



VAPT-SE Installation Guide

2020-11-03

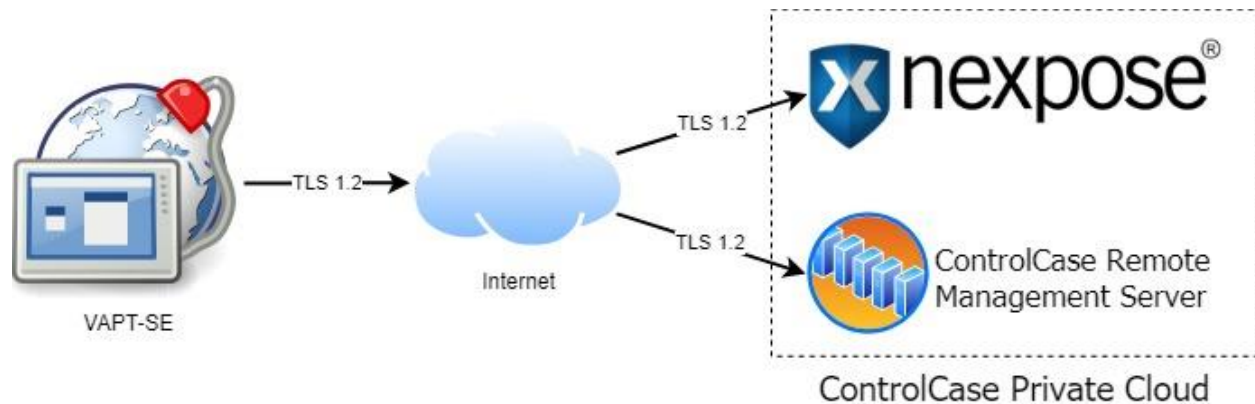
Special Edition (SE)

Table of Contents

About VAPT-SE	3
Introduction to the VAPT-SE Installation	3
Requirements.....	4
Customer Credentials	4
Hardware	4
Operating System.....	4
Network Access.....	5
Installation	6
Install.....	6
Syntax.....	6
Example Output	7
Proinstall	8
Syntax.....	8
Example Output	8
Uninstallation.....	9
Uninstall	9
Syntax.....	9
Example Output	9
Uninstallall	10
Syntax.....	10
Software List	11
Kali Packages.....	11
Rapid7	11
Ubuntu Packages	11
Troubleshooting.....	12
Syntax.....	12
Example Output	12

About VAPT-SE

Vulnerability assessment and penetration testing (VAPT) is a service that ControlCase provides. The VAPT-SE solution is intended to be the replacement for the VAPT virtual machine solution that is now agnostic of the underlying hardware and can be successfully deployed on bare metal, virtual machines, or even cloud machines in a few minutes.



Introduction to the VAPT-SE Installation

The VAPT-SE solution provides various options for installation. To ensure a successful VAPT-SE deployment, we will step through each of the installation methods, and the sequence of tasks.

The four core components of the VAPT-SE solution are:

- The ControlCase remote management software
- A Custom selection of Linux tools required to support the vulnerability assessment and penetration testing operation
- The Rapid7 Nexpose engine
- The Rapid7 Metasploit engine

Requirements

Customer Credentials

- ClientK number from ControlCase
- Remote Management Key (RemoteID) from ControlCase
- root/sudo access to elevate permissions on the target machine

Hardware

- **CPU:** Quad Core
- **RAM:** 8 GB
- **Free Disk Space:** 100 GB (in /opt)

Operating System

- Ubuntu 18 LTS Server (Please do not install the desktop environment)
 - Fresh Installation (No unauthorized 3rd party software installed)
 - Root access to download and install the ControlCase software

Network Access

Direct internet access is required

NOTE: The use of a proxy to reach our remote management servers or the scan engine console is not supported at this time

If firewalls are present on your network, please ensure you allow access to the necessary network locations and ports as described here:

Source	Destination	TCP Port	Description
VAPT-SE	con.controlcase.com	443	Non-European ControlCase Remote Management
VAPT-SE	con-eu.controlcase.com	443	European ControlCase Remote Management
VAPT-SE	ccst.controlcase.com ccst1.controlcase.com ccst2.controlcase.com ccst3.controlcase.com ccst4.controlcase.com ccst5.controlcase.com ccst6.controlcase.com	443	Non-European Scan Engines Console NOTE: ControlCase will provide the console details that applies.
VAPT-SE	ccst-eu.controlcase.com	443	European ControlCase Scan Engine Console
VAPT-SE	download2.rapid7.com	80	Rapid7 Metasploit and Nexpose Installers
VAPT-SE	cs-api.controlcase.com	443	ControlCase API

NOTE: The installer will need to access the local Ubuntu repositories as defined in /etc/apt/sources to install software using the advanced package tool (apt)

NOTE: If you manually download and transfer the Rapid7 installers to the VAPT-SE machine you will not have to open the firewall to download2.rapid7.com

Installation

In this section we will discuss the installation of the VAPT-SE solution

This will install **all** the software defined in the [Software List](#), including the ControlCase Remote Management Agent.

Install

Syntax

```
./VAPT-SE.sh install --clientk <####> --remoteid '<RemoteID>'
```

NOTE: It is expected that the VAPT-SE.sh file is set to executable. If it is not, you may issue the command '**chmod +x VAPT-SE.sh**' to make it executable.

Example Output

```

  _____
 |  _   _  |  _   _  |  _   _  |  _   _  | | | | | | | | | | | | | | | |
 | | | | | | | | | | | | | | | | | | | |
 | |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
 [ Vulnerability Assessment and Penetration Testing ]
 [ Supplementary Tools Suite ]
 Version: 1.6506

[11:06:56 | DISTRO | Detected Ubuntu 18 ]
[11:06:56 | PREFLIGHT| Verifying apt status ]
[11:06:56 | PREFLIGHT| Verifying system RAM ]
[11:06:56 | PREFLIGHT| Verifying system disk space ]
[11:06:56 | PREFLIGHT| Verifying network connectivity ]
[11:06:57 | AGENT | Installing Remote Agent ]
[11:07:03 | SCREENRC | Shell is already defined in screenrc file ]
[11:07:03 | APT | Updating apt system repos ]
[11:07:09 | APT | Installing cryptcat ]
[11:07:18 | APT | Installing dnswalk ]
[11:07:24 | APT | Installing hping3 ]
[11:07:30 | APT | Installing httptunnel ]
[11:07:36 | APT | Installing nmap ]
[11:07:44 | APT | Installing sqlmap ]
[11:07:52 | BINARY | Installing dnsenum ]
[11:07:54 | BINARY | Installing snmpcheck ]
[11:07:56 | BINARY | Installing tlssled ]
[11:07:58 | APT | Installing wfuzz ]
[11:08:05 | KALI | Installing braa ]
[11:08:37 | KALI | Installing cisco-auditing-tool ]
[11:09:04 | KALI | Installing exploitdb ]
[11:09:52 | KALI | Installing firewalk ]
[11:10:21 | KALI | Installing nishang ]
[11:10:49 | KALI | Installing sidguesser ]
[11:11:17 | KALI | Installing smtp-user-enum ]
[11:11:44 | VALIDATE | Testing software packages ]
[11:11:44 | OK | braa appears to function ]
[11:11:44 | OK | cisco auditing tool appears to function ]
[11:11:44 | OK | crypcat appears to exist ]
[11:11:44 | OK | dnsenum appears to exist ]
[11:11:44 | OK | dnswalk appears to exist ]
[11:11:44 | OK | exploitDB appears to exist ]
[11:11:44 | OK | firewalk appears to function ]
[11:11:44 | OK | hping3 appears to function ]
[11:11:44 | OK | httptunnel appears to function ]
[11:11:44 | OK | nishang appears to exist ]
[11:11:44 | OK | nmap appears to function ]
[11:11:44 | OK | sidguesser appears to exist ]
[11:11:44 | OK | smtp-user-enum appears to function ]
[11:11:44 | OK | snmpcheck appears to function ]
[11:11:45 | OK | sqlmap appears to function ]
[11:11:45 | OK | tlssled appears to function ]
[11:11:45 | OK | wfuzz appears to function ]

```

Proinstall

The proinstall method will skip the apt-status verification, RAM allocation, free disk space allocation verification and the network connectivity verification steps as observed in the regular installation. This method should be used by experts or at the request of ControlCase support.

