User Guide

PowerChute™ Network Shutdown v5.1

Nutanix™

990-4595L-001
05/2024

Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted by Schneider Electric to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Table of Contents

Introduction

PowerChute™ Network Shutdown (PowerChute) works in conjunction with the UPS Network Management Card (NMC) to provide network-based shutdown of multiple computer systems.

In the case of a UPS critical event, the software performs a graceful, unattended system shutdown before the UPS battery is exhausted. The number of protected systems is limited only by the capacity of the UPS.

View these Application Notes for detailed information on using PowerChute in specific environments.

After installation, it is essential to configure the software using the PowerChute Setup wizard. This ensures that PowerChute is aware of UPS critical events in order to protect your system.

UPS Configuration

This section contains information on the topics below:

- Network Configuration
- UPS Configuration Options
- Network Management Card Connection
- Advanced UPS Setups
- Outlet Group Registration
- Network Management Card Settings

Network Configuration

PowerChute can use IPv4 or IPv6 to communicate with the Network Management Card(s).

IPv6 support is available only for Network Management Card firmware 2.6.0.X or higher, and Network Management Card 3.

Select IP

If your computer has more than one IPv4 address you will need to select one of the available addresses. The IP address you select will be registered with the NMC and displayed in the NMC user interface under Configuration - PowerChute Clients.

IPv6 Configuration

If you are using IPv6 to communicate with the NMC(s), each network adapter on your machine will typically have several IP addresses assigned to it. Each adapter will have at least one link-local address and one global unicast address assigned to it.

Use the **Unicast IP Address** drop-down box to specify which address to use. The address type selected in this drop-down box must match the address type that you enter for the NMC(s) on the Network Management Card Connection page. This unicast address will be registered on the NMC(s) and displayed on the PowerChute Network Shutdown Clients page of the NMC.

> **fe80::88c8:3d95:bc02:74cc** is an example of a link-local address.
>
> **2001:112:1:0:88c8:3d95:bc02:74cc** is an example of a global unicast address.

Multicast Option

The NMC supports sending communication packets to an IPv6 Multicast address instead of sending unicast packets to each PowerChute agent. To use this, enable the **Multicast** check box and enter an IPv6 Multicast address.

The multicast address that is entered here will be registered on the NMC(s) instead of the unicast address and displayed on the PowerChute Network Shutdown Clients page of the NMC. The NMC(s) will send communication packets to that multicast address.

> **FF02::1** is an example of a **multicast address with link-local scope** so that only nodes on the same physical network segment will receive it. If using a link-local unicast address, you must use a multicast address with link-local scope.
>
> **FF0E::1** is an example of a **multicast address with global scope** and the NMC will use its global unicast address to send the packet. If using a global unicast address you must use a multicast address with global scope.

For detailed information, please view "The Communications Process of PowerChute Network Shutdown" here.

UPS Configuration Options

For a detailed overview of which UPS's support each configuration, please view the "PowerChute Network Shutdown Operating Modes and supported UPS Configurations" Application Note here.

Single-UPS Configuration

Single-UPS Configuration: All servers are protected by a single UPS. The UPS Network Management Card communicates with each server that has PowerChute installed.
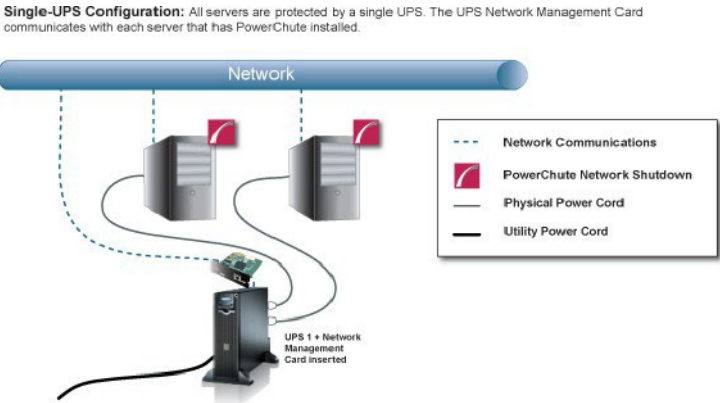
Redundant-UPS Configuration

Redundant-UPS Configuration: Two or more UPS's of the same model protect each server. Each UPS can support the server load on its own. All UPS Network Management Cards communicate with each server that has PowerChute installed.
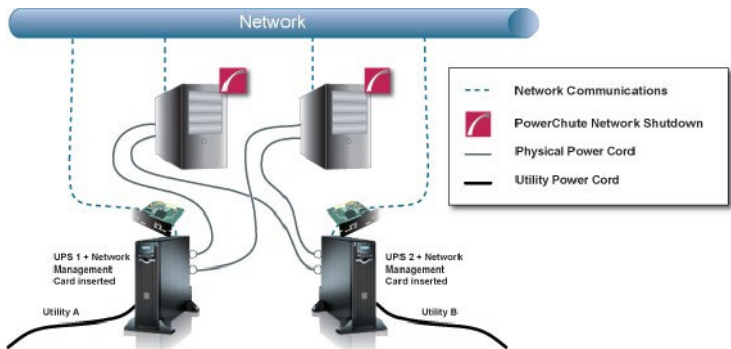
For detailed information, please view "Using PowerChute Network Shutdown in a Redundant-UPS Configuration" Application Note here.

Parallel-UPS Configuration

Parallel-UPS Configuration: Two or more UPS's of the same model protect the load and provide redundancy or increased capacity depending on the load. The UPS outputs are tied together so a single output goes to the load. All UPS Network Management Cards communicate with each server that has PowerChute installed.
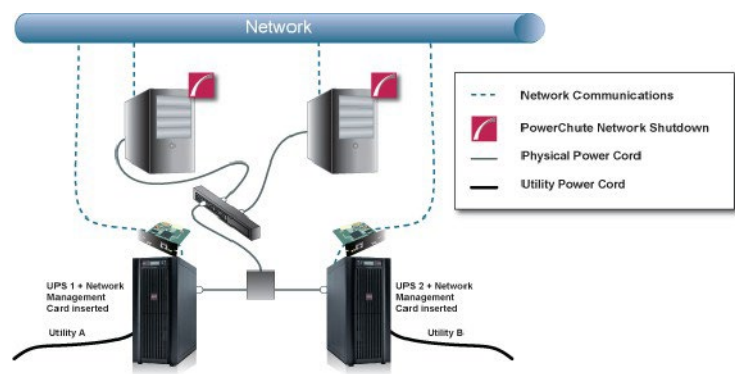
Note: To use the Parallel-UPS configuration, your UPS devices must already be configured to operate in parallel mode.

For detailed information, please view "Using PowerChute Network Shutdown in a Parallel-UPS Configuration" Application Note here.

Advanced UPS Configuration

Advanced UPS Configuration: PowerChute can monitor both Single UPS's and groups of Redundant UPS's protecting your virtualization environment. If using Redundant UPS groups, redundancy levels can be set on a per group basis e.g. N+1, N+2.
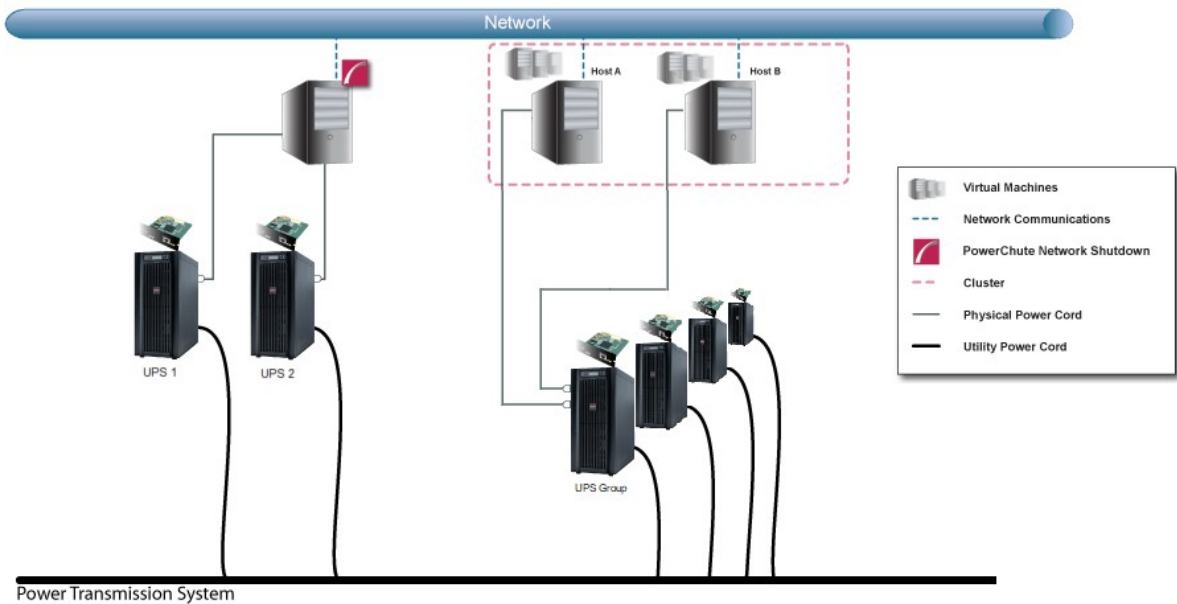
In an advanced UPS configuration, all hosts in the Nutanix Cluster must be protected by the same UPS or UPS group.

Network Management Card Connection

Network Management Card 2 firmware v6.8.0 and higher, and Network Management Card 3 firmware v1.1.0.16 and higher uses the HTTPS protocol by default. The default protocol for PowerChute is HTTPS which can be changed to HTTP, although it is not recommended.

The default port is 80 for HTTP, and 443 for HTTPS. Do not change this number unless you changed the port being used by your NMC.

For Redundant and Parallel configurations, you need to enter more than one **IP address** to enable communications with all the relevant NMCs.

For more information on UPS configurations and supported UPS models, view the Application Note "PowerChute Network Shutdown Operating Modes and supported UPS Configurations" here.

Add each IP address using the **+ Add IP Address** button. Enter the IP address of the NMC in the UPS. Click **OK**.

To edit an IP address, click the ✎ icon. To delete an IP address, click the 🗑 icon.

Certificate Management

The registration process will be unsuccessful if you attempt to register an NMC with an untrusted SSL certificate and the "Error registering with the Network Management Card(s)" error message will be displayed. Click the **Fix Issues** button to view the Certificate Management page where you can view the certificate details including the hostname, and expiry date.

You can only add the NMC host certificate to the PowerChute-keystore via this method. You can add CA certificates to the PowerChute-keystore using the keytool command. Please refer to the steps outlined in the "Changing the password for the Java Keystore" topic in the PowerChute Security Handbook for more information.

If you exit the PowerChute Setup wizard without adding the NMC SSL certificate(s) to the **PowerChute-keystore**, PowerChute will not be able to communicate properly with the NMC. Ensure that you complete the NMC registration process in the PowerChute Setup wizard and add any NMC SSL certificates to the **PowerChute-keystore** if you trust them.

Click the ⬚ button to view additional details of a certificate including:

- Version

- Subject

- Issuer

- Serial Number

- Valid From

- Valid To

- Public Key Information

- Signature Algorithm

- Certificate Chain

Check the checkbox and click the **Accept Certificate** button to add the displayed certificate to the **PowerChute-keystore**. If there are multiple certificates listed in the Certificate Chain, you can select them and import them at the same time. When all certificates have been validated, click **Next** to continue with your PowerChute setup. You should only add certificates you recognize and trust to the **PowerChute-keystore**.

PowerChute does not validate certificates added to the **PowerChute-keystore**. PowerChute will continue to trust certificates in the **PowerChute-keystore** after they have expired or been revoked. It is your responsibility to remove these certificates from the **PowerChute-keystore** once they are no longer needed.

Verify Certificates in PowerChute-keystore

You can verify that the displayed certificates were successfully added to the **PowerChute-keystore**:

1. Launch a terminal or command prompt and change the directory to the group1 directory of where PowerChute is installed. If the default location was chosen during installation, this will be:
   - C:\Program Files\APC\PowerChute\group1\ for Windows machines
   - opt/APC/PowerChute/group1 for Linux machines

2. Run the command:
   - `..\jre_x64\bin\keytool.exe -list -keystore PowerChute-keystore` for Windows machines
   - `../jre_x64/bin/keytool -list -keystore PowerChute-keystore` for Linux machines

3. When prompted, enter the password you created for the PowerChute-keystore.

> You must manually change the **PowerChute-keystore** password before you can access it. Please refer to the steps outlined in the "Changing the password for the Java Keystore" topic in the PowerChute Security Handbook for more information.

4. The certificates and their fingerprints will be displayed.

> The contents of the **PowerChute-keystore** can be viewed without a password. However, the integrity of the **PowerChute-keystore** cannot be verified without a password.

NMC PowerChute Support

In NMC 2 firmware v6.8.0 and higher and NMC 3 firmware v1.1.0.16 and higher, PowerChute support is disabled by default. This may result in an error while PowerChute registers with the NMC(s). If an error is displayed, log in to the NMC UI and ensure PowerChute support is enabled.

In the NMC Web UI, you must specify a user name and authentication phrase before PowerChute can be enabled. You must also choose the protocol used to communicate with PowerChute (HTTP/HTTPS). **NOTE:** The chosen protocol must be enabled on the NMC before PowerChute communications can be established. For more information, refer to the NMC User Guide.

Advanced UPS Setups
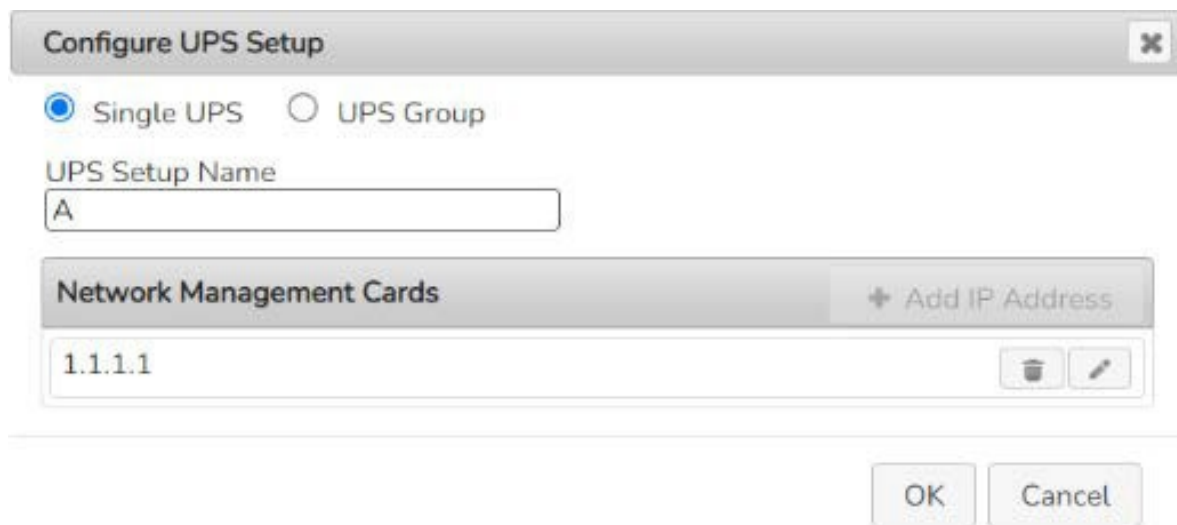
Add UPS Setup

In an Advanced UPS configuration, a single instance of PowerChute Network Shutdown can monitor multiple UPS setups and initiate graceful shutdown of equipment based on different redundancy levels. Each setup can be a single UPS or a UPS group. A single UPS setup is represented by the ![icon] icon. A UPS group is represented by the ![icon] icon.

For example, one setup may be a group of UPS's that are configured with N+2 redundancy. Another setup may be a single UPS.

On the **UPS Details** page of the Setup Wizard, click the **+ Add UPS(s)** button to create a new setup.
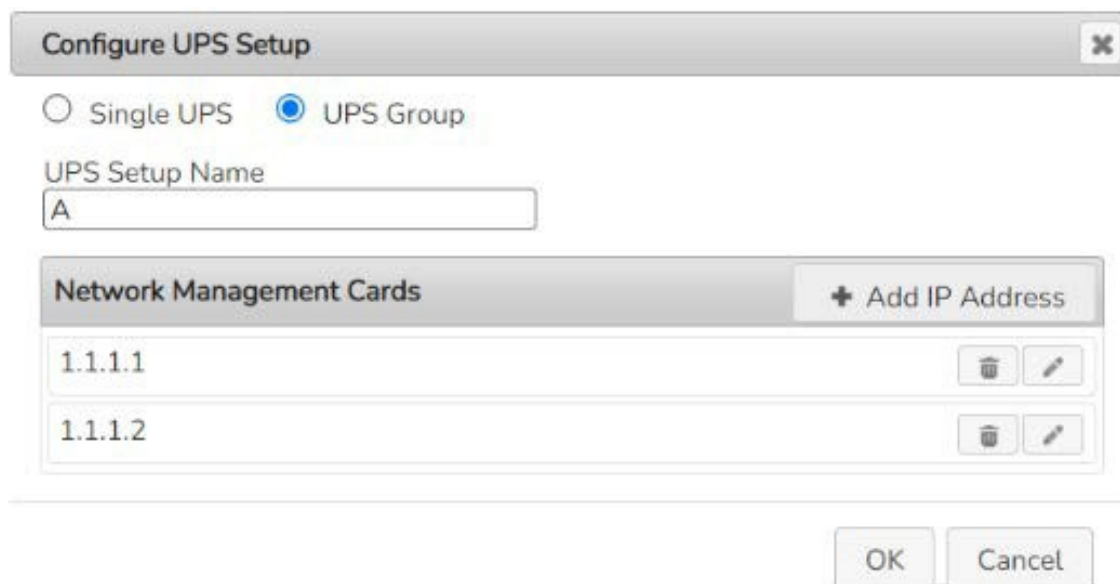
To create a setup with a single UPS, on the Configure UPS Setup dialog choose **Single UPS**:

1. Enter a **UPS Setup Name** (with a maximum of 20 ASCII characters)

2. Click the **+ Add IP Address** button and enter the IP address of the Network Management card in the UPS. Click **OK**.

3. Click **OK** to complete Single UPS Setup.

To create a setup with a group of UPS devices, choose **UPS Group**:

1. Enter a **UPS Setup Name** (with a maximum of 20 ASCII characters)

2. Click the **+ Add IP Address** button and enter the IP address of the Network Management card in the UPS. Click **OK**.

3. Repeat for each of the UPS devices to be added to the UPS group. A minimum of 2 IP addresses is required to set up a UPS Group.

4. Click **OK** to complete Group UPS Setup.

Repeat for each UPS setup required.

To edit a UPS Setup, click the ⟋ icon. To delete a UPS setup, click the 🗑 icon.

Click the **Next** button to go to the next step of the Setup Wizard.

PowerChute has been tested with a total of 16 NMCs in an advanced configuration. However it is possible to configure for more than 16 NMCs in this configuration.

For detailed information, please view the "Using PowerChute Network Shutdown in an Advanced Redundant Setup" Application Note here.

Outlet Group Registration

If your UPS supports outlet groups you must specify which one the server is being powered by so that PowerChute can monitor it for shutdown events and also issue turn-off commands to that outlet group.

If PowerChute is re-configured to use a different UPS in an Advanced UPS Configuration, you may not be able to map Hosts to the new UPS on the Host Protection page. This only occurs if the new UPS has the same UPS Setup name but a different outlet group configuration to the original one. To reconfigure a PowerChute installation with a new UPS under the same Setup name, use a different UPS Setup name when re-running the Setup Wizard to change the UPS.

 It is not supported to map UPS outlet groups when PowerChute is configured with Nutanix.

UPS Shutdown Behavior in Mixed UPS Environments

If your servers are being powered by a mix of outlet-aware UPS's (e.g. SMX/ SMT) and non-outlet-aware UPS's (e.g. SU/ SUA) in a Redundant UPS Configuration, PowerChute only provides the option to turn off the UPS and not the outlet group.

Your servers are still protected if there is a UPS critical event or if the outlet group is commanded to shut down e.g. via the NMC User Interface.

Network Management Card Settings

For Single and Redundant and Parallel UPS configurations, the IP address of each NMC that PowerChute is communicating with is displayed under the **UPS Configuration** menu option.

For Advanced UPS configuration, each UPS Setup is displayed as a menu item and the IP address of the NMC(s) with which PowerChute is communicating is displayed under each UPS setup.

Click on the IP address to view the UPS information specific to that NMC.

UPS information displayed includes:

- NMC IP Address
- UPS model name
- UPS configuration

The NMC Host Name from the NMC's DNS settings page under Network - DNS - Configuration is also displayed. This is not the same as the UPS name that can be set under Configuration - UPS General on the NMC.

Clicking the **Launch** button opens the NMC user interface.

Nutanix Configuration

To enable Nutanix™ Acropolis Hypervisor (AHV) support configuration options in the PowerChute Setup wizard, **Enable Nutanix AHV Support** must be selected during the installation.
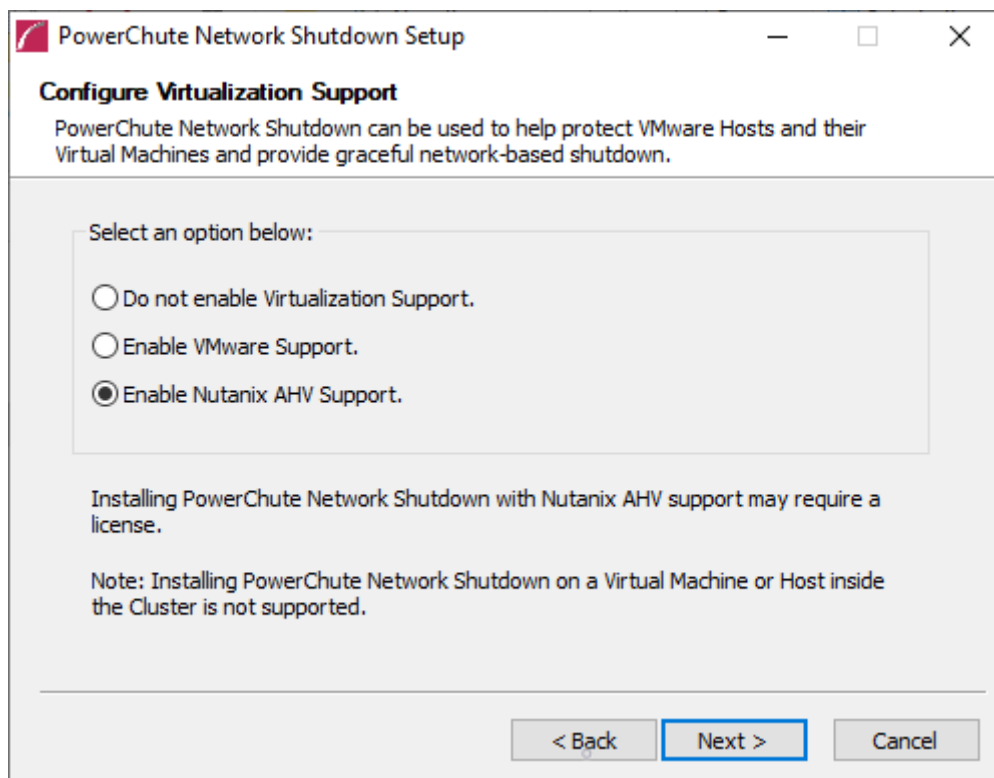
For more information on configuring PowerChute with Nutanix, see the PowerChute Network Shutdown Installation Guide.

