SKYBOX APPLIANCE

RELEASE NOTES

11.3.100

CentOS Linux release 7.9.2009 (Core)

CONTENTS

Introduction 4

New Features 5

- Skybox Virtual Appliance Installation on Microsoft Hyper-V 5
- Changes to Skybox Appliance Interactive Installation 5
- Installation Option for Skybox Standalone Elasticsearch Node 7

Known Limitations 8

Support Issues Fixed in this ISO 9

Fixed Vulnerabilities 10

Chapter 1

INTRODUCTION

This document includes information about Skybox Appliance version 11.3.105-7.1.300, including new features, known limitations, support issues fixed in this ISO, and fixed vulnerabilities.

Unless otherwise noted, the information in this document is relevant to all Skybox Appliances, including virtual Appliances.

Chapter 2

NEW FEATURES

Version 11.3.105-7.1.300 includes the following feature enhancements:

- Skybox Virtual Appliance Installation on Microsoft Hyper-V
- Changes to Skybox Appliance Interactive Installation
- Installation Option for Skybox Standalone Elasticsearch Node

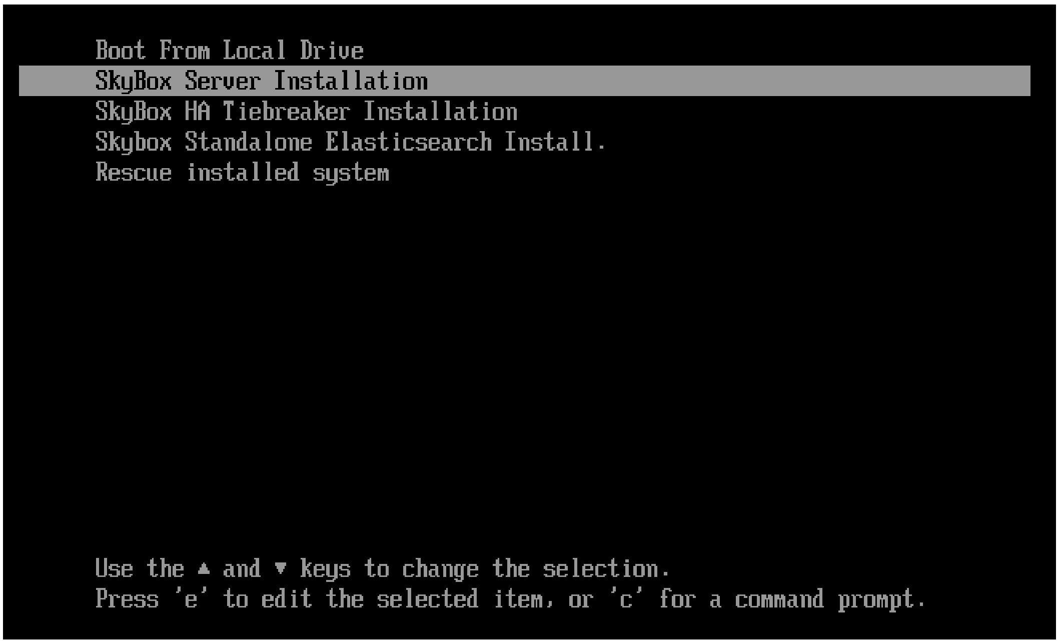
Skybox Virtual Appliance Installation on Microsoft Hyper-V

Microsoft Hyper-V is now supported as a hypervisor for Skybox Virtual Appliance, in addition to VMWare ESX.

Installation instructions for Hyper-V were added to the Skybox Virtual Appliance Quick Start Guide.

