

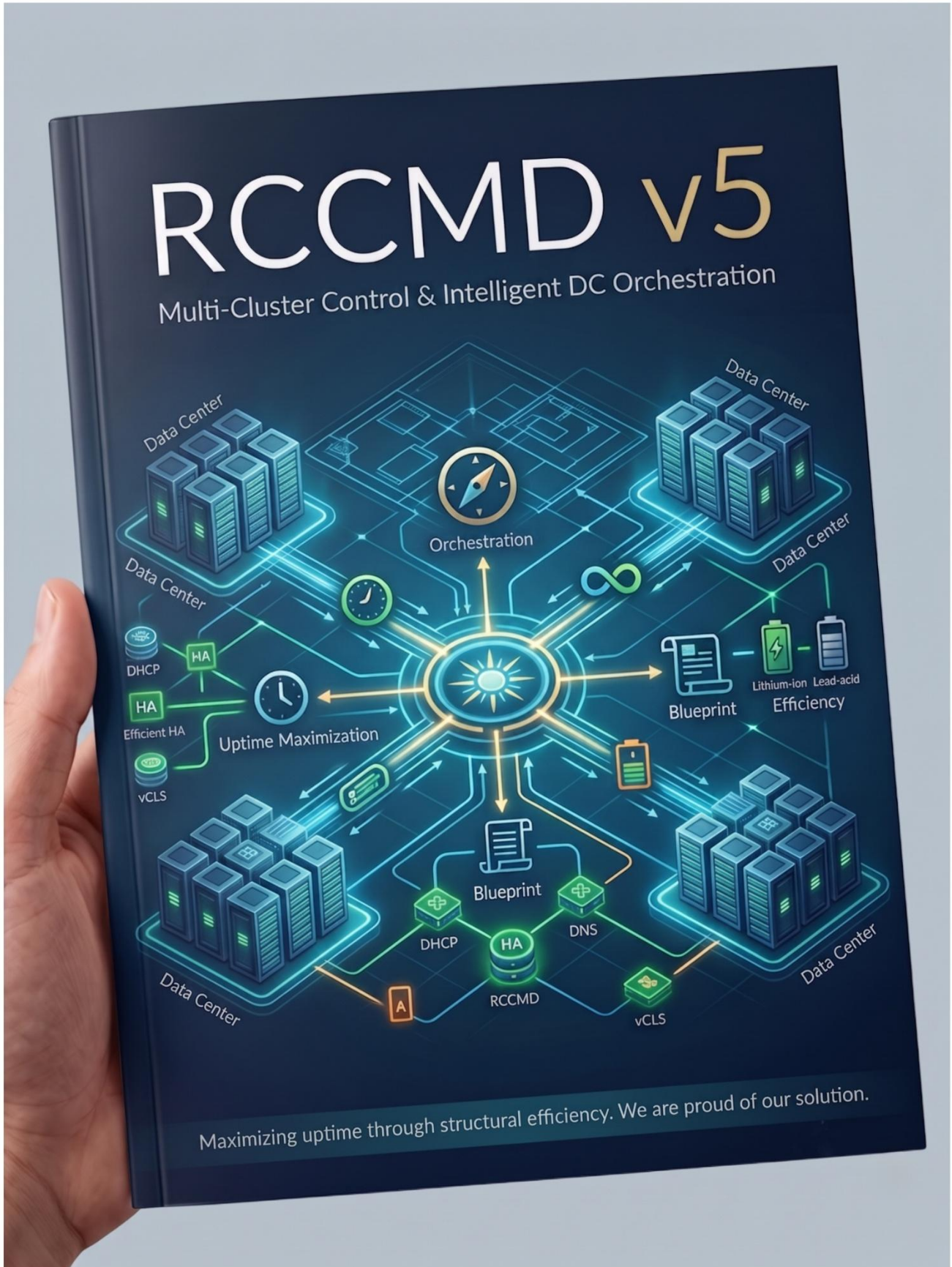




Table of contents

Foreword	3
Applications.....	4
RCCMD v5: Multi-Cluster Control & Intelligent Data Center Orchestration.....	4
The central paradigm of our new version	4
All new features at a glance.....	5
Overview: RCCMD v4 vs RCCMD v5	5
The 7 pillars of the RCCMD v5 architecture.....	6
1. Architecture, Identity Management & Dynamic Blueprinting	6
Harmonised authentication	6
New: Dynamic Blueprinting.....	6
Direct interaction	7
Infrastructure self-protection	7
2. Dynamic Resource Control & Maximized UPS Efficiency.....	7
Synchronization vs. Migration	7
Resource conservation	7
UPS optimization.....	7
3. Prevention of cluster conflicts & controlled cluster isolation (“cluster sterilization”)	7
RCCMD in practice: The DRS endless loop	8
4. Special scenarios: Storage (SAN/NAS) and network disruptions.....	8
Protection for shared storage:	9
Response to fiber breakage	9
RCCMD in practice: When the network abandons us.....	9
5. Multi-site management and redundant data center control	10
Infrastructure in transition.....	10
Redundancy group scaling:	10
Parallel redundancy.....	10
Cross-cluster control.....	10
RCCMD in practice: When multiple UPS systems are being used for protection ...	10
6. Security, Simulation & Intelligent Trigger Logic	11
Principle of Least Privilege (RBAC)	11

Auditing & Dry-Run Mode	11
Dynamic trigger criteria	11
7. Intuitive administration & transparency	11
Quick and intuitive setup	11
Drag and drop assignment	11
Visualized Infrastructure - Health.....	11
RCCMD in practice: Complex shutdown control implemented intuitively.....	12
Conclusion: A future-proof resilience concept.....	14

Foreword

For many years, RCCMD has been one of the established solutions for the safe shutdown and controlled management of IT infrastructures in emergencies. A key reason for this is our fundamental principle:

High-performance technology with fair and transparent licensing terms

For many years, the RCCMD standard package included a single license for Windows, Linux, Unix, and VMware environments. For the vast majority of our customers, this was a simple, economical, and predictable long-term solution.

In recent years, both the requirements of modern VMware infrastructures and the market's perspective on licensing models have fundamentally changed. While many vendors now rely exclusively on subscription-based models for exclusive software usage rights, we remain committed to offering our customers a predictable long-term alternative.

For this reason, we have decided to treat the VMware platform as a separate product area in the future, as the technical requirements of highly available, distributed VMware environments differ significantly from classic shutdown scenarios.

