
ディスクスペース飽和防止方法



Rev. 1.0

2017.02.17



目次

1	はじめに	1
2	各設定の説明	1
3	ディスク最大使用量アラート設定	2
4	ログデータの定期的なアーカイブ/クリーンナップ設定	3
5	ディスクスペース飽和防止設定	5
6	補足	5
6.1	ディスク使用容量の確認方法	5
6.2	アラートの通知例	6
6.3	ログ保持日数(Retention time in days)の算出例	9
	お問い合わせ	10

1 はじめに

syslog-ng Store Box(SSB)の設定がお客様の運用に適した設定になされていないことにより、ディスクスペース飽和状態(ディスクがログデータでいっぱい)になると、次のようなアラートが通知され、Web I/F にもメッセージが表示されます。Web I/F でのアクセスコントロールが出来なくなる他、システムも正常に動作しなくなることがあります。

例. ディスクスペース飽和状態アラート例

Failed to write to the disk; Disk is probably full, please use the console to free up some space

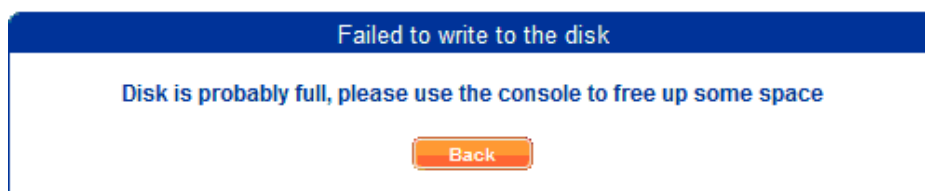


図 1 ディスクスペース飽和状態メッセージ

ここでは、ディスクスペース飽和防止の方法を以下の手順に沿って説明します。設定をご確認いただき、お客様の運用に適した設定にされるようお願いいたします。

ここでの手順はバージョン 4 LTS に沿っています、3 LTS をお使いの方は [3 LTS 管理者ガイド](#) をあわせてお読みください。

2 各設定の説明

- ディスク最大使用量アラート設定:

ディスクが最大ディスク使用量を超えた場合、アラートを通知させます。これにより、古いログデータのアーカイブ/クリーンナップなど、対策することでディスクスペース飽和を防ぐようにします。

このアラートが通知されないように、次の「ログデータの定期的なアーカイブ/クリーンナップ設定」を適切に行います。

- ログデータの定期的なアーカイブ/クリーンナップ設定:

最大ディスク使用量に達する前にログデータの定期的なアーカイブ/クリーンナップを行うことで、ディスクスペース飽和を防ぐようにします。

定期的なアーカイブ/クリーンナップはログの保持日数を指定し、それ以前の古いログデータを SSB のローカルディスクから削除し適切なディスクスペースを保ちます。

ここでの設定をお客様の運用に適した設定にすることがログ管理の安定稼働につながります。組織変更、クライアントの増設など運用形態に変更(特に一日の受信ログ容量が増加するような)があった場合、必ずこの設定を見直してください。

- ディスクスペース飽和防止設定:

ディスクがディスクスペース飽和防止使用量を越えた場合、SSBはログ受信を切断してログデータをディスクに保存するのを停止しディスクスペース飽和を防ぎます。

この設定はログデータの定期的なアーカイブ/クリーンアップを行っていても設定することを推奨します。運用形態の変更などでログ受信容量が急激に増加した場合のディスクスペース飽和を防止します。

- 補足:

「6.1 ディスク使用容量の確認方法」、「6.2 アラートの通知例」、「6.3 ログ保持日数(Retention time in days)の算出例」を説明しています。

