



Hard Disks and Persistent Devices Installation Guide, 17.2.0

Contents

About This Guide.....	5
Installing the System.....	6
Overview.....	6
Before you begin.....	6
Image-based installation.....	6
Sample installation session.....	7
Specify the boot device in the system BIOS.....	8
Test your installation.....	8
Verify the release and system type.....	8
Verify connectivity.....	9
Upgrading the System.....	10
Release-specific upgrade information.....	10
Upgrade overview.....	10
Before upgrading.....	10
Upgrading the Vyatta ISO using "add system image".....	10
Sample session: "add system image".....	10
Installation and Upgrade Commands.....	12
add system image.....	12
clone system image.....	13



delete system image.....	14
install image.....	14
rename system image.....	15
set system image default-boot.....	15
show system image.....	15
spawn.....	16
List of Acronyms.....	17

Copyright Statement

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners.

The training materials and other content provided herein for assistance in training on the Vyatta vRouter may have references to Brocade as the Vyatta vRouter was formerly a Brocade product prior to AT&T's acquisition of Vyatta. Brocade remains a separate company and is not affiliated to AT&T.



About This Guide

This guide describes how to install and upgrade software on a persistent device, such as hard disk, flash drive, or USB stick on AT&T products that run on the AT&T Vyatta Network Operating System (referred to as a virtual router, vRouter, or router in the guide).



Installing the System

Overview

The AT&T Vyatta vRouter installs and runs on most standard x86 servers and PCs. The system installs from AT&T Vyatta vRouter LiveCD onto a variety of persistent devices, including a hard drive, USB memory stick, and compact Flash.

You install the system from LiveCD, which you create before installation. The installation process uses LiveCD as the source image, formats the device on which the system is being installed, installs the system, and, if possible, preserves configuration from previous installations. When the installation is completed, you reboot your system and the newly installed system begins running. This method is called disk-based installation and uses the binary system image for installation. Disk-based installation allows you to install multiple versions of the AT&T Vyatta vRouter as images and switch between the images easily.

Note: Not all hardware supports the ability to boot from a USB device or compact Flash; check the BIOS of your hardware to see if it does.

Before you begin

Before installing an AT&T Vyatta vRouter, prepare for the installation by performing these tasks:

- Find out the system name of the device onto which the software is to be installed. The installation process reformats the specified partition, so it is critical to specify the correct partition. For systems dedicated to AT&T Vyatta vRouter, the system-selected defaults can be used.
If you are installing a system onto a USB memory stick, insert the memory stick into a USB port. The system detects that the USB device is installed and notifies you; record the name of the device as displayed in the system message (for example, `/dev/sdb`). Specify this device when prompted during the installation procedure.
- Make sure you have a minimum of 2 GB of free space on the system for a root partition. A minimum of 4 GB of free space is recommended for a production installation.
- Make sure you have a minimum of 2 GB of RAM on the system. A minimum of 4 GB is recommended.
- The data plane supports from 1 to 128 CPUs. At least 4 CPUs are recommended for optimum performance.
- If you plan to install a system onto a USB stick, check the BIOS setup of your hardware to confirm that it supports the ability to boot from a USB device.
- Make sure any firmware- or driver-based RAID functionality, such as Intel Matrix Storage Manager (IMSM), is disabled in the BIOS of your system. Firmware-based RAID is not supported by the AT&T Vyatta vRouter. The AT&T Vyatta vRouter installation process offers to enable software RAID if two hard disks of equal size are detected. Software-based RAID is more reliable and compatible on AT&T Vyatta vRouter. Consult the documentation from your hardware manufacturer for instructions on disabling firmware-based RAID.
- Specify the boot device for the CD before installing the system, and change the boot device to hard drive after the installation. For more information about specifying the boot device, refer to [Specify the boot device in the system BIOS \(page 8\)](#)

Installing the system

To perform the installation, run the `install image` command from a running system. For a fresh installation, the running system is LiveCD, which you create before installation.

The process for creating LiveCD is described in AT&T Vyatta vRouter LiveCD Installation Guide.

To install the binary image, perform the following steps.

