Charon on Windows Charon instance clean shutdown

Contents

Introduction . . . 3
About this guide . . . 4
Installation . . . 6
Configuration file settings . . . 9
- Using opa0 . . . 10
- Using rsh . . . 19
- Using ssh . . . 27

Running the script . . . 41
Integration with Windows shutdown . . . 42

Introduction

Contents

- Description
- Related products
- Supported Guest Operating System versions
- Supported Windows versions

Description

When a Charon instance is stopped using the Charon tray icon, the Charon service management utility, Windows service management or the Virtual Machines Manager (depending on Charon version installed) or in case the Windows server is shutdown, it is like powering off a physical system without shutting it down first from the Charon emulated server point of view. In such a case, there is no clean shutdown of the legacy operating system (Tru64 or VMS). The services and applications are not stopped properly, and the file systems are not dismounted cleanly.

The Charon Instance Clean Shutdown Utility is designed to perform a clean shutdown of the emulated server before the Windows server power off occurs.

This document explains how to configure the utility and the methods that can be used to execute the remote shutdown. **It relates to script version 2.9**.

Related products

- CHARON-AXP on Windows, versions 4.8 and above
- CHARON-VAX on Windows, versions 4.8 and above

Supported Guest Operating System versions

- All VMS versions
- All Tru64 versions

Supported Windows versions

This version of the utility has been validated on the following operating systems:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 10

PowerShell V5.1 or newer version is required.

About this guide

Obtaining Documentation

The latest released version of this manual and other related documentation are available on the Stromasys support website at Product Documentation and Knowledge Base.

Obtaining Technical Assistance or General Product Information

Obtaining Technical Assistance

Several support channels are available to cover the Charon virtualization products.

If you have a support contract with Stromasys, please visit http://www.stromasys.com/support/ for up-to-date support telephone numbers and business hours. Alternatively, the support center is available via email at support@stromasys.com.

If you purchased a Charon product through a Value-Added Reseller (VAR), please contact them directly.

Obtaining General Product Information

If you require information in addition to what is available on the Stromasys Product Documentation and Knowledge Base and on the Stromasys web site you can contact the Stromasys team using https://www.stromasys.com/contact/, or by sending an email to info@stromasys.com.

For further information on purchases and the product best suited to your requirements, you can also contact your regional sales team by phone:

Region	Phone	Address
Australasia-Pacific	+852 3520 1030	Room 1113, 11/F, Leighton Centre 77 Leighton Road, Causeway Bay, Hong Kong, China
Americas	+1 919 239 8450	2840 Plaza Place, Ste 450 Raleigh, NC 27612 U.S.A.
Europe, Middle-East and Africa	+41 22 794 1070	Avenue Louis-Casai 84 5th Floor 1216 Cointrin Switzerland

Conventions

Notation	Description
$	The dollar sign in interactive examples indicates an operating system prompt for VMS. The dollar sign can also indicate non superuser prompt for UNIX / Linux.
#	The number sign represents the superuser prompt for UNIX / Linux.
>	The right angle bracket in interactive examples indicates an operating system prompt for Windows command (cmd.exe).
`User input`	Bold monospace type in interactive examples indicates typed user input.
<**`path`**>	Bold monospace type enclosed by angle brackets indicates command parameters and parameter values.
`Output`	Monospace type in interactive examples, indicates command response output.
[ ]	In syntax definitions, brackets indicate items that are optional.
...	In syntax definitions, a horizontal ellipsis indicates that the preceding item can be repeated one or more times.
`dsk0`	Italic monospace type, in interactive examples, indicates typed context dependent user input.

Definitions

Term	Description
Host	The system on which the emulator runs, also called the Charon server
Guest	The operating system running on a Charon instance, for example, Tru64 UNIX, OpenVMS, Solaris, MPE or HP-UX

Installation

Kit download

Download the kit from our SFTP server (please ask us connection credentials if you have no access) and extract all files in a dedicated folder, "`C:\Charon`" for example.

The kit contains the following files:

File	Description
`charon_cleanshutdown.ps1`	PowerShell main script
`rsh.exe`	Used if 'rsh' mode is selected
`template.ini`	Used to facilitate the creation of a customized configuration file for the CHARON instance
`psexec.exe`	Downloaded from Microsoft Sysinternals and used in case of integration to Windows shutdown

Shutdown command

Depending on the guest operating system running on the CHARON instance, the following commands are executed to perform a clean shutdown:

Tru64	`/sbin/init 0`
OpenVMS	`@SYS$MANAGER:CHARON_SHUTDOWN.COM`

Requirements

PowerShell V5.1 or newer version is required.

To run PowerShell scripts (files that end with .ps1), you must first set the execution policy to Unrestricted (This operation has to be done once).

To do so, open a command line window (cmd.exe) as an Administrator and use the following command:

```
c:\Charon>powershell -command "Set-ExecutionPolicy Unrestricted"
```

ℹ The ExecutionPolicy can also be set to "`RemoteSigned`". In this case the `.ps1` script files will have to be unblocked as described below.

If you are still prompted to allow for execution of the script, please run the following command to unblock the downloaded `charon_cleanshutdown.ps1` file:

```
c:\Charon>powershell -command "Unblock-File -path c:\charon\charon_cleanshutdown.ps1"
```

💡 See PowerShell version, upgrade, enabling scripts execution, tips and tricks.

Available methods

Four methods are available to perform the remote shutdown. For all methods except 'opa0', the Charon host must be able to communicate via TCP /IP with the guest operating system(s) running on the CHARON instance(s).

Please select the method that is best suited to your configuration:

Mode	Description	Requirements	Notes
opa0	Connection to the OPA0 console via telnet on the specified port using PowerShell internal functions	The '`SYS$MANAGER:CHARON_SHUTDOWN.COM`' script must exist on the emulated VMS system. No requirement if Tru64 is used.	• Does not work if the console is running an application. Works only if the console is at the SRM prompt, prompting for username or password, or at the shell prompt. • Does not work if a connection to the console is already active from another host than the CHARON server. • If the password of the guest operating system changes, either the encrypted password file has to be updated or the password stored in clear text in the configuration file. • Useful if TCP/IP is not available on the guest operating system running on the CHARON instance.
rsh	Executes a remote command on the guest operating system (TCP /IP is required). On Tru64 the .rhosts file must be configured and on OpenVMS the rexec/rsh services must have been enabled and a proxy must have been created.	The '`rsh.exe`' file is included in the kit. Copy it to a folder of your choice ("`C:\Bin`" or "`C:\Charon`" for example). The Charon Windows server and the emulated operating system must be able to communicate via TCPIP. The '`SYS$MANAGER:CHARON_SHUTDOWN.COM`' script must exist on the emulated VMS system. No requirement if Tru64 is used.	• Not subject to password change.
ssh	Executes a remote command on the guest operating system over a secure connection (TCP/IP is required).	Download and install OpenSSH from the https://github.com/PowerShell/Win32-OpenSSH/releases web site or preferably the version attached to this document. As a user with Administrator privileges, extract the package to `C:\Program Files\OpenSSH`. The Charon Windows server and the emulated operating system must be able to communicate via TCPIP. The '`SYS$MANAGER:CHARON_SHUTDOWN.COM`' script must exist on the emulated VMS system. No requirement if Tru64 is used.	• Not subject to password change. • Secure connection.

OpenVMS shutdown script

Copy/paste this script on your OpenVMS system, it will be used to issue the shutdown command for "rsh", "ssh" and "opa0" modes:

$ EDIT SYS$MANAGER:CHARON_SHUTDOWN.COM

```
$ IF F$MODE() .eqs. "OTHER"
$ THEN
$   DEFINE SYS$OUTPUT OPA0:
$   @SYS$SYSTEM:SHUTDOWN 0 SHUTDOWN NO YES LATER NO NONE
$
$ ELSE
$   IF "''P1'".EQS."CHECK"
$   THEN
$     WRITE SYS$OUTPUT "''P2' was successful"
$   ELSE
$     SET VERIFY
$     PURGE /KEEP=20 SYS$MANAGER:CHARON_SHUTDOWN.LOG
$     RUN /DETACH SYS$SYSTEM:LOGINOUT.EXE /INPUT=SYS$MANAGER:CHARON_SHUTDOWN -
          /OUTPUT=SYS$MANAGER:CHARON_SHUTDOWN.LOG /UIC=[1,4]
$   ENDIF
$ ENDIF
$ EXIT
```

Configuration file settings

Definition

One configuration file is required per Charon instance, it is used to store the necessary parameters to execute the remote shutdown command.

? This file is not the configuration file used by Charon to define the virtual machine settings, this is why it is recommended to name it `.ini` and not `.cfg`

This file typically has the extension .ini. The file name can be set at your convenience. As good practice, we recommend to include the CHARON instance service name in the configuration file name.

ℹ The file can handle blank lines and comments (lines starting with '#').

⚠ Do not use simple or double quotes within values.

⚠ Parameters and values are case sensitive.

💡 The template.ini file is provided as an example. Copy it, uncomment all necessary lines depending on the selected mode, and fill in the required values.

Configuration details are explained below.

Contents

- Using opa0
- Using rsh
- Using ssh

Using opa0

Contents

- Parameters
  - logfile
  - windowsevent
  - mode
  - os
  - servicename
  - username
  - password
  - cryptedpass
  - cryptedpsys
  - port
  - prompt
  - timelimitsec
  - windowwidth and windowheight
- Examples
  - Configuration file
  - Script execution
    - Check mode
    - Shutdown execution - Tru64 example
    - Shutdown execution - VMS example

Parameters

logfile

Optional full path to the logfile that will be used to log the script output. If not specified a file name and path will be chosen based on session log file (one file per script execution). The file name is usually based on the configuration_name followed by "-SHUTDOWN-" and date/time.

Example:

```
logfile=C:\Charon\myds20_shutdown.log
```

windowsevent

Defines which message levels will create a new entry in the Windows Application Events (Source="CHARON")

Can be either "none" or any combination of S, W and E. 'S' for Success, 'W' for Warning and 'E' for Error. Default is 'SE' so Success and Error only.

Example:

```
windowsevent=SWE
```

mode

`opa0`

Example:

```
mode=opa0
```

os

Either Tru64 or VMS

Example:
`os=Tru64`

servicename

CHARON instance service name.

⚠ When using "opa0" mode, the service is stopped by a "`power off`" or the "`F6`" key. If this operation does not succeed (cannot connect to console or "F6" key not enabled for example), it is then stopped using a Windows service command.

Example:
`servicename=myds20`

username

Defines the remote username that will be used to connect to the console of the CHARON instance (if not already logged in)

Example / OpenVMS:
`username=system`

Example / Tru64:
`username=root`

password

Defines the password in clear text that will be used to connect to the console.

The password can be also stored in an encrypted file as described below.

⚠ If password is used then `cryptedpass` (below) value must be set to "`none`" or left empty.

Example:
`password=12345`

cryptedpass

Full path to the text file containing the encrypted password. To create this file, open a command window "`cmd.exe`" and enter the following command ("More ?" is the continuation line prompt)

```
C:\Users\Spock> powershell -command "ConvertTo-SecureString -String '<password>' -AsPlainText -Force ^
More ? | ConvertFrom-SecureString | Out-File '<full path to the file>'"
```

⚠ Please note the password encryption is based on current user credentials

ℹ The parameter can be set to "`none`" or simply commented if not used.

Example:
`cryptedpass=C:\Charon\myds20pwd.txt`

cryptedpsys

Full path to the text file containing the encrypted password that will be used as "system" user (during Windows server shutdown). To create this file, open a command window "`cmd.exe`", run "`psexec -i -s cmd.exe`" (psexec is provided in the kit) and run "`powershell`" from the newly opened window. At the PowerShell prompt, enter the following command:

```
C:\Users\Spock> powershell -command "ConvertTo-SecureString -String '<password>' -AsPlainText -Force ^
More ? | ConvertFrom-SecureString | Out-File '<full path to the file>'"
```

Use a different name for the output file as the one user for "`cryptedpass`"

The parameter can be set to "`none`" or simply commented if not used.

Example:
`cryptedpsys=C:\Charon\myds20pwd_sys.txt`

port

Defines the port to access the console (same as the one defined in the configuration file).

Example:
`port=10003`

prompt

Defines the prompt at the shell level of the guest operating system. Used to check the user is connected.

Notes:

- If the prompt contain spaces, it is necessary to add them in the configuration file
- The prompt must not contain any escape character.

Example:
`prompt=myds20>`

timelimitsec

Defines the maximum number of seconds the script can run (default = 180 seconds). This value depends on the time needed to shutdown properly the operating system.

Example:
`timelimitsec=600`

windowwidth and windowheight

Optional parameters used to resize the window when running with service user ("system" account).

Useful during Windows shutdown to check operations executed.

Width = 132 and Height = 32 by default. BufferHeight set 2000 lines by default.

