LynxSecure 6.3.0 Release Notes

LynxSecure Release 6.3.0-rev16326

Product names, screen captures, and other related information listed in LynxSecure® product documentation are copyright materials or trademarks, as recorded, of the respective manufacturers and are included for attribution purposes.

U.S. Patents 9,390,267; 8,745,745; 9,218,489; 9,129,123; 8,782,365; 9,208,030; 9,213,840.

Printed in the United States of America.

Contents

List of Tables

CHAPTER 1 *Overview*

Introduction

These release notes provide information about the following:

- What's new
- Features provided
- Supported Hardware
- Supported Guest OSes
- Known Issues

What's new in 6.3.0

LynxSecure® 6.3.0 is a limited release covering a reduced set of target hardware and guest operating systems (see section “Verified Guest OSes” (page 5) and section “Reference Target Platforms Supported by LynxSecure” (page 5)). LynxSecure 6.3.0 includes the following changes relative to 6.2.0:

Separation Kernel Hypervisor

- Added support for Cache Allocation Technology (CAT) on supported Intel® processors. LynxSecure now supports configuring the cache capacity bitmask for the virtual CPUs assigned to subjects. See Chapter 4, “*XML Reference*” in *LynxSecure 6.3.0 Advanced Configuration Guide* for details.
- Added support for Resource Director Technology (RDT), including Memory Bandwidth Monitoring (MBM), on supported Intel processors. See the description of `rdt.monitor` in Chapter 7, “*Subjects*” in *LynxSecure 6.3.0 Getting Started and Configuration Guide* for details.
- Added virtualization of the Performance Monitor Unit (PMU) on supported Armv8-A® processors. Virtual machines running on Armv8-A processors with PMU support can now access the PMU to gather performance metrics at run time. No configuration changes are necessary to make use of this feature.

Buildroot Linux

- The Buildroot Linux framework has been upgraded to the 2019.02 release.
- Added support for legacy serial ports with non-standard IRQs.
- Added support for "jitterentropy" in the stock Virtual Device Server image to ensure that the boot sequence does not hang on systems without other entropy sources.

What's new in 6.2.0

LynxSecure 6.2.0 is a limited release covering a reduced set of target hardware and guest operating systems (see section “Verified Guest OSes” (page 5) and section “Reference Target Platforms Supported by LynxSecure” (page 5)). LynxSecure 6.2.0 includes the following changes relative to 6.1.2:

LynxSecure Tools

- Fixed a bug in CREATE_PROJECT that prevented the default path from including the product version on which the project is based.

Virtual Device Server

- Fix a bug that prevented static IP address assignment for VDS interfaces that are part of a bridged configuration.
- Fix a bug that prevented bridged network configurations from passing traffic through the bridge when one of the subjects assigned an interface on the bridge is stopped.

What's new in 6.1.2

LynxSecure 6.1.2 includes the following changes relative to 6.1.1:

Runtime Initialization Function

- Fixed the invalid memory maps created by RIF for SR-IOV devices regardless of whether SR-IOV is "enabled" by the firmware.

Fully Virtualized Subject

- Ignore the JUMP option AP CPUs for non-LSA’s on x86 and AP CPUs on Arm® and go into ap_start_default because the x86 FV LSAs expect to start in protected mode. In Arm, with virtual PSCI startup method, it is not possible for that domain loader to continue the startup sequence on the secondary CPUs, because the information captured by the virtual PSCI (such as the entry point location) is destroyed by FVS before jumping into the subject.
- Improved serial port configuration in RIF on Arm by adding "rif_serial=none".

Virtual Device Server

- PV linuxes with directly assigned network cards now correctly recognize static IP address configuration option.

What's new in 6.1.1

LynxSecure 6.1.1 includes the following changes relative to 6.1.0:

Separation Kernel Hypervisor

- Added support for targets with a PCI device that advertise an MSI-X capability referencing a nonexistent BAR. Such devices will have their MSI-X capability disabled. This change is only applicable to Intel targets.

