



0898601-8.4-5 December 2024 Copyright 2024 by Concurrent Real-Time, Inc. All rights reserved. This publication or any part thereof is intended for use with Concurrent Real-Time products by Concurrent Real-Time personnel, customers, and end-users. It may not be reproduced in any form without the written permission of the publisher.

The information contained in this document is believed to be correct at the time of publication. It is subject to change without notice. Concurrent Real-Time makes no warranties, expressed or implied, concerning the information contained in this document.

To report an error or comment on a specific portion of the manual, photocopy the page in question and mark the correction or comment on the copy. Mail the copy (and any additional comments) to Concurrent Real-Time, 800 NW 33rd Street, Pompano Beach, Florida 33064. Mark the envelope **"Attention: Publications Department**." This publication may not be reproduced for any other reason in any form without written permission of the publisher.

Concurrent Real-Time and its logo are registered trademarks of Concurrent Real-Time, Inc. All other Concurrent Real-Time product names are trademarks of Concurrent Real-Time while all other product names are trademarks or registered trademarks of their respective owners. Linux® is used pursuant to a sublicense from the Linux Mark Institute.

Printed in U. S. A.			
Revision	n History:	Level:	Effective With:
Novemb	per 2008	000	RedHawk Linux 5.1
January	2009	100	RedHawk Linux 5.2
Februar	y 2009	200	RedHawk Linux 5.2
July 200)9	300	RedHawk Linux 5.2
October	2009	400	RedHawk Linux 5.2
July 201	10	600	RedHawk Linux 5.4
October	2011	700	RedHawk Linux 6.0
April 20)12	720	RedHawk Linux 6.0
Decemb	per 2012	800	RedHawk Linux 6.3
July 201	13	900	RedHawk Linux 6.3
Septemb	ber 2013	92	RedHawk Linux 6.3
Februar	y 2014	930	RedHawk Linux 6.3
August	2014	940	RedHawk Linux 6.5
Septemb	ber 2014	950	RedHawk Linux 6.5
October	2014	960	RedHawk Linux 6.5
May 20	15	7.0	RedHawk Linux 7.0
August	2015	7.0-1	RedHawk Linux 7.0
June 20	16	7.2	RedHawk Linux 7.2
Decemb	per 2016	7.2-1	RedHawk Linux 7.2
August	2017	7.2-2	RedHawk Linux 7.2
October	2017	7.3	RedHawk Linux 7.3
April 20)18	7.3-1	RedHawk Linux 7.3
Septemb	ber 2018	7.5	RedHawk Linux 7.5
March 2	2019	7.5-1	RedHawk Linux 7.5
June 202	20	8.0	RedHawk Linux 8.0
June 202	21	8.2	RedHawk Linux 8.2
March 2	2022	8.4	RedHawk Linux 8.4
June 202	22	8.4-1	RedHawk Linux 8.4
June 202	22	8.4-1a	RedHawk Linux 8.4
Septemb	ber 2022	8.4-2	RedHawk Linux 8.4
June 202	23	8.4-3	RedHawk Linux 8.4
July 202	24	8.4-4	RedHawk Linux 8.
Decemb	per 2024	8.4-5	RedHawk Linux 8.4

Scope of Manual

This manual describes the RedHawk Architect[™], an easy-to-use GUI interface for creating and maintaining a runtime and development environment for a target computer.

Structure of Manual

This manual consists of:

- Chapter 1, which introduces you to RedHawk Architect and guides you through its use.
- Chapter 2, which explains how to use the security extension of the Advanced Security Edition of Architect.
- Chapter 3, which explains Importing ISO Images to avoid repetitive manual optical media insertion.
- Chapter 4, which explains PXE Management.
- Appendix A explains Manual DHCP configuration for Architect PXE targets.
- Appendix B lists the python scripts that can be used to perform some of the functions provided by the GUI.
- An index in the back of the book containing an alphabetical reference to key terms and concepts and the pages where they occur in the text.

Syntax Notation

The following notation is used throughout this manual:

italic	Books, reference cards, and items that the user must specify appear in <i>italic</i> type. Special terms may also appear in <i>italic</i> .
list bold	User input appears in list bold type and must be entered exactly as shown. Names of directories, files, commands, options and man page references also appear in listbold type.
list	Operating system and program output such as prompts, messages and listings of files and programs appears in list type.
[]	Brackets enclose command options and arguments that are optional. You do not type the brackets if you choose to specify these options or arguments.
hypertext links	When viewing this document online, clicking on chapter, section, figure, table and page number references will display the

corresponding text. Clicking on Internet URLs provided in blue type will launch your web browser and display the web site. Clicking on publication names and numbers in red type will display the corresponding manual PDF, if accessible.

Related Publications

The following table lists Concurrent Real-Time documentation for RedHawk Architect and the components that can be installed using RedHawk Architect. Depending upon the document, they are available online on RedHawk Linux systems or from Concurrent Real-Time's documentation web site at http://redhawk.concurrent-rt.com/docs.

RedHawk Architect	Pub. Number
RedHawk Architect Release Notes	0898600
RedHawk Architect User's Guide	0898601
RedHawk Linux	
RedHawk Linux Release Notes	0898003
RedHawk Linux User's Guide	0898004
RedHawk Linux FAQ	N/A
NightStar RT Development Tools	·
NightView User's Guide	0898395
NightTrace User's Guide	0898398
NightProbe User's Guide	0898465
NightTune User's Guide	0898515

Contents

Preface	iii

Chapter 1 Using RedHawk Architect

Introducing Architect	1-1
Creating a root File System for Target Systems	1-2
Running Architect.	1-2
Creating a New Session	1-5
Selecting Software to Install in the Image	1-6
Selecting Base Distribution Linux Packages	1-6
Using the Base Environments View.	1-7
Using the Categories and Groups View	1-8
Using the All Packages View	1-9
Using the Selected Packages View.	1-10
Selecting RedHawk OS Options	1-11
Selecting NightStar Options	1-13
Configuring an Image	1-14
Configuring General Settings	1-14
Configuring a Console	1-16
Configuring Networking	1-17
Configuring File Systems	1-19
Simple Disk Partitioning	1-21
Advanced Disk Partitioning	1-22
Default File System Configuration	1-22
Optional File System Configurations	1-24
Example Using Optional Configurations	1-24
Steps in Configuring Additional Logical Volumes (LVM)	
Example Configuring Logical Volumes (LVM)	1-27
Redundant Array of Independent Disks (RAID)	1-29
Steps in configuring a RAID	1-29
Example System Configuration Using RAID Partitions	1-30
Example RAID Using Whole Disks	1-38
Example Configuration Using multiple RAID levels	1-40
Read-Only Root Configuration	1-42
Configuring Special File Systems (tmpfs, bind)	
Configuring SELinux	1-44
Building an Image	1-44
Customizing an Image	1-48
Software Updates	1-49
Additional RPMs	1-50
Installing Board Support Packages.	1-51
System Services	1-51
Kernel	1-52
Configure Custom Kernel.	1-53
Import Kernel Configuration	1-55
Export Kernel Configuration	1-56
Compile Custom Kernel	1-56
Remove Custom Kernel	1-58

File Manager 1	1-58
Chroot Shell 1	-59
Image Cleanup 1	-60
Deploying an Image 1	-61
Deploying to USB Devices 1	1-62
Installing via USB drive 1	1-65
Installing via Disc media 1	L-69
Installing via PXE over a Network 1	1-71
Booting Diskless via PXE over a Network 1	1-73
Remote Sync 1	l-78
Deploying to Virtual Machine 1	1-83
Editing an Existing Session 1	-84

Chapter 2 Security Extensions

UEFI Secure Boot.	2-1
Configuring SELinux	2-2
Customizing the kernel with FIPS	2-4
Security Content Automation Protocol (SCAP)	2-6
Introduction to SCAP	2-6
Understanding SCAP Evaluation and Remediation Scans	2-7
SCAP System Requirements	2-7
SCAP Workflow	2-8
Workflow Overview	2-8
1. Configure SCAP security policy	2-9
2. Build the target system image	2-12
3. Customize the target image	2-12
4. Run post-deploy scans	2-14
Remotely from Architect.	2-14
Remotely via ssh	2-16
Directly from console	2-17
Customizing SCAP Content Using SCAP Workbench	2-17

Chapter 3 Importing ISO Images

Importing ISO Images	3-1
Importing ISO Images From Optical Media	3-2
Copying ISO Images From Existing ISO Images	3-3
Linking To Existing ISO Images.	3-4
Deleting Imported ISO Images	3-5

Chapter 4 PXE Management

Enabling PXE on Targets	4-1
Initializing PXE Services	4-1
Managing PXE Images	4-3
PXE Diskless Images.	4-6
Managing PXE Targets	
Adding Targets	
Adding Single Targets	4-8
Adding Multiple Targets	4-9
Removing Targets	4-11
Editing Targets	4-11

Appendix A	Manual DHCP Configuration	A-1
	Overview Installing DHCP Configuration	
Appendix B	Command Line Interface	B-1
Index	Ind	dex-1

RedHawk Architect User's Guide

This chapter introduces you to RedHawk Architect and provides instructions for its use.

Introducing Architect

RedHawk Architect is a powerful tool with an easy-to-use GUI that lets a developer choose the Linux and application modules to be included in RedHawk target images.

Designed to scale from complete workstations to dedicated servers and even down to small embedded applications, users can select as few or as many packages as desired from many different package groups. Architect allows the file system to be customized using as much or as little space as desired.

Architect saves all the configuration choices made by the user in the session file. Architect processes the session file to create and configure the target system image by installing all necessary RPM packages and dependencies and making the desired configuration changes. Packages are installed from system installation media which may be saved on the host system as ISO images.

After building the target system image, Architect allows customization of the target system image and also the RedHawk kernel itself.

Architect provides several deployment methods for installing the target system image onto the target system hard drives and/or flash memories. Architect can boot diskless targets with a target system image. It can also build virtual machine images of target system images for use with QEMU/KVM, allowing complete target system images to be deployed without a physical target.

Architect's PXE target manager makes it simple for users to install and configure systems as highly-integrated, high-performance computing clusters. Architect uses PXE to remotely install any number of targets over a network and also for diskless-booting multiple nodes with the same version of RedHawk.

Architect greatly simplifies the following tasks to create and maintain a target system's runtime and development environment:

- installing custom configurations of the RockyTM, CentOS[®] or Red Hat[®] Enterprise Linux distribution
- installing and configuring the RedHawkTM operating system
- installing target-specific board support packages (BSPs)
- installing NightStarTM RT application development tools
- installing RedHawk and NightStar software updates
- maintaining and reconfiguring a target root file system and kernel

• deploying target system images onto target systems or virtual machines

Creating a root File System for Target Systems

To create a target system image, use RedHawk Architect on a supported host system to perform the following steps:

- 1. Select the software to install in the image.
- 2. Configure the image.
- 3. Customize the image for your application.
- 4. Deploy the image on your target boards or to virtual machines.

These procedures are described in the sections that follow. The steps may be repeated to change the image and/or deploy it any number of times.

Running Architect

For instructions on installing RedHawk Architect, refer to the *RedHawk Architect Release* Notes.

Architect must be run as the root user. Note that the **sudo (8)** command can alternatively be used to run Architect.

You can start Architect from the command line or it can be launched from the GNOME or MATE desktop environments as follows:

- as root user, command line: # architect
- as non-root user, command line: # sudo -E architect
- 3. for GNOME and MATE desktops environments: from the desktop's applications launcher search for Architect and click on it. If you are not logged in as the root user, you will be prompted for a password.

The very first time Architect is invoked after it is installed, a dialog appears presenting you with the Concurrent Real-Time End User Agreement.

Scroll down and press the Accept button to continue.

	End User Agreement	,
Λ	RedHawk Architect 8.2	
	Please read the following End User Agreement and click the Accept button if you agree to the terms.	ş
Agreement,	shall survive the termination or expiration of this Agreement.	ľ
its obliga or resulti not restri enemy, fir strike, fr weather, a the date b (other tha	URE. Neither party shall be liable for delays in performance of tions hereunder (other than payment obligations) arising out of ng from causes beyond its control. Such causes include, but are cted to, acts of God, any government authority, or the public es, floods, terrorism, epidemics, quarantine restrictions, eight embargoes, shortages of materials, unusually severe nd default or delay of suppliers. In the event of such delay, y which performance of any such obligation hereunder is required n payment obligations) shall be extended for a period equal to ost by reason of the delay.	l
	y failure or delay in exercising any right or remedy by either not be deemed a waiver of any further, prior, or future right hereunder.	
you desire CONCURRENT	hould you have any questions concerning this Agreement, or if to contact CONCURRENT for any reason, please contact the REAL-TIME subsidiary serving your country, or write: CONCURRENT 800 NW 33rd Street, Pompano Beach, Florida 33064.	
this Agree conditions	EMENT. By using the PRODUCTS, you acknowledge that you have read ment, understand it, and agree to be bound by its terms and . Should you have any questions concerning this Agreement, NCURRENT, at the above stated address.	
(C)2020 Concur	rent Real-Time. All rights reserved.	
4		
	Reject Ackep	t

Figure 1-1 Architect End User Agreement

When Architect starts, a dialog appears presenting you with the option to start a new session or load an existing session.



Figure 1-2 Opening RedHawk Architect Dialog

To start a new session, click on the New button. See "Creating a New Session" on page 1-5 for details.

A session can be saved at any time and loaded later to continue work on the target system image. To edit an existing session, click on the Open button. See "Editing an Existing Session" on page 1-84 for details.

When the Cancel button is clicked, the RedHawk Architect main window appears, as shown in the following figure.

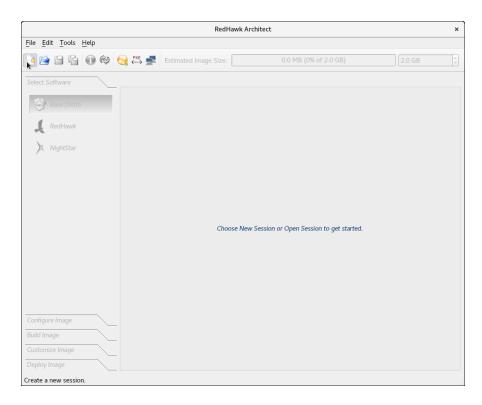


Figure 1-3 RedHawk Architect Main Window

From this window, the most common tasks performed are:

- start a new session by clicking on the New Session icon or selecting New Session from the File menu along the top of the window. See "Creating a New Session" on page 1-5 for details.
- edit an existing session by clicking on the Open Session icon icon selecting Open Session in the File menu. See "Editing an Existing Session" on page 1-84 for details.

At this time you may also select your directory default preferences by selecting Preferences in the Edit menu. These defaults avoid having to enter a directory path each time.

The Default session directory is where you will find the session files created by Architect. The Default image directory is where the target system images are created. The Default VM directory and the Default ISO directory are the directories where, respectively, the virtual machine images and the disc installer ISO images are saved.

The following figure shows the default User Preferences settings:

User Preferences		
Directories Notices	Packages	
Default session directory:	/root/Documents)
Default image directory:	/var/lib/architect/images)
Default VM directory:	/var/lib/architect/VMs)
Default ISO directory:	/root	•
Temporary directory:	/var/tmp	•
	Cancel	₩

Figure 1-4 User Preferences Page

If space is limited in your **/root** partition, you will want to change your defaults to a partition with more available disk space. In the following example, the default settings were changed to reside in the **/home/architect** directory.

	User Preferences	×
Directories Notices	Packages	
Default session directory:	/home/architect/sessions	•
Default image directory:	/home/architect/images	•
Default VM directory:	/home/architect/VMs	•
Default ISO directory:	/home/architect/ISOs	•
Temporary directory:	/var/tmp	•
	Cancel	¢₽ОК

Figure 1-5 User Preferences Modified

Creating a New Session

An Architect session file is used to store all the configuration choices for a target. It also contains data about recent deployments.

When you select the New button from the opening Architect dialog, or the New Session icon or New Session from the File menu along the top of the RedHawk Architect main window, the New Session dialog, shown below, displays.

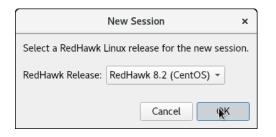


Figure 1-6 New Session Dialog

This dialog enables you to specify the version of RedHawk and the base distribution to be used for creating the target system image. Be sure that you have the correct version of the RedHawk and either the Rocky, CentOS or Red Hat Enterprise Linux media (or ISO files) necessary to create a target system image of the specified RedHawk release.

Selecting Software to Install in the Image

To select the software to install in the target system image, click on Select Software from the toolbox on the left side of the RedHawk Architect main window. This allows you to select software from the following three groups:

- Base Distribution Linux packages
- RedHawk Linux operating system
- NightStar tools

Some initial selections are made for you by default; e.g. the core RedHawk OS. These packages appear with a gray check mark and cannot be deselected.

The Estimated Image Size gauge at the top of the RedHawk Architect main window indicates the approximate size the target system image will be when built. It also indicates the percentage of the target board's root device that will be consumed by the image.

Once an image is built, you may click on the interval Refresh Image Size button to calculate the actual image size as it is stored on disk. Alternatively, you may select Refresh Image Size from the Tools menu. The Estimated Image Size gauge will be updated to reflect the *current* actual size.

The spin control box to the right of the Estimated Image Size gauge may be used to change the desired maximum size of the image. This value cannot exceed the known size of the root device but it can be made smaller. If the size of the root device is unknown the maximum value allowed is 1 terabyte.

Selecting Base Distribution Linux Packages

To select Rocky, CentOS or Red Hat packages for the target system image, click on the Base Distro selection from the Select Software toolbox.

Rocky, CentOS or Red Hat packages may be navigated by way of the "Package View" drop down menu on the top right hand of the page. Select the desired package view from the Package View menu. The following views are available and are described in the subsections that follow.

- Base Environments
- Categories and Groups
- All Packages
- Selected Packages

Note that the Base Environments view will be initially selected; a base package environment must be chosen before the other package views will become available.

Note that the following features are available in all the views except for the Base Environments view:

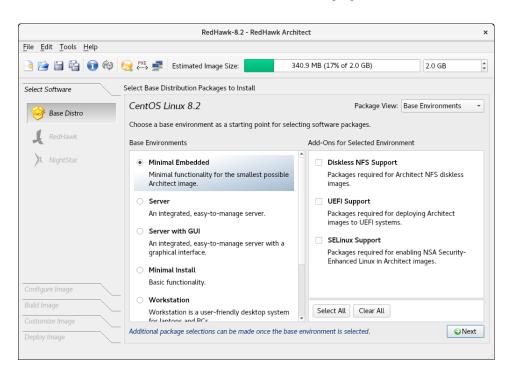
- The Undo button can be used to reverse the last package select or package deselect operation. This can be used repeatedly to reverse several operations if desired, which is useful for experimenting with package sets to see the effect on the estimated image size.
- To get more information about a package, right-click to display a menu of options. Multiple packages can be processed as a group by highlighting the packages and then right-click to display the menu of options. When choosing the select or deselect menu options, software dependent on the highlighted packages will be automatically selected or deselected. The figure below shows two packages selected as a group.

nstall	Package	Size (KB)	I	Description			
V	efibootmgr	92	EFI Boot Manager (optional)				
	gdisk	894	894 An fdisk-like partitioning tool for GPT disks (optional)				
	grub2-efi-x64	1734	GRUB for EFI systems.				
	shim-x64	🛃 Sele	ct Package(s)				
		Des	elect Package(s)				
		🗊 Get					
		😌 Sho	w Package Dependencies				

Figure 1-7 Selecting Multiple Packages

Using the Base Environments View

The Base Environments view requires the user to choose a high-level task-based characterization of the Rocky, CentOS or Red Hat packages that will be initially selected. This view should be very familiar to users that have previously performed a native Rocky,



CentOS or Red Hat installation; it is shown in the following figure.

Figure 1-8 Choosing Target Characterization, Base Environments View

For example, if the target will primarily be used to run a web server, choose the Server or Server GUI environment. Note that the set of base environments available may be different depending on the current session's distribution type and revision.

To see more information about a particular environment, click on the Get Environment Info button that is displayed when you place the cursor over the environment and right-click.

Once a Base Environment has been chosen, a list of corresponding optional package groups will be displayed in the Add-Ons for Selected Environment area. You can choose these package groups individually or press the Select All and Clear All buttons to affect all optional package groups at once.

After you have chosen the desired base environment and associated optional packages, press the $N \oplus X^{\dagger}$ button at the lower right to add all of the corresponding packages to the session and enable the other package views for further package customization.

Using the Categories and Groups View

The Categories and Groups view provides a view of Rocky, CentOS or Red Hat packages organized in a hierarchy of groups. The package group hierarchy is the standard Rocky, CentOS or Red Hat package group hierarchy. This view is shown in the following figure.

			RedHawk	<-8.2 - R€	dHawk Architect			>	
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp									
) 😭 🗎 🔓 🐑	🛛 😥 🖓	Estimated	Image Si	ize:	665.3 MB	(33% of 2.0 GB)	2.0 GB	÷	
Select Software	Select Bas	se Distribution P	'ackages t	to Install					
😝 Base Distro	CentC	S Linux 8.2				Package	View: Categories and Group	s Ŧ	
	Archit	ect System	Servers	5 Desk	tops Applications	Development			
RedHawk		Group			ſ	Description		-	
ALL LIG	Archite	ect Core	The min	imal set (of packages required f	or all Architect ima	ges.		
X NightStar	Diskles	Diskless NFS Support Packages required for Architect NFS diskless images.						11	
	UEFI S	UEFI Support Packages required for deploying Architect images to UEFI systems.					Н		
	SELinu	SELinux Support Packages required for enabling NSA Security-Enhanced Linux in Architect images.					-		
	Architec	t Core:				✓Select All Group	ups 🖋 Select All Categori	es	
	Install	Package	S	Size (KB)		Description	n	-	
		NetworkManag	jer	6568	Network connection r	manager and user a	pplications		
		basesystem		0	The skeleton package	which defines a sir	mple centos system		
		bash		6930	The GNU Bourne Agai	in shell			
Configure Image		coreutils		6115	L5 A set of basic GNU tools commonly used in shell scripts				
Build Image		dracut-config-	generic	0	0 dracut configuration to turn off hostonly image generation				
Customize Image	Ref.	e2fsproas		4343	Utilities for managing	ext2. ext3. and ext	4 file systems	Ŧ	
Deploy Image	Type Ctr	1-F or / to search	h for pack	ages in g	roup.	25 packages	✓Select Group	do	

Figure 1-9 Selecting Base Distro Packages, Categories and Groups View

Packages may be selected or deselected by choosing a package group in the upper pane and then checking or unchecking packages in that group in the lower pane. All the packages in a chosen group may be selected with the Select Group button.

All the packages that are in all the groups of the currently chosen package category may be selected with the Select All Groups... button. Also, the Select All Categories... button may be used to select all of the packages in all of the groups of all of the categories.

Using the All Packages View

The All Packages view provides a sorted linear list of all Rocky, CentOS or Red Hat packages.

ieie Edit Tools Help ieie Edit Tools Help ieie Edit Tools Help ieieect Software Select Base Distribution Packages to Install CentOS Linux 8.2 Package View: All Package Size (KB) Description Install Package Size (KB) Description Install Package Size (KB) Description Install Package Size (KB) Description CUnit 132 GConf2 (686) 6679 GConf2 (666) 6679 A process-transparent config HdrHistogram 156 Judy 472 General purpose dynamic arr LibRaw 1997 LibRaw 1997 ModemManager 3410	
elect Software Select Base Distribution Packages to Install Select Base Distribution Packages to Install CentOS Linux 8.2 Package View: All Package Filter packages by name: * Install Package Size (KB) Description CUnit (i686) 135 Unit testing framework for C CUnit 132 Octor 2 (i686) 66679 A process-transparent config HdrHistogram 156 HdrHistogram 156 Judy 472 General purpose dynamic arrow LibRaw (i686) 2027 Libraw 1997	
State CentOS Linux 8.2 Package View: All Package View: All Package View: All Package View: All Package Size (KB) Install Package Size (KB) Description Cunit 135 Unit testing framework for C C Cunit 132 Unit testing framework for C C GConf2 (i686) 6679 A process-transparent config HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram 156 A High Dynamic Range (HDR) Judy 472 General purpose dynamic arrow LibRaw (i686) 2022 Library for reading RAW files	2.0 GB
We base Distro Filter packages by name: * Install Package Size (KB) Description CUnit (i686) 135 Unit testing framework for C CUnit 132 Unit testing framework for C GConf2 (i686) 6679 A process-transparent config HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic array LibRaw (i686) 2027 Library for reading RAW files	
Install Package Size (KB) Description CUnit (i686) 135 Unit testing framework for C CUnit 132 Unit testing framework for C GConf2 (i686) 6679 A process-transparent config HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arrow LibRaw (i686) 2022 Library for reading RAW files	kages
Install Package Size (RB) Description NightStar CUnit (i686) 135 Unit testing framework for C CUnit CUnit 132 Unit testing framework for C GConf2 (i686) 6679 A process-transparent config HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arrow LibRaw (i686) 2022 Library for reading RAW files	
NightStar CUnit 132 Unit testing framework for C GConf2 (i686) 6679 A process-transparent config HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arrow LibRaw (i686) 2027 Library for reading RAW files	
CUnit 132 Unit testing framework for C GConf2 (i686) 6679 A process-transparent config HdrHistogram 56 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arra LibRaw (i686) 2027 Library for reading RAW files Library for reading RAW files 1997 Library for reading RAW files	
GConf2 6660 A process-transparent config HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arra LibRaw (1686) 2027 Library for reading RAW files LibRaw 1997 Library for reading RAW files	
HdrHistogram 156 A High Dynamic Range (HDR) HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arra LibRaw (1686) 2027 Library for reading RAW files LibRaw 1997 Library for reading RAW files	uration system
HdrHistogram-javadoc 2889 Javadoc for HdrHistogram Judy 472 General purpose dynamic arra LibRaw (I686) 2027 Library for reading RAW files LibRaw 1997 Library for reading RAW files	uration system
Judy 472 General purpose dynamic array LibRaw (i686) 2027 Library for reading RAW files LibRaw 1997 Library for reading RAW files) Histogram
LibRaw (i686) 2027 Library for reading RAW files LibRaw 1997 Library for reading RAW files	
LibRaw 1997 Library for reading RAW files	ay
	obtained from
ModemManager 3410 Mobile broadband modem ma	obtained from
	anagement
ionfigure Image ModemManager-glib (i686) 1252 Libraries for adding ModemM	lanager support
wild Image ModemManager-glib 1187 Libraries for adding ModemM	lanager support
Sustomize image	
Deploy Image Type Ctrl-F or / to search for packages. 6603 packa	ages 🔍 Undo

The following figure shows the All Packages view.

Figure 1-10 Selecting Base Distro Packages, All Packages View

Packages may be selected or deselected from this list. The Filter packages by name box allows you to search for packages by name.