CVM/Cluster Details

This screen appears in the PowerChute Setup wizard and the details entered here are used to connect to your Nutanix Controller Virtual Machine or Cluster. The recommended configuration is to connect to your Nutanix Cluster.

You can authenticate the connection to your Controller VM or Cluster using the following options:

- Enter your CVM/Cluster IP address, Controller VM/Cluster password **and** AHV Host password. Both passwords must be set to connect to your Controller VM/Cluster. If the **Nutanix AHV Host Password** field is left blank in the PowerChute Setup wizard, the CVM/Cluster password specified will be copied to this field.
- Enter your CVM/Cluster IP address, the SSH key file path and its passphrase, if available.

These connection settings can be edited later through the PowerChute UI in the **Communication Settings** screen.

If both authentication options are specified in the PowerChute Setup wizard, PowerChute will use the passwords to connect to the Controller VM/Cluster.

NOTE: You must use the "nutanix" user account credentials to connect to the Cluster/Controller VM. You cannot use Prism user account credentials to connect.

The SSH key file, if configured, must be located in the user_files folder, or a sub-folder, in the PowerChute installation directory. If the default installation directory was chosen during installation, this location will be:

- C:\Program Files\APC\PowerChute\user_files for Windows systems

- /opt/APC/PowerChute/user_files/ for Linux systems

NOTE: If you are upgrading to PowerChute v4.4, any SSH key files used in a previous version of PowerChute must be manually added to the user_files folder. If the key files are not added to the directory, you will see the below error in the Event Log:

```
ERROR: The ini contains an invalid value for ssh_keyfile_path in
nutanixClusterDetails.
```

It is strongly recommended you validate your configuration after an upgrade.

In the **Communication Settings** screen in the PowerChute UI, if you wish to change your authentication method, PowerChute will erase your previous authentication details. For example, if you connected to your Nutanix Cluster using the passwords option in the PowerChute Setup wizard and you want to use a SSH key file instead, when the **Path to SSH Key File** field is edited and the changes are applied, PowerChute will erase your configured passwords.

If you are authenticating the connection to your Controller VM/Cluster using passwords, you can use the **Check Nutanix AHV Host Details** button in the UI to check if your AHV hosts are online and accessible.

NOTES:

- If you do not specify a **Nutanix AHV Host Password** in the PowerChute Setup wizard, this field will be set to the password specified for **Nutanix CVM/Cluster Password**.

- If you specify a **Nutanix AHV Host Password**, you must click the **Apply** button before you can check to see if your AHV hosts are online.

- If the **Nutanix AHV Host Password** and the **Nutanix CVM/Cluster Password** are not the same, you cannot update the **Nutanix AHV Host Password** via the PowerChute UI. See Nutanix Troubleshooting.

CVM/Cluster Details

Nutanix Host Protection

Once connected to the Nutanix Cluster, PowerChute displays all of the Nutanix hosts in the inventory in a tree view. From this screen you can select the hosts that PowerChute should protect.

Single, Redundant, and Parallel-UPS configurations

Specify the hosts in the left-hand panel you want to protect by dragging them to the right-hand panel of this screen. Each host listed in the left-hand panel must be added to the right-hand panel of this screen before you can proceed with your configuration.
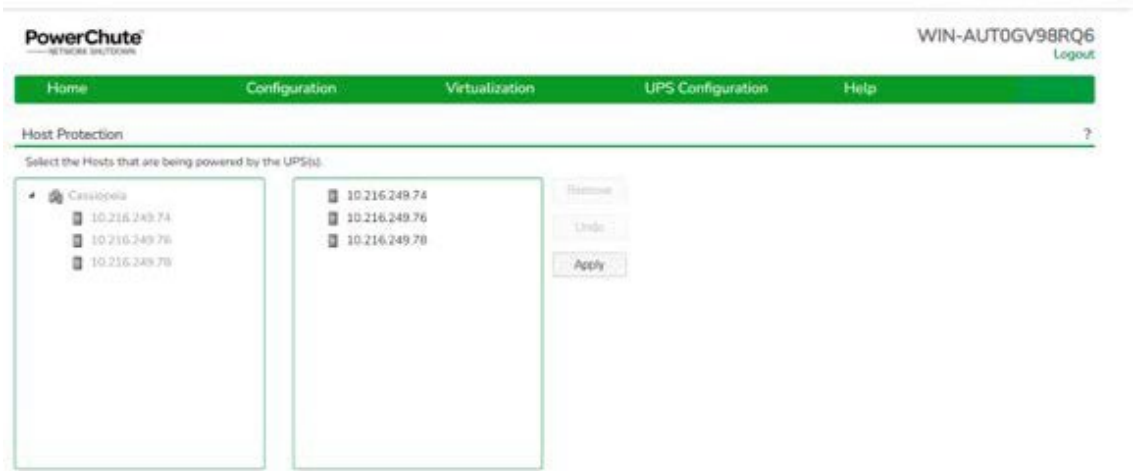
When a critical UPS event occurs, PowerChute will shut down hosts in the order that they appear in the right-hand panel. You can change this order by clicking on a host in the right-hand panel and dragging it up and down.

Advanced UPS configuration

Advanced UPS configuration

In an advanced UPS configuration, the Nutanix hosts are powered separately by one or more UPS device(s) in a UPS Setup. The right-hand panel shows the UPS Setups that have been configured and are monitored by PowerChute. You need to associate each Nutanix host in the left-hand panel with the UPS by which it is powered. To do this, drag each host to the UPS/UPS group in the right-hand panel.

In an advanced UPS configuration, all hosts in the Nutanix Cluster must be protected by the same UPS or UPS group.

For this configuration, PowerChute must be installed on a physical Windows machine outside the Cluster.

If the IP address/Hostname of any of the hosts are changed, it will be necessary to re-associate the hosts with the UPS devices.

Physical UPS Setup Power Protection

In Advanced UPS Setups, PowerChute can monitor UPS devices which are powering equipment outside a Nutanix Cluster (e.g. a Storage Array Device or a physical server machine running PowerChute).

For more information see Shutdown Settings for Advanced UPS Setups.

> On the **Host Protection** page, do not link Nutanix hosts with the UPS devices that are powering the physical equipment.

The following additional options will then be displayed on the Shutdown Settings page:

- **Shutdown PowerChute Server -** This is enabled by default and is used to gracefully shut down the physical machine running PowerChute. This option can be disabled if the UPS is powering a Storage Array Device.
- **Execute Virtualization Shutdown Sequence -** This triggers a shutdown sequence using the actions configured on the Virtualization Settings page. This option should be enabled for all UPS Setups that are powering physical equipment.

PowerChute User Interface - Configure Shutdown Conditions

PowerChute Setup - Configure Shutdown Conditions

Virtualization Settings

Virtual machine (VM) settings like VM Shutdown, Controller VM Shutdown, and Cluster Shutdown can be configured in the **Virtualization Settings** screen.
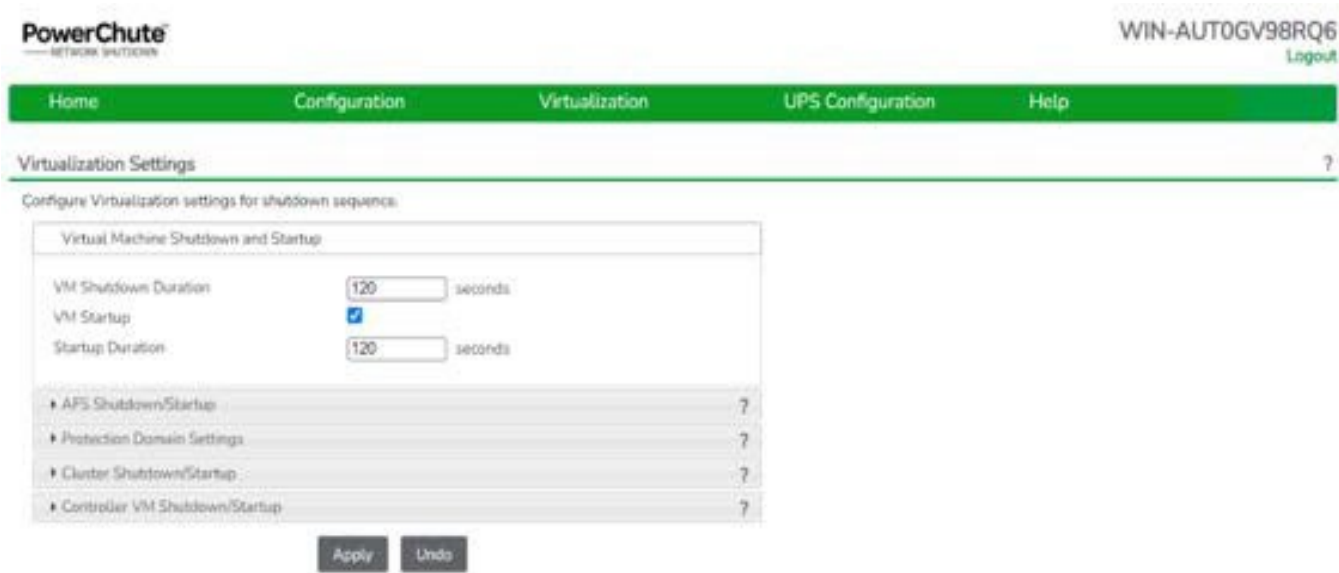
Virtualization Settings

For more information see:

- Virtual Machine Shutdown/Startup
- Controller Virtual Machine Shutdown/Startup
- Acropolis File Services Shutdown/Startup
- Cluster Shutdown/Startup

Virtualization Settings in Advanced UPS Configuration

In an advanced UPS configuration, settings entered on this page will be applied to all UPS Setups if the **Apply Virtualization**

Settings to all UPS Setups checkbox is selected. This checkbox is enabled by default.

If you have applied settings to individual UPS Setups, you should uncheck this option to prevent them from being overwritten.

Individual UPS Setup Settings applied

Virtual Machine Shutdown and Startup

The **Duration** field is the time allowed for all the VMs to gracefully shut down (AFS VMs and Controller VMs are not included). If the VMs are shut down before the Duration time, PowerChute waits until this time has elapsed before proceeding to the next step in the sequence.

> ⚠️ Using the **Duration** field, you must allow sufficient time for all your VMs to gracefully shut down before the hosts are commanded to shut down.

VM shutdown unsuccessful

When PowerChute issues a VM shutdown command, PowerChute will use the time specified in the **Shutdown Duration** field to allow VMs to gracefully shut down. If VM shutdown is unsuccessful, PowerChute logs the "Nutanix User VMs cannot be gracefully shut down. Powering off UVMs." event in the Event Log and will attempt to power off the VMs. PowerChute will wait 15 seconds to power off the VMs, and if this is unsuccessful, they will be forced off. PowerChute will wait an additional 15 seconds to force off the VMs, and if they cannot be forced off, PowerChute logs the "Insufficient time configured to shut down VMs on Cluster [Cluster]." event.

The 15 seconds durations PowerChute uses to power off and force off your VMs are taken from the configuration file.

Re-starting after a shutdown

Selecting the **VM Startup** checkbox re-starts any VMs that were shut down when a UPS critical event has been resolved and the Nutanix Hosts are powered on. PowerChute first checks that all hosts are available, all Controller VMs are running and the Cluster is available before starting the VMs.

If VMs are in the process of being started when a critical event occurs, PowerChute waits for the **Duration** time to elapse before shutting down VMs. This is to ensure that the VMs are shut down gracefully.

Nutanix Files (Acropolis File Services) Shutdown/Startup

The **AFS Shutdown** checkbox is enabled by default, and this option should be left enabled to allow graceful Cluster shutdown. In the event of a shutdown, PowerChute stops the AFS service, which shuts down the AFS VMs. This step occurs after the User VMs are gracefully shut down.

The **Duration** field is the time allowed for the AFS service and VMs to gracefully shut down and start up following a UPS critical event.

> ⚠️ Using the **Duration** field, you must allow sufficient time for all your AFS VMs to gracefully shut down. If the AFS VMs are not shut down, this may prevent the Cluster and Controller VMs from shutting down.

AFS Shutdown/Startup

Re-starting after a shutdown

Selecting the **AFS Startup** checkbox re-starts the AFS service, which also powers on any AFS VMs that were shut down when a UPS critical event has been resolved and the Nutanix Hosts are powered on.

If the AFS VMs are in the process of being started when a critical event occurs, PowerChute waits for the **Duration** time to elapse before shutting down the VMs. This is to ensure that the VMs are shut down gracefully.

Protection Domain Settings

A protection domain is a collection of VMs that are backed up or replicated on a schedule to recover data. The **Abort Active Replications** checkbox is enabled by default, and this option should be enabled if your protection domain is configured to replicate on a schedule.

If enabled, PowerChute will wait the time specified in the **Duration** field before aborting any active protection domain replications in the event of a critical UPS event.

NOTE: The **Duration** field will only be taken into consideration if there are active replications when PowerChute reaches this step in the shutdown sequence. If there are no active replications this duration will not be included in the shutdown sequence.

Protection Domain Settings

Cluster Shutdown/Startup

Cluster Shutdown occurs after PowerChute has completed the previous steps in the shutdown sequence: User VM Shutdown, AFS Shutdown, and abort active replications.

Cluster Shutdown/Startup

If the Cluster is shut down before the Duration time, PowerChute waits until this time has elapsed before proceeding to the next step in the sequence (shutting down the physical PowerChute host).

> ⚠️ Using the **Shutdown Duration** field, you must allow sufficient time for your Cluster to gracefully shut down before the physical PowerChute host is commanded to shut down.

Re-starting after a shutdown

The time specified in the **Startup Duration** field will be the time, in seconds, PowerChute will wait after issuing the Cluster start command before proceeding with the next steps in the startup sequence. The Cluster is re-started after the Controller VMs are powered on.

Controller Virtual Machine Shutdown/Startup

A Controller Virtual Machine runs on each node in a Nutanix block and is responsible for running the Nutanix Cluster. Controller VM Shutdown is enabled by default. In the PowerChute shutdown sequence, the Controller VM is shut down after all other VMs in the Cluster, and the Nutanix Cluster itself are shut down.

The **Duration** field is the time allowed for all the Controller VMs to gracefully shut down. If the Controller VMs are shut down before the Duration time, PowerChute waits until this time has elapsed before proceeding to the next step in the sequence.

> ⚠️ Using the **Shutdown Duration** field, you must allow sufficient time for all your Controller VMs to gracefully shut down before the hosts are commanded to shut down.

Controller VM Shutdown/Startup

Re-starting after a shutdown

Selecting the **Controller VM Startup** checkbox re-starts any Controller VMs that were shut down when a UPS critical event has been resolved and the Nutanix Hosts are powered on. PowerChute first checks that the host is available.

If Controller VMs are in the process of being started when a critical event occurs, PowerChute waits for the **Startup Duration** time to elapse before shutting down Controller VMs. This is to ensure that the Controller VMs are shut down gracefully.

> ⚠️ It is recommended to wait at least 5 minutes after Controller VM startup to ensure all services are running before re-starting the Cluster. You should account for this using the **Startup Duration** field.

Virtual Machine Prioritization

Use **Virtual Machine Prioritization** settings to specify the order in which VMs shut down and power on. VM Prioritization is configured in the main PowerChute interface and is disabled by default.
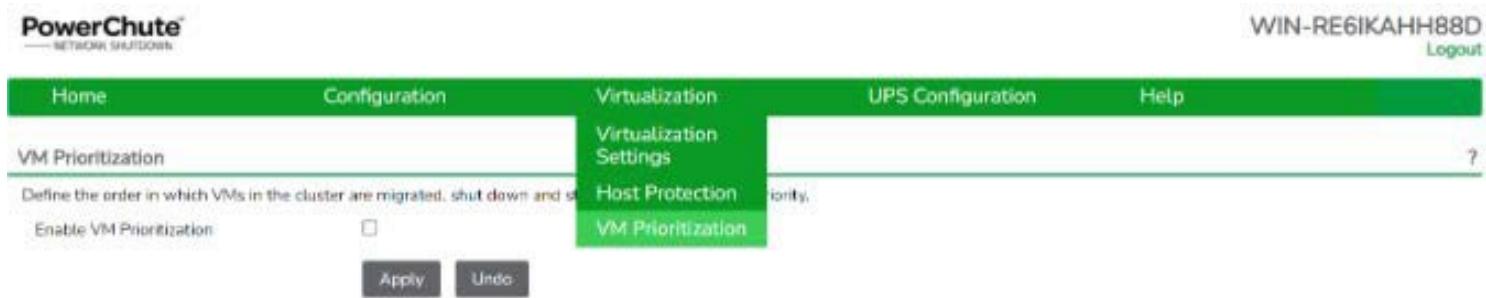
Enable VM Prioritization screen

To enable VM Prioritization, select the **Enable VM Prioritization** checkbox. Three options display:

- Prioritize VMs (below)
- Set VM Shutdown Duration
- Set VM Startup Duration

Prioritize VMs

Virtual Machines can be grouped into five priority groups – High, Medium, Low, Group 1 and Group 2. When VM Prioritization is enabled, an **inventory view** of the datacenter, clusters, and VMs appears on the left. On the right, the High, Medium, Low, Group 1 and Group 2 priority groups are listed.

NOTE: Controller VMs and AFS VMs are not displayed and cannot be added to a priority group.

For PowerChute to correctly identify Clusters and VMs, their names must be unique. It is not supported to have more than one VM with the same VM name.
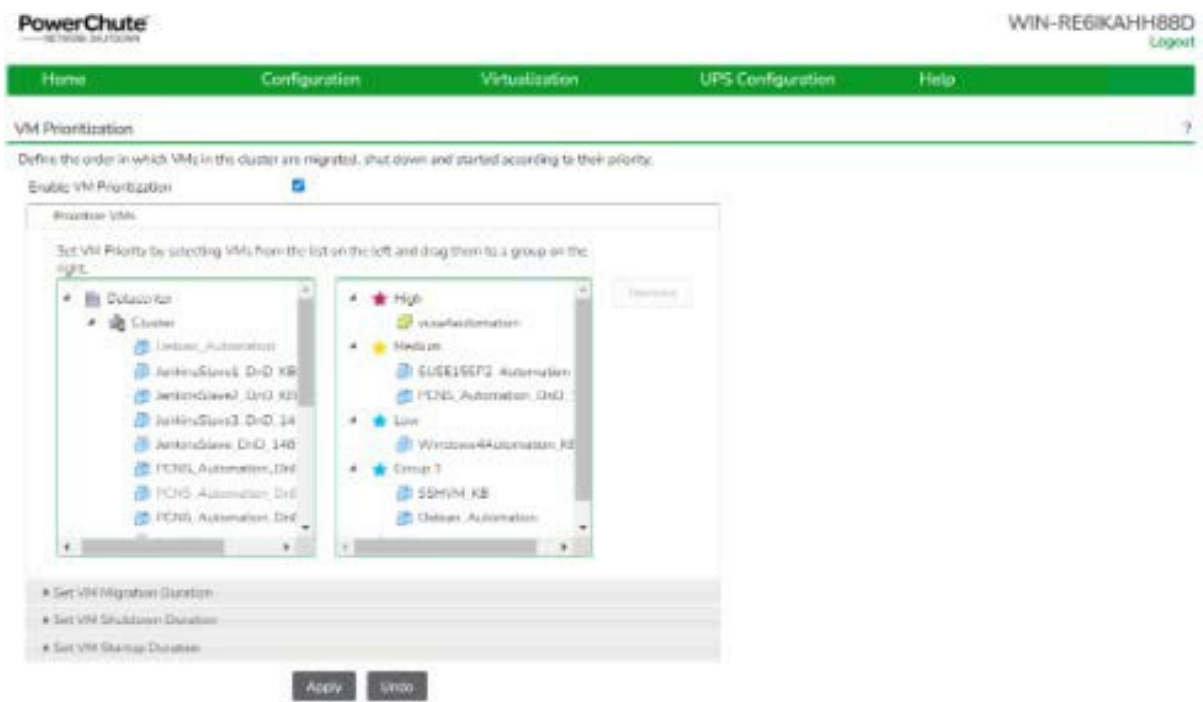
Datacenter inventory view and VM Priority Groups

You can assign a VM to a priority group by clicking on a VM on the left-hand side and dragging it to a priority group on the right.

Move VMs between priority groups by dragging them from one group to another. To remove a VM from a priority group, select the VM and click the **Remove** button. Any VM in the inventory that is not assigned to a priority group is considered to be **Un-prioritized**.

Setting Priority Group Durations

You can configure durations for each priority group, for VM Shutdown and VM Startup.

For Priority Groups:

- **VM Shutdown duration** sets the time allowed for all VMs in the Priority Group to shut down gracefully. This also represents the delay between shutting down VMs for each Priority Group.

> ℹ️ The **VM Shutdown Duration** can be set to 0 seconds for any priority group to handle any special VMs that need to be shut down later in the shutdown sequence via a command file or SSH action.
>
> If you set a 0 second shutdown duration for a priority group, the shutdown action will be skipped for all VMs in that priority group.

