never Ending Story“):

Wir beobachten in hochverfügbaren Umgebungen häufig eine gefährliche Diskrepanz

Wenn das vCenter im Notfall VMs von einem Host wegmigriert, erkennt der Distributed Resource Scheduler (DRS) in Echtzeit die freiwerdenden Ressourcen und schiebt Daten im Hintergrund genau dorthin zurück. Durch



diese Konkurrenzsituation entsteht eine Endlosschleife. Der Shutdownbefehl wird immer wieder aufgehoben, bis die USV hart abschaltet und laufende Prozesse und nicht abgeschlossene Schreibvorgänge gefährdet werden können.



Die Lösung – Cluster-Sterilisierung & Retreat Mode:

RCCMD v5 durchbricht dies präventiv. Die HA-Funktion wird im Vorfeld temporär kontrolliert deaktiviert („Sterilisierung“). Betroffene System-VMs werden über die vSphere Cluster Services (vCLS) in den „Retreat Mode“ versetzt, was die saubere Entfernung erzwingt. Zusätzlich setzen wir den DRS via API auf „Manual“, was die Netzwerklast sofort senkt.

4. Spezial-Szenarien: Storage (SAN/NAS) und Netzwerkstörungen

Die Absicherung gemeinsamer Speichermedien und der Umgang mit Leitungsausfällen erfordern spezifische, normativ saubere Handlungsrouninen.

Schutz für Shared Storage:

Gemeinsame Speichermedien (z.B. vSAN oder Metro Cluster) werden von klassischen Skripten meist ignoriert und hart abgeschaltet. RCCMD v5 nutzt stattdessen die native vCenter-Methode „PlaceVm“, um eine DRS-konforme und saubere Verarbeitung sicherzustellen.

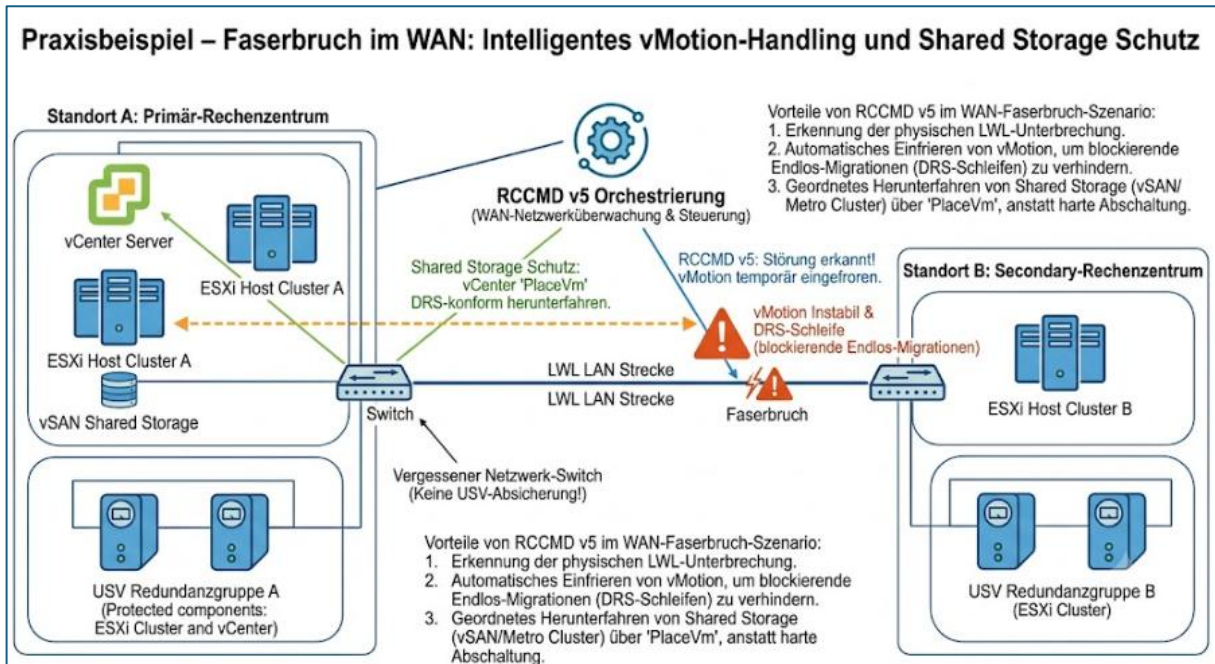
Reaktion auf Faserbruch

Brechen LWL-Verbindungen ab, werden laufende vMotion-Tasks instabil. Bei solchen Netzwerkstörungen friert RCCMD v5 das vMotion temporär ein. Sinnlose Endlos-Migrationen werden blockiert, sodass Ihre Techniker gefahrlos mit der Fehleranalyse beginnen können.