- LynxSecure now correctly interprets the 'ranges' property when this property contains more than one (child-bus-addr, parent-bus-addr, size) tuple. Previously, tuples after the first tuple were incorrectly interpreted to contain the host physical address without any translation. This change is only applicable to Arm targets.

Autoconfig

- It is now possible to create a virtual FIFO device with one or both of the FIFO endpoints in a paravirtualized LynxOS®-178 subject. Previously, the autoconfig tool would reject such a configuration even if the version of LynxOS-178 used included a supported FIFO driver. This change is only applicable to Intel targets (Arm targets use fully virtualized versions of LynxOS-178 and were not subject to the same check by autoconfig).

Miscellaneous

- It is now possible to provide access to the boot memory region for another subject to an LSA-based subject. Previously, adding a memory flow to another subject's boot region would cause the LSA-based subject to have an unhandled exception during subject boot.

What's new in 6.1.0

LynxSecure 6.1.0 includes the following changes relative to 6.0.1:

Separation Kernel Hypervisor

- Add support for Intel targets. This release brings support for Intel targets to LynxSecure 6.x, and replaces LynxSecure 5.3.x as the current supported version of LynxSecure on Intel targets.

Autoconfig

- Add support for multiple "identitymem" subjects on ARM. This simplifies configurations for multiple subjects that need access to DMA-capable devices on platforms that don't support an SMMU, like the NXP® S32V234™ MPSoC.

Notable changes in 6.1.0 relative to 5.3.x (Intel targets only).

- Re-designed autoconfig command line syntax (See Chapter 4, "*Introduction to the Autoconfig Tool*" in *LynxSecure 6.3.0 Getting Started and Configuration Guide* for details). Note that the syntax of the 5.3 version of the autoconfig command line may be invoked by running the `autoconfig-5.3.x` command.
- Add support for disabling system management interrupts (SMI) on PCH200 and C620 series chipsets.
- Add support for automatically disabling the alternative routing id interpretation (ARI) feature from PCIe bridges and devices. Previously, LynxSecure would fail on an attempt to assign such devices to guests. Now, LynxSecure is able to assign them to subjects with the limitation that the increased number of functions for multi-function devices (e.g., devices supporting SR-IOV) enabled by ARI are not supported by LynxSecure.
- Initial support for SR-IOV. LynxSecure now supports separate assignment of the physical and virtual functions of a PCIe device to different paravirtual Linux subjects. See Chapter 8, "*Physical Device Assignment to Subjects*" in *LynxSecure 6.3.0 Getting Started and Configuration Guide* for details.
- Removed support for targets with CPUs that do not support the Extended Page Table (EPT) second-level address translation feature.

- UEFI virtual firmware support for fully virtualized subjects. In addition to SeaBIOS, fully virtual subjects can use OVMF-based UEFI firmware to load guest operating systems. See the section “FV Subject Autoconfig Syntax” in *LynxSecure 6.3.0 Getting Started and Configuration Guide* for details.
- Support for assigning PCI devices with resources above 4 GiB to fully virtualized subjects.
- Remove the hard-coded limit of 256 interrupt vectors per target.

What's new in 6.0.1

LynxSecure 6.0.1 includes the following changes relative to 6.0.0:

Separation Kernel Hypervisor

- Add support for jumping to a configurable address on a hypervisor panic (either during boot or at run-time). See the `paniccall` description in section “Passing Options to RIF from a Custom Bootstrap Loader” in *LynxSecure 6.3.0 Getting Started and Configuration Guide* for further details.
- Reduce the amount of memory used by the IBIT subject.
- Implement handling of the OSLAR_EL1 register in the virtual platform. This register is used to implement self-hosted debugging, for example, using debuggers like GDB.

Autoconfig

- Improved handling of architecture-specific options.
- Fix a bug in the generation of page table regions when an explicit HCV is requested.

