



システムメンテナンスガイド

バージョン 11.0



連絡先情報

RSA Link(<https://community.rsa.com>) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/EMC-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、EMCが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サードパーティライセンス

この製品にはRSA以外のサードパーティによって開発されたソフトウェアが含まれます。本製品内のサードパーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、本使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

EMC Corporationは、この資料に記載される情報が、発行日時点で正確であるとみなしていません。予告なく変更される場合があります。

2月 2018

目次

NetWitness Suiteシステムメンテナンス	7
ベスト プラクティス	8
RSAが提供するポリシーを使用した資産の保護	8
ご使用の環境に合わせたポリシーを使用した資産の保護	8
ルールと通知の作成は慎重に	8
問題のトラブルシューティング	8
NetWitness Suiteのヘルスマニタの監視	9
.....	10
ポリシーの管理	10
ポリシーの追加	10
ポリシー例の追加	13
ポリシーの編集	15
ポリシーの複製	16
サービスまたはグループの割り当て	17
サービスまたはグループの削除	19
ルールの追加または編集	20
ルール条件列の非表示/表示	20
ルールの削除	21
ルールの抑制	22
ポリシーの抑制	22
メール通知の追加	22
メール通知の削除	23
デフォルトのメール件名を含める	23
システム統計の監視	25
システム統計のフィルタ	26
システム統計の履歴チャートの表示	29
サービス統計情報の監視	30
ゲージまたはチャートへの統計情報の追加	31
統計情報ゲージのプロパティの編集	33
タイムライン チャートのプロパティの編集	34
ホストとサービスの監視	36

[監視]ビューでのホストとサービスのフィルタ	37
ホストの詳細の監視	39
サービスの詳細の監視	40
イベントソースの監視	42
イベントソースモニタリングの構成	43
イベントソースのフィルタ	45
イベントソースでの収集イベントの履歴チャートの表示	46
アラームの監視	47
SNMPアラートを使用したヘルスマニタの監視	49
ヘルスマニタのトラブルシューティング	52
すべてのホストおよびサービスに共通する問題	52
インタフェースまたはログファイルのメッセージから特定される問題	52
ユーザインタフェースまたはログから特定できない問題	59
NetWitness Suiteでの更新の管理	62
システムログとサービスログの表示	63
システムログの表示	63
サービスログの表示	63
ログエントリーのフィルタ	64
ログエントリーの詳細を表示	64
Reporting Engineのログファイルへのアクセス	65
すべてのログファイル	65
Upstartログ	65
履歴ログの検索とエクスポート	66
URL統合を使用したクエリのメンテナンス	69
クエリの編集	69
クエリの削除	70
すべてのクエリのクリア	70
URIでのクエリの使用	71
FIPSサポート	73
Log CollectorでのFIPSのサポート	73
Log DecodersおよびDecoderでのFIPSのサポート	74
NetWitness Suiteのトラブルシューティング	75
デバッグ情報	75
NetWitness Suiteログファイル	75

関係するファイル	76
エラー通知	77
その他のヒント	78
管理者アカウントの保護	78
監査ログログメッセージ	78
NwConsoleによるチェック	79
シッククライアント エラー: リモート コンテンツ デバイス エントリーが見つからない	79
サンプルParserの入手	79
WinRMイベント ソースの構成	79
NwLogPlayer	79
使用方法	80
Feedのトラブルシューティング	81
概要	81
詳細	81
仕組み	81
Feedファイル	82
トラブルシューティング	82
参考情報	88
[ヘルス モニタ]ビュー	88
[ヘルス モニタ]ビュー: [アラーム]ビュー	88
[イベント ソース モニタリング]ビュー	92
[ヘルスモニタ]の[履歴チャート]	95
[ヘルスモニタの設定]ビュー: Archiver	99
[ヘルスモニタの設定]ビュー: イベント ソース	101
[ヘルスモニタの設定]ビュー: Warehouse Connector	107
[監視]ビュー	109
[監視]タブ	120
ESA Analyticsの詳細	122
稼働状態ステータス	122
[収集]タブ	126
[イベント処理]タブ	126
[ポリシー]ビュー	132
ヘルスモニタ デフォルトSMTPテンプレート	140

アラーム テンプレート	141
[システム統計ブラウザ]ビュー	152
[システム]ビュー:[システム]の[情報]パネル	155
[システム]の[更新]パネル-[設定]タブ	157
実行したいことは何ですか?	157
関連トピック	157
簡単な説明	157
機能	157
[システム ログ]:[設定]ビュー	158
実行したいことは何ですか?	158
関連トピック	159
簡単な説明	159
機能	159
[システム ログ]:[リアルタイム]タブ	161
実行したいことは何ですか?	161
関連トピック	161
簡単な説明	162
機能	163
[システム ログ]:[履歴]タブ	164
実行したいことは何ですか?	164
関連トピック	164
簡単な説明	165
機能	166
ログ エントリーの検索	167
ログ エントリーの詳細を表示	167

NetWitness Suiteシステムメンテナンス

このガイドでは、NetWitness Suite環境におけるホストとサービスの管理、ネットワークのメンテナンスと監視、ジョブの管理、パフォーマンスのチューニングなど、管理者が実行するメンテナンスタスクについて説明します。

次の図は、実行できるさまざまなシステムメンテナンスタスクを示しています。



次のトピックでは、これらのタスクについて説明します。

- [ベスト プラクティス](#)
- [NetWitness Suiteのヘルスマニタの監視](#)
- [システム ログとサービス ログの表示](#)
- [URL統合を使用したクエリのメンテナンス](#)
- [NetWitness Suiteでの更新の管理](#)
- [FIPSサポート](#)
- [NetWitness Suiteのトラブルシューティング](#)

ベスト プラクティス

RSAが提供するポリシーを使用した資産の保護

NetWitness Suiteに付属のRSAコアポリシーの目的は、(お客様の環境およびセキュリティポリシーに固有のルールを構成する前に) NetWitness Suite導入環境の資産をすぐに保護できるようにすることです。

これらのポリシーに、適切な資産管理責任者へのメール通知の設定をできるだけ早く行うことを推奨します。これにより、パフォーマンスや容量の閾値を超えたときにその管理責任者に通知が送信されるので、すぐに対処できます。

また、コアポリシーを評価して、固有のモニタリング要件に基づき、ポリシーを無効化するか、または、モニタリング対象のサービスまたはグループの割り当てを変更することを推奨します。

ご使用の環境に合わせたポリシーを使用した資産の保護

RSAコアポリシーは、汎用的であるため、環境によってはモニタリング対象範囲が十分でない可能性があります。一定の期間、RSAコアポリシーによって識別されない問題を集め、その問題を防ぐことができるルールを構成することをお勧めします。

ルールと通知の作成は慎重に

ルールとポリシーを実装する前に、可能な場合は各ルールとポリシーが必要であることを確認するようお勧めします。また、実装したポリシーの妥当性を定期的に検証することをお勧めします。無効なアラームとメール通知は、資産管理責任者の業務に悪影響を与える可能性があります。

問題のトラブルシューティング

ユーザ インタフェース、ホスト やサービスのログ ファイルでエラー メッセージを受信した場合は、「[ヘルスマニタのトラブルシューティング](#)」と「[NetWitness Suiteのトラブルシューティング](#)」を確認することをお勧めします。

NetWitness Suiteのヘルスマニタの監視

NetWitness Suiteのヘルスマニタ モジュールには、次の機能があります。

- すべてのホストとそこで実行されているサービスの最新の稼働状態を表示し、ホストの稼働状態をさまざまな角度から確認する。
- ホストとサービスのネットワーク環境を監視する。
- NetWitness Suiteに構成されているさまざまなイベント ソースの詳細を表示する。
- 選択されたホストのシステム統計情報を表示する(必要に応じてビューをフィルタリング可能)。

加えて、ArchiverモニタリングやWarehouse Connectorモニタリングの構成、ホストの統計情報の監視、システム ログを利用したNetWitness Suiteの監視を実行できます。

注: すべてのユーザにはデフォルトで、ヘルスマニタのインタフェース全体を参照する権限があります。AdministratorsロールとOperatorsロールのみが、デフォルトで[ポリシー]ビューを管理できます。NetWitness Suiteインタフェースのすべてのデフォルト権限のリストについては、「システムセキュリティとユーザ管理ガイド」の「ロールの権限」トピックを参照してください。

次の図は、NetWitness Suiteのユーザ インタフェースのヘルスマニタ モジュールとそのセクションを示しています。

Time	State	Severity	Rule Name	Service	Hostname	IP Address	Stat	Value
2017-09-13 10:06:40 AM	Active	Critical	Concentrator/Meta Rate Zero	Concentrator	nwappliance28765	10.31.125.172	Concentrator/Meta Rate (current)	0
2017-09-09 09:38:29 AM	Active	Critical	Log Decoder Capture Rate Zero	Log Decoder	nwappliance19848	10.31.125.173	Capture/Capture Packet Rate (current)	0
2017-09-09 09:34:36 AM	Active	Critical	ESA stopped aggregating	Event Stream Analysis	nwappliance7450	10.31.125.171	Workflow/NextGen/WorkUnit/ProcessingRate	0
2017-09-09 09:10:13 AM	Active	Critical	Broker Aggregation Stopped	Broker	nwappliance13731	10.31.125.170	Broker/Status	stopped
2017-09-09 09:10:13 AM	Active	High	Broker Session Rate Zero	Broker	nwappliance13731	10.31.125.170	Broker/Session Rate (current)	0
2017-09-26 07:00:57 AM	Cleared	Critical	ESA Service Stopped	Event Stream Analysis	nwappliance7450	10.31.125.171	ProcessInfo/Service Status	unknown
2017-09-19 08:31:25 PM	Cleared	Critical	Admin Server Stopped	Admin Server	nwappliance13731	10.31.125.170	ProcessInfo/Service Status	unknown
2017-09-19 02:53:49 AM	Cleared	Critical	Log Decoder Capture Not Started	Log Decoder	nwappliance19848	10.31.125.173	Capture/Capture Status	stopped
2017-09-14 09:30:14 AM	Cleared	Critical	ContextHub Service Stopped	ContextHub Server	nwappliance7450	10.31.125.171	ProcessInfo/Service Status	unknown
2017-09-09 09:38:29 AM	Cleared	Critical	Log Decoder Log Capture Pool Depleted	Log Decoder	nwappliance19848	10.31.125.173	Pool/Package Capture Queue	0
2017-09-09 09:34:32 AM	Cleared	Critical	Concentrator Aggregation Stopped	Concentrator	nwappliance28765	10.31.125.172	Concentrator/Status	stopped
2017-09-26 06:57:57 AM	Cleared	High	Custom Feeds Failure	NetWitness UI	nwappliance13731	10.31.125.170	Feeds/Custom Feeds Deployment Status	fail
2017-09-09 09:05:18 AM	Cleared	High	Admin Server in Unhealthy State	Admin Server	nwappliance13731	10.31.125.170	ProcessInfo/Overall Processing Status Indicator	PARTIALLY WOR...