Modern infrastructure systems require a specially designed architecture.

Therefore, with RCCMD v5 we are not simply presenting a further development of existing functions, but a complete new development for modern VMware infrastructures.

From September 1, 2026, RCCMD for VMware will be offered exclusively as RCCMD v5 under its own article number and in a separate license package.

Support for RCCMD v4 will continue for VMware 7 environments until the end of 2026. For VMware 8, we already recommend using RCCMD v5. For future VMware versions, RCCMD v5 will be the central platform for safe and controlled shutdown operations.

Our goal was not simply to adapt existing concepts:

We wanted to fundamentally rethink the possibilities of modern shutdown and orchestration software without abandoning our established approach. The result is a solution that goes far beyond classic shutdown functions and addresses the specific requirements of distributed,

highly available VMware infrastructures. While manufacturers like APC or Eaton, in our opinion, merely develop the *"theoretical authorization to use software modules" annually with new or increasingly expensive licensing models* that miss the mark with the market, we continue to offer our professional software as a lifetime license.

We will explain the exact difference between the previous RCCMD V4 for VMware and the new RCCMD V5 on the following pages.

Applications

RCCMD v5: Multi-Cluster Control & Intelligent Data Center Orchestration

For many years, our team has been supporting IT managers through the growing challenges of highly available data centers. From this close, trusting collaboration, we know that modern, distributed VMware infrastructures require far more than simple, static shutdown commands. Proactive risk management today absolutely demands a move away from isolated, reactive scripted solutions.

We are proud to present RCCMD v5, an architecture that dynamically integrates into the system environment, rather than operating as a rigid, isolated solution, as was often the case in the past.

Our developers have completely redesigned the software architecture to fully meet the stringent normative security and automation requirements of modern IT infrastructures.

The primary advantage for you lies in the intuitive automation and the noticeable relief in your daily administrative work:

The central paradigm of our new version

"Maximizing uptime through structural efficiency. RCCMD v5 coordinates available computing, storage, and network resources in such a way that redundancies are used effectively and unplanned shutdowns are avoided as much as possible."

