

Change Auditor for Windows File Servers

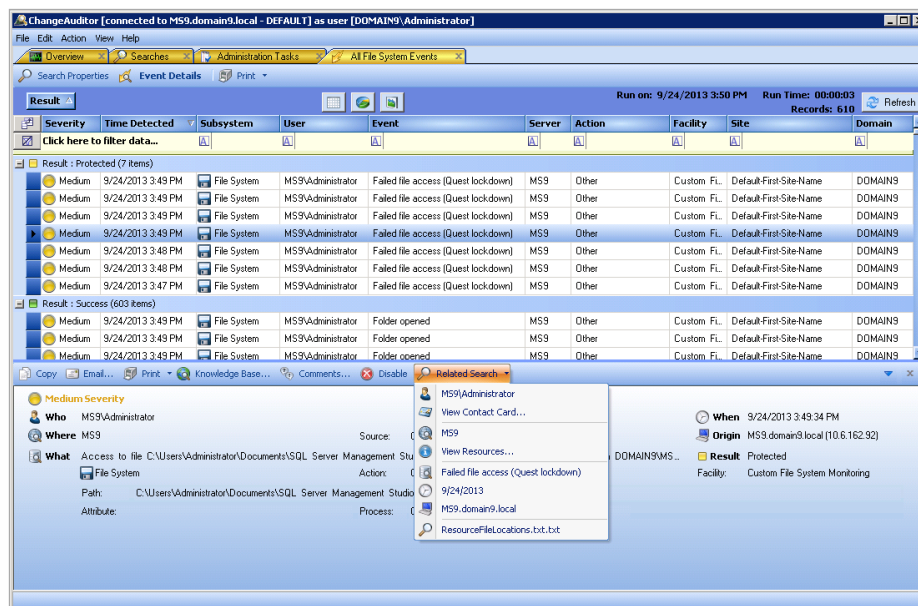
Windowsファイルサーバのツールによる重要な変更の追跡、監査、レポート作成、および通知

お使いのMicrosoft Windowsファイルサーバには、重要な機密情報が保存されています。しかし通常、文書に対するアクセス権を追跡したり順守させたりするのは非常に困難で、情報セキュリティのポリシー違反およびアクセス権の不正利用のほとんどは検知されません。

さらに、Windowsファイルサーバに問題が発生すれば、痛手の大きいサービス中断、およびビジネスに致命的な影響を与えるネットワークのダウンタイムを招きかねません。サーバの問題はセキュリティ違反も引き起こし、一般データ保護規則 (GDPR)、サーベンスオクスリー法 (SOX)、クレジットカード業界のセキュリティ基準 (PCI DSS)、および医療保険の携行性と責任に関する法律 (HIPAA) などの、重要な政府機関規制への非準拠につながる可能性もあります。これらの問題を避けるため、Windowsファイルサーバへの重要な変更についてリアルタイムに通知を受信できることが組織には必要です。

Quest® Change Auditor for Windows File Serversでは、重要なファイルとフォルダの変更すべてをリアルタイムに追跡することで、Windowsファイルサーバのセキュリティを確保し、サーバを管理します。

Change Auditorは、Windowsファイルサーバに影響を及ぼす変更について追跡、監査、報告、および警告を行います。その際に、ネイティブの監査機能実行によるオーバーヘッドは生じません。Change Auditor for Windows File Serversによって、時間の経過と共に完全な可視性を時系列順に得ることが可能です。すべての変更について、誰が、何を、いつ、どこで、どのワークステーションで行ったのか、その詳細なフォレンジック、その他の関連イベントの詳細、およびイベント前後の値も確認できます。また、監査要件を満たすために特定の変更が行われた理由について、コメントを追加することも可能です。



保護されている資産に対して試行された変更の潜在的な厳密さと、それ以外にユーザが関連検索を利用して行おうとした変更または削除の試みを表示しています。

Change Auditorは、リアルタイムの監視および過去のイベント分析に大変優れたツールです。今ではファイルサーバ全体の99%をセキュアに表示できるようになりました。監査に関する問題をすべて発見でき、短時間で修正して保護できます。

Global 500プロフェッショナルサービス会社、CEO

メリット:

- ユーザ行動パターンに基づいてプロアクティブに脅威を検知
- 機密ファイル/フォルダへのアクセスを阻止することで内部制御を強化し、アクセス権限のあるユーザを制御
- すべてのイベントおよび特定のインシデントに関する変更を追跡して未知のセキュリティの問題をなくし、ファイル、フォルダ、およびユーザへの継続的なアクセスを確保
- デバイスを問わないリアルタイム通知で即座に対応し、セキュリティリスクを低減
- 暗号化されたデータをインテリジェントで詳細なフォレンジックに変換することで、監査およびマネジメントのレビューを円滑化
- ネイティブの監査機能を使用せずにイベントを収集することにより、サーバ上でのパフォーマンスの低下を抑えてストレージリソースを節約
- GDPR、SOX、PCI DSS、HIPAA、FISMA、SAS 70を含む社内ポリシーおよび外部規制への確実なコンプライアンス準拠
- 数分程度でインストールでき、迅速なイベント収集でWindowsファイルサーバのアクティビティを即座に分析

