



The Linux & Open Source Company

Automated Provisioning with SecureBoot and Foreman

Jan Löser

THE Linux & Open Source Company!



Consulting



Engineering



Support



Training



About Me

- ▶ Jan Löser
- ▶ IT consultant at ATIX AG since 2022
- ▶ 15+ years experience in (professional) Linux
- ▶ Focus
 - ▶ Security/hardening (Secure Boot, Measured Boot)
 - ▶ DevOps, Automation
- ▶ openSUSE & vim user

Contact:

- ▶ Mail: loeser@atix.de
- ▶ GitHub: <https://github.com/jloeser>
- ▶ Matrix: [@jloe:matrix.org](https://matrix.org/#/@jloe:matrix.org)

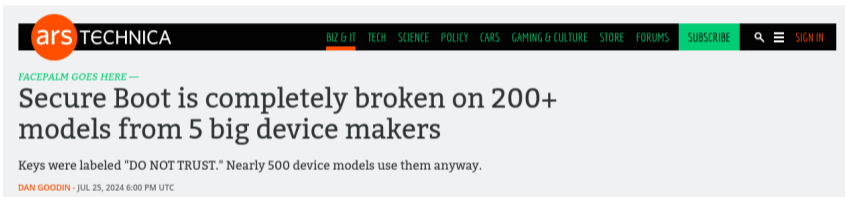
Agenda

- ▶ Introduction to Secure Boot
- ▶ Provisioning with Foreman (so far)
- ▶ Host Specific Network Boot Files in Foreman
- ▶ Status & Outlook

Secure What?

- ▶ Part of the Unified Extensible Firmware Interface (UEFI) specification
- ▶ Ensures the authenticity of software which is loaded and executed by the firmware utilizing cryptographic mechanisms ("Chain of Trust")
- ▶ Not without controversy
 - ▶ MS is certificate authority (at least by default)
 - ▶ Kernel ok, but initrd?
 - ▶ More complexity, more code, more bugs, more potential attack vectors for attackers

Secure What?



The screenshot shows the top portion of a web page. At the top left is the 'ars TECHNICA' logo, with 'ars' in a red circle and 'TECHNICA' in white on a black background. To the right is a navigation bar with links for 'BIZ & IT', 'TECH', 'SCIENCE', 'POLICY', 'CARS', 'GAMING & CULTURE', 'STORE', 'FORUMS', 'SUBSCRIBE', a search icon, and 'SIGN IN'. Below the navigation bar is a green placeholder text 'FACEPALM GOES HERE —'. The main headline reads 'Secure Boot is completely broken on 200+ models from 5 big device makers'. A sub-headline below it says 'Keys were labeled "DO NOT TRUST." Nearly 500 device models use them anyway.' At the bottom left of the article header, it says 'DAN GOODIN - JUL 25, 2024 6:00 PM UTC'.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS SUBSCRIBE 🔍 ☰ SIGN IN

FACEPALM GOES HERE —

Secure Boot is completely broken on 200+ models from 5 big device makers

Keys were labeled "DO NOT TRUST." Nearly 500 device models use them anyway.

DAN GOODIN - JUL 25, 2024 6:00 PM UTC

UEFI-Schwachstelle LogoFAIL: Secure Boot mit manipulierten Bootlogos umgehbar

Sicherheitsforscher haben Schwachstellen beim Verarbeiten von Bootlogos auf BIOS/UEFI-Ebene entdeckt. Angreifer können Systeme kompromittieren.



(Bild: LuckyStep/Shutterstock.com)

03.12.2023, 14:45 Uhr | Lesezeit: 2 Min. | Security

Von Dennis Schirmacher

Secure What?



Support

Certain BIOS versions may include an AMI Test Key that could compromise Secure Boot protections

RSS

Lenovo Security Advisory: LEN-7806

Potential Impact: Secure boot may be compromised by an attacker with local access

Severity: High

Scope of Impact: Lenovo-specific

Secure What?



The screenshot shows a Reddit post interface. At the top left is the Reddit logo and a search bar containing 'r/MSI_Gaming'. Below the search bar, the post header shows a back arrow, the subreddit 'r/MSI_Gaming' with a location pin icon, the user 'MSI_TechK MOD' with a verified badge, and the time '2 yr. ago'. The title of the post is 'MSI Statement on Secure Boot'. The main text of the post is as follows:

MSI implemented the Secure Boot mechanism in our motherboard products by following the design guidance defined by Microsoft and AMI before the launch of Windows 11. We preemptively set Secure Boot as Enabled and "Always Execute" as the default setting to offer a user-friendly environment that allows multiple end-users flexibility to build their PC systems with thousands (or more) of components that included their built-in option ROM, including OS images, resulting in higher compatibility configurations. For users who are highly concerned about security, they can still set "Image Execution Policy" as "Deny Execute" or other options manually to meet their security needs.