As a direct consequence, your existing UPS systems – regardless of the battery chemistry used (such as lead, sodium or lithium) – can make significantly better use of the gained runtime to keep the system active and available for longer.



All new features at a glance

The central paradigm of our new version is: **maximizing uptime through structural efficiency**. RCCMD v5 coordinates available computing, storage, and network resources in such a way that **unplanned shutdowns are avoided as much as possible**.

As a direct consequence, your existing UPS systems – regardless of the battery chemistry used (such as lead, sodium or lithium) – can make significantly better use of the gained runtime to keep the system active and available for longer.

Overview: RCCMD v4 vs RCCMD v5

Traditional UPS Management (RCCMD v4)	RCCMD v5 Orchestration
Rigid, manual scripts and list maintenance	Dynamic onboarding through vCenter inventory
Decentralized logins are required on each ESXi host.	Centralized authentication (vCenter, Active Domain) with secure fallback
Risk of boot loops due to DRS conflicts in an emergency	Prevention of boot loops through temporary cluster sterilization and vCLS retreat mode

RCCMD v5 is not just a general "functionality enhancement", but a completely new development that offers functions to transparently and compliantly meet the requirements of modern infrastructures:

- ✓ No more static host lists
- ✓ Central authentication
- ✓ Multi-site support
- ✓ DRS and vCLS integration
- ✓ Intelligent trigger logic
- ✓ Significantly less maintenance required
- ✓ Intuitive and central overview of the entire system in case of emergency

The 7 pillars of the RCCMD v5 architecture

1. Architecture, Identity Management & Dynamic Blueprinting

A fault-resistant VMware infrastructure requires that IT administrators are not tied down by manual list maintenance or decentralized logins. This is where we have focused our efforts significantly:

Dynamic onboarding: Instead of manually adding hosts to static shutdown scripts, RCCMD v5 dynamically reads the vCenter directory tree. New hosts or those moved to different locations are automatically detected and assigned to the correct shutdown group.

Harmonised authentication

Local login on each ESXi host is no longer mandatory. The software enables centralized authentication via vCenter, Active Directory, or shared users. If vCenter fails, the appliance uses local, host-based credentials as an additional fallback level.

New: Dynamic Blueprinting

As soon as a shutdown signal is detected on the network, RCCMD v5 creates a dedicated network map (blueprint) in real time. This blueprint is used to evaluate whether a vCenter is partnered with other clusters or operating as an isolated system. This decision is made within milliseconds within RCCMD.

VMware Settings

Shutdown Groups & Inventory

Shutdown Sender (Redundancy Groups) - Hamburg

Hamburg Redundancy Level: 0

- 192.168.200.224
- 192.168.200.221
- 192.168.200.220
- DC-01
 - Cluster-01-01
 - esx-01-01-01
 - esx-01-01-02
 - esx-01-01-03
 - esx-01-01-04
 - esx-01-01-05
 - Cluster-01-02
 - Cluster-01-03
 - Cluster-01-04
 - esx-01-standalone-01
 - esx-01-standalone-02
 - esx-01-standalone-03

Düsseldorf Redundancy Level: 0

- 192.168.200.226
- 192.168.200.251
- 192.168.200.225
- DC-02
 - Cluster-02-01
 - Cluster-02-02
 - Cluster-02-03
 - Cluster-02-04
 - esx-02-standalone-01
 - esx-02-standalone-02
 - esx-02-standalone-03

vCenter Inventory

DC-01

- Cluster-01-01 HA DRS vSAN
- Cluster-01-02 HA DRS vSAN
- Cluster-01-03 HA DRS vSAN
- Cluster-01-04 HA DRS vSAN
- esx-01-standalone-01
- esx-01-standalone-02
- esx-01-standalone-03

DC-02

- Cluster-02-01 HA DRS vSAN
- Cluster-02-02 HA DRS vSAN
- Cluster-02-03 HA DRS vSAN
- Cluster-02-04 HA DRS vSAN
- esx-02-standalone-01 MM
- esx-02-standalone-02

Fig.: As soon as a UPS sends an RCCMD shutdown signal, RCCMD generates an internal network map in real time and subsequently evaluates the appropriate course of action. Notably, RCCMD provides not only a location-based overview of the assigned hosts belonging to a specific UPS or redundancy group but also a practical summary of the health status of all known clusters, data centers, and hosts across the network, using a convenient color-coding system: Green – hosts are operating within established parameters; Yellow – the relevant vCenter is reporting an operational warning; Red – the system has a confirmed error; Gray – service disabled. Status details are conveniently displayed via "mouse-over" actions.