3 ディスク最大使用量アラート設定

1. Basic Settings > Alerting & Monitoring > Health monitoring に移動します。

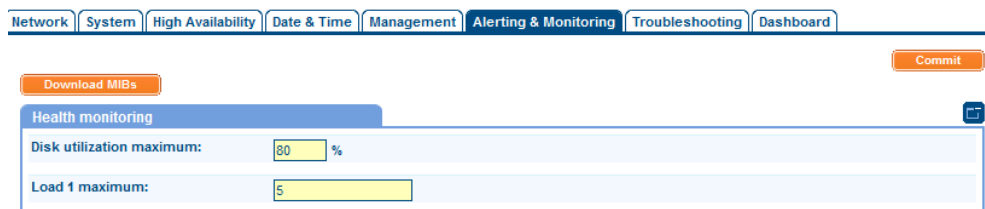


図 2 Health monitoring 画面

2. 最大ディスク使用量(Disk utilization maximum:)をパーセントで指定します。[Commit]をクリックします。(デフォルトで 80%が設定されています。この値は、ほとんどの使用環境に適合します。必要な場合のみ変更してください。)
3. 次の「3.1 E メールアラートの通知設定」または「3.2 SNMP(trap)アラートの通知設定」を有効にするとアラート通知が送信されます。

3.1 E メールアラートの通知設定

1. Basic Settings > Management > Mail settings に移動します。
2. メールサーバー(SMTP server address:)、アラートの送信先アドレス(Administrator's e-mail address:)を設定して、[Commit]をクリックします。
3. [Test]をクリックして、メールが正しく送信されているか確認します。

図 3 Mail settings 画面

3.2 SNMP(trap)アラートの通知設定

1. Basic Settings > Management > SNMP trap settings に移動します。
2. SNMP サーバー(SNMP server address:)および SNMP のバージョンを設定し、[Commit]をクリックします。
3. [Test]をクリックして、SNMPトラップが正しく送信されているか確認します。

図 4 SNMP trap settings

※現在のディスク使用量を確認するには「6.1 ディスク使用容量の確認方法」をご覧ください。

詳しくは、[4 LTS 管理者ガイド](#)『4.6.1 監視の設定、4.6.2 システムヘルス監視および 4.5 SNMP と E メールアラート』をお読みください。3 LTS をお使いの方は [3 LTS 管理者ガイド](#)『4.3.4 SSB のシステム監視設定および 4.3.3 SNMP と E メールアラート』をお読みください。

4 ログデータの定期的なアーカイブ/クリーンアップ設定

1. Policies > Backup & Archive/Cleanup > Archive/Cleanup policies に移動し、[+]をクリックします。
2. ポリシー名、開始時間(Start time:)、アーカイブ先(Target settings:)、ログデータの保持日数(Retention time in days:)(ここで指定した日数のログデータが SSB のローカルディスクに保持され、それ以前の古いログデータはアーカイブ後、削除されます。)を設定して [Commit]をクリックします。