Example:

```
windowwidth=120
windowheight=50
```

Examples

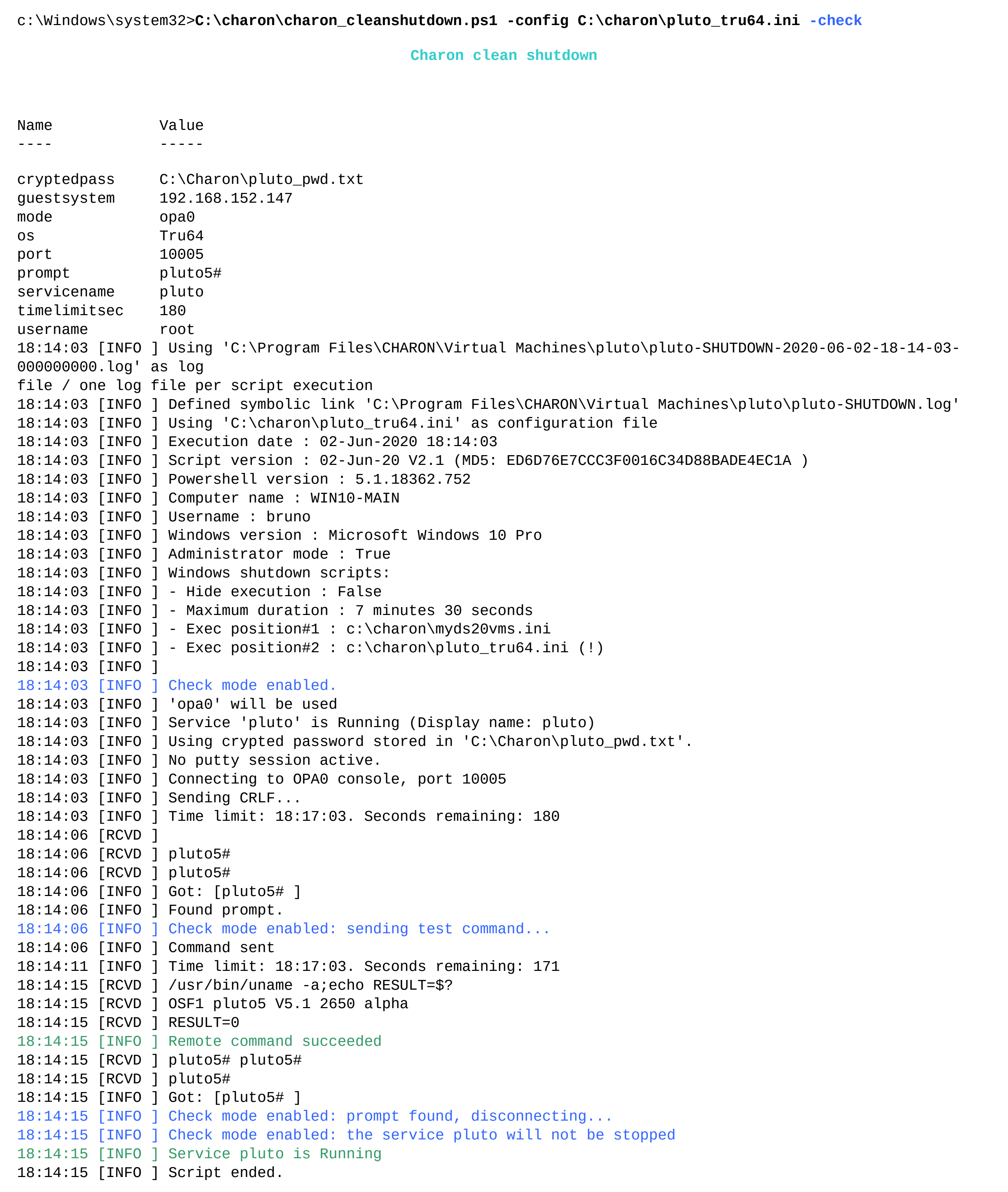
Configuration file

```
#----------------------------------------
# myds20 Tru64 V5.1 machine
#----------------------------------------
windowwidth=132
windowheight=50
servicename=pluto
os=Tru64
username=root
mode=opa0
cryptedpass=C:\Charon\pluto_pwd.txt
port=10005
prompt=pluto5#
timelimitsec=180
```

Script execution

Check mode

When check mode is enabled, a pop-up window will be displayed to check the operations performed on the CHARON instance console.



```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\pluto_tru64.ini -check

                                             Charon clean shutdown



Name            Value
----            -----

cryptedpass     C:\Charon\pluto_pwd.txt
guestsystem     192.168.152.147
mode            opa0
os              Tru64
port            10005
prompt          pluto5#
servicename     pluto
timelimitsec    180
username        root
18:14:03 [INFO ] Using 'C:\Program Files\CHARON\Virtual Machines\pluto\pluto-SHUTDOWN-2020-06-02-18-14-03-
000000000.log' as log
file / one log file per script execution
18:14:03 [INFO ] Defined symbolic link 'C:\Program Files\CHARON\Virtual Machines\pluto\pluto-SHUTDOWN.log'
18:14:03 [INFO ] Using 'C:\charon\pluto_tru64.ini' as configuration file
18:14:03 [INFO ] Execution date : 02-Jun-2020 18:14:03
18:14:03 [INFO ] Script version : 02-Jun-20 V2.1 (MD5: ED6D76E7CCC3F0016C34D88BADE4EC1A )
18:14:03 [INFO ] Powershell version : 5.1.18362.752
18:14:03 [INFO ] Computer name : WIN10-MAIN
18:14:03 [INFO ] Username : bruno
18:14:03 [INFO ] Windows version : Microsoft Windows 10 Pro
18:14:03 [INFO ] Administrator mode : True
18:14:03 [INFO ] Windows shutdown scripts:
18:14:03 [INFO ] - Hide execution : False
18:14:03 [INFO ] - Maximum duration : 7 minutes 30 seconds
18:14:03 [INFO ] - Exec position#1 : c:\charon\myds20vms.ini
18:14:03 [INFO ] - Exec position#2 : c:\charon\pluto_tru64.ini (!)
18:14:03 [INFO ]
18:14:03 [INFO ] Check mode enabled.
18:14:03 [INFO ] 'opa0' will be used
18:14:03 [INFO ] Service 'pluto' is Running (Display name: pluto)
18:14:03 [INFO ] Using crypted password stored in 'C:\Charon\pluto_pwd.txt'.
18:14:03 [INFO ] No putty session active.
18:14:03 [INFO ] Connecting to OPA0 console, port 10005
18:14:03 [INFO ] Sending CRLF...
18:14:03 [INFO ] Time limit: 18:17:03. Seconds remaining: 180
18:14:06 [RCVD ]
18:14:06 [RCVD ] pluto5#
18:14:06 [RCVD ] pluto5#
18:14:06 [INFO ] Got: [pluto5# ]
18:14:06 [INFO ] Found prompt.
18:14:06 [INFO ] Check mode enabled: sending test command...
18:14:06 [INFO ] Command sent
18:14:11 [INFO ] Time limit: 18:17:03. Seconds remaining: 171
18:14:15 [RCVD ] /usr/bin/uname -a;echo RESULT=$?
18:14:15 [RCVD ] OSF1 pluto5 V5.1 2650 alpha
18:14:15 [RCVD ] RESULT=0
18:14:15 [INFO ] Remote command succeeded
18:14:15 [RCVD ] pluto5# pluto5#
18:14:15 [RCVD ] pluto5#
18:14:15 [INFO ] Got: [pluto5# ]
18:14:15 [INFO ] Check mode enabled: prompt found, disconnecting...
18:14:15 [INFO ] Check mode enabled: the service pluto will not be stopped
18:14:15 [INFO ] Service pluto is Running
18:14:15 [INFO ] Script ended.
```

RCVD messages correspond to the received data from the OPA0 console.

Shutdown execution - Tru64 example

```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\pluto_tru64.ini
                                            Charon clean shutdown



Name            Value
----            -----



cryptedpass     C:\Charon\pluto_pwd.txt
guestsystem     192.168.152.147
mode            opa0
os              Tru64
port            10005
prompt          pluto5#
servicename     pluto
timelimitsec    180
username        root



18:19:17 [INFO ] Using 'C:\Program Files\CHARON\Virtual Machines\pluto\pluto-SHUTDOWN-2020-06-02-18-19-17-
000000000.log' as logfile / one log file per script execution
18:19:17 [INFO ] Defined symbolic link 'C:\Program Files\CHARON\Virtual Machines\pluto\pluto-SHUTDOWN.log'
18:19:17 [INFO ] Using 'C:\charon\pluto_tru64.ini' as configuration file
18:19:17 [INFO ] Execution date : 02-Jun-2020 18:19:17
18:19:17 [INFO ] Script version : 02-Jun-20 V2.1 (MD5: ED6D76E7CCC3F0016C34D88BADE4EC1A )
18:19:17 [INFO ] Powershell version : 5.1.18362.752
18:19:17 [INFO ] Computer name : WIN10-MAIN
18:19:17 [INFO ] Username : bruno
18:19:17 [INFO ] Windows version : Microsoft Windows 10 Pro
18:19:17 [INFO ] Administrator mode : True
18:19:17 [INFO ] Windows shutdown scripts:
18:19:17 [INFO ] - Hide execution : False
18:19:17 [INFO ] - Maximum duration : 7 minutes 30 seconds
18:19:17 [INFO ] - Exec position#1 : c:\charon\myds20vms.ini
18:19:17 [INFO ] - Exec position#2 : c:\charon\pluto_tru64.ini (!)
18:19:17 [INFO ]
18:19:17 [INFO ] 'opa0' will be used
18:19:17 [INFO ] Service 'pluto' is Running (Display name: pluto)
18:19:17 [INFO ] Using crypted password stored in 'C:\Charon\pluto_pwd.txt'.
18:19:17 [INFO ] No putty session active.
18:19:17 [INFO ] Connecting to OPA0 console, port 10005
18:19:17 [INFO ] Sending CRLF...
18:19:17 [INFO ] Time limit: 18:22:17. Seconds remaining: 180
18:19:21 [RCVD ]
18:19:21 [RCVD ] pluto5#
18:19:21 [RCVD ] pluto5#
18:19:21 [INFO ] Got: [pluto5# ]
18:19:21 [INFO ] Found prompt.
18:19:21 [INFO ] Send Tru64 shutdown...
18:19:21 [INFO ] Command sent
18:19:26 [INFO ] Time limit: 18:22:17. Seconds remaining: 171
18:19:29 [RCVD ] /sbin/init 0;echo RESULT=$?
18:19:29 [RCVD ] RESULT=0
18:19:29 [INFO ] Remote command succeeded
18:19:29 [RCVD ] pluto5# pluto5#
18:19:29 [RCVD ] pluto5#
18:19:29 [INFO ] Got: [pluto5# ]
18:19:29 [INFO ] Found prompt, waiting for shutdown to start or complete...
18:19:34 [INFO ] Time limit: 18:22:17. Seconds remaining: 163
18:19:38 [RCVD ]
18:19:38 [RCVD ] INIT: New run level: 0
18:19:38 [RCVD ] The system is coming down. Please wait...
18:19:38 [RCVD ] Logins disabled
18:19:38 [RCVD ] Stopping Zabbix agent...
18:19:38 [RCVD ]
18:19:38 [INFO ] Got: [Stopping Zabbix agent...]
```

```
18:19:38 [INFO ] Case unknown: [Stopping Zabbix agent...]. Retrying...
18:19:40 [INFO ] Time limit: 18:22:17. Seconds remaining: 157
18:19:43 [RCVD ] Zabbix agent stopped.
18:19:43 [RCVD ]
18:19:43 [INFO ] Got: [Zabbix agent stopped.]
18:19:43 [INFO ] Case unknown: [Zabbix agent stopped.]. Retrying...
18:19:45 [INFO ] Time limit: 18:22:17. Seconds remaining: 152
18:19:49 [RCVD ] LAT stopped.
18:19:49 [RCVD ] Unmounting NFS filesystems
18:19:49 [RCVD ] The interface tu0, does not exist.
18:19:49 [RCVD ]
18:19:49 [RCVD ] Halting processes ...
18:19:49 [RCVD ]
18:19:49 [INFO ] Got: [Halting processes ...]
18:19:49 [INFO ] Halting processes ...
18:19:49 [INFO ] Time limit: 18:22:17. Seconds remaining: 148
18:19:52 [INFO ] Timeout #1...
18:19:54 [INFO ] Time limit: 18:22:17. Seconds remaining: 143
18:19:58 [RCVD ] The system is down.
18:19:58 [RCVD ]
18:19:58 [INFO ] Got: [The system is down.]
18:19:58 [INFO ] The system is down.
18:19:58 [INFO ] Time limit: 18:22:17. Seconds remaining: 139
18:20:01 [INFO ] Timeout #1...
18:20:03 [INFO ] Time limit: 18:22:17. Seconds remaining: 134
18:20:07 [RCVD ] /proc: Invalid argument
18:20:07 [RCVD ] ....Halt completed....
18:20:07 [RCVD ] syncing disks... done
18:20:07 [RCVD ] CPU 0: Halting... (transferring to monitor)
18:20:07 [RCVD ]
18:20:07 [RCVD ] halted CPU 1
18:20:07 [RCVD ]
18:20:07 [RCVD ]
18:20:07 [RCVD ] halted CPU 0
18:20:07 [RCVD ]
18:20:07 [RCVD ] halt code = 5
18:20:07 [RCVD ] HALT instruction executed
18:20:07 [RCVD ] PC = fffffc00006bde70
18:20:07 [RCVD ] P00>>>
18:20:07 [INFO ] Got: [P00>>>]
18:20:07 [INFO ] Sending 'power off'...
18:20:08 [INFO ] Service pluto is stopped
18:20:08 [INFO ] Script ended.
```

RCVD messages correspond to the received data from the OPA0 console.