In emergency situations, administrators can immediately gain a system-wide overview without having to analyze VMware-specific system logs.



Direct interaction

Unlike its predecessor, RCCMD v5 can proactively query the UPS status of other cluster nodes or data centers through this blueprinting , thus potentially avoiding a shutdown.

Infrastructure self-protection

RCCMD v5 can now recognize its own exposed position in the network. In critical situations, the RCCMD system ensures prioritized migration behavior for its own instance, so that RCCMD's infrastructure control remains available even during critical migration phases.

2. Dynamic Resource Control & Maximized UPS Efficiency

RCCMD places particular emphasis on ensuring that an orderly emergency process intelligently utilizes existing resources. **A complete shutdown should always be the last resort in cases of absolute resource scarcity.**

Synchronization vs. Migration

The VMware system precisely distinguishes between a regular "VM migration" and a "failover". RCCMD v5 identifies existing high-availability and replication concepts and analyzes whether they run synchronously or asynchronously.

Resource conservation

If mirrored data sets exist due to "vSphere Fault Tolerance " or "vSphere Replication," our system only synchronizes the latest data set. This significantly reduces the transfer overhead and shortens the response time, especially for large virtual machines.

UPS optimization

This efficiency often means that the short holding time of more cost-effective battery technologies is sufficient to safely shut down data centers. The software also actively respects the individual migration preferences you, as an administrator, have defined in vCenter.

3. Prevention of cluster conflicts & controlled cluster isolation ("cluster sterilization")

From our experience with RCCMD V4, we know...

When a physical shutdown becomes absolutely necessary, VMware's internal services must not block the process under any circumstances. This aspect was a key focus during the development of RCCMD v5.

- Preventing boot loops: In high-availability environments, vCenter moves VMs in case of an emergency, while DRS simultaneously detects available resources and pushes data back in the background. This endless loop ultimately forces the UPS to perform a hard shutdown.

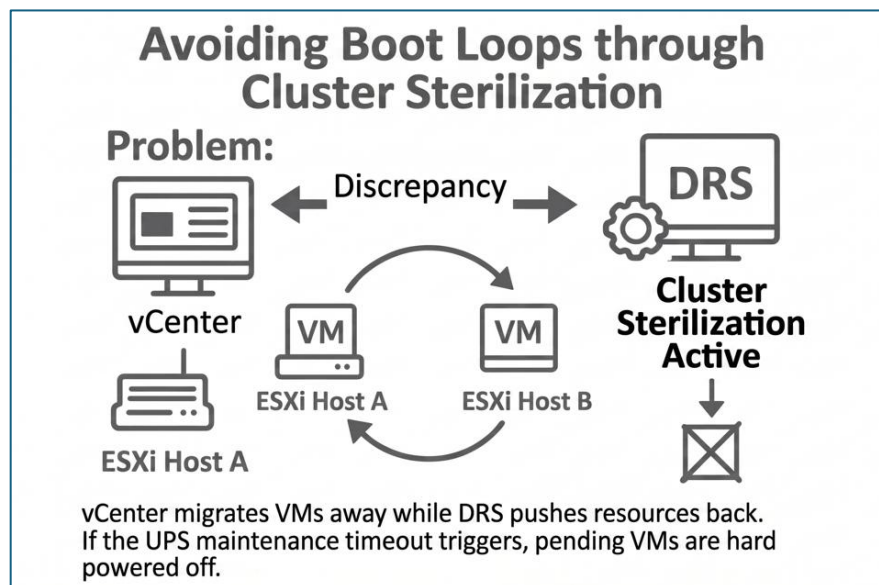
- Cluster sterilization: RCCMD v5 prevents this conflict proactively. In the event of a necessary shutdown, the HA function is temporarily disabled by temporarily blinding it ("sterilizing"). Upon restart, the system automatically restores normal operation.
- Secure Retreat Mode & Infrastructure Discovery: RCCMD v5 leverages vCenter to actively discover vCLS , DHCP, DNS, as well as virtual switches and routers. With a single command, it places affected system VMs into "Retreat Mode," forcing their clean removal from the cluster and ensuring a secure physical shutdown.
- DRS Intervention: During the shutdown phase, the DRS is set to "Manual" status via API to immediately reduce CPU and network load and significantly speed up the process.