In response to the report of security concerns with the preset bios settings, MSI will be rolling out new BIOS files for our motherboards with "Deny Execute" as the default setting for higher security levels. MSI will also keep a fully functional Secure Boot mechanism in the BIOS for end-users so that they can modify it according to their needs.



Alert!

BootHole: Bugs im Bootloader Grub gefährden Linux und Windows

Angreifer könnten sich in den Boot-Prozess einklinken und quasi unsichtbare Schadsoftware einschleusen – trotz Secure Boot.



(Bild: Eclipsium)

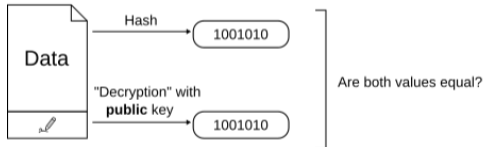
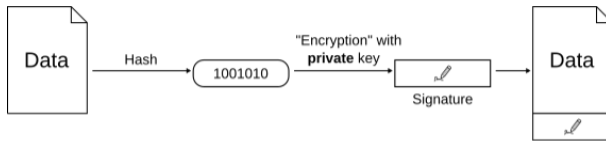
30.07.2020, 15:36 Uhr | Lesezeit: 2 Min. | Security

Von Jürgen Schmidt

Secure What?

- ▶ Part of the Unified Extensible Firmware Interface (UEFI) specification
- ▶ Ensures the authenticity of software which is loaded and executed by the firmware utilizing cryptographic mechanisms ("Chain of Trust")
- ▶ Not without controversy
 - ▶ MS is certificate authority (at least by default)
 - ▶ Kernel ok, but initrd?
 - ▶ More complexity, more code, more bugs, more potential attack vectors for attackers
- ▶ SecureBoot changes require physical access to the system
- ▶ SecureBoot is **not** Measured/Trusted Boot (keyword "TPM")

Signature Basics



Certificates contain the public key portion!

Signatures in the Wild

```
1 xps:~ # pesign -S -i /boot/vmlinuz
2 -----
3 certificate address is 0x7fd95e5289e8
4 Content was not encrypted.
5 Content is detached; signature cannot be verified.
6 The signer's common name is SUSE Linux Enterprise Secure Boot Signkey
7 The signer's email address is build@suse.de
8 Signing time: Fri Jun 07, 2024
9 There were certs or crls included.
10 -----
```

```
1 xps:~ # pesign -S -i /boot/efi/EFI/opensuse/shim.efi
2 -----
3 certificate address is 0x7f3307126e90
4 Content was not encrypted.
5 Content is detached; signature cannot be verified.
6 The signer's common name is Microsoft Windows UEFI Driver Publisher
7 No signer email address.
8 No signing time included.
9 There were certs or crls included.
10 -----
```

Is this Thing On?

UEFI?

```
1 xps:~ # readlink -f /sys/firmware/efi/efivars/  
2 /sys/firmware/efi/efivars
```

SecureBoot?

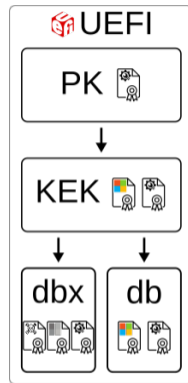
```
1 xps:~ # od --address-radix=n --format=u1 /sys/firmware/efi/efivars/SecureBoot-*  
2 6 0 0 0 1
```

Easier!

```
1 xps:~ # mokutil --sb  
2 SecureBoot enabled
```

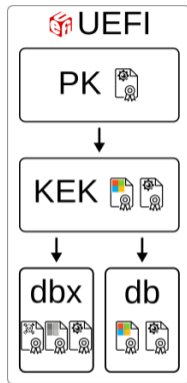
Chain of Trust

- ▶ Platform Key (PK):
 - ▶ Root-of-trust anchor embedded into the system firmware
 - ▶ Certificate installed by the hardware/platform vendor on the system
 - ▶ Establishes trust between the hardware vendor and the firmware that runs on it
 - ▶ To modify PK a valid signature of the PK is required (self-signed)
- ▶ Key Exchange Key (KEK):
 - ▶ Establishes trust between the hardware vendor and the operating system
 - ▶ To modify KEK a valid signature of the PK is required