Shutdown execution - VMS example

```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\myds20vms.ini

                                         Charon clean shutdown

Name            Value
----            -----



cryptedpass     C:\Charon\myds20vms_cryptpass.txt
mode            opa0
os              VMS
port            10007
prompt          VMS084>
servicename     ds20vms
timelimitsec    180
username        system
waitbeforestop  10
windowheight    50
windowwidth     132



18:24:38 [INFO ] Using 'C:\Program Files\CHARON\Virtual Machines\ds20vms\ds20vms-SHUTDOWN-2020-06-02-18-24-
```

```
38-000000000.log' as
log file / one log file per script execution
18:24:38 [INFO ] Defined symbolic link 'C:\Program Files\CHARON\Virtual Machines\ds20vms\ds20vms-SHUTDOWN.
log'
18:24:38 [INFO ] Using 'C:\charon\myds20vms.ini' as configuration file
18:24:38 [INFO ] Execution date : 02-Jun-2020 18:24:38
18:24:38 [INFO ] Script version : 02-Jun-20 V2.1 (MD5: ED6D76E7CCC3F0016C34D88BADE4EC1A )
18:24:38 [INFO ] Powershell version : 5.1.18362.752
18:24:38 [INFO ] Computer name : WIN10-MAIN
18:24:38 [INFO ] Username : bruno
18:24:38 [INFO ] Windows version : Microsoft Windows 10 Pro
18:24:38 [INFO ] Administrator mode : True
18:24:38 [INFO ] Windows shutdown scripts:
18:24:38 [INFO ] - Hide execution : False
18:24:38 [INFO ] - Maximum duration : 7 minutes 30 seconds
18:24:38 [INFO ] - Exec position#1 : c:\charon\myds20vms.ini (!)
18:24:38 [INFO ] - Exec position#2 : c:\charon\pluto_tru64.ini
18:24:38 [INFO ]
18:24:38 [INFO ] 'opa0' will be used
18:24:38 [INFO ] Service 'ds20vms' is Running (Display name: ds20vms)
18:24:38 [INFO ] Using crypted password stored in 'C:\Charon\myds20vms_cryptpass.txt'.
18:24:38 [INFO ] No putty session active.
18:24:38 [INFO ] Connecting to OPA0 console, port 10007
18:24:38 [INFO ] Sending CRLF...
18:24:38 [INFO ] Time limit: 18:27:38. Seconds remaining: 180
18:24:42 [RCVD ]
18:24:42 [RCVD ]
18:24:42 [RCVD ] Welcome to OpenVMS (TM) Alpha Operating System, Version V8.4
18:24:42 [RCVD ]
18:24:42 [RCVD ] Username:
18:24:42 [INFO ] Got: [Username: ]
18:24:42 [INFO ] Sending VMS username...
18:24:42 [INFO ] Username sent
18:24:42 [INFO ] Time limit: 18:27:38. Seconds remaining: 176
18:24:45 [RCVD ] system
18:24:45 [RCVD ] Password:
18:24:45 [INFO ] Got: [Password: ]
18:24:45 [INFO ] Sending password, try #1 of 3
18:24:45 [INFO ] Password sent
18:24:47 [INFO ] Time limit: 18:27:38. Seconds remaining: 171
18:24:51 [RCVD ]
18:24:51 [RCVD ] Welcome to OpenVMS (TM) Alpha Operating System, Version V8.4
18:24:51 [RCVD ] Last interactive login on Tuesday, 2-JUN-2020 17:23:59.38
18:24:51 [RCVD ] Last non-interactive login on Friday, 15-MAY-2020 11:34:51.97[c\Z
18:24:51 [INFO ] Got: [ Last non-interactive login on Friday, 15-MAY-2020 11:34:51.97[c\Z]
18:24:51 [INFO ] Case unknown: [ Last non-interactive login on Friday, 15-MAY-2020 11:34:51.97[c\Z].
Retrying...
18:24:53 [INFO ] Time limit: 18:27:38. Seconds remaining: 165
18:24:56 [RCVD ] [0c
18:24:56 [INFO ] Got: [[0c]
18:24:56 [INFO ] Case unknown: [[0c]. Retrying...
18:24:58 [INFO ] Time limit: 18:27:38. Seconds remaining: 160
18:25:02 [RCVD ]
18:25:02 [RCVD ] %SET-W-NOTSET, error modifying OPA0:
18:25:02 [RCVD ] -SET-I-UNKTERM, unknown terminal type[c\Z
18:25:02 [INFO ] Got: [-SET-I-UNKTERM, unknown terminal type[c\Z]
18:25:02 [INFO ] Case unknown: [-SET-I-UNKTERM, unknown terminal type[c\Z]. Retrying...
18:25:04 [INFO ] Time limit: 18:27:38. Seconds remaining: 154
18:25:07 [RCVD ] [0c
18:25:07 [INFO ] Got: [[0c]
18:25:07 [INFO ] Case unknown: [[0c]. Retrying...
18:25:09 [INFO ] Time limit: 18:27:38. Seconds remaining: 149
18:25:13 [RCVD ]
18:25:13 [RCVD ] %SET-W-NOTSET, error modifying OPA0:
18:25:13 [RCVD ] -SET-I-UNKTERM, unknown terminal type
18:25:13 [RCVD ] VMS084>
18:25:13 [INFO ] Got: [ VMS084> ]
18:25:13 [INFO ] Found prompt.
18:25:13 [INFO ] Sending VMS shutdown...
18:25:13 [INFO ] Command sent
18:25:18 [INFO ] Time limit: 18:27:38. Seconds remaining: 140
```

```
18:25:21 [RCVD ] @SYS$MANAGER:CHARON_SHUTDOWN.COM
18:25:21 [RCVD ] $ PURGE /KEEP=20 SYS$MANAGER:CHARON_SHUTDOWN.LOG
18:25:21 [RCVD ] $ RUN /DETACH SYS$SYSTEM:LOGINOUT.EXE /INPUT=SYS$MANAGER:CHARON_SHUTDOWN -
18:25:21 [RCVD ] /OUTPUT=SYS$MANAGER:CHARON_SHUTDOWN.LOG /UIC=[1,4]
18:25:21 [RCVD ] %RUN-S-PROC_ID, identification of created process is 00000125
18:25:21 [RCVD ] $ ENDIF
18:25:21 [RCVD ] $ ENDIF
18:25:21 [RCVD ] $ EXIT
18:25:21 [RCVD ] VMS084>
18:25:21 [RCVD ]
18:25:21 [RCVD ]
18:25:21 [RCVD ] SHUTDOWN -- Perform an Orderly System Shutdown
18:25:21 [RCVD ] on node VMS084
18:25:21 [RCVD ]
18:25:21 [RCVD ]
18:25:21 [RCVD ] %SHUTDOWN-I-OPERATOR, this terminal is now an operator's console
18:25:21 [RCVD ] %SHUTDOWN-I-DISLOGINS, interactive logins will now be disabled
18:25:21 [RCVD ] %SET-I-INTSET, login interactive limit = 0, current interactive value = 1
18:25:21 [RCVD ] %SHUTDOWN-I-STOPQUEUES, the queues on this node will now be stopped
18:25:21 [RCVD ]
18:25:21 [RCVD ] SHUTDOWN message on VMS084 from user SYSTEM at VMS084 Batch 17:25:30
18:25:21 [RCVD ] VMS084 will shut down in 0 minutes; back up LATER. Please log off node VMS084.
18:25:21 [RCVD ] SHUTDOWN
18:25:21 [RCVD ]

... (truncated)
18:25:22 [RCVD ] %%%%%%%%%%% OPCOM 2-JUN-2020 17:25:33.68 %%%%%%%%%%%
18:25:22 [RCVD ] Message from user SYSTEM on VMS084
18:25:22 [RCVD ] %SECSRV-I-SERVERSHUTDOWN, security server shutting down
18:25:22 [RCVD ]
18:25:22 [RCVD ] VMS084>
18:25:22 [INFO ] Got: [ VMS084> ]
18:25:22 [INFO ] Found prompt, waiting for shutdown to start or complete...
18:25:27 [INFO ] Time limit: 18:27:38. Seconds remaining: 131
18:25:30 [RCVD ]
18:25:30 [RCVD ] SYSTEM SHUTDOWN COMPLETE
18:25:30 [RCVD ]
18:25:30 [RCVD ]
18:25:30 [RCVD ]
18:25:30 [RCVD ] halted CPU 0
18:25:30 [RCVD ]
18:25:30 [RCVD ] halt code = 5
18:25:30 [RCVD ] HALT instruction executed
18:25:30 [RCVD ] PC = ffffffff8008fa84
18:25:30 [RCVD ] P00>>>
18:25:30 [INFO ] Got: [P00>>>]
18:25:30 [INFO ] Sending 'power off'...
18:25:31 [INFO ] Service ds20vms is stopped
18:25:31 [INFO ] Script ended.
```

RCVD messages correspond to the received data from the OPA0 console.

Using rsh

Contents

- Parameters
  - logfile
  - windowsevent
  - waitbeforestop
  - servicename
  - guestsystem
  - os
  - mode
  - rshbin
  - username
  - openconsolecmd
  - openconsolearg
  - windowwidth and windowheight
- Enabling remote connection on Tru64
- Enabling remote connection on OpenVMS
- Examples
  - Configuration file
  - Script execution
    - Check mode
    - Shutdown execution

Parameters

logfile

Full path to the log file that will be used to log the script output.

Example:
```
logfile=C:\Charon\myds20vms_shutdown.log
```

windowsevent

Defines which message levels will create a new entry in the Windows Application Events (Source="CHARON")

Can be either "none" or any combination of S, W and E. 'S' for Success, 'W' for Warning and 'E' for Error. Default is 'SE' so Success and Error only.

Example:
```
windowsevent=SWE
```

waitbeforestop

Number of seconds to wait before stopping the service once the guest operating system no longer responds to 'ping'. If not set, default value = 60.

Example:
```
waitbeforestop=10
```

servicename

CHARON instance service name

Example:
```
servicename=myds20vms
```

guestsystem

Server name or IP address

Example:
```
guestsystem=10.0.0.3
```

os

`VMS or Tru64`

Example:
```
os=VMS
```

mode

`rsh`

Example:
```
mode=rsh
```

rshbin

Defines the location of the "rsh.exe" program.

Example:
```
rshbin=C:\charon\rsh.exe
```

username

Defines the remote username that will be used to connect to the guest operating system via rsh.

Example:
```
username=system
```

openconsolecmd

Optional parameter used to open the console program while executing the script. This parameter must contain the full path to the software used to connect to the console. In case putty is going to be used, it is possible to set it to 'putty' without any path. Doing so, the script will look for the latest version available in the Charon installation folder.

? It is recommended to define this parameter in case of integration with Windows shutdown

Example 1:
```
openconsolecmd=C:\Program Files\CHARON\Build_20203\x64\putty
```

Example 2:
```
openconsolecmd=putty
```

openconsolearg

Optional parameter defining the parameters of the `openconsolecmd` parameter above.

Example:
`openconsolearg=-load OPA0 -P 10003`

windowwidth and windowheight

Optional parameters used to resize the window when running with service user ("system" account).

Useful during Windows shutdown to check operations executed.

Width = 132 and Height = 32 by default. BufferHeight set 2000 lines by default.

Example:
```
windowwidth=120
windowheight=50
```

Enabling remote connection on Tru64

To allow connections from the Windows server to the Tru64 guest system without having to specify a password, the Tru64 local account's `.rhosts` file has to be updated with the name or IP address of the Windows system and the account used.

The `.rhosts` file contains a list of remote users who are not required to supply a login password when they use the local user account and execute the rcp, rlogin, and rsh commands (see "`# man rhosts`" for more).

In the example below, a proxy will be created between the Windows '`administrator`' account (the IP address of the Windows system is 10.0.0.1) and the Tru64 '`root`' account (the IP address of the Tru64 system is 10.0.0.2).

```
# vi $HOME/.rhosts

10.0.0.1 Administrator
```

Enabling remote connection on OpenVMS

Enable the REXEC and RSH service on OpenVMS by executing the `TCPIP$CONFIG` script (depending on the OpenVMS version, the script could also be called `UCX$CONFIG`):

```
VMS084> @sys$manager:tcpip$config

        Checking TCP/IP Services for OpenVMS configuration database files.

        HP TCP/IP Services for OpenVMS Configuration Menu

        Configuration options:

                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure

Enter configuration option: 2

        HP TCP/IP Services for OpenVMS Client Components Configuration Menu
        Configuration options:

                 1  -  DHCP Client      Disabled Stopped
                 2  -  FTP Client       Disabled Stopped
                 3  -  NFS Client       Disabled Stopped
                 4  -  REXEC and RSH    Disabled Stopped
                 5  -  RLOGIN           Disabled Stopped
                 6  -  SMTP             Disabled Stopped
                 7  -  SSH Client       Disabled Stopped
                 8  -  TELNET           Enabled  Started
                 9  -  TELNETSYM        Disabled Stopped
                 A  -  Configure options 1 - 9
                [E] -  Exit menu

Enter configuration option: 4

RSH Configuration

Service is defined in the SYSUAF.
Service is defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.

        RSH configuration options:

                 1 - Enable service on this node
                 2 - Enable & Start service on this node
                [E] - Exit RSH configuration

Enter configuration option: 2

%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$RSH.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$RCP.EXE installed
%TCPIP-I-INFO, logical names created
%%%%%%%%%%%  OPCOM   8-JUL-2016 01:28:23.22  %%%%%%%%%%%
Message from user INTERnet on VMS084
INTERnet ACP Activate RSH Server

%TCPIP-I-INFO, service enabled
%TCPIP-S-STARTDONE, TCPIP$RSH startup completed
Press <ENTER> key to continue ...

REXEC Configuration
Service is not defined in the SYSUAF.
Service is not defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.

        REXEC configuration options:

                 1 - Enable service on this node
                 2 - Enable & Start service on this node
                [E] - Exit REXEC configuration

Enter configuration option: 2

…

        HP TCP/IP Services for OpenVMS Client Components Configuration Menu

        Configuration options:

                 1  -  DHCP Client      Disabled Stopped
                 2  -  FTP Client       Disabled Stopped
                 3  -  NFS Client       Disabled Stopped
                 4  -  REXEC and RSH    Enabled  Started
                 5  -  RLOGIN           Disabled Stopped
                 6  -  SMTP             Disabled Stopped
                 7  -  SSH Client       Disabled Stopped
                 8  -  TELNET           Enabled  Started
                 9  -  TELNETSYM        Disabled Stopped
                 A  -  Configure options 1 - 9
                [E] -  Exit menu

Enter configuration option: E
```

Check that the service is enabled:

```
VMS084> tcpip show service

Service             Port  Proto    Process          Address            State
RSH                  514  TCP      TCPIP$RSH        0.0.0.0             Enabled
SSH                   22  TCP      TCPIP$SSH        0.0.0.0             Enabled
TELNET                23  TCP      not defined      0.0.0.0             Enabled
```

To allow connection from the Windows server to the OpenVMS guest system without specifying a password, a proxy must be created between the Windows user that will execute the '`rsh`' command and the OpenVMS user account:

In the example below, a proxy will be created between the Windows '`administrator`' account (the IP address of the Windows system is 10.0.0.1) and the OpenVMS '`system`' account (the IP address of the OpenVMS system is 10.0.0.3)

```
VMS084> tcpip
TCPIP> add proxy system /remote=administrator /host=10.0.0.1
TCPIP> show proxy
VMS User_name      Type      User_ID    Group_ID    Host_name
SYSTEM             CD     ADMINISTRATOR             10.0.0.1
```

Examples

Configuration file

```
#-----------------------------------------
# myds20 OpenVMS 8.4 machine
#-----------------------------------------
windowwidth=132
windowheight=50
logfile=C:\Charon\myds20vms_shutdown.log
servicename=ds20vms
os=VMS
username=system
waitbeforestop=10
mode=rsh
guestsystem=10.0.0.3
rshbin=C:\charon\rsh.exe
```

Script execution

Check mode

```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\myds20vms.ini -check

                                      Charon clean shutdown

Name                  Value
----                  -----
windowheight          50
openconsolecmd        C:\Program Files\CHARON\Build_20203\x64\putty
servicename           ds20vms
username              system
waitbeforestop        10
guestsystem           10.0.0.3
os                    VMS
openconsolearg        -load OPA0 -P 10003
mode                  rsh
windowwidth           132
rshbin                C:\charon\rsh.exe
logfile               C:\Charon\myds20vms_shutdown.log

17:26:44 [INFO ] Using 'C:\Charon\myds20vms_shutdown.log' as log file / append
17:26:44 [INFO ] Execution date : 27-avr.-2020 17:26:44
17:26:44 [INFO ] Script version : 27-Apr-20 V2.0 (MD5: 4BA97792A105C9E0E484850B88B866F8 )
17:26:44 [INFO ] Powershell version : 5.1.14409.1018
17:26:44 [INFO ] Computer name : WIN2008BM
17:26:44 [INFO ] Username : Administrateur
17:26:44 [INFO ] Windows version : Microsoft Windows Server 2008 R2 Standard
17:26:44 [INFO ] Administrator mode : True
17:26:44 [INFO ]
17:26:44 [INFO ] Check mode enabled.
17:26:44 [INFO ] 'rsh' will be used
17:26:44 [INFO ] Service 'ds20vms' is Running (Display name: ds20vms)
17:26:44 [INFO ] Testing guest system '10.0.0.3' response
17:26:47 [INFO ] Opening console.
17:26:47 [INFO ] Invoking 'rsh' command and executing check command...
17:26:47 [INFO ] C:\charon\rsh.exe -l system 10.0.0.3 '@SYS$MANAGER:CHARON_SHUTDOWN.COM CHECK RSH'
17:26:47 [INFO ] Output results:
17:26:47 [INFO ] RSH was successful
17:26:47 [INFO ]
17:26:47 [INFO ]
17:26:47 [INFO ] Command successfully completed.
17:26:47 [INFO ] Check mode enabled: no connection test to be performed.
17:26:47 [INFO ] Check mode enabled: no wait / stop service.
17:26:47 [INFO ] Check mode enabled: the service ds20vms will not be stopped
17:26:47 [INFO ] Service ds20vms is Running
17:26:47 [INFO ] Script ended.
```

Shutdown execution

```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\myds20vms.ini -check


                                    Charon clean shutdown



Name                 Value
----                 -----
windowheight         50
openconsolecmd       C:\Program Files\CHARON\Build_20203\x64\putty
servicename          ds20vms
username             system
waitbeforestop       10
guestsystem          10.0.0.3
os                   VMS
openconsolearg       -load OPA0 -P 10003
mode                 rsh
windowwidth          132
rshbin               C:\charon\rsh.exe
logfile              C:\Charon\myds20vms_shutdown.log

17:29:13 [INFO ] Using 'C:\Charon\myds20vms_shutdown.log' as log file / append
17:29:13 [INFO ] Execution date : 27-avr.-2020 17:29:13
17:29:13 [INFO ] Script version : 27-Apr-20 V2.0 (MD5: 4BA97792A105C9E0E484850B88B866F8 )
17:29:13 [INFO ] Powershell version : 5.1.14409.1018
17:29:13 [INFO ] Computer name : WIN2008BM
17:29:13 [INFO ] Username : Administrateur
17:29:14 [INFO ] Windows version : Microsoft Windows Server 2008 R2 Standard
17:29:14 [INFO ] Administrator mode : True
17:29:14 [INFO ]
17:29:14 [INFO ] 'rsh' will be used
17:29:14 [INFO ] Service 'ds20vms' is Running (Display name: ds20vms)
17:29:14 [INFO ] Testing guest system '10.0.0.3' response
17:29:17 [INFO ] Opening console.
17:29:17 [INFO ] Invoking 'rsh' command and executing shutdown...
17:29:17 [INFO ] C:\charon\rsh.exe -l system 10.0.0.3 '@SYS$MANAGER:CHARON_SHUTDOWN.COM'
17:29:17 [INFO ] Output results:
17:29:17 [INFO ] $ PURGE /KEEP=20 SYS$MANAGER:CHARON_SHUTDOWN.LOG
17:29:17 [INFO ] $ RUN /DETACH SYS$SYSTEM:LOGINOUT.EXE /INPUT=SYS$MANAGER:CHARON_SHUTDOWN -
17:29:17 [INFO ] /OUTPUT=SYS$MANAGER:CHARON_SHUTDOWN.LOG /UIC=[1,4]
17:29:17 [INFO ] %RUN-S-PROC_ID, identification of created process is 00000122
17:29:17 [INFO ] $ ENDIF
17:29:17 [INFO ] $ ENDIF
17:29:17 [INFO ] $ EXIT
17:29:17 [INFO ] $
17:29:17 [INFO ] $ !
17:29:17 [INFO ] $ ! Force any output to the standard output socket.
17:29:17 [INFO ] $ ! Most useful when client is Un*x.
17:29:17 [INFO ] $ !
17:29:17 [INFO ] $ WRITE SYS$OUTPUT ""
17:29:17 [INFO ] $
17:29:17 [INFO ] $ IF (RSHD$ERROR .NES. RSHD$INPUT_OUTPUT)
17:29:17 [INFO ] $ ENDIF
17:29:17 [INFO ] $
17:29:17 [INFO ] $ ! SS_NORMAL, RSH was succcessful, command should send its error over net.
17:29:17 [INFO ] $ EXIT 1
17:29:18 [INFO ] Command successfully completed.
17:29:20 [INFO ] Testing connection to '10.0.0.3' = True
17:29:43 [INFO ] Testing connection to '10.0.0.3' = False
17:29:53 [INFO ] Sleeping for 10 seconds...
17:30:03 [INFO ] Stopping service ds20vms
17:30:04 [INFO ] Service ds20vms is Stopped
17:30:04 [INFO ] Script ended.
```

Using ssh

Contents

- Parameters
  - logfile
  - windowsevent
  - waitbeforestop
  - servicename
  - guestsystem
  - os
  - mode
  - sshbin
  - username
  - identityfile
  - identityfsys
  - openconsolecmd
  - openconsolearg
  - commandparams
  - windowwidth and windowheight
- ssh Key Infrastructure
  - OpenVMS - Windows pair
  - Tru64 - Windows pair
  - Managing CYGWIN and ssh error messages
    - cygwin warning
    - Could not create directory ssh error
    - To view or change environment variables
      - Using the Windows GUI
      - Using Powershell
  - Managing ciphers, hashes and key-exchange algorithms
- Example - OpenVMS
  - Configuration file
  - Script execution
    - Check mode
    - Shutdown execution

Parameters

logfile

Full path to the log file that will be used to log the script output.

Example:
```
logfile=C:\Charon\myds20vms_shutdown.log
```

windowsevent

Defines which message levels will create a new entry in the Windows Application Events (Source="CHARON")

Can be either "none" or any combination of S, W and E. 'S' for Success, 'W' for Warning and 'E' for Error. Default is 'SE' so Success and Error only.

Example:
```
windowsevent=SWE
```

waitbeforestop

Number of seconds to wait before stopping the service once the guest operating system no longer responds to 'ping'. If not set, default value = 60.

Example:

```
waitbeforestop=10
```

servicename

CHARON instance service name

Example:

```
servicename=myds20vms
```

guestsystem

Server name or IP address

Example:

```
guestsystem=10.0.0.3
```

os

`VMS or Tru64`

Example:

```
os=VMS
```

mode

`ssh`

Example:

```
mode=ssh
```

sshbin

Defines the location of the "ssh.exe" program.

Example:

```
sshbin=C:\Program Files (x86)\OpenSSH\ssh.exe
```

username

Defines the remote username that will be used to connect to the guest operating system via rsh.

Example:

```
username=system
```

identityfile

Identity file that stores the Key infrastructure.

Example:

```
identityfile=C:\Charon\win2008bm
```

identityfsys

Identity file that stores the Key infrastructure for the "system" account. Used in case of integration with Windows shutdown.

ℹ If not specified, `identityfile` is used

Example:

```
identityfsys=C:\Charon\win2008bm_sys
```

openconsolecmd

Optional parameter used to open the console program while executing the script. This parameter must contain the full path to the software used to connect to the console. In case putty is going to be used, it is possible to set it to 'putty' without any path. Doing so, the script will look for the latest version available in the Charon installation folder.

? It is recommended to define this parameter in case of integration with Windows shutdown

Example 1:

```
openconsolecmd=C:\Program Files\CHARON\Build_20203\x64\putty
```

Example 2:

```
openconsolecmd=putty
```

openconsolearg

Optional parameter defining the parameters of the `openconsolecmd` parameter above.

Example:

```
openconsolearg=-load OPA0 -P 10003
```

commandparams

"ssh" command optional parameters. Most of the time necessary to enable connection to old versions of "ssh" running on OpenVMS or Tru64

Example:

```
commandparams=-o Ciphers=+3des-cbc -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlgorithms=+ssh-dss
```

windowwidth and windowheight

Optional parameters used to resize the window when running with service user ("system" account).

Useful during Windows shutdown to check operations executed.

Width = 132 and Height = 32 by default. BufferHeight set 2000 lines by default.

Example:

```
windowwidth=120
windowheight=50
```

ssh Key Infrastructure

The examples provided use a Windows Server 2008 R2 machine named WIN2008BM. This name will be used for the files created for the key pair.

OpenVMS - Windows pair

On the Windows server – create the key pair and export the public key to be readable by OpenVMS:

```
c:\Charon>"C:\Program Files (x86)\OpenSSH\ssh-keygen" -f c:\charon\win2008bmrsa -t rsa -b 2048
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):  do not specify any passphrase
Enter same passphrase again:
Your identification has been saved in c:\charon\win2008bmrsa.
Your public key has been saved in c:\charon\win2008bmrsa.pub.
The key fingerprint is:
SHA256:DmB9rFQYeGlzM6uL51Y4EVR8XoCEb+SXFrw7ZD0Khv4 administrateur@WIN2008BM
The key's randomart image is:
+---[RSA 2048]----+
(truncated)
+----[SHA256]-----+
c:\Charon>"C:\Program Files (x86)\OpenSSH\ssh-keygen" -f c:\charon\win2008bmrsa -e
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by administrateur@WIN2008BM from Ope"
(truncated)
---- END SSH2 PUBLIC KEY ----
```

Depending on OpenSSH version used, the installation folder could be "`C:\Program Files (x86)\OpenSSH for Windows`" and executables in the "`bin`" child folder

The public key (text above in dark grey marked by the BEGIN SHS2 and END SSH2 labels) will have to be copied to the OpenVMS system in a later step.

On OpenVMS – enable the SSH server by executing the TCPIP$CONFIG script (depending on the OpenVMS version, the script could also be called UCX$CONFIG):

```
VMS084> @tcpip$config

        Checking TCP/IP Services for OpenVMS configuration database files.

        HP TCP/IP Services for OpenVMS Configuration Menu

        Configuration options:

                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure

Enter configuration option: 3

  HP TCP/IP Services for OpenVMS Server Components Configuration Menu

  Configuration options:

    1 - BIND         Disabled Stopped      12 - NTP          Disabled Stopped
    2 - BOOTP        Disabled Stopped      13 - PC-NFS       Disabled Stopped
    3 - DHCP         Disabled Stopped      14 - POP          Disabled Stopped
    4 - FINGER       Disabled Stopped      15 - PORTMAPPER   Disabled Stopped
    5 - FTP          Disabled Stopped      16 - RLOGIN       Enabled  Started
    6 - IMAP         Disabled Stopped      17 - RMT          Disabled Stopped
    7 - LBROKER      Disabled Stopped      18 - SNMP         Disabled Stopped
    8 - LPR/LPD      Disabled Stopped      19 - SSH          Disabled Stopped
    9 - METRIC       Disabled Stopped      20 - TELNET       Enabled  Started
   10 - NFS          Disabled Stopped      21 - TFTP         Disabled Stopped
   11 - LOCKD/STATD  Disabled Stopped      22 - XDM          Disabled Stopped
    A  -  Configure options 1 - 22
   [E] -  Exit menu

Enter configuration option: 19

SSH Configuration
Service is defined in the SYSUAF.
Service is defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.

        SSH configuration options:

                 1 - Enable service on this node
                 2 - Enable & Start service on this node
                [E] - Exit SSH configuration

Enter configuration option: 2

* Create a new default server host key? [NO]:
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SSHD2.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$SSH_SFTP-SERVER2.EXE installed
%TCPIP-I-INFO, logical names created
%%%%%%%%%%%  OPCOM   8-JUL-2016 03:50:16.47  %%%%%%%%%%%
Message from user INTERnet on VMS084
INTERnet ACP Activate SSH Server

%TCPIP-I-INFO, service enabled
%TCPIP-S-STARTDONE, TCPIP$SSH startup completed
Press <ENTER> key to continue ...

The SSH CLIENT is not enabled.

* Do you want to configure SSH CLIENT [NO]:

  HP TCP/IP Services for OpenVMS Server Components Configuration Menu
  Configuration options:

    1 - BIND         Disabled Stopped      12 - NTP          Disabled Stopped
    2 - BOOTP        Disabled Stopped      13 - PC-NFS       Disabled Stopped
    3 - DHCP         Disabled Stopped      14 - POP          Disabled Stopped
    4 - FINGER       Disabled Stopped      15 - PORTMAPPER   Disabled Stopped
    5 - FTP          Disabled Stopped      16 - RLOGIN       Enabled  Started
    6 - IMAP         Disabled Stopped      17 - RMT          Disabled Stopped
    7 - LBROKER      Disabled Stopped      18 - SNMP         Disabled Stopped
    8 - LPR/LPD      Disabled Stopped      19 - SSH          Enabled  Started
    9 - METRIC       Disabled Stopped      20 - TELNET       Enabled  Started
   10 - NFS          Disabled Stopped      21 - TFTP         Disabled Stopped
   11 - LOCKD/STATD  Disabled Stopped      22 - XDM          Disabled Stopped
    A  -  Configure options 1 - 22
   [E] -  Exit menu

Enter configuration option: e

        HP TCP/IP Services for OpenVMS Configuration Menu

        Configuration options:

                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure

Enter configuration option: e

VMS084>
```

Copy the public key created above to OpenVMS (either with 'scp' or with copy/paste).