ポリシーの管理


ポリシーには、ユーザが定義したものと、RSAが提供するものがあります。ポリシーでは、次の内容を定義します。

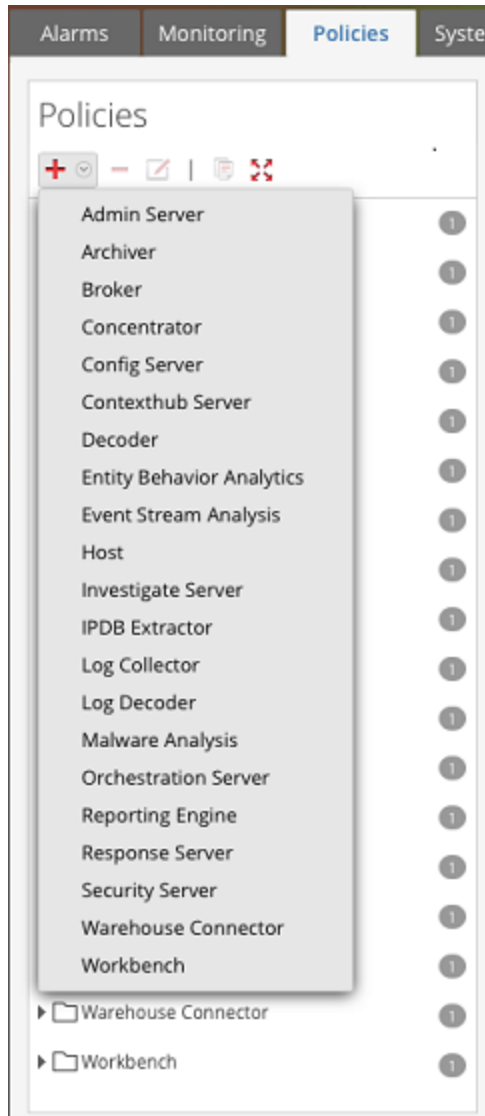
- ポリシーの適用対象とするサービスとホスト
- アラームを生成するルール(統計閾値により指定)
- ポリシーを抑制するタイミング
- アラームがトリガーされたときに通知する相手とそのタイミング。

関連する参照トピックとして、「[NetWitness Suiteの事前定義ポリシー](#)」を参照してください。

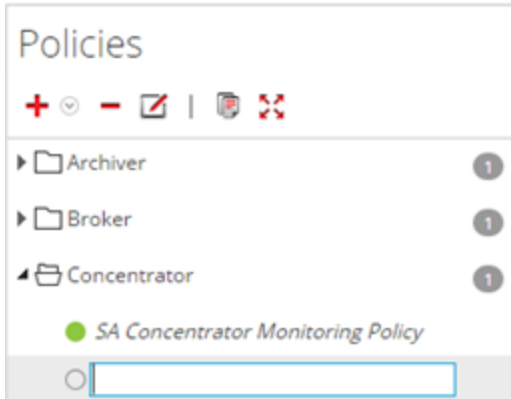
注: PKI(公開鍵基盤)証明書の期限切れステータスを通知するポリシーを構成できるようになりました。

ポリシーの追加

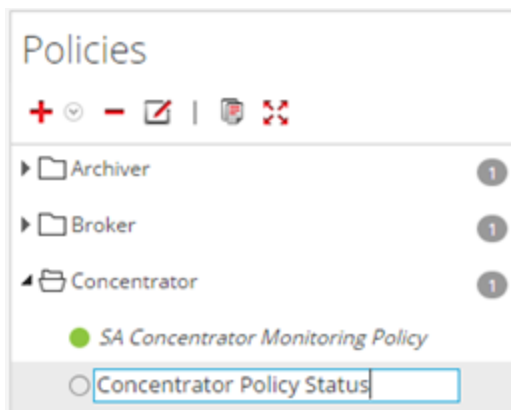
1. [管理]>[ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。
[ポリシー]ビューが表示されます。
3. [ポリシー]パネルで  をクリックします。
作成するポリシーの監視対象に指定できるホストとサービスの一覧が表示されます。



4. ホストまたはサービス(たとえばConcentrator)を選択します。
PKIポリシーに対しては、ホスト(たとえばHost)を選択する必要があります。
[ポリシー]パネルに選択したホストまたはサービスが表示され、ポリシー詳細パネルには空のポリシーが表示されます。



5. [ポリシー] パネルでポリシーの名前 (たとえば **Concentrator Policy Status**) を入力します。



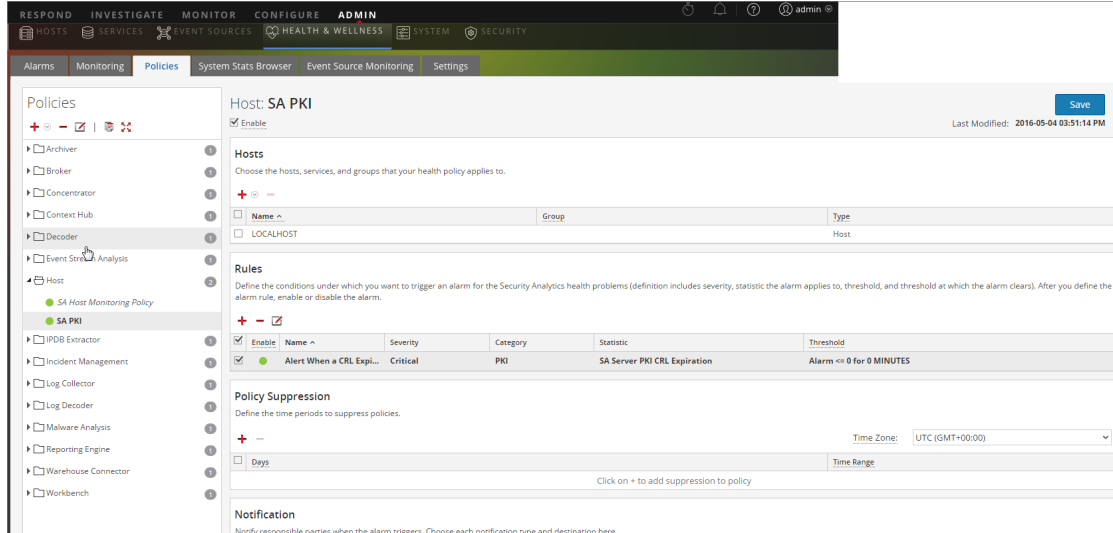
入力した名前 (たとえば **Concentrator Policy Status**) がポリシー詳細パネルにポリシー名として表示されます。

6. ポリシー詳細パネルで、次のようにしてポリシーを作成します。
 - a. [有効化] チェックボックスを選択します。
 - b. 稼働状態の統計を監視するサービス (この例では、Concentrator 上で稼働するサービス) を追加します。
PKI ポリシーに対しては、稼働状態の統計を監視するために LOCALHOST を選択する必要があります。
 - c. ポリシーに構成するルール条件を追加します。
 - d. ポリシーの適用を抑制する期間を指定します。
 - e. ポリシーに関するメール通知が必要な場合は追加します。
 - f. ポリシー詳細パネルで [保存] をクリックします。
ポリシーが追加されます。

ポリシー例の追加

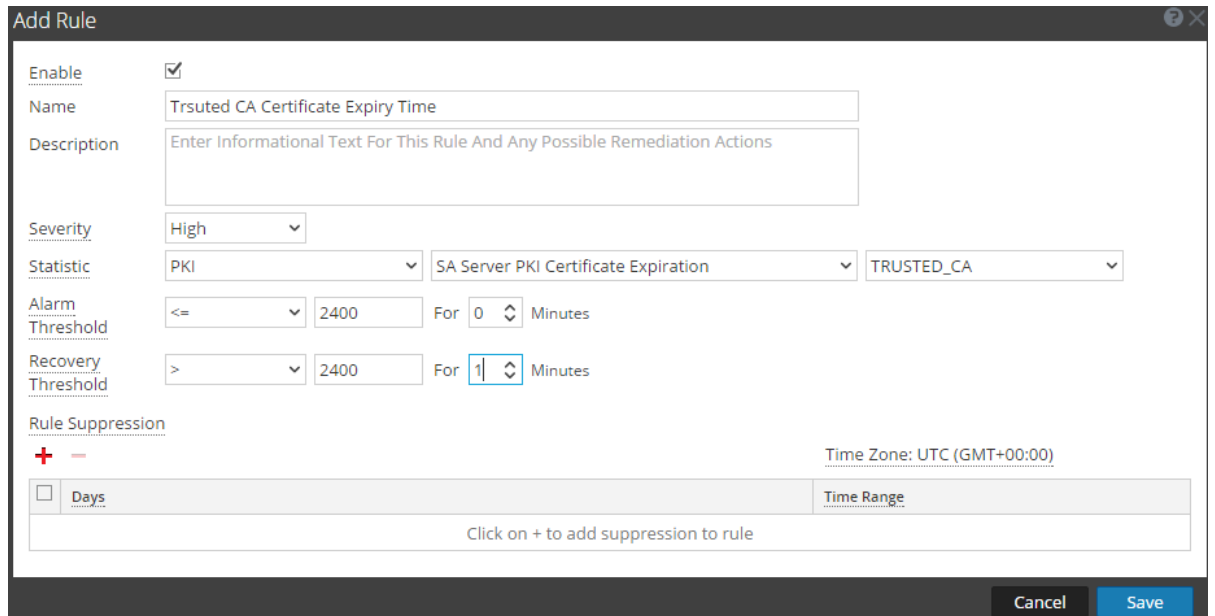
PKIポリシーの構成は大まかには以下ようになります。

1. 新しいPKIポリシーを追加します。



2. 統計情報に関するルールを追加します。

- CAの有効期限



- CRLの有効期限

Add Rule

Enable

Name CRL Expiration Based On Time

Description Enter Informational Text For This Rule And Any Possible Remediation Actions

Severity High

Statistic PKI SA Server PKI CRL Expiration

Alarm Threshold <= 2400 For 0 Minutes

Recovery Threshold > 1 For 1 Minutes

Rule Suppression

Days Time Range Time Zone: UTC (GMT+00:00)

Click on + to add suppression to rule

Cancel Save

- CRLのステータス

Add Rule

Enable

Name CRL Status

Description Enter Informational Text For This Rule And Any Possible Remediation Actions

Severity High

Statistic PKI SA Server PKI CRL Status

Alarm Threshold != Valid For 0 Minutes

Recovery Threshold = Valid For 1 Minutes

Rule Suppression

Days Time Range Time Zone: UTC (GMT+00:00)

Click on + to add suppression to rule

Cancel Save

- サーバ証明書の有効期限

Add Rule

Enable

Name Server Certificate Expiry Time

Description Enter Informational Text For This Rule And Any Possible Remediation Actions

Severity High

Statistic PKI SA Server PKI Certificate Expiration SERVER_CERT

Alarm Threshold <= 2400 For 0 Minutes

Recovery Threshold > 2400 For 1 Minutes


Rule Suppression

+ - Time Zone: UTC (GMT+00:00)