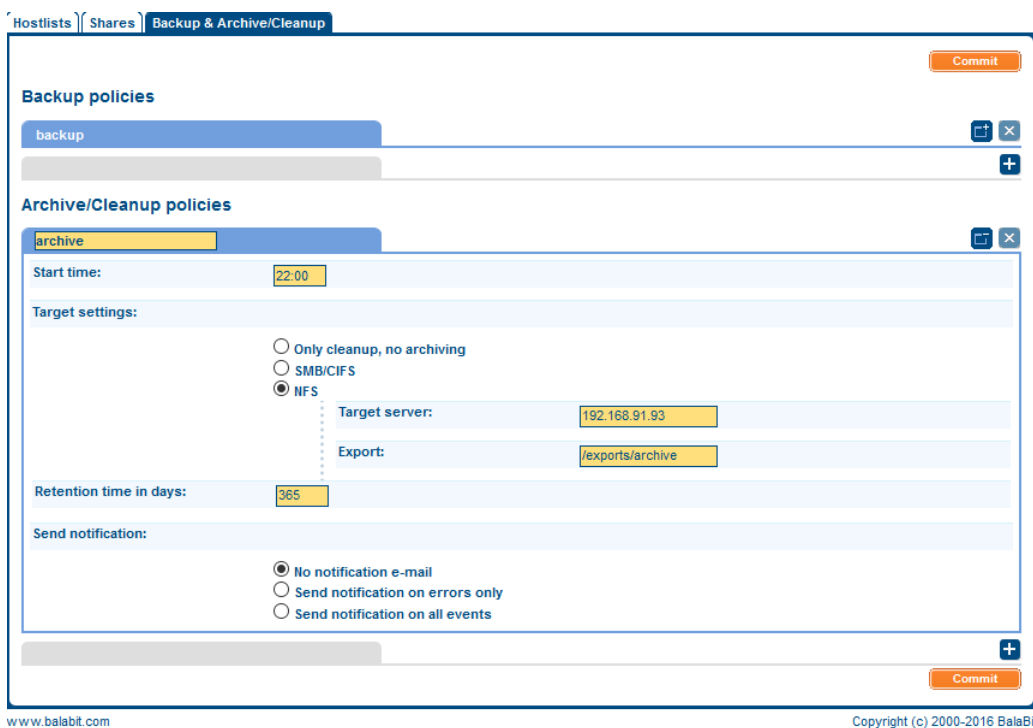


図 5 Archive/Cleanup policies 画面

- その後、Log > Spaces に移動し、アーカイブ/クリーンナップしたいログスペースを選択します。

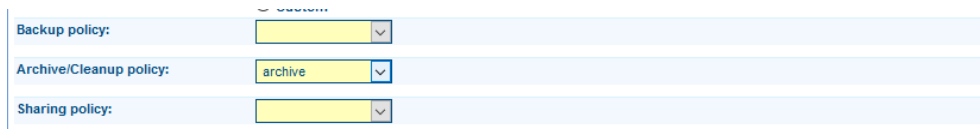


図 6 Archive/Cleanup policy フィールド画面

これにより、ポリシーで設定した時間にアーカイブ/クリーンナップが開始されます。この例では、毎日 22:00 時にアーカイブ/クリーンナップが開始され、365 日より前のログデータが NFS サーバー(192.168.91.93 の /exports/archive 以下)にアーカイブされます。アーカイブされたログデータは SSB のハードディスクから削除されディスクスペースを作ります。

※アーカイブしたログデータは、アクセスと検索ができますが、SSB にリストア(戻す)することはできません。

※手順 2.で[Only cleanup, no archiving]を選択するとログファイルの削除のみ行われます。アーカイブは行われません。

※手順 2.で[Retention time in days]の値は一日の受信ログ容量に応じて適宜、設定してください。詳しくは、「6.3 ログ保持日数(Retention time in days)の算出例」を参照してください。

詳しくは、[4 LTS 管理者ガイド](#)『4.8 アーカイブとクリーンナップ』をお読みください。3 LTS をお使いの方は [3 LTS 管理者ガイド](#)『4.3.5 データと設定のアーカイブとバックアップ』および『5.2.5 ログスペースの管理』をお読みください。

5 ディスクスペース飽和防止設定

1. Basic Settings > Management > Disk space fill up prevention に移動します。
2. ディスクスペース飽和防止使用量をパーセントで指定します。[Commit]をクリックします。

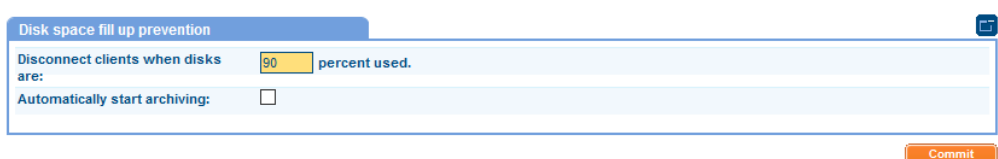


図 7 Disk space fill up prevention 画面

3. Basic Settings > Alerting & Monitoring > System related traps に移動します。
4. Disk usage is above the defined ratio にチェックを入れアラートを有効にし、[Commit]をクリックします。



図 8 Disk usage is above the defined ratio フィールド

※ディスクスペース飽和防止使用量がこの値(この例では、90%)を超えた場合、SSB はすべてのクライアントからのログ受信を切断し、ログデータによるディスクスペースの飽和を防ぎます。