Features

LynxSecure provides the following features:

- Efficient virtualization using Armv8-A and Intel platform features
- Symmetric Multiprocessing
- Direct Device Assignment (See Chapter 4, “*Introduction to the Autoconfig Tool*” in *LynxSecure 6.3.0 Getting Started and Configuration Guide* for details).
- Fully Virtualized Uniprocessor and Symmetric Multiprocessor Subjects
- LynxSecure Application (LSA) fully virtualized 32-bit and 64-bit
- Multiple Scheduling Policies
- Enhanced ARINC-653 Scheduling
- Flexible Scheduling
- Security Extensions and Policy Enforcement
- Inter-subject Communication
- XML Configuration Tool, Auto Configuration Tool
- Audit Capability
- Built in Test (BIT) Module

- Memory Sanitization
- Execute-Disable Bit
- Virtualized Device Support

Development Host Requirements

The following system requirements are recommended for the host development system:

- X86 64-bit machine running CentOS™ 7.3 (1611).
- Standard set of GNU/ Linux® Utilities (the `bash` shell must be used on the cross development host)
- At least 4GB RAM for a disk based installation.
- At least 40GB free disk space for the binary product installation
- At least 256GB free disk space for the source product installation

Verified Guest OSes

The following table shows the list of validated and reference Guest operating systems with LynxSecure 64-bit.

Table 1-1: Verified Guest OSes

Guest OS	Type	Comment
LynxOS-178 2.2.5	32-bit, Intel and Arm	Reference Guest
Buildroot-based Linux	64-bit, Intel	Reference Guest

Reference Target Platforms Supported by LynxSecure

Reference targets have been extensively tested with LynxSecure features. Note that for 6.3.0, this a a reduced set of targets relative to other releases. The following standard systems are supported configurations as reference targets for LynxSecure in this release.:

Server

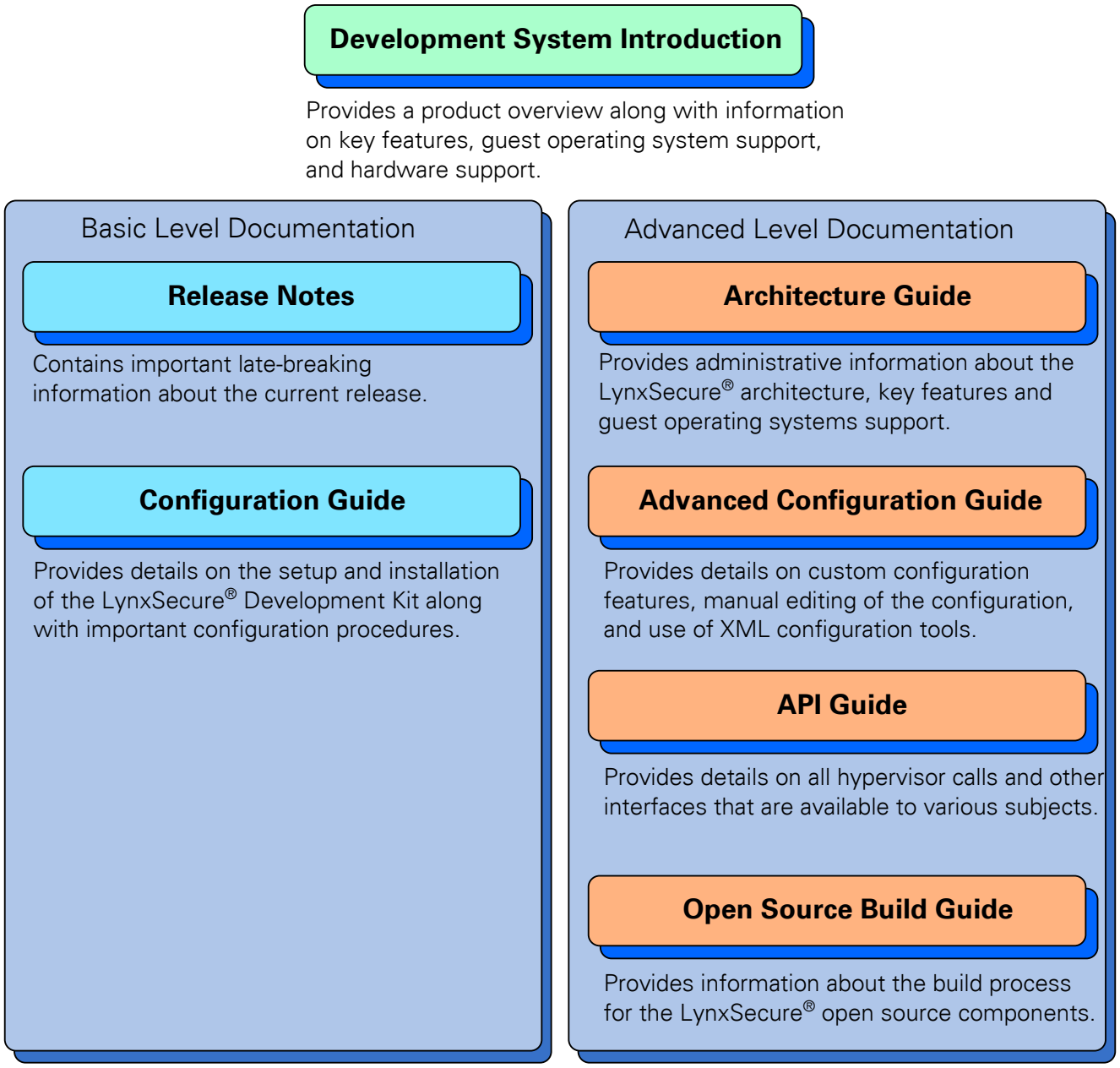
- Supermicro X10SDV-TLN4F
- Supermicro A2SDV-8C-TLN5F