- **VM Startup duration** sets the time allowed for all VMs in the Priority Group to start up. This also represents the delay between starting VMs for each Priority Group.

Set VM Operation durations - VM Shutown and Startup

You can set durations for the VM in the High, Medium, Low, Group 1 and Group 2 priority Groups, and for VMs that are Un-prioritized. When VM Prioritization is enabled for the first time, High, Medium, Low, Group 1 and Group 2 durations will have a default value of 0.

Durations for Un-prioritized VMs are automatically set to the global duration values for VM Shutdown and VM Startup, as configured on the Virtualization Settings page.

VM Startup durations can be configured to have a value of zero, to skip the start up of VMs after a critical event is resolved. If VM Startup is set to zero for a priority group, VMs will not start up when the critical event is resolved.

A warning will display in the **VM Prioritization** screen if a VM Shutdown Duration is set to zero for any priority group.

> ⚠️ If the **VM Shutdown Duration** is set to zero for a priority group, the VMs in that group will not be shut down. This may result in the Nutanix Controller VMs and the Cluster unsuccessfully shutting down as VMs are still running.
>
> To ensure graceful shutdown of your Nutanix Cluster, configure a VM Shutdown Duration for priority groups in the **VM Prioritization** screen, or configure a command file or SSH action to shut down VMs in priority groups later in the shutdown sequence.

Global Virtualization Settings and VM Prioritization

When VM Prioritization is enabled, the VM Startup and VM Shutdown durations set on the Virtualization Settings page automatically match the sum of the respective priority group durations set on the VM Prioritization page.

For example, if VM Shutdown durations set on the VM Prioritization screen are as follows:

- High: 90 seconds
- Medium: 60 seconds
- Low: 60 seconds
- Group 1: 30 seconds
- Group 2: 30 seconds
- Un-prioritized: 30 seconds

Then, the VM Shutdown duration on the Virtualization Settings page is automatically set to: 90 + 60 + 60 + 30 + 30 + 30 = **300 seconds**

Virtualization Setting page - VM Shutdown duration

If Advanced UPS Configuration is used, the durations for each UPS Setup are also changed to reflect the sum of the respective priority group durations for VM Startup and Shutdown.

On the Virtualization Settings page when VM Prioritization is enabled, VM Startup and Shutdown durations become read-only and are automatically populated, as described above. If VM Prioritization is disabled, the durations retain the values set by VM Prioritization, but become editable once more.

Prioritized VM Operations Sequence

Operations such as VM Shutdown and VM Startup can be performed for VMs in a priority group.

For VM Startup, the order in which priority groups are processed is as follows:

For VM Shutdown the order in which priority groups are processed is:

The sequences below describe the VM Shutdown and Startup Sequence for all UPS

Configurations. In this scenario:

- VM Shutdown is enabled
- VM Startup is enabled

Priority Group VM Shutdown
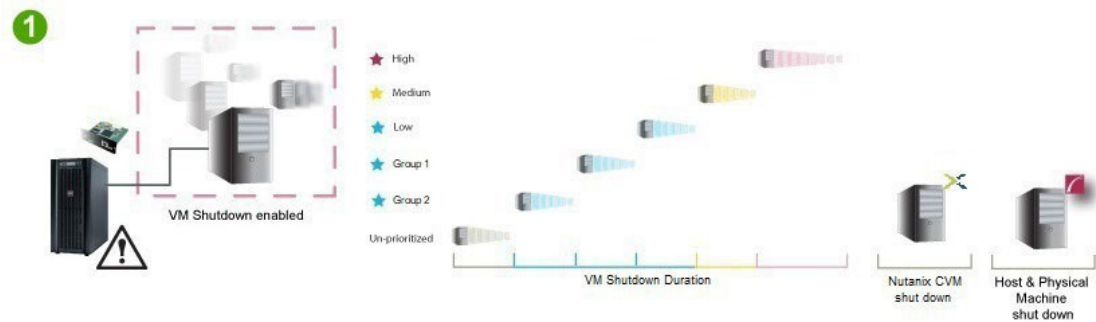
As the critical event continues, PowerChute begins sequenced VM Shutdown. First, the un-prioritized VMs are shut down sequentially. After the duration for un-prioritized VMs elapses, the Group 2 priority VMs are shut down sequentially, followed by Group 1 priority VMs, Low priority VMs, Medium priority VMs and finally the High priority VMs are shut down sequentially. When all priority group VMs have been shut down, PowerChute shuts down the AFS VMs, the Nutanix Cluster, and Controller VMs. PowerChute then shuts down the hosts and the physical PowerChute server.

Priority Group VM Startup
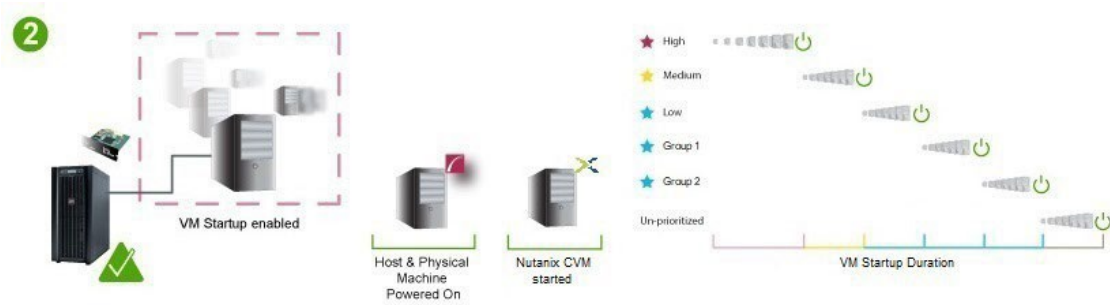
When the UPS critical event is resolved and the hosts and physical machine running PowerChute are powered back on, the Controller VM starts up, followed by the Cluster and AFS VMs, if running. PowerChute begins to start the High priority VMs with respect to their VM startup duration. When the High priority startup duration elapses, the Medium priority VMs are started, followed by the Low priority VMs, Group 1 and Group 2 priority VMs, and finally, the un-prioritized VMs are started.

Priority Group VM Operations in Advanced UPS Configuration

In Advanced UPS configuration, all hosts in the Nutanix Cluster must be protected by the same UPS or UPS group..
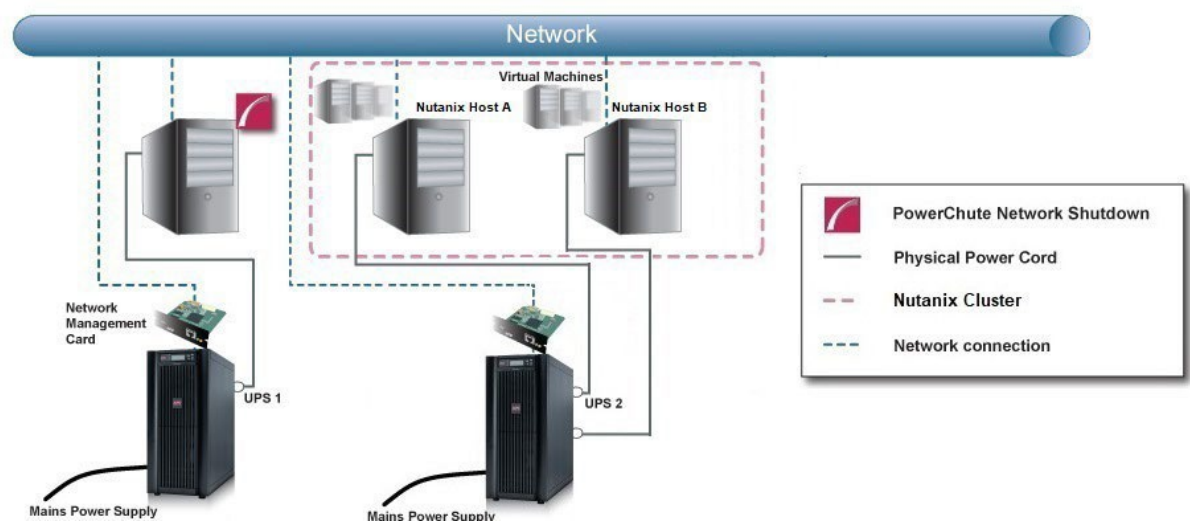
In this example, UPS 2 may experience a critical event at a different time to UPS 1. If the UPS Setups for Host A and B have VM Prioritization enabled, the VM operations that are performed on the priority groups of the two hosts will occur at different times. For example, if UPS 2 experiences a critical event 2 minutes before UPS 1, the High priority VMs on Host B may be shut down at the same time as the Low priority VMs on Host A. VM operations on priority groups occur at the host level.

Shutdown Settings

The Shutdown Settings page enables you to configure UPS turnoff and the shutdown command files.

- UPS Shutdown
- Shutdown Command Files
- Shutdown Settings for Advanced UPS Configurations

UPS Shutdown

The default setting is **Do not turn off the UPS**.

You can select **Turn off the UPS** if you want to preserve battery power. Some UPS's do not support UPS turnoff through PowerChute or the NMC. For these models, it can only be done at the UPS itself. Please check your UPS documentation to ensure your model supports UPS turnoff.

If your UPS has Switched Outlet Groups, then the **Turn off the UPS Outlet Group** option enables you to turn off the outlet group that supplies power to the PowerChute protected server after a critical event occurs.

The default behavior for most UPS's if they are turned off following an on-battery shutdown is that they will turn on again once input power is restored.

The **On-Battery Shutdown Behavior** setting can be found in the NMC under Configuration – Shutdown where you can change the behavior to Turn off and Stay off if required.

Turn Off Single UPS On Battery in a Redundant-UPS Configuration

This is not available for an Advanced UPS Configuration that contains UPS Setups with Redundant UPS devices.

In a Redundant UPS configuration you have the option to turn off one of the UPS's after it has switched to battery power. This is designed to prolong the battery life and preserve the battery power of the UPS. If using this feature on a UPS that supports outlet groups the option "Turn off the UPS" should be enabled.

The load is still protected by the other UPS in the configuration.

After the specified delay, PowerChute will issue a command to gracefully turn off the UPS.

If one UPS is on battery and another UPS switches to battery before the configured delay for Single UPS turn off has elapsed, then the first UPS will not be turned off.

If the shutdown action is enabled for the **On Battery** event, a Multiple Critical event condition will occur if a second UPS switches to battery power (after the first UPS has been commanded to turn off by PowerChute). When this occurs the shutdown sequence will start after 10 seconds.

Shutdown Command Files

A Shutdown Command File can be configured to run if a UPS critical event is triggered.

Full path to command file: You must specify the full path name of the command file, including the disk drive or volume name. For Linux and Unix systems, the file should execute permissions of **chmod +x [command file name]**.

> The command file must be located in the user_files folder, or a sub-folder, in the PowerChute installation directory. If the default installation directory was chosen during installation, this location will be:
>
> - C:\Program Files\APC\PowerChute\user_files for Windows systems
>
> - /opt/APC/PowerChute/user_files/ for Linux systems

NOTE: If you are upgrading to PowerChute v5.1, any command files used in a previous version of PowerChute must be manually added to the user_files folder. If the command files are not added to the directory, you will see the below errors/warnings for the ShutdownStarting event, and all events configured to run a command file, in the Event Log:

```
ERROR: Event ShutdownStarting is enabled for command file execution,
but an invalid value for shutdownCommandFile is specified.

WARNING: Disabling command file execution for event ShutdownStarting
due to bad parameters. Please validate the configuration.
```

It is strongly recommended you validate your configuration after an upgrade.

Duration: Enter the number of seconds that the shutdown command file requires to execute.

> **NOTE**: For Advanced UPS Configurations, if there are different command files configured for each UPS Setup, PowerChute may need to wait for all command files to finish executing before proceeding with the final steps in the shutdown sequence. This is dependent on the timing that UPS critical events occur on each UPS Setup. PowerChute will automatically increase the Outlet Group Power Off delay or Maximum Required delay (non-outlet aware UPS) to include the combined total of the shutdown command file durations for each UPS Setup. This can impact the runtime available on the UPSs during a shutdown. To accommodate this, set the low battery duration on the UPSs accordingly.

Execute Command File After Host Shutdown: Enable this option to execute the command file following Host Shutdown. This option is only available when PowerChute is installed on a physical machine, and not on a VM.

D**elay:** Enter the number of seconds that the Host requires to shut down, before the command file is executed.

> You must determine the time required for your command file to execute. PowerChute cannot determine whether the command file has completed, so it will wait only the amount of time entered before triggering an operating system shutdown.

The command file runs using the local system account. For Linux/Unix the command file must be executed with root privileges. PowerChute cannot execute programs that require interaction with the desktop; only command line enabled programs are supported.

Shutdown Settings for Advanced UPS Configurations

With Advanced UPS configurations, PowerChute can monitor multiple UPS setups, including single UPS devices and groups of redundant UPS devices that you have created (see "Advanced UPS Setups").

For each setup, you need to specify the following:

Field	Description
Number of UPS's required to power load	Set this value to the minimum number of UPS's that must be available to support the equipment that is being powered by the UPS's in the setup. The value set here will be subtracted from the total number of UPS's in the setup and used to calculate the number of additional (redundant) UPS's. In redundancy terminology, this is the N in N+x. This setting is not displayed for UPS Setups with a Single UPS device.
Number of additional (redundant) UPS's	This will appear in a setup with more than one UPS. It represents the number of extra UPS's in the setup. This option is associated with the number of UPS critical events required to trigger shutdown:

Redundancy level	No. of critical events that will trigger a shutdown sequence
N+1	2
N+2	3
N+3	4

Multiple critical events occurring on the same UPS does not impact the above table values.

In redundancy terminology, this is the x in N+x.

This setting is not displayed for UPS Setups with a Single UPS device. |
| Total number of UPS's in Setup | This is the total of the above two rows and is calculated automatically. |

Run Command	When a shutdown sequence is triggered you can configure PowerChute to execute a command file.
	Note: If the same command file is configured for each setup and a shutdown sequence is triggered for more than one setup at the same time, the command file is only executed once.
	See Shutdown Command Files.
Shut down PowerChute Server	This is enabled by default and is used to gracefully shut down the physical machine running PowerChute.
	This option should be disabled if the PowerChute machine is not being powered by the UPS's in a particular setup, and if it is being used to remotely shut down other servers/ equipment.
	This option is not available if PowerChute is installed on a Nutanix host.
Shut down if Redundancy lost	If this option is enabled, when the number of UPS critical events is the same as the number of additional (redundant) UPS's, a shutdown sequence will be triggered.
	This option is associated with the number of UPS critical events required to trigger shutdown:
	<table><tr><th>Redundancy level</th><th>No. of critical events that will trigger a shutdown sequence</th></tr><tr><td>N+1</td><td>1</td></tr><tr><td>N+2</td><td>2</td></tr><tr><td>N+3</td><td>3</td></tr></table>
	Multiple critical events occurring on the same UPS does not impact the above table values.
	This option is not shown if there are no additional (redundant) UPS's. For example, this option will not appear if the number of UPS's required to power the load is the same as the total number of UPS's in the group.
UPS Shutdown	Use this option to set the required UPS behavior after connected equipment or servers are gracefully shut down. For more information see UPS Shutdown.

SSH Settings

PowerChute Network Shutdown can be configured to execute commands on a remote host via an SSH connection. To create an SSH action, click **Add Action** and configure the following:

1. **Name:** A unique name for each SSH action of a length less than or equal to 255 ASCII characters.
2. Configure one of the following authentication methods:
   - **User Name** and **Password:** Enter the user name and password to connect to the remote host.
   - **User Name**, **SSH Key File Path** and **SSH Key File Password:** Specify the path to a shared SSH key. This option requires you to generate an SSH key and copy it to your target systems. See SSH Command File Location.
3. **IP Addresses/FQDN** and **Port:** The IP address or Fully Qualified Domain Name (FQDN) and port of the target SSH component.
4. **Path to SSH command file:** You must specify the full path name of the command file, including the disk drive or volume number. See SSH Command File Location.
5. **SSH Action Delay:** Enter the amount of time, in seconds, that PowerChute will wait before connecting to the remote host and begin sending commands. The default value is 0.
6. **SSH Action Duration:** Enter the amount of time, in seconds, for the SSH action to complete before proceeding with the rest of the shutdown sequence.

> ⚠️ Using the **SSH Action Duration** field, you must allow sufficient time for all your SSH actions to complete.

7. **Execute SSH Action:**
   - **On Startup:** Execute the SSH command file when the PowerChute service re-starts. In an advanced configuration, the SSH command file is executed when the critical UPS event is resolved.
   - **Before VM Shutdown:** Execute the SSH command file before the User VM Migration and Shutdown Step.
   - **Before Host Shutdown:** Execute the SSH command file before host shutdown.
   - **After Host Shutdown:** Execute the SSH command file after host shutdown.

8. **Enable SSH Action:** Allows you to enable or disable the configured SSH action. This checkbox is enabled by default when a new SSH action is created.

NOTES:

- PowerChute takes the command file provided and passes it line-by-line to the remote host over an SSH connection. As a result, incomplete lines may be interpreted incorrectly by the remote host. You must ensure that your SSH command file contains complete lines and commands so the remote host can interpret the file correctly.
- The line ending style of the command file must match that of the PowerChute target host operating system. For example, a command file configured on PowerChute running on a Windows host must contain Windows style text line endings.
- Recognized command prompts are:
    - $ (Linux)
    - # (Linux admin/root)
    - > (Windows, or RPDU)
- Custom command prompts can be added via the PowerChute configuration file (`pcnsconfig.ini`) by adding the "`ssh_prompt_regex`" setting to the `[SSHAction]` section. For example: to add a custom command prompt of "~", add "`ssh_prompt_regex = \~\s`".
- The PowerChute Event Log only displays that an SSH action has completed. The Event Log does not show if the SSH action has completed successfully or not.
- If a value is specified in the **SSH Action Delay** field, the Event Log does not log that an SSH action is running with a configured delay.

SSH Command File Location

The SSH key file, if configured, and command file must be located in the user_files folder, or a sub-folder, in the PowerChute installation directory. If the default installation directory was chosen during installation, this location will be:

- C:\Program Files\APC\PowerChute\user_files for Windows systems

- /opt/APC/PowerChute/user_files/ for Linux systems

NOTE: If you are upgrading to PowerChute v5.1, any key files and/or command files used in a previous version of PowerChute must be manually added to the user_files folder. If the files are not added to the directory, you will see the below errors in the Event Log:

```
ERROR: The ini contains an invalid value for ssh_command_file_path
in section SSHAction0.
```

```
ERROR: The ini contains an invalid value for ssh_keyfile_path in
section SSHAction0.
```

It is strongly recommended you validate your configuration after an upgrade.

SSH Settings in an Advanced UPS Configuration

In an Advanced UPS configuration, SSH actions can be enabled and disabled for each UPS setup.

The ✅ symbol indicates that an SSH action is enabled in the main SSH Settings screen. To run an SSH action for a particular UPS setup, enable the checkbox next to the ✅ symbol.

SSH actions that are not enabled do not display the ✅ symbol. These disabled actions will not be executed if enabled for a UPS setup.

SNMP Configuration

PowerChute Network Shutdown can be configured to communicate via Simple Network Management Protocol (SNMP), and can be discovered via SNMP by Network Management tools, such as StruxureWare Data Center Expert. Using SNMP, you can query and configure PowerChute settings, and generate SNMP traps for UPS critical events and lost communication events.

SNMPv1 and SNMPv3 are supported by PowerChute Network Shutdown. IPv4 and IPv6 are both supported. Go to **SNMP Settings** in the web user interface to complete the configuration and make PowerChute accessible via SNMP. It is not necessary to re-start the PowerChute service when enabling SNMP or making SNMP configuration changes via the web user interface. PowerChute configuration changes via SNMP are logged to the Event Log.

Enter the **SNMP Discovery Port**. The default value of 161 is automatically populated, but this can be edited if this port is already in use. The Port number availability is automatically checked, and if it is not available, a new port number must be entered.

See:

- SNMPv1 Configuration
- SNMPv3 Configuration
- SNMP Trap Configuration
- SNMP Data Points
- SNMP Troubleshooting

SNMPv1 Configuration

Select **Enable SNMPv1 access** to configure the User Profiles required to communicate via SNMPv1. Select **Add Profile** and configure:

1. **Community Name**: The Community Name is sent with each SNMP request to obtain access to a device. The maximum length is 15 ASCII characters.
2. **NMS IP/Host Name**: The IP address, Host Name or Fully Qualified Domain Name of the Network Management System (NMS). An NMS is software that is used to manage software and hardware components on the network. It can be used to manage PowerChute via SNMP by issuing SNMP GET and SET commands. The default value of 0.0.0.0 permits access from any NMS.
3. **Access Type:**
   o **Disable**: No SNMP GET or SET requests are permitted.
   o **Read**: Only SNMP GET requests are permitted.
   o **Read/Write**: SNMP GET and SET requests are permitted.

To edit an existing SNMPv1 user profile, click the [pencil icon] button. To delete an SNMPv1 user profile, click the [trash icon] button.

Click **Apply** to save the SNMPv1 configuration.

[info icon] Certain Network Management Systems require the SNMP Engine ID to communicate via SNMP. The **SNMP Engine ID** is displayed on the SNMP Settings page of the PowerChute user interface.

[warning icon] SNMPv1 is less secure than SNMPv3. SNMPv1 does not provide encryption or authentication, and the Community Name is sent over the network in plain text. To use encryption and authentication with SNMP, configure SNMPv3 settings.

SNMPv3 Configuration

Select **Enable SNMPv3 access** to configure the SNMPv3 settings. Select **Add Profile** and configure:

1. **User Name**: In SNMPv3, all GET and SET requests and SNMP Traps are matched to a user profile by the User Name. Enter a user name of a length less than or equal to 32 ASCII characters.
2. **Authentication Protocol**: Select MD5, SHA-1 or SHA-2 (SHA256 or SHA512) protocol. It is recommended to use an SHA-2 protocol, if the NMS supports it.

> It is not recommended to use the MD5 protocol.

3. **Authentication Passphrase**: Enter an authentication password for the protocol selected, of 8-32 ASCII characters.
4. **Privacy Protocol**: Select AES-128, AES-192*, AES-192 Ex†, AES-256* , AES-256 Ex†, or DES. It is recommended to use the AES-256 protocol, if the NMS and PowerChute JRE support it.
5. **Privacy Passphrase**: Enter a privacy password for the encryption protocol selected, of 8-32 ASCII characters.
6. **Access Type:**
   - **Disable**: No SNMP GET or SET requests are permitted.
   - **Read**: Only SNMP GET requests are permitted.
   - **Read/Write**: SNMP GET and SET requests are permitted.