RCCMD in der Praxis: Wenn das Netzwerk uns verlässt

Praxisbeispiel – Der Faserbruch im WAN

In der Praxis zeigt sich immer wieder, dass Netzwerkkomponenten als nicht relevante Infrastruktur betrachtet wird. Wir beobachten immer wieder, dass vereinzelt Switches oder Router bei der Absicherung vergessen wurden, was weitreichende Konsequenzen für das Notfallmanagement hat.



Bei einer physischen Unterbrechung von LWL-Verbindungen (Faserbruch) im WAN werden laufende vMotion-Tasks instabil. Anstatt nun in blockierende Endlos-Migrationen zu verfallen, erkennt RCCMD v5 die Netzwerkstörung und friert das vMotion temporär ein. Dies gibt Ihren Technikern die notwendige Zeit, gefahrlos mit der Fehleranalyse zu beginnen.

Die Lösung zum Schutz für Shared Storages:

Gemeinsame Speichermedien (z.B. vSAN oder Metro Cluster) werden im Gegensatz zu klassischen Skripten nicht ignoriert und hart abgeschaltet, sondern über die native vCenter-Methode „PlaceVm“ DRS-konform heruntergefahren.

5. Multi-Site-Management und redundante RZ-Steuerung

Die Infrastruktur im Wandel

Große, verteilte Rechenzentrumsstrukturen profitieren von einer zentralen Orchestrierungsinstanz und konsistenten Betriebsprozessen.

Redundanzgruppen-Skalierung:

Mehrere USV-Anlagen können nun zu unterschiedlichen Redundanzgruppen zusammengeführt und logisch verknüpft werden, selbst wenn sie von unterschiedlichen Herstellern stammen.

Parallel-Redundanz

Bei Anlagen, deren Leistungsmodule sich gegenseitig redundant absichern, sorgt ein einziges RCCMD v5 dafür, dass die abhängigen Rechenzentren erst angehalten werden, wenn tatsächlich keine Leistungsmodule mehr zur Verfügung stehen.

Cluster-übergreifende Kontrolle

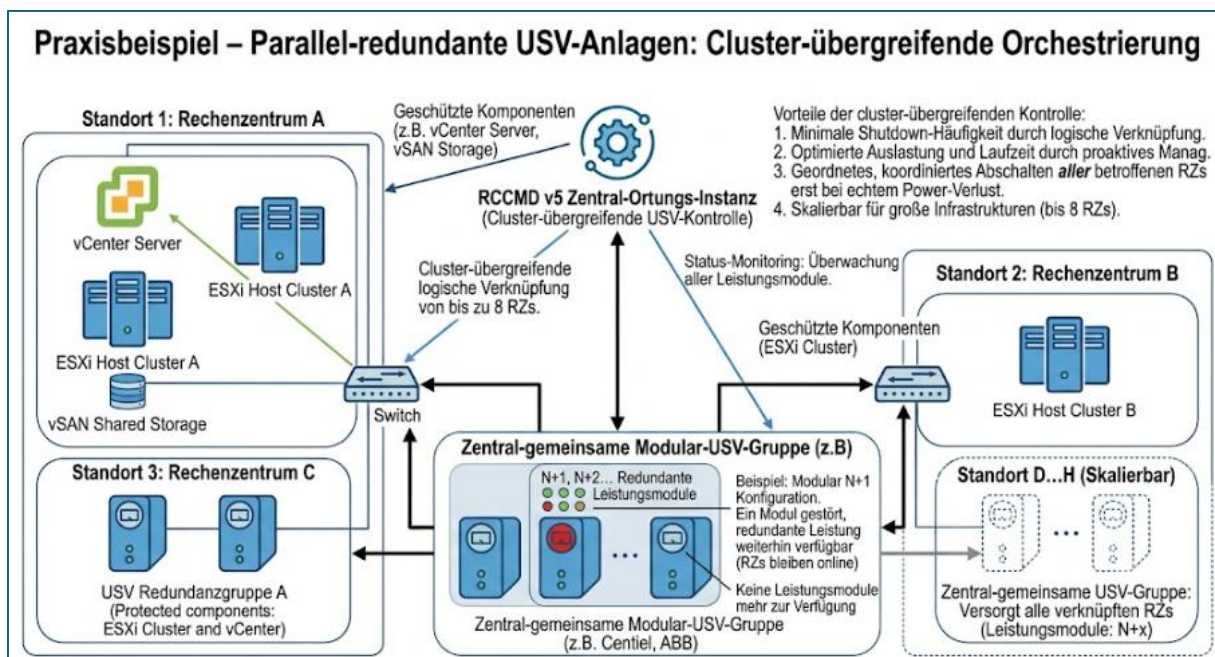
Administratoren können bis zu acht Rechenzentren über eine zentrale Managementinstanz koordinieren.