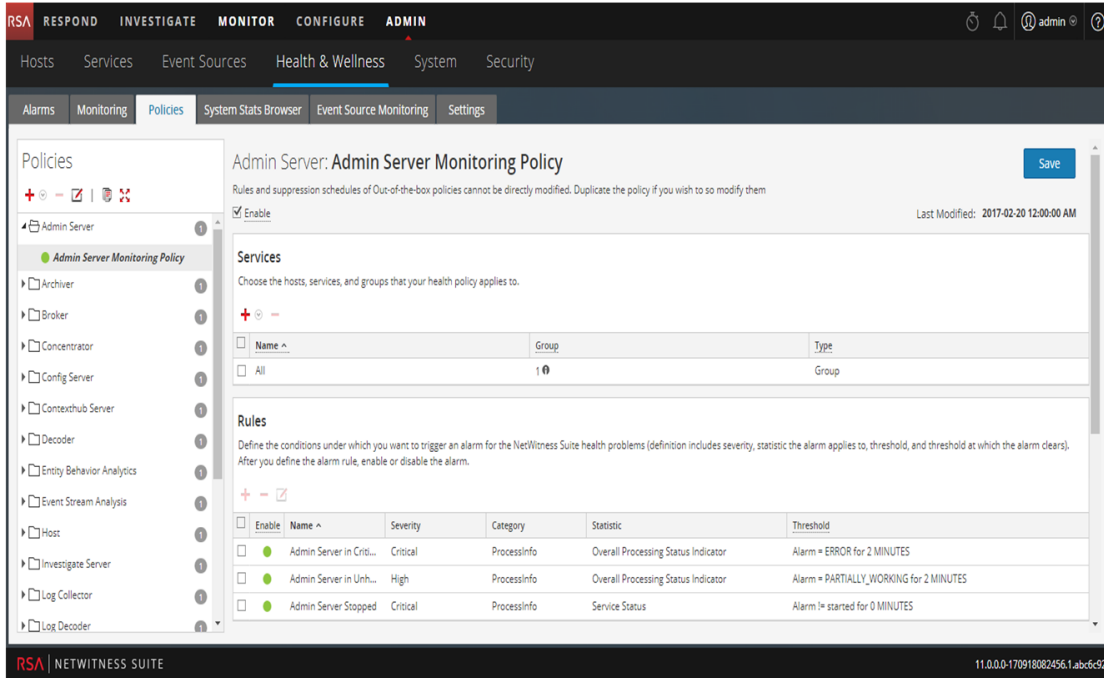
Days	Time Range
Click on + to add suppression to rule	

Cancel Save

ポリシーの編集

1. [管理] > [ヘルスマニタ]に移動します。
2. [ポリシー] タブをクリックします。
[ポリシー]ビューが表示されます。
3. ホストまたはサービスの下でポリシー(たとえばConcentrator Policy Status)を選択します。
ポリシーの詳細が表示されます。
4. をクリックします。


ポリシーの名前(たとえばAdmin Server Monitoring Policy)とポリシー詳細パネルが編集可能になります。

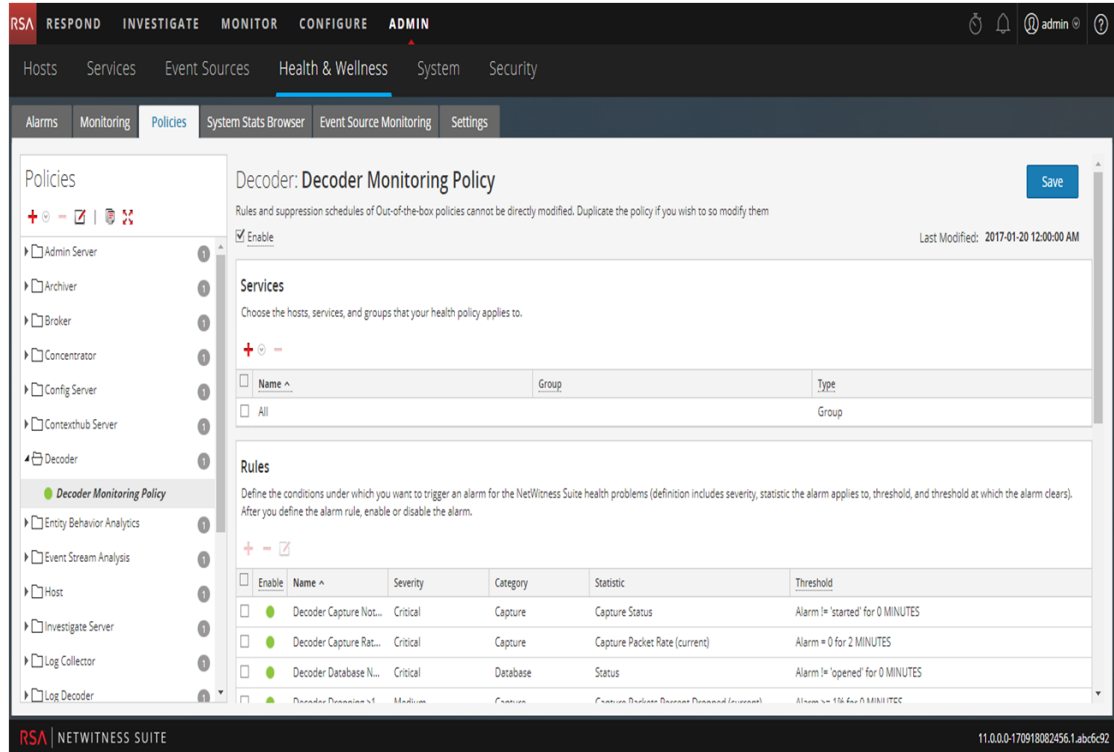



5. ポリシー詳細パネルで必要な変更を加えて、[保存]をクリックします。次の操作を実行できます。
 - ポリシー名を編集する。
 - ポリシーを有効化または無効化する。
 - ポリシーでホストおよびサービスを追加または削除する。
 - ポリシーでルールを追加、削除、変更する。
 - ポリシーで抑制を追加/編集/削除する。
 - ポリシーで通知を追加/編集/削除する。

注：[保存]をクリックすると、有効化/無効化の選択に基づいてポリシールールが適用されます。また、変更されたルールのルール条件タイマーとポリシー全体がリセットされます。

ポリシーの複製

1. [管理] > [ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。
3. ホストまたはサービスの下でポリシー(たとえばConcentrator Policy Status)を選択します。
4.  をクリックします。NetWitness Suiteによってポリシーがコピーされ、元のポリシー名に(1)を付加した名前が表示されます。




5.  をクリックし、ポリシーの名前を変更します (たとえば、**Decoder Monitoring Policy(1)** を **New Concentrator Policy Status** に変更します)。

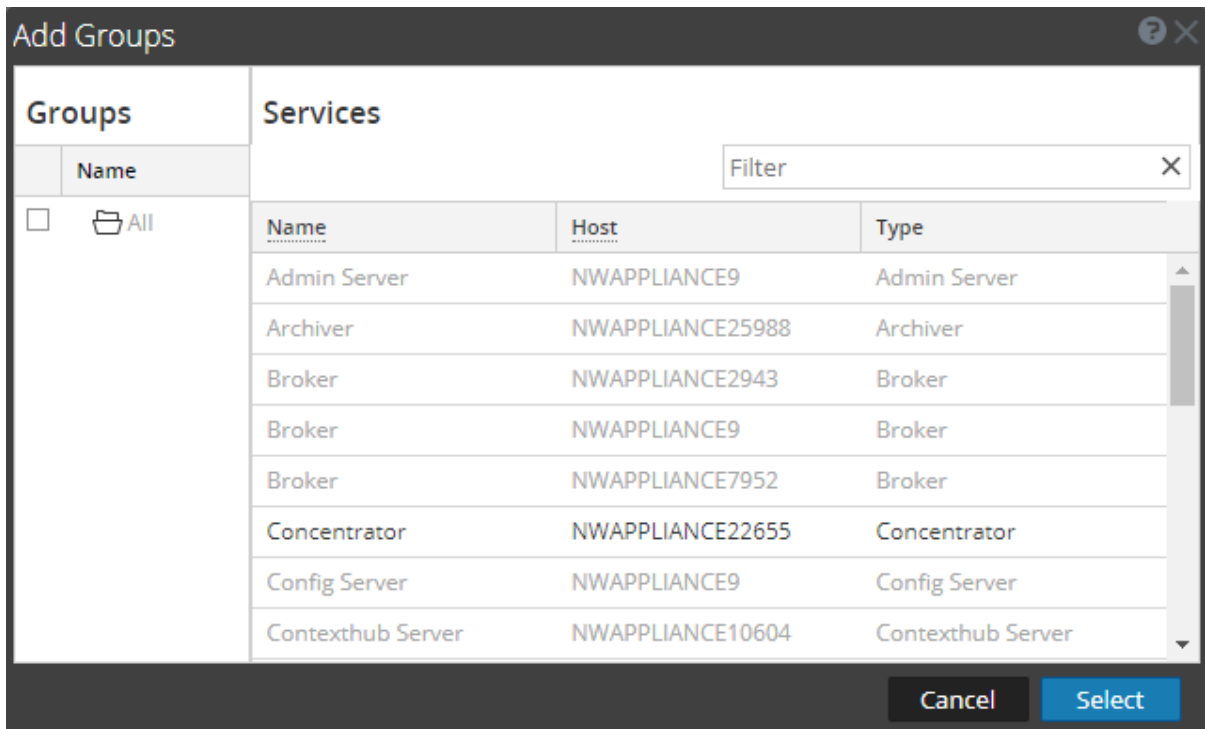
注: 複製したポリシーはデフォルトで無効化され、ホストとサービスの割り当ては複製されません。複製したポリシーを使用して NetWitness Suite インフラストラクチャの正常稼働状態を監視する前に、関連するホストとサービスをそのポリシーに割り当てます。

サービスまたはグループの割り当て

ホストまたはサービスをポリシーに割り当てるには、次の手順を実行します。

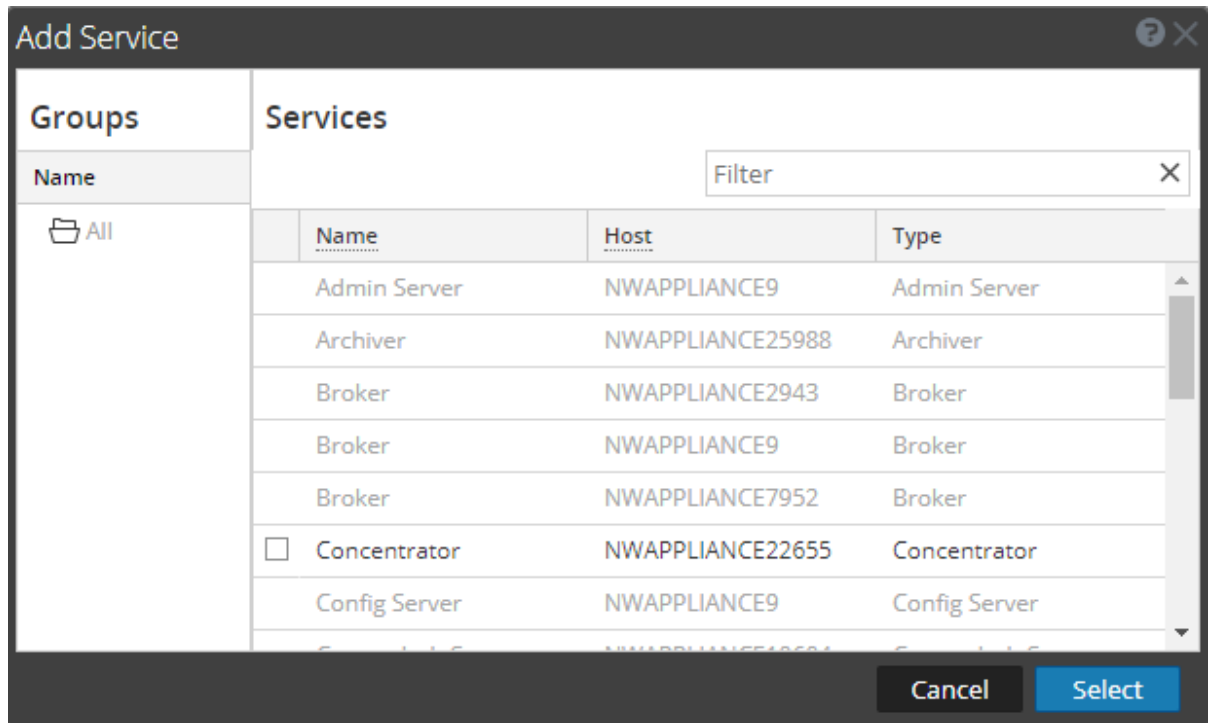
1. [管理] > [ヘルスマニタ] に移動します。
2. [ポリシー] タブをクリックします。
[ポリシー] ビューが表示されます。
3. ホストまたはサービスの下でポリシー (たとえば第 1 ポリシー) を選択します。
ポリシーの詳細が表示されます。
4. [サービス] セクションのツールバーで  をクリックします。
5. 次のいずれかのアクションを選択してください。