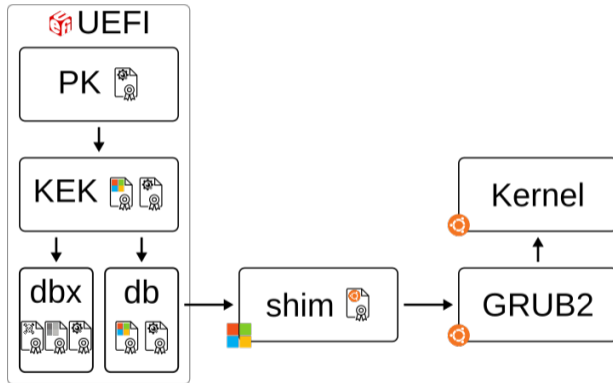


Chain of Trust

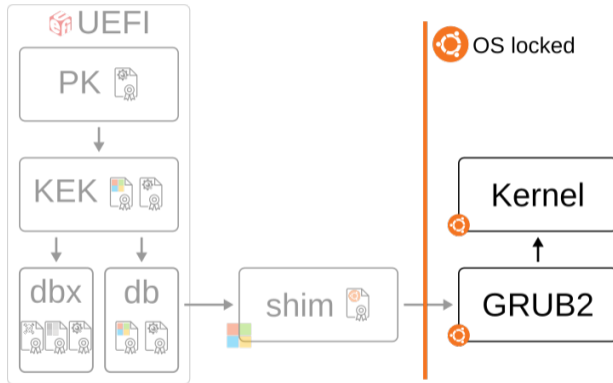
- ▶ Signature Database (db):
 - ▶ Database containing trusted signatures and certificates for third-party UEFI components and boot loaders
 - ▶ To modify db a valid signature of the KEK is required
- ▶ Forbidden Signature Database (dbx):
 - ▶ Database of signatures and certificates used for revoking previously trusted boot components so they can no longer run during bootup
 - ▶ To modify dbx a valid signature of the KEK is required



Chain of Trust



Chain of Trust



Where is This shim Born?

rhboot / shim-review

Code Issues 32 Pull requests 1 Actions Projects Security Insights

Search: Type to search

Filters: is:issue is:closed

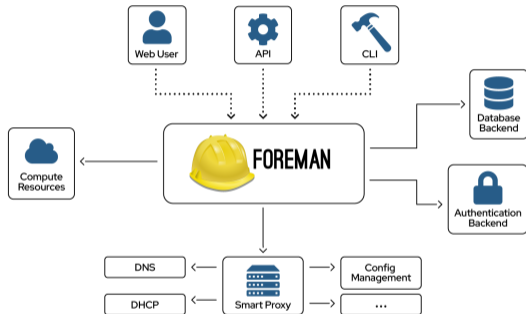
Labels 15 Milestones 0 New issue

Clear current search query, filters, and sorts

Issue	Author	Label	Projects	Milestones	Assignee	Sort
Shim 15.8 for AlmaLinux OS 8 (aarch64) accepted contracts verified OK easy to review	#432 by esbdulf1					0
Alpaquita Linux shim-15.8 x64 and aarch64 accepted contracts verified OK	#426 by akotanev					0
SUSE Liberty Linux 9 accepted contracts verified OK easy to review	#419 by jseitz					12
Debian GNU/Linux 10 (buster LTS) shim-15.8-1 x64 and ia32 accepted contracts verified OK easy to review	#418 by steve-mcintyre					0
Debian GNU/Linux 11 (bullseye) shim-15.8-1 x64 and ia32 accepted contracts verified OK easy to review	#417 by steve-mcintyre					3
Debian GNU/Linux 12 (bookworm) shim-15.8-1 x64, ia32 and aarch64 accepted contracts verified OK	#416 by steve-mcintyre					3
Debian GNU/Linux 13 (trixie) shim-15.8-1 x64 and aarch64 accepted contracts verified OK	#415 by steve-mcintyre					0
Shim 15.8 for Proxmox Bookworm-based accepted	#414 by Fabian-Graebtlicher					0
Shim 15.8 for Navix 9 accepted contracts verified OK easy to review						21

The Foreman

- ▶ Complete lifecycle management tool for physical and virtual hosts
- ▶ Easy to automate repetitive tasks, quickly deploy applications, and proactively manage hosts
- ▶ Provisions hosts
- ▶ Upstream project for orcharhino (ATIX) and Red Hat Satellite
- ▶ Recently celebrated its 15th birthday



The Foreman

The screenshot displays the Foreman web interface. At the top, there is a navigation bar with the Foreman logo, a search bar, and filters for organization and location. A left sidebar contains a menu with options like Monitor, Content, Hosts, and Configure. The main area is titled 'Hosts' and features a search bar, a 'Manage columns' button, and a 'Select Action' dropdown. Below this is a table listing 19 hosts with columns for Power, Name, OS, Owner, Host group, Boot time, Last report, Comm..., Puppet env, and Actions. The table shows various operating systems including CentOS Stream 9, Debian 11, RHEL 9, Rocky Linux 8, SLES 15 SP6, Ubuntu 22.04 LTS, and Windows 11. The bottom of the page shows pagination information: '1 - 19 of 19 items' and '1 of 1'.