RCCMD in der Praxis: Wenn mehrere USV-Anlagen absichern

Praxisbeispiel – Parallel-redundante USV-Anlagen:

In großen Infrastrukturen hängen oft mehrere Rechenzentren an derselben USV-Gruppe (z.B. von CENTIEL oder ABB), die durch unterschiedliche Leistungsmodule redundant abgesichert sind. RCCMD v5 verknüpft diese Anlagen logisch miteinander.

Die Lösung: Cluster-übergreifende Kontrolle:



RCCMD v5 liefert alle notwendigen Funktionen, um alle an dieser Gruppe hängenden Rechenzentren erst dann anzuhalten, wenn tatsächlich keine Leistungsmodule mehr zur Verfügung stehen – das schützt vor unnötigen Abschaltungen.

Administratoren können bis zu 8 Rechenzentren effizient über eine einzige Instanz verwalten.



6. Sicherheit, Simulation & Intelligente Trigger-Logik

Eine professionelle IT-Plattform erfordert neben Automatismen auch Transparenz und strikte Zugriffskontrollen.

Principle of Least Privilege (RBAC)

Die Software integriert sich sauber in das Role-Based Access Control System von VMware. RCCMD v5 folgt konsequent dem Principle of Least Privilege und benötigt lediglich die für die jeweiligen Funktionen erforderlichen API-Berechtigungen.

Auditierung & Dry-Run Modus

Über Syslog-Integrationen lassen sich API-Aufrufe lückenlos protokollieren und evaluieren. Sie können so exakt nachvollziehen, wie ein Shutdown ablaufen würde, ohne die Produktion im Vorfeld zu unterbrechen.

Dynamische Auslösekriterien

Das System reagiert nicht starr auf bloße Batterie-Prozentangaben. Es korreliert die verbleibende Autonomiezeit dynamisch mit den kalkulierten Migrations- und Shutdownzeiten der Cluster. So ermittelt die Logik den absolut spätesten, aber sichersten Zeitpunkt.

7. Intuitive Verwaltung & Transparenz

Schnelle und intuitiv gestaltete Einrichtung

Wir wissen, wie wertvoll Ihre Zeit ist. Daher haben wir besonderen Wert auf eine schnelle Inbetriebnahme, eine intuitive Bedienung und ein übersichtliches Interface gelegt.

Drag'n'Drop Zuweisung

Sie definieren USV-Gruppen mit wenigen Klicks und weisen Sie dynamisch einzelne Hosts, ganze Cluster oder DataCenter zu.

Visualisierte Infrastruktur-Gesundheit

RCCMD v5 liefert Ihnen umfassende Statusinformationen über den aktuellen Gesundheitszustand des Clusters. Ein intuitives Ampelsystem zeigt den aktuellen Status gefundener Server; prägnante Hinweistexte erscheinen direkt, wenn Sie mit der Maus über die Kacheln fahren.

RCCMD in der Praxis: Komplexe Shutdown-Kontrolle intuitiv umgesetzt

Praxisbeispiel – Redundanzgruppen-Zuordnung

Stellen Sie sich vor, Sie verwalten drei USV-Anlagen. RCCMD strukturiert diese auf Basis ihrer IP-Adressen. Sie können z.B. eine Anlage der Gruppe 1 (als Einzelanlage) zuweisen und die beiden anderen Anlagen in Gruppe 2 zu einer Redundanzgruppe zusammenführen:

Abb.: Bekannt gemachte USV-Anlagen werden innerhalb der Redundanz zu Gruppen zusammengeführt.

- Group 1: Eine einzelne USV liefert den Notstrom.
- Group 2: Hier sind zwei USV-Anlagen gemeinsam in einer Redundanzgruppe miteinander logisch verknüpft, und der Redundanzlevel auf 1 gestellt.