To edit an existing SNMPv3 user profile, click the [edit] button. To delete an SNMPv3 user profile, click the [delete] button.

Click **Apply** to save the SNMPv3 configuration.

> Certain Network Management Systems require the SNMP Engine ID to communicate via SNMP. The **SNMP Engine ID** is displayed on the SNMP Settings page of the PowerChute user interface.

SNMP Trap Configuration

You can specify the device(s) that receive the SNMP traps generated by PowerChute for UPS critical and lost communication events.

To configure a Trap Receiver, select **Add Trap Receiver** and configure:

1. **Enable**: Select the checkbox to enable the Trap Receiver.
2. **NMS IP/Host Name**: The IP address, Host Name or Fully Qualified Domain Name of the NMS.
3. **Port**: The port on which the NMS will listen for incoming traps. The default port number is 162.
4. **SNMPv1**: Select this if you want to send the traps via SNMPv1.
   - **Community Name**: Enter the Community Name of the SNMPv1 user profile to be used as an identifier when SNMPv1 traps are sent to this receiver.
5. **SNMPv3**: Select this if you want to send the traps via SNMPv3.

   - **User Name**: Select the user name of the SNMPv3 user profile to be used as an identifier when SNMPv3 traps are sent to this receiver.

Click the **SNMP Trap Receiver Test** to send a test trap to the configured Trap Receiver. Check the Trap Receiver to ensure that the test trap was received.

To edit an existing SNMP Trap Receiver, click the [pencil] button. To delete an SNMP Trap Receiver, click the [trash] button.

UPS Critical Events

PowerChute sends SNMP traps to the configured Trap Receiver(s) upon the following events:

- **PowerChute Critical Event triggers a Shutdown**
  When a critical event (such as On Battery) occurs and a Shutdown is triggered, PowerChute sends an SNMP trap detailing the **Event Name, UPS Setup** (for advanced configurations)**,** and **Affected Virtual Hosts** (if Virtualization support is enabled).
- **PowerChute Critical Event Resolved**
  If the option to **Send Trap when condition is cleared** is enabled, when a PowerChute Critical Event which triggered a Shutdown is resolved, PowerChute sends an SNMP trap to the configured NMS.

Lost Communication Events

PowerChute sends SNMP traps to the configured Trap Receiver(s) upon the following events:

- **Network Communications Lost**
  If PowerChute cannot communicate with the Network Management Card of the UPS, a trap is sent to the configured Trap Receiver.
- **UPS Communications Lost**
  If the Network Management Card cannot communicate with the UPS, a trap is sent to the configured Trap Receiver.

If the option to **Send Trap when condition is cleared** is enabled, the following traps are sent:

- **Network Communications Lost Resolved**
  If PowerChute regains communication with the Network Management Card of the UPS, a trap is sent to the configured Trap Receiver.
- **UPS Communications Lost Resolved**
  If communication is regained between the NMC and the UPS, a trap is sent to the configured Trap Receiver.

Other Events

- **Software Update Available Trap**
  When the PowerChute Auto Update functionality detects that there is a new update available; a trap is sent to the configured Trap Receiver.
- **PowerChute Test Trap**
  When configuring a Trap Receiver, a test trap can be sent to determine if the Trap Receiver is receiving the traps. See SNMP Trap Receiver Test.

See SNMP Data Points > PowerChute Traps for more information on PowerChute SNMP Trap OIDs.

Configuring SNMP Trap Notification Settings

To configure the settings for UPS Critical Event or Lost Communication traps:

1. Go to **SNMP Settings > SNMP Traps**
2. Click on the ⚙ icon next to **UPS Critical Events** or **Lost Communication Events**
3. Select the **Enable** checkbox to enable traps for critical events.
4. **Delay**: Specify the length of time that Event must persist before a trap is sent. If the Event is cleared before this time, no trap is sent.
5. **Repeat Interval**: Specify the time interval in seconds that the trap is re-sent.
6. Select:
   - **Repeat until condition clears** if you want the trap to be sent at the repeat interval until the Event is cleared.
   - **Repeat X times** to specify the number of times the trap will be sent when the Event occurs.
7. Select **Send Trap when condition is cleared** to be notified when the Event is cleared.
   Note: If the PowerChute server is shut down due to a UPS Critical Event, no clearing Trap will be sent to the NMS.

SNMP Data Points

The tables below describe the PowerChute configuration details that are available for SNMP polling and/or configuration.

PowerChute Identity Information

Object Identifier Name	Access	Description
pcnshostname	read-only	The hostname of the PowerChute instance.
pcnsVersion	read-only	The version of PowerChute installed.
pcnsOS	read-only	The version of the Operating System upon which PowerChute is installed.
pcnsJavaVersion	read-only	The version of Java upon which PowerChute is running.

PowerChute Networking Settings

Object Identifier Name	Access	Description
pcnsUIProtocol	read-only	The web protocol that is used to connect to the PowerChute web user interface.
pcnsHttpPort	read-only	The port that is used to connect to the PowerChute web user interface.
pcnsHttpsPort	read-only	The port that is used to connect via https to the PowerChute web user interface.
pcnsNetworkConfig	read-only	Configuration of the TCP network: IPv4/IPv6.
pcnsVirtualInstall	read-only	The Virtualization technology for which PowerChute is configured.

PowerChute Network Management Card Settings

Object Identifier Name	Access	Description
pcnsMode	read-only	The configuration of the UPSs that PowerChute is monitoring. See UPS Configuration Options.
pcnsNMCPort	read-only	The port used to connect to all of the Network Management Card(s).
pcnsNMCProtocol	read-only	The web protocol used to connect to all of the Network Management Card(s).
NMC details are contained in an SNMP table named `pcnsNmcTable`. Each table entry contains:		
pcnsNMCIndex	read-only	The Index of the NMC within the PowerChute setup.
pcnsNMCAddr	read-only	The IP address of the NMC
pcnsNMCOutlet	read-only	The Outlet Group of the NMC on which PowerChute is enrolled.

PowerChute Shutdown Settings

Object Identifier Name	Access	Description
pcnsShutdownCommandFileEnabled*	read-write	Specify if Shutdown a Command File is configured to run if a UPS critical event is triggered. See Shutdown Command Files.
pcnsShutdownCommandFileDelay*	read-write	The number of seconds that a host requires to shut down, before the command file is executed. This setting is applicable to virtualization support only.
pcnsShutdownCommandFile*	read-write	The full path name of the command file, including the disk drive or volume name. See Shutdown Command Files.
pcnsShutdownCommandFileDuration*	read-write	The number of seconds that the shutdown command file requires to execute.
pcnsTurnOffUps*	read-write	The setting to turn off the UPS after performing a graceful shutdown.
pcnsTurnOffSOG*	read-write	The setting to turn off the Outlet Group of the UPS when performing a graceful shutdown.
pcnsRuntimeRemainingThreshold	read-write	This defines a threshold for runtime remaining. When the UPS in running on battery power and the runtime remaining on the UPS drops below the threshold, PowerChute triggers a shutdown sequence. See Sequenced Server Shutdown for more information.

pcnsRuntimeRemainingCmdFileThreshold	read-write	This defines a threshold for runtime remaining. When runtime remaining drops below this threshold, PowerChute executes the command file.

* **Note**: These OIDs are not available for Advanced UPS Setups. See below for equivalent OIDs for Advanced UPS Setups.

Shutdown Settings for Advanced UPS Setups

The PowerChute Shutdown Settings for Advanced UPS Setups are contained in an SNMP Table named `pcnsAdvancedShutdownTable`. To SNMP GET or SET a property of a specific Advanced UPS Configuration, you must specify the group number of the UPS Setup in the GET or SET command. To see a list of UPS Setups and their associated numbers, perform an SNMP Get on `.pcnsAdvancedGroupName`

To perform an SNMP GET or SET command on each UPS Setup is, use the format `.[Object Identifier Name].[UPS Setup Number]`

For example, to specify that a command file is configured for the first UPS Setup, the perform an SNMP SET on `.pcnsAdvancedShutdownCommandFileEnabled.1`

Object Identifier Name	Access	Description
pcnsAdvancedGroupNo	read-only	The number of the Advanced UPS Setup.
pcnsAdvancedGroupName	read-write	The name of the Advanced UPS Setup.
pcnsAdvancedGroupNMC	read-only	A list of IP addresses of the NMCs in the Advanced UPS Setup, and the outlets in the associated outlet groups.
pcnsAdvancedShutdownUPSRequiredForLoad	read-write	The number of UPS devices required to power the load.
pcnsAdvancedShutdownCommandFileEnabled	read-write	Specify if a Shutdown Command File is configured to run if a UPS critical event is triggered. See Shutdown Command Files.
pcnsAdvancedShutdownCommandFile	read-write	The full path name of the command file, including the disk drive or volume name. See Shutdown Command Files.
pcnsAdvancedShutdownCommandFileDuration	read-write	The number of seconds that the shutdown command file requires to execute.
pcnsAdvancedShutdownPowerchuteServer	read-write	The setting to gracefully shut down the physical machine running PowerChute. See Shutdown Settings for Advanced UPS Configurations.
pcnsAdvancedShutdownOnLostRedundancy	read-write	If this option is enabled, when the number of UPS critical events is the same as the number of additional (redundant) UPS's, a shutdown sequence will be triggered. See Shutdown Settings for Advanced UPS Configurations.

pcnsAdvancedTurnOffUps	read-write	The setting to turn off the UPS when performing a graceful shutdown.
pcnsAdvancedTurnOffSOG	read-write	The setting to turn off the Outlet Group of the UPS when performing a graceful shutdown.

PowerChute Events

The table below details the OID Names of the Configurable Events that can be configured via SNMP, and the names of the Events as seen in the PowerChute User Interface.

Object Identifier Name	PowerChute UI Reference
pcnsPowerFailed	UPS On Battery
pcnsPowerRestored	Input Power Restored
pcnsOverload	UPS Overloaded
pcnsOverloadSolved	UPS Overload Corrected
pcnsRunTimExceeded	Runtime exceeded
pcnsRunTimeWithinRange	Runtime is sufficient
pcnsRunTimeBelowThreshold	Runtime remaining below threshold
pcnsRunTimeAboveThreshold	Runtime remaining above threshold
pcnsBatteryDischarged	Battery Discharged
pcnsBatteryChargeInRange	Battery Recharged
pcnsFaultBypassEnabled	Bypass due to hardware error or overload
pcnsBypassEnabled	Maintenance Bypass
pcnsBypassManualEnabled	Bypass ended
pcnsBypassDisabled	Bypass ended
pcnsBypassContactorFailed	Bypass Switch failed
pcnsBypasContactorOk	Bypass Switch replaced

pcnsCommunicationLostOnBattery	Communication lost while on Battery
pcnsCommunicationLost	NMC cannot communicate with the UPS

Object Identifier Name	PowerChute UI Reference
pcnsNetCommunicationLost	PowerChute cannot communicate with the NMC
pcnsCommunicationEstablished	Communication established
pcnsMinRedundancyLost	Minimum Redundancy lost
pcnsMinRedundancyRegained	Minimum Redundancy restored
pcnsParallelRedundancyLost	Parallel Redundancy lost
pcnsParallelRedundancyRegained	Parallel Redundancy restored
pcnsMaxInternalTempExceeded	UPS Temperature Overheated
pcnsMaxInternalTempInRange	UPS Temperature Normal Again
pcnsMinLoadCapabilityLost	Load (kVA) Alarm Violation
pcnsMinLoadCapabilityRegained	Load (kVA) Alarm Violation cleared
pcnsEnviornmentCommunicationEstablished	Communication Established with EMC
pcnsEnviornmentCommunicationLost	Communication Lost with EMC
pcnsTempInRangeProbeX	Temperature Probe X In Range
pcnsTempOutOfRangeProbeX	Temperature Probe X Out Of Range
pcnsHumidityInRangeProbeX	Humidity Probe X In Range
pcnsHumidityOutOfRangeProbeX	Humidity Probe X Out Of Range
pcnsContactFaultX	Contact Zone X Alarm
pcnsContactNormalX	Contact Zone X Normal

For each event you can access:

OID Name	Access	Description
[event name]Desc	read-only	The description of the event.
[event name]EnableLogging	read-write	Enable or disable logging to the event log for this event.
[event name]EnableCommandFile	read-write	Enable or disable command file execution for this event.
[event name]CommandFilePath	read-write	Specify a Command File and full path to be executed upon this event.
[event name]CommandFileDelay	read-write	The number of seconds that a host requires to shut down, before the command file is executed. **Note**: This is not available for pcnsRunTimeBelowThreshold. See pcnsRunTimeBelowThresholdCommandFileThreshold below.

For some events you can access:

OID Name	Access	Description
[event name]EnableShutdown	read-write	Perform a graceful shutdown of the host when this event occurs.
[event name]ShutdownDelay	read-write	The amount of time in seconds that PowerChute should wait before initiating the shutdown process.

For `pcnsRunTimeBelowThreshold` you can access:

OID Name	Access	Description
pcnsRunTimeBelowThresholdCommandFileThreshold	read-write	If Runtime Remaining falls below this threshold, the command file is executed.
pcnsRunTimeBelowThresholdShutdownThreshold	read-write	If Runtime Remaining falls below this threshold, a graceful shutdown of the host is initiated.

c

PowerChute Traps

The table below details the OID Names of the SNMP traps sent by PowerChute for critical and lost communication events.

UPS Critical Events

OID Name	Level	Description
pcnsCriticalEventActive	Severe	PowerChute Network Shutdown has begun a graceful shutdown of the host due to a critical event.
pcnsCriticalEventResolved	Informational	The PowerChute Network Shutdown critical event has been resolved, and graceful shutdown of the host continues.

Lost Communication Events

OID Name	Level	Description
pcnsNetworkComsLost	Severe	PowerChute cannot communicate with the NMC.
pcnsNetworkComsLostResolved	Informational	PowerChute has regained communication with the NMC.
pcnsNMCComsLost	Severe	The NMC cannot communicate with the UPS.
pcnsNMCComsLostResolved	Informational	The NMC has regained communication with the UPS.

Other Events

OID Name	Level	Description
pcnsTest	Informational	PowerChute has sent a test trap to the NMS.
pcnsUpdateAvailable	Informational	PowerChute has detected that an update is available.

Event Configuration

When UPS events occur, PowerChute can be configured to log the event, notify users, execute a command file or initiate a system shutdown through the Configure Events screen.

The ✅ symbol indicates that the action is enabled for this event while the ⚙ symbol indicates that the action is not enabled.

Descriptions of events are in the PowerChute Events and Logging sections.

Notifications

PowerChute can send a message to one user or all logged-in users when an event occurs:

Notify all users: For Linux or Unix, all users who are logged onto the server with a terminal prompt open will be notified.

Notify only this user: On Windows, enter the machine name. On Linux or Unix systems, enter the user name. The user will still need to be logged onto the server with a terminal prompt open to be notified.

Repeat Interval: The time interval, in seconds, at which the message will be repeated while the event condition exists. If this field is blank or zero, the message will not be repeated.

Delay (if required): Enter the amount of time in seconds that PowerChute should wait after the event occurs before notifying users. Users will be notified immediately if a shutdown event is triggered.

Event-Driven Command Files

If required, PowerChute can be configured to execute a command file after certain events are triggered. Click the ⚙ symbol on the event row and select the **Enable Command File** check box.

Delay: Enter the amount of time in seconds that PowerChute should wait when the event occurs before executing the command file.

> ℹ️ If a shutdown command file is also configured, both command files will be executed in parallel.

Full path to command file: You must specify the full path name of the command file, including the disk drive or volume name.

The command file runs using the local system account. PowerChute cannot execute programs that require interaction with the desktop; only command line-enabled programs are supported.

> The command file must be located in the user_files folder, or a sub-folder, in the PowerChute installation directory. If the default installation directory was chosen during installation, this location will be:
>
> - C:\Program Files\APC\PowerChute\user_files for Windows systems
>
> - /opt/APC/PowerChute/user_files/ for Linux systems

> ℹ️ **NOTE:** If you are upgrading to PowerChute v5.1, any command files used in a previous version of PowerChute must be manually added to the user_files folder. If the command files are not added to the directory, you will see the below errors/warnings for all events configured to run a command file in the Event Log. For example:

```
ERROR: Event PowerFailed is enabled for command file execution,
but an invalid value for event_PowerFailed_commandFilePath is
specified.
```

```
WARNING: Disabling command file execution for event PowerFailed due
to bad parameters. Please validate the configuration.
```

> It is strongly recommended you validate your configuration after an upgrade.

Shutdown Actions

When the Shutdown Action is enabled for an event, PowerChute treats the event as critical and will trigger a shutdown sequence. Shutdown is not supported for all events: this is indicated by the presence or absence of an icon on the event row.

The **Delay** field is the amount of time in seconds that PowerChute should wait before initiating the shutdown sequence. By default, the **On Battery** event has a delay of 120 seconds, whereas the default for all other events is 0 seconds.

By default, PowerChute will only trigger a shutdown sequence if a low battery condition occurs or the UPS is commanded to turn off. Shutdown cannot be disabled for these events using the PowerChute user interface

Start-up and Shut-down Scheduling

PowerChute does not directly support the start-up and shut-down scheduling feature as it is available from the Network Management Card. For more information on supported scheduling features, refer to the NMC User Guide.

Sequenced Server Shutdown

The **Runtime Remaining below Threshold** event can be used to sequence the order that your servers shut down during an extended power outage.

This is useful if you have multiple servers powered by the same UPS and you want to extend the runtime for your higher priority servers. It also ensures that lower priority servers are the first to be shut down.

This event will trigger a server shutdown command when the UPS is running on battery power and the runtime has dropped below the threshold configured. You can also configure a command file to execute before shutdown occurs by specifying a higher runtime threshold value for the **Run Command File** event action.

Example

1. You have 3 servers powered by the same UPS. Your lower priority server is Server C while you want to keep Server A running as long as possible.

2. You want Server A to shut down when the UPS protecting it has 10 minutes runtime remaining.

3. You want Server B to shut down when the UPS protecting it has 15 minutes runtime remaining.

4. You want Server C to shut down when the UPS protecting it has 20 minutes runtime remaining.

5. Configure each PowerChute Agent with the following threshold values:

   o   Server A – 10 minutes
   o   Server B - 15 minutes
   o   Server C - 20 minutes

6. Each server is shut down when the runtime remaining drops below the threshold configured.
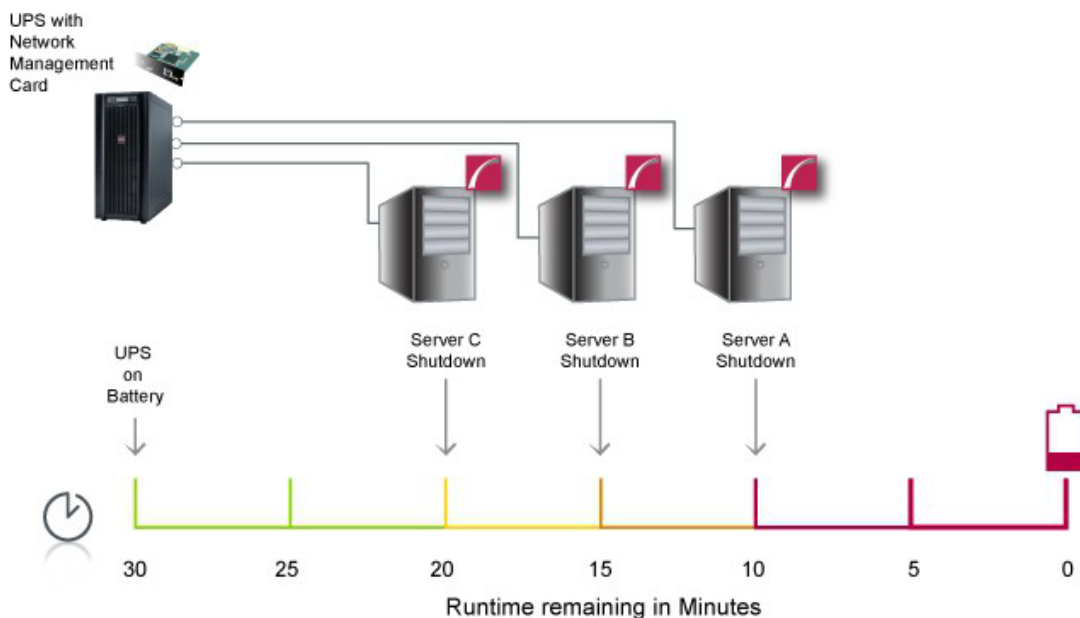
Sample Shutdown Scenarios

The following scenarios provide examples of how PowerChute and the UPS behave when a shutdown sequence is triggered.

- Nutanix AHV: UPS without Outlet Groups
- Nutanix AHV: UPS with Outlet Groups
- Nutanix AHV Shutdown - Single UPS Configuration
- Nutanix AHV Shutdown - Advanced UPS Configuration
- Nutanix Shutdown - VM Prioritization

Nutanix AHV: UPS without Outlet Groups

Example 1: Turn off the UPS enabled, AFS shutdown enabled, abort active replications enabled, no shutdown command file or SSH action configured.

PowerChute is installed on a physical machine outside the Cluster, configured for a Single/Redundant UPS configuration with several Nutanix Hosts in a Cluster. The option to Turn off the UPS is enabled on the Shutdown Settings page. No shutdown command file or SSH action configured. The durations in this example are as follows:

- VM Shutdown = 120 seconds
- Abort Active Replications Duration = 80 seconds
- AFS Shutdown Duration = 60 seconds
- Cluster Shutdown Duration = 60 seconds
- Controller VM Shutdown Duration = 120 seconds

When a critical UPS event, such as On Battery occurs, the following sequence is triggered.

1. PowerChute reports that the UPS is on battery.

2. After the shutdown delay configured for the On Battery event has elapsed, PowerChute issues a command to turn off the UPS. UPS turnoff starts.