All packages can be selected by clicking on the Select All Packages button.

Using the Selected Packages View

The Selected Packages view provides a sorted linear list of all Rocky, CentOS or Red Hat packages that are currently selected for installation.

		RedHawk-8.2 -	RedHawk A	rchitect		;
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp						
è 📔 🖺 📦	Mark Constraints (Estimated Image Size:		665.3 MB (33% of 2.0 GB)	2.0 GE	3
Select Software	Select Ba	se Distribution Packages to Inst	all			
Base Distro	Cent	OS Linux 8.2		Package View:	Selected Pack	kages 👻
	<u> </u>	required packages		Filter packages by name: .*		
📕 RedHawk	Install	Package	Size (KB)	Description		
X NightStar	gmp 1678 A GNU arbitrary precision		A GNU arbitrary precision library	sion library		
Nightstar		gnupg2	9632	Utility for secure communication and	data storage	
		gnutls	2687	A TLS protocol implementation		
		gpgme	741	GnuPG Made Easy - high level crypto	API	
		grep	835	Pattern matching utilities		
		grub2-common	5041	grub2 common layout		
		grub2-pc	0	Bootloader with support for Linux, M	lultiboot, and n	nore
		grub2-pc-modules	2887	Modules used to build custom grub i	mages	
		grub2-tools	9196	Support tools for GRUB.		
		grub2-tools-extra	6583	Support tools for GRUB.		
Configure Image	-	grub2-tools-minimal	768	Support tools for GRUB.		
Build Image		grubby	64	Command line tool for updating Boo	tLoaderSpec fil	.es
Customize Image	_	i-	400	The CAUL data commenced and and and		-
Deploy Image	Type Ct	rl-F or / to search for packages.		21	.1 packages	€Undo

The figure below shows the Selected Packages view.

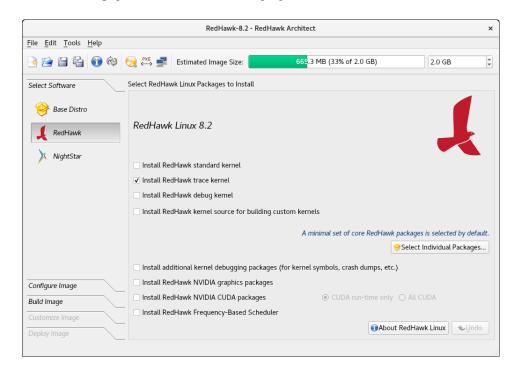
Figure 1-11 Selecting Base Distro Packages, Selected Packages View

Packages may be deselected from this list. The Filter packages by name box allows you to search for packages by name.

To exclude the required packages from the list, check the Hide required packages check box. When this box is checked, only the optional packages are shown.

Selecting RedHawk OS Options

To select RedHawk Linux OS and kernels for the target system image, click on the RedHawk selection from the Select Software toolbox.



The RedHawk page is shown in the following figure.

Figure 1-12 Selecting RedHawk Options

Select which RedHawk kernel(s) to install by checking the appropriate check box(es): Standard, Trace and/or Debug. The standard kernel does not have tracing or debugging capabilities and it is the smallest sized kernel option. The trace kernel does offer tracing capabilities but it does not have debugging capabilities. The debug kernel offers both debugging and tracing capabilities. Note that at least one kernel *must* be selected; the GUI enforces this by ensuring that a sole remaining selection cannot be deselected.

Select Install RedHawk kernel source for building custom kernels to ensure that the complete kernel source code will be installed in the image. The kernel source is only required for building custom kernels and loadable kernel drivers.

Advanced users may wish to press the Select Individual Packages... button to refine exactly which RedHawk packages they wish to install from the complete set of RedHawk packages that are available on the media. Normally this is not necessary, but the option exists to facilitate minimizing the image size for very small flash devices.

Select Install additional kernel debugging packages to install extra support for live kernel debugging. This option is also required for RedHawk to be able to create crash dumps. See the *RedHawk User's Guide* for more information.

If the target system has an NVIDIA graphics or CUDA card you may want to select the Install RedHawk NVIDIA graphics packages and Install RedHawk NVIDIA CUDA packages radio buttons. Note that you should only select this option if the target system actually has NVIDIA hardware. If you select the NVIDIA CUDA option, then you will be allowed to choose all the CUDA software or only run-time software.

Select Install Frequency-Based Scheduler if you have previously purchased and wish to install the RedHawk FBS software into the target image.

Selecting NightStar Options

To select NightStar tools for the image, click on the NightStar selection from the Select Products toolbox. The NightStar RT page, shown in the following figure, displays.

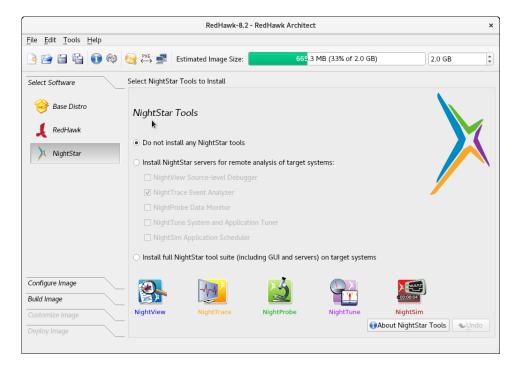


Figure 1-13 Selecting NightStar Tools

By default no NightStar tools will be installed in the target image. Choose the Install select NightStar servers only radio button if you wish to only install NightStar remote support for various tools. You may select individual servers from the list by clicking on the check boxes for each tool. The remote support allows NightStar tools running on a host system to connect to and control the target remotely.

Choose the Install all NightStar clients and servers radio button to indicate that all NightStar servers and clients are to be installed in the image. This allows the target to run all NightStar tools locally, in addition to providing the remote support described above.

Click on the About NightStar button to see a detailed description of each of the individual NightStar tools that are available for installation.

Configuring an Image

It is possible to configure a target system image before or after the image has been built by selecting Configure Image from the toolbox on the left side of the RedHawk Architect main window. This selection is available before and after an image is built, however note that there are additional Apply buttons present on the pages *after* an image has been built. It is necessary to apply any changes made after the image has been built in order for the changes to be reflected in the on-disk target system image.

To configure the target system image, select Configure Image from the toolbox on the left side of the RedHawk Architect main window. This allows you to configure the following four groups:

- General Settings
- Console
- Networking
- File Systems
- SELinux

Some initial selections are made for you by default.

Configuring General Settings

To configure time zone, root password and default system run level for the target system image, click on General Settings from the Configure Image toolbox.

	RedHawk-8.2	- RedHawk Architect	×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp			
	Estimated Image Size:	665.3 MB (33% of 2.0 GB) 2.0 GB	-
Select Software	Configure General Settings		
Configure Image			
General Settings	Time Zone: America/New York ✓ Hardware clock is set to UTC	•	
Console			
Networking	Root Password: •••••• Confirm Password: ••••••	Q	
Eile Systems	System Run Level: 3 Multi-user		
SELinux			
Build Image			
Customize Image			
Deploy Image			

The General Settings configuration page appears, as shown in the following figure.

Figure 1-14 General Settings Configuration Page

In the Time Zone section, select the proper time zone for your location from the dropdown menu. Click in the check box to indicate if your system clock uses UTC.

NOTE

By default the Hardware clock is set to UTC check box is selected, so be sure to set the target system's BIOS clock in Coordinated Universal Time. If you do not select this, set the BIOS clock according to the selected time zone.

In the Root Password section, enter the root password in the Password field. Reenter it in the Confirm Password field.

The Root Password is hashed and the hash value is saved in the session file. The actual password is not saved.

NOTE

The default root password is redhawk (all lowercase letters and only one word with no spaces).

In the System Run Level section, select the desired default run level from the dropdown menu. If a change is made to the general settings after the target system image has been built, an *Out-of-Sync Notice* will appear at the bottom of the page, as shown in the following figure:



Figure 1-15 General Settings and Image Out-of-Sync Notice

The appearance of an Out-of-Sync Notice on any page indicates that the settings currently displayed in the session do not match the state of the associated target image. Click on Show Differences to see which settings are currently out-of-sync. To resolve the issue, it is necessary to either click on Update Image or Update Session.

The Update Image button will apply the currently displayed settings to the target image, whereas the Update Session button will change the currently displayed settings to match the state of the target image. The Out-of-Sync Notice will disappear once an update direction has been selected.

Configuring a Console

To configure a serial console for the target system image, click on Console from the Configure Image toolbox.

The Configure Console page appears, as shown in the following figure.

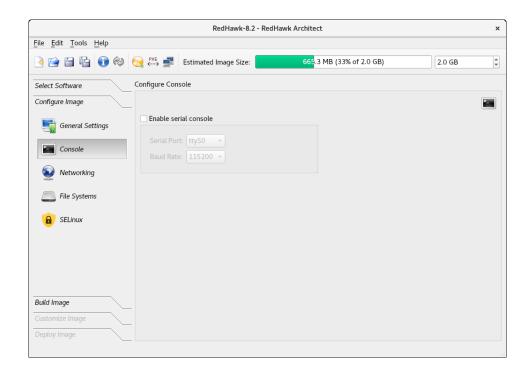


Figure 1-16 Console Configuration Page

Click on the Enable serial console check box to activate the fields that define the port and baud rate for the console.

Select a port from the Serial Port drop-down menu.

Select a baud rate from the Baud Rate drop-down menu.

If a change is made to the console settings after the target system image has been built, an *Out-of-Sync Notice* will appear at the bottom of the page, as shown in the following figure:

Δ Some settings on this page are out of sync with the target system image.							
Show Differences See what settings are different in the image.	Update Image Apply settings on this page to the image.	Update Session Update this page with settings from the image.					

Figure 1-17 Console Settings and Image Out-of-Sync Notice

The appearance of an Out-of-Sync Notice on any page indicates that the settings currently displayed in the session do not match the state of the associated target image. Click on Show Differences to see which settings are currently out-of-sync. To resolve the issue, it is necessary to either click on Update Image or Update Session.

The Update Image button will apply the currently displayed settings to the target image, whereas the Update Session button will change the currently displayed settings to match the state of the target image. The Out-of-Sync Notice will disappear once an update direction has been selected.

NOTE

If your target system does not have a serial port do not configure a serial console on this page.

Configuring Networking

To configure networking for the target system image, click on Networking from the Configure Image toolbox. The Configure Networking page appears, as shown in the following figure.

		RedH	lawk-8.2 - RedHawk Architect	×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp				
è 🖹 🗄 🔂 🔞 🌔	📎 👯 拱	Estimated Imag	ge Size: 665.3 MB (33% of 2.0 GB) 2.0 GB	*
Select Software	Configure Netv	vorking		
Configure Image				2
General Settings	Network Inte	rfaces		
	Device Ena	abled IP Addres	s Netmask 🗖	
Console	eth0	DHCP	DHCP	
	eth1 [DHCP	DHCP	
Wetworking		DHCP	DHCP	
Eile Systems		DUCB	DUCB *	
0.051	Hostname			
SELinux		P hostname		
	 Use stat 	ic hostname:	edhawk	
	Miscellaneou	s Settings		
	Use DHO	3 0		
Build Image				
Customize Image	 Use stat 	c settings:	hese static settings may be overriden by DHCP-supplied values.	
Deploy Image				

Figure 1-18 Network Configuration Page

All available network interfaces are listed in the Network Interfaces section. There may be more or less interfaces shown depending on the target board selected.

To configure a particular network interface, click on the interface to select it, then click on the Edi^\dagger button.

The Configure Network Interface dialog shown in the following figure displays.

Configure Network Interface	×
Configuring network interface eth0.	
✓ Enable eth0 at boot time	
IP Address Configuration	
Use DHCP to obtain IP address	
○ Use static IP address	
IP Address: Netmask:	
● Cancel	<

Figure 1-19 Configure Network Interface Dialog

The selected network interface is displayed at the top of the dialog.

Click on the Enable eth0 at boot time check box to enable/disable the interface automatically on boot.

Choose the Use DHCP to obtain IP address radio button to enable dynamic address configuration, or choose the Use static IP address radio button to enable manual address configuration. For manual configurations, enter the IP address and netmask in the appropriate fields.

Click on OK to apply the settings to the image and close the dialog. Click Cancel to cancel changes.

On the Configure Networking dialog under the Hostname and Miscellaneous Settings areas, either choose to use DHCP or supply the hostname, default gateway, domains, and DNS server addresses in the appropriate fields. Note that multiple DNS domains and DNS servers may be specified by separating multiple entries with either spaces or commas. Be sure to choose to use DHCP appropriately if a DHCP server will be providing some or all of the network parameters dynamically.

If a change is made to the network settings after the target system image has been built, an *Out-of-Sync Notice* will appear at the bottom of the page, as shown in the following figure:



Figure 1-20 Network Settings and Image Out-of-Sync Notice

The appearance of an Out-of-Sync Notice on any page indicates that the settings currently displayed in the session do not match the state of the associated target image. Click on Show Differences to see which settings are currently out-of-sync. To resolve the issue, it is necessary to either click on Update Image or Update Session.

The Update Image button will apply the currently displayed settings to the target image, whereas the Update Session button will change the currently displayed settings to match the state of the target image. The Out-of-Sync Notice will disappear once an update direction has been selected.

Configuring File Systems

To configure file system options for the target system image, click on File Systems from the Configure Image toolbox. The Configure File System page appears, as shown in the following figure.

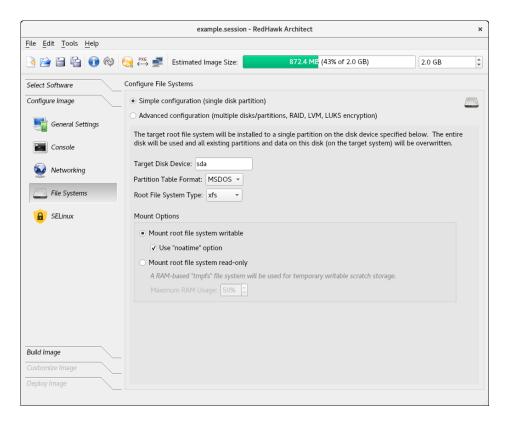


Figure 1-21 File System Configuration Page

There are two different partitioning modes supported: Simple configuration and Advanced configuration. This page defaults to the simple disk partitioning mode.

The following are the possible Target Disk Device names:

- 1. SATA disks: sdX where X can be from a-z. For example, sda.
- 2. NVMe disks: nvmeXnY where X can be from 0-9 and Y from 1-99. For example, nvme0n1.
- 3. eMMC disks: mmcblkX where X can be from 0-99. For example **mmcblk0**.
- 4. VirtIO disks: vdX where X can be from a-z. For example, vda.

NOTES

Architect attempts to match your disk device configuration. However, if it finds no matching disk device on the target system, Architect will map the configured disk device to the actual disk device found on the target system. When installing in interactive mode, Architect will show the mapping and prompt to confirm the chosen disk device. When using the PXE Diskless deployment method, all file system configuration settings are ignored; any local drive media that is present on the target will be untouched and ignored. See "Booting Diskless via PXE over a Network" on page 1-73 for more information.

Simple Disk Partitioning

Simple disk partitioning is the traditional partitioning that was offered by early versions of RedHawk Architect. In this mode only a single partition will be created on the specified disk device.

Indicate the desired root device in the Target Disk Device field.

Select the desired Partition Table Format to be used when initializing the root device; both the MSDOS and GPT partition table formats are supported.

Select the desired Root File System Type to be used for the file system on the disk partition; currently the XFS, EXT4, EXT3 and EXT2 file system types are supported.

By default Mount writable is selected and the root file system will be mounted with both read and write permissions.

Check the Use "noatime" option box to mount the root file system with the *noatime* option. This helps to minimize the number of writes to the root device when root is *not* mounted read-only.

Select Mount root file system read-only to mount the root file system *read-only*. Mounting the root file system read-only offers improved security and it will also help preserve the life of root flash devices. When mounting the root file system read-only, a RAM-based file system is then allocated for temporary storage. The Maximum RAM Usage for this file system is set, by default, to 50 percent of RAM. The default can be changed by clicking on the up and down arrows of the spin control box.

If a change is made to the file-system settings after the target system image has been built, an *Out-of-Sync Notice* will appear at the bottom of the page, as shown in the following figure:



Figure 1-22 File-System Settings and Image Out-of-Sync Notice

The appearance of an Out-of-Sync Notice on any page indicates that the settings currently displayed in the session do not match the state of the associated target image. Click on Show Differences to see which settings are currently out-of-sync. To resolve the issue, it is necessary to either click on Update Image or Update Session.

The Update Image button will apply the currently displayed settings to the target image, whereas the Update Session button will change the currently displayed settings to match the state of the target image. The Out-of-Sync Notice will disappear once an update direction has been selected.

Advanced Disk Partitioning

The advanced disk partition mode provides a more modern and flexible disk partitioning scheme. In this mode you can configure multiple partitions and even multiple disks using the Disk Partitioning tab, Logical Volumes via the LVM tab, RAIDs, and special file systems like **tmpfs** and **bind** via the Special File Systems tab. The All File Systems tab will list all the file systems to be configured on the target system. You can also configure partitions and logical volumes with LUKS2 encryption.

NOTE

You must ensure that any additional disks defined using advanced partitioning, in fact, exist on the target for the installation to succeed.

NOTE

Multiple disks cannot be partitioned with the USB Devices or the Virtual Machines deployment methods. In order to use multiple disks you must deploy with one of the Installer methods (via Disc, USB or PXE).

If a change is made to the file-system settings after the target system image has been built, an *Out-of-Sync Notice* will appear at the bottom of the page, as shown in the figure below.

$ m \Delta$ Some settings on this page are out of sync with the target system image.							
See what settings are different in the image.	Update Image Apply settings on this page to the image.	G Update Session Update this page with settings from the image.					

Figure 1-23 Advanced Disk Partitioning and Image Out-Of-Sync Notice

Default File System Configuration

Starting in the Configure File Systems page, click on the Advanced configuration button and the following menu appears. Press OK for the default file system configuration.

All the partitions will be made with the same basic options. You can modify the settings later, on a per partition basis, using the Edit Partition button found in the Disk Partitioning tab.

Note that you get this menu at the start and anytime you reset settings to the defaults.

Default File System Configuration ×							
Choose default file system configuration.							
Partition Table Format: MSDOS 🔹							
Use LVM							
Encrypt with LUKS2							
● Cancel							

Figure 1-24 File System Default Configuration

The Disk File Partitioning tab as shown below shows the disk partitioning for the basic default configuration.

		example.sessi	on - RedHawl	Architect			×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp							
è 🖹 🛱 🚱 🗞	PXE 🛃 Estima	ted Image Size:		872.4 MB	(43% of 2.0 GB)		2.0 GB
Select Software Co	onfigure File Systems	5					
Configure Image	 Simple configurat 	ion (single disk j	partition)				
General Settings	 Advanced configu 	ration (multiple	disks/partitio	ns, RAID, LVM	, LUKS encryption	ר)	
	Disk Partitioning	RAID LVM	Special Fil	e Systems	All File Systems		
Console	Configure disks an used entirely for L						
🥺 Networking	Disk	Partition 5	Size	Mount Point	Туре	Options	
File Systems	 sda (MSDOS) The bootlos 	ader will be insta	alled in the MI	3R of this disk	ί.		
O CELinna		sda1 sda2	1 GiB 1 GiB	/boot	xfs swap	defaults	
SELinux		sda3	maximum	/	xfs	defaults	
	All data on i	this disk will be o	verwritten.				
	+Add Partition	-Remove Pa	rtition 🔏 Ec	lit Partition	+Add Disk	-Remove D	visk 🔌 Edit Disk
	Install boot loader	on disk: sda	•				
Build Image	🛆 If the size of an	y disk device is e	xceeded, you	will get an erro	or when the syste	m is installed.	
Customize Image					Read-Only Roo	t Settings 🥱	Reset to Defaults
Deploy Image							

Figure 1-25 Disk Partitioning with Basic Default Configuration

Press Add Partition to add new partitions to the currently selected disk. Press Remove Partition to remove the currently selected partition. Press Edit Partition to edit attributes of the currently selected partition. Press Add Disk to add a new disk to the set of currently available disks. Press Remove Disk to remove the currently selected disk from the set of available disks.

Press Edi[†] Disk to edit attributes of the currently selected disk.

Use the Install boot-loader on disk pull-down menu to choose the disk that you will be booting from if multiple disks have been defined.

Press Reset To Defaults to discard all the current settings and start from the beginning.

Optional File System Configurations

Optionally you can configure:

- the GPT partitioning table format
- logical volumes (LVM)
- the Linux Unified Key Setup (LUKS2) for encryption
- Redundant Array of Independent (or Inexpensive) Disks (RAID)

It is beyond the scope of this guide to fully document these features, however, documentation can be found on-line.

GPT stands for GUID Partition Table. It is a new standard that is gradually replacing MBR (Master Boot Record). It is required when using UEFI, which replaces the old BIOS.

LVM stands for Logical Volume Management. The main advantages of LVM are: increased abstraction, flexibility, and control in managing disk storage space. Volumes can be resized dynamically as space requirements change and volumes may be migrated between physical devices on a running system.

LUKS2 is the second version of the Linux Unified Key Setup for disk encryption management. LUKS enables you to encrypt block devices. It allows multiple user keys to decrypt a master key, which is used for the bulk encryption of the partition. Architect supports one passphrase per target for all LUKS2 configured partitions, however, multiple user keys may be configured by the user on the target system. Architect will prompt for the passphrase in the deployment stage.

A RAID may be constructed from any number of physical disk devices to form a single logical, large capacity storage device that offers a number of advantages over conventional hard disk storage device. It can improve performance, resiliency and costs, depending on the RAID level. It uses the techniques of striping, mirroring and parity.

Example Using Optional Configurations

For conciseness, the optional GPT table format, LVM and LUKS2 are all set in this example. Note that they can be chosen independent of each other.

When any of these options are set in the Default File System Configuration menu, all the system partitions will be made with these options. The settings can be modified at a later time, on a per partition or per logical volume basis, using the Edit Partition button in the Disk Partitioning tab or the Edit Logical Volume in the LVM tab.

Default File System Configuration ×
Choose default file system configuration.
Partition Table Format: GPT 🔹
✔ Use LVM
✓ Encrypt with LUKS2
●Cancel

Figure 1-26 File System Optional Configuration

When GPT, LVM, and LUKS2 encryption are all configured, the Disk Partitioning configuration looks as follows:

		example	.session	n - RedHa	wk Architect				×
<u>File Edit T</u> ools <u>H</u> elp									
🖻 😭 🛱 😭 🏟 🄇	浸 🚧 🛃 Estir	mated Image	Size:		872.4 M	1 <mark>6</mark> (43% of 2.0	GB)	2.0 GB	-
Select Software	Configure File Syste	ms							
Configure Image	 Simple configure 	ration (single	disk pa	rtition)					
General Settings	 Advanced confi 	guration (mu	ıltiple di	sks/parti	ions, RAID, L\	VM, LUKS encry	/ption)		
	Disk Partitionin	g RAID	LVM	Special	File Systems	All File Syst	ems		
Console								d partitions, or be	
😡 Networking	,	artition	D. Each	·	Mount Point	Type	r be used for LVM Options	or RAID.	
File Systems	✓ sda (GPT)								
File Systems		loader will b da1		ed in the 0 MiB	BIOS_GRUB F	partition of this BIOS_GRUB	disk. ESP on UEFI		
🔒 SELinux		da2 da3		1 GiB ximum	/boot	xfs LVM	defaults "redhawk"		
	-	n this disk wi				2000	- culture		
	+Add Partition	n 🗕 Remo	ove Part	ition 🍳	Edit Partition	💠 Add Di	isk 🗕 Remove	Disk Kedit Di	sk
Ruild Image	Install boot load	ler on disk:	sda	•					
Build Image	\triangle If the size of	any disk devi	ce is exc	eeded, ye	ou will get an e	error when the s	system is installed.		
Customize Image						Read-Only	Root Settings	Reset to Defaul	ts
Deploy Image									



The LVM tab shows the logical volumes configured. The lock symbol on the left side of each logical volume shows that the LUKS2 encryption is enabled:

		example.sessior	n - RedHawk Archite	ect	×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp					
è 🖻 🖹 🗊 🏟 🍕	🚽 🚧 🛒 Estimat	ted Image Size:	872.4	ME (43% of 2.0 GB)	2.0 GB 🗘
Select Software Co	onfigure File Systems				
Configure Image	 Simple configurati 	on (single disk pa	rtition)		
General Settings	Advanced configur	ration (multiple di	sks/partitions, RAID,	LVM, LUKS encryption)	
	Disk Partitioning	RAID LVM	Special File System	ns All File Systems	
Console	Configure LVM Log system.	gical Volumes her	e. A Logical Volume	exists within a Volume Grou	ip and contains a file
Networking	Volume Group Lo	ogical Volume Size	Mount P	oint Type Mount	Options
File Systems SELinux		vap pot p	1 GiB naximum /	swap xfs defaul	ts
	Add Logical Vo	lume	ove Logical Volume	Edit Logical Volume	Edit Volume Group
Build Image			5	s to LVM. See the Disk Partitio	· · · · ·
Customize Image		,		Read-Only Root Sett	
Deploy Image					

Figure 1-28 LVM tab showing LVM Logical Volumes and LUKS2 encryption

Press Add Logical Volume to add a new logical volume to the currently selected volume group.

Press Remove Logical Volume to remove the currently selected logical volume.

Press Edit Logical Volume to edit attributes of the currently selected logical volume.

Press Edit Volume Group to edit attributes of the currently selected volume group.

Steps in Configuring Additional Logical Volumes (LVM)

To setup additional logical volumes:

1. Configure a volume group. To add a new volume group, add a disk partition or a whole disk using the respective button in the Disk Partitioning tab. In the respective menus, set the Use this partition for LVM option and specify a Volume Group name.

If you are adding a logical volume to an existing volume group, then continue to step 2. 2. Configure the logical volumes. From the LVM tab, highlight the volume group by clicking on it and use the Add Logical Volume button to create a logical volume.

Example Configuring Logical Volumes (LVM)

In the next example, an additional disk partition will be configured for LVM. Click on the Use this Partition for LVM box and assign the Volume Group name 'DATA'. If instead of a disk partition, you want to use a whole disk, use the Add Disk, instead of the Add Disk Partition button.

Add Disk	Partition ×
Creating GPT disk p	artition sda2.
\bigcirc Do not use this	partition
 Use this partition 	n for a file system
 Use this partition 	n for LVM
 Use this partition 	n for RAID
Size: 1	€ GiB →
This partition will be Physical Volume.	used as an LVM
Volume Group:	DATA -
Cai	ncel JOK

Figure 1-29 Adding a new disk partition to be used for LVM

The following snippet shows a new partition, **sda2**, added in the Disk Partitioning tab.

