Balabit
Syslog-ng Store Box
(SSB) 3 LTS

管理者ガイド Rev. 1.3

2013.12.27

ジュピターテクノロジー

目　次

まえがき 1
1.　本ガイドの構成 1
2.　このガイドの対象となる読者と、前提となる知識 2
3.　対象製品 2
4.　本ガイドの表記 2
1　イントロダクション 4
1.1　SSBとは 4
1.2　SSBの範囲外 5
1.3　SSBが必要な理由 5
1.4　SSBの想定ユーザ 6
2　SSBのコンセプト 7
2.1　SSBの製品思想 7
2.2　SSBでログを収集する 8
2.3　受信メッセージと送信メッセージをフローコントロールで管理する 10
2.3.1　フローコントロールと複数の宛先 11
2.4　セキュアチャンネルからログを受け取る 12
2.5　ネットワークインターフェイス 13
2.6　SSBでのハイアベイラビリティ(高可用性)サポート 14
2.7　SSBのファームウェア 14
2.7.1　ファームウェアとハイアベイラビリティ 14
2.8　SSBのバージョンとリリース 15
2.9　ライセンス 16
2.10　ログメッセージの構造 17
2.10.1　BSD-syslogあるいはlegacy-syslog メッセージ 18
2.10.2　IETF-syslogメッセージ 20
3　ウェルカムウィザードと最初のログイン 24
3.1　SSBへの初回ログイン 24
3.1.1　エイリアスIPアドレスの作成（Microsoft Windows） 25
3.1.2　エイリアスIPアドレスの作成（Linux） 29
3.1.3　SSBのIPアドレスの変更 30
3.2　ウェルカムウィザードでのSSBの設定をする 30
3.3　SAN Storageへのアクセスを設定する 40
4　SSBの管理と設定 42
4.1　サポートしているブラウザならびにOS 42

4.2 Webインターフェイスの構成 43
4.2.1 複数のユーザからのWeb経由のアクセスと、排他制御 48
4.3 Basic settings(基本設定) 48
4.3.1 ネットワーク設定 49
4.3.2 日付と時刻の設定 54
4.3.3 SNMPとEメールアラート 55
4.3.4 SSBのシステム監視設定 59
4.3.5 データと設定のアーカイブとバックアップ 67
4.4 ユーザ管理とアクセス制御 83
4.4.1 SSBユーザをローカル環境で管理する 83
4.4.2 ローカルユーザのパスワードポリシーを設定する 84
4.4.3 ローカルユーザグループを管理する 86
4.4.4 LDAPデータベースによるSSBユーザの管理 87
4.4.5 RADIUSサーバーでユーザ認証する 90
4.4.6 ユーザ権限とユーザグループを管理する 92
4.4.7 設定に対する変更を一覧化し、検索する 98
4.5 SSBの管理 99
4.5.1 SSBの制御－再起動、シャットダウン 99
4.5.2 SSBハイアベイラビリティのクラスターを管理する 100
4.5.3 SSBのアップグレード 110
4.5.4 SSBのコンソールにアクセスする 118
4.5.5 シールドモード 122
4.5.6 SSBのアウトオブバンド 管理 123
4.5.7 SSBに適用されている証明書を変更する 124
4.5.8 ホストリストポリシーを作成する 127
4.6 SSBにおけるSANへのアクセス管理 130
5 SSBのシスログサーバーを設定する 131
5.1 メッセージソースの設定 131
5.1.1 SSBのデフォルトのメッセージソース 132
5.1.2 SNMPメッセージの受信 132
5.1.3 SSBでメッセージソースを作成する 133
5.2 SSBにログメッセージを蓄積する 136
5.2.1 SSBのデフォルトログスペース 137
5.2.2 インデクサ（インデックス付け）を設定する 137
5.2.3 ログストアを使う 138
5.2.4 SSBにカスタムメッセージスペースを構築する 139

5.2.5 ログスペースの管理 145
5.2.6 ネットワーク経由でログファイルにアクセスする 147
5.3 SSBからログメッセージを転送する 152
5.3.1 SQLデータベースにログメッセージを転送する 152
5.3.2 SSBのSQLテンプレート 155
5.3.3 リモートサーバーにログメッセージを転送する 158
5.3.4 SNMPサーバーにログメッセージを転送する 161
5.4 ログパスを管理する 163
5.4.1 SSBのデフォルトのログパス 163
5.4.2 新しいログパスを作成する 164
5.4.3 メッセージのフィルタリング 166
5.5 syslog-ngのオプションを設定する 169
5.5.1 syslog-ngの全般的な設定 169
5.5.2 SSBにおけるタイムスタンプ設定 170
5.5.3 SSBにおける名前解決 171
5.5.4 TLS暗号化ログ送受信に用いる証明書の設定 173
6 ログメッセージとレポートを閲覧する 176
6.1 searchインターフェイスを使う 177
6.1.1 テーブルの列をカスタマイズする 177
6.1.2 動的列を追加/削除する 179
6.2 SSBにおける設定変更ログ 180
6.3 SSBで収集されたログメッセージ 180
6.3.1 収集されたログメッセージに関するメタデータ 181
6.3.2 ワイルドカードとブーリアンを使った検索 182
6.3.3 検索フィルターの使用と管理 188
6.3.4 検索結果の統計を表示する 190
6.3.5 暗号化されたログスペース内のブラウズ 193
6.4 syslog-ngのピアー(クライアントコンピュータ)の設定変更 197
6.5 アーカイブ・バックアップの通知 197
6.6 ログメッセージのアラート 198
6.7 統計収集のオプション 199
6.8 レポート 200
6.9 カスタムレポートの設定 202
7 パターンデータベースによる、ログメッセージのクラス分け 204
7.1 パターンDBの構造 204
7.2 パターンマッチング 206

7.3 ルールセットの検索 207
7.4 新たなルールセット･ルールを作成する 208
7.5 パターンDB及びルールセットのエクスポート 210
7.6 パターンDBのインポート 210
7.7 パターンパーサの使用 210
7.8 フィルターとテンプレートで、パーサによる解析結果を利用する 212
8 SSBのトラブルシューティング 215
8.1 ネットワークのトラブルシューティング 215
8.2 システムの問題を解決するためのデータを収集する 216
8.3 SSBのログを確認する 217
8.4 エラーレポートのための、ログ及びシステム情報を収集する 218
8.5 ステータス履歴と統計 219
8.5.1 syslog-ng統計情報のカスタム表示 221
8.6 SSBクラスターのトラブルシューティング 221
8.6.1 両方のノードがダウンした際のSSBのリカバリー 221
8.6.2 スプリットブレイン状況からのリカバリー 222
8.6.3 HAノードのリプレース 224
8.7 コンフィグレーションバックアップからコンフィグレーションをリストアする 226
付録 1 syslog-ng Store Box ハードウェアインストレーションガイド 227
付録 1.1 SSBハードウェアのセットアップ 227
付録 1.2 二つのSSBユニットをHAモードで設定する。 228
付録 2 VMware環境でのsyslog-ng Store Box インストレーションガイド 230
用語集 233

まえがき

この文書では syslog-ng Store Box (SSB) の設定および管理方法について説明します。
製品の技術的な背景知識や概要についても紹介します。

1. 本ガイドの構成

本ガイドは以下の章から構成されています。

第1章 イントロダクション

SSB の主な機能と目的について説明します。

第2章 SSB のコンセプト

SSB の技術的な概念及び製品思想について説明します。

第3章 ウェルカムウィザードと最初のログイン

SSB インストール時及びその後の初期設定をステップバイステップで説明します。

第4章 SSB の設定と管理

SSB の設定と管理について詳しく説明します。

第5章 SSB syslog-ng サーバーの設定

ログメッセージを受信し処理するために SSB 内の syslog-ng サーバーの設定について説明します。

第6章 ログメッセージと SSB レポートの閲覧

ログ、アラート、レポートをオンラインで閲覧する方法について説明します。

第7章 パターンデータベースによるメッセージのクラス分け

パターンデータベースを用いてメッセージを解析し、クラス分けする方法について説明します。

第8章 SSB のトラブルシューティング

SSB のトラブルシューティングとメンテナンスについて説明します。

付録 1　VMware 環境での BalaBit・SSB インストレーションガイド

SSB を仮想アプライアンスとしてインストールする方法について説明します。

用語集　このガイドで使用される重要な用語の意味を説明します。

2.　このガイドの対象となる読者と、前提となる知識

このガイドは、監査役、コンサルタント、サーバー管理（特にリモートサーバー管理）プロセスのセキュリティ、監査、監視を担当するセキュリティ専門家を対象にしています。また、サーバーのセキュリティと監査能力を向上させるツール、あるいはサーベンス・オクスリー法(Sarbanes-Oxley Act(SOX))、医療保険の携行と責任に関する法律(Health Insurance Portability and Accountability Act(HIPAA))、バーゼルⅡ(Basel II)、Payment Card Industry(PCI)スタンダードの順守を容易にするツールを探している情報システム部門担当者にも役立ちます。

SSB 管理者に必要なスキルと知識は以下の通りです。

- ■システム管理の基礎知識
- ■ネットワーク、TCP/IP プロトコル、一般的なネットワーク専門用語の理解
- ■リモートシステムのログ取得・管理に用いられる、ログ及びそのプロトコル
- ■syslog-ng 及び Windows 向け syslog-ng エージェントの概念の理解
- ■UNIX あるいは Linux OS の知識（必須ではありませんが、あれば大変役に立ちます。）

3.　対象製品

このガイドでは、syslog-ng Store Box の使用方法について説明します。

注記

SSB のユーザーは syslog-ng Premium(有償) Edition アプリケーションを SSB 用のログ収集エージェントとして使用することができます。このガイドでは syslog-ng Premium Edition のインストールと設定については扱っていませんので、詳細は syslog-ng 3.0 管理者ガイドをご参照下さい。

4.　本ガイドの表記

本ガイドをお読みいただく前に、この文書で使用される用語とアイコンの意味をご理解ください。
本ガイドで使用される専門用語と略称については 用語集をご参照下さい。

次の表記規則を使用します。

ヒント

ヒントでは、ベストプラクティスと推奨を提供します。

例

例ではトピックについての詳細な情報を実例とともに提供します。

注記

注記では、トピックに関する追加情報を提供し、重要事項と考慮すべき事柄を強調します。

警告

警告では、指示に従わない場合にデータの喪失や装置の設定ミスを
引き起こす可能性があることを示します。

等幅（例： `command`）	実行するコマンド
	参照項目
	ファイル名（`/path/to/file`）
	パラメータや属性名（`Parameters`）
太字（例： **Button**）	GUI メッセージやダイアログのラベル
	メニューバーのサブメニューやメニュー項目
	ダイアログウィンドウのボタン

1　イントロダクション

この章では、技術仕様ではなく、どのように、そしてなぜ SSB が有益なのかについて説明し、現在の IT インフラにどのように付加的な効果をもたらすかについて紹介します。

1.1　SSBとは

SSB はログメッセージを収集、処理、記録、監視、そして管理するデバイスです。SSB は集中ログサーバーアプライアンスで、ネットワークデバイスとコンピューターからシステムのログメッセージ（シスログとイベントログ）や Simple Network Management Protocol(SNMP) メッセージを受信して、それらのメッセージを、信頼できる署名付きのログ保存先（logstore）に記録します。また、自動的にメッセージのアーカイブとバックアップを行い、人工知能を使ってメッセージをクラス分けします。

SSB の特筆すべき特長は以下のとおりです。

- Transport Layer Security(TLS)を使用した安全なログ収集
- 暗号化され、署名とタイムスタンプが付加された、安全性の高いログ記憶領域
- Microsoft Windows XP, Server 2003, Vista, Server 2008 に加えて Linux, Unix, BSD, Sun Solaris, HP-UX, IBM AIX, IBM System i を含む、幅広いプラットフォームからログメッセージを収集可能
- ログ解析ツールにメッセージを転送可能
- リアルタイムでのログ監視、アラート送信及び人工無能のための、カスタマイズ可能なパターンデータベースを使ったメッセージのクラス分け
- ハイアベイラビリティ(HA)で、ビジネスの重要な環境における継続的なログ収集に確実に対応
- リアルタイムでのログ監視とアラート送信
- Lightweight Directory Access Protocol(LDAP)データベースから管理者のグループメンバーシップを取得
- 選択されたログメッセージにのみアクセスを許可するよう、厳格な、しかしカスタマイズは容易に行えるアクセスコントロール設定

SSB は、HTTPS 接続、JavaScript、クッキーに対応する最近の Web ブラウザの大半から設定、管理できます。サポートされるブラウザは、Mozilla Firefox のバージョン 10 と Microsoft Internet Explorer のバージョン 8 とバージョン 9 です。

1.2 SSBの範囲外

SSB はログ分析エンジンではありません。Unix 業界の一般的なログチェックのアプリケーションと同様、SSB は人工知能を使ってそれぞれのログメッセージをクラス分けすることならできます。SSB には“通常”とされるログメッセージのパターンのデータベースが内蔵されています。アプリケーション（例えば sendmail, Postfix, MySQL など）を正しく使用している間、これらのパターンに合致するメッセージが作成されます。これらのメッセージはログ監視の観点からはさほど重要ではありませんが、残っているメッセージには“重要な”内容が含まれている場合があります。管理者は、SSB のインターフェイス上でログパターンを定義したり、合致するメッセージにラベル（例えば「セキュリティイベント」など）を付けたり、特定のパターンに一致するログを受信した場合にアラートの送信を要求したりできます。より詳細なログ解析のために、SSB は受信したログメッセージを外部のログ解析ツールに転送できます。

1.3 SSBが必要な理由

ログメッセージには、ホストで発生しているイベントに関する情報が含まれています。システムイベントの監視は、セキュリティ上、そしてシステムヘルス監視の点で大変重要です。安定したログ管理ソリューションにより、組織・事業体は多くの恩恵を受けます。ログ管理ソリューションによって、コンピューターセキュリティの詳細な記録が確実に保存されて、それらのログを簡単に監視して確認できます。日々ログを確認して継続的に分析することは、セキュリティ事故やポリシー違反、その他の運用上の問題を把握するために役立ちます。また、ログは監査やフォレンジックの際の分析、製品のトラブルシューティングやサポートの基盤となります。ログメッセージをまとめて収集して定期的に確認し、長期間保存することを明示的に定めた法律や規則、業界基準も複数存在します。例えば、サーベンス・オクスリー法（Sarbanes-Oxley Act (SOX)）やバーゼルⅡ（Basel Ⅱ）、医療保険の携行と責任に関する法律(Health Insurance Portability and Accountability Act (HIPAA))、クレジットカード業界の安全基準(Payment Card Industry Data Security Standard (PCI-DSS))などです。

SSBは、世界中で数千の企業で使われ人気を博しているsyslog-ngのアプリケーションを中心として開発された、ログの収集と保存を目的としたアプライアンスです。強力ですが簡単に設定できます。最新の syslog-ng Premium Edition の機能を最大限に活用することで、SSB で幅広いプラットフォームとデバイスからログメッセージを収集して処理して保存できます。

すべてのデータを暗号化して電子署名付きで保存することが可能であり、ファイルにタイムスタンプを付けて、データの修正や改ざんを防ぐことが出来ます。また、最高レベルのセキュリティ基準とポリシーコンプライアンスの要件を満たすことができます。

1.4 SSBの想定ユーザ

SSB はログメッセージの収集、保管、確認を必要とする全ての人に有益です。特に SSB は以下の点で威力を発揮します。

■一元的なログ収集とアーカイブ
SSB を使えば、簡単かつ便利で信頼できるログメッセージの収集を一元的に行うことができます。SSB は本来、ハイアベイラビリティ(高可用性)に対応できる大容量のログサーバーです。複数の異なるプラットフォームからログを収集できるので、あらゆる環境に容易に統合することができます。

■安全なログ転送と保存
ログメッセージには取り扱いに注意が必要な情報が含まれていることが多々あり、複数のアプリケーションにおいて監査トレイルの基盤を成すものです。セキュリティとプライバシー上の理由から、メッセージが転送される際に漏洩したり、メッセージがログサーバーに到達した後に許可なくアクセスされたりするのを防ぐことが不可欠です。

■ポリシーコンプライアンス
多くの企業は、サーベンス・オクスリー法（Sarbanes-Oxley Act （SOX））、バーゼルⅡ（Basel II）、医療保険の携行と責任に関する法律（Health Insurance Portability and Accountability Act （HIPAA））、クレジットカード業界安全基準 （PCI-DSS)のような法律を遵守する必要があります。これらの規制により、ログの管理が明示的または黙示的に義務付けられています。ログ管理とは、例えば、ログメッセージの一元的な収集や、セキュリティ事故の発生防止及び問題の検出のためのログの分析、最大数年に渡って長期間ログを確実に入手できるようにすることなどです。SSB は、企業がこれらの規制を遵守するためのお手伝いを行います。

■ログの監視と前処理の自動化
ログメッセージの監視は、システムヘルスの監視とセキュリティ事故の検出及び防止の一端として必要不可欠です。SSB は、数万のメッセージをリアルタイムにクラス分けできる強力なプラットフォームを提供し、通常のものとは異なるメッセージを検出して適切なアラートをあげることができます。このクラス分けはログ分析アプリケーションとしては完璧なものではありませんが、SSB は通常のログ分析エンジンよりもはるかに多くのメッセージを処理することができ、重要でないメッセージを除外することでログ分析アプリケーションへの負荷を軽減することができます。

2　SSBのコンセプト

この章では、SSB の技術的な概念について説明します。

2.1　SSBの製品思想

SSB は、ネットワークデバイス、アプリケーション、コンピューターによって送信されたログメッセージを収集、保存、監視するログサーバーアプライアンスです。SSB は従来のシスログメッセージ、Internet Engineering Task Force(IETF)の新しい基準に準拠するシスログメッセージ、Microsoft Windows ホストから送信されるイベントログメッセージ、SNMP メッセージを受信できます。

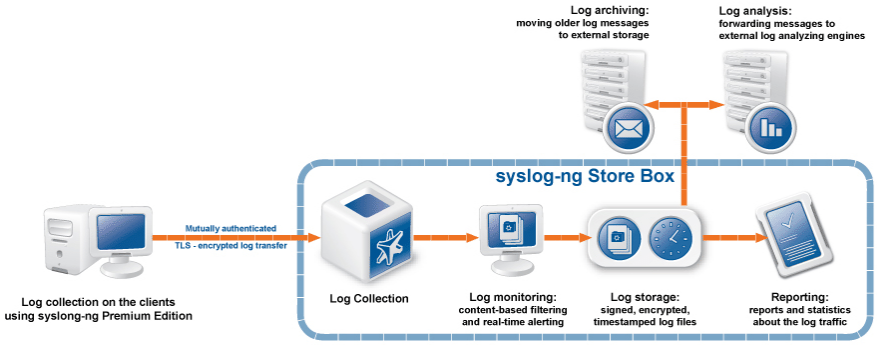


図 2-1　SSB の製品思想

クライアントは、BSD-syslog(RFC 3164)または IETF-syslog(RFC 5424-5428)プロトコルをサポートするアプリケーションが生成するログをSSBに送信できます。または、syslog-ng Premium Editionアプリケーションを使用してSSBのログ転送エージェントとして動作させることもできます。

SSB を使用する主な目的は、クライアントからログを収集してそれをハードディスクに保存することです。メッセージは「ログスペース」と呼ばれる領域に保存されます。ログスペースには 2 つの種類があります。1 つ目は、従来の平文のテキストファイルでメッセージを保存するもので、2 つ目は圧縮・暗号化・電子署名・タイムスタンプが可能なバイナリフォーマットを使用するものです。

syslog-ng アプリケーションは、受信メッセージを判定して、指定された宛先(destinations)に転送します。syslog-ng アプリケーションは、ファイル、リモートホスト、その他の送信元-これらは全て、「source」と呼ばれます－から、メッセージを受信できます。

syslog-ng 上で入ってくるログメッセージは、定義されたソースの内の一つに収まり、1 つあるいは複数の宛先に送信されます。クライアントの場合、宛先の 1 つが SSB で、SSB 上での宛先はログスペースでもデータベースサーバーやログ分析エンジンのようなリモートサーバーでも可能です。

送信元と宛先は独立したオブジェクトです。ログパス(log paths)は syslog-ng がメッセージをどう処理するかを定義して、送信元と宛先の橋渡しをします。ログパスは 1 つあるいは複数の送信元と 1 つあるいは複数の宛先から成っています。送信元に到着するメッセージはログパス内に記述された宛先それぞれに送信されます。syslog-ng で定義されるログパスはログステートメント(log statement)と呼ばれます。

ログパスにはオプションでフィルター(filters)を含むことが出来ます。フィルターとは、特定のメッセージ、例えば特定のアプリケーションから送信されたメッセージのみを選択するルールです。ログパスにフィルターが含まれる場合、syslog-ng は、ログパスに記述されたフィルター条件に合致するログメッセージのみを、宛先に転送します。

管理者または監査者が Web ブラウザを使って SSB を設定します。

2.2 SSBでログを収集する

目的:

ここでは syslog-ng クライアントにおけるソースから SSB へのログメッセージのルートを図式化します。

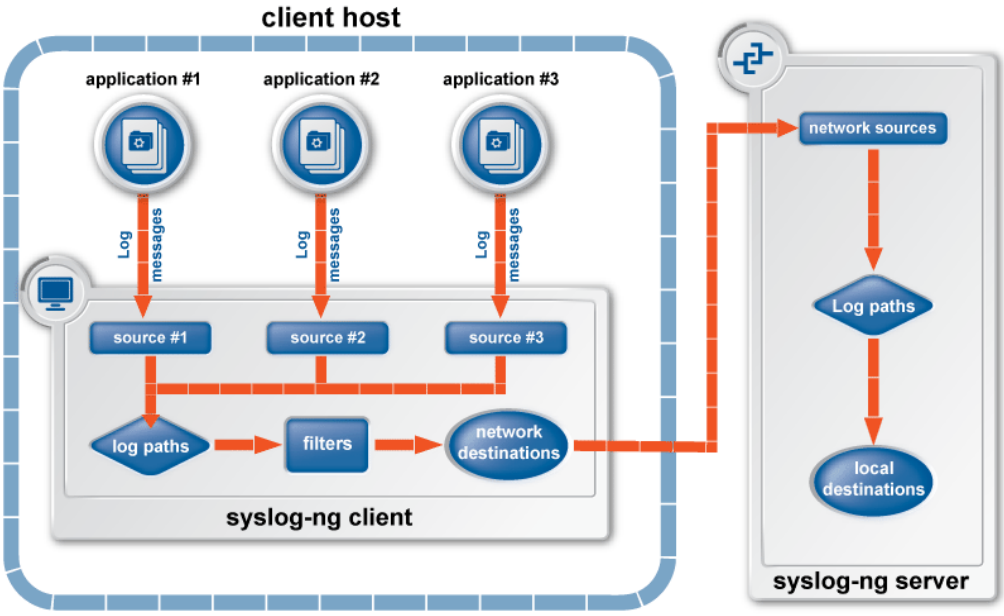


図 2-2 ログメッセージのルート

Step

Step 1. syslog-ng クライアント上でデバイスまたはアプリケーションがソースにログメッセージを送信します。例えば、Linux 上で動作している Apache Web サーバーは/var/log/apache ファイルにメッセージを入力します。

Step 2. Web サーバー上の syslog-ng クライアントは、/var/log/apache からメッセージを読みます。

Step 3. syslog-ng クライアントは、/var/log/apache を含む最初のログステートメントを処理します。

Step 4. syslog-ng クライアントは、メッセージにオプションで選択されている処理（例えばメッセージのフィルタリング）を行います。例えば、メッセージを、（もしあれば）ログステートメントのフィルターと比較します。メッセージがすべてのフィルタールールに適合した場合、syslog-ng はログステートメントで設定されている宛先、例えばリモートの syslog-ng サーバーにメッセージを送信します。その後、syslog-ng クライアントは、Step3 から Step4 を繰り返して、/var/log/apache を含む次のログステートメントを処理します。

Step 5. syslog-ng クライアントによって送信されたメッセージが SSB 上で設定されたソースに到着します。

Step 6. SSB は、ソースからのメッセージを読んで、この送信元を含む最初のログパスを処理します。

Step 7. syslog-ng サーバーは、オプションで選択されている処理（例えばメッセージのフィルタリングや既知のメッセージの一覧と比較するためのパターン照合）を実行します。メッセージがすべてのフィルタールールに適合した場合、SSB はメッセージをログパスで設定されている宛先に送信します。宛先は、SSB 上のローカルの任意で暗号化されたファイルか、またはデータベースサーバーなどのリモートサーバーです。

Step 8. SSB は、Step6 から Step8 を繰り返して、次のログステートメントを処理します。

注記

宛先が送信されたメッセージを処理できなくなった場合、syslog-ngアプリケーションはその送信元からメッセージを読むのをやめることができます。この機能はフローコントロールと呼ばれ、詳細は 2.3 受信メッセージと送信メッセージをフローコントロールで管理するをご参照ください。

2.3 受信メッセージと送信メッセージをフローコントロールで管理する

この章では、メッセージロストを防ぐフローコントロール機能と、syslog-ng 内部のメッセージ処理のモデルを説明します。フローコントロールを使うには、ログパス内で **Flow** オプションを有効にする必要があります。

syslog-ng アプリケーションは、設定ファイルで定義した送信元を監視(ポーリング)して、それぞれの送信元のメッセージを定期的に確認します。送信元の 1 つにログメッセージが見つかると、syslog-ng はそれぞれの送信元をポーリングして読むことのできるメッセージを読みます。これらのメッセージは処理されて syslog-ng の出力バッファー(fifo)に蓄えられます。出力バッファーから、OS が適切な宛先にメッセージを送信します。

膨大な量のトラフィックをさばくネットワーク環境では、ひとかたまりのポーリング処理(ポーリングループ)の間に多くのメッセージが到達することがあります。そのため、syslog-ng はそれぞれの送信元から決まった数のメッセージだけを読みます。ポーリングループの間に 1 つの送信元から読むメッセージの数は、**Messages fetched in a single poll** オプションで指定します。

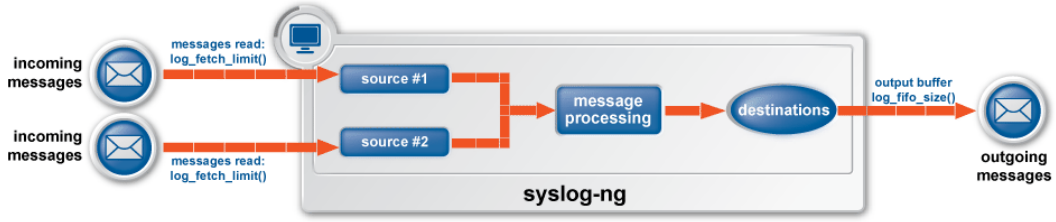


図 2-3 syslog-ng でログメッセージを管理する

注記

SSB の **Messages fetched in a single poll** オプションは **Log > Options** でグローバルオプションとして設定できます。

それぞれの宛先には固有の出力バッファーがあります。宛先がすべてのメッセージを即座に受け入れることができない場合があるので、出力バッファーは必要です。SSB では、**Output memory buffer** のパラメータで出力バッファーのサイズを設定します。ポーリングループの間それぞれのメッセージの読み込みが出力バッファーに確実に適合するように、出力バッファーは送信元の **Messages fetched in a single poll** の値より大きくなくてはいけません。ログパスが複数の送信元から宛先にメッセージを送信する場合、出力バッファーにはそれぞれの送信元の受信メッセージを保存できるだけの大きさが必要です。

TCP と TLS の送信元は、いくつかの受信接続(例えば異なる多くのクライアントやアプリケーション)からログを受信できます。これらの送信元に関しては、syslog-ng がそれぞれの接続からメッセージを読むので、送信元の接続ごとにそれぞれ **Messages fetched in a single poll** のパラメータが適用されます。

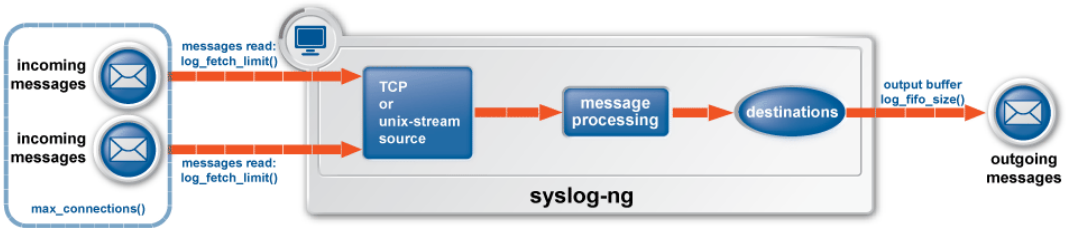


図 2-4 syslog-ng で、TCP 送信元のログメッセージを管理する

syslog-ng のフローコントロールは、syslog-ng が送信元からどのくらいのメッセージを受信できるかを追跡するコントロールウィンドウをソースに取り入れます。syslog-ng が送信元からメッセージを読む度に、自由に使えるスロットの数が 1 つずつ減ります。syslog-ng が出力バッファーからメッセージの送信に成功する度に、自由に使えるスロットの数は 1 つずつ増えます。ウィンドウがいっぱいになる(＝自由に使えるスロットがなくなる)と、syslog-ng はそのソースからメッセージを読むのを停止します。コントロールウィンドウのデフォルトのサイズは 100 です。フローコントロールが効果をあげるには、**Output memory buffer** はデフォルトサイズの値より大きくなくてはいけません。送信元が複数の接続からメッセージを受け付ける場合、すべてのメッセージは同じコントロールウィンドウを使用します。

フローコントロールを使用する場合、それぞれのソースに固有のコントロールウィンドウがあります。最悪の場合、宛先の出力バッファーを、それぞれのコントロールウィンドウのすべてのメッセージを収容できるよう、設定する必要もありえます。つまり、宛先の **Output memory buffer** は((Number of sources) × (Initial window size))より大きくなくてはいけません。これは特定の宛先にログを送るすべてのソースに当てはまります。そのため、仮に 2 つのソースに複数の接続があり、それらが同じ宛先に大量のログを送信する場合、それぞれのソースのコントロールウィンドウサイズは宛先の出力バッファーサイズにふさわしい大きさにする必要があります。さもないと、syslog-ng はフローコントロールを有効にできず、メッセージロストの可能性があります。

2.3.1 フローコントロールと複数の宛先

ソースのメッセージを複数の宛先に送信する場合、ソース上でフローコントロールを使用すると重大な副作用が生じます。フローコントロールを使用して宛先の 1 つがメッセージを受信できない場合、他の宛先もメッセージを受け取れません。これは syslog-ng がソースからログを読み出すのを止めてしまうからです。例えば、ソースからのメッセージがリモートサーバーに送られ、同時にローカルファイルにも保存される場合、サーバーへのネットワーク接続は無効になり、リモートサーバーもローカルファイルもメッセージを受け取りません。このフローコントロールの副作用は syslog-ng のディスクベースのバッファリングの特徴を使用することで避けることができます。

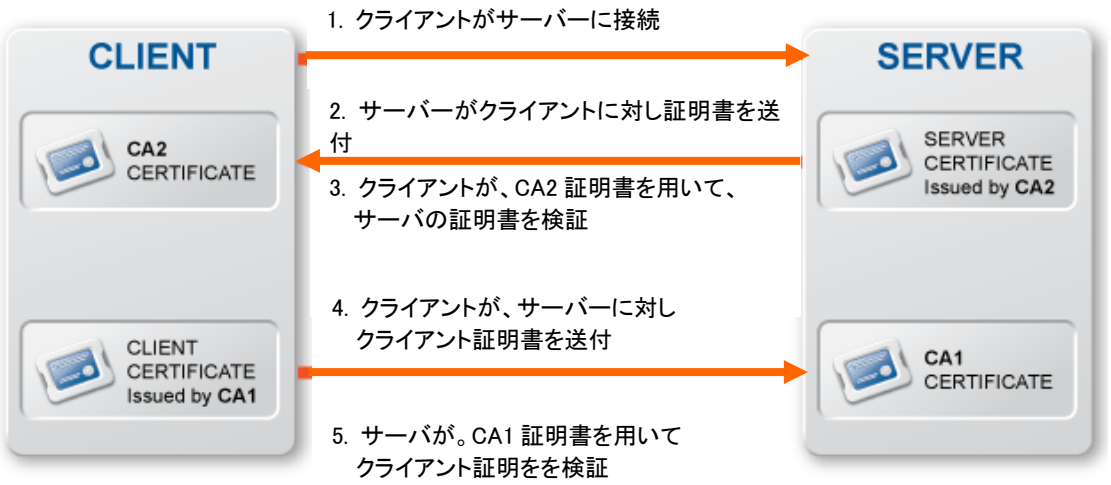
注記

同じフローコントロールのソースを使用する宛先に別々のログパスを作成しても問題を避けることはできません。

2.4 セキュアチャンネルからログを受け取る

SSB は Transport Layer Security(TLS)を使用するネットワーク上でログメッセージを安全に受け取ります(TLS は TCP/IP ネットワークプロトコル上の暗号プロトコルです。)

TLS は通信を認証し暗号化するために証明書を使用します。以下のイラストで表わします。



図表 2-5 証明書ベースの認証

SSB にログを送信するクライアントは、証明書及び公開鍵の送付を SSB に要請し、それによって認証を行います。オプションとして、SSB がクライアントに対し証明書の送付を要求でき、それによって相互認証も可能となります。

syslog-ng において TLS 暗号化を行うためには、以下の条件が揃っていることが必要です。

- SSB 自身を証明する証明書が存在すること。(デフォルトで実装されています)
- SSB 自身の証明書を発行した CA(認証局)が発行する証明書を、syslog-ng クライアントが検査できること

クライアントの本人性(identity)を確認するために相互認証を使用する時は、以下の条件が揃っていることが必要です。

- 証明書は syslog-ng クライアントに適用できること。この証明書は syslog-ng クライアントを識別します。
- syslog-ng クライアントの証明書を発行した認証局の証明書を SSB が検査できること。

相互認証は権限を与えれらたクライアントだけから SSB がログメッセージを受け取ることを保障します。

syslog-ngにおけるTLS通信を設定する詳細については、5.1メッセージソースの設定をご参照下さい。

2.5 ネットワークインターフェイス

SSB ハードウェアには 5 つのインターフェイスがあります。外部、管理、内部（SSB では現在使用されていません）、HA そして IPMI インターフェイスです。

外部インターフェイスはSSBとクライアント間の通信に使用します。クライアントはシスログメッセージをSSBの外部インターフェイス経由で送ります。また、SSBの初期設定は常に外部インターフェイスを使用して実行されます。（初期設定についての詳細は、3.2ウェルカムウィザードでのSSBの設定をするをご参照下さい。）外部インターフェイスは、管理インターフェイスが設定されていない場合、管理目的でも使用されます。外部インターフェイスはEXTラベルがついたイーサネットコネクタを使用します。

管理インターフェイスは、SSB と SSB 監査者もしくは SSB 管理者間のコミュニケーションのために**のみ**使用されます。このインターフェイスへの接続要求は、SSB の Web インターフェイスにアクセスするためだけに受け入れられ、他の要求は拒否されます。管理インターフェイスは MGMT ラベルがついたイーサネットコネクタを使用します。

ルーティング規則は、どのインターフェイスが SSB のリモートバックアップやシスログメッセージの転送に使用されるかを決定します。

ヒント

バックアップ、Eメールアラートは管理インターフェイス向けに送信することを推奨します。詳細については 4.3.1.2管理用途のトラフィックを、管理インターフェイスに集約する, をご参照下さい

管理インターフェイスを設定していない場合、外部インターフェイスが管理インターフェイスの役割をします。

HAインターフェイスはSSBクラスターのノード間の通信専用です。HAインターフェイスはHAラベルがついたイーサネットコネクタを使用します。ハイアベイラビリティの詳細については2.6 SSBでのハイアベイラビリティ(高可用性)サポートをご参照下さい。

Intelligent Platform Management Interface(IPMI)インターフェイスによりシステム管理者がシステムの健全性を監視してリモートで SSB イベントを管理することができます。IPMI は SSB のオペレーティングシステムと独立して動作します。

2.6 SSBでのハイアベイラビリティ(高可用性)サポート

ハイアベイラビリティ(HA)モードでは、専用の設定を施された 2 つの SSB ユニット(マスターノードとスレーブノード)が同時に動作します。マスターノードはスレーブノードと全てのデータを共有し、マスターノードが機能を停止した場合、スレーブノードが即座にアクティブになるので、クラインアンとは引き続き、サーバーにアクセスできます。スレーブノードはマスターノードのインターフェイスの MAC アドレスを引き継ぎます。

警告

2 つのノードが互いに通信できない場合、スレーブノードはマスターノードが故障して停止したとみなしてアクティブになり、両方のノードが同時にアクティブになる可能性があります(スプリットブレイン状態)。これによりデータの喪失が引き起こされることがあります。スプリットブレイン状態からの回復方法に関する詳細については 8.6.2スプリットブレイン状況からのリカバリーをご参照ください。
スプリットブレイン状態の回避方法に関する詳細については 4.5.2.3 冗長化ハートビートインターフェイスの設定をご参照ください。

スレーブノードは HA ネットワークインターフェイス経由でマスターノードのハードディスクと自動的に同期します。ディスクは HA サポートが正しく動作するように同期されなければなりません。

警告

管理インターフェイスとハイアベイラビリティ(HA)を一緒に使うときは、忘れずに両方の SSB ノードの管理インターフェイスをネットワークに接続してください。切り替えが起こった時に、SSB にリモートからアクセスすることができなくなってしまいます。

2.7 SSBのファームウェア

SSB のファームウェアは、external(外部)ファームウェアと internal(内部)ファームウェアの 2 つに分かれています。

- external(外部)ファームウェア(boot(ブート)ファームウェア)は、SSB を起動し、ハイアベイラビリティサポートを提供し、internal(内部)ファームウェアを起動します。外部ファームウェアはめったに変更されません。
- internal(内部)ファームウェア(core(コア)ファームウェア)は、その他全て(Web インターフェイスの提供、ログメッセージの受け取りと処理など)を処理します。内部ファームウェアは、SSB に新たな機能が加えられるたびに定期的に更新されます。

どちらのファームウェアもSSB Webインターフェイスから更新することができます。詳細は、4.5.3 SSBのアップグレードをご参照下さい。

2.7.1 ファームウェアとハイアベイラビリティ

ハイアベイラビリティモードで SSB ノードの電源を入れたとき、両方のノードが起動しブートファームウェアを開始します。そしてブートファームウェアは、どちらのユニットがマスターかを決めます。(コアファームウェアは、マスターノード上でのみ開始します)。

SSB ファームウェアを Web インターフェイスから更新すると、両方のノード上のファームウェアを自動的に更新します。

2.8 SSBのバージョンとリリース

2011 年 6 月より、SSB は以下のサポートポリシーに従います。

■Long Term Supported or LTS リリース（例：SSB 3.0.1）
リリースから 3 年間、あるいは、次の LTS リリースがリリースされてから1年間のいずれか遅い方の期間までサポートされます。このリリースの 2 桁目のリビジョンは 0 です（例：SSB 3.0.1）。LTS リリースに対するメンテナンスリリースはバグフィックスとセキュリティーアップデートのみを含みます。

■Feature リリース（例：SSB 3 F1）
.リリースから 6 か月、あるいは、次の Feature または LTS リリースがリリースされてから 2 か月のいずれか遅い方の期間までサポートされます。このリリースは、機能強化と新機能（1 回のリリースでおおよそ 1～3 つ）を含みます。

警告

以前の Feature リリース、または Stable リリースへのダウングレードはサポートされません。Stable リリース（例： 1.0）から Feature リリース(例： 1.1)にシステムを更新した場合、次の Stable バージョンリリース（例： 2.0）が発表されるまで新しい Feature リリースへ更新し続けるか、リスクを負ってサポートされていない製品を使う必要があります。

2.9 ライセンス

SSB のライセンスはログメッセージを SSB に送ることができる個々のホスト（ログソースホスト）の数で決まります。

ログソースホストは syslog-ng サーバーにログを送るホストあるいはネットワークデバイス（syslog-ng クライアントとリレー含む）です。ログソースホストはサーバー、ルーター、デスクトップコンピューター、もしくはシスログメッセージを送り、syslog-ng を実行することができる他のデバイスです。ログソースホストは IP アドレスで識別されるので、仮想マシンや仮想ホストは別々にカウントされます。

警告

syslog-ng の *chain_hostnames()*オプションは syslog-ng のログソースホストのカウント方法に干渉し、中央サーバーに実際以上のログ送信ホストがあるかのような動作を syslog-ng が行う原因となります。*chain_hostnames()*は非推奨オプションです。ログソースでライセンス集計に関連する問題を起こさぬよう、このオプションは無効にしておいてください。

SSB ライセンスで syslog-ng Premium Edition アプリケーション（syslog-ng Agent for Windows 含む）をダウンロードできます。そして SSB 用のログ収集エージェントとしてサポートされたどんなプラットフォーム上でもインストールできます。

- syslog-ng Box SSB1000,SSB1000d
  50 IP アドレスからログ収集ができます。無制限にアップグレードできます。

- syslog-ng Store Box SSB5000,SSB10000
  無制限の IP アドレスからログを収集できます。

詳細は弊社にお問合せ下さい。新しいライセンスのインストールについての詳細は、4.5.3.2 SSBライセンスキーのアップデートをご参照下さい。

例　2.1.ログソースホストをカウントする

この例では 2 つのファシリティ（例えばデータセンターもしくはサーバーファーム）があります。80 台の AIX サーバーと 20 台の Microsoft Windows ホストがファシリティ 1、5 台の HP-UX サーバーと40 台のDebianサーバーがファシリティ2です。145ホストが一緒になっています。

これらのホストのログメッセージを 1 つの SSB に収集したいときは、少なくとも 145 ホストからログを受け取ることができるライセンスが必要です。（実際は 150 ホスト用のライセンスを購入する必要があります。）
それぞれのファシリティに SSB が必要で、両方のファシリティのログメッセージを収集する中央サーバーは必要ない場合、別々の SSB が必要です。ファシリティ 1 では 100 ホスト用のライセンス、ファシリティ 2 では少なくとも 45 ホスト用のライセンスです（実際には 50 ホスト用ライセンス購入が必要です）。
ログをローカルに保存するローカルなログサーバーをそれぞれに持つファシリティと、その 2 つのローカルなログザーバーから独立して全てのログメッセージを収集する中央ログサーバーが必要な場合、以下のように 3 つの SSB ライセンスが必要です。ファシリティ 1 で 100 ホスト用のライセンス、ファシリティ 2 で少なくとも 45 ホスト用のライセンス、中央ログサーバー用のライセンスです。中央サーバーのライセンス数は 100（ファシリティ 1 のホスト）＋45（ファシリティ 2 のホスト）＋2（それぞれのファシリティの 2 つのローカルログサーバー）＝147（実際には 150 ホストライセンス）となります。

注記

例えば、ファシリティ 2 の 40 台の Debian サーバーが 3 つのバーチャルホストを実行している場合、ファシリティ 2 のホスト数は 125 になります。これに従ってライセンス数を計算します。

2.10　ログメッセージの構造

以下のセクションではログメッセージの構造について説明します。現在、2 つの標準シスログメッセージのフォーマットがあります。

- RFC3164 で表記される古いスタンダード（BSD-syslogあるいはlegacy-syslogプロトコルとも呼ぶ）。詳細は 2.10.1　BSD-syslogあるいはlegacy-syslog メッセージをご参照下さい。
- RFC5424 で表記される新しいスタンダード（IETF-syslogプロトコルとも呼ぶ）。詳細は 2.10.2　IETF-syslogメッセージをご参照下さい。

2.10.1 BSD-syslogあるいはlegacy-syslog メッセージ

このセクションではlegacy-syslogあるいはBSD-syslogプロトコルに従ってシスログメッセージのフォーマットを説明します(RFC3164 をご参照下さい)。シスログメッセージは以下のパーツで構成されています。

PRI

HEADER

MSG

メッセージはトータルで 1024bytes 以下でなければなりません。

以下はシスログメッセージのサンプルです。
<133>Feb 25 14:09:07 webserver syslogd: restart.

メッセージは*<priority>*timestamp *hostname application: message.*に相当します。以下のセクションでメッセージの異なるパーツについて説明します。

注記
syslog-ng アプリケーションはもっと長いメッセージもサポートします。詳細は **Message size** オプションをご参照下さい。しかし UDP の宛先を使用する際、パケットサイズより長いメッセージを有効にすることは推奨しません。

2.10.1.1 PRI メッセージ部分

シスログメッセージの PRI の部分(Priority value と呼ばれます)はメッセージの Facility(ファシリティ)と Severity(重要度)を表わします。facility はメッセージを送信するシステムを表わす部分で、severity はその重要度を表わします。Priority value は最初に Facility 数に 8 を掛けて Severity の数値を追加します。可能な facility と severity の数値を以下に表わします。

注記
ファシリティコードは異なるプラットフォームで若干違うことがあります。
syslog-ng アプリケーションは数値としてもファシリティコードを受け取ります。

以下のテーブルは facility の値です。

Numerical Code （数値）	Facility （ファシリティ）
0	カーネルメッセージ
1	ユーザーレベルのメッセージ
2	メールシステム
3	システムデーモン
4	セキュリティ/許可メッセージ
5	syslogd による内部発生メッセージ
6	ラインプリンターサブシステム
7	ネットワークニュース　サブシステム
8	UUCP サブシステム
9	クロックデーモン
10	セキュリティ/許可メッセージ
11	FTP デーモン
12	NTP サブシステム
13	ログ監査
14	ログアラート
15	クロックデーモン
16-23	ローカル使用ファシリティ（local10-local7）

テーブル 2.1.シスログメッセージ Facilities

以下のテーブルリストは severity の値です。

Numerical Code （数値）	Severity（重要度）
0	Emergency: システムが使用不可能
1	Alert: 至急対応が必要
2	Critical: 重大な状況
3	Error: エラーの状況
4	Warning: 警告の状況
5	Notice: ノーマルだが重要な状況
6	Informational: 情報メッセージ
7	Debug:: デバッグレベルの状況

テーブル 2.2 シスログメッセージ Severities

2.10.1.2 Header(ヘッダー)部分

Header(ヘッダー)部分はタイムスタンプとホストネーム(ドメインネーム抜き)あるいはデバイスの IP アドレスを含みます。タイムスタンプフィールドはローカルタイムを Mmm dd hh:mm:ss フォーマットで表わします。

- Mmm は月を英語の略で表わしたものです。すなわち Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.です。
- dd は 2 つの数字で表わす日にちです。値が 10 以下の場合、最初の桁はスペースになります。(例えば Aug　7)
- hh:mm:ss はローカルタイムです。時間(hh)は 24 時間フォーマットで表記され、有効な入力値は 00 から 23 です。分(mm)と秒(ss)の入力値は 00 から 59 です。

2.10.1.3 MSG メッセージ部分

MSG の部分はメッセージを作成したプログラムの名前あるいはプロセス、そしてメッセージそのものテキストを含みます。MSG 部分は通常以下のフォーマットで表わします。
program [pid] : message text.

2.10.2 IETF-syslogメッセージ

このセクションではIETF-syslogプロトコル(RFC5424-5428 をご参照下さい)に従ってsyslog メッセージのフォーマットを説明します。シスログメッセージは以下のパーツを含みます。

- HEADER(PRI を含む)
- STRUCTURE-DATA
- MSG

以下はシスログメッセージのサンプルです。

```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - ID47 - BOM'su root' failed for lonvick on /dev/pts/8
```

メッセージは以下のフォーマットに相当します。

```
<priority>VERSION ISOTIMESTAMP HOSTNAME APPLICATION PID MESSAGEID STRUCTURED-DATA MSG
```

この例では Facility が 4 の値で、severity が 2 です。従って PRI は 34(4x8+2)です。VERSION は 1 です。メッセージは 2003 年 10 月 11 日、午前 10 時 14 分 15.003 秒に作成されました。メッセージはもともと"mymachine.example.com"として認識するホストから作成されました。
APP-NAME は'su'で PROCID は不明です。MSGID は"ID47"です。MSG は"'su root' failed for lonvick..."、UTF-8 でエンコードされます。エンコードは BOM で定義されます。メッセージには STRUCTURED-DATA(構造データ)が存在せず、TRUCTURED-DATA(構造データ)フィールドで"-"で示されます。MSG は"'su root' failed for lonvick...".です。

メッセージの Header(ヘッダー)部分は単純な ASCII フォーマットで、STRUCTURED-DATA(構造データ)部分のパラメータ値は UTF-8 でなければなりません。一方 MSG 部分は UTF-8 でなければなりません。メッセージの異なる部分は次のセクションで説明します。

2.10.2.1 PRI メッセージ部分

シスログメッセージの PRI の部分(Priority value として知られています)はメッセージの Facility(ファシリティ)と Severity(重要度)を表わします。Facility はメッセージを送信するシステムを表す部分で、severity はその重要度を表わします。Prioirty value は最初に Facility の数に 8 を掛けて Severity の数値を加えます。可能な facility と severity の値は以下の通りです。

注記
ファシリティコードは異なるプラットフォームで若干違うことがあります。
syslog-ng アプリケーションは数値としてもファシリティコードを受け取ります。

Numerical Code (数値)	Facility(ファシリティ)
0	カーネルメッセージ
1	ユーザーレベルのメッセージ
2	メールシステム
3	システムデーモン
4	セキュリティ/許可メッセージ
5	Syslogd による内部発生メッセージ
6	ラインプリンターサブシステム
7	ネットワークニュース サブシステム
8	UUCP サブシステム
9	クロックデーモン
10	セキュリティ/許可メッセージ
11	FTP デーモン
12	NTP サブシステム
13	ログ監査

Numerical Code（数値）	Facility（ファシリティ）
14	ログアラート
15	クロックデーモン
16-23	ローカル使用ファシリティ（local10-local7）

テーブル 2.3.シスログメッセージファシリティ

以下のテーブルリストは severity の値です。

Numerical Code（数値）	Severity（重要度）
0	Emergency: システムが使用不可能
1	Alert: 至急対応が必要
2	Critical: 重大な状況
3	Error: エラーの状況
4	Warning: 警告の状況
5	Notice: ノーマルだが重要な状況
6	Informational: 情報メッセージ
7	Debug:: デバッグレベルメッセージ

テーブル 2.4.シスログメッセージ重要度

2.10.2.2 Header(ヘッダー)メッセージ部分

Header（ヘッダー）部分は以下の要素を含みます。

■VERSION: シスログプロトコルスタンダードの Version 番号。現在は 1 だけになります。

■ISOTIMESTAMP: ISO 8601 互換スタンダードタイムスタンプフォーマット（yyyy-mm-ddThh:mm:ss+_ZONE）でメッセージを作成したときの時間。例えば、*2006-06-13T15:58:00.123+01:00*.

■HOSTNAME: 最初にメッセージを送ったマシン。

■APPLICATION: メッセージを作成したデバイスあるいはアプリケーション。

■PID: メッセージを送ったシスログアプリケーションのプロセスの名前あるいはプロセスの ID。メッセージを作成したアプリケーションのプロセス ID とは限らない。

■MESSAGEID: メッセージの ID ナンバー。

注記

syslog-ngアプリケーションは他のタイムスタンプフォーマット、例えばISO、拡張PIXフォーマットもサポートします。IETF-syslogプロトコルで使用するタイムスタンプはRFC3339 に由来し、ISO8601 をベースとしています。詳細については、The syslog-ng Premium Edition Administrator Guide.のthe ts_format()　optionをご参照ください。

2.10.2.3　STRUCTURED-DATA(構造化データ)　メッセージ部分

STRUCTURED-DATA(構造化データ)のメッセージの部分はシスログメッセージについてのメタ情報、あるいはトラフィックカウンタやIPアドレスのような、アプリケーション特定の情報を含みます。STRUCTURED-DATA(構造化データ)は括弧([ ]).で囲まれたデータのブロックから構成されます。すべてのブロックはブロックのID、1 つ以上の　パラメータ名=値　のペアを含みます。syslog-ngアプリケーションは自動的にシスログメッセージのSTRUCTURED-DATA(構造化データ)部分を解析し、マクロ(詳細は、The syslog-ng Premium Edition Administrator Guideを参照ください。)で参照できます。STRUCTURED-DATA(構造化データ)のブロックの例は以下のようになります。

```
[exampleSDID@0　iut="3"　eventSource="Application"　eventID="1011"][examplePriority@0class="high"]
```

2.10.2.4　MSGメッセージ部分

MSG 部分はメッセージそのもののテキストを含みます。BOM 文字がメッセージに表われる場合テキストのエンコードはUTF-8 でなければなりません。メッセージがBOM 文字を含まない場合、エンコードは unknown(不明)として扱います。通常 legacy(昔の)ソースから届いたメッセージはBOM 文字を含みません。

3　ウェルカムウィザードと最初のログイン

この章では、SSB 設定の最初のステップを説明していきます。まず、ハードウェアの梱包を解き、組み立て、電源を入れます。そして、SSB の外部インターフェイスをネットワークに接続するか、お持ちのコンピューターに SSB を直接接続して、SSB の設定ができる環境を整えます。

3.1　SSBへの初回ログイン

お使いのクライアントコンピュータから、Web ブラウザで SSB にアクセスすることが出来ます。

サポート対象の Web ブラウザとオペレーティングシステム

サポート対象ブラウザ
Mozilla Firefox 10、Microsoft Internet Explorer 8, 9
ブラウザは HTTPS 接続、JavaScript、cookie をサポートしている必要があります。JavaScript と cookie が有効であることをご確認ください。
他のテスト済みブラウザー　Mozilla FireFox　3.6、Google Chrome 17

注記

SSB はブラウザがサポートされていないか、JavaScript が無効の場合、警告メッセージを表示します。

サポート対象オペレーティングシステム
Microsoft Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows 7, Linux

SSBWeb インターフェイスへは、SSLv3 または TLSv1 暗号と強力な暗号アルゴリズムを使用してのみアクセスできます。

Windows Server 2008 R2 Enterprise 上の　Internet Explorer 8.0 を使用する場合は、Internet Explorer のコンテンツ アドバイザーを無効にします。コンテンツ アドバイザーを無効にするには、**ツール** > **インターネット オプション** > **コンテンツ** > **コンテンツ アドバイザー** > **無効にする** を選択します。

SSBにはローカルネットワークからアクセスすることができます。バージョン 2.1 からは、SSBはDHCPから自動的にIPアドレスを受信しようとします。自動的にIPアドレスを取得できなかった場合は、192.168.1.1 IPアドレスでHTTPS接続のリッスンを開始します。スイッチ設定やセキュリティ設定が、SSBがDHCPからIPアドレスを受け取ることを妨げる場合があることにご注意ください。SSBは、external（外部）インターフェイス（EXT）経由で接続を受信します（ネットワークインターフェイスに関する詳細については、2.5 ネットワークインターフェイスをご参照ください）。

ヒント

SSB コンソールは、外部インターフェイスがリッスンしている IP アドレスを表示します。

SSB が 192.168.1.1 アドレスでリッスンしている場合、192.168.1.0/24 サブネットがクライアントからアクセスできなければならないことにご注意ください。クライアントマシーンがサブネットの異なる（例えば、IP アドレスが 192.168.10.X）が同じネットワークセグメントに存在する場合、クライアントマシーンにエイリアス IP アドレスを指定するのが一番簡単です。クライアントマシーン上でエイリアス IP を作成すると、クライアントと SSB の両方が仮想的に同じサブネットに置かれるため、それらは互いに通信することができます。エイリアス IP は以下で説明する手順で作成できます。

- Microsoft Windowsでのエイリアスの作成に関する詳細については、3.1.1 エイリアスIPアドレスの作成（Microsoft Windows） をご参照ください。
- Linuxでのエイリアスの作成に関する詳細については、3.1.2 エイリアスIPアドレスの作成（Linux） をご参照ください。
- なんらかの理由でエイリアスインターフェイスを設定できない場合は、SSBのIPアドレスを変更することができます。詳細については、3.1.3 SSBのIPアドレスの変更 をご参照ください。

警告

ウェルカムウィザードへは、SSB の外部ネットワークインターフェイス経由でのみ、アクセスすることができます。管理インターフェイスがまだ設定されていないためです。

3.1.1 エイリアスIPアドレスの作成（Microsoft Windows）

目的 ：

ここでは、Microsoft Windows プラットフォームでエイリアス IP アドレスをネットワークインターフェイスに割り当てる方法について説明します。

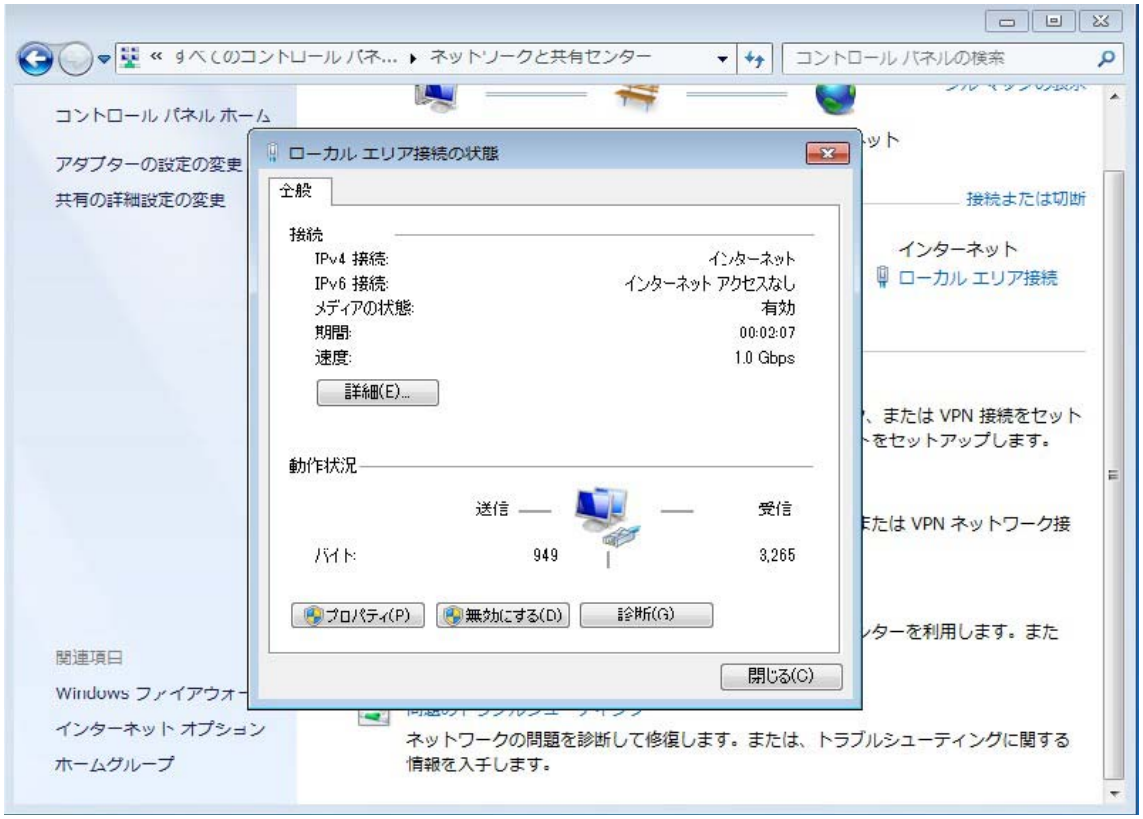
Step ：

Step 1. スタート ＞ コントロールパネル を選択します。

Step 2. **ネットワークと共有センター** を選択します。

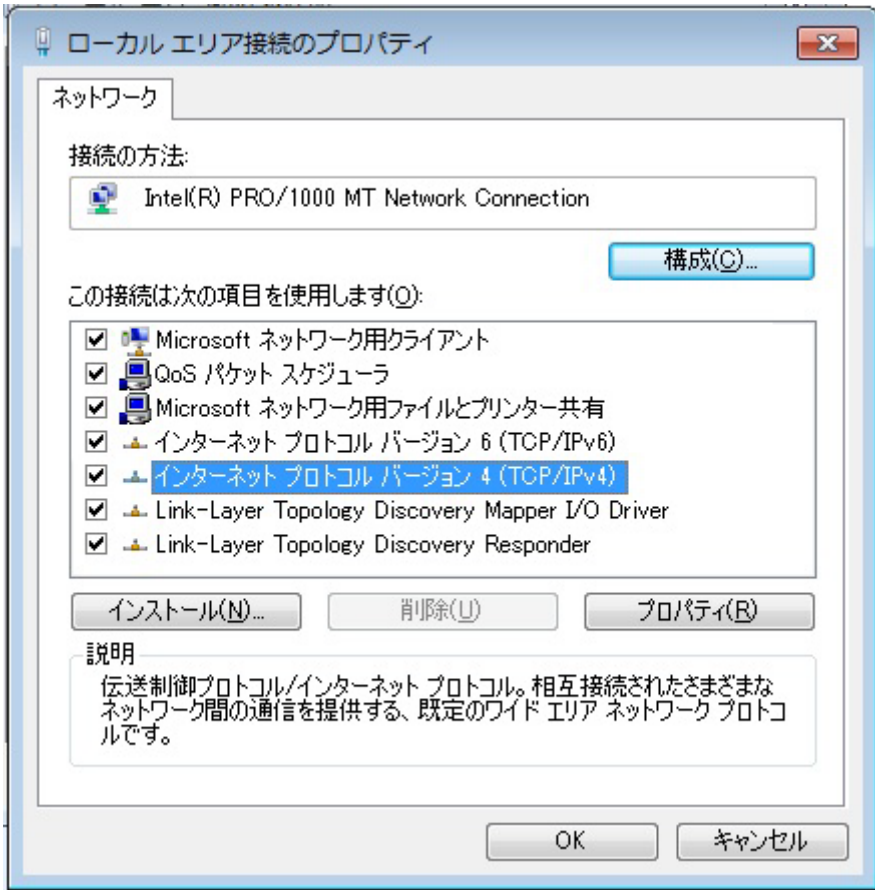
※Windows2003/XP は、「**ネットワーク接続**」

Step 3. ローカル **エリア接続** をダブルクリックし、**プロパティ** をクリックします。



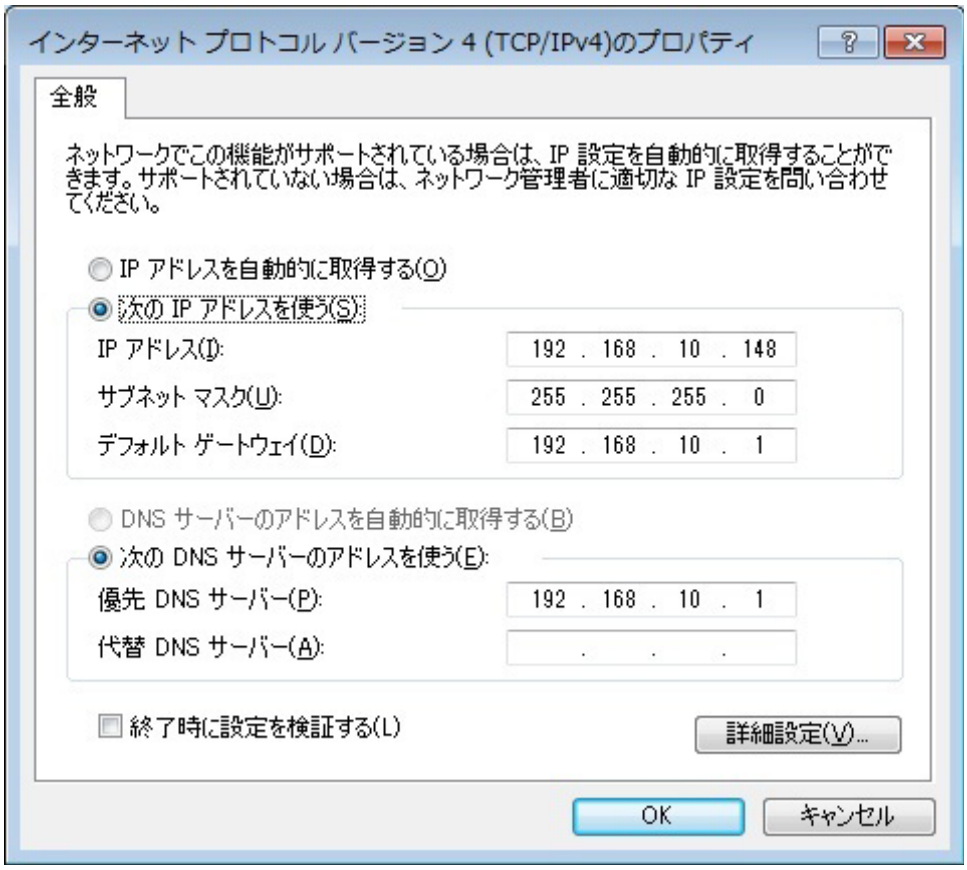
図表 3.1

Step 4. リストから、**インターネット プロトコル バージョン 4 (TCP/IPv4)** を選択し、**プロパティ**をクリックします。



図表 3.2

Step 5. **詳細設定** をクリックし、TCP/IP 詳細設定ウィンドウを開きます。



図表 3.3

Step 6. IP アドレスとサブネットマスクを入力し、 **追加** をクリックします。

図表 3.4

警告

192.168.1.0/24 IP アドレス範囲をお使いで、かつ DHCP が有効でない場合、192.168.1.1 と 192.168.1.2 アドレスが既に使用されていると、SSB は自動で IP アドレスを取得することができません。この場合は、ネットワークから SSB を切り離し、一般的なクロスケーブルを使ってコンピューターを外部インターフェイスへ直接つないでください。

3.1.2 エイリアスIPアドレスの作成（Linux）

目的 ：

ここでは、Linux プラットフォームでエイリアス IP アドレスをネットワークインターフェイスに割り当てる方法について説明します

Step ：

Step 1. ターミナルコンソール（例: `gnome-terminal, konsole, xterm` など）を開始します。

Step 2. root 権限で、以下のコマンドを投入します。

```
ifconfig <ethX>:0 192.168.1.2
```

`<ethX>` にはクライアントのネットワークインターフェイスの ID を入力します。通常は `eth0` か `eth1` です。

Step 3. ifconfig コマンドを発行します。`<ethX>:0` インターフェイスが出力に表示されます（`inet addr:192.168.1.2`）。

Step 4. ping –c 3 192.168.1.1 コマンドを発行し、SSB が利用可能であることを確認します。以下のような結果が表示されます。

```
user@computer:~$ ping -c 3 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp-seq=1 ttl=63 time=0.357 ms
64 bytes from 192.168.1.1: icmp-seq=2 ttl=63 time=0.306 ms
64 bytes from 192.168.1.1: icmp-seq=3 ttl=63 time=0.314 ms

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.306/0.325/0.357/0.030 ms
```

Step 5. ブラウザから `https://192.168.1.1` を開き証明書を承認すると、SSB のウェルカムウィザードが表示されます。

3.1.3 SSBのIPアドレスの変更

目的 ：

ここでは、任意のIPアドレス上で接続をリッスンするように、SSBを設定する方法について説明します。
なお、この手順は、SSBがIPアドレスをDHCP取得できた場合、あるいは、SSBが自動で192.168.1.1 のアドレスになった(DHCP取得に失敗した)場合に、クライアントコンピュータからWebブラウザでアクセスが可能な場合、省略できます。その際は手順 3.2　ウェルカムウィザードでのSSBの設定をするに進んでください。

警告

この設定は、SSBの初期設定前（ウェルカムウィザードの完了前）にのみ行ってください。構成済みSSBシステムのIPアドレスまたはネットワーク設定の変更に関する詳細については、4.3.1ネットワーク設定をご参照ください。

Step ：

Step 1. サーバーのローカルコンソールから SSB にアクセスします。

Step 2. 「username」は "root"、「password」は "default"でログインします。

Step 3. コンソールメニューで、**Shells > Core shell** を選択します。

Step 4. 以下のコマンドを使用して SSB の IP アドレスを変更します。
※< *IP アドレス*> は、実際に設定する IPv4 アドレスを入力します。
`ifconfig eth0 <`*IP アドレス*`> netmask 255.255.255.0`

Step 5. 以下のコマンドを使用してデフォルトゲートウェイを設定します。
`route add default gw <`*デフォルトゲートウェイの IP アドレス*`>`

Step 6. `exit` と入力し、コンソールメニューから **Logout** を選択します。

Step 7. ブラウザから https://<Step4 で設定した IP アドレス> を開き証明書を承認します。
SSB のウェルカムウィザードが表示されます。

3.2　ウェルカムウィザードでのSSBの設定をする

目的 ：

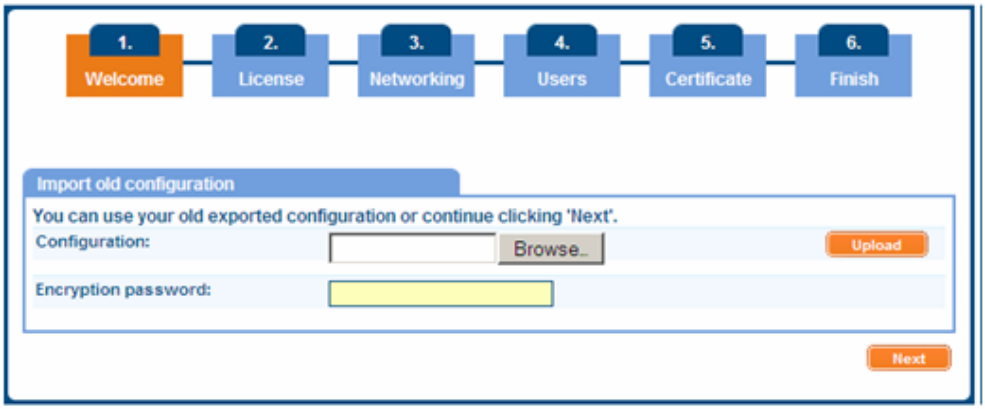
ウェルカムウィザードは SSB の基本設定作業をガイドします。全てのパラメータは、最終 Step の前にウィザードの **Back**（戻る）ボタンで戻って設定し直すか、後で SSB の Web インターフェイスから入って変更することができます。ここでは、ウェルカムウィザードでの設定手順を説明します。

Step ：

Step 1. ブラウザで、https://<SSB の外部インターフェイスアドレス>を開き、表示される証明書を承認します。SSB のウェルカムウィザードが表示されます。

ヒント:
「外部インターフェイス」の IP アドレスとは、①SSB が DHCP から取得した IP アドレス ②DHCP 取得に失敗した際の 192.168.1.1 ③手順 3.1.3 で設定した IP アドレスのいずれかです。

Step 2. SSB への初回ログインの場合は、「Next」をクリックします。



図表 3-5 ウェルカムウィザード

バックアップファイルから、既存の設定をインポートすることも可能です。システムリカバリー後にバックアップ設定を修復するときや、新しいデバイスに既存の SSB 設定を移行するときに、この機能を使用します。

注:設定ファイルのインポートを行わない場合は、このまま「Next」をクリックします。

Step a. **Browse** をクリックし、予めエクスポートした設定ファイルを選択します。

注記
GPG で暗号化されたコンフィグレーションを直接インポートすることはできません。ローカルで最初に復号される必要があります。

Step b. **Encryption passphrase**(暗号パスフレーズ)フィールドに設定をエクスポートしたときに設定したパスフレーズを入力します。(エクスポート時、パスワードを設定した場合のみ)