- ホストの場合は、選択メニューから[グループ]または[ホスト]を選択します。
 - サービスの場合は、選択メニューから[グループ]または[サービス]を選択します。
6. サービスまたはグループのどちらを割り当てたかにより、次のいずれかのアクションを実行します。
- [グループ]を選択した場合は、表示される[追加グループ]ダイアログで、既存のホストまたはサービスのグループを選択します。



- [サービス]を選択した場合は、表示される[追加 サービス]ダイアログで、個々のサービ

スを選択します。




7. ポリシーに割り当てるグループまたはサービスの横にあるチェックボックスを選択して、ダイアログの[選択]をクリックし、ポリシー詳細パネルで[保存]をクリックします。

注: ポリシーのタイプに基づいて、選択可能なサービスがフィルタされます。たとえば、Concentratorタイプのポリシーの場合は、Concentratorサービスのみを選択できます。

サービスまたはグループの削除

ポリシーからホストまたはサービスを削除するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。
[ポリシー]ビューが表示されます。
3. サービスの下でポリシーを選択します。
ポリシーの詳細が表示されます。
4. ホストまたはサービスを選択します。
5.  をクリックします。
選択したホストまたはサービスがポリシーから削除されます。

ルールの追加または編集

ポリシーにルールを追加するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。
[ポリシー]ビューが表示されます。
3. ホストまたはサービスの下でポリシー(たとえばCheckpoint)を選択します。
ポリシーの詳細が表示されます。
4. 既存のルールを追加するか、またはルールを追加するかによって、次を実行します。
 - 追加するには、[ルール]セクションのツールバーで+をクリックします。
 - 編集するには、[ルール]リストからルールを選択し、✎をクリックします。
5. ダイアログに必要な値を入力して、ルールを定義または更新します。
6. 次の例に示すように、[説明]フィールドが追加されています。

7. [OK]をクリックします。
ルールがポリシーに追加(または更新)されます。

ルール条件列の非表示/表示

[ルール]パネルでルール条件の列を表示または非表示にするには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。
[ポリシー]ビューが表示されます。
3. サービスの下でポリシーを選択します。
ポリシーの詳細が表示されます。
4. [ルール]パネルに移動します。

Rules

Define the conditions under which you want to trigger an alarm for the NetWitness Suite health problems (definition includes severity, statistic the alarm applies to, threshold, and threshold at which the alarm clears). After you define the alarm rule, enable or disable the alarm.

+ -

<input type="checkbox"/>	Enable	Name ^	Severity	Category	Statistic	Threshold
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	Medium	Concentrator	Queries Pending	Alarm >= 5 for 10 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	Medium	Devices	Sessions Behind	Alarm >= 100000 for 30 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	High	Devices	Sessions Behind	Alarm >= 1000000 for 30 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	Critical	Devices	Sessions Behind	Alarm >= 50000000 for 30 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	Critical	Concentrator	Status	Alarm != 'started' for 0 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	Critical	Database	Status	Alarm != 'opened' for 0 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	High	Concentrator	Rule Error Count	Alarm > 0 for 0 MINUTES
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Concentrator...	Critical	Concentrator	Meta Base (urgent)	Alarm = 0 for 2 MINUTES

5. [カテゴリ]の右の[v]をクリックして、[列]を選択し、[統計]および[閾値]のチェックボックスをオフにします。

ルールの一覧での列の表示と非表示は、チェックボックスをオンまたはオフにすることによって切り替えることができます。

[ルール]パネルがルール条件なしで表示されます。

ルールの削除

ポリシーからホストまたはサービスを削除するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。
[ポリシー]ビューが表示されます。
3. サービスの下でポリシーを選択します。
ポリシーの詳細が表示されます。
4. [ルール]リストからルール(たとえばCheckpoint)を選択します。
5. をクリックします。
選択したルールがポリシーから削除されます。

ルールの抑制

1. [ポリシー]タブをクリックします。
[ポリシー]ビューが表示されます。
2. サービスの下でポリシーを選択します。
ポリシーの詳細が表示されます。ルールを抑制する時間の範囲は、ルールを最初に追加するとき、またはルールを編集するときに指定できます。
3. ルールを追加または編集します。
4. [ルールの追加]または[ルールの編集]ダイアログの[ルール抑制]パネルで、ルールを抑制する曜日と時刻の範囲を指定します。

ポリシーの抑制

1. ポリシーを追加または編集します。
[ポリシー]ビューが表示されます。
2. [ポリシーの抑制]パネルで次の操作を行います。
 - a. [タイムゾーン]ドロップダウンリストからタイムゾーンを選択します。
このタイムゾーンはポリシー全体(ポリシー抑制とルール抑制の両方)に適用されます。
 - b. ツールバーの+をクリックします。
 - c. ポリシーを抑制する曜日と時刻の範囲を指定します。

メール通知の追加

ポリシーにメール通知を追加するには、次の手順を実行します。


1. ポリシーを追加または編集します。
[ポリシー]ビューが表示されます。
2. [通知]パネルで次の操作を行います。
 - a. ツールバーの+をクリックします。
空白のメール通知行が表示されます。
 - b. メールに関する以下の設定を選択します。
 - [受信者]列で通知タイプを選択します(このドロップダウンリストの値のソースについては、「*NetWitness Suite*システム構成ガイド」の「通知出力の構成」を参照してください)。

- [通知サーバ]列で通知サーバを選択します(このドロップダウンリストの値のソースについては、「*NetWitness Suite*システム構成ガイド」の「**通知サーバの構成**」を参照してください)。
- [テンプレート]列でテンプレートサーバを選択します(このドロップダウンリストの値のソースについては、「*NetWitness Suite*システム構成ガイド」の「**通知テンプレートの構成**」を参照してください)。

注: 指定した受信者へのヘルスマニタメール通知に、ヘルスマニタテンプレートのデフォルトのメール件名を追加する場合は、「**デフォルトのメール件名を含める**」を参照してください。

メール通知の削除

ポリシーにメール通知を追加するには、次の手順を実行します。

1. ポリシーを追加または編集します。
[ポリシー]ビューが表示されます。
2. [通知]パネルで次の操作を行います。
 - a. メール通知を選択します。
 - b.  をクリックします。
選択した通知が削除されます。

デフォルトのメール件名を含める

ポリシーに設定した通知によって生成されるメールには、ヘルスマニタのデフォルトのメール通知テンプレートから件名が取り込まれません。件名が取り込まれない場合には、件名を指定する必要があります。この処理手順では件名をテンプレートに挿入する方法について説明します。関連するトピックとして、「[\[ポリシー\]ビュー](#)」および「[NetWitness Suiteの事前定義ポリシー](#)」を参照してください。

メール通知にヘルスマニタのメールテンプレートの件名を追加するには、次の手順を実行します。

1. [管理]>[システム]に移動します。
2. [オプション]パネルで、[グローバル通知]を選択します。
3. ヘルスマニタのメールテンプレート(Health & Wellness Default SMTP Templateなど)を選択します。

The screenshot shows the 'Global Notifications' section in the Admin console, specifically the 'Templates' tab. A table lists 12 templates. The 'Health & Wellness Default SMTP Template' is highlighted in blue. The table has columns for Name, Template Type, Description, and Actions. The status bar at the bottom indicates 'Displaying 1 - 12 of 12 templates'.

Name	Template Type	Description	Actions
Default Audit CEF Template	Audit Logging	Default Audit CEF Template	[Settings]
Default Audit Human-Readable Format	Audit Logging	Default Audit Human-Readable Format	[Settings]
Default SMTP Template	Event Stream Analysis	Default SMTP Template	[Settings]
Default SNMP Template	Event Stream Analysis	Default SNMP Template	[Settings]
Default Script Template	Event Stream Analysis	System default FreeMarker template for Script notifications	[Settings]
Default Syslog Template	Event Stream Analysis	Default Syslog Template	[Settings]
ESM Default Email Template	Event Source Monitoring	ESM Default Email Template	[Settings]
ESM Default SNMP Template	Event Source Monitoring	ESM Default SNMP Template	[Settings]
ESM Default Syslog Template	Event Source Monitoring	ESM Default Syslog Template	[Settings]
Health & Wellness Default SMTP Template	Health Alarms	Health & Wellness Default SMTP Template	[Settings]

[テンプレートの定義]ダイアログが表示されます。


4. をクリックし、[テンプレート]フィールドで、件名をバッファにコピーします(件名をハイライト表示してCtrl-Cを押します)。

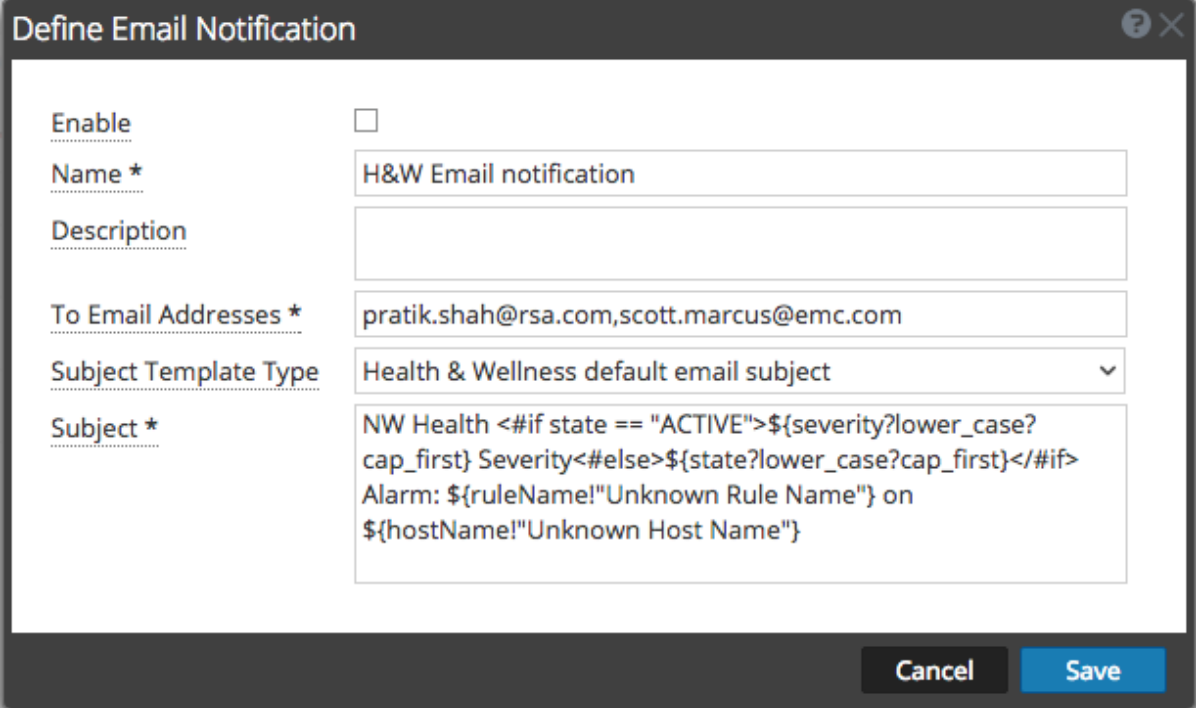
The 'Define Template' dialog box shows the following fields:

- Name *: Health & Wellness Default SMTP Template
- Template Type: Health Alarms
- Description: Health & Wellness Default SMTP Template
- Template *:


```
<html>
<!--
  // RECOMMEND: Use this line from the template as the Email Subject line
  when defining Notification Type
  NW Health <#if state == "ACTIVE">${severity?lower_case?cap_first}
  Severity<#else>${state?lower_case?cap_first}</#if> Alarm:
  ${ruleName!"Unknown Rule Name"} on ${hostName!"Unknown Host Name"}
-->
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
</head>
<body bgcolor="#e0e0e0" leftmargin="0" topmargin="0" marginwidth="0"
marginheight="0">
<table border="0" cellpadding="0" cellspacing="0" height="100%"
width="100%" id="bodyTable">
```

Buttons: Cancel, Save

5. [キャンセル]をクリックして、テンプレートを閉じます。
6. [出力]タブをクリックして、通知を選択します(たとえば[ヘルスマニタ])。
7. をクリックします。
[メール通知の定義]ダイアログが表示されます。
8. [件名]フィールドのテキストボックスの値をバッファー内の件名に置き換えます(既存のテキストをハイライト表示して、Ctl-Vを押します)。



The image shows a 'Define Email Notification' dialog box with the following fields and values:

- Enable:**
- Name *:** H&W Email notification
- Description:** (empty)
- To Email Addresses *:** pratik.shah@rsa.com,scott.marcus@emc.com
- Subject Template Type:** Health & Wellness default email subject
- Subject *:** NW Health <#if state == "ACTIVE">\${severity?lower_case?cap_first} Severity<#else>\${state?lower_case?cap_first}</#if> Alarm: \${ruleName!"Unknown Rule Name"} on \${hostName!"Unknown Host Name"}

Buttons: Cancel, Save

9. [保存]をクリックします。

システム統計の監視

[システム統計ブラウザ]では、ホスト、ホストで実行されているコンポーネント、統計カテゴリ、個別の統計を選択するか、またはホスト、コンポーネント、カテゴリ、統計の任意の組み合わせによって表示する統計情報をフィルタします。情報を表示する順序も選択できます。

システム統計ブラウザにアクセスするには、次の手順を実行します。

1. [管理]>[ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [システム統計ブラウザ]タブをクリックします。

[システム統計ブラウザ]タブが表示されます。

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
nwappliance13731	Admin Server	Health Checks	Configuration.Server-Connection		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Configuration.Update-Status		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Process.Jvm.Memory-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Process.Modules.Module-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Security.Pki.Certificate-Health		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Transport.Bus.Subscription.Config-Server-Nostic...		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Health Checks	Transport.Bus.Subscription.Rsa-Contexthub-Agy...		Healthy	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process	Mode		Normal	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process	Status		Running	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process Jvm	Memory Total Max		7.86 GB	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Process Jvm	Memory Total Used		515.56 MB	2017-09-30 05:51:52 A...	
nwappliance13731	Admin Server	Processinfo	Build Date		2017-Sep-06 21:47:03	2017-09-30 05:51:51 A...	
nwappliance13731	Admin Server	Processinfo	CPU Utilization		0.1%	2017-09-30 05:52:41 A...	
nwappliance13731	Admin Server	Processinfo	Maximum Memory		31.42 GB	2017-09-30 05:52:41 A...	
nwappliance13731	Admin Server	Processinfo	Memory Utilization		741.16 MB	2017-09-30 05:52:41 A...	

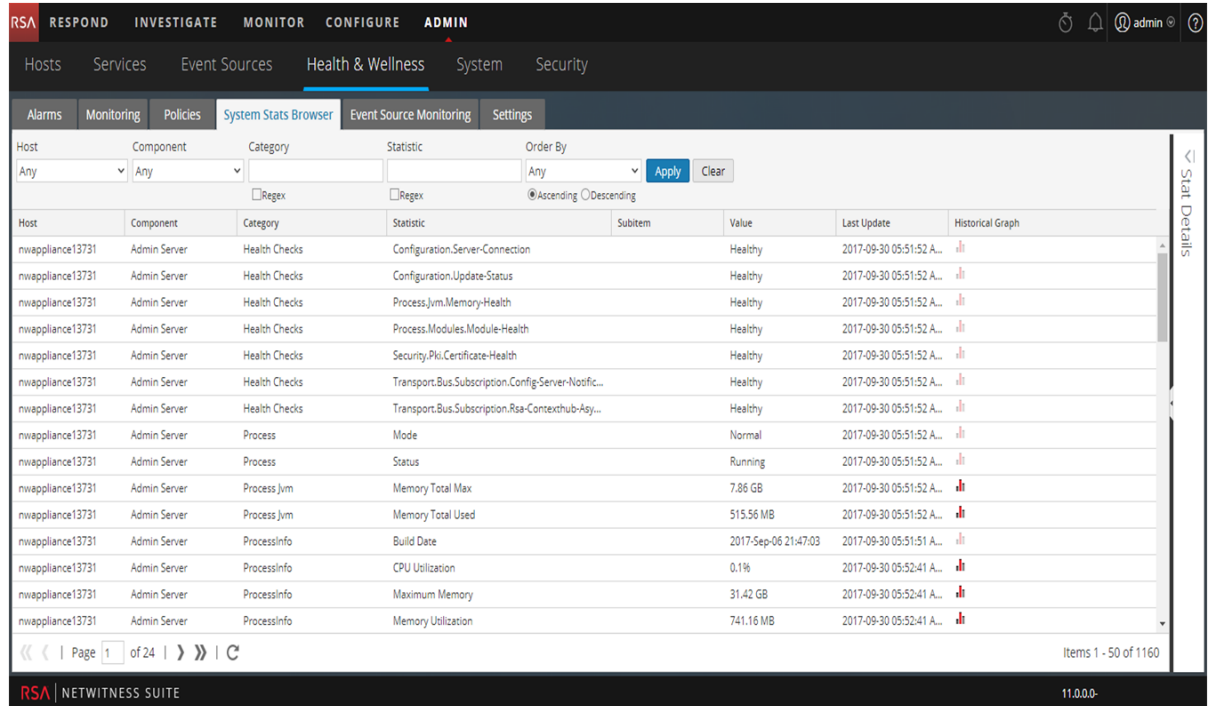
システム統計のフィルタ

システム統計は次のいずれかの方法でフィルタして監視することができます。

- 特定のホストで収集された統計
- 特定のコンポーネントで収集された統計
- 特定のタイプまたは特定のカテゴリに属する統計
- 選択した基準で統計をソート

システム統計のリストをフィルタする方法

1. [管理]>[ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [システム統計ブラウザ]をクリックします。
[システム統計ブラウザ]タブが表示されます。



システム統計のリストを次のいずれかの方法でフィルタします。

- 特定のホストのシステム統計を表示するには、[ホスト]ドロップダウン リストからホストを選択します。
選択したホストのシステム統計が表示されます。
- 特定のコンポーネントのシステム統計を表示するには、[コンポーネント]ドロップダウン リストからコンポーネントを選択します。
選択したコンポーネントのシステム統計が表示されます。
- 特定のカテゴリのシステム統計を表示するには、[カテゴリ]フィールドでカテゴリの名前を入力します。
[Regex]を選択すると、Regexフィルタが有効になります。このフィルタを有効にすると、テキストの正規表現検索が実行され、一致するカテゴリがリストされます。[Regex]を選択しない場合は、グローピングパターン マッチがサポートされます。
選択したカテゴリのシステム統計が表示されます。
- 統計のリストをソートするには、[OrderBy]列で順序を設定します。
- 全ホストから特定の統計を表示するには、[統計]フィールドに統計の名前を入力します。
[Regex]を選択すると、Regexフィルタが有効になります。このフィルタを有効にすると、テキストの正規表現検索が実行され、一致するカテゴリがリストされます。[Regex]を選択しない場合は、グローピングパターン マッチがサポートされます。
選択した統計のシステム統計が表示されます。

次の図は、NWAPPLIANCE10604ホストでフィルタし、統計カテゴリの降順でリストされた

システム統計ブラウザを示しています。

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
localhost.localdomain	Event Stream Analysis	JVM.Memory	Used Non-heap Memory Usage		90.83 MB	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Used Heap Memory Usage		492.83 MB	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Maximum Non-heap Memory Usage		-1 bytes	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Maximum Heap Memory Usage		64.00 GB	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Initial Non-heap Memory Usage		2.44 MB	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Initial Heap Memory Usage		8.00 GB	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Committed Non-heap Memory Usage		92.00 MB	2017-05-17 07:21:38 P...	
localhost.localdomain	Event Stream Analysis	JVM.Memory	Committed Heap Memory Usage		8.00 GB	2017-05-17 07:21:38 P...	

3. 個々の統計の詳細を表示するには、次の手順を実行します。
 - a. 行を選択して統計を選択します。
 - b. をクリックします。
[統計の詳細]が表示されます。


Stat Details	
Host	14e55a22-12ba-4af2-a376-80a2ebe49993
Hostname	NWAPPLIANCE10604
Component ID	appliance
Component	Host
Name	Mounted Filesystem Disk Usage
Subitem	/dev/shm
Path	
Plugin	appliance_df
Plugin Instance	dev_shm
Type	fs_usage
Type Instance	
Description	Disk usage information for mounted filesystem /dev/shm
Category	FileSystem
Last Updated Time	2017-07-14 03:11:18 PM
Value	15.71 GB size, 12.00 KB used, 15.71 GB available
Raw Value	1.686945792E10 bytes size, 12288.0 bytes used, 1.6869445632E10 bytes available
Graph Data Key	14e55a22-12ba-4af2-a376-80a2ebe49993/appliance_df-dev_shm/fs_usage
Stat Key	14e55a22-12ba-4af2-a376-80a2ebe49993/appliance_df-dev_shm/fs_usage
stat_collector_version	11.0.0.0
Filesystem	tmpfs

