BalaBit
syslog-ng Store Box
5 LTS
リリースノート

Rev.2.0

BALABIT

2018.02.09

ジュピターテクノロジー

目次

変更履歴

版	発行日	変更内容
Rev. 1.0	2018/02/09	新規作成

お問合せ先、およびカスタマーポータル

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F
URL：　http://www.jtc-i.co.jp/
電話番号：　042-358-1250
FAX 番号：　042-360-6221

ご購入のお問い合わせ：
- お問い合わせフォーム　https://www.jtc-i.co.jp/contact/scontact.php
- メール　sales@jtc-i.co.jp

製品サポートのお問い合わせ：
- カスタマーポータル　https://www.jtc-i.co.jp/support/customerportal/

評価版のダウンロード：
https://www.jtc-i.co.jp/support/download/

1　新リリースへのアップグレード

これは長期サポートリリース（LTS）で、オリジナルの公開後 3 年間、または、次の LTS リリース後 1 年間のどちらか遅い時期までサポートされます。また、フィーチャーリリース版を使用している場合は、2 か月以内に最新の LTS リリースにアップグレードすることにより、サポートされたリリースを使用し続けることができます。

アップグレードする必要のある方

N1000 や N10000 を使用しておらず（SSB 5 LTS は N1000、N10000 ではサポートされません）、以下の場合、SSB 5 LTS へのアップグレードを推奨します。