RCCMD in practice: The DRS endless loop

Practical example – The DRS endless loop (“The Never Ending Story”):

In highly available environments, we frequently observe a dangerous discrepancy.

If vCenter migrates VMs away from a host in an emergency, the Distributed Resource Scheduler (DRS) detects the available resources in real time and pushes data back to them in the background. This conflicting situation creates an endless loop. The shutdown command is repeatedly canceled until the UPS shuts down completely, potentially endangering running processes and incomplete write operations.



The solution – cluster sterilization & retreat mode:

RCCMD v5 proactively prevents this. The HA function is temporarily and controllably disabled ("sterilized") in advance. Affected system VMs are placed in "Retreat Mode" via vSphere Cluster Services (vCLS), which forces their clean removal. Additionally, we set the DRS to "Manual" via API, which immediately reduces network load.

4. Special scenarios: Storage (SAN/NAS) and network disruptions

Securing shared storage media and dealing with line failures require specific, normatively sound procedures.

Protection for shared storage:

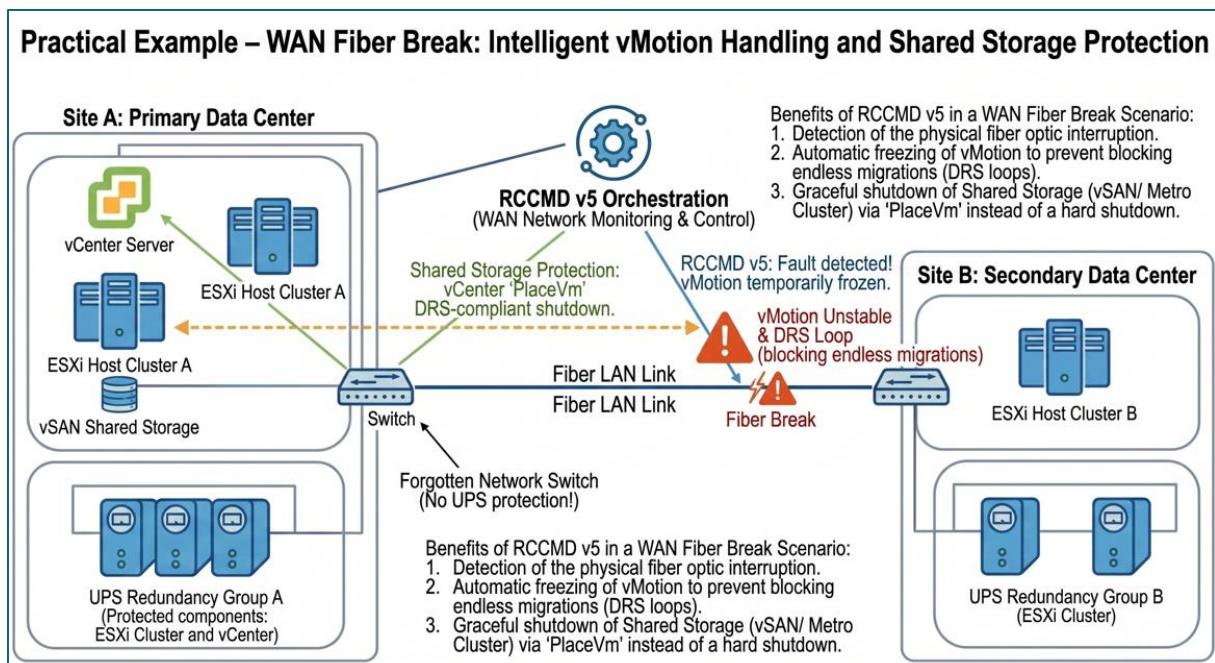
Shared storage media (e.g., vSAN or Metro Cluster) are typically ignored and hard-disabled by traditional scripts. RCCMD v5, however, utilizes the native vCenter method "PlaceVm" to ensure DRS-compliant and clean processing.

Response to fiber breakage

If fiber optic connections are interrupted, ongoing vMotion tasks become unstable. In such network disruptions, RCCMD v5 temporarily freezes vMotion. Pointless, endless migrations are blocked, allowing your technicians to safely begin troubleshooting.