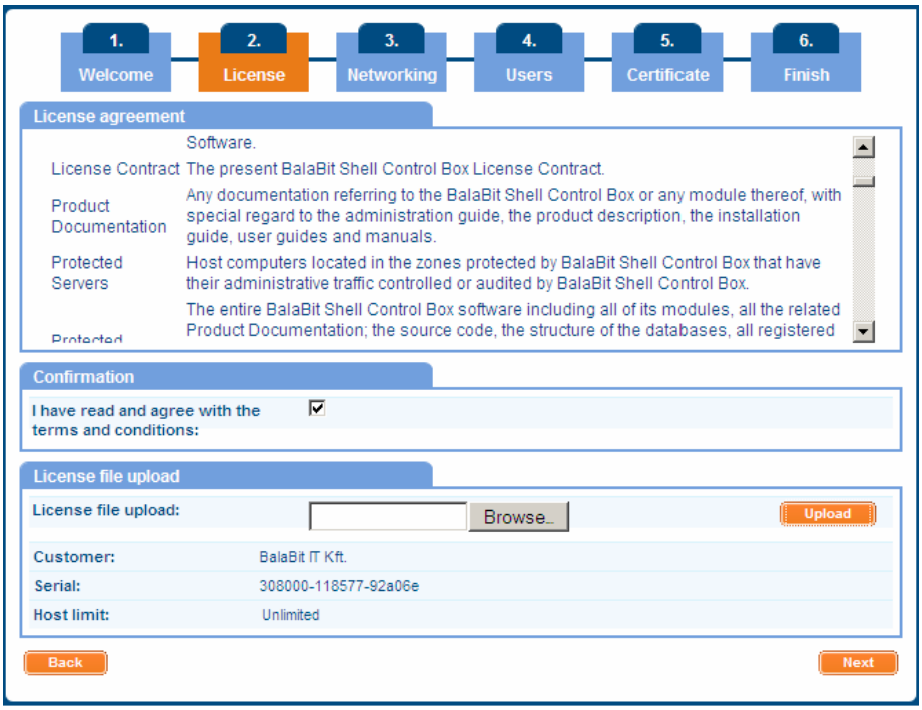
コンフィグレーションバックアップからコンフィグレーションをリストアする詳細については、プロシージャ 8.7 コンフィグレーションバックアップからコンフィグレーションをリストアする を参照してください。

Step c. **Import** (インポート)をクリックします。

警告

ある SSB から他の SSB へ設定をコピーする為にインポート機能を使用する際、移行先の SSB の IP アドレスを忘れずに設定し直してください。同じネットワーク上に同一の IP アドレスを持つデバイスが複数存在するとエラーになります。

Step 3.　エンドユーザーライセンスに同意し、SSB ライセンスをインストールします。

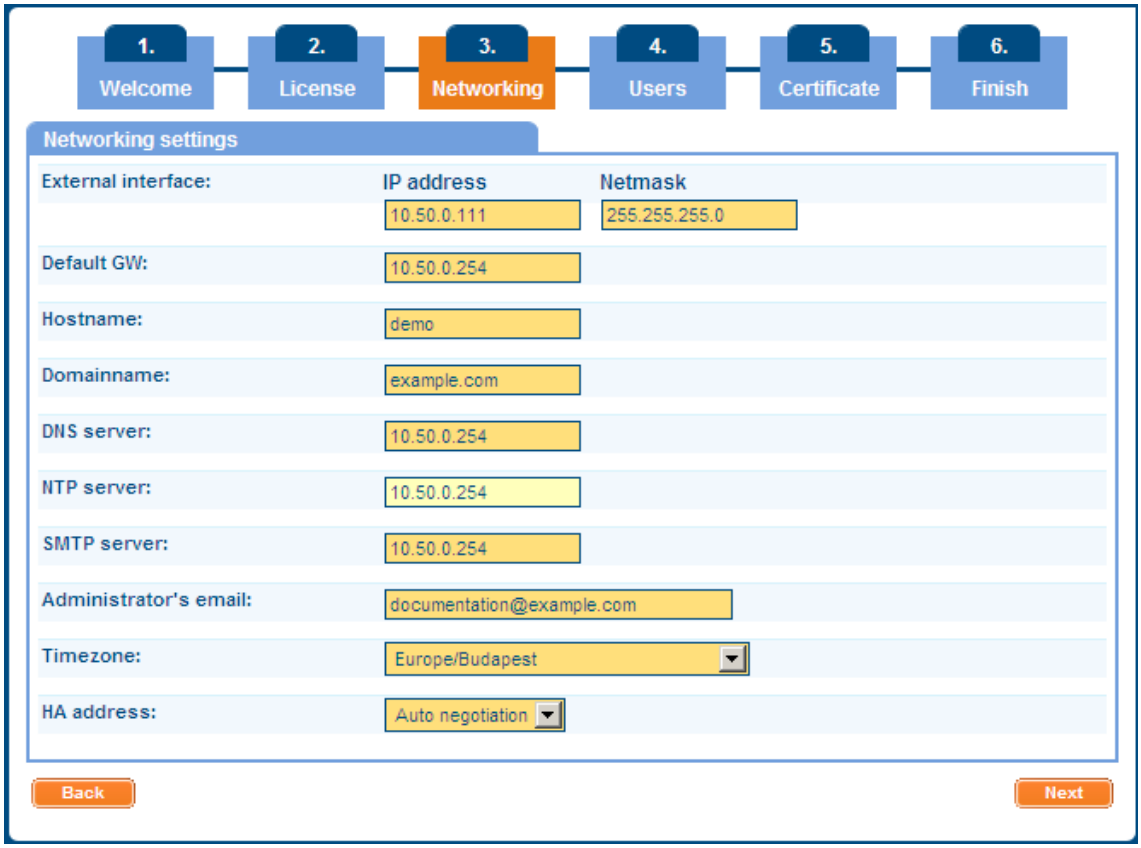


図表 3.6　エンドユーザ同意書及びライセンスキー

Step a.　License agreement（エンドユーザーライセンス同意書）を読み、Confirmation 欄の **I have read and agree with the terms and conditions**（この条項および条件を読み同意しました）のチェックボックスを選択します。

Step b.　**License file** upload（ライセンスファイルのアップロード）の**参照**をクリックして SSB のライセンスファイルを選択し、**Upload** をクリックします。

Step c.　**Next** をクリックします。



図表 3.7 ネットワーク初期設定

Step 4. 上記画面に移ります。フィールドに必要事項を入力し、ネットワーク設定を行います。各フィールドの意味は以下に説明します。

入力が必須のフィールドが空欄の場合、フィールドが赤色で表示されます。全てのパラメータは、後で SSB のインターフェイスから変更することができます。

Step a. **Hostname**(ホスト名):SSB を起動するマシンの名前(例: SSB)

Step b. **Domainname**(ドメイン名):ネットワークで使用されているドメインの名前

Step c. **DNS server**(DNS サーバー):ドメイン名解決のために使用されているネームサーバーの IP アドレス

Step d. **NTP server**(NTP サーバー):NTP サーバーの IP アドレスまたはホスト名

Step e. **SMTP server**(SMTP サーバー):E メール配信のために使用される SMTP サーバーの IP アドレスまたはホスト名

Step f. **Administrator's e-mail**(管理者の E メール):SSB 管理者の E メールアドレス

Step g. **Timezone**(タイムゾーン):SSB が稼動している場所が属する標準時

Step h. **External interface** – IP address(外部インターフェイス – IP アドレス):SSB の外部インターフェイスの IP アドレス(例: 192.168.1.1)。対応する物理サブネットの範囲から IP アドレスを選ぶこともできます。クライアントが外部

インターフェイスに接続するので、これにアクセスできなければなりません。

注記

ホストは、次の範囲に該当しないようにしてください。
`1.2.0.0/16`（SSB クラスターノード間のコミュニケーションに予約されています。）
`127.0.0.0/8` の（ローカルホスト IP アドレス）

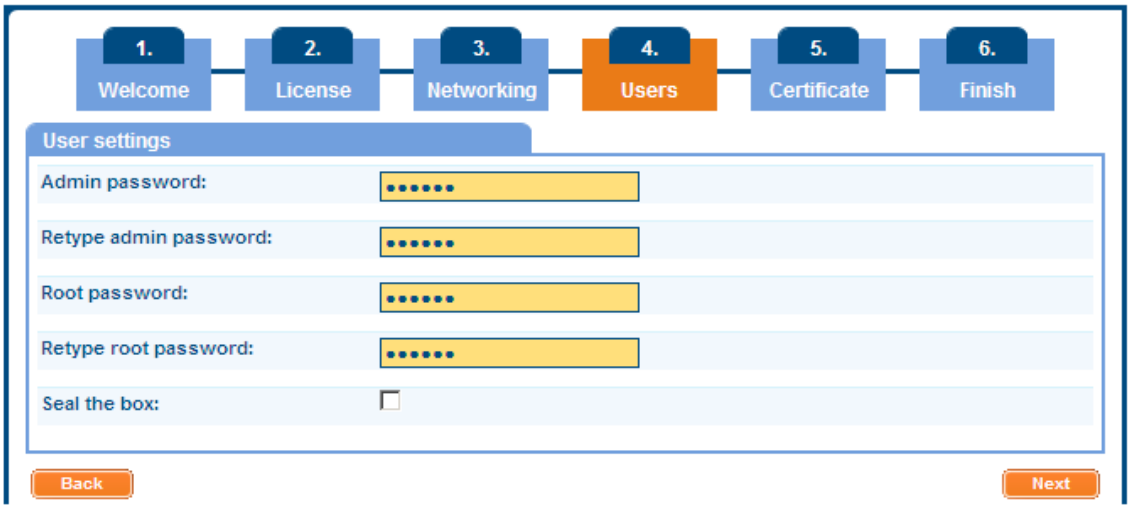
Step i. **External interface** – Netmask（外部インターフェイス – ネットマスク）
：お使いの IP ネットワークのサブネットマスクを入力します。

Step j. **Default GW**（デフォルトゲートウェイ）
：デフォルトゲートウェイの IP アドレス。複数のネットワークカードを使用している場合は、デフォルトゲートウェイは通常外部インターフェイスの方向にあります。

Step k. **HA address**（ハイアベイラビリティ アドレス）
：ハイアベイラビリティ（HA）インターフェイスの IP アドレス。このフィールドはシステム管理者から特に指定された場合を除き、**Auto negotiation**（自動ネゴシエーション）のままにしておきます。

Step l. すべてのパラメータの入力が終了したら、**Next** をクリックします。

Step 5. SSB にアクセスするために用いるパスワードを入力します。



図表 3.8 パスワード

注記：

SSB のパスワードには、以下の特殊文字を含めることができます。
`!"#$%&'()*+,-./:;<=>?@[\]^-`{|}`

Step a. **Admin password**: SSB に Web アクセスする、admin ユーザが使用するパスワードを入力します。

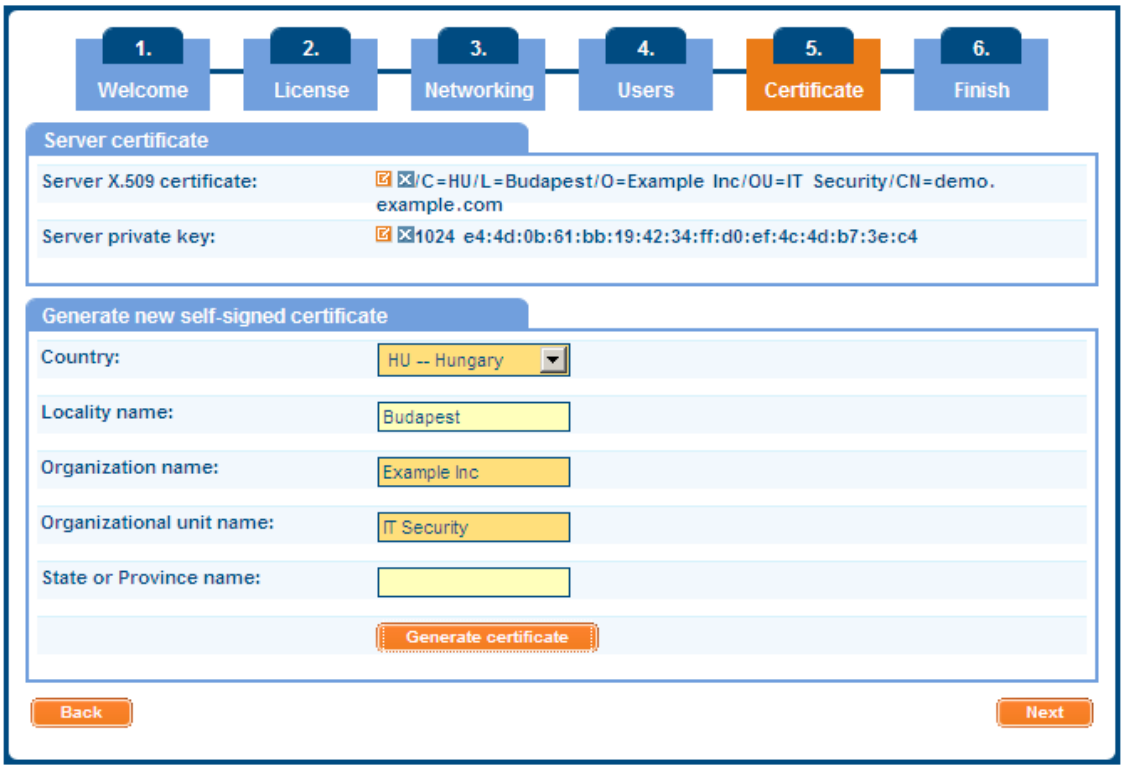
Step b. **Root password**: root 権限のパスワード。SSH でログインする場合、またはローカルコンソールで SSB を操作する場合に使用します。

注記

SSH を使用して SSB へアクセスする必要はほとんどありません。上級ユーザがトラブルシューティング目的でのみ使用することを推奨します。

Step c. ユーザがSSH経由でSSBにリモートアクセスすることを防ぎたい場合、またはSSBのrootパスワードを変更するのを防ぎたい場合は、**Seal the box**（このボックスを封印する）チェックボックスを選択します。シールドモードは後でWebインターフェイスから有効化することができます。詳細については、4.5.5シールドモードをご参照ください。

Step d. **Next** をクリックします。



図表 3.9 SSB の証明書作成

Step 6. 上記画面に変わります。SSB Web インターフェイスの証明書を作成またはアップロードします。この SSL 証明書は、管理者(admin ユーザ)が Web インターフェイスに

HTTPS 接続をする際の認証を行うために、表示されるものです。

自己署名証明書を作成するために、**Generate new self-signed certificate**(新しい自己署名証明書の生成)セクションのフィールドに入力し、**Generate Certificate**(証明書を生成)をクリックします。証明書は SSB アプライアンスによって自己署名されます(SSB のホスト名が issuer(発行元)と common name に使用されます)。

Step a. **Country**(国):国名(例: JP-Japan)

Step b. **Locality name**(地域名):SSB が稼動しているマシンのある市区町村名(例: Fuchu)

Step c. **Organization name**(組織名):SSB を所有している会社名(例: Example Inc.)

Step d. **Organization unit name**(部門名):SSB を所有している会社の部署名(例: IT Security Department)

Step e. **State or Province name**(都道府県名):SSB が稼動しているマシンのある都道府県名

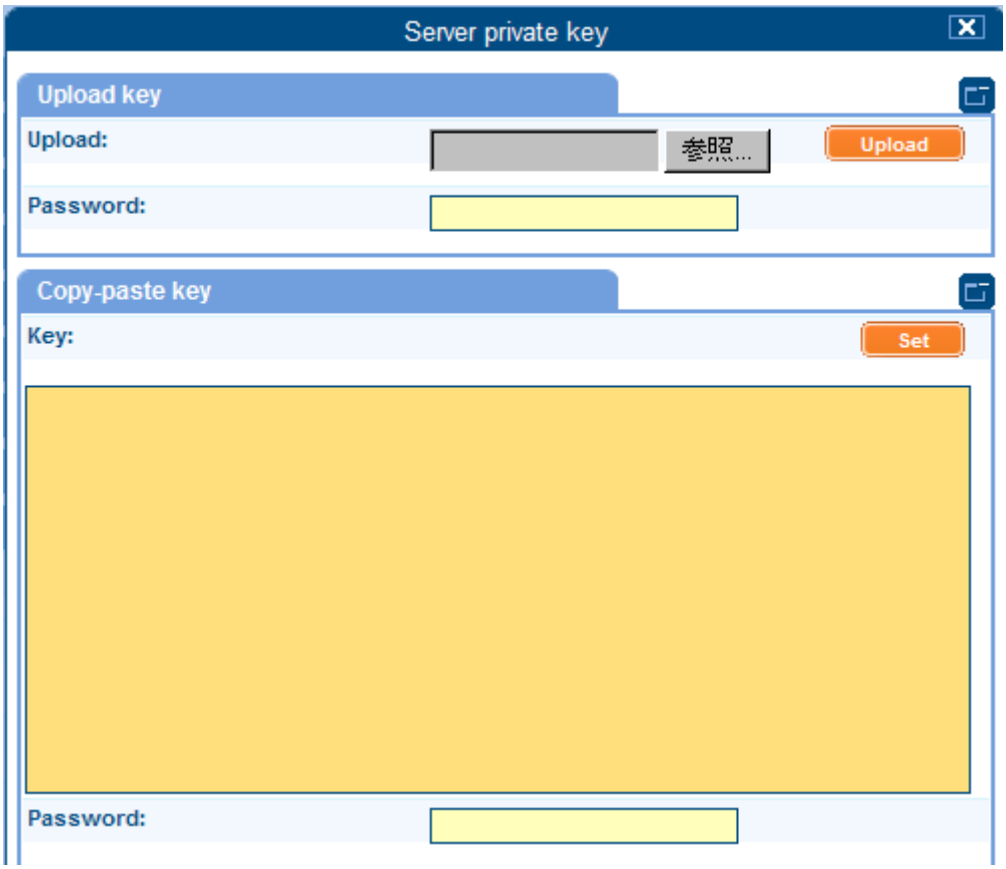
Step f. **Generate certificate**(生成)をクリックします。

外部の認証局による証明書をお使いになりたい場合は、"Server X.509 sertificate" 欄の をクリックし、以下手順で証明書をアップロードします。

図表 3.10 SSB の証明書アップロード画面

上記画面が現れますので、アップロードするファイルを選択して、
「**Upload**」をクリックします。

つぎに、"**Server Private Key**" 欄の をクリックし、秘密鍵をアップします。



図表 3.11 秘密鍵のアップロード

上記画面が出現します。アップロードする秘密鍵を選択します。

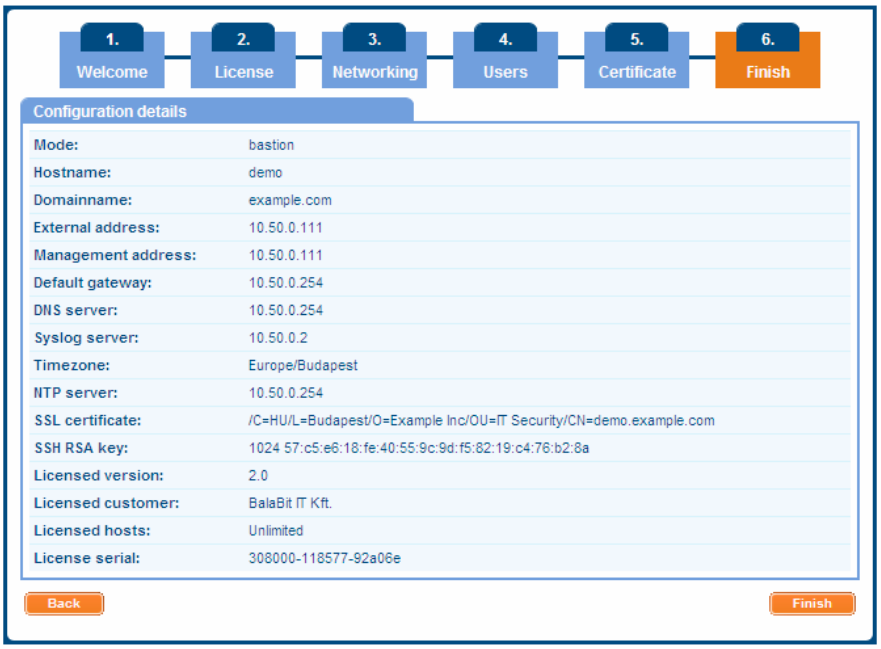
“**password**” 欄に、その秘密鍵をプロテクトしているパスワードを入力します。

“**Upload**” を**クリック**します。

注記

SSB は、PEM(RSA 及び DSA)、PUTTY、SSHCOM/Tectia 形式の秘密鍵を認識可能です。パスワード保護された秘密鍵もサポートしています。

Step 7. ここまでのステップで入力した設定値を再確認します。直前のステップで生成した証明書、RSA/SSH キー、ライセンス情報も表示されるので、あわせて確認します。



図表 3.12 設定値の再確認

Step 8. 正しいことが確認できたら、”**Finish**” をクリックします。

警告

“Finish” を押下した時点で、設定値が直ちに反映されます。したがってネットワークの設定を誤ると、ウェルカムウィザード終了後、SSB にアクセスができなくなります。

ここまで終了すると、”external interface” の IP アドレスにて、SSB への Web アクセスが可能になります。

Step 9. “Finish” をクリックすると、お使いの Web ブラウザは、自動的に SSB の external interface にリダイレクトされます。ユーザ名”admin” 、パスワードは、ウェルカムウィザードで設定したパスワードにて、ログインしてください。

3.3 SAN Storageへのアクセスを設定する

目的 :

SSB の、”SAN Connect” 版は、データの蓄積に、SAN ストレージモジュールを使用できます。ここでは、SSB から SAN へのアクセス設定手順を説明しています。

注 SSBからSANへのアクセスに関して詳しくは、4.6 SSBにおけるSANへのアクセス管理をご参照ください。

Step 1. ストレッジに関しての設定は全て、**Basic Settings > Storage** の順にクリックします。

注記

Basic Setteings > Storage メニューは、ストレージサポートを含むライセンス版でのみ表示されます。ストレージサポートを含むライセンスをご購入いただいたにもかかわらず、Storage メニューが現れない場合は、弊社までご連絡ください。

Step 2. (該当する場合のみ)お使いの SAN にネームサーバーが存在する場合、iSCSI のネームサーバーの IP アドレスを、**ISNS** 欄に入力します。

Step 3. SSB の iSCSI カードの IP アドレス及びサブネットマスクを入力します。この時、ストレージモジュールと SSB の iSCSI インターフェイスが、同一サブネット内に存在していることを確認してください。ハイアベイラビリティモードで SSB が稼動している場合は、スタンバイ側の SSB の iSCSI インターフェイスも設定することを忘れないでください。双方の SSB の iSCSI インターフェイスは、IP アドレスが重複しないよう注意してください。

Step 4. iSCSI ターゲットに、ストレージモジュールを追加します。**iSCSI Target** 欄に、必要な IP アドレスと IQN(=iSCSI 修飾名)全てを入力します。入力が終わると、ストレージとして使用可能な全てのボリュームが、LUN(論理ユニット番号)と WWN(ワールド・ワイド・ネーム)の情報付きで表示されます。

ストレージモジュールの IP アドレスと iSCSI 修飾名は、SSB ご購入時に発行されたライセンス証書に記載されております。

注記

ハイアベイラビリティモードでお使いの場合、または、ストレージモジュールに接続されているiSCSIインターフェイスが2ポートある場合、ボリュームのリストが複数回表示されます。しかし、全てのターゲットからアクセス可能とはなりません。これは仕様です。

Step 5. 必要な場合は、ボリュームのフォーマットを行います。Format を選択し、ボリューム名を入力します。フォーマットが終了すると、ボリューム上の使用可能空き領域の大きさが表示されます。

Step 6. ログスペースを生成する場合は、SANボリュームをログスペースとして割り当てます。ローカルディスク上に作成されたログスペースと、SAN上に構成されたログスペースが、同一のものとして扱われることに注意してください。双方がシェアー可能です。また、全てのログスペースは、独立したディレクトリ下に構成されます。ログスペース構築について詳しくは、5.2.4 SSBにカスタムメッセージスペースを構築するをご参照ください。

注記
単一のボリュームは複数のログスペースを保持することができますが、全てのログスペースは単一のボリューム上にしか構築できません。

4　SSBの管理と設定

SSB は、Web インターフェイスより設定を行います。変更は、**Commit**をクリックした時点で直ちに反映されます。その時点で設定を編集しているページあるいはタブのみ、変更が反映されます。つまり、ページまたはタブごとに、**Commit** が押下される必要があります。

目的:

この章では、SSB をどのように設定・管理・維持していくかを説明します。

■サポートしているブラウザについては、4.1サポートしているブラウザならびにOSをご参照ください。

■SSBにおけるWebインターフェイスの使い方は、4.2 Webインターフェイスの構成をご参照ください。

■SSBの基本的な設定(ネットワーク、システム監視、バックアップ設定等)は、4.3 Basic settings(基本設定)をご参照ください。

■ユーザアカウントと、ユーザに付与される特権に関しては、4.4ユーザ管理とアクセス制御をご参照ください。

■SSBの操作管理、リブート、アップデートならびにトラブルシューティングについては、4.5 SSBの管理をご参照ください。

4.1　サポートしているブラウザならびにOS

サポートしているブラウザ:

Mozilla FireFox　10

Internet Explorer　8 と 9

https 接続と、Java スクリプト、そして cookie をサポートしていることが必須です。Java スクリプトと、cookie が有効になっていることをご確認ください。

他のテスト済みブラウザ　Mozilla FireFox　3.6、Google Chrome 17

注記
お使いのブラウザがサポート外、あるいは Java スクリプトが無効になっている場合は、警告が表示されます。

サポートしているクライアントの OS:WindowsXP、Windows2003 Server、Windows Vista、Windows2008 Server、Windows7、Linux

SSB の Web インターフェイスは、SSLv3 または TLSv1 暗号化方式と、強力な暗号化アルゴリズムを実現できる環境からのみ、アクセス可能です。

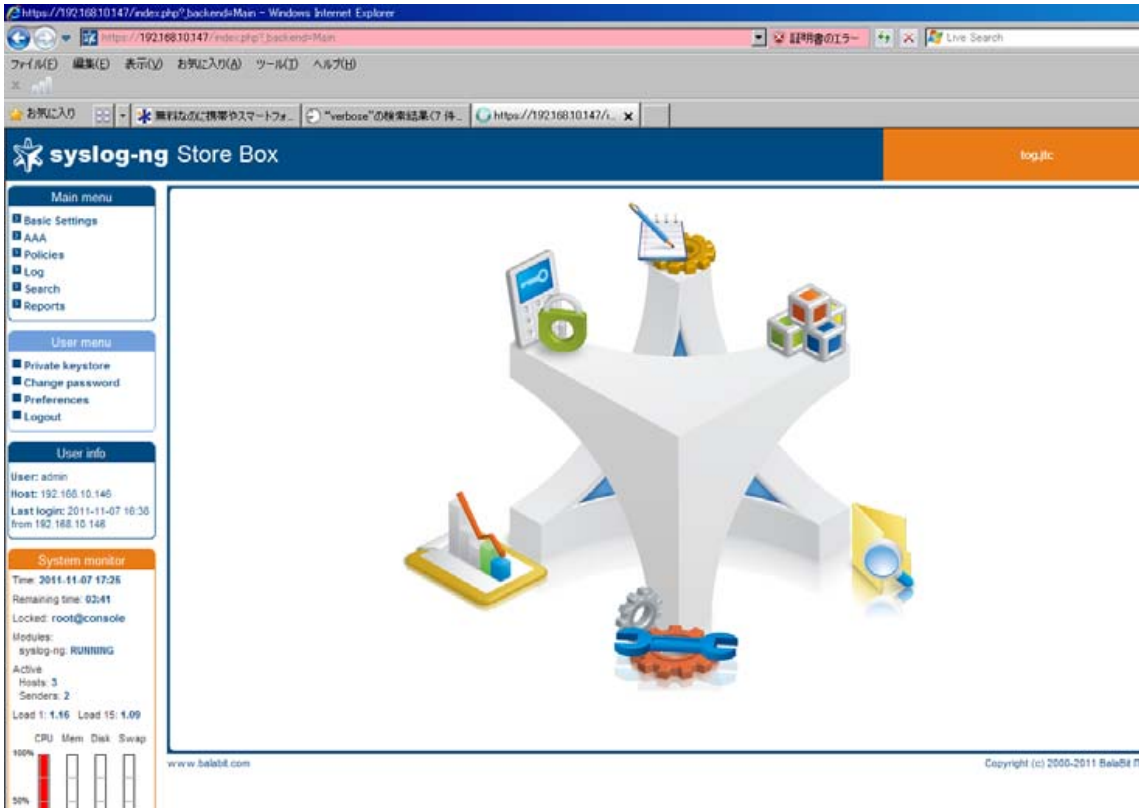
Windows2008 で SSB にアクセスする場合、「インターネットゾーン」のアクティブスクリプトを有効にする必要があります。そうでないと、SSB の Web インターフェイスは正しく機能しません。IE の、**ツール>インターネットオプション>セキュリティ>インターネットゾーン>レベルのカスタマイズ** の順にクリックし、アクティブスクリプトを有効にしてください。(これは、IE の他のバージョン、他のブラウザ、または他の Winodws 製品には当てはまりません。)

Windows Server 2008 R2 Enterprise 上の Internet Explorer 8.0 を使用する場合は、Internet Explorer のコンテンツ アドバイザーを無効にします。コンテンツアドバイザーを無効にするには、**ツール > インターネット オプション >コンテンツ > コンテンツ アドバイザー > 無効にする** を選択します。

4.2 Webインターフェイスの構成

SSB の Web インターフェイスは、以下の主要なセクションから構成されています。

- Main menu(メインメニュー):各メニューは、オプションを表示させるワークスペースを持つ、一つ以上のタブを含んでいます。メニュー項目横の▾をクリックすると、選択可能なタブが展開されます。



図表 4.1 Web インターフェイスの構成

- User menu(ユーザメニュー):ログインの際のパスワード変更、ログアウトへ進む、あるいは、パラメータの削除や、未保存の設定変更がある場合の警告ウィンドウを非表示にする、ツールティップ(パラメータ入力欄にマウスポインタをあてた際にポップアップされるヒント)を非表示にする、などの設定変更が、「Preferences」メニューから行えます。

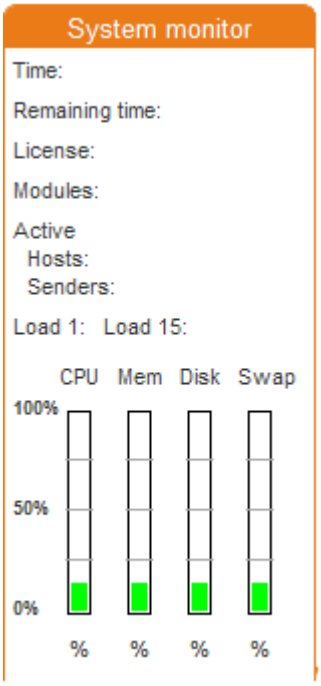
- User info(ユーザ情報):現在ログオンしているユーザの情報が表示されます。

  ■User:ユーザ名

  ■Host:ユーザがアクセスをしている、クライアントコンピュータの IP アドレス

  ■Last Login:ユーザがログインした最新の時刻と、IP アドレス

図表 4.2 ユーザメニューとユーザ情報



図表 4.3 システムモニター

- System monitor(システムモニター):SSB サーバーの状態と、システムヘルスの状態が表示されます。内容は以下のとおりです。

  ■**Time**:システム日付及び時刻

  ■**Remaining time**:Web インターフェイスのセッションが時間切れになるまでの残り時間

  ■**Modules**:SSB 上で稼動している syslog-ng デーモンの状態

  ■**License information**:ライセンスが期限切れ、あるいは評価版の期日終了している場合のみ表示

  ■**The status of the RAID devices**:ディスク間で同期を取っている最中のみ表示

■Active:

- **Hosts**:SSB が収集しているログの発生元の装置またはシステム数
- **Senders**:SSB の直前でログを送信してきている装置の数(リレーなど)

例

「hosts」と「sender」はどうカウントされるか

a. 300 のクライアントが全て、直接 SSB に対しログを送信している場合、「Hosts」、「Sender」ともに 300

b. 300 のクライアントが、3 台のリレーにログを送信し、その 3 台のリレー自身はログを吐いていない場合、「Hosts」は 300、「Sender」は 3

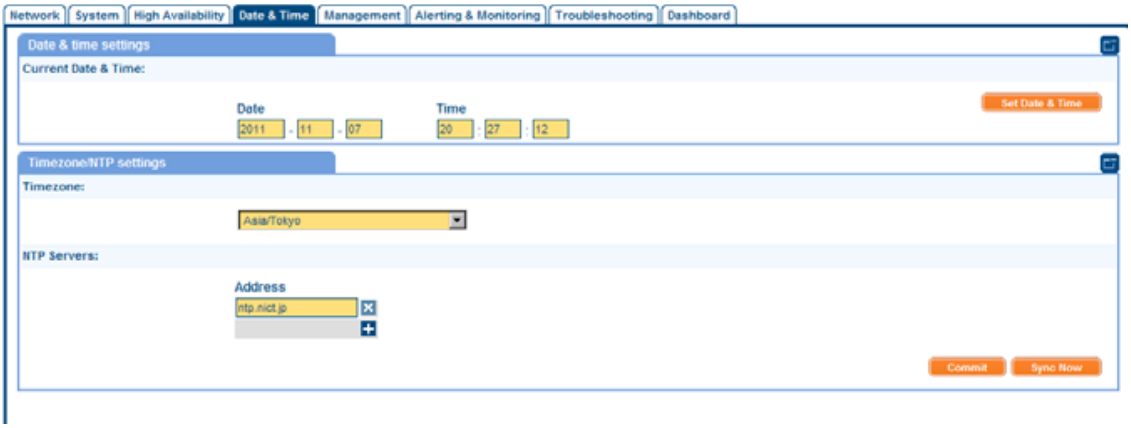
c. b のケースで、リレー自身もログを出力している場合、「Hosts」は 303、「Sender」は 3

- **HA**(ハイアベイラビリティ):ハイアベイラビリティ(高可用性)クラスターモードで SSB が稼動している場合、ステータスと、稼動しているマシンの ID が表示されます。冗長化ハートビートが設定されている場合には、状態が同じく表示されます。また、クラスターを構成するマシン同士が、データの同期を取っている最中は、そのステータス及び残り時間も表示されます。
- **Average system load during the**(以下の時間内のシステム平均負荷):
  Load1:過去 1 分間
  Load15:過去 15 分間
- **CPU、memory、disk、swapUSE**:グラフの棒の上にマウスポインタを当てると、詳細の情報がツールティップにて表示されます。また、**Basic Settings > Dashboard** とクリックすれば、より詳細なレポートが閲覧できます。

システムモニターは、SSBの現在の状況を表示します。これらの情報をさかのぼってみたい場合は、**Basic Settings > Dashboard** でレポートを見ます。詳細は、8.5 ステータス履歴と統計

をご参照ください。メインワークスペースの構成要素

Web インターフェイスのメインワークスペースは、現在選択されているメインメニュー項目に関連する設定値が表示されます。メインメニュー項目は、ひとつ以上のタブから構成されます。そのタブに含まれる設定項目は、青地の部分に表示されます。



図表 4.4 メインワークスペース

Commit：全てのページに、ひとつ以上の、オレンジ色のアクションボタンが配置されています。もっともよく使われるアクションボタンは、「Commit」です。設定項目に対する変更を反映させます。

/ 詳細の表示/非表示：設定を追加する欄の表示/非表示を切り替えます。

/入力欄の追加：新たな入力行、または入力欄を追加表示します。
(例：IP アドレス、新規ポリシー)

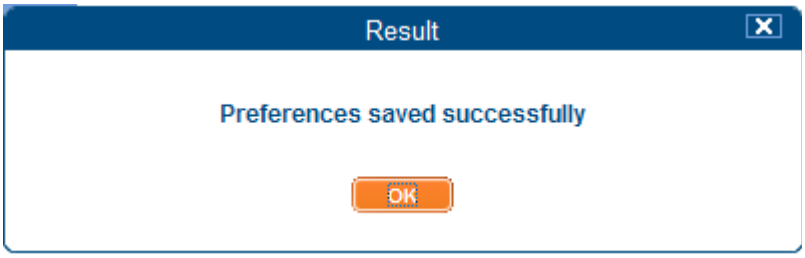
/ 入力欄の削除：入力行または入力欄を削除します。

/一覧表示/非表示：オプション一覧の表示/非表示を切り替えます。
(例：設定可能なレポート一覧)

既設定値の修正またはファイルのアップロード：既に設定済みの値を修正します。(例：ホストキー、一覧)またはファイルのアップロード時にも用います。(例：秘密鍵)これらを実行する際は、ポップアップウインドウが現れ、そこから実際のアクションを実行します。

▲/▼一覧中の項目の並べ替え：一覧の中の、項目順を入れ替えます。一覧に表示されている項目(例：接続の順番、チャネルポリシーの中の、許可されているチャネル)の順序は、大変重要です。SSB は、ポリシーを検査する際、一覧の上に位置する項目から、その条件に一致するか否かを評価していくからです。例えば、保護されているサーバーに対しクライアントが接続要求をしてきた場合、SSB は一覧の最初に位置する接続ポリシーを見て、クライアントの IP アドレス、サーバーの IP アドレス、そしてターゲットポートの番号が一致するかを判断します。(接続ポリシーの From、To、そしてポートフィールドを見ます)

Message window(メッセージウインドウ)：ユーザが実行したアクションに対して、SSB からの応答を表示します。(例："Configuration saved successfully" –設定の変更は正しく保存されました–)エラーメッセージも、ポップアップで表示されます。これら全ての、表示されるメッセージは、SSB のシステムログにも記録されます。ログを確認したい場合は、Basic Settings > Troubleshooting の順にクリックしてください。なお、アクションが成功した際に、ポップアップメッセージウインドウを自動で閉じるようにするには、**User menu > Preferences** の順にクリックし、**Autoclose successful commit messages**(成功した設定変更のメッセージを自動で閉じる)オプションにチェックを入れます。



図表 4.5 メッセージウインドウ

4.2.1 複数のユーザからのWeb経由のアクセスと、排他制御

複数の管理者(administrator)が、Webインターフェイスから SSBにアクセスすることは可能です。しかし、設定の変更を行えるのは、そのうちの 1 ユーザのみです。つまり、設定変更の権限を持つ、最初のユーザがSSBの設定メニュー(例:Basic Settings、AAA、Logs等)にアクセスした時点で、他のユーザに対して排他制御をすることを意味します。System Monitor欄に、現在、他のユーザをロックしている(設定の変更が可能な)管理者ユーザのユーザ名及びIPアドレスが表示されます。他の管理者ユーザは、排他している管理者ユーザがログアウトするか、セッションの時間切れになるまで待たなければなりません。しかし、設定変更を伴わない、Search(検索)や、Reporting(レポート)などのメニューにはアクセスできます。また、確認するのみであれば、設定内容にもアクセスできます。詳細は、4.4.6ユーザ権限とユーザグループを管理するをご参照ください。

注記
管理者権限を持つユーザが、ローカルコンソール、または SSH で SSB にアクセスしている場合、Webインターフェイスによる他のユーザのアクセスは完全にブロックされます。. また、Webインターフェイスからのアクセス同様、一定時間アクセスのないローカルコンソールからのあるいはリモートSSHアクセスは、タイムアウトしてセッションが切断されます。詳しくは、4.5.4SSBのコンソールにアクセスするをご参照ください。

4.3 Basic settings(基本設定)

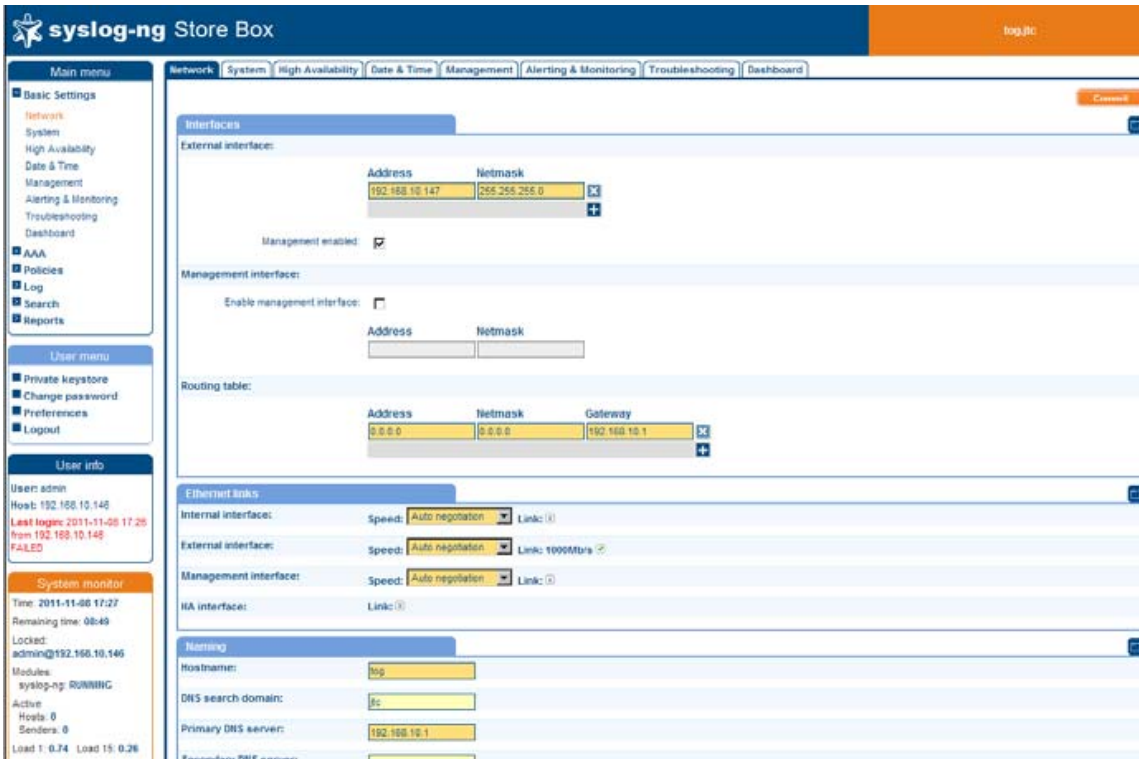
メインメニューの **Basic Settings** オプションにて、SSB ホストマシンの設定を行います。各項目は以下の部分に記載されています。

- ■ネットワークインターフェイス、名前解決、その他ネットワークに関連する設定に関しては、4.3.1ネットワーク設定
- ■SSBの取扱い(例:再起動方法)、新しいファームウェアまたはライセンスキーのアップロード、現在の設定のエクスポート等は、4.3.1ネットワーク設定
- ■システム時刻の設定、NTPサーバーとの時刻同期に関しては、4.3.2日付と時刻の設定
- ■SNMP及びE-Mailアラートの送信先に関しては、4.3.3 SNMPとEメールアラート
- ■システム監視とアラートに関しては、4.3.4 SSBのシステム監視設定
- ■データのアーカイブ及びバックアップに関しては、4.3.5データと設定のアーカイブとバックアップ

を、それぞれご参照ください。

4.3.1 ネットワーク設定

Network タブには、ネットワークインターフェイスと、ホスト名、DNS 等に関する設定項目が包含されています。



図表 4.6 ネットワーク設定

■**Interfaces > External interface**(外部インターフェイス)

クライアントからの接続インターフェイスとなる、IP アドレスとサブネットマスクを設定します。新たなエイリアス IP アドレス(エイリアスインターフェイスとも呼ばれます)を追加するには アイコンを、設定済みのインターフェイスを削除するには アイコンをクリックします。最低ひとつの外部インターフェイスが定義されている必要があります。管理インターフェイスが有効(Enable)になっていない場合は、SSB に対しては全て外部インターフェイス経由でのアクセスとなります。複数のインターフェイスが設定されている場合、最初に設定されている値が物理インターフェイスとみなされ、残りはエイリアスインターフェイスとみなされます。管理インターフェイスが有効になっていない場合、設定されている全ての外部インターフェイスからのアクセスが可能です。

オプションとして、管理インターフェイスをそのまま外部インターフェイスと兼ねさせる設定も可能です。「Management Enabled」のチェックを ON にします。

警告

「Management Enabled」を ON にし、かつ同じインターフェイス(例えば、eth:0)でエイリアスを設定した場合、SSB はもとの IP アドレスのみから管理アクセスを受付けます。

注記

ホストは、次の範囲に該当しないようにしてください。

`1.2.0.0/16`(SSB クラスターノード間のコミュニケーションに予約されています。)

`127.0.0.0/8` の(ローカルホスト IP アドレス)

注記

各インターフェイスごとに、速度が表示されています。(「Ethernet Links」セクション)速度を明示的に設定したい場合は、**Speed** プルダウンから選択できますが、上級ユーザ向けの設定項目です。なお、もともと装てんされていた SSB の NIC を交換してしまうと、この設定変更は効果がありません。

■**Interfaces > Management interface**(管理インターフェイス)

SSB に Web アクセスをするための IP アドレスとサブネットマスクを設定します。管理インターフェイスが設定されると、他の外部インターフェイスが設定され有効になっていない限り、SSB への Web アクセスはこのインターフェイス経由のみ可能となります。

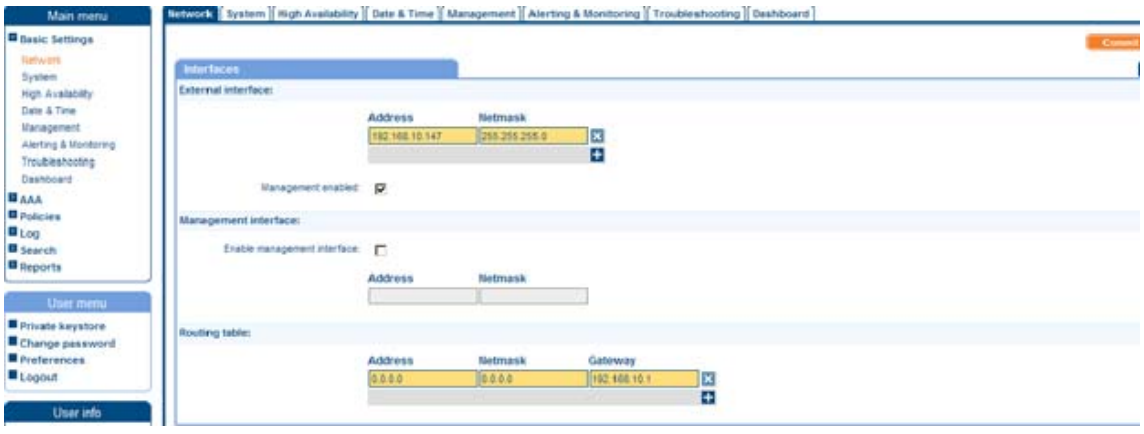
4.3.1.1 管理インターフェイスの設定

目的:

管理インターフェイスへの設定を変更する手順を説明します。

Step:

Step 1. **Basic Settings > Network > Interfaces** の順にクリックします。



図表 4.7 管理インターフェイスの設定

Step 2. **Management interface** フィールドで、"**Enable Management Interface**"

(管理インターフェイスを有効にする)にチェックを入れます。

Step 3. **Address** 欄に、管理インターフェイスの IP アドレスを入力します。

Step 4. **Netmask** 欄に、上記 IP アドレスのサブネットマスクを入力します。

Step 5.

警告

Commit を押下すると即座に、Web インターフェイスはここで設定した管理インターフェイス経由に切り替わります。**External interface** で、**Management Enalbed** を ON にしていない限り、これまでアクセスしていた外部インターフェイス経由でのアクセスはできなくなります。
LAN ケーブルが接続されていること、管理インターフェイスに設定するアドレスが、有効なネットワーク内に存在することを確認してください。
HA モードにおいて各インターフェイスがネットワークとの疎通が取れているかどうかは、**Basic Settings** > **Network** > **Ethernet links** > **HA interface** > **Link** 欄の、各インターフェイス欄の横に緑色チェックで示されています。

HA interface セクションは、ハイアベイラビリティインターフェイスにおいてリンクが検知された場合のみ、表示されます。

Commit をクリックします。

■**HA address**

ハイアベイラビリティのインターフェイスにおける IP アドレスを設定します。システム管理者からの要請がない場合は、**Auto negotiation** のままにしておきます。

注記

SSB バージョン 1.1.1 までは、ハイアベイラビリティの双方のクラスターが同時にブートしていました。1.2.4.1 のアドレスを持つノードが自動的にマスターになっていました。

■**Interfaces** > **Rouiting table**(ルーティングテーブル)

SSBがリモートネットワーク環境へパケットを送信する際、どのパスを経由させるかを判断するために、ルーティングテーブルを参照します。ルーティングテーブルに何も情報がない場合は、デフォルトゲートウェイに向けて送出します。ルーティングテーブルは、特定のホストまたはネットワーク向けに、静的ルートを設定したい場合に用います。また、もしinternal interface(内部インターフェイス)が複数のサブネットに接続されている場合は、ルーティングテーブルの設定は必須となります。デフォルトゲートウェイは、たいていは外部インターフェイスに向いているからです。新たにルーティング情報を追加するには、 アイコンをクリックして入力フィールドを展開させます。設定済みの情報を削除するには、 アイコンをクリックします。「ルート」とは、IPアドレス/サブネットマスク で指定したネットワークに向けて送出されるパケットがGateway向けに送信されることを意味します。

詳細な設定例については、4.3.1.2管理用途のトラフィックを、管理インターフェイスに集約するをご参照ください。

■**Naming** > **Hostname**(ホスト名)

SSB が稼動しているマシンの名称を定義します。

■ **Naming > Primary DNS server**(プライマリ DNS サーバー)サーバー
名前解決の際用いられる DNS のプライマリサーバーの IP アドレスを指定します。

■ **Naming > Secondary DNS server**(セカンダリ DNS サーバー)
プライマリサーバーが使用不能になった場合、名前解決に用いられるセカンダリサーバーの IP アドレスを指定します。

4.3.1.2 管理用途のトラフィックを、管理インターフェイスに集約する

目的:

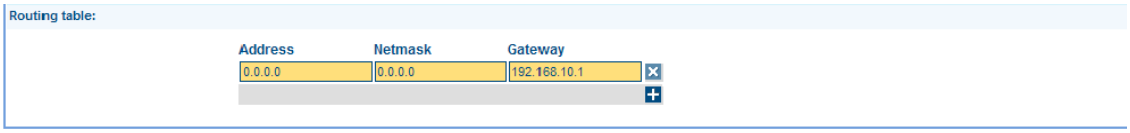
セキュリティ上の観点から、そして、ネットワーク上のトラフィック輻輳を回避するために、管理用途で発生するトラフィックは、全て管理インターフェイスに集約することを推奨します。例えば、設定変更のための Web インターフェイスへのアクセス、バックアップ/アーカイブに伴うトラフィック、リモートホストへのデータ転送、E メールまたは SNMP アラートで発生するトラフィックなどです。

警告

管理インターフェイスの設定が完了してから、この設定作業を行ってください。そうでないと、SSBから発せられたデータが失われる可能性があります。設定に関する詳細は、4.3.1.1管理インターフェイスの設定をご参照ください。

Step:

Step 1. 新たなルーティング情報を設定したい場合は、**Basic settings > Network > Interfaces** の順にクリックし、**Routing table** 欄で⊞をクリックします。



図表 4.8 ルーティング

Step 2. バックアップサーバーのIPアドレスを、**Address**欄に入力します。(4.3.5.1設定とデータのバックアップを定義するで指定します)

Step 3. 入力した IP アドレスのサブネットマスクを、**Netmask** 欄に入力します。

Step 4. 指定したサブネットワークのゲートウェイのアドレスを、**Gateway** 欄に入力します。

Step 5. **Commit** を押下します。

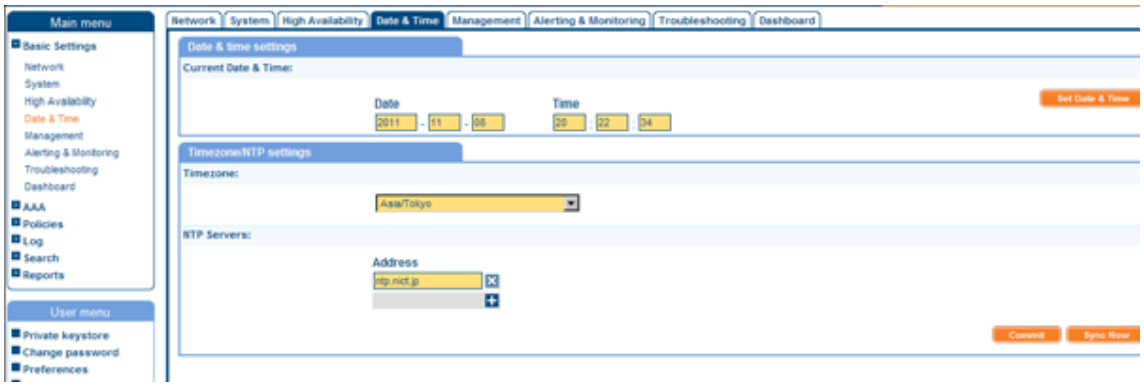
Step 6. 他にもバックアップサーバーが定義されている場合、1-5 のステップを繰り返します。

Step 7. SMTPサーバーの設定のために、1-5 のステップを実行します。(SMTPサーバーに関しては、4.3.3 SNMPとEメールアラートで設定しています)

Step 8. リモート転送のために、1-5 を実行します。(リモート転送に関しては、5.3 SSBからログメッセージを転送するで設定します)

4.3.2 日付と時刻の設定

日付と時刻に関する設定は、**Basic settings** > **Date & Time** の順にクリックします。



図表 4.9 日付と時刻の設定

警告

SSB の時刻を正確に合わせておくことは大変重要です。時刻の同期が取れなくなった場合、このページに警告メッセージが表示され、管理者にアラートが発せられます。

日付・時刻を明示的にセットしたい場合は、**Date and time settings** フィールド内の入力欄に日付・時刻を入力し、**Set Date & Time** をクリックします。

4.3.2.1 NTPサーバーによる時刻同期

目的:

時刻サーバーに時刻の同期を取る設定を説明します。

Step:

Step 1. **Timezone** フィールドから、地域の属するタイムゾーンを選択します。

Step 2. **Address** フィールドに、NTP サーバーの IP アドレスを入力します。

Step 3. **Commit** を押下します。

Step 4. NTP サーバーを追加する場合は を、設定値を削除する場合はをクリックします。

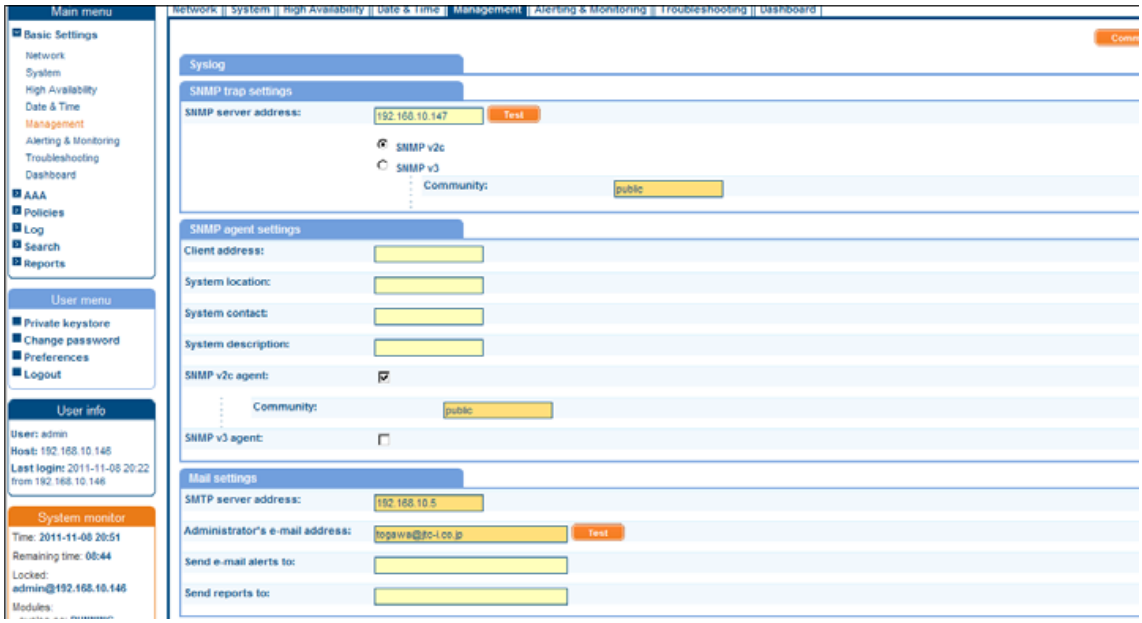
注記

システム時刻と SSB の保持している時刻との乖離が大きい場合等、NTP サーバーとの同期に時間がかかる場合があります。その際は **Sync now** をクリックし、SNTP サーバーと即座に同期を取ってください。

ハイアベイラビリティモードで二つのマシンが稼動している場合、**Sync now** ボタンではなく、**Sync_Master** ボタンになります。これは、マスターノードを NTP サーバーと同期させます。マスター～スレーブノード間の時刻を同期するには、**Sync Slave to Master** を押下します。

4.3.3 SNMPとEメールアラート

E メールアラートに関する設定を行うには、**Basic Settings > Management** の順にクリックします。



図表 4.10 SNMP と E メールアラートの設定

4.3.3.1 Eメールアラートの設定

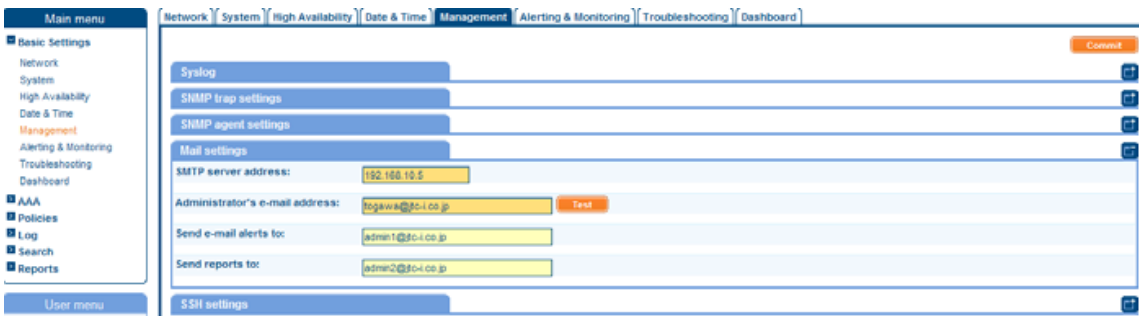
目的:

E メールアラートに関する設定方法の説明です。

Step:

Step 1. **Basic Settings > Management > Mail settings** の順にクリックします。

Step 2. **SMTP server address** 欄に、メールサーバーの IP アドレスを入力します。



図表 4.11 E メールの設定

Step 3. **Administrator's e-mail address** 欄に、管理者の E メールアドレスを入力します。SSB は、システムイベント関連の通知メールをこのアドレスに向けて送信します。ただし、監視アラートとレポートのメールは含まれません。

Step 4. **Send e-mail alerts** 欄に、管理者の E メールアドレスを入力します。SSB は、監視アラートをこのアドレスに向けて送信します。

Step 5. **Send reports**欄に、トラフィックレポートを受信したい人のEメールアドレスを入力します。レポートに関して詳細は、6.8レポートをご参照ください。

警告

アラート E メールを得るためには、このフィールドにメールアドレスを入れてください。これらの設定が正しくないとアラート送信は失敗します。デフォルトでは、アラートメールアドレスは、管理者メールアドレスにフォールバックしません。

Step 6. **Commit** をクリックします。

Step 7. **Test**をクリックし、送信テストを行います。正しく送信されない場合、SSBからメールサーバーに疎通が取れていない可能性があります。詳しくは 8 章 トラブルシューティングをご参照ください。

Step 8. **Basic Settings > Alerting & Monitoring**の順にクリックし、どのような状況において、SSBからのアラートメールを受信するかを設定します。詳しくは、4.3.4 SSBのシステム監視設定をご参照ください。

Step 9. **Comiit** をクリックします。

4.3.3.2 SNMPアラートを設定する

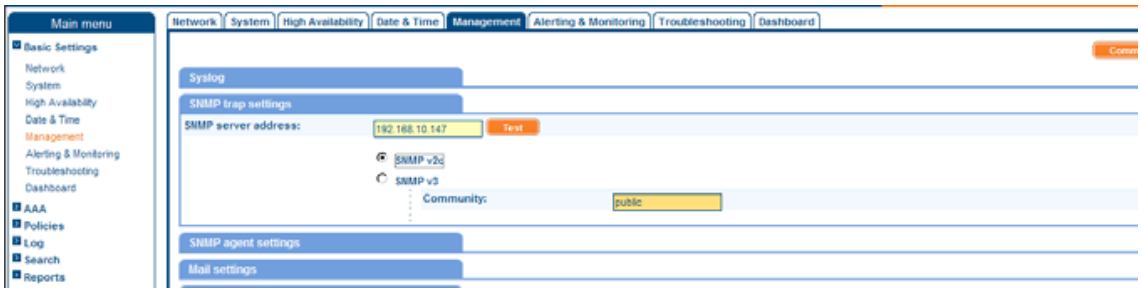
目的:

SSB は、監視サーバーに向けて SNMP 経由でアラートを送信することが可能です。SNMP によるアラート送信の設定方法を説明します。

Step:

Step 1. **Basic Settings > Management > SNMP trap settings** の順にクリックします。

Step 2. **SNMP server address** 欄に、SNMP サーバーの IP アドレスまたはホスト名を入力します。

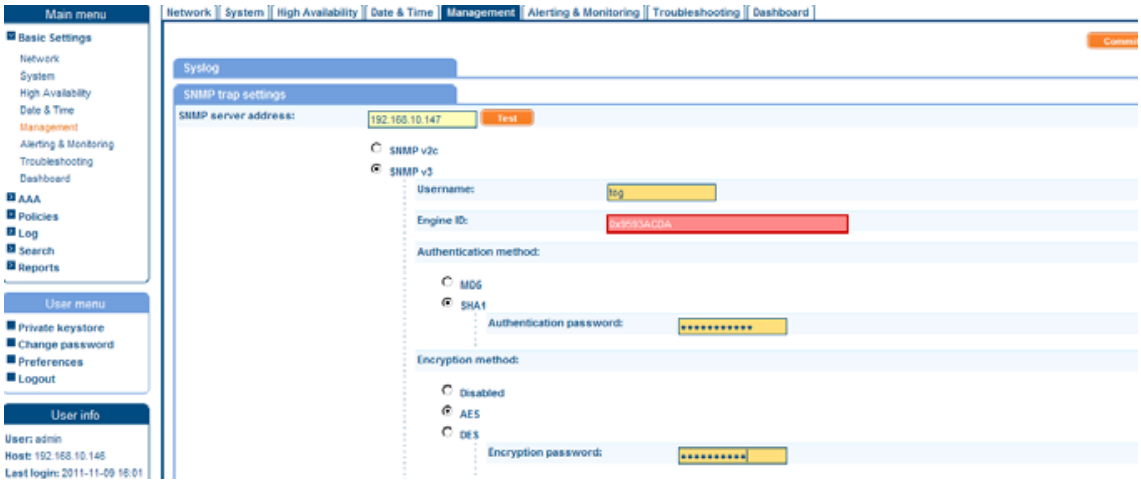


図表 4.12　SNMP アラートの設定

Step 3.　SNMP のバージョンを選択します。

■ SNMP v2 をお使いになるのであれば、**SNMP v2** を選択し、コミュニティ名を **Community** 欄に入力します。

■ SNMP v3 をお使いなら、**SNMP v3** を選択します。SNMP v3 に関するパラメータの入力欄が展開されるので、以下手順で入力を完了させます。



図表 4.13　v3c による SNMP アラートの設定

Step a.　**Username** 欄に、ユーザ名を入力します。

Step b.　**Engine ID** 欄に、SNMP v3 のエンジン ID を入力します。エンジン ID は、最低 10 桁の 16 進数表記で、必ず「0x」で始まります。例：0xABABABABAB

Step c.　**Authentication method** 欄で、認証方法(例：MD5、SHA1)を選択します。

Step d.　**Authentication password** 欄に、認証で用いるパスワードを入力します。

Step e.　**Encryption method** 欄で、暗号化の方法(例：Disabled、DES、AES)を選択します。

Step f.　**Encryption password** 欄に、暗号化で用いるパスワードを入力します。

Step 4.　**Commit** をクリックします。

Step 5.　**Basic Settings Alerting & Monitoring**の順にクリックし、どのような状況でSSBがSNMPアラートを送出するかを選択します。詳細は、4.3.4 SSBのシステム監視設定を

ご参照ください。

Step 6. **Commit** をクリックします。

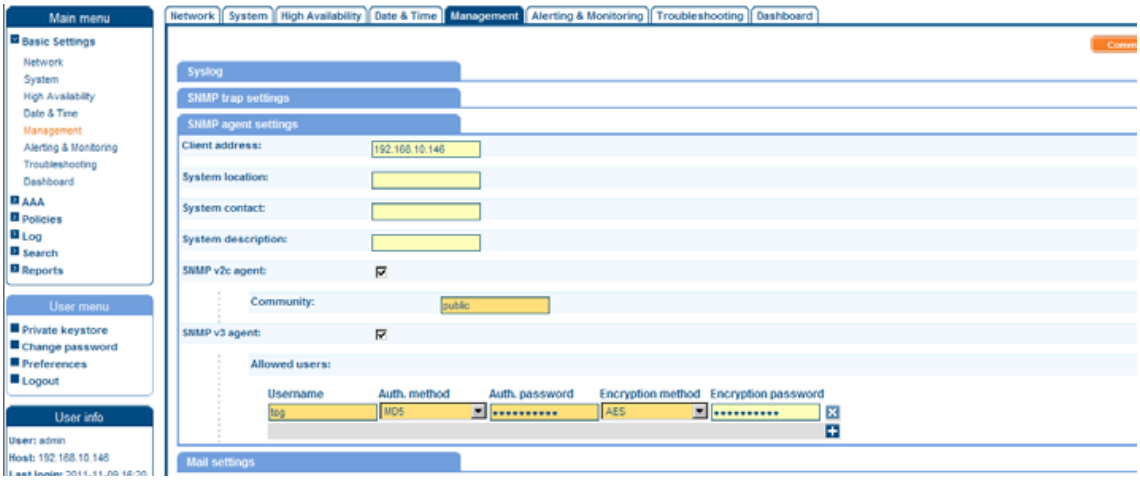
4.3.3.3 エージェントを使ってSSBのステータス情報を得る

目的:

外部のSNMPエージェントは、SSBの状態を問合せることができます。問合せができるクライアントを設定する手順を説明します。

Step;

Step 1. **Basic Settings** > **Management** > **SNMP agent settings** の順にクリックします。



図表 4.14 SNMP エージェントからのアクセスを設定

Step 2. SNMP 経由で、SSB の状態は動的に問合せされます。デフォルトでは、どのホストからも問合せが発せられます。問合せを受け付けるホストをひとつに絞りたい場合は、**Client address** 欄に、そのホストの IP アドレスを入力します。

Step 3. オプションとして、**System location**、**System contact**、**System description** 欄に入力することにより、SNMP サーバーに関する詳細情報を定義することができます。

Step 4. お使いになる SNMP のバージョンを選択します。

- SNMP v2 をお使いになる場合、SNMP V2c agent を選択し、Community 欄にコミュニティ名を入力します。
- SNMP v3 をお使いになる場合、SNMP v3 agent を選択します。v3 に関連するパラメータの入力欄が展開されるので、以下の通り入力をしていきます。

Step a. ＋をクリックします。

Step b. **Username** 欄に、SNMP エンティティが使用しているユーザ名を入力します。

Step c. **Auth.method** 欄で、認証方法(MD5、SHA1)を選択します。

Step d. **Auth.password** 欄に、SNMP エージェントが用いているパスワードを入力します。

Step e. **Encryption method** 欄で、暗号化方法(Disabled、DES、AES)を選択します。

Step f. **Encryption password** 欄に、暗号化で用いるパスワードを入力します。

Step g. さらにエンティティを追加する場合、 をクリックします。

Step 5. **Commit** をクリックします。

4.3.4 SSBのシステム監視設定

SSB は、ハードウェア及びその環境に関する、数々のパラメータを継続的に監視しています。設定が閾値に近くなると、(値は、各項目の **Maximum** 欄に定義されている)SSB は管理者に向け、E メール及び SNMP アラートを発し警告します。

SSB は、デフォルトでは SNMP アラートを管理インターフェイス経由で送信します。管理インターフェイスが設定(有効化)されていない場合のみ、外部インターフェイス経由で送信します。SSB は、SNMP v2c と SNMP v3 をサポートします。**Management** タブにて定義されている SNMP サーバーは、SSB の状態を問合せすることができます。

ヒント

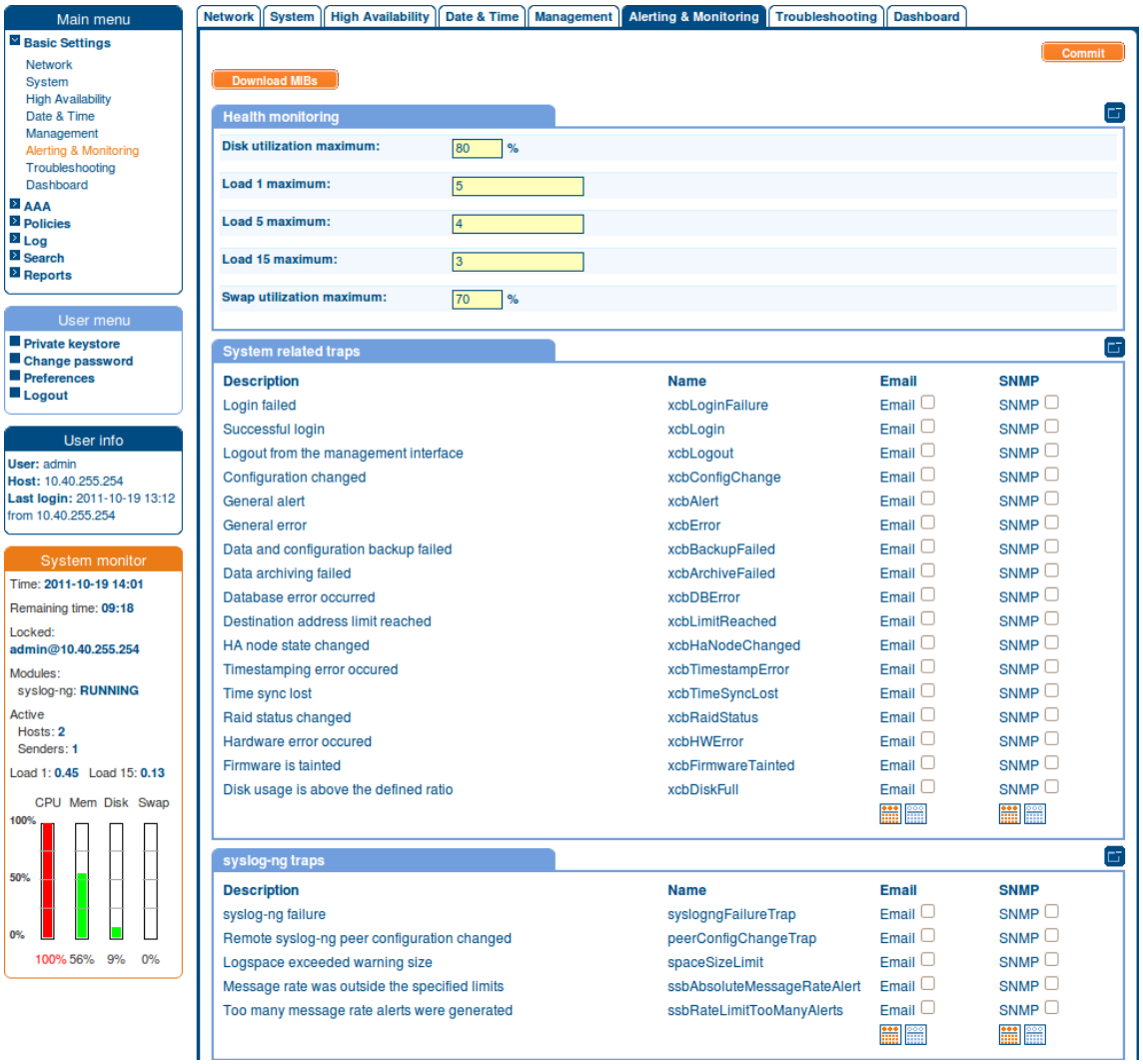
お使いの監視システムが SSB の SNMP アラートを検知できるよう、SSB 独自の MIB をインポートしておいてください。以下に示す URL から、両方の MIB をダウンロードし、お使いの監視システムにインポートしてください。

http://www.balabit.com/dl/SSB-SNMP-MIB.txt

http://www.balabit.com/dl/BALABIT-SNMP-MIB.txt

http://www.balabit.com/dl/XCB-SNMP-MIB.txt

詳細は、お使いの監視システムのドキュメントをご参照ください。



図表 4.15　SNMP と E メールアラートの設定

4.3.4.1　　監視の設定

目的:

システム監視に関する項目を設定する方法を説明します。

Step:

Step 1.　Basic Settings > Alerting & Monitoring の順にクリックします。

Step 2.　デフォルトの閾値は、ほとんどのご使用環境に適合します。必要なときのみ、閾値を変更してください。

Step 3.　**Commit** をクリックします。

Step 4.　**Basinc Settings > Management** の順にクリックし、SNMP 及びメールの設定が正しいかどうか、再度確認してください。SSB は、設定された E メールアドレスと SNMP サーバーにのみ、アラートを送信します。

警告

アラートメールを得るには、このフィールドに E メールアドレスを入力してください。この設定が正しくない場合、送信は失敗します。なぜなら、アラートメールアドレスは管理者のメールアドレスにデフォルトではフォールバックしないからです。。

以下に記述するセクションは、アラート受信が可能なパラメータに関して説明しています。

■システムヘルスのアラートに関しては、4.3.4.2システムヘルス監視

システム監視のアラートに関しては、4.3.4.5 システム関連のトラップ

■シスログ関連のアラートに関しては、4.3.4.6 Syslog-ngに関するアラート

を、それぞれご参照ください。

4.3.4.2 システムヘルス監視

■Disk Utilization maximum:
ハードディスク内の、使用可能な空き領域。ログファイルが設定された値以上の領域を使おうとすると、SSBはアラートを送信します。バックアップサーバーの空き領域に、ログファイルをアーカイブしてください。詳しくは、4.3.5.2収集したログデータのアーカイブをご参照ください。

注記

アラートメッセージには、実際のディスク使用率が含まれます。設定の上限値でないことに注意してください。例えば、ディスク使用率が 10%を越えた際にアラートを出すと設定したとします。ここで使用率が 17%になったとすると、SSB は次のようなアラートメッセージを発します。"less than 90 % free"これは、使用されているディスク領域が合計で 10%を超えたことを示しています。

■Load 1|5|15 maximum:
過去 1・5・15 分間の、SSB の平均システム負荷を設定します。Swap utilization maximum:
SSB が使用するスワップ領域を設定します。設定値以上のスワップ領域を SSB が
使おうとすると、アラートを送信します。

警告

SNMP やメールの設定等が誤っていると、アラートが正しく送信
されません。

4.3.4.3 ディスクスペース飽和防止手順

目的:

ディスクがいっぱいになるのを防止する方法を説明します。

Step:

Step 1. Basic Settings > Management > Disk space fill up prevention の順にクリックします。

Step 2. 最大ディスク使用量をパーセントで該当のフィールドに設定して下さい。ディスクスペースが設定したリミットを超えて使用されると、SSB は全てのクライアントを切断します。0 を入力すると、この機能がオフになります。デフォルト値は 0 です。

Step 3. オプション:ディスク使用がリミットを超えた時、全ての設定されたアーカイブ/クリーンアップジョブが自動的にスタートするようにするためには、**Automatically start archiving** オプションを有効にしてください。

注記

ひとつもアーカイブポリシーが存在しない場合は、このオプションを有効にしても自動アーカイブは始まりません。

Step 4. **Basic Settings > Alerting & Monitoring > System related traps** の順にクリックし、**Disk usage is above the defined ratio.**アラートを有効にします。

Step 5. **Commit** ボタンをクリックします。

4.3.4.4 メッセージレートアラートの設定

目的:

メッセージレートアラートによって、SSB の以下の異常を検出できます。

■SSB 内の Syslog-ng が停止した。

■クライアント/サイトの内の一つがログを送信していない。

■クライアント/サイトの内の一つがおそらく必要でない非常に多いログを送信している。

メッセージレートアラーティングは、Souces,Spaces,Destinations(リモート、またはローカル)に設定可能です。

Step:

Step 1. Log をクリックし、Sources,Spaces,または Destinations を選択します。.