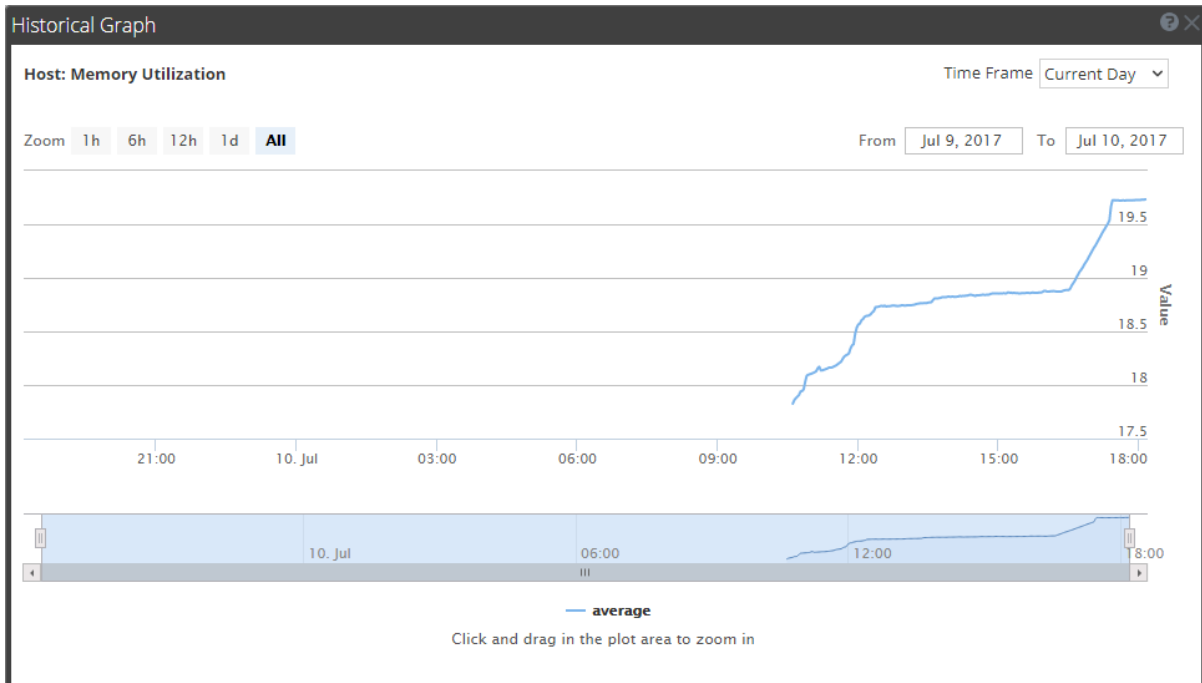
[ADMIN] > [ヘルスマニタ] > [システム統計ブラウザ]ビューのさまざまなパラメータや説明については、「[\[システム統計ブラウザ\]ビュー](#)」を参照してください。

システム統計の履歴チャートの表示

収集したシステム統計の履歴チャートには、選択した時間範囲にわたる各種の統計に関する情報が表示されます。

履歴チャートを表示するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [システム統計ブラウザ]タブをクリックします。
3. [システム統計ブラウザ]タブで、目的の統計を表示するためのフィルタ基準を指定します。
4. [履歴チャート]列で、を選択します。
選択した統計の履歴チャートが表示されます。
次の図は、ホストのメモリ利用率統計の履歴チャートの例を示しています。



このチャートは、今日1日の統計を表示し、1時間(10時15分～11時15分)の値をズームイン表示するようにカスタマイズされています。チャートにポインタを合わせると、特定の時点での詳細が表示されます。たとえば、この図では、11時00分のメモリ使用率が表示されています。

注: [時間範囲]および[日付範囲]を選択することにより、チャート表示をカスタマイズできます。値のズームインや時間範囲を設定できるほか、プロット領域をクリックしてドラッグすることにより、チャートをズーム表示できます。表示のカスタマイズやズームイン機能の詳細については、「[システム統計の履歴チャート](#)」を参照してください。グラフの切れ目や隙間は、サービスまたはホストがその時間停止していたことを示します。

サービス統計情報の監視

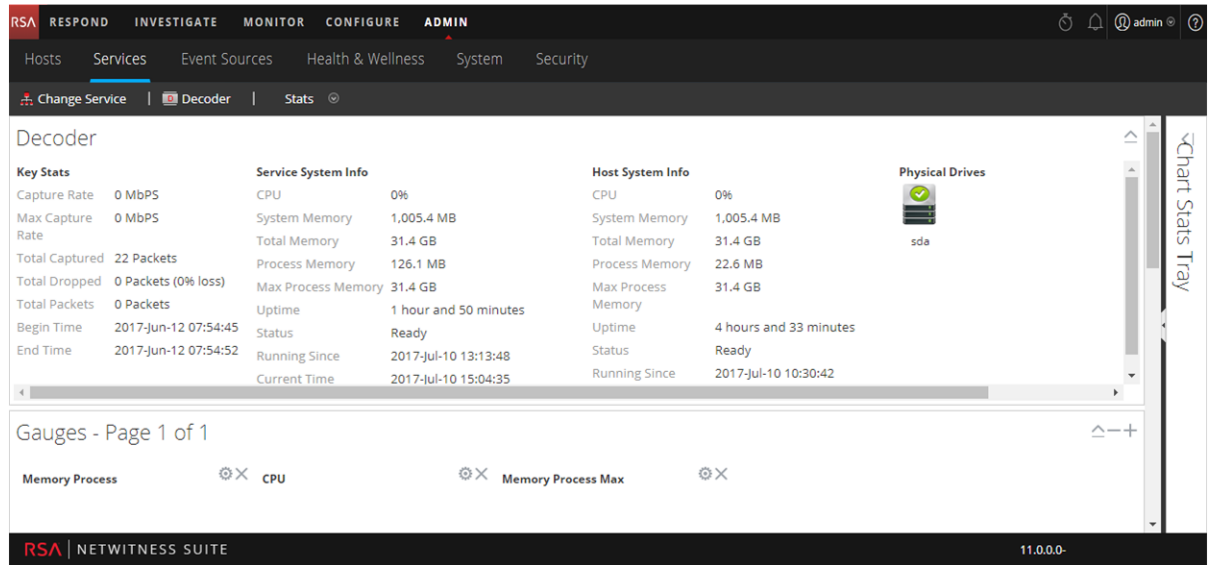
NetWitness Suiteには、サービスのステータスや動作を監視する方法が用意されています。[サービス]の[統計]ビューには、収集状況、サービスのシステム情報、デバイスが稼働しているホストのシステム情報が表示されます。さらに、80個を超える統計をゲージやタイムラインチャートで表示できます。セッションサイズ、セッション、パケットの統計情報については、履歴タイムラインチャートで表示できます。

サービスのタイプに応じて利用できる統計情報は異なりますが、特定の要素はすべてのコアデバイスに共通です。

NetWitness Suiteでサービス統計情報を監視するには、次の手順を実行します。

1. [管理]>[サービス]に移動します。
[サービス]ビューが表示されます。

2. サービスを選択し、[アクション]列で[表示]>[統計]を選択します。




3. ビューをカスタマイズするには、次の手順を実行します。チャートを折りたたむか、展開します。たとえば、[統計チャートトレイ]を展開すると、利用可能なチャートが表示されます。セクションを上下にドラッグして、順序を変更します。たとえば、[ゲージ]セクションを一番上にドラッグして、[サマリ統計]セクションの上に配置できます。

ゲージまたはチャートへの統計情報の追加

[サービス]の[統計]ビューでは、サービスごとに、監視する統計情報をカスタマイズすることができます。[統計チャートトレイ]には、サービスで利用可能なすべての統計情報が一覧表示されます。統計情報は、監視されるサービスのタイプに応じて異なります。[統計チャートトレイ]内の統計情報は、ゲージまたはタイムラインチャートで表示できます。セッションサイズ、セッション、パケットの統計情報については、履歴タイムラインチャートで表示できます。

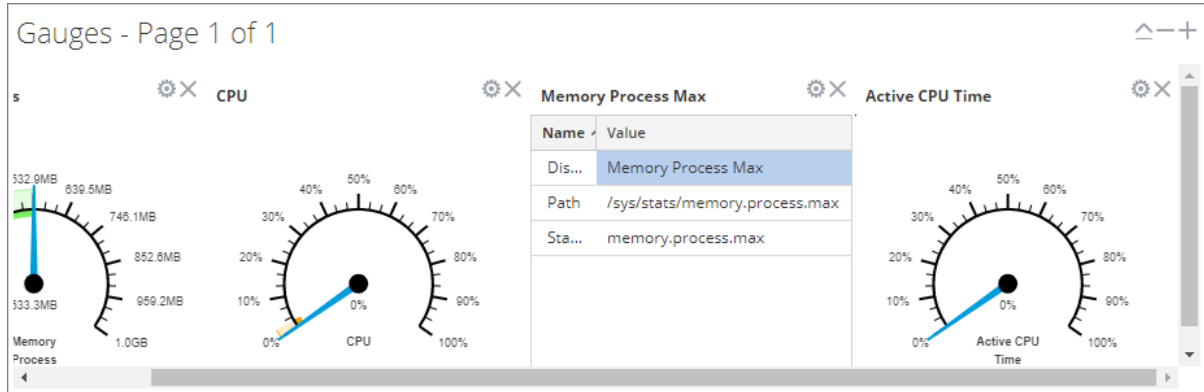
統計情報のゲージの作成

[サービス]の[統計]ビューで統計情報のゲージを作成するには、次の手順を実行します。

1. [管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、[アクション]列で[表示]>[統計]を選択します。
右側に統計チャートトレイが表示されます。
3. トレイが折りたたまれている場合、をクリックすると、使用可能な統計情報のリストが表示されます。
4. [統計チャートトレイ]から、任意の統計情報をクリックし、[ゲージ]セクションにドラッグしま

す。

統計情報のゲージが作成されます。ゲージのスペースがない場合は、[ゲージ]セクションに新しいページが作成され、新しいページにゲージが追加されます。下の例では、[統計チャートトレイ]からドラッグすることによって、[ゲージ]セクションにActive CPU Timeチャートが追加されています。

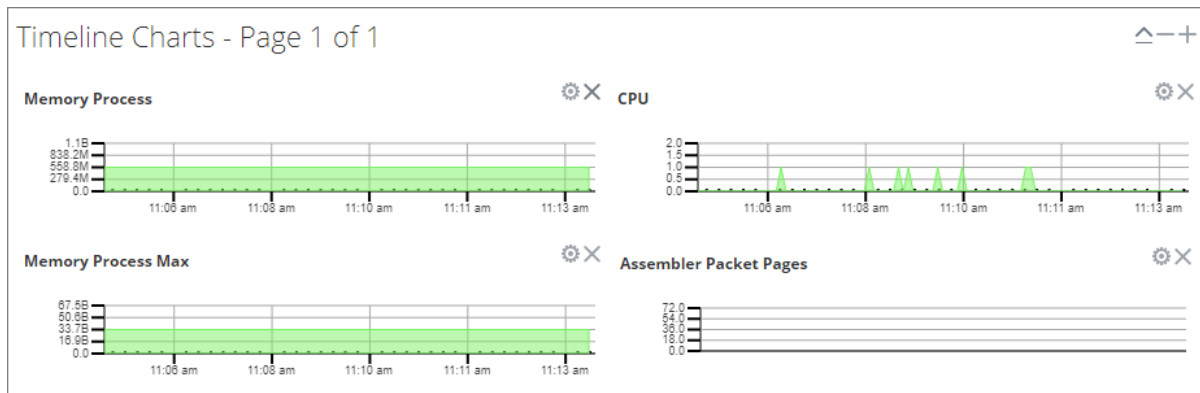


統計情報のタイムラインチャートの作成

統計情報のタイムラインを作成するには、次の手順を実行します。

[統計チャートトレイ]から、統計情報をクリックし、[タイムラインチャート]または[履歴チャート]セクションにドラッグします。

統計情報のタイムラインチャートが作成されます。チャートのスペースがない場合は、[タイムラインチャート]セクションに新しいページが作成され、新しいページにチャートが追加されます。下の例では、[統計チャートトレイ]からドラッグすることによって、[タイムラインチャート]セクションにAssembler Packet Pagesチャートが追加されています。



[統計チャートトレイ]での統計情報の検索

統計情報を検索するには、[検索]フィールドに検索語(「session」など)を入力して、Enterを押します。合致する統計が表示され、一致する単語が強調表示されます。