RCCMD in practice: When the network abandons us

Practical example – Fiber breakage in the WAN



In practice, it repeatedly becomes apparent that network components are considered irrelevant infrastructure. We frequently observe that individual switches or routers are overlooked during security measures, which has far-reaching consequences for disaster recovery management.

A physical break in fiber optic connections within the WAN causes ongoing vMotion tasks to become unstable. Instead of resorting to blocking, endless migrations, RCCMD v5 detects the network disruption and temporarily freezes the vMotion process. This gives your technicians the necessary time to safely begin troubleshooting.

The solution for protecting shared storage:

Unlike traditional scripts, shared storage media (e.g., vSAN or Metro Cluster) are not ignored and hard-switched off, but rather shut down in a DRS-compliant manner using the native vCenter method "PlaceVm".

5. Multi-site management and redundant data center control

Infrastructure in transition

Large, distributed data center structures benefit from a central orchestration instance and consistent operational processes.

Redundancy group scaling:

Multiple UPS systems can now be combined into different redundancy groups and logically linked, even if they come from different manufacturers.

Parallel redundancy

In systems where the power modules provide redundant backup, a single RCCMD v5 ensures that the dependent data centers are only shut down when no power modules are actually available.

Cross-cluster control

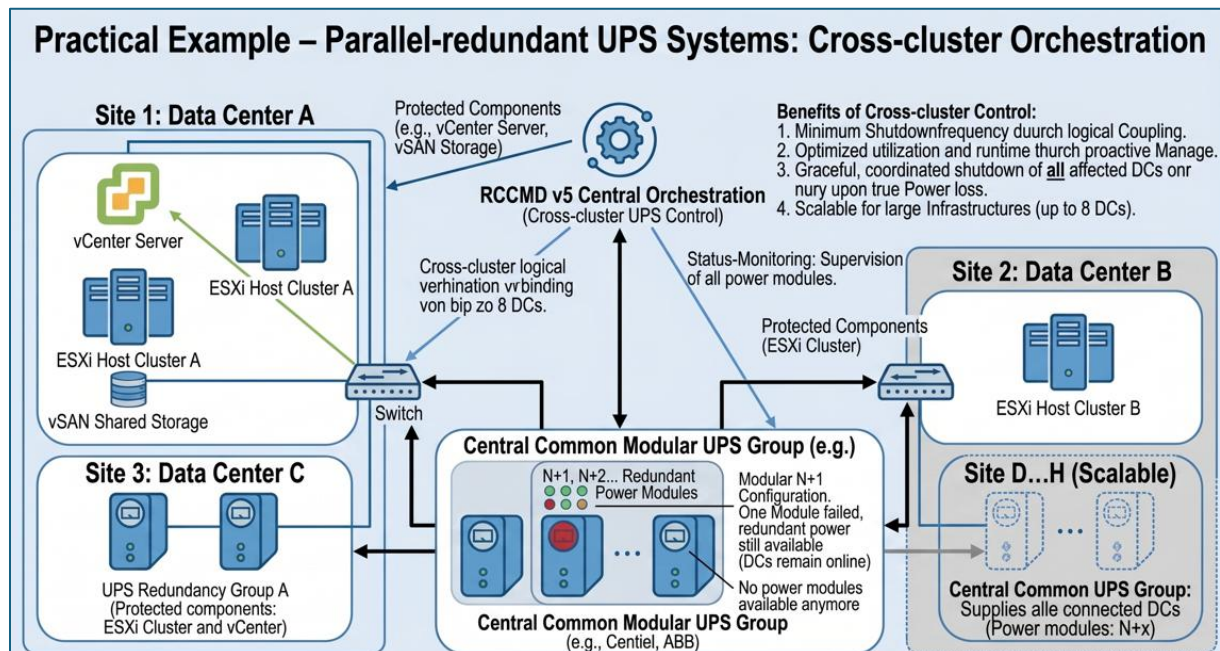
Administrators can coordinate up to eight data centers through a central management instance.

RCCMD in practice: When multiple UPS systems are being used for protection

Practical example – Parallel redundant UPS systems:

In large infrastructures, multiple data centers are often connected to the same UPS group (e.g., from CENTIEL or ABB), which are redundantly protected by different power modules. RCCMD v5 logically links these systems together.