1. Create and boot LiveCD.
2. Enter the `install image` command.



3. Enter values to create drives and partitions, as required, in your server.
4. Enter a username for the administrator account.
5. Enter a password for the new username that you provided for the administrator.
6. When installation is completed, remove the LiveCD disk.
7. Set the BIOS on your system to boot from the device on which the AT&T Vyatta vRouter software is now installed.
8. Reboot the system.
9. Test the installation.

Sample installation session

The following example shows how to install an AT&T Vyatta vRouter by using the `install image` command.

Installing an AT&T Vyatta vRouter

The following example shows how to install AT&T Vyatta vRouter by using the `install image` command. The name of the image in the example is 17.1.0.

```
vyatta@vyatta:~$ install image

Welcome to the AT&T Vyatta vRouter image installer.
What would you like to name this image? [17.1.0-MASTER.12302358]:
This image will be named: 17.1.0-MASTER.12302358
The vRouter system requires a minimum 4096MB disk space
on a partition type 83 (Linux).
Probing drives: OK

The following drives were detected on your system:
sda    7516MB

Install the image on? [sda]:

Validating defaults... [OK]
Checking drive for previous configurations...
Cannot mount /dev/sda1
Looking for config files from previous installations on sda2...
I found the following installed system image(s) with config files on sda2:
  1: 17.1.0-MASTER.12221817
Would you like to save config information from it? (Yes/No) [Yes] No
OK. Config information not saved.

Enter username for administrator account [vyatta]:

Enter password for administrator account
Enter password for user 'vyatta':
Retype password for user 'vyatta':

I found the following configuration files:
  /config/config.boot
  /opt/vyatta/etc/config.boot.default
Which one should I copy? [/config/config.boot]:
Enter the desired system console [ttyS0]:
Enter the console speed [115200]:
A legacy partition table (msdos) supports drives up to 2 TB
GPT partition format supports larger drives and partitions
Disk label type (msdos/gpt) [gpt]:
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted?

If partitions are already set up, you may skip this step.
Partition (Auto/Parted/Skip) [Auto]:
Welcome to the Automated Partition Installer!
Size of BIOS_BOOT partition? [256]:
```



```
Size of the log partition? [0]:
Size of the virt-images (libvirt) partition? [1024]:
Size of the swap partition? [1024]:
Using 4690 for the vRouter.
Ready to write partitions to disk
Continue (Yes/No) [No]: Yes
Removing old partitions...
Writing partition to disk: [sda] [BIOS_PART] [256]
Writing partition to disk: [sda] [vRouter] [4690] [ext4]
Creating filesystem on /dev/sda2...OK
Writing partition to disk: [sda] [LIBVIRT] [1024] [ext4]
Creating filesystem on /dev/sda3...OK
Writing partition to disk: [sda] [linux-swap] [1024]
Setting up swapspace version 1, size = 1000444 KiB
no label, UUID=ac002778-a285-4e4e-aa31-81963ac881a5
Settling...Done!
Mounting /dev/sda2...
Setting up grub on /dev/sda: OK
Copying squashfs image...
Copying kernel and initrd images...
Copying /config/config.boot...
Running post-install script...
Done.

vyatta@vyatta:~$
```

Note: The password for the vyatta user must be changed from its default of vyatta.

Specify the boot device in the system BIOS

You can configure the BIOS to specify the device from which to boot.

To specify the boot device:

1. During the boot sequence press the appropriate key sequence (for example, <F2>) to interrupt the boot sequence and enter the BIOS setup program for your system.
2. In the boot sequence menu, arrange the boot devices such that the device name (for example, USB HDD for a USB stick or IDE or SATA for a compact Flash) is first in the list so that the system attempts to boot from it first.
3. Save the settings and reboot the system. When the system restarts, it boots from the device specified.

Testing your installation

After the system has successfully booted, you see the `login:` prompt. This prompt indicates that the system is operational.

Perform the following procedures to test your installation:

- Verify the release and system type
- Verify connectivity

Verifying the release and system type

You must confirm that the correct release version is running on the system.

To verify the release and system type, perform the following steps.