Syntax

```
./VAPT-SE.sh proinstall --clientk <#####> --remotid '<RemoteID>'
```

Example Output

```

  _____
 |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
 | |_| |_| | |_| |_| | |_| |_| | |_| |_| | |_| |_| | |_| |_| | |_| |_| | |_| |_| | |_| |_|
 |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  |
 |_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|
 [ Vulnerability Assessment and Penetration Testing ]
 [ Supplementary Tools Suite ]
 [ Version: 1.6506 ]

[10:59:27 | DISTRO | Detected Ubuntu 18 ]
[10:59:28 | AGENT | Installing Remote Agent ]
[10:59:33 | SCREENRC | Shell is already defined in screenrc file ]
[10:59:33 | APT | Updating apt system repos ]
[10:59:47 | APT | Installing cryptcat ]
[10:59:48 | APT | Installing dnswalk ]
[10:59:49 | APT | Installing hping3 ]
[10:59:50 | APT | Installing httptunnel ]
[10:59:51 | APT | Installing nmap ]
[10:59:52 | APT | Installing sqlmap ]
[10:59:52 | BINARY | Installing dnsenum ]
[10:59:54 | BINARY | Installing snmpcheck ]
[10:59:56 | BINARY | Installing tlssled ]
[10:59:58 | APT | Installing wfuzz ]
[11:00:06 | KALI | Installing braa ]
[11:00:32 | KALI | Installing cisco-auditing-tool ]
[11:00:53 | KALI | Installing exploitdb ]
[11:01:14 | KALI | Installing firewalk ]
[11:01:36 | KALI | Installing nishang ]
[11:01:58 | KALI | Installing sidguesser ]
[11:02:19 | KALI | Installing smtp-user-enum ]
```


Uninstallation

If you wish to uninstall the software, there are multiple methods:

Uninstall

This will only uninstall the ControlCase Remote Management Agent.

Syntax

```
./VAPT-SE.sh uninstall --clientk <####>
```

Example Output

```
ControlCase
[ Vulnerability Assessment and Penetration Testing ]
  [ Supplementary Tools Suite ]
    Version: 1.6506

[10:58:24 | AGENT | Uninstalling Remote Agent ]
Removed /etc/systemd/system/meshagent.service.
Removed /etc/systemd/system/multi-user.target.wants/meshagent.service.
```