Step 2. **Message rate alerting** を有効にします。

Step 3. Sources の場合、以下のカウントが計測できます。

■Messages.メッセージ数

■Messages/ sender.送信者【ラストホップ】ごとのメッセージ数

■Messages/ hostname.メッセージ内のホスト名に基づいたホストごとのメッセージ数

Spaces または宛先の場合、カウンターはメッセージ数です。

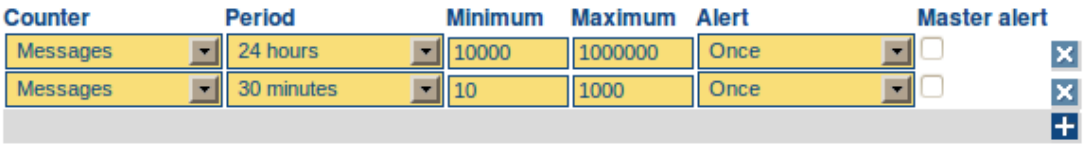
Step 4. 計測される期間(5 分から 24 時間)を選択してください。

Step 5. 正常と判断されるレンジを **Minimum** と **Maximum** フィールドに入力してください。

Step 6. **Alert** フィールドでアラート頻度を選択してください。**Once**:ひとつのアラートのみ送信(そして、問題が解決した後、"Fixed メッセージ"を送信)。**Always**:警告結果がセットしたレンジをはずれた場合、その都度アラートを送信。

例 4.2 早期のアラート(early time alert)を作成する

早期のアラートを作成したい場合は、マスターアラートでは無い通常アラートを非常に低い Minimum メッセージ数と低いチェック間隔で作成します。



図表 4.16 早期アラートの作成

Step 7. もし、一つ以上のメッセージレートアラートを設定した場合、マスターアラートを設定できます。マスターアラートを設定するには、Master alert チェックボックスを選択します。

マスターアラートがトリガーされ、トリガーされたままの間は、source/destination/space の他の全てのアラートは抑制されます。マスターアラートはタイムスロットでトリガーされる他のアラートのみブロックします。24 時間アラートは、例えば、00:05 にトリガーされるアラートをブロックしません。

マスターアラート設定の例

■マスターアラートを低いチェック間隔(可能であれば、5 分)で設定します。

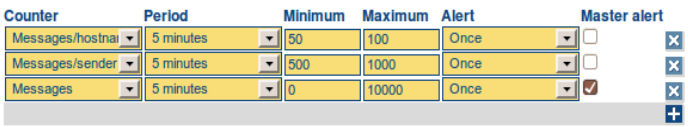
■マスターアラートを、抑制するアラートよりも低い間隔で設定します。

■マスターアラートを、抑制するアラートよりもより緩慢な限度で設定します。

マスターアラート設定の例

例 4.3 予期しないイベントを示すマスターアラートの使用

ユーザーは2つのリレー(sender)と 10 個のホストを一つのリレーごと(=20 ホスト)に持っている。それぞれのホストは約 5-10 メッセージを 5 分毎に送信している。二つのメッセージレートアラートが設定されており、予期しない多くのイベントを示す一つのマスターアラートがある。ホストが検出できないそして、おそらく停止しているあるいは、エラーのためホストが過剰に多くのログを送信しているといったイベントが考えられる。以下の設定は、これらのエラーを不必要なアラートを多数受けることなく検出することを助けます。



図表 4.17 予期せぬイベントのためのマスターアラート使用

Step 8. **オプションの手順：グローバルアラートは内部メッセージも含む sources に sylog-ng が受信した全てのメッセージを集計します。**

Step a　**Log > Options > Message rate alerting statistics** をクリックします。グローバルアラートを追加するために Global alerts の＋ボタンをクリックします

Step b　測られる期間（5 分から 24 時間）を選択します

Step c　正常と思われる範囲を **Minimum** と **Maximum** フィールドに入力します。

Step d　**Alert** フィールドにアラート頻度を選択します。**Once**:ひとつのアラートのみ送信（そして、問題が解決した後、“Fixed メッセージ”を送信）。**Always**:警告結果がセットしたレンジをはずれた場合、その都度アラートを送信。

Step e　システムワイドなマスターアラートを設定したい場合、**Global master alert.** を選択してください。Global master alert がトリガーされると、他の全てのログレイトアラートが抑制されます。

注記

以下のケースにおいて、いわゆる“always”タイプのスーパーマスターアラートが自動的にトリガーされます。

全てあるいはいくつかの syslog-ng の統計が取得できないとき、アラートが送信され、他のエラーはこのエラーが修復されるまで、抑制されます。

なんらかの原因で、syslog-ng が処理できないの量の統計（例：不正な入力データなどによるもの）を送信するとき、同様のスーパーマスターアラートがトリガーされ、インプットの処理を停止します。

Step 9. オプションのステップ：**Log > Options > Message rate alerting statistics をクリック**します。アラートが溢れることを防止するため、**Limit of alerts sent out in a batch** に受信したいアラートの最大数を設定します。SSB は、決定した値まで、アラートを送信し、過剰な数のアラートが生成されたことを示す一つのアラートの後、それ以上のアラートは送られません。

警告

データ損失の危険。定義した以上の制限のアラートは到達できません。

4.3.4.5 システム関連のトラップ

トラップ名	SNMP アラート ID	説明
Login failed	xcbLoginFfailure	SSB の Web インターフェイスからのログイン失敗
Successful login	xcbLogin	SSBWeb インターフェイスからのログイン成功
Logout from the management interface	xcbLogout	SSBWeb インターフェイスからのログアウト
Configuration changed	xcbConfigChange	SSB の設定変更全て
General alert	xcbAlert	全般的なアラートまたはエラーメッセージ
General error	xcbError	**注記** SSB のシステムログに、アラートまたはエラーに相当するメッセージが含まれていた場合、ここで設定するアラート及びエラーが常に送信されます。何度も送信されるので、デバッグの時などを除き、有効化しないほうがよいでしょう。有効にすると、同じ E メールまたは SNMP トラップのメッセージが、同一イベントに対して多数送信される恐れがあります。
Data and configuration backup failed	xcbBackupFailed	バックアッププロシージャが失敗したときにアラートを送信
Data archiving failed	xcbArchiveFailed	アーカイブプロシージャが失敗したときにアラートを送信
Database error occurred	xcbDBError	SSB がアラートやアカウント情報を蓄積しているデータベースにエラーが発生。弊社までご連絡ください。
Destination address limit reached	xcbLimitReached	クライアント数が上限に達した
HA node state changed	xcbHaNodeChanged	マスターからスレイブへのフェイルオーバー発生等、ハイアベイラビリティの状態に変化が起こった
Timestamping error occurred	xcbTimestampError	タイムスタンプサーバーが応答しない等、タイムスタンプ付与時にエラーが発生した
Time sync lost	xcbTimeSyncLost	システム時刻の同期がずれた
Raid status changed	xcbRaidStatus	装置の RAID の状態に変化が起こった
Hardware error occurred	xcbHWError	SSB が、ハードウェアのエラーを検知した

4.3.4.6 Syslog-ngに関するアラート

トラップ名	SNMP アラート ID	説明
syslog-ng failure	syslogngFailureTrap	Syslog-ngアプリケーションが正しく起動しなかった、想定外に終了した、あるいは他の問題に直面した。エラーの内容によっては、SSB がログメッセージを受け取れなかったり、転送ができなくなったりする。
Remote syslog-ng peer configuration changed	peerConfigChenge Trap	ネットワーク上で稼動しているマシンの syslog-ng アプリケーションの設定に変更が加えられた。この様な設定変更は、そのマシンに syslog-ng の 3.0 以降か、3.0 以降の syslog-ng エージェントがインストールされており、かつ、内部のソースからメッセージが送信されている場合に限り、検知できる。
Logspace exceeded warning size	spaceSizeLimit	閾値として設定した領域のサイズを、ログのスペースが超過した
Message rate was outside the specified limits	ssbAbsoluteMessageRateAlert	メッセージレートが指定したレンジよりも高いまたは低い
Too many message rate alerts were generated	ssbRateLimitTooManyAlerts	メッセージレートアラート数が警告リミットで設定したサイズを超過した。

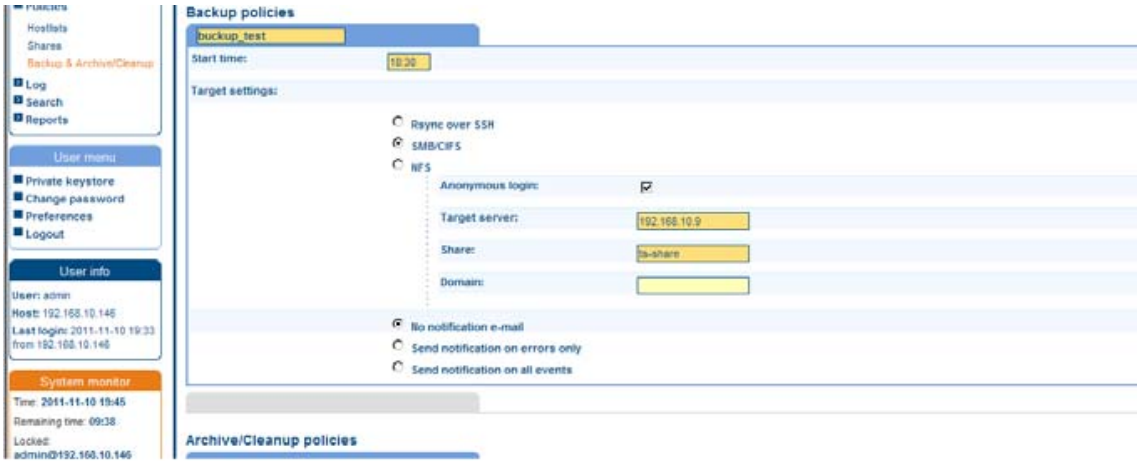
4.3.5 データと設定のアーカイブとバックアップ

SSB は、設定ファイル及び蓄積したログデータをリモートサーバーに自動でバックアップすることができます。ログのアーカイブについても同様に可能です。バックアップとアーカイブは、使用するプロトコル、リモートサーバーのアドレス、その他のパラメータを設定したポリシーにしたがって実行されます。

4.3.5.1 設定とデータのバックアップを定義する

目的:

自動でバックアップが実行されるように設定する方法を説明します。



図表 4.18 バックアップ及びアーカイブの設定

Step:

Step 1. バックアップポリシーを作成する

Step a. **Policies > Backup & Archive/Cleanup** の順にクリックします。新たなポリシーを作成するには、**+**をクリックして、入力欄を展開させます。

Step b. バックアップポリシーの名称を決定し、青い帯の部分の欄に入力します。（例：config-backup）

Step c. **Start time** 欄に、バックアップが起動する時刻を hh:mm 形式で入力します。

Step d. **Target server** 欄に、バックアップ先となるリモートサーバーの IP アドレスまたはホスト名を、入力します。（例 backup.example.com）

図表 4.19 バックアップとアーカイブの設定

SSB からリモートサーバーへの接続に際し、プロトコルを選択することが可能です。選択可能な中から、以下を注記に選んでください。

■ **Rsync over SSH**：セキュアシェルプロトコルで、rsync コマンドを実行します。バックアップサーバーで、rsync のバージョン 3.0 以降が実行可能であることが必須です。

■ **SMB/CIFS**：マイクロソフト・Windows ネットワークにおける SMB
（サーバーメッセージブロックプロトコル）

警告

NetApp(ネットアップ)ストレッジデバイスの、CIFS 実装は、SSB の CIFS とは互換性がありません。したがって、SSB から、CIFS プロトコルを使用するネットアップデバイスへのバックアップやアーカイブは失敗します。この際、以下のようなエラーメッセージを出力します。/opt/ssb/mnt/14719217504d41370514043/reports/2010″: Permission denied (13)　'2010/day/' rsync: failed to set times on
回避するには、以下のいずれかを行ってください。
①NFS プロトコルでアクセスする
②SSB と互換性のある CIFS 実装のデバイスを使用する。例えば、Windows、または Linux の Samba。

警告

NTLMv2 認証を利用する Windows 2008 R2 にバックアップあるいはアーカイブを行うため、CIFS プロトコルを使用すると、オペレーションは以下のようなエラーとともに失敗致します。

CIFS VFS: Unexpected SMB signature
Status code returned 0xc000000d
NT_STATUS_INVALID_PARAMETER
CIFS VFS: Send error in SessSetup = -22
CIFS VFS: cifs_mount failed w/return code = -22
CIFS VFS: Server requires packet signing to be enabled
in /proc/fs/cifs/SecurityFlags.
CIFS VFS: cifs_mount failed w/return code = -95
CIFS VFS: Server requires packet signing to be enabled
in /proc/fs/cifs/SecurityFlags.
CIFS VFS: cifs_mount failed w/return code = -95

この問題を回避するには以下を実施してください。

・Windows 2008 R2 サーバーにアクセスするのに NFS プロトコルを使用する。
・Windows 2008 R2 サーバーのレジストリを編集するか、ホットフィックスを適用する。
詳細は、Microsoft® Support　サイトのArticle 957441
（http://support.microsoft.com/kb/957441）をご参照ください。

■　**NFS**：ネットワークファイルシステムプロトコル

Step e.　選択したプロトコル固有の設定値を入力します。各プロトコル固有の設定値については、4.3.5.4バックアッププロトコルのパラメータをご参照ください。

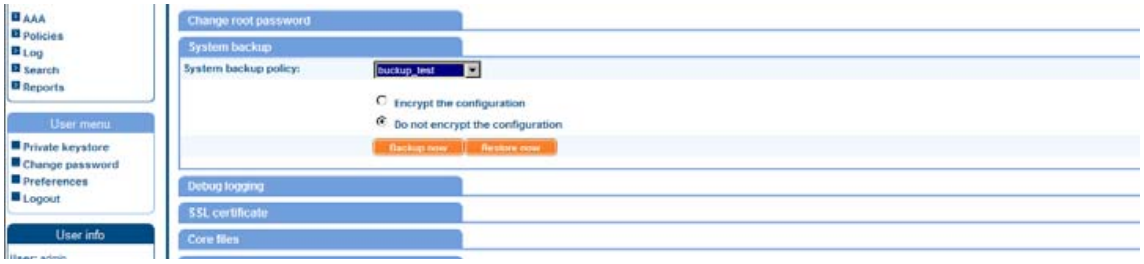
Step f.　バックアップに関してのメールを受信したい場合は、**Send notification on**

errors only または **Send notification on all events** のどちらかを ON にします。通知は、Management タブ内で設定した、管理者のメールアドレスに向けて送信され、バックアップされたファイルの一覧を含みます。

注記
ここでのEメール通知は、"Alerting & Monitoring" タブ内で設定したメール送信設定とは別です。ここでの通知メールは管理者のアドレスに送信され、アラートメールは、アラート受信者として設定されたアドレスに向けて送信されます。(4.3.4 SSBのシステム監視設定)をご参照ください。

Step g. **Commit** をクリックします。

Step 2. Step1 で作成したポリシーを適用して実際に設定ファイルのバックアップを実行させるには、**Basic settings** > **Management** > **System backup** の順にクリックし、**System back up policy** プルダウンから、適用させたいバックアップポリシーを選択します。



図表 4.20 システムバックアップの設定

ログデータのバックアップに、作成したポリシーを適用したい場合は、**Log** > **Space** の順にクリックし、バックアップしたいログスペースを選択します。次に、適用させたいバックアップポリシーを選択します。

Step 3. **Commit** をクリックします。

ヒント
設定ファイルを、リモートサーバー向けでなく即座にバックアップしたい場合は、**Basic settings** > **System** > **Export configuration** の順にクリックしてエクスポートします。
エクスポートしたファイルは、システム設定、設定ファイル、そして変更ログのみが含まれます。システムバックアップには、レポート、アラートなど、さらに多くの情報が含まれます。

コンフィグレーションバックアップからコンフィグレーションをリストアする詳細については、プロシージャ 8.7 コンフィグレーションバックアップからコンフィグレーションをリストアする を参照してください。

注記
バックアップは、アーカイブとは異なります。バックアップの目的は、SSB に蓄積されたデータ、またはその時点での設定でスナップショットを作成し、エラー発生時のリカバリーに備えることです。バックアップの際、対象ディレクトリの、バックアップ対象外のファイルは全て削除されます。リストア時は、SSB の他の全てのデータが削除されます。

ヒント
バックアップをすぐ実行するには、**Backup now** をクリックします。ただし、バックアップポリシーを先に作成しておく必要があります。ログ、レポート等、データのリストアを即実行するには、**Restore now** をクリックします。なお、**Restore now** 機能では、SSB の設定ファイルはリストアされません。

警告

リストア実行の前に、SSB におけるログ収集を必ず停止してください。そうでないと、その日のログファイルに不整合が起きる可能性があります。

ログ収集を停止するには、**Basic Settings** > **System** > **System Control** >**Syslog traffic** > **Disable** の順にクリックします。

特定のログスペースのみ、収集を停止するには、**Log** > **Paths** とクリックし、そのログスペースの **Enabled** 欄のチェックを外します。

4.3.5.2 収集したログデータのアーカイブ

目的:

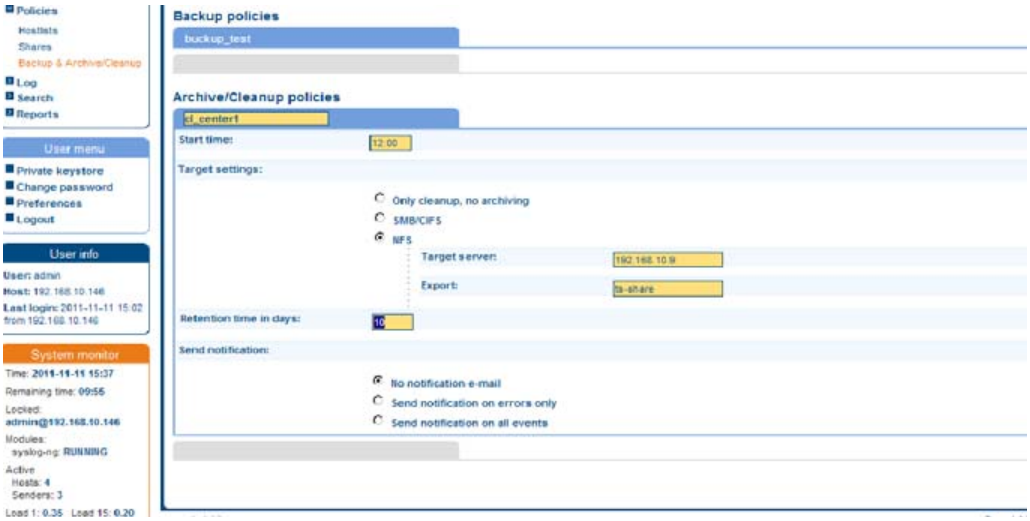
データのアーカイブ設定の方法を説明します。

Step:

Step 1. アーカイブポリシーの作成

Step a. **Policies** > **Backup & Arichive/Cleanup** の順にクリックし、**Archive/Cleanup policies** の部分の**+**をクリックし、新たな入力欄を展開させます。

Step b.



図表 4.21 バックアップとアーカイブの設定

ポリシーの名前を、青地の帯の中にある入力欄に入力します。

Step c. **Start time** 欄に、アーカイブ開始時刻を hh:mm 形式で入力します。

Step d. SSB は、アーカイブの際、いくつかのプロトコルを使用することができます。以下に従い、プロトコルを選択してください。

■**Only clearnup, no archiving**:アーカイブは行わず、単に **Retention time in days** で指定した期間より古いデータを削除します。

警告

このオプションでは、対象のファイルを全て削除します。回復させることは二度とできません。慎重に行ってください。

■**SMB/CIFS**：マイクロソフト　Windows ネットワークで用いられる、サーバーメッセージブロックプロトコル

警告

NetApp(ネットアップ)ストレッジデバイスの、CIFS 実装は、SSB の CIFS とは互換性がありません。したがって、SSB から、CIFS プロトコルを使用するネットアップデバイスへのバックアップやアーカイブは失敗します。この際、以下のようなエラーメッセージを出力します。

/opt/ssb/mnt/14719217504d41370514043/reports/2010″: Permission denied (13)　'2010/day/' rsync: failed to set times on

回避するには、以下のいずれかを行ってください。

①NFS プロトコルでアクセスする

②SSB と互換性のある CIFS 実装のデバイスを使用する。例えば、Windows、または Linux の Samba。

警告

NTLMv2 認証を利用する Windows 2008 R2 にバックアップあるいはアーカイブを行うため、CIFS プロトコルを使用すると、オペレーションは以下のようなエラーとともに失敗致します。

CIFS VFS: Unexpected SMB signature
Status code returned 0xc000000d
NT_STATUS_INVALID_PARAMETER
CIFS VFS: Send error in SessSetup = -22
CIFS VFS: cifs_mount failed w/return code = -22
CIFS VFS: Server requires packet signing to be enabled in /proc/fs/cifs/SecurityFlags.
CIFS VFS: cifs_mount failed w/return code = -95
CIFS VFS: Server requires packet signing to be enabled in /proc/fs/cifs/SecurityFlags.
CIFS VFS: cifs_mount failed w/return code = -95

この問題を回避するには以下を実施してください。

・Windows 2008 R2 サーバーにアクセスするのに NFS プロトコルを使用する。
・Windows 2008 R2 サーバーのレジストリを編集するか、ホットフィックスを適用する。
詳細は、Microsoft® Support　サイトのArticle 957441
(http://support.microsoft.com/kb/957441)をご参照ください。

■NFS：ネットワークファイルシステムプロトコル

Step e. **Target settings** > **Target server** 欄に、アーカイブ先となるリモートサーバーの IP アドレスを入力します。

Step f. **Retention time in days** 欄を入力します。ここで指定された期間より古いデータのみ、リモートサーバーにアーカイブされます。

注記
アーカイブされたデータは、SSB からは削除されます。
ただし、コネクションメタデータは削除されません。この時点では
ログファイルは削除されず、週単位でローテーションされます。

Step g. 各プロトコル固有の設定値を入力します。詳細は、4.3.5.4バックアッププロトコルのパラメータをご参照ください。

Step h. バックアップに関しての通知メールを受信したい場合は、**Send notification on errors only** または **Send notification on all events** のいずれかを選択します。通知メールは、Management タブ内で設定した、管理者のメールアドレスに向けて送信されます。バックアップ/アーカイブされたファイルの一覧が含まれます。

注記
ここでのEメール通知は、"Alerting & Monitoring" タブ内で設定したメール送信設定とは別です。ここでの通知メールは管理者のアドレスに送信され、アラートメールは、アラート受信者として設定されたアドレスに向けて送信されます。
(4.3.4 SSBのシステム監視設定)をご参照ください。

Step i. **Commit** をクリックします。

Step 2. ここで作成したアーカイブポリシーを、ログスペース内に蓄積されたデータのアーカイブに用いたい場合は、**Log** > **Spaces** の順にクリックし、アーカイブしたいログのログスペースを指定します。その後、**Arichive/Cleanup policy** プルダウンで、用いたいアーカイブポリシーを選択します。

Step 3. **Commit** をクリックします。

ヒント
アーカイブをすぐ実行するには、Archive now をクリックします。ただし
アーカイブポリシーを先に作成しておく必要があります。

4.3.5.3 GPGを用いて、設定ファイルのバックアップを暗号化する

目的:

GPG 鍵の公開の部分を用いて、SSB は、システムバックアップ時に設定ファイルを暗号化できます。そのための手順を説明します。

警告

SSB のシステムバックアップは、サンプルデータベースなど、他の情報も含まれています。ただし、ここで説明している手順で暗号化されるのは、設定情報のみです。システムバックアップには、ログスペース等、データは含まれないことにご注意ください。

Steps:

Step 1. **Basic** > **System** > **Management** > **System backup** の順にクリックします。

Step 2. **Encrypt configuration** を選択します。

Step 3. をクリックします。

■鍵ファイルをアップロードするには、**参照**をクリックします。GPG 公開鍵を含むファイルを選択し、**Upload** をクリックします。SSB は、バイナリと ASCII、両方の GPG 鍵を認識できます。

■クリップボードからコピー＆ペーストをするには、**Key** 欄にキーを貼り付け、**Set** をクリックします。

注記
アップロードする GPG 鍵は、データを暗号化することが可能なものを選んでください。単に署名する機能しかない鍵は、設定ファイルの暗号化に用いることはできません。

Step 4. **Commit** をクリックします。

注記
SSB に GPG で暗号化されたコンフィグレーションを直接インポートすることはできません。それは、最初にローカルで復号される必要があります。

4.3.5.4 バックアッププロトコルのパラメータ

ここでは、バックアップとアーカイブで用いられるプロトコルの詳細を説明します。

■Rsyncに関しては、4.3.5.4.1 Rsync over SSHの設定

■Sambaに関しては、4.3.5.4.2 SMBの設定

■NFSに関しては、4.3.5.4.3 NFSの設定

を、それぞれご参照ください。

4.3.5.4.1 Rsync over SSHの設定

目的:

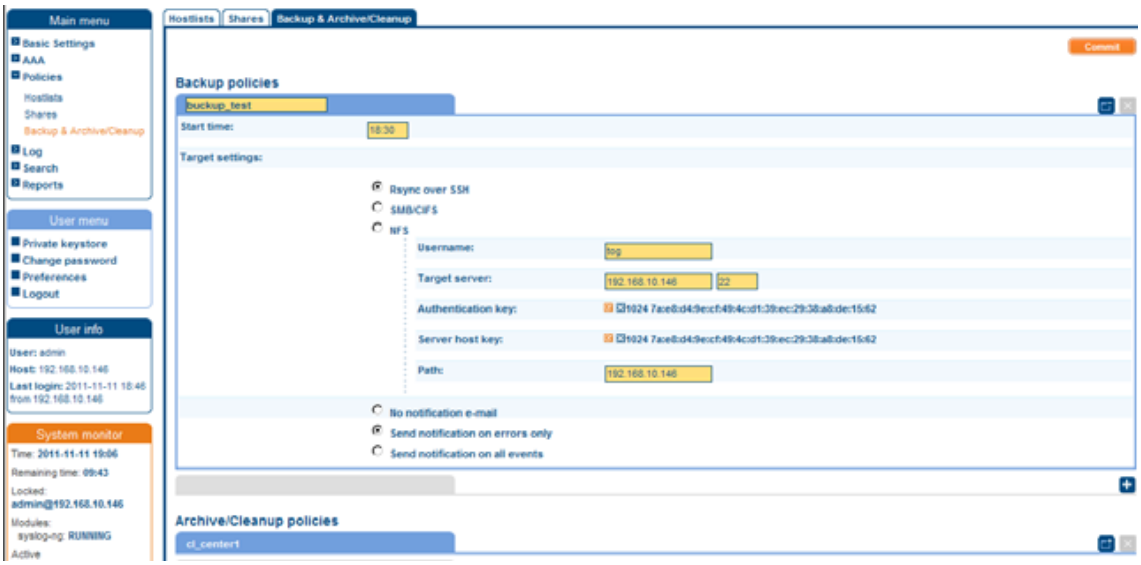
Rsync over SSH メソッドは、ターゲットサーバーに SSH で接続し、サーバーにデータをコピーするために"rsync" UNIX コマンドを発行します。SSB は、公開鍵で認証を行い、パスワード認証はサポートしていません。このプロトコルを使用する場合の設定を説明します。

警告

バックアップサーバーは、rsync のバージョン 3.0 以降が実装されている必要があります。

Step:

Step 1. **Target settings** のラジオボタンから、**Rsync over SSH** を選択します。



図表 4.22 rsync を用いた設定ファイルのバックアップ

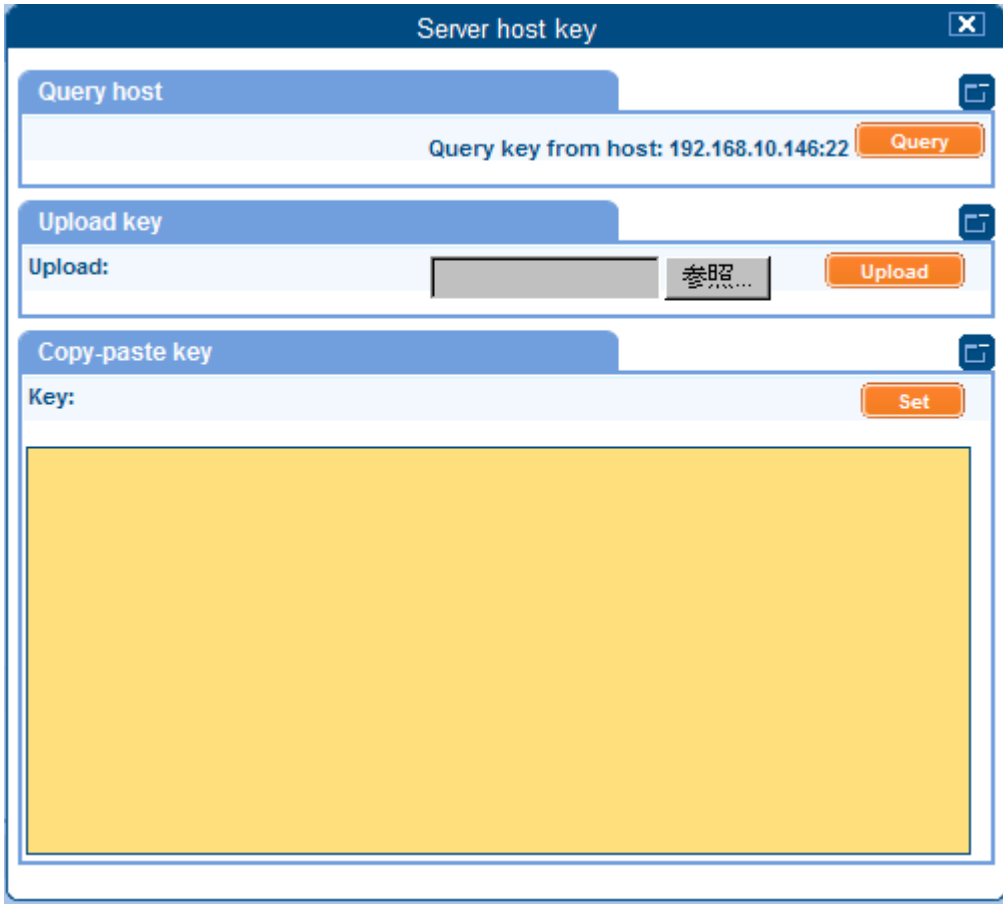
Step 2. **UserName** 欄に、リモートサーバーにログオンするためのユーザ名を入力します。

Step 3. **Authentication key** 欄の をクリックします。ポップアップウインドウが現れます。

Step 4. ポップアップウインドウの **Generate key** をクリックして生成するか、既存のキーをアップロードまたは貼り付けをして、新たな鍵ペアを作成します。このペアは、リモートサーバーが SSB を認証する際に用いられます。この鍵ペアの公開鍵が、リモートサーバー側にインポートされている必要があります。

Step 5. **Server host key** 欄の をクリックします。ポップアップウインドウが現れます。

Step 6.



図表 4.23 SSH キーの設定

Query host をクリックして、サーバーのホストキーをダウンロードします。あるいは、キーを手動でアップロードするか、貼り付けをします。SSB は、サーバーが提示したホストキーと、ここで設定したキーとを比較して認証します。一致した場合のみ、接続を許可します。

Step 7. リモートサーバーのポート番号を、**Target server** 右側の入力欄に入力します。

Step 8. **Path** 欄に、リモートサーバーへのパスを、入力します（例： /backups）。SSB は、自動的にログスペースのために、サブディレクトリを作成し、データを保存します。その結果、複数のログスペースのために同じバックアップポリシーが使用されることができます。ログスペースがリネームされてもリストアが実行されるようにするため、サブディレクトリはログスペ—スの持続するインターナル ID を使用してつくられます。手動でのデバッグを促進するため、ログスペースのためのインターナル ID を含む、テキストファイルもログスペースの名前と共に、ディレクトリ内に保存されます。このテキストファイルは、トラブルシューティング目的のために提供され、SSB では使用されません。

Step 9. **Commit** をクリックします。

4.3.5.4.2 SMBの設定

目的:

SMB/CIFS バックアップメソッドは、ターゲットサーバーの共有領域に、サーバーメッセージブロックプロトコルで接続します。主に、Windows ネットワークで使用されます。SMB/CIFS プロトコルを使用する際の設定方法を説明します。

警告

NetApp(ネットアップ)ストレージデバイスの CIFS 実装は、SSB の CIFS とは互換性がありません。したがって、SSB から、CIFS プロトコルを使用する netApp デバイスへのバックアップやアーカイブは失敗します。この際、以下のようなエラーメッセージを出力します。/opt/ssb/mnt/14719217504d41370514043/reports/2010″: Permission denied (13)
'2010/day/' rsync: failed to set times on
回避するには、以下のいずれかを行ってください。
①NFS プロトコルでアクセスする
②SSB と互換性のある CIFS 実装のデバイスを使用する。例えば、
Windows、または Linux の Samba

警告

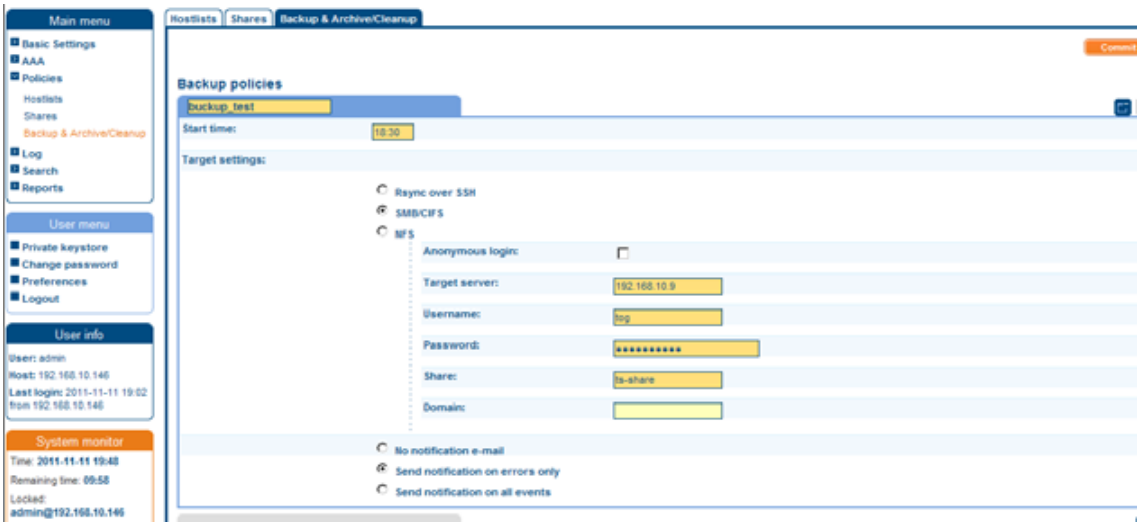
NTLMv2 認証を利用する Windows 2008 R2 にバックアップあるいはアーカイブを行うため、CIFS プロトコルを使用すると、オペレーションは以下のようなエラーとともに失敗致します。

CIFS VFS: Unexpected SMB signature
Status code returned 0xc000000d
NT_STATUS_INVALID_PARAMETER
CIFS VFS: Send error in SessSetup = -22
CIFS VFS: cifs_mount failed w/return code = -22
CIFS VFS: Server requires packet signing to be enabled
in /proc/fs/cifs/SecurityFlags.
CIFS VFS: cifs_mount failed w/return code = -95
CIFS VFS: Server requires packet signing to be enabled
in /proc/fs/cifs/SecurityFlags.
CIFS VFS: cifs_mount failed w/return code = -95

この問題を回避するには以下を実施してください。

・Windows 2008 R2 サーバーにアクセスするのに NFS プロトコルを使用する。
・Windows 2008 R2 サーバーのレジストリを編集するか、ホットフィックスを適用する。
詳細は、Microsoft® Support サイトのArticle 957441
(http://support.microsoft.com/kb/957441)をご参照ください。

Step 1. Target settings のラジオボタンから、SMB/CIFS を選択します。



図表 4.24 SMB/CIFS におけるバックアップの設定

Step 2. **Username** 欄に、リモートサーバーにログオンするためのユーザ名を入力するか、**Anonymous** ログオンを選択します。

Step 3. **Password** 欄に、ユーザ名に対応するパスワードを入力します。

Step 4. **Share** 欄に、共有領域の名称を入力します。

SSB は、この共有ディレクトリ下に自動でサブディレクトリを生成し、それらに全てのデータを格納します。"data"サブディレクトリに、ログファイルのバックアップ、"config"サブディレクトリに、設定ファイルのバックアップが入ります。

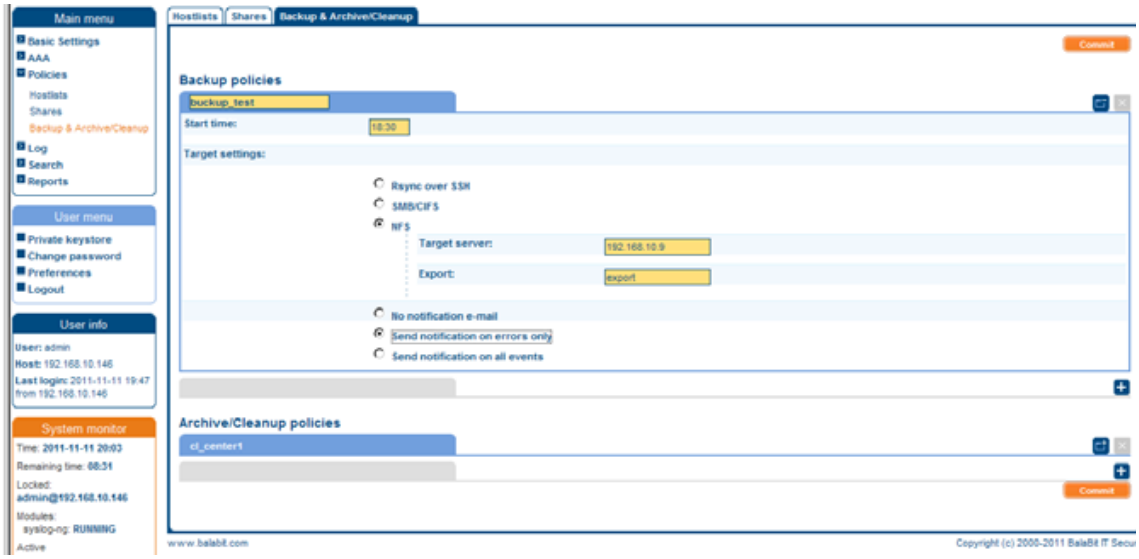
Step 5. **Domain** 欄に、ターゲットサーバーのドメイン名を入力します。

Step 6. **Commit** をクリックします。

4.3.5.4.3 NFSの設定

目的:

NFS バックアップメソッドは、ネットワークファイルシェアプロトコルを用いて、ターゲットサーバーの共有ディレクトリに接続します。設定を行うには、Export 欄に、NFS エクスポートの名称を入力する必要があります。SSB は、この共有ディレクトリに自動でサブディレクトリを生成し、それらに全てのデータを格納します。



図表 4.25 NFS のバックアップ設定

リモートサーバーが、SSB からのバックアップを許可するよう、設定しておく必要があります。NFS バックアップの設定手順を説明します。

注記

これらの手順は SSB ではなくリモートサーバー上で行います。

Step:

Step 1. バックアップサーバーの/etc/exports ファイルに、SSB に対する設定に合うようにスクリプトを追加します。以下のようなパラメータを含みます

■バックアップディレクトリへのパス:SSB のバックアップ/アーカイブポリシーで、**Export** 欄に設定したパス

■SSBインターフェイスのIPアドレス:リモートサーバーにアクセスするためのアドレス(SSBの外部インターフェイスか、管理インターフェイス:後者の場合は、有効化されていること、そして、ルーティングテーブルが正しく設定されていることが前提です) 詳細は、4.3.1ネットワーク設定 をご参照ください。

■次のパラメーター "rw,no_root_squash,sync"

例 4.4:リモートサーバー上で NFS を設定する

SSB が 192.168.1.15 で接続するとし、データを /var/backups/SSB ディレクトリに保存したい場合、スクリプトは以下のようになります。

/var/backups/SSB 192.168.1.15(rw,no_root_squash,sync)

Step 2. コマンド **exports -a** を投入します。

Step 3. **rpc portmapper** と、**rpc.statd** アプリケーションが稼動していることを確認します。

4.3.5.5 バックアップファイルの所有権

バックアップに用いるプロトコルが異なれば、バックアップされたファイルに付与される所有権も異なります。以下は、それぞれのプロトコルに対する所有権です。

■**rsync**：Web GUI で、設定時に入力したユーザ名

■**SMB**：www-data

■**NFS**：root(no_root_squash パラメータを記述しているの場合。行っていない場合、nobody)

警告

既にリモートサーバーにバックアップ済のファイルの所有権を SSB が変更することはできません。既にファイルが保存されている同一サーバー・同一ディレクトリに向けて、異なるプロトコルでバックアップをする際は、保存済のファイルの所有権を、これから使用するバックアッププロトコルに合うように変更することを必ず行ってください。そうでないと、SSB はファイルの上書きができず、バックアップが失敗します。

4.4　ユーザ管理とアクセス制御

AAA(Authentication：認証、Authorization：許可、Accounting：アカウンティング)メニューは、それぞれの要素に関して、ユーザのアクセス制御の設定を提供します。このセクションでは、以下に掲げる事項を説明していきます。

- ■ローカル環境でSSBが認証する方法－4.4.1 SSBユーザをローカル環境で管理する
- ■外部 LDAP データベース(例：マイクロソフト社・Active Directory)によるユーザ認証－4.4.4LDAP データベースによる SSB ユーザの管理
- ■外部RADIUSサーバーによるユーザ認証方－4.4.5 RADIUSサーバーでユーザ認証する
- ■ユーザ及びユーザグループの特権を管理する－4.4.6ユーザ権限とユーザグループを管理する
- ■SSBの設定に対する変更履歴を記録する－4.4.7　設定に対する変更を一覧化し、検索する

を、それぞれご参照ください。

4.4.1 SSBユーザをローカル環境で管理する

目的：

デフォルトでは、SSB ユーザはローカル環境で管理されます。ここでは、ローカルユーザの作成／削除、ユーザの参加グループの変更、パスワードの変更について説明します。

注記

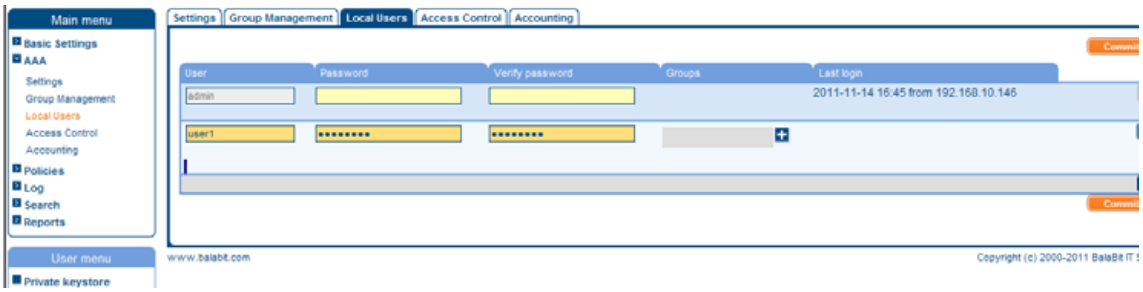
"admin"ユーザは、デフォルトで設定されており、全ての特権を有します。また、削除することはできません。

LDAP 認証が行われているときは、ローカルユーザの管理はできません。(4.4.4「LDAP データベースによる SSB ユーザの管理」をご参照ください)同時に、**AAA > Local Users** ページに表示がされませんが、削除されているわけではありません。

RADIUS サーバーによる認証をローカルユーザと共に行っている場合、ローカルユーザも RADIUS によって認証されます。参加グループに関することのみが、ローカル環境で管理されます。詳細は、4.4.5 RADIUSサーバーでユーザ認証するをご参照ください。

Step：

Step 1.　**AAA > Local Users** の順にクリックし、＋をクリックして入力欄を展開させます。



図表 4.26 ローカルユーザーを設定する

Step 2. **User** 欄に、ユーザ名を決めて入力します。

Step 3. **Password**欄にパスワードを入力、**Verify password** 欄に確認のため再入力します。パスワードの安全性が、入力欄の下に表示されます。パスワード安全性に関する設定を行うには、4.4.2ローカルユーザのパスワードポリシーを設定するをご参照ください。ユーザは、SSBのWebインターフェイスで、自分のパスワードを後で変更することができます。

Step 4. **Groups**セクションの⊞をクリックしてプルダウンを表示させ、ユーザに付与される権限のグループを選択します。一つのユーザに複数の権限グループを付与するには、このステップを繰り返します。異なるグループに関して詳細は、4.4.6ユーザ権限とユーザグループを管理するをご参照ください。

■グループからユーザを外す場合は、グループのプルダウン右の⊠をクリックします。

■ユーザを削除するには、そのユーザ設定欄の一番右側にあるを⊠クリックします。

注記

次に挙げる文字は、ユーザ名に使用できません。
/ [ ] : ; | = , + * ? < > と、¥(英語キーボードの場合バックスラッシュ)

Step 5. **Commit** をクリックします。

4.4.2 ローカルユーザのパスワードポリシーを設定する

目的:

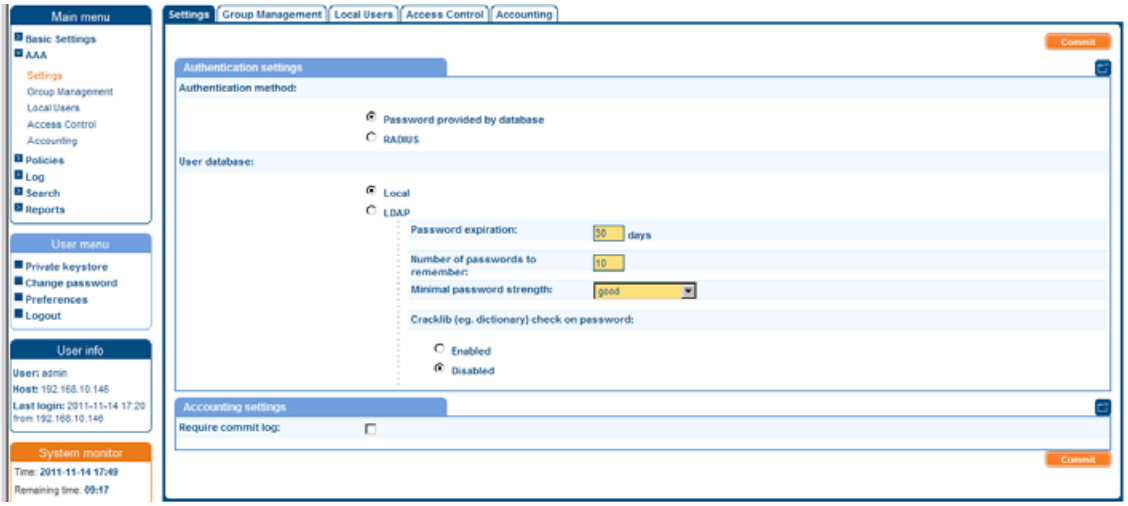
SSB は、パスワードの最低限の安全性と、有効期限を設定することができます。
パスワードポリシーに関しての設定を説明します。

注記

パスワードポリシーは、ローカル環境で管理されるユーザのみカバーします。
LDAP 及び RADIUS サーバーで管理してされるユーザに対しては何の影響もありません。
また、もともと組み込まれている admin ユーザにも影響しません。

Step:

Step 1. AAA > Settings の順にクリックします。



図表 4.27 パスワードポリシーを設定する

Step 2. Authentication method(認証方法)が、"Password provided by database"、User database が"Local" であることを確認します。

注記

LDAP または RADIUS 認証に設定されている場合、SSB はパスワードのローカル管理を行いません。

Step 3. **Password expiration** 欄に、一度設定したパスワードがどのくらいの期間有効かを入力します。この期間が経過すると、ユーザはパスワードの変更をしなくてはなりません。有効期間を設定したくない場合は、この欄に 0 を入力します。

Step 4. パスワードの使いまわし(例:有効期間が切れるたびに、2 回前に使っていたパスワードを再入力する、つまり2種類だけのパスワードを交互に使う)を防止するためには、**Number of passwords to remember** 欄に、使用履歴のあるパスワードが再使用できるようになるまで、新たなパスワードを何種類使用せねばならないか、を入力します。0 にすれば、制限なく使い回しを許可することになります。

Step 5. より安全性の高いパスワード設定を強制するなら、**Minimal password strength** 欄で、パスワードの完全性を選択します。

注記

パスワードの安全性は、エントロピー(複雑さ)によって決まります。すなわち、数字や文字の種類の多さ、大文字小文字の混ざり具合、特殊文字や記号の有無等です。単に長さだけではありません。

cracklib を Enable にすると、辞書ベースのパスワード総当りの簡易検査を行い、パスワードの安全性チェックができます。

Step 6. **Commit** をクリックします。

注記

パスワードポリシーを変更しても、既に設定済みのパスワードに影響はありません。ただし、パスワードの有効期限を新たに設定した場合は、期限が切れた後は全てのユーザがパスワードを再設定する必要があり、またパスワード安全性等、最新の設定条件に全ユーザが従わなくてはなりません。

4.4.3 ローカルユーザグループを管理する

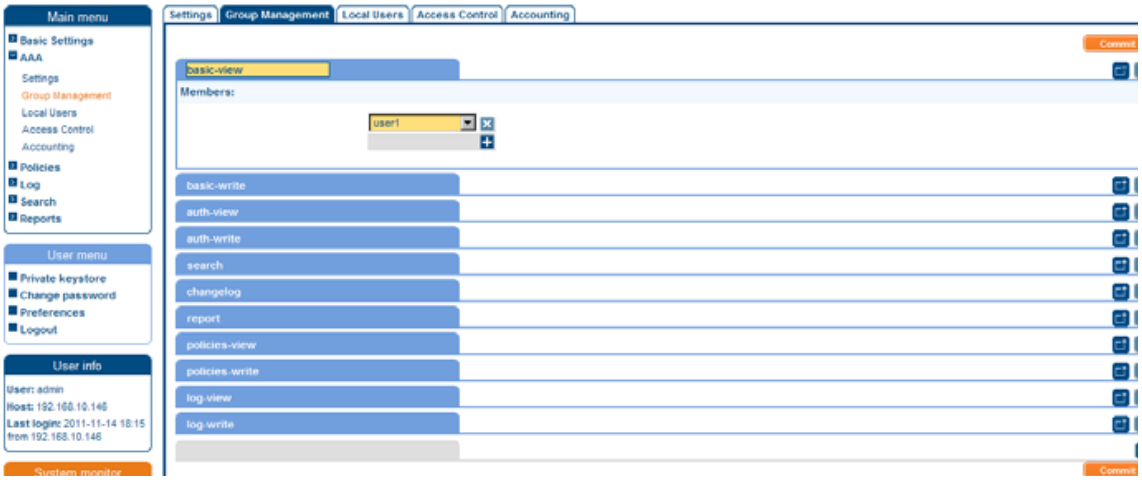
目的:

ユーザがどのローカルユーザグループに入っているかを表示させるには、AAA > Group Managementの順にクリックします。グループに含まれるユーザを変更することもできます。ローカルグループを、SSBのローカルならびにLDAPユーザの管理に用いることができます。ファイルや設定を閲覧するのみ、変更もか、などです。ローカルユーザを管理することにより、共有フォルダに対するアクセスをコントロールすることもできます。詳細は、5.2.6 ネットワーク経由でログファイルにアクセスするをご参照ください。
組込み済のグループに関しては、4.4.6.5 SSB組込みのユーザグループをご参照ください。

新たなグループを作成する手順を説明します。

Step:

Step 1. AAA > Group Management の順にクリックし、＋をクリックします。



図表 4.28 グループ管理

Step 2. グループの名称を決めて、青地の入力欄に入力します。

Step 3. プルダウンから、この権限グループを付与するユーザを選択します。複数のユーザに付与するなら、＋をクリックしてプルダウンを追加表示させます。

Step 4. 最後に **Commit** をクリックします。

4.4.4 LDAPデータベースによるSSBユーザの管理

目的:

SSB の Web インターフェイスは、外部の LDAP サーバーに、ユーザ認証をゆだねることができます。これにより、SSB を既存のインフラに統合する作業が、単純化されます。複数の LDAP サーバーを登録しておくことも可能で、こうすれば 1 台の LDAP サーバーがダウンしても、残りの LDAP サーバーに接続して認証要求をすることができます。LDAP 認証の設定方法を説明します。

注記

admin ユーザはデフォルトで存在し、全ての特権を有します。削除することはできません。また、LDAP サーバーによる認証が行われていても、SSB にログインすることができます。LDAP 認証を有効にすると、全てのローカルユーザはアクセス不可になりますが、admin は例外です。
SSB は、pre-win2000-style 及び Win2003-style のアカウント名(ユーザプリンシパル名)を認識できます。ユーザプリンシパル名(UPNs)は、ユーザ名、@、そしてドメイン名からなります。例: administration@example.com

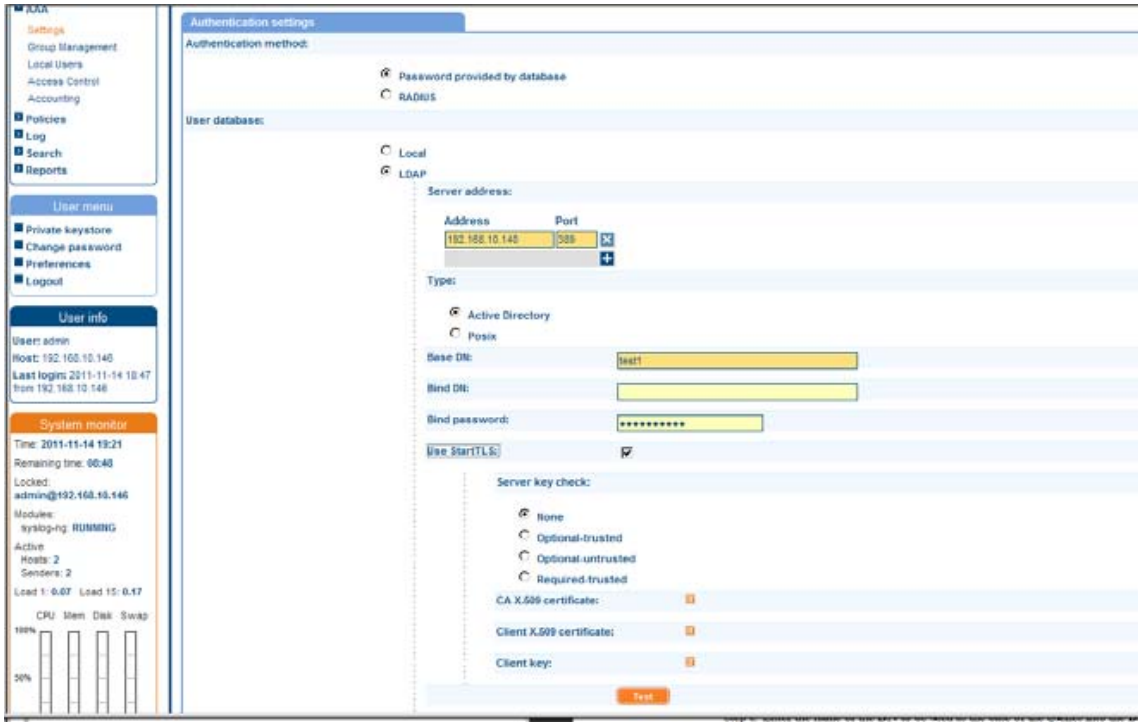
次に挙げる文字は、ユーザ名に使用できません。
/ [ ] : ; | = , + * ? < > と、¥(英語キーボードの場合、バックスラッシュ)

RADIUS サーバーによる認証と LDAP 認証を併用している場合、ユーザ自身は RADIUS サーバーによって認証され、グループ権限の付与のみ、LDAP で管理されます。詳細は、4.4.5 RADIUSサーバーでユーザ認証するをご参照ください。

Step:

Step 1. **AAA > Settings > Authenticatin settings** の順にクリックします。

Step 2. **LDAP** ラジオボタンを選択し、お使いの LDAP サーバーに関するパラメータを入力します。



図表 4.29 LDAP 認証の設定

Step a. **Server address** 欄に、お使いの LDAP サーバーのホスト名か IP アドレス、ポート番号を入力します。複数のサーバーを登録する場合は、**+**をクリックして、このステップを繰り返します。SSB は、一つ目のサーバーにアクセスできなくなった際、フェイルオーバーをして次に登録されている LDAP サーバーに、認証要求を出します。

警告

TLS 暗号化を、LDAP 接続の際の証明書検査に用いている場合は、Server addoress 欄には必ずフルドメイン名を入力してください。(例:ldap.example.com)
そうでないと、証明書検査で失敗します。LDAP サーバーのサーバー名は、証明書の"Common Name" に記されているものでなければなりません。

Step b. **Type** 欄で、お使いの LDAP サーバーの種類を選択します。マイクロソフト・アクティブディレクトリサーバーの場合は **Active Directory** を、POSIX LDAP サーバーの場合は **Posix** を選択します。

Step c. **Base DN** 欄に、クエリのベースとなる DN(識別名)を入力します。(例:DC=demodomain DC=exampleinc)

Step d. **Bind DN** 欄に、SSB がデータベースにアクセスする際にバインドされるべき識別名を入力します。例:CN=Administrator, CN=Users, DC=demodomai, DC=exampleinc.

注記

SSB は、pre-win2000-style 及び Win2003-style のアカウント名(ユーザプリンシパル名)を認識できます。administrator@example.com も、同じく受け付けられます。

Step e. **Bind Password** 欄に、LDAP サーバーバインドの際のパスワードを入力します。

Step 3. SSB と LDAP サーバー間の通信を暗号化したい場合は、**Use StartTLS** オプションにチェックを入れ、以下の手順を実行してください。

注記

マイクロソフト・アクティブディレクトリとの TLS 暗号化通信は、Windows2003 サーバー以降の OS でのみサポートされており、Windows2000 サーバーはサポート
していません。
SSB と LDAP サーバー間の暗号化通信は"START TLS"方のみサポートしており、LDAPS プロトコルはサポートしていません。

■サーバーの証明書検査を SSB にさせたい場合、**CA X.509 certificate** 欄の をクリックします。ポップアップウインドウが現れます。
Brows をクリックし、サーバーの証明書を発行した CA(認証局)を選択します。そして、**Upload** をクリックします。また、その代わりに証明書の内容を **Copy-paste** 欄に貼り付け、**Set** をクリックすることもできます。

SSB は、ここで選択された認証局の証明書を検査します。検査の結果、証明書の正当性を確認できない場合は、接続を拒否します。
LDAP サーバーが提示した証明書を全て受け入れるようにしたい場合は、**Server key check** 欄の **Rquired untrusted** をチェックします。

注記

LDAP サーバーの証明書検査方のオプションとして、以下から選択できます。

- **None**:証明書提示をリモートホストにリクエストしない。また、リモートホストから提示された証明書は全て受け付ける。
- **Optinal Tursted**:リモートサーバーが証明書を提示したら、SSB はそれが有効期限内か、また Common Name に、ホストの IP アドレスあるいはドメイン名が含まれているかをチェックする。このチェックで引っかかると、SSB は接続を拒否する。ただし、リモートホストが証明書を提示しない場合は、接続を許可する。
- **Optional untrusted**:リモートホストは必ず証明書を提示しなくてはならない。SSB は、それがどんな証明書であっても受付けて、接続する。
- **Required trusted**:リモートホストの証明書を検査する。認証局によって署名された証明書のみ受付ける。認証局による証明書に関して詳細は、4.5.8.2「外部認証された証明書をアップロードする」をご参照ください。証明書の Common Name に、ホストのドメイン名か IP アドレスのいずれかが含まれている必要がある。
- **Request untrusted**:SSB は、リモートホストに証明書提示をリクエストする。以下の場

合、接続を拒否する ①リモートホストが証明書を提示しない場合 ②証明書が有効期限切れの場合 ③Common Name 内に、ホストのドメイン名または IP アドレスが含まれていない場合

警告

TLS 暗号化を LDAP 接続の際の証明書検査に用いている場合は、**Server Aaddoress** 欄には必ずフルドメイン名を入力してください。(例:ldap.example.com)そうでないと、証明書検査で失敗します。LDAP サーバーのサーバー名は、証明書の"Common Name" に記されているものでなければなりません。

■LDAP サーバー側が、相互認証を必要としている(=SSB 側も証明書提示が必要な)場合、SSB の証明書を作成し、署名をしてもらいます。次に、ClientX..509 certificate 欄の をクリックして、証明書をアップロードします。その後、Client key 欄の をクリックして、その証明書の秘密鍵をアップロードします。

Step 4. Commit をクリックします。

警告

上記設定と同時に、SSBにおいては必ず、また場合によってはお使いのLDAPデータベースでユーザグループの設定が必要になります。詳細は、4.4.6.4 ユーザグループを使うをご参照ください。

Step 5. Test をクリックし、接続のテストを行います。(ただし、この機能は、現在はまだサポートされていません)

4.4.5 RADIUSサーバーでユーザ認証する

目的:

SSB は、外部の RADIUS サーバーに、ユーザ認証をゆだねることができます。なお、グループ参加の設定は、ローカル環境もしくは LDAP データベースにて行います。

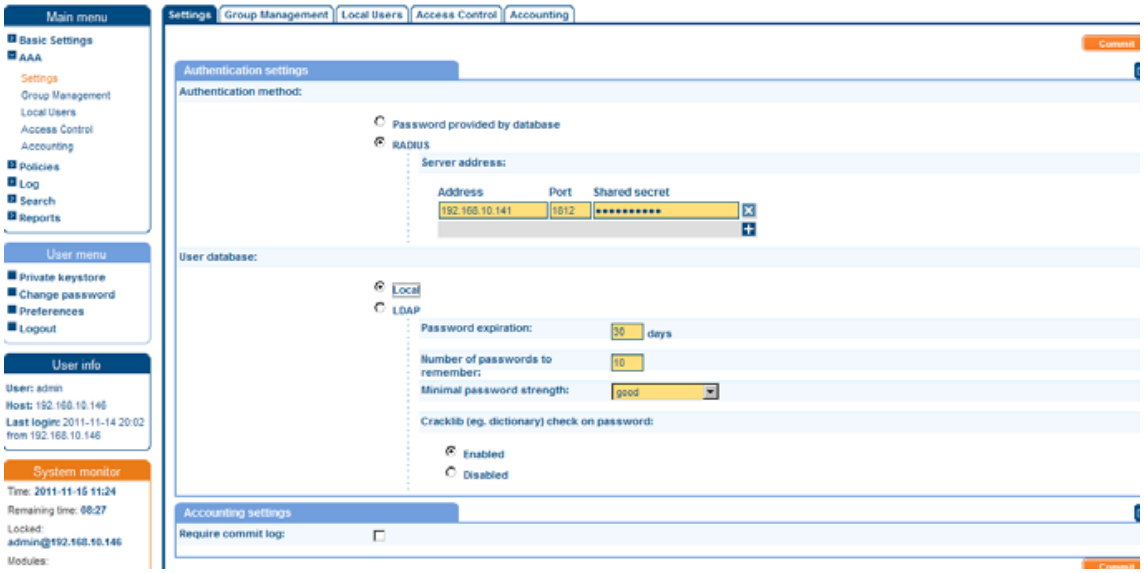
警告

チャレンジ/レスポンス認証方は、SSB では現在サポートしていません。
パスワード、セキュア ID 等の認証方のみサポートしています。

RADIUS サーバーによるユーザ認証の設定について説明していきます。

Step:

Step 1. **AAA > Settings** の順にクリックします。



図表 4.30 RADIUS 認証の設定

Step 2. Authentication method 欄で、RADIUS を選択します。

Step 3. **Address** 欄に、RADIUS サーバーの IP アドレスかドメイン名を入力します。

Step 4. **Shared secret** 欄に、SSB が RADIUS サーバーに接続するためのパスワードを入力します。

Step 5. さらに RADIUS サーバーを追加する場合は、**+**をクリックして、ステップ 2～4 を繰り返します。複数の RADIUS サーバーを設定することにより、万一 1 台目のサーバーがダウンしても、ファイルオーバーで SSB が自動的に次に登録されている RADIUS サーバーにアクセスします。

Step 6. ローカルユーザーデータベースと共に、RADIUS 認証を設定する時は、以下の手順に従ってください。

- Step a. Password expiration をOに設定する。
- Step b. Number of passwords をOに設定する。
- Step c. Minimal password strength を無効にする。
- Step d. Cracklib check on password を無効にする。

Step 7.

