

MylogStar FileServer

かんたん設定ガイド



1. 取得ログの内容確認



2. アラート設定の確認

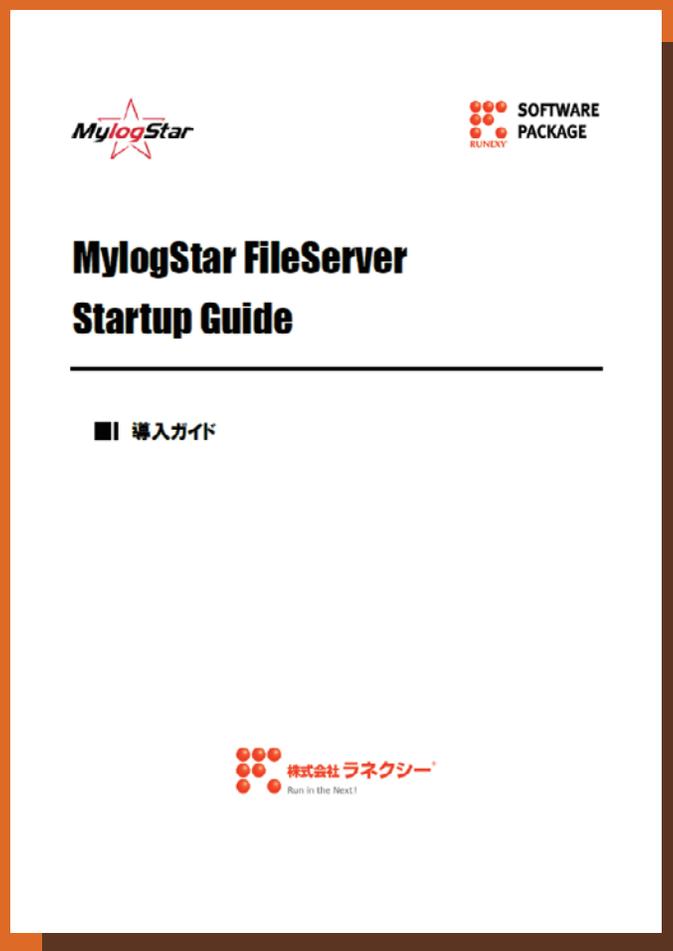


3. ログ保存期間の確認

はじめに . MylogStar FileServer のインストール



インストールについては製品 DVD もしくはトライアル内にある「MylogStar_FileSever_Startup_Guide.pdf」の「2. MylogStar FileServer のインストール」を元に MylogStar FileServer のインストールを行ってください。「MylogStar_FileSever_Startup_Guide.pdf」は、MylogStar のインストール・詳細設定・機能に及んで説明を行っている資料となります。



MylogStar 公式 Web サイトにインストール手順を動画でまとめたインストールチュートリアルムービーもございます。ご参考までにご利用ください。

<http://www.mylogstar.net/movie/mylogstar-desktop-fileserver-tutorial.html>



1. 取得ログの内容確認

< ログ取得・フィルター設定 >



ファイルサーバーの監視に必要なログ種別の指定と、共有フォルダーのファイル操作を詳細に取得するため、ログ取得設定およびフィルターを調整します。

1 [設定]→[ポリシー設定]→[ポリシー設定]→[新しいポリシー]をクリックし、ポリシー名を設定して[登録]をクリック。



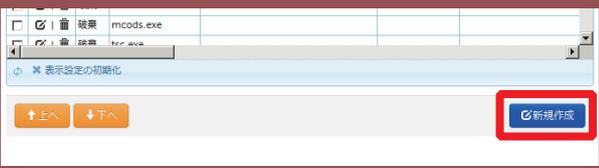
2 [ログ取得]をクリックして、取得対象の項目を選択し、[更新]をクリック



3 [フィルター]タブから[ファイル]を選択



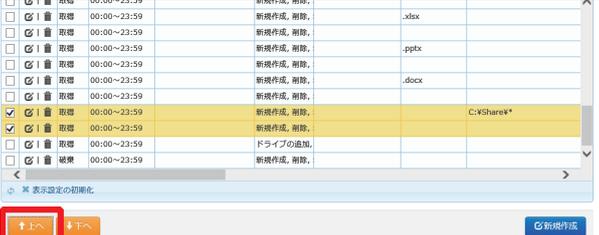
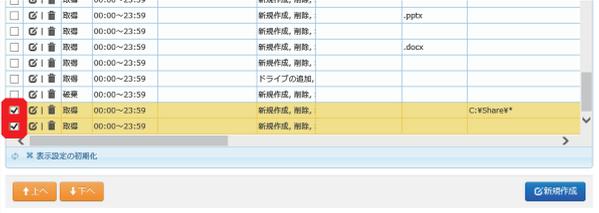
4 [新規作成]をクリック、「パス (操作前)」に共有フォルダーのパスを指定して[登録]をクリック



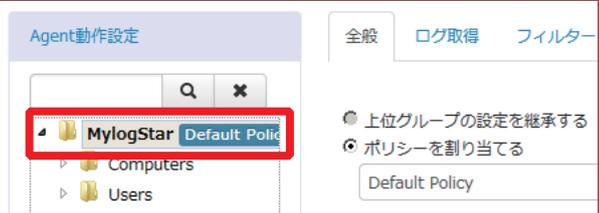
5 ④の手順と同様に「パス (操作後)」に共有フォルダーのパスを指定したフィルターを新規作成