- 新機能を利用したい
- フィーチャーリリースを使用している

SSB 5 LTS がサポートしている新ハードウェア（T1/T4/T10）に変更したい場合、弊社まで連絡をお願いいたします。

アップグレードの方法

アップグレードの手順は、syslog-ng Store Box 5 LTS アップグレードガイド を参照してください。

2　SSB 4 F9 からの変更

新しいユーザ インターフェース

ユーザ インターフェースをよりモダンなルック アンド フィールに変更しました。

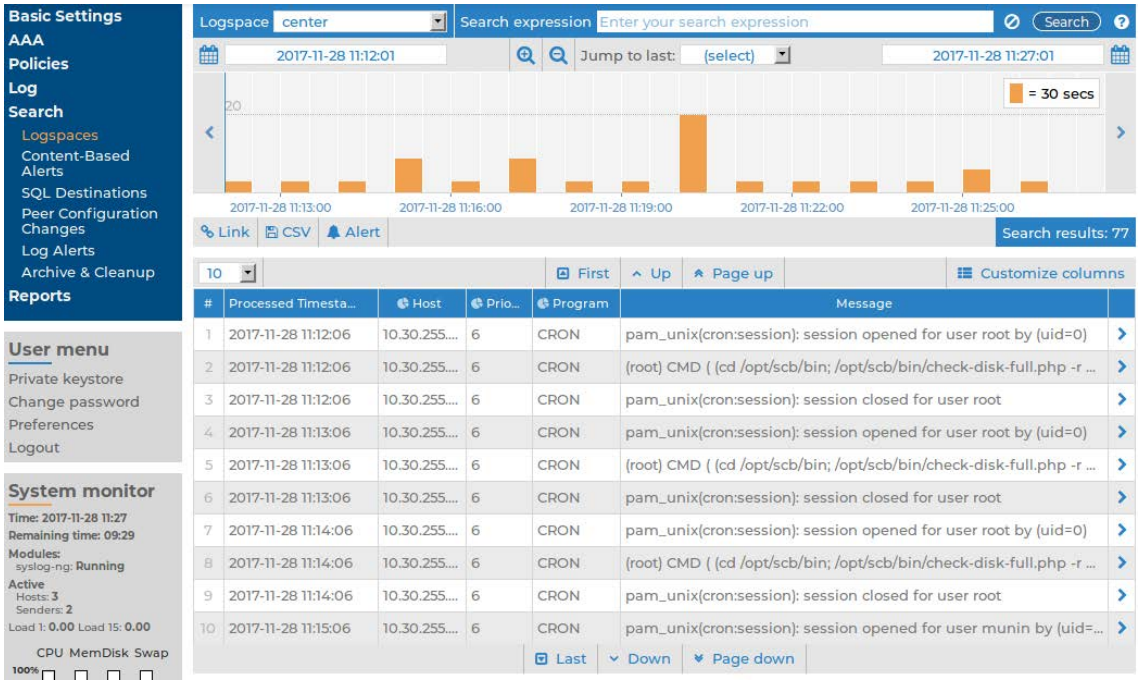

図1.　Search > Logspaces – ログメッセージの検索インターフェース

ログのテキストを検索して置換

受信中のログを検索して文字を置換することができます。詳細は SSB 5 LTS の管理者ガイド「10.5 ログのテキストを検索して置換」を参照してください。

ブラウザのサポート

以下のブラウザをサポートします。他のブラウザや古いバージョンは未サポートです。

Mozilla Firefox 52 ESR

以下のブラウザは未サポートですが、テストしたところ SSB の機能は使えますが、見え方がサポートしているブラウザと異なることがあります。

Internet Explorer 11, Microsoft Edge, 現在リリースされている Mozilla Firefox、Google Chrome.

パスワードのポリシー

ローカルの SSB ユーザのパスワード ポリシーは、admin と root にも適用されます。 詳細は SSB 5 LTS の管理者ガイド 「5.2 ローカルユーザのパスワード設定ポリシー」 を参照してください。

デフォルトのパスワード ポリシーは、admin や root 用として、簡単なパスワードを拒否します。パスワードの入力フィールドで、少なくとも"good"のレベルにする必要があります。

ハイ アベイラビリティのライセンス

SSB は、ハイ アベイラビリティのライセンスを厳密にチェックするようになります。HA 環境でシングル モードのライセンスを使用している場合、5 LTS へアップグレードできません。5 LTS 以降にアップグレードする場合、有効な HA ライセンスの場合のみ HA にコンバートできます。

有効な HA ライセンスを購入する場合、弊社まで連絡をお願いします。

仮想アプライアンスや HA ライセンスがないハードウェア アプライアンスを購入した場合、Basic Settings > High Availability メニューで項目は表示されません。

その他の変更

・最大接続数のデフォルトの値が 10000 に増加しました。

Log > Sources > Maximum connections

3　SSB 4 LTSから 4 F9 までの変更

3.1　仮想化

Microsoft Azure に SSB をデプロイ（展開）

Microsoft Azure に自前のライセンスを使用して SSB をデプロイすることができます。

SSB を Microsoft Azure 上で使用すると、クラウドでアプリケーションを使用する恩恵を受けることができます。もっとも顕著なものは、アプリケーションのキャパシティ・ニーズに対応できる能力です。Azure Linux Virtual Machines は、オンデマンド、ハイ スケール、セキュア、仮想化したインフラを提供しています。Microsoft Azure は、異なる利用ケースに合った SKU を提供しており、インスタンスの詳細（例えは、メモリ、CPU、ストレージ）を選ぶことができます。

手順は、「Deploying syslog-ng Store Box 5 LTS on Microsoft Azure」(英文)を参照してください。

Amazon Web Services に SSB をデプロイ（展開）

Amazon Web Services (AWS)に自前のライセンスを使用して SSB をデプロイすることができます。

SSB を AWS 上で使用すると、クラウドでアプリケーションを使用する恩恵を受けることができます。もっとも顕著なものは、アプリケーションのキャパシティ・ニーズに対応できる能力です。AWS は異なった利用ケースに適したインスタンスタイプを用意しており、インスタンスの詳細（例えば、メモリ、CPU、ストレージ）を選ぶことができます。インスタンスは数分以内に起動し、使用した分のみの支払いになります。

詳細は、「Deploying syslog-ng Store Box 5 LTS on Amazon Web Services」(英文)を参照してください。

新たな仮想アプライアンス

SSB 仮想アプライアンスは、正式に Microsoft Hyper-V でサポートされます。詳細は、syslog-ng Store Box 5 LTS インストレーションガイドの「7. syslog-ng Store Box Hyper-V インストレーションガイド」を参照してください。