The solution: Cross-cluster control:



RCCMD v5 provides all the necessary functions to ensure that all data centers connected to this group are only shut down when there are actually no more power modules available – this protects against unnecessary shutdowns.

Administrators can efficiently manage up to 8 data centers through a single instance.



6. Security, Simulation & Intelligent Trigger Logic

A professional IT platform requires not only automation but also transparency and strict access controls.

Principle of Least Privilege (RBAC)

The software integrates seamlessly into VMware's Role- Based Access Control system. RCCMD v5 consistently adheres to the principle. of Least Privilege and only requires the API permissions necessary for the respective functions.

Auditing & Dry-Run Mode

Syslog integrations allow for the seamless logging and evaluation of API calls. This enables you to precisely track how a shutdown would unfold without interrupting production beforehand.

Dynamic trigger criteria

The system doesn't react rigidly to mere battery percentage readings. It dynamically correlates the remaining autonomy time with the calculated migration and shutdown times of the clusters. In this way, the logic determines the absolute latest, but safest, time.

7. Intuitive administration & transparency

Quick and intuitive setup

We know how valuable your time is. That's why we placed particular emphasis on quick setup, intuitive operation, and a clear interface.

Drag and drop assignment

You can define UPS groups with just a few clicks and dynamically assign them to individual hosts, entire clusters, or data centers .

Visualized Infrastructure - Health

RCCMD v5 provides comprehensive status information about the current health of the cluster. An intuitive traffic light system displays the current status of detected servers; concise explanatory text appears directly when you hover your mouse over the tiles.

RCCMD in practice: Complex shutdown control implemented intuitively

Practical example – Redundancy group assignment

Imagine you are managing three UPS systems. RCCMD structures them based on their IP addresses. For example, you can assign one system to group 1 (as a single unit) and combine the other two systems into a redundancy group in group 2:

The screenshot shows the 'RCCMD-Redundanz aktivieren' (Activate RCCMD Redundancy) interface. On the left, there is a table with columns 'Gruppe' and 'Sender Adressen'. The table contains three rows, each with a checkbox and an IP address: 192.168.200.221, 192.168.200.225, and 192.168.200.222. The checkboxes for the last two rows are checked. On the right, there are two 'Redundancy Groups' panels. 'Group 2' contains the IP addresses 192.168.200.225 and 192.168.200.222, with a 'Redundancy Level' of 0. 'Group 1' contains the IP address 192.168.200.221, with a 'Redundancy Level' of 0.

Abb.: Bekannt gemachte USV-Anlagen werden innerhalb der Redundanzen 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.

Now that RCCMD knows exactly how to view the UPS systems and how they might cooperate to ensure emergency power, the second step is to determine which servers need to be shut down. RCCMD allows you to choose whether the hosts need to be shut down directly or whether a separate, stand-alone solution is also required.

You can therefore freely define whether the RCCMD Appliance:

- Individual hosts or standalone servers
- Cluster
- Data Center

explicitly include in the shutdown concept or exclude individual hosts, for example because a special shutdown solution with its own approach needs to run there, which was implemented completely independently of the rest of the infrastructure.

Administrators have full control over the appliance:

RCCMD v5 provides a quickly grasped interface through which administrators can immediately see the cross-reference to UPS systems and the respective protected servers.