※現在のディスク使用量を確認するには「6.1 ディスク使用容量の確認方法」をご覧ください。

※アラートを通知する為に、SMTP サーバーまたは SNMP サーバーを設定する必要があります。「3.1 E メールアラートの通知設定」、「3.2 SNMP(trap)アラートの通知設定」をご覧ください。(「3.1 E メールアラートの通知設定」では“Send e-mail alerts to:”欄にメールアドレスを追加する必要があります。)

詳しくは、[4 LTS 管理者ガイド](#)『4.6.3 ディスクスペース飽和防止手順』をお読みください。3 LTS をお使いの方は [3 LTS 管理者ガイド](#)『4.3.4.3 ディスクスペース飽和防止手順』をお読みください。

6 補足

6.1 ディスク使用容量の確認方法

SSB の Web インターフェイスで System monitor(システムモニター)の disk 棒グラフにマウスポインタを当てると、詳細の情報がツールチップにて表示されます。

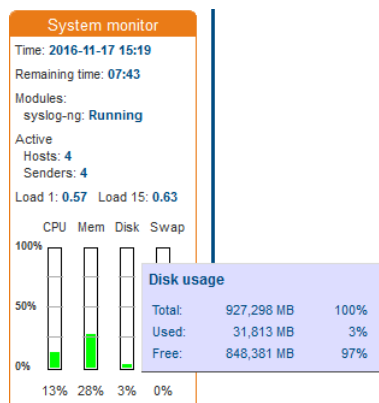


図 9 System monitor のディスク情報表示

詳しくは、[4 LTS 管理者ガイド](#)『4.2 Web インターフェイスの構成』をお読みください。3 LTS をお使いの方は [3 LTS 管理者ガイド](#)『4.2 Web インターフェイスの構成』をお読みください。

または、Basic Settings > Dashboard に移動し、Disk グラフを確認します。

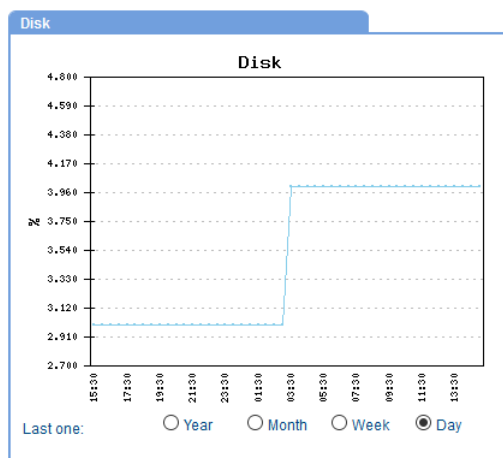


図 10 Dashboard のディスク表示

詳しくは、[4 LTS 管理ガイド](#)『16.5 ステータス履歴と統計』をお読みください。3 LTS をお使いの方は [3 LTS 管理者ガイド](#)『8.5 ステータス履歴と統計』をお読みください。

6.2 アラートの通知例

ディスク使用量アラート設定およびディスクスペース飽和防止設定関連のアラート例を次に示します。

例. ディスク使用量アラートで設定したディスク容量を超えた場合

メール通知例:

```
DISMAN-EVENT-MIB::sysUpTimeInstance 2303453
      SNMPv2-MIB::snmpTrapOID.0
DISMAN-EVENT-MIB::mteTriggerFired
      DISMAN-EVENT-MIB::mteHotTrigger.0 high disk utilization
DISMAN-EVENT-MIB::mteHotTargetName.0
DISMAN-EVENT-MIB::mteHotContextName.0
      DISMAN-EVENT-MIB::mteHotOID.0 UCD-SNMP-MIB::dskErrorFlag.1
DISMAN-EVENT-MIB::mteHotValue.0 1
      UCD-SNMP-MIB::dskErrorMsg.1 /: less than 20% free (= 80%)
      UCD-SNMP-MIB::dskDevice.1 rootfs
      UCD-SNMP-MIB::dskTotal.1 4127240
      UCD-SNMP-MIB::dskAvail.1 786572
```