警告

Commit をクリックした後は、SSB の Web インターフェイスは、RADIUS サーバーによる認証が成功した後に初めてアクセス可能となります。なお、admin ユーザは、RADIUS サーバーに SSB からアクセス不能の場合でも、通常のログインができます。

Commit をクリックします。

4.4.6 ユーザ権限とユーザグループを管理する

SSB では、所属するユーザグループによって、付与されるユーザ権限が決まります。デフォルトでも数多くのユーザグループが組み込まれており、またカスタムメイドも可能です。それぞれのグループが、Web インターフェイスのどのページを閲覧、あるいは閲覧と変更/実行が可能か、というような権限のセットから構成されています。

注記

Web インターフェイスのページセットに対して、閲覧あるいは閲覧/編集/実行ができる権限が必ず、各グループに含まれています。

■既に存在するグループの設定の変更に関しては、4.4.6.1グループの権限を編集する

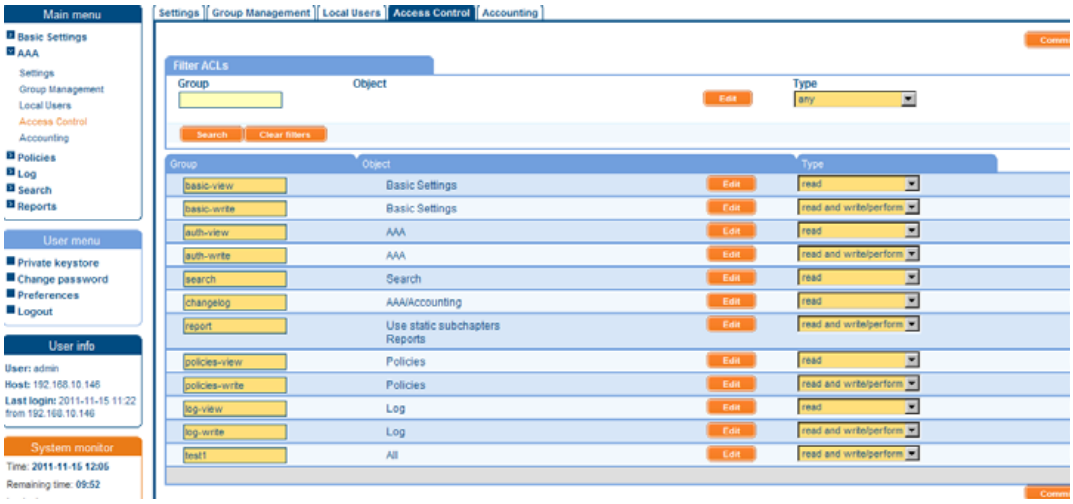
■新たなグループ作成に関しては、4.4.6.2SSBインターフェイスの、新たなユーザグループを作成する

■ある特定の権限を含むグループを検索することに関しては、4.4.6.3　特定のユーザグループを検索する

■ユーザグループ使用に関するヒントは、4.4.6.4　ユーザグループを使うをご参照ください。

■デフォルトで組み込まれているグループの権限に関して詳細は、4.4.6.5SSB組込みのユーザグループ

を、それぞれご参照ください。



図表 4.31　SSB ユーザーの管理

4.4.6.1　　グループの権限を編集する

目的:

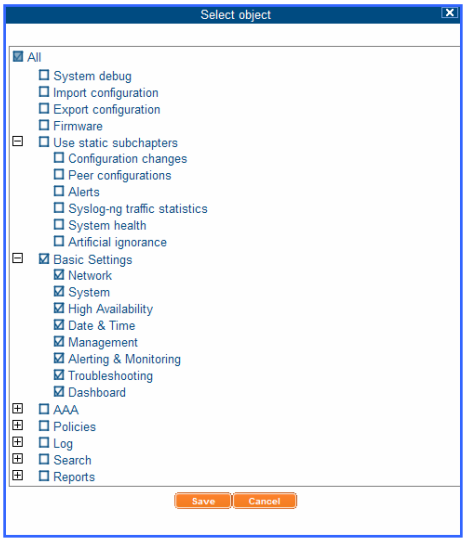
既に存在するユーザグループの権限を編集する方法を説明します。

Step:

Step 1. **AAA > Acess Control** の順にクリックします。

Step 2. 権限を編集したいグループを探し、 をクリックします。設定可能な権限が別ウィンドウで開きます。

Step 3. 権限(=Web インターフェイスのページ)を選択/解除し、Save をクリックして変更を反映させます。



図表 4.32 グループ権限の修正

警告

AAA ページにおける"Search"権限をユーザに付与すると、そのユーザは、たとえ Access control オプションである特定のログスペースのグループに属していなくとも、全てのログスペースにおいて検索が可能となります。

Step 4. **Type** 欄で、アクセスの種類'(readまたは read and write/perform)を選択します。

Step 5. **Commit** をクリックします。

4.4.6.2 SSBインターフェイスの、新たなユーザグループを作成する

目的:

新たなグループを作成する手順を説明します。

Step:

Step 1. **AAA > Access Control** の順にクリックし、をクリックします。

Step 2. グループ名を決めて入力します。グループのネーミングに関して詳細は、4.4.6.4 ユーザグループを使うをご参照ください。

Step 3. アイコンをクリックし、設定可能な権限を表示させます。

Step 4. グループに付与する権限(SSB Web インターフェイスのページ)にチェックを入れます。終わったら **Save** をクリックします。

Step 5. **Type** 欄で、アクセスの種類(read または read and write/perform)を選択します。

Step 6. **Commit** をクリックします。

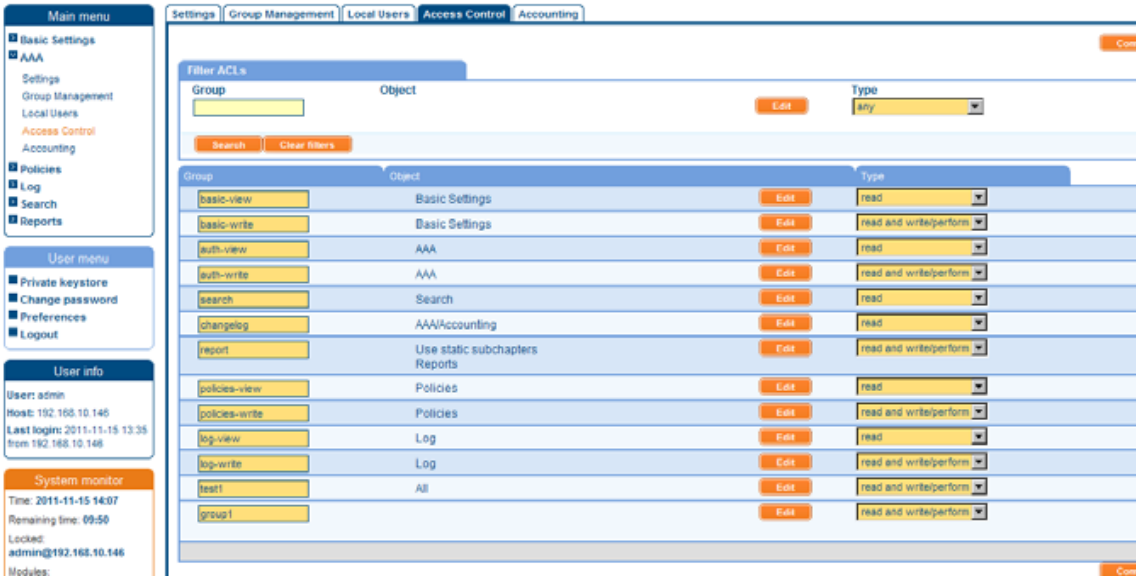
注記

- 設定ファイルのエクスポートを行いたい場合、Export 権限を含める必要があります。
- 設定ファイルのインポートを行いたい場合、Import 権限を含める必要があります。
- ファームウェアのアップデートまたはアクティブファームウェアのセットを行いたい場合、Firmware 権限を含める必要があります。

admin ユーザはデフォルトで作成されており、全ての特権を有します。唯一不可能なのは、共有ログスペースにリモートでアクセスできないことです。admin ユーザを削除することはできません。

4.4.6.3 特定のユーザグループを検索する

AAA > Access Control ページの Filter ACLs セクションで、ユーザグループの名称または付与されている権限をキーに、グループを簡単に検索することが可能です。



図表 4.33 特定のユーザを検索する

■特定の文字で始まるユーザグループを検索するには、始まりの文字列を Group 欄に入力し、Search をクリックします。

■特定の権限が付与されているグループを検索するには、Edit をクリックし、検索している権限名(完全にわからない場合は、途中までででも可)を入力し、Search をクリックします。

■アクセス種別(read/read and write/perfoem)でさらに絞り込む場合は、Type プルダウンで選択します。

4.4.6.4 ユーザグループを使う

ユーザグループをどうネーミングするかは、SSB ユーザの管理方法によって変わってきます。

■ローカルユーザ:SSB ローカル環境でのみユーザ管理を行う場合は、**AAA > Access Control** ページで、ユーザの作成及び管理をします。ユーザのグループ所属に関する設定は、**AAA > Local Users** または **AAA > Group Management** ページにて行います。

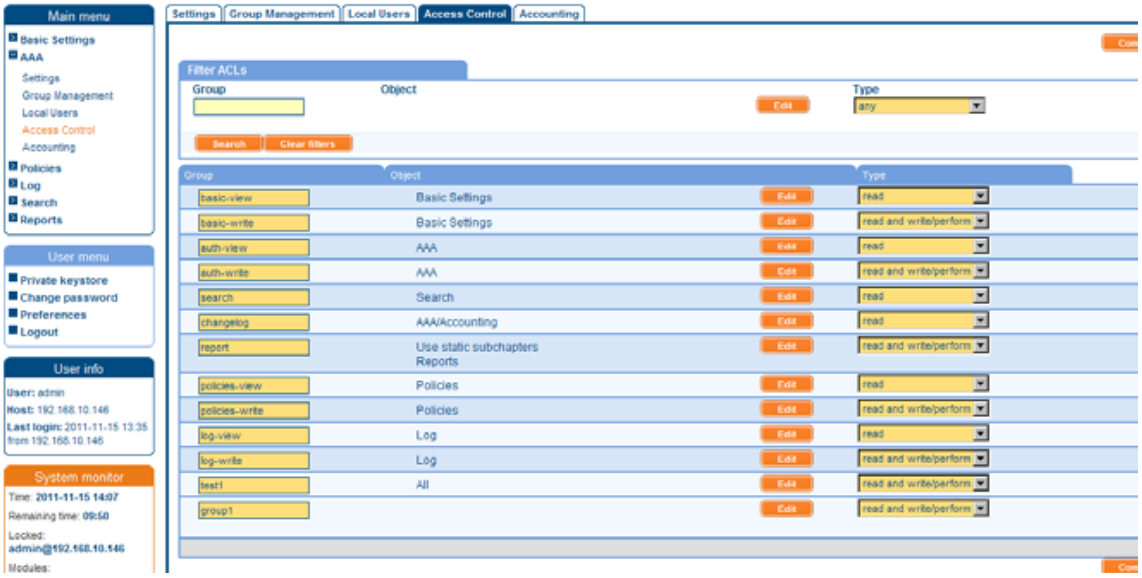
■LDAP ユーザ・LADP グループ:ユーザ管理を LDAP で行っており、SSB のユーザグルーピングと同じ LDAP グループが設定されているなら、**AAA > Access Control** ページにて、ユーザ作成と編集を行います。その際、LDAP のグループ名と SSB のユーザグループ名が同一になるようにしてください。たとえば、admin という LDAP グループを作成し、SSB でも使えるようにしたい場合、SSB の **AAA > Access Control** ページにて、admin というグループを作成します。その後、付与する権限を設定します。

■RADIUS ユーザとローカルグループ:LDAP サーバー上でグループを作成できない(または作成したくない)が、ユーザは RADIUS で管理する、というケースです。

ローカルのユーザグループを AAA > Group Management ページで作成します。

4.4.6.5 SSB組込みのユーザグループ

SSB は、デフォルトで以下のユーザグループが設定されています。



図表 4.34 SSB 組み込みのユーザグループ

警告

LDAPサーバーによるユーザ認証を行っていて、かつSSBデフォルトのユーザグループをお使いになりたい場合は、全く同じ名前のユーザグループをLDAPデータベースに作成し、ユーザを割り振る必要があります。ユーザグループ使用に関して詳細は、4.4.6.4 ユーザグループを使うをご参照ください。

■**basic-view**：SSB のシステムログ及び Basic Settings の設定メニューを閲覧できる権限。Troubleshooting タブ内のコマンド実行も可能

■**basic-write**：Basic Setteings メニューの設定内容を変更できる権限。このグループの権限が付与されているユーザは、SSB をホストとして管理できます。

■**auth-view**：AAA メニュー内、SSB 管理者の名称及び権限、ユーザグループの設定内容、認証設定を閲覧できる権限。このグループ権限が付与されていると、設定内容の変更履歴も閲覧できます。

■**auth-write**：認証関連の設定を編集でき、またユーザ及びユーザグループの管理ができる権限

警告

auth-write、あるいは他の、AAA メニューに対する write 権限を含むグループに属するユーザは全て、実質的には SSB のシステム管理者と同等です。自分であらゆる特権を付け足せるからです。権限を制限したいユーザに、write 権限を与えてはなりません。
ユーザが自ら、AAA メニューに関する新たな特権を付与した場合、反映させるために、SSB に再ログインする必要があります。

■search：**Search** メニューにて、さまざまなログやアラートを閲覧し、ダウンロードできる権限

注記

admin ユーザは、デフォルトではこのグループ権限は付与されていません。したがって、共有ログスペースにリモートアクセスすることはできません。

■changelog：**AAA** > **Accounting** メニューにて、SSB の設定に対する変更の履歴を閲覧できる権限

■report：**Report** メニューにて、レポートを閲覧、作成、管理でき、またレポートに統計ベースの章を挿入できる権限

注記

レポートに、どの統計ベース章を挿入するか、細かく設定したい場合は、"Use static subchapters" 権限を付与してください。

■policies-view：**Policies** メニューにて、ポリシー及びその設定を閲覧できる権限

■policies-write：**Policies** メニューにて、ポリシー及びその設定を編集できる権限

警告

この権限グループを付与されているユーザは、蓄積されたログを、共有ネットワークドライブへの接続するのと同様にアクセス可能です。暗号化されていないログファイルでは、重要なデータも丸見えとなってしまう危険性があります。

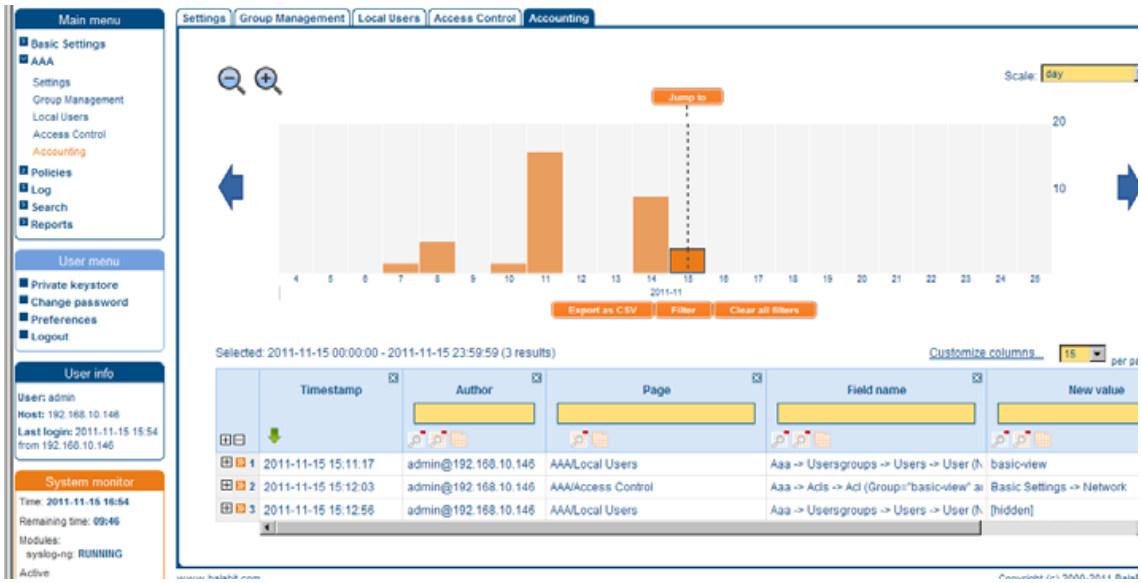
■log-view：**Log** メニューの、ロギングの設定を閲覧できる権限

■log-write：**Log** メニューの、ロギングの設定を編集できる権限

4.4.7 設定に対する変更を一覧化し、検索する

SSBは、設定に対する変更を全て記録します。その履歴を閲覧するには、**AAA** > **Accounting**の順にクリックします。変更履歴はログとして残り、SSBの通常のWebインターフェイスから検索・閲覧することができます。(詳細は、第 6 章 ログメッセージとレポートを閲覧するをご参照くださ

い)以下説明は、それぞれの情報について記述しています。



図表 4.35 設定変更履歴の閲覧

- **Timestamp**：変更が加わった日付
- **Author**：設定変更を行った SSB 管理者のユーザ名
- **Page**：変更された項目が属するメニュー
- **Field name**：変更された項目またはオプション名
- **New value**：変更後のパラメータの値
- **Message**：管理者が記録した、変更に当たっての説明。**Require commit log** オプションが ON になっているときのみ、このフィールドに値が入る(下記説明参照)
- **Old value**：変更前のパラメータの値

設定変更に関して、説明を毎回必ず記述させるには、**AAA** > **Settings** の順にクリックし、**Accounting settings** フィールドの、**Require commit log** オプションを ON にします。

4.5 SSBの管理

以下のセクションでは、アプライアンスの基本的なコントロール(例：シャットダウンやリブート)、アップグレード、トラブルシューティングのチップスを含む SSB の基本マネージメントを説明します。

4.5.1 SSBの制御ー再起動、シャットダウン

SSBの再起動またはシャットダウンを行うには、**Basic Settings** > **System**の順にクリックし、

System controlタブをクリックします。This node であることを確認し、RestartまたはShutdownいずれかをクリックします。もし、The Other node と表示されていたら、それはハイアベイラビリティモードで稼動している場合の、スレーブマシンを意味します。ハイアベイラビリティのクラスターに関して詳細は、4.5.2 SSBハイアベイラビリティのクラスターを管理するをご参照ください。

警告

- クラスターノードをリブートするときは、不必要なテークオーバーを避けるため、他（スレイブ）ノードを先にリブートしてください
- クラスターのノードをシャットダウンするときは、他（スレイブ）ノードを先にシャットダウンしてください。ノードをパワーオンするときは、不必要なテークオーバーを避けるため、マスターノードを先に開始してください。
- 両方のノードが動作中、ノード間の接続を遮ることを避けるため、イーサネットケーブルを抜いたり、ノード間のスイッチやルータをリブートしたり、SSB の HA インターフェイスを無効にしたりしないでください。

図表 4.36　基本設定

注記

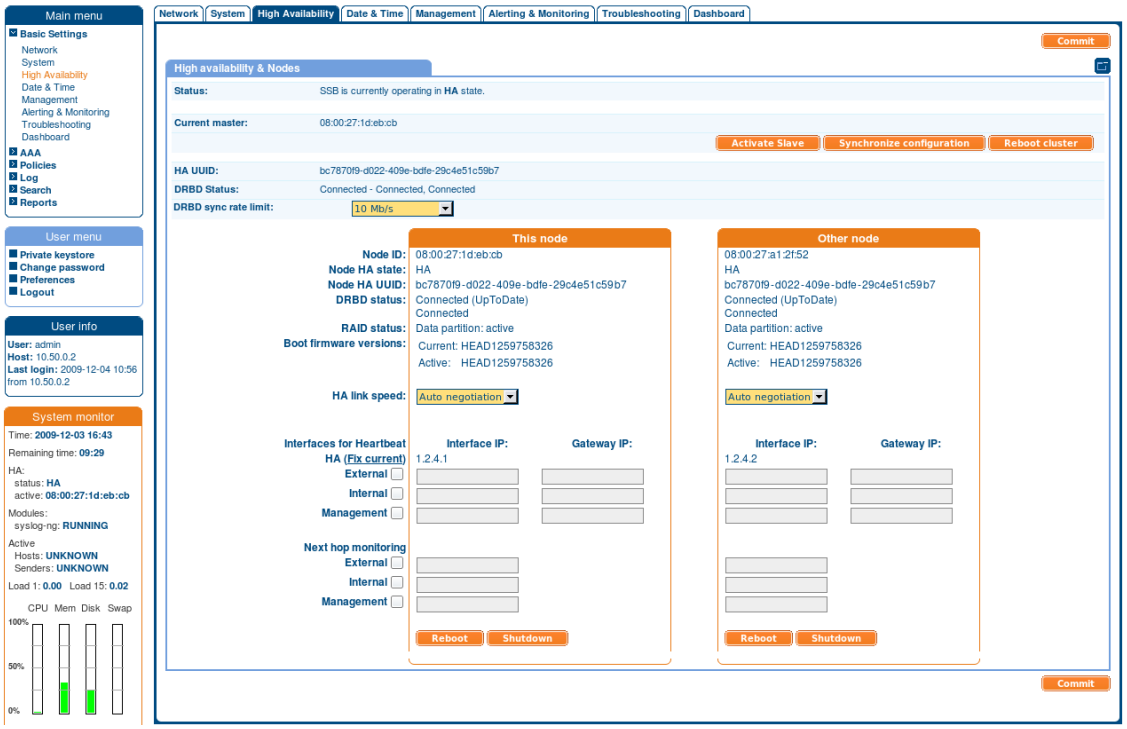
SSB のインターフェイスに対する Web セッションは、再起動後も保持されています。よって再起動後にログインし直す必要はありません。

4.5.2 SSBハイアベイラビリティのクラスターを管理する

Basic Settings > High Availability ページは、以下の情報を提供します。

警告

- クラスターノードをリブートするときは、不必要なテークオーバーを避けるため、他（スレイブ）ノードを先にリブートしてください
- クラスターのノードをシャットダウンするときは、他（スレイブ）ノードを先にシャットダウンしてください。ノードをパワーオンするときは、不必要なテークオーバーを避けるため、マスターノードを先に開始してください。
- 両方のノードが動作中、ノード間の接続を遮ることを避けるため、イーサネットケーブルを抜いたり、ノード間のスイッチやルータをリブートしたり、SSB の HA インターフェイスを無効にしたりしないでください。



図表 4.37 HA クラスタの管理

- ***status***: SSB が、ハイアベイラビリティモードか、スタンドアロンで稼動しているかを表示します。
- ***Node ID***: ハイアベイラビリティモードにおける、ノード間インターフェイスの MAC アドレスです。この MAC アドレスは、SSB マシン筐体の上部カバーにあるラベルにも印刷されています。
- ***Node HA state***: SSB の各ノードが、ハイアベイラビリティモードか、スタンドアロンで稼動しているかを表示します。
- ***Node HA UUID***: ノードをユニークに識別する識別子。ハイアベイラビリティモードでのみ表示されます。
- ***DRBD status***: SSB に蓄えられたデータのステータス。アクティブなノードでは必ず"Consistent"でないと、データ喪失を発生させる危険性がある。
- ***RAID status***: ノードの RAID デバイスのステータス。

アクティブ(マスター)ノードは、Web インターフェイス上では"This node"と表示されます。ログメッセージを受信し、ユーザに Web インターフェイスを提供します。"Other node" と表示されているノードは、スレーブで、マスターノードに不具合が発生した場合に本番機となります。

注記

ノード ID(ハイアベイラビリティインターフェイスの MAC アドレス)は、SSB クラスターが送信するログメッセージに含まれます。

現在アクティブなマスターノードをダウンさせてスレーブノードを稼動させるには、**Activete slave** をクリックします。

両方を再起動させるには、**Reboot** Cluster をクリックします。これにより両方のクラスタマシンで再起動がかかりますが、フェイルオーバーが起こるわけではありません。

警告

データロストにご注意ください！スレーブノードをアクティベイトすると、SSB と、ログを転送しているデバイス間の全接続が切れます。スレーブノードは、60 秒後にアクティブになりますが、それまで、SSB はログを受信することができません。お使いの syslog-ng クライアント及びリレーにおいて、デスクバッファリングを有効にし、データロストを防いでください。

4.5.2.1 ハイアベイラビリティのステータスに関する説明

このセクションでは、SSB ノードのステータス及び DRBD データストレッジシステムに関して説明します。SSB では、これらに関して **Basic Settings > High Availability** ページで表示しています。

Status 欄は、SSB のノードが互いを認識できているか、ハイアベイラビリティモードとして正しく設定されているか、を表示します。個々の SSB ノードのステータスは、各々の **Node HA Status** 欄に表示されています。ステータスは以下のいずれかです。

- ***Standalone***: もともと 1 台の SSB マシンしか存在していないか、複数台あってもクラスターモードに移行していない場合。(後者の場合は、**Node HA status** がいずれのマシンにおいても"standalone"です)ハイアベイラビリティモードに移行させるには、**Convert to Cluster** をクリックします。
- ***HA***: 二つの SSB ノードがハイアベイラビリティモードで稼働中。**Node HA status** は、両方とも"**HA**"、**Node HA UUID** は、どちらも同一の表示になります。
- ***Half***: ハイアベイラビリティモードが正しく設定されていません。片方は standalone で、もう片方が HA になっています。ハイアベイラビリティモードでノードを接続し、**Join HA** をクリックして、ハイアベイラビリティモードを有効にしてください。
- ***Broken***: 二つの SSB ノードが、ハイアベイラビリティモードで稼動しています。**Node HA statsu** はどちらも HA になっていますが、**Node HA UUID** が異なっています。弊社サポートにご連絡ください。
- ***Degraded***: SSB はハイアベイラビリティモードで稼動していたが、片方のノードが認識できなくなった。(例えば、ダウンした、ネットワークから撤去された)電源を入れ、ネットワークに接続し直してください。あるいはダウンしたノードを修理してください。
- ***Degraded Sync***: 二つの SSB マシンが、ハイアベイラビリティモードで接続され、最初の同

期を行っている最中。終了までお待ちください。なお、大容量ディスクに大量のデータが保存されている場合、この同期は数時間かかる場合もあります。

■ *Split brain*: 二つのノード間の接続が失われました。両方が同時にマスターになってしまった可能性があります。

警告

Split brainになった場合のデータロストにご注意ください！ 重要なデータがいずれのノードにも転送されてしまう可能性があります。そのようなトラブルを防ぐには、8.6.2スプリットブレイン状況からのリカバリーをご参照ください。
決して、ノードをリブートしたりシャットダウンしたりしないでください。

■ *Invalidated*: 片方のノードのデータが不整合を起こしており、もう片方からのノードからアップデートが必要です。これは、Split brain ステータスからのリカバリー時、DRBD が手動で無効化された際に発生します。

■ *Converted*: "Convert to Cluster"をクリックしてクラスターに移行した後、、あるいは Join HA をクリックしてハイアベイラビリティを有効にした後で、かつノードの再起動前にこのステータスになります。

注記

システムのセットアップ時に、ハイアベイラビリティのノードがお互いを認識できない場合は、**Basic Settings > High Availability** の順にクリックし、**Make HA IP premanent** を選択します。これにより、ノード間インターフェイスの IP アドレスは固定され、ハイアベイラビリティの接続が遅い場合のトラブルシューティングに役立ちます。

DRBD status 欄は、SSB の設定ファイル、ログファイル、その他を含む最新のデータが、双方のノードから参照できるか否かを表示します。マスター("this node")は、データロストを防ぐために、常にこのステータスは"consistent"でなければなりません。"inconsistent"だと、データが常に最新に保たれておらず、最新の状態になっているいずれかのノードに同期させる必要があることを意味しています。

DRBD status は、SSB ノード間のディスクシステムの接続状況も表示します。以下のいずれかになります。

■ *Connected*: 両ノードとも正常に稼動しています。

■ *Invalidated*: いずれかのノードのデータに不整合が発生しています。もう片方のノードから、データの同期を取る必要があります。この状態は、Split-brain ステータスからのリカバリー時、DRBD が手動で無効化された際に発生します。

■ *Sync source* または Sync target: 一つ(Sync source)のノードが、もう片方(Sync source)から、データをダウンロードしています。

注記

両ノードがデータ同期を取っている最中は、マスターノードの再起動やシャットダウンを行うことはできません。この様な状況でもやむを得ずシャットダウンしなければならない場合は、まずスレーブノードを落とし、次にマスターをシャットダウンします。
データの同期を取っている最中は、進捗と残り時間が System monitor 欄に表示

されます。

■ *Split brain*: ノード間の接続が失われました。両ノードともアクティブ(マスター)になってしまったことが考えられます。

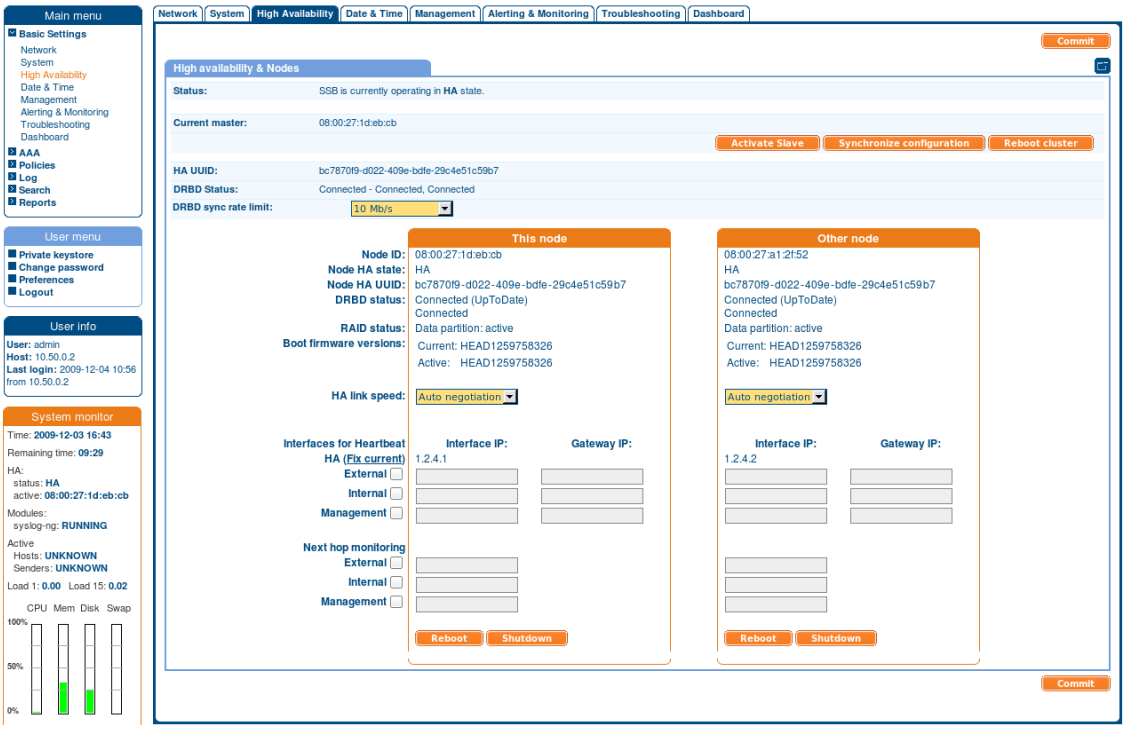
警告

Split brain状態になった場合、データロストにご注意ください！重要なデータがいずれのノードにも転送されてしまう可能性があります。そのようなトラブルを防ぐには、8.6.2 スプリットブレイン状況からのリカバリーをご参照ください。

■ *WFConnection*: 片方のノードが、もう片方との接続を待っている状態。まだ双方の接続が確立していないことを意味します。

4.5.2.2 DRBDの同期速度の調整

SSB が二つのマシンで、ハイアベイラビリティモードで稼動している際、入ってくる全てのデータが、マスター(アクティブな)ノードから、スレイブ(準備中の)ノードへとコピーされます。データ同期はシステムのリソースを大量に消費することから、同期の速度は制限されています。デフォルトでは 10MB/Sec です。しかしこれでは、大量のデータの同期には長時間かかってしまいます。したがって、状況によっては、同期速度を高くすることが役立ちます。例えば、スタンドアロンモードからハイアベイラビリティモードに移行した後のデータ同期です。



図表 4.38 DRBD 同期スピードの調整

DRBD 同期速度を調整するには、**Basic Settings > High Availability** の順にクリックし、**DRBD sync rate limit** プルダウンで、設定したい速度にします。

注記

SSB に負荷がかかっているときに、同期速度を速くすることは推奨しません。データ同期によってシステムリソースの使用率が上がり、SSB 全般のパフォーマンスが落ちるからです。

4.5.2.3 冗長化ハートビートインターフェイスの設定

目的:

無用なフェイルオーバーや Split-brain 状態を発生させないために、SSB に冗長化ハートビートインターフェイスを設定することができます。これは、単にもう片方のノードが正常な状態であることを確認するためだけの目的であり、データ等の同期を取るものではありません。(ハートビートメッセージのやり取りのみ行われます)例えば、メインのハイアベイラビリティインターフェイスがダウンし、あるいは電源が喪失してしまったが、冗長化ハートビートインターフェイスによるやり取りができているのであれば,、ファイルオーバーは発生しません。ただしこの場合、ハイアベイラビリティのインターフェイスは切断されているため、データの同期は行われません。逆に冗長化ハートビートインターフェイスが失われ、しかしハイアベイラビリティインターフェイスではお互いを認識できていたら、やはりフェイルオーバーは起こりません。

冗長化ハートビートインターフェイスは、既存の物理的インターフェイス(例:SSB の外部または管理インターフェイス)上に、仮想的に構築されるものです。

もともとの MAC アドレスは、

Basic Settings > High Availability > Interfaces for Heartbeat > Production MAC に表示され、

冗長化ハートビートインターフェイスの MAC アドレスは、

Basic Settings > High Availability > Interfaces for Heartbeat > HA MAC にて表示されます。

冗長化ハートビートインターフェイスの MAC アドレスは、もともとの物理 MAC アドレスではインターフェイスを形成できないため、仮想的に生成されます。

警告

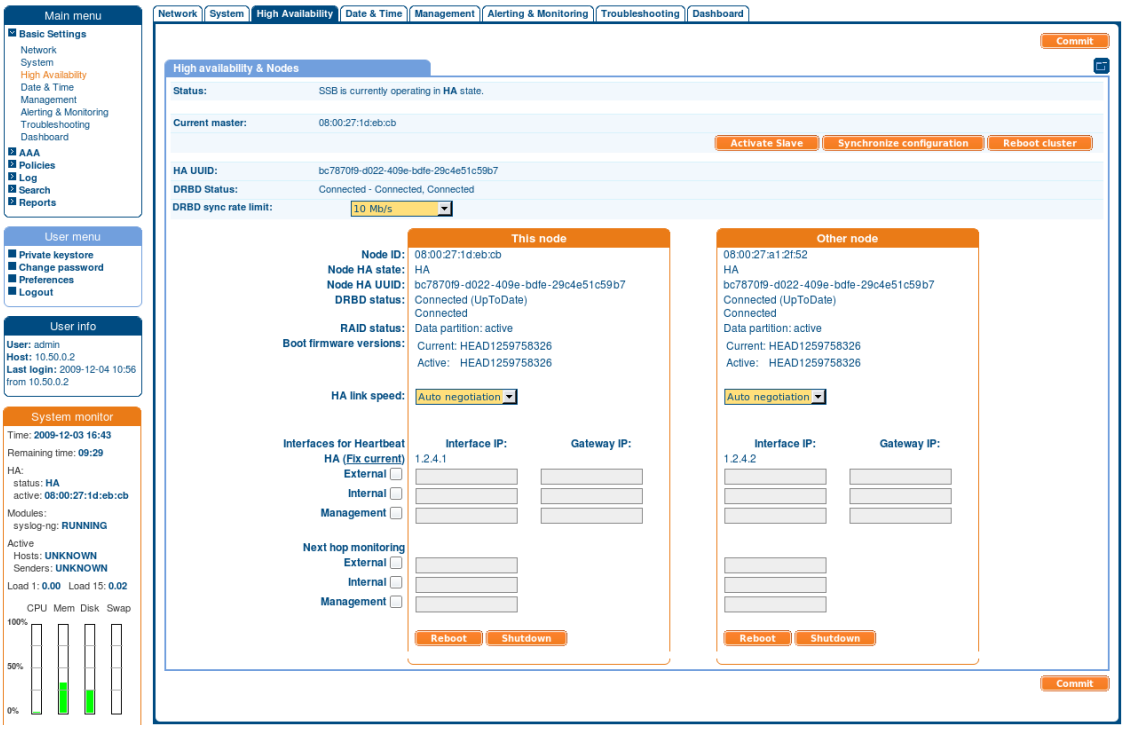
メインのハイアベイラビリティインターフェイスの接続が切れ、その後しばらくして冗長化ハートビートの相互認識も不可となった場合、スレーブノードがアクティブになります。
ただし、マスターノードがしばらくの間アクティブで、その間にデータ同期が全く取られないと、Split brain のステータスになってしまいます。この場合、ハイアベイラビリティに関する機能の修復より前に、Split brain からの回復を**先に**行う必要があります。
詳細は、8.6.2スプリットブレイン状況からのリカバリーをご参照下さい。

冗長化ハートビートインターフェイスの設定方法を説明します。

Step:

Step 1. **Basic Settings > High Availability > Interfaces for Hearbeat** の順にクリックします。

Step 2. 冗長化ハートビートでお使いになりたいインターフェイスを選択します。(例:External)
冗長化ハートビートのインターフェイスに指定されても、そのインターフェイスのもともとのトラフィックには影響ありません。



図表 4.39 冗長ハートビートインターフェイス設定

Step 3. **This node > Interfaces IP** 欄に、選択したインターフェイスの IP アドレスを入力します。ここで設定するIP アドレスは、もう片方のノードからもアクセスできるものでなくてはなりません。冗長化ハートビートインターフェイスにおいて、複数のノードに同一の IP アドレスを持たせることはできません。必要であれば、**Gateway IP** 欄に、ゲートウェイの IP アドレスを入力します。

Step 4. **Other node > Interface IP** 欄に、選択したインターフェイスの IP アドレスを入力します。こちらも、もう片方のノードからもアクセスできるアドレスを設定します。複数で同一のアドレスは持てない点と、Gateway IP を必要に応じて設定する点は Step3 と同様です。

Step 5. 冗長化ハートビートインターフェイスを追加する場合は上記ステップを繰り返します。

Step 6. **Commit** をクリックします。

警告

以上の設定変更を反映させるには、両ノードを再起動する必要があります。
Reboot Cluster をクリックしてください。

4.5.2.4 冗長化ハートビートインターフェイスの説明

目的:

冗長化ハートビートインターフェイスのステータスは、Basic Settings > High Availability > Redundant Hearbeat status あるいは System monitor の HA > Redundant 欄にて確認できます。ステータスは以下のいずれかです。

- ***NOT USED***: 冗長化ハートビートインターフェイスは設定されていません。
- ***OK***: 通常の稼動状態。冗長化ハートビートインターフェイスは正しく稼動しています。
- ***DEGRADED-WORKING***: 二つ以上の冗長化ハートビートインターフェイスが設定されており、うち最低ひとつは正しく稼動しています。新たな冗長化ハートビートインターフェイスが追加され、しかし SSB クラスターがまだ再起動していない場合にもこのステータスが表示されます。
- ***DEGRADED***: 冗長化ハートビートインターフェイスの接続が失われました。原因を究明し、接続を復旧させてください。
- ***INVALID***: 冗長化ハートビートインターフェイスにエラーが発生しました。弊社サポートにご連絡下さい。

4.5.2.5 ネクストホップルータの監視設定

目的:

デフォルトでは、ハイアベイラビリティモードで稼動している際にフェイルオーバーが起こるのは、マスターノードが停止し、スレーブノードから認識ができなくなった場合のみです。マスターノードが、外部のネットワークに接続できなくなった(例:SSB の外部インターフェイス、ルータ、あるいはスイッチの不具合で外部ネットワークに接続できなくなった)が、スレーブノードは問題なく接続できている場合等はフェイルオーバーの対象外です。

こういった状況を回避するには、IP アドレス(通常はネクストホップアドレス)を、マスター・スレイブ双方から、ICMP(ping)で常に監視可能なアドレスに設定することです。このとき、全てのインターフェイスは、同一のネットワークセグメント内にあることが必要です。マスターノードからの監視対象のアドレスの内、一つでも接続不能になり、しかしスレーブノードからはそのアドレスに接続できる場合(言い換えれば、スレーブノードからのアクセス可能アドレスのほうが多い場合)、マスターノード自体は稼動していても、スレイブからみてマスターはアクセス不能になったと判断し、フェイルオーバーが起こります。

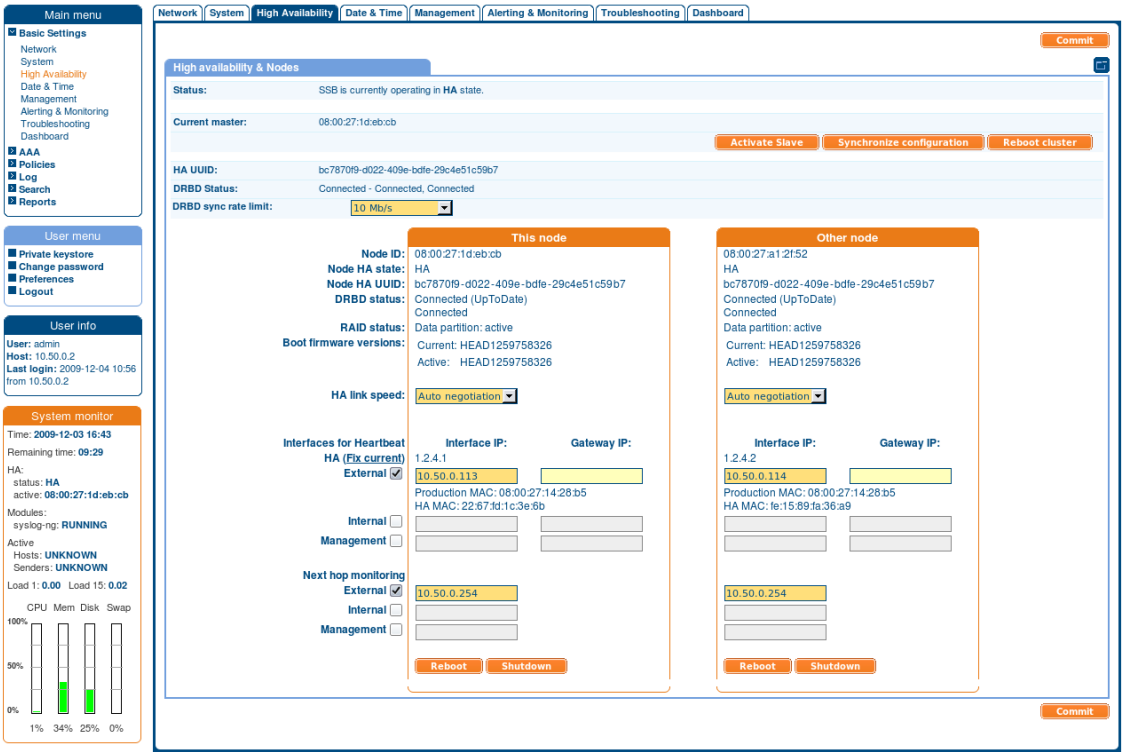
通常、スレーブノードがマスターノードの代わりになるための条件が整っていない場合(例:データの同期が取れていない)、フェイルオーバーは発生しません。

ネクストホップの監視設定方法を説明します。

Step:

Step 1. Basic Settings > High Availability > Next hop monitoring の順にクリックします。

Step 2.　上記ネクストホップルータを監視するためのインターフェイスを選択します。



図表 4.40　ネクストホップモニタリングの設定

Step 3.　選択した側のインターフェイスの **This node > Next hop IP** に、現在マスターとなっているノードから監視する IP アドレス(例：SSB のインターフェイスに接続されている、ルータやスイッチの IP アドレス)を入力します。ここで設定する IP アドレスは、インターフェイス間でアクセス可能であり、かつ同一のローカルネットワークセグメント上に存在する必要があります。

Step 4.　選択した側のインターフェイスの **Other node > Next hop IP** に、現在マスターとなっているノードから監視する IP アドレス(例：SSB のインターフェイスに接続されている、ルータやスイッチの IP アドレス)を入力します。ここで設定する IP アドレスは、インターフェイス間でアクセス可能であり、かつ同一のローカルネットワークセグメント上に存在する必要があります。

Step 5.　他のインターフェイスから監視すべき IP アドレスを追加する必要があるなら、上記ステップを繰り返します。

Step 6.　**Commit** をクリックします。

警告

以上の設定変更を反映させるには、両ノードを再起動する必要があります。**Reboot Cluster** をクリックしてください。

4.5.3 SSBのアップグレード

このセクションでは、SSB を最新バージョンに維持する方法、また必要な際に新たなライセンスファイルをインストールする方法について説明します。

- ■SSBアップグレードの詳細は、4.5.3.1 SSBファームウェアのアップデート
- ■SSBクラスターのファームウェアップグレードの詳細は、4.5.3.1.2ハイアベイラビリティシステムのコア及びブートファームウェアのアップグレード
- ■新しいライセンスファイルのインストールに関して詳細は、4.5.3.2SSBライセンスキーのアップデート
- ■SSBの設定ファイルのインポート/エクスポートに関して詳細は、4.5.3.3 SSBの設定ファイルをエクスポートする

を、それぞれご参照下さい。

警告

featureリリース版から旧バージョン(=サポート外です)へ、または安定板へのダウングレードは推奨しません。安定版から feature リリース版へーたびアップグレードを行ったら、次の安定版がリリースされるまではその feature リリース版を継続してお使いいただくか、サポート対象外の古いバージョンに戻していただくリスクを負っていただくかのどちらかになります。

4.5.3.1 SSBファームウェアのアップデート

SSB は、新たなバージョンのファームウェアがリリースされた後、アップデートできます。現在稼動しているファームウェアのバージョンを表示させるには、**Basic Settings > System > Version details** の順にクリックします。以下の情報が表示されます。

■**Core firmware/Boot firmware**：現在 SSB 上で稼動しているファームウェアのバージョン。

■**Build date**：稼働中のファームウェアが作成された日付。

アップデート手順に関しては後述します。

警告

新たなファームウェアのアップロードを行う前に、SSB 設定ファイルのバックアップを保存してください。詳細は、4.5.3.3 SSBの設定ファイルをエクスポートするをご参照ください。

アップグレードの前に、必ずリリースノートを呼んでください。そのバージョン特有の注意事項が記載されているかもしれないからです。リリースノートは、http://www.balabit.com/network-security/syslog-ng/log-server-appliance/support/から参照いただけます。

■スタンドアロンのSSBのアップグレード手順は、4.5.3.1.1 SSBのアップデートとファームウェアの管理

■SSBクラスターのアップグレード手順は、4.5.3.1.2 ハイアベイラビリティシステムのコア及びブートファームウェアのアップグレード

に、それぞれしたがってください。また、

■(可能な場合のみ)以前のバージョンのファームウェアに戻す手順の詳細は、4.5.3.1.3 以前のバージョンのファームウェアに戻すを、ご参照ください。

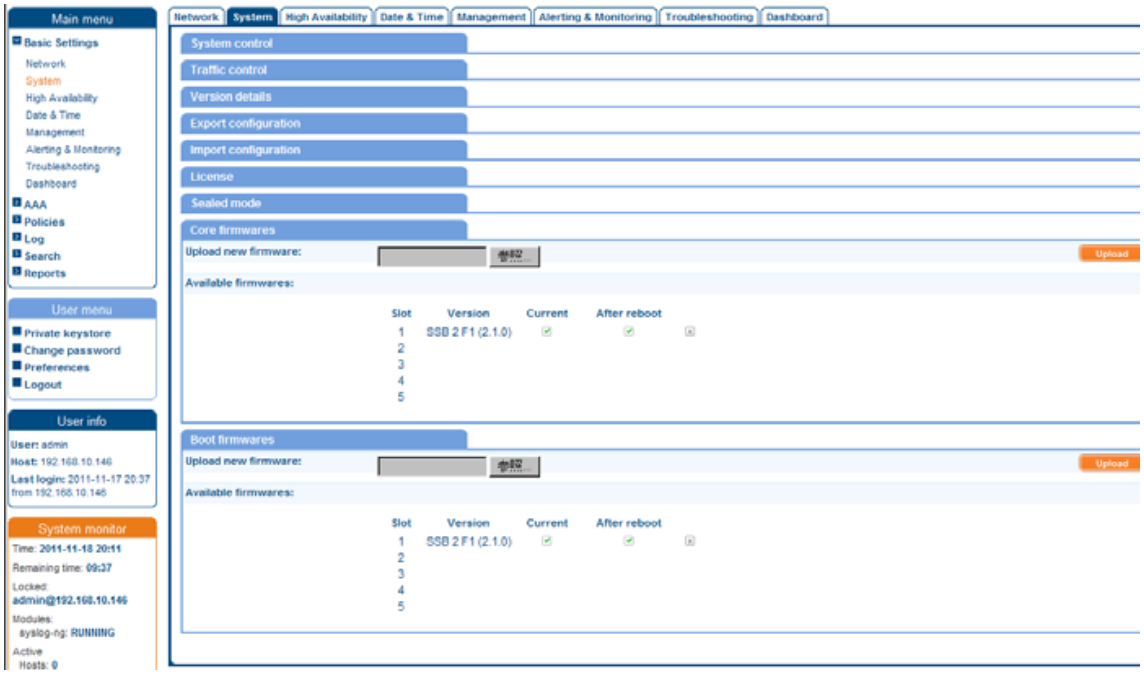
4.5.3.1.1 SSBのアップデートとファームウェアの管理

Step:

Step 1. Balabit社のWebサイトから、最新のファームウェアをダウンロードします。(こちらから)

Step 2. SSB に戻り、Basic Settings > System の順にクリックします。

Step 3. 内部(コア)ファームウェアをアップデートする場合、**Core firmwares** を選択します。外部(ブート)ファームウェアをアップデートする場合、**Boot firmware** を選択します。



図表 4.41　ファームウェアの管理

これらと異なるファームウェアに関しては、2.7 SSBのファームウェアをご参照ください。

Step 4.　**参照**ボタンをクリックし、アップロードするファームウェアを選択します。
拡張子は .bin です。

Step 5.　Upload をクリックします。アップロードが終わると、Available firmwares list に追加されます。

Step 6.　アップロードしたファームウェアの、After reboot の下の□にチェックを入れます。

Step 7.　System Control > This node の順にクリックし、Rebbot をクリックして再起動させます。

ヒント

SSB が起動した際、立ち上がったファームウェアのバージョン番号を含むログメッセージが system log に出力されます。

注記

アップグレード後、SSB の Web インターフェイスの表示に問題が発生した場合は、ブラウザのキャッシュをクリアするか、あるいは「スーパーリロード」(例：shift+F5) を行ってください。

4.5.3.1.2 ハイアベイラビリティシステムのコア及びブートファームウェアのアップグレード

目的:

ブートファームウェア、コア(内部)ファームウェア双方のアップグレードを必要とするリリースがあった場合のアップグレード手順を説明します。

Step:

Step 1. コア(内部)・ブート(外部)両方のファームウェアをダウンロードします。

Step 2. Web インターフェイスから、コアファームウェアをアップデートします。

Step 3. **Basic Settings > System > Core firmwares** の順にクリックし、ダウンロードしたコアファームウェアをアップロードします。

Step 4. アップロードが終了したら、リストに追加された新しいファームウェアの **After reboot** オプションにチェックを入れます。

警告

この段階ではまだ再起動を行いません。コア・ブート両方のファームウェアがアップデートされてから行います。

Step 5. ブートファームウェアに関して、ステップ 1 と 2 を同様に行います。

Step 6. **Basic Settings > High Availability > Reboot Cluster** の順にクリックし、両ノードを再起動します。

警告

データ喪失にご注意ください！この手順を実行すると、それまでのアクティブなネットワーク接続は全て切断されます。この作業は、保守の時間にのみ行い、データ喪失を起こさないよう留意してください。

注記

アップグレード後、SSB の Web インターフェイスの表示灯に問題が発生した場合は、ブラウザのキャッシュをクリアするか、あるいは「スーパーリロード」(例: shift+F5) を行ってください。

4.5.3.1.3 以前のバージョンのファームウェアに戻す

目的:

SSB は、5 代の異なるバージョンのファームウェアを保持しておくことができます。必要であれば、その 5 代のうちいずれでも SSB を起動させることが可能です。起動時使用可能なファームウェアは、**Basic Settings > System > Boot fiemware** 及び、**Basic Setings > System > Core firmware** にて確認できます。一覧には、バージョン番号、リビジョン番号、作成日といった、それぞれのバージョンに関する情報が表示されています。現在稼動しているバージョンのファームウェアは、Current 列の□にチェックが入っています。また、SSB が再起動する場合、その後立ち上がってくるバージョンの After reboot 欄□に、やはりチェックが入っています。

以前のバージョンで SSB を起動させる手順について説明します。

警告

SSBのファームウェアのアップグレードの場合は、設定ファイルも自動的にアップデートされます。しかし、以前のバージョンに戻す場合、単に旧バージョンのファームウェアでSSBを起動しただけでは不完全です。旧バージョンのファームウェアは、新しいバージョンのファームウェア上で作られた設定ファイルを読込めないからです。この様な場合は、コンソールからログインし、Revert Configrationオプションを**ON**にし、ファームウェアがアップグレードされる前の状態と同じ設定ファイルにします。コンソールメニューの詳細は、4.5.4.1 SSBのコンソールメニューを使用するをご参照ください。

警告

featureリリース版から旧バージョン(=サポート外です)へ、または安定板へのダウングレードは推奨しません。安定版から feature リリース版へーたびアップグレードを行ったら、次の安定版がリリースされるまではその feature リリース版を継続してお使いいただくか、サポート対象外の古いバージョンに戻していただくリスクを負っていただくかのどちらかになります。

Step:

Step 1. Basic Settings > System の順にクリックし、Boot fimeware のタブをクリックして展開させます。

Step 2. ファームウェアのバージョンを選択し、**After reboot** の下の□にチェックを入れます。

Step 3. 続いて、**Core firmware** のタブをクリックして展開させます。

Step 4. ファームウェアのバージョンを選択し、**After reboot** の下の□にチェックを入れます。

Step 5. System Control > This node > Reboot の順にクリックして SSB を再起動します。SSB をハイアベイラビリティのクラスターでお使いの場合は、Basic Settings > High Availability > Reboot Cluster の順にクリックします。

4.5.3.2 SSBライセンスキーのアップデート

目的:

お使いの SSB ライセンスの有効期限が切れる以前に、あるいは新たなライセンスをご購入いただいた際は、ライセンスキーをアップデートしていただく必要があります。現在適用されているライセンスに関しては、**Basic Settings > System > License** 画面にてご確認いただけます。以下の情報が表示されます。

図表 4.42 ライセンスのアップデート

■ **Customer**:ライセンス使用を許された会社名

■ **Serial**:ライセンスのユニークなシリアル番号

■ **Host limit**:このライセンスにおいて SSB がログを受信できるデバイスの上限台数

SSB は、ライセンスが期限切れとなる 1 週間前に、自動でアラートを発行します。Host limit で指定されている台数の 90 パーセントを超える接続台数が設定されると、やはりアラートを自動発行します。

ライセンスキーをアップデートする手順を説明します。

警告

ライセンスキーのアップデートを行う前に、設定ファイルのバックアップを取得することを推奨します。詳細は、4.5.3.3 SSBの設定ファイルをエクスポートするをご参照ください。

Step:

Step 1. **Basic Setings > System > License** の順にクリックします。

Step 2. **参照**をクリックしてアップデートすべき新たなライセンスキーのファイルを選択します。

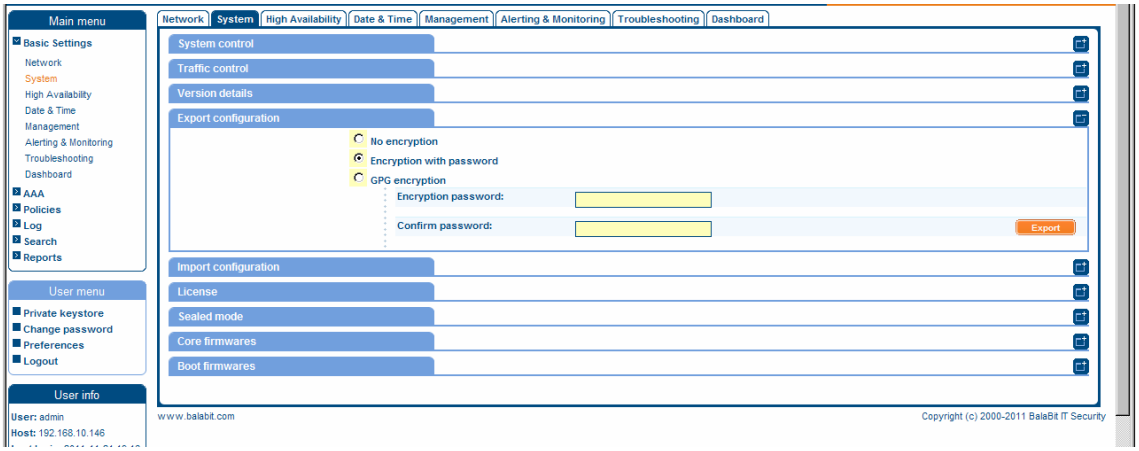
Step 3. **Upload** をクリックし、**Commit** をクリックします。

Step 4. **Traffic control > Syslog traffic > Restart syslog-ng** の順にクリックし、新しいライセンスを有効にします。

4.5.3.3 SSBの設定ファイルをエクスポートする

目的:

SSB の設定ファイルは、手動で、あるいは他の SSB ユニットに移植する形でのエクスポートが可能です。**Basic Settings > System** 画面から、実行したい操作のボタンをクリックします。



図表 4.43 SSB の設定ファイルをエクスポートする

Step:

Step 1. Basic Settings > System の順にクリックし、Export configuration タブをクリックして展開させます。

Step 2. 設定ファイルをどう暗号化するかを選択します。

■暗号化せずにエクスポートするには、No encryption を選択します。

警告

暗号化せずに設定ファイルをエクスポートすることは推奨しません。パスワードのハッシュや秘密鍵等、重要なデータを含んでいるからです。

■パスワードのみで保護する場合は、**Encrypt with password** を選択し、**Encryption password** 欄と **Confirm password** 欄に、パスワードを入力します。

■GPG鍵で暗号化する場合は、**GPG cncryption**を選択します。なお、ここで用いるGPG鍵は、自動システムバックアップで用いられるときのと同一の鍵であること、また、**Basic Settings > Management > System backup**でGPG鍵の公開部分をアップしておかないと使用できない点にご注意ください。詳細は、4.3.5.3 GPGを用いて、設定ファイルのバックアップを暗号化するをご参照ください。

Step a **Export** をクリックします。

注記

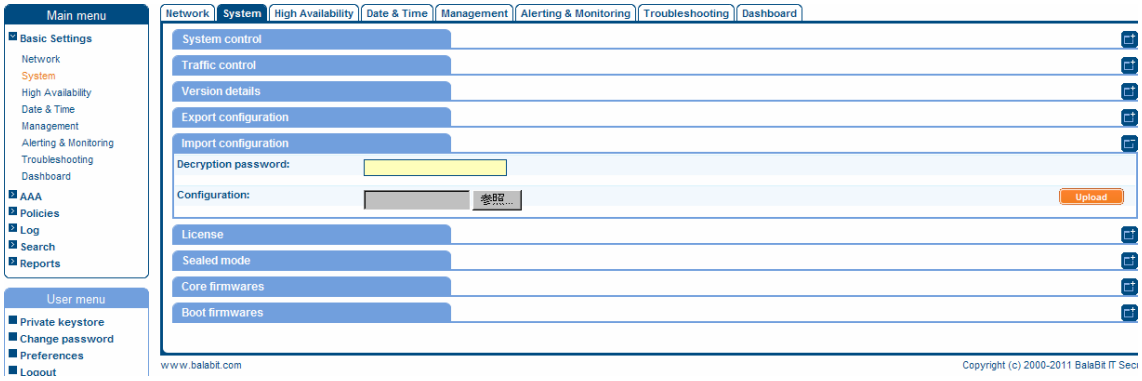
エクスポートされたファイルは、gzip 圧縮形式になります。Windows 環境で解凍するには、free-7-Zip tool などの解凍ツールが必要になります。

エクスポートされたファイルのファイル名は、{ホスト名_of_SSB}-YYYYMMDDHHMM.config になります。パスワード保護で保存した場合は「-encrypted」サフィックス、GPG 暗号化の場合は、「-gpg」サフィックスが、それぞれ付加されます。

4.5.3.4 SSBの設定ファイルをインポートする

目的:

SSB の設定ファイルは、**Basic Settings > System** 画面からインポートが可能です。実行したい操作のボタンをクリックします。



図表 4.44 SSB の設定ファイルのインポート

警告

古いバージョンにおける設定ファイル(例:SSB1.0)を、新しいバージョン(例:2.0)にインポートすることは出来ません。

Step:

Step 1. **Basic Settings > System** の順にクリックし、**Import configuration** タブをクリックして展開させます。

Step 2. **参照**をクリックし、インポートすべき設定ファイルを選択します。

Step 3. 設定ファイルがパスワード保護されている場合は、**Encryption password** 欄に、パスワードを入力します。Upload をクリックします。

警告

設定ファイルをインポートした際は、そのファイルをエクスポートした後に、ログスペースに新たなログが積みあがっていることが考えられます。インポート後もそのログスペースは保持されますが、アクセスは出来なくなります。再度アクセス可能にするためには、以下を行ってください。

1. **Log > Spaces** の順にクリックし、ログスペースの設定を行います。**Access Control** 欄に入力することはとても重要です。そうでないと、**Search > Logs** から、アクセスすることが出来ません。
2. **Log > Paths** 画面から、ログのパスを設定します。ログをログスペースに向かって転送していたログパスを再設定する必要があります。

4.5.4 SSBのコンソールにアクセスする

ここでは、SSB コンソールメニューの使い方、SSH によるリモート接続の方法、Web インターフェイスからの root 権限パスワードの変更方法を説明します。

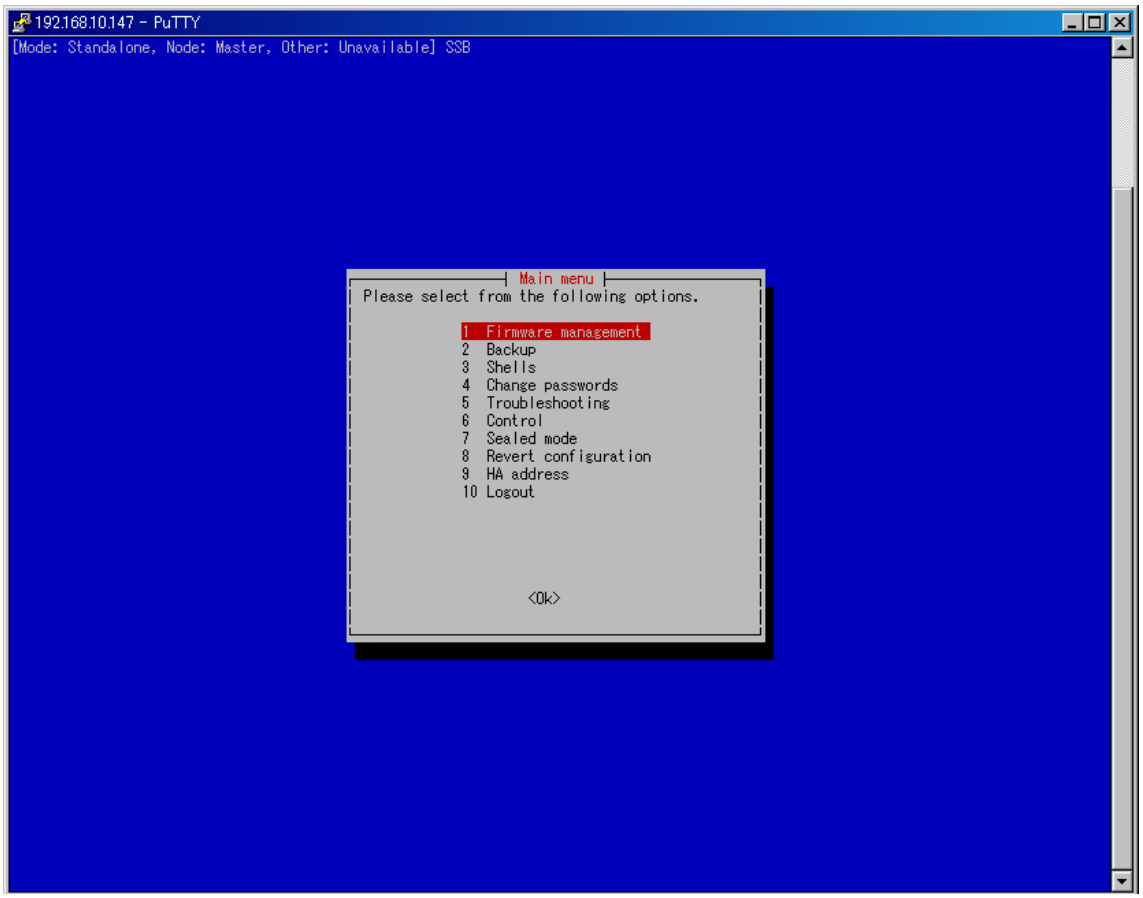
ヒント

サーバールーム内で SSB アプライアンスをすばやく見つけるには、Web インターフェイスの Basic Settings > System > Hardware information の順にクリックし、Blink system idenrification lights を ON にします。これにより、SSB ハードウェアプライアンスの、前面ハードディスクトレイ LED が赤に点滅します。なお、この機能は SSB5000 及び SSB10000 のみ実装しています。

4.5.4.1 SSBのコンソールメニューを使用する

SecureShell(SSH)を用いてローカルで、またはリモートアクセスすることにより、SSB のコンソールメニューをお使いいただけます。コンソールメニューから、SSB のもっとも基本的な設定及び管理項目にアクセスすることが可能になります。なお、コンソールメニューへのアクセスは、主にトラブルシューティングの目的においてです。メインのインターフェイスは WebUI です。

コンソールメニューには、ウェルカムウィザードで設定したパスワードで認証される root ユーザがアクセスできます。



図表 4.45 コンソールメニュー

コンソールメニューにアクセスすることにより、以下のオペレーションが可能になります。

■アクティブなコアならびにブートファームウェアを選択する、あるいは不要なファームウェアを削除する。コンソールからのファームウェア管理は、アップグレード後うまく動作しない場合、または前バージョンをアクティベイトしようとした際、Web インターフェイスからアクセス不能の場合に役立ちます。

■バックアップを開始する

■root 及び admin ユーザのパスワード変更

■コア及びブートファームウェアのローカルシェルへのアクセス。通常はこの様なオペレーションを推奨しません。トラブルシューティングでどうしても必要なときのみ行ってください。

■ネットワークトラブルシューティング機能にアクセスする、または閲覧可能なログファイルにアクセスする。

■システムの再起動及びシャットダウン

■シールドモードのON・OFF。詳細は、4.5.5シールドモードをご参照ください。

■設定ファイルを前に戻す。詳細は、4.5.3.1.3以前のバージョンのファームウェアに戻すをご参

照ください。

■ハイアベイラビリティインターフェイスの IP アドレスを設定する

注記

コンソールメニューにアクセスが発生している間、Web インターフェイスからのアクセスは排他されます。つまり、コンソールアクセスは、Web インターフェイスからのアクセスが 1 件もない場合にのみ可能です。コンソールアクセスをしようとする際、既に接続されていた Web インターフェイスからのアクセスは、強制的に切断されます。

4.5.4.2 SSBホストへのSSHによるアクセスを可能にする

目的:

トラブルシューティングの目的に限定の上、SSH によるコンソールアクセスを行ってください。ウェルカムウィザードを完了させると、SSH によるアクセスは不可能に設定されます。再度可能にする方法を説明します。

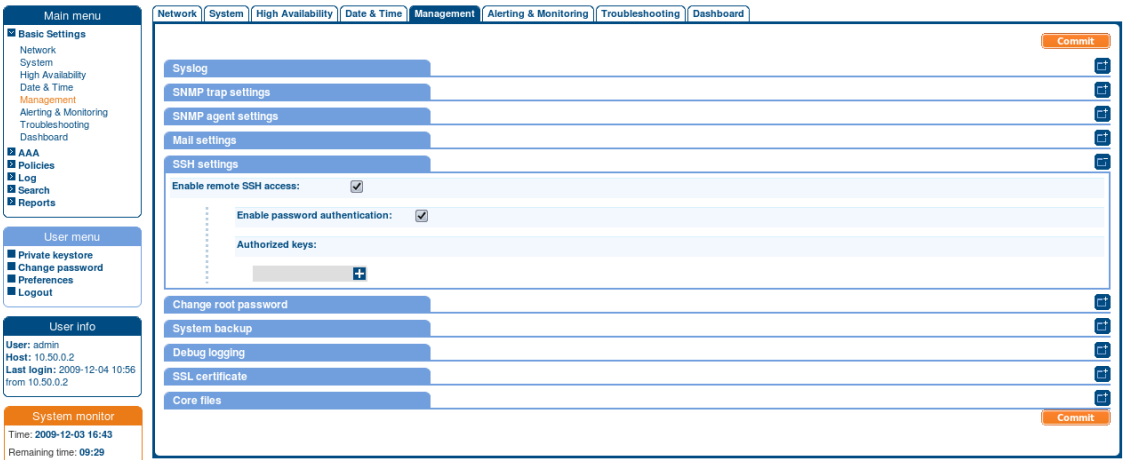
警告

SSH で直接 SSB ホストにアクセスすることは推奨しておりませんし、サポートの対象外です。ただしトラブルシューティングに関しては例外です。SSH によるコンソールアクセスを必要とするようなトラブルの際は、弊社サポートにご連絡ください。問題解決の手順をお示しいたします。

SSHによるアクセスを可能にすると、rootユーザとして、リモート環境からSSBにログインできます。rootユーザのパスワードは、ウェルカムウィザードで入力されたものが使用されます。Webインターフェイスからrootユーザのパスワードを変更するには、4.5.4.3 rootユーザのパスワードを変更するをご参照ください。

Step:

Step 1. Basic Settings > Management > SSH settings の順にクリックします。



図表 4.46 SSB へのリモート SSH 接続有効化

Step 2. **Enable remote SSH access** オプションを ON にします。

注記

シールドモードが有効になっている場合、SSH アクセスは自動的に無効になります。詳細は、4.5.5シールドモードをご参照ください。

Step 3. リモート SSH 接続の認証方法を指定します。

- パスワード認証にするには、**Enable password authentication** オプションにチェックを入れます。
- 公開鍵認証を行うには、**Authorized keys** 欄の をクリックして公開鍵欄を展開させ、 をクリックして、SSB をリモートアクセス及び管理できるユーザの秘密鍵をアップロードします。

Step 4. **Commit** をクリックします。

SSBのSSHサーバーは、管理インターフェイスが設定されている場合は、その管理インターフェイスからのみの接続を受け付けます。設定されていない場合は、外部インターフェイス経由での接続を受付けます。可能な限り、管理インターフェイスが設定されていない場合にSSHアクセスを可能にはしないでください。管理インターフェイスの設定に関して詳細は、4.3.1.1管理インターフェイスの設定をご参照ください。

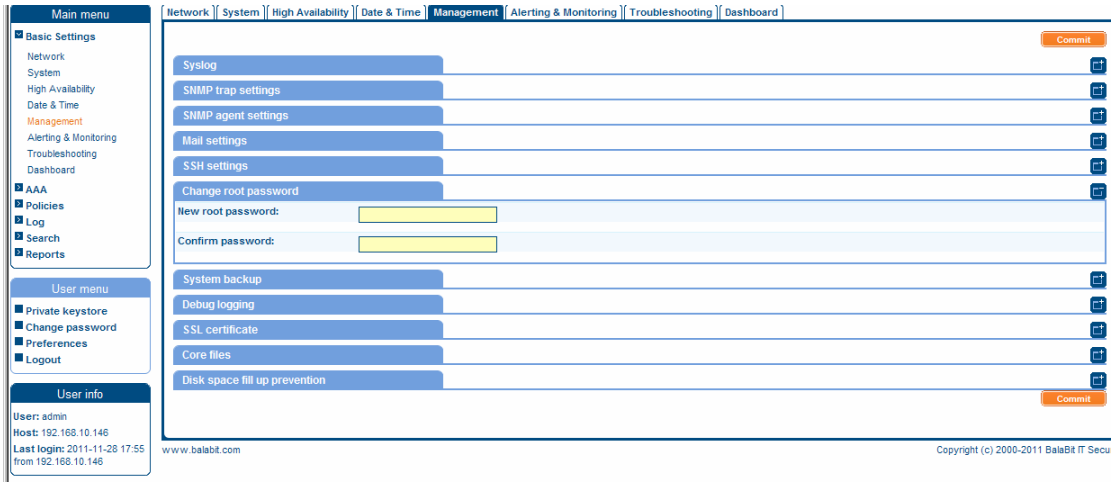
4.5.4.3 rootユーザのパスワードを変更する

目的:

rootユーザのパスワードは、SSBのコンソールにローカルで、またはSSHでリモート接続する場合に必要です。rootユーザは、コンソールメニューからもパスワードを変更できることに留意してください。詳細は、4.5.4 SSBのコンソールにアクセスするをご参照ください。

Step:

Step 1. **Basic Settings** > **Management** > **Change root password** の順にクリックします。



図表 4.47 SSB のパスワード変更

Step 2. **New password** 欄に、新たなパスワードを入力し、**Confirm password** 欄に再度入力します。

注記:
SSB のパスワードには、以下の特殊文字を含めることができます。
`!"#$%&'()*+,-./:;<=>?@[\]^-`{|}`

Step 3. **Commit** をクリックします。

4.5.5 シールドモード

シールドモードが有効になっているとき、以下の設定が自動的に適用されます。

- SSH によるリモートアクセスは不可
- root ユーザのパスワードは変更不可
- シールドモードはローカルコンソールからのみ無効に出来る。詳細は、4.5.5.1シールドモードを無効にするをご参照ください。