Disk Part	itioning RAID	LVM	Specia	al File Systems	All File Syste	ems
						partition table and partitions, or be be used for LVM or RAID.
Disk	Partition	Size		Mount Point	Туре	Options
✓ sda (6)	βPT)					
The	e bootloader wil	l be installe	ed in the	BIOS_GRUB	partition of this	disk.
	sda1	10	0 MiB		BIOS_GRUB	ESP on UEFI
	sda2		1 GiB		LVM	"DATA"
	sda3		1 GiB	/boot	xfs	defaults
	sda4	ma	ximum		LVM	"redhawk"

Figure 1-30 New disk partition added to be used for LVM

		example.session -	RedHawk Architect		
ile <u>E</u> dit <u>T</u> ools <u>H</u> elp					
è 🗁 🖴 😫 📀 🍩 🛛	😪 👯 🚅 Estim	ated Image Size:	872.4 MB	(43% of 2.0 GB)	2.0 GB
Select Software	Configure File System	15			
Configure Image	 Simple configura 	ition (single disk parti	tion)		4
General Settings	Advanced config	uration (multiple disk	i/partitions, RAID, LVN	1, LUKS encryption)	
Console	Disk Partitioning	RAID LVM 5	Special File Systems	All File Systems	
	Configure LVM L system.	ogical Volumes here.	A Logical Volume exis	its within a Volume (Sroup and contains a file
- Hettionking	Volume Group	Logical Volume Size	Mount Point	Type Mo	ount Options
Elinux			1 GIB Nimum /	swap xfs de	faults
	-Add Logical V		Logical Volume		Sedit Volume Group
Suild Image	Volume Groups a	re created by allocatin	g Physical Volumes to I	VM. See the Disk Pa	rtitioning and RAID tabs.
				Read-Only Root S	Settings 👌 Reset to Defaults

The LVM tab will show a new volume group 'DATA' created:

Figure 1-31 New Volume Group 'DATA' created

From the LVM tab, click on the new volume group 'DATA' and press the Add Logical Volume to create a logical volume. In this example the mount point is set to '/private':

A	dd Logic	al Volume	×
Creating Logical	Volume	for Volume Group 'DAT,	Α'.
Use all remai	ning spac	e in Volume Group	
Size:	1	‡ GiB	•
		1,073,741,824 byt	es
File System:		xfs	•
Mount Point: /p	rivate		
Mount read-o	only		
Mount Options:	defaults	;	
 Encrypt with 	LUKS2		
		Cancel JOK	

Figure 1-32 Adding logical volume 'private' to new volume group

The following snippet shows a new logical volume 'private' in the newly created volume group 'DATA':

g RAID	LVM	Speci	Special File Systems		All File Systen	ns
Logical Vo	olumes he	ere. A Lo	ogical	Volume exis	s within a Volu	Ime Group and contains a file
Logical V	olume Siz	e	Ν	1ount Point	Туре	Mount Options
private		1 G	iB /	private	xfs	defaults
swap		1 G	iВ		swap	
root		maximu	m /		xfs	defaults
	Logical Vo Logical V private swap	Logical Volumes he Logical Volume Siz private swap	Logical Volumes here. A Lo Logical Volume Size private 1 G swap 1 G	Logical Volume Size M private 1 GiB / swap 1 GiB	Logical Volume here. A Logical Volume exist private 1 GiB /private swap 1 GiB	Logical Volume here. A Logical Volume exists within a Volu Logical Volume Size Mount Point Type private 1 GiB /private xfs swap 1 GiB swap

Figure 1-33 Logical Volume 'private' created in new group 'DATA'

Redundant Array of Independent Disks (RAID)

A RAID device is a logical partition. It can either contain a file system or be used as an LVM physical volume.

RAID devices may be constructed from any number of physical disk devices, as long as the required minimum number of physical devices is met for a particular RAID level.

A RAID device can be made up of the following physical devices:

- a whole physical disk or
- a disk partition

All the physical devices used in a RAID must be of the same type; all whole disks or all disk partitions. If disk partitions are used, then all the partitions in a RAID must be on different disks.

If the **/boot** file system is on a RAID device then it must be configured for RAID level 1. This extends to the **root** file system if there is no **/boot** partition.

The only deployment methods that support RAIDs are the on-target installer methods: USB Installer, Disc Installer, and PXE installer. All other methods support a single disk only.

The following RAID levels are supported:

- RAID 0 : based on striping technique. This level does not provide fault tolerance but increases the system performance with higher read and write speeds. Minimum number of disk devices required is 2.
- RAID 1 : utilizes mirroring technique. This level provides fault tolerance in the loss of no more than one member disk and, in some cases, increases read speed. Minimum number of disk devices required is 2.
- RAID 10 (0+1) : based on the combination of striping and mirroring techniques. This level exhibits RAID 0 performance and RAID 1 fault tolerance. Minimum number of disk devices required is 4.
- RAID 5 : utilizes both striping and parity techniques. This level provides the read speed improvement as in RAID 0 and survives the loss of one RAID member disk. Minimum number of disk devices required is 3.
- RAID 6 : similar to RAID 5 but uses two different parity functions. Thi s level can sustain two simultaneous RAID disk failures and still continue to function. Minimum number of disk devices required is 4.

Not supported at this time:

- The partitioning of a RAID
- Booting from a RAID
- Nesting of RAIDs

Steps in configuring a RAID

Steps to configure a RAID:

1. Configure the RAID by adding the appropriate number of physical devices. For example, for a level 1 RAID, this will be at the minimum two partitions or two whole disks. Use either the Add Partition... or Add Disk... buttons respectively from the Disk Partitioning tab.

Click respectively on Use this Partition for RAID or Use this disk for Raid button and give the RAID a name. Use the same RAID name when configuring all the physical devices in the RAID. If the RAID is using partitions, you must also specify the size of the partition.

NOTE

All the physical devices used by a RAID must be of the same type; either all whole disks or all partitions. If using partitions, all the partitions must be on different disks.

When adding a new disk for the purpose of creating a partition to be used for a RAID device, make sure to choose Create Partitions when adding the disk and Use this partition for RAID when adding the partition. The option Use this Disk for RAID should only be used when the entire disk is to be allocated to a RAID.

2. Configure the RAID device from the RAID tab. Double click on the specific RAID and, on the Edit RAID menu that pops up, specify the RAID level and click on your preference of: Use this RAID for a file system or Use this RAID for LVM.

If you choose to use a file system, you will be asked to enter file system related information. If you choose to use LVM, then you must enter the desired volume group name or use the default.

3. Configure the logical volumes from the LVM tab if you chose Use this RAID for LVM in the previous step. Click to highlight the volume group name and then click on the Add Logical Volume button and enter the file system information requested.

When a RAID has the incorrect number of physical devices configured for the specific RAID level, the following error message will appear at the bottom of the Disk Partitioning screen. Switching over to the RAID tab, the error printed there will show the number of physical devices expected. When the RAID configuration is completed with the correct number of physical devices, the errors disappear.

One or more RAID devices has an invalid configuration.
 Some deployment methods cannot partition multiple disks.
 If the size of any disk device is exceeded, you will get an error when the system is installed.

Figure 1-34 Invalid RAID configuration error message

Example System Configuration Using RAID Partitions

In this example, two RAIDs will be configured. For each RAID, two partitions will be allocated; one on the disk labeled **sda** and one on **sdb**.

The two RAIDS in this example are:

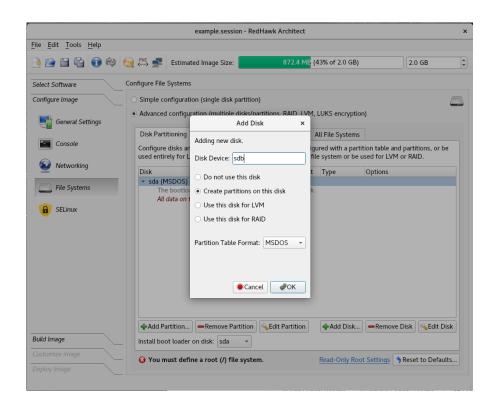
- 1. boot-raid: the RAID will be configured for RAID level 1 and a file system; both are requirements for the system's **/boot** partition.
- 2. lvm-raid: The RAID will be configured for RAID level 0. It will use logical volumes (LVM) for the system's **swap** and / directory.

To start, remove the current system configuration by clicking on the disk and using the Remove Disk button:

File Edit Tools Help	example.session - RedHawk Architect	×
File Edit Tools Help Image: Second se	😡 🚓 🛃 Estimated Image Size: 872.4 ME (43% of 2.0 G	3) 2.0 GB 🗘
Select Software Configure Image General Settings	Configure File Systems O Simple configuration (single disk partition) O Advanced configuration (multiple disks/partitions, RAID, LVM, LUKS encryp	(Lion)
Console	Disk Partitioning RAID LVM Special File Systems All File Syster Configure disks and disk partitions here. A disk may be configured with a pused entirely for LVM or RAID. Each partition may contain a file system or b	artition table and partitions, or be
Wetworking	Disk Partition Size Mount Point Type	Options
File Systems	The bootloader sda1 sda2 All data on this d	defaults defaults
	Add Partition Remove Partition Edit Partition Add Disk Install boot loader on disk: Sda -	-Remove Disk
Build Image	▲ If the size of any disk device is exceeded, you will get an error when the sys	stem is installed.
Customize Image Deploy Image	Read-Only F	oot Settings Reset to Defaults

Figure 1-35 Remove system disk sda

Next, create two disks using the Add Disk... button. On the menu that pops up, click on the Create partitions on this disk and choose the partition table format of your choice. For this example, the MSDOS partition table format is used.



The image below shows the disk **sda** already created and now adding the disk **sdb**.

Figure 1-36 Adding disk sdb

Now add a partition to each disk using the Add Partition... button. Configure each partition for RAID and assign the partition size and a name for the RAID. In this example the size is 1 GiB and the name of the RAID is 'boot-raid'. Use the same size and RAID name for all the physical devices in the RAID.

In the following image, the boot-raid partition on disk **sda** has already been created with the same options as shown below for **sdb**.

The following snapshot shows the partition 'boot-raid' created on disk **sdb**:

		example.sessio	on - RedHawk Architect			>
<u>File</u> <u>E</u> dit <u>T</u> ools <u>H</u> elp						
) پې 🕞 🖆 🖆 🔄	🚱 🚧 🛃 Esti	mated Image Size:	Image Size: 872.4 MB)	2.0 GB
Select Software	Configure File Syste		Disk Partition ×			
Configure Image	O Simple configu	Creating MSDO	S disk partition sdb1.			
	Advanced conf	ig 🔿 Do not use th	nis partition	, LUKS encrypti	ion)	
General Settings	Disk Partitionir	าต	DOS extended partition	All File System	s	
Console	Configure disks		ition for a file system			nd partitions, or be
Networking	used entirely fo	 Use this part 		ile system or be Type	Options	1 or RAID.
Eile Systems	✓ sda (MSDO The boo	1	ning space on disk	RAID	"boot-raid	" (RAID 0)
SELinux	All data o sdb (MSDO All data o	oS; on	1,073,741,824 bytes			
		This partition will RAID:	l be used in a RAID.			
	Add Partitio			+Add Disk.	Remov	e Disk Kelit Disk
Build Image	 One or mor Some deplo If the size of 	уп	Cancel	ər when the syst	em is installed	I.
Customize Image Deploy Image	😣 You must d	lefine a root (/) file	system.	Read-Only Ro	oot Settings	Reset to Defaults

Figure 1-37 Adding the boot-raid RAID partition on disk sdb

The same as with 'boot-raid', add another partition on each disk to be used for the RAID labeled 'lvm-raid'.

The following image shows the 'lvm-raid' partition has already been created on disk **sda** and now it is being created with the same options on disk **sdb**:

		example.sessio	n - RedHawk Archit	ect			×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp							
📑 😭 😭 🏟	🛞 🚧 Esti	mated Image Size:	872.	4 MB (43% of 2	.0 GB)	2.0 GB	¢
Select Software	Configure File Syste		Disk Partition	×			
Configure Image	 Simple configu 	Creating MSDOS	disk partition sdb2				
	 Advanced conf 	ig 🔿 Do not use th	is partition	, LUKS en	cryption)		
General Settings	Disk Partitionir	na	DOS extended parti	All File Sv	ystems		
Console	Configure disks used entirely fo	a an ar a	tion for a file systen tion for LVM	jured with	n a partition table n or be used for L		s, or be
Networking	Disk	 Use this parti 	tion for RAID	Туре	Options		
File Systems	 sda (MSDO The boo All data (sdb (MSDO All data o 	This partition will RAID:	iing space on disk be used in a RAID. tvm <mark>-raid</mark>	RAID RAID	"lvm-raio	id" (RAID 0) d" (RAID 0) id" (RAID 0)	-
Build Image	Add Partitio	de re yn	Cancel	· · · · · · · · · · · · · · · · · · ·			Edit Disk
		lefine a root (/) file			nly Root Settings		Defaults
	_				,		

Figure 1-38 Adding the lvm-raid partition on disk sdb

The following snippet shows the Disk Partitioning tab after all the partitions have been created. Note that the RAID level always defaults to 0 when adding a disk or partition but it can be changed when configuring the RAID in the next step.

Disk Partitio	oning RAID I	_VM Special Fi	le Systems 🛛 A	All File System	15
			, ,		rtition table and partitions, or be e used for LVM or RAID.
Disk	Partition	Size	Mount Point	Type	Options
✓ sda (MS)	DOS			- 7F -	
	ootloader will be	installed in the M	BR of this disk.		
1110 1	sda1	1 GiB		RAID	"boot-raid" (RAID 0)
	sda2	maximum		RAID	"lvm-raid" (RAID 0)
All da	ta on this disk will	be overwritten.			
✓ sdb (MS)	DOS)				
	sdb1	1 GiB		RAID	"boot-raid" (RAID 0)
	sdb2	maximum		RAID	"lvm-raid" (RAID 0)
All da	ta on this disk will	be overwritten.			

Figure 1-39 Disk Partitioning snippet after RAID partitions created

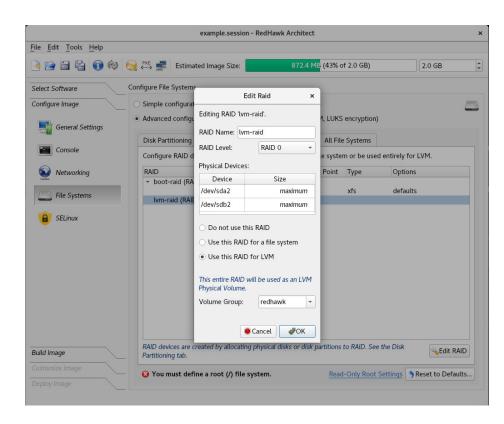
Next configure the RAIDs. Double click on the 'boot-raid', and on the Edi† RAID menu that pops up, change the RAID level to 1 as it is the only run level that can be assigned to a

/boot system partition. It also requires a file system. Its mount point is **/boot** as shown below:

		example.ses	sion - RedHawk Archite	ct			د
<u>File Edit T</u> ools <u>H</u> elp							
🔌 🔂 🗄 🗳 🕤 🏟	i 😥 🔛 👷	Estimated Image Size	: 872.4	MB (43%	of 2.0 GB)		2.0 GB
Select Software	Configure File S	ystem	Edit Raid	×			
Configure Image	 Simple cont 	Editing RAID	'boot-raid'.				
General Settings	Advanced c	onfigi, RAID Name:	boot-raid	1, LUK	S encryption)		
General Settings	Disk Partitio	RAID Level:	RAID 1	- All Fi	le Systems		
Console	Configure R	AID d Physical Devi		.e syst	em or be used	entirely for L	/M.
🕥 Networking	RAID	Device /dev/sda1	Size 1 GiB	Point	Туре	Options	
	boot-rai	id (RA		•			
File Systems	WIT-Taic	O Do not us	e this RAID				
🔒 SELinux		Use this R	AID for a file system				
		 Use this R 	AID for LVM				
		File System:	xfs	-			
		Mount Point:	/boot	٦.			
		Mount real	d-only				
		Mount Option	ns: defaults				
		Encrypt w	th LUKS2				
		_					
Build Image	RAID device Partitioning		● Cancel	Intition	s to RAID. See t	the Disk	Kedit RAID
	😣 You mu	st define a root (/) f	ile system.	Rea	d-Only Root S	ettings 🥱 Re	eset to Defaults

Figure 1-40 Configuring the RAID named boot-raid

Double click on the 'lvm-raid' to now configure the second RAID. Set the Use this RAID for LVM button. Use the RAID level 0 which is the default setting. The volume group name is 'redhawk' which is also the default setting.



The image below shows the Edi[†] RAID menu settings for the 'lvm-raid' RAID:

Figure 1-41 Configuring the RAID 'lvm-raid' for LVM

The following snippet shows the RAID configuration. The RAID named 'boot-raid' is configured as a file system while 'lvm-raid' is configured for LVM.

Disk Partitioning	RAID	LVM	Special Fil	e Systems	All File	e Systems		
Configure RAID dev	vices her	e. RAID	devices may	/ contain a fi	e syste	m or be used	entirely for LVM.	
RAID	Parti	tion	Size	Mount	Point	Туре	Options	_
✓ boot-raid (RAID)) 1)							
	-		-	/boot		xfs	defaults	
✓ lvm-raid (RAID)	0)							
This entire F	AID will	be used	for LVM Vo	lume Group	'redhaw	/k".		

Figure 1-42 Snippet of the RAID tab showing the RAIDs created

The final step is to configure logical volumes in the volume group 'redhawk' from the LVM tab. First add a logical volume for **swap**. The size is set to 8 GiBs and the file system type is **swap**.

	exa	mple.session - Rec	Hawk Architect		×
<u>File E</u> dit <u>T</u> ools <u>H</u> elp					
🖻 😂 🗎 🔓 🔞 🍕	PXE Estimated I	mage Size:	872.4 MB (439	6 of 2.0 GB)	2.0 GB
Select Software C	nfigure File Systems				
Configure Image	Simple configuration (single disk partition	1)		
General Settings	Advanced	Add Logical	Volume ×	encryption)	
	Disk Partit Creating Lo	ogical Volume for V	/olume Group 'redhawk'	e Systems	
Console	Configura			in a Volume Group ar	nd contains a file
Wetworking	system.	remaining space in		in a rotaine broup a	
Networking	Volume G	8	¢ GiB →	Mount Opt	ions
Eile Systems	redhav		8,589,934,592 byte	5	
SELinux	File System	n:	wap 👻		
JELMAX		with LUKS2	wap	1	
	Encrypt	With EONS2			
			● Cancel ● Cancel	1	
				,	
Build Image	Add Logical Volume		gical Volume Selit L		Cell Colume Group
Customize Image	·				
	😧 You must define a	root (/) file syster	m. <u>Re</u>	ad-Only Root Settings	Reset to Defaults

Figure 1-43 Configuring the swap logical volume

Next, add a logical volume for the **root** file system and allocate to it the remaining space in the volume group.

		example.session	- RedHawk Architect		×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp					
📑 🖆 🛱 🚯 😢	阙 👯 🚅	Estimated Image Size:	872.4 MB <mark> (4</mark>	3% of 2.0 GB)	2.0 GB
Select Software	Configure File S	systems			
Configure Image	○ Simple cor	nfiguration (single disk par	tition)		
General Settings	Advanced	Add Lo	gical Volume	× encryption)	
Cancela	Disk Partit	Creating Logical Volume	for Volume Group 'redhaw	/k'. e Systems	
Console	Configure system.	✔ Use all remaining spa	ce in Volume Group	in a Volume Group a	and contains a file
Wetworking	Volume G			Mount Op	otions
File Systems	✓ redhav	File System: Mount Point:	xfs		
SELinux		Mount read-only			
		Mount Options: default	s		
		Encrypt with LUKS2			
			Cancel		
	+Add Lo	gical Volume	ve Logical Volume 🛛 💊 Edit	t Logical Volume	💫 Edit Volume Group
Build Image	Volume Gre	oups are created by allocat	ing Physical Volumes to LVI	M. See the Disk Partitionin	g and RAID tabs.
	😣 You mu	ıst define a root (/) file s	ystem.	Read-Only Root Settings	Reset to Defaults
Deploy Image					

Figure 1-44 Configure the root logical volume

The snippet that follows shows the contents of the LVM tab:

Volume Group Logical Volume Size Mount Point Type Mount Options	Disk Partitionin	g RAID	LVM Special	File Systems	All File Syster	ms
 redhawk swap 8 GiB swap 	Configure LVM system.	Logical Voli	umes here. A Logi	cal Volume exis	ts within a Vol	ume Group and contains a file
swap 8 GiB swap	Volume Group	Logical Vo	lume Size	Mount Point	Туре	Mount Options
	✓ redhawk					
root <i>maximum /</i> xfs defaults		swap	8 GiB		swap	
		root	maximum	/	xfs	defaults

Figure 1-45 Logical volumes swap and root configured

Example RAID Using Whole Disks

For this example, two whole disks will be allocated for a RAID named 'raid0'. It will be configured as RAID level 1 and the file system will be encrypted.

In the following image, disk **sda** has been created and the second disk, **sdb**, is being created using the same RAID name.

		*example.session - RedHawk	Architect	
ile <u>E</u> dit <u>T</u> ools <u>H</u> elp				
è 🗎 🗄 🕤 🕸 '	😥 🚧 🛃 Estima	ted Image Size:	872.4 MB (43% of 2.0 GB)	2.0 GB
Select Software	Configure File Systems			
Configure Image	 Simple configuration 	on (single disk partition)		Ľ
General Settings	Advanced configu	ation (multiple disks/partitions Add Disk	RAID_LVM, LUKS encryption)	
	Disk Partitioning	Adding new disk.	All File Systems	
Console	Configure disks an used entirely for L	Disk Device: sdc	igured with a partition tab file system or be used for	
Networking	Disk		t Type Option	
Eile Systems	✓ sda (MSDOS) The bootlos	 Do not use this disk Create partitions on this discussion 	sk k. xfs defaul	ts
B SELinux	All data on t	 Use this disk for LVM Use this disk for RAID 	swap xfs defaul	ts
	 sdb (RAID) This entire All data on t 	This entire disk will be used in a RAID: raid0	RAID.	
	Add Partition	Cancel	₽OK	move Disk
	Install boot loader	on disk: sda 👻		
		AID devices has an invalid con		
ild Image		ent methods cannot partition mu y disk device is exceeded, you wi	ltiple disks. Il get an error when the system is inst	talled.
ustomize Image			Read-Only Root Settin	gs 🔦 Reset to Defaults.

Figure 1-46 Adding disk sdb to raid0

The following snippet shows the Disk Partitioning tab with disks **sda** and **sdb** created to be used in the RAID named 'raid0':

	g for Evillor for to the.	Each partition n	nay contain a fil	e system or b	e used for LVM or RAID.
Disk	Partition	Size	Mount Point	Туре	Options
→ sda (MS)	SDOS)				
The	bootloader will be ir	nstalled in the M	BR of this disk.		
	sda1	1 GiB	/boot	xfs	defaults
	sda2	1 GiB		swap	
	sda3	maximum	/	xfs	defaults
All da	ata on this disk will b	e overwritten.			
✓ sdb (RA)	ID)				
This	entire disk will be u	sed for RAID "rai	id0" (RAID 0).		
All da	ata on this disk will b	e overwritten.			
✓ sdc (RA)	ID)				
This	entire disk will be u	sed for RAID "rai	id0" (RAID 0).		
All di	ata on this disk will b	e overwritten.			

Figure 1-47 Disk devices for RAID 'raid0' created

Now configure the RAID to be used for a file system and the RAID run level to be 1. Assign the mount point '/data' and click on the box labeled Encrypt with LUKS2.

			example.session	n - RedHawk Architec	t		×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp							
🎯 🗊 🖆 🖬 🏟	阙 🚧 🚅	Estima	ited Image Size:	872.4	ME (43% of 2.0 GB)		2.0 GB
Select Software	Configure File	System	E	dit Raid >	<		
Configure Image	🔿 Simple co	nfigurat	Editing RAID 'rai	d0'.			
General Settings Console Networking File Systems ELinux	Advanced Disk Parti Configure RAID raid0	tioning	RAID Level: Physical Devices Device /dev/sdb /dev/edc O Do not use th	RAID 1 Size Maximum Kfs Maximum Kfs Maximum M	All File Systems e system or be us nt Type]	for LVM.
Build Image Customize Image Deploy Image	RAID devia Partitionin		•	Cancel	rtitions to RAID. Se		Seset to Defaults

Figure 1-48 Configuring 'raid0' two physical disk devices

The snippet below shows the resulting RAID configuration:

Disk Partitioning	RAID	LVM	Special File	Systems	All File Systems					
Configure RAID devices here. RAID devices may contain a file system or be used entirely for LVM.										
RAID	Partition	S	ize	Mount Point	Туре	Options				
 raid0 (RAID 1) 										
6	-	-		/data	xfs	defaults				

Figure 1-49 Configuration of RAID labeled 'raid0'

Example Configuration Using multiple RAID levels

In this example, four disks are added and partitioned. The partitions are shared by three different RAIDs, each configured at different RAID levels: one uses level 10, one level 5 and one level 6.

Each RAID is using the minimum physical devices required for the run level: four partitions for RAID levels 10 and 6, and three partitions for RAID level 5.

The four disks are created using the Add Disk... button and the Create partitions on this disk setting. The partitions are created using the Add Partition... button and the Use this partition for RAID setting. The RAID level is configured from the RAID tab.

The image below shows the disk partitioning for this configuration. Note that this image is taken after the RAIDs are configured with their respective RAID levels, otherwise it would show 0 for all the RAID levels.

isk	Partition	Size	Mount Point	Туре	Options
sda (MSD	OS)				
The bo	ootloader will be i	nstalled in the Mi	BR of this disk.		
	sda1	1 GiB	/boot	xfs	defaults
	sda2	1 GiB		swap	
	sda3	maximum	/	xfs	defaults
All data	a on this disk will l	oe overwritten.			
sdb (MSD	OS)				
	sdb1	10 GiB		RAID	"raid-0" (RAID 10)
	sdb2	10 GiB		RAID	"raid-1" (RAID 5)
	sdb3	maximum		RAID	"raid-2" (RAID 6)
	a on this disk will l	oe overwritten.			
sdc (MSD	,				
	sdc1	10 GiB		RAID	"raid-0" (RAID 10)
	sdc2	10 GiB		RAID	"raid-1" (RAID 5)
	sdc3	maximum		RAID	"raid-2" (RAID 6)
	a on this disk will l	oe overwritten.			
sdd (MSD					
	sdd1	10 GiB		RAID	"raid-0" (RAID 10)
	sdd2	10 GiB		RAID	"raid-1" (RAID 5)
	sdd3	maximum		RAID	"raid-2" (RAID 6)
	a on this disk will l	oe overwritten.			
sde (MSD		10 010		5.415	
	sde1	10 GiB		RAID	"raid-0" (RAID 10)
All date	sde2 a on this disk will l	maximum		RAID	"raid-2" (RAID 6)
All data	a on this disk will t	be overwritten.			
Add Partit	ion Remov	e Partition 🛛 🔌 Eo	lit Partition	+Add Disk	🗕 Remove Disk 🛛 🛶 Edit Disk
stall boot lo	oader on disk: sd	a 👻			
Como don	lowmont mothods	cannot partition p	outtiplo dicks		
some aep	ioyment methods	cannot partition n	nuttiple alsks.		