On OpenVMS – make the key available to the system and authorize it for use:

```
$ SET DEF SYS$LOGIN
If needed:  $ CREATE /DIR [.SSH2]
$ SET DEF [.SSH2]
$ EDIT WIN2008BMRSA.PUB
```

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by administrateur@WIN2008BM from Ope"
(truncated)
---- END SSH2 PUBLIC KEY ----
```

```
$ EDIT AUTHORIZATION.
```

```
KEY WIN2008BMRSA.PUB
```

```
$
```

On the Windows server – check that the key pair works:

⚠ Do not forget to specify the identity file using the "`-i`" parameter.

```
c:\Charon>"C:\Program Files (x86)\OpenSSH\ssh" -i c:\charon\win2008bmrsa -l system 10.0.0.3 ^
More? "show system/noprocess"

 Welcome to OpenVMS (TM) Alpha Operating System, Version V8.4

OpenVMS V8.4  on node VMS084    8-JUL-2016 04:10:47.57   Uptime  0 00:24:13
```

ℹ On first connection attempt you will have to answer "yes" to the "Are you sure you want to continue connecting" question.

❓ If you encounter a "`cygwin warning`" error message and/or a message like: `Could not create directory '/home/<user>/.ssh'` , please see Managing CYGWIN and ssh error messages chapter.

❓ If you encounter an error message related to **`diffie-hellman-group1-sha1`** , please see Managing ciphers, hashes and key-exchange algorithms chapter.

Tru64 - Windows pair

On the Windows server – create the key pair and export the public key to be readable by Tru64:

```
c:\Charon>"C:\Program Files (x86)\OpenSSH\ssh-keygen" -f c:\charon\win2008bmrsa -t rsa -b 2048
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):  do not specify any passphrase
Enter same passphrase again:
Your identification has been saved in c:\charon\win2008bmrsa.
Your public key has been saved in c:\charon\win2008bmrsa.pub.
The key fingerprint is:
SHA256:DmB9rFQYeGlzM6uL51Y4EVR8XoCEb+SXFrw7ZD0Khv4 administrateur@WIN2008BM
The key's randomart image is:
+---[RSA 2048]----+
(truncated)
+----[SHA256]-----+
c:\Charon>"C:\Program Files (x86)\OpenSSH\ssh-keygen" -f c:\charon\win2008bmrsa -e
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by administrateur@WIN2008BM from Ope"
(truncated)
---- END SSH2 PUBLIC KEY ----
```

Depending on OpenSSH version used, the installation folder could be "`C:\Program Files (x86)\OpenSSH for Windows`" and executables in the "`bin`" child folder

Copy the public key (text above in dark gray marked by the BEGIN SSH2 and END SSH2 labels) to the Tru64 system (either with 'scp' or with copy /paste).

On Tru64 – make the key available to the system and authorize it for use:

```
# cd /.ssh2
# vi win2008bmrsa.pub
```

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by administrateur@WIN2008BM from Ope"
(truncated)
---- END SSH2 PUBLIC KEY ----
```

```
# echo "Key win2008bmrsa.pub" >> authorization
```

On the Windows server – check that the key pair works:

⚠ Do not forget to specify the identity file using the "-i" parameter.

```
c:\Charon>"C:\Program Files (x86)\OpenSSH\ssh" -i c:\charon\WIN2008BM_RSA -l root 10.0.0.2 "uname -a"
OSF1 pluto.localdomain V5.1 2650 alpha
```

ℹ On first connection attempt you will have to answer "yes" to the "Are you sure you want to continue connecting" question.

? If you encounter a "`cygwin warning`" error message and/or a message like: `Could not create directory '/home/<user>/.ssh'` while executing this command, please see Managing CYGWIN and ssh error messages.

? If you encounter an error message related to **`diffie-hellman-group1-sha1`** , please see Managing ciphers, hashes and key-exchange algorithms chapter.

Managing CYGWIN and ssh error messages

cygwin warning

You can ignore the "cygwin warning" message or define the environment variable (see how-to) "`CYGWIN`" to "`nodosfilewarning`" as explained in the displayed text if it appears. This warning message will not be displayed while running the Powershell script as this environment variable is set inside the script.

Example:

```
cygwin warning:
  MS-DOS style path detected: c:\charon\WIN7BM_DSA
  Preferred POSIX equivalent is: /cygdrive/c/charon/WIN7BM_DSA
  CYGWIN environment variable option "nodosfilewarning" turns off this warning.
  Consult the user's guide for more details about POSIX paths:
    http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
```

💡 To remove this message you can set the "CYGWIN" Windows environment variable or use this DOS command before running the '`ssh`' test command (⚠ the following command will not set a permanent variable):

```
c:\Charon>set CYGWIN=nodosfilewarning
```

Could not create directory ssh error

💡 If you encounter an error message like: `Could not create directory '/home/<user>/.ssh'`, please create the "`HOME`" Windows environment variable (see how-to) and set it to your home folder, for example.

Please note: this variable will be set on the next login. So if you need it immediately, use the following DOS command before running the '`ssh`' test command (⚠️ the following command will not set a permanent variable):

```
c:\Charon>set HOME=%userprofile%
```

To view or change environment variables

Using the Windows GUI

1. Either right-click on "My Computer" and then click on "Properties" and "Advanced tab" or press the Windows key+R and enter "`systempropertiesadvanced`"
2. Click on "Environment variables".
3. Click on one of the following options, for either a user or a system variable:
   a. Click on New to add a new variable name and value.
   b. Click on an existing variable, and then click on Edit to change its name or value.
   c. Click on an existing variable, and then click on Delete to remove it.

Using Powershell

Powershell can be used to define user environment variables. Please refer to the examples below:

```
c:\Charon> powershell
PS c:\Charon> [Environment]::SetEnvironmentVariable("CYGWIN", "nodosfilewarning", "User")
PS c:\Charon> [Environment]::SetEnvironmentVariable("HOME", "$env:userprofile", "User")
PS c:\Charon> exit
```

Managing ciphers, hashes and key-exchange algorithms

Starting with OpenSSH version 7.0, ciphers, hashes and key-exchange algorithms are disabled by default. This means that for newer versions of OpenSSH, connecting to Tru64 or OpenVMS systems can be a problem.

To solve this problem:

- Set the "`commandparams`" value in the .ini file as shown below:
  `commandparams=-o Ciphers=+3des-cbc -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlgorithms=+ssh-dss`

  or

- create a file named "`config`" (no extension) in the user's folder `C:\Users\<user>\.ssh` (create the `.ssh` folder if it does not exist) and add the following lines:

```
Host 10.0.0.3
  Hostname myds20vms
  KexAlgorithms +diffie-hellman-group1-sha1
  HostKeyAlgorithms +ssh-dss
  Ciphers +3des-cbc
```

💡 If the hostname is known to the system, replace the IP address in the 1st line by hostname or add it at the end of the line (blank separated). **Example**: "`Host 10.0.0.3 ds20vms`"

Example - OpenVMS

Configuration file

```
#-----------------------------------------
# myds20 OpenVMS 8.4 machine
#-----------------------------------------
logfile=C:\Charon\myds20vms_shutdown.log
waitbeforestop=10
guestsystem=10.0.0.3
servicename=myds20vms
os=VMS
mode=ssh
sshbin=C:\Program Files (x86)\OpenSSH\ssh.exe
username=system
identityfile=C:\Charon\win2008bm_dsa
```

Script execution

Check mode

```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\myds20vms.ini -check

                                              Charon clean shutdown



Name                 Value
----                 -----
os                   VMS
waitbeforestop       10
windowwidth          132
servicename          ds20vms
openconsolecmd       C:\Program Files\CHARON\Build_20203\x64\putty
username             system
identityfile         C:\Charon\win2008system
commandparams        -o Ciphers=+3des-cbc -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlgorithms=+...
windowheight         50
openconsolearg       -load OPA0 -P 10003
guestsystem          10.0.0.3
mode                 ssh
sshbin               C:\Program Files (x86)\OpenSSH\ssh.exe
logfile              C:\Charon\myds20vms_shutdown.log



17:34:11 [INFO ] Using 'C:\Charon\myds20vms_shutdown.log' as log file / append
17:34:11 [INFO ] Execution date : 27-avr.-2020 17:34:11
17:34:11 [INFO ] Script version : 27-Apr-20 V2.0 (MD5: 4BA97792A105C9E0E484850B88B866F8 )
17:34:11 [INFO ] Powershell version : 5.1.14409.1018
17:34:11 [INFO ] Computer name : WIN2008BM
17:34:11 [INFO ] Username : Administrateur
17:34:11 [INFO ] Windows version : Microsoft Windows Server 2008 R2 Standard
17:34:11 [INFO ] Administrator mode : True
17:34:11 [INFO ]
17:34:11 [INFO ] Check mode enabled.
17:34:11 [INFO ] 'ssh' will be used
17:34:11 [INFO ] Using 'C:\Charon\win2008system' as identity file.
17:34:11 [INFO ] Service 'ds20vms' is Running (Display name: ds20vms)
17:34:11 [INFO ] Testing guest system '10.0.0.3' response
17:34:15 [INFO ] Opening console.
17:34:15 [INFO ] Invoking 'ssh' command and executing check command as Administrateur ...
17:34:15 [INFO ] C:\Program Files (x86)\OpenSSH\ssh.exe -i C:\Charon\win2008system -q -l system -o
BatchMode=yes -o Ciphers
=+3des-cbc -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlgorithms=+ssh-dss 10.0.0.3 '@SYS$MANAGER:
CHARON_SHUTDOW
N.COM CHECK SSH'
17:34:16 [INFO ] Output results:
17:34:16 [INFO ]
17:34:16 [INFO ] SSH was successful
17:34:16 [INFO ]
17:34:16 [INFO ] Checking command results...
17:34:16 [INFO ] Command successfully completed.
17:34:16 [INFO ] Check mode enabled: no connection test to be performed.
17:34:16 [INFO ] Check mode enabled: no wait / stop service.
17:34:16 [INFO ] Check mode enabled: the service ds20vms will not be stopped
17:34:16 [INFO ] Service ds20vms is Running
17:34:16 [INFO ] Script ended.
```

Shutdown execution

```
c:\Windows\system32>C:\charon\charon_cleanshutdown.ps1 -config C:\charon\myds20vms.ini

                                        Charon clean shutdown

Name                 Value
----                 -----
os                   VMS
waitbeforestop       10
windowwidth          132
servicename          ds20vms
openconsolecmd       C:\Program Files\CHARON\Build_20203\x64\putty
username             system
identityfile         C:\Charon\win2008system
commandparams        -o Ciphers=+3des-cbc -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlgorithms=+...
windowheight         50
openconsolearg       -load OPA0 -P 10003
guestsystem          10.0.0.3
mode                 ssh
sshbin               C:\Program Files (x86)\OpenSSH\ssh.exe
logfile              C:\Charon\myds20vms_shutdown.log
```

```
17:41:40 [INFO ] Using 'C:\Charon\myds20vms_shutdown.log' as log file / append
17:41:40 [INFO ] Execution date : 27-avr.-2020 17:41:40
17:41:40 [INFO ] Script version : 27-Apr-20 V2.0 (MD5: 5CA44D034529A2BF7E868463F1B7A93C )
17:41:40 [INFO ] Powershell version : 5.1.14409.1018
17:41:40 [INFO ] Computer name : WIN2008BM
17:41:40 [INFO ] Username : Administrateur
17:41:40 [INFO ] Windows version : Microsoft Windows Server 2008 R2 Standard
17:41:40 [INFO ] Administrator mode : True
17:41:40 [INFO ]
17:41:41 [INFO ] 'ssh' will be used
17:41:41 [INFO ] Using 'C:\Charon\win2008system' as identity file.
17:41:41 [INFO ] Service 'ds20vms' is Running (Display name: ds20vms)
17:41:41 [INFO ] Testing guest system '10.0.0.3' response
17:41:44 [INFO ] Killing putty sessions...
17:41:45 [INFO ] Done.
17:41:45 [INFO ] Opening console.
17:41:45 [INFO ] Invoking 'ssh' command and executing shutdown as Administrateur ...
17:41:45 [INFO ] C:\Program Files (x86)\OpenSSH\ssh.exe -i C:\Charon\win2008system -q -l system -o
BatchMode=yes -o Ciphers=+3des-cbc -o KexAlgorithms=+diffie-hellman-group1-sha1 -o HostKeyAlgorithms=+ssh-
dss 10.0.0.3 '@SYS$MANAGER:CHARON_SHUTDOWN.COM'
17:41:46 [INFO ] Output results:
17:41:46 [INFO ]
17:41:46 [INFO ] $ PURGE /KEEP=20 SYS$MANAGER:CHARON_SHUTDOWN.LOG
17:41:46 [INFO ] $ RUN /DETACH SYS$SYSTEM:LOGINOUT.EXE /INPUT=SYS$MANAGER:CHARON_SHUTDOWN -
17:41:46 [INFO ] /OUTPUT=SYS$MANAGER:CHARON_SHUTDOWN.LOG /UIC=[1,4]
17:41:46 [INFO ] %RUN-S-PROC_ID, identification of created process is 00000122
17:41:46 [INFO ] $ ENDIF
17:41:46 [INFO ] $ ENDIF
17:41:46 [INFO ] $ EXIT
17:41:46 [INFO ] $
17:41:46 [INFO ] $ !
17:41:46 [INFO ] $ ! Force any output to the standard output device.
17:41:46 [INFO ] $ ! Most useful when client is Un*x.
17:41:46 [INFO ] $ !
17:41:46 [INFO ] $ ! V5.4-03
17:41:46 [INFO ] $ ! WRITE SYS$OUTPUT -
17:41:46 [INFO ] $ ! "ssh-rcmd 'f$getjpi("","USERNAME")' logged out at 'f$time()'" ! V5.4-02
17:41:46 [INFO ]
17:41:46 [INFO ] $ WRITE SYS$OUTPUT ""
17:41:46 [INFO ]
17:41:46 [INFO ] $
17:41:46 [INFO ] $ IF (SSHD$ERROR .NES. SSHD$INPUT_OUTPUT)
17:41:46 [INFO ] $ ENDIF
17:41:46 [INFO ] $
17:41:46 [INFO ] $ ! SS_NORMAL, SSH was succcessful, command should send its error over net.
17:41:46 [INFO ] $ EXIT 1
17:41:46 [INFO ] Checking command results...
17:41:46 [INFO ] Command successfully completed.
17:41:49 [INFO ] Testing connection to '10.0.0.3' = True
17:42:12 [INFO ] Testing connection to '10.0.0.3' = False
17:42:22 [INFO ] Sleeping for 10 seconds...
17:42:32 [INFO ] Stopping service ds20vms
17:42:33 [INFO ] Service ds20vms is Stopped
17:42:33 [INFO ] Script ended.
```