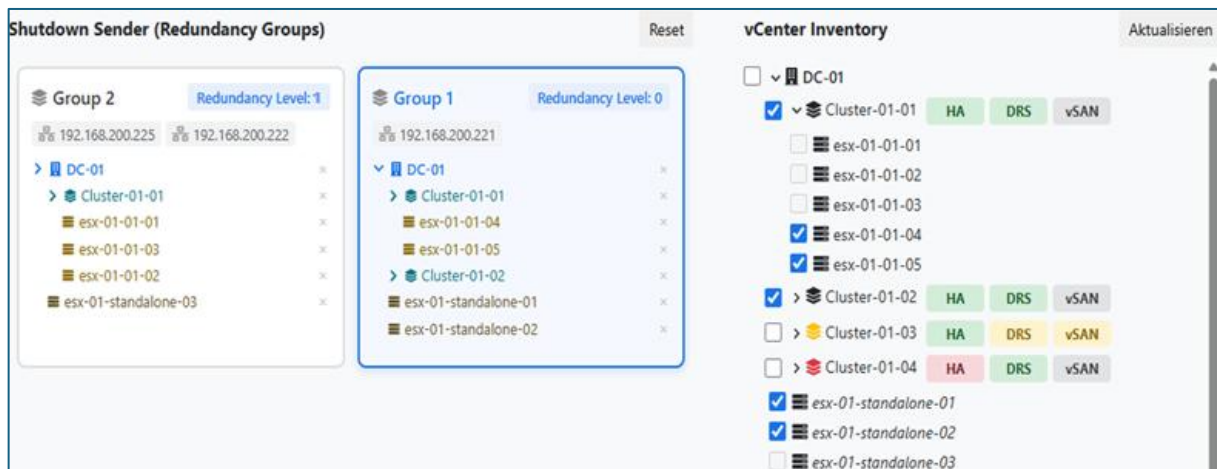


Fig.: Once RCCMD identifies which of the three UPS units are available and how they interact within redundancy groups, a shutdown sequence can easily be implemented with a single mouse click: The web interface provides a clear overview of the following information:

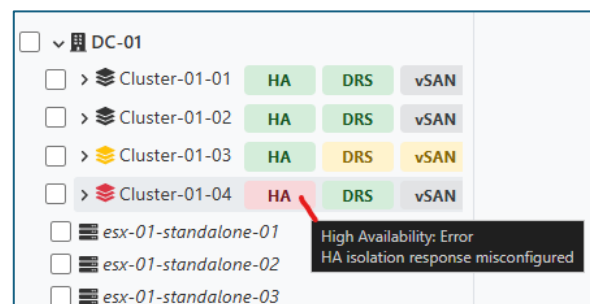
- Which UPS units are in redundancy mode (Group 2)?
The display shows not only the UPS units in a group but also the corresponding redundancy levels. RCCMD always knows why and when a shutdown must be performed: only when an RCCMD shutdown signal is received
- In which UPS group is the administrator currently located (Group 1)?
This group is highlighted in color.
- Which hosts/servers are currently assigned to this group?
The assigned hosts appear not only in the UPS group window but are also automatically displayed on the right with an active checkmark.

Administrators get a clear overview of all assigned servers. Servers can be easily added to or removed from the respective group by selecting or deselecting the checkbox.

Visualized Infrastructure - Health

Additionally, RCCMD provides an up-to-date overview of the health of every known server within the VMware environment:

An intuitive, easy-to-understand traffic light system shows the current status of found servers; concise information texts appear directly when you hover your mouse over the tiles.



In the event of a malfunction, administrators and system managers can directly check in RCCMD whether system integrity is guaranteed, without having to access central administration menus via a vCenter.

The individual shutdown within a large data center can be monitored directly.



Conclusion: A future-proof resilience concept

With RCCMD v5, the classic UPS-based shutdown software evolves into an intelligent orchestration solution for VMware-based infrastructures. Direct integration with vCenter, dynamic dependency detection, and coordinated control of clusters, storage, and network resources make disaster recovery processes more predictable and manageable.

Instead of solely reacting to shutdowns, RCCMD v5 strategically utilizes existing redundancies, creating the basis for longer availability, reduced administrative effort, and consistent control of even complex multi-site environments.

The likelihood of an emergency shutdown is minimized by consistently utilizing redundancies.

RCCMD Version 5 will continue to be offered as a lifetime license.

RCCMD licenses can continue to be used indefinitely as long as the underlying system environment (e.g., VMware or other integrated platforms) does not undergo any changes that require technical adjustments and thus a new license version due to manufacturer updates.

Should a system-related upgrade become necessary, we will provide a free upgrade to the corresponding new version within two years of the purchase date. Only after this period will a new license be required for a necessary system-related upgrade.

Regardless of the above, the following applies:

As long as your VMware environment or the systems used remain unchanged, the RCCMD license will also remain permanently valid and fully usable – for a lifetime if necessary.

Operational bottlenecks and cluster conflicts can be identified early and treated in a controlled manner.

At the same time, RCCMD v5 reduces administrative effort through automated processes.

With scalable multi-site capabilities, dynamic blueprint architectures and intelligent trigger logic, RCCMD v5 provides the foundation for the secure operation of modern and highly available infrastructures.