仮想環境で SSB の仮想ディスクサイズを拡張

仮想環境で SSB の仮想ディスクサイズを拡張することが容易になりました。仮想マシンをパワーダウンし、ディスクサイズを増やし、仮想マシンを再起動するだけです。

手順は、syslog-ng Store Box 5 LTS のインストレーション ガイド 「8. 仮想環境での SSB の仮想ディスクサイズの拡張」 を参照してください。

仮想環境で管理インターフェースの使用を変更

SSB を仮想環境で使用する場合、シングル ネットワーク インターフェースで十分です。ネットワーク インターフェースが一つのみ定義された場合、そのインターフェースは管理目的にも使用されます。

3.2 ログスペースと複数ノード

リモート ログスペース

SSB は、他の SSB のログスペース(フィルターされたログスペース含む)をアクセスして検索することができます。他(リモート)の SSB のログスペースをアクセスできるように構成するには、リモートログスペースを設定します。一度設定すれば、リモート ログスペースは、SSB の他のログスペースのように検索することができます。また、リモート ログスペースをベースにしたフィルターしたログスペースも作成することができます。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド「8.5 リモート ログスペースの作成」 を参照してください。

フィルターされたログスペース

フィルターされたログスペースは、ローカルやリモート ログスペースのログをフィルターして小さくしたサブセットを作成することができます。フィルターしたログスペースにユーザグループを割当てると、ログスペースのサブセットのみをアクセスできるグループの作成により、細かいアクセス制御ができるようになります。フィルターされたログスペースを作成する場合、検索インターフェースと同じ検索表現やロジックを使用できます。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド 「8.4 フィルターされたログスペースの作成」 を参照してください。

複数のログスペース

複数の SSB が異なった場所に設置されている場合、同じ Web インターフェースでそれらのマシンのログをログオンすることなしに閲覧し検索できます。

複数のログスペースを作成すると、例えば、異なった視点に基づいてログを事前にフィルターして、

それらのフィルターしたログを特定のユーザグループのみと共有することができ便利になります。

複数のログスペースは、ログスペースのメンバーから届くメッセージを集めます。新しいログメッセージは、毎秒それぞれの下にリストされます。

複数のログスペースは、一度設定すると、SSB の他のログスペースと同様に検索することができます。また、複数のログスペースをベースにしたフィルターされたログスペースも作成することもできます。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド 「8.6 複数のログスペースの作成」 を参照してください。

3.3 検索とインデクサーの改善

検索インターフェースの改善

- 検索結果のリストにフルのログメッセージを表示させるオプションが追加されました。
  Search > Logspaces > Customize columns
- ダイナミックコラムは、ログメッセージの詳細ビューからログメッセージのリストに直接追加することができます。
- ログメッセージの詳細ビューから直接統計情報を見ることもできます。
- ログスペースビューのプロパティは各ログスペース毎（クライアント側で）に保存されます。
- 使い易さが改善されています。
- Link と CSV ボタンが新しい位置に移動しました。新しい位置は、カレンダーバーのオーバービューセクションの下のアクションバーです。
- アクションバーに Alert ボタンが追加され、コンテンツベースのアラートの作成ができます。詳細は、「コンテンツ ベース アラート」 を参照してください。
- ユーザの操作でエラーになった場合、アクションバーにエラーやワーニングが表示されます。詳細は、syslog-ng Store Box 5 LTS 管理者ガイド 「アクションバー」 を参照してください。

インデクサーの改善

- ログスペース内でインデックスされるログの数が、一日当たり、4294967296 (2^32) 以上になりました。
- 検索と統計情報作成用のタイムフレームが非常に短くなり、一秒単位（以前は一分）で検索できるようになりました。
- 検索表現で最初のキーワードとして'NOT'を使用することができます。

■ SSB のインデクサー サービスは、以前のバージョンより性能が向上しメモリ使用量が減りました。

3.4 メッセージの処理、パース、アラート

高信頼ログ転送プロトコル(RLTP)