<input type="checkbox"/>	Power	Name	OS	Owner	Host group	Boot time	Last report	Comm...	Puppet env	Actions
<input type="checkbox"/>		fm-c9s.testproxy.atix	CentOS Stream 9	Admin ..	CentOS Stream 9/sta...	3 days ago	13 minutes a...		production	Edit
<input type="checkbox"/>		fm-e9.testforeman.atix	CentOS Stream 9	Admin ..	CentOS Stream 9	3 days ago	30 minutes a...		production	Edit
<input type="checkbox"/>		fm-d1s.testproxy.atix	Debian 11	Admin ..	Debian 11/static				production	Edit
<input type="checkbox"/>		fm-d11.testforeman.atix	Debian 11	Admin ..		3 days ago	less than a m...		production	Edit
<input type="checkbox"/>		fm-r9.testforeman.atix	RHEL 9	Admin ..	RHEL 9	2 days ago	16 minutes a...		production	Edit
<input type="checkbox"/>		fm-r8s.testproxy.atix	Rocky Linux 8	Admin ..	Rocky Linux 8/static	3 days ago	8 minutes ago		production	Edit
<input type="checkbox"/>		fm-r8.testforeman.atix	Rocky Linux 8	Admin ..	Rocky Linux 8	3 days ago	24 minutes a...		production	Edit
<input type="checkbox"/>		fm-s156s.testproxy.atix	SLES 15 SP6	Admin ..	SLES 15 SP6/static				production	Edit
<input type="checkbox"/>		fm-s156.testforeman.atix	SLES 15 SP6	Admin ..	SLES 15 SP6	3 days ago	5 minutes ago		production	Edit
<input type="checkbox"/>		fm-u22.testforeman.atix	Ubuntu 22.04 LTS	Admin ..	Ubuntu 22.04	3 days ago	16 minutes a...		production	Edit
<input type="checkbox"/>		fm-u24s.testproxy.atix	Ubuntu 24.04 LTS	Admin ..	Ubuntu 24.04/static				production	Edit
<input type="checkbox"/>		fm-u24.testforeman.atix	Ubuntu 24.04 LTS	Admin ..	Ubuntu 24.04	3 days ago	13 minutes a...		production	Edit
<input type="checkbox"/>		fm-w1s.testproxy.atix	Windows 11	Admin ..	Windows 11/static	3 days ago	18 minutes a...		production	Edit
<input type="checkbox"/>		fm-w11.testforeman.atix	Windows 11	Admin ..	Windows 11	3 days ago	23 minutes a...		production	Edit
<input type="checkbox"/>		fm-w2022s.testproxy.atix	Windows Server 2022	Admin ..	Windows 2022/static	3 days ago	24 minutes a...		production	Edit
<input type="checkbox"/>		fm-w2022.testforeman.atix	Windows Server 2022	Admin ..	Windows 2022	3 days ago	30 minutes a...		production	Edit
<input type="checkbox"/>		foreman-proxy.testproxy.atix	Rocky Linux 8	Fabrice...		2 days ago	12 minutes a...		production	Edit
<input type="checkbox"/>		foreman.testforeman.atix	Rocky Linux 8	Fabrice...		2 days ago	11 minutes ago		production	Edit
<input type="checkbox"/>		or-4846-thorbend-rocky8-testte...	Rocky Linux 8	Thorbe...	Rocky Linux 8	1 month ago	2 minutes ago		production	Edit

The Foreman

The screenshot displays the Foreman web interface for a host named 'fm-s156.testforeman.atix'. The interface includes a navigation sidebar on the left with options like Monitor, Content, Hosts, Configure, Infrastructure, and Administer. The main content area shows the host's overview, including its status (3 green, 0 yellow, 2 red, 1 grey), content view details (Composite SLES 15 SP6, Testing), and a pie chart of errata (44 total: 13 security advisories, 30 bug fixes, 1 enhancement). Other sections include recent jobs (one failed), recent communication (last configuration report 5 minutes ago), host collections, recent audits, and system purpose.

FOREMAN Any organization Any location Jan Loeser

Search and go

Monitor

Content

Hosts

Configure

Infrastructure

Administer

Hosts > fm-s156.testforeman.atix

fm-s156.testforeman.atix **SLES 15 SP6** x86_64

Schedule a job Edit

Created 3 days ago by Admin User (updated 3 minutes ago)

Overview Details Content Parameters Traces Puppet Ansible Reports

Host status

3 0 2 1

Manage all statuses

Content view details

Content view

Composite SLES 15 SP6 **Testing**

Version in use

Version 2.0 (latest)

Errata Applicable Installable

44 errata

13 security advisories

30 bug fixes

1 enhancement

Details

IPv6 address

Not available

IPv4 address

192.168.185.57

MAC address

00:50:56:b4:cb:fe

Host group

SLES 15 SP6

Host owner

Admin User

Comment

Recent jobs

Finished Running Scheduled

Run Ansible roles 3 days ago failed

Recent communication

Last configuration report 5 minutes ago

Last check-in: 3 days ago

Host collections

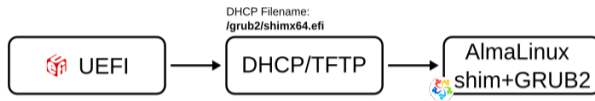
Recent audits All audits

update 3 days ago foreman_...