The screenshot shows the 'Chart Stats Tray' interface. At the top, there is a search bar containing the text 'session'. Below the search bar, a list of statistics is displayed. Each entry includes a title, a 'Stat Name', and a 'Path'. The statistics listed are:

- Assembler Sessions**
Stat Name: assembler.sessions
Path: /decoder/stats/assembler.sessions
- Session Bytes**
Stat Name: session.bytes
Path: /database/stats/session.bytes
- Session Bytes Last Hour**
Stat Name: session.bytes.last.hour
Path: /database/stats/session.bytes.last.hour
- Session Completion Queue**
Stat Name: pool.session.complete
Path: /decoder/parsers/stats/pool.session.complete
- Session Correlation Queue**
Stat Name: pool.session.correlate
Path: /decoder/stats/pool.session.correlate
- Session Decrement Queue**
Stat Name: pool.session.decrement
Path: /decoder/stats/pool.session.decrement
- Session Export Cache Files**
Stat Name: export.session.cache.files
Path: /decoder/stats/export.session.cache.files

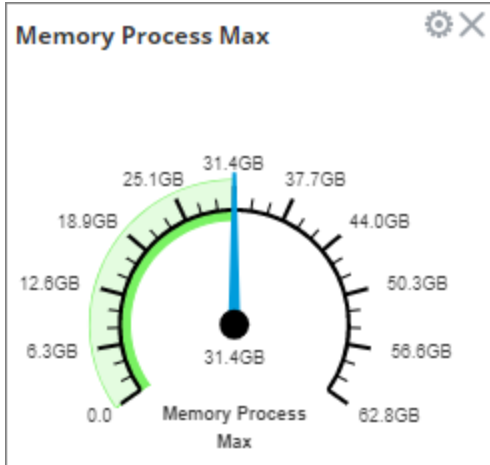
At the bottom of the tray, there is a pagination control showing 'Page 1 of 2' and a refresh icon. On the right side, it indicates 'Stats 1 - 12 of 24'.


統計情報ゲージのプロパティの編集

[サービス]の[統計]ビューの[ゲージ]セクションでは、統計情報がアナログゲージ形式で表示されます。個々のゲージのプロパティは編集可能です。すべてのゲージでタイトルを編集できます。さらに編集可能なプロパティがあるものもあります。


ゲージのプロパティの編集

1. [管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、[アクション]列で[表示]>[統計]を選択します。
[サービス]の[統計]ビューには[ゲージ]セクションがあります。
3. プロパティを編集するゲージに移動します(たとえば、[Memory Process])。




4. [プロパティ]アイコン()をクリックして、パラメータ名と値を表示します。
5. [表示名]フィールドの値をハイライト表示するには、値の部分([Memory Process]など)をダブルクリックします。

注:この例では、他の2つの値をクリックしても編集状態にはなりません。これらのプロパティはゲージでは編集できないためです。

6. [表示名]に新しい値を入力して、[プロパティ]アイコン()をクリックします。
[Memory Process]の代わりに新しいタイトルが表示されます。

[ゲージ]セクションへの統計情報の追加

[統計チャートトレイ]から[ゲージ]セクションに統計情報をドラッグすることによって、ゲージを追加できます。

1. [統計チャートトレイ]を展開するには、 をクリックします。
2. 下へスクロールし、[Session Rate (maximum)](セッションレート(最大))などの統計情報を選択します。
3. [ゲージ]セクションに統計情報をドラッグします。
新しいゲージが[ゲージ]セクションに表示されます。

タイムラインチャートのプロパティの編集

タイムラインチャートには、実行中の統計がタイムラインに表示されます。[サービス]の[統計]ビューには、リアルタイムと履歴という2種類のタイムラインがあります。[統計チャートトレイ]にある統計は[タイムラインチャート]セクションにドラッグできます。セッションサイズ、セッション、パケットの統計情報については、履歴タイムラインチャートで表示できます。個々のタイムラインチャートのプロパティは編集可能です。すべてのタイムラインチャートでタイトルを編集できます。さらに編集可能なプロパティがある統計もあります。

チャートにアクセスするには、次の手順を実行します。

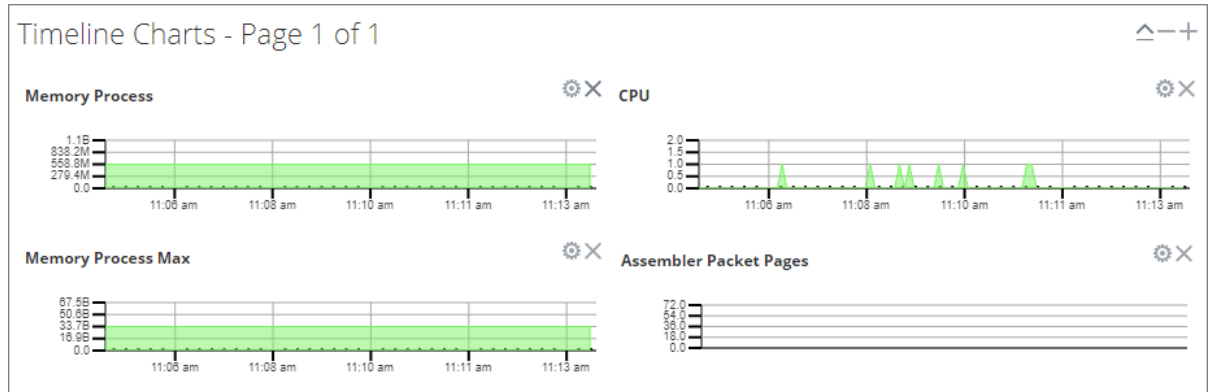
1. [管理]>[サービス]に移動します。
2. サービスを選択し、[統計]をクリックします。


[サービス]の[統計]ビューが表示されます。チャートは、このビューにあります。

タイムラインのプロパティの編集


タイムライン チャートのプロパティを編集するには、次の手順を実行します。

1. プロパティを編集するタイムライン チャートに移動します(たとえば、[Memory Process])。





2. [プロパティ]アイコン()をクリックして、パラメータ名と値を表示します。
3. 値をダブルクリックして(たとえば、[表示名]フィールド) 値を編集可能にします。

注: この例では、他の2つの値をクリックしても編集状態にはなりません。これらのプロパティはチャートでは編集できないためです。

4. 新しい値を入力し、[プロパティ]アイコン()をクリックします。
新しい値が反映されたタイムライン チャートが表示されます。

履歴チャートのプロパティの編集


履歴チャートのプロパティを編集するには、次の手順を実行します。

1. 履歴チャートに移動します。
2. [プロパティ]アイコン()をクリックして、パラメータ名と値を表示します。
3. 値をクリックして(たとえば、[開始日]フィールドの「01/27/2015」) 値を編集可能にします。
4. 新しい値を入力します。
5. 必要であれば、[終了日]と[表示名]を編集します。
6. [プロパティ]アイコン()をクリックします。
新しい値が反映された履歴チャートが表示されます。

注:履歴チャートのプロパティをデフォルトに戻し、開始日と終了日の値が動的に更新されるようにするには、開始日と終了日の値を削除し、[開始日]フィールドにカーソルを置いて、ブラウザを更新します。

タイムラインチャートへの統計情報の追加

[統計チャートトレイ]から[タイムライン]セクションに統計情報をドラッグすることによって、タイムラインチャートを追加できます。

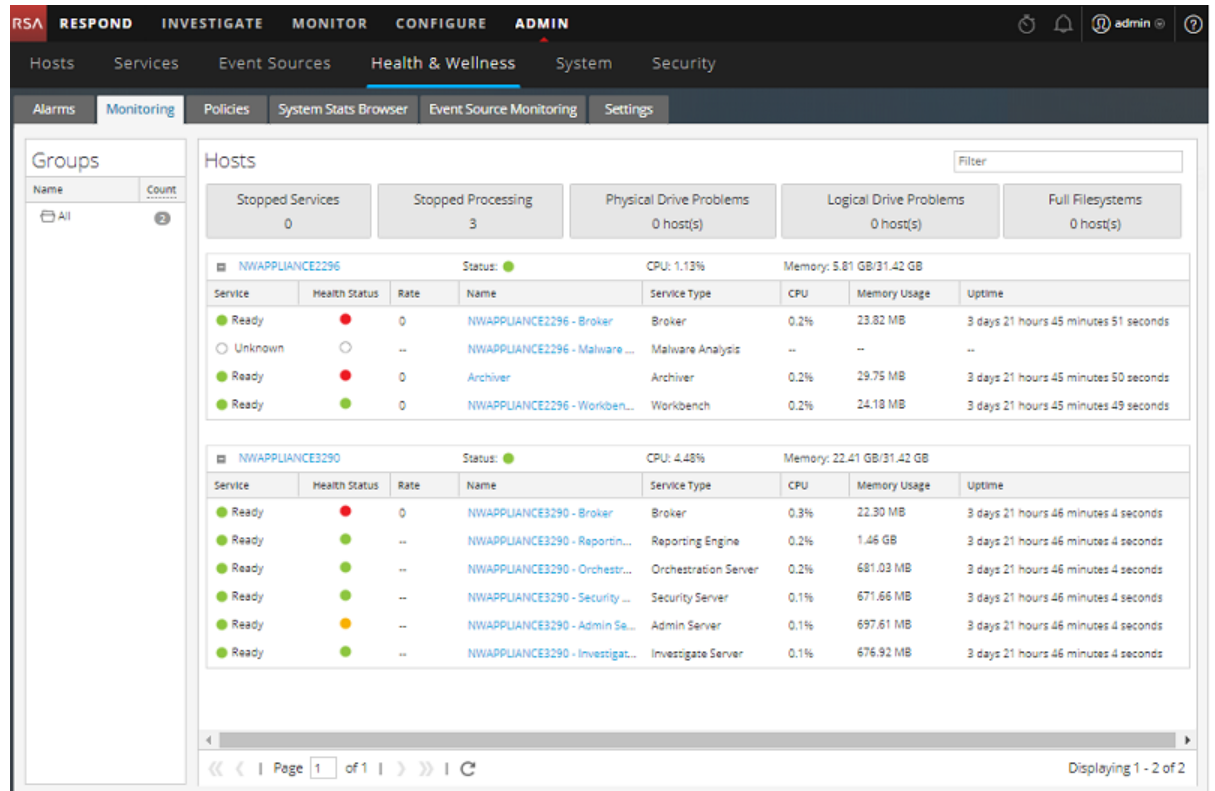
1. [統計チャートトレイ]を展開するには、 をクリックします。
2. 下へスクロールし、[Session Rate (maximum)](セッションレート(最大))などの統計情報を選択します。
3. [タイムライン]セクションに統計情報をドラッグします。
新しいタイムラインが[タイムライン]セクションに表示されます。

ホストとサービスの監視

NetWitness Suiteには、インストールされているホストおよびサービスのステータスを監視する方法が用意されています。すべてのホストの現在の稼働状態、各ホストで実行中のサービス、CPU使用率とメモリ使用量、ホストの詳細、サービスの詳細を表示できます。

NetWitness Suiteでホストおよびサービスを監視するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [監視]タブを選択します。
デフォルトでは、[すべて]グループに属するすべてのホストおよびその関連サービスのリストが表示されます。
各ホストの動作動作ステータス、CPU使用率、メモリ使用量が表示されます。



ホストの左側にある をクリックします (は、ホストにサービスがインストールされている場合に表示されます)。

3. 選択したホストにインストールされているサービスのリストが表示されます。
サービスごとに名前、動作動作ステータス、CPU使用率、メモリ使用量、稼働時間が表示されます。