3. PowerChute issues a command on the Nutanix Controller VMs to shut down User VMs.

4. After 120 seconds (VM Shutdown Duration), PowerChute shuts down Acropolis File Services and the AFS VMs.

5. After 60 seconds (AFS Shutdown Duration), PowerChute aborts any ongoing VM replications.

6. After 80 seconds (Abort Active Replications Duration), PowerChute shuts down the Nutanix Cluster.

7. After 60 seconds (Cluster Shutdown Duration), PowerChute issues a command to shut down the Controller VMs.

8. After 120 seconds (Controller VM Shutdown Duration), PowerChute issues commands to shut down the Nutanix Hosts.

9. After a 70 second delay, the operating system on the physical machine running PowerChute starts to shut down.

10. The UPS will wait the amount of time indicated by one of the following, whichever is greater:

   Low Battery Duration or **Maximum Required Delay**.

   These are shown on the Configuration - Shutdown page in the NMC interface.

11. After this delay, a further non-configurable two minute delay is counted down.

12. The UPS will then turn off after the user-configurable **Shutdown Delay** time has elapsed. This is configurable on the Configuration - Shutdown page in the NMC user interface.

It is recommended that the **Low Battery Duration** is configured to allow enough time for the Operating System shutdown to complete. Ideally the operating system should have shut down before the non-configurable two minute delay (step 10) starts to count down.

Example 2: Turn off the UPS enabled, shutdown command file configured.

PowerChute is installed on a physical machine outside the Cluster, configured for a Single/Redundant UPS configuration with several Nutanix Hosts in a Cluster. The option to Turn off the UPS is enabled on the Shutdown Settings page. A shutdown command file is configured. The durations in this example are as follows:

- VM Shutdown Duration = 120 seconds
- Abort Active Replications Duration = 80 seconds
- AFS Shutdown Duration = 60 seconds
- Cluster Shutdown Duration = 60 seconds
- Controller VM Shutdown Duration = 120 seconds

When a critical UPS event, such as On Battery occurs, the following sequence is triggered.

1. PowerChute reports that the UPS is on battery.

2. After the shutdown delay configured for the On Battery event has elapsed, PowerChute issues a command to turn off the UPS. UPS turnoff starts.

3. PowerChute issues a command on the Nutanix Controller VMs to shut down User VMs.

4. After 120 seconds (VM Shutdown Duration), PowerChute shuts down Acropolis File Services and the AFS VMs.

5. After 60 seconds (AFS Shutdown Durations), PowerChute aborts any ongoing VM replications.

6. After 80 seconds (Abort Active Replications Duration), PowerChute shuts down the Nutanix Cluster.

7. After 60 seconds (Cluster Shutdown Duration), PowerChute issues a command to shut down the Controller VMs.

8. After 120 seconds (Controller VM Shutdown Duration), PowerChute starts to execute the shutdown command file.

9. After the delay configured for the command file has elapsed, PowerChute issues commands to shut down the Nutanix Hosts.

10. After a 70 second delay, the operating system on the physical machine running PowerChute starts to shut down.

11. The UPS will wait the amount of time indicated by one of the following, whichever is greater:

Low Battery Duration or **Maximum Required Delay**.

These are shown on the Configuration - Shutdown page in the NMC interface.

12. After this delay, a further non-configurable two minute delay is counted down.

13. The UPS will then turn off after the user-configurable **Shutdown Delay** time has elapsed. This is configurable on the Configuration - Shutdown page in the NMC user interface.

It is recommended that the **Low Battery Duration** is configured to allow enough time for the Operating System shutdown to complete. Ideally the operating system should have shut down before the non-configurable two minute delay (step 11) starts to count down.

Example 3: Turn off the UPS enabled, shutdown command file configured, Execute Command File after Host Shutdown enabled.

PowerChute is installed on a physical machine outside the Cluster, configured for a Single/Redundant UPS configuration with several Nutanix Hosts in a Cluster. The option to Turn off the UPS is enabled on the Shutdown Settings page. A shutdown command file is configured. Execute Command File after Host Shutdown is enabled, with a delay of 30 seconds applied. The durations in this example are as follows:

- VM Shutdown Duration = 120 seconds
- Abort Active Replications Duration = 80 seconds
- AFS Shutdown Duration = 60 seconds
- Cluster Shutdown Duration = 60 seconds
- Controller VM Shutdown Duration = 120 seconds

When a critical UPS event, such as On Battery occurs, the following sequence is triggered.

1. PowerChute reports that the UPS is on battery.

2. After the shutdown delay configured for the On Battery event has elapsed, PowerChute issues a command to turn off the UPS. UPS turnoff starts.

3. PowerChute issues a command on the Nutanix Controller VMs to shut down User VMs.

4. After 120 seconds (VM Shutdown Delay), PowerChute shuts down Acropolis File Services and the AFS VMs.

5. After 60 seconds (AFS Shutdown Delay), PowerChute aborts any ongoing VM replications.

6. After 80 seconds (Abort Active Replications Duration), PowerChute shuts down the Nutanix Cluster.

7. After 60 seconds (Cluster Shutdown Delay), PowerChute issues a command to shut down the Controller VMs.

8. After 120 seconds (Controller VM Shutdown Delay), PowerChute issues a command to shut down the Nutanix Hosts,

9. Following the 30 second delay configured for the **Execute Command File after Host Shutdown** option, PowerChute starts to execute the shutdown command file.

10. After the duration configured for the shutdown command file has elapsed, the OS Shutdown Command is issued and an additional 70 second delay is counted down before the operating system on the physical machine running PowerChute starts to shut down.

11. The UPS will wait the amount of time indicated by one of the following, whichever is greater:

   Low Battery Duration or **Maximum Required Delay**.

   These are shown on the Configuration - Shutdown page in the NMC interface.

12. After this delay, a further non-configurable two minute delay is counted down.

13. The UPS will then turn off after the user-configurable **Shutdown Delay** time has elapsed. This is configurable on the Configuration - Shutdown page in the NMC user interface.
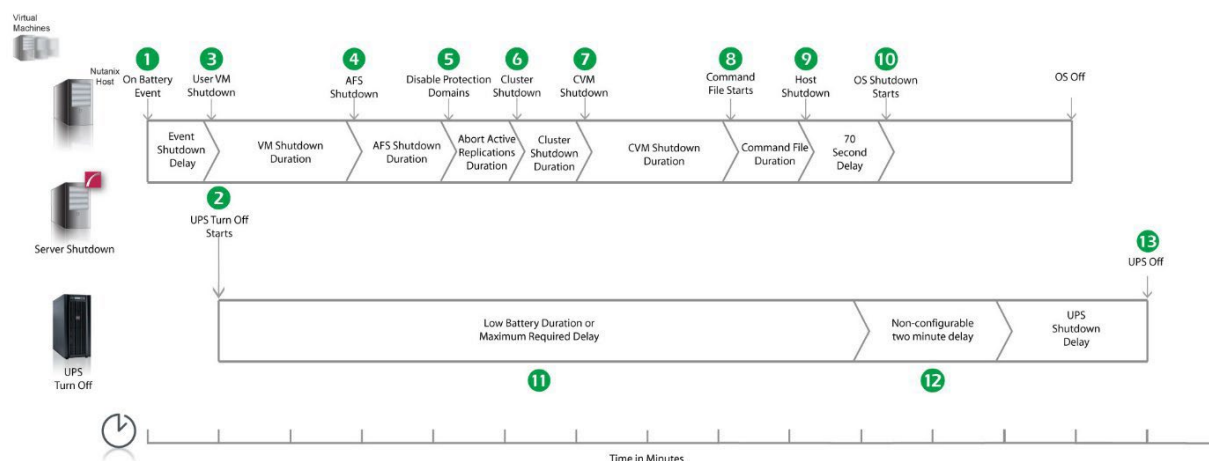
Nutanix AHV: UPS with Outlet Groups

Example 1: Turn off the Outlet Group enabled, AFS shutdown enabled, abort active replications enabled, no shutdown command file or SSH action configured.

PowerChute is installed on a physical machine outside the Cluster, configured for a Single/Redundant UPS configuration with several Nutanix Hosts in a Cluster. The option to Turn off the Outlet Group is enabled on the Shutdown Settings page. No shutdown command file or SSH action configured. The durations in this example are as follows:

- VM Shutdown Duration= 120 seconds
- Abort Active Replications Duration= 80 seconds
- AFS Shutdown Duration 60 seconds
- Cluster Shutdown Duration = 60 seconds
- Controller VM Shutdown Duration = 120 seconds

When a critical UPS event, such as On Battery occurs, the following sequence is triggered.

1. PowerChute reports that the UPS is on battery.

2. After the shutdown delay configured for the On Battery event has elapsed, PowerChute issues a command to turn off the Outlet Group and the Outlet Group turn off starts.

3. PowerChute issues a command on the Nutanix Controller VMs to shut down User VMs.

4. After 120 seconds (VM Shutdown Delay), PowerChute shuts down Acropolis File Services and the AFS VMs.

5. After 60 seconds (AFS Shutdown Delay), PowerChute aborts any ongoing VM replications.

6. After 80 seconds (Abort Active Replications Duration), PowerChute shuts down the Nutanix Cluster.

7. After 60 seconds (Cluster Shutdown Delay), PowerChute issues a command to shut down the Controller VMs.

8. After 120 seconds (Controller VM Shutdown Delay), PowerChute issues commands to shut down the Nutanix Hosts.

9. PowerChute issues the operating system shutdown command.

10. After a 70 second delay, the operating system on the physical machine running PowerChute starts to shut down.

11. The Outlet Group will turn off after the **Power Off Delay** (configurable on the **Configuration** – **Outlet Group** page in the NMC user interface) has elapsed.
    - If registered with the Main Outlet Group, the UPS will wait for any Switched Outlet Groups to turn off before the

> Main Outlet Group turnoff starts.

- If registered with a Switched Outlet Group, only that delay is counted down.

It is recommended that the Outlet Group **Power Off Delay** is configured to allow enough time for the operating system shutdown to complete. You should allow extra time to ensure that the Outlet Group does not turn off before the operating system.

Example 2: Turn off the Outlet Group enabled, shutdown command file configured.

PowerChute is installed on a physical machine outside the Cluster, configured for a Single/Redundant UPS configuration with several Nutanix Hosts in a Cluster. The option to Turn off the Outlet Group is enabled on the Shutdown Settings page. A shutdown command file is configured. The durations in this example are as follows:

- VM Shutdown Duration = 120 seconds
- Abort Active Replications Duration = 80 seconds
- AFS Shutdown Duration = 60 seconds
- Cluster Shutdown Duration = 60 seconds
- Controller VM Shutdown Duration = 120 seconds

When a critical UPS event, such as On Battery occurs, the following sequence is triggered.

1. PowerChute reports that the UPS is on battery.

2. After the shutdown delay configured for the On Battery event has elapsed, PowerChute issues a command to turn off the Outlet Group and the Outlet Group turn off starts.

3. PowerChute issues a command on the Nutanix Controller VMs to shut down User VMs.

4. After 120 seconds (VM Shutdown Duration), PowerChute shuts down Acropolis File Services and the AFS VMs.

5. After 60 seconds (AFS Shutdown Duration), PowerChute aborts any ongoing VM replications.

6. After 80 seconds (Abort Active Replications Duration), PowerChute shuts down the Nutanix Cluster.

7. After 60 seconds (Cluster Shutdown Duration), PowerChute issues a command to shut down the Controller VMs.

8. After 120 seconds (Controller VM Shutdown Delay), PowerChute starts to execute the shutdown command file.

9. After the delay configured for the command file has elapsed, PowerChute issues commands to shut down the Nutanix Hosts.

10. An additional 70 second delay is counted down before the operating system starts to shut down.

11. The Outlet Group will turn off after the **Power Off Delay** (configurable on the **Configuration – Outlet Group** page in the NMC user interface) has elapsed.

   - If registered with the Main Outlet Group, the UPS will wait for any Switched Outlet Groups to turn off before the Main Outlet Group turnoff starts.
   - If registered with a Switched Outlet Group, only that delay is counted down.

It is recommended that the outlet group **Power Off Delay** is configured to allow enough time for the operating system shutdown to complete. You should allow extra time to ensure that the outlet group does not turn off before the operating system.

Example 3: Turn off the Outlet Group enabled, shutdown command file configured, Execute Command File after Host Shutdown enabled.

PowerChute is installed on a physical machine outside the Cluster, configured for a Single/Redundant UPS configuration with several Nutanix Hosts in a Cluster. The option to Turn off the Outlet Group is enabled on the Shutdown Settings page. A shutdown command file is configured. Execute Command File after Host Shutdown is enabled, with a delay of 30 seconds applied. The durations in this example are as follows:

   - VM Shutdown Duration = 120 seconds
   - Abort Active Replications Duration = 80 seconds
   - AFS Shutdown Duration = 60 seconds
   - Cluster Shutdown Duration = 60 seconds
   - Controller VM Shutdown Duration = 120 seconds

When a critical UPS event, such as On Battery occurs, the following sequence is triggered.

1. PowerChute reports that the UPS is on battery.

2. After the shutdown delay configured for the On Battery event has elapsed, PowerChute issues a command to turn off the Outlet Group and the Outlet Group turnoff starts.

3. PowerChute issues a command on the Nutanix Controller VMs to shut down User VMs.

4. After 120 seconds (VM Shutdown Duration), PowerChute shuts down Acropolis File Services and the AFS VMs.
5. After 60 seconds (AFS Shutdown Duration), PowerChute aborts any ongoing VM replications.

6. After 80 seconds (Abort Active Replications Duration), PowerChute shuts down the Nutanix Cluster.

7. After 60 seconds (Cluster Shutdown Delay), PowerChute issues a command to shut down the Controller VMs.

8. After 120 seconds (Controller VM Shutdown Delay), PowerChute issues a command to shut down the Nutanix Hosts.

9. Following the 30 second delay configured for the **Execute Command File after Host Shutdown** option, PowerChute starts to execute the shutdown command file.

10. After the duration configured for the shutdown command file has elapsed, an additional 70 second delay is counted down before the operating system starts to shut down.

11. The Outlet Group will turn off after the **Power Off Delay** (configurable on the **Configuration – Outlet Group** page in the NMC user interface) has elapsed.

    o If registered with the Main Outlet Group, the UPS will wait for any Switched Outlet Groups to turn off before the Main Outlet Group turnoff starts.

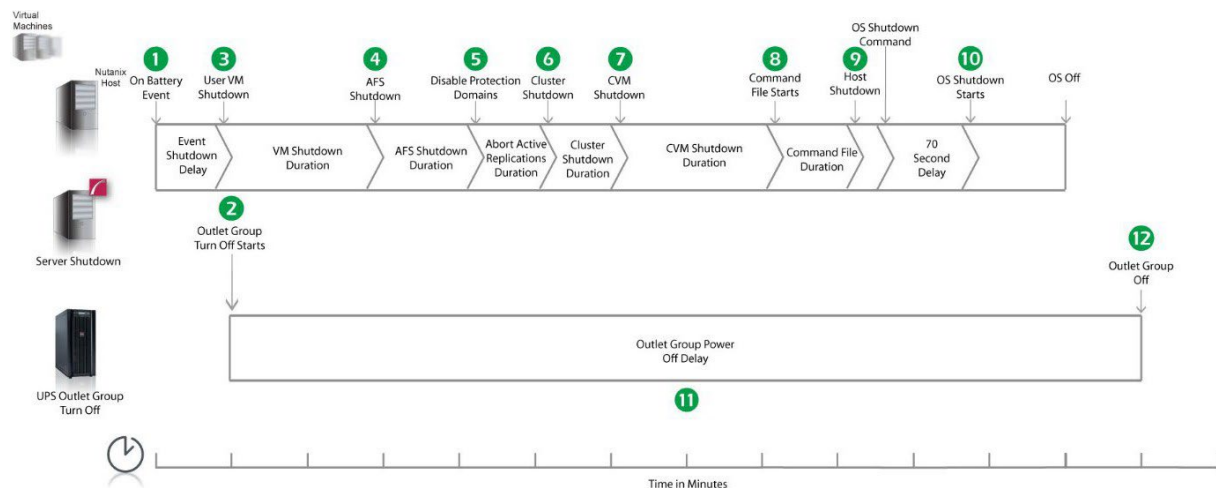   o If registered with a Switched Outlet Group, only that delay is counted down.

12. It is recommended that the Outlet Group **Power Off Delay** is configured to allow enough time for the operating system shutdown to complete. You should allow extra time to ensure that the Outlet Group does not turn off before the operating system.

Recommended Power-Off Delays for Outlet Groups

By default, the outlet group **Power Off Delay** will be the same value as the Low Battery duration configured on the NMC. PowerChute will automatically increase the Power Off Delay for the outlet group it is registered with, if the total shutdown time it needs is greater than the Power Off Delay.

The total shutdown time includes the following values:

- VM Shutdown and Startup Durations

- AFS Shutdown Duration

- Abort Active Replications Duration

- Cluster Shutdown Duration

- Controller VM Shutdown and Startup Durations

- Execute Command File after Host Shutdown delay

- Shutdown Command File Duration

- SSH Action Delay

- Built-in delay of 2 minutes (this consists of a 10 second OS shutdown delay and a 60 second OS shutdown duration; rounded up)

The time required to gracefully shut down your operating system is not covered by the total shutdown time, as PowerChute cannot determine how long it will take to complete.

The Power Off Delay for the outlet group should be long enough for the OS to gracefully shut down. You should add extra time to allow for unforeseen circumstances.

The Low Battery Duration set on the NMC should be equal to or greater than the Power Off Delay for the outlet group.

Nutanix Shutdown - Single UPS Configuration
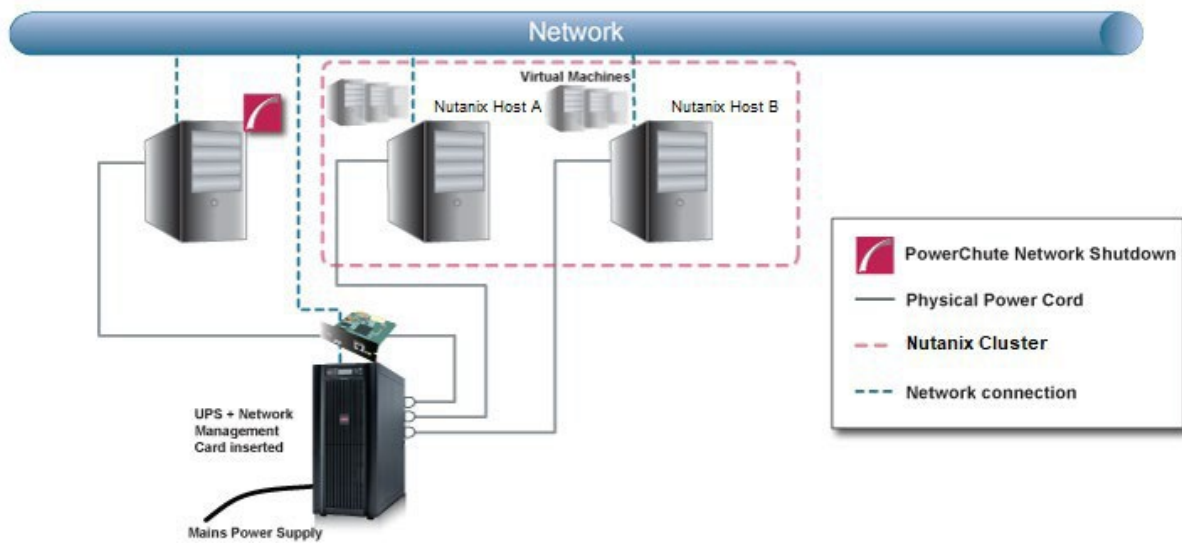
The following shutdown sequence occurs when the shutdown action is enabled for the On Battery event.

1. The UPS has been running on Battery power for x number of seconds.

2. PowerChute issues a command to turn off the UPS and UPS turnoff starts.

3. PowerChute issues a command to shut down the Nutanix hosts and shuts down the User VMs, AFS VMs, and Controller VMs on Nutanix hosts A and B.

4. PowerChute runs the shutdown command file if configured.

5. After the shutdown command file duration has elapsed, PowerChute shuts down the Nutanix hosts.

6. PowerChute shuts down the operating system on the physical machine running PowerChute.

Nutanix AHV Shutdown - Advanced UPS Configuration

Here, a UPS device is powering the physical PowerChute, and a single UPS is powering the two Nutanix hosts. PowerChute is installed on a physical machine outside of the Cluster and is monitoring all UPS devices. A shutdown command file has been configured for UPS Setup #1 containing UPS #1.
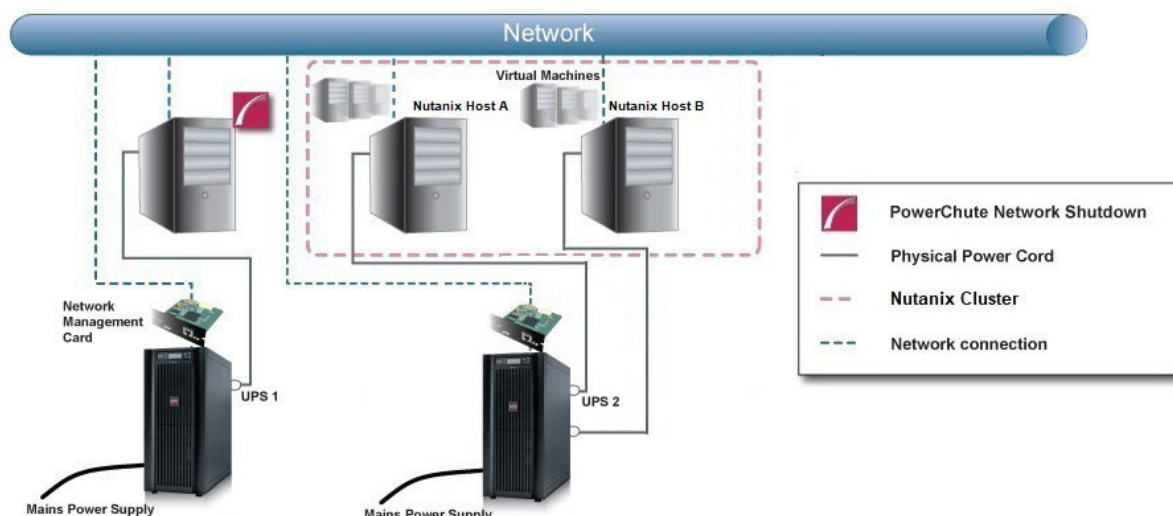
Critical event on UPS #1: Option to shut down virtual hosts and the physical machine are enabled for this UPS.