Embedded

- Xilinx® Zynq® Ultrascale+™ MPSoC ZCU102 Evaluation Kit.

For More Information

For more information on the features of LynxSecure, refer to the following printed and online documentation.


Development System Introduction
Provides a product overview along with information on key features, guest operating system support, and hardware support.
Basic Level Documentation
Release Notes
Contains important late-breaking information about the current release.
Configuration Guide
Provides details on the setup and installation of the LynxSecure® Development Kit along with important configuration procedures.
Advanced Level Documentation
Architecture Guide
Provides administrative information about the LynxSecure® architecture, key features and guest operating systems support.
Advanced Configuration Guide
Provides details on custom configuration features, manual editing of the configuration, and use of XML configuration tools.
API Guide
Provides details on all hypervisor calls and other interfaces that are available to various subjects.
Open Source Build Guide
Provides information about the build process for the LynxSecure® open source components.

CHAPTER 2 Known Issues

This chapter describes the known issues for this release.

BIOS/Hardware

Supermicro A2SDV

- Assigning the ACPI resources to VDS is not supported on this target.

Supermicro X10SAE

- This target will not successfully boot autoconfig images from a USB stick in UEFI mode created using the following command: `dd if= $ENV_PREFIX /autoconfig/autoconfig.iso of=/dev/sdX`. To boot autoconfig from USB, please use `$ENV_PREFIX/bin/create-superstick.sh /dev/sdX` instead, where /dev/sdX is the block device node for your USB device.