6 追加された⑤のフィルター(最下部の2件)にチェックを入れ、[上へ]ボタンを2回クリックして移動



7 [Agent 動作設定] を選択し、[MylogStar] を選択、「ポリシーを割り当てる」から作成したポリシーを指定して[更新]をクリック



①で指定したポリシーを指定

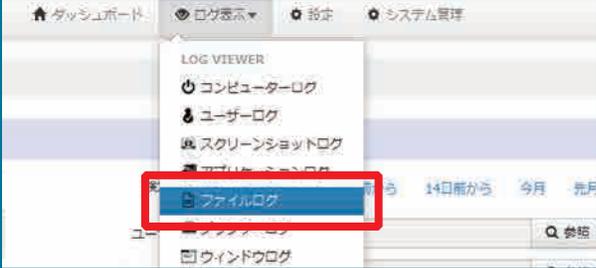
2. アラート設定の確認

< アラートタグの設定 >



重要フォルダー（例：顧客情報）へのアクセスがあった場合に、タグを付加します。
これにより危険操作を強調し、容易に検索することができます。

1 [ログ表示] から [ファイルログ] をクリック



2 [詳細検索] → [追加条件] をクリック



3 パスを入力して、リストから [いずれかを含む] を選択し、[検索] をクリック



4 [検索条件の保存] をクリックし、検索条件名を入力して [登録] をクリック



5 [設定] → [アラートタグ設定] を開き、[新規作成] をクリックし、アラートタグ名の入力とカラーを指定して [登録] をクリック



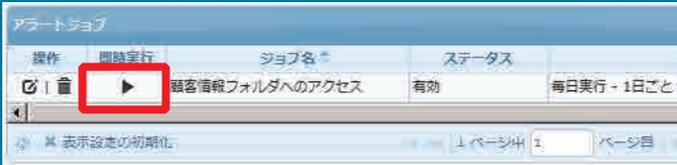
6 [設定] → [アラートジョブ] を開き、[新規作成] をクリックし、ジョブ名、スケジュールタイプ、実行時間、アラートジョブ条件で使用される条件、付与するアラートタグを設定し、[登録] をクリック



以上でアラート設定が完了。指定時刻にアラートが付加されます。

すぐに確認したい場合・・・

登録したアラートジョブの「即時実行」にある「▶」ボタンをクリックし、「はい」をクリックしてジョブを実行することで、しばらく後にログにて確認できます。



3. ログ保存期間の確認



< アーカイブの設定 >

当月+1か月以上経過したログをアーカイブファイルとして切り出します。
アーカイブ処理を行うことでパフォーマンスを一定に保つことができます。

1 [設定]→[アーカイブジョブ]を開き、[新規作成]をクリックし、下記情報を設定し、[登録]をクリック

アーカイブジョブ登録

全般

ジョブ名
月次アーカイブジョブ

スケジュールタイプ
毎月 (日付指定)

実行時刻
00:00

実行日
1 日

説明
月次のアーカイブジョブ
当月+1ヶ月より超過したログはアーカイブファイルに切り出し

ステータス
 有効

アーカイブジョブ条件

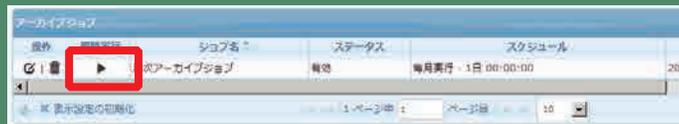
保存先フォルダー
D:\MylogStarArchive

MylogStar Serverでの保存先フォルダーを指定してください。

ログ保持期間
 当月 + nヶ月間
 当日 + n日間
n= 1

キャンセル

2 登録後、指定のスケジュールにて、アーカイブが実行されます。即時実行する場合は、下記 [設定]→[アーカイブジョブ] より、作成したジョブにおける即時実行にある「▶」をクリックすることで、実行することができます



補足：

アーカイブされたログを復元する場合は、[システム管理]→[アーカイブされたログの管理]より、復元対象の該当月にチェックを入れ、[参照用データベースへの展開]を実行後、しばらくの後[参照用データベースへの接続]から、ログデータを参照することが可能です。



SQL Server では、データベースへの変更情報（トランザクションログ）を逐次的に記録・蓄積しています。実運用や長期運用では、変更情報が蓄積されることによりハードディスクの空き容量を圧迫する可能性があるため、定期的（毎週または隔週）に、「MylogStar_FileServer_Startup_Guide.pdf」の「3.6.4. バックアップジョブ」を参考に、「完全バックアップ」および「トランザクションログのバックアップ」の順番でデータベースのバックアップを行い、変更情報を肥大化させないようにしてください。

推奨値。1ヶ月を超えたログを別ファイルに切り出します。



当ガイドに含まれない機能（バックアップ・管理ユーザー設定・アンインストール）についての設定方法は、
MylogStar FileServer インストールメディアに格納されている
「MylogStar_FileServer_Startup_Guide.pdf」をご参照ください。

導入後の設定等については、「MylogStar_Operation_Manual.pdf」をご参照ください。