1. UPS #1 goes on battery.

2. PowerChute issues command to gracefully turn off UPS #1, if configured.

3. A UPS critical event is triggered for the two Nutanix hosts.

4. PowerChute issues a command to shut down the Nutanix hosts, and shuts down the User VMs, AFS VMs and Controller VMs on the two Nutanix hosts.

5. The shutdown command file or SSH action is executed.

6. After the shutdown command file duration has elapsed, if all VMs have shut down, PowerChute shuts down the two Nutanix hosts.

7. PowerChute shuts down the operating system on the physical machine running PowerChute.

Nutanix Shutdown - VM Prioritization - Single UPS Configuration

In this example, there are two Nutanix hosts, and the physical PowerChute server being powered by a single UPS. PowerChute is installed on a physical machine outside of the Cluster. VM Prioritization is enabled and VMs are prioritized into High, Medium, Low, Group 1, Group 2 priority groups.
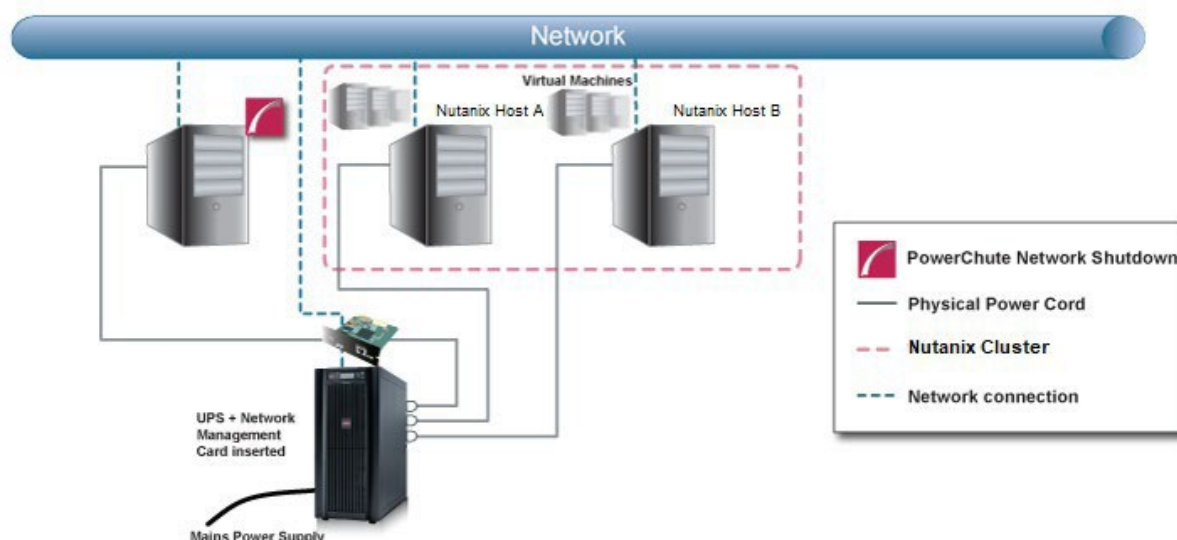
The following shutdown sequence occurs when the shutdown action is enabled for the On Battery event.

1. The UPS has been running on Battery power for x number of seconds. PowerChute starts the shutdown sequence on each protected host.

2. PowerChute issues a command to turn off the UPS, if configured.

3. PowerChute begins to shut down the VMs on Nutanix hosts A and B in the order in which they are prioritized:

   First, the un-prioritized VMs are shut down sequentially. As the duration for un-prioritized VMs elapses, the Group 2 VMs are shut down sequentially, followed by Group 1 priority VMs, then Low priority VMs, and Medium priority VMs, and finally the High priority VMs are shut down sequentially. The VMs within each priority group are not shut down in a particular order.

4. PowerChute runs the shutdown command file or SSH action.

5. After the shutdown command file duration has elapsed, PowerChute shuts down the Nutanix hosts.

6. PowerChute shuts down the operating system on the physical machine running PowerChute.

7. The UPS shuts down.

Nutanix Shutdown - VM Prioritization - Advanced UPS Configuration

In this example, a UPS device is powering the vCenter Server, and a single UPS is powering the two Nutanix hosts in the Cluster. PowerChute is installed on a physical machine outside of the Cluster. VM Prioritization is enabled and VMs are prioritized into High, Medium, Low, Group 1, Group 2 priority groups.
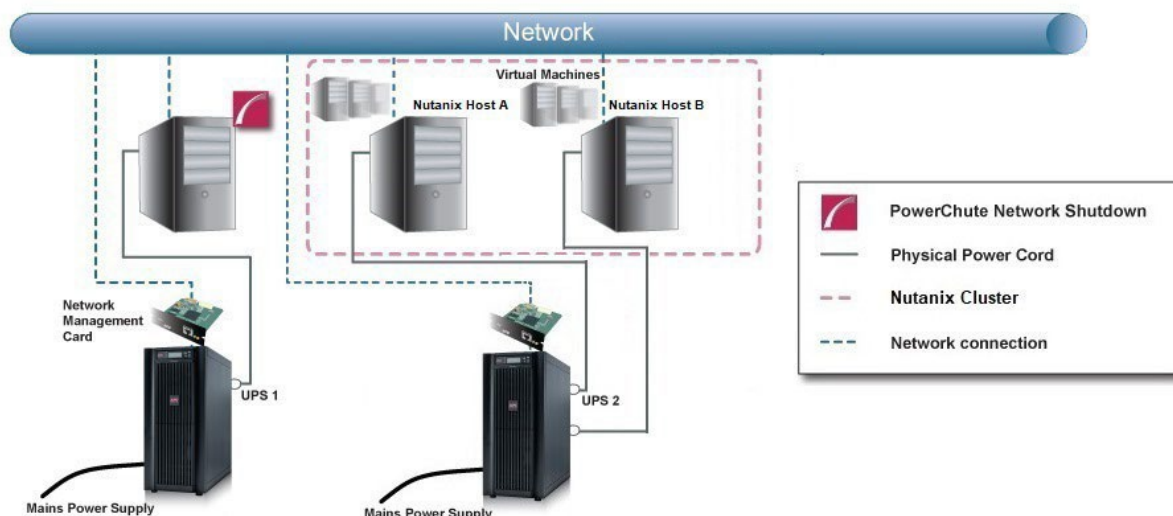
Critical event on UPS #2: Option to shut down virtual hosts is enabled for this UPS. VM Prioritization is enabled.

1. UPS #2 goes on battery.

2. A UPS critical event is triggered for Host A and Host B and PowerChute issues a shutdown command on the hosts.

3. PowerChute issues a command to turn off the UPS, if configured.

4. VMs will be shut down in the VM Shutdown sequence, in the order in which they are prioritized:

   First, the un-prioritized VMs are shut down sequentially. As the duration for un-prioritized VMs elapses, the Group 2 VMs are shut down, followed by Group 1 priority VMs, then Low priority VMs, and Medium priority VMs, and finally the High priority VMs are shut down. The VMs within each priority group are not shut down in a particular order.

5. After the shutdown command file or SSH action duration has elapsed, PowerChute shuts down Host A and Host B.

6. The UPS shuts down.

PowerChute Events and Logging

The Event Log displays UPS events that affect PowerChute and the load that it is protecting. Not all UPS events are logged. The log is refreshed automatically every 30 seconds.

By default, event logging is enabled for all configurable and non-configurable PowerChute events. To disable logging of an event, use the **Configure Events** screen.

The **EventLog.txt** file is located in the **group1** folder where PowerChute is installed. When the file reaches 1000 log entries, the oldest third of the file is deleted.

> 1000 is the default value, but you can change it using the PowerChute Configuration (INI) File. To do this:
>
> 1. Stop the PowerChute service/daemon. For more information, see Knowledge Base article FA290624.
>
> 2. Locate the **pcnsconfig.ini** file in the **group1** folder where PowerChute is installed and open it using a text editor.
>
> 3. In the section **[EventLog]** change the value for `logsize` to the desired value.
>
>   For example, to change the value to 2000 entries, change `logsize` to:
>
>   `logsize = 2000`
>
> 4. Save the pcnsconfig.ini file.
>
> 5. Restart the PowerChute service/daemon.

To completely clear the Event Log, use the **Delete Log File** button. Use **Export Log** to download a copy of the Event Log as a text file.

Configurable Events

- Available runtime has been exceeded

  For both conditions below, the "total shutdown time" includes the following durations:

  - Shutdown command file duration

  - SSH action duration

  - Built-in duration of 2 minutes (this consists of a 10 second OS shutdown duration and a 60 second OS shutdown duration; rounded up)

  This event occurs with either of the following conditions:

  Condition 1.

  When the total shutdown time required by PowerChute is greater than the Low Battery Duration minus two minutes configured for the UPS. In the event of a low battery condition, PowerChute will not have enough time to complete the shutdown sequence before the UPS powers off. For example, if the total shutdown time required is 3 minutes and Low Battery Duration is 4 minutes, the Available Runtime has been Exceeded event will be triggered.

  Resolution: Increase the Low Battery Duration value on the NMC using Configure - Shutdown or decrease the shutdown durations being used by PowerChute.

  Condition 2.

  When the shutdown duration configured for the UPS On Battery event plus the total shutdown time required by PowerChute is greater than the Runtime Remaining on the UPS minus two minutes. This condition can be caused by having too great a load on the UPS when the battery is fully charged.

  Resolution:

  1. Remove some equipment from the UPS to increase the available runtime.

  2. Decrease the shutdown duration time for the UPS On Battery event.

  3. Decrease the command file execution time using the Shutdown Settings screen.

  This event is logged and event actions are carried out even if it occurs on a single UPS in a Redundant or Parallel UPS configuration.

  - Available runtime is sufficient

    The available UPS Runtime/ Low Battery Duration is sufficient for PowerChute to shut down all equipment gracefully.

- Battery is discharged

  The UPS battery runtime has fallen below an acceptable range. If there is a power outage, a low battery condition will occur. This can be caused if the UPS has been operating on battery for an extended time period.

  If a Battery Recharged event does not occur within four hours, the UPS may not be charging properly, please contact APC Customer Support.

- Battery has recharged.

  The battery runtime of the UPS has returned to within an acceptable range.

- UPS in Bypass due to an internal hardware problem or UPS overload.

  The UPS has switched to bypass due to an internal hardware problem or because the UPS is overloaded.

- UPS has switched to bypass in response to the bypass switch at the UPS, typically for maintenance.

  A user put the UPS into bypass mode using a hardware switch.

- UPS has switched to bypass in response to the UPS front-panel or a user-initiated software command, typically for maintenance.

  The UPS has switched to bypass and cannot protect the load if a power outage occurs. This is a normal condition if maintenance is being performed on the UPS.

  If this event occurs when the UPS was not deliberately put into bypass, please contact Customer Support.

- UPS is no longer in Bypass.

  The UPS is no longer in a bypass state.

- Bypass switch is not working properly.

  The bypass contactor is not operating properly. This will prevent the UPS from being placed in bypass or returning from bypass. Please contact Customer Support.

- Bypass switch has been replaced.

  The bypass contactor is now operating properly.

- Communication has been lost while on battery.

  PowerChute lost communication while the UPS was on battery and cannot detect a Low Battery condition if the power outage continues. Graceful shutdown cannot be guaranteed.

  This occurs when the UPS is on battery and:

- The Management Card cannot communicate with the UPS or
- PowerChute cannot communicate with the Management Card.

- **Network Management Card cannot communicate with the UPS.**

  Communication between the NMC and the UPS has been lost. Make sure that the NMC is firmly inserted in its slot. This can occur during a firmware upgrade of the NMC.

- **PowerChute cannot communicate with the Network Management Card.**

  Network communication between PowerChute and the NMC has been lost. See Network Management Card Troubleshooting. This can occur during a firmware upgrade of the NMC.

- **Communication has been established.**

  Communication has been established between PowerChute and the NMC.

- **UPS has switched to battery power.**

  The UPS has switched to battery operation due to a power outage. If you can't restore power to the UPS, do the following:

  1. If there is no general power outage (i.e. if only this UPS has lost input power), check the building wiring and circuit breakers.

  2. If this event occurs occasionally and briefly, check to see if equipment on the same electrical circuit as the UPS uses high power periodically.

  3. This event can also be caused by poor power quality (i.e. power fluctuation). Decrease the sensitivity of the UPS through the NMC user interface.

  4. If the condition persists, contact an electrician to analyze your utility power.

- **UPS is no longer running on battery power or output power has been turned on.**

  The UPS is no longer running on battery power.

- **The load has exceeded the user specified alarm threshold.**

  The load on your UPS has exceeded the maximum load threshold, set in the NMC user interface. Reduce the load on the UPS or upgrade to a device that can support the existing load.

- **The load no longer exceeds the user specified alarm threshold.**

  The load on your UPS is no longer above the load threshold.

- **Minimum redundancy lost.**

  The UPS has too great a load or there are not enough power modules operational to support the desired redundancy.

  Check to see that all power modules are functioning properly and that the redundancy configuration is correct.

  If the condition persists, contact Customer Support.

- Minimum redundancy restored.

  The UPS can now support the desired redundancy.

- Parallel redundancy lost.

  The system has too great a load or there are not enough operational UPS's to support the desired redundancy level.

  Check to see that all UPS's are functioning properly and that the redundancy configuration is

  correct. If the condition persists, contact Customer Support.

- Parallel redundancy restored.

  The Parallel UPS system can now support the desired redundancy.

- The runtime remaining has dropped below the configured threshold while on Battery.

  The runtime remaining has dropped below the configured threshold while on battery. You can configure this threshold using the shutdown action on the Configure Events page.

  When the UPS in running on battery power and the runtime remaining on the UPS drops below the threshold, PowerChute will trigger a shutdown sequence. See "Sequenced Server Shutdown" for more information.

- The runtime remaining is now above the configured threshold or input power has been restored.

  Occurs when the UPS runtime is greater than the user defined threshold or if the UPS is no longer running on battery power.

- UPS has overheated which can cause damage.

  The UPS's internal temperature is too high. Make sure that there is at least one inch of clearance around the UPS, and that the UPS ventilation ports are not blocked. If this condition is not resolved quickly, damage may occur to your UPS.

- UPS is no longer overheated.

  The UPS's internal temperature has returned to an acceptable level.

- UPS output overload.

  The UPS has sensed a load greater than 100 per cent of its rated capacity. Remove attached equipment from the UPS until the condition is corrected. If this condition happens occasionally and briefly, check to see if some equipment connected to the UPS is using high power periodically (e.g. connected laser printers or photocopiers). If the condition persists, contact Customer Support.

- UPS overload condition has been corrected.

  A condition that caused the UPS output overload event to occur has been corrected.

Configurable Environmental Events

The following events are logged and event actions are carried out even if they occur on a single UPS in a Redundant or Parallel UPS configuration.

- Ambient Temperature Out Of Range Probe X.

  The temperature exceeds the threshold configured for the Environmental temperature probe.

- Ambient Temperature In Range Probe X.

  The temperature no longer exceeds the threshold configured for the Environmental temperature probe.

- Humidity out of Range Probe X.

  The humidity exceeds the threshold configured for the Environmental humidity probe.

- Humidity In Range Probe X.

  The humidity no longer exceeds the threshold configured for the Environmental humidity probe.

- Communication lost with Environmental Monitor.

  PowerChute has stopped receiving data from the Environmental Monitoring Card or the probe has been removed from the Universal I/O (UIO) port on the NMC.

  Check to see that the Environmental Monitoring Card is firmly inserted in its slot and has power. Check that environmental monitoring information is accessible through the NMC user interface.

  If PowerChute cannot communicate with the NMC you will need to correct that problem first.

- Communication established with the Environmental Monitor.

  PowerChute Network Shutdown is receiving data from the Environmental Monitoring Card/Probe.

- Contact X Alarm.

  One of the environmental input contacts is in an alarm state. Check in the location being monitored by this contact.

- Contact X Normal.

  One of the environmental input contacts has returned to a normal condition.

Non-Configurable Events

- Three unsuccessful logon attempts detected. Temporarily denying logon attempts from machine with IP <IP address>.

  There have been three invalid login attempts from a machine with the IP address listed in the event. Further login attempts will be prevented from this machine for two minutes. This is a security measure designed to prevent brute-force login attempts.

- Username was changed by user [User] from IP address [IP address]. New username is [Username].

  The Username has been changed by the user at the specified IP address. This is a security feature to notify the user when the Username has been changed.

- Password was changed by user [User] from IP address [IP address].

  The password has been changed by the user at the specified IP address. This is a security feature to notify the user when the password has been changed.

- Authentication phrase was changed by user [User] from IP address [IP address].

  The authentication phrase has been changed by the user at the specified IP address. This is a security feature to notify the user when the authentication phrase has been changed.

- Low-battery condition occurred.

  The runtime remaining on the UPS has dropped below the Low battery duration value while the UPS was on battery.

- UPS Turn off has been initiated.

  A graceful shutdown command has been issued to the UPS using the NMC User Interface, the LCD display or by PowerChute. This event is logged for all UPS Configurations.

- PowerChute Network Shutdown version X monitoring started.

  The PowerChute Web service has been started.

- Shutdown process started ‹OS name› will shut down soon.

  The operating system has started to shut down in response to a critical UPS event.

- Error: Outlet Group X is turned off for NMC X.

  The outlet group that PowerChute is registered with is turned off. This can indicate that PowerChute is not configured for the correct outlet group.

- Warning: Outlet Group X is turning off for NMC X.

  The outlet group that PowerChute is registered with is shutting down. A shutdown sequence will be started as a result.

- No Outlet Group specified. Using outlet group X.

  If PowerChute was not registered with an Outlet group during setup it will be automatically registered with the first outlet group on the UPS by default.

- PowerChute is unable to open TCP port [number]. Check that TCP port [number] is free.

  PowerChute uses TCP ports 3052 and 6547 for the Web User Interface. This event will be logged if another application is already using either of the above ports.

  Use the netstat command to identify which process is using these ports or change the values using the PowerChute Configuration File.

- PowerChute is attempting to open TCP port [number]

  PowerChute has begun to open the port it requires for the Web UI.

- PowerChute successfully opened TCP port [number].

  PowerChute has successfully opened the port it requires for the Web UI.

- PowerChute is unable to open UDP port 3052. Check that UDP port 3052 is free. This is required for NMC communication.

  PowerChute uses UDP port 3052 for communication with the NMC. This event will be logged if another application is already using this port. Use the netstat command to identify which application is using the port. This port cannot be changed.

- PowerChute is attempting to open UDP port 3052.

  PowerChute has begun to open the port required for NMC communications.

- PowerChute successfully opened UDP port 3052.

  PowerChute was able to open the port it needs for NMC communications.

- PowerChute cannot communicate with Network Management Card [ip_address]

  Reported when the PowerChute Agent cannot communicate with the Network Management Card over the network. This could be due to a mismatch in security credentials or a network issue.

- Network Management Card [ip_address] cannot communicate with the UPS.

  Reported when the Network Management Card cannot communicate with the UPS. If this issue persists please contact technical support.

- Connection unsuccessful because PowerChute received an untrusted SSL certificate from the NMC [protocol]://[ip_address]

  This can occur if registering with an NMC that has HTTPS enabled and is using an SSL certificate that is not signed by a trusted root certification authority.

  Ensure that trusted certificates are added to the **PowerChute-keystore** during registration. See Certificate Management for more information.

- PowerChute received an untrusted SSL certificate from the NMC https://[ip_address].

  Occurs when registering with an NMC that has HTTPS enabled if the SSL cert is not signed by a trusted root certification authority.

- PowerChute added a Network Management Card Self-Signed Certificate to the keystore.

  PowerChute added an NMC SSL certificate to the PowerChute-keystore. See Certificate Management for more information.

- UPS [ip_address] is running on battery power

  Reported when one UPS goes on battery in a UPS configuration with multiple UPS's.

- The On Battery UPS is no longer running on Battery power or output power has been turned on.

  Reported when one UPS in a UPS configuration with multiple UPS's returns to On Line operation.

- Outlet on UPS is turning off / UPS is turning off.

  The advanced option is enabled under UPS Shutdown Settings for a Redundant UPS Configuration and one UPS is on Battery.

- UPS [ip_address] has turned off.

  Reported when one UPS turns off in a UPS configuration with multiple UPS's.

- The turned off UPS has switched to On Line operation.

  Reported when one UPS turns back on in a UPS configuration with multiple UPS's.

- Multiple UPS's have been commanded to turn off / Outlet Group turn off has been initiated on Multiple UPS's.

  Reported in a Redundant UPS Configuration.

  In n+1 redundancy, this is reported when 2 UPS's turn

  off. In n+2 redundancy, this is reported when 3 UPS's

  turn off. In n+3 redundancy, this is reported when 4

  UPS's turn off.

- Multiple UPS have turned off.

Reported in a Redundant UPS Configuration.

In n+1 redundancy, this is reported when 2 UPS's turn

off. In n+2 redundancy, this is reported when 3 UPS's

turn off. In n+3 redundancy, this is reported when 4

UPS's turn off.

- Multiple Critical Events occurred.

  This occurs in a Redundant or Parallel-Redundant UPS Configuration when two different critical UPS events are active.

- Parallel-UPS Configuration not supported at address [ip_address].

  One of the UPS devices in a Parallel-UPS configuration has been removed from the Parallel system.

- Turning off UPS [NMC IP Address].

  PowerChute has sent a graceful shutdown command to the UPS. This is logged when a critical event occurs and the option to Turn off the UPS is enabled on the Shutdown settings page.

- Turning off outlet [Outlet Name] on UPS [NMC IP Address]

  PowerChute has sent a graceful shutdown command to the UPS Outlet group. This is logged when a critical event occurs and the option to Turn off the UPS Outlet Group is enabled on the Shutdown settings page.

- SNMP[version]: New connection by user [User] from [IP Address].

  A new user has connected to PowerChute via SNMP. This event is logged the first time a user connects after the PowerChute service restarts, or a SNMP setting is changed.

- SNMP[version]: Unsuccessful connection attempt by user [User] from [IP Address].

  PowerChute detected a new user attempting to connect via SNMP. This event is logged the first time a user is unable to connect after the PowerChute service restarts, or a SNMP setting is changed.