シールドモードを有効にするには、以下のいずれかのオペレーションを行ってください。

- ウェルカムウィザードで、シールドモードオプションを ON にする。
- Web インターフェイスで、**Basic Settings** > **System** > **Seald mode** の順にクリックし、**Activate sealed mode** をクリックする。
- ローカルコンソールまたは SSH で、root ログインする。コンソールメニューで、**Sealed mode** > **Enable** の順に押下する。

4.5.5.1 シールドモードを無効にする

目的:

シールドモードを無効にする手順を説明します。

Step:

Step 1. SSB アプライアンスの場所に行きます。

Step 2. コンソールから、root でログインします。

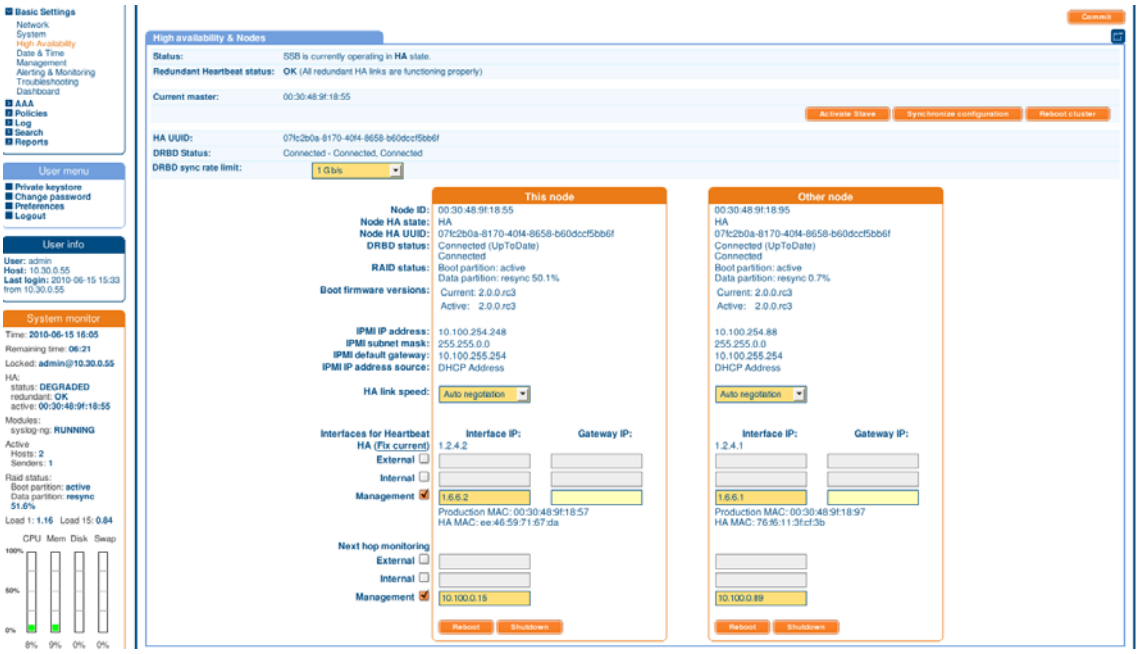
Step 3. コンソールメニューで、**Seald mode > Disable** の順に押下します。

Step 4. **Back to Main menu > Logout** の順に押下します

4.5.6 SSBのアウトオブバンド 管理

SSB には、インテリジェントプラットフォームマネージメントインターフェイス(IPMI)V2.0 スタンダードに準拠した専用のアウトオブバンド管理インターフェイスが含まれています。IPMI インターフェイスは、管理者に SSB のシステムヘルスを監視させ、コンピューターイベントをリモートで SSB の OS とは独立して、管理させることができます。SSB は、IPMI インターフェイスが物理的にネットワークに接続されているときのみ、IPMI インターフェイスからアクセスできます。

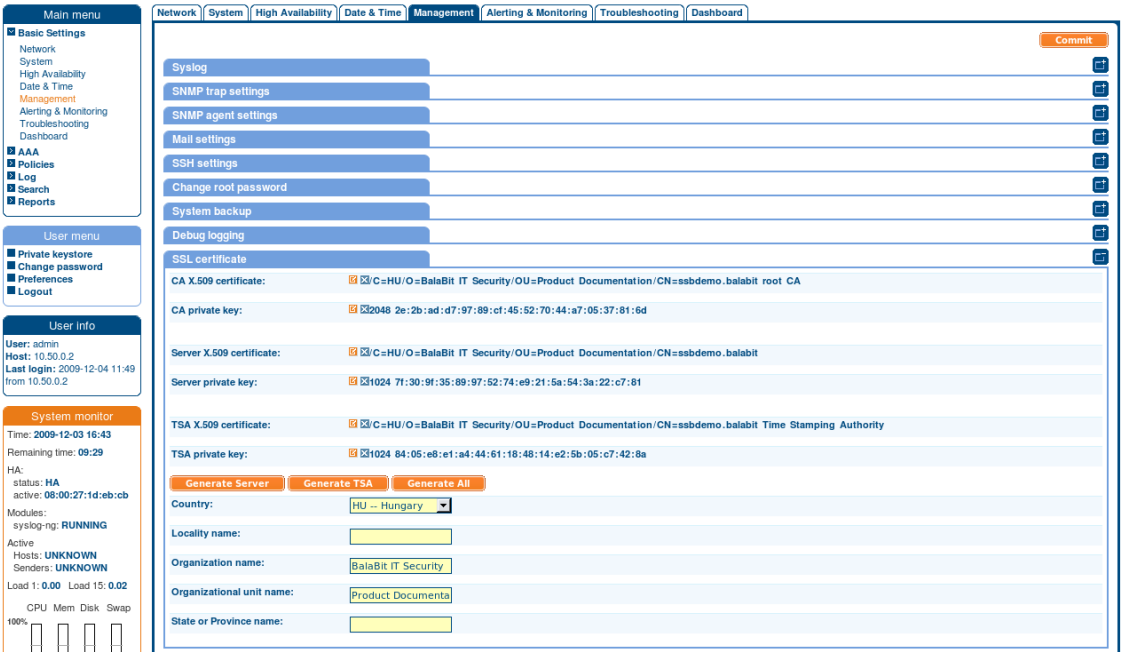
IPMI インターフェイスの基本情報は、**Basic Settings >High Availability** の WEB インターフェイスでも確認できます。以下の情報が表示されます。



図表 4.48 IPMI インターフェイスの情

4.5.7 SSBに適用されている証明書を変更する

SSB は、タスクごとにさまざまな証明書を適用させることが可能です。
Basic Settings > Management > SSL certificate メニューで管理できます。



図表 4.49 SSB における Web 証明書の変更

このメニューで、以下の証明書の設定変更が可能です。

■CA 証明書：SSB 内蔵の認証機関によるもの。この機関は、自己署名の証明書ならびに SSB によって生成された証明書に対して認証をする役割を持っています。例：Web インターフェイスの証明書、内部タイムスタンプ認証機関(TSA 証明書)

■サーバー証明書：SSB と管理者のコミュニケーションを暗号化するために用いられる、SSB Web インターフェイスの証明書

注記：
この証明書が変更された場合、SSB ユーザのブラウザは、このサイトの証明書が変更されたことを警告メッセージとして表示します。

■TSA 証明書：暗号化されたログ保存領域が生成された際、タイムスタンプを付与する内部機関

全ての証明書に関し、X.509 の識別名(DN)と、秘密鍵の指紋が表示されます。証明書全てを表示させるには、DN をクリックします。秘密鍵の公開部分を表示させるには、指紋の部分をクリックします。SSB において、秘密鍵そのものだけをダウンロードすることは不可能ですが、証明書はさまざまなフォーマットで(例：PEM、OpenSSH、Tectia)ダウンロードすることが出来ます。

注記:
ここで説明されている以外の部分では、SSB はさらに別の証明書を必要とする場合があります。

証明書を変更するには、SSB にて新たな証明書を生成するか、あるいは外部 PKI(Public Key Infrastructure/公開鍵基盤)を利用して生成した証明書をアップロードします。

■SSBにて証明書と鍵を生成するには、4.5.7.1 SSBの証明書を生成する手順を行ってください。

■外部PKIによる証明書をアップロードするには、4.5.7.2 外部認証による証明書をアップロードする手順を行ってください。

注記:
御自身の PKI による証明書をアップロードすることも可能です。ただし、SSB にて生成された証明書は破棄することは出来ないので、脆弱な場合は、セキュリティ面でのリスクになる可能性があります。

4.5.7.1 SSBの証明書を生成する

Step:

Step 1. Basic Settings > Management > SSL certificate の順にクリックします。

Step 2. 新たな証明書に関する、以下の事項を入力します。

Step a. ***Country***: SSB が稼動しているサーバーのある国名を入力します。

Step b. ***Locality***: SSB が稼動しているサーバーのある都市名を入力します。

Step c. ***Organization***: SSB を所有している会社名を入力します。

Step d. ***Organization unit***: SSB を所有している会社の部署名を入力します。

Step e. ***State or Province***: SSB が稼動しているサーバーのある州または県を入力します。

Step 3. SSBWeb インターフェイスの証明書を新たに生成したい場合は、**Generate Server certificate** をクリックします。
タイムスタンプ認証用の証明書を新たに生成するには、**Generate TSA certificate** をクリックします。
SSB 内部の認証機関向け証明書を生成するには、Generate All をクリックします。
この場合は、サーバー及び TSA 証明書が同時に生成されます。

注記:
新たな証明書が生成される過程で、サーバー及び TSA 証明書は、認証局による証明書の情報を元に署名されます。外部認証局の証明書をアップロードしている場合、新たなサーバー及び TSA 証明書が生成される際には、その情報が参照されます。

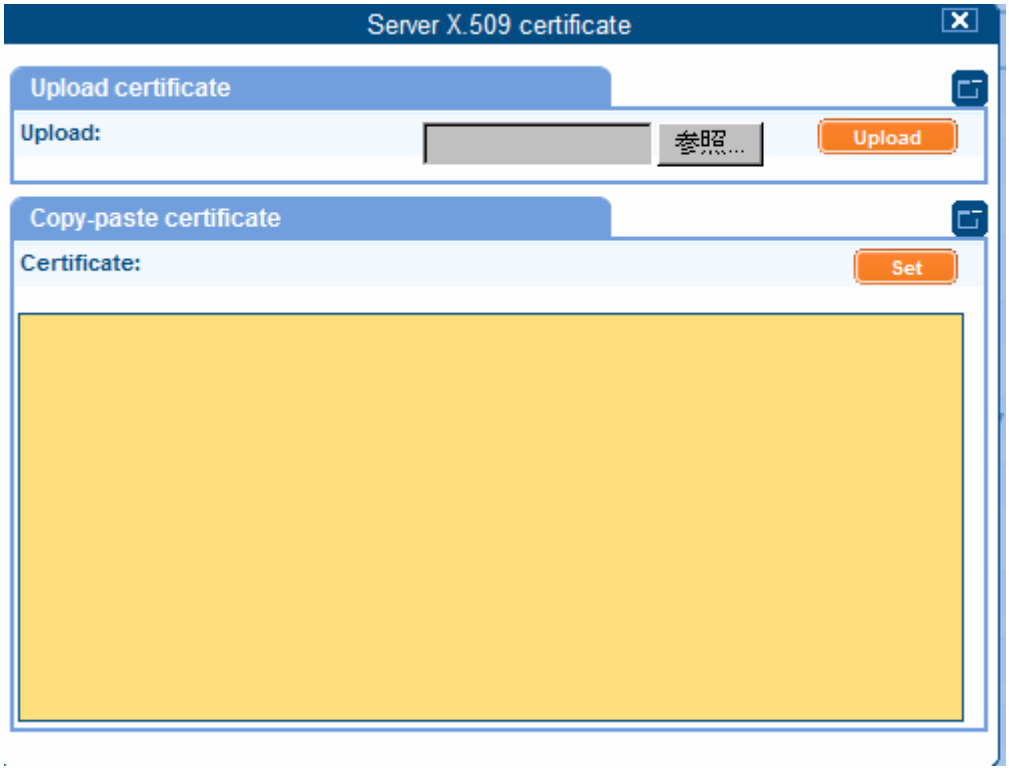
Step 4. **Commit** をクリックし、変更を反映させます。

4.5.7.2 外部認証による証明書をアップロードする

Step:

Step 1. Basic Settings > Management > SSL certificate の順にクリックします。

Step 2. 修正したい証明書横の をクリックします。ポップアップウインドウが表れます。



図表 4.50 証明書のアップロード

参照をクリックし、証明書を包含しているファイルを選択し、**Upload** をクリックします。あるいは、証明書の中身をコピーし、**Copy paste certificate** 欄に貼り付けて、**Set** をクリックすることも出来ます。

注記:
SSB は PEM 形式のみ認識します。DER 形式は現在のところサポートしていません。

Step 3. 証明書に関連する秘密鍵をアップロードしたい場合は、修正したい秘密鍵の左の をクリックします。ポップアップウインドウが表れます。Step2 と同様、ファイルから選択して Upload をクリックするか、または中身をコピーして貼り付け、Set をクリックするか、いずれかの方法でアップデートします。

注記:
SSB は、PEM(RSA 及び DSA)、PUTTY、SSHCOM/Tectia 形式の秘密鍵を認識可能です。パスワード保護された秘密鍵もサポートしています。

4.5.8 ホストリストポリシーを作成する

SSB では、例えばソースにログを送信するクライアントを限定する、あるいは共有スペースに蓄積されたログへアクセスできるホストを限定する、といった場合に「ホストリスト」をあらかじめ作成して、適用させます。

■ホストリストの作成手順に関しては、4.5.8.1ホストリストを作成する

■ホストリストをファイルからインポートする手順に関しては、4.5.8.2ファイルからホストリストをインポートする

をそれぞれご参照ください。

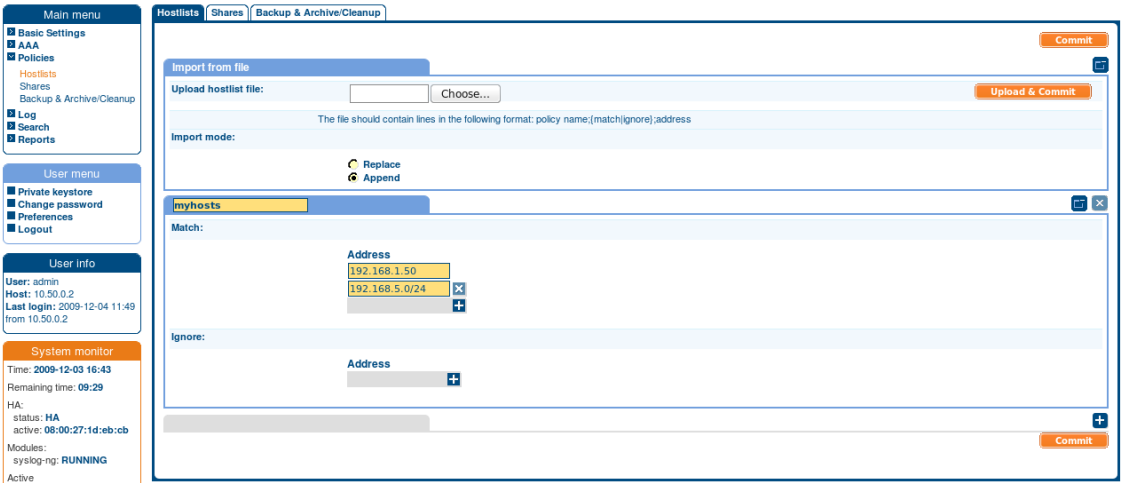
4.5.8.1 ホストリストを作成する

目的:
新たなホストリストを作成する手順を説明します。

Step:

Step 1. **Policies** > **Hostlist** の順にクリックし、をクリックして展開させます。

Step 2. ホストリストの名前を決定し、入力します。(例:servers)



図表 4.51 ホストリストの作成

Step 3. 許可するホストの IP アドレスを、**Match > Address** 欄に入力します。その際、サブネットマスクを付加することもできます。(プリフィックス表記。例：192.168.1.1/24)さらにホストを追加する場合は、入力欄右下の＋をクリックし、この手順を繰り返します。

Step 4. 許可しないホストを設定する場合は、**Ignore > Address** 欄に、該当するホストの IP アドレスを入力します。

ヒント

いくつかのホストを除いて全てのホストを許可とする場合は、Match のリストには IP アドレス 0.0.0.0/0 を、そして Ignore のリストに、許可しないホストのアドレスを入力します。

Step 5. Commit をクリックします。

警告

ホストリストを作成/変更したら、**Basic Settings > System > Traffic control** の順にクリックし、Restart syslog-ng を選択して、変更を反映させてください。

4.5.8.2 ファイルからホストリストをインポートする

目的：

テキストファイルからホストリストをインポートする方法を説明します。

Step：

Step 1. ホストリストのポリシーと、IP アドレスを含んだテキストファイルを作成します。記述されている全ての行の IP アドレスまたはネットワークがポリシーに追加されます。書き方は以下の形式です；

ポリシー名；{ignore|match}；IP アドレス

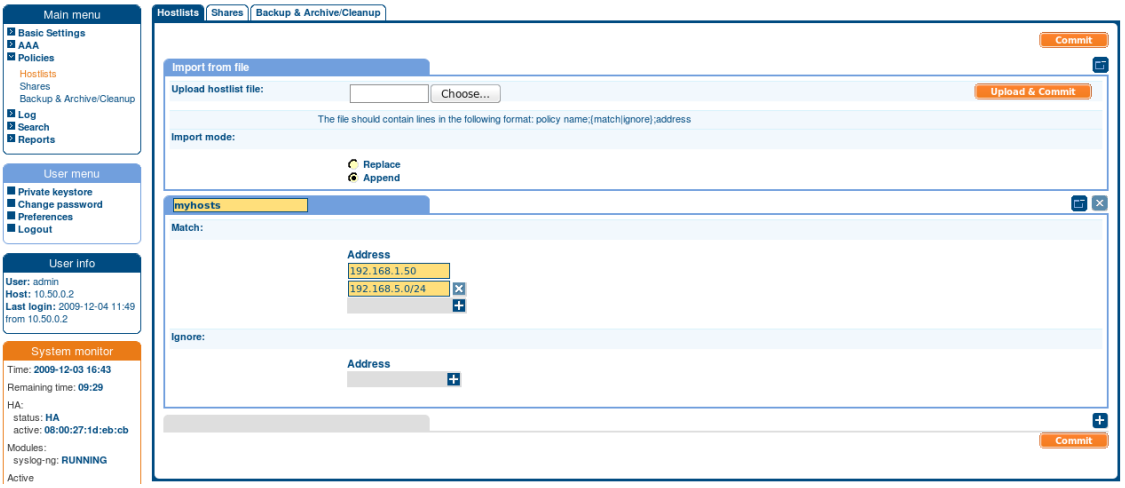
例：192.168.5.5 のホストは不許可、サブネット 10.70.0.0/24 内の全ホストを許可する場合

```
policy1;ignore;192.168.5.5
policy2;match;10.70.0.0/24
```

同じポリシーに複数のホストまたはネットワークを含める場合、全てを 1 行ごとに記述します。以下が例です。

```
policy1;ignore;192.168.7.5
policy1;ignore;192.168.5.5
policy1;match;10.70.0.0/24
```

Step 2. Policies > Hostlists > Import from file の順にクリックし、参照をクリックしてインポートするファイルを選択します。



図表 4.52 ホストリストのインポート

Step 3. 既存のポリシーに、新たにホストを追加する場合は、**Append** を選択します。これからアップロードするホストリストで、既存のリストを上書きする場合は、**Replace** を選択します。

Step 4. **Upload** をクリックし、その後、**Commit** をクリックします。

警告

ホストリストを作成/変更したら、**Basic Settings > System > Traffic control** の順にクリックし、Restart syslog-ng を選択して、変更を反映させてください。

4.6 SSBにおけるSANへのアクセス管理

SAN 上のボリュームは、例えば Sun Common Array Manager(CAM)といったような専用のアプリケーションによって管理されます。一例が Sun StorageTek モジュールです。SAN 上のモジュールに新たなボリュームを作成したら、**Basic Settings > Storage > Refresh** の順にクリックし、SSB からそのボリュームにアクセスできるようにしてください。

警告

ボリュームマッピングに用いられる LUN(論理識別番号)は、1 から 30 の間にしてください。0、または 31 以上の値では、SSB が SAN ボリュームにアクセスすることはできません。

警告

SSB がアクセスしているボリュームをアンマップしないでください。SSB の再起動が必要になってしまいます。

5　SSBのシスログサーバーを設定する

この章では、SSB のシスログサーバーをどのように設定するかを説明していきます。特に重要なのは以下の項目です。

- リモートホストからSSBがログメッセージを受信できるようにする手順は、5.1メッセージソースの設定
- ログメッセージを、SSBのローカル環境に、暗号化された状態またはプレーンテキストファイルで保存する手順は、5.2 SSBにログメッセージを蓄積する
- ログメッセージを外部のサーバー(例：ログ解析エンジン)や、SQLデータベースに転送する手順は、5.3 SSBからログメッセージを転送する
- 意図した宛先へログメッセージを誘導する手順は、5.4ログパスを管理する
- syslog-ngサーバーのグローバルオプションに関して詳細は、5.5　syslog-ngのオプションを設定する
- 共有ネットワークドライブにて、ログファイルにアクセスする手順は、5.2.6ネットワーク経由でログファイルにアクセスする

を、それぞれご参照ください。

5.1　メッセージソースの設定

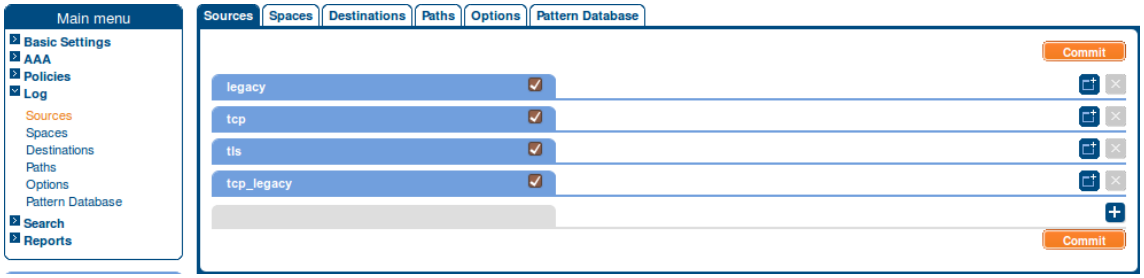
SSB は、"sources"パラメータにより、リモートホストからログメッセージを受信することができます。デフォルトでも、数多くのソースを設定可能ですし、新たなソースを設定することも可能です。またそれとは別に、SSB は SNMP プロトコルによるメッセージの受信と、それらをシスログメッセージに変換することも可能です。

- SSB組み込みのメッセージソースに関して詳細は、5.1.1　SSBのデフォルトのメッセージソース
- SNMPメッセージ受信に関して詳細は、5.1.2　SNMPメッセージの受信
- 新たなメッセージソースを作成する手順の詳細は、5.1.3　SSBでメッセージソースを作成する

を、それぞれご参照ください。

5.1.1 SSBのデフォルトのメッセージソース

SSB は、以下の、組込み済みのソースから自動的にログメッセージを受信できます。



図表 5.1 SSB のデフォルトメッセージソース

- ***legacy***: BSD シスログプロトコル、ポート 514 番で転送されてくる UDP メッセージを受入
- ***tcp***: IETF シスログプロトコル(RFC 5424)ポート 601 番で転送されてくる TCP メッセージを受入
- ***tls***: tls により暗号化された、IETF シスログプロトコル、ポート 6514 番によるメッセージ転送を受入。SSB とリモートホスト間で相互認証が必要です。リモートホスト側は、証明書(必ずしも有効である必要は無い)の提示を求められます。SSB は、ウェルカムウィザードで生成された証明書をリモートホストに送信します。
- **tcp_legacy**: BSD シスログプロトコル(RFC 3164)、ポート 514 番で送られる TCP メッセージを受入

各種設定に関して詳細は、5.1.3 SSBでメッセージソースを作成するをご参照ください。

注記:
デフォルトのメッセージソース全てで、名前解決が可能です。

5.1.2 SNMPメッセージの受信

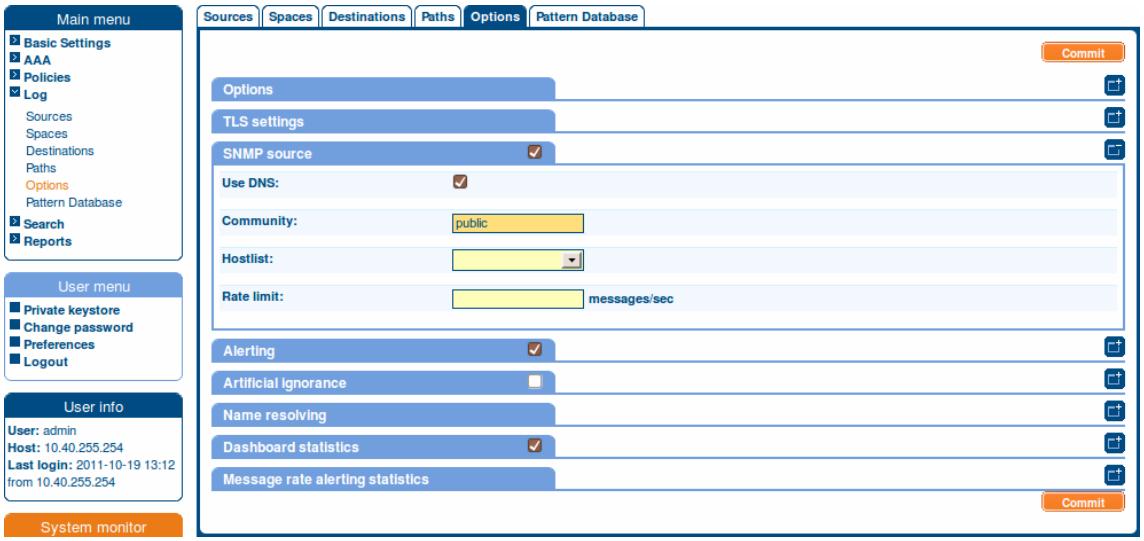
目的:

SSB は、SNMPv2c プロトコルを用いて、SNMP メッセージを受信でき、また受信したメッセージをシスログメッセージに変換することが可能です。SNMP メッセージは、特別な SNMP ソースを、他のログメッセージ同様にログパスに定義することによって送受信が可能になります。SNMP メッセージの送受信を行う方法を説明していきます。

Step:

Step 1. Log > Options > SNMP source の順にクリックします。

Step 2. **SNMP source** のチェックが入っていることを確認します。



図表 5.2 SNMP メッセージの受信

Step 3. SNMP メッセージのデフォルトのコミュニティは、**public** です。もしリモートホストが異なるコミュニティ名をお使いなら、それに合せてください。

注記:
SSB は、一つのコミュニティからのみ、SNMP メッセージを受信できます。

Step 4. SNMPメッセージを送信してくるホストを限定するには、まずホストリストポリシーを作成し、Hostlist欄から、許可するホスト群を選択します。ホストリスト作成に関して詳細は、4.5.8ホストリストポリシーを作成するをご参照ください。

Step 5. メッセージが転送されてくる量を制限するには、**Rate limit** 欄に、SSB が一つのホストから受け入れられる上限のパケット数(メッセージ数ではありません)を入力します。(この設定値は、ソースに適用される、iptables パケットフィルターの hashlimit パラメータをセットします)

警告
レートリミットが設定されている状態でホストからその上限を超えるメッセージが送信されると、Rate limit 欄に入力された値までのログメッセージを処理し、それ以上は捨てられます。ほぼ確実に、捨てられたログメッセージは喪失します。

Step 6. 名前解決をさせたい場合は、**Use DNS** オプションのチェックを入れます。

Step 7. **Commit** をクリックします。

5.1.3 SSBでメッセージソースを作成する

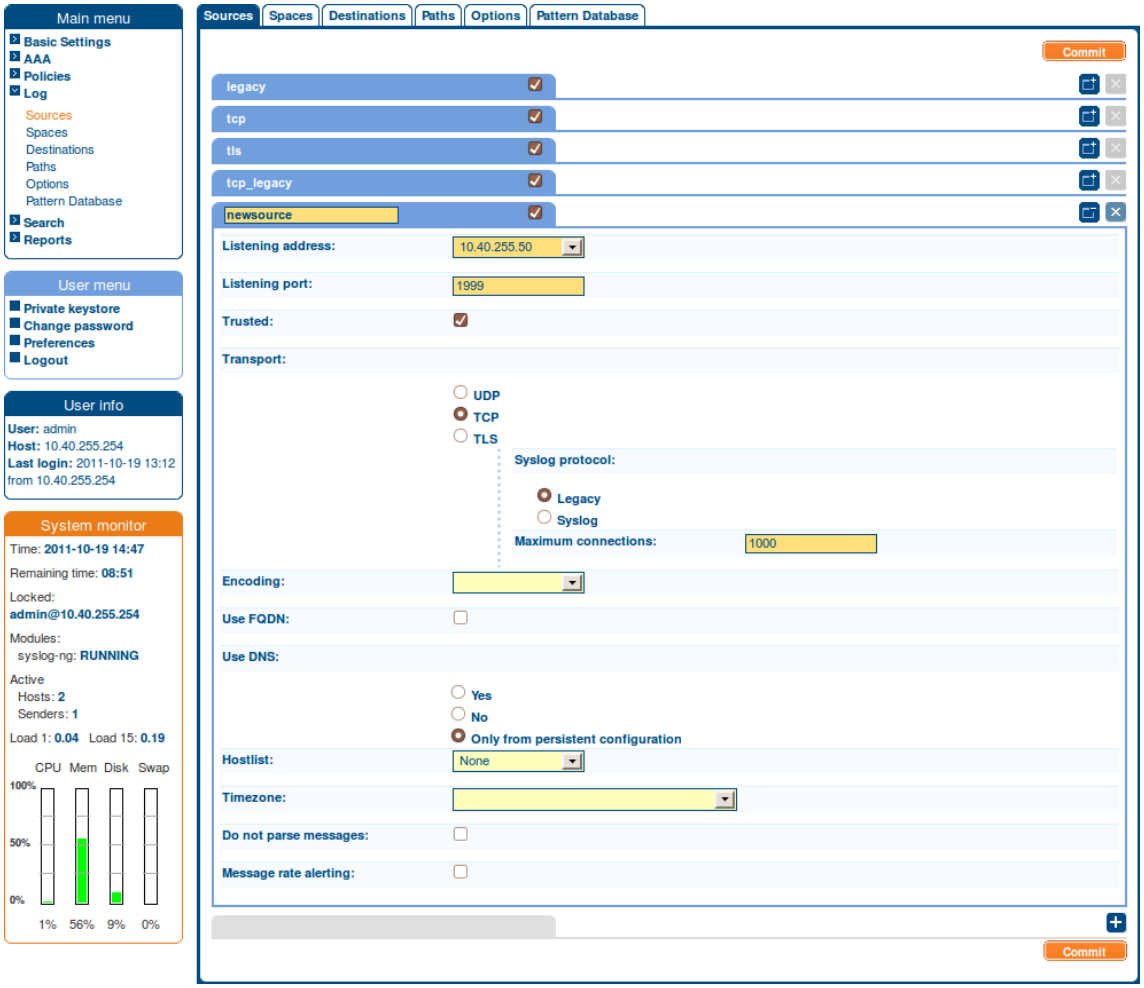
目的:

カスタムメッセージソースを作成する手順を説明します。

Step:

Step 1. **Log > Sources** の順にクリックし、 をクリックして新たな入力欄を展開させます。

Step 2. 青地のタブ部分の入力欄に、ソースの名称を入力します。あとで、どのソースかわかりやすい名称にしてください。



図表 5.3 新たなメッセージソースの作成

Step 3. **Listening address** プルダウンで、SSB がログメッセージを受信する、エイリアス IP アドレスを選択します。

Step 4. **Listening port** 欄に、SSB がログメッセージを受信するポート番号を入力します。

Step 5. このソースに向けてホストから送信される情報が信頼できるなら、Trusted のチェックを入れます。SSB は、"trusted"ホストからのログメッセージに含まれているタイムスタンプとホスト名を保持します。なお、これらは syslog-ng の keep_time_stamp()ならびに keep_hostname()オプションを有効にすることに相当します。

Step 6. **Transport**欄にて、クライアントがSSBにログメッセージを送信する際に用いるプロトコ

ル(UDP、TCPまたはTLS)を選択します。TCPまたはTLSを選択した場合、**Maximum connection**欄に、クライアントの最大同時接続数を設定することができます。なお、これはsyslog-ngのmax_connections()オプションに値を設定することに相当します。
TLSを使用する場合、SSBはクライアントに対し証明書を提示します。これは、**Log > Options > TLS settings**にて設定できます。(詳細は、5.5.4TLS暗号化ログ送受信に用いる証明書の設定をご参照ください)オプション的に、SSBにリモートホストとの間の相互認証と、リモートホストに対して証明書の提示要求とその信頼性の検証を行わせることができます。**Log > Options > Peer verification**欄で、以下の中から、検証に用いる方法を選択してください。

- **None**:証明書提示をリモートホストにリクエストしない。また、リモートホストから提示された証明書は全て受け付ける。
- **Optional Tursted**:リモートサーバーが証明書を提示したら、SSB はそれが有効期限内か、また Common Name に、ホストの IP アドレスあるいはドメイン名が含まれているかをチェックする。このチェックで引っかかると、SSB は接続を拒否する。ただし、リモートホストが証明書を提示しない場合は、接続を許可する。
- **Optional untrusted**:リモートホストは必ず証明書を提示しなくてはならない。SSB は、それがどんな証明書であっても受付けて、接続する。
- **Required trusted**:リモートホストの証明書を検査する。認証局によって署名された証明書のみ受付ける。認証局による証明書に関して詳細は、4.5.7.2外部認証による証明書をアップロードするをご参照ください。証明書のCommon Nameに、ホストのドメイン名かIPアドレスのいずれかが含まれている必要がある。
- **Request untrusted**:SSB は、リモートホストに証明書提示をリクエストする。以下の場合、接続を拒否する ①リモートホストが証明書を提示しない場合 ②証明書が有効期限切れの場合 ③Common Name 内に、ホストのドメイン名または IP アドレスが含まれていない場合。

警告

UDP は非常に信頼性の低いプロトコルです。何の警告も無しに、大量のログメッセージが喪失する危険性があります。可能な限り、TCP か TLS をお使いいただくことを推奨します。

Step 7. **Syslog protocol** 欄で、クライアントが使用するシスログ転送プロトコルを指定します。

- クライアントが BSD プロトコル(RFC3164 準拠)で送信するのであれば、**Legacy** を選択します。これは、シスログを送信するほとんどのデバイスまたはアプリケーションがサポートしているプロトコルです。

■ クライアントが IETF プロトコル(例：syslog ドライバー、あるいは flags(syslog-protocol) オプションを伴うその他のドライバーを用いる syslog-ng3.0 アプリケーション)を使用するのであれば、**Syslog** を選択します。

Step 8. **Encording** 欄で、受信するログメッセージの文字コード変換を、**Timezone** 欄で標準時を、必要に応じて設定します。

Step 9. ログ送信元ホストの完全ドメイン名を保持したい場合は、**Use FQDN** にチェックを入れます。

Step 10. **Use DNS** 欄で、名前解決の方法を指定します。

Step 11. ログ転送をしてくるホストを限定する場合は、まずホストリストを作成し、Hostlistプルダウンから、許可するホスト群を選択します。ホストリスト作成に関して詳細は、4.5.8 ホストリストポリシーを作成するをご参照ください。

Step 12. ある理由で、ソースに到着したメッセージが標準のシスログメッセージフォーマットに準拠しない場合は、Do not Parse message オプションを選択してください。このオプションはシスログメッセージの解析を完全に使用停止し、シスログメッセージのメッセージパートとして、完全に扱います。他のオペレーション（タイムスタンプ、ホスト、等）は SSB によって自動的に追加されます。

Step 13. ソースのために、メッセージレートアラートを設定する場合、4.3.4.6 メッセージレートアラートの設定をご参照ください。

Step 14. Commit をクリックし、変更を反映させます。

注記：
ここで設定したソースに正しくログメッセージが到達するよう、このソースをログパスに記述する必要があります。詳細は、5.4ログパスを管理するをご参照ください。

5.2 SSBにログメッセージを蓄積する

SSB は、log spaces(ログスペース) と呼ばれる領域に、バイナリまたはプレーンテキスト形式でログメッセージを蓄積していきます。この領域(ログの到達先)は、syslog-ng の logstore()と、file() デスティネーションに相当します。ログスペースは、SSB サーバーのローカル環境に、あるいは SAN 上のボリュームに蓄積することができます。

注記：
syslog-ngStore Box SANConnect 版のみ、SAN 装置接続が可能です。

■デフォルトで生成されるlogspacesに関して詳細は、5.2.1 SSBのデフォルトログスペース

■暗号化されたログファイル(ログストア)を使用する際の重要な情報は、5.2.3ログストアを使う

■追加のログスペースを作成する手順は、5.2.4 SSBにカスタムメッセージスペースを構築する

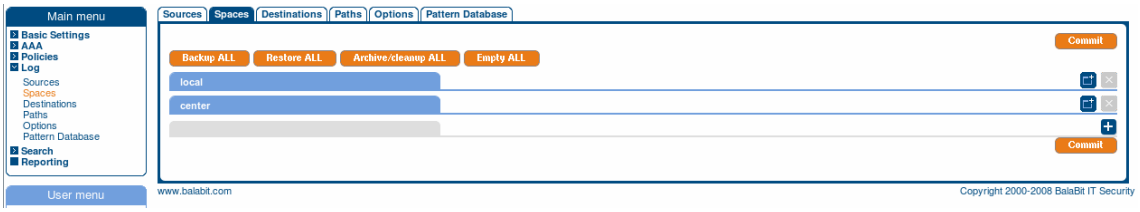
■ログスペースの管理に関して詳細は、5.2.5ログスペースの管理

■ログスペースを、あたかもネットワークドライブのようにアクセスできるようにする手順は、5.2.6ネットワーク経由でログファイルにアクセスする

を、それぞれご参照ください。

5.2.1 SSBのデフォルトログスペース

SSB には、以下のログスペースがデフォルトで作成済です。全ての受信ログメッセージはこの領域に蓄積されます。



図表 5.4　デフォルトログスペース

local: 非暗号化、バイナリ形式で、SSB 自身のログを蓄積する領域

center: 非暗号化、バイナリ形式で、クライアントから受信したログメッセージを蓄積する領域

5.2.2 インデクサ(インデックス付け)を設定する

Logs > **Spaces** の順にクリックし、表示させたいログスペースのタブをクリックします。

インデクサ(インデックス付け)は、インデックスを付加する、と選択されたフィールドにインデックスを設定し、それらを検索可能にします。インデックスが付加されると、その分ディスク領域を消費し、CPU の負荷が増します。

Memory limit 欄で、そのログスペースにおいてインデクサ(インデックス付け)が使用できるメモリ領域の上限値を設定します。

Indexed fields 欄で、インデックスを付加したいフィールドを選択します。以下のフィールドにインデックスを付加することができます。Facility、Priority、Program、Pid、Host、Tags、Name/value pairs、Message。Name/value フィールドに関し、全ての パラメータ名－値 のペアにインデックス付加する場合は、その下の **All** を選択します。指定した名前のみにインデックスを付加する場合は、**Only with the name** を選択します。後者の場合、コンマで区切られたフィールド名を、**commma separated list of names** 欄に入力します。Message フィールドにインデックス付加がされている場合、現在適用されているデリミターが表示されます。
デフォルトでは、全フィールドがインデックス付加になっています。

注記:
少なくとも 1 つのフィールドにインデックスが付加されている必要があります。

5.2.3 ログストアを使う

このセクションは、ログメッセージを蓄積するログストアファイルに関しての重要な情報と、現在のバージョンにおける技術的な限界について説明しています。技術的限界については、将来リリースされるバージョンにて、順次解消される予定です。

■SSBバージョン 1.0.xまでは、暗号化されて蓄積されたログをWebインターフェイスからブラウズすることができませんでした。これは 1.1 において解消されています。詳細は、6.3.5.1ログストアに複号鍵を適用するをご参照ください。

■ログストア内のファイルにインデックスるを付加するのは、現バージョンでは限界があります。インデクサ(インデックス付け)は一日分の　ログストアの内の 1 ファイルにしか、インデックス付加ができません。(SSB は、日付が変わるとログファイルを自動的に新しくします。これは、syslog-ng の$DAY マクロに相当します)ただし、送信元ホストあるいはアプリケーションごとにログファイルのファイル名を分けるようなマクロをお使いの場合、またはより細かい時間指定のできるマクロ(例:$HOUR)を仕込んだカスタムテンプレートをお使いの場合は、現状では日々の最初のファイルのみ、インデックスが付加されます。

■ログストア内のファイルは、チャンク(塊)で構成されています。まれとはいえ、SSB 上で稼動している syslog-ng アプリケーションが、何らかの理由でクラッシュした場合、チャンクもクラッシュします。チャンクはログメッセージを含んでおり、しかし不完全な状態のままになってしまいます。しかし、SSB バージョン 2 F1 から SSB 上で動作する syslog-ng アプリケーションはログメッセージがログストアファイルに書かれる前に、ジャーナルファイルに処理します。そのため、ログストアファイルは予期せぬクラッシュの間も一貫性をたもち、メッセージの消失を避けます同様に、もしインデクサ(インデックス付け)がクラッシュした場合は、ログストア内の一部のログメッセージにインデックスが付かないままになってしまう可能性があります。そうすると、そのログは検索してもヒットしません。しかし、これは、メッセージが消失したことを意味しません。現在、ファイルをリインデックスすることはできません。

これらの限界は、将来リリースされるバージョンで対応される予定です。

5.2.3.1 "logcat"コマンドで、暗号化されたログを閲覧する

ログストア内のファイルにアクセスする方法は、、以下のいずれかです。

■ネットワーク共有を用いてアクセスする(推奨)ー詳細は、5.2.6ネットワーク経由でログファイルにアクセスするをご参照ください。

■SSB にローカルで、あるいは SSH でリモートログインする

ログストア内のファイルのコンテンツを表示させるには、syslog-ng における"logcat"コマンドを用います。例：logcat /var/log/messages.lgs
暗号化されたログファイルを表示させるには、暗号化で用いられた、証明書の秘密鍵を指定します。例：logcat -k privete.key /var/log/messageslgs
ログストア内のファイルは、標準出力形式で保存されているので、例えば grep などのツールを使って特定のログを検索することが可能です。例：logcat /var/log/messages.lgs | grep 192.168.1.1

ログストアに蓄積されている全てのログレコードは、ユニークなレコード ID を保持しています。logcat アプリケーションは、--seek オプションにより、特定のレコードにすばやくたどり着くことができます。

syslog-ng によって生成されるファイルの、現在書込みがされているチャンクは、開き、また読込むことができません。チャンクは、ファイルサイズが chunk_size パラメータで指定されている大きさを超えるか、あるいは chunk_time パラメータで指定されている時間を越え、新たなログメッセージが到着しない場合に初めてクローズされます。

ログストア内のファイルが暗号化されている場合、全てのチャンクに対してハッシュが生成されます。これは、チャンク間の連関を保つためです。各チャンクのハッシュは連結され、それによって、不整合な形でチャンクがはさまることを防止しています。暗号化のアルゴリズムは、CBC モードの aes128、ハッシングのアルゴリズムは hmac-sha1 です。

警告

syslog-ng アプリケーション、またはサーバー機がダウンした場合、クローズされていないチャンクは、EOF のままでいます。このチャンクは壊れたとマーキングされます。ログデータは失われませんが、logcat の結果には表れません。

5.2.4 SSBにカスタムメッセージスペースを構築する

カスタムログスペースを構築するには、以下のいずれかの手順を行ってください。

■バイナリログストアにログメッセージを保存する→5.2.4.1新しいログストアを作成する

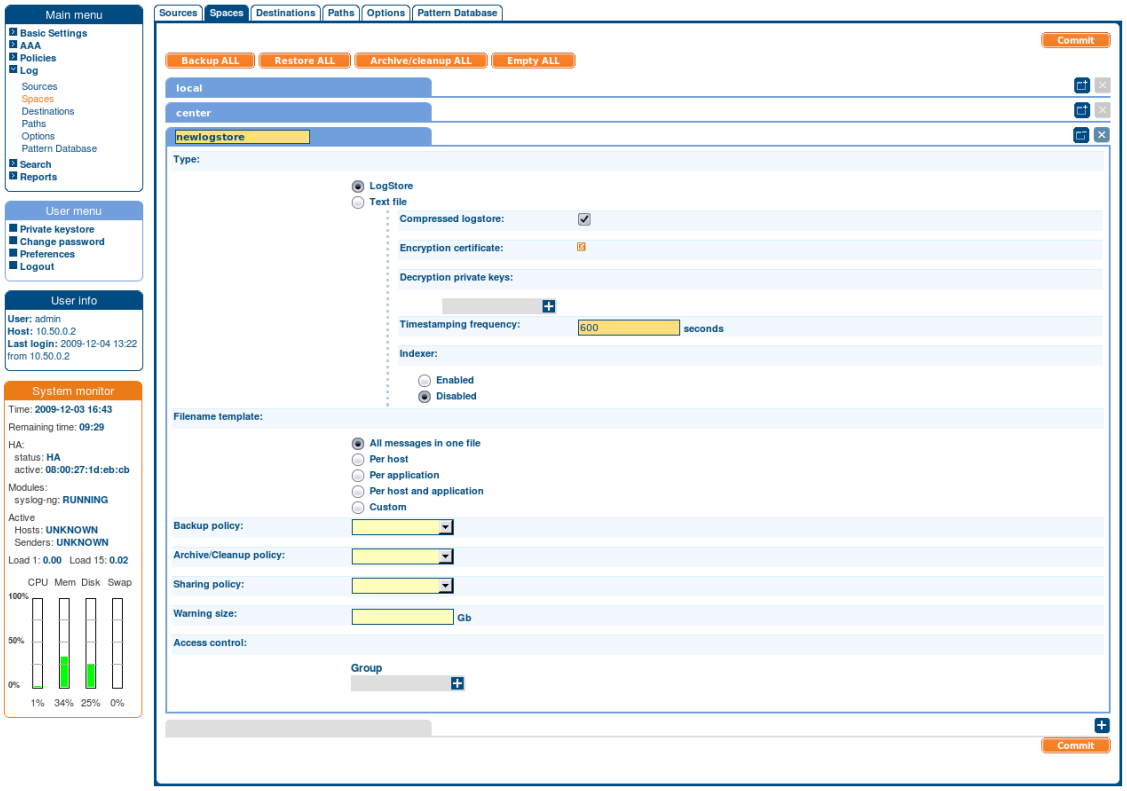
■従来のプレーンテキスト形式でログを保存する→5.2.4.2新たなテキスト形式ログスペースを作成する

5.2.4.1 新しいログストアを作成する

Step：

Step 1. **Log** > **Spaces** の順にクリックし、＋をクリックして展開させます。

Step 2. 青地のタブ内の入力欄に、ログスペースの名称を入力します。保存するログが後でわかりやすいような名称を決めて入力してください。ログスペースの名称は、文字か数字で始めなくてはなりません。



図表 5.5 新たなログストアの作成

Step 3. **Type** 欄で、**LogStore** を選択します。

Step 4. 公開鍵を使用してログファイルを暗号化する場合は、**Encryption certificate** 欄の をクリックします。ポップアップウインドウが現れます。
ポップアップウインドウの参照をクリックし、ログ暗号化で使用したい証明書を選択して、**Upload** をクリックします。または、**Certificate** 欄に、証明書の中身をコピーして貼り付け、**Set** をクリックします。

注記:
暗号化されたログメッセージを閲覧するには、証明書の秘密鍵も必要になります。暗号化されたログストアを、SSBWebインターフェイスにてオンラインでブラウズする方法は、6.3.5暗号化されたログスペース内のブラウズをご参照ください。暗号化されたログファイルは、logcatコマンドラインツールでも閲覧できます。なお、logcatアプリケーションは現在のところ、UNIXベースのプラットフォーム上でのみ実行可能です。

Step 5. デフォルトでは、SSBは 10 分間核で内部のタイムスタンプ認証機関に、タイムスタンプを要請します。**Timestamping frequency**欄にて、その間隔を調整できます。外部の認証機関にタイムスタンプを要請する方法については、5.5.2 SSBにおけるタイムスタンプ設定をご参照ください。

Step 6. ログストア内のファイルに自動的にインデックスを付加したい場合、Indexer 欄の

Enabled を選択します。

ログストアを検索する際に、ヒット件数を制限するには、**Maximum number of search results** フィールドに最大の検索結果ヒット数を入力してください。制限を無効にするには、0 を入力してください。

デフォルトでは、インデックスが有効な場合、以下のフィールドがインデックスされます。**Program, Host, Name/value pairs, Message.**

デフォルトでは、インデクサ（インデックス付け）は次の区切り文字を使い、ログメッセージを単語(トークン)単位に分割します。: & ~ ? ! [ ] = , ; ( ) ' ″ もし、ログメッセージ内で左記の文字のいずれかが、語を分割する記号として機能しており、かつ、その記号も含めて大きな塊で検索したい場合は、区切り文字から削除する必要があります。例えば、ログメッセージ内にMACアドレスが含まれるなら、:(コロン)を区切り文字から削除します。そうしないと、MAC アドレスの各オクテットが個々のトークンとして分割して検索表示されてしまいます。

Step 7. ログストア内のファイルはデフォルトで圧縮されています。圧縮したくない場合は、**Compressed logstore** 欄のチェックを外します。

Step 8. **Filename template** 欄にて、このログスペース内のファイルをどう細分化するかを決定します。

- 一日のログメッセージを単一のファイルに保存するなら、**All messages in one file** を選択します。
- ホストごと(IP アドレスないしはホスト名)でログファイルを分割するなら、**Per host** を選択します。この設定は、syslog-ng の $HOST マクロを使用することに相当します。
- ログを送信してくるアプリケーション単位でログファイルを分割するなら、**Per application** を選択します。この設定は、syslog-ng の$PROGRAM マクロを使用することに相当します。
- ログを送信してくる各ホストの、さらにアプリケーション単位で分割したい場合は、**Per host and application** を選択します。この設定は、syslog-ng の $HOST-$PROGRAM マクロを使用することに相当します。
- ログファイルのネーミングに用いるカスタムテンプレートを指定する場合は、**Custom** を選択します。**Template** 欄が現れるので、テンプレート名を入力します。ファイル名テンプレートの使用に関して詳細は、The syslog-ng 3.0 Administrator Guide をご参照ください。

Step 9. ログスペースの、リモートサーバーへのバックアップを自動化したい場合、バックアップポリシーを作成し、**Backup policy**プルダウンから、ポリシーを選択します。バックアップポリシーの作成に関して詳細は、4.3.5データと設定のアーカイブとバックアップをご参照ください。

Step 10. ログスペースのアーカイブを日時で自動化したい場合、アーカイブポリシーを作成し、**Archive/Cleanup policy**プルダウンで、ポリシーを選択します。アーカイブポリシー作成に関して詳細は、4.3.5データと設定のアーカイブとバックアップをご参照ください。

警告

アーカイブ/クリーンアップポリシーを必ず適用し、古いログデータを定期的に削除して、ログスペースが満杯にならないように留意してください。

Step 11. ネットワーク上で、ログスペース内のログスペースを共有するには、共有ポリシーをSSBで作成し、**Sharing policy**プルダウンから選択します。共有ポリシー作成に関して詳細は、5.2.6ネットワーク経由でログファイルにアクセスするをご参照ください。

Step 12. SSBSANConnect 版をお使いの場合、ログメッセージを蓄積させるボリュームを必ず指定してください。SANConnect 版では、ローカルのディスクにはログを蓄積しません。SAN 装置への接続設定は、**Basic Settings > Strage** にて行います。

注記:

既存のログスペースの設定を変更するにあたり、新たなボリュームをログスペースに割り当てた場合、以前からあるボリューム上のログメッセージは削除も、また新たなボリュームへのコピーもされることはありません。

Step 13. **Warining size** 欄で、ログスペースの容量を指定します。SSB は、ログスペースの大きさが個々で指定した容量を超えると、アラートを発します。

警告

アラートを正しく受信できるよう、以下の設定が正しいことをご確認ください。

① **Basic Settings > Alerting & Monitoring** にて、**Logspace exceeded warning size** アラートが **Enable** であること

② **Basic Settings > Management** にて、メール及び SMTP の設定が正しいこと

アラート及びシステム監視に関して詳細は、4.3.4 SSBのシステム監視設定をご参照下さい。

Step 14. デフォルトでは、**search**グループに含まれているメンバが、蓄積されたログメッセージをオンライン参照できます。**Access control**オプションで、どのユーザグループがログスペースにアクセス可能かを設定できます。詳細は、4.4.6ユーザ権限とユーザグループを管理するをご参照下さい。

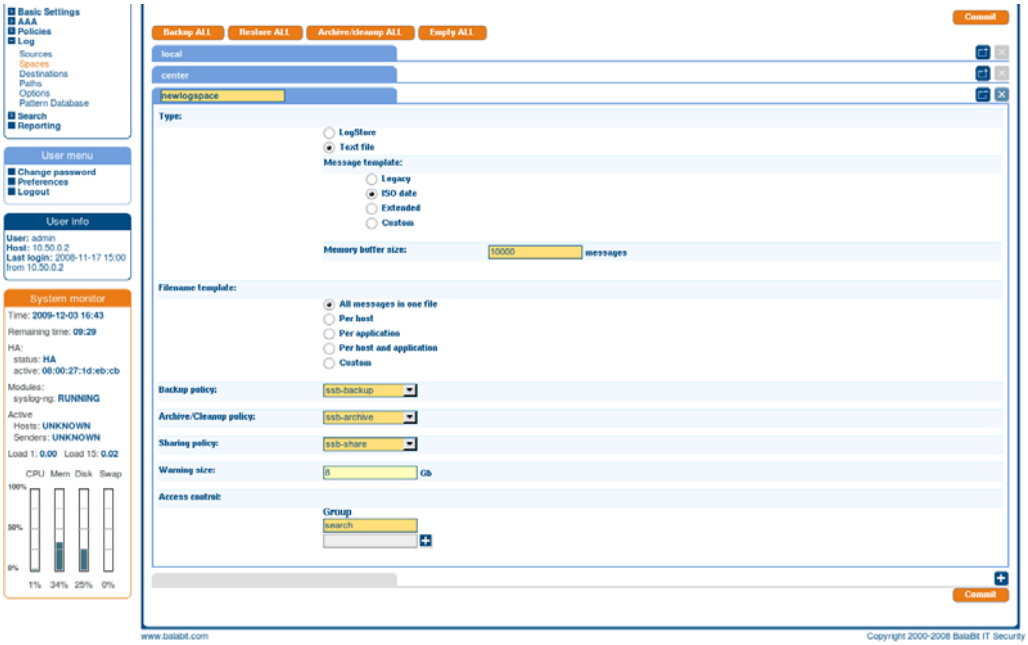
Step 15. **Commit** をクリックし、変更を反映させます。

5.2.4.2 新たなテキスト形式ログスペースを作成する

Step:

Step 1. **Log > Spaces** の順にクリックし、**+**をクリックして入力欄を展開させます。

Step 2. ログスペースの名称を、青地のタブ部分の入力欄に入力します。あとで何のログを保存しているスペースかが容易にわかるような名称をつけてください。



図表 5.6 新たなテキストログストアの作成

Step 3. **Type** 欄で、**Text file** を選択します。

Step 4. **Message tmplate** 欄で、受信するログが用いるテンプレートを、以下のうちから選択します。

- ***Legacy***: template("$DATE $HOST $MSGHDR$MSG¥n")
- ***ISO date***: template("$ISODATE $HOST $MSGHDR$MSG¥n")
- ***Extend***: template("$ISODATE $HOST $MSGHDR$MSG¥n")
- ***Custom***: Template 欄が現れるので、カスタムテンプレート名を入力します。テンプレートの使用に関しては、*The syslog-ng 3.0 Administraotr Guide* をご参照下さい。

Step 5. **Memory buffer size** 欄に、メモリに保持するメッセージの最大数を入力します。この設定は、syslog-ng の log_fifo_size()パラメータに相当します。

Step 6. **Filename template** 欄で、このログスペース内のログファイルをどう細分化するかを指定します。

■ 一日のログメッセージを単一のファイルに保存するなら、**All messages in one file** を選択します。

■ ホストごと(IP アドレスないしはホスト名)でログファイルを分割するなら、**Per host** を選択します。この設定は、syslog-ng の $HOST マクロを使用することに相当します。

■ ログを送信してくるアプリケーション単位でログファイルを分割するなら、**Per application** を選択します。この設定は、syslog-ng の$PROGRAM マクロを使用することに相当します。

■ ログを送信してくる各ホストの、さらにアプリケーション単位で分割したい場合は、**Per host and application** を選択します。この設定は、syslog-ng の $HOST-$PROGRAM マクロを使用することに相当します。

■ ログファイルのネーミングに用いるカスタムテンプレートを指定する場合は、**Custom** を選択します。**Template** 欄が現れるので、テンプレート名を入力します。ファイル名テンプレートの使用に関して詳細は、*The syslog-ng 3.0 Administraotr Guide* をご参照ください。

Step 7. ログスペースの、リモートサーバーへのバックアップを自動化したい場合、バックアップポリシーを作成し、**Backup policy**プルダウンから、ポリシーを選択します。バックアップポリシーの作成に関して詳細は、4.3.5データと設定のアーカイブとバックアップをご参照ください。

Step 8. ログスペースのアーカイブを日次で自動化したい場合、アーカイブポリシーを作成し、**Archive/Cleanup policy**プルダウンで、ポリシーを選択します。アーカイブポリシー作成に関して詳細は、4.3.5データと設定のアーカイブとバックアップをご参照ください。

警告

アーカイブ/クリーンアップポリシーを必ず適用し、古いログデータを定期的に削除して、ログスペースが満杯にならないように留意してください。

Step 9. ネットワーク上で、ログスペース内のログスペースを共有するには、共有ポリシーをSSBで作成し、**Sharing policy**プルダウンから選択します。共有ポリシー作成に関して詳細は、5.2.6ネットワーク経由でログファイルにアクセスするをご参照ください。

Step 10. SSB SANConnect 版をお使いの場合、ログメッセージを蓄積させるボリュームを必ず指定してください。SANConnect 版では、ローカルのディスクにはログを蓄積しません。SAN 装置への接続設定は、**Basic Settings > Storage** にて行います。

注記:
既存のログスペースの設定を変更するにあたり、新たなボリュームをログスペースに割り当てた場合、以前からあるボリューム上のログメッセージは削除も、また新たなボリュームへのコピーもされることはありません。

Step 11. **Warining size** 欄で、ログスペースの容量を指定します。SSB は、ログスペースの大きさが個々で指定した容量を超えると、アラートを発します。

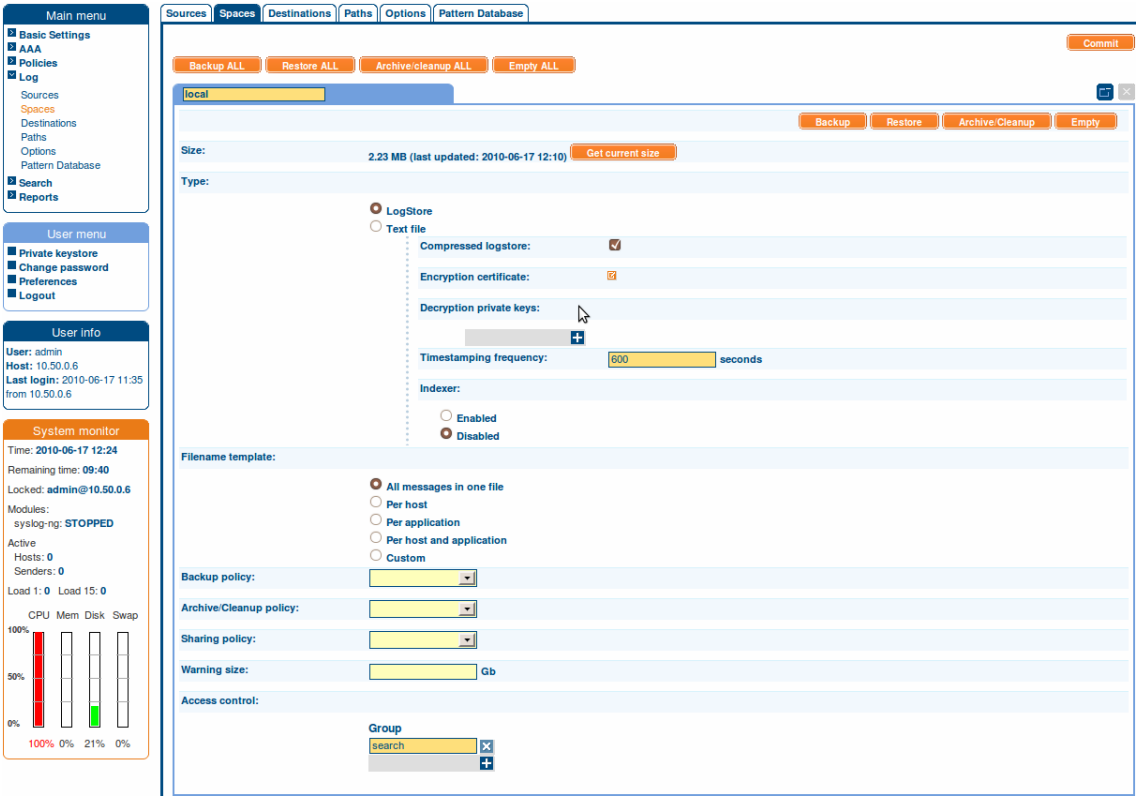
警告
アラートを正しく受信できるよう、以下の設定が正しいことをご確認ください。
① **Basic Settings** > **Alerting & Monitoring** にて、**Logspace exceeded warning size** アラートが **Enable** であること
② **Basic Settings** > **Management** にて、メール及び SMTP の設定が正しいこと
アラート及びシステム監視に関して詳細は、4.3.4 SSBのシステム監視設定をご参照下さい。

Step 12. デフォルトでは、**search**グループに含まれているメンバが、蓄積されたログメッセージをオンライン参照できます。**Access control**オプションで、どのユーザグループがログスペースにアクセス可能かを設定できます。詳細は、4.4.6ユーザ権限とユーザグループを管理するをご参照下さい。

Step 13. **Commit** をクリックし、変更を反映させます。

5.2.5 ログスペースの管理

ログスペースは、バックアップ及びアーカイブポリシーを適用させることにより、通常は自動的に管理できます。(詳細は 4.3.5データと設定のアーカイブとバックアップ)ですがこれらのアクションを手動で起動することも可能です。をクリックしてログスペースの詳細を展開すれば、最上部にアクションボタンが現れます。



図表 5.7 ログスペースの管理

ヒント

ログスペースの現在のサイズは、**Size** 欄に表示されます。このデータを最新の状態に更新するには、**Get current size** をクリックします。

■**Backup** をクリックすると、手動でバックアップを起動できます。

■**Restore** をクリックすると、バックアップサーバーからログファイルへのリストアが起動します。

警告

リストアを行うと、ログスペース内の全ログが、リストアされるファイルないのログに置き換えられます。したがってバックアップより後に蓄積されたログスペース内のログは、リストアによって全て消失し、修復はできません。

■**Archive/Cleanup** をクリックすると、アーカイブやクリーンアップが手動で起動できます。

警告

ログスペースに適用されたアーカイブポリシーが、クリーンアップのみの設定である場合、Retantion Timeの設定値より古いログメッセージは全て消去されます。修復はできません。詳細は、4.3.5データと設定のアーカイブとバックアップをご参照下さい。

■**Empty** をクリックすると、ログスペース内の全てのログが消去されます。SSB に空き領域をすばやく生み出したい場合や、ログスペースを消去したい場合に有益です。

0

警告

Empty アクションは、ログスペース内の全てのログファイルを消去します。バックアップあるいはアーカイブされていなかったログメッセージは全て失われ、修復はできません。

同じようなアクションボタンが、**Log > Spaces** 画面の最上部に表示されています。これらのボタンは、全てのログスペースに対し適用されるアクションで、動作条件は各々のログスペースの設定値によります。例えば、**Backup ALL** をクリックすると、各ログスペースで指定されているバックアップポリシーで、全てのログスペースのバックアップが実行される、という意味です。

5.2.6 ネットワーク経由でログファイルにアクセスする

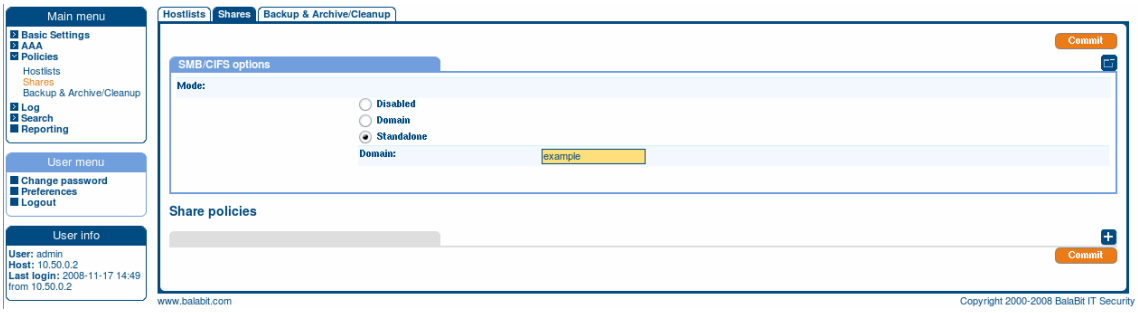
必要に応じて、SSB のログファイルは、Samba(CIFS)あるいはネットワークファイルシステム(NFS)を使用して、ネットワーク上の共有ドライブのようにアクセスすることが可能です。共有に関する設定は、共有の種類、アクセス可能なクライアント(ホスト)、そしてユーザを指定するポリシーによって管理できます。SSB がドメインのメンバである場合も、共有が可能です。

- SSBのユーザをローカルで管理している場合、SSBのアカウントを持つユーザは共有フォルダにアクセス可能です。5.2.6.1スタンドアロンモードでログファイルを共有する手順を実行してください。
- LDAPにてSSBユーザを管理している場合は、SSBをドメインのメンバに加える必要があります。5.2.6.2ドメインモードでログファイルを共有する手順を実行してください。
- 共有ログファイルにアクセスする方法については、5.2.6.3共有ファイルにアクセスするをご参照下さい。

5.2.6.1 スタンドアロンモードでログファイルを共有する

Step:

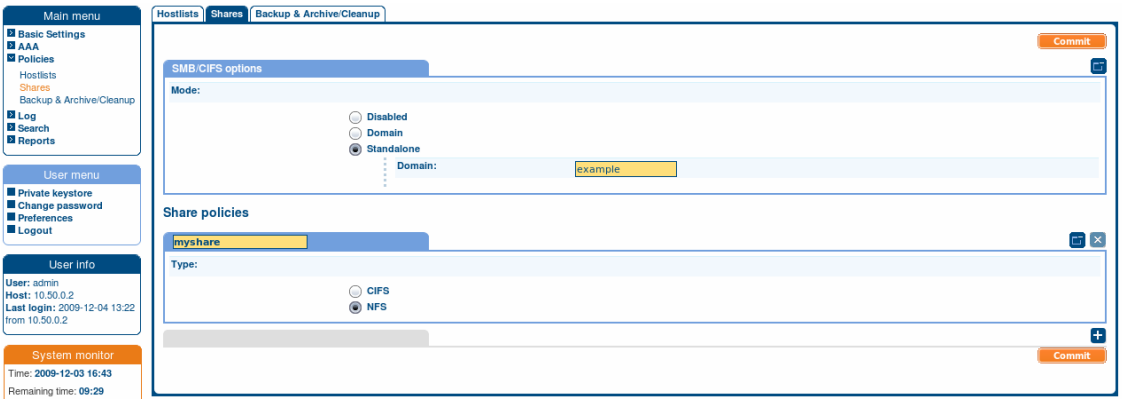
Step 1. **Policies > Shares > SMB/CIFS options** の順にクリックし、**Standalone** を選択します。



図表 5.8 ログスペースの共有

Step 2. ＋をクリックして、新たな共有ポリシー設定欄を展開させます。ポリシー名を決め、青地タブ内の入力欄に入力します。

Step 3.



図表 5.9 共有ポリシーの作成

Type 欄から、ネットワーク共有の種類を選択します。

- NFS(ネットワークファイルシステム)を使用する場合、NFS を選択します。
- Samba をお使いになる場合は、CIFS を選択します。

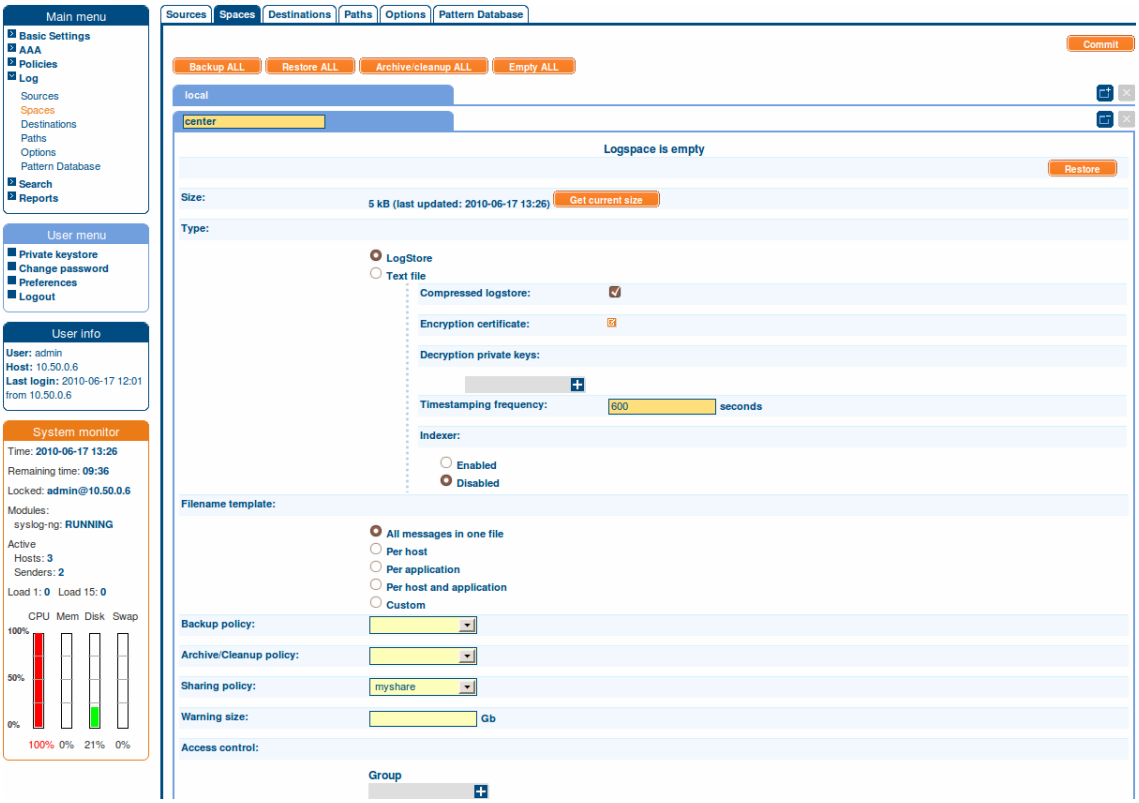
Step 4. Samba をお使いの場合は、共有領域にアクセス可能なユーザ及びホストを限定することができます。その設定をしないと、SSB のアカウントを持つ全てのユーザが、全ての共有領域内のログファイルにアクセス可能になります。

- Step3 で**CIFS**を選択すると、新たに入力欄が展開します。その、**Allowed group**欄に、アクセスを許可するユーザグループ名を入力します。ローカルユーザグループに関する詳細は、4.4.3ローカルユーザグループを管理するをご参照ください。
- **Hostlist**プルダウンで、アクセスを許可するホストリストを設定可能です。ホストリストの作成に関して詳細は、4.5.8ホストリストポリシーを作成するをご参照ください。

Step 5. **Commit** をクリックします。

Step 6. ログスペースの詳細を表示させるには、**Log** > **Spaces** の順にクリックし、⧉をクリックします。

Step 7.