Figure 1-50 Disk partitioning for the three RAIDs configured

The image below shows the RAIDs configured.

Disk Partitioning RAID LVM Special File Systems All File Systems Configure RAID devices here. RAID devices may contain a file system or be used e							d antiraly far LVM
onfigure RAID devi	ces nere.	RAID	devices ma	ay contain a n	te sys	tem or be use	a entirety for LVM.
RAID	Partition		Size	Mount F	Point	Туре	Options
 raid-0 (RAID 10) 							
	-		-	/DATA-	L10	xfs	defaults
raid-1 (RAID 5)							
	-		-	/DATA-	L5	xfs	defaults
raid-2 (RAID 6)							
				/DATA-	L6	xfs	defaults

Figure 1-51 RAID tab showing three RAIDs using different RAID levels

Read-Only Root Configuration

To configure the root file system read-only, click on the Configure Read-only Root Settings link on the lower right hand of the Configure File Systems page.

This will bring up a dialog that will instruct you on the steps to take and on implementation choices. The first step is to configure the root file system as read-only via the Edit Partition button. Then, click again on the Configure Read-only Root Settings link for information on the next steps.

Temporary storage is required when root is configured as read-only. This can be achieved via a RAM-based file system (the default) or by creating a writable file system named /var/lib/stateless/writable using the Add Partition button.

Note that the RAM-based file system size is configurable as a percentage of RAM space. While these two options are writable they are not persistent over boots. Optionally, a persistent file system can be created with a mount point of /var/lib/stateless/state.

When finished partitioning the disk, verify the configuration by clicking on the Configure Read-only Root Settings link one last time.

The figure below shows an example of a root read-only partition scheme with the required scratch storage for root configured as a disk partition (/var/lib/stateless/writable) and the optional persistent disk partition (/var/lib/stateless/state).

- ile Edit Tools Help								
	🕥 PXE 🖃				_	CR 2 MD (220) -62	0.00	
<u>)</u>	🍠 «> 🔤	Estimated	Image Si	ze:		565.3 MB (33% of 2	.0 GB)	2.0 GB
Select Software	Configure File	Systems						
Configure Image	 Simple co 	nfiguration	(single di	sk partition)				
General Settings	Advanced	configurati	ion (multij	ole disks and	/or part	itions, LVM, encrypt	ion)	_
	Disk Parti	tioning L	VM S	oecial File Sy	stems	All File Systems		
Console	Configure	disks and d	lisk partiti	ons here. A	disk ma	v contain partitions	or be used as a	n LVM Physical Volume.
_						d as an LVM Physica		in Evi in hysical volume.
🥺 Networking	Disk	Partitio	n S	ize	Moun	t Point	File System	Mount Options
	✓ sda (G	PT)					,	
Eile Systems		sda1		100 MiB				BIOS_GRUB / ESP
		sda2		1 GiB	/boot		xfs	defaults
G SELinux		sda3		1 GiB			swap	
-		sda4		200 MiB		b/stateless/writable		defaults
		sda5		200 MiB	/var/li	b/stateless/state	xfs	defaults
		sda6		maximum	/		xfs	ro
	Ine	partition ta	ble and al	data on this	disk wil	be overwritten.		
	💠 Add Pa	rtition	-Remove	Partition	💊 Edit F	artition 🔶 Add	Disk 🗕 Re	move Disk 🔍 Edit Disk
	Install boo	t loader on	disk: sd	a 👻				
Build Image	∧ If the c	ize of any di	ick device	is exceeded	in the second	get an error when th	a system is incl	talled
	as il ule s	ize or any un	isk device	is exceeded,	you will	ger an en or when th	e system is mis	aucu.
Customize Image						Read-O	nly Root Settin	gs 👌 Reset to Defaults
Deploy Image								

Figure 1-52 Example root read-only partitioning scheme

Configuring Special File Systems (tmpfs, bind)

The Special File Systems tab is used to configure special (non-disk) file systems. See the mount (8) man page for more information on these special file systems.

Initially this page is blank but in the following figure below two example entries have been added; one of type **tmpfs** and one of type **bind**.

		RedHa	wk-8.2 - RedHaw	k Arcl	nitect			×		
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp										
è 🖹 🖹 🚯 🍪 😔	PXE 🛃 Esti	mated Image	Size:	6	6 <mark>5</mark> .3 MB (33% of 2.0 GB)		2.0 GB	-		
Select Software Co	nfigure File Syste	ems								
Configure Image	Simple configu	ration (single	e disk partition)							
Advanced configuration (multiple disks and/or partitions, LVM, encryption) General Settings										
	Disk Partitionir	ng LVM	Special File Syste	ems	All File Systems					
Console	Configure spec	ial (non-disk)	file systems here	, such	as tmpfs and bind-mount	ts.				
😡 Networking	Mount Point	Туре	Special		Mount	t Options				
- <u>_</u>	/tmp	tmpfs	size=15%	defau						
Eile Systems	/var/tmp	bind	/tmp	defau	ılts					
B SELinux										
Build Image Customize Image Deploy Image	◆ Add ●	Remove	Edit		<u>Read-Oniy Ro</u>	ot Settings	∱Reset to Default	:s		

Figure 1-53 Example Special File Systems page entries

The All File Systems tab is used to view all the file systems to be configured on the target system. Both disk and special file system entries are listed. The following figure

ile <u>E</u> dit <u>T</u> ools <u>H</u> elp						
è 🖻 🖹 🔂 🏟 🍕	y 👯 🛃 Estima	ited Image	e Size:	665 <mark>.3 MB (</mark> 33	3% of 2.0 GB)	2.0 GB
Select Software	Configure File System:	s				
Configure Image	 Simple configurat 	tion (singl	e disk partition)			
General Settings	 Advanced configu 	iration (m	ultiple disks and/or par	titions, LVM, e	encryption)	_
	Disk Partitioning	LVM	Special File Systems	All File Sys	tems	
Console	This is a consolida	ted read-	only view of all configu	red file syster	ns.	
🐼 Networking	Mount Point		Device	Туре	Mount Opt	ions
<u> </u>	/		/dev/sda6	xfs	ro	
Eile Systems	/boot		/dev/sda2	xfs	defaults	
	/tmp	/tmp		tmpfs	size=15%	
SELinux	/var/lib/stateless/	/var/lib/stateless/state /var/lib/stateless/writable /var/tmp		xfs	defaults	
	/var/lib/stateless/			xfs	defaults	
	/var/tmp			none	bind	
	(swap)		/dev/sda3	swap	defaults	
Build Image	This view is read-o	nly. Use t	he other tabs to make c	hanges.		
Customize Image				-	Read-Only Root Settings 🦄	

shows entries corresponding to the examples above.

Figure 1-54 Example All File Systems list

Configuring SELinux

The security-enhanced option is disabled in RedHawk but it can be enabled in the permissive or enforcing mode.

See the section "Configuring SELinux", in Chapter 2:Security Extensions for more information.

Building an Image

To build the target system image by installing the selected software, select Build Image from the toolbox on the left side of the RedHawk Architect main window.

The Build Image page shown in the following figure displays.

		RedHawk-8.2 - Red	Hawk Architect	>
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp				
	📎 👯 🛃 Esti	imated Image Size:	747.5 MB (37% of 2.0 GB)	2.0 GB
Select Software	Build Target Systen	n Image		
Configure Image Build Image	Use this page to b Build Options	ouild and configure the tar	get system image from the selected softwa	re and configuration settings.
Build		d ISO images instead of m	edia	🨡 Import ISO Images
	Target System I	mage Location:		
	Directory:	/home/architect/images		∮ ØBrowse
	Image Name:	RedHawk-8.2)
			Build Image	
Customize Image Deploy Image				nages have not been imported. media during the build process.

Figure 1-55 Build Image Page

Choose a directory in which to build the target system image and enter it in the Directory field, or click on the Browse button to display a file browser from which to choose.

NOTE

Do not use **/tmp** as the target directory. Packages like "tmpwatch" might remove files that have not been accessed in a certain number of days, thereby sabotaging the image directory.

Choose a name for the target system image and enter it in the Image Name field.

NOTE

Make sure that the directory you specify has enough free disk space to hold one or more target system images, each of which can be several gigabytes in size.

Click on the Build Image button to begin the build process. The rest of this section assumes that you have *not* previously imported the ISOs from their respective media by clicking on the Import ISO Images... button or selecting Media ISO Manager in the Tools menu. Advanced users may wish to do that to avoid inserting media repeatedly. See "Chapter 3: Importing ISO Images" for more information.

Dialogs are presented to guide you through the process of installing the software into the image. For example, you will be prompted to insert specific media, as shown in the following figure. Follow the directions to load the media, then click OK to begin.

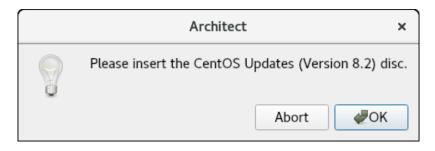


Figure 1-56 Build Prompt to Insert CentOS Updates Media

NOTE

The 8.4 system release installation discs for Rocky, CentOS and Red Hat are created using Blu-ray technology and require a Bluray drive to read the data correctly.

When OK is selected, the CentOS installation begins. The Build Image screen overlays the RedHawk Architect main window and tracks the progress, as shown in the following figure.

Clicking Abort at any time in the build process aborts the build. A confirmation message then displays and you must click on the Close button to close the message box and reactivate the RedHawk Architect main window.

	Image Builder	×
Building imag	e (/home/architect/images/RedHawk-8.2).	.
	15%	
Installing CentOS	Linux 8.2 packages.	11%
Output Log		
dbus-common centos-gpg- centos-rele centos-repo setup-2.12. filesystem- efi-filesys basesystem- pcre2-10.32 libselinux- ncurses-lib glibc-langp	-12:4.3.6-40.el8.noarch -1:1.12.8-10.el8_2.noarch keys-8.2-2.2004.0.2.el8.noarch ase-8.2-2.2004.0.2.el8.x86_64 s-8.2-2.2004.0.2.el8.x86_64 2-5.el8.noarch 3.8-2.el8.x86_64 tem-3-2.el8.noarch 11-5.el8.noarch -1.el8.x86_64 2.9-3.el8.x86_64 s-6.1-7.20180224.el8.x86_64 ack-aa-2.28-101.el8.x86_64 n-2.28-101.el8.x86_64	×
	Ab	ort de CK

Figure 1-57 Status of CentOS Installation

An overall progress bar at the top of the Image Builder screen shows the progress of the entire build; the entire build will be complete once this progress bar is full.

The current stage of the build is listed immediately underneath the overall progress bar, along with a smaller stage-specific progress bar; the current stage of the build will be complete once this stage-specific progress bar is full, and it will reset for the next stage.

An Output Log status area in the lower half of the dialog shows the detailed output that is generated during the entire build, including any error messages generated by the build process. Note that critical error messages result in pop-up error dialogs with which you can interact.

Abort

Click on this button to abort the build. A confirmation dialog displays allowing you to confirm or decline aborting the build process.

οκ

Once the build is completed or aborted, click on the OK button to close the Build Image screen and reactivate the RedHawk Architect main window.

When the CentOS installation is complete, the dialog shown in the following figure appears.

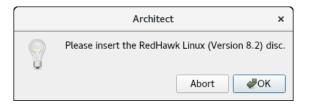


Figure 1-58 Build Prompt to Insert RedHawk Media

Load the RedHawk Linux media, then click OK. The RedHawk installation begins and the Image Builder screen tracks the progress, as shown below.

Image Builder	×					
Building image (/home/architect/images/RedHawk-8.2).						
100%						
The image has been built.						
Output Log						
<pre>Running post-install script. * Fetching RedHawk Linux 8.2 packages. * Installing RedHawk Linux 8.2 packages. Running pre-install script. Installing 6 RPMs: ccur-rt-8.2-20201124.x86_64 ccur-redhawk-setup-8.2-20201124.noarch ccur-redhawk-release-8.2-20201124.noarch ccur-redhawk-release-8.2-20201124.x86_64 ccur-kprel-trace-8.2-20201124.x86_64 Running post-install script. * Configuring image. * The image has been built.</pre>	*					
Save Output Log	∉ОК					

Figure 1-59 Status of RedHawk Installation

The same steps as above will be repeated for any optional software selected during the Select Software step; a prompt will ask the user to insert the product disc and the software will be installed in the target's build image.

Customizing an Image

To further customize the target system image, select Customize Image from the toolbox on the left side of the RedHawk Architect main window. This allows you to customize the following groups:

- Software Updates
- Additional RPMs

- System Services
- Kernel
- File Manager
- Chroot Shell
- Image Cleanup

Each of these customizations will be fully described in the following sections.

NOTE

Image customizations are *not* saved in the session, and will not be automatically re-applied to future images built from the session.

Software Updates

To install RedHawk and NightStar updates into the target system image, click on Software Updates in the Customize Image toolbox. The Software Updates page appears, as shown in the following figure.

		RedHawk-8.2 - Red	Hawk Architect			×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp						
è 🗎 🛱 🚯 🖗	😡 👯 🚅	Estimated Image Size:	2747.4 MB (54% of 5.0 GB)	5.0 GB	*
Select Software	Install Concurre	ent-RT Software Updates				
Configure Image Build Image			NightStar Tools updates in the targe ławk Update CD/DVD (or ISO image			
Customize Image			rtal to download an Update CD/DVI assword to access network reposito		ith the latest upda	ites
Software Updates	Update Optic	ons				
發 Additional RPMs		pdates from CD/DVD (or ISO in			import ISO Images	
System Services		imported ISO image instead of pdates from network (redhawk			import iso images	»
📕 Kernel	Login:					
File Manager						
Chroot Shell			Install Updates			
🦼 Image Cleanup						
				The ISO image	has not been impo	orted.
Deploy Image			You will have to in	nsert media dur	ring the update pro	ocess.

Figure 1-60 Software Updates Page

Installing updates can be done from local media (Discs or ISO images) or directly over the network if the host system is connected to the Internet.

Select Install updates from CD/DVD (or ISO image) if you wish to use local media; then press the Install Updates button and you will be prompted to insert the media.

Select Install updates from network instead of media if you wish to download updates via the Internet. You will need to enter your site's assigned login and password to be granted access to the RedHawk Updates repositories, and you will also need an active maintenance subscription.

Follow the instructions as they are presented. You should see something similar to the following dialog displayed once all updates have been successfully installed.

Software Updater	×
Updating image (/home/architect/images/RedHawk-8.2).	٢
100%	
The image has been updated.	
Output Log	
<pre>Verifying : ccur-rcim-8.2.1-20210331.x86_64 Verifying : ccur-rcim-8.2-20201124.x86_64 Upgraded: ccur-rcim-8.2.1-20210331.x86_64</pre>	6/7 * 7/7
Complete! Installed all applicable updates. * The image has been updated. 4	
Save Output Log Abort	ØK

Figure 1-61 Software Updater Dialog

Additional RPMs

To install additional RPMs into the target system image manually, click on Additional RPMs from the Customize Image toolbox.

The Install Additional RPMs page appears, as shown in the following figure.

RedHawk-8.2 - RedHawk Architect										
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp										
🎯 💮 🖆 🗎 🏟	🥎 👯 🚅	Estimated Image Size:	1272.4 MB (63% of 2 <mark>.</mark> 0 GB)	2.0 GB	-					
Select Software	Install Addition	nal RPMs								
Configure Image	Use this page	e to install additional soft	ware RPMs into the target system image.							
Build Image Customize Image	Click the but	ton below to select any n	umber of RPM files and install them into the image.							
Software Updates	Se	elect RPMs and Install								
Additional RPMs										
System Services										
📕 Kernel										
File Manager										
Chroot Shell										
/ Image Cleanup										
Deploy Image										

Figure 1-62 Install Additional RPMs Page

The Install Additional RPMs page can be used to locate RPM files on the host system and then easily install them into the target system image. Note that the interface supports multiple selection; if you have a set of RPMs that have dependencies upon each other you will need to select all of the RPMs simultaneously to have them properly installed together into the target system image.

Installing Board Support Packages

Concurrent Real-Time provides *Board Support Packages* (BSPs) for several supported SBCs. These BSPs are distributed as RPMs that may be installed in an image using the Additional RPMs page as described above. Contact Concurrent Real-Time (*support@concurrent-rt.com* or 1-800-245-6453) for information on how to obtain BSPs for a particular SBC.

System Services

To customize the settings of the system services that are present in the target image, click on System Services in the Customize Image toolbox. The System Services page appears, as shown in the following figure. Note that the actual list of system services shown depends on the set of packages installed in the target image.

) 🖻 🗄 🚰 🕦 🏟 😣	👯 🛃 E	stimated Image Size:	1510.5 MB (75% of 2.0 GB)	2.0 GB
Select Software	Configure Sy	vstem Services		
Configure Image			abled or disabled in the target system image. T	his includes
Build Image	systemd se	ervices as well as legacy SysV init	scripts.	
Customize Image	Systemd	Services SysV Services		
C Software Updates	Enabled	Service	Description	
		auditd	Security Auditing Service (<u>auditd(8)</u> , <u>ht</u> github.com/linux-audit/audit-document	tps:// ation)
Additional RPMs		auth-rpcgss-module (static)	Kernel Module supporting RPCSEC_GSS	5
System Services		blk-availability	Availability of block devices	
Kernel		ccur-default-kernel	Restore default kernel to the last kerne -d or -D(on BLS systems), or ccur-grub non-BLS systems).	
File Manager		cgconfig	Control Group configuration service	k
Chroot Shell		console-getty	Console Getty (<u>agetty(8)</u> , <u>systemd-gett</u> <u>generator(8)</u>)	ty-
🦼 Image Cleanup		container-getty@ (static)	Container Getty on /dev/pts/%l (<u>agetty</u> getty-generator(8), machinectl(1))	<u>(8), systemd-</u>
© SCAP Scanner		dbus (static)	D-Bus System Message Bus (dbus-dae	<u>mon(1)</u>)
		dbxtool	Secure Boot DBX (blacklist) updater	
		debug-shell	Early root shell on /dev/tty9 FOR DEBU (<u>systemd-debug-generator(8)</u>)	GGING ONLY
		dm-event (static)	Device-mapper event daemon (dmeve	ntd(8))

Figure 1-63 System Services Page

There are tabs for both modern Systemd Services and also legacy SysV Services. Only the system services that are actually present in the built target system image are available for customization on the System Services page.

You can bring up a search box by typing on the page CTRL-F or the '/' character, as noted at the bottom of the page.

Note that any changes made on the System Services page take effect in the target system image immediately.

Kernel

By default you can choose to boot a standard RedHawk kernel in your target image. However you may also wish to customize the kernel to include additional components or possibly to exclude existing components. In order to customize the kernel, you must select the RedHawk kernel source software when configuring the target.

To customize kernel settings for the target image, click on Kernel from the Customize Image toolbox.

The Customize Kernels page appears, as shown in the following figure.

	RedHawk-8.2 - RedHawk Architect	×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp		
è 🗎 🗄 🚯	🥎 ፻드 물로timated Image Size: 2468.7 MB (49% of 5.0 GB) 5.0 GB	÷
Select Software	Customize Kernels	
Configure Image	Use this page to configure the default kernel to boot on the target system, edit kernel boot options, or build cust	om
Build Image	RedHawk kernels.	
Customize Image	Default Kernel to Boot: RedHawk Linux (5.4.66-rt38-RedHawk-8.2-trace) 8.2 (Taal) *	
💩 Software Updates	Fixed Boot Options: net.ifnames=0 biosdevname=0 root=/dev/sda3 ro	
× ·	Extra Boot Options:	
🥰 Additional RPMs		
System Services		
Kernel	Create a custom kernel configuration or import one from the host file system. Configure Custom Kernel based on: RedHawk standard kernel Import Kernel Configuration	
A Keller	Configure custom remet bused on. Real tarres standard remet	
File Manager	You can also export your custom kernel configuration to the host file system.	
Chroot Shell	Export Kernel Configuration	
/ Image Cleanup		
-	Build or remove a custom kernel in the target system image.	
	Build Custom Kernel	
Deploy Image		

Figure 1-64 Customize Kernels Page

The Customize Kernels page allows you to perform different functions with the kernel configuration in the target image.

The Default Kernel to Boot pull-down menu allows you to choose which installed kernel should be the default kernel that boots in the target image. Any change made to this setting is customized in the target system image immediately.

The Fixed Boot Options text area displays the required kernel boot options for the selected kernel; these kernel boot options are fixed and may not be changed by the user.

The Extra Boot Options text field displays optional kernel boot options for the selected kernel; these kernel boot options are fully customizable by the user.

At the bottom of this page there are functions to configure and build custom kernels for the target image. These functions will be described in the following sections.

Note that only one custom kernel configuration, and therefore one custom kernel, can be associated with a specific target system image at any given time.

Configure Custom Kernel

The Configure Custom Kernel button begins the process of creating a custom kernel configuration. The custom kernel configuration is based upon the kernel

configuration that is selected in the drop-down menu that is immediately to the right of the Configure Custom Kernel button.

The choices in the drop-down menu are: RedHawk standard kernel, RedHawk trace kernel, RedHawk debug kernel and Custom kernel (available once a custom kernel configuration has been imported or configured). The first three create new configurations based on the configurations of the standard RedHawk kernels.

The Custom kernel choice bases the new configuration on the current custom kernel configuration that is associated with the image; thus, the Custom kernel choice can be used to further customize a configuration that you have already customized or imported.

Pressing the Configure Custom Kernel button will bring up two different dialog windows. The first dialog window displays overall configuration progress status, as shown in the following figure.

Custom Kernel Manager	×	
Configuring custom kernel in image.		
100%		
The custom kernel has been configured.		
Output Log		
<pre>* Verifying host dependencies. * Verifying kernel source tree in image. * Creating custom kernel configuration from "trace" configuration. scripts/kconfig/confoldconfig Kconfig # # No change to .config # * Launching kernel configuration tool (xconfig). scripts/kconfig/qconf Kconfig # # configuration written to .config # * The custom kernel has been configured.</pre>		
Save Output Log	Abort CK	

Figure 1-65 Custom Kernel Dialog

This window shows the status of running the **ccur-config** command in the target system image kernel source directory.

The **ccur-config** command will eventually bring up the Linux Kernel Configuration window to customize the kernel, as shown in the following figure.

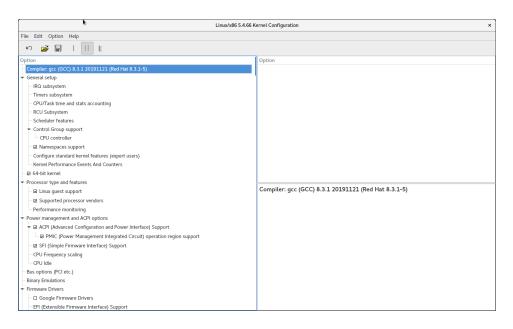


Figure 1-66 Linux Kernel Configuration Dialog

This window allows you to customize almost any aspect of the custom kernel configuration. It is expected that users who are performing this step have a thorough understanding of Linux kernel configuration.

Note that you must Save the kernel configuration before you exit the Linux Kernel Configuration window. Failure to Save the configuration will result in an error being displayed in the Custom Kernel Manager dialog window and no changes to the custom kernel configuration will be made.

NOTE

Certain compilation related RPMs must be installed on the host system in order to successfully configure and build a custom kernel (e.g. **make**, **gcc**). If any of these RPMs are missing you will be presented with a dialog detailing which RPMs must first be installed on the host system before you can proceed.

Import Kernel Configuration

The Import Kernel Configuration button allows you to choose a Linux kernel configuration file on the host system and import it to become the custom kernel configuration in the target image.

Note that once a custom kernel configuration has been imported you can further customize it by using the Configure Custom Kernel button and selecting the Custom kernel to base the configuration on.

Export Kernel Configuration

The Export Kernel Configuration button allows you to copy the target's current custom kernel configuration to the host system.

Compile Custom Kernel

The Build Custom Kernel button allows you to build and install a complete custom kernel in the target image. You must first have created a custom kernel configuration, either by using the Configure Custom Kernel button or by using the Import Kernel Configuration button.

Building a custom kernel compiles each file that comprises the Linux kernel and this process can take quite a bit of time to complete. Once you start the process, you will see the Custom Kernel Manager dialog appear, as shown in the following figure and it will describe the entire process.

	Custom Kernel Manager	×
uilding cu	٢	
	25%	
uilding kerne		
utput Log		
* Setting scripts/k # # No char # * Buildir Running:	ng kernel source tree in image. kernel source configuration to "custom". config/confoldconfig Kconfig ge to .config g kernel. make -j12 bzImage config/confsyncconfig Kconfig arch/x86/include/generated/asm/syscalls 32.h	

Figure 1-67 Initial Build Progress

Initially **ccur-config** will be invoked and once that completes the kernel build stages will begin, as shown in the following figure.

	Custom Kernel Manager	×
Building cu	stom kernel in image.	L
	38%	
Building kernel	modules	
building kernet	mounes.	
Output Log		
CC [M]	arch/x86/kvm/page_track.o	
CC [M]		-
CC [M]		
AS [M]		
CC [M]	block/bfg-cgroup.o	
CC [M]		
CC [M]		
CC [M]		
CC [M]	sound/core/oss/route.o	
CC [M]	sound/core/seq/oss/seq_oss_rw.o	
AS [M]	arch/x86/crypto/camellia-aesni-avx-asm_64.o	
CC [M]		
CC [M]		
CC [M]	arch/x86/crypto/camellia_aesni_avx_glue.o	
		•
		About 400K
		Abort #OK

Figure 1-68 Kernel Build Stages

Finally, once the entire build and install process is complete, the kernel source tree will be cleaned to free up the temporary space used to build the kernel. At this point the entire build process will be complete, as shown in the following figure.

	100%	
ne custom ke	ernel has been built.	
utput Log		
utput Log		
CLEAN	.tmp_versions	
CLEAN		
CLEAN	scripts/basic	
CLEAN		
CLEAN	scripts/kconfig	
CLEAN		
CLEAN	scripts/package	
CLEAN	scripts/selinux/genheaders	
CLEAN		
CLEAN		
CLEAN		ed
CLEAN	.config .config.old .version Module.symvers vmlinux-gdb.py	
* Cleani		
* The cus	stom kernel has been built.	