  NOTE: Some SNMP managers make unsuccessful attempts as part of their connection process. This will be indicated by the user "initial".

- SNMP: Configuration changed by user [User] from [IP Address]. [Config.ini Section].[Config.ini Key] set to [New Value].

  A PowerChute setting has been changed by [User] via SNMP.

Configuration (INI) File Events

The table below lists events that may be logged as a result of manual changes to the PowerChute Configuration File.

See PowerChute Configuration File.

> ⚠️ Before editing the Configuration file manually you should save a backup copy locally.

- **Error: PowerChute cannot find the configuration file or the backup configuration file. Shutting down.**

  PowerChute cannot locate pcsnconfig.ini or pcnsconfig_backup.ini to error.log in the group1 folder where PowerChute is installed. Please re-install PowerChute. If this does not resolve the issue contact APC technical support.

- **Error: The ini file is missing the required [x] section**

  A required section is missing or incorrectly named.

- **Error: The ini file is missing [x] key from section [x].**

  A required key is missing. Replace the missing key from a backup file.

- **Error: The ini file could not find IP address information in section [x].**

  NMC IP addresses are missing from the [NetworkManagementCard] section.

- **Error: The ini contains an invalid value for [x] in section [x].**

  An invalid value is present in the file and no previous good value or default is available in the backup file.

- **Error: The ini contains an invalid value for [x] in section [x]. Using {2} instead. Please validate the configuration.**

  An invalid value is found in the file but a previous valid value or default value is available in the backup file. This should be checked but no further action may be needed.

- **Error: The key [x] in section [x], did not match the supplied regular expression.**

  This can occur if you enter a username value that contains unsupported characters or if you entered a value other than http/https for the key protocol.

- **Error: Could not convert the value of [x] in section [x] to its expected type.**

  This can occur if you enter a non-numeric value where a numeric value is expected for example.

- **Error: Event [x] is enabled for command file execution, but an invalid value for [x] is specified**

  The command file specified cannot be found.
- **The ini file has entries defined outside of a section.**

  There are extra entries outside of a section that PowerChute does not recognize. These can be deleted.

- The invalid key [x] should be deleted from section [x] in the ini file.

  The configuration file contains keys that PowerChute does not recognize. These can be deleted.

- The ini file has detected duplicate values for [x] in section [x].

  When this occurs PowerChute will use the first value and this may result in an incorrect value being used e.g. if you enter 2 values for the HTTP port (80 and 8080), PowerChute will use 80 instead of 8080.

- The invalid section [x] should be removed from the ini file.

  The configuration file contains a section that PowerChute does not recognize. This can be deleted.

- Disabling command file execution for event [x] due to bad parameters. Please validate the configuration.

  This can occur on a Linux/ Unix system if the path to the command file is valid but the file itself does not have execute permissions.

- Username was changed from [Username 1] to [Username 2] via ini file.

  This notifies the user that the username has been changed via the ini file, for security purposes.

- Password was changed via ini file.

  This notifies the user that the password has been changed via the ini file, for security purposes.

- Authentication phrase was changed via ini file.

  This notifies the user that the authentication phrase has been modified via the ini file, for security purposes.

SSH Action Events

- Running SSH Action: [Action].

  PowerChute is running the SSH action [Action] on the remote host.

- SSH Action [Action] has already run.

  In an advanced UPS configuration, PowerChute runs each SSH action once for each host in the advanced group. This may result in multiple hosts attempting to run the same SSH action at the same time.

  This event is shown if a SSH action has already run on a host in the advanced group.

- SSH Action [Action] has completed.

  PowerChute has successfully completed executing the SSH action [Action] on the remote host.

- SSH Action [Action] has not completed within the configured duration.

  The SSH action [Action] could not complete as insufficient time was configured. Ensure sufficient time is provided in the **SSH Action Duration** field in the SSH Settings screen for your SSH actions to complete.

Java Update Events

- Updating Java using [Java file].

  PowerChute is attempting to update the Java version used by PowerChute to [Java file]. Allow 2-3 minutes for the Java update to complete.

- Java has successfully updated. Restarting PowerChute.

  The Java version used with PowerChute has successfully updated. The PowerChute service will restart for changes to take effect.

- Unable to update Java. See error.log for details.

  PowerChute was unable to update the Java version used with PowerChute. For more information, see error.log.

Nutanix Virtualization Events

The events below are non-configurable and relate to virtualization tasks such as VM shutdown.

- Shutting down User VMs in the Cluster.

  A critical event has occurred on the UPS powering the Nutanix Cluster and PowerChute is shutting down the User Virtual Machines (UVMs) in the Cluster. This is the first step in the shutdown sequence.

- Nutanix User VMs cannot be gracefully shut down. Powering off UVMs.

  PowerChute was unable to gracefully shut down the Nutanix User Virtual Machines (UVMs). PowerChute will attempt to power off the UVMs.

- Powering on VMs on Cluster [Cluster].

  A critical event has resolved on the UPS powering the Nutanix Cluster and PowerChute is powering on the User Virtual Machines (UVMs) in the Cluster.

- Insufficient time configured to shut down VMs on Cluster [Cluster].

  PowerChute was unable to gracefully shut down your VMs, power off your VMs, and force them off, on Cluster [Cluster] as insufficient time was configured. Ensure sufficient time is provided in the **Duration** field in the Virtual Machine Shutdown/Startup screen for all your VMs to gracefully shut down.

- Shutting down Nutanix AFS.

  A critical event has occurred on the UPS powering the Nutanix Cluster and PowerChute stops the Acropolis File Service which shuts down the AFS VMs in the Cluster. This step occurs after the User VMs are shut down.

- Nutanix AFS cannot be gracefully shut down.

  PowerChute was unable to stop the Acropolis File Service and shut down the AFS VMs in the Cluster.

- Starting Nutanix AFS.

  A critical event has been resolved and PowerChute is trying to start the Acropolis File Service which will start up the AFS VMs in the Cluster.

- Nutanix AFS cannot be started.

  PowerChute was unable to start the Acropolis File Service and start up the AFS VMs in the Cluster.

- No replication in progress for Protection Domain. Proceeding with shutdown sequence.

  PowerChute did not detect any active replications for a Protection Domain. This step of the shutdown sequence is skipped, and PowerChute continues to the next step, shutting down the Nutanix Cluster.

- Replication in progress for Protection Domain detected. Waiting the configured delay.

  PowerChute detected active replications for a Protection Domain. PowerChute will wait the delay specified in the **Duration** field on the Protection Domain Settings screen before aborting replications.

- Aborting replication in progress for Nutanix Protection Domain.

  PowerChute is aborting any active replications of your protection domain(s).

- Nutanix Protection Domain replications cannot be gracefully aborted.

  PowerChute was unable to abort your active protection domain replications.

- Shutting down Cluster.

  PowerChute is attempting to shut down the Nutanix Cluster.

- Cluster cannot be gracefully shut down.

  PowerChute was unable to shut down the Nutanix Cluster.

- Starting up Cluster.

  PowerChute is attempting to start up the Nutanix Cluster.

- Cluster started successfully.

  PowerChute successfully started up the Nutanix Cluster.

- Cluster cannot be started.

  PowerChute was unable to start up the Nutanix Cluster.

- Could not connect to the Nutanix Cluster. Cannot stop Nutanix Cluster services.

  PowerChute was unable to establish a connection to the Nutanix Cluster.

  Verify that your Cluster is running and verify the credentials specified in the **CVM/Cluster Details** screen.

- Shutting down Controller VMs [CVM].

  A critical event has occurred on the UPS powering the Nutanix Cluster and PowerChute is shutting down all Controller Virtual Machines in the Cluster. Controller VMs are shut down after all other VMs in the Cluster, and the Nutanix Cluster itself are shut down.

- Attempting to start Controller VM [CVM].

  A critical event has been resolved and PowerChute is attempting to start up the Controller Virtual Machine [CVM]. This event is triggered after the Nutanix host is online.

- Waiting for Controller VM startup to complete.

  A critical event has been resolved and PowerChute is waiting for the Controller Virtual Machines in the Nutanix Cluster to startup. The Nutanix Cluster will start up when Controller VM startup is complete.

- Controller VM startup is in progress for Host [Host]. PowerChute will wait for the startup delay to elapse before starting the shutdown sequence.

  The Controller Virtual Machines on [Host] are starting up. PowerChute will wait the specified duration in the **Startup Duration** field in the Controller VM Shutdown/Startup screen before proceeding with the shutdown sequence.

Critical Events in a Redundant-UPS Configuration

This topic does not apply to Advanced Configuration with Advanced UPS Setups. For more information about Critical Events in Advanced UPS Setups, please view the "Using PowerChute Network Shutdown in an Advanced Redundant Setup" Application Note here.

PowerChute Network Shutdown considers all UPS devices in a Redundant configuration as one UPS System. Each UPS must be able to support the entire load itself.

PowerChute follows these shutdown rules when it detects critical events:

- 2 identical critical events (such as **Low-Battery Condition Occurred** OR **UPS turn off has been initiated**) occurring in succession on 2 UPS devices cause a shutdown. The shutdown is immediate and no configured delay is counted down.

- 2 identical user-configured critical events such as **UPS On Battery**

- **Low-Battery Condition Occurred** and **PowerChute cannot communicate with the Management Card** which always leads to a shutdown. Prior to the PowerChute shutdown process starting, a 10-second delay is counted. No configured delay time is counted down.

Critical Events in a Parallel-UPS Configuration

In Parallel-UPS configurations, the combined outputs of several UPS devices support the load. With this setup, PowerChute monitors the load as it changes to determine whether the mode of operation is Parallel Capacity or Parallel Redundant.

For example, you are operating in a Parallel Redundant mode (i.e., there are more UPS devices available than are required to provide power to the load) and then you increase the load by adding new servers. PowerChute detects if the mode of operation changes to Parallel Capacity (i.e., all UPS devices in the configuration are now required to provide power to the load). This could cause PowerChute to initiate a shutdown if just one critical event is triggered.

Scenario 1: Three 10kVA UPS devices supporting a 16kVA Server Load (Parallel Redundant)

In this Parallel Redundant configuration, two or more critical events occurring cause PowerChute to trigger a graceful shutdown of the server(s).

PowerChute follows these shutdown rules.

- 2 identical critical events (such as **Low-Battery Condition: Occurred** OR **UPS turn off has been initiated**) occurring in succession on 2 UPS devices cause a shutdown. The shutdown is immediate and no configured delay is counted down.

- 2 identical user-configured critical events such as **UPS: On Battery** occurring in succession on 2 UPS devices will cause a shutdown. Any configured delay is counted down first.

- 2 different critical events (such as **Low-Battery Condition: Occurred** and **PowerChute cannot communicate with the Management Card**) occurring in succession on 2 UPS devices cause the event called **Multiple Critical Events occurred** which always leads to a shutdown. Prior to the PowerChute shutdown process starting, a 10-second delay is counted. No configured delay time is counted down.

Scenario 2: Three 10kVA UPS devices supporting a 23kVA Server Load (Parallel Capacity)

In this Parallel Capacity configuration, one critical event triggers a graceful shutdown of the

server(s). However, if 2 occur, they have these delays.

- If 2 *identical* critical events occur in a parallel capacity configuration, then the event is only reported once and any configured delay is counted down.

- If 2 *different* critical events occur, then both events are reported separately and the shortest shutdown delay of the two is counted down.

Scenario 3: Two 10kVA UPS devices supporting an 8kVA Server Load (Parallel Capacity)

In this Parallel Capacity configuration, one critical event occurs and graceful shutdown of the server(s) is not triggered as the single UPS device can still support the connected load.

Scenario 4: Two 10kVA UPS devices supporting an 8kVA Server Load (Parallel Capacity)

In this Parallel Capacity configuration, two *identical* critical events occurring causes PowerChute to trigger a graceful shutdown of the server(s). The shutdown is immediate and no configured delay is counted down.

Logging

Fatal Errors

Microsoft Windows

On Windows operating systems, use Microsoft Event Viewer to view the messages wriitten to the Operating System Event Log. PowerChute Logs are displayed under Windows Logs - Application. In the **Source** field, the "PowerChute" value is provided for PowerChute events.

The PowerChute service will not start if the configuration files are missing, or the service is prevented from accessing the files due to permissions.

The following image shows an example of a service start error:
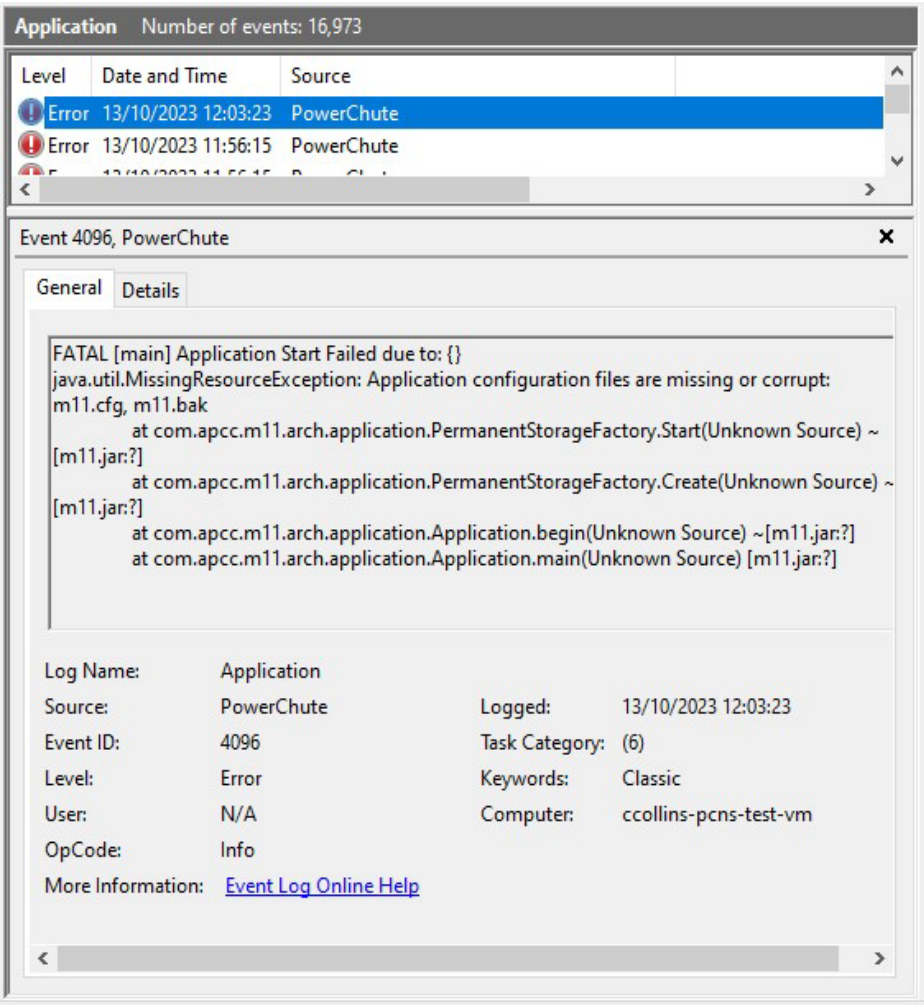
Linux

On Linux operating systems, service logs are written to the system journal. To review all the service events related to PowerChute, use the following command: `journalctl -u PowerChute.service`

To review the most recent service action, use the following command as an alternative: `systemctl status PowerChute`

The service indicates "inactive (dead)" status, when the service has stopped, and the context provides additional information about why the service has ended. Additional logs in error.log file will display information on unexpected service halts.

Non-Fatal Errors

Error conditions that are significant to operators but do not cause the service to stop are logged in the error.log. Examples include network conditions preventing connection to VCenter, controller VMs, cluster hosts, and other collaborating systems. Operators are advised to review logs periodically to ensure PowerChute configuration and network conditions enable PowerChute to react to UPS events.

Logging to Third Party Systems

PowerChute manages logging through Log4J. This is configured by the configuration file `log4j2.xml` in the installation directory.

Windows Event Log

On Windows installations, the Event Log records the below events. You can view these events with Windows Event Viewer in the Application Log.

1. **UPS Events**

   - All events enabled for logging are reported to the Windows Event Log.
2. **Service Fatalities**

   - Any event causing PowerChute to stop running.
3. Unsuccessful Command File execution 4. Unsuccessful SSH Action execution

   PowerChute issues the Command File and SSH Action events at pre-defined stages of the startup and shutdown procedure and it considers them successful once they begin running. Warning or error events are not logged for command files or SSH Actions which run for extended periods, or for scripts which have errors during execution.

Syslog (Insecure)

PowerChute uses Log4J SyslogAppender to direct logs to an appropriately configured syslog server.

The following configuration is provided in the `log4j2.xml` file, in the installation directory.

```
<Syslog name="syslog" format="RFC5424" host="localhost" port="514" protocol="UDP"
appName="PowerChute" facility="ALERT" enterpriseNumber="1.3.6.1.4.1.318"
messageId="PowerChute"/>
```

This configuration will forward log events to a syslog server over UDP to port 514. This transport mechanism is considered insecure because data on the network is not encrypted, and the network endpoints do not mutually authenticate each other. This configuration is not recommended for production deployments.

Configure Insecure Syslog

1. Modify the **host** setting and specify the syslog server host details, with the IP address for Fully Qualified Domain Name.
2. Modify the **port** setting to specify the syslog server input port.
3. Modify the **protocol** setting to specify TCP or UDP transport.

Syslog (Secure)

PowerChute uses Log4J SyslogAppender to direct logs to an appropriately configured syslog server.

The following configuration is provided in the `log4j2.xml` file, in the installation directory.

```
<Syslog name="syslog_sec" format="RFC5424" host="localhost" port="6541" protocol="TLS"
appName="PowerChute" facility="ALERT" enterpriseNumber="1.3.6.1.4.1.318"
messageId="PowerChute">
<SSL>
 <KeyStore location="/path/to/syslog_keystore.jks" type="PKCS12" password="apassword" />
      <TrustStore location="/path/to/syslog_truststore.jks" type="PKCS12"
password="apassword" /> </SSL>
</Syslog>
```

This transport mechanism is considered secure because the data transported over the network is protected by TLS, and network endpoints can mutually authenticate each other.

Configure Secure Syslog

1. Modify the **host** setting and specify the syslog server host details, with the IP address or Fully Qualified Domain Name.
2. Modify the **port** setting to specify the syslog server input port.
3. Modify the KeyStore and TrustStore file settings.

KeyStore and TrustStore file for Secure Syslog

The PowerChute KeyStore contains a certificate which is presented to the server to establish trust in the connecting client. The client certificate should be countersigned by your trusted Certificate Authority. The TrustStore file contains the syslog server certificate from the Certificate Authority and enables PowerChute to authenticate the server's certificate. For information on the passwords required for the KeyStore and the TrustStore, see Log4J SSL configuration manual.

Create a KeyStore

1. To create a KeyStore, issue the following commands:
    ```
    keytool -keystore syslog_keystore.jks -genkey -keysize 4096 keyalg RSA -alias client
    ```

2. Enter the KeyStore password when prompted and follow the prompts to set the certificate details for your location and organization. Ensure that the certificate **Common Name** contains the **Fully Qualified Domain Name** for the PowerChute host.

3. Generate a Certificate Signing Request from your new KeyStore:
    ```
    keytool -certreq -alias client -file client.csr -keystore syslog_keystore.jks
    ```

4. Enter the KeyStore password when prompted. This will generate a certificate signing request file to `client.csr`. Use the certificate signing request to sign the client certificate with your trusted Root Certificate Authority certificate.

5. Import the public root Certificate Authority certificate into the KeyStore:
    ```
    keytool -keystore syslog_keystore.jks -import -file rootCA.crt alias root-ca
    ```

6. Import the signed client certificate into the KeyStore:
    ```
    keytool -keystore syslog_keystore.jks -import -file client.crt alias client
    ```

7. Copy the `syslog_keystore.jks` file into the PowerChute installation directory.

8. Modify the `log4j2.xml` configuration file to specify the full path to the file in the KeyStore location setting.

9. Modify the password setting to contain the KeyStore password.

Create a TrustStore file

1. To create a TrustStore file, issue the following commands:
    ```
    keytool -keystore syslog_truststore.jks -genkey -alias deleteme
    ```

2. When prompted, provide the values for a new certificate in the file and create a password for the TrustStore.

3. Delete the certificate to create an empty KeyStore:
    ```
    keytool -keystore syslog_truststore.jks -delete -alias deleteme
    ```

4. Import the Certificate Authority public certificate into the KeyStore:
    ```
    Keytool -keystore syslog_truststore.jks -import -file
    /path/to/rootCA.crt -alias syslog-ca
    ```

5. Copy the `syslog_truststore.jks` file to the PowerChute installation directory

6. Modify the `log4j2.xml` configuration file to specify the full path to the file in the TrustStore file location setting.

7. Modify the password setting to contain the TrustStore file password.

General

This section contains information on the topics below:

- Communications Settings
- PowerChute Agents
- PowerChute Configuration (INI) File
- Resetting your PowerChute username or password
- Java Update
- User Interface Session Timeout
- Check for Updates
- Customer Support
- Customer Experience Improvement Program (CEIP)
- License

Communications Settings

PowerChute Access

HTTPS is enabled by default and provides secure access to the PowerChute user interface. You may change the Protocol to HTTP (unencrypted) and this will come into effect after you restart the PowerChute service. For more information, please see the PowerChute Security Handbook.

PowerChute Security

The Username and Authentication Phrase are used to authenticate communications between PowerChute and the NMC. Therefore, you must set these values to be the same in both PowerChute and the NMC.

- The maximum number of characters for the user name is 10.

- The authentication phrase must be 15 to 32 ASCII characters.

- The password specified here is unique to PowerChute. The password requires:

  - Minimum 8 and maximum 128 characters in length

  - One upper and lower case letter

  - One number and special character

  - The username cannot be part of the password.

  - Passwords with leading and trailing white spaces are removed.

  - Passwords containing a white space are kept.

Changes to the Username, Password and Authentication Phrase are logged to the event log. For more information see Non-Configurable Events.

If you forget your password, see Resetting your PowerChute username or password.

If PowerChute is registered with more than one NMC, they should all use the same administrator user name and authentication phrase.

Click the **Check Details** button on the Communications Settings page to validate that the PowerChute settings are the same as the NMC(s).