1. Log in with the username and password that you provided during installation. During installation, if you did not select the default user of `vyatta`, use the new username and password you created during the installation. Use the default password of `vyatta` unless you have changed it.
2. Enter the `show version` command.

Info:



- The `Version:` line displays the version number of the system that is running. Ensure that the displayed result is the version you require.
- The `System type:` line displays the type of hardware on which the system is running and whether it is in a virtual environment. Ensure that the displayed result is the version you require.
- The `Boot via:` line displays the type of system that is running.

Verifying connectivity

After you confirm that the correct version is running, you must confirm that the system can be accessed on the local network. Configure an Ethernet interface on the system and ping the interface from another host on the network.

Note: In the system, a data plane interface is an abstraction that represents the underlying physical or virtual Ethernet interface of the system. The terms Ethernet interface and data plane interface are synonymous in this guide.

To test the system connectivity, perform the following steps:

1. At the command prompt, enter the commands that are shown in the example, substituting an IP address from your existing subnet. The example uses the following network and IP address.

Info:

- The network is 192.168.1.0/24.
- The IP address of the interface is 192.168.1.81.

Make the appropriate substitutions for your network, as shown in the following example.

Example:

```
vyatta@vyatta:~$ configure
vyatta@vyatta# set interfaces dataplane dp0sN address 192.168.1.81/24
vyatta@vyatta# commit
vyatta@vyatta# save
vyatta@vyatta# exit
vyatta@vyatta:~$
```

2. From another host on the same subnet, ping the interface to ensure that it is up. From a Linux or Windows command prompt, enter the following command, substituting the IP address you assigned to the interface.

Info:

```
ping 192.168.1.81
```

If the system can be reached, you see replies from it in response to the pings. If so, your system is installed and can be accessed on your network.



Upgrading the System

Release-specific upgrade information

Your system may have special upgrade considerations, depending on your release. For release-specific upgrade information and to ensure that configuration information is correctly preserved, see the release notes for your release.

Upgrade overview

Using the `add system image` command is currently the only supported upgrade method for physical hardware systems.

You must download a new system image from Business Center, and then add the image to previous versions of the system that are present by using the `add system image` command. The `add system image` command also allows you to migrate the current configuration to the new image. After the system is rebooted, the new image is running.

Before upgrading

Before upgrading the system, you must perform the following tasks.

- Save your existing configuration file for reference. Your configuration file is named `config.boot` and is located in the `/config` directory.
- Ensure that you have enough space on your root partition to load the image. You can determine the amount of space that is available by using the `show system storage` command.
- Download the ISO image file to use for your upgrade.

Upgrading the ISO

The `add system image` command uses an ISO file as the image source. The command installs the image with existing images and sets the new image as the default boot image. The new image is run the next time the system is rebooted.

Determine the location of the ISO file and record the name of the file.

To prepare for the upgrade, perform the following steps.

1. Enter the `add system image` command. Use the location and name of the ISO file as arguments in the command, as shown in [Example of upgrading the ISO \(page 10\)](#).
2. Before you reboot the system, confirm that the new image is loaded and ready to run the next time the system is rebooted. (Enter the `show system image` command; see [Example of upgrading the ISO \(page 10\)](#).)
3. Reboot the system by entering the `reboot` command. The system restarts with the new system image.

Example of upgrading the ISO

The following example shows how to use the `add system image` command to upgrade the `xxx.iso` system image, where `xxx` is the file name of the ISO image that you have downloaded. The following example uses the `4.xR1` image.

```
vyatta@vyatta:~$ add system image /home/vyatta/xxx.iso
Checking MD5 checksums of files on the ISO image...OK.
Done!
What would you like to name this image? [4.xR1]:
OK. This image will be named: 4.xR1
```



```
Installing "4.xR1" image.  
Copying new release files...  
Would you like to save the current configuration  
directory and config file? (Yes/No) [Yes]:  
Copying current configuration...  
Would you like to save the SSH host keys from your  
current configuration? (Yes/No) [Yes]:  
Copying SSH keys...  
Setting up grub configuration...  
Done.  
vyatta@vyatta:~$
```

The following example shows how to display installed images.

```
vyatta@vyatta:~$ show system image  
The system currently has the following image(s) installed:  
  1: xxx (default boot)  
  2: yyy (running version)
```



Installation and Upgrade Commands

add system image

Adds a binary system image to the currently running system.