Dell Inspiron, Supermicro X10SAE

- LynxSecure® may hang during the boot time, this is most likely caused by a bug in the host's System Management Mode (SMM) BIOS. As a workaround, use `--smidisable` option in the Autoconfig command line while generating SRP

X-ES XPedite 7674

- LynxSecure is unable to discover the ACPI RSDP table at boot time on this target. To work around this issue, specify the RSDP table address using the 'uefi_acpi_rsdp=' RIF option. The correct address can be determined by examining the kernel log within the Hardware Discovery Linux®:

```
# dmesg | grep "RSDP"
[0.000000] ACPI: RSDP 0x00000000C9E17000 000024 (v02 ALASKA)
```

Xilinx Zynq Ultrascale+ MPSoC

- When using dma-capable devices with Linux, DMA bus errors like the following may occur:

  ```
  [ 5.831314] macb ff0e0000.ethernet eth0: DMA bus error: HRESP not OK
  ```

  A fix for this issue is planned for a future release. Please contact Lynx Software Technologies, Inc. technical support for details on this issue.
- When booting a Linux guest using execute in place segmented boot, the default autoconfig strategy for RAM allocation may cause there to be no suitable location for the virtual FDT. A fix for this issue is planned for a future release. Please contact Lynx Software Technologies, Inc. technical support for a work-around for this issue.

LynxSecure

Hardware Discovery

- The Hardware Discovery Linux does not correctly record resources for Trusted Platform Modules (TPM). This makes it impossible to assign a TPM to a subject, such as when using LSA.store full disk encryption. A fix for this issue is planned for a future release of LynxSecure.

Buildroot Linux

- The driver for the LynxSecure virtual FIFO does not load successfully on fully virtualized Linux guests running on Intel® targets. A fix for this issue is planned for a future release.

Virtual Platform

- When running LynxOS®-178, it may not be possible to successfully assign the maximum supported 2 gigabytes of RAM to the LynxOS-178 subject. The limit will be lower when directly assigning PCIe devices to the LynxOS-178 subject on targets that have large PCI address windows, as both RAM and PCI address space must fit into a single 32-bit guest physical address space. If you encounter this issue, LynxSecure will fail to boot and a message similar to the following will be displayed on the configured diagnostic console:

  ```
  LS<2> ptbl_map_page: host physical address 0x100000000 is out of the page table range (pt type 2009)
  LS<0> vcpu_vmmu_initial_ptbl_map_range: subject `pvlos178_1': mapping addr 0x7bb04000, size 0x44fc0)
  LynxSecure stops.
  ```

- The Hardware Discovery Linux may fail to boot as a fully virtualized subject on some targets. A fix for this issue is planned for a future release of LynxSecure.
- The option ROM provided for use with emulated e1000 network card in fully virtualized subjects may not successfully boot over the network in some circumstances. A fix for this issue is planned for a future release of LynxSecure.
- Some NVIDIA® graphics cards do not operate correctly when directly assigned to a Windows® 10 guest. This issue does not affect Linux guests using the NVIDIA driver.
- Booting from XHCI-based USB controllers is not supported when using SeaBIOS. A fix for this issue is planned for a future release of LynxSecure.
- 32-bit Linux guests may fail to boot in fully virtualized guests on Intel targets. No work-around is currently available. A fix for this issue is planned for a future release of LynxSecure.
- Virtual network configurations involving multiple virtual Ethernet bridges result in an invalid VDS network configuration. As a work-around, you must rebuild the virtual device server with a manually created network configuration script. Please contact Lynx Software Technologies, Inc. technical support for details.
- Video camera devices may not function when assigned to guests using the virtual USB stack. No work-around is currently available.
- USB devices assigned to subjects using the virtual USB stack may fail to enumerate on Windows guests when the guest is rebooted. No workaround is currently available.
- When directly assigning a PS2 keyboard or mouse to a FV subject, both the keyboard and mouse must be assigned together to the same subject.
- When Ubuntu-18.04 is used as Guest, it is recommended to assign a minimum of 2GB ram.
- It's not possible to configure persistent storage partition for the Virtual Device Server. A fix for this issue is planned for a future release of LynxSecure.
- On UEFI targets that do not include a compatibility support module (CSM), LynxSecure cannot automatically discover the location of the ACPI RSDP table. See RSDP note for the X-ES XPedite 7674 (page 7).