PowerChute Agents

The PowerChute Agents page, under the **UPS Configuration** menu option, lists all PowerChute Agents registered with the same NMC(s).

Loading this screen may be slow as PowerChute tries to resolve the host name for each Agent. If the host name cannot be resolved, just the IP address will be displayed. You can click on an IP address to launch the PowerChute user interface for that Agent.

A maximum of 50 PowerChute Agents can be registered with a single NMC. For more information, please view Application Note "PowerChute Network Shutdown with more than 50 computers" here.

> If you uninstall a PowerChute Agent, its IP address remains registered with the NMC and must be removed manually using the NMC UI.

If **System Problem Report** is displayed when accessing the screen, this is because PowerChute has not received the information it requires from the NMC(s). During normal operation, this can happen due to network traffic. Try the menu selection again in a few minutes.This may also occur if PowerChute cannot establish communication with the NMC. See Network Management Card Troubleshooting.

PowerChute Configuration File

PowerChute stores all its settings in a configuration file called **pcnsconfig.ini**, located in the **group1** folder where PowerChute is installed.

This file is updated when running the PowerChute Setup and when you make configuration changes through the user interface, e.g. enabling shutdown actions for events.

After you have configured one installation of PowerChute with your required settings you can use the pcnsconfig.ini file to apply the same settings to another copy of PowerChute on a different machine. Certain settings such as the **localHostAddress** or **UnicastAddress** values in the [**Networking**] section will need to be edited manually for the target machine.

To apply the settings on the target machine:

Stop the PowerChute service. For more information, see Knowledge Base article FA290624.

Replace the existing copy of pcnsconfig.ini in the group1 folder.

Start the PowerChute service.

Resetting your PowerChute username or password

If you forget your username or password, you can re-set them by editing the pcnsconfig.ini file.

In the [**NetworkManagementCard**] section of the INI file, set the following lines with your new

values: username= new user name

password= new password

Save the file and re-start the PowerChute service.

Java Update

The Java Update feature enables you to change the Java Runtime Environment (JRE) used by PowerChute to any other JRE already installed on your system. Follow the steps below to update the Java version used by PowerChute.

1. Download a valid JRE on your system. JREs can be downloaded from the AdoptOpenJDK website.

   PowerChute supports AdoptOpenJDK 11. You can only update the Java version used with PowerChute to a 64-bit JRE.

   The Java versions supported by PowerChute are posted on the APC website here.

2. Navigate to the PowerChute installation directory, and create a new folder called "Updates". If the default installation directory was chosen during installation, this location will be:

   - C:\Program Files\APC\PowerChute\Updates for Windows systems

   - /opt/APC/PowerChute/Updates/ for Linux systems

3. Copy the Java file downloaded in Step 1 above to the Updates directory.

4. Navigate to the **About** screen in the PowerChute UI (**Help > About**). In the **Java Update Available** field, the downloaded Java file will be listed in a drop-down box.

5. Select the Java version you want to update PowerChute to use from the drop-down box, and click **Upgrade**.

6. A confirmation dialog will appear. Click **OK**.

7. Another dialog will appear and PowerChute restarts. Wait 2-3 minutes for the Java version to successfully update.

8. When the PowerChute service restarts, refresh your browser and navigate to the **About** screen. The **Java Version** field will be updated to show the new Java used by PowerChute.

It is not necessary to keep the downloaded Java files in the Updates directory after the Java update is complete.

User Interface Session Timeout

The PowerChute user interface has a ten minute session timeout by default. Following ten minutes of inactivity, the session will be terminated and the login screen will display to enter the username and password. It is possible to increase or decrease the duration of the session timeout by editing the **Web.xml** file.

To change the session timeout duration:

1. Stop the PowerChute service. For more information, see Knowledge Base article FA290624.

2. Open the folder where the installed files are located, and locate the file at the following location:

   ```
   \group1\comp\http\html\WEB-INF\web.xml
   ```

   Open the **Web.xml** file with a text editor.

3. Locate the the **<session-config>** element, e.g:

   ```
   <session-config>

       <session-timeout>10</session-timeout>

   </session-config>
   ```

4. The duration value in the **<session-timeout>** element can be changed. For example to change the timeout to 15 minutes, change the **<session-timeout>** value to 15, e.g.:

   ```
   <session-config>

       <session-timeout>15</session-timeout>

   </session-config>
   ```

5. Save the Web.xml file.

6. Start the PowerChute service.

The PowerChute UI will now timeout following a period of inactivity that corresponds to the new **<session-timeout>** value.

Check for Updates

The **Enable Automatic Updates** feature is selected by default and informs you when a new software update is available.

When enabled, PowerChute checks for available software updates when the service is started and every seven days after that. You can also check for updates immediately by clicking the **Check Now** button.

When a new software version is released, key details and a link to download the new version are displayed on the Check for Updates screen and logged in the Event Log and MIB browser via SNMP traps.

You can disable the software update notifications feature on the last screen of the PowerChute Setup wizard or on the Check for Updates page.

Customer Support

For customer support options, please visit www.apc.com/support as a starting point.

The Knowledge Base there contains detailed troubleshooting information for product issues.

You can also browse discussion forums or submit a query using e-mail.

For country-specific support centers' contact details, go to www.apc.com/support/contact-us and select your country from the drop-down box list. This lists the contact details for support services you may require.

Customer Experience Improvement Program (CEIP)

PowerChute's Customer Experience Improvement Program (CEIP) provides us with the information that enables us to improve our product and services, and helps us to advise you on how best to deploy and configure PowerChute.

As part of the CEIP, we will collect certain information about how you configure and use PowerChute Network Shutdown in your environment. This information is completely anonymous, and cannot be used to personally identity any individual. For more information, please refer to the CEIP Frequently Asked Questions on the APC website.

By default, you are participating in the PowerChute CEIP. If you prefer not to participate, unselect the **Join PowerChute Customer Experience Improvement Program ("CEIP")** checkbox in the PowerChute CEIP page. You can join or leave the CEIP at any time.

License

PowerChute v5.1 is a licensed product. A license can be purchased through your Schneider Electric IT Partner and is required for PowerChute to function and to perform graceful system shutdown.

NOTE: A PowerChute license is required for all configurations except local OS shutdown, configured by selecting **Do not enable Virtualization Support** in the installer or selecting the **Standalone VMware Host** option in the **VMware Configuration** page in the PowerChute Setup wizard.

Cloned PowerChute VMs are considered unlicensed.

License screen in the PowerChute Setup wizard

Purchase a License

A PowerChute license can be purchased through your Schneider Electric IT Partner.

Activate License

You can activate your purchased license online using the Schneider Electric Cloud Licensing Server or offline. **NOTE:** The validation process requires an Internet connection to connect to the Schneider Electric Cloud Licensing Server.

You can also use the Schneider Electric Local Licensing Server to activate your license. See the Local Licensing Server Guide for more information.

If you purchased more than one license, you can enter the same Activation ID for each PowerChute agent that you install. You can return a license before uninstalling PowerChute to reuse the license for a new agent. See Return License.

Activate a Trial License

PowerChute v5.1.0 allows customers to avail of a trial license which can be activated during the Setup Wizard. A trial license enables all PowerChute functionalities for 30 days from the date of license activation. The purpose of the trial is to test PowerChute in your virtualized or HCI environment before purchasing a license.

> The trial license can only be activated once. When the trial period has expired, PowerChute becomes unlicensed. Functionalities will be restricted and your environment will no longer be protected.

To enable full functionality, you must purchase a license which can be deployed at any time before, during, or after a trial license.

Online Activation

If the machine running PowerChute has an Internet connection, you can use the Schneider Electric Cloud Licensing Server to validate your license:

1. Select the **Activate Online** radio button.

2. Enter the license's **Activation ID.** This is in the format ACT-XXXX-XXXX-XXXX-XXXX.

3. Enter your **Proxy IP Address and Port Number**, **Proxy Username** and **Proxy Password** if required.

4. Enter the **Quantity** of nodes in your cluster protected by the PowerChute instance. One license is required for each node protected by PowerChute.

5. Click the **Activate** button.

6. PowerChute will contact the Schneider Electric Cloud Licensing Server to validate the provided Activation ID. If the license is successfully validated, PowerChute will display the license details.

Offline Activation

If the machine running PowerChute does not have an Internet connection, you can validate your license offline:

1. Select the **Activate Offline** radio button.

2. Enter the license's **Activation ID.** This is in the format ACT-XXXX-XXXX-XXXX-XXXX.

3. Enter the **Quantity** of nodes in your cluster protected by the PowerChute instance. One license is required for each node protected by PowerChute.

4. Click the **Generate Request** button. This will generate and download a request file called `request_[GUID].bin` in your Downloads folder. This file can also be found in the user_files directory. If the default location was chosen during installation, this location will be: /opt/APC/PowerChute/user_files/

   - C:\Program Files\APC\PowerChute\user_files for Windows systems

   - /opt/APC/PowerChute/user_files/ for Linux systems

5. Click the **Open Licensing Portal** button to open the Schneider Electric Licensing Portal in a new browser tab.

   a   Log in via your **Activation ID**.

   b   Navigate to **Devices > Offline Device Management** and upload the `request_[GUID].bin` file generated in step 4.

c   Download the generated license (`capabilityResponse.bin` file).

6. Return to PowerChute and click the **Upload Response** button and select the downloaded `capabilityResponse.bin` file using the file selector.

> ⚠️ If the `capabilityResponse.bin` file is modified or the download was corrupt, the file will be invalid, and the license cannot be activated. If an error message is displayed in the UI related to the capability response, follow the above steps again to generate and download a new `capabilityResponse.bin` file.

7. If the license is successfully validated, PowerChute will display the license details.

Renew License

The displayed **Renewal Date** is when your PowerChute license will expire. You can renew your license **before** the **Renewal Date** is reached. You will be notified 60 days in advance of your license expiring. If you do not renew your license before it expires, you must purchase and activate a new license.

Expired License

PowerChute provides a 60-day grace period after your license expires to allow you to purchase a new license. See Purchase a License. Once you have purchased a license, update your license details in the **Renew License** screen for continued PowerChute functionality. **NOTE:** PowerChute remains functional during the grace period.

If you do not update your license details during the grace period, you will no longer have access to configuration options in the PowerChute UI and the PowerChute Setup wizard − except the **License** screen − and shutdowns and startups will be canceled.

> ⚠️ PowerChute cannot perform graceful system shutdown if the software is unlicensed. It is highly recommended that you renew your license to prevent potential data loss.

Return License

You can return a license before uninstalling a PowerChute agent to be reused for a new agent. Returning a license will increase the **Quantity** associated with your **Activation ID** by the quantity that was returned. For example, if you returned 5 PowerChute licenses, your **Quantity** will increase by 5.

You can view how many licenses you have remaining in the Schneider Electric Licensing Portal:

1. Log in via your Activation ID.

2. Navigate to **Activation & Entitlements > List Entitlements**.

3. You can view the total quantity, available quantity, and expiration date of the licenses associated with your Activation ID.

NOTE: When you return a license, the PowerChute agent will be unlicensed and no longer function.

If you activated your license via the online method, click the **Return License** button in the **License** screen.

It is not supported to return a license if you activated your license via the offline method. To reuse licenses on offline PowerChute machines, contact Customer Support.

When you have successfully returned a license, you can uninstall the PowerChute agent.

Free/Open Source License Details

PowerChute stores the details of the free and open source licenses used in PowerChute in the notice.txt file located in the PowerChute installation directory. If the default installation directory was chosen during installation, this location will be:

- C:\Program Files\APC\PowerChute for Windows systems

- /opt/APC/PowerChute for Linux systems

Troubleshooting

This section contains information on the topics below:

- Network Management Card Troubleshooting
- Nutanix Troubleshooting
- Browser Troubleshooting
- SSH Actions Troubleshooting
- SNMP Troubleshooting
- General Troubleshooting

Network Management Card Troubleshooting

PowerChute does not register with the Network Management Card(s) or PowerChute reports communications lost with the Network Management Card(s):

1. Verify that the Administrator Username and Authentication Phrase are the same for PowerChute and the NMC.

2. Verify that UDP port 3052 is not being blocked by a firewall.

3. Check the IP settings on the PowerChute machine and on the NMC user interface to verify that the default gateway and subnet mask are correct.

4. Check that the IP address of the Network Management Card has not changed after PowerChute was registered with the NMC. To check this, click on the Communications Settings menu item in PowerChute and check that the IP address shown in the Network Management Card section is correct.

5. Verify that there is a network connection between the PowerChute client computer and the Network Management Card. Attempt to access the Network Management Card from the PowerChute client computer, or use the ping utility from the Network Management Card.

6. A PowerChute Network Shutdown client that acquires its IP address through DHCP will lose communications with the Network Management Card when the client renews its DHCP address lease and acquires a different IP address. To resolve this issue,each system using PowerChute Network Shutdown must have a permanent IP address. Reserve IP addresses in the DHCP server by using the MAC address of the clients, so that they never change for the specified machines. The NMC should also have a static IP address.

7. Verify that the PowerChute service is started. If it is already started, stop the service and then restart it again.

8. Update the firmware on the NMC to the latest version which can be downloaded from the APC Web site, or contact "Customer Support".

Nutanix Troubleshooting

Cluster Connection

If the connection to your Nutanix Cluster or Nutanix Controller Virtual Machines is lost, the following log messages and exceptions may appear in the error.log:

"Failed to start connection; nested exception is:"

"net.schmizz.sshj.transport.TransportException: Broken transport; encountered EOF"

"java.net.ConnectException: Connection times out: connect"

Nutanix Cluster not available for any cluster service stop operations

This error may occur if the Cluster is down when PowerChute attempts to stop the Cluster. This could also happen if your Nutanix Cluster credentials have changed after configuring PowerChute. Ensure the correct Cluster/Controller VM credentials are provided via the PowerChute Setup wizard, or the Nutanix Settings screen.

The error below is written to the PowerChute Event Log:

"Could not connect to the Nutanix Cluster. Cannot stop Nutanix Cluster services."

Nutanix Cluster cannot be stopped

This can be caused by an unsuccessful attempt to stop AFS or an unsuccessful attempt to power off all User VMs. To resolve this issue, ensure you configure a sufficient duration to successfully stop AFS and power off all the User VMs.

The error below is written to the PowerChute Event Log:

"Cluster cannot be gracefully shut down."

Unable to start Nutanix Cluster

Cluster may not start if the time drift is incorrectly set. To check if the time between the individual Controller VMs is correctly synchronized, execute the following command:

allssh date

For information on configuring time synchronization for your Nutanix Cluster, see the following recommendations from Nutanix.

This could also happen if your Nutanix Cluster credentials have changed after configuring PowerChute. Ensure the correct Cluster/Controller VM credentials are provided via the PowerChute Setup wizard, or the Nutanix Settings screen.

The error below is written to the PowerChute Event Log:

"Cluster cannot be started."

VM Shutdown

Unable to shut down User VM

When PowerChute issues a VM shutdown command, PowerChute will use the time specified in the **Shutdown Duration** field to allow VMs to gracefully shut down. If VM shutdown is unsuccessful, PowerChute will attempt to power off the VMs. If PowerChute cannot power off the VMs, they will be forced off.

The error below is written to the PowerChute Event Log:

"Nutanix User VMs cannot be gracefully shut down. Powering off UVMs."

The errors below are written to the PowerChute error.log:

"User VMs did not shutdown in time, trying to power off."

"Force off remaining Nutanix User VMs."

The time set in the Duration field was insufficient to allow VMs to gracefully shut down

To resolve this issue, increase the **VM Shutdown Duration** provided in the Virtual Machine Shutdown and Startup screen to allow sufficient time for User VMs to gracefully shut down.

The error below is written to the PowerChute Event Log:

"Insufficient time to shut down all VMs using the VM Shutdown Duration

configured." The error below is written to the PowerChute error.log:

"User VMs did not shut down in time."

Nutanix Guest VM tools have not been installed. This will cause a hard shutdown of the VM

To install Nutanix Guest Tools (NGT) on VMs in your Cluster, follow the steps detailed in the Enabling and Mounting Nutanix Guest Tools article published by Nutanix.

VM Startup

Unable to power on User VMs

The error below is written to the PowerChute Event Log:

"Attempting to power on VMs on Host [Host] that did not start."

The error below is written to the PowerChute error.log:

"Failed to power on UVMs from startup list: [error received]."

AHV Host Shutdown

Unable to shut down AHV Host

AHV Host shutdown may be unsuccessful if the root password for the AHV host does not match the Controller VM password. This could also happen if your AHV Host credentials have changed after configuring PowerChute. Ensure the correct password is provided in the **Nutanix AHV Host Password** field in the CVM/Cluster Details screen.

The errors below are written to the PowerChute error.log:

"Failed to connect to AHV: [error received]."

"Failed to connect session due authentication failure: [error received]."

Controller VM Shutdown

Unable to shut down Controller VM

This error may occur if the Nutanix Controller VM is down when PowerChute attempts to shut the Controller VM down. For more information, refer to the error message generated in the error.log.

The error below is written to the PowerChute error.log:

"Failed to connect to CVM: [error received]."

Acropolis File Services (AFS)

Unable to stop AFS

If AFS cannot be successfully stopped, the Cluster cannot be stopped and Controller VMs cannot be gracefully shut down. To resolve this issue, increase the AFS stop duration. It is recommended that you manually test the time needed to stop AFS on your Cluster and specify that as the duration in the PowerChute UI.

To do this, connect to any Controller VM while AFS is running, and use the following command:

afs infra.stop <file server name>

Note the duration it takes for the AFS service to fully stop and use this as the **AFS Shutdown Duration** in the Virtualization Settings screen in the PowerChute UI.

The error below is written to the PowerChute Event Log:

"Nutanix AFS cannot be gracefully shut down."

The error below is written to the PowerChute error.log:
"Failed to stop Nutanix AFS: [error received]"

Protection Domain

Unable to abort Protection Domain Replications

The error below is written to the PowerChute Event Log:

"Nutanix Protection Domain replications cannot be gracefully aborted."

Browser Troubleshooting

The PowerChute Web UI is accessed using a browser. For a list of supported browsers please view the Operating System Compatibility chart.

PowerChute requires cookies and JavaScript to be enabled in the browser in order to function correctly. If cookies are being blocked this will prevent logging into the PowerChute UI. To avoid this, allow cookies for the PowerChute URL.

SSH Actions Troubleshooting

Error shown on screen when session times out

- When the user session times out or the PowerChute service restarts, clicking on the edit or delete icons on the SSH List View screen will result in an error message being shown on screen. Click on any of the menu items to return to the log in screen.

SNMP Troubleshooting

The Network Management System (NMS) cannot connect to PowerChute via SNMPv1:

1. Verify that there is a network connection between the NMS and PowerChute.

2. Verify that the SNMP Port specified during installation (161 by default) is not blocked for inbound communications by a firewall.

3. Verify that SNMPv1 is enabled in the PowerChute.

4. Verify that the Community Name specified in PowerChute matches the Community Name used by the NMS. The Community Name is case sensitive.

5. Verify that the NMS IP or Hostname specified in PowerChute matches the IP/Hostname of the NMS.

6. Verify that the Access Type specified in PowerChute is set to Read for SNMP Get requests, or Read/Write for SNMP Set requests.

The Network Management System (NMS) cannot connect to PowerChute via SNMPv3:

1. Verify that there is a network connection between the NMS and PowerChute.

2. Verify that the SNMP Port specified during installation (161 by default) is not blocked for inbound communications by a firewall.

3. Verify that SNMPv3 is enabled in the PowerChute.

4. Verify that the User Name specified in PowerChute matches the User Name used by the NMS. The user name is case sensitive.

5. Verify that the Authentication Protocol. Authentication Passphrase, Privacy Protocol and Privacy Passphrase used by the NMS match those specified in PowerChute.

6. Verify that the Access Type specified in PowerChute is set to Read for SNMP Get requests, or Read/Write for SNMP Set requests.

SNMP Traps sent by PowerChute are not received by the NMS:

1. Verify that there is a network connection between PowerChute and the NMS.

2. Verify that a Trap receiver has been added in PowerChute:

    - Verify that the UDP Port specified (162 by default) is not blocked for outbound communications by a firewall.

    - Verify that the SNMPv1 Community Name, or SNMPv3 User Profile used to send the Trap is configured in the NMS.

    - Verify that the Privacy Protocol selected is compatible with the Java JRE used by PowerChute:

    - Verify that the SNMP Trap Receiver Test was successful.

3. Verify that Traps for UPS Critical events are enabled.

4. Verify that Traps for Lost Communication events are enabled.

General Troubleshooting

The PowerChute service does not start if m11.cfg file is missing

If the m11.cfg file is moved, renamed, or deleted, the PowerChute service cannot start. If the m11.bak file is present, PowerChute will restore the m11.cfg file using this backup file when the PowerChute service is started. However, you will need to start the PowerChute service again after the m11.cfg file is restored.

If both the m11.cfg and m11.bak files are not present, you must uninstall and reinstall PowerChute.

> ⚠️ Administrator access is required on all operating systems to open and edit the m11.cfg file. Ensure that the m11.cfg file is not modified in any way.

Parallel UPS Configuration is not possible with Easy UPS

Several SRV UPS devices with capacities of 10 kVA and above can be configured into a parallel configuration through the use of external hardware, such as an SRV Parallel Board.

Network Management Card(s) deployed within this configuration cannot detect this parallel configuration. PowerChute, which relies on Network Management Card data, is also not capable of recognizing this configuration as a parallel UPS setup.

APC by Schneider Electric Worldwide Customer Support

Customer support for this or any other APC by Schneider Electric product is available at no charge in any of the following ways:

- Visit the APC by Schneider Electric web site, www.apc.com to access documents in the APC Knowledge Base and to submit customer support requests.

  – **www.apc.com** (Corporate Headquarters)
    Connect to localized APC by Schneider Electric web site for specific countries, each of which provides customer support information.

  – **www.apc.com/support/**
    Global support searching APC Knowledge Base and using e-support.

- Contact the APC by Schneider Electric Customer Support Center by telephone or e-mail.

  – Local, country specific centers: go to **www.apc.com/support/contact** for contact information.

  – For information on how to obtain local customer support, contact the APC by Schneider Electric representative or other distributor from whom you purchased your APC by Schneider Electric product.

990-4595L-001   **05/2024**