図表 5.10 ログスペース共有ポリシーの設定

Sharing policy プルダウンから、ポリシーを選択します。

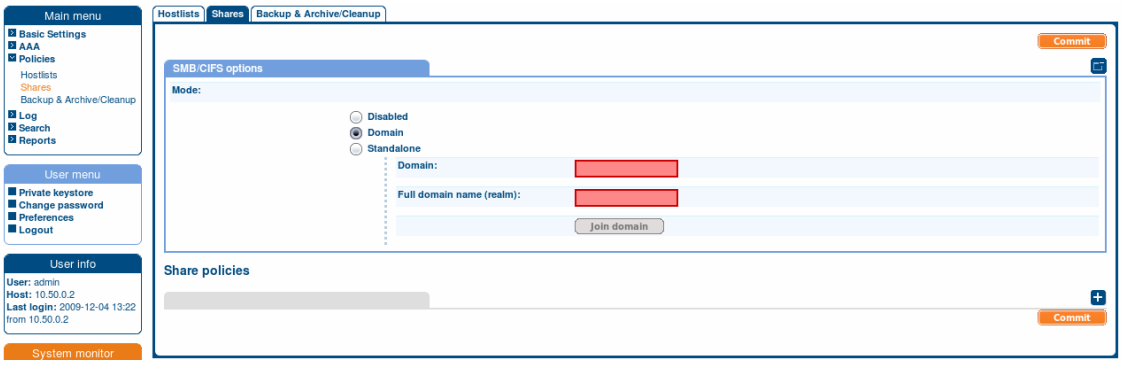
Step 8. **Commit** をクリックします。

5.2.6.2 ドメインモードでログファイルを共有する

Stetp：

Step 1. Policies > Shares > SMB/CIFS options の順にクリックし、Domain mode を選択します。

Step 2. **Domain** 欄に、ドメイン名を入力します。



図表 5.11 ドメインへの参加

Step 3. **Full domain name** 欄に、レルム(認証設定を特定する名前)入力します。

注記:
DNS の設定が正しいこと、すなわち、完全ドメイン名が SSB にて解決できることを確認してください。確認方法は、**Basic Settings** > **Troubleshooting** > **Ping** の順にクリックし、**Hostname** 欄に完全ドメイン名を入力して **Ping host** をクリックします。

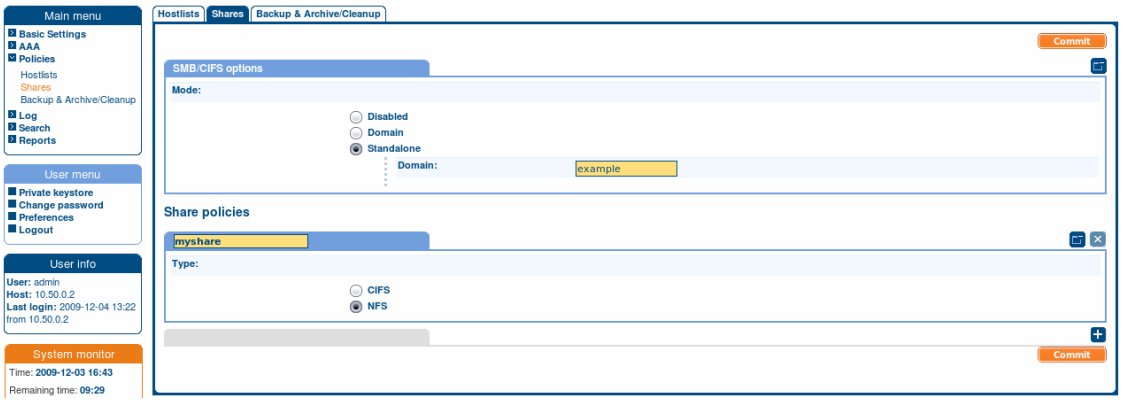
Step 4. **Join domain** をクリックします。ポップアップウインドウが現れます。

Step 5. SSB は、ドメインに参加するのにアカウント情報が必要です。ユーザ名を **Username** 欄に、パスワードを **Password** 欄に入力します。
オプションとして、**Domain controller** 欄に、ドメインコントローラの名前を入力することができます。ここを空欄にしておくと、SSB は自動的にドメインコントローラを探します。

注記:
DNS の設定が正しいこと、すなわち、ドメインコントローラのホスト名が SSB にて解決できることを確認してください。確認方法は、**Basic Settings** > **Troubleshooting** > **Ping** の順にクリックし、**Hostname** 欄に完全ドメイン名を入力して **Ping host** をクリックします。

Step 6. **Join domain** をクリックします。

Step 7. ✚をクリックし、新たな共有ポリシーの設定欄を展開させます。ポリシー名を、青地タブ内の入力欄に入力します。



図表 5.12 共有ポリシーの作成

Step 8. **Type** 欄から、ネットワーク共有の種類を選択します。

- NFS(ネットワークファイルシステム)を使用する場合、**NFS** を選択します。
- Samba をお使いになる場合は、**CIFS** を選択します。

Step 9. Samba をお使いの場合は、共有領域にアクセス可能なユーザ及びホストを限定することができます。その設定をしないと、SSB のアカウントを持つ全てのユーザが、全て

の共有領域内のログファイルにアクセス可能になります。

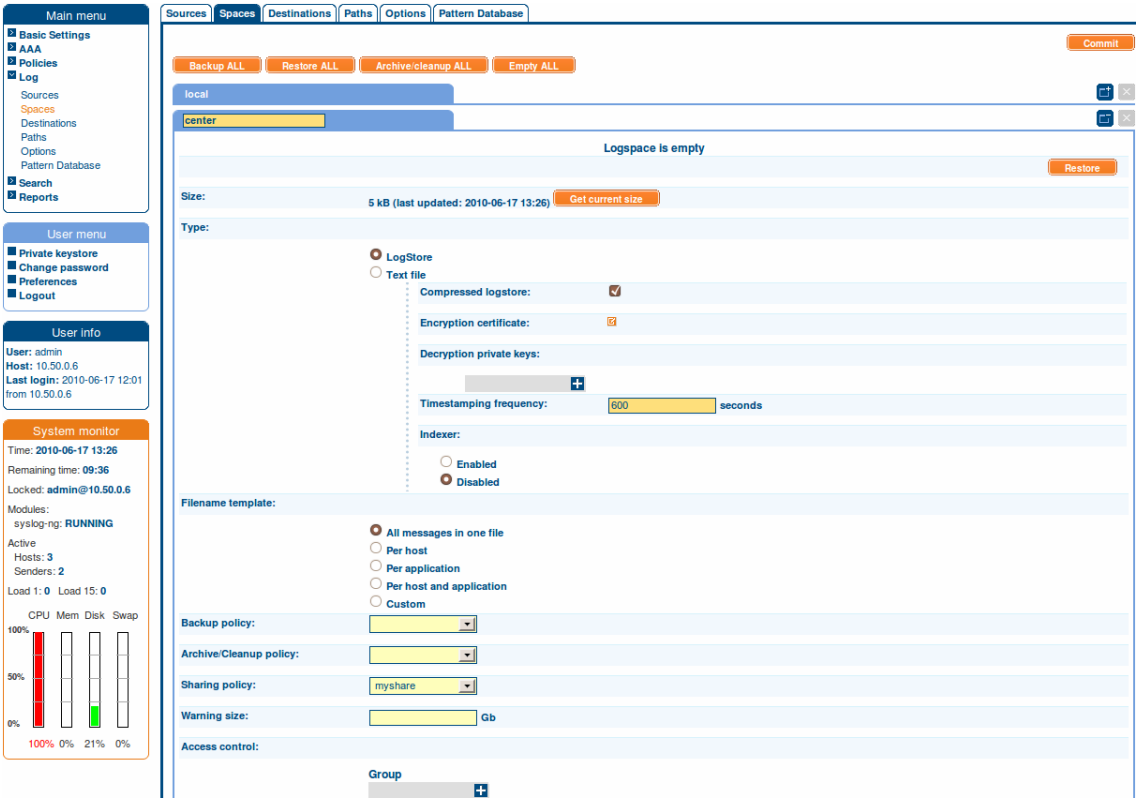
■ Step3 で **CIFS** を選択すると、新たに入力欄が展開します。その、**Allowed group** 欄に、アクセスを許可するユーザグループ名を入力します。ユーザと SSB が、同一のドメインメンバーであることが必要です。

■ **Hostlist**プルダウンで、アクセスを許可するホストリストを設定可能です。ホストリストの作成に関して詳細は、4.5.8ホストリストポリシーを作成するをご参照ください。

Step 10. **Commit** をクリックします。

Step 11. ログスペースの詳細を表示させるには、**Log** > **Spaces** の順にクリックし、をクリックします。

Step 12.



図表 5.13 ログスペースの共有ポリシー設定

Sharing policy プルダウンから、ポリシーを選択します。

Step 13. **Commit** を選択します。

5.2.6.3 共有ファイルにアクセスする

ここでは、共有ポリシーを用いてログファイルにアクセスする方法を説明します。共有領域内のログファイルに関して詳細は、5.2.6ネットワーク経由でログファイルにアクセスするをご参照ください。

仮に、全てに単一の共有ポリシーが適用されているとしても、各ログスペースはあたかも、各々独立した共有フォルダのようにアクセスできます。その、共有フォルダの名称は、ログスペースの名称と同一になります。共有フォルダ配下では、ログファイルは以下の形式のサブフォルダ下に格納されます。 yyyy/mm-dd/ ファイル名は、ログスペース毎に設定されたファイル名テンプレートの記述内容によって決まります。ログストアの拡張子は、.store です。テキスト形式のログの拡張子は、.log になります。共有フォルダのルートディレクトリには、インデックスファイルのような、ログスペースを管理するために必要ないくつかのファイルが含まれていることにご注意ください。これらのファイルは全て、リードオンリー(書込み禁止)です。

注記:

ログスペースの共有に NFS をご使用になる場合、共有フォルダの名称は以下のようになります。/exports/{logspace_id}/...下記の例 5.1 は、共有ログスペースを、NFS を用いて Linux プラットフォームでマウントする方法を示しています。

例 5.1 :NFS を用いて Linux にログスペースをマウントする方法

mount –t nfs {ssb-ip} : /exports/{logspace_id} /mnt/testmount

5.3 SSBからログメッセージを転送する

SSB は、リモートの宛先に向けてログメッセージを転送することができます。転送先には、リモートサーバー上の SQL データベース、同じく、ログ解析アプリケーションなどが設定可能です。

■リモートサーバー上のSQLデータベースに転送するには、5.3.1 SQLデータベースにログメッセージを転送するを実行してください。現在、Oracle、MSSQL、MySQL、PostgreSQLをサポートしています。

■リモートサーバーに転送するには、5.3.3リモートサーバーにログメッセージを転送するを実行してください。

5.3.1 SQLデータベースにログメッセージを転送する

目的:

ここでは、ログメッセージを SSB からリモートの SQL サーバーに転送する手順を説明します。

Step:

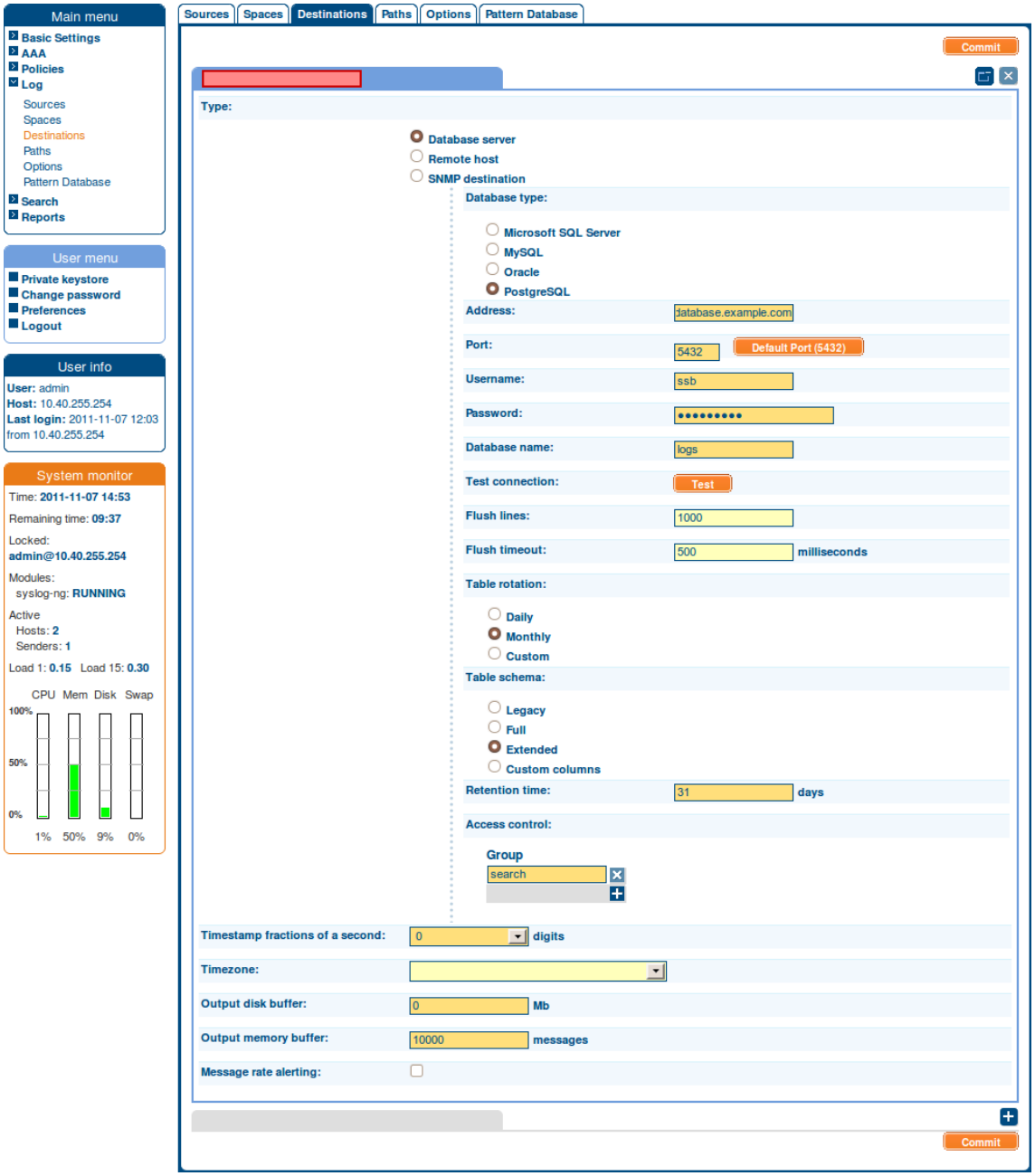
Step 1. リモートのログ転送先を新たに作成する場合は、**Log** > **Destination** の順にクリックし、**+**をクリックして入力欄を展開させます。

Step 2. 青地タブ部分の入力欄に、転送先の名前を入力します。

注記:

ここでつけられる名前は、SSB によって生成されたデータベーステーブルでも用いられます。互換性を保つために、半角の数字、アルファベット、そしてアンダーバー(_)のみをお使いになれます。

Step 3. Type 欄で Database server を選択します。



図表 5.14 転送先にデータベースサーバーを指定する

Step 4. **Database type** 欄にて、お使いになるデータベースの種類を選択します。

Step 5. **Address** 欄に、データベースサーバーの IP アドレスまたはホスト名を入力します。また、DB サーバーがデフォルト以外のポート番号を使用している場合は、Port 欄にその番号を入力します。

Step 6. **Username** 欄に、データベースにアクセスする際のユーザ名を、**Password** 欄に、同じくパスワードを入力します。なお、ここで指定するユーザは、新しいテーブルをデータベースに構築できる権限を持っていることが必要です。

Step 7. **Database name** 欄に、ログメッセージを蓄積するデータベースの名前を入力します。

Step 8. (オプションのステップ) **Flush lines** フィールドに SSB が一回に送信する前に待機するログメッセージライン数を入力してください。この数値を高くすると、完全に満たされたフレームがネットワークに送られるので、スループットが増加します。しかし、同時に、メッセージレーテンシーも増加します。このレーテンシーは、**Flush timeout** オプションを使用することで制限することが可能です。

注記

Flush lines は、**Output memory buffer** 値に関係しています。(**Output memory buffer** 値を設定するためには、**Log > Destinations** に移動してください。) **Output memory buffer** の値は、**Flush lines** の値と等しいか、大きい必要があります。

Step 9. (オプションのステップ) **Flush timeout** フィールドに、**Flush lines** フィールドに指定した数のログが無い場合に、SSB が一回に送信する前に待機するミリセカンド数を入力してください。この数値を高くすると、完全に満たされたフレームがネットワークに送られるので、スループットが増加します。しかし、同時に、メッセージレーテンシーも増加します。このレーテンシーは、**Flush lines** オプションを使用することで制限することが可能です。

Step 10. 日次または月次でテーブルを新しくするよう選択できます。また、カスタムテーブルを作成することも可能です。その場合、**Table rotation** 欄で、テーブルネーミングテンプレートを指定します。

Step 11. データベースにどのフィールドを挿入するかを選択します。定義済みのテンプレート、または**Custom columns**を選択して、カスタムテンプレートを作成することもできます。利用可能なテンプレートに関しては、5.3.2 SSBのSQLテンプレートをご参照ください。

Step 12. SSB は、データベース内の古いデータやテーブルを自動的に削除することができます。デフォルトでは、1 ヶ月以前が対象です。必要に応じて、**Retention time** 欄で変更できます。

Step 13. データベースに蓄積されたログは、SSB の **search** インターフェイスからアクセスする

ことができます。**Access control** > **Group** 欄に、許可するユーザを入力します。許可するユーザグループを追加する場合は、➕をクリックして入力欄を増やします。

Step 14. ほとんどのログメッセージのタイムスタンプは、秒単位までの正確性しか担保されていません。SSB は、もっと細かい単位のタイムスタンプ付加が可能です。**Timestamp fractions of a second** 欄で、秒の部分に何桁(=何分の 1 秒)までを含めるか指定します。この設定は、syslog-ng の frac_digits()パラメータに相当します。

Step 15. リモート DB サーバーと SSB が稼動しているマシンが、別個の標準時間帯地域に存在する場合で、レガシーメッセージテンプレートをお使いの場合、**Timezone** プルダウンで、サーバーの標準時間帯を選択します。これは、レガシーメッセージテンプレートには標準時間帯地域の情報が含まれていないためです。

Step 16. **Output disk buffer** 欄に、ディスクバッファサイズを入力します。リモートサーバーにアクセス不能になった場合、SSB はハードディスクにログを保持し、復旧後に送信を再開します。この設定は、syslog-ng の log_disk_fifo_size()パラメータに相当します。

Step 17. リモートサーバーが、ログメッセージの受入をする処理速度が低下している場合に、SSB はデフォルトで 10000 件までをメモリに保持します。この値を変更するには、**Output memory buffer** 欄にて行います。この設定は、syslog-ng の log_fifo_size()パラメータに相当します。

Step 18. **Commit** をクリックします。

Step 19. ここで設定したリモートサーバーにログメッセージの転送を開始するには、ログパスにこのリモートサーバーを含める必要があります。詳細は 5.4 ログパスを管理するをご参照ください。

Step 20. **Test connection** をクリックすると、データベースに接続可能かのテストができます。

5.3.2 SSBのSQLテンプレート

以下のセクションでは、SSB において使用可能な SQL テンプレートについて説明します。

- ***Legacy***
- ***Full***
- ***Extended***
- ***Custom***

5.3.2.1 Legacyテンプレート

Legacy テンプレートでは、ログメッセージを ssb_sql_messages_$(R_YEAR)_$(R_MONTH)テーブルに蓄積します。以下のフィールドが生成されます。

- *inset_time*: SSB がログメッセージを受信した時刻。UNIXTime 形式です。
- *rule_id*
- *__row_id*
- *date_time*: ログメッセージが送信された時刻。YYYY-MM-DD hh:mm:ss 形式です。
- *facility*: メッセージを送信したファシリティ。
- *priority*: メッセージの優先度レベル。
- *host*: ログメッセージが生成されたホストの IP アドレスまたはホスト名。
- *program*: ログメッセージを生成したアプリケーションの名前。
- *pid*: ログメッセージを生成したプロセスの ID 番号。(ログにこの値が含まれていない場合、自動で 0 がセットされます)
- *message*: ログのメッセージ部分

insert_time、rule_id、date_time、facility、host、program の各フィールドは、インデックスが付加されます。

5.3.2.2 Fullテンプレート

Full テンプレートでは、ログメッセージを ssb_sql_messages_$(R_YEAR)_$(R_MONTH)テーブルに蓄積します。以下のフィールドが生成されます。

- *inset_time*: SSB がログメッセージを受信した時刻。UNIXTime 形式です。
- *rule_id*
- *__row_id*
- *date_time*: ログメッセージが送信された時刻。YYYY-MM-DD hh:mm:ss 形式です。
- *facility*: メッセージを送信したファシリティ。
- *priority*: メッセージの優先度レベル。
- *sourceip*: ログを送信したホストの IP アドレス。
- *host*: ログメッセージが生成されたホストの IP アドレスまたはホスト名。
- *program*: ログメッセージを生成したアプリケーションの名前。
- *pid*: ログメッセージを生成したプロセスの ID 番号。(ログにこの値が含まれていない場合、自動で 0 がセットされます)
- *message*: ログのメッセージ部分

insert_time、rule_id、date_time、facility、host、source_ip、program の各フィールドは、インデックスが付加されます。

5.3.2.3 Extendedテンプレート

Extended テンプレートでは、ログメッセージを ssb_sql_messages_$(R_YEAR)_$(R_MONTH)テーブルに蓄積します。以下のフィールドが生成されます。

- *inset_time*: SSB がログメッセージを受信した時刻。UNIXTime 形式です。
- *rule_id*
- *__row_id*
- *date_time*: ログメッセージが送信された時刻。YYYY-MM-DD hh:mm:ss 形式です。
- *facility*: メッセージを送信したファシリティ。
- *priority*: メッセージの優先度レベル。
- *sourceip*: ログを送信したホストの IP アドレス。

■ *host*: ログメッセージが生成されたホストの IP アドレスまたはホスト名。

■ *program*: ログメッセージを生成したアプリケーションの名前。

■ *pid*: ログメッセージを生成したプロセスの ID 番号。(ログにこの値が含まれていない場合、自動で 0 がセットされます)

■ *message*: ログのメッセージ部分

insert_time、rule_id、date_time、facility、host、source_ip、program の各フィールドは、
インデックスが付加されます。

5.3.2.4 Customテンプレート

Custom テンプレートを使用することにより、テーブルのフィールドを特定することが可能になります。フィールド名を指定し、種類を選択し、マクロを用いてコンテンツを指定します。マクロの使用に関して詳細は、*The syslog-ng 3.0 Administrator Guide* をご参照ください。フィールドにインデックスを付加したい場合は、**Indexed** オプションにチェックを入れます。

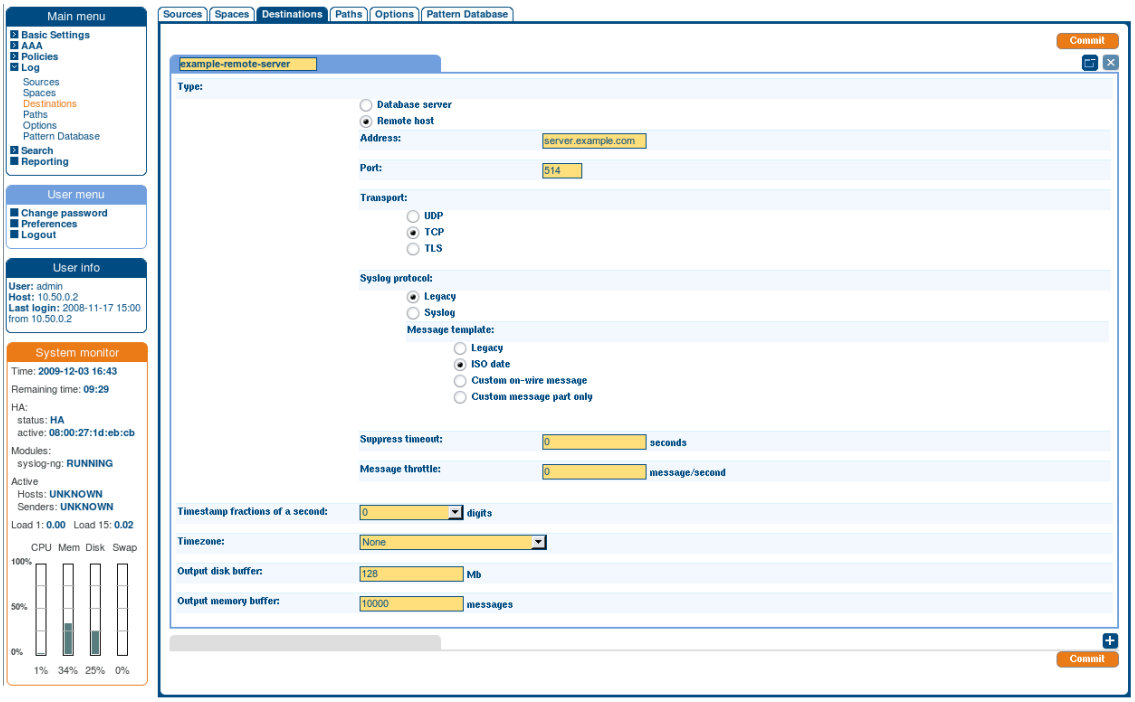
5.3.3 リモートサーバーにログメッセージを転送する

目的:
SSB からリモートサーバーへのログメッセージ転送の手順を説明します。

Step:

Step 1. **Log** > **Destination** の順にクリックし、をクリックして入力欄を展開させます。

Step 2. **Remote host** を選択します。



図表 5.15 サーバーへの転送設定

Step 3. **Address** 欄に、ログ転送先リモートサーバーの IP アドレスまたはホスト名を入力します。**Port** 欄に、リモートサーバーがログを受け入れるポートの番号を指定します。

Step 4. **Transport** 欄で、ログメッセージ転送に用いるプロトコルを選択します。UDP、TCP、そして暗号化された TLS プロトコルのいずれかを選択できます。UDP または TLS を選択すると、さらにパラメータを入力するための欄が現れます。UDP を選択した場合、転送先リモートサーバーは、受け入れたログメッセージはもともと SSB で生成されたものとみなします。最初ののログ送信元を保持するためには、**Spoof source address** オプションにチェックを入れます。

TLS を選択した場合、リモートサーバーの独自性を証明する必要があります。以下から選択します。

- **None**：証明書提示をリモートホストにリクエストしない。しかし、リモートホストから証明書が提示された場合は、全て受け入れる。

- **Optional Tursted**：リモートサーバーが証明書を提示したら、SSB はそれが有効期限内か、また **Common Name** に、ホストの IP アドレスあるいはドメイン名が含まれているかをチェックする。このチェックで引っかかると、SSB は接続を拒否する。ただし、リモートホストが証明書を提示しない場合は、接続を許可する。

- **Optional untrusted**：リモートホストは必ず証明書を提示しなくてはならない。SSB は、それがどんな証明書であっても受付けて、接続する。

■ **Required trusted**:リモートホストの証明書を検査する。認証局によって署名された証明書のみ受付ける。認証局による証明書に関して詳細は、4.5.7.2外部認証による証明書をアップロードするをご参照ください。証明書のCommon Nameに、ホストのドメイン名かIPアドレスのいずれかが含まれている必要がある。

■ **Request untrusted**:SSB は、リモートホストに証明書提示をリクエストする。以下の場合、接続を拒否する ①リモートホストが証明書を提示しない場合 ②証明書が有効期限切れの場合 ③Common Name 内に、ホストのドメイン名または IP アドレスが含まれていない場合。

注記

リモートサーバーの説明文書を読み、どのプロトコルがサポートされているかをご確認ください。

UDP は非常に信頼性の低いプロトコルです。何の警告も無しに、大量のログメッセージが喪失する危険性があります。可能な限り、TCP か TLS をお使いいただくことを推奨します。

Step 5. **Syslog protocl** 欄から、シスログのプロトコルを選択します。

■ 従来の BSD シスログプロトコル(RFC3164 準拠)をお使いになる場合、**Legacy** を選択します。次に、**message template** 欄で、お使いになるメッセージテンプレートを選択します。

- RFC3164 に定義されているフォーマットに従う場合、**Legacy**
- もともとのログのタイムスタンプを、ISO8061 準拠のタイムスタンプ付き(年及び標準時間帯地域の情報を含む)フォーマットに置換えたい場合→**ISOdate**
- ログのメッセージ部分を、マクロを用いて置換えたい場合→**Custom message part only**
- ログメッセージのフォーマットを全て(ヘッダ含めて)書き換えたい場合 →**Custom on-wire message**

を、それぞれ選択してください。マクロの使用に関する詳細は、*The syslog-ng 3.0 Administrator Guide* をご参照ください。特に必要がなければ、ISOdate テンプレートを選択してください。

■ IETF 形式シスログプロトコルをお使いになりたい場合は、リモートサーバーのアプリケーションに関する説明文をご確認ください。現状、多くの装置･アプリケーションは、まだ従来の BSD プロトコルしかサポートしていません。必要に応じて、マクロを用いてメッセージコンテンツをカスタマイズすることが可能です。なお、IETF シスログプロトコルにおいては、ヘッダーはカスタマイズできないことにご注意ください。マクロの使用に関する詳細は、*The syslog-ng 3.0 Administrator Guide* をご参照ください。

Step 6. SSB がリモートサーバーに対し、同一メッセージを複数回送信する可能性がある場合、Last message repeated n times. というメッセージを代わりに 1 回だけ送信することができます。同一メッセージの出現(代わりのメッセージを送出するまでの)待ち時間は、**Suppress timeout** 欄に入力します。この設定は、syslog-ng の suppress()パラメータに相当します。

Step 7. 秒あたりに転送するログメッセージの件数に上限を設けたい場合は、**Message throttle** 欄にその値を入力します。このオプションは、ログの喪失を防ぐために、ディスクバッファ機能と共に用いる場合のみ機能します。この値を 0 または 0 以下にすると、「上限無し」になります。この設定は、syslog-ng の throttle()パラメータに相当します。

Step 8. ほとんどのログメッセージのタイムスタンプは、秒単位までの正確性しか担保されていません。SSB は、もっと細かい単位のタイムスタンプ付加が可能です。**Timestamp fractions of a second** 欄で、秒の部分に何桁(=何分の 1 秒)までを含めるか指定します。この設定は、syslog-ng の frac_digits()パラメータに相当します。

Step 9. リモート DB サーバーと SSB が稼動しているマシンが、別個の標準時間帯地域に存在する場合で、レガシーメッセージテンプレートをお使いの場合、**Timezone** プルダウンで、サーバーの標準時間帯を選択します。これは、レガシーメッセージテンプレートには標準時間帯地域の情報が含まれていないためです。

Step 10. **Output disk buffer** 欄にて、ログメッセージを一時保持するディスクバッファの領域を設定します。リモートサーバーにアクセス不能となった場合、SSB はハードディスク上にログメッセージを保持し、復旧後に転送を再開します。この設定は、syslog-ng の log_disk_fifo_size()パラメータに相当します。

Step 11. リモートサーバーが、ログメッセージの受入をする処理速度が低下している場合に、SSB はデフォルトで 10000 件までをメモリに保持します。この値を変更するには、**Output memory buffer** 欄にて行います。この設定は、syslog-ng の log_fifo_size()パラメータに相当します。

Step 12. **Commit** をクリックします。

Step 13. リモートサーバーへログ転送を開始するには、ログパスに新たな転送先を加える必要があります。詳細は、5.4ログパスを管理するをご参照ください。

5.3.4 SNMPサーバーにログメッセージを転送する

目的:

ここでは、SSB から SNMP サーバーにログメッセージを転送する手順を説明します。

Step:

Step 1. **Log > Destination** の順にクリックし、 をクリックして入力欄を展開させます。

Step 2. **Type** 欄から、**SNMP destination** を選択します。

Step 3. **Address** 欄に、転送先 SNMP サーバーの IP アドレスまたはホスト名を入力します。Port 欄に、SNMP トラップを受け入れているポート番号を入力します。

Step 4. **SNMP trap settings** 欄にて、SNMP プロトコルのバージョンを選択します。

■ SNMP v2c をお使いになる場合、**SNMP v2c** を選択します。**Community** 欄に、コミュニティ名を入力します。デフォルトは public です。

■ SNMP v3c をお使いになる場合、**SNMP v3c** を選択します。パラメータ入力欄が現れます。

- username：SNMP トラップを転送するのに必要なユーザ名
- Engine ID：同じくエンジン ID
- Authentication method：認証の方法を選択します。(MD5 または SHA1)いずれを選択しても、Authentication password 欄が現れるので、認証パスワードを入力します。
- Encryption method：暗号化の方法を選択します。(Disabled または DES)DES を選択した場合、Encryption password 欄が現れるので、暗号化パスワードを入力します。

Step 5. ほとんどのログメッセージのタイムスタンプは、秒単位までの正確性しか担保されていません。SSB は、もっと細かい単位のタイムスタンプ付加が可能です。**Timestamp fractions of a second** 欄で、秒の部分に何桁(=何分の 1 秒)までを含めるか指定します。この設定は、syslog-ng の frac_digits()パラメータに相当します。

Step 6. リモート DB サーバーと SSB が稼動しているマシンが、別個の標準時間帯地域に存在する場合で、レガシーメッセージテンプレートをお使いの場合、**Timezone** プルダウンで、サーバーの標準時間帯を選択します。これは、レガシーメッセージテンプレートには標準時間帯地域の情報が含まれていないためです。

Step 7. **Output disk buffer** 欄にて、ログメッセージを一時保持するディスクバッファの領域を設定します。リモートサーバーにアクセス不能となった場合、SSB はハードディスク上にログメッセージを保持し、復旧後に転送を再開します。この設定は、syslog-ng の log_disk_fifo_size()パラメータに相当します。

Step 8. リモートサーバーが、ログメッセージの受入をする処理速度が低下している場合に、SSB はデフォルトで 10000 件までをメモリに保持します。この値を変更するには、**Output memory buffer** 欄にて行います。この設定は、syslog-ng の log_fifo_size()パラメータに相当します。

Step 9. **Commit** をクリックします。

Step 10. リモートサーバーへログ転送を開始するには、ログパスに新たな転送先を加える必要があります。詳細は、5.4ログパスを管理するをご参照ください。

5.4 ログパスを管理する

ここでは、ログパスの生成及び管理について説明します。

■デフォルトのログパス一覧に関しては、5.4.1SSBのデフォルトのログパス

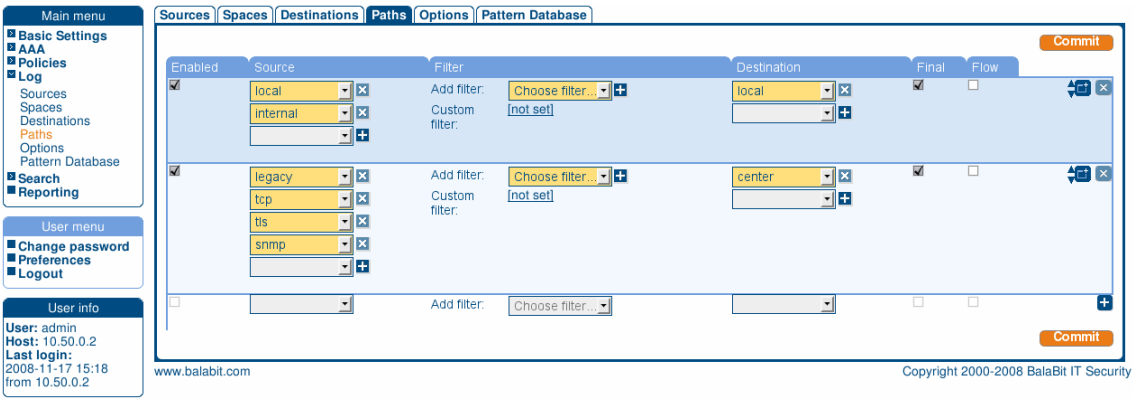
■新たなログパスを作成する手順は、5.4.2新しいログパスを作成する

■条件に合致したログメッセージのみを送信する設定手順は、5.4.3メッセージのフィルタリング

を、それぞれご参照ください。

5.4.1 SSBのデフォルトのログパス

Log > Paths の順にクリックします。デフォルトで、二つのログパスが既に設定されています。



図表 5.16 SSB のデフォルトのログパス

■最初のログパスは、SSB のローカルメッセージを収集します。Web インターフェイス、ビルトインの syslog-ng サーバー、そして他の内部コンポーネントにおいて生成されたログを、**local** ログスペースに送信します。

■二つ目は、デフォルトのシスログソース(詳細は 5.1.1 SSBのデフォルトのメッセージソースをご参照ください)から、あるいはSNMP(詳細は 5.1.2 SNMPメッセージの受信をご参照ください)経由で送信されるログパスです。これらのログメッセージは、**center**ログスペースに蓄積されます。

注記

このニつのデフォルトログパスには、**Final** のオプションにチェックが入っています。これは、条件に合致したら、それより下に定義されているログパスには当該ログメッセージが渡らない、という意味です。新たにログパスを作成する場合、順番を調整するか(より上に定義されたパスから検査されます)、**Final** のオプションを外してください。

5.4.2 新しいログパスを作成する

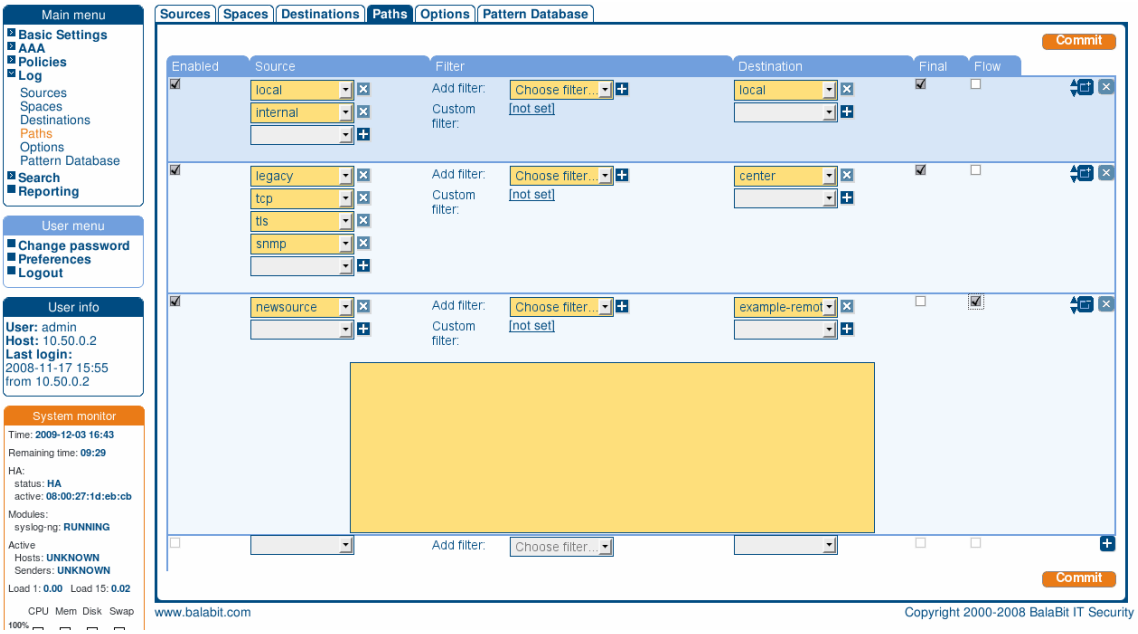
目的:

新たなログパスを作成する方法を説明します。

Step:

Step 1. **Log > Paths** の順にクリックし、**+**をクリックします。画面に新たなログパスが追加されます。

Step 2. **Source** フィールドのプルダウンで、このログパスで処理すべきログのソースを選択します。このログパスにさらにソースを追加する場合は、Source フィールドの**+**をクリックしてプルダウンを追加し、このステップを繰り返します。



図表 5.17 新たなログパスの作成

Remoteソースは、ネットワーク経由で到達したログを受信し、ビルトインソースは、SSBにて生成されたログメッセージをさします。SNMPソース(詳細は、5.1.2 SNMPメッセージの受信をご参照ください)も、ビルトインのソースに組込まれています。

ヒント

全てのソースの全てのログメッセージを処理対象にするには、source フィールドの選択欄を削除して、all にします。これは、syslog-ng の catchall フラグに相当します。

Step 3. **Destination** フィールドのプルダウンで、このログパスにおけるログメッセージ転送先を選択します。転送先をさらに追加する場合は、+をクリックしてプルダウンを増やし、このステップを繰り返します。

注記

Remote デスティネーションは、リモートサーバーまたはデータベースにログを転送するオプションで、**Log > Destination**画面にて設定します。(詳細は、5.3 SSBからログメッセージを転送するをご参照ください)

Local デスティネーションは、SSB ローカルの環境にログを蓄積します。**Log > Space** 画面にて設定します。(詳細は、5.2 SSBにログメッセージを蓄積するをご参照ください)

このログパスにおいて受信するログメッセージを蓄積しない場合は、**Destination** フィールドのプルダウンを **none-omitted** のままにしておきます。

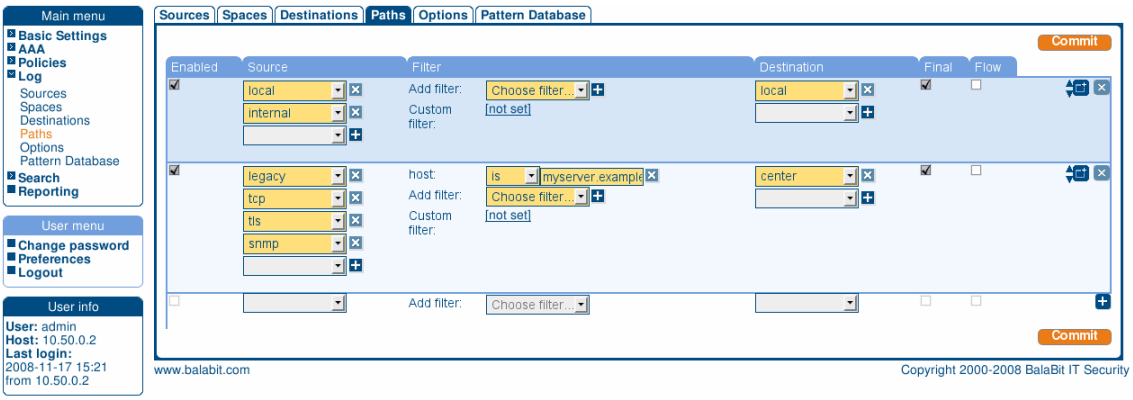
警告

デスティネーションを none に設定すると、このログパスで受信したログメッセージは全て捨てられます。これは、ログを警告無しに削除する唯一のオプションです。

Step 4. このログパスにおいて処理されたログメッセージを、他のログパスで処理させないようにするには、**Final** オプションのチェックを入れます。
ログパス一覧の順序は重要です。上位にあるログパスから優先的に処理される為です。**Final** にチェックが入っていると、そのログパスで処理されたログメッセージは下位のログパスに渡りません。ログパスの並び順を調整するには、ボタンをクリックします。

Step 5. フローコントロールを有効にするには、**Flow**フィールドの**Flow control**オプションにチェックを入れます。フローコントロールの機能に関して詳細は、2.3受信メッセージと送信メッセージをフローコントロールで管理するをご参照ください。

Step 6. このログパスで受信したログメッセージの一部のみを転送したい場合、フィルターを設定します。**Filter**フィールドの+をクリックして、必要に応じてフィルター条件を設定します。フィルター条件を追加するには、+をクリックしてプルダウンを増やします。ログパス内に設定した全てのフィルターにマッチしたログメッセージのみが、指定された転送先に転送されます。設定可能なフィルターについては、5.4.3メッセージのフィルタリングをご参照ください。



図表 5.18 ログメッセージのフィルタリング

Step 7. Commit をクリックします。その後、設定したログパスが、ログメッセージの収集を開始します。

ヒント

ログパスをすぐ無効にしたい場合、Enable オプションのチェックを外します。

5.4.3 メッセージのフィルタリング

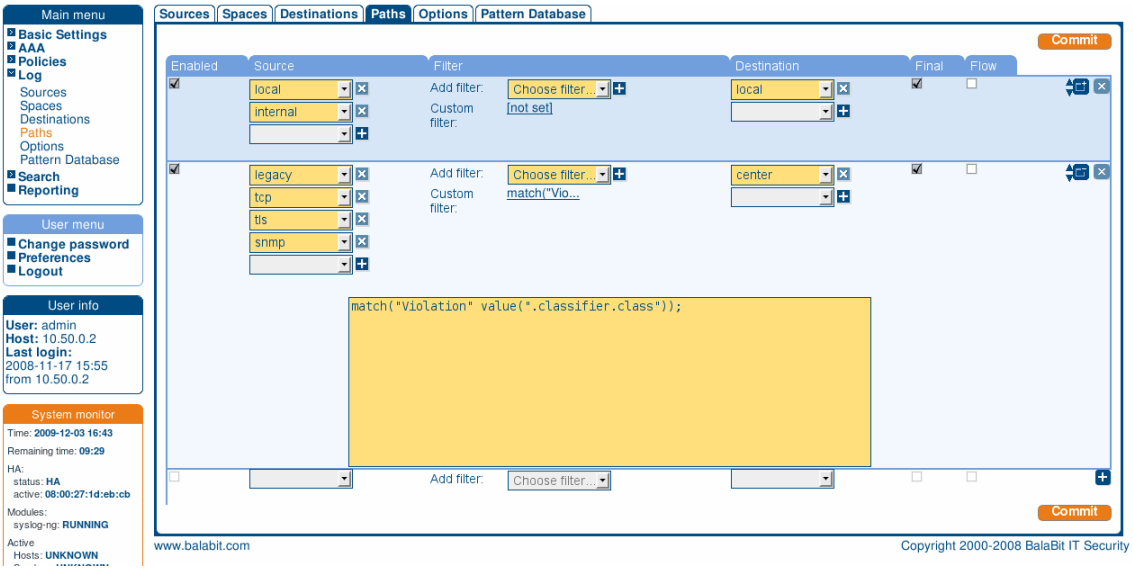
ここでは、ログパスにおいてフィルタリングをどのように用いるかを説明します。全てのフィルタリング条件で、マッチ(例:priority is) またはアンマッチ(例:priority is not)を適用できます。以下のフィルタリング項目を使用できます。

- ***facility***: 特定のファシリティ(例:kernel)から送信されログたメッセージのみを抽出します
- ***host***: 特定のホストから送信されたログメッセージのみを抽出します。ホスト名か IP アドレスを入力するか、正規表現で指定します。
- ***message***: メッセージのテキスト部分(ヘッダを除く)に対し、特定のキーワード、または、正規表現を指定して抽出します。
- ***priority***: 特定の優先度のログメッセージのみ抽出します。
- ***program***: 特定のアプリケーションから送信されたログメッセージのみ抽出します。アプリケーション名または正規表現で指定します。
- ***sender***: SSB にログメッセージを送信しているホストのアドレスで抽出します。

注記

全てのクライアントが SSB に直接、ログメッセージを送信している場合、"sender"と"host"のいずれのフィルターも同じように機能します。しかし、間にリレーサーバーが入っている場合は、"host"フィルターはクライアント(ログ発生元)のアドレスに適用され、"sender"フィルターは、リレーサーバーのアドレスに適用されます。

複数のフィルタリング条件が設定されている場合、**全ての**条件にマッチしたログメッセージのみ、指定された転送先に送信されます。(つまり、ログパス内のフィルタリングは論理積をとる、という意味になります)



図表 5.19 カスタムフィルターを使う

ログパスにより複雑なフィルタリング条件を設定したい場合は、をクリックして、展開された入力欄にカスタムフィルタリングの条件を入力します。ここに入力された値は、syslog-ng の filter()パラメータにペーストされます。

5.4.3.1 手順 rewriteを使用しメッセージを修正する

目的:

Syslog-ng アプリケーションは rewrite ルールを使用し、メッセージの部分を書き換えることができます。ほぼ全てのメッセージのパーツが書き換え可能です。ルールは、key-value ペアフォーマットを使用します。

Step:

Step 1. **Log > Paths** の順にクリックします。

Step 2. rewrite ルールを使用した path(s)を選択します。

Step 3. **Rewrites** セクションにてボタンをクリックし、新規 rewrite ルールを追加します。Rewrite ルールはフィルタリング前、あるいはフィルタリング後に適用されます。フィルタリングと rewrite のシーケンスは log path にそれがどのように指定されているかに依存します。処理シーケンスは以下の通りです。

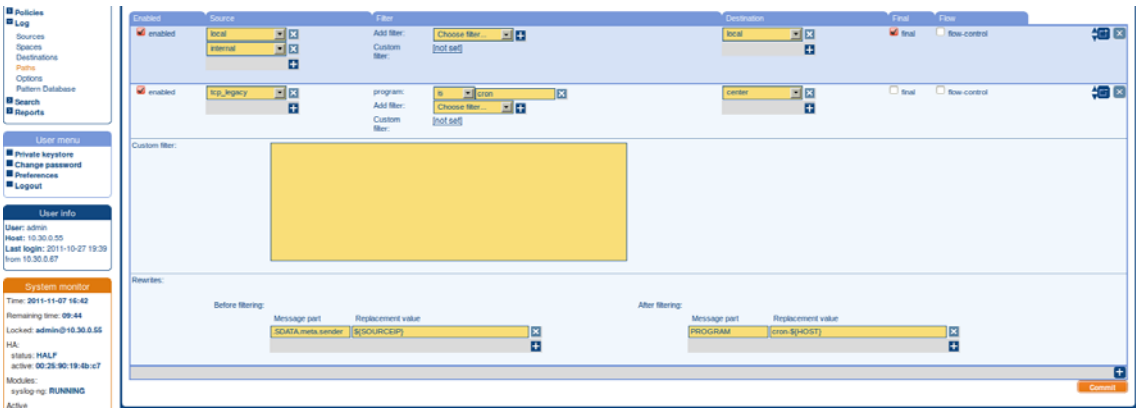
1. rewrite ルールの順番に沿って、“before filtering”rewrite ルールを使用すること

によってメッセージパートを書き換えます。

2. メッセージをフィルターします。

3. rewrite ルールの順番に沿って、“after filtering”rewrite ルールを使用することによってメッセージパートを書き換えます。

4. メッセージを destination に送信します。



図表 5.20 rewrite ルールを使用したメッセージの修正

Step 4. rewrite のため、**Message part** フィールドにメッセージのパートを入力します。例: MESSAGE; HOST;.SDATA.meta.custom. もし、指定したフィールドが存在しなかった場合、それは自動的に作成され **Replacement value** フィールドに設定されます。

Step 5. 書き換え後の **Replacement value** フィールドにメッセージパートの値を入力してください。マクロを使用するには、$からはじめ括弧でマクロ名を囲ってください。例 : ${MSG};${.SDATA.meta.custom}

注記

交換する値はメッセージパートの古い値を完全に置き換えます。

注記

ハードマクロは、ログメッセージから直接引き出されたデータを含みます。rewriteルールにおいてハードマクロの値を変更することは不可能です。ハードマクロのリストについては、*syslog-ng Premium Edition Administrator Guide.* の*Hard vs. soft macros*、セクションを参照してください。

5.5 syslog-ngのオプションを設定する

SSB 内部で稼動している syslog-ng サーバーには、設定変更可能な以下のオプションがあります。

■syslog-ng全般的な設定に関して詳細は、5.5.1 syslog-ngの全般的な設定

■タイムスタンプ関連のオプションに関して詳細は、5.5.2 SSBにおけるタイムスタンプ設定

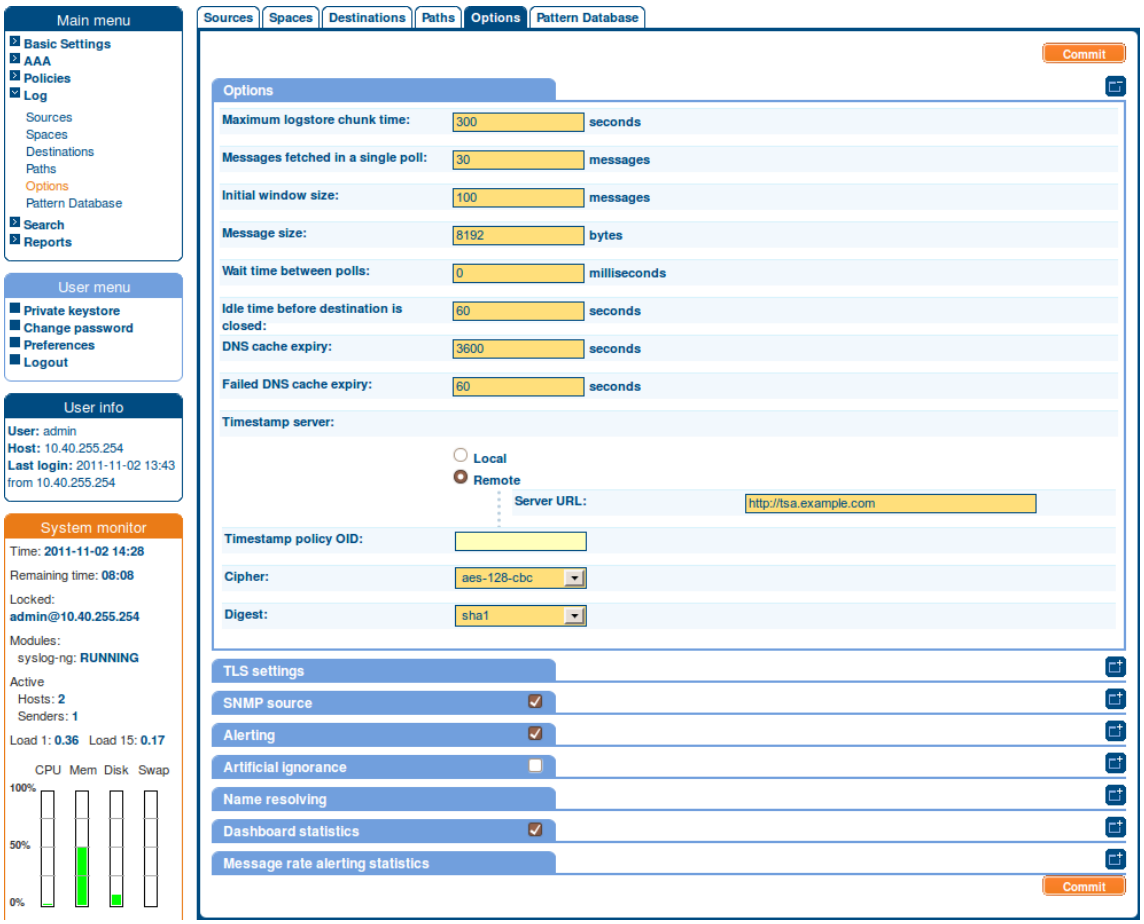
■TLS暗号化によるログメッセージ送受信の際の証明書管理に関する詳細は、5.5.4 TLS暗号化ログ送受信に用いる証明書の設定

■ログメッセージのドメイン名解決に関する詳細は、5.5.3 SSBにおける名前解決

を、それぞれご参照ください。

5.5.1 syslog-ngの全般的な設定

SSB内部で稼動しているsyslog-ngサーバーの全般的な設定項目は、**Log > Options**の順にクリックして表示させます。以下のオプションを設定できます。(名前解決に関するオプションは、5.5.3 SSBにおける名前解決にて説明します)



図表 5.20 syslog-ng のオプション設定

■ ***Maximum logstore chunk time***:(秒)syslog-ng は、ここの設定値の間に新たなログメッセージがログスペースに到着しなかった場合、チャンクをクローズします。なお、"Idle time before destination is closed" オプションの設定値に達した場合、全ファイルがクローズされます。この設定項目は、syslog-ng の chunk_time()パラメータに相当します。

■ ***Message fetched in a single poll***:ポーリング時のループ 1 回ごとに、ソースから取込まれるログメッセージの件数に上限値を設定します。この設定値が大きいと、フローコントロールがログの新たな取り込みを中断する以前に、ログ転送先のキューがあふれてしまう可能性があります。この設定項目は、syslog-ng の log_fetch_limit()パラメータに相当します。

■ ***Initial window size***:フローコントロールに用いられる、メッセージウインドウの初期サイズを設定します。この項目は、syslog-ng の log_iw_size()パラメータに相当します。

■ ***Message size***: 受信するログメッセージ長の上限をバイト単位で指定します。この項目は、syslog-ng の log_msg_size()パラメータに相当します。

■ ***Wait time between polls***:ログのソースに、新たなメッセージが到着していないかポーリングをするまでの待ち時間を、ミリ秒で指定します。この項目は、syslog-ng の time_sleep()パラメータに相当します。

■ ***Idle time before destination is closed***:アイドル状態のログ転送先がクローズされるまでの時間を秒で指定します。この項目は、syslog-ng の time_reap()パラメータに相当します。

5.5.2 SSBにおけるタイムスタンプ設定

SSB におけるタイムスタンプの方法を設定するには、**Log > Options** の順にクリックします。
以下のオプションが設定可能です。

■ ***Timestamp server***: 暗号化されたログスペースに用いられるタイムスタンプ方法を指定します。

- **Local**: SSB 内蔵のタイムスタンプサーバーを使用する場合
- **Remote**: 外部のタイムスタンプサーバーを使用する場合

→**Server URL** 欄が現れるので、タイムスタンプサーバーの IP アドレスを入力します。なお、現在のところプレーンの HTTP サーバーのみサポートしています。パスワード保護、または HTTPS サーバーはサポートしておりません。

警告

SSB では、現在のところ Internet X.509 Public Key Infrastructure Time Stamp Protocol(TSP – RFC3161 準拠)のみを現在サポートしています。

■ Timestamp policy OID:タイムスタンプサーバーに、そのポリシーが設定されている場合は、その OID を入力します。SSB は、TSA(タイムスタンプ認証局)にタイムスタンプリクエストを送

信する際、その ID 情報を含めます。

■Cipher：ログストアを暗号化するための方法を、以下のメソッドからプルダウンで選択します。

aes-128-cbc, *aes-128-cfb*, *aes-128-cfb1*, *aes-128-cfb8*, *aes-128-ecb*, *aes-128-ofb*, *aes-192-cbc*, *aes-192-cfb*, *aes-192-cfb1*, *aes-192-cfb8*, *aes-192-ecb*, *aes-192-ofb*, *aes-256-cbc*, *aes-256-cfb*, *aes-256-cfb1*, *aes-256-cfb8*, *aes-256-ecb*, *aes-256-ofb*, *aes128* , *aes192* , *aes256*, *bf* , *bf-cbc* , *bf-cfb*, *bf-ecb* , *bf-ofb* , *blowfish*, *cast* ,*cast-cbc* , *cast5-cbc* , *cast5-cfb*, *cast5-ecb*, *cast5-ofb* , *des*, *des-cbc*, *des-cfb* ,*des-cfb1* , *des-cfb8* , *des-ecb* , *des-ede*, *des-ede-cbc*, *des-ede-cfb* , *des-ede-ofb*,*des-ede3* , *des-ede3-cbc*, *des-ede3-cfb*, *des-ede3-ofb*, *des-ofb* , *des3* , *desx* ,*desx-cbc*, *rc2*, *rc2-40-cbc* , *rc2-64-cbc*, *rc2-cbc*, *rc2-cfb*, *rc2-ecb* , *rc2-ofb*, *rc4*, *rc4-40*.

デフォルトでは、aes-128-cbc メソッドを使用します。

■Digest：ダイジェストの方法を、以下からプルダウンで選択します。

MD2, *MD4*, *MD5*,*SHA-0 (SHA)*, *SHA-1*, *RIPEMD-160*, *SHA-224*, *SHA-256*, *SHA-384*,*SHA-512*.

デフォルトでは、SHA-1 を使用します。

警告

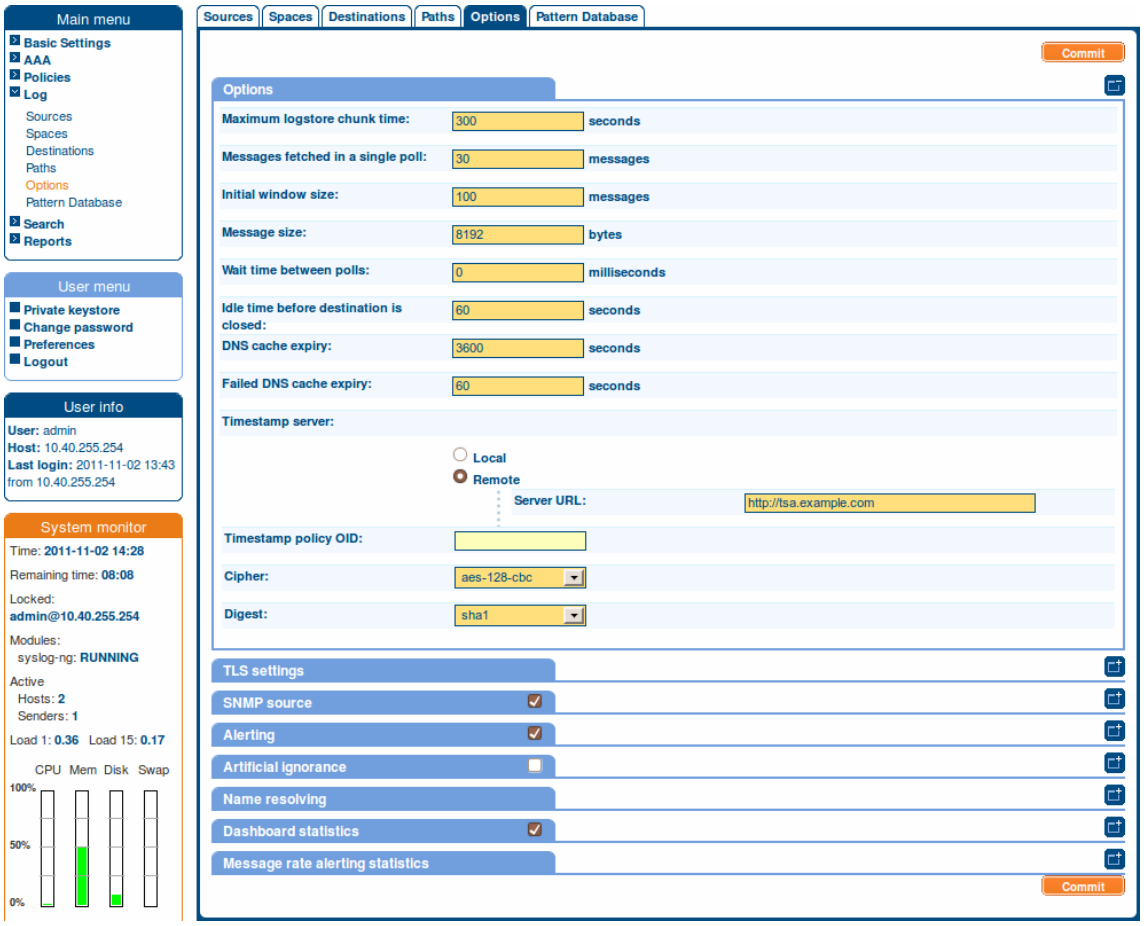
ダイジェストのハッシュ関数の大きさは、暗号化方法の鍵サイズに等しいか、それより大きくなければなりません。例えば、aes-256cbc を用いる場合、ダイジェストハッシュは少なくとも SHA-256 である必要があります。

注記

タイムスタンプリクエストは、独立したプロセスで処理されます。ログメッセージの処理が、タイムスタンプサーバーの処理遅延またはアクセス障害に影響されることはありません。

5.5.3 SSBにおける名前解決

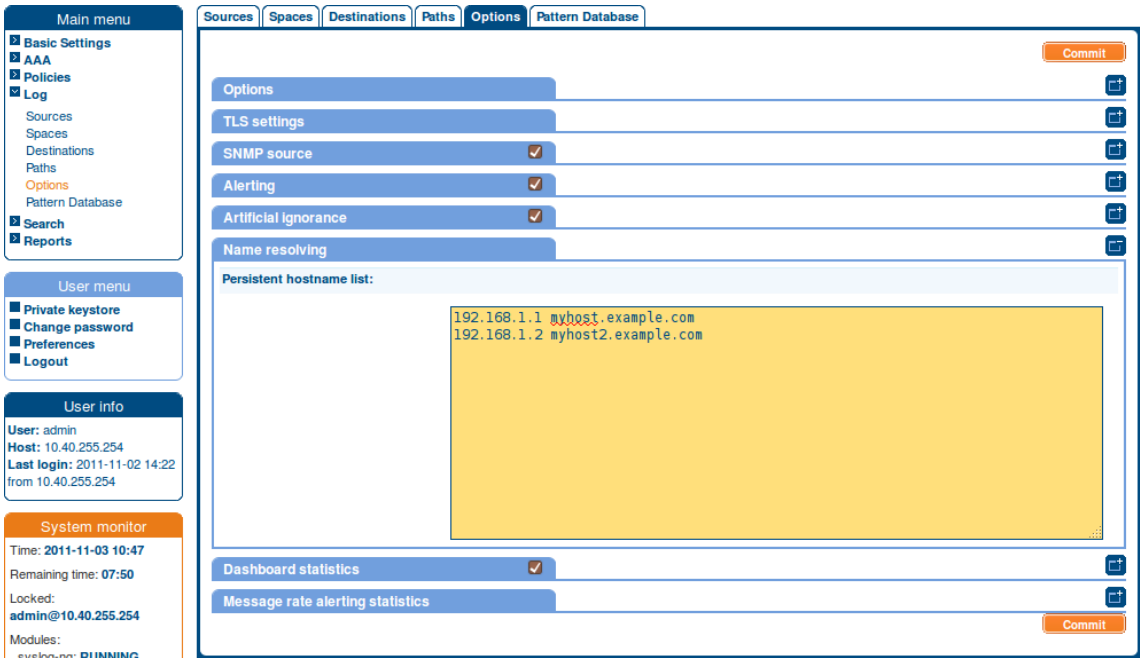
SSB は、クライアントのホスト名を解決し、ログメッセージにそれを含ませることができます。しかし、DNS サーバーにアクセス障害が発生したり、処理が極端に遅くなったりした場合に、SSB 全体の処理に大きな影響がでます。SSB は名前解決ができたかどうかの情報を自動でキャッシュします。もし負荷が高い状況下で問題が発生するようであれば、名前解決機能をオフにすることを推奨します。名前解決が必須の場合は、以下を考慮してください。



図表 5.21　DNS オプションの設定

■Log > Options の順にクリックします。
クライアントの IP アドレスがめったに変更されない場合は、DNS Cache expiry と Failed DNS chache expiry を大きな値にします。デフォルトでは、それぞれ、1 時間、1 分となっています。

■ローカルでの(静的な)ホスト名解決を検討します。頻繁にログを送信してくるホストの解決を、DNS サーバーに依存することなくローカルで行えます。IP アドレスーホスト名のペアを、ファイルとしてローカル環境にあらかじめ設定しておきます。syslog-ng が、ログメッセージ上の該当する IP アドレスをホスト名に置換えます。ローカル環境での解決を設定するには、Log > Options > Name resolving の順にクリックし、展開された入力欄 Persistant hostname list 欄に、ホスト名ーIP アドレスのペアを入力します。その後、Log > Sources の順にクリックし、Use DNS 欄のオプションで、Only from persistent configration を選択します。



図表 5.22 静的な名前解決の設定

5.5.4 TLS暗号化ログ送受信に用いる証明書の設定

目的:

カスタム証明書、または認証局による証明書を暗号化されたログ送受信に用いるための手順を説明します。

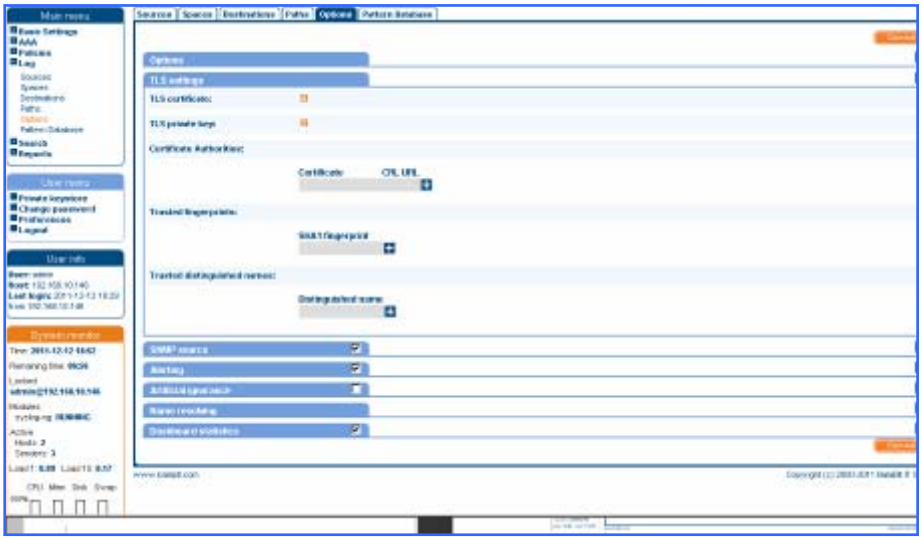
注記

TLS 通信における証明書をアップロードしていない(=TLS 証明書及び TLS 秘密鍵オプションが設定されていない状態)場合、SSB は Web インターフェイス用に設定された証明書、または認証局証明書を適用します。(この証明書は、**Basic Settings > Management > SSL certificate** にて設定されます)

Step:

Step 1. まず、PKI(公開鍵基盤)にてあなたご自身の証明書を作成し署名します。そして、**Log > Options > TLS settings** の順にクリックします。