Figure 1-69 Kernel Build Complete

The custom kernel automatically becomes the default kernel to boot. If this choice is not desired, change the kernel to boot using the Default Kernel to Boot pull-down menu as described above.

Remove Custom Kernel

The Remove Custom Kernel button allows you to remove the current custom kernel from the target image. This will remove the entry in **grub**.conf as well as all of the associated kernel files in the image.

Note that the custom kernel configuration itself is not removed. Thus, it is still possible to build a custom kernel based on the current custom kernel configuration that still remains in the target image.

File Manager

To copy files to and from the host file system and the target system image, click on File Manager from the Customize Image toolbox. Manage Files In Image page appears, as shown in the following figure.

		RedHawk-8.2 - RedH	awk Architec	t		
<u>-</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp						
è 🗎 🗳 🕡 🕸	😥 🚧 🚅	Estimated Image Size:	2747.	4 MB (54% of 5.0 (GB) 5.0 GB	
Select Software	Manage Files ir	ı İmage				
Configure Image	Use this page	to manage files in the target sys	tem image. F	iles can be transfe	erred to and from the host file sys	tem
Build Image	and the targe	t system image.	-			
Customize Image	Host File Sy	stem		Target System Im	nage	
	/	👘 💮 🔊 😭 Filter		/	🗇 📀 📄 🎦 Filter	
Software Updates	Name	Size 🔺 Date Modi	fied	Name	 Size Date Modified 	-
😪 Additional RPMs	🛅 work	2/8/21 9:4	I5 AM	📴 bin	4/14/21 3:23 PM	1
	📒 var	2/8/21 11	:31 AM	🛅 boot	4/14/21 3:22 PM	1
System Services	📒 usr	2/8/21 11	24 AM	🛅 dev	4/14/21 11:01 /	١M
	📁 userland	3/12/21 9	18 AM	📁 etc	4/14/21 3:23 PM	1
📕 Kernel	🛅 tmp	4/14/21 8	:52 AM	🛅 home	5/10/19 8:33 PM	1
File Manager	🛅 sys	5/10/19 8	:33 PM	📴 lib	4/14/21 11:03 /	١M
	🚞 srv	5/10/19 8	:33 PM	📄 lib64	4/14/21 11:03 /	١M
🔳 Chroot Shell	📄 sbin	2/25/21 3	:07 PM	🛅 media	5/10/19 8:33 PM	1
	🛅 run	4/14/216	25 AM	🛅 mnt	5/10/19 8:33 PM	1
🦼 Image Cleanup	🛅 root	4/14/21 8	26 AM	📁 opt	4/14/21 11:03 /	١M
	📁 proc	5/10/19 8	:33 PM	📁 proc	4/14/21 11:01 /	١M
	🛅 opt	2/8/21 1:2	0 PM	🛅 root	4/14/21 11:03 4	١M
	🛅 mnt	5/10/19 8	:33 PM	🛅 run	4/14/21 11:03 4	١M
	🛅 media	5/10/19 8	:33 PM	📴 sbin	4/14/21 3:23 PM	1
	E libe/	2/25/21 2	07 DM *	F= cn/	E/10/10 0-22 DM	∧ ▼
Deploy Image	Allow host	file system to be modified				

Figure 1-70 Manage Files In Image Page

The buttons just below the Host File System and Target System Image headings help you traverse directories in the host and target system, create new directories and do file name searches. To see a menu of the file system operations supported, right click while in either the target or host system boxes.

The default mode does not allow the host file system to be modified. To allow modifications, click on the bottom left of the page on the box labeled Allow host file system to be modified.

Chroot Shell

To customize the target system image manually, click on the Chroot Shell from the Customize Image toolbox. The Customize Image in Chroot Shell page appears, as shown in the following figure.

	example.session - RedHaw	k Architect (on rodrigo)		×
<u>File Edit T</u> ools <u>H</u> elp				
隆 😭 🚰 🔛	😥 🚧 🛃 Estimated Image Size:	883.9 MB (44% of 2.0 GB)	2.0 GB	\$
Select Software	Customize Image in Chroot Shell			
Configure Image Build Image Customize Image	The root directory of the shell will be in the ta All actions done from the Chroot Shell will only affect t	here you can run commands to further custom rget system image. he target system image. The host system will not be aff		age.
Software Updates	Chroot Shell Options Terminal Emulator: xterm Allow local X server to accept X connection	ons launched from shell		
System Services	Mount DNF repositories from imported m Mount /proc, /sys, and /dev from host (re			
Kernel		Run Chroot Shell		
Chroot Shell		k		
Image Cleanup				
SCAP Scanner				

Figure 1-71 Chroot Shell Page

From this toolbox you can open a "chroot" shell in a terminal window. Select the type of terminal from the dropdown and click on the Run chroot Shell button. A terminal screen opens, as shown in the following figure.

The following options are enabled by default in the chroot but can be disabled by clicking on the check-marked box:

- Allow local X server to accept X connections launched from the shell. This option will allow any X application to run on the chroot.
- Mount DNF repositories from imported media ISOs. This option will automatically mount the ISOs you have imported in the build and configure the repositories so that you can run **dnf** operations inside the chroot, on any package in those ISOs.

The following option is disabled by default but can be enabled by clicking on the box:

• Mount /proc, /sys, and /dev from host (read-only) inside the chroot shell. This option will mount the mentioned file systems from the host in the chroot. The file systems are mounted read-only so that no changes can be made on the host system.



Figure 1-72 chroot Shell

This provides a shell with the root directory being the target system image directory. All changes made to system files (including software installed or removed) will be done in the target system image directory only. The host's root file system will not be affected.

Exit the shell when changes are complete.

Image Cleanup

You may reduce the size of the target system image by removing various types of files that may be unnecessary for the image. To remove unnecessary files from the image, click on Image Cleanup in the Customize Image toolbox. Clean up Image page appears, as shown in the following figure.

	RedHawk-8.2	- RedHawk Architect		×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp				
🍓 😭 🖆 😭 🏟	Estimated Image Size:	2747.4 MB (54% of 5.0 GB)	5.0 GB	÷
Select Software	Clean Up Image			
Configure Image	_ Use this page to remove unneeded file	s from the target system image.		
Build Image	Remove Select Files	Remove RPM Database		
Customize Image	Select the types of files to remove fr target system image:	om the This will remove the RPM database target system image.	e from the	
😋 Additional RPMs	PDF documents			
System Services	 Locale archive README, /usr/share/doc etc. 	Once this is done you will not be at or remove RPMs in the target syste		
📕 Kernel				
File Manager	Remove Files	Remove RPM Databa	se	
Chroot Shell				
🦼 Image Cleanup				
Deploy Image				

Figure 1-73 Clean Up Image Page

Select the types of files to remove from the target system image and click the Remove Files button.

To remove the RPM database from the file system click the Remove RPM Database button. Once this is done you will lose all ability to manage RPMs in the image. This cannot be undone. Only do this once you are sure you do not have to add or update any more RPMs in the image.

Deploying an Image

Target system images can be deployed onto target boards in several different ways with RedHawk Architect. Note that it is also possible to deploy target system images without the use of any target hardware with the Virtual Machines deployment method.

- USB Devices. USB devices can be directly flashed with the target system image. This includes USB drives and also CompactFlash cards in CompactFlash-to-USB adapters. These devices can then be inserted into a target board and the board will boot the image upon a restart. See "Deploying to USB Devices" on page 1-62 for more information.
- USB Installer. A USB drive installer can be created with the root file system on it. Architect creates a bootable installation USB drive that will boot on the target and install the root file system onto the target board's local media. Once complete, the USB drive is removed and the board will

boot the image upon a restart. See "Installing via USB drive" on page 1-65 for more information.

- Disc Installer. Disc media installers can be created with the target system image on it. Architect creates a bootable installation disc that will boot on the target and install the root file system onto the target board's local media. Once complete, the disc is removed and the board will boot the image upon a restart. See "Installing via Disc media" on page 1-69 for more information.
- PXE Installer/PXE Diskless. Architect can deploy the target system image over the network. It can deploy an installer that will install the target system image onto the target board's local media, or it can deploy the target system image via NFS for fully diskless booting. See "Installing via PXE over a Network" on page 1-71 for more information on network installation, and see "Booting Diskless via PXE over a Network" on page 1-73 for more information on diskless booting.
- Virtual Machines. Architect can deploy the target system image directly to a virtual machine image that can be booted, via QEMU, directly on the host. See "Deploying to Virtual Machine" on page 1-83 for more information.

The UEFI firmware target configuration is currently supported by all deployment methods. In the USB Device and Virtual Machine deployment methods, the Configure for UEFI firmware box must be set if the intended target system utilizes UEFI firmware. In the other deployment methods (PXE, USB Installer and Disc Installer), there is no UEFI configuration box as those methods work with either UEFI or BIOS systems.

Deploying to USB Devices

To copy a target system image to a USB device, select Deploy Image from the toolbox on the left side of the RedHawk Architect main window and click on the USB Devices button.

This will display the Deploy to USB Devices page, as shown in the following figure.

example - RedHawk Architect ×						
<u>File Edit Tools H</u> elp						
) 🗞 🕞 🖴 😂 🔄	🨡 🚓 🚅 Estimated Image Size: 876.5 MB (43% of 2.0 GB) 2.0 GB	-				
Select Software	Deploy to USB Devices					
Configure Image Build Image	Use this page to install the target system image on a USB storage device connected to this host. That device can then be transferred to the target system and used as the bootable root device of that system.					
Customize Image	Use a CompactFlash USB adapter to install on a CompactFlash card.					
Deploy Image	The settings on the <u>Configure File Systems</u> page will be used to partition the USB device.					
USB Devices	USB Device Options					
USB Installer	Configure for BIOS firmware Configure for UEFI firmware					
🧑 Disc Installer		-				
PXE Installer	Elash USB Device					
→💻 PXE Diskless						
Remote Sync						
Virtual Machines						

Figure 1-74 Deploy to USB Devices Page

The Flash USB Device... button allows you to copy a target system image onto a USB flash device (e.g. a standard USB Flash Drive or a CompactFlash that is connected directly to the host machine via a USB-to-CompactFlash adapter). Note that IDE/SATA CompactFlash adapters are not supported at this time.

Make sure to select the Configure for UEFI firmware check box if the intended target system utilizes UEFI firmware.

NOTE

CompactFlash devices and USB drives can be bought inexpensively at many retail stores that sell computer accessories. Note that the duration of the flashing process depends upon the performance rating of the specific CompactFlash device or USB drive. It is recommended to use CompactFlash devices or USB drives that have a minimum of a 40MB/s read/write performance rating.

Pressing the Flash USB Device... button will begin copying the target root file system onto the USB device. The host system will be scanned for attached USB flash storage devices. If multiple devices are found a choice will be presented to the user, otherwise the sole device found will be selected by default. Once a device is found or chosen, a confirmation dialog similar to the following will appear:



Figure 1-75 Flash Device Confirmation

Press OK to confirm the operation and then the copy will begin, as shown in Figure 1-76.

USB Device Flasher	×
Flashing image to USB device.	<u>e</u>
57%	
Copying image files to '/dev/sdd'.	0%
Output Log	
Using device /dev/sdd (ASolid USB). * Wiping device '/dev/sdd'. * Partitioning device '/dev/sdd'. * Creating file systems on '/dev/sdd'. Making xfs file system for '/on '/dev/sdd'. Making swap file system for 'swap' on '/dev/sdd2'. * Mounting file systems on '/dev/sdd'. Mounting '/ on '/dev/sdd3'. Mounting '/ boot' on '/dev/sdd1'. * Copying image files to '/dev/sdd'.	
	Abort @OK

Figure 1-76 Flash Copy In Progress

Note that no initial check is made to determine whether the image will fit onto the size of the selected USB device. If the copy fails because of insufficient space, an error message will be displayed

If the USB device is large enough to hold the image, and no other error occurs during the copy, a success dialog will be presented, as shown in Figure 1-78.



Figure 1-77 Device Removal Notification

Remove the USB device if desired and then click OK to continue.

You will now be presented with a final dialog indicating that the transfer is complete.

USB Device Flasher		×
lashing image to USB device.		
100%		
he image has been flashed to the USB device.		
Dutput Log		
* Creating file systems on '/dev/sdd'.		
Making xfs file system for '/' on '/dev/sdd3'.		
Making xfs file system for '/boot' on '/dev/sdd1'.		
Making swap file system for 'swap' on '/dev/sdd2'.		
* Mounting file systems on '/dev/sdd'. Mounting '/' on '/dev/sdd3'.		
Mounting '/ on '/dev/sdd3'.		
* Copying image files to '/dev/sdd'.		
* Installing grub bootloader on '/dev/sdd'.		
* Unmounting (and flushing) file systems on '/dev/sdd'.		
Unmounting '/boot'. Unmounting '/'.		
* Cleaning up.		
* The image has been flashed to the USB device.		
		T
Save Output Log	Abort	₫ок

Figure 1-78 Flash Copy Completed

Installing via USB drive

To create a bootable USB drive that will install the target system image into a target system, select USB Installer from the toolbox on the left side of the RedHawk Architect main window.

This will display the Deploy via Installation USB Drive page, as shown in the following figure.

·		example - R	edHawk Architect		×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp					
) 🗞 😭 🖆 🖆 🔄	😡 🚧 💻	Estimated Image Size:	876.5 MB (43% of 2.0	GB)	2.0 GB
Select Software	Deploy via Inst	allation USB Drive			
Configure Image	Use this page	e to create a bootable USE	3 drive that can be used to install the	image on target sy	/stems.
Build Image	The disk dev	ices specified on the Confi	igure File Systems page will be install	ed on the target sy	ystem.
Customize Image	USB Drive O	ntions			
Deploy Image	Serial Cons				
USB Devices			when USB drive is booted		
USB Installer	Encrypt	installation image (passw	ord required to install)		
🧑 Disc Installer			🔋 Make Installation USB Drive		
• PXE Installer					
→ 📃 PXE Diskless					
Remote Sync					
Virtual Machines					

Figure 1-79 Deploy via Installation USB Drive Page

Press the Make Installation USB Drive... button to write a bootable installer image to an attached USB drive.

Choose the Serial Console setting that the target system will use for communicating with the host. If set to none the target will default the console to the VGA display.

Check the box labeled Automatically install image to disk when USB drive is booted to create a USB drive that will install the target system image onto a target board's local disks without any prompting or user interaction.

NOTE

This will destroy any data on the target system's local disks and therefore automatic installations should be used carefully; however, it is useful on systems without an attached console display or configured and connected serial console.

Check the box labeled Encrypt installation image (password required to install) if encryption of the target image is desired. You will be prompted for a password which will be required when installing the target. Note that the

Automatically install image to disk and the Encrypt install image options cannot both be set.

Also note that if there is more than one disk on the target system, Architect will take an educated guess at the most appropriate disk to use based on your configuration. For example, if you've configured an **sda** disk, it will choose a SATA disk over a NVMe disk. Nevertheless, it is suggested that you use the interactive installation method if you do not want to run the risk of over-writing a disk.

In an automatic installation you are still given 10 seconds to intervene. If you hit any key during the 10 seconds you will be presented with an interactive menu.



Figure 1-80 Automatic installation on target without user interaction

The default mode is an interactive installation. In this mode, the installation on the target will stop at the page shown below until a choice is entered. Press ENTER to continue with the interactive installation.



Figure 1-81 Interactive installation on Target

In an interactive installation you will be able to map disks configured in Architect with the physical disks on the target system.

The screen that follows shows two disks were configured in Architect but three disks were found on the target system. In this example, the two disks configured in Architect, **sda** and **sdb**, have been reassigned from the mapping suggested by Architect.

```
Would you like to change any disk assignments? (y/n) [n] y
Which disk assignment would you like to change? (sda/sdb) sda
Choose a local disk to use for "sda":
  * 1) 465.8G ATA WDC WD5003ABYX-0 (/deu/sda)
    2) 1.8T ATA ST2000NM0008-2F3 (/dev/sdb)
    3) 29.3G ASolid USB (/deu/sdc)
: 2
The following disk assignments will be used for this installation:
    sda => 1.8T ATA ST2000NM0008-2F3 (/deu/sdb)
    sdb => 465.8G ATA WDC WD5003ABYX-0 (/dev/sda)
Would you like to change any disk assignments? (y/n) [n] y
Which disk assignment would you like to change? (sda/sdb) sdb Choose a local disk to use for "sdb":
  * 1) 465.8G ATA WDC WD5003ABYX-0 (/dev/sda)
    2) 1.8T ATA ST2000NM0008-2F3 (/deu/sdb)
    3) 29.3G ASolid USB (/deu/sdc)
: 3
The following disk assignments will be used for this installation:
    sda => 1.8T ATA ST2000NM0008-2F3 (/deu/sdb)
    sdb => 29.3G ASolid USB (/dev/sdc)
Would you like to change any disk assignments? (y/n) [n]
```

Figure 1-82 Remapping of configured disks to physical disks on target

When you have finished with the disk assignments, the installation will resume without further user interaction.

Installing via Disc media

To create a bootable disc media that will install the target system image into a target system, select Disc Installer from the toolbox on the left side of the RedHawk

Architect main window. This will display the Deploy via Installation Disc page, as shown in the following figure.

	example	- RedHawk Architect	×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp			
è 🖻 🖹 🕤 🖗	Estimated Image Size	: 876.5 MB (43% of 2.0 GB)	2.0 GB
Select Software	Deploy via Installation Disc		
Configure Image	Use this page to create ISO images systems.	and burn them to optical media that can be used t	o install the image on target
Build Image Customize Image	-	2 1001	
Deploy Image	Create Disc Create ISO Image	Burn ISO Image	
USB Devices		reated and burned to a disc for the current target <u>Configure File Systems</u> page will be installed on th	
USB Installer	Disc Options		
Disc Installer	Serial Console: none 👻		
PXE Installer	 Automatically install image to Encrypt installation image (page 1) 		
→ PXE Diskless	Device: /dev/sr1 - Spec	ed: Maximum 👻	Rescan Devices
Remote Sync			
Virtual Machines		Nake Installation Disc	

Figure 1-83 Deploy via Installation Disc Page

Choose Create Disc tab to directly burn a disc that will install the target system image onto disc media. No ISO image will be saved on disk in this mode.

Choose Create ISO Image tab to create an ISO file that contains an installer image. This ISO image can be later burned to a disc, or it may be useful with other tools or for long term storage.

Choose Burn ISO Image tab to burn a previously created ISO image to disc media.

Check the box labeled Automatically install image to disk when disc is booted in the Create Disc tab or the Automatically install image to disk when ISO is booted in the Create ISO Image tab, to create a disc or ISO that will install the target system image onto a target system without any prompting or user interaction. In the "Installing via USB drive" section, starting on page 1-66, there is a full description of this option.

Check the box labeled Encrypt installation image (password required to install) if encryption of the target image is desired. You will be prompted for a password which will be required when installing the target. Note that the Automatically install image to disk and the Encrypt install image options cannot both be set.

NOTE

DVD and Blu-ray are the currently supported disc media. Writing a bootable installer image onto a CD disc is not supported at this time.

The size of the compressed image is printed during the process when you press Make Installation Disc from the Create Disc tab and also when you press Make ISO Image from the Create ISO Image tab.

Depending on which operation mode is chosen, various options will be available for selection. Choose the options and settings that are appropriate for your specific needs.

Installing via PXE over a Network

RedHawk Architect can deploy a target system image to a target system over an Ethernet network connecting the host machine to the target machine. Installation of the root file system is performed by first creating a PXE-bootable installation image. A target machine can boot this installation image via PXE, which will then remotely copy the target system image into the target's local drive media.

This deployment method does not require the preparation of any removable installation media and it is often the fastest installation deployment method, however it does require some initial networking configuration on both the host and target systems.

NOTE

Various host system networking services must be properly configured before attempting to deploy a PXE-bootable installation image for the first time. If you have not configured the host networking services yet, you will need to invoke the PXE Target Manager and choose to Initialize PXE Services. See "Managing PXE Targets" on page 4-7 for more information.

To create a PXE-bootable installation image that will install the target system image over a network into a target system, select PXE Installer from the toolbox on the left side of the RedHawk Architect main window. The Deploy via PXE Installation page will then appear, as shown in the following figure.

~		example.ses	sion - RedHawk Architect	×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp				
🖻 🖆 🖆 🔞) 🛞 👯 🛃	Estimated Image Size:	1063.7 MB (53% of 2.0 GB)	2.0 GB
Select Software Configure Image Build Image Customize Image Deploy Image USB Devices USB Installer OVD Installer OVD Installer PXE Installer PXE Diskless Remote Sync Virtual Machines	Deploy via PXE Use this page to remotely ii The disk devi PXE Installati Serial Cons Automat Encrypt	Installation to create a PXE installation tall PXE-bootable target ces specified on the <u>Confi</u> on Image Options ole: <u>none</u>	on image for the current target system image. A PXE installation t systems over the network. gure File Systems page will be installed on the target system. when target system is PXE-booted ord required to install)	

Figure 1-84 Deploy via PXE Installation Page

Choose the Serial Console setting that the target system will use for communicating with the host. If set to none the target will default the console to the VGA display.

Check the box labeled Automatically Install Image to disk when target system is PXE-booted to create a PXE image that will install the target system image onto a target system without any prompting or user interaction. In the "Installing via USB drive" section, starting on page 1-66 there is a full description of this option.

Check the box labeled Encrypt installation image (password required to install) if encryption of the target image is desired. You will be prompted for a password which will be required when installing the target. Note that the Automatically install image to disk and the Encrypt install image options cannot both be set.

Enter a PXE Image Name for the installation image that will be created. Each installation image must have a unique name to identify it, though the names can be arbitrarily chosen by the user. Multiple images may be created and shared between targets. See "Managing PXE Images" on page 4-3 for more information.

Press Make PXE Installation Image to begin building the named PXE installation image.

NOTE

The PXE installation images are placed under a directory named architect which must reside under the system's tftpboot directory. The tftpboot directory defaults to /var/lib/tftpboot. While this directory is configurable, at this time the Architect tool only supports the default location.

Packing the PXE installation image will take several minutes. Once complete the PXE Installation Image Builder dialog will appear as shown in the following figure.

PXE Installation Image Builder	×
Building PXE installation image (RedHawk-8.2).	
100%	
The PXE installation image has been built.	
Output Log	
 Packing image directory. Configuring installation image. The PXE installation image has been built. 	
Save Output Log	Abort #OK

Figure 1-85 PXE Installation Image Building Complete

Press Okay to dismiss the dialog.

Once the PXE installation image is successfully built you can use the PXE Target Manager to schedule installation of the image for specific targets, and you can use the PXE Image Manager to edit or delete PXE installation images. See "Managing PXE Targets" on page 4-7 for more information.

Booting Diskless via PXE over a Network

Architect can create and then deploy a PXE-bootable diskless image to a diskless target system. When you select PXE Diskless from the toolbox on the left side of the RedHawk Architect main window, the Deploy to Diskless Systems page will be displayed.

The Deploy to Diskless Systems page provides two different implementations for booting diskless. The first implementation NFS uses NFS, the second labeled RAMDISK uses a Live RAMDISK.

Host and target connect over an Ethernet network. This deployment method does not require any local drive media to be present on the target system; any local drive media that is present on the target will be untouched and ignored. This method also requires some initial networking configuration on both the host and target systems. Note that the file system configuration for this deployment method is custom and ignores the settings in the File Systems configuration page.

With NFS, the target machine boots a diskless image via PXE, which will then mount the target system image via NFS. In a Live RAMDISK boot, the entire target system image is downloaded to the target's RAM.

NFS versus Live RAMDISK considerations:

- Persistent Storage: with the NFS option, the kernel mounts the root file system read-only over NFS but the user may optionally configure persistent storage via the Configure Read-only Root Settings link explained below. With the Live RAMDISK option, the entire root file system is writable but volatile.
- Network Connection: with the NFS option, the host and target must maintain an Ethernet working connection for the duration of the time the target is booted. With the Live RAMDISK, the connection is required only for booting.
- Boot time and RAM Allocations: with the NFS option, the read-only root file system is accessed via NFS although some system directories that require to be writable are RAM-based and volatile. With the Live RAMDISK option the entire SquashFS root file system is downloaded and copied to RAM during the boot.

NOTE

Various host system networking services must be properly configured before attempting to make an NFS diskless installation image and before booting a RAMDISK diskless installation image. If you have not configured the host networking services prior, you will instead be presented with a page allowing you to Initialize PXE Services. See "Managing PXE Targets" on page 4-7 for more information. Once PXE Services have been initialized you will be allowed to continue. To create a PXE-bootable diskless image that will mount the target system image via NFS select the NFS tab and the page, shown in the figure below, will appear.

[example - RedHawk Architect	×
<u>File Edit T</u> ools <u>H</u> elp		
🎯 🚯 🗳 🖆 🚳		*
Select Software	Deploy to Diskless Systems	
Configure Image Build Image	Use this page to create a diskless image for the current target system image. Target systems can boot this im disklessly. Multiple targets may use a single diskless image simultaneously.	age
Customize Image	All settings on the Configure File Systems page will be ignored and no disks on the target systems will be used	l.
Deploy Image	NFS RAMDISK	
USB Devices	An NFS diskless image is booted with the root file system NFS-mounted (read-only) over the network. Read- only root support makes select parts of the root file system writable but volatile on the running system.	
👖 USB Installer	PXE Options for NFS Diskless Image	ings
Disc Installer	Target PXE/DHCP Interface: eth0 •	
PXE Installer	Serial Console: none Kernel to Boot: vmlinuz-5.10.59-rt52-RedHawk-8.4-trace	
→ PXE Diskless	Fixed Kernel Options: root=nfs:10.134.30.4:/var/lib/tftpboot/architect/diskless/example.session/root ro ip=::::eth0:dhcp net.ifnames=0 biosdevname=0	
🔁 Remote Sync	Extra Kernel Options:	
Virtual Machines	Boot Timeout: 3	
	PXE Image Name: example.session	
	-> Make NFS Diskless Image	
	↔ PXE Image Manager	nager

Figure 1-86 Initial PXE NFS Diskless Deployment Page

				example - Re	dHawk Architect			×
<u>File</u> <u>E</u> dit <u>T</u> ool	s <u>H</u> elp							
3 😭 🗎		¢	🥎 👯 🚅	Estimated Image Size:	876.5 ME	(43% of 2.0 GB)	2.0 GB	*
Select Software			Deploy to Disk	less Systems				
Configure Image Build Image		$\overline{}$		e to create a diskless image fultiple targets may use a s			tems can boot this imag	je
Customize Image		$\overline{}$	All settings o	n the <u>Configure File Syster</u>	<u>ns</u> page will be ignored	and no disks on the targe	t systems will be used.	
Deploy Image		<u> </u>	NFS RA	MDISK				
📇 USB Dev	ices			C diskless image is booted of but volatile on the running		a SquashFS Live image. Th	e entire root file system	n
📋 USB Inst	aller		PXE Option	ns for RAMDISK Diskless Im	age			
🧑 Disc Inst	aller			nsole: none 👻				
••••• PXE Inst	aller			Boot: vmlinuz-5.10.59-rt nel Options: ro net.ifname				
→ 🖳 PXE Disk	less			nel Options:				
Remote	Sync		Boot Tim	eout: 3 🌲				
Virtual M	lachines		PXE Imag	e Name: example.session		•		
					→ Make RAMDISK D	iskless Image		
						PXE Image Manager	🚅 PXE Target Mana	ger
						PXE Image Manager	PXE Target Mana	ger

When the RAMDISK tab is selected, a different but similar page will appear as shown in the figure below.