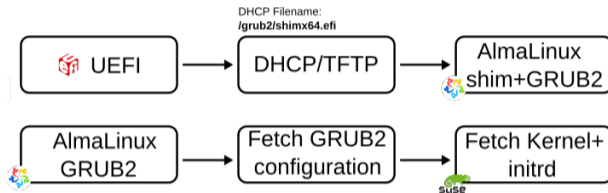
System purpose Edit

Role

Provisioning with Foreman - Network Provisioning



Provisioning with Foreman - Network Provisioning

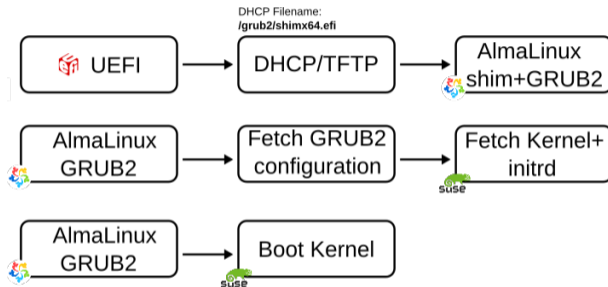


Provisioning with Foreman - Network Provisioning

GRUB2 configuration:

```
1 # This file was deployed via 'AutoYaST default PXEGrub2' template
2
3 set default=0
4 set timeout=10
5
6 menuentry 'AutoYaST default PXEGrub2' {
7     linux boot/sles-12-sp5-local-RwGLJDBLRnmP-linux ramdisk_size=65536 install=http://foreman.
           foreman.test/pulp/isos/ATIX/Media/Media/custom/Media/SLES_12_SP5/ autoyast=http://
           foreman.foreman.test:8000/unattended/provision textmode=1
8     initrd boot/sles-12-sp5-local-RwGLJDBLRnmP-initrd
9 }
10 ...
```

Provisioning with Foreman - Network Provisioning



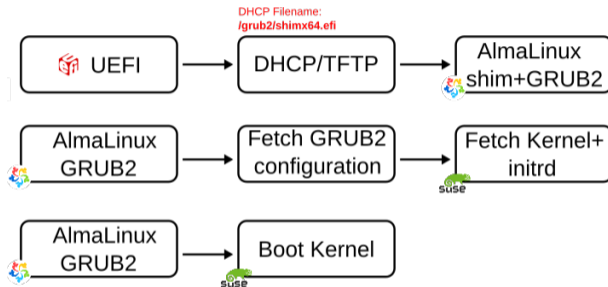
Provisioning with Foreman - Network Provisioning

:(

```
1 error: bad shim signature.  
2 error: you need to load the kernel first.  
3  
4 Press any key to continue...
```

That is a great pity! But understandable by design, isn't it?

Provisioning with Foreman - Network Provisioning



Provisioning with Foreman - Network Provisioning

Let's check the DHCP filename option:

```
1  ...
2  host suselinux.foreman.test {
3    dynamic;
4    hardware ethernet 00:50:56:b4:ee:9b;
5    fixed-address 192.168.145.118;
6        supersede server.filename = "grub2/shimx64.efi";
7        supersede server.next-server = c0:a8:91:0a;
8        supersede host-name = "suselinux.foreman.test";
9  }
10 host ubuntu.foreman.test {
11  dynamic;
12  hardware ethernet 00:50:56:f4:ae:97;
13  fixed-address 192.168.145.116;
14      supersede server.filename = "grub2/shimx64.efi";
15      supersede server.next-server = c0:a8:91:0a;
16      supersede host-name = "ubuntu.foreman.test";
17  }
18  ...
```

Provisioning with Foreman - Network Provisioning

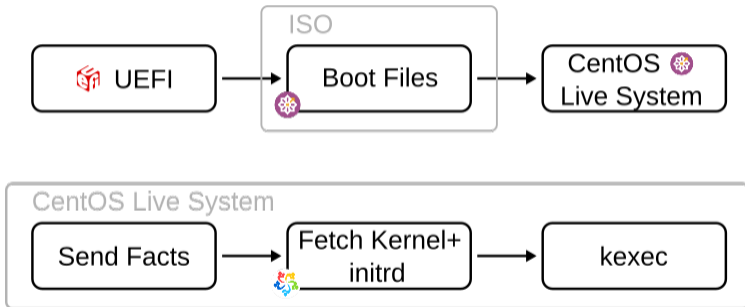
Let's check the `grub2/shimx64.efi` on the TFTP server:

```
1 [root@foreman ~]# strings /var/lib/tftpboot/grub2/shimx64.efi | grep ",shim,"
2 shim,4,UEFI shim,shim,1,https://github.com/rhboot/shim
3 shim.almalinux,3,AlmaLinux,shim,15.8,security@almalinux.org
```

