What is new in Balabit Shell Control Box 4 F2

January 15, 2016

Table of Contents

1. Preface

Welcome to Balabit Shell Control Box (SCB) version 4 F2 and thank you for choosing our product. This document describes the new features and most important changes since the latest release of SCB. The main aim of this paper is to aid system administrators in planning the migration to the new version of SCB. The following simplesects describe the news and highlights of SCB 4 F2.

This document covers the Balabit Shell Control Box 4 F2 and Audit Player 2015.2 products.

1.1. Versions and releases of SCB

As of June 2011, the following release policy applies to Balabit Shell Control Box:

- *Long Term Supported or LTS releases* (for example, SCB 4 LTS) are supported for 3 years after their original publication date and for 1 year after the next LTS release is published (whichever date is later). The second digit of the revisions of such releases is 0 (for example, SCB 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SCB 4 F1) are supported for 6 months after their original publication date and for 2 months after succeeding Feature or LTS Release is published (whichever date is later). Feature releases contain enhancements and new features, presumably 1-3 new feature per release. Only the last feature release is supported (for example when a new feature release comes out, the last one becomes unsupported within two months).

For a full description on stable and feature releases, see *Stable and feature releases*.

Warning
Downgrading from a feature release is not supported. If you upgrade from an LTS release (for example, 4.0) to a feature release (4.1), you have to keep upgrading with each new feature release until the next LTS version (in this case, 5.0) is published.

IPv6 support for the audited traffic

SCB now supports the auditing of IPv6 environments. You can audit IPv4 clients accessing IPv6 servers, IPv6 clients accessing IPv4 servers, and naturally, IPv6 clients accessing IPv6 servers. You can also use IPv6 addresses with inband destination selection.

SCB in Azure Cloud

You can deploy SCB as a virtual machine in the Microsoft Azure cloud computing platform. This allows you to conveniently audit access to your entire virtualized infrastructure.

Scaling audit trail processing

If SCB audits lots of connections, processing and indexing the created audit trails requires significant computing resources, which may not be available in the SCB appliance. To decrease the load on the SCB appliance, you can install the indexer service on external Linux hosts. These external indexer hosts run the same indexer service as the SCB appliance, and can index audit trails, or generate screenshots and replayable video files from the audit trails as needed. The external indexers register on SCB, wait for SCB to send an audit trail to process,

process the audit trail, then return the processed data to SCB. The external indexer hosts do not store any data, thus any sensitive data is available on the host while it is being processed.

Integration with Blindspotter

SCB now supports the operation of Blindspotter, the real-time user behavior analytics solution of Balabit. Blindspotter is a monitoring tool that maps and profiles user behavior to reveal human risk, and can analyze user behavior using the data from the audit trails recorded by SCB. *Learn more about SCB*

Configuring SCB using a REST API

To make integrating SCB into various management systems possible, you can now access SCB using a RESTful API. Currently the API supports only the parts of the configuration that are changed most often at large enterprises, namely Channel policies.

Other features will be available via the REST API in future releases.

For details, see *Using the Balabit Shell Control Box REST API*.

Authentication improvements in HTTP

SCB now supports the following inband authentication methods for the HTTP protocol: Basic Access Authentication (according to *RFC2617*), and the NTLM authentication method commonly used by Microsoft browsers, proxies, and servers. This allows SCB to identify HTTP sessions better, and also makes it possible to match authorized sessions to real users.

Furthermore, for authenticated sessions, SCB can perform group-based user authorization that allows you to finetune access to your servers and services: you can now set the required group membership in the Channel policy of the HTTP connection.

Network Level Authentication in RDP without domain membership

There are scenarios when you want to use SCB to monitor RDP access to servers that accept only Network Level Authentication (NLA, also called CredSSP), but SCB is not a member of the same domain (or of a trusted domain) as the RDP server. For example, you cannot add SCB to that domain for some reason, or the RDP server is a standalone server that is not part of a domain. Now SCB support such scenarios as well.

Windows 10 support and new client applications

SCB now supports the Remote Desktop client of Windows 10.

In addition, the Royal TSX client application running on OS X, and the WinFIOL SSH client are also supported.

Updated browser support

The SCB web interface supports the following new browsers.

- The current versions of Google Chrome and Mozilla Firefox
- Microsoft Edge

Warning

Since the official *support of Internet Explorer 9 and 10 ends* in January, 2016, they will not be supported in SCB version 4 F3 and later.

Audit Player improvements

Audit Player version 2015.2 handles IPv6 metadata, and Citrix ICA connections that use the H.264 codec.

FSTEK certification

SCB has obtained the Federal Service for Technical and Export Control (FSTEK) certification, which is compulsory for information security products in Russia.

General improvements and changes

- To make sharing easier, the Connection details popup now includes a permalink for the connection.
- Protecting SCB against brute-force attacks has been improved: after five unsuccessful login attempts, SCB denies following attempts for increasing periods of time.
- SCB now sends an `xcbLicenseAlmostExpired` alert 60 days before its license expires, in order to give you more time to renew your license.
- From SCB 4 F2, the MAC address of the interfaces will be different on the HA nodes, which means that during HA failover the MAC address for the configured IP addresses will change and no MAC address will be taken over to the slave node. This change will be propagated in Layer 2 by sending Gratuitous ARP requests, informing every host on that Local network about this change.
- Previous versions of SCB always implicitly assumed the Primary Search Domain (**Basic Settings > Network**) as an Append Domain in Inband Destination Selection settings of Connection policies, even when a custom DNS Server was set up for the connection. This behavior was changed: the Primary Search Domain is only used if no custom DNS Server is set. In order to not break existing configurations, the Primary Search Domain is set as an Append Domain explicitly for all affected policies during upgrade. If this is not the desired behavior for you, remove that additional entry.

Deprecated features

- Sending data to IDS/DLP systems is deprecated and is going to be removed in SCB version 4 F3 and later.
- Support for GSSAPI-based authentication is deprecated and will not be supported in version 4 F3 and later. For recommendations on migrating to a different operating mode, contact the *Balabit Support Team*.

Warning

Since the official *support of Internet Explorer 9 and 10 ends* in January, 2016, they will not be supported in SCB version 4 F3 and later.