SNMP trap 通知例:

```
sysUpTimeInstance = Timeticks: (11) 0:00:00.11
TRAP 種別 = OID: mteTriggerFired
mteHotTrigger.0 = STRING: high disk utilization
mteHotOID.0 = OID: dskErrorFlag.1
mteHotValue.0 = INTEGER: 1
dskErrorMsg.1 = STRING: /: less than 85% free (= 23%)
dskDevice.1 = STRING: rootfs
dskTotal.1 = INTEGER: 4127240
dskAvail.1 = INTEGER: 3036056
```

例. ディスクスペース飽和防止設定ディスク容量を超えた場合(ログ受信を停止します。)

メール通知例:

```
DISMAN-EVENT-MIB::sysUpTimeInstance 2354859
      SNMPv2-MIB::snmpTrapOID.0 XCB-SNMP-MIB::xcbDiskFull
      XCB-SNMP-MIB::description Disk usage ratio limit reached,
stopping services; limit='90', usage='92'
```

SNMP trap 通知例:

```
sysUpTimeInstance = Timeticks: (644537) 1:47:25.37
TRAP 種別 = OID: xcbDiskFull
description = STRING: Disk usage ratio limit reached, stopping services;
limit='90', usage='92'
```

System monitor(システムモニター)にも“Disk fill-up prevention active! Rejecting connections!”と表示され、ログ受信が切断されたことがわかります。

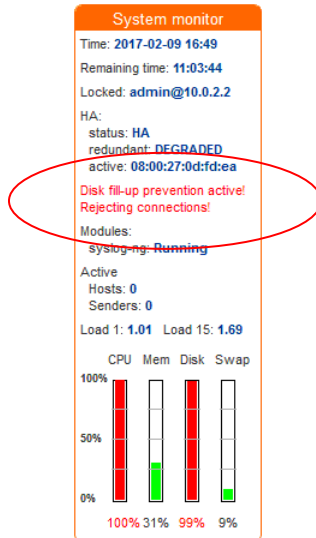


図 11 System monitor のディスクスペース飽和状態表示

例. ディスクスペース飽和防止設定ディスク容量を下回った場合(ログ受信を再開します。)

```

メール通知例：
DISMAN-EVENT-MIB::sysUpTimeInstance 10047
      SNMPv2-MIB::snmpTrapOID.0 XCB-SNMP-MIB::xcbDiskFull
      XCB-SNMP-MIB::description Disk usage ratio went below limit,
restarting services; limit='90', usage='61'

SNMP trap 通知例：
sysUpTimeInstance = Timeticks: (342788) 0:57:07.88
  TRAP 種別 = OID: xcbDiskFull
description = STRING: Disk usage ratio went below limit, restarting
services; limit='20', usage='13'

```

例. ディスクが飽和状態になった場合

```

メール通知例：
DISMAN-EVENT-MIB::sysUpTimeInstance 2765905
      SNMPv2-MIB::snmpTrapOID.0 XCB-SNMP-MIB::xcbError
      XCB-SNMP-MIB::description Failed to write to the disk; Disk is
probably full, please use the console to free up some space
      XCB-SNMP-MIB::username admin
      XCB-SNMP-MIB::peerAddress 10.0.2.2

SNMP trap 通知例：
sysUpTimeInstance = Timeticks: (11) 0:00:00.11
  TRAP 種別 = OID: xcbError
description = STRING: Failed to write to the disk; Disk is probably full,
please use the console to free up some space
  username = STRING: admin
peerAddress = IpAddress: 10.0.2.2