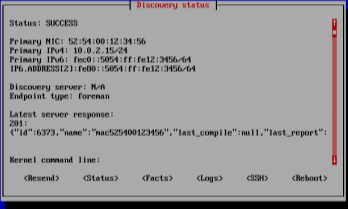
Why AlmaLinux?

```
1 [root@foreman ~]# . /etc/os-release ; echo $PRETTY_NAME
2 AlmaLinux 8.10 (Cerulean Leopard)
```

Provisioning with Foreman - Foreman Discovery Image & kexec



Provisioning with Foreman - Foreman Discovery Image & kexec



```
Discovery status
Status: SUCCESS
Primary NIC: 52:54:00:12:34:56
Primary IPv4: 10.0.2.15/24
Primary IPv6: fe80::5054:ff:fe12:3456/64
IPv6 ADDRESS(2): fe80::5054:ff:fe12:3456/64
Discovery server: N/A
Endpoint type: foreman
Latest server response:
201:
{"id":6373,"name":"mac525400123456","last_compile":null,"last_report":
Kernel command line:
  <Resend>  <Status>  <Facts>  <Logs>  <SSH>  <Reboot>
```

Foreman Discovery Image v4.1.0 (20220719.1) x86_64-linux UEFI 0 EFI UGA

Provisioning with Foreman - Foreman Discovery Image & kexec

Go for it!

```
1 [root@fdi ~]# kexec --force -s --append="console=ttyS0" --initrd=/tmp/almalinux8-mirror-  
    tb70qghGi6RT-initrd.img /tmp/almalinux8-mirror-tb70qghGi6RT-vmlinuz  
2 kexec_load failed: Permission denied  
3 entry      = 0x27fff7730 flags = 0x3e0000  
4 ...
```

:(

```
1 [root@fdi ~]# dmesg -T | tail -n1  
2 [Fri Aug  9 05:56:31 2024] Lockdown: kexec: kexec of unsigned images is restricted; see man  
    kernel_lockdown.7
```

Provisioning with Foreman - Foreman Discovery Image & kexec

Why?

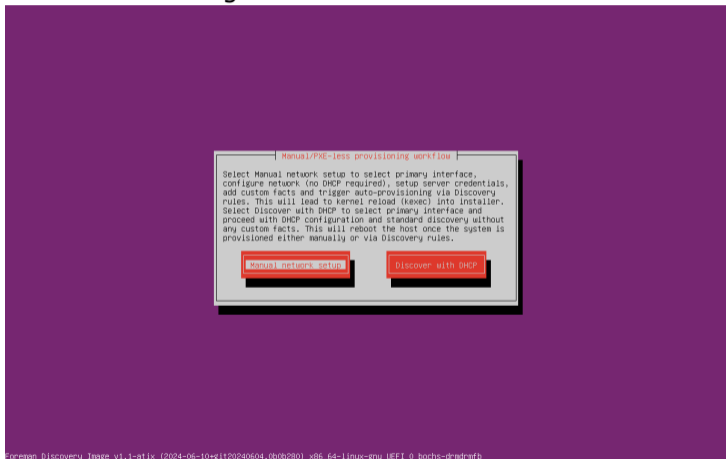
```
1 [root@fdi ~]# mokutil --sb
2 SecureBoot enabled
3 [root@fdi ~]# mokutil --list-enrolled | grep Issuer
4     Issuer: CN=CentOS Secure Boot CA 2/emailAddress=security@centos.org
```

```
1 xps:~ # pesign -S -i /tmp/almalinux8-mirror-tb70qghGi6RT-vmlinuz | grep name
2 The signer's common name is AlmaLinux OS Foundation
```

Somehow expected.

Workaround Foreman Discovery Image & kexec

Build your own FDI based on target OS!

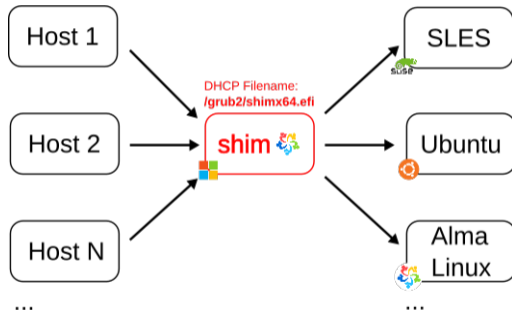


Workaround Foreman Discovery Image & kexec

- ▶ Build FDI based on target OS/distribution
- ▶ We did it for Ubuntu Focal with KIWI (appliance builder)
- ▶ Downsides
 - ▶ We are committed to Ubuntu only per subnet (when FDI is booted via network)
 - ▶ Additional maintenance effort (especially with multiple OSs)
- ▶ Building an ISO and make it running needs some effort at the beginning

The Better Solution - Host Specific Network Boot Files

The problem:



The Better Solution - Host Specific Network Boot Files

Host Salt States Ansible Roles **Operating System** Interfaces Puppet ENC Parameters Additional Information

Architecture *

Operating system *

Build Mode Enable this host for provisioning

Media Selection Synced Content All Media
Select the installation media that will be used to provision this host. Choose "Synced Content" for Synced Kickstart Repositories or "All Media" for other media.