SSB は、信頼できる方法(TCP 上で RLTP を使用)でログメッセージを受信することができます。RLTP™は、独自の転送プロトコルで、切断時のメッセージ ロスを防止します。このプロトコルは、syslog-ng Premium Edition ホストと SSB の間(クライアント- SSB、クライアント-リレーSSB)で使用され、フロー コントロールと syslog-ng Premium Edition の信頼できるディスク バッファの仕組みと共に動作し、メッセージ ロスを防止する最善の方法を提供します。送信者はどのメッセージが受信に成功したか検出しています。もしメッセージが転送中にロストすると、最後に受信が成功したメッセージから始まるロストしたメッセージを再送します。従いまして、接続が切れた場合でも、メッセージは受信側で重複することはありません。ただし、フェールオーバーの場合は完全ではありません。RLTP はまた暗号化した接続にも対応しています。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド 「7.3 SSB でシスログ メッセージ ソースの作成」を参照してください。

key-value ペアのパース(解析)

SSB は、空白やカンマで分けられた key-value ペア(例:ファイアウォールや Postfix のログ)メッセージを name-value ペアに分割します。異なったログメッセージをパースするため、セパレート文字を指定できます。例えば、MySQL のログメッセージ用にコロン(:)、ファイアウォールのログ用に等号文字(=)。詳細は、syslog-ng Store Box 5 LTS 管理者ガイド 「10.7 key-value ペアのパース」 を参照してください。

sudo ログメッセージのパース(解析)

SSB は、sudo ログメッセージを name-value ペアに分割します。sudo パーサは、特権昇格のイベント詳細情報などでログメッセージの情報量を向上させます。例えば、誰がこのイベントを発生させたか、発行されたコマンドは何かなどです。パースした値からのメタデータは検索でき、統計やカスタムレポートに使用できます。
詳細は、syslog-ng Store Box 5 LTS 管理者ガイド「10.6 sudo ログメッセージのパース」 を参照してください。

コンテンツベースのアラート

SSB は、ログメッセージ用に検索表現を設定したコンテンツベースのアラートを作成できます。検索は数秒間隔で実行され、ログメッセージのコンテンツと検索表現が一致した時にアラートを発行します。アラートは集められ、事前に定義された E メールアドレスに送信します。

ログメッセージの中には、ユーザにとり非常に重要なものがある場合があり、それらについての通知を得るのは、手動で検索するのよりも効果的です。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド「12.4 コンテンツベースのアラートの作成」 を参照してください。

3.5 SSBへのアクセス

WEB ユーザインターフェースと RPC API の証明書チェーンのサポート

SSB は証明書チェーンをサポートします。これは、Web サーバの証明書でエンドユーザサブスクライバーまたはサーバの証明書に追加された中間証明書が入っています。以前 SSL または TLS セッションの開始時点では、SSB はサーバの証明書のみをクライアントマシンに提示していました。5 LTS からは、証明書チェーンのアップロードを選択することができ、SSB はクライアントマシンにサーバの証明書と追加の中間証明書を送付します。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド 「3.2 Welcome ウィザードで SSB を構成」、「6.7.2 外部証明書をSSBにアップロード」、および「11.4 TLS（暗号化）で使用される証明書の設定」を参照してください。

HTTP Strict Transport Security (HSTS)のサポート（SSB の Web インターフェースでセルフサインの証明書へ切り替える時、または、CA がサインした証明書の有効期間が切れた時）

SSB の Web インターフェースに HTTPS で一度でもアクセスして成功した場合、ブラウザはこれを記憶して SSB へのアクセスには HTTPS の使用を強要します。これは、CA サインの証明書からセルフサインの証明書に切り替える場合や Web インターフェースの SSL 証明書の有効期間が切れた場合に問題になります。

解決方法は、ブラウザから HSTS 設定を外す、または、異なったマシン上で異なったブラウザを用いて新しい証明書をアップロードすることです。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド「4.1 サポートしているブラウザ」 を参照してください。

3.6 ハードウェアとオペレーティング・システム

10Gbit インターフェースのサポート

SSB は、ログメッセージの受信に 10Gbit ネットワーク インターフェースをサポートします。10Gbit インターフェースを 1Gbit ネットワークの代わり、または、一緒に使用することができます。これにより、ネットワーク デバイスが 10Gbit のみをサポートしており、SSB を 10Gbit のみのネットワークに接続しなければならない場合でも、SSB を変更することなしに使用することができます。
詳細は、syslog-ng Store Box 5 LTS 管理者ガイド「外部インターフェースとして 10Gbit インターフェースを使用」 を参照してください。