```

SSB Web I/F には以下のようなメッセージダイアログが表示されます。

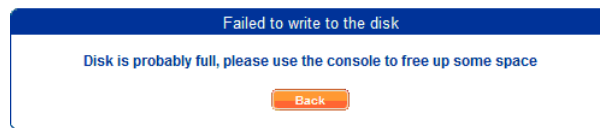


図 12 ディスクスペース飽和状態時の Web I/F メッセージ

6.3 ログ保持日数(Retention time in days)の算出例

ログ保持日数(Retention time in days)は、一日の受信ログ容量(平均)×Retention time in days(日数)が「3 ディスク最大使用量アラート設定」で設定した最大ディスク使用量を越えないようにします。つまり、([ディスク容量×Disk utilization maximum 設定値]<[一日の受信ログ容量(平均)×Retention time in days 値])になるように設定します。

ここでは、ログスペースのサイズからログ保持日数を算出する方法を示します。

1. Log > Spaces に移動します。
2. 各スペースで[Get current size]をクリックし、最新のデータを表示します。

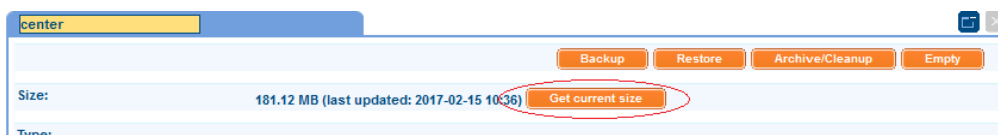


図 13 [Get current size]

3. 各スペースのサイズを合計します。
4. 合計サイズをログ取得日数(稼働日数)で除算し、一日のログ容量を求めます。
例: 合計サイズが 50GB でログ取得日数が 1 週間の場合
 $7\text{GB} \doteq 50\text{GB} \div 7$
5. 最大ディスク使用量を求めます。
例: HDD 容量が 1TB で Disk utilization maximum 値が 80 の場合
 $819\text{GB} \doteq 1\text{TB} \times 0.8$
6. ログ保存日数を求めます。
例: 最大ディスク使用量を一日のログ容量で除算
 $117\text{日} \doteq 819\text{GB} \div 7\text{GB}$

この例では、ログ保持日数(Retention time in days)に 117(日)以下を設定します。

※ログスペースにログストアを使用し圧縮している場合は、圧縮率が約 50%になります。この例で、ログが圧縮保存されている場合は、実際のログデータは合計サイズが約 100GB、一日のログ容量が約 14GB になることに注意してください。

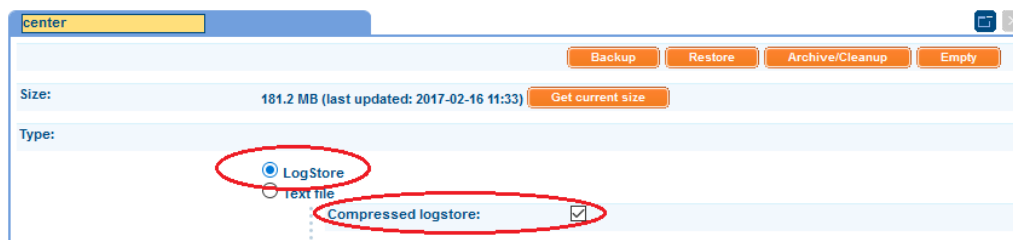


図 14 スペースの圧縮設定

お問い合わせ

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

住所: 〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F

URL: <http://www.jtc-i.co.jp/>

電話番号: 042-358-1250

FAX 番号: 042-360-6221

ご購入のお問い合わせ:

お問い合わせフォーム <https://www.jtc-i.co.jp/contact/scontact.php>

メール sales@jtc-i.co.jp

製品サポートのお問い合わせ:

カスタマーポータル <https://www.jtc-i.co.jp/support/customerportal/>

本文書に関する諸権利は、特に記載されているもの以外は、すべてジュピターテクノロジー株式会社
会社に帰属しており、著作権法上認められた場合を除き、無断使用・無断転載を禁止します。

マニュアル発行日 2017年2月17日

ジュピターテクノロジー株式会社

Copyright © 2016 ジュピターテクノロジー株式会社 All Rights Reserved.