Media *

Synced Content

Partition Table *

PXE loader

Custom Partition Table

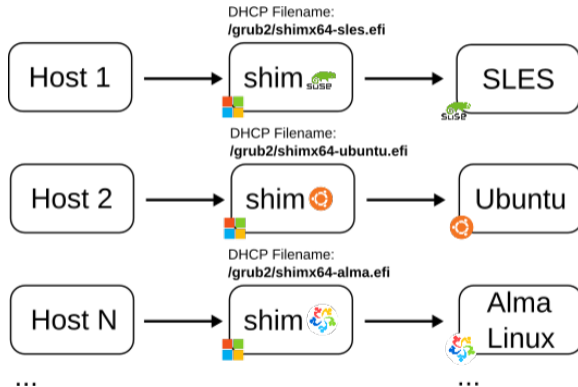
What ever text(or ERB template) you use in here, would be used as your OS disk layout options if you want to use the partition table option, delete all of the text from this field

Root Password * Password must be 8 characters or more.

Provisioning Templates
Display the templates that will be used to provision this host

The Better Solution - Host Specific Network Boot Files

The idea:



The Better Solution - Host Specific Network Boot Files

- ▶ What do we know at the time of host creation?
 - ▶ The target OS & version
 - ▶ SecureBoot state (PXE loader)
 - ▶ The host's MAC address (= host specific identifier)

The Better Solution - Host Specific Network Boot Files

- ▶ What do we need?
 - ▶ OS specific boot files (shim+GRUB2 EFI binaries)
 - ▶ File structure on TFTP server providing host specific boot files (shim+GRUB2 EFI binaries)
 - ▶ DHCP filename option considering host specific values

The Better Solution - Host Specific Network Boot Files

The bootloader universe directory:

```
1 [root@foreman tftboot]# tree bootloader-universe/
2 bootloader-universe/
3 |-- pxegrub2
4 |   |-- sles
5 |     |-- default
6 |       |-- x86_64
7 |         |-- boot.efi -> grubx64.efi
8 |         |-- boot-sp.efi -> shimx64.efi
9 |         |-- grubx64.efi
10 |         |-- shimx64.efi
11 |   |-- ubuntu
12 |     |-- 20.04
13 |       |-- x86_64
14 |         |-- boot.efi -> grub.efi
15 |         |-- boot-sp.efi -> shim.efi
16 |         |-- grub.efi
17 |         |-- shim.efi
18 |     |-- default
19 |       |-- x86_64
20 |         |-- boot.efi -> grubx64.efi
21 |         |-- boot-sp.efi -> shimx64.efi
22 |         |-- grubx64.efi
23 |         |-- shimx64.efi
```

The Better Solution - Host Specific Network Boot Files

TFTP file structure:

```
1 [root@foreman ~]# tree /var/lib/tftpboot/host-config/00-50-56-b4-ee-9b
2 /var/lib/tftpboot/host-config/00-50-56-b4-ee-9b/
3 |-- grub2
4 |   |-- boot.efi -> ../../../../bootloader-universe/pxegrub2/ubuntu/default/x86_64/grubx64.efi
5 |   |-- boot-sb.efi -> ../../../../bootloader-universe/pxegrub2/ubuntu/default/x86_64/shimx64.efi
6 |   |-- boot-sb.efi
7 |   |-- grub.cfg
8 |   |-- grub.cfg-00:50:56:b4:ee:9b
9 |   |-- grub.cfg-00-50-56-b4-ee-9b
10 |   |-- grubx64.efi -> ../../../../bootloader-universe/pxegrub2/ubuntu/default/x86_64/grubx64.efi
11 |   |-- os_info
12 |   |-- shimx64.efi -> ../../../../bootloader-universe/pxegrub2/ubuntu/default/x86_64/shimx64.efi
```

The Better Solution - Host Specific Network Boot Files

DHCP filename option:

```
1  ...
2  host suselinux.foreman.test {
3      dynamic;
4      hardware ethernet 00:50:56:b4:ee:9b;
5      fixed-address 192.168.145.118;
6          supersede server.filename = "/host-config/00-50-56-b4-ee-9b/grub2/boot-sp.efi";
7          supersede server.next-server = c0:a8:91:0a;
8          supersede host-name = "suselinux.foreman.test";
9  }
10 host ubuntu.foreman.test {
11     dynamic;
12     hardware ethernet 00:50:56:f4:ae:97;
13     fixed-address 192.168.145.116;
14         supersede server.filename = "/host-config/00-50-56-f4-ae-97/grub2/boot-sp.efi";
15         supersede server.next-server = c0:a8:91:0a;
16         supersede host-name = "ubuntu.foreman.test";
17 }
18 ...
```