オペレーティング システムのアップグレード

このリリースでは、SSB アプライアンスのオペレーティング システムをアップグレードしました。これにより、最新で信頼性のあるオペレーティング システムを、より長期にサポートできます。

N シリーズのサーバは未サポート

SSB5 LTS は、次のハードウェアではサポートされません。SSB N1000、SSB N5000、SSB N10000

SSB を他の新しいハードウェア、または、SSB4LTS を使用している場合、特に影響はありません。

3.7 セキュリティ関連の変更

SNMP v3 trap 設定の変更

MD5 認証方式と DES 暗号化方式は、SSB で以下を設定する場合 SNMP trap 設定で使用できません。

- 監視サーバに SNMP v3 でアラートを送信
- ログメッセージを SNMP v3 プロトコルで SNMP デスティネーションへ転送

これらの方式はセキュリティ レベル上の懸念があるため外されました。

詳細は、syslog-ng Store Box 5 LTS 管理者ガイド「4.5.2 SNMP アラートの設定」、「9.4 ログメッセージを SNMP デスティネーションへ転送」 を参照してください。

注意事項: SSBをバージョン 4 F8 以降にアップグレードすると、SNMP trap MD5 (認証方式)設定

が自動的に SHA1 になり、SNMP trap DES (暗号化方式)は、自動的に AES に設定されます。

詳細は、syslog-ng Store Box 5 LTS アップグレードガイド の「SNMP v3 trap 設定」 を参照してください。

注意事項: これらの自動的な変更により、関連する設定を手動で再設定する必要があります。

キーのフィンガープリントを生成する時 MD5 は SHA-256 になります。
プライベートキーのフィンガープリントを計算する時、以前使用していた MD5 ハッシュ機能が SHA-256 アルゴリズムになります。SSB の Web インターフェースは、キーのフィンガープリントの横に使用しているハッシュ機能を表示します。

3.8 SSBの監視

Disk space fill up prevention (ディスクスペースの飽和防止) の変更
以下の設定のデフォルト値が変更になりました。
Basic Settings > Management > Disk space fill up prevention > Disconnect clients when disks are

デフォルト値は、0 から 90 に変更になり、デフォルトで Disk space fill up prevention が ON になります。

設定値が 100 の場合も変更になり、4 F8 から、1～99 の間の値のみ設定できます。これにより、アップグレード前に 100 を設定していた場合、アップグレード後は 99 になります。

詳細は、syslog-ng Store Box 5 LTS アップグレードガイドの 「ディスクスペースの飽和防止の変更」 を参照してください。

SNMP high disk utilization trap (高ディスク使用率トラップ) の変更
ディスクの高使用率に関係するトラップが変更になりました。詳細は、syslog-ng Store Box 5 LTS アップグレードガイドの「SNMP 高ディスク使用率トラップ」 を参照してください。

3.9 その他の改善と変更

- Log > Sources > Do not parse messages オプションが Do not parse に変更。
- SSB は、LDAP への問合せにバインドユーザを使用します。
- SSB 4 F5 以降では、ネットワーク インターフェースのスピートを手動で変更できません。
- Anonymous login は、SMB/CIFS アーカイブとバックアップ から削除されました。anonymous login を継続して使用したい時、ユーザ名として anonymous と入力して Password は空白にしてください。(Anonymous login オプションを有効にしている場合、この変更は自動で行われます。)

新しいガイド

ドキュメント内の情報整理を改善し、役割に関連する情報を探し易くするため、新たに 2 つのガイドを追加しました。ユーザガイドとインストレーションガイドです。これらのガイドの内容は、以前は管理者ガイドに含まれていました。

詳細は、syslog-ng Store Box 5 LTS ユーザガイド と syslog-ng Store Box 5 LTS インストレーションガイド を参照してください。

日本語マニュアル発行日 2018 年 02 月 09 日

本マニュアル原文は『What is new in syslog-ng Store Box 5 LTS January 31, 2018』です

ジュピターテクノロジー株式会社 技術グループ