Changes to Skybox Appliance Interactive Installation

The following are the options now available in the boot menu of the Appliance ISO.



```
      Boot From Local Drive
      SkyBox Server Installation
      SkyBox HA Tiebreaker Installation
      Skybox Standalone Elasticsearch Install.
      Rescue installed system









      Use the ▲ and ▼ keys to change the selection.
      Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Boot From Local Drive

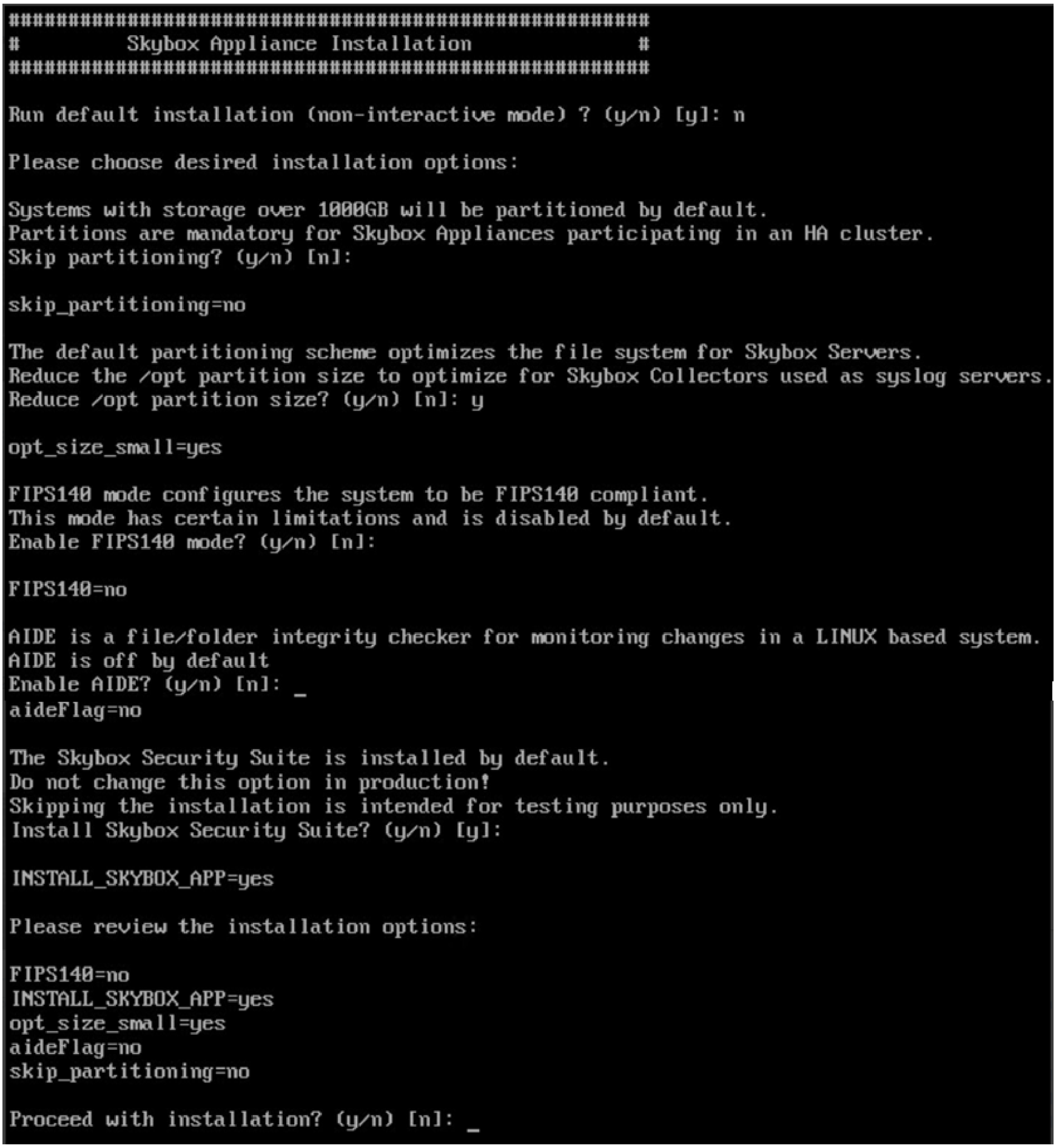
Without user intervention, after several seconds the Appliance will Boot From Local Drive. Click the up or down arrow keys to stop the countdown before the boot runs.

Skybox Server Installation

As in previous versions, to install an Appliance to be used as a Skybox Server or Skybox Collector, select **Skybox Server Installation**.

The installation dialog appears, asking whether you want to run the default installation. It allows 60 seconds for user response.

- If the response is **Yes**, or if no response is provided within 60 seconds, the default installation commences, which installs the Appliance as a Skybox Server, including a local Collector.
- If the response is **No**, the following dialog explains the various installation options and allows the user to change the default values.