Uninstallall

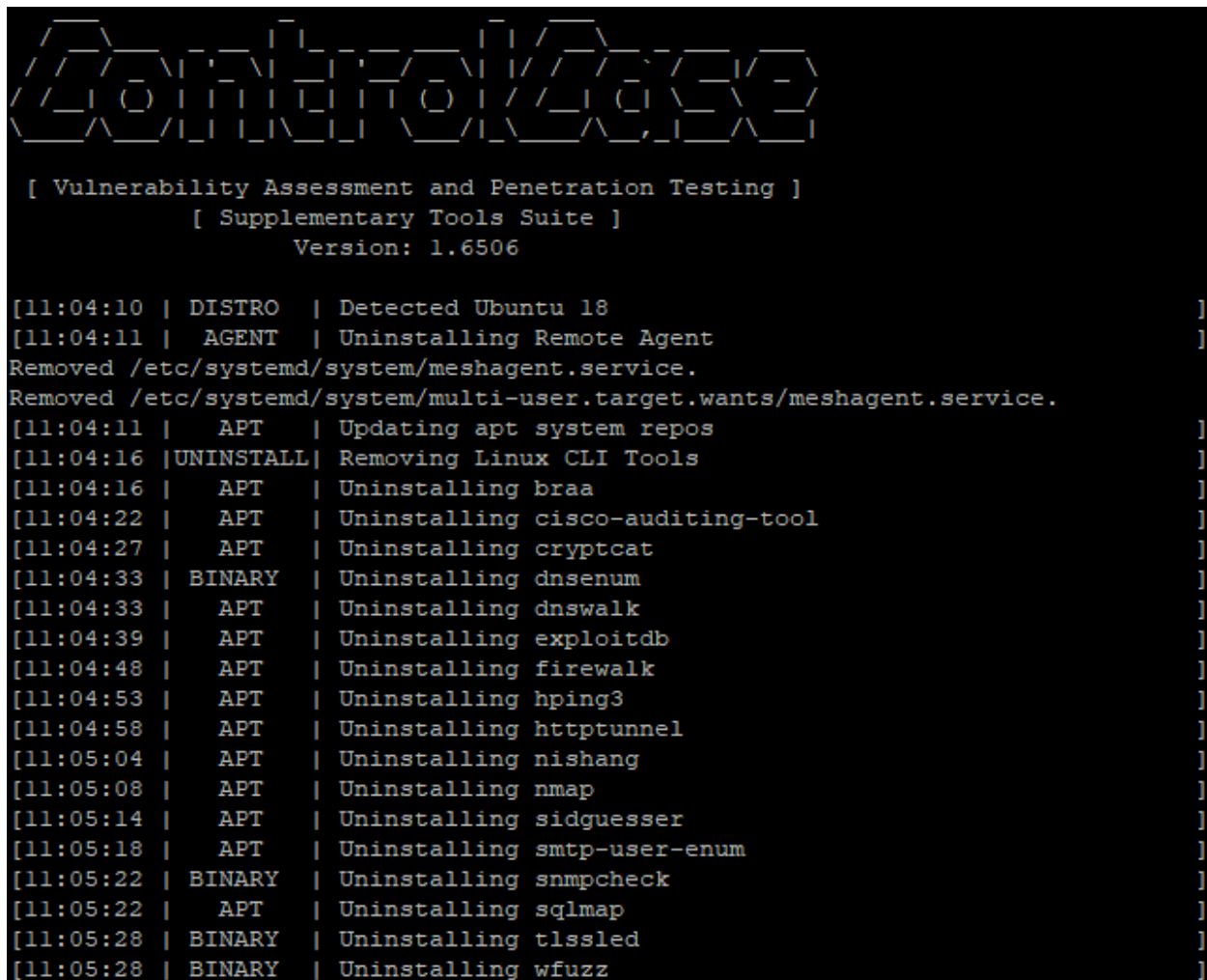
This will uninstall **all** the software defined in the [Software List](#) including the ControlCase Remove Management Agent

Syntax

```
./VAPT-SE.sh uninstallall --clientk <####>
```

NOTE: It is expected that the VAPT-SE.sh file is set to executable. If it is not, you may issue the command **'chmod +x VAPT-SE.sh'** to make it executable.

Example Output



```
[ Vulnerability Assessment and Penetration Testing ]
[ Supplementary Tools Suite ]
Version: 1.6506

[11:04:10 | DISTRO | Detected Ubuntu 18 ]
[11:04:11 | AGENT | Uninstalling Remote Agent ]
Removed /etc/systemd/system/meshagent.service.
Removed /etc/systemd/system/multi-user.target.wants/meshagent.service.
[11:04:11 | APT | Updating apt system repos ]
[11:04:16 | UNINSTALL | Removing Linux CLI Tools ]
[11:04:16 | APT | Uninstalling braa ]
[11:04:22 | APT | Uninstalling cisco-auditing-tool ]
[11:04:27 | APT | Uninstalling cryptcat ]
[11:04:33 | BINARY | Uninstalling dnsenum ]
[11:04:33 | APT | Uninstalling dnswalk ]
[11:04:39 | APT | Uninstalling exploitdb ]
[11:04:48 | APT | Uninstalling firewalk ]
[11:04:53 | APT | Uninstalling hping3 ]
[11:04:58 | APT | Uninstalling httptunnel ]
[11:05:04 | APT | Uninstalling nishang ]
[11:05:08 | APT | Uninstalling nmap ]
[11:05:14 | APT | Uninstalling sidguesser ]
[11:05:18 | APT | Uninstalling smtp-user-enum ]
[11:05:22 | BINARY | Uninstalling snmpcheck ]
[11:05:22 | APT | Uninstalling sqlmap ]
[11:05:28 | BINARY | Uninstalling tlssled ]
[11:05:28 | BINARY | Uninstalling wfuzz ]
```