Running the script

Usage

Invoke the script from the PowerShell command window, specify the configuration file and – optionally – if you want to run the script in "check" mode.

It is recommended to execute the script interactively first, using "check" mode. Using this mode, the script will only setup the connection and execute simple remote display commands. No shutdown will be performed.

Once you are satisfied with the operation of the script, use it at your convenience from any utility (scheduler, backup agent, ...) to shut down the CHARON instance.

> To display the script's help text, please use either this Windows command:
>
> ```
> c:\Charon>powershell -file charon_cleanshutdown.ps1 -help
> ```
>
> or the PowerShell "get-help" command:
>
> ```
> PS C:\Charon> get-help c:\charon\charon_cleanshutdown.ps1 -full
> ```

To automatically restart the guest operating system running on the CHARON instance, the automatic boot on restart has to be set at SRM level and the following Windows service command must be executed:

```
c:\Charon>sc start <servicename>
```

To tell the script how the shutdown will be performed, some parameters are necessary. They are defined in a configuration file that is described in the Configuration file settings chapter.

Note on CHARON instance service:

The 'opa0' mode will perform the "`power off`" command itself or will send the "`F6`" key if this command is not available, thus stopping the service. The other modes will perform a clean shutdown without powering off the CHARON instance, thus leaving the service active and the instance at the SRM prompt. To recognize the completion of the shutdown process in this case, a loop has been introduced to check if the guest operating system running on the instance responds to "`ping`". Once it no longer responds, the script waits for a specified amount of time (`waitbeforestop` parameter) before stopping the service.

Examples

Check mode:

```
C:\Users\Administrator> powershell -file c:\charon\charon_cleanshutdown.ps1 ^
More? -config c:\charon\myds20vms.ini-check
```

Shutdown execution mode:

```
C:\Users\Administrator> powershell -file c:\charon\charon_cleanshutdown.ps1 -config c:\charon\myds20vms.ini
```

Service restart:

```
C:\Users\Administrator> sc start myds20vms
```

Integration with Windows shutdown

Contents

- Principle
- opa0 mode preparation
- rsh mode preparation
- ssh mode preparation
- Windows settings - Local group policy
  - Adding the script to the shutdown Powershell scripts
  - Display instructions in shutdown scripts as they run
  - Specify maximum wait time for Group Policy scripts
- Windows shutdown example

Principle

Using the "Local Group Policy Editor", it is possible to add the execution of a Powershell script at Windows shutdown. As this operation is performed with the "`system`" account, some operations have to be performed depending on the method chosen (`opa0`, `rsh` or `ssh`).

Please note shutdown scripts are executed when the shutdown is executed either from the "Windows Start" menu or using the shutdown command line. They are not always executed when clicking on the "Restart" button from the Windows Update tool.

opa0 mode preparation

If the combination of username/password is used, there is no need for configuration change.

If an encrypted file is used to store the password using the "`cryptedpsys`" parameter, it must be created on a session as "`system`" account.

To do so, open a `cmd.exe` window as Administrator and run the following command:

```
C:\WINDOWS\system32>C:\Charon\psexec.exe -i -s cmd.exe
```

A new window will popup. To check you're connected as "system", run:

```
C:\WINDOWS\system32>whoami
nt authority\system
```

Run the following command to create the encrypted file:

```
C:\Users\Spock> powershell -command "ConvertTo-SecureString -String '<password>' -AsPlainText -Force ^
More? | ConvertFrom-SecureString | Out-File '<full path to the file>'"
```

Example:

```
C:\Users\Spock> powershell -command "ConvertTo-SecureString -String '12345' -AsPlainText -Force ^
More? | ConvertFrom-SecureString | Out-File 'c:\charon\msds20vmspwd.txt'"
```

Run the Powershell script in check mode:

```
C:\WINDOWS\system32>powershell -file c:\charon\charon_cleanshutdown.ps1 -config c:\charon\myds20vms.ini -check
```

then check the "`OPA0 was successful`" message is displayed followed by "`Command successfully completed.`"

> ⚠ It is recommended to move the `psexec.exe` program file to a secured folder or to remove it when it is no more needed (check completed)

rsh mode preparation

> A proxy has to be defined at OpenVMS level hence the local "`system`" user must be specified. This user name is translated depending on the language of the Windows distribution.
>
> It is then highly recommended to install an English version of Windows to avoid issues with accents and non standard characters when creating this proxy.

Execute the same operations as described in chapter "Using rsh" for Tru64 or VMS to enable remote connection for the "`SYSTEM`" user.

⚠ This is case sensitive so for Tru64, specify "`SYSTEM`" and not "`system`" in the `.rhosts` file

It is highly recommended to test the execution of the script in check mode while connected as "`system`" account. To do so, use the `psexec.exe` program file provided in the kit or download it from the Microsoft Sysinternals page.

Open a `cmd.exe` window as Administrator and run the following command:

```
C:\WINDOWS\system32>C:\Charon\psexec.exe -i -s cmd.exe
```

A new window will popup. To check you're connected as "system", run:

```
C:\WINDOWS\system32>whoami
nt authority\system
```

Run the Powershell script in check mode:

```
C:\WINDOWS\system32>powershell -file c:\charon\charon_cleanshutdown.ps1 -config c:\charon\myds20vms.ini -check
```

then check the "`RSH was successful`" message is displayed followed by "`Command successfully completed.`"

> ⚠ It is recommended to move the `psexec.exe` program file to a secured folder or to remove it when it is no more needed (check completed)

ssh mode preparation

Execute the same operations as described in chapter "Using ssh" for Tru64 or VMS to create a key pair with "`SYSTEM`" user with a different identity file.

To do so, use the `psexec.exe` program file provided in the kit or download it from the Microsoft Sysinternals page.

Open a `cmd.exe` window as Administrator and run the following command:

```
C:\WINDOWS\system32>C:\Charon\psexec.exe -i -s cmd.exe
```

A new window will popup. To check you're connected as "system", run:

```
C:\WINDOWS\system32>whoami
nt authority\system
```

Create a new ssh trust as described in the "Using ssh" chapter.

✓ Remember to specify a different identity file in the .ini file. This can be done thanks to the "`identityfsys`" parameter (see: Using ssh)

Run the Powershell script in check mode:

```
C:\WINDOWS\system32>powershell -file c:\charon\charon_cleanshutdown.ps1 -config c:\charon\myds20vms.ini -check
```

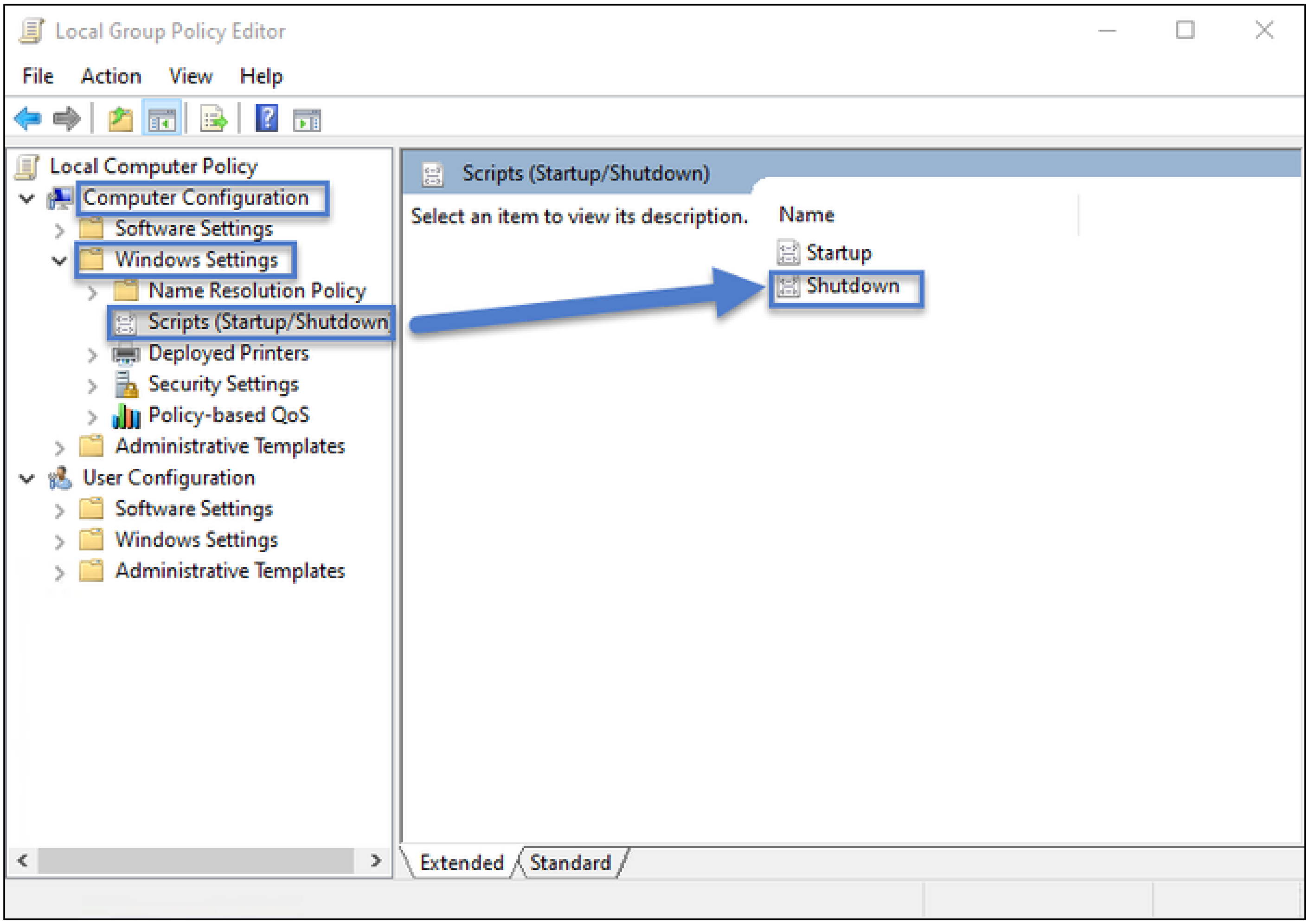
then check the "`SSH was successful`" message is displayed followed by "`Command successfully completed.`"

⚠ It is recommended to move the `psexec.exe` program file to a secured folder or to remove it when it is no more needed (check completed)

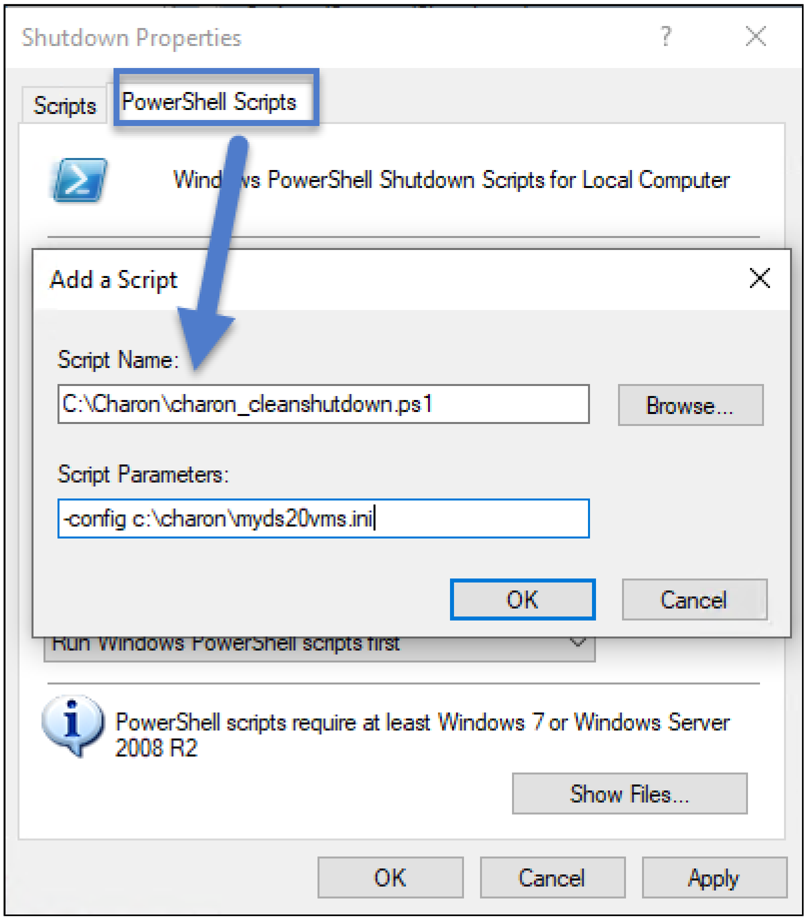
Windows settings - Local group policy

Adding the script to the shutdown Powershell scripts

Open the "Local Group Policy Editor" (run gpedit.msc) and go to the Shutdown script setup:



Select the "Powershell Scripts" tab, click on the "Add..." button, specify the path to the `charon_cleanshutdown.ps1` script and its parameters:



Script Name: C:\Charon\charon_cleanshutdown.ps1

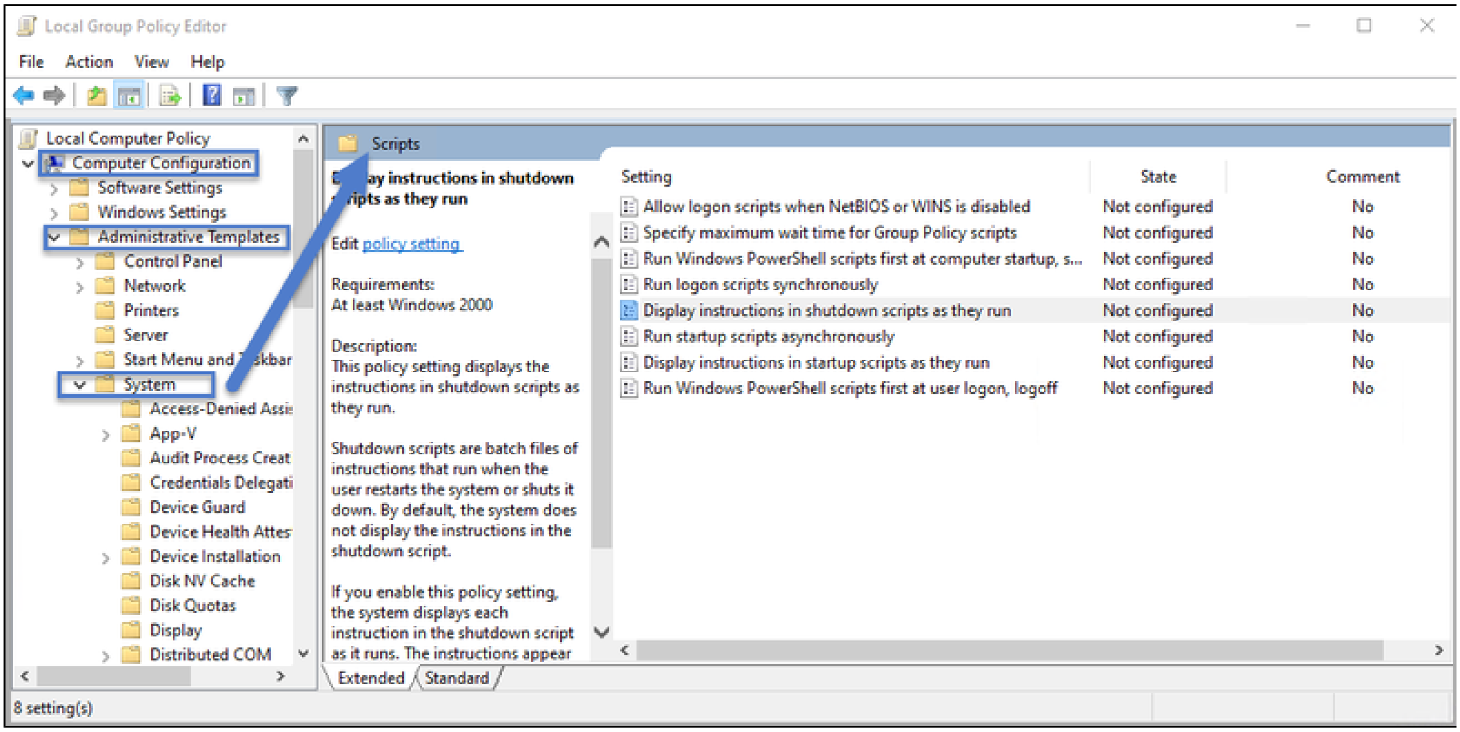
Script Parameters: -config c:\charon\myds20vms.ini

PowerShell scripts require at least Windows 7 or Windows Server 2008 R2

Display instructions in shutdown scripts as they run

It is recommended to enable the display instructions during shutdown to check the Charon Legacy OS shutdown is correctly performed.

Open the "Local Group Policy Editor" (run gpedit.msc) and go to the "Computer Configuration" → "Administrative Templates" → "System" → "Scripts" setup:



Display instructions in shutdown scripts as they run

Edit policy setting

Requirements:
At least Windows 2000

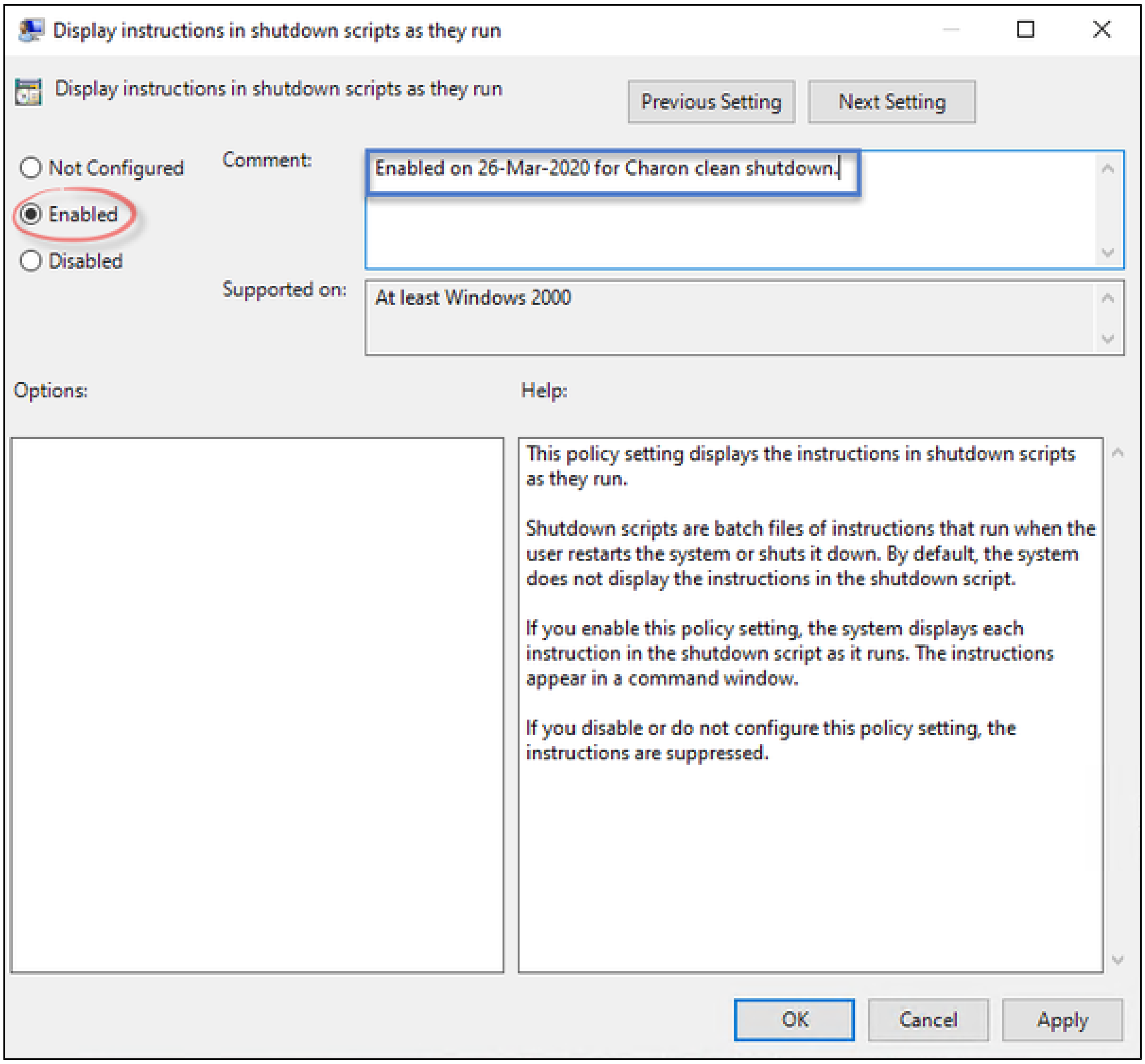
Description:
This policy setting displays the instructions in shutdown scripts as they run.

Shutdown scripts are batch files of instructions that run when the user restarts the system or shuts it down. By default, the system does not display the instructions in the shutdown script.

If you enable this policy setting, the system displays each instruction in the shutdown script as it runs. The instructions appear

Setting	State	Comment
Allow logon scripts when NetBIOS or WINS is disabled	Not configured	No
Specify maximum wait time for Group Policy scripts	Not configured	No
Run Windows PowerShell scripts first at computer startup, s...	Not configured	No
Run logon scripts synchronously	Not configured	No
Display instructions in shutdown scripts as they run	Not configured	No
Run startup scripts asynchronously	Not configured	No
Display instructions in startup scripts as they run	Not configured	No
Run Windows PowerShell scripts first at user logon, logoff	Not configured	No

Enable this functionality and optionally leave a comment:



Display instructions in shutdown scripts as they run

Display instructions in shutdown scripts as they run

○ Not Configured

● Enabled

○ Disabled

Comment: Enabled on 26-Mar-2020 for Charon clean shutdown.

Supported on: At least Windows 2000

Options:

Help:

This policy setting displays the instructions in shutdown scripts as they run.

Shutdown scripts are batch files of instructions that run when the user restarts the system or shuts it down. By default, the system does not display the instructions in the shutdown script.

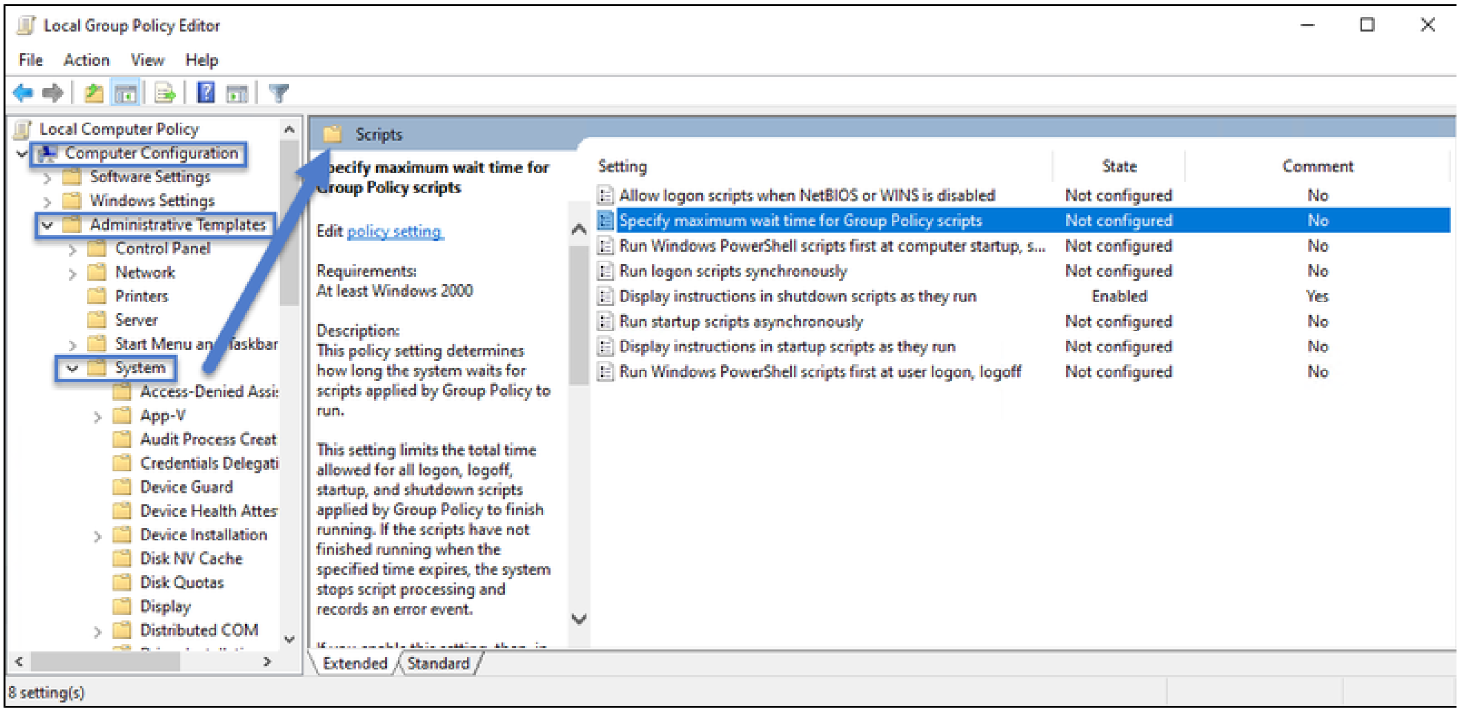
If you enable this policy setting, the system displays each instruction in the shutdown script as it runs. The instructions appear in a command window.

If you disable or do not configure this policy setting, the instructions are suppressed.