In unserem Beispiel weiß RCCMD ab diesem Zeitpunkt, wie diese 3 USV-Anlagen zusammenhängen und kann genau unterscheiden, ob ein Shutdownszenario sofort ausgeführt werden muss oder aber zwei USV-Anlagen gemeinsam das Netzwerk absichern (Shutdown unterdrückt). Im nächsten Schritt müssen nur noch diesen USV-Gruppen Server zugeordnet werden.

Nachdem RCCMD jetzt nun exakt weiß, wie die USV-Anlagen zu betrachten sind und wie sie eventuell miteinander kooperieren, um den Notstrom zu sichern, kann im zweiten Schritt bestimmt werden, welche Server heruntergefahren werden. RCCMD stellt es einem dabei frei, ob die Hosts direkt heruntergefahren werden müssen, oder aber, ob zusätzlich eine eigene Insellösung benötigt wird.

Sie können also frei definieren, ob die RCCMD Appliance:

- Einzelne Hosts bzw. Standalone-Server
- Cluster
- DataCenter

explizit in das Shutdownkonzept inkludieren oder aber einzelne Hosts herausnehmen wollen, etwa, weil dort eine spezielle Shutdownlösung mit einem eigenen Ansatz laufen muss, die vollständig unabhängig von der restlichen Infrastruktur realisiert wurde.

Administratoren haben über die Appliance die volle Kontrolle:

RCCMD v5 liefert ein schnell erfassbares Interface, über das Administratoren sofort über den Querbezug zu USV-Anlagen und den jeweils abgesicherten Servern.

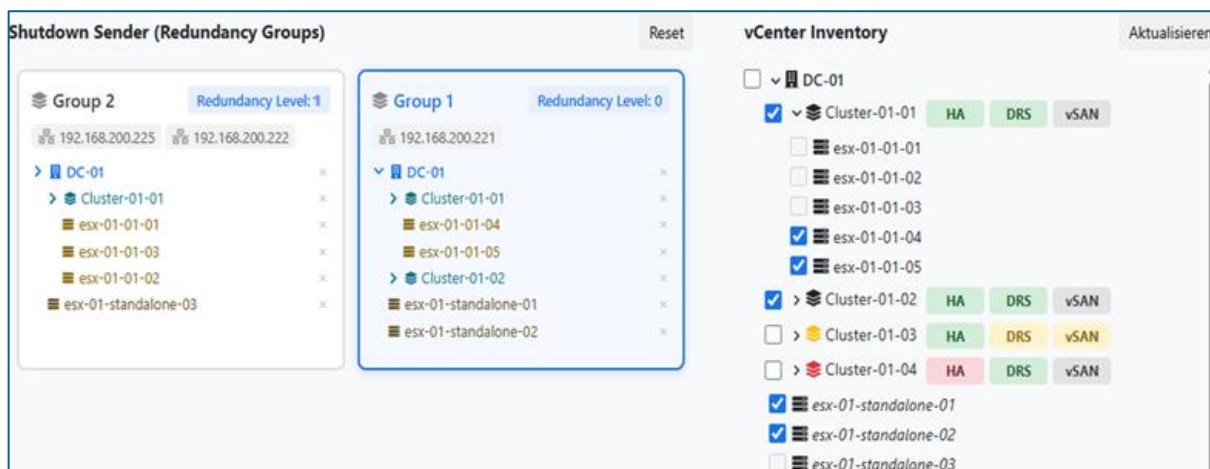


Abb.: Nachdem RCCMD weiß, welche der drei USV-Anlagen verfügbar sind und wie diese in Redundanzgruppen miteinander kooperieren, kann im nächsten Schritt per Mausklick ganz einfach ein Shutdownverhalten realisiert werden: Die Anzeige des über das Webinterface liefert hierzu übersichtlich folgende Informationen:

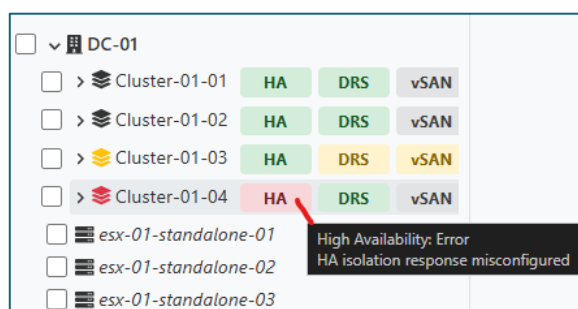
- Welche USV-Anlagen befinden sich im Redundanzmodus (Group 2)?
Es werden nicht nur die Die USV-Anlagen in einer Gruppe angezeigt, sondern auch die zugehörigen Redundanzlevel. RCCMD weiß zu jeder Zeit, warum und wann ein Shutdown ausgeführt werden muss: Erst, wenn ein RCCMD-Shutdown von beiden USV-Anlagen vorliegt.
- In welcher USV-Gruppe befindet sich gerade der Administrator (Group 1)?
Diese Gruppe wird farblich markiert.
- Welche Hosts / Server sind dieser Gruppe aktuell zugeordnet?
Die zugewiesenen Hosts stehen nicht nur im Fenster der USV-Gruppe, sondern werden Automatisch auch rechts mit einem aktiven Haken angezeigt.

Administratoren erhalten eine übersichtliche Aufstellung über alle zugewiesenen Server. Durch einfaches An/ Abwählen des Hakens in der Checkbox kann der Server aus der jeweiligen Gruppe herausgenommen oder hinzugefügt werden.

Visualisierte Infrastruktur-Gesundheit

Zusätzlich liefert RCCMD eine aktuelle Übersicht über die Gesundheit jedes bekannten Servers innerhalb der VMware – Umgebung:

Ein intuitives verständliches Ampelsystem zeigt den aktuellen Status gefundener Server; prägnante Hinweistexte erscheinen direkt, wenn Sie mit der Maus über die Kacheln fahren.



Im Störfall können Administratoren und Systembetreuer bei Bedarf direkt im RCCMD erkennen, ob die Systemintegrität gewährleistet ist, ohne direkt über ein vCenter zentrale Administrationsmenüs aufrufen zu müssen.

Der Individuelle Shutdown innerhalb eines großen Rechenzentrums kann direkt mitverfolgt werden.



Fazit: Ein zukunftssicheres Resilienz-Konzept

Mit RCCMD v5 entwickelt sich die klassische USV-gestützte Shutdown-Software zu einer intelligenten Orchestrierungslösung für VMware-basierte Infrastrukturen. Durch die direkte Integration in das vCenter, die dynamische Erkennung von Abhängigkeiten und die koordinierte Steuerung von Clustern, Storage- und Netzwerkressourcen werden Notfallprozesse planbarer und besser beherrschbar.

Anstatt ausschließlich auf den Shutdown zu reagieren, nutzt RCCMD v5 vorhandene Redundanzen gezielt aus und schafft die Grundlage für längere Verfügbarkeit, geringeren Administrationsaufwand und eine konsistente Steuerung auch komplexer Multi-Site-Umgebungen.

Die Wahrscheinlichkeit eines Notfall-Shutdowns wird durch die konsequente Ausnutzung von Redundanzen minimiert.

RCCMD Version 5 wird weiterhin als Lifetime-Lizenz angeboten.

Die RCCMD-Lizenzen können weiterhin zeitlich unbegrenzt genutzt werden, solange die zugrunde liegende Systemumgebung (z.B. VMware oder andere eingebundene Plattformen) keine Änderungen erfährt, die aufgrund von Hersteller-Updates eine technische Anpassung und damit eine neue Lizenzversion erforderlich machen.

Sollte ein systembedingtes Upgrade notwendig werden, gewähren wir innerhalb von zwei Jahren ab Kaufdatum ein kostenfreies Upgrade auf die entsprechende neue Version. Erst nach Ablauf dieses Zeitraums wird für ein erforderliches systembedingtes Upgrade der Erwerb einer neuen Lizenz notwendig.

Unabhängig davon gilt:

Solange Ihre VMware-Umgebung bzw. die eingesetzten Systeme unverändert bestehen bleiben, bleibt auch die RCCMD-Lizenz dauerhaft gültig und uneingeschränkt nutzbar – bei Bedarf ein Leben lang.

Operative Engpässe und Cluster-Konflikte lassen sich frühzeitig erkennen und kontrolliert behandeln.

Gleichzeitig reduziert RCCMD v5 den administrativen Aufwand durch automatisierte Abläufe.

Mit skalierbaren Multi-Site-Funktionen, dynamischen Blueprint-Architekturen und einer intelligenten Trigger-Logik bietet RCCMD v5 die Grundlage für den sicheren Betrieb moderner und hochverfügbarer Infrastrukturen.