Software List

Kali Packages

- braa
- cisco-auditing-tools
- exploitdb
- firewalk
- nishang
- sidguesser

Rapid7

- Nexpose
- Metasploit

Ubuntu Packages

- apt-transport-https
- cryptcat
- dnswalk
- hping3
- httptunnel
- nmap
- sqlmap
- wfuzz

Binary Packages

- dnsenum
- snmpcheck
- tlssled

Troubleshooting

If you are having issues with the solution, you can invoke the 'test' method which will run through the pre-flight checks to ensure that the RAM, free disk space and network target (con.controlcase.com) are **currently** reachable.

Syntax

```
./VAPT-SE.sh test
```

NOTE: It is expected that the VAPT-SE.sh file is set to executable. If it is not, you may issue the command 'chmod +x VAPT-SE.sh' to make it executable.

Example Output

```
ControlCase
[ Vulnerability Assessment and Penetration Testing ]
[ Supplementary Tools Suite ]
Version: 1.6506

[12:22:30 | DISTRO | Detected Ubuntu 18 ]
[12:22:30 | SCREENRC | Shell is already defined in screenrc file ]
[12:22:30 | PREFLIGHT| Verifying apt status ]
[12:22:30 | PREFLIGHT| Verifying system RAM ]
[12:22:30 | PREFLIGHT| Verifying system disk space ]
[12:22:30 | PREFLIGHT| Verifying network connectivity ]
[12:22:30 | PREFLIGHT| Restarting remote service ]
[12:22:40 | PREFLIGHT| Remote service status ]
● meshagent.service - MeshCentral Agent
   Loaded: loaded (/lib/systemd/system/meshagent.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-10-20 12:22:30 EDT; 10s ago
   Main PID: 23875 (meshagent)
   Tasks: 2 (limit: 503)
   CGroup: /system.slice/meshagent.service
           └─23875 /usr/local/mesh/meshagent

Oct 20 12:22:30 ubuntu-18-04LTS systemd[1]: Stopped MeshCentral Agent.
Oct 20 12:22:30 ubuntu-18-04LTS systemd[1]: Started MeshCentral Agent.
[12:22:40 | VALIDATE | Testing software packages ]
[12:22:40 | OK | braa appears to function ]
[12:22:40 | OK | cisco auditing tool appears to function ]
[12:22:40 | OK | crypcat appears to exist ]
[12:22:40 | OK | dnsenum appears to exist ]
[12:22:40 | OK | dnswalk appears to exist ]
[12:22:40 | OK | exploitDB appears to exist ]
[12:22:40 | OK | firewall appears to function ]
[12:22:40 | OK | hping3 appears to function ]
[12:22:40 | OK | httptunnel appears to function ]
[12:22:40 | OK | nishang appears to exist ]
[12:22:40 | OK | nmap appears to function ]
[12:22:40 | OK | sidguesser appears to exist ]
[12:22:40 | OK | smtp-user-enum appears to function ]
[12:22:40 | OK | snmpcheck appears to function ]
[12:22:41 | OK | sqlmap appears to function ]
[12:22:41 | OK | tlsled appears to function ]
[12:22:41 | OK | wfuzz appears to function ]
```

NOTE: Please include the ~/VAPTSE-Install.log file if you encounter any issues.