Specify maximum wait time for Group Policy scripts

By default the script executed at Windows shutdown have a default timeout of 10 minutes (600 seconds). It is possible to change this value in case the shutdown takes more time.

Open the "Local Group Policy Editor" (run gpedit.msc) and go to the "Computer Configuration" → "Administrative Templates" → "System" → "Scripts" setup:



Specify maximum wait time for Group Policy scripts

Edit policy setting.

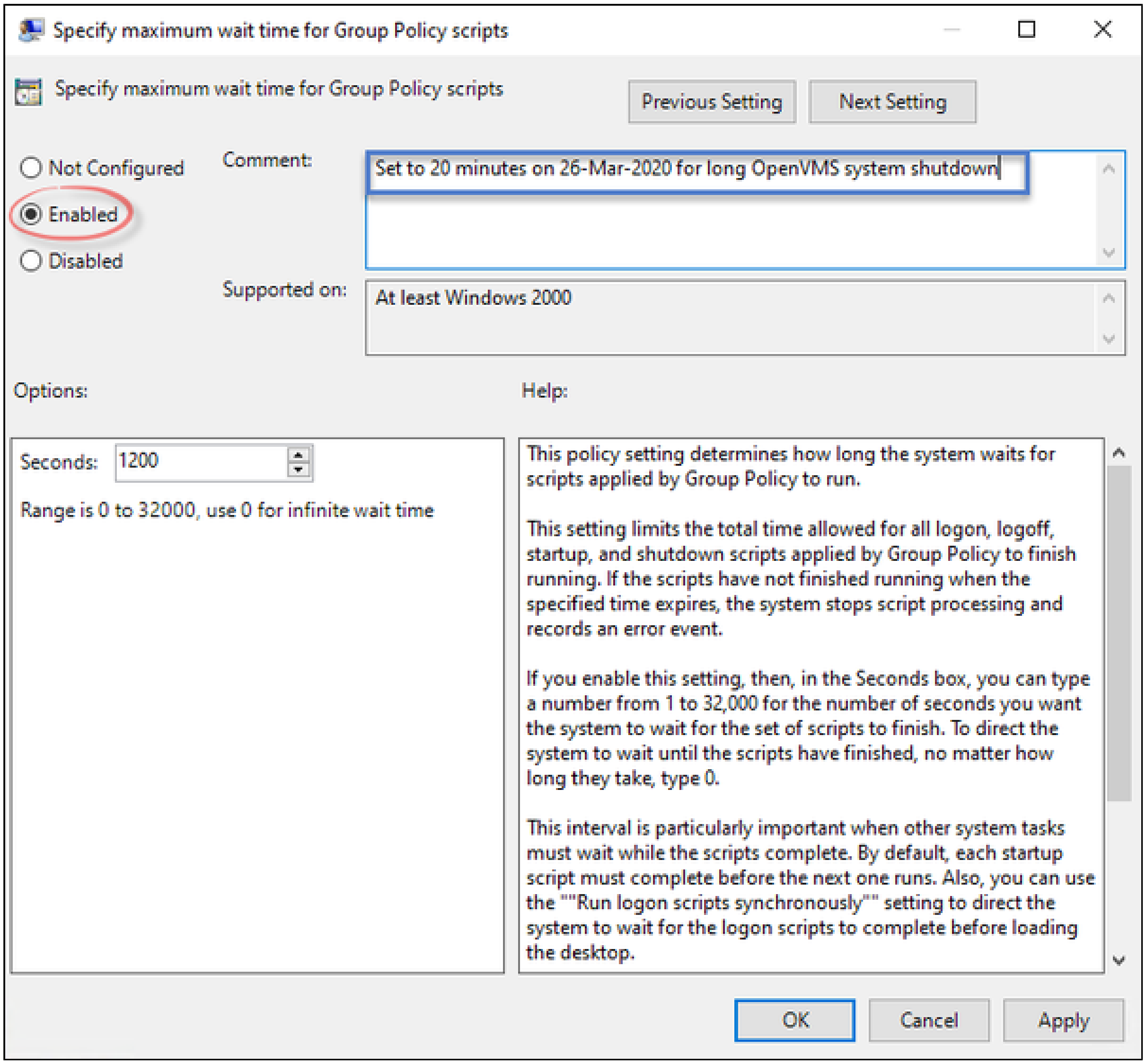
Requirements:
At least Windows 2000

Description:
This policy setting determines how long the system waits for scripts applied by Group Policy to run.

This setting limits the total time allowed for all logon, logoff, startup, and shutdown scripts applied by Group Policy to finish running. If the scripts have not finished running when the specified time expires, the system stops script processing and records an error event.

Setting	State	Comment
Allow logon scripts when NetBIOS or WINS is disabled	Not configured	No
Specify maximum wait time for Group Policy scripts	Not configured	No
Run Windows PowerShell scripts first at computer startup, s...	Not configured	No
Run logon scripts synchronously	Not configured	No
Display instructions in shutdown scripts as they run	Enabled	Yes
Run startup scripts asynchronously	Not configured	No
Display instructions in startup scripts as they run	Not configured	No
Run Windows PowerShell scripts first at user logon, logoff	Not configured	No

Enable this functionality, define the new timeout and optionally leave a comment:


Specify maximum wait time for Group Policy scripts
Specify maximum wait time for Group Policy scripts
Previous Setting
Next Setting
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Comment: Set to 20 minutes on 26-Mar-2020 for long OpenVMS system shutdown

Supported on: At least Windows 2000

Options:

Seconds: 1200

Range is 0 to 32000, use 0 for infinite wait time

Help:

This policy setting determines how long the system waits for scripts applied by Group Policy to run.

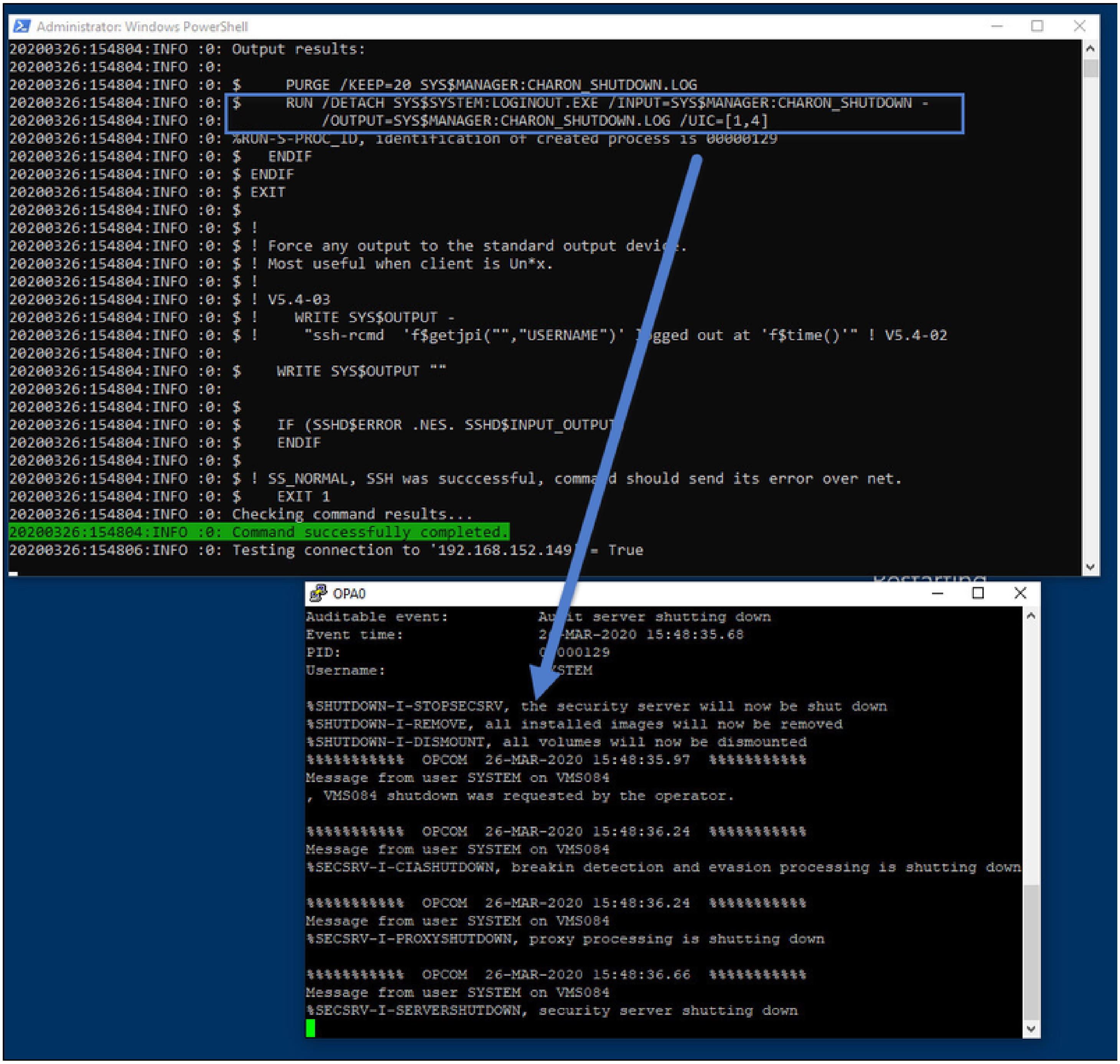
This setting limits the total time allowed for all logon, logoff, startup, and shutdown scripts applied by Group Policy to finish running. If the scripts have not finished running when the specified time expires, the system stops script processing and records an error event.

If you enable this setting, then, in the Seconds box, you can type a number from 1 to 32,000 for the number of seconds you want the system to wait for the set of scripts to finish. To direct the system to wait until the scripts have finished, no matter how long they take, type 0.

This interval is particularly important when other system tasks must wait while the scripts complete. By default, each startup script must complete before the next one runs. Also, you can use the ""Run logon scripts synchronously"" setting to direct the system to wait for the logon scripts to complete before loading the desktop.

Windows shutdown example

This example is given for a Windows 10 Professional version running Charon-AXP V4.10 B202-03. The emulated Alphaserver is a DS20 running OpenVMS 8.4:



Administrator: Windows PowerShell

```
20200326:154804:INFO :0: Output results:
20200326:154804:INFO :0:
20200326:154804:INFO :0: $     PURGE /KEEP=20 SYS$MANAGER:CHARON_SHUTDOWN.LOG
20200326:154804:INFO :0: $     RUN /DETACH SYS$SYSTEM:LOGINOUT.EXE /INPUT=SYS$MANAGER:CHARON_SHUTDOWN -
20200326:154804:INFO :0:           /OUTPUT=SYS$MANAGER:CHARON_SHUTDOWN.LOG /UIC=[1,4]
20200326:154804:INFO :0: %RUN-S-PROC_ID, identification of created process is 00000129
20200326:154804:INFO :0: $   ENDIF
20200326:154804:INFO :0: $ ENDIF
20200326:154804:INFO :0: $ EXIT
20200326:154804:INFO :0: $
20200326:154804:INFO :0: $ !
20200326:154804:INFO :0: $ ! Force any output to the standard output device.
20200326:154804:INFO :0: $ ! Most useful when client is Un*x.
20200326:154804:INFO :0: $ !
20200326:154804:INFO :0: $ ! V5.4-03
20200326:154804:INFO :0: $ !    WRITE SYS$OUTPUT -
20200326:154804:INFO :0: $ !     "ssh-rcmd  'f$getjpi("","USERNAME")' logged out at 'f$time()'" ! V5.4-02
20200326:154804:INFO :0:
20200326:154804:INFO :0: $    WRITE SYS$OUTPUT ""
20200326:154804:INFO :0:
20200326:154804:INFO :0: $
20200326:154804:INFO :0: $    IF (SSHD$ERROR .NES. SSHD$INPUT_OUTPUT
20200326:154804:INFO :0: $    ENDIF
20200326:154804:INFO :0: $
20200326:154804:INFO :0: $ ! SS_NORMAL, SSH was succcessful, command should send its error over net.
20200326:154804:INFO :0: $    EXIT 1
20200326:154804:INFO :0: Checking command results...
20200326:154804:INFO :0: Command successfully completed.
20200326:154806:INFO :0: Testing connection to '192.168.152.149' = True
```

OPA0

```
Auditable event:          Audit server shutting down
Event time:               26-MAR-2020 15:48:35.68
PID:                      00000129
Username:                 SYSTEM

%SHUTDOWN-I-STOPSECSRV, the security server will now be shut down
%SHUTDOWN-I-REMOVE, all installed images will now be removed
%SHUTDOWN-I-DISMOUNT, all volumes will now be dismounted
%%%%%%%%%%%  OPCOM  26-MAR-2020 15:48:35.97  %%%%%%%%%%%
Message from user SYSTEM on VMS084
, VMS084 shutdown was requested by the operator.

%%%%%%%%%%%  OPCOM  26-MAR-2020 15:48:36.24  %%%%%%%%%%%
Message from user SYSTEM on VMS084
%SECSRV-I-CIASHUTDOWN, breakin detection and evasion processing is shutting down

%%%%%%%%%%%  OPCOM  26-MAR-2020 15:48:36.24  %%%%%%%%%%%
Message from user SYSTEM on VMS084
%SECSRV-I-PROXYSHUTDOWN, proxy processing is shutting down

%%%%%%%%%%%  OPCOM  26-MAR-2020 15:48:36.66  %%%%%%%%%%%
Message from user SYSTEM on VMS084
%SECSRV-I-SERVERSHUTDOWN, security server shutting down
```

ⓘ The PowerShell window is displayed during Windows shutdown thanks to the enabled "Display instructions in shutdown scripts as they run" feature and the putty / OPA0 window is opened thanks to the "`openconsolecmd`" and "`openconsolearg`" parameters in the .ini file.

✓ It is recommended to check the log files once the Windows server has rebooted:

- the shutdown log file from this script and
- the OPA0 log file defined in the Charon configuration file (if not set, it is recommended to define it)