Step 2. **TLS certificate** 欄の をクリックして、証明書をアップロードします。



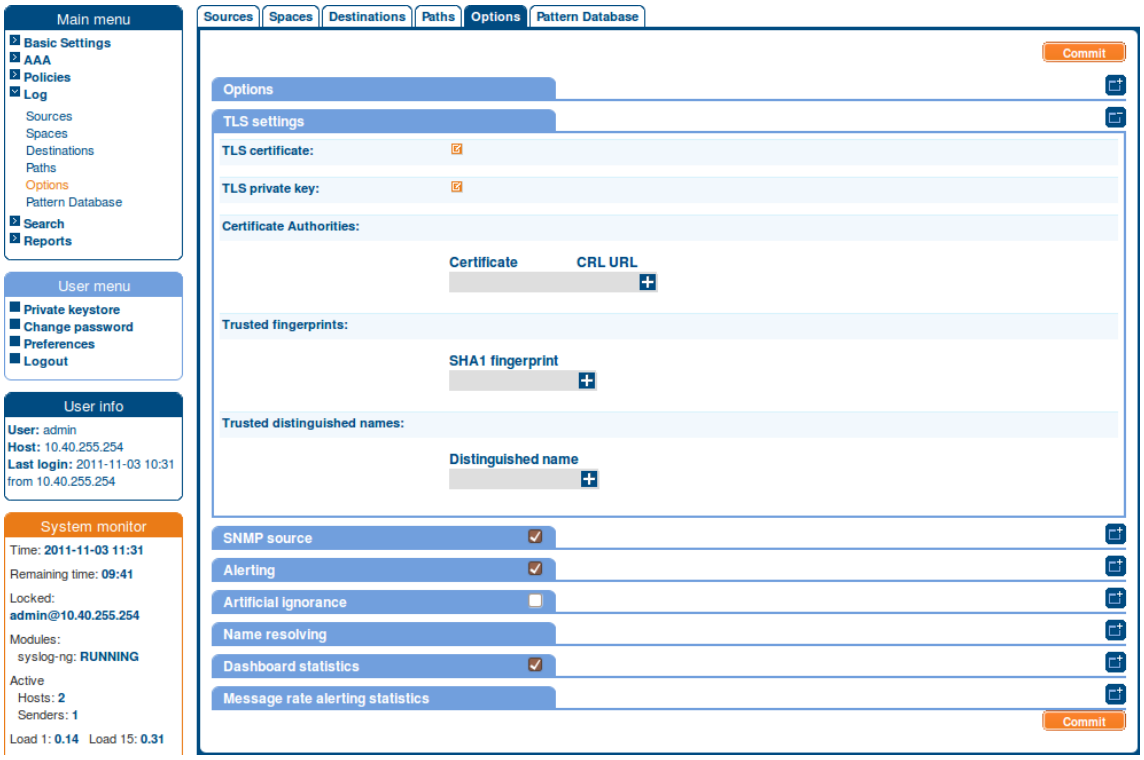
図表 5.23 syslog-ng の TLS 設定

ファイルからアップロードする証明書を選択する場合は、開いたポップアップウインドウ内の**参照**をクリックし、ファイルを選択します。その後、**Upload** をクリックします。

あるいは、**Copy and paste certificate** セクションの Key 欄に、証明書を貼り付け、**Upload** をクリックすることもできます。

Step 3. **TLS private** key 欄の をクリックし、証明書に紐づいている秘密鍵をアップロードします。

Step 4. ログを送信するホストのアイデンティティを、認証局による証明書で検査する場合は、 **Certificate Authorities** 欄の をクリックし、 をクリックします。ポップアップ画面が開きます。



図表 5.24 証明書のアップロード

ファイルから証明書をアップロードする場合は、**参照**をクリックし、ファイルを選択します。その後、**Upload** をクリックします。

あるいは、**Copy-paste certificate** 欄の Key 欄に、証明書を貼り付け、**Upload** をクリックすることもできます。

認証局による証明書をさらに追加したい場合、このステップを繰り返します。

Step 5. 指定した認証局が CRL(失効したデジタル証明書のリスト)を発行している場合、そのURL を **CRL URL** 欄に入力します。それにより、SSB は CRL を定期的にダウンロードし、リストに存在する証明書の使用を拒否します

注記

..pem フォーマットの CRL のみ許可されます。PKCS7 フォーマット(.crl)の CRL は許可されません。

Step 6. 認証局により署名された特定の証明書のみを使用しているホストからのみ、接続を許可したい場合、**Trusted distinguished names** 欄の+をクリックして、現れた入力欄に DN(識別名)を入力します。

Step 7. 認証局による証明書のアップロード無しで証明書を受付けたい場合、**Trusted fingerprints** 欄の+をクリックし、受付けられた SHA-1 指紋を **SHA-1 fingerprint** 欄に入力します。

6　ログメッセージとレポートを閲覧する

ここでは、SSB においてさまざまなログメッセージをどのように見るか、そしてどういった情報をそれらが含んでいるのかを説明します。

■全般的なsearchインターフェイスの使用に関しては、6.1　searchインターフェイスを使う（一部の検索インターフェイスには、特別な機能が含まれており、該当するセクションで各々説明されています)をご参照ください。

■SSBWebインターフェイス上で実行された、設定変更に関するアカウント情報：SSBのユーザ(Adminユーザを含む)が行ったオペレーション履歴を表示します。**AAA > Acounting**の順にクリックして表示させます。表示されるパラメーター覧は、6.2　SSBにおける設定変更ログをご参照ください。

■収集されたログメッセージ：ローカル環境のログスペースないしは外部データベースシステムに蓄積されたログは、**Search > Logs**の順にクリックし、保存先（ログスペースまたはデータベースサーバー）を、**Destinations**から選択することで閲覧できます。表示されるパラメーター覧は、6.3　SSBで収集されたログメッセージをご参照ください。

■ピアーの設定変更：syslog-ngプレミアムエディション 3.0 または以降がインストールされているピアー(クライアントコンピュータ)は、設定が変更された際に、SSBに向けて特別なメッセージを送信します。**Search > Peer configuration changes**の順にクリックして閲覧できます。表示されるパラメーター覧は、6.4　syslog-ngのピアー(クライアントコンピュータ)の設定変更をご参照ください。

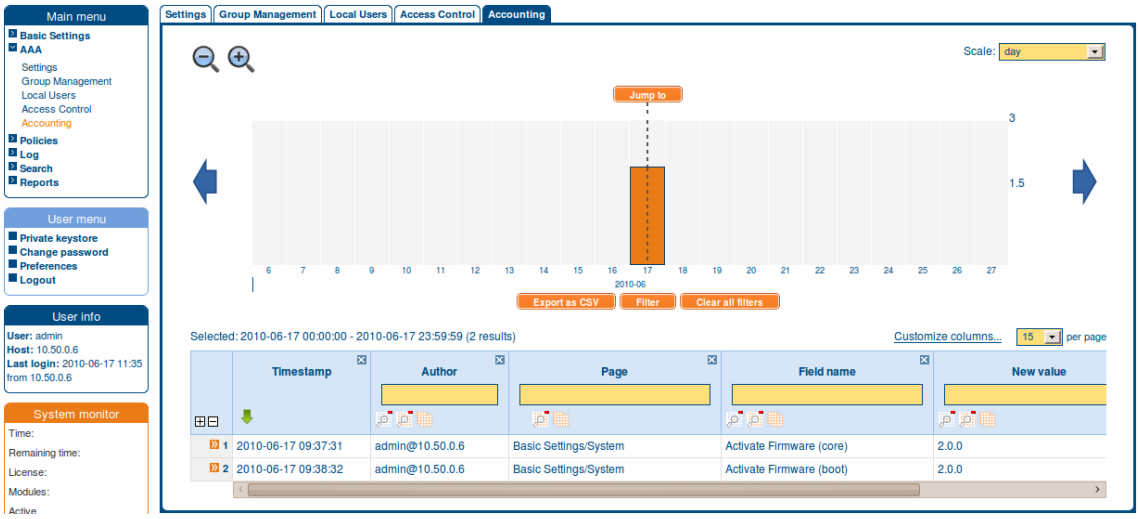
■ログメッセージ上のアラート：パターンデータベースを用いて、条件に合致したらアラートを発信するように設定している場合、アラート履歴が**Search > Log Alerts**の順にクリックして閲覧できます。表示されるパラメーター覧は、6.6ログメッセージのアラートをご参照ください。

■バックアップ・アーカイブ通知：バックアップあるいはアーカイブ中に発生した通知・アラートは、**Search > Archive & Cleanup**の順にクリックすると表示できます。表示されるパラメーター覧は、6.5アーカイブ・バックアップの通知をご参照ください。

■SSBのレポート：設定変更・システムヘルス・その他のアクティビティに関するレポートをpdf形式で、**Reports > Generated reports**の順にクリックすると閲覧できます。表示されるパラメーター覧は、6.8レポートをご参照ください。

6.1 searchインターフェイスを使う

SSB は、ログメッセージの閲覧・設定変更・レポート閲覧に、統一されたインターフェイスを提供します。search インターフェイスは、大きく分けて日付バーとテーブル、2 つの部分から構成されています。



図表 6.1 検索インターフェイスを使用する

日付バー部分は、指定された期間内のログメッセージ件数を表示します。アイコンで、ズームとズーム解除ができます。矢印をクリックすれば、表示されている機関より前後を表示します。表示させる日付を明示的に指定するには、**Jump to** をクリックするとカレンダーがポップアップで現れ、日を指定できます。1 画面に表示させる期間は、**Scale** プルダウンで変更できます。

日付バーの上にマウスポインタを当てると、そのグラフが表している、件数と、表示されている期間の日付範囲が表示されます。グラフをクリックすると、データが表になって画面中央より下の部分に表示されます。複数のグラフを選択したい場合、shift キーを押したままクリックします。**Selected** 欄は、表に現れているデータの日付範囲を表示します。

6.1.1 テーブルの列をカスタマイズする

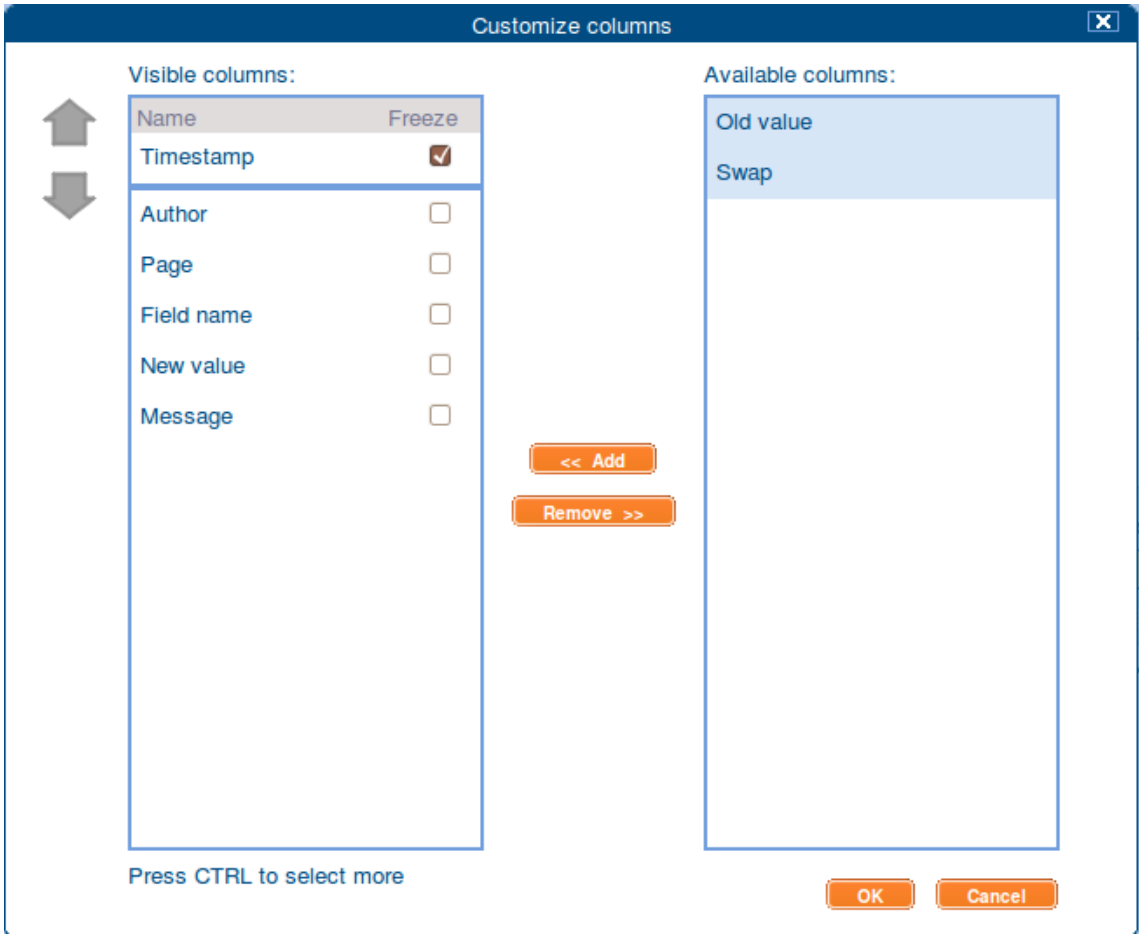
目的:

SSB は、全てのログメッセージでさまざまなパラメータを記録します。表示させるデータの指定方法を説明していきます。

Step:

Step 1. 閲覧したいデータを表示させます。(例:**AAA > Acounting**)

Step 2. **Customize Columns** をクリックします。ポップアップウインドウが現れ、現在表示されている列と、追加可能な列が表示されます。



図表 6.2 search 情報

Step 3. **Visible columns** 欄に表示されているのが、現在表示されている列、**Available columns** 欄は、その他の、表示に追加することが可能な列を表します。

- **Visible columns** 欄に列を追加する場合、追加したい列名をクリックして、**Add** をクリックします。
- **Visible columns** 欄から列を削除したい場合、削除したい列名をクリックして **Remove** をクリックします。
- 列をフリーズ(スクロールしても列名が見えているようにする)するには、列名右の **Freeze** オプションにチェックを入れます。

注記

複数の列を選択するには、Ctrl を押下したままクリックします。

Step 4.　表示させたい列が決まったら、**OK** をクリックします。

6.1.2 動的列を追加/削除する

目的:

動的列は、パラメータ名－値　のペアで定義されます。定義された列は、Customize Columnsウィンドウに表示されます。(詳細は 6.1.1テーブルの列をカスタマイズするをご参照ください)また、オートコンプリート機能で検索することもできます。パラメータ名－値のペアから動的列を作成する方法を説明します。

Step:

Step 1.　パラメータ名－値のペアは、**Details**　列欄にて、カンマで分割されています。選択したいキー値の上にマウスポインタを置きます。

Step 2.　をクリックします。

Step 3.　Step2 で選択されたキー値のパラメータ名部分が、そのまま列名になり、**Dtails**　列の前に挿入されます。ペアとなっている値は、それぞれのセルに格納されます。

Step 4.　テーブルから動的列を削除する場合は、列名右上の をクリックします。パラメータ名－値ペアは、**Details** 列に戻ります。

値の文字数が長くて 1 行に収まりきらない場合、デフォルト状態では最初の行のみ表示されます。表示領域を拡大して値を全て見えるようにするには、⊞をクリックします。元に戻すには、⊟をクリックします。また、テーブルの該当行のどこかをダブルクリックしても、同じように拡大/縮小が行えます。

テーブルの表示は、単一または複合条件によるフィルタリングが可能です。フィルタリングを行うには、条件を **Search** 欄に入力し、**Filter** をクリックします。あるいは、テーブル内に表示されている値をクリックします。例えば、設定変更ログのテーブルで、特定のユーザに絞って表示させたい場合、ユーザ名を **Search** 欄に入力して **Search** をクリックするか、またはテーブル内データのユーザ名を直接ダブルクリックすれば、フィルタリングされた結果が表示されます。

注記

フィルタリングを設定した後は、日付バー部分にはフィルタリングされた結果のデータが表示されます。

フィルタリングの際、部分的に一致するデータも表示されます。例えば、設定変更ログで Author のフィルタリングを"adm"とした場合、adm の文字を含む全てのユーザが表示されます。

注記

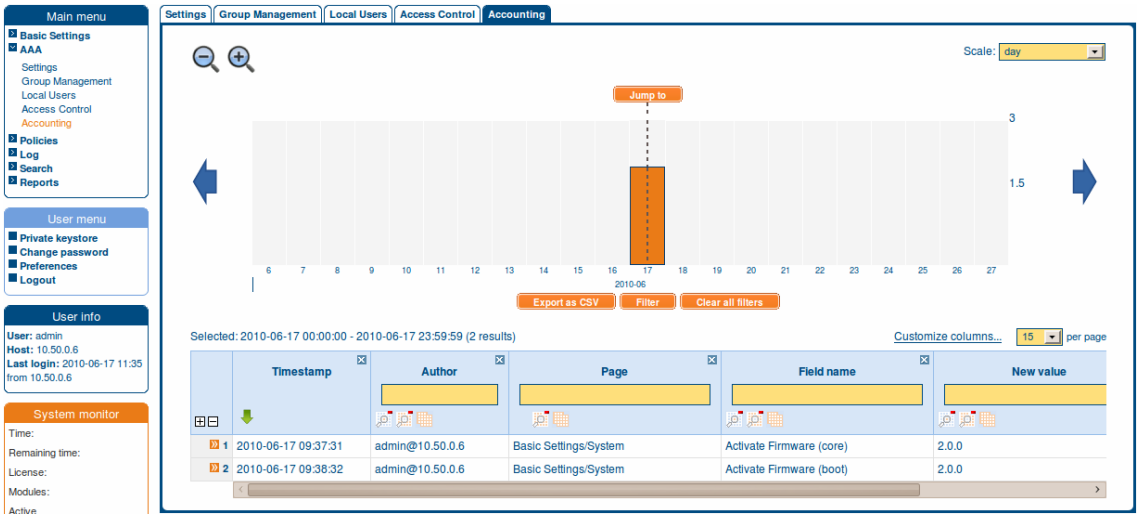
ログストア内の検索においては、部分一致検索は機能しません。
完全一致のみです。

フィルタリングした結果を保存したい場合は、**Export as CSV** をクリックします。カンマ区切りのテキストファイルとして保存されます。エクスポート時にエラーが発生した場合、CSV ファイルには "0"と、問題の詳細を記述した行のみが保存されます。例：0;description_of_the_error

テーブルを元の表示状態に戻すには、**Clear all fiters** をクリックします。

6.2 SSBにおける設定変更ログ

SSB は、ユーザ(Administrator 含む)の行ったオペレーションを自動的に記録・蓄積します。**AAA > Acounting** の順にクリックすると表示されます。以下の情報が取得できます。



図表 6.3 設定変更履歴の表示

- ***Timestamp***：変更が行われた日付・時刻。yyyy-mm-dd hh:mm:ss 形式です
- ***Author***：設定変更を行ったユーザ名
- ***Page***：変更が加えられたメインメニュー(例：Basic Settings > Management)
- ***Field name***：上記「Page」内の、実際に変更が加えられたフィールド名
- ***New value***：変更後の新しい設定値
- ***Description***：変更が実施された際、ユーザによって入力された説明。これは、**AAA > Settings > Require commit log** オプションが有効になっている場合のみ記録されます。
- ***Old value***：変更前の設定値
- ***Swap***：変更対象のオブジェクトがリスト形式で、その並び順に変更が加えられた場合にサインされる

6.3 SSBで収集されたログメッセージ

SSB ローカルに、あるいはリモートサーバー上に蓄積されたログメッセージは、**Search > Logs**

の順にクリックして閲覧できます。ログメッセージを蓄積しているデスティネーションを、Destination 欄から選択します。

■表示可能な列に関しては、6.3.1収集されたログメッセージに関するメタデータ

■フィルターの適用･保存に関して詳細は 6.3.3検索フィルターの使用と管理

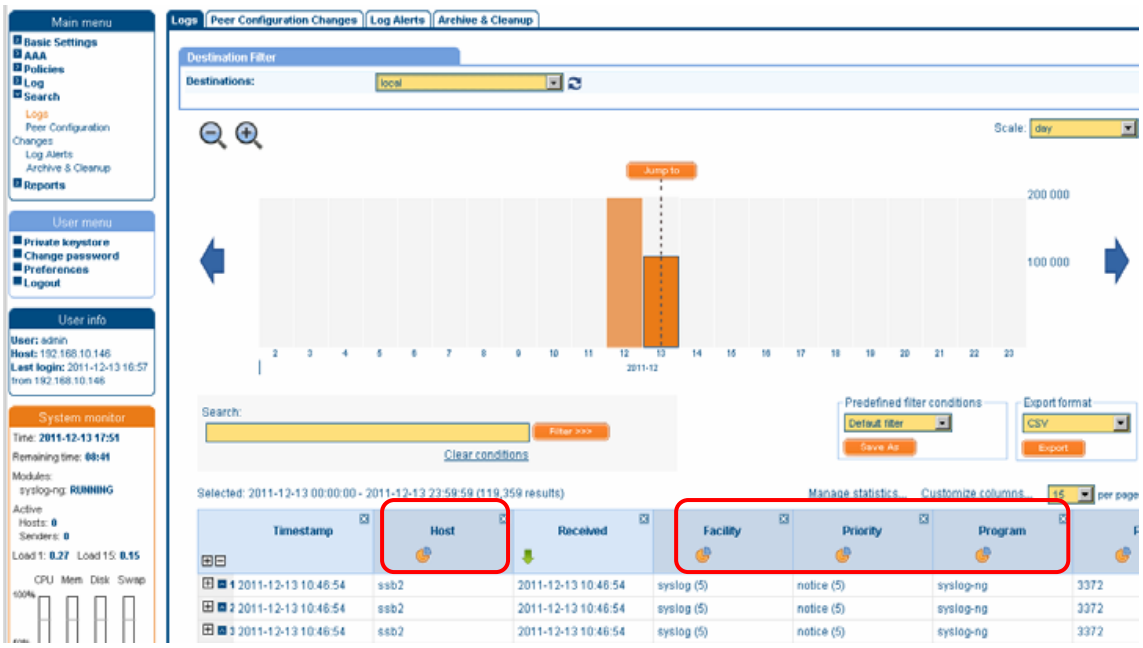
■検索結果を統計表示させる方法に関しては、6.3.4検索結果の統計を表示する

■暗号化されたログストア内の、ログメッセージブラウズ･検索に関して詳細は、6.3.5暗号化されたログスペース内のブラウズ

をそれぞれご参照ください。

6.3.1 収集されたログメッセージに関するメタデータ

ログメッセージに関して以下の情報が取得できます。



図表 6.4　search 情報の画面表示

インデックス付加され、検索可能なフィールドは、ヘッダー部分がやや濃い色になっていて区別できます。(上図赤枠)

■ ***Received***: SSB がログメッセージを受信した日付･時刻。yyyy-mm-dd　hh:mm:ss 形式

■ ***Timestamp***: 受信したログメッセージのタイムスタンプ。ログが生成された時刻。
yyyy-mm-dd　hh:mm:ss 形式

■ ***Facility***: ログを送信したファシリティ

■ ***Priority***: ログメッセージの優先度

■ *Program*: ログが生成されたアプリケーション

■ *Pid*: ログメッセージが生成されたアプリケーションのプロセス ID

■ *Host*: SSB にログを送信したクライアントの IP アドレスあるいはホスト名

■ *Message*: ログのメッセージ部分

■ *Tags*: 特定のパターンデータベースに合致したメッセージに付加されたタグ

■ *Rule ID*: メッセージに合致したパターンデータベースのルール ID

■ *Details*: パラメータ名－値のペア

■ *Rule description*: メッセージに合致したパターンデータベースのルールに関する説明

6.3.2 ワイルドカードとブーリアンを使った検索

検索は、ワイルドカードとブーリアン表現【ブール式】にて SSB で容易に使用することができます。以下のセクションにてサーチクエリの例を挙げます。

■ 完全一致と複雑なクエリの詳細については、セクション 完全一致と複雑なクエリによる検索を参照してください。

■ メッセージの指定のパート内の検索についての詳細は、セクション メッセージの指定のパート内の検索を参照してください。

■ 検索キーワードの組み合わせについての詳細は、セクション 検索キーワードの組み合わせを参照してください。

■ ワイルドカード検索の使用の詳細については、セクション ワイルドカード検索の使用 を参照してください。

■ スペシャルキャラクターの検索の詳細については、セクション スペシャルキャラクターの検索 を参照してください。

完全一致と複雑なクエリによる検索

デフォルトでは、SSB はログメッセージの MESSAGE パート内の全ワードをキーワードとして検索します。そして、完全一致のみ表示します。

例 6.1 : 完全一致の検索

例 : キーワード example による検索:

検索表現:

■ example

マッチする場合:

■ example

マッチしない場合:

■ examples

■ example.com

■ query-by-example

■ exam

検索を実行するために、メッセージの特定の部分を指定することができ、より複雑な検索クエリを書き込むことができます。ブーリアンを使用したワイルドカード検索は、すべてのフィールドでサポートされています。

例 6.2 複雑な検索クエリ

例:キーワード example による検索:

検索表現:

■ message1 AND (host:testhost OR program:syslog*)

メッセージの指定のパート内の検索

<type>: プレフィックスを使用して、メッセージの指定パート内の検索が可能です。message: (or msg:)プレフィックスは、メッセージパートを意味し、省略可能です。例:アプリケーション名を検索したい場合は、program;プレフィックスを使用してください。ホスト名を検索したい場合は、host: プ レフィックスを使用してください。

検索キーワードの組み合わせ

ブーリアン演算子を検索キーワードを組み合わせるために使用できます。より複雑な検索表現も

()を使用することで可能です。

例 6.3 検索におけるキーワードの組み合わせ

あなたは、AND,OR,NOT 演算子によって、キーワードを組み合わせることができます。

例:

■ keyword1 AND keyword2 (returns log messages that contain both keywords)

■ keyword1 OR keyword2 (returns log messages that contain at least one of the keywords)

■ host:host1 AND program:prg1

■ message:example AND program:prg1

ブーリアン演算子(例:AND)として解釈できる表現を検索するには、以下の形式を使用してください。: message:AND.

例 6.4 検索における()の使用

括弧()を使用して、より複雑な検索表現を作成することができます。

例:

■ (keyword1 OR keyword2) AND keyword3

ワイルドカード検索の使用

検索表現に、以下のワイルドカードキャラクターが使用可能です。

例 6.5 検索におけるワイルドカードの使用

? (クエスチョンマーク)は正確に一つの任意の文字を意味します。

例:

■ 検索表現

・ example?

マッチする場合:

・ example1

・ examples

マッチしない場合:

- example.com
- example12
- query-by-example
- example?

■ 検索表現

- ?example?

マッチする場合:

- 1example2

マッチしない場合:

- example.com
- example12
- query-by-example

■ 検索表現:

- example??

マッチする場合:

- example12

マッチしない場合:

www.balabit.com 151

Using wildcards and boolean search

- example.com
- example1
- query-by-example

? ワイルドカート検索は、 UTF-8 でない文字あるいは、マルチバイト文字を検索することができません。これらの文字を検索する場合、検索表現 ?? が使えるかもしれません。* ワイルドカード検索は、UTF-8 でない文字あるいは、マルチバイト文字を検索します。

例 6.6 検索におけるワイルドカード*の使用

*は 0 あるいはそれ以上の任意の文字を意味します。例:

■ 検索表現

・ example*

マッチする場合:

・ example

・ examples

・ example.com

マッチしない場合:

・ query-by-example

・ example*

■ 検索表現:

・ *example

マッチする場合:

・ example

・ query-by-example

マッチしない場合:

・ example.com

・ example12

■ 検索表現:

・ *example*

マッチする場合:

・ example

・ query-by-example

・ example.com

・ example12

*ワイルドカード検索は、UTF-8 でない文字、マルチバイト文字を検索します。

例 6.7 検索におけるワイルドカードの組み合わせの使用について
ワイルドカード文字は組み合わせできます。
例:

検索表現:

■ ex?mple*

マッチする場合:

■ example1
■ examples
■ example.com
■ exemple.com

マッチしない場合:

■ exmples
■ example12

www.balabit.com 152

Using wildcards and boolean search

■ query-by-example

ワイルドカード文字はどのメッセージパートでも動作します。例:program:postfix*

スペシャルキャラクターの検索

クエスチョンマーク(?), アスタリスク (*), バックスラッシュ (\) または スペース ( ) 文字を検索するためには、接頭辞としてバックスラッシュ (\を使用しなければなりません。バックスラッシュの後の文字は、検索されるための文字として扱われます。例:

例 6.8 スペシャルキャラクターの検索
スペシャルキャラクターを使用する場合は、バックスラッシュ (/)を使用してください。

.

検索表現:

■ example\?

マッチする場合:

■ example?

マッチしない場合:

■ examples

■ example1

スペシャルキャラクターバックスラッシュキャラクターを検索する場合二つのバックスラッシュを使用してください(¥¥)。

.

検索表現:

■ C:¥¥Windows

マッチする場合:

■ C:¥Windows

検索表現:

■ C:¥¥Program¥ Files

マッチする場合:

■ C:¥Program Files

6.3.3 検索フィルターの使用と管理

検索条件を入力する際、AND、OR、NOT 演算子を用いてより複雑な条件を設定することができます。このとき、スペースは"AND" とみなされることにご留意ください。また、**"NOT"** 演算子は、必ず**他の演算子と併用**しなくてはなりません。(例:adm AND NOT admin)また、「フィールド名:検索語」の組合せを用いて検索をすることもできます。(例:プログラム名フィールドで値が CRON のみのレコードを抽出するなら、program:CRON)

設定したフィルタ条件は保存して再利用することが可能です。

6.3.3.1 フィルター条件を作成し、再利用するために保存する

目的:

フィルター条件設定ならびに後で再利用する方法を説明します。

Step:

Step 1. **Search** > **Logs** の順にクリックし、転送先を選択します。

Step 2. フィルター条件を設定し、**Predefined filter condtions** > **Save As** の順にクリックします。

ポップアップウインドウが開きます。

Step 3. **Name** 欄に、フィルター条件の名前を入力します。

図表 6.5 フィルタリング条件の検索

Step 4. 他の SSB ユーザにもこのフィルターを利用させる場合は、**Global** を選択します。特定のユーザに限定したい場合は、**Group** 欄にユーザグループ名を入力します。**Local** を選択すると、作成したあなたのみが、このフィルターを後で利用できます。

Step 5. 検索対象のログの日付範囲を絞る場合は、Interval オプションにチェックを入れます。日付を入力する欄が現れるので、開始/終了日付を入力します。これは、特定のイベントのみを検索したい場合などに有効です。なお、**Global** を選択した場合は、日付範囲指定は必須となります。(Global を選択すると、日付入力欄が現れます)

Step 6. **OK** をクリックし、保存します。

Step 7. 保存済フィルター条件を適用させるには、**Predefined filter condtions** プルダウンから、フィルターを選択します。保存済フィルターの削除をしたい場合、ここで **Delete** をクリックします。なお、保存済フィルターの削除は、**Manage global fiters** 権限を許可されているユーザのみが行えます。

注記

ログメッセージの検索において、検索エンジンの処理能力は、対象となるログスペースのログに付加されているインデックスのデリミッタによります。Ver1.0.2 以降は、インデックス付加の際にデリミッタを指定できるようになりました。しかし、一度受信したログメッセージは、インデックスの再付加はできません。

このことは、Ver1.0.2 以前は、IPアドレスやMACアドレスのような形式の値は、全体がそのままの形でログメッセージからは拾われないことを意味します。"."(ピリオド)や":"(コロン)が、デリミッタとして認識され、その間の値がそれぞれ独立したフィールドの値として扱われてしまうからです。インデックス付加の際のデリミッタ設定に関して詳細は、5.2.4.1新しいログストアを作成するとご参照ください。

6.3.4 検索結果の統計を表示する

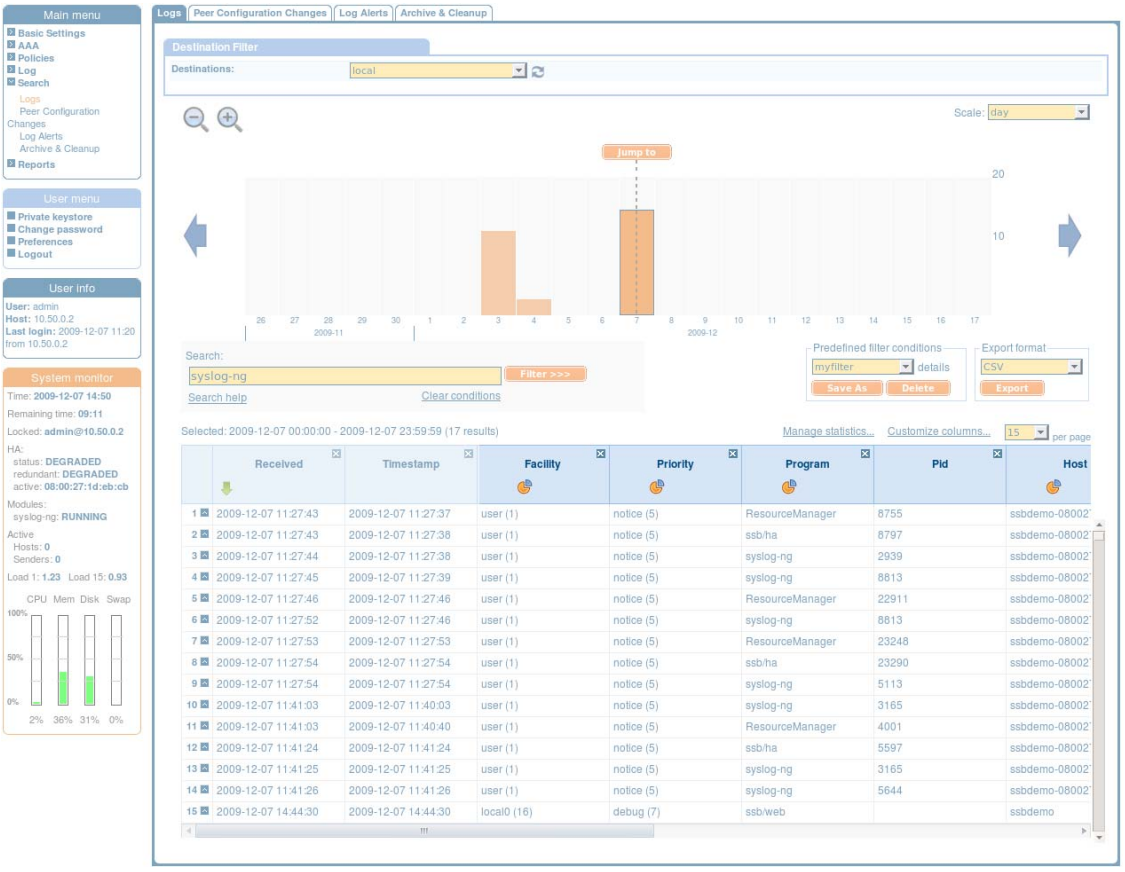
目的:

SSB は、さまざまな情報を統計化して棒グラフ、円グラフ、表形式で表示させることができます。(例:ログ送信元ホストの分布)収集したログメッセージに関する統計を表示させる手順を説明します。

Step:

Step 1. **Search** > **Logs** の順にクリックし、転送先を選択します。

Step 2. 必要に応じてフィルター条件を設定し、テーブル部分のフィールド名下にある円グラフアイコンをクリックします。ポップアップウインドウが現れます。



図表 6.6 統計情報の画面表示

Step 3. メタデータを表示させたいフィールドを選択します。フィールド名欄に、円グラフアイコンが表示されているフィールドのみ、表示が可能です。現在のところ、**Facility**、**Priority**、**Program**、**Pid**、**Host**、**Tags**、**.classifier.class** フィールドが統計表示可能です。

注記

.classifier.classデータは、パターンデータベースが設定されているときのみ、メッセージに適用されるクラスです。詳細は、第 7 章 パターンデータベ

ースによるメッセージのクラス分けをご参照ください。Balabit社から提供している現状のパターンデータベースにおいては、デフォルトで以下のメッセージクラスがあります。system、security、violation、unknown

Step 4. 表示形式を、**Bar**(棒グラフ)・**Pie**(円グラフ)・**List**(表形式)の中から選択します。表示は同じポップアップウインドウ内に展開されます。

注記

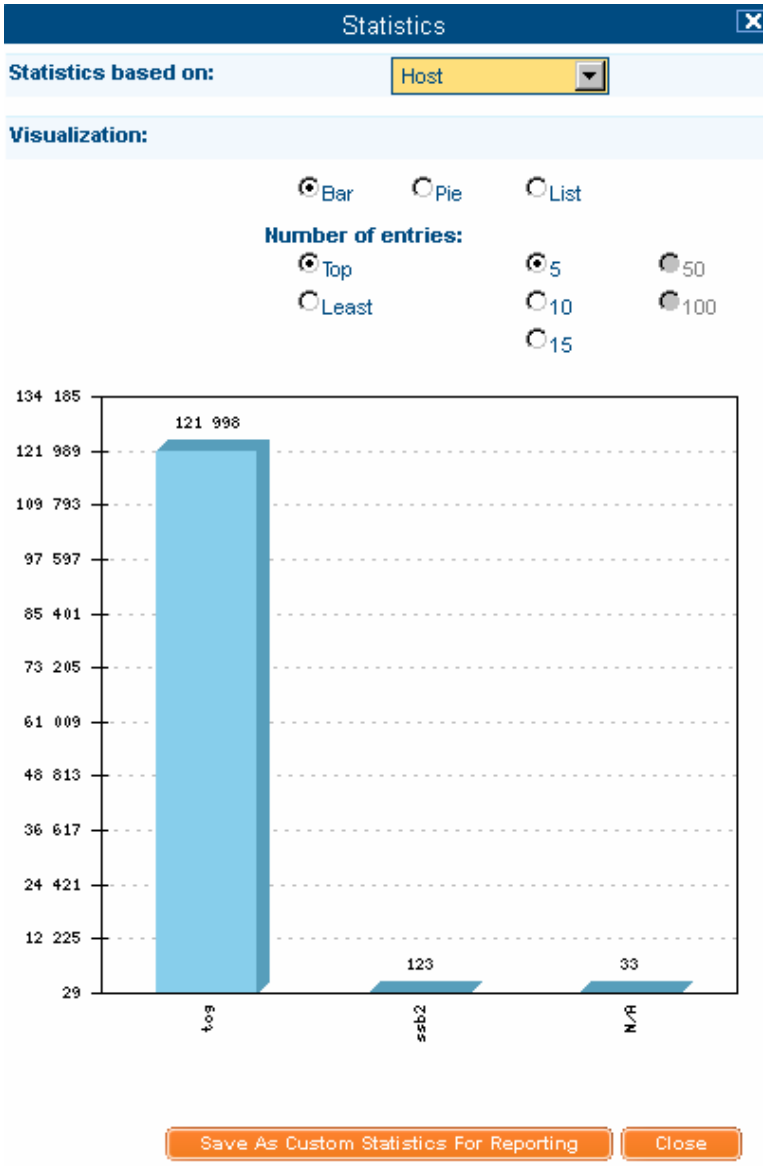
表形式表示では、パーセンテージが 100%になることがあります。ただし、統計がタグに基づいている場合、メッセージに複数のタグが紐づいている関係上、100%を上回る数値になることもありえます。

Step 5. デフォルトでは、統計は降順(件数の多い方から)表示になります。昇順に変更するには、Least を選択します。

Step 6. Number of entries グループで、表示させるデータのグループを選択します。例えば、ログを SSB に送信しているホストの上位 10 までを表示させたいなら、Top と 10 を選択します。すると、トップ 10 が個別に表示され、それ以外のホストは"Others"にまとめて表示されます。

注記

円グラフや棒グラフの場合は、5、10、15 を、表形式では 5、10、15、50、100 を指定できます。



図表 6.7 表示形式の選択

Step 7. (オプション)CSV で統計を出力するには、List を選択し、number of entries を選択後、Export all to CSV をくりっくします。SSB は、results.csv ファイルに統計を出力します。

注記

このオペレーションでは、表示されているレコードのみではなく、対象となる全てのレコードが出力されます。

Step 8. (オプション)これらの統計は、保存した上で、既にあるレポートの項目として、その中に入れ込むことが可能です。この設定は、**Reports > Configuration** の順にクリックして行います。

Step e. Save As Custom Statistics For Reporting をクリックし、レポートに用いるカスタム統計として保存します。

Step f. **Name** 欄に、この統計の名前を入力します。

Step g. **Group** 欄に、定義済のグループ名を入力します。選択の際、オートコンプリート機能が手助けをしてくれます。

Step h. (オプション)**Add to report as a subchapter** 機能は、この統計を、選択したレポートの項目として即座に入れ込むことを可能にします。

Step i. **Save**をクリックします。これにより、**Reports > Configuration**画面で選択可能な、保存済み統計になります。選択したレポートに項目を入れ込む手順について詳細は、6.9カスタムレポートの設定をご参照ください。

6.3.5 暗号化されたログスペース内のブラウズ

デフォルトでは、SSBWebインターフェイスから暗号化されたログスペースを閲覧することはできません。SSBが、必要とされる複号鍵の情報を持っていないからです。暗号化されたログスペースを見られるようにするために、SSBは以下のオプションを提供します。**複号鍵をSSBにアップロードし、全ユーザが使えるようにする**:秘密鍵(または公開鍵-秘密鍵のペア)をアップロードし、ログスペース内のログファイル複号にそれを用いることが可能です。これにより、当該ログスペースにアクセスする権限を有するユーザは誰でも暗号化されたログスペースを閲覧することができますが、同時に、その複号鍵は、SSBの設定ファイル内に、**暗号化されない状態で**保存されます。このことがセキュリティ上問題となる場合、ほんとうに必要な場合以外はこの方法を用いないでください。詳細は、6.3.5.1ログストアに複号鍵を適用するをご参照ください。

■**特定ユーザ向けの複号鍵をアップロードする**:複号鍵をSSBにアップロードし、それを特定にユーザに紐付けてそのユーザのみが利用できるように設定することが可能です。複号鍵はSSB内に保存されますが、パスワード保護され、そのパスワードを知っているユーザのみが使用できます。詳細は、6.3.5.2ユーザアカウントに複号鍵を割り当てるをご参照ください。

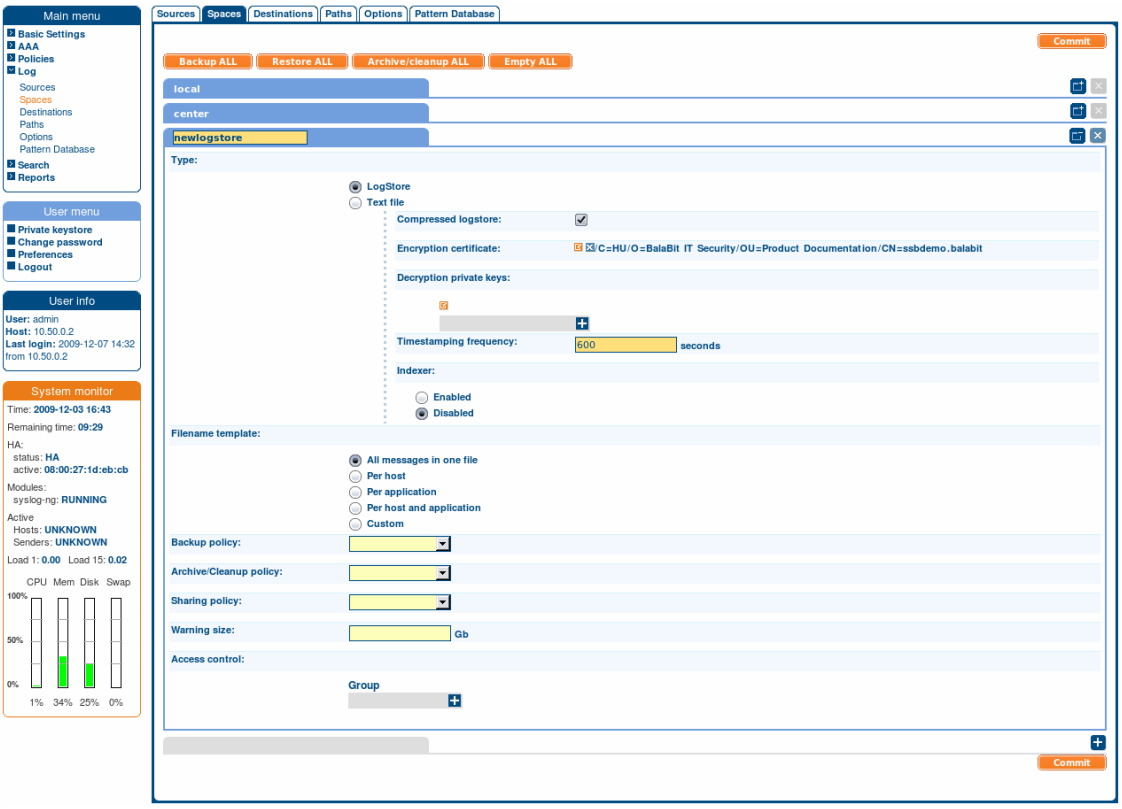
■**一時的に複号鍵をアップロードする**:SSBに、一時的な複号鍵をアップロードすることができます。アップロード後、ユーザが暗号化されたログスペースにアクセスし、ユーザがログアウトした時点で、その一時複号鍵は捨てられます。詳細は、6.3.5.3一時的な複号鍵を使うをご参照ください。

6.3.5.1 ログストアに複号鍵を適用する

Steps:

Step 1. **Log > Spaces** の順にクリックし、SSBWeb インターフェイスから全ユーザのアクセスを可能にしたい、暗号化ログスペースを指定します。

Step 2. **Decryption private Keys** 欄の をクリックします。ポップアップウインドウが現れます。



図表 6.8 ログストアに暗号化キーを追加する

Step 3. ログスペースを暗号化するための証明書秘密鍵を、ポップアップウインドウで**参照**から選択するか、直接データを貼り付けてアップロードします。

Step 4. さらに鍵を追加する場合は、上記ステップを繰り返します。

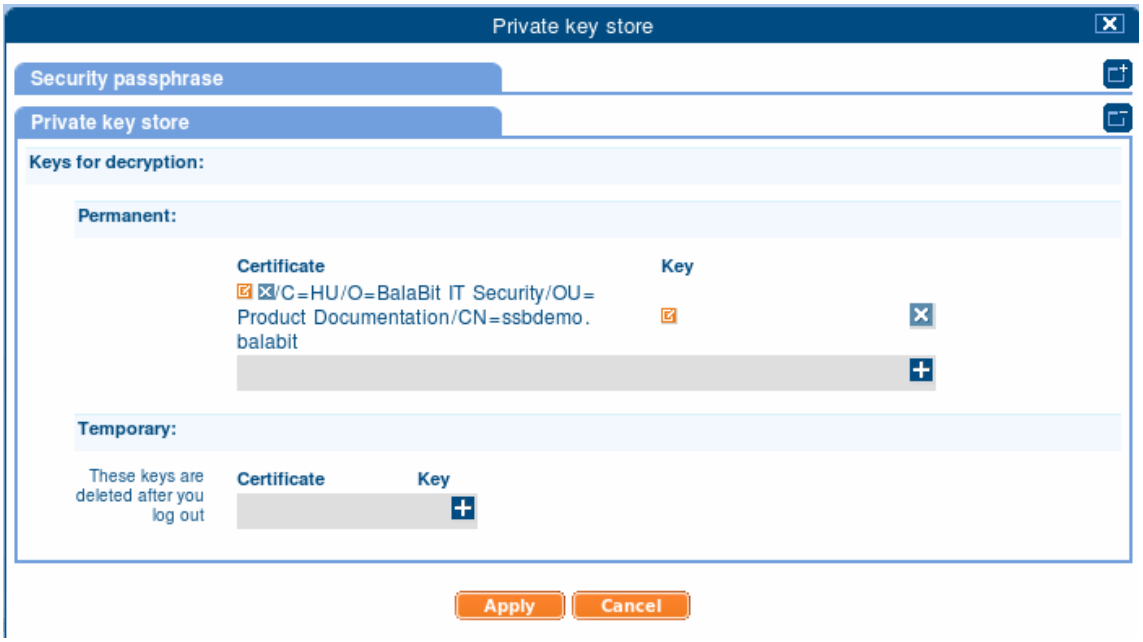
Step 5. **Commit** をクリックします。

6.3.5.2 ユーザアカウントに複号鍵を割り当てる

Step:

Step 1. UserMenu の **Private keystore** をクリックします。ポップアップウインドウが現れます。

Step 2. **Permanent** の をクリックします。さらに欄が現れます。Certificate の方の をクリックします。するとさらにポップアップウインドウが表示されます。



図表 6.9 秘密鍵ストアに、暗号化キーを追加する

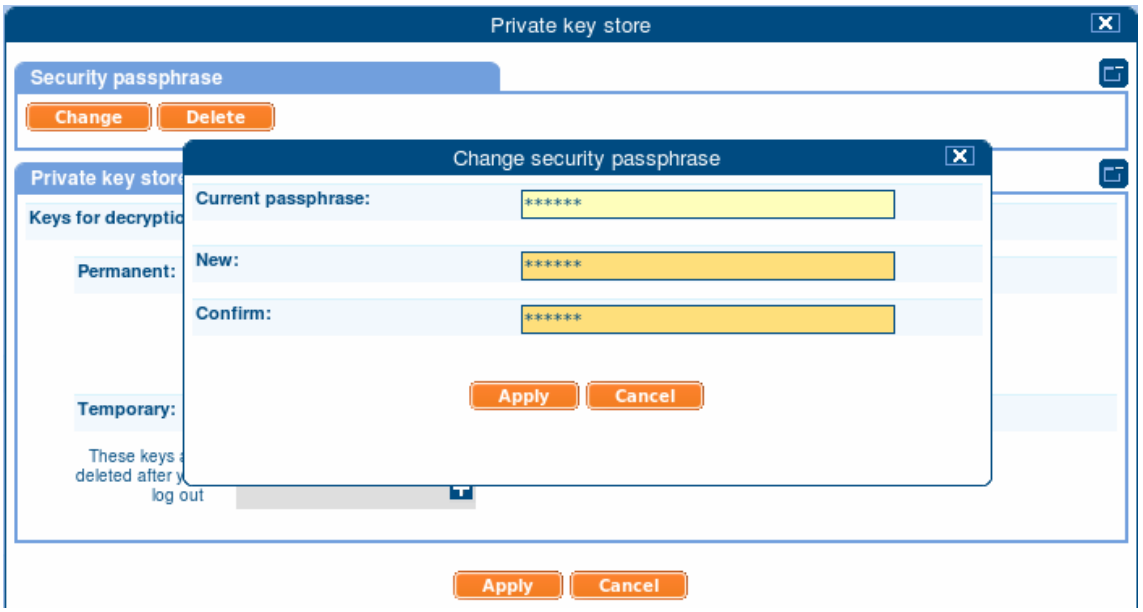
Step 3. ログスペースを暗号化するための証明書を、ポップアップウインドウの**参照**で選択するか、直接貼り付けてアップロードします。

Step 4. **Key** の方の をクリックします。同じく、ポップアップウインドウが開きます。

Step 5. ログスペースを暗号化するための秘密鍵を、**参照**で選択するか直接貼り付けるかでアップロードします。

Step 6. さらに鍵を追加する場合は、Step2～5 を繰り返します。

Step 7. **Security passphrase** タブ ＞ **Change** の順にクリックします。秘密鍵を保護するパスワードを入力します。



図表 6.10 秘密鍵ストアに、暗号化キーを追加する

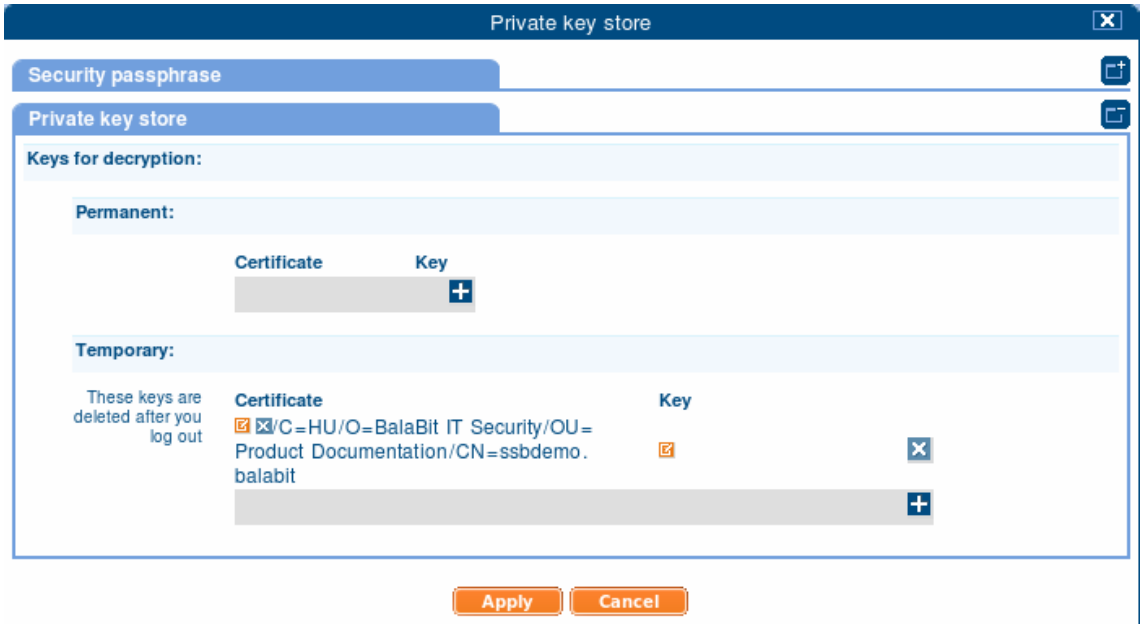
Step 8. 全て入力したら、**Apply** をクリックします。

6.3.5.3 一時的な複号鍵を使う

Step:

Step 1. **UserMenu** の **Private keystore** をクリックします。ポップアップウインドウが現れます。

Step 2. **Temporary** の をクリックします。さらに欄が現れます。Certificate の方の をクリックします。するとさらにポップアップウインドウが表示されます。



図表 6.11 秘密鍵ストアに暗号化キーを追加する

Step 3. ログスペースを暗号化するための証明書を、ポップアップウインドウの**参照**で選択するか、直接貼り付けてアップロードします。

Step 4. **Key** の方の をクリックします。同じく、ポップアップウインドウが開きます。

Step 5. ログスペースを暗号化するための秘密鍵を、**参照**で選択するか直接貼り付けるかでアップロードします。

Step 6. さらに鍵を追加する場合は、Step2～5 を繰り返します。

Step 7. 全て入力したら、**Apply** をクリックします。

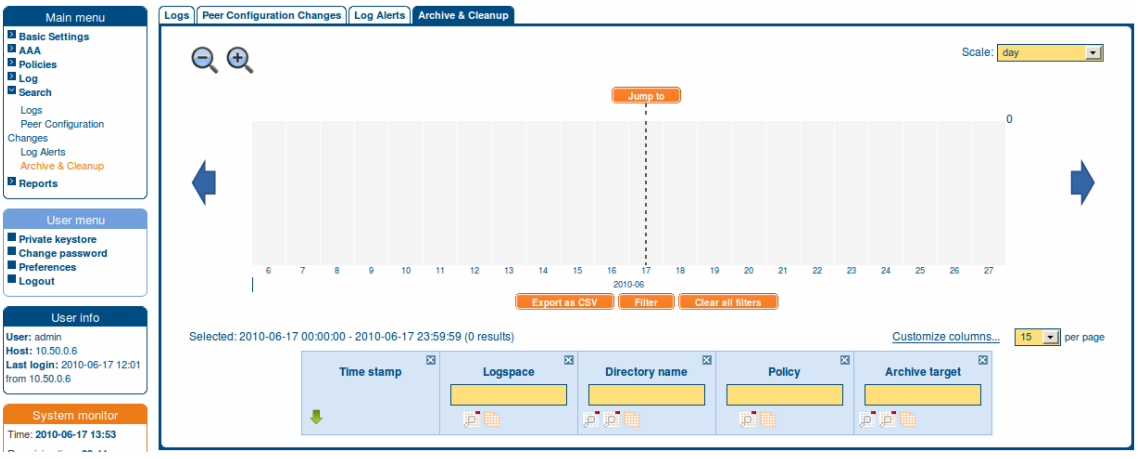
6.4 syslog-ngのピアー(クライアントコンピュータ)の設定変更

syslog-ng プレミアム(有償)エディションのバージョン 3.0 及び以降がインストールされているピアーは、設定変更がなされると SSB に対して自動的に通知します。そのログは、SSB の **Search > Prre Configuration Change** で確認できます。ただし、その通知ログには、変更内容は含まれないことにご留意ください。単に、変更が加えられたことのみを通知します。以下の情報が通知ログより取得可能です。

- ***Timestamp***: 受信したログのタイムスタンプ。ログが生成された日付と時刻を意味し、yyyy-mm-dd hh:mm:ss 形式
- ***Hostname***: 設定変更が加えられた、クライアントの IP アドレスまたはホスト名
- ***Validity***: チェックサム署名の検証
- ***Version***: ログ送信元の、syslog-ng アプリケーションのバージョン番号
- ***Sender address***: 最終的に SSB にログを送信した、クライアントまたはリレーの IP アドレス
- ***Signature***: syslog-ng クライアントのシグネチャ
- ***Fingerprint***: 変更後の設定ファイルの SHA-1 ハッシュ

6.5 アーカイブ・バックアップの通知

アーカイブ・クリーンアップ・バックアップにおける通知やエラーメッセージに関しては、**Search > Archive & Cleanup** で確認できます。以下の情報を取得できます。



図表 6.12 アーカイブ及びバックアップ通知設定の画面表示

- ***Timestamp***: ***メッセージ***の日付と時刻。yyyy-mm-dd hh:mm:ss 形式
- ***Logspace***: アーカイブまたはバックアップされたログスペースの名称
- ***Directory name***:

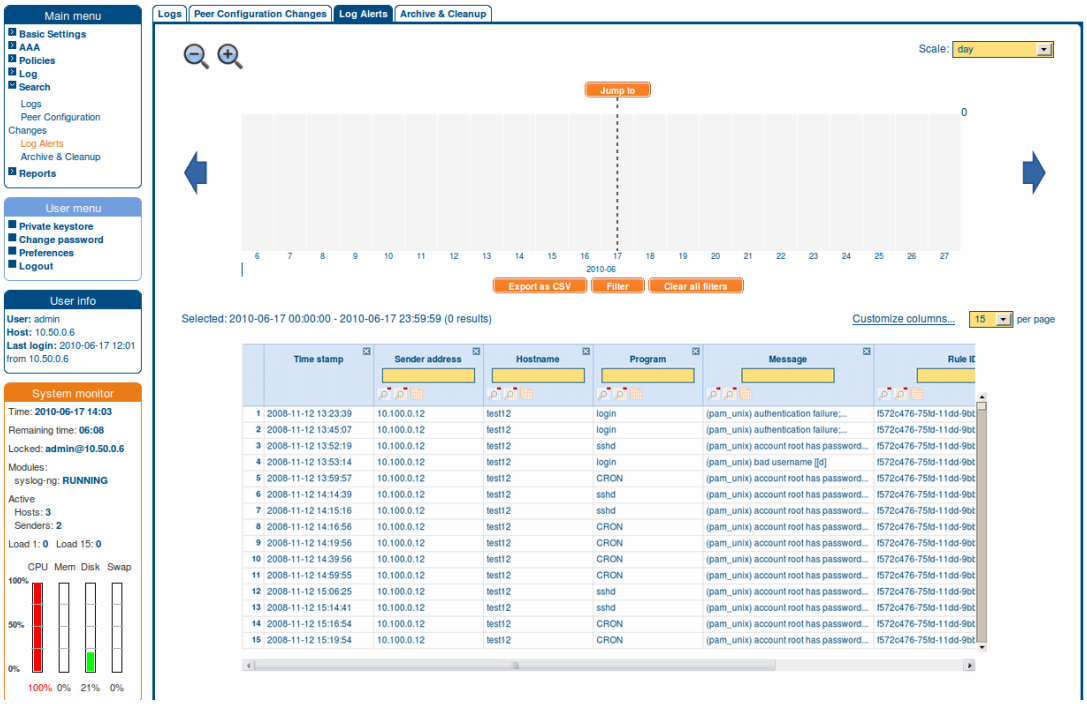
■ *Policy*: 実行されたアーカイブまたはバックアップポリシーの名称

■ *Archive Target*: 実行されたポリシーで対象となったサーバーのアドレス

■ *Manual archiving*: アーカイブまたはバックアップが手動で起動された場合に表示

6.6 ログメッセージのアラート

パターンデータベースを使用している場合、Violation とクラス分けされたログメッセージが発生すると、SSB はアラートを発信します。こうしたアラート発生の履歴は、**Search > Log Alerts** にて確認できます。以下の情報を取得できます。



図表 6.13 アラートメッセージの画面表示

■ *Timestamp*: アラート発生の日付と時刻。yyyy-mm-dd hh:mm:ss 形式

■ *Sender address*: 最終的に SSB にログを送信した、クライアントまたはリレーの IP アドレス

■ *Hostname*: アラートの原因となったログを送信した、クライアントの IP アドレスまたはホスト名

■ *Program*: 当該ログが生成されたアプリケーション

■ *Message*: ログのメッセージ部分の内容

■ *Rule ID*: メッセージに合致したパターンデータベースのルール ID。

■ *Rule description*: メッセージに合致したパターンデータベースのルールに関する説明。パターンデータベースに関して詳細は、第 7 章 パターンデータベースによるメッセージのクラス分けをご参照ください。

6.7 統計収集のオプション

Dashboard(詳細は、8.5 ステータス履歴と統計をご参照ください)に集められた統計の内容や量的な管理･制御は、統計オプションにて行います。**Log > Options > Dashboard Statistics**の順にクリックします。

■**Time-based statistics･･･**デフォルト:Enabled

■**Cleanup if unchanged for**:統計に対し、変更が加えられていない(表示･出力が全くされていない)期間が指定した日数に達した場合、削除します。0 を入力すれば、削除は一切行いません。削除をすぐに実行する場合は、Cleanup now をクリックします。

■**Enable statistics for:** デフォルトでは、全てのチェックボックスが有効です。これは、どのオプションのために統計を集めるかを選択します。ひとつのオプションのために、収取した統計を表示するためには、**Basic Settings > Dashboard > Syslog-ng statistics**,に進み、**Time-based statistics** を選択し、希望のオプションを選択してください。

注記

オプションを無効にするときは、データは最初のクリーンアップの後のみ削除されます。その時まで、既に収集されたデータはダッシュボードからアクセスできます。

■**Top/Least statistics･･･**デフォルト:**Enalbed** かつ、全てのチェックボックスが ON

統計のオプションを選択できます。取得した統計データは、**Basic Settings > Dashboard > Syslog-ng statistics** の順にクリックし、**Top/Least statistics** を選択し、表示させたいオプションを選択して表示させます。

■**Maximum number of statistics to process**:システムに貯めておく統計ファイルの数を入力します。0を入力すると、無制限に統計ファイルを保存します。この制限以上の統計はドロップし、SSB はドロップしたエントリ数と最初にドロップしたエントリを含むエラーメッセージを送信します。この設定は、10000 ホストよりも多くを持っている場合のみ増やす必要があるでしょう。

■**Smpling interval**:統計を取得する間隔を調整します。間隔を詰めれば、より詳細な統計情報になりますが、その分システムに負荷がかかります。デフォルトでは 5 分になっており、プルダウンから以下の間隔を選択できます。5 分、10 分、30 分、60 分、2 時間、4 時間、8 時間、1 日。

警告

データ喪失にご注意ください！統計取得の間隔を変更すると、それまでに取得した統計ファイルは全て削除されます。

全ての統計ファイルを削除したい場合は、**Clear all statistics** をクリックします。統計ファイル保持

の上限値を変更した際、あるいは **time-based statistics** を **Disabled** にした場合は、統計を全削除することを推奨いたします。

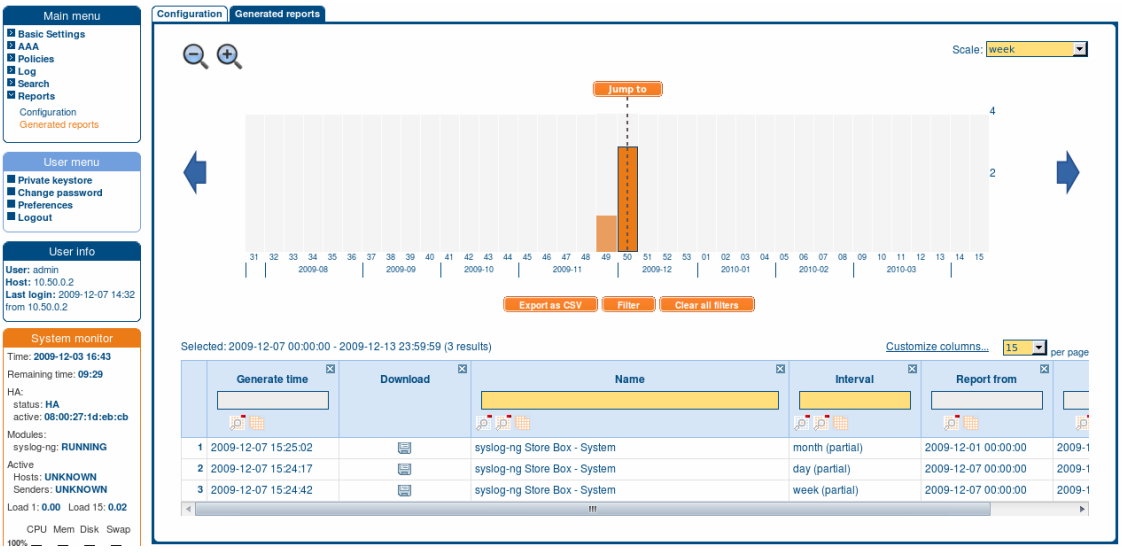
6.8 レポート

SSB は、管理者の行った作業、システムヘルスの状態、あるいは処理したトラフィックなどに関してのレポートを定期的に作成します。これらのレポートは、メインメニューで **Reports** > **Generated reports** の順にクリックして閲覧することができます。また、**Basic Settings** > **Management** > **Mail settings** > **Send reports** で設定されたアドレスに、メールでレポートを送信することも可能です。

SSB の Web インターフェイスからレポートにアクセスするには、ユーザがその権限を有していなければなりません。

注記

Basic Settings > Management > Mail settings > Send reports の設定がなされていない場合、SSB は、レポートを管理者のアドレスに送信します。



図表 6.14 レポートの閲覧

レポートは以下の時刻に生成されます。

- **Daily** レポート：毎日午前 0:01
- **Weekly** レポート：毎週月曜日の午前 0:01
- **Monthly** レポート：毎月 1 日の午前 0:01

ヒント

ある期間内のレポートに絞る場合、日付バーをを使用します。期間を明示的に選択した場合、その範囲内のデータのみが表示されます。

レポートは PDF 形式で出力され、選択された期間内で以下の情報を含みます。

- ***Configuration changes***: 画面(メニュー)ごと、ユーザごとの設定変更回数を一覧にします。設定変更の頻度も図示します。
- ***Peer configration***: クライアントごとに、syslog-ng の設定が何回変更されたかを、syslog-ng アプリケーションのバージョン番号(情報が確認できる場合のみ)と共にレポートします。
- ***Alerts***: パターンデータベースにより、クラス分けされたメッセージがトリガーとなって発信されたアラートに関するさまざまな統計を表示します。(SSB にパターンデータベースがアップロードされている場合のみ)
- ***syslog-ng traffic statistics***: 受信、転送、蓄積、そして破棄されたメッセージの割合を、件数/秒で表示します。
- ***System health information***: SSB のファイルシステム及びネットワークを使用率と、システム負荷を表示します。

レポートに関する情報は以下の通りです。

- *Download*: レポートをダウンロードするためのリンク
- *Name*: レポートの名称
- *Interval*: レポーティング期間。週、月など
- *Report from*: レポート期間の始まり
- *Report to*: レポート期間の終わり
- *Generate time*: レポートが生成された時刻

ヒント

本日分のレポートをすぐに作成したい場合は、**Reports > Configuration** の順にクリックし、レポート名タブをクリックして **Generate partial daily report** をクリックします。午前 0 時からその時刻までのレポートが生成されます。人工無能(詳細は、第 7 章パターンデータベースによるメッセージのクラス分けをご参照ください)がEnableになっている場合、人工無能レポートも同時に作成されます。

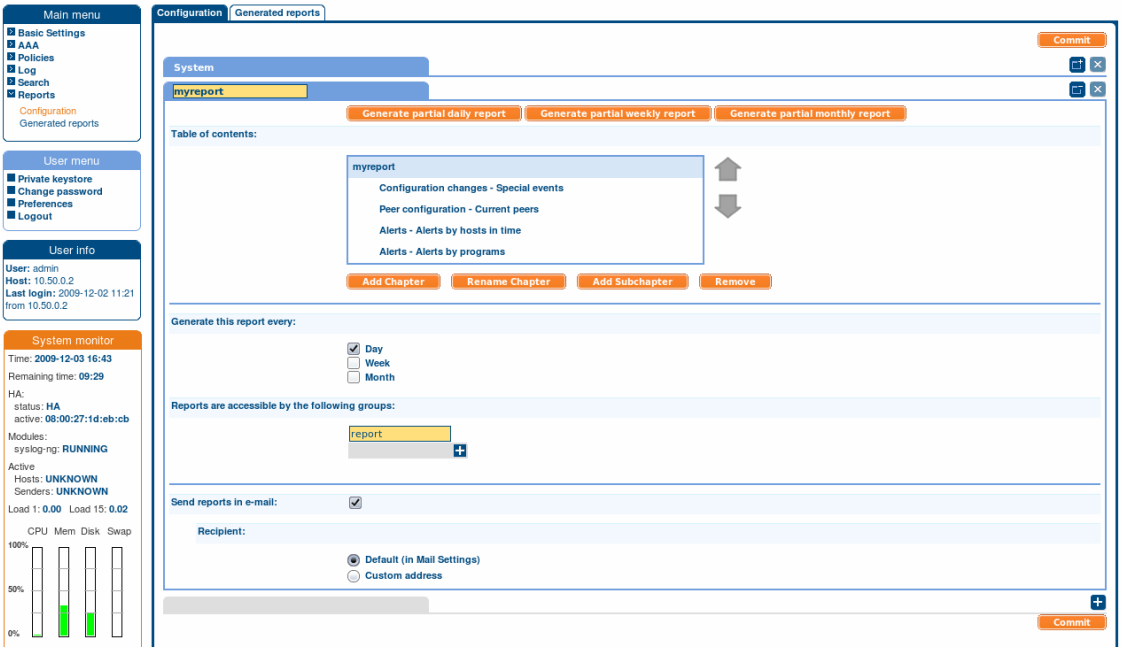
6.9 カスタムレポートの設定

目的:

カスタムレポートを作成する SSB の設定方法について説明します。

Step:

Step 1. Reports > Configuration の順にクリックします。



図表 6.15 カスタムレポートの設定

Step 2. ＋をクリックし、入力欄を展開させます。レポートの名称を決め、青地タブ内の入力欄に入力します。

Step 3. レポートは、Chapter(章)-Sub chapter(項目)の階層で形作られます。新しい章を追加するには、**Table of contents** 欄の **Add chapter** をクリックし、章の名前を決めて入力し、OK をクリックします。必要な分だけ、このステップを繰り返します。

Step 4. 項目には、**Add subchapter** をクリックした際に表示される、ポップアップウインドウに盛り込まれているさまざまな統計レポートの中から選択をします。カスタム統計によって作成されたレポートは、その一覧の最下部に表示されています。

Step 5. 項目の順序を入れ替えたい場合は、矢印アイコンを用います。

Step 6. **Generate this report every** 欄で、このレポート出力の間隔を指定します。**Week** を選択すると、毎週月曜日に、**Month** を選択すると、毎月 1 日がレポート日になります。手動で都度出力するだけにしたい場合、何も選択しないで置きます。

Step 7. デフォルトでは、search グループのみが、SSB の Web インターフェイスよりカスタムレポートを閲覧できます。他のユーザグループにも閲覧を許可するには、**Reports are**

accessible by the following groups プルダウンを➕をクリックして表示させ、許可するグループを指定します。

注記

Reporting > generated reports メニューに、許可グループとして設定されていないユーザグループは、ここで許可したカスタムレポートに対するアクセスのみが許されます。

Step 8. デフォルトでは、SSB は Basic Settings > Management .> Mail settings Send reports を順にクリックした画面に設定されているメールアドレスに、レポートを送信します。

注記

上記の設定がなされていない場合、SSB は、レポートを管理者のアドレスに送信します。

■メールによるレポート送信をしない場合は、Send reports in e-mail オプションのチェックを外します。

■Step8 の設定とは異なるアドレスにメール送信したい場合、Recipient 欄の Custom address を選択し、送信先メールアドレスを入力します。

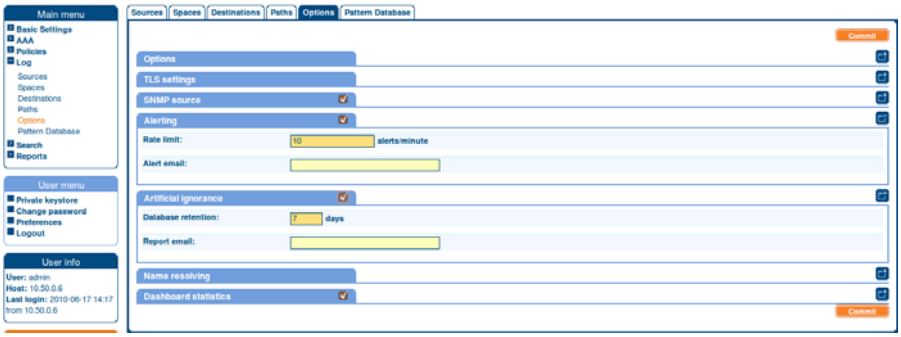
Step 9. Commit をクリックします。

7　パターンデータベースによる、ログメッセージのクラス分け

パターンデータベース(以下、「パターン DB」)を使うことで、受信したログメッセージをさまざまなクラスに分類する、アラートを受信する、また、パターンに合致しないログメッセージを、artificial ingnorance(人口無能)により収集することができます。

注記

ログメッセージのクラス分けは常時実行されます。ただし、分類した結果を統計等に用いるためには、**Log > Options** の順にクリックし、明示的な設定をする必要があります。



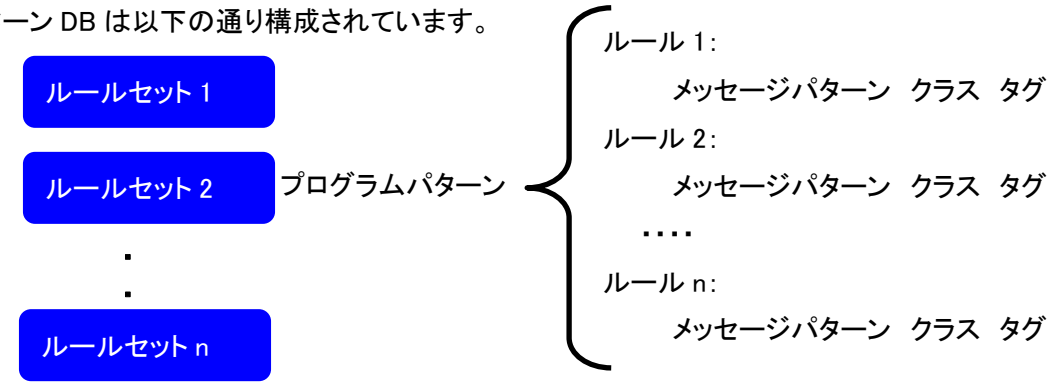
図表 7.1　人口無能とパターンマッチングを有効にする

"**Violation**"と分類されたログメッセージがある場合にアラートを受信するには、**Log > Optins** の順にクリックし、**Alerts** オプションのチェックを入れます。

■ パターンデータベースに合致しないログメッセージに関するレポートを受信したい場合は、**Log > Options** の順にクリックし、**Artificial ignorance** オプションのチェックを入れます。

7.1　パターンDBの構造

パターン DB は以下の通り構成されています。



■パターン DB は、「ルールセット」から成っています。ルールセットは、「プログラムパターン」と、「ルール」から成っています。ログを生成したアプリケーションがルールセット中の「プログラムパターン」と一致した場合、ルールセット中の各ルールは、ログメッセージを検査します。アプリケーション名(syslog-ng の$PROGRAM マクロの値)は、適用可能なプログラムパターンと比較され、それらが一致したルールセット中のルールが、そのログメッセージに対して適用されます。

■「プログラムパターン」は、アプリケーション名、あるいはアプリケーション名の先頭から一部分を表す文字列です。(例:sendmail が生成したログに合致させる場合、プログラムパターンは"sendmail"あるいは単に"send"となります)そして、プログラムパターンには、パターンパーサを含めることができます。パターンパーサは、メッセージをセグメント分けするための syslog-ng パターンパーサとは全く独立したものです。また、全てのルールには識別子が付きます。ログメッセージがルールに合致した場合、ルール内の識別子は、ログメッセージそのものと一緒に保存されます。

■ルールは、「メッセージパターン」と「クラス」から成ります。「メッセージパターン」はプログラムパターンと似ていますが、「メッセージパターン」は、ログのメッセージ部分(すなわち、syslog-ng の$MESAGE マクロの値)の比較に用いられます。「メッセージパターン」が、ログのメッセージ部分と合致したら、ルール中の「クラス」(例:Security、Violation)に分類されます。

■「ルール」には、合致したログメッセージに関する情報を付加することができます。例えば、ルールの説明、URL、パラメータ名ー値のペア、あるいは自由なフォーマットのタグです。ルールにアラート受信が設定されていれば、これらの情報は syslog-ng プレミアム(有償)版のeメールアラートに表示されます。SSBWeb インターフェイスの search インターフェイスにも表示されます。

■パターンには、キーワード、キーキャラクター等の定数、パターンパーサを含めることもできます。

注記

$PROGRAM の値が空白のログメッセージを受信した場合、「プログラムパターン」が空白のルールが適用されます。
「プログラムパターン」が、複数の「ルールセット」で用いられる場合、これらのルールセット内のルールはマージされ、それぞれのルールが、メッセージのクラス分けに用いられます。マージされたルールセット内では、メッセージパターンは一意である必要があります。しかし、現在では一つのルールセットにのみ、一意か否かの検査が行われます。

7.2 パターンマッチング

例(サンプルログ) <133> Feb 25 14:09:17 webserver syslogd : restart .