Figure 1-87 Initial PXE RAMDISK Diskless Deployment Page

The following settings are common to both creating an NFS and a RAMDISK bootable diskless image, with the exception of the Configure Read-only Root Settings and the Target PXE/DHCP Interface which pertains only to making NFS diskless images.

Choose the Target PXE/DHCP Interface network interface that the target system will use for communicating with the host. The target hardware must be configured to perform a PXE broadcast on this network interface at boot time.

Choose the Serial Console setting that the target system will use for communicating with the host. If set to none the target will default the console to the VGA display.

Choose the Kernel to Boot for the target. This will default to the kernel that has already been chosen as the default in the Kernel Manager, however a diskless image may specify a different default if desired.

The Fixed Kernel Options text area displays the required kernel boot options for the selected kernel; these kernel boot options are fixed and may not be changed by the user.

Enter any Extra Kernel Options that you would like to use for the diskless image. All kernel parameters specified here will be appended to the kernel's boot-time options. See the **kernel-parameters.txt** file in the kernel source Documentation directory for a complete list of the standard boot options. Modify the BOO† Timeout count to change the number of seconds the boot menu will be displayed before the diskless image will start booting. Increase the timeout if you wish to have more time to interrupt the boot menu to choose different kernels or boot options.

The Configure Read-only Root Settings pertains only when making NFS diskless images but not RAMDISK diskless images. Click on this link to adjust the size of RAM space alloted for temporary storage space. Use the up and down arrows to change the default size. Persistent storage, private to each target, can be accessed on the target under /var/lib/stateless/state and on the nfs server under /var/lib/tfptboot/clientstate/<target-system>.

Enter a PXE Image Name for the diskless image that will be created. Each diskless image must have a unique name to identify it, though the names can be arbitrarily chosen by the user. Multiple images may be created and shared between targets. See "Managing PXE Images" on page 4-3 for more information.

When choosing to create an NFS Diskless Image, Press Make NFS Diskless Image to begin building the named PXE diskless image.

Creating the PXE NFS diskless image should take several minutes. Once complete the PXE Diskless Image Builder dialog will appear as shown in the following figure.

PXE Diskless Image Builder	×
Building PXE diskless image (RedHawk-8.2).	·> <u>=</u>
100%	
The PXE diskless image has been built.	
Output Log	
 Removing existing PXE diskless image. Creating NFS diskless image root. Configuring NFS diskless root. Configuring PXE diskless image. The PXE diskless image has been built. 	
Save Output Log	Abort CK

Figure 1-88 PXE NFS Diskless Image Building Complete

Press Okay to dismiss the dialog.

When choosing to create a RAMDISK Diskless image, Press Make Live RAMDISK Diskless Image to begin building the named PXE diskless image.

Creating the PXE RAMDISK Diskless image should take several minutes. Once complete the PXE Diskless Image Builder dialog will appear as shown in the following figure.

PXE Diskless Image Builder	×
Building PXE diskless image (RedHawk-8.2-RAM).	
100%	
The PXE diskless image has been built.	
Output Log	
* Creating Live RAMDISK image. Creating SquashFS of root Building initrd file * Configuring PXE diskless image. * The PXE diskless image has been built.	
Save Output Log	Abort @OK

Figure 1-89 PXE RAMDISK Diskless Image Building Complete

Press Okay to dismiss the dialog.

NOTE

The PXE diskless images are placed under a directory named architect which must reside under the system's tftpboot directory. The tftpboot directory defaults to /var/lib/tftpboot. While this directory is configurable, at this time the Architect tool only supports the default location.

Once the PXE diskless image is successfully built you can use the PXE Target Manager to configure diskless booting of the image for specific targets, and you can use the PXE Image Manager to edit or delete PXE diskless images. See Section "Managing PXE Targets" on page 4-7 for more information.

Remote Sync

Synchronization between a target system and the target system image on the host is supported by the Remote Sync function found in the toolbox on the left side of the RedHawk Architect main window.

Changes made on the target can be applied to the target system image (sync from target) and changes made in the target system image can be applied to the target (sync to target).

Following is a summary of the steps:

1. Configure the target for syncing in the PXE Target Manager page.

- 2. Reboot the target.
- 3. Select the target in the Synchronize with Remote Targets page.
- 4. Click on the desired sync action button in the Synchronize with Remote Targets page.

To configure the target for synchronization, from the Architect PXE Target Manager page, click on the desired target and use the Edit Target button to select Start remote sync process as shown below:

Edit PX	Æ Target ×				
Editing target 'speedy'.					
Hostname: speedy					
IP Address: 192.168.1.6					
MAC Address: C8:F7:50:FC	::47:BA				
On Next Boot					
 Boot local disk 					
\bigcirc Install local disk with:	RAM-analyzer.diskless 👻				
\bigcirc Boot diskless with:	RedHawk-8.2 (NFS) -				
Start remote sync process					
	Cancel				

Figure 1-90 Configure target 'speedy' for remote sync

Press OK and you will see the menu showing the target has been configured to sync on the next boot as shown below:

		Archite	ect PXE Target Manager		×			
PXE-boo	PXE-bootable target systems must be configured here before deploying PXE installation or diskless images.							
Hostname 🔻	IP Address	MAC Address	Next Boot	Status				
speedy	192.168.1.6	C8:F7:50:FC:47:BA	sync					
sphynx	192.168.1.11	C8:1F:66:06:84:A8	install (RAM-analyzer.diskless)					
💠 Add Target	💠 Add Target 📕 🖛 Remove Target 🛛 🍋 Edit Target 🗽 Add Multiple Targets 🖗 Refresh							
View DHCP	Configuration	Reinitialize PXE S	ervices					
1 target set to b	e installed on ne	ext PXE boot.		×C	lose			

Figure 1-91 Target 'speedy' configured for remote sync

Reboot the target system and you will see a splash screen with a count down of 10 seconds. If you hit any key during those 10 seconds, you will be presented with the menu shown below. Note that the default is a non-interactive sync as no interaction is really required but, for this example, an interactive sync was chosen.

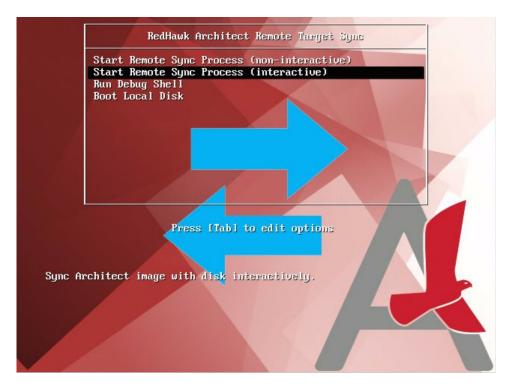


Figure 1-92 Sync Menu with interactive selected

On the target system you will see some start-up messages and then the 'waiting for host' message. Note that you do not have to wait for this message as the host and target will wait for each other.

Start Remote Sync from Architect to continue. (waiting for host...)

Figure 1-93 Waiting on host

Now on the host system, go to the Remote Sync Deployment Page and verify that the target's name appears in the Target to Sync with: box and then press on the desired action: Sync From Target or Sync to Target.

In Sync To Torget, the target will be updated with changes made in the target system image. Files added or deleted in the target system image will be added or deleted on the target system.

In Sync From Target, the target system image will be updated with changes made in the target system. Files added or deleted in the target system will be added or deleted on the target system image.

For this example, Sync To Target, was selected:

		example - R	edHawk Archite	ect		×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp						
📑 😭 😭 🕅	🥹 🛞 🎮 🚅	Estimated Image Size:	8	76.5 MB (43% of 2.0 GB)	2.0 GB	÷
Select Software	Synchronize w	ith Remote Targets				
Configure Image Build Image		made on a previously dep target system image can		tem can be copied to the target system existing target system.	image, or ch	anges
Customize Image	Changes in f will be ignor		annot be synchr	onized and all settings on the <u>Configure</u>	File Systems	page
Deploy Image	Remote Syn	c Options				
USB Devices		Sync with: speedy	•			
USB Installer	Configure	argets for syncing in the P	KE Target Manag	er.		
🧑 Disc Installer		From Target		→ Sync To Target		
• PXE Installer		e target system image wit ave been made on the targ		Update target with changes that made in the target system image		
→💻 PXE Diskless						
Remote Sync						
Virtual Machines						
				PXE Image Manager	PXE Target	Manager

Figure 1-94 Sync To Target 'speedy'

Once you pressed one of the sync buttons on the host, you will get a prompt on the target asking if you wish to continue (if in interactive sync mode). Type 'y' to continue. When the sync completes, the messages on the target system will look similar to the ones on the following page:

Start Remote Sync from Architect to continue. (waiting for host...)
This tool will synchronize the file systems on this system with the Architect image 'RedHawk-8.2'.
Do you wish to continue? (y/n) y
Mounting disk file systems.
Syncing target with Architect image 'RedHawk-8.2'.
(waiting for host to finish sync...)
Host finished syncing.
Unmounting disk file systems.
Syncing is complete!
Removing PXE config file (0A861EAC) from server.
Press ENTER to reboot. _

Figure 1-95 Synchronization complete; messages on the target

After the synchronization, the target system must be rebooted. This happens automatically in the non-interactive mode while in the interactive you have to press ENTER to reboot the system.

In this example, a new software package was installed in the target system image and it was applied to the target via the Sync to Target function. The output log below shows the **rpm** related files added to the target system:

Remote Target Synchronization	×
Synchronizing target "speedy" with target system image.	\$
100%	
Synchronization complete.	
Output Log	
<pre>var/lib/rpm/Group var/lib/rpm/Installtid var/lib/rpm/Packages var/lib/rpm/Packages var/lib/rpm/Requirename var/lib/rpm/Requirename var/lib/rpm/Sha1header var/lib/rpm/_db.001 var/lib/rpm/_db.001 var/lib/rpm/_db.002 var/lib/rpm/_db.003 var/lib/systemd/random-seed var/lib/systemd/catalog/database * Synchronization complete. 4</pre>	
Save Output Log	Abort CK

Figure 1-96 Synchronization Complete Messages on Host

Deploying to Virtual Machine

To deploy a target system image to a virtual machine image which can be booted in a virtual machine, click on the Virtual Machine button. This will display the Deploy to Virtual Machine page, as shown in the following figure.

		example - R	edHawk Architect			×
<u>File Edit T</u> ools <u>H</u> elp						
è 🖻 🗄 🕤 🕸	😔 🚧 🛃 Estimat	ed Image Size:	876.	5 MB (43% of 2.0 GB)	2.0 GB	*
Select Software	Deploy to Virtual Machi	nes				
Configure Image	Use this page to creat	e and boot virtu	al machine disk imag	jes.		
Build Image Customize Image	Create VM Boot	VM Sync VM	Export to VMM	Export to KVM-RT		
Deploy Image	-			rrent target system image. used to partition the disk image.		
USB Devices	The seconds on the	configure rite by	puge with be	used to partition the disk image.		
🗓 USB Installer	VM Disk Image Opti	ons				
Disc Installer	Virtual Disk Size:	3 GiB 🏮		igure for BIOS firmware igure for UEFI firmware 📃 Secu	ire boot	
• PXE Installer	VM Disk Image Lo	cation:				-
→ 💻 PXE Diskless	Directory: /var	/lib/architect/VM	s			e
Remote Sync	File Name: example a second se	nple.session.img			9	
Virtual Machines			Make	VM Image		
			Tiake	vi mage		

Figure 1-97 Deploy to Virtual Machines Page

The Deploy to Virtual Machines Page defaults to the CREATE VM tab. In this mode, pressing the Make VM Image button will simply create a virtual machine image file from the session's target system image. The name and location of the virtual machine image file created can be customized using the Directory and File Name text fields, and the directory Browse button.

Make sure to select the Configure for UEFI firmware check box in the VM Disk Image Options section if the intended target system utilizes UEFI firmware.

Selecting the BOO[†] VM tab allows you to boot a previously created virtual machine image directly on the host using the QEMU PC System Emulator. Choose the virtual machine image using the Disk Image to BoO[†] text field or the file Browse button.

Selecting the Sync VM tab allows you to perform file synchronization between the target system image and the virtual machine disk image in both directions:

• Use the Sync From VM button to update the target system image with all file changes that have been made inside the booted virtual machine image.

• Use the Sync To VM button to update the virtual machine with all the changes that have been made in the target system image. The exported changes will be visible in the virtual machine disk image the next time it is booted using QEMU.

These two synchronization features provide additional flexibility for customizing a target system image. Image customization can also be accomplished inside a booted virtual machine, and this customization is very natural as the environment closely resembles the final booted environment that will be available on the actual target hardware.

Selecting Export to VMM allows you to utilize a previously created virtual machine image with very flexible and powerful virtual machine management tools provided on the host. Once the image has been exported, the graphical VMM tools can boot and manipulate the image completely independently of Architect. See the **virt-manager**(1) man page for more information.

Selecting Export to KVM-RT allows you to utilize a previously created virtual machine image with KVM-RT. RedHawk KVM-RT is a Real-Time Hypervisor solution utilizing QEMU/KVM and RedHawk Linux real-time kernel features.

Editing an Existing Session

A session can be saved at any time and loaded later to continue work on a target system image.

To save the current session click on the Save Session icon \exists or on Save Session in the File menu. Selecting Save Session As in the File menu displays a file selection dialog and allows you to save the current session using a different name.

To make a copy of the current session click on the Duplicate Session icon in Duplicate Session in the File menu. Duplicating a session makes a copy of the current session and optionally copies an existing image to go with it.

To load an existing session, click on the Open Session icon \bowtie or on Open Session in the File menu. You may also click on the Open button from the opening dialog when Architect first starts.

Architect includes support for enhancing the security of deployed target systems. This includes configuring, creating, and deploying target system images with FIPS, SELinux and SCAP security policy enabled.

UEFI Secure Boot is also supported, however, Architect configuration is only required when deploying the target to a virtual machine.

Note that SCAP support is provided in the Advanced Security Edition of Architect by an optional package named **ccur-architect-security**. If this package is not installed on the system, the SCAP security extension will not be available.

Note

The images shown in this chapter were captured on a system with the optional **ccur-architect-security** package installed. The SCAP functionality will be missing and the SCAP menu options will not be visible if you do not have the package installed.

The following instructions are specific to enabling the various security extensions in a target image. These are additions to the instructions in the previous chapters.

UEFI Secure Boot

Secure Boot is a UEFI firmware security feature that ensures only immutable and signed software are loaded during the boot time. To boot a target in UEFI Secure Boot mode, follow the instructions in the "UEFI Secure Boot" Appendix of the RedHawk Release Notes.

Architect only needs to know about UEFI Secure Boot when deploying a virtual machine image so that it can simulate firmware changes. In the case of booting a virtual machine target, check the Secure Boot box in the Create VM tab of the Deploy to Virtual Machines page as shown in the image below.

		example - Re	dHawk Architect				×
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp							
🏟 🗊 🖆 🛍 🤞	阙 🚧 🛃 Es	timated Image Size:	876.	5 MB (43% of 2.0 GB)		2.0 GB	*
Select Software	Deploy to Virtual N	Machines					
Configure Image	Use this page to	create and boot virtua	l machine disk imag	es.			
Build Image Customize Image	Create VM	Boot VM Sync VM	Export to VMM	Export to KVM-RT			
Deploy Image		ne disk image will be c		5 /	5		
USB Devices	The settings or	n the <u>Configure File Sy</u> s	stems page will be i	used to partition the d	isk image.		
👔 USB Installer	VM Disk Image	Options					
isc Installer	Virtual Disk S	Size: 3 GiB		igure for BIOS firmwa igure for UEFI firmwar		oot	
• PXE Installer	VM Disk Ima	ge Location:					-
→ 📃 PXE Diskless	Directory:	/var/lib/architect/VMs	;			Srowse	
Remote Sync	File Name:	example.session.img				•	
Virtual Machines			📦 Make	VM Image			

Figure 2-1 Secure Boot Configuration for virtual machines

Configuring SELinux

Before building the target system image, configure SELinux in the image via the Configure SELinux page. Click on the SELinux button of the Configure Image toolbox to display the Configure SELinux page. By default, SELinux is disabled in RedHawk but it can be configured in the permissive or enforcing mode. See figure below.

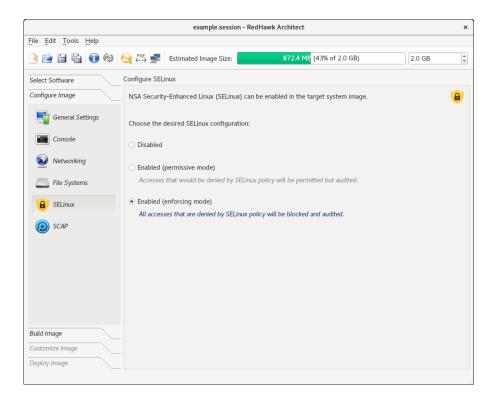


Figure 2-2 SELinux enabled in the enforcing mode

Alternatively, SELinux can be configured after the target's image is built. After the target's image is created and following a change in the SELinux configuration, the user will be prompted to update the target system image. Click on the button labeled Update Image that appears at the bottom of the page to update the target's image. See figure below.

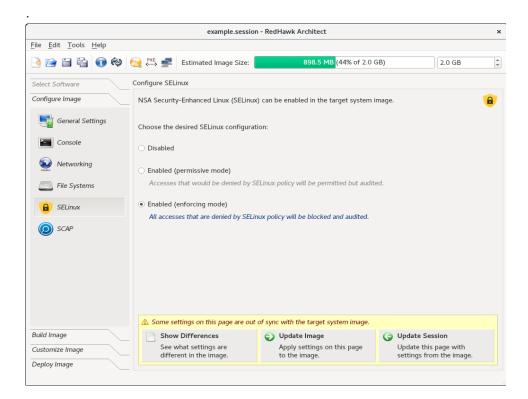


Figure 2-3 SELinux enabled after the target image is built

Note

SELinux support is not possible over NFS, therefore, the diskless deployment method that uses NFS is not supported.

Note

Optionally after the target system image is built, the target's software can be automatically updated via the SOftware Updates button of the Customize Image toolbox. If the **ccur-redhawk-setup** package is updated, the SELinux configuration will be reset to disabled as this is the default for RedHawk systems. This package is rarely updated but in such a case, reconfigure SELinux after the software update.

Customizing the kernel with FIPS

To enable support for the Federal Information Processing Standards (FIPS) in the kernel, the boot option fips=1 must be set in the Extra Boot Options text field of the Customize Kernels page. This must be set for each kernel to be booted on the target.

It is not necessary to rebuild a kernel. All that is required is to add the FIPS boot option as highlighted in the example below.

		example.session - Re	edHawk Architect		>
<u>F</u> ile <u>E</u> dit <u>T</u> ools <u>H</u> elp					
è 😭 😫 😭 🏟	😥 👯 🚅	Estimated Image Size:	898.5 MB (44% of 2.0 GB)	2.0 GB	÷
Select Software	Customize Ke	rnels			
Configure Image	Use this pag	e to configure kernel boot opti	ons or to configure and build custom RedHav	vk kernels.	
Build Image					
Customize Image	- 1	rnel boot options in the target s	, ,		
📥 c a			.10.59-rt52-RedHawk-8.4-trace) 8.4 (Hadron		
🤤 Software Updates	Fixed Boot C	Options: net.ifnames=0 biosde	vname=0 boot=/dev/sda1 root=/dev/sda1 ro)	
Additional RPMs	Extra Boot C	Options: fips=1			
System Services					
1	Create a cust	tom kernel configuration or impo	ort one from the host file system.		
Kernel	💫 Configure	e Custom Kernel based on:	¥		
File Manager	G Import C	ustom Kernel Configuration			
Chroot Shell	You can also	export your custom kernel conf	iguration to the host file system.		
	Export C	ustom Kernel Configuration			
Image Cleanup					
SCAP Scanner					
	Build or rem	ove a custom kernel in the targe	t system image.		
	Build Cus	stom Kernel 🔏 Clean Source	Tree 🔋 Remove Custom Kernel		
Deploy Image					

Figure 2-4 Customizing kernel with support for FIPS

NOTE

There is no support for FIPS in the Rocky distribution's first release, the 8.4 release. It will be supported in a future release. However, it is supported by RedHawk with the other base distributions (RHEL, CentOS).

NOTE

A separate /boot partition is required when using FIPS.

NOTE

FIPS is not supported for the PXE diskless deployment method.

If the installer methods (USB Installer, Disc Installer or PXE Installer) will be used to deploy the target image, there is nothing more to do. The rest of the configuration is done by Architect.

If the USB Devices or the Virtual Machines deployment methods will be used, these additional steps must be taken on the target system:

- 1. Boot the target with a kernel that does not have FIPS enabled. This is a default kernel or a kernel with the boot option 'fips=0' set.
- 2. If the target system image is based on the 8.0 release, then the **fips-finish-install** script must be patched with the following command:

```
sed -i 's/dracut -f$/dracut -f \
--regenerate-all/' /usr/bin/fips-finish-install
```

3. Run the following command:

fips-mode-setup --enable

- 4. Reboot the target with a kernel with FIPS support enabled. This a kernel with the boot option 'fips=1' set.
- 5. To check that FIPS is enabled on the target, run:

fips-mode-setup --check

Security Content Automation Protocol (SCAP)

Introduction to SCAP

The Secure Content Automation Protocol (SCAP) was developed by the U.S. government's NIST organization to create security-oriented operating system configuration checklists.

The SCAP Security Guide implements security guidances recommended by respected authorities, namely PCI DSS, STIG, and USGCB. The SCAP Security Guide transforms these security guidances into a machine readable format referred as content files which can be used to audit your system in an automated way. The SCAP content files are provided in the **scap-security-guide** package and are installed in the directory /usr/share/xml/scap/ssg/content/. There are files for every platform available in the forms XCCDF (Extensible Configuration Checklist Description Format), OVAL (Open Vulnerability Assessment Language) or datastream documents. In most cases, the datastream is used, which are the file names ending with -ds.xml.

The SCAP Security Guide builds multiple security benchmarks and corresponding profiles from a single SCAP content. Profiles provide a set of rules to be applied.

Custom profiles can also be derived from existing profiles using the SCAP Workbench graphical tool. This is often referred to as SCAP content tailoring and is further explained in the "Customizing SCAP Content Using SCAP Workbench" on page 2-17.

Understanding SCAP Evaluation and Remediation Scans

SCAP scans are performed with the **oscap(8)** tool installed by the **openscap-scanner** package. Two types of scans may be performed: evaluation and remediation. Evaluation scans report on the current security status of the system, according to a selected security profile. Remediation scans attempt to fix security discrepancies found on the system, then report on the status of this process. This process is also called "auto-remediation".

Additionally, the SCAP Workbench GUI tool can be used to perform scans. This tool has the ability to scan a remote system over an SSH connection.

Auto-remediation is not perfect. Rarely are all SCAP rules fixed by auto-remediation, therefore manual remediation or custom SCAP tailoring is often required to achieve the desired level of security policy compliance.

Manual remediation can be done by editing user-level configuration files. This can either be done in a chroot of a target system image or on target systems once deployed.

Custom SCAP tailoring can be used to modify existing SCAP policy. This is useful to change or exclude certain security rules in a profile. Custom tailoring also provides a way to codify manual remediation steps into auto-remediation scripts contained within a custom SCAP profile. Most of the tools that accept a SCAP content file as input, will optionally also allow both a SCAP tailoring file and its corresponding SCAP content file to be specified. This includes **oscap(8)**, **scap-workbench(8)**, and the Architect GUI.

Note

Some SCAP rules may be broken and do not pass evaluation no matter what you do. Always be sure to use the most up-to-date SCAP content files provided by your host distribution. See "SCAP System Requirements" on page 2-7 for information on updating the SCAP packages.

Red Hat also has problems posted to their issue-tracking system, Bugzilla (https://bugzilla.redhat.com). You can search on that site for existing bugs related to any of the SCAP packages.

SCAP System Requirements

The system chosen to be the Architect host must be running any of the RHEL-compatible distributions supported by Architect (RHEL, Fedora, Rocky). CentOS has reached its end-of-life and does not have any SCAP updates in any of its 8.x repositories, therefore, we do not recommend a CentOS-installed system be used as the Architect host.

It is recommended that the target image use a RHEL-based distribution. This choice is made at the first prompt when you start a new session. When asked to select a RedHawk Release, choose any RedHawk 8.x (RHEL) release.

Before starting, the latest SCAP packages should be updated on the host system:

dnf update openscap scap-security-guide

SCAP Workflow

Workflow Overview

The following steps are typically performed to configure, build, and deploy targets that adhere to some SCAP security policy.

- 1. Configure SCAP security policy. The desired SCAP security policy is chosen prior to building a target system image. Image software and configuration settings are made to comply with the chosen security policy's preinstallation rules, before the target system image is built.
- 2. Build the target image. A post-build SCAP remediation scan is done automatically in the target system image when the image is built.
- 3. Customize the target image. Some customization may be needed and, optionally, you can run additional post-build SCAP scans in the chroot of the target system image prior to image deployment to the target systems. These scans may be evaluation scans or remediation scans. If desired, manual remediation can also be performed at this time.
- 4. Run post-deployment scans. These scans may be evaluation scans or remediation scans. If desired, manual remediation can also be performed at this time.

Note

It is common for some auto-remediation rules to fail when run in the chroot of a target system image; therefore an additional remediation scan and/or manual remediation is often required to be performed after target deployment.

It may be possible to avoid these extra steps by doing appropriate manual remediation in the chroot of the target system image and/or using a custom SCAP tailoring file.

Note

Some SCAP pre-installation rules require that additional file systems be configured. The diskless deployment methods may not be a good choice for some SCAP policies since they ignore all file system configuration settings and instead use a single mount point for the root '/' file system.

Each step is explained further in the sections that follow.

1. Configure SCAP security policy

To configure SCAP, click on the SCAP button of the Configure Image toolbox. The Configure SCAP Security Policy page will display the default SCAP content file loaded and the corresponding benchmark(s) and profile(s) available for the corresponding RedHawk release specified when the target's session was created.

SCAP must be configured before the target system image is built. If an image has already been created, it must first be removed via the Delete Image button of the Build Image toolbox.