The Better Solution - Host Specific Network Boot Files

Considerations:

- ▶ Keep compatibility
- ▶ Must also work with absent bootloader universe directory
- ▶ Revoked and expired certificates
- ▶ Chainloading
 - ▶ Workflow: always boot from network, chainload local bootloader from disk if not in provisioning mode

Conditions:

- ▶ Foreman must orchestrate the DHCP server

Development & Status

- ▶ How it started: Provide own shim containing certificates of all major OS vendors?
 - ▶ Too much maintenance effort (OS vendor key changes, shim updates, etc.)
 - ▶ Would probably not have been signed
- ▶ First RFC on March 2023 in the Foreman community
- ▶ PRs are open:
 - ▶ Code changes & documentation
 - ▶ Waiting for the finishing touches and testing
 - ▶ Many thanks to Markus Reisner (ATIX Engineering)
- ▶ Bootloader universe directory must currently be created and filled by yourself

Findings:

- ▶ Every OS vendor patches shim & GRUB2 differently

Status & Outlook

- ▶ We are on a good way to get it merged upstream in Foreman
 - ▶ Already available downstream in orcharhino v6.9 (release in June 2024)
- ▶ Some discussions are still ongoing regarding chainloading
 - ▶ Use boot order?
 - ▶ Preferred: Load GRUB2 binary over network, load local GRUB2 configuration from disk, boot?
- ▶ Bundle OS specific boot files and provide them in a proper way ("nboci" project)

Status & Outlook

← Repositories ↑ Organization foreman / nboci-files

Repository Tags

Compact Expanded Show Signatures

1 - 3 of 3 Filter Tags...

TAG	LAST MODIFIED ↓	SECURITY SCAN	SIZE	EXPIRES	MANIFEST
<input type="checkbox"/> fedora-40	14 days ago	See Child Manifests	N/A	Never	SHA256 532b4948867a
<input type="checkbox"/> fedora-40-arm64	14 days ago	See Child Manifests	N/A	Never	SHA256 6e3c1946cd32
<input type="checkbox"/> fedora-40-amd64	14 days ago	See Child Manifests	N/A	Never	SHA256 48a342af8853

```
1 $ nboci pull quay.io/foreman/nboci-files/fedora
2 $ tree fedora
3 fedora
4 `-- 40
5     |-- x86_64
6         |-- grubx64.efi
7         |-- initrd.img
8         |-- install.img
9         |-- pxelinux.0
10        |-- shim.efi
11       ...
```


Excursus - Do I Still Have Sovereignty Over My System?

There is a way:

- ▶ Boot system in Setup Mode
- ▶ Create own key pairs
- ▶ Enroll own PK, KEK, db, dbx certificates
- ▶ Bundle kernel+initrd, add EFI stub, and sign it with own key
- ▶ Works standalone or with systemd-boot bootloader

Software:

- ▶ sbctl - Secure Boot Manager
- ▶ systemd-ukify - Combine kernel and initrd into a signed Unified Kernel Image

Q&A

Questions?

You Have Made It!

Thank you.

Sources & Links

<https://arstechnica.com/security/2024/07/secure-boot-is-completely-compromised-on-200-models-from-5-big-device-makers/>
<https://www.heise.de/news/UEFI-Schwachstelle-LogoFAIL-Secure-Boot-mit-manipulierten-Bootlogos-umgehbar-9547013.html>
https://support.lenovo.com/de/en/product_security/ps500067
https://www.reddit.com/r/MSI_Gaming/comments/10g9v3m/msi_statement_on_secure_boot/
<https://www.heise.de/news/BootHole-Bugs-im-Bootloader-Grub-gefaehrden-Linux-und-Windows-4859293.html>
<https://github.com/rhboot/shim-review>
<https://theforeman.org/>
<https://osinside.github.io/kiwi/>
<https://github.com/ATIX-AG/foreman-discovery-image-kiwi>
https://wiki.archlinux.org/title/Unified_Extensible_Firmware_Interface/Secure_Boot
<https://quay.io/repository/foreman/nboci-files?tab=tags>
<https://github.com/osbuild/nboci>
<https://github.com/Foxboron/sbctl>
https://wiki.archlinux.org/title/Unified_kernel_image#ukify

Development:

<https://community.theforeman.org/t/add-secureboot-support-for-arbitrary-distributions/32601>
<https://community.theforeman.org/t/rfc-distribution-of-netboot-files-via-oci-registry/36791>
<https://github.com/theforeman/foreman-documentation/pull/2145>
<https://github.com/theforeman/foreman/pull/9864>
<https://github.com/theforeman/foreman/pull/10207>
<https://github.com/theforeman/smart-proxy/pull/877>