↓ ↓

プログラムパターン メッセージパターン

ここでは、パターンがどう機能するかを説明します。「プログラムパターン」と「メッセージパターン」いずれにも当てはまる説明ですが、メッセージパターンは、プロシージャを表しています。

パターンには、キーワード、キーキャラクターといった定数と、パターンパーサを含めることができます。パターンパーサは、文字列の順序を、そのルールにのっとって解析します。

注記

パターンでワイルドカードや正規表現は使えません。また、"@"を文字そのものとして解析したい場合は、エスケープ文字を前におく必要があります。具体的には"@@"と表記します。syslog-ng のパターンパーサは、"@"で囲まれているからです。

新たなログメッセージが到着すると、syslog-ng はパターン DB を適用してメッセージのクラス分けを開始します。適用できるパターンは、アルファベット順にツリー構造になっており、syslog-ng は、ログメッセージの文字列を先頭から、一文字ずつ検査していきます。これはすなわち、各ステップにおいてはルールの一部分のみが適用されていることを意味し、結果、処理速度の向上に貢献しています。ルールの総数が増えても、クラス分けの速度は実質、低下しません。

例えば、"Apple"という文字列から始まるログメッセージを受信したとします。まずは、先頭の"A"が、パターンに合致するかどうか検査されます。次のステップで、"Ap"というパターンを syslog-ng が選択し、検査します。この様にして 2 文字目、3 文字目･･･と進んでいきます。これは、パターンを検査しきって残りがなくなるまで繰り返されます。

文字による照合が、パターンパーサよりも優先されることにご注意ください。あるステップにおいて、文字ごとのマッチングで次の文字に合致したとし、また同時にパターンパーサでも合致したとすると、文字ごとの照合で合致した方が選択されます。上記例で言えば、文字ごとの照合条件は、"Apport"であり、パターンパーサには"Ap@STRING@"と定義されていた場合、文字ごとの照合の"Apport"が優先されます。次に来る文字と、文字列検索の条件が合致しない(例:検索対象の文字が"Apple"→"Apport"に 4 文字目が合致しない)場合に初めて、syslog-ng はパーサの解析パターンと合致するかどうかを検査します。ただし、同一階層に複数のパターンパーサが定義されている場合、たとえメッセージ(内の文字列)と完全に合致しなくとも、最初のパターンのみが適用されます。

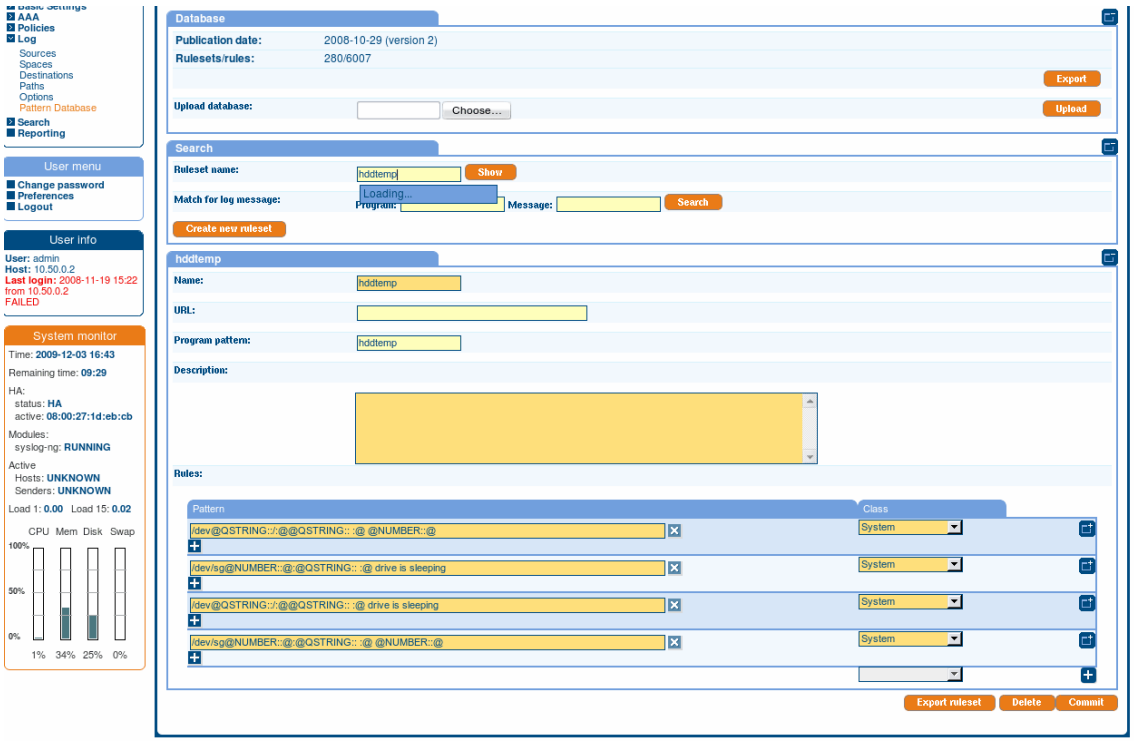
同一階層に複数のパターン解析エンジンが定義されている場合、(例:"Ap@STRING"と"Ap@QSTRING")どのパターンが用いられるかは、ランダムです。ただし、最初に適用されたパターンで一文字たりとも合致しなかった場合のみ、他のパターンが用いられます。とはいえ、同一階層に複数のパターンパーサエンジンを定義することはまれであり、したがってこの制限は、さほど実運用に大きな影響を及ぼすものではありません。

7.3 ルールセットの検索

ルールセット内のルールを表示させるには、**Log > Pattern Database > Seach** の順にクリックし、**Ruleset name** 欄にルール名を入力します。そして、**Show** をクリックします。ルールセット名を完全に覚えていないときは、始まりの文字を入力して **Show** をクリックすれば、それに合致する全てのルールセット名が表示されます。特定の条件に合うルールを検索するには、**Program** または **Message** 欄に条件を入力し、**Search** をクリックします。入力した条件に合致するルールをもつルールセットが表示されます。

注記

莫大な数のルールを定義してあるルールセットは、正しく表示されない場合もあります。



図表 7.2 ルールの検索

7.4 新たなルールセット・ルールを作成する

目的:

新たなルールセット及びルールの作成方法を説明します。

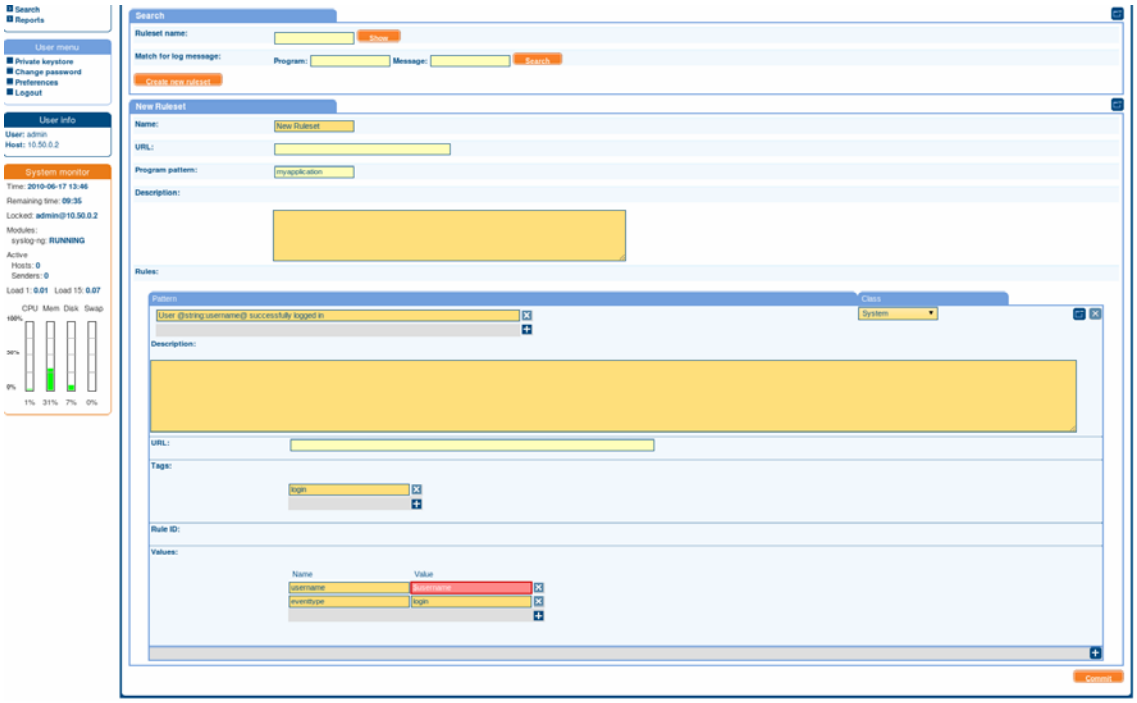
Step:

Step 1. Log > Pattern Databse の順にクリックし、Search 欄の Create new ruleset をクリックします。

ヒント

存在しないルールセット名(の一部)で検索をかけた場合、SSB は、その名前を持つ新たなルールセットを作成するように促します。

Step 2. **Name** 欄に、ルールセット名を入力します。



図表 7.3 パターン DB のルールセットを作成する

Step 3. **Program pattern**欄に、対象となるログのアプリケーションに合致するアプリケーション名、あるいはパターン名を入力します。詳細は、7.7パターンパーサの使用をご参照ください。

Step 4. オプションとして、ルールセットの説明を、**Description** 欄に記入することができます。

Step 5. クラスに、ルールを追加します。

Step a. **Rules** 欄の+をクリックします。

Step b. **Pattern**タブ内の入力欄に、対象となるログのメッセージに合致する、メッセージの最初の数文字、あるいはパターンを入力します。詳細は、7.7パターンパーサ

の使用をご参照ください。なお、Step3 のProgram Pattern欄に入力したアプリケーション名に合致するアプリケーションが送出したログメッセージにのみ、この設定が適用されることにご留意ください。

Step c. メッセージの分類を、**Class** プルダウンから選択します。このルールのパターンに合致するログメッセージが、ここで選択したクラスに分類されます。**Violation**、**Security**、そして **System** の 3 種類から選択できます。

Log > **Options** > **Alerting** 画面で、アラート受信を有効に設定しておくと、"**Violation**"に該当するログメッセージが到着した場合に、SSB は自動でアラートを送信します。

Step d. オプションとして、説明、カスタムタグ、パラメータ名－値のペア、をルールに設定することができます。パラメータ名－値のペアには、マクロを含めることもできます。パターン DB 及びマクロに関しての詳細は、*The syslog-ng Premium Edition Guide* をご参照ください。

Step 6. さらにルールを追加する場合、上記ステップを繰り返します。

Step 7. **Commit** をクリックします。

7.5 パターンDB及びルールセットのエクスポート

パターン DB 全体をエクスポートするには、**Log** > **Pattern Database** .> **Export** の順にクリックします。

ルールセットをエクスポートするには、同じ画面の、**Search** > **Ruleset name** 欄に、エクスポートしたいルールセット名を入力します。**Show** をクリックしてルールセットの設定値が表示されたら、**Export ruleset** をクリックします。もし、ルールセット名が不明の場合は、**Program** あるいは **Message** 欄から検索語を入力し、**Search** をクリックします。条件に合致するルールセットが表示されます。

7.6 パターンDBのインポート

Blabit 社からの公式パターン DB、または SSB かエクスポートしたそれを、SSB にアップロードすることができます。公式パターン DB は、Balabit 社のサイトから入手できます。公式パターン DB は、さまざまな Linux/Unix アプリケーションのパターンを含んでおり、またさらに重要なのは、"logcheck"アプリケーションからコンバージョンされた DB にも対応していることです。Cisco 社製品向け、Windows アプリケーション向けのパターン DB は、現在開発中です。

注記

インポートされたルールは、アップロードが終了するとすぐに適用されます。
公式パターン DB の一部分をご自身で編集すると、次回の公式な更新においてはその部分に対する変更が及びません。

7.7 パターンパーサの使用

パターンパーサは、パーサの種類に特有のルールに基づいて、メッセージの解析を試みます。解析パターンは"@"で囲まれます。パターン解析は、以下の文法にのっとって記述します。

- 最初の"@"
- パーサの種類(大文字表記)
- 名前(オプション)
- 解析エンジンのパラメータ(任意)
- おしまいの"@"

例 7.1 : パターンパーサの文法
シンプルなパーサ
@STRING@
名前付きパーサ
@STRING:myparser_name@
パラメータありの名前付きパーサ
@STING:myparser_name : *@
パラメータ付き、しかし名前のないパーサ
@STRING : :* @

以下のパーサが使用できます。

■ ***@ANYSTRING@***: ログメッセージの最後まで、どんな文字列であろうが解析します。つまり、特別のマクロにとらわれず、全てのメッセージを収集したい場合に用います。この点では、CSV パーサの greedy()オプションに似ています。

■ ***@DOUBLE@***: @FLOAT@パーサの、古いエイリアス

■ ***@ESTRING@***: このパーサは、ストップ文字として機能するパラメータが必要です。このパーサは、ストップ文字が現れるまで解析を続けます。例えば、次に現れるダブルクォーテーション「″」まで解析をさせたいなら、@ESTRING: :″@ と記述します。syslog-ng の Ver3.1 では、一文字の代わりとなる、ストップ文字(列)を定義することも
可能です。例 : @ESTRING: : stop_here.@。

■ ***@FLOAT@***: ドット(.)を含む、浮動小数。syslog-ng Ver3.1 までは、このパーサ名は、@DOUBLE@でした。

■ ***@IPv4@***: IPv4 アドレスを解析(最大 3 つの.″″(ドット)で区切られた数値)

■ ***@IPv6@***: 有効な全ての IPv6 アドレスを解析

■ ***@IPvANY@***: あらゆる IP アドレスを解析

■ ***@NUMBER@***: 10 進数表記の数値。ただし、「0x」で始まり、少なくとも一桁以上の、有効な 16 進数値が 0x の直後に続く場合のみ、16 進表記として解析される。

■ ***@QSTRING@***: パラメータに指定された引用符間の文字を解析。なお、引用符は、はじめと終わりで異なる文字を指定できることにご留意ください。たとえば、@QSTRIG: :″@ は、クォーテーション「″」で囲まれる全ての文字を解析し、@QSTRING:<>@ の場合、開き括弧<と閉じ括弧>の間に挟まれた文字列を解析します。

■ ***@STRING@***: アルファベットまたは数字の文字列を解析。空白は対象外です。オプションとして、数字・アルファベット以外に解析対象とする文字をパラメータとして指定できます。(例 : 文全体を解析対象とするために、スペースを対象に加える @STRING: : @)″@″は、パラメータ、改行文字、タブとしては使えません。

パターン及び文字列は、混合させて指定することができます。例えば、文字列 Host ：で始まるログメッセージで、その後 IP アドレスが続くような場合、(Host ： 192.168.10.140)、以下のパターンでマッチします。 Host ： @IPv4@

注記
パーサの使用は、CPU への負荷を高めます。可能な限り、ESTRING または QSTRING パーサをお使いください。他のパーサに比べ、大幅に速い処理が期待できます。

例 7.2：STRING 及び ESTRING エンジンの使用
例として、受信するログメッセージが user = joe96 group = somegroup の場合、
@STRING:mytext:@パーサは、アルファベット･数字**以外の**最初の文字のみを解析対象とし、結果「user」のみが解析･抽出されます。
@STRING:mytext:=@ パーサは、"="も、他の文字同様解析対象とし、次のアルファベット・数字以外の値(この場合空白)に進みます。結果、「user = joe96」が解析・抽出されます。
@STRING:mytext:= @ パーサにすると、空白も解析対象とするので、結果 user = joe group = somegroup が解析・抽出されます。
もちろん、異なる値は各々解析する方が好ましい設定といえます。例えば、
"user = @STRING:user@ group = @STRING:group@"
username または group に、空白のようなアルファベット・数字以外の値が含まれる場合は、2 番目のパラメータに空白を明示的に入れるか、**ESTRING** パーサを使います。**ESTRING** パーサは、次の空白が現れるまでメッセージを解析します。例：
"user = @ESTRING:user: @group = @ESTRING:group: @"

7.8 フィルターとテンプレートで、パーサによる解析結果を利用する

目的:

メッセージのクラス分けや解析の結果は、カスタムフィルターやファイル、データベーステンプレートに用いることが可能です。クラス分け結果を用いることができる、次の 2 つのマクロが SSB に組込まれています。.classifier.class は、メッセージが分類されたクラス(Vialation、Security、あるいは Unknown)を含み、.classifier.rule_id マクロは、ログメッセージにマッチしたメッセージパターンの識別子が含まれます。

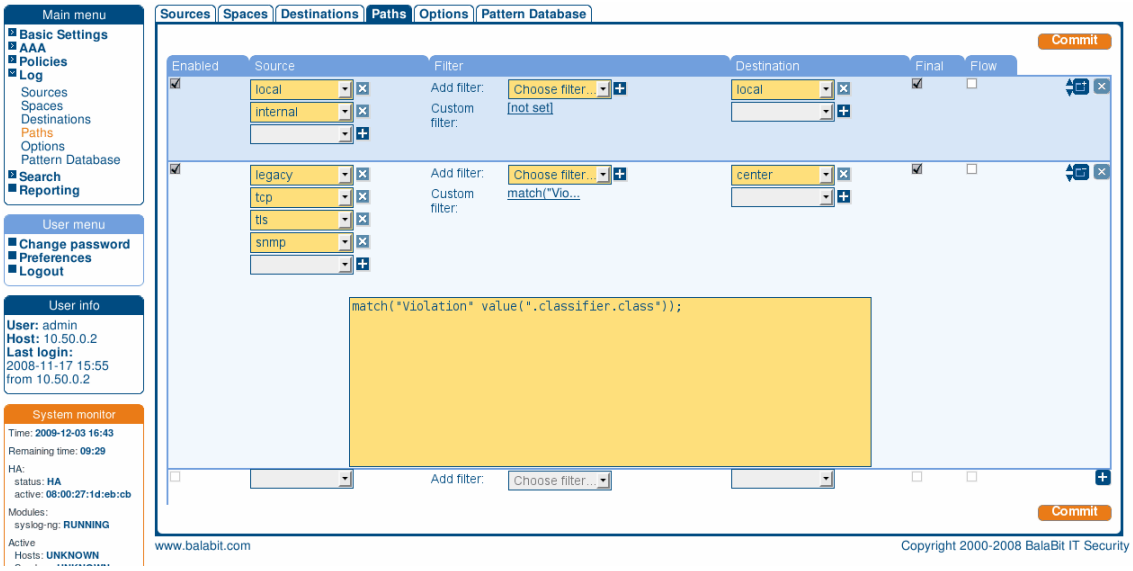
注記
ログメッセージが SQL データベースに転送される場合、メッセージの ID が自動的にテンプレートに挿入されます。

ログパスにおいて、これらのマクロをフィルターのように使用する方法を説明します。

Step:

Step 1. **Log** > **Paths** の順にクリックし、目的のログパスを選択します。

Step 2.



図表 7.4 クラス分類によるメッセージのフィルタリング

特定のメッセージクラスにフィルタリングするには、**Add filter** > **classifer_class** の順にクリックし、**+**をクリックしてプルダウンを展開させます。そして、合致するクラス(例:Vilolation)を選択します。

Step 3. 特定のクラス分けルールに合致するメッセージをフィルタリングするには、**Add filter** > **classifer_rule_id** の順にクリックし、**+**をクリックしてプルダウンを展開させます。そして、ルールを一意に識別する識別子(例:e1e9c0d8-13bb-11de-8293-000c2922ed0a)を、**classifier_rule_id** 欄に入力します。

注記

タグのような、別のクラス分け規則に基づいたメッセージをフィルタリングするには、カスタムフィルターを使用する必要があります。詳細は、5.4.3メッセージのフィルタリングをご参照ください。

Step 4. **Commit** をクリックします。

同様に、パターンパーサによる解析結果を用いることができます。そのためには、エンジンに名称をつける必要があります。その後、その名称をマクロとして、解析されたメッセージの値を参照するために使用することができます。

< 例 >

アプリケーションが生成した次のようなログを解析するとします。"Transaction : <type>. "ここで、<type>は、"refused"、"accepted"、"incomplete"等の、異なる値を持つ文字列です。こういったメッセージを解析するには、以下のようなパターンを定義してください。

'Transaction: @ESTRING::.@'

@ESTRING@エンジンは、次のフルストップ文字が現れるまで、メッセージを解析します。解析結果をフィルターや、ファイル名テンプレートで利用する場合は、パーサの名称をパターンに含めます。以下のようになります。

'Transaction:

@ESTRING@:TRANSACTIONTYPE:.@'

その後、このテンプレートを用いるログパスに、カスタムテンプレートを追加します。例えば、"accepted"トランザクションを全て拾うようにするには、以下のようなカスタムフィルターを定義します。

much("accepted" value("TRANSACTIONTYPE"));

注記

ログ転送先またはログスペースにカスタムテンプレートを作成すれば、上記のマクロを、データベースの列やファイル名テンプレートに用いることができます。

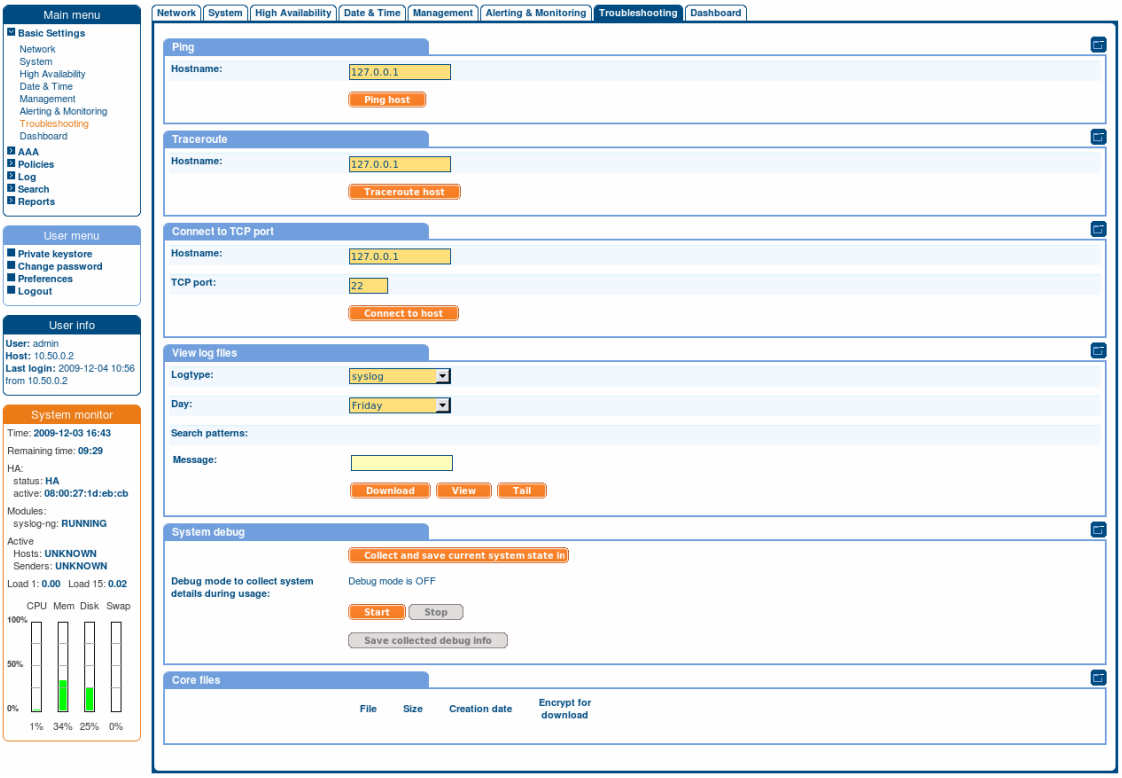
8 SSBのトラブルシューティング

ここでは、ネットワークの問題を検知するツールと、**コアファイル**の収集方　及び SSB のシステムログを確認する方法について説明していきます。

8.1 ネットワークのトラブルシューティング

目的:

Troubleshootingメニューは、ネットワークに関連する問題の原因を探るためのさまざまな診断コマンドを提供します。SSBのログファイルも、この画面内に表示されます。詳細は、1.1 SSBとはをご参照ください。



図表 8.1　SSB におけるネットワークトラブルシューティング

以下のコマンドを発行できます。

- ***ping***: 指定したホストに向けて、ネットワークの疎通が取れているかどうかの確認(ICPM)を送信します。
- ***traceroute***: SSB から指定したホストに向けて、メッセージが到達するまでの全経路を表示させます。ホスト間のメッセージがどのような経路で転送されているかを確認するために用います。
- ***connect***: 指定したホストに、特定のポート番号経由で接続を試みます。ターゲットホスト上のアプリケーションのサービスを利用できるかどうか確認するために用います。

上記コマンドを発行するための手順を説明します。

Step:

Step 1. **Basic Settings** > **Troubleshooting** の順にクリックします。

Step 2. **Hostname** 欄に、ターゲットとなるホストの IP アドレスを入力します。**Connect** コマンドの場合は、Port 欄に、ターゲットポート番号も入力します。

Step 3. 診断をしたい項目のボタンをクリックします。

Step 4. ポップアップウインドウに表示される結果をご確認ください。ログファイル確認の場合は、別のブラウザ画面が立ち上がって表示されます。

8.2 システムの問題を解決するためのデータを収集する

何らかの理由でシステムクラッシュが発生した場合、SSBは、例えばsyslog-ngやindexerなどの重要なソフトウェアコンポーネントに関するコアファイルを自動的に生成します。これらのファイルは、問題解決に際し重要な手がかりを与えてくれるものです。コアファイルが生成されると、SSBは、管理者に向けてアラートメールを送信し、またそのアラートが正しく送信されているかを確認するために、SNMPトラップを発生させます。(詳細は、4.3.4 SSBのシステム監視設定と、4.3.3 SNMPとEメールアラートをご参照ください)システム監視が設定されていない場合は、**Search** > **Log Alerts**の順にクリックし、アラートの履歴を確認してください。

生成されたコアファイルをダウンロードして一覧にするには、**Basic Settings** > **Troubleshooting** > **Management** > **Cire files** の順にクリックしてください。

デフォルトでは、コアファイルは 14 日で消去されます。この期間を変更するには、**Basic Settings** > **Management** > **Core files** の順にクリックして、変更してください。

警告

現在のバージョンでは、SSB のコアファイルは
再起動後自動的に消去されます。

8.3 SSBのログを確認する

目的:

Troubleshootingメニューは、SSBのさまざまなコンポーネントが生成したログを確認するインターフェイスを提供します。SSBに接続されているホストから送信されたログメッセージの確認方は、第 6 章、ログメッセージとレポートを閲覧するをご参照ください。

注記

パフォーマンス維持の観点から、2MB を超えるログファイルは、Web インターフェイスには表示されません。ダウンロードしてください。

Step:

Step 1. **Basic Settings** > **Troubleshooting** の順にクリックし、**View log files** タブをクリックします。

Step 2. Logtype プルダウンから、ログメッセージの種類を選択します。

- ***SSB***: SSBWeb インターフェイスのログ
- ***syslog***: SSB ホストに蓄積されている全てのシステムログ
- ***syslog-ng***: 組込まれている syslog-ng サーバーの内部メッセージ。この中には、SSB に向けて転送されてきた syslog は含まれていません。

Step 3.

- ログファイルをダウンロードするには、**Download** をクリックします。
- リアルタイムで現在のログを監視するには、**Tail** をクリックします。
- ログメッセージを表示させるには、**View** をクリックします。

Step 4. 本日より以前(7 日前まで可)のログメッセージを表示させるには、Day プルダウンで曜日を選択し、**View** をクリックします。

注記

特定のホストあるいはプロセスのログメッセージのみを表示させたい場合、Message 欄に、ホスト名またはプロセス名を入力します。

Message 欄は、全体的なフィルターとして機能します。キーワードまたは正規表現を入力することで、それらにマッチしたログメッセージのみを抽出することが可能です。

8.4 エラーレポートのための、ログ及びシステム情報を収集する

目的:

サポートを行うに当たり、問題の原因などを追求する目的で、システムのステータス及びでバッギングに関する情報の提供をお願いすることがあります。これらの情報は SSB 上で自動的に収集され、ログファイル、設定ファイル、そしていろいろなシステム統計情報も、この中に含まれます。

注記

鍵のファイルやパスワード等、重要な情報は自動的にこれらのファイル群から除外されます。

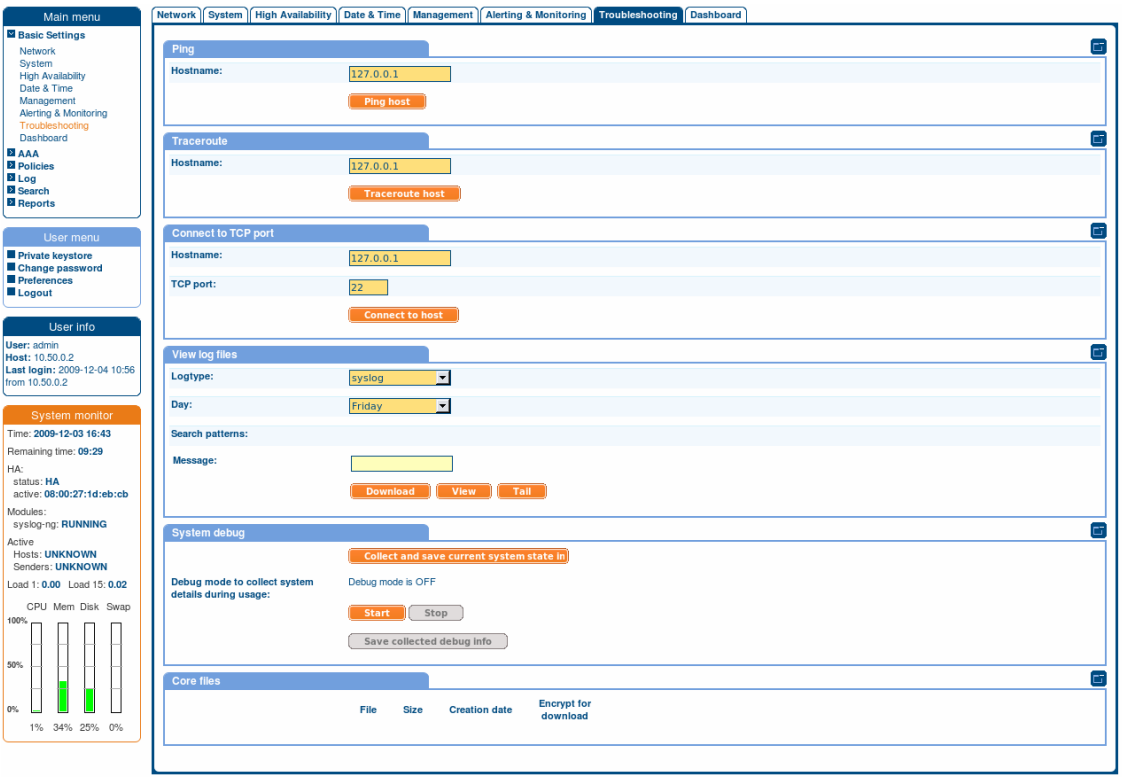
Basic Settings > Management > Debug logging > Enable debug logs オプションは、ログメッセージの冗長性には影響を与えません。SSBWeb インターフェイス上で発行されたコマンド履歴を、ログに追加するオプションです。

システムステータスの情報を収集するには、**Basic** Settings > **Troubleshooting > System debug** の順にクリックし、**Collect and save current system state info** をクリックします。zip ファイルが生成されるので、保存します。ファイル名は、debug_info-{ホスト名}YYYYMMDDHHMM の形式になります。

特定のエラーに関する情報を収集する方法を説明します。

Step:

Step 1. **Basic Settings > Troubleshooting > System debug** の順にクリックします。



図表 8.2 デバッグ情報の収集

Step 2. **Start** をクリックします。

注記
デバッグモードに入ると、SSB のログレベルが上昇します。システムに負荷がかかっている最中ですと、パフォーマンスが低下する恐れがあります。

Step 3. エラーの原因となったイベントを再発生させます。(例:ある特定のホストからのログ受信)

Step 4. **Stop** をクリックします。

Step 5. **Save the collected debug info** をクリックし、生成された zip ファイルを保存します。ファイル名は、
debug_info-{ホスト名}YYYYMMDDHHMM の形式です。

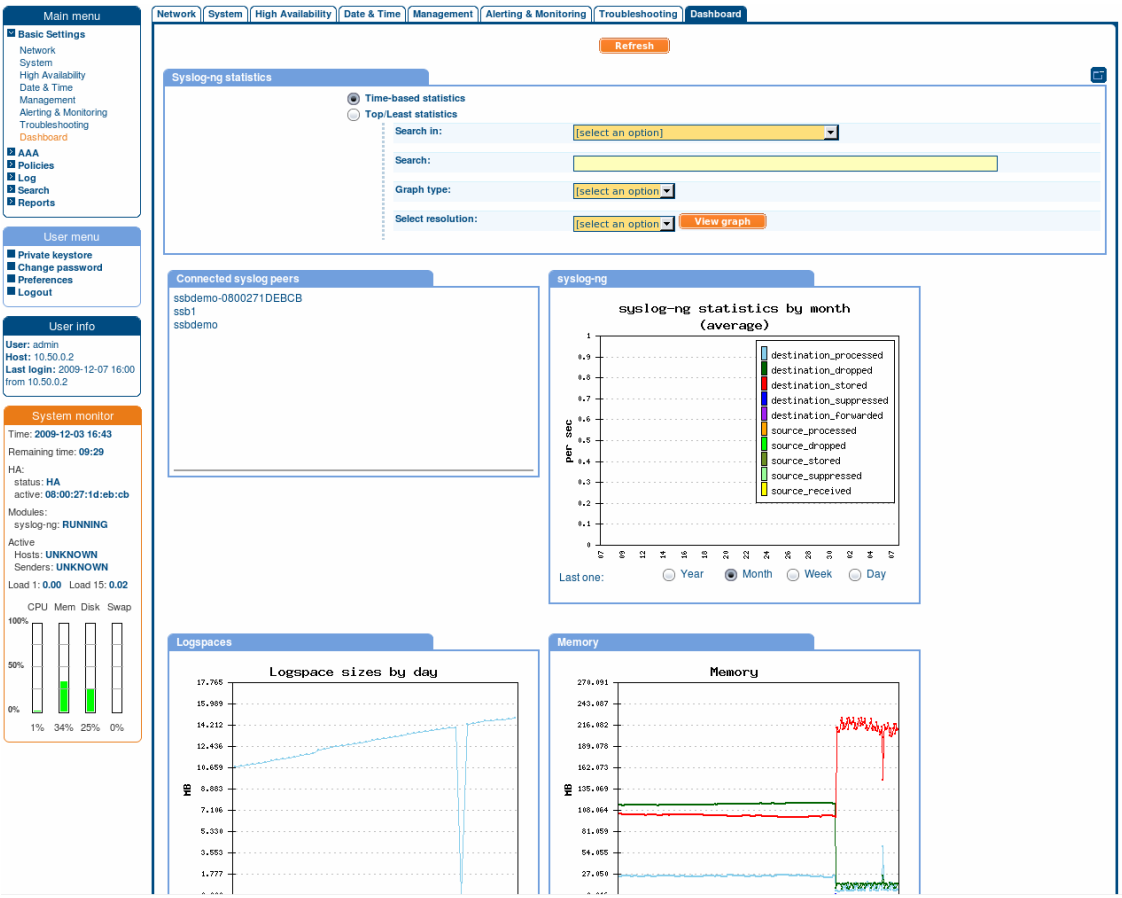
Step 6. サポート担当者にファイルを送付します。

8.5 ステータス履歴と統計

SSB は、さまざまな統計情報やシステムデータ・パフォーマンスの履歴を、**Basic Settings > Dashboard** で表示される、ダッシュボード画面で提供します。ダッシュボードは、基本的にはシステム監視機能の拡張機能です。システム監視機能は、現在の状況を未表示にしますが、ダッシュボードは、システムパラメータのグラフや統計情報をもたらします。

ダッシュボードは異なったモジュールから構成されています。全てのモジュールにおいて、当日のシステムパラメータ履歴が表示されます。先週、先月、昨年、などもっと長い期間のグラフを表示させたい場合は、**Week**、**Month**、**Year** などを選択します。グラフの上にマウスポインタをかざすと、グラフは拡大され、グラフに用いられている色の説明が表れます。

グラフ表示になっているそれぞれの統計を表形式で表示させるには、グラフの上をクリックします。クリックするたびにグラフと表形式で交互に表示されます。



図表 8.3 ダッシュボード

以下のモジュールが、SSB のダッシュボードに表示されます。

- ***syslog-ng***: 受信・処理済・ドロップされたsyslog-ngの統計を表示します。
  8.5.1syslog-ng統計情報のカスタム表示も合わせてご参照ください。
- ***Connected syslog peers***: SSB に、現在ログを送信しているホストの一覧
- ***syslog-ng statistics***: 受信しているログメッセージ件数を、メッセージ件数/秒で表示します。
  ※※この表示情報は、10 分おきに最新に更新されます。
- ***Logspaces***: ログスペースの容量。
  ※この表示情報は、10 分おきに最新に更新されます。
- ***Memory***: システムが使用しているメモリ領域
- ***Disk***: 異なるパーティションにおけるファイルシステムの仕様領域
- ***CPU***: CPU 使用率
- ***Network connections***: ネットワーク接続数
- ***External interface***: 外部インターフェイスのトラフィック

■ *Management interface*: 管理インターフェイスのトラフィック

■ *Load average*: システム負荷の平均値

■ *Processes*: 稼働中のプロセス数

統計情報収集のオプション設定に関しては、6.7統計収集のオプションをご参照ください。

8.5.1 syslog-ng統計情報のカスタム表示

目的:

特定のソース、デスティネーション、またはホストにのみ関連する統計情報を取得する手順を説明します。

Step:

Step 1. **Basic Settings** > **Dashboard** > **syslog-ng statistics** の順にクリックします。

Step 2.

■ デスティネーションファイルの統計を取得するには、**Search in** プルダウンで、**destination** を選択します。そして、デスティネーションの名前を、**Search** 欄に入力します。デスティネーション名は、必ず ds で始まります。

■ 特定のホストに関する統計情報であれば、**Search in** プルダウンで **source** を選択します。次に、**Search** 欄に、IP アドレスあるいはホスト名を入力します。

Step 3. **Select resolution** プルダウンで、表示させたい期間を選択します。

Step 4. **View graph** をクリックします。

8.6 SSBクラスターのトラブルシューティング

ここでは、ハイアベイラビリティモードに関連する問題の解決に役立つと思われる事項を説明していきます。

■ クラスター自体がダウンした場合の回復手順は、8.6.1両方のノードがダウンした際のSSBのリカバリー

■ 両ノードが同時にactiveとなり、Split-brain状況になってしまった場合の解決方法は、8.6.2スプリットブレイン状況からのリカバリーを、それぞれご参照ください。

8.6.1 両方のノードがダウンした際のSSBのリカバリー

目的:

両方のノードが同時にダウンしてしまうことも、ありえないとは言えません。(電源喪失時、など)あるいは、スレーブノードがマスターノードよりも先にダウンしてしまうかもしれません。SSB を正しくリカバリーさせる手順を説明します。

注記

バージョン 1.1.1 までは、クラスターの両ノードが同時に起動した場合、1.2.4.1 のハイアベイラビリティ IP アドレスを得た方がマスターノードとして機能しました。

Steps:

Step 1. power ボタンを長押しして離し、SSB をインストールしたマシンの電源を落とします。

警告

データ喪失にご注意ください！SSB のシャットダウンがされない場合は、power ボタンを 4 秒ほど押し続けてください。この手順を実行すると、それまでのアクティブなネットワーク接続は全て切断され、データを喪失する恐れがあります。

Step 2. SSB がダウンした以前の状態でマスターノードだった方のマシンを先に、電源を入れます。どちらのノードがマスターだったかは、システムログをみればわかります。

注記

SSBに蓄積されているログにアクセスできない場合でも、SSB自身のログメッセージをリモートサーバーに転送するように設定することは可能です。リモートログ転送に関して詳細は、4.3.3 SNMPとEメールアラートをご参照ください。

Step 3. マスターノードのブートが終了するまで待ちます。

Step 4. もう一つのノードの電源を入れます。

8.6.2 スプリットブレイン状況からのリカバリー

目的:

スプリットブレイン状況は、クラスター間のネットワークリンクが切断されてしまい、両方ともマスターノードとして稼動しようとしてしまうことから発生します。転送されてきたログメッセージなどの新たなデータの、もう片方へのデータ複製がされません。したがって双方がそれぞれデータを蓄積していってしまい、あとでマージすることは容易ではなくなります。

警告

データ喪失にご注意ください！スプリットブレイン状況下では、重要なデータが、双方のノードから見ることができてしまいます。データを喪失しないよう、特に慎重な対処が必要です。

SSB のクラスターを構成しているノードは、再接続がされた際に自動的にスプリットブレイン状況を検知します。また、データ喪失を防ぐため、データ同期は行われません。スプリットブレイン状況が検知された際は、SSB のシステムモニター画面ならびにシステムログ上(Split-Brain detected, dropping connection!)で確認できます。そしてアラートを送信します。

スプリットブレイン状況からのリカバリー方法を説明していきます。

警告
ノードは決してシャットダウンしないでください。

Step:

Step 1. **Basic Settings > System > Traffic control** の順にクリックし、**Disable** をクリックし、ログ転送等、現在アクティブなトラフィックを一時的にとめます。

■Web インターフェイスからの操作が不能、あるいは不安定な場合は、以下の手順に従ってください。

Step a. ローカルコンソール、あるいは SSH で、SSB に root でログインします。

Step b. **Shells > Core Shell** の順に押下し、"service syslog-ng stop" コマンドを投入して syslog-ng を停止します。。

Step c. "date"コマンドを投入し、システム日付と時刻が正しいかを確認します。もし不正確な場合は、システムのバッテリーを交換してください。詳細は、アプライアンスのマニュアルをご参照ください。

Step d. 他のノードに関し、上記ステップを繰り返します。

Step 2. ***データ修復のためのオプション手順***: SSB のノードに蓄積されたログスペースを確認します。

Step a. ローカルコンソールから SSB のノードにログインします。

Step b. **Shells > Core Shell** の順に押下します。"cd /opt/ssb/var/logspace" コマンドを投入します。ログスペースは、このディレクトリ下に配置されています。

Step a. スプリットブレイン状況が検知されてから、どのログファイルに変更が加えられたか、以下のコマンドで探します。

■ # find . -mtime -n : 過去 n 時間の間に、変更が加えられたログファイルが表示されます。

■ # find . -mmin -n : 過去 n 分の間に、変更が加えられたログファイルが表示されます。

Step 3. どのノードが、この後のマスターになるべきかを決定し、**これからスレーブになる**べきノードで以下のオペレーションを実施します。

Step a. ローカルコンソールから root でログインします。

Step b. ***データ修復のためのオプション手順:***スプリットブレイン状況が発生して以降、修正が加えられたログメッセージをバックアップします。

警告

上記ログファイルは、スプリットブレイン状況が解消された際には自動的に削除されます。オフラインで使用している場合を除いては、SSB のデータベースにこのデータを戻す方法はありません。

Step c. ***データ修復のためのオプション手順:***Exit とタイプして、コンソールメニューに戻ります。

Step d. **Shells > Boot shell** の順にクリックします。もし、ログインしている、スレイブになる「べき」ノードがまだスレイブになっていない場合は、下記コマンドを投入して強制的にフェイルオーバーを行います。

```
# /sbin/lib/heartbeat/hb_standby
```

Step e. コアファームウェアを、以下のコマンドで停止します。

```
# /etc/init.d/boot-xcb stop
```

Step f. DRBD を、以下のコマンドで無効にします。

```
# /sbin/drbdsetup /dev/drbd0 disconnect
# /sbin/drbdsetup /dev/drbd0 invalidate
```

Step 4. スレイブになるべきノードを再起動します。

Step 5. マスターになるべきノードを再起動します。これにより、SSB のクラスターは以前の通り機能し始めます。

Step 6. 双方のノードが立ち上がると、SSBクラスターは"Degraded Sync"ステータスになります。これは、マスターノードが"Sync Source"、スレーブノードが"Sync Target"になっている状態です。マスターノードは、スレーブノードとのデータ同期を始めます。データの量によりますが、これには長時間かかります。同期の速度を調節するには、4.5.2.2DRBDの同期速度の調整をご参照ください。

8.6.3 HAノードのリプレイス

目的:

SSB クラスターのユニットを交換する場合は、以下の手順に従って下さい。

Step:

Step 1. **Basic Settings > High Availability** をクリックし、ワーキングノードの HA ステータスを確認してください。もし、ノードの内のいくつかがダウンあるいは、消失していた場合、Status フィールドは、*DEGRADED.* を表示します。

Step 2. フルシステムバックアップを実行してください。ノードをリプレイスする前に、ワーキングノードの完全なシステムバックアップを作成してください。詳細については、セクション 4.3.5 データと設定のアーカイブとバックアップ をご参照ください。

Step 3. ワーキングノードでどのファームウェアバージョンが使用されているか確認してください。Basic Settings > System > Version details を選択し、正確なバージョン番号をメモしてください。

Step 4. MyBalaBitアカウントに以下よりログインし https://www.balabit.com/mybalabit/ワーキングノードとおなじ同じSSBバージョンのISOファイルをダウンロードしてください。

Step 5. リプレイスするユニットをネットワークへつなげないで、ISO ファイルからリプレイスメントするユニットに ISO ファイルからインストールしてください。必要であれば、IPMI インターフェイスを使用してください。

Step 6. インストレーションが完了したら、*HA とレーベルされたイーサネットコネクタにてイーサネットケーブルで二つの SSB ユニットをつなげてください。*

Step 7. リプレイスするユニットをリブートし、起動完了するまで待ちます。

Step 8. ワーキングノードにログインし、HA ステートを確認します。Basic Settings > High Availability を選択します。Status フィールドは *HALF* を表示しているはずです。

Step 9. **Other node > Join HA**.をクリックします。

Step 10. **Other node > Reboot** をクリックします。

Step 11. リプレイスするユニットはリブートし、ワーキングノードからデータを同期しはじめます。**Basic Settings> High Availability > Status** フィールドは同期が完了するまで、*DEGRADED SYNC* を表示します。ハードディスクのサイズ、ストアされたデータ量に依存して、この作業には数時間かかります。

Step 12. 同期が完了しましたら、必要であれば、他のイーサネットケーブル(*EXT*, *INT*, *MGMT*)を接続してください。

期待される結果:

SSB クラスターのノードは新しい機器に交換されます。

8.7 コンフィグレーションバックアップからコンフィグレーションをリストアする

目的:

システムの不具合の場合、初期のコンフィグレーションバックアップよりコンフィグレーションをリストアできます。これを実施するには、以下の手順に従ってください。

前提条件:

コンフィグレーションバックアップからコンフィグレーションをリストアする前に、以前の既存のコンフィギュレーションのバックアップが必要になります。

■コンフィグレーションバックアップを作成する場合、詳細については、手順 4.3.5.1設定とデータのバックアップを定義する を参照してください。

オプションとして、GPGでコンフィグレーションバックアップを暗号化できます。詳細については、手順 4.3.5.3 設定とデータのバックアップを定義する をご参照ください。以下の手順は、GPGで暗号化されたコンフィグレーションバックアップからのリストア手順を説明しています。

Step:

Step 1. あなたの秘密鍵でコンフィグレーションを復号してください。

注記

SSB に GPG で暗号化されたコンフィグレーションを直接インポートすることはできません。それは、最初にローカルで復号される必要があります。

注記

システムバックアップのリストア(**Basic Settings > Management > System backup > Restore now**)は統計とレポート等のみリストアします。コンフィグレーションはリストアされません。

Step 2. ウェブインターフェイスが機能しない場合、SSBをインストールし直し、復号化されたコンフィグレーションをウェルカムウィザードでアップロードしてください。詳細については、手順 3.2 ウェルカムウィザードでのSSBの設定をする をご参照ください。

付録1　syslog-ng Store Box　ハードウェアインストレーションガイド

付録1.1　　SSB ハードウェアのセットアップ

この章では、syslog-ng Store Box (SSB)ハードウェアをセットアップする方法を案内します。

ハードウェア詳細についてのドキュメントは、BalaBit Hardware Documentation page.にて入手できます。

※　ハードウェア部品等の詳細、名称等は、変更される可能性があります。

目的:

ここでは、一つの SSB をセットアップする方法を案内します。

Step:

Step 1.　SSB を開梱します。

Step 2.　(オプションのステップ)SSB をスライドレールとともにラックに設置します。

Step 3.　ケーブルの接続。

Step a.　*EXT* とレーベルされたイーサネットコネクタに LAN 側のイーサネットケーブルを接続します。

Step b.　SSBハードウェアをリモートサポートするためにSSBのIPMI インターフェイスに、イーサネットケーブルを接続します。詳細については、以下ドキュメントを参照してください。

Onboard BMC/IPMI ユーザーガイドは、 the BalaBit Hardware Documentation page. にあります(英語)。

インターネットからIPMIインターフェイスにアクセスできるようにすることは必須ではありません。しかし、SSB管理者はベンダーサポートが必要になった場合は、サポートとトラブルシューティングのために、アクセスできなければなりません。

警告

IPMI インターフェイスからのみ入手できる情報にアクセスすることは、必須ではありませんが、サポートとトラブルシューティングプロセスをスピードアップするために、強く推奨します。

Step c. （オプションのステップ）初期設定完了後SSBを管理するために、*MGMT*とレーベルされたイーサネットコネクタ（これはマネージメント用のインターフェイスです）にイーサネットケーブルを接続します。（それぞれのインターフェイスの役割の詳細については、セクション　2.5　ネットワークインターフェイスをご参照ください。）

Step d. （オプションのステップ）*HA*とレーベルされたイーサネットコネクタに他のSSBノードへイーサネットケーブルを接続してください。これは、SSB の high availability(HA)インターフェイスです。（それぞれのインターフェイスの役割の詳細については、セクション　2.5 ネットワークインターフェイスをご参照ください。）

Step 4. ハードウェアをパワーオンしてください。

Step 5. syslog-ng Store Box の BIOS と IPMI パスワードを変更してください。（Balabit から出荷時のデフォルトパスワードは　*changeme*　です。）

Step 6. クライアントマシーンから SSB web インターフェイスに接続し設定してください。

付録1.2　　二つの SSB ユニットを HA モードで設定する。

目的:

ここでは、High availability サポートとともに、SSB をセットアップする方法を案内します。

Step:

Step 1. 最初のSSBユニットを、付録 1.1　SSBハードウェアのセットアップのステップ1から最後までの手順にしたがってセットアップします。

Step 2. 二つ目のSSBユニットを 付録 1.1　SSBハードウェアのセットアップのステップ1からステップ2までの手順にしたがってセットアップします。

Step 3. 二つのユニットを HA とレーベルされたイーサネットコネクタにイーサネットケーブルで接続します。

Step 4. 二つ目のユニットをパワーオンします。

Step 5. クライアントマシーンから、最初のユニットの　SSB　web　インターフェイスに接続し、**Basic Settings > High Availability** に進み、**Convert to Cluster** をクリックし、web　ブラウザで、

ページをリロードしてください。

Step 6.　スレイヴユニットを再起動しそしてマスターユニットを再起動してください。マスターユニットが起動するまで、数分お待ちください、そして web ブラウザで、ページをリロードしてください。

Step 7.　スレイヴユニットが、そのディスクをマスターユニットに同期するまでお待ちください。ハードディスクサイズに依存し、この作業には、数時間かかる場合があります。SSB web インターフェイスの **Basic Settings > High Availability > DRBD sync rate limit** にて、同期スピードを増やすことが可能です。

付録2　VMware 環境での syslog-ng Store Box インストレーションガイド

この章では、syslog-ng Store Box (SSB)を VMware ESXi サーバーに仮想アプライアンスとしてインストールする際に実現できることと制限されることについて説明します。

VMware 環境での SSB の制限

SSB は、VMware 環境での動作に関して特別なサポートはありません。仮想アプライアンスとして稼働させても、SSB の基本的な機能には影響はありませんが、以下のような制限があります。

- SSB は、インストレーション中に仮想ホストに割り当てた固定のディスク容量のみを使用できます。ディスクサイズを後から修正することはできません。また、オンデマンドでディスクを割り当てることもできません。
- 現在 SSB は VMware Ready プログラムに認定されておらず、VMware Tools もインストールされていません。その結果、SSB は VMotion をサポートしていませんし、vmware-tools を必要とする他のいかなる vmware 機能もサポートしません。あなたの VMware サーバーのドキュメントを確認し、vmware-tools 無しで、どの機能が動作するかご確認ください。
- ハイアベイラビリティ(High Availability)モードはサポートされません。
- ハードウェアに関するアラートや SSB のステータスインジケーターが不正な情報を表示することがあります。例;RAID ステータス Degraded 表示　等

プロシージャ – VMware ESXi に SSB をインストールする

目的:

ここでは、VMware ESXi に SSB をインストールする手順について説明します。

警告

VMware ESXi 4.0 以降のバージョンに SSB をインストールできます。
それ以前のバージョンは、サポートされません。

Step:

Step 1.　以下の設定で、SSB の仮想マシンを作成します。

■ゲスト OS には、一覧より、**Linux/Ubuntu 64bit** を選択してください。

■仮想マシンにメモリを割り当てます。4GB が通常ほとんどのタスクにおいて十分です。最小要件は、512MB です。推奨メモリサイズは環境に依存しますが、以下を考慮して下さい。

- 基本システムに 256MB が必要です。
- SSB 上で稼動する syslog-ng サーバーが 128MB～1GB 程度のメモリを消費します。消費するメモリ量はメッセージの負荷と SSB の設定に依存します。
- SSB はログスペースごとに受信メッセージのインデックスを作成するためのメモリを消費します。インデクサ（インデックス付け）に割り当てるメモリの量は、ログスペースごとに個別に設定できます。
- VMware 環境で 8GB 以上のメモリ使用はサポートされません。ほとんどのタスクには、4GB で十分です。

■ハードディスクコントローラは **LSI Logic Parallel** を使用します。

■ハードディスクに RAID を使用しないで下さい。（VMware 配下の実際のハードディスクに RAID を使用することは可能ですが、VMware 環境では、シングルハードディスクとして表示されます。）

■SSB は単一の固定サイズのディスクを使用します。基本システムに 5GB ほど要求され、残りのディスク容量はデータを保存するために使用されます。以下のディスクサイズ（単位は GB）の中から 1 つを選んで使用します。

8, 12, 68, 160, 230, 250, 465, 500, 925, 1029, 2053, 3077, 4101, 4645, 5125, 6149, 7173, 8197, 9205

■SSB のネットワークカードには **E1000** を使用して下さい。

Step 2.　仮想マシンの作成後、マシン設定を修正します。以下のオプションを設定します：

Step a.　**Option > VMware Tools** から **Shutdown**、**Suspend**、**Reset** オプションを有効にします。有効にしないと、SSB の管理者は SSB の Web インターフェイスからこれらの機能にアクセスできません。

Step b.　**オプション > Force BIOS Setup** オプションを有効にします。このオプションを有効にすると、SSB をインストールする前にシステム時間をチェックする（そして必要であれば修正する）ことができます。

Step c. **オプション** > **Paravirtualization** から Support **VMI Paravirtualization** オプションを有効にします。(これは必須ではありません。お使いの ESXi サーバーが、**VMI Paravirtualization** をサポートしていない場合などは、有効にしなくてもかまいません。)

Step 3. SSB のインストレーション ISO イメージをマウントして仮想マシンを起動します。画面上の指示に従って SSB をインストールします。

用語集

alias IP （エイリアス IP）	すでに IP アドレスを持つインターフェイスに割り当てられる追加の IP アドレス。通常の IP アドレスとエイリアス IP アドレスは、両方とも同じ物理インターフェイスを参照する。
auditing policy （監査ポリシー）	Windows が稼動しているホストに対し、どのログオンイヴェントを監査対象とするかを定義するポリシー。
authentication （認証）	ネットワークシステムやサービスへのアクセスを許可する前にユーザーまたはクライアントの認証を検証する処理。
BSD-syslog protocol （BSD-シスログプロトコル）	RFC3164 The BSD syslog Protocolに記載されている古いシスログプロトコルの規格。レガシーシスログプロトコルとして参照されることもある。
CA （認証局）	Certificate Authority（認証局）の略。証明書を発行する機関。
certificate （証明書）	一意に所有者を識別するファイル。証明書は所有者の識別情報、公開鍵、証明書の有効期限、証明書に署名した CA 名などのデータを含む。
client mode （クライアントモード）	クライアントモードでは、syslog-ngはホストで作成されたローカルログを収集し、ネットワーク接続からsyslog-ngセントラルサーバーまたはリレーに、収集したログをフォワードする。
destination （宛先）	ログメッセージが保存されているログスペース、リモートデータベース、またはサーバー。
destination driver	例えば、リモートサーバーやハードディスクなどの宛先に、syslog-ngがログメッセージを送るために使用する通信方法。
destination, remote	ネットワーク接続を使って、リモートホスト（つまりsyslog-ngリレー、またはサーバー）にログメッセージを送る宛先。

destination, local	ログメッセージをログスペースに転送する宛先。
disk buffer （ディスクバッファ）	syslog-ngのプレミアムエディションは、セントラルログサーバーや、サーバーへのネットワーク接続が利用できない場合、ローカルハードディスクにメッセージを保管することができる。
disk queue （ディスクキュー）	disk buffer（ディスクバッファ）をご参照下さい。
domain name （ドメイン名）	ネットワークの名前。例えば、balabit.com。
External network interface （外部ネットワークインターフェイス）	（EXTとラベルされた）外部インターフェイスは、クライアントとサーバーの一般通信で使用される。 「管理インターフェイス」(後述)が設定されていない場合は、この外部インターフェイスが管理インターフェイスをもかねます。
filter	フィルターで設定された条件と一致するログメッセージのみをソースから選択する。
firmware （ファームウェア）	SSB 上で稼動するソフトウェアコンポーネントの集合体。ファームウェア全体のアップグレードは可能だが、ファームウェアを構成する個々のソフトウェアコンポーネントを SSB 上でアップグレードすることはできない。SSB には external（外部）ファームウェア（または boot（ブート）ファームウェア）と internal（内部）ファームウェア（または core（コア）ファームウェア）の2つのファームウェアがある。この2つのファームウェアはそれぞれ別にアップグレードすることができる。
gateway （ゲートウェイ）	例えば、ローカルイントラネットと外部ネットワーク（インターネット）など、2箇所以上のネットワークを接続するデバイス。ゲートウェイは、他のネットワークへの入り口としての役割を果たす。
High Availability （ハイアベイラビリティ）	ハイアベイラビリティ(HA)モードでは、1つ目の SSB ユニット（マスターノード）が機能を停止した場合でもサービスを利用できるように、2つ目のユニット（スレーブノード）も動作する。

host （ホスト）	ネットワークに接続されているコンピューター。
hostname （ホスト名）	ネットワーク上でホストを特定するための名前。ホスト名には、英数字（A-Z, a-z, 0-9）とハイフン（-）のみ使用できる。
HA network interface （HA ネットワークインターフェイス）	SSB クラスターノード間の通信のための（HA ラベル付きの）インターフェイス。
IETF-syslog protocol （IETF シスログプロトコル）	Internet Engineering Task Force(IETF)が開発した標準のシスログプロトコル。RFC 5424 の The BSD syslog Protocolをご参照下さい。
key pair （鍵ペア）	秘密鍵とそれに関連する公開鍵。秘密鍵は所有者のみが知っている。公開鍵は自由に配布できる。秘密鍵で暗号化された情報は、公開鍵を使わないと復号化することができない。
LDAP	Lightweight Directory Access Protocol の略。TCP/IP 上でディレクトリサービスを使用してデータの検索と修正を行うためのアプリケーションプロトコル。
log path （パス）	送信元、フィルター、パーサ、リライトルール、宛先の組み合わせ。syslogng-ng は、パスの送信元に届くすべてのメッセージを検査して、すべてのフィルターに合致するメッセージを指定の宛先に送信する。
logstore （ログストア）	ログメッセージを暗号化、署名、圧縮そしてタイムスタンプすることができる、バイナリログファイル形式**で蓄積されたログ保存領域。**
log source host （ログの発生元の装置）	SSB にログを送るホストかネットワークデバイス（syslog-ng クライアントとリレーを含む）。ログソースホストは、サーバー、ルータ、デスクトップコンピューター、またはシスログメッセージを送ったり、syslog-ng を起動したりできるその他のデバイスなどがあります。
LSH	log source host をご参照ください。

Management network interface （管理インターフェイス）	管理インターフェイス(MGMT ラベル付)は、SSB と監査者、または SSB と管理者の間の通信に限って使用される。
master node （マスターノード）	SSB を High Availability（ハイアベイラビリティ）モードで使用している時にアクティブな SSB マシン。
name server （ネームサーバー）	ドメイン名に相当する IP アドレスを保存するネットワークコンピューター。
node （ノード）	High Availability（ハイアベイラビリティ）モードで起動している SSB ユニット。
output buffer （出力バッファ）	宛先がすぐにメッセージを受け取ることができない場合、syslog-ng が送信ログメッセージを保存するホストのメモリの一部。
output queue （出力キュー）	出力キューからのメッセージはターゲット syslog-ng サーバーに送られる。出力キューが満杯ではない限り、syslog-ng アプリケーションは、出力キューに送信メッセージを直接加える。出力キューは 64 メッセージまで保存することができる。これは固定値で、変更することはできない。
overflow queue （オーバーフロウキュー）	output buffer をご参照ください。
ping	ネットワーク上でホストから別のホストにメッセージを送るコマンドで接続性とパケットロスをテストする。
port （ポート）	送信されたデータの宛先アプリケーションを識別する 1 から 65535 までの数字。例えば、SSH は通常ポート 22 を使用し、Web サーバー(HTTP)はポート 80 を使用する。
Publice-key authentication （公開鍵認証）	ユーザあるいはクライアントの identity（身元）確認のために暗号化された鍵ペアを使用する認証方式。

redundant Heartbeat interface （冗長 Heartbeat（ハートビート）インターフェイス）	冗長 Heartbeat（ハートビート）インターフェイスは SSB デバイスの既存のインターフェイスを使用する仮想インターフェイス。HA モードにおける、SSB クラスターの他のノードが正常な状態であることを検出する。仮想インターフェイスはノード間のデータを同期させるためには使用されず、Heartbeat（ハートビート）メッセージだけが転送される。
regular expression （正規表現）	正規表現は一連の文字列を説明したり、一致させたりする文字列。syslog-ng アプリケーションは拡張された正規表現（POSIX（新しい正規表現）と呼ばれることもある）をサポートしている。
relay mode （リレーモード）	リレーモードでは、syslog-ng は syslog-ng クライアントからネットワークを通じてログを受信し、ネットワーク接続を使用して中央 syslog-ng サーバーに受信したログをフォワードする。
SSB	syslog-ng Store Box の略。
slave node （スレーブノード）	マスターが利用できなくなった際にアクティブユニット(マスターノード)に置き換わる、普段はスタンバイ中の SSB ユニット。
source （ソース）	SSB のシスログメッセージの受信方法。
source, network （ソース、ネットワーク）	ネットワーク接続を使用してリモートホストからログメッセージを受信するソース。UDP、TCP、TLS 方法は、BSD シスログプロトコルと IETF シスログプロトコルを使用して、サポートされている。
source, local （ソース、ローカル）	SSB からローカル環境でログメッセージを受信するソース。
source driver （ソース、ドライバー）	ログメッセージを受信するために使用される通信方法。
SNMP	Simple Network Management Protocol(SNMP)はネットワーク管理で使用される業界標準プロトコル。SSB はリモートホストからの SNMP メッセージの受信、それらの syslog メッセージへの変換、そしてリモートホストに対しての SNMP トラップ送信が可能。

split brain （スプリットブレイン）	スプリットブレイン状況は何らかの理由（例： ノード間の接続喪失）により SSB クラスターの両ノードがアクティブ（マスター）になってしまう状況。新しいデータ（例： ログメッセージ）が他のノードに対して複製を作ることなしに両ノード上に作成される原因となる可能性がある。そのため、この状況ではマージできない2つの異なるデータのセットが作成される可能性がある。
syslog-ng	syslog-ng アプリケーションは柔軟で拡張性の高いシステムロギングアプリケーションである。一般にはログメッセージを管理やログの一元管理するために使用される。
syslog-ng agent	Windows の syslog-ng エージェントは、Microsoft Windows プラットフォーム用のログ収集・ログ転送アプリケーションである。Windows ベースのホストのログメッセージを収集し、通常または SSL で暗号化された TCP 接続を使用して、SSB にログメッセージをフォワードする。
syslog-ng client	クライアントモードで syslog-ng を実行しているホスト。
syslog-ng Premium Edition	syslog-ngプレミアムエディションはオープンソースアプリケーションの商用バージョンである。暗号メッセージの転送、Microsoft Windows プラットフォーム用のエージェントといった追加の機能を提供する。
syslog-ng relay	リレーモードで syslog-ng を実行しているホスト。
syslog-ng server	SSB のようにサーバーモードで syslog-ng を実行しているホスト。
TLS	Transport Layer Security (TLS)とその先行版の、Secure Sockets Layer (SSL)は、インターネット上で安全な通信を提供する暗号プロトコル。syslog-ng アプリケーションは機密ログメッセージへの不正アクセスを防ぐために、TLS を使用してクライアントとサーバー間の暗号化通信を可能にする。
template	ログメッセージの再構築やファイル名の自動作成に使用することができるユーザー定義構造。

Traceroute	2 つのホスト間で全てのルーティングステップ（メッセージのパス）を表すコマンド。

日本語マニュアル改定日　2013 年 12 月 27 日

本マニュアル原文は『The syslog-ng Store Box 3.0 Administrator Guide』です

ジュピターテクノロジー株式会社 翻訳グループ