Syntax:

```
add system image { iso-filename | iso-URL [ username username password password ] }
```

iso-filename

Name of the image file to be added.

iso-URL

URL location of the image file to be added.

username *username*

Specifies the username that is required to log in to the remote system at the indicated URL location.

password *password*

Specifies the password that is required to log in to the remote system at the indicated URL location. If the username is specified, then a password must also be specified.

Operational mode

Use this command to add a binary image to the currently running system. A system image can be added to a system that was installed by using a disk-based installation or an image-based installation. After an image is added, it is set as the new default boot image and is run the next time the system is booted.

The command validates the MD5 checksums of the files that are contained in the ISO image to ensure that the image has not been corrupted. In addition, the command does not allow more than one copy of an image to exist on the same system.

The *iso-filename* and *iso-URL* arguments provide the source for the ISO image file.

The following table shows how to specify the file syntax for different file locations.

Location	Specification
An absolute path	For <i>iso-filename</i> , use standard UNIX file specification.
A relative path	For <i>iso-filename</i> , you can also specify the path name relative to the current directory.
FTP server	Use the following syntax for the <i>iso-URL</i> argument: <code>ftp://user:passwd@host/image-file</code> where <i>user</i> is the username on the host, <i>passwd</i> is the password that is associated with the username, <i>host</i> is the host name or IP address of the FTP server, and <i>image-file</i> is the ISO image file, including the path. Alternatively, the username and password can be specified as username and password arguments of the <code>add system image</code> command. If you do not specify <i>user</i> and <i>passwd</i> , you are prompted for them.



Location	Specification
SCP server	Use the following syntax for the <i>iso-URL</i> argument: <code>scp://user:passwd@host/image-file</code> where <i>user</i> is the username on the host, <i>passwd</i> is the password that is associated with the username, <i>host</i> is the host name or IP address of the SCP server, and <i>image-file</i> is the ISO image file, including the path. Alternatively, the username and password can be specified as username and password arguments to the <code>add system image</code> command. If you do not specify <i>user</i> and <i>passwd</i> , you are prompted for them.
HTTP server	Use the following syntax for the <i>iso-URL</i> argument: <code>http://host/image-file</code> where <i>host</i> is the host name or IP address of the HTTP server and <i>image-file</i> is the ISO image file, including the path relative to the HTTP root directory.
TFTP server	Use the following syntax for the <i>iso-URL</i> argument: <code>tftp://host/image-file</code> where <i>host</i> is the host name or IP address of the TFTP server, and <i>image-file</i> is the ISO image file, including the path relative to the TFTP root directory.

clone system image

Creates a copy of a system image that is installed on the local system or a remote system.

Syntax:

```
clone system image [ user@host: ] source-image-name new-image-name [ clean ]
```

user

Username on a remote host. A username is required for remote host access through SCP and is not required for cloning a local system image.

host

Host name or IP address of a remote host. The host name or IP address is required for remote access through SCP and is not required for cloning a local system image.

source-image-name

Name of a system image to be copied. The source image can exist on the local system or a remote system.

new-image-name

Name of the new (copied) system image. An image with this name must not exist on the system.

clean

Creates an empty read/write directory tree for the new image, which is a new image that is functionally equivalent to the source image as it existed when it was originally installed.

Operational mode

Use this command to create a copy of a system image that is installed on the local system or a remote system.

If *user@host* is specified, the image is fetched from the named host by using the Secure Copy Protocol (SCP). If *user@host* is omitted, *source-image-name* is the name of an image that exists on the system, and *new-image-*



name is the image name that the system uses for the clone. No image that is named *source-image-name* can exist on the system.

Command completion is performed for local image names if *user@host* is not specified. No command completion is performed on remote image names if *user@host* is specified.

If the **c1ean** argument is omitted, the command copies the *squashfs* file that is being used by the image named *source-image-name* and the read/write directory tree of *source-image-name*. If the **c1ean** argument is given, the read/write directory tree of *source-image-name* is not copied. Instead, an empty read/write directory tree is created for the new image, which creates a new image that is functionally equivalent to the source image as it existed when it was initially installed.