In the figure below the following default SCAP settings are shown for a session building a RedHawk 8.4 (RHEL) target system image.

	example.session - RedHawk Architect (on rodrigo)	×
<u>File Edit T</u> ools <u>H</u> elp		
🖻 😭 🛱 😭 🏟 (PXE ## Estimated Image Size: 876.4 Me (43% of 2.0 GB) 2.0 GB	\$
Select Software	Configure SCAP Security Policy	
Configure Image	Use this page to enforce SCAP security policy upon image configuration prior to building a target system image.	Ø
General Settings	Benchmark: Guide to the Secure Configuration of Red Hat Enterprise Linux 8	▼ <u>(info)</u>
Console	Profiles Select the security profiles you would like to enforce in the target system image:	
Networking	ANSSI-BP-028 (enhanced) (info) ANSSI-BP-028 (high) (info)	-
File Systems	ANSSI-BP-028 (intermediary) (info) ANSSI-BP-028 (ininimal) (info)	*
SELinux	Rules (0)	
SCAP	Only pre-installation rules are enforced here. Additional rules are enforced once an image is built.	
Build Image Customize Image Deploy Image	SCAP Content File: /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml SCAP Tailoring File: none	hange

Figure 2-5 Configure SCAP Security Policy page

The default SCAP content file in the above figure provides a choice of benchmarks and profiles. The SCAP content and tailoring files are listed at the bottom of the page. Use the Change button on the right hand corner of the page to load a different content file or a tailoring file. For information on tailoring files, see "Customizing SCAP Content Using SCAP Workbench" on page 2-17.

Note

To execute pre-installation SCAP rules, Architect relies on special formatting that is unique to Red Hat content files in the **scap-secu-rity-guide** package. If more recent SCAP content is required, additional scans can be done using newer content after the initial target system image has been built.

Click on the (info) links in the Configure SCAP Security Policy page to obtain information about the benchmark and the profiles listed. Click on the box by a profile to select that profile. Note that one or more profiles may be selected.

Once one or more profiles are selected, a list of pre-installation rules will appear in the bottom window of the Configure SCAP Security Policy page. Note that each one has an (info) link also. For each pre-installation rule to be applied, there are two buttons with choices to either Fix or Ignore the rule. The target system image cannot be built until each pre-installation rule is either applied or ignored.

The Benchmark and SCAP content file are initially set by Architect. The profile must be selected. In this example, we have selected the "DISA STIG for Red Hat Enterprise Linux 8" profile as shown in the figure below. The DISA STIG profile is designed for safeguarding the Department of Defense (DoD) IT network and systems. Note that the instructions that follow are the same for any profile.

Following are the corresponding SCAP settings when building a RedHawk 8.4 (RHEL) target system image and selecting the "DISA STIG for RHEL 8" profile.

content file: /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml

benchmark: Guide to the Secure Configuration of Red Hat Enterprise Linux 8 *profile:* DISA STIG for Red Hat Enterprise Linux 8

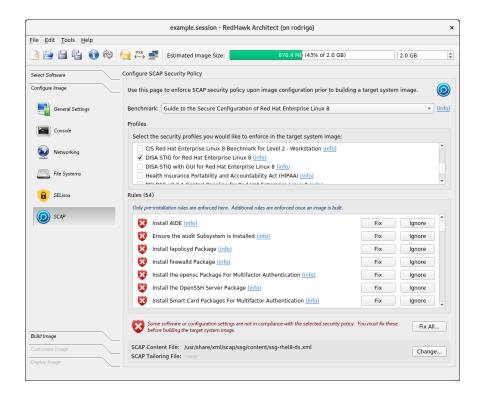


Figure 2-6 SCAP's DISA STIG profile selected

If you have a tailoring file, use the Change... button to include it before starting the pre-installation fixes. The tailoring file is explained in the section "Customizing SCAP Content Using SCAP Workbench" on page 2-17.

Architect automates most of the pre-installation fixes. In some cases, however, the user is asked to confirm a step to be taken and in other cases more manual intervention is required. An example of the latter is a rule requiring that an additional file system be created.

In the case where additional file systems are required, Architect will redirect the user to the Configure File System page so that the user may manually add the requested partition. Once finished adding the partition, the user is returned back to the Configure SCAP Security Policy page.

Note that (info) links are also available for the rules.

Use the Fix All... button on the bottom right of the screen to automate the fixing of all the rules shown. If something needs manual intervention Architect will redirect the user as stated above and afterwards continue to the next rule. If for some reason the scan is paused, you can use the Resume button to continue. See the Stop and Resume buttons in the image below.

	example.session - RedHawk Architect (on rodrigo)			×
<u>File Edit T</u> ools <u>H</u> elp				
🎯 🗊 🖆 🔛	Estimated Image Size: 1028.4 MB (51% of 2.0 GB)		2.0 GB	-
Select Software	Configure SCAP Security Policy			
Configure Image	Use this page to enforce SCAP security policy upon image configuration prior to building a	a target syster	n image.	0
General Settings	Benchmark: Guide to the Secure Configuration of Red Hat Enterprise Linux 8		•	(info)
Console	Profiles			
Console	Select the security profiles you would like to enforce in the target system image:			
Networking	CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Workstation (info)			•
-25-	DISA STIG for Red Hat Enterprise Linux 8 (info) DISA STIG with GUI for Red Hat Enterprise Linux 8 (info)			_
File Systems	Health Insurance Portability and Accountability Act (HIPAA) (info)			Ŧ
SELinux	Rules (54)			
	Only pre-installation rules are enforced here. Additional rules are enforced once an image is built.			
(D) SCAP				
Back to Configure SCAP Security	Ensure /var Located On Separate Partition (info)			
Policy	Ensure /var/log Located On Separate Partition (info)	Fix	Ignore	
	Add nodev Option to /var/log (info)	Fix	Ignore	
	X Add noexec Option to /var/log (info)	Fix	Ignore	
	Add nosuid Option to /var/log (info)	Fix	Ignore	
	Some software or configuration settings are not in compliance with the selected security policy. Y target system image.	'ou must fix these	e before building	the
Build Image	In progress: Fixing "Ensure /var/log Located On Separate Partition"	Sto	p Resu	ime
Customize Image Deploy Image	SCAP Content File: /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml SCAP Tailoring File: none		Chang	je

Figure 2-7 Using Fix All... option showing Stop and Resume buttons

After SCAP has been configured and the rules applied or ignored, the target system image can be created.

2. Build the target system image

To start the build, click on the Build Image button of the Build toolbox. Once the target system image is built, a remediation scan will automatically start in the chroot of the target system image on the host.

Image Builder (on rodrigo)	×
Building image (/var/lib/architect/images/example-build).	
100%	
The image has been built.	
Output Log	
Scanning with profile stig Created /root/scap/stig-fix-report.html Created /root/scap/stig-fix-results.txt Created /root/scap/stig-fix-summary.txt Content File: ssg-rhel8-ds.xml Tailoring File: Benchmark ID: xccdf_org.ssgproject.content_benchmark_RHEL-8 Profile ID: xccdf_org.ssgproject.content_profile_stig Pass: 924 Fail: 243 Fixed: 149 Error: 91 Not Checked: 8 Not Applicable: 20 Unknown: 30 * The image has been built.	
Save Output Log	Abort

Figure 2-8 Architect's post-build remediation completes

The post-build auto-remediation scan in the chroot of the target system image on the host will most likely complete with failures as in the figure above. This is expected as usually not all SCAP rules are fixed by auto-remediation in a chroot shell.

The results of the scan can be viewed and further scans can be run from the SCAP Scanner tab of the Customize Image toolbox. See the section "3. Customize the target image" that follows.

3. Customize the target image

The results from previous remediation and evaluation scans can be viewed from the SCAP Scanner page of the Customize Image toolbox. Both evaluation and remediation scans on the target's chroot can be run from this page. Also a scan can be started remotely from the host on a deployed target using the Launch SCAP Workbench GUI... button. The SCAP Scanner page is shown below.

	example.session - F	edHawk Architect (on rodrigo)	×
<u>File Edit Tools H</u> elp			
📑 😭 😭 🧐	Estimated Image Size:	1454.0 MB (72% of 2.0 GB)	2.0 GB
Select Software	CAP Scanner		
Configure Image	Use this page to run additional SCAP	cans after a target system image has been built or deployed.	0
Build Image			
Customize Image	The target system image has already using the <u>selected SCAP policy</u> .	been built and a post-build remediation scan has been run in	the target system image
Software Updates			
Additional RPMs	View the most recent SCAP remediation reso	Its in the target system image, or run a new remediation scan here.	
System Services	View Results Summary View Result	s View Full Report	Run Remediation Scan
Kernel			
File Manager	View Results Summary View Result	s in the target system image, or run a new evaluation scan here. s View Full Report	Run Evaluation Scan
Chroot Shell			
Image Cleanup		ol that can be used to run SCAP scans remotely on deployed target syster	ms.
SCAP Scanner	Launch SCAP Workbench GUI		
Deploy Image			

Figure 2-9 SCAP Scanner page

Some customization can be done in the chroot of the target system image. To access the Chroot Shell, select the Chroot Shell button of the Customize Image toolbox and then click on Run Chroot Shell.

Below are some customizations, specific to SCAP-configured systems, that can be executed in the Chroot Shell:

• Perform Manual Remediation of Failed Rules

Most manual remediation involves editing system files. Information on steps to remediate a failed rule can be obtained from the reports generated by scans, mentioned in the "Run Additional Scans" item below.

Add Non-root Users

Additional users can be added in the Chroot Shell using the **useradd(8)** command. This might be necessary since security-enhanced systems usually put restrictions on root logins.

• Re-enable root SSH login

Some SCAP remediation rules remove root user's privilege to remotely login to the system with **ssh(1)**. To circumvent this, edit the file /**etc/ssh/sshd_config** in the Chroot Shell, search for *PermitRootLogin* in that file and verify that it is set to a value of 'yes'. If not, change the 'no' to a 'yes'. Make sure that the entry does not have a '#' sign at the beginning. Those entries are ignored. Also note that this will change back to a 'no' each time a remediation scan is run.

4. Run post-deploy scans

It is possible and sometimes necessary to run SCAP evaluation and remediation scans on a target system once deployed. This can be done remotely using SCAP Workbench or locally using the scan tools provided on the target.

Post-deploy scans can be done in various ways which are listed below and explained in the sections that follows.

- 1. Remotely, from Architect, using the **scap-workbench** tool which uses an **ssh** connection.
- 2. Remotely, logging in from another system via **ssh**, and running local commands.
- 3. Directly, logging in to the console of the target system, and running local commands.

When connecting remotely, the remote system must be able to **ssh** into the target system and the root user must have privileges to log in.

Note

The privilege allowing root to log in is sometimes removed by rules applied during the post-build remediation scan. Before deploying the target, edit the file /etc/ssh/sshd_config in the chroot of the target. Verify that the *PermitRootLogin* option in that file is set to the value 'yes'.

Post-deployment reports from Architect system scans, are generated as .html and .txt files and placed in the /**root/scap** directory of the target system. Note that **scap-workbench** has its own way of generating reports, hence, you will not find those reports in this directory.

Besides reporting on the pass/fail status, the reports provide information about the steps necessary to comply with each rule; information useful when manual steps are required.

Initially, the report files from the last scans done in Architect are found in the /root/scap directory.

Notes

Reports generated are overwritten each time a scan is initiated. If reports need to be saved, make sure to move them to another filename before initiating a new scan.

Remotely from Architect

SCAP Workbench is a graphical tool that can be used to perform SCAP scans on a target system. Scans can be done remotely over an **ssh** connection. To execute a remote scan of a target system using SCAP Workbench follow the steps below:

1. Launch SCAP Workbench from the button labeled Launch SCAP Workbench GUI... found in the SCAP Scanner page of the Customize Image toolbox of Architect. The SCAP content file, and the optional tailoring file, used in the session will be loaded into SCAP Workbench.

NOTE

scap-workbench requires to be run from an X session having DISPLAY set to ':0'. If X11 forwarding is used (e.g., **ssh -X**) to launch the GUI, it will not be able to authenticate when connecting to a remote target for scanning and will fail with the error message: cannot open display :0.

Even when executing on the console of the system running Architect DISPLAY setting may differ. Verify your DISPLAY environment setting by issuing **echo \$DISPLAY** on the command line. For more information, see the Known Issues section in Architect's 8.4-1 Release Notes Manual.

- 2. Select the Profile of interest at the top of the page.
- 3. Click on Remote Machine (over SSH) and enter the User and host of the target.

Important Warning

It is very important that the Remote Machine (over SSH) button be set on the SCAP Workbench page. If not, system changes will be applied to the host system.

- 4. Check Fetch remote resources at the bottom of the page.
- 5. Check Remediate to perform a remediation scan; otherwise an evaluation scan will be done.

Click the SCON button. Note that if you are using multiple profiles you will have to repeat steps 2 through 6 for each profile.

The root user must have privileges to log in. If you get an error trying to **ssh** into the system (e.g., your valid passwd is not accepted), verify that *PermitRootLogin* is set to 'yes' in the /etc/ssh/sshd_config file. For more details, see the note on page 2-14.

The following figure shows SCAP Workbench ready to run a remote remediation scan of the DISA STIG profile rules on a deployed target system specified by its IP address.

	Guide to the Secure Configuration of Red Hat Enterprise Linux 8	
Customizatio	None selected	
Profile	DISA STIG for Red Hat Enterprise Linux 8 (370)	Customize
Target	Local Machine emote Machine (over SSH)	
Jser and hos	root@10.192.168.30.215 Port 22 user is sudoer root@kitschy:22	
ules		Expand al
Install All)F	
	AIDE to Verify the Audit Tools	
	Notification of Post-AIDE Scan Details	
5	AIDE to Verify Access Control Lists (ACLs)	
-	AIDE to Verify Extended Attributes	
5		
	racut FIPS Module	
Enable FI	acut FIPS Module PS Mode	
Enable FI	PS Mode	
 Enable FI Set kerne 		
 Enable Fl Set kerne Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1	
 Enable FI Set kerne Configure Configure 	PS Mode parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy	
 Enable FI Set kerne Configure Configure Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy s System Cryptography Policy	
 Enable FI Set kerne Configure Configure Configure Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 : BIND to use System Crypto Policy : System Cryptography Policy : GnuTLS library to use DoD-approved TLS Encryption	
 Enable FI Set kerne Configure Configure Configure Configure Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 : BIND to use System Crypto Policy : System Cryptography Policy : GnuTLS library to use DoD-approved TLS Encryption : Kerberos to use System Crypto Policy	
 Enable FI Set kerne Configure Configure Configure Configure Configure Configure Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 : BIND to use System Crypto Policy : System Cryptography Policy : GnuTLS library to use DoD-approved TLS Encryption : Kerberos to use System Crypto Policy : Libreswan to use System Crypto Policy	
 Enable FI Set kerne Configure Configure Configure Configure Configure Configure Configure Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy System Cryptography Policy I GNUTLS library to use DoD-approved TLS Encryption Kerberos to use System Crypto Policy Libreswan to use System Crypto Policy OpenSSL library to use System Crypto Policy	
 Enable FI Set kerner Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy System Cryptography Policy I GnuTLS library to use DoD-approved TLS Encryption Verberos to use System Crypto Policy Libreswan to use System Crypto Policy OpenSSL library to use System Crypto Policy OpenSSL library to use TLS Encryption	
 Enable FI Set kerner Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy System Cryptography Policy GnuTLS library to use DoD-approved TLS Encryption Kerberos to use System Crypto Policy Libreswan to use System Crypto Policy OpenSSL library to use TLS Encryption SSH to use System Crypto Policy	
 Enable FI Set kerne Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy System Cryptography Policy GruTLS library to use DoD-approved TLS Encryption Kerberos to use System Crypto Policy Libreswan to use System Crypto Policy OpenSSL library to use System Crypto Policy SSH to use System Crypto Policy SSH to use System Crypto Policy SSH to use System Crypto Policy	
 Enable FI Set kernet Configure 	PS Mode I parameter 'crypto.fips_enabled' to 1 BIND to use System Crypto Policy System Cryptography Policy GouTLS library to use DoD-approved TLS Encryption Kerberos to use System Crypto Policy Libreswan to use System Crypto Policy OpenSSL library to use System Crypto Policy SopenSSL library to use TLS Encryption SSH to use System Crypto Policy SSH to use System Crypto Policy SSH Client to Use FIPS 140-2 Validated Ciphers: openssh.config SSH Server to Use FIPS 140-2 Validated Ciphers: opensshserver.config	

Figure 2-10 SCAP Workbench settings example

Remotely via ssh

Evaluation and remediation scans can be performed by executing commands on the target system. The files needed have been placed under the **/root/scap** directory of the target. The scan commands use the SCAP content file also placed in the **/root/scap** directory.

To run an evaluation scan and/or a remediation scan, **ssh** into the target system and execute the respective scan command:

cd /root/scap ./run-eval-scan ./run-remediate-scan

These commands can also be invoked remotely using an ssh connection:

ssh root@target 'cd /root/scap; ./run-eval-scan'
ssh root@target 'cd /root/scap; ./run-remediate-scan'

The root user must have privileges to log in. If you get an error trying to **ssh** into the system (e.g., your valid passwd is not accepted), verify that *PermitRootLogin* is set to 'yes' in the /etc/ssh/sshd_config file. For more details, see the note on page 2-14.

Directly from console

To run an evaluation scan and/or a remediation scan on the target, execute the respective scan command:

cd /root/scap ./run-eval-scan ./run-remediate-scan

If you encountered problems logging in to the target system, it may be due to blocked access to the target's USB devices or that the root user is blocked from logging in.

Some SCAP profiles (e.g., the DISA STIG profile) have rules preventing access to USB devices. If you have a USB keyboard or other USB devices on the target, you will be denied access to them.

The instructions below will allow you to log in to the target system and then generate rules to exempt the USB devices.

- 1. Before deploying your system, disable the **ubsguard** daemon in the chroot of the target. Bring up the System Services page of the Customize Image toolbox, find the **usbguard** service and disable it (clear the check mark).
- 2. After deploying the target system, log in to the target and run the following commands to generate exemption entries, install them in the **usbguard** rules file, and then enable/restart the **usbguard** service:

usbguard generate-policy > /tmp/rules.conf install -m 0600 -o root -g root /tmp/rules.conf /etc/usbguard/rules.conf systemctl enable --now usbguard.service systemctl status usbguard.service reboot

The root user must have privileges to log in. If you get an error trying to log in to the system, (e.g., your valid passwd is not accepted), verify that *PermitRootLogin* is set to 'yes' in the /etc/ssh/sshd_config file. For more details, see the note on page 2-14.

Customizing SCAP Content Using SCAP Workbench

Customization, also called tailoring, allows existing SCAP policies to be customized without having to rewrite the policy. Tailoring is useful to change or exclude certain security rules in a profile. You can deselect rules that do not apply to your company, select optional rules not selected by default, or change modifiable settings in the policy. All these policy changes are then saved in the tailoring file. Architect can then load the tailoring file and apply the changes in policy.

Note

Tailoring files must be created outside of Architect and be available to be used by Architect during the SCAP configuration step, before the build image is created.

The SCAP Workbench tool can be used to create SCAP tailoring files. To create a SCAP tailoring file, perform the following steps:

- 1. Run the scap-workbench command-line tool on the host system.
- 2. Select the content file of interest and press the Load Content button.
- 3. Select the Profile of interest.
- 4. Click on the Customize button to the right of the Profile box. A new window will be displayed.
- 5. Enter the new profile ID. Choose the name provided or follow the instructions specified for naming the profile.
- 6. Make the desired changes by making the desired modifications. Then press the OK button to close the window.
- 7. Save the customized profile to a SCAP tailoring file. Click on File, then Save Customization Only.

The following figure shows a customized version of the RHEL8-DISA STIG profile being created with the ntp rule "Configure Time Service Maxpoll Interval" deselected.

Customizing "DISA STIG for Red Hat Enterprise Linux 8 [CUSTOMIZED]	(on rodrigo)	×
Select All Deselect All ntp Search Showing match 3 out of 13 total fou	ıd.	
Use Root-Squashing on All Exports Configure the Exports File Restrictively Export Filesystems Read-Only if Possible Second Start Bark Configure Authorization Restrictions Vendor Approved Time Servers Maximum NTP or Chrony Poll The Chrony package is installed Install the ntp service Fine Chrony dervice is enabled Enable the NTP Daemon Enable the NTP Daemon Enable the NTP Daemon	Selected Item Title Conf ID onter Type xccd Description The mappell 3 etc/chrony.co maxpoll in /et after each 'ss	igure Time Service Maxpoll Interval nt_rule_chronyd_or_ntpd_set_maxpoll fr:Rule should be configured to 10 in (atc/ntb_conf or / m nt to continuously poll time servers. To configure ricrito, conf or (etc/chrony.conf add the following erver or 'pool' entry: maxpoll to to server using chrony any pool directives should be 0. If no server or econfigured.
Obsolete Services Ensure rsynck service is diabled Vinetd Dinistall xinetd Package Disable xinetd Service	Security Identi [https://nvd.n	ifiers ist.gov/cce/index.cfm] - CCE-84059-5
	Depends on Va	alues um NTP or Chrony Poll = 10

Figure 2-11 Using SCAP Workbench to create a customized profile

Once saved, the tailoring file can be used in the SCAP configuration. In the Configure SCAP Security Policy page, click on the Change... button at the right bottom of the page and enter the tailoring file which, in this example, was saved as /root/Documents/ssg-rhel8-ds-tailoring.xml file. See the following image.

	example.session - RedHawk Architect (on rodrigo)	×
<u>File Edit T</u> ools <u>H</u> elp		
	🖗 😡 👯 Estimated Image Size: 1028.4 MB (51% of 2.0 GB) 2.0 GB	\$
Select Software	Configure SCAP Security Policy	
Configure Image	Use this page to enforce SCAP security policy upon image configuration prior to building a target system image.	
General Settings	Benchmark: Guide to the Secure Configuration of Red Hat Enterprise Linux 8 🔹 👘	<u>o)</u>
Console	Profiles	
Networking	Select the security profiles you would like to enforce in the target system image: CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Server (info) CIS Red Hat Enterprise Linux 8 Benchmark for Level 2 - Workstation (info) CIS Action of the tenterprise Linux 8 (info) CIS Action of tenterprise	
File Systems	Select SCAP Content (on rodrigo) ×	
SELinux	SCAP Content File: /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml	
SCAP	SCAP Tailoring File: /root/Documents/ssg-rhel8-ds-tailoring.xml	
	Ensure the audit Subsystem is Installed (info)	
	V Install fapolicyd Package (info)	
	V Install firewalld Package (info)	
	V Install the opensc Package For Multifactor Authentication (info)	
	V Install the OpenSSH Server Package (info)	
	V Install Smart Card Packages For Multifactor Authentication (info)	
Build Image	V All software and configuration settings are in compliance with the selected security policy.	
Customize Image	SCAP Content File: /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml SCAP Tailoring File: none Change	
and any and		

Figure 2-12 SCAP Workbench, customized profile loaded

More information about SCAP Workbench and customizing profiles can be found at https://www.open-scap.org/resources/documentation/customizing-scap-security-guide-for-your-use-case and other sites.

RedHawk Architect User's Guide

This chapter describes how to create or import on-disk ISO images to dramatically speed up and virtually automate target system image creation.

Importing ISO Images

Normally when building a target system image the user is prompted to insert various optical media discs containing the software that is required in order to create the initial target system image. If only one or two images are being produced, manually inserting optical media is generally acceptable.

However, if the user is generating and maintaining several different target system image configurations, it is often preferable to create on-disk ISO images of the various optical media discs. To accomplish this, select the Media ISO Manager item in the Tools menu, or click the Import ISO Images button on the Build Image page, and the following dialog will appear.

Architect Media ISO Manager			×
The RedHawk installation media can be imported to the loc: allows Architect to build target system images more quickly media. ISO images may be imported either by ripping them image files already on your hard disk.	, without prompti	ng fo	r installation
RedHawk Release: RedHawk 8.2 (CentOS) -			
CentOS Updates (8.2) ISO	not imported	0	🤤Import
RedHawk Linux (8.2) ISO	not imported	0	ତୁ Import
RedHawk FBS (8.2) ISO	not imported	0	🤤 Import
NightStar RT (5.0 or newer) ISO	not imported	0	⊗ Import
RedHawk Update ISO	not imported	0	🧐 Import
Media ISO directory: /var/lib/architect/ISOs/redhawk-8.2			@ <u>R</u> efresh

Figure 3-1 Import ISO Images Dialog

Pressing the Import button, will display a menu with three different options to import ISO images:

- · Import ISO images directly from manually inserted optical media
- Copy ISO images from already existing ISO image files

· Link ISO images to already existing ISO images files

These various methods will be described in the following sections.

The user can import different sets of ISO images for different RedHawk release versions; use the Select a RedHawk release pull-down menu to select which version of RedHawk to import ISO images for.

In addition, different import methods can be used *within* a specific RedHawk release. For example, it is possible to use one import method to import the CentOS ISO image and a different import method to import the RedHawk and NightStar ISO images. All combinations are valid.

Importing ISO Images From Optical Media

To use this method select the Rip ISO from media import method and then press the OK button to begin the import process. A dialog similar to the following dialog will be displayed.

	Media ISO Image Ripper	×
Ripping ISO image f	rom media.	<u></u>
	2%	
Output Log		
	Architect ×	
	Please insert the CentOS Updates (Version 8.2) disc.	
	Abort JOK	
		Abort JOK

Figure 3-2 Rip ISO Images From Media

At this point the correct optical media disc for the requested item should be manually inserted into the host system's optical media tray. Once the optical media has been inserted, press OK to begin copying the ISO image from the optical media onto the host system's hard-drive. Various status messages will be displayed as the copy progresses.

NOTE

The 8.4 system release installation discs for Rocky, CentOS and Red Hat, are created using Blu-Ray technology and require a Blu-ray drive to read the data correctly.

Copying ISO Images From Existing ISO Images

If you already have the required media in ISO format on disk, Architect can import the ISO by creating Architect-specific copies of the ISO images; copying is useful when the original ISO images may be removed or unavailable at some point in the future.

To make ISO copies, select the Copy existing ISO file on disk import method and then press the OK button to begin the import process. A file selection dialog will be displayed. Navigate the file selection dialog to the appropriate directory to select the ISO image. An example ISO file selection is presented below. In this example, the ISO images are stored in the /root/Downloads directory and the CentOS Updates ISO image has been selected.