```
#####################################################
#         Skybox Appliance Installation             #
#####################################################

Run default installation (non-interactive mode) ? (y/n) [y]: n

Please choose desired installation options:

Systems with storage over 1000GB will be partitioned by default.
Partitions are mandatory for Skybox Appliances participating in an HA cluster.
Skip partitioning? (y/n) [n]:

skip_partitioning=no

The default partitioning scheme optimizes the file system for Skybox Servers.
Reduce the /opt partition size to optimize for Skybox Collectors used as syslog servers.
Reduce /opt partition size? (y/n) [n]: y

opt_size_small=yes

FIPS140 mode configures the system to be FIPS140 compliant.
This mode has certain limitations and is disabled by default.
Enable FIPS140 mode? (y/n) [n]:

FIPS140=no

AIDE is a file/folder integrity checker for monitoring changes in a LINUX based system.
AIDE is off by default
Enable AIDE? (y/n) [n]: _
aideFlag=no

The Skybox Security Suite is installed by default.
Do not change this option in production!
Skipping the installation is intended for testing purposes only.
Install Skybox Security Suite? (y/n) [y]:

INSTALL_SKYBOX_APP=yes

Please review the installation options:

FIPS140=no
INSTALL_SKYBOX_APP=yes
opt_size_small=yes
aideFlag=no
skip_partitioning=no