すべての重要な変更を監査し、ユーザアクティビティを追跡

Change Auditor for Windows File Servers は、重要なWindowsファイルサーバのすべての変更について、広範囲でカスタマイズ可能な監査およびレポート作成機能を提供します。これには、ファイル/フォルダに関するユーザと管理者のアクティビティ、およびアクセス権限の変更も含まれます。また、リアルタイムの通知によって、重要な変更とセキュリティ違反の発生を把握できるため、場所とお使いのデバイスを問わず、どこからでも迅速に対応が可能です。

CHANGE AUDITOR THREAT DETECTIONによるプロアクティブな脅威検知

異常なアクティビティを分析して組織におけるユーザのリスクをランク付けすることにより、ユーザ脅威の検知を簡素化し、潜在的な脅威を識別すると同時に、誤検知アラートによるノイズを削減します。

意図しない変更から機密データを保護

Change Auditor for Windows File Servers は、重要なファイルおよびフォルダの変更および不注意による削除を防ぐことで、セキュリティリスクを低減します。このプロアクティブな方法によって、不審な行動また

は不正アクセスからWindowsファイルサーバを保護します。

無関係なデータを意味のある情報に変換してセキュリティとコンプライアンスを促進

Change Auditor for Windows File Servers は、ファイルおよびフォルダにおける重要な変更を追跡し、生データを意味のあるインテリジェントなデータに変換することで、インフラストラクチャのセキュリティとコンプライアンスを保護します。今や、Change Auditorのハイパフォーマンスな監査エンジンにより、監査上の制約は過去のものとなりました。暗号化されたネイティブ監査ログを必要とせずに、より短時間で結果が得られ、ストレージリソースも節約できます。

統合イベント転送

SIEMソリューションと簡単に統合でき、Change AuditorイベントをSplunkやArcSight、QRadarに転送できます。さらに、Change AuditorはQuest® InTrust®と統合して、20:1に圧縮されたイベントストレージおよび一元化されたネイティブまたはサードパーティのログ収集、アラート機能による解析と分析、および不審なイベントに対する自動応答アクションを実現します。

企業と政府の規制に合わせてレポート作成を自動化

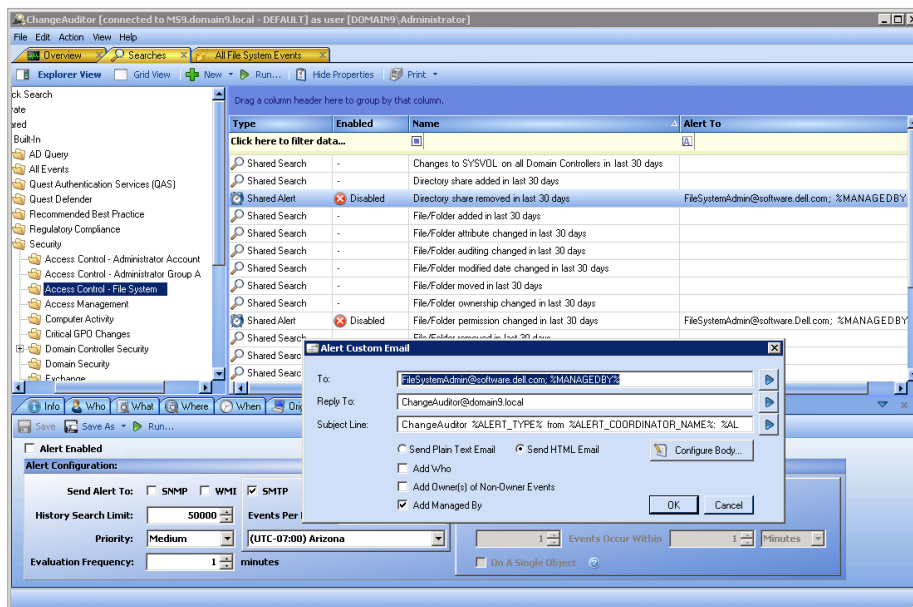
MicrosoftのSQL Server Reporting Servicesを利用して、Change Auditor for Windows File Serversでは、クリーンかつ理解可能で安全なコンプライアンスレポートの作成が即座に実現します。内蔵のコンプライアンスライブラリとカスタムレポート作成機能により、GDPR、SOX、PCI DSS、HIPAA、連邦情報セキュリティマネジメント法 (FISMA)、監査基準書No. 70 (SAS 70) などの規格に応じたコンプライアンスを即座に実現します。

QUESTについて

Questは、急速に変化するエンタープライズITの世界にソフトウェアソリューションを提供しています。データの爆発、クラウドサービスへの拡張、ハイブリッドデータセンター、セキュリティ脅威、規制上の要件によって生じる課題のシンプル化を支援します。Questのポートフォリオは、データベース管理、データ保護、統合エンドポイントの管理、IDおよびアクセス管理、Microsoftプラットフォーム管理などのソリューションで構成されます。

システム要件

システム要件の詳細な一覧については quest.com/products/change-auditor-for-windows-file-servers をご覧ください。



変更をリアルタイムに把握して監査に先手を打ちましょう。

Quest
quest.com/jp
世界各地のオフィスの情報については、
(quest.com/jp-ja/locations) をご覧ください

Quest, InTrust, およびQuestロゴは、Quest Software Inc. の商標または登録商標です。Questの商標の一覧については、www.quest.com/legal/trademark-information.aspx をご覧ください。その他すべての商標は各所有者に帰属します。

© 2019 Quest Software Inc. ALL RIGHTS RESERVED.
DataSheet-ChangeAuditor4WFS-US-KS-JA-WL-40818

Quest