Images created by this command behave the same as images that are installed by [install image \(page 14\)](#) or [add system image \(page 12\)](#).

Both the HTTPS and SSH services must be enabled on the remote system for [clone system image \(page 13\)](#) to work properly. The HTTPS service is enabled by using the `set service https` command in configuration mode. The SSH service is enabled by using the `set service ssh` command in configuration mode.

delete system image

Deletes an image from the local disk drive.

Syntax:

```
delete system image [ image-name ]
```

When the command is entered without an image name, the system prompts for the image to delete.

image-name

Name of an image to be deleted.

Operational mode

Use this command to delete an image from the local disk drive.

The image and all its local files, including its configuration file, are destroyed. Because this command is destructive, the system prompts for confirmation.

Command completion displays all valid completions for the *image-name* argument. If the *image-name* argument is omitted, the system displays a list of available images and prompts you to select one.

If the system was originally installed in disk-based mode, an **image-name** option is available that you can use to direct that the disk-based installation must be deleted.

The system does not allow you to delete the currently running system image. However, the system does allow you to delete the image currently selected to be run at the next reboot. If you delete that image, the system uses the currently running image when the system is next rebooted.

install image

Installs a binary image of the system.

Syntax:

```
install image
```

Operational mode

Use this command to install a binary image of the system.

After the installation is completed, you can add multiple image versions to the same partition by using the `add system image` command, and you can then choose which version to boot by using the `set system image default-boot` command. This functionality allows you to move easily between different versions of the system.

If you have a new system and want to install from scratch, you can boot LiveCD or LiveUSB and run the `install image` command to install the image on LiveCD or LiveUSB to the disk. The `install image` command operates similarly to the `install system` command—it creates and formats a new disk partition and then installs the image to the partition while preserving the system configuration.



rename system image

Renames an image.

Syntax:

```
rename system image old-image-name new-image-name
```

old-image-name

Name of an existing image to be renamed.

new-image-name

New name for the image.

Operational mode.

Use this command to rename an image.

The old name must match the name of an image on the system. The system does not allow you to rename the currently running system image. The new system image name cannot be in use by another image.

set system image default-boot

Selects an image to be run when the system is next rebooted.

Syntax:

```
set system image default-boot [ image-name ]
```

If the command is used without specifying an image name, the system displays a list of available images and prompts you to select one.

image-name

Name of an image to be run when the system is rebooted.

Operational mode

Use this command to select an image to run when the system is next rebooted.

When multiple system images have been installed by using the `add system image` command, you can use this command to direct the system to boot from a specific system image the next time the system is restarted.

Command completion displays all valid completions for the *image-name* argument. If the *image-name* argument is omitted, the system displays a list that shows all images that are installed on the system and prompts you to select one. If the system was originally installed in disk-based mode, a special **image-name** option is available so that you can select the disk-based system as the default system from which to boot.

show system image

Displays a list of all images that are installed on the system.

Syntax:

```
show system image [ storage | version ]
```

storage

Displays the amount of disk space that is used by each image.

version

Includes the image version number in the display of system images.

Operational mode

Use this command to display a list of all images that are installed on the system.

The command output identifies the image that is currently running and the image that has been selected to run when the system is next rebooted. If the system was originally installed in disk-based mode, one of the image names identifies that installation.



spawn

Allows you to run any native Linux command through the operational mode infrastructure.

Syntax:

```
spawn command-name [ text ]
```

command-name

Command to run

text

An argument to a command

Operational mode

Use this command to run any native Linux command through the operational mode infrastructure.

Commands that are spawned are run by the local shell, and with the current user's permissions. The spawned command provides a documented and supported way of running any Linux command.

The spawned command prevents any changes to the set of modeled commands from effecting the user's ability to run native commands consistently, if they are using this supported method.



List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System



Acronym	Description
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP Security
IPv4	IP Version 4
IPv6	IP Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast



Acronym	Description
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect



Acronym	Description
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell



Acronym	Description
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access