Cancel	Choose File to Copy For CentOS Updates (8.2) ISO		Q Open
⊘ Recent			
🔂 Home	Name 👻	Size	Modified
Documents	CentOS_Updates-8.2-x86_64.iso	7.9 GB	11:14
	NightStar_RT-x86_64.iso	426.1 MB	11:14
🕹 Downloads	RedHawk_FBS-8.2-x86_64.iso	5.0 MB	11:14
JJ Music	RedHawk_Linux-8.2-x86_64.iso	4.4 GB	11:15
Pictures			
▶ Videos			
🔳 1.1 GB V 🔺			
🔳 29 GB V 🔺			
+ Other Locations			
			ISOs 💌

Figure 3-3 Copy ISO Image File Selector

Press the Open button to begin the process of copying the ISO image file into Architect's /var/lib/architect/ISOs directory. Once the copy is completed, the ISO image file that was copied is no longer needed and can be removed if necessary.

Linking To Existing ISO Images

If you already have the required media in ISO format on disk, Architect can import the ISO by creating symbolic links to the ISO images; linking is useful when you can be sure that the original ISO images will persist indefinitely.

To create ISO symbolic links, select the Symbolically link to existing ISO file on disk import method and then press the OK button. Navigate the file selection dialog presented to the appropriate directory and select the ISO image. An example ISO file selection is presented below. In the example, the ISO images are stored in the /root/Downloads directory and the RedHawk Linux ISO image has been selected.

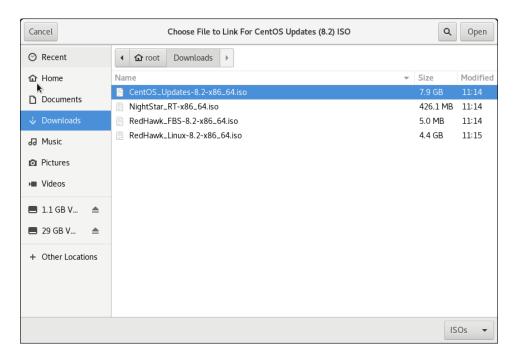


Figure 3-4 Symlink To ISO Image File Selector

Press the Open button to immediately create a symbolic link to the selected ISO image file. The symbolic link will be created and placed inside Architect's /var/lib/architect/ISOs directory. Once the copy is completed, the ISO image file that was linked to must be preserved and kept at the exact same file-system location in order for Architect's symbolic link to be valid.

NOTE

Architect will detect if it has symbolic links to ISO image files that have been erroneously removed and ISO image will no longer be shown as a valid ISO image in the list of imported ISO images.

If this happens, the ISO image must be imported again to be valid, otherwise Architect will prompt for the corresponding optical media disc during any subsequent target system image builds.

Deleting Imported ISO Images

Previously imported ISO images can be deleted at any time by pressing the Delete button of the corresponding ISO image. This is not generally necessary, but can be done in order to save disk space or to recover from the rare case of a file corruption.

RedHawk Architect User's Guide

This chapter describes how to manage PXE resources on the host and how targets in your network environment will use these PXE resources.

Enabling PXE on Targets

The Preboot eXecution Environment (PXE) provides a method for booting target systems using a network interface, without the requirement of having access to any local storage on the target system.

To use PXE, targets must first be configured to perform a PXE broadcast during boot. To enable the PXE broadcast perform the following steps:

- 1. Reboot the target and stop the system immediately after POST (Power-On Self-Test), normally by pressing Delete or F2, to get into the BIOS settings menu.
- 2. Each kind of computer has a slightly different BIOS settings menu, however the general rule is to navigate to the 'PCI Device' or the 'Integrated Devices' section of the BIOS menu and enable PXE boot on the first Ethernet interface that is present. Ensure that the chosen interface is connected to a switch that is present on the same network as the host system.
- 3. Record the MAC address of the target's Ethernet interface for later use with Architect's PXE Target Manager dialog. See "Managing PXE Targets" on page 4-7 for more information.

NOTE

Some older BIOSes do not provide an option to boot with PXE. The *Etherboot* utility can be used instead, however Concurrent Real-Time does not support this configuration. See http://etherboot.org for more information.

Initializing PXE Services

Various PXE-related services on the host system need to be properly initialized before any of the PXE-based image deployment methods can be used.

To initialize these services, click on PXE Target Manager in the Tools menu and you will be presented with the following dialog.

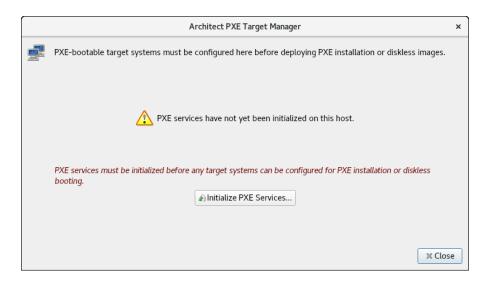


Figure 4-1 PXE Target Manager Unitialized

Press Initialize PXE Services... to begin initializing the PXE services and you will then be presented with the following dialog.

	Initialize PXE Services	×
æ]	This process will initialize all services needed to perform PXE installations or diskless booting from this host. This includes configuring and enabling the DHCP, TFTP, and NFS network services on this host.	
	vices Options	
The PX	KE subnet is "192.168.1.0/255.255.255.0".	
✓ Aut	omatically configure DHCP on this host	
	✓ Apply	શ

Figure 4-2 Initialize PXE Services Dialog

First, choose the network subnet that you wish to use for all PXE communications between the host and its targets. If only one subnet is available a choice as in the figure above, the information is still presented so that the user can verify that the subnet is the desired subnet.

By default DHCP services will be automatically configured and enabled on the host, and this is the recommended approach. However if another DHCP server already exists on the chosen subnet you will need to uncheck Automatically configure DHCP on this host or the two DHCP servers will conflict with each other. In this case, you will need to manually merge the DHCP configuration files generated by Architect on the host with those of the actual DHCP server. See Appendix A, Manual DHCP Configuration, on page A-1 for more information.

Once these settings are correct for your environment click Apply and the initialization will begin. Once the initialization has completed successfully you will see the following displayed in the dialog.

PXE Services Initializer	×
Initializing PXE services.	æ
100%	
PXE services have been initialized.	
Output Log	
Setting up the /var/lib/tftpboot/architect directory. Creating DHCP configuration (/etc/dhcp/architect/dhcpd.conf). Hooking to DHCP server configuration (/etc/dhcp/dhcpd.conf). Starting the dhcpd service. Starting the tftp.socket service. The firewalld service is currently not running. If you enable firewalld, be sure to allow access for the tftp service. Starting the nfs-server service. Enabling the dhcpd service (for next boot). Enabling the tftp.socket service (for next boot). Enabling the nfs-server service (for next boot). * PXE services have been initialized.	•
Save Output Log	ОК

Figure 4-3 PXE Services Initializer Done

Press OK to return to the main PXE Target Manager window. At this point the host is now configured with the required networking services to enable PXE image deployments.

Managing PXE Images

PXE images that have been created with the PXE Installer and PXE Diskless tools in RedHawk Architect's Deploy Image toolbox are resources that can be inspected and managed with the PXE Image Manager.

Select PXE Image Manager from the Tools menu to access the PXE Image Manager.

If no PXE images have yet been deployed you will be presented with the following empty dialog. The PXE Image Manager will remain empty until PXE images are created using the PXE deployment tools in the Deploy Image toolbox.

The PXE Image Manager lists all of the installation images that have been deployed by the PXE Installer tool. The Remote Sync Preferences allows you to change global parameters affecting remote syncs.

Arch	itect PXE Image Manager
	stalling or diskless-booting PXE targets may be Sync PXE preferences may also be edited.
Installation Images:	-> Diskless Images:
Edit 🖀 Delete	@ <u>R</u> efresh
Build date:	
Session file:	
Image path:	
🔁 Remote Sync Preferences:	
PXE-boot preferences for Remote	Syncing are global.
Edit	
	× Close
	a close

Figure 4-4 PXE Image Manager.

Clicking on the Edit button of the Architect PXE image Manager page will bring up the Edit Remote Sync Preferences page shown below. Note that changes are not applied to a particular target but globally.

Edit Remote Sync Preferences ×
Editing Remote Sync PXE-boot preferences.
Serial Console: none 🔻
✓ Automatically start sync when target system is PXE-booted
Cancel 🥏 Cancel

Figure 4-5 Global parameters for Sync Operations

The following dialog shows an example of the PXE Image Manger with installation images.

Architect PXE	Image Manager ×
PXE PXE images that exist for installing o edited or deleted. Remote Sync PXE	r diskless-booting PXE targets may be preferences may also be edited.
· Installation Images:	-> Diskless Images:
RedHawk-8.2-UEFI real-time.installer	
	€ Refresh
Build date: Mon Apr 26 10:13:57 2021 Session file: (none)	
Image path: /home/architect/images/RedHa	wk-8.2-UEFI
Remote Sync Preferences: PXE-boot preferences for Remote Syncing a	re global. X Close

Figure 4-6 PXE Image Manager with Installation Images

Each PXE installation image that is created using the PXE Installer deployment method is effectively a snapshot in time of the target system image being managed during an Architect session. These images can be inspected and/or individually removed.

Selecting an installation image from the list will display the following details about the image:

- The date the installation image was deployed
- The session file that was being used at the time of creation; if the session has not yet been saved the string None will be displayed instead
- The path of the target system image that the installation image was created for

To delete an installation image, first select it in the list and then press the Delete button. You will be presented with a dialog asking for confirmation and simply press Yes to delete it.

To edit the attributes of an installation image, first select it in the list and then press the Edit button. You will be presented with a dialog allowing you to modify several attributes of the installation image including:

- The Serial Console for the install image.
- The Automatically install image to disk when target is PXE-booted checkbox.

Press OK to apply any changes made to the attributes of the installation image.

The Refresh button will refresh the list to match the resources currently on disk, however refresh is only useful if multiple copies of Architect are being used simultaneously to create and manage PXE installation images.

Press Close at any time to dismiss the dialog and return to the Architect main window.

PXE Diskless Images

The PXE Image Manager lists all of the diskless images that have been created by the PXE Diskless tool. The following dialog shows an example of the PXE Image Manger with diskless images.

Architect PXE	Image Manager ×
PXE PXE images that exist for installing o edited or deleted. Remote Sync PXE	r diskless-booting PXE targets may be preferences may also be edited.
Installation Images:	··>靊 Diskless Images:
	RedHawk-8-RAM (RAMDISK) RedHawk-8.2 (NFS)
<u>▲</u> Edit	® <u>R</u> efresh
Build date: Thu Apr 15 16:24:12 2021	
Session file: /home/architect/RedHawk-8.2	session
Image path: /home/architect/images/RedHa	wk-8.2
Remote Sync Preferences:	
PXE-boot preferences for Remote Syncing a	re global.
Edit	
	₩ Close

Figure 4-7 PXE Image Manager with Diskless Images

Similar to PXE installation images, PXE diskless images created using the PXE Diskless deployment method create a snapshot in time of the target system image being managed. These images can be inspected and/or individually removed.

Selecting a diskless image from the list will display the following details about the image:

- The date the diskless image was created
- The session file that was being used at the time of creation; if the session has not yet been saved the string None will be displayed instead
- The path of the target system image that the diskless image was created for

To delete a diskless image, first select it in the list and then press the Delete button. You will be presented with a dialog asking for confirmation and simply press Yes to delete it.

To edit the attributes of a diskless image, first select it in the list and then press the Edit button. You will be presented with a dialog allowing you to modify several attributes of the diskless image including:

- The PXE/DHCP Device that the diskless image should use for all PXE and DHCP network traffic.
- The Serial Console for the diskless image.
- The Kernel to Boot for the diskless image.
- Any Extra Kernel Options for the diskless image's kernel to use.
- The Boot Timeout for the diskless image's boot menu to use.

Press OK to apply any changes made to the attributes of the diskless image.

The Refresh button will refresh the list to match the resources currently on disk, however refresh is only useful if multiple copies of Architect are being used simultaneously to create and manage PXE diskless images.

Press Close at any time to dismiss the dialog and return to the Architect main window.

Managing PXE Targets

PXE images that have been created with the PXE Installer and PXE Diskless tools in RedHawk Architect's Deploy Image toolbox are resources that can be assigned to targets using the PXE Target Manager.

Select PXE Target Manager from the Tools menu to access the PXE Target Manager. If no targets have yet been added you will be presented with the following dialog showing an empty list of targets.

PXE-boot	able target sys	stems must be conf	figured here before deplo	oying PXE installation or dis	kless images.
Hostname 🔻	IP Address	MAC Address	Next Boot	Status	
Add Target	-Remove T	arget 🛛 🖧 Edit Tar	get 🔩 Add Multiple Tar	gets	€ <u>R</u> efre
Add Target ∑View DHCP C	·	arget Keinitialize PXE		gets	€® <u>R</u> efre

Figure 4-8 PXE Target Manager

The PXE Target Manager's target list will remain empty until targets are added using one of the Add buttons below the list.

Adding Targets

All targets that will be using PXE installation images and/or PXE diskless images must first be added to the PXE Target Manager. Targets can be added either individually or in groups, and these two methods are described in the following sections.

Adding Single Targets

A single target can be added to the PXE Target Manager by pressing the Add Target... button on the PXE Target Manager dialog.

The following dialog will be shown.

Add PXE Target ×
Configure new PXE target system.
Hostname:
IP Address:
MAC Address:
On Next Boot
Boot local disk
O Install local disk with:
O Boot diskless with: RedHawk-8-RAM (RAMDISK)
 Start remote sync process
Cancel JOK

Figure 4-9 Add PXE Target Dialog

Enter the hostname, IP address and MAC address of the target in the corresponding fields.

In the On Nex† Boo† area of the dialog, choose the desired target behavior that it will perform after its next reboot and subsequent PXE broadcast. The following behaviors are supported:

- Choose Boot local disk to have the target simply boot from its local disk upon next reboot.
- Choose Install local disk with and select a PXE installation image from the pulldown to have the target install the local disk with the selected PXE installation image upon next reboot. This option is only available if

PXE installation images have previously been created; see "Installing via PXE over a Network" on page 1-71 for more information.

• Choose BOO† diskless with and select a PXE diskless image from the pulldown to have the target boot disklessly with the selected PXE diskless image upon next reboot. This option is only available if PXE diskless images have previously been created; see "Booting Diskless via PXE over a Network" on page 1-73 for more information.

Press OK to add this target to the PXE Target Manager and dismiss the dialog.

After targets have been entered the PXE Target Manager will look similar to the following example:

		Archite	ect PXE Target Manager		×
PXE-boo	otable target sys	stems must be config	gured here before deploying PX	E installation or diskless images.	
Hostname 💌	IP Address	MAC Address	Next Boot	Status	
speedy	192.168.1.6	C8:F7:50:FC:47:BA	diskless (RedHawk-8.2)		
sphynx	192.168.1.11	C8:1F:66:06:84:A8	install (RAM-analyzer.diskless)		
+Add Target.		arget Sedit Targ		@ <u>R</u> efre	sh
1 target set to b	e installed on ne	ext PXE boot.		× Clos	se

Figure 4-10 PXE Target Manager with Targets

When you are finished adding targets press the Close button to return to the Architect main page.

Adding Multiple Targets

Multiple target can be added to the PXE Target Manager by pressing the Add Multiple Targets... button on the PXE Target Manager dialog. The following dialog will be shown.

Add	Multiple PXE Targets	×
You may configure multiple new PXE target system These targets will be configured with IP addresses (192.168.1.0/255.255.255.0). Hostnames for the Starting IP Address: 192.168.1.20 How many targets would you like to configure? 1 Base Hostname: target- Apply	from a range of contiguous addresses targets will be generated automatically On Next Boot	RAM-analyzer.diskless × RedHawk-8.2 (NFS) ×
Hostname IP Address	<u>MAC Add</u>	iress Cancel

Figure 4-11 Add Multiple PXE Targets Dialog

Enter the starting IP address in the corresponding field. This will be the address of the *first* target in the target group, and each additional target will simply increment this setting by one IP address.

Choose the number of targets to configure in the corresponding field. You can configure up to 256 targets simultaneously using this interface.

Enter the hostname prefix to be used for all targets in the Base Hostname field. This prefix will be used for the start of each hostname generated and a unique integer suffix will be appended for each target.

In the On Next Boot area of the dialog, choose the desired target behavior that it will perform after its next reboot and subsequent PXE broadcast. See the discussion of On Next Boot above on page 4-8 for more information.

Once the desired settings have been entered, click the Apply button. A dialog similar to the following will be shown:

		Add Multiple	PXE Targets	×
You may confi	igure multiple new	v PXE target systems at one	time.	
			ange of contiguous addresses will be generated automaticall	
Starting IP Ad	dress: 192.168.1	.20	On Next Boot	
			 Boot local disk 	
How many tar	gets would you li	ke to configure? 10 🗘	\bigcirc Install local disk with:	RAM-analyzer.diskless -
Base Hostnam	ne: target-		\bigcirc Boot diskless with:	RedHawk-8.2 (NFS) -
	Apply		 Start remote sync proc 	ess
Hostname	IP Address	MAC Address		
target-020	192.168.1.20			
target-021	192.168.1.21			
target-022	192.168.1.22			
target-023	192.168.1.23			
target-024	192.168.1.24			
target-025	192.168.1.25			
target-026	192.168.1.26			
target-027	192.168.1.27			
target-028	192.168.1.28			
target-029	192.168.1.29			
				Cancel @OK
				Cancel @OK

Figure 4-12 Add Multiple PXE Targets after Apply

Pressing Apply caused the dialog to generate hostname entries for all of the requested targets. Enter the MAC address of each target into its corresponding MAC Address field.

A MAC addresses is required for each target if Architect is directly managing DHCP services. However, MAC addresses are not necessary when you are *not* using Architect to directly manage DHCP services; in that case you can leave them blank. See Appendix A, Manual DHCP Configuration, on page A-1, for more information.

Removing Targets

To remove a target that is currently being managed by the PXE Target Manager first select the target hostname in the list and then press the Remove Target button. You will be presented with a confirmation dialog. Press Yes to remove the target. Note that the target can be again added at any time if desired.

Editing Targets

To change the settings for a target currently being managed by the PXE Target Manager first select the target hostname in the list and then press the Edit Target button. You will be presented with a dialog similar to the following:

Edit PX	E Target ×	
Editing target 'sphynx'.		
Hostname: sphynx		
IP Address: 192.168.1.11		
MAC Address: C8:1F:66:06:84:A8		
On Next Boot		
○ Boot local disk		
Install local disk with:	RAM-analyzer.diskless 👻	
○ Boot diskless with:	RedHawk-8.2 (NFS) 🔻	
○ Start remote sync proc	ess	
	Cancel @OK	

Figure 4-13 Edit PXE Target Dialog

With this dialog you can change the hostname, IP address and MAC address of the host. You can also change the On Next Boot setting to change the behavior of the target upon next reboot. Refer to the discussion of On Next Boot above on page 4-8 for more information.

Press OK to apply these settings and return to the PXE Target Manager.

This appendix describes how to add the required DHCP configuration for Architect PXE targets to an active existing DHCP server configuration. It is preferable to allow the Architect tool to administer DHCP by checking the box labeled Automatically configure DHCP on this host, however if another DHCP server already exists on the desired subnet you must follow the steps described in this section. Refer to "Initializing PXE Services" on page 4-1 and also the **dhcpd.conf**(5) man page for more information.

Overview

The View DHCP Configuration button on the PXE Target Manager may be used to view the required DHCP configuration for Architect PXE targets. The information displayed may be cut and pasted into a text editor when editing the existing DHCP server configuration.

Alternatively, the DHCP configuration files maintained by Architect may be viewed or copied directly from the /etc/dhcp/architect directory on the host system where Architect is installed. This directory contains two files: dhcpd.conf and dhcpd-targets.conf. The dhcpd.conf file contains a subnet stanza with all required DHCP parameters set for PXE targets and it will look similar to the following example:

```
option pxe-client-arch-type code 93 = unsigned integer
16;
subnet 10.134.30.0 netmask 255.255.255.0 {
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.134.30.255;
        server-name cholula;
        next-server 10.134.30.166;
        if option pxe-client-arch-type = 00:09 {
            filename "architect/efi64/syslinux.efi";
        } elsif option pxe-client-arch-type = 00:07 {
            filename "architect/efi64/syslinux.efi";
        } else {
            filename "architect/bios/pxelinux.0";
        }
        use-host-decl-names on;
        include "/etc/dhcp/architect/dhcpd-targets.conf";
}
```

In this example, the PXE subnet is the 10.134.30.0/24 subnet. The last line includes all PXE target host declarations from the dhcpd-targets.conf file, which will look similar to the following example:

```
host monitor2 {
    hardware ethernet 00:02:AC:55:88:A9;
    fixed-address 10.134.30.65;
}
host analyzer {
    hardware ethernet 00:1B:21:D8:51:0C;
    fixed-address 10.134.30.11;
}
host ccenter {
    hardware ethernet 84:2B:2B:9E:6E:1B;
    fixed-address 10.134.30.17;
}
host monitor1 {
    hardware ethernet 00:23:AE:D9:1C:AF;
    fixed-address 10.134.30.64;
}
host recorder {
    hardware ethernet 00:80:8E:02:9A:92;
    fixed-address 10.134.30.72;
}
```

This configuration data must be added to the active DHCP server configuration file(s). On most systems, the main DHCP configuration file is /etc/dhcp/dhcpd.conf.

Installing DHCP Configuration

The simplest way to add the Architect DHCP configuration to the DHCP server is to copy the files from /etc/dhcp/architect on the Architect host to the same location on the DHCP server host, and then add a single include line to the existing /etc/dhcp/dhcpd.conf file to include the Architect configuration. If creating the /etc/dhcp/architect directory on the DHCP server host is not possible, you may use any valid location on the file system; simply adjust the include lines accordingly.

To accomplish this perform the following steps:

1. Copy files from the Architect host to the DHCP server host. For example, run this command on the Architect host:

scp -r /etc/dhcp/architect dhcp server:/etc/dhcp

where *dhcp* server is the name or IP address of the DHCP server host.

2. Include this configuration in the main DHCP server configuration file. Edit /etc/dhcp/dhcpd.conf on the DHCP server host and add this line near the bottom of the file:

include "/etc/dhcp/architect/dhcpd.conf";

Note that most DHCP servers allow multiple subnet stanzas to be defined for the same subnet, each with different parameters defined within the scope of the stanza. Because of this, you are allowed to have the PXE target systems declared within one subnet stanza, and other DHCP clients or a dynamic IP address pool declared in another subnet stanza for the same subnet.

NOTE

You cannot have duplicate host declarations or reuse an IP address or MAC address in different host declarations anywhere in the entire DHCP configuration.

See the **dhcpd**. conf(5) man page for more information.

RedHawk Architect User's Guide

This appendix describes the python scripts that can be run independent of the Architect GUI tool. Note that the scripts coordinate with the Architect tool by reading and updating the session file. These scripts are found under the directory: /usr/lib/architect/cli-tools.

build-image

mage	Builds an architect target image based on settings specified in the <i>session</i> file. It will replace the <i>root</i> path in the <i>session</i> file if a different path was previously used.
	<pre>build-image [-n][-l log] root session</pre>

Arguments:

Usage:

-	root	Specifies the <i>root</i> directory of the build image to be created.
	session	Specifies the architect <i>session</i> file to use.

Options:

-n	Run non-interactively.
-l log	Log output to the file log .
help	Display this help information.

Example:

```
cd /usr/lib/architect/cli-tools
sudo ./build-image -n -l /tmp/log.out \
    /var/lib/architect/images/rocky-8.4 \
    /root/Documents/sessions/rocky-8.4.session
```

chroot

	Executes a command in a chroot shell for the <i>root</i> system image directory specified.
Usage:	<pre>chroot [-m][-k kernel-release] root [cmd]</pre>
Arguments: root cmd	Specifies the <i>root</i> directory of the image to chroot to. An optional command to execute. If not specified, <i>cmd</i> defaults to /bin/bash .
Options:	
-m	Bind-mount read-only the host system's /proc, /sys, and /dev directories.
-k [kern	nel-release]

Fake the kernel release name in **/bin/uname**, necessary when building kernels in the chroot. The **kernel-release** format should

```
resemble the output from the command uname -r; for example
5.10.59-rt52-RedHawk-8.4-trace.
--help Display this help information.
--version
Display software version.
```

Examples:

```
cd /usr/lib/architect/cli-tools
sudo ./chroot /var/lib/architect/images/rocky8.4 blscfg
sudo ./chroot -m -k 5.10.59-rt52-RedHawk-8.4-trace \
    /var/lib/architect/images/rocky-8.4
```

make-pxe-diskless-image

Builds a PXE-bootable diskless image for an existing architect target system image based on settings specified in the *session* file. If it is the first time a PXE diskless image is built for this session, the script will use the corresponding GUI page defaults.

The settings can be modified using the GUI or editing the session file directly. Note that if you choose to modify the settings using the GUI, you must also build the PXE diskless image and then save the session.

NFS is the default diskless type. In order to switch to RAMDISK, you must build a RAMDISK diskless image using the GUI and save the session or edit the session file directly.

Usage: make-pxe-diskless-image [-n] [-l log] session pxe-name

Arguments:

session Specifies the architect session file to use. *pxe-name* Specifies the name of the PXE diskless image to be created.

Options:

-n	Run non-interactively.
-l log	Log output to the file log .
help	Display this help information.

Example:

```
cd /usr/lib/architect/cli-tools
sudo ./make-pxe-diskless-image -n -l /tmp/log.out \
    /root/Documents/rocky8.4.session rocky8.4-NFS
```

make-pxe-install-image

Builds a PXE-bootable installation image for an existing architect target system image based on settings specified in the *session* file. If it is the first time a PXE installation image is built for this session, the script will use the corresponding GUI page defaults.

The settings can be modified using the GUI or editing the session file directly. Note that if you choose to modify the settings using the GUI, you must also build the PXE install image and then save the session.

```
Usage: make-pxe-install-image [-n][-l log]
[-L LUKS-passphrase][-E encrypt-password]
session pxe-name
```

Arguments:

session	Specifies the architect session file to use.
pxe-name	Specifies the name of the PXE installation image to be created.

Options:

-n Run non-interactivel
-n Run non-interactivel

-1 log Log output to the file log.

-L passphrase

Use this **passphrase** for any LUKS volumes that are defined in the session file.

-E password

Use this **password** to encrypt the image.

--help Display this help information.

Example:

```
cd /usr/lib/architect/cli-tools
sudo ./make-pxe-install-image -n -l /tmp/log.out \
    -L londonbridgeisfallingup -E WxYZ1976 \
    /root/Documents/rocky8.4.session rocky8.4-pxe
```

setup-pxe

Configures PXE services on the current host. When executed with no arguments it will print the available subnets. The *dhcp subnet* is specified in the form ip_address/mask.

Usage: setup-pxe [-d] dhcp_subnet

Arguments:

```
dhcp subnet
```

Specifies which subnet on the host should be used when PXE booting from architect.

Options:

-d Do not configure DHCP server on this host.

--help Display this help information.

Examples:

cd /usr/lib/architect/cli-tools sudo ./setup-pxe sudo ./setup-pxe -d 192.0.2.0/255.255.255.0 RedHawk Architect User's Guide