Proceed with installation? (y/n) [n]: _
```

Most of these options were available in previous releases (with slightly different wording).

Reduce the /opt partition size

The **Reduce the /opt partition size** option is new. This option is used to optimize the partitioning scheme for Appliances intended to run only the Skybox Collector and to be used as Syslog-ng servers, which typically require a lot of space under /var for storing syslog records.

On systems with storage greater than 1000 GB, enabling this option sets the /opt partition size to 100 GB and allocates most of the storage to the /var partition.

Important: This reduced size /opt partition is not adequate and should not be used for an Appliance intended to run the Skybox Server.

Installation Option for Skybox Standalone Elasticsearch Node

In the boot menu of the Appliance ISO (see Changes to Skybox Appliance Interactive Installation), there is a new installation option for the Skybox standalone Elasticsearch node.

Standalone Elasticsearch nodes can be used to enhance the scalability of the new, Elasticsearch-based Skybox Web Client.

Choosing this option in the boot menu skips the interactive installation dialog and selects the following options:

- No partitioning
- No AIDE
- No FIPS140 compliance
- Install the Skybox Server in Standalone Elasticsearch mode

A standalone Elasticsearch node must be connected to the master Skybox Server node, as described in *Skybox Standalone Elasticsearch Server*.

If you are using a 3-node cluster, all 3 nodes must be must be connected to the master Skybox Server node.

The Skybox version included with this ISO, 11.3.105, has a known issue related to the installation of the server in standalone Elasticsearch mode.

To work around this issue, after the ISO installation is completed and before connecting the node to the master Skybox Server node, perform the following steps :

1. Log in as user `skyboxview`
2. Edit the file `/opt/skyboxview/server/conf/servertype.properties`
3. Replace `servertype=master` with `servertype=elasticsearch`
4. Restart the server service: `service sbvserver restart`

Chapter 3

KNOWN LIMITATIONS

- Skybox Appliance is not supported on IPv6-only networks; it requires an IPv4 address.
- Host names that include underscores should not be used.

  Due to the updated RFC 3986, which claims that underscores are unsafe in virtual host server names, Apache does not allow virtual host names with underscores.

  Workaround: Change the underscores "_" to hyphens "-" in the host names ("host-name" instead of "host_name").

Chapter 4

SUPPORT ISSUES FIXED IN THIS ISO

The following support issues are fixed in this ISO (11.3.105-7.1.300).

Issue key	CRM IDs	Summary
AP-748	107440	syslog-ng filter should include WEB_API pattern
AP-743	108229	Security Vulnerability found Apache Subversion Client version 1.7.14
AP-739	107768	CentOS logs

Chapter 5

FIXED VULNERABILITIES

The vulnerabilities in the following table, found in version 11.1.452-7.2.245, were fixed for version 11.3.105-7.1.300.

SBV-ID	CVE	Exploit Status	Severity	Description
SBV-125558	CVE-2020-12321	No Exploit	Critical	Intel Wireless Bluetooth Remote Privilege Escalation Vulnerability - CVE-2020-12321
SBV-128473	CVE-2021-3156	Exploit Available	High	Sudo Local Code Execution Vulnerability via Backslash in Sudoers - CVE-2021-3156
SBV-118352	CVE-2020-10878	No Exploit	High	Perl <5.30.3 Remote DoS Vulnerability - CVE-2020-10878
SBV-118356	CVE-2020-10543	No Exploit	High	Perl <5.30.3 Remote Unspecified Vulnerability - CVE-2020-10543
SBV-121613	CVE-2020-15862	No Exploit	High	Net-SNMP Local Privilege Escalation Vulnerability - CVE-2020-15862
SBV-126186	CVE-2020-14360	No Exploit	High	X.Org Server Local Privilege Escalation Vulnerability - CVE-2020-14360
SBV-126187	CVE-2020-25712	No Exploit	High	X.Org Server Local Privilege Escalation Vulnerability - CVE-2020-25712
SBV-118355	CVE-2020-12723	No Exploit	High	Perl <5.30.3 Remote DoS Vulnerability in regcomp.c - CVE-2020-12723
SBV-126233	CVE-2020-29573	No Exploit	High	GNU GLibC <2.23 Remote DoS Vulnerability via Long Double Inputs to Printf - CVE-2020-29573
SBV-123501	CVE-2020-25643	No Exploit	High	Linux Kernel Remote DoS or Other Vulnerability in HDLC_PPP - CVE-2020-25643
SBV-124660	CVE-2020-25654	No Exploit	High	Pacemaker Remote Restrictions Bypass Vulnerability - CVE-2020-25654
SBV-121795	CVE-2020-24394	No Exploit	High	Linux Kernel <5.7.8 Local

SBV-ID	CVE	Exploit Status	Severity	Description
				Restrictions Bypass Vulnerability - CVE-2020-24394
SBV-122425	CVE-2020-25212	No Exploit	High	Linux Kernel <5.8.3 Local Memory Corruption Vulnerability - CVE-2020-25212
SBV-127386	CVE-2019-25013	No Exploit	Medium	GNU GLibC Remote Buffer Over-Read Vulnerability - CVE-2019-25013
SBV-122049	CVE-2020-14385	No Exploit	Medium	Linux Kernel Local DoS Vulnerability - CVE-2020-14385
SBV-119133	CVE-2020-10769	No Exploit	Medium	Linux Kernel Local Buffer Over-Read Vulnerability in crypto/authenc.c - CVE-2020-10769
SBV-119508	CVE-2020-14314	No Exploit	Medium	Linux Kernel Local DoS Vulnerability in namei.c - CVE-2020-14314
SBV-113997	CVE-2020-10029	No Exploit	Medium	GNU glibc <2.32 Local DoS Vulnerability - CVE-2020-10029
SBV-120744	CVE-2020-14347	No Exploit	Medium	X.org Xserver Local ASLR bypass Vulnerability - CVE-2020-14347
SBV-112382	CVE-2019-18282	No Exploit	Medium	Linux Kernel Remote Information Disclosure Vulnerability - CVE-2019-18282
SBV-126481	CVE-2020-1971	No Exploit	Medium	OpenSSL Remote DoS Vulnerability - CVE-2020-197