[監視]ビューでのホストとサービスのフィルタ

次の方法のいずれかを使用して、[監視]ビューに表示するホストとサービスをフィルタすることができます。

- 特定のグループに属するホスト
- 特定のホストとそれに関連づけられているサービス
- サービスが停止されているホスト
- サービスで処理が停止されているか、処理がオフになっているホスト
- 物理ドライブに問題があるホスト
- 論理ドライブに問題があるホスト
- ファイルシステムが一杯になっているホスト

関連するトピックについては、「[\[監視\]ビュー](#)」を参照してください。

ホストとサービスをフィルタ処理するには、次の手順を実行します。

1. [管理]>[ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、デフォルトで[アラーム]タブが開きます。
2. [監視]タブを選択します。
3. 次のいずれかの方法で、ホストとサービスをフィルタします。
 - 特定のグループに属するホストと、そのホストに関連づけられたサービスを表示するには、[グループ]パネルでグループを選択します。
選択したグループに属するすべてのホストと、そのホストに関連づけられたサービスが、[ホスト]パネルに表示されます。

注:ホストのグループは、[管理]ページで作成するグループから取得されます。[管理]ページで作成されるすべてのグループがここに表示されます。

たとえば、[グループ]パネルでLC_Groupグループを選択すると、そのグループに属するすべてのホストが表示されます。

- 処理を停止しているサービスのリストを表示するには、[ホスト]パネルで[処理停止中]をクリックします。
少なくとも1つのサービスのステータスが[処理停止中]になっているホストのリストが表示されます。

注:上部のボタンは、NetWitness Suiteに構成されたすべてのホストのシステム統計を表示します。グループのフィルタを適用しても、表示内容は変わりません。

注: 同様に、適切なフィルタを選択することにより、ホストとそれに関連づけられたサービスのリストをフィルタできます。

- [サービス停止中]をクリックすると、サービスが停止中のすべてのホストのリストを表示します。
- [物理ドライブ障害]をクリックすると、物理ドライブに問題があるホストのリストを表示します。
- [フィルタ]ボックスにホストの名前を入力すると、目的のホストとそのホストで実行されているサービスのリストのみを表示します。

ホストの詳細の監視

ホストで問題が発生した場合、ホスト、メモリおよびCPUの使用状況、システム情報、物理ドライブ、論理ドライブ、ファイルシステムの詳細を表示して、さらに詳しく調査できます。

ホストの詳細を表示するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [監視]タブを選択します。
3. [ホスト]パネルでホストをクリックします。
[ホストの詳細]ビューが新しいページに表示されます。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, there are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Health & Wellness' tab is active, and within it, the 'System Stats Browser' sub-tab is selected. The main content area is titled 'Host Details' and shows information for host 'NWAPPLIANCE9'. The 'System Info' section includes:

Host	NWAPPLIANCE9	Memory Utilization	69.18%
CPU	3.01%	Used Memory	21.74 GB
Running Since	2017-Jul-10 09:44:02	Total Memory	31.42 GB
Current Time	2017-Jul-11 16:43:42	Cached Memory	2.05 GB
Uptime	1 day 6 hours 59 minutes 40 seconds	Swap Utilization	0%
System Info	Linux 3.10.0-514.26.2.el7.x86_64 x86_64	Used Swap	0 bytes
		Total Swap	4.00 GB

Below the System Info section, there are tabs for 'Physical Drive', 'Logical Drive', 'File System', 'Adapter', and 'Message Bus'. The 'Physical Drive' tab is active, showing a table with columns: State, Enclosure, Slot, Failure Count, Raw Size, and Inquiry Data.

サービスの詳細の監視

サービスの詳細、メモリの使用量とCPUの使用率、システム情報、選択したサービスに固有の各種詳細情報を表示できます。

サービスの詳細を表示するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ] に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [監視]タブを選択します。
3. [ホスト]パネルでホストの+をクリックします。
そのホストで実行中のサービス一覧が表示されます。
4. いずれかのサービスをクリックします。

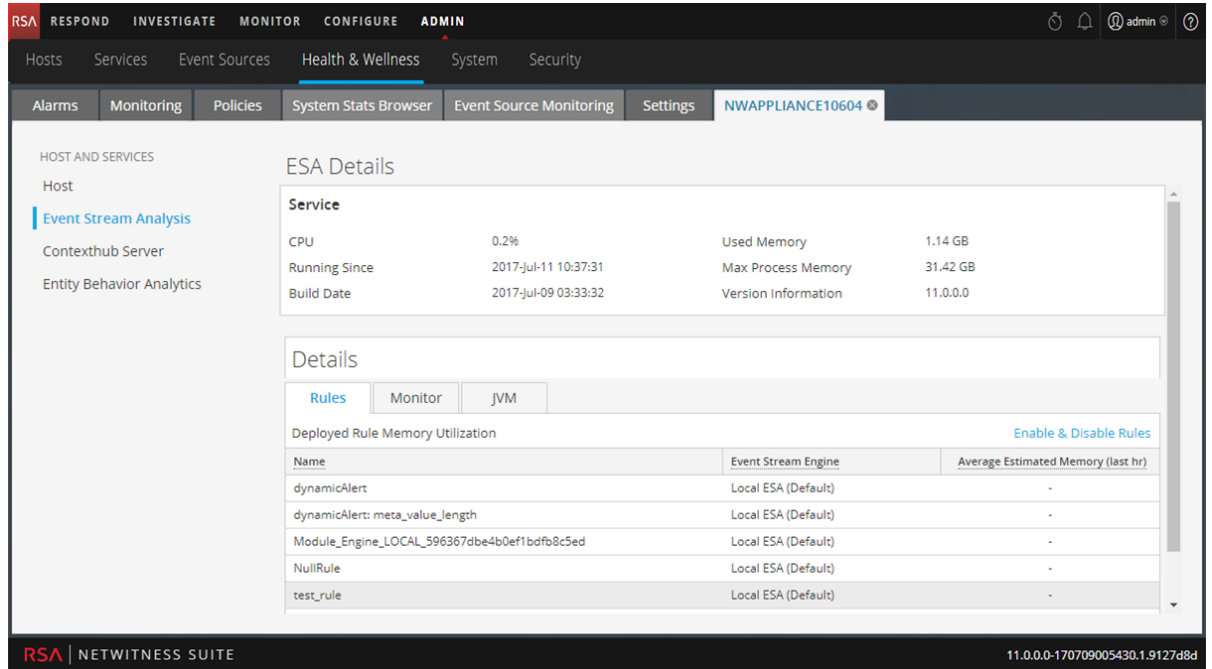
新しいページにサービスの詳細ビューが表示されます。Archiver、Broker、Concentrator、Decoderサービスの[詳細]ビューには、[サービス]と[詳細]パネルがあります。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, there are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Health & Wellness' tab is active, and the 'Monitoring' sub-tab is selected. The main content area displays 'Concentrator Details' for a host named 'Concentrator'. The details are organized into two tables:

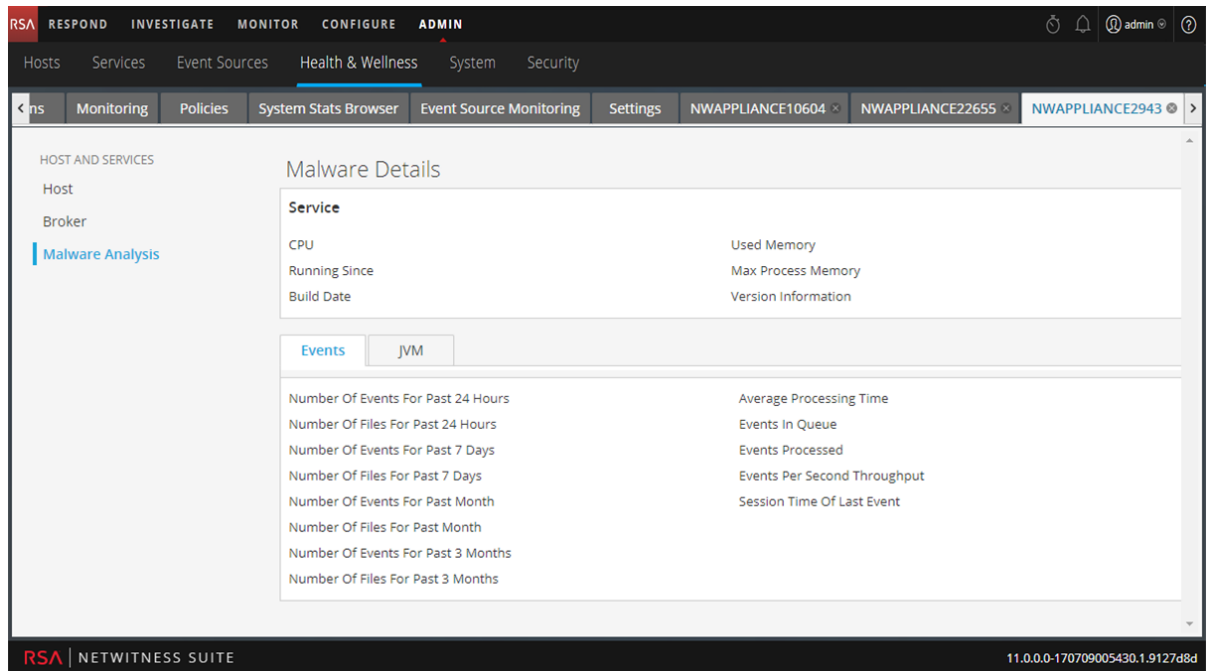
Service			
CPU	0.5%	Used Memory	2.62 GB
Running Since	2017-Jul-10 10:30:32	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:19:42	Version Information	11.0.0.0

Details			
Aggregation State	started	Time Begin	2017-Jun-12 07:54:45
Meta Rate	0	Time End	2017-Jul-11 16:28:44
Meta Rate Max	97222		
Session Rate	0		
Session Rate Max	1943		

ESA (Event Stream Analysis) サービスの[詳細]ビューには、[サービス]および[詳細]パネルに加えて、追加の統計情報が表示される[監視]タブと[JVM]タブがあります。



Malware Analysisサービスの[詳細]ビューには、[サービス]パネルに加えて、追加の統計情報が表示される[ルール]、[イベント]および[JVM]タブがあります。



Reporting Engineサービスの[詳細]ビューには、[サービス]パネルに加えて、追加の統計情報が表示される[レポート]タブと[JVM]タブがあります。

The screenshot shows the NetWitness Suite interface with the 'Reporting Engine Details' page selected. The page is divided into two main sections: 'Service' and 'Report'.

Service Details:

CPU	14.8%	Used Memory	1.53 GB
Running Since	2017-Jul-10 10:04:28	Max Process Memory	31.42 GB
Build Date		Version Information	

Report Details (JVM):

Number Of OAs Failed In Last Hour	0	Number Of Active Requests	0
Number Of Reports Failed In Last Hour	0	Average Time Taken For RE Requests	0 milliseconds
Number Of Rules Failed In Last Hour	0	Number Of Enabled Alerts	0
Maximum Time Taken For RE Request	215 milliseconds	Number Of Alert Execution Failed In Last 10 Minutes	0
Number Of Requests Completed	2543	Max Rows Fetched For Alerts	0
Max Number Of Rows Fetched For Charts	10	Number Of Requests Failed In Last 10 Mins	0
Number Of Chart Executions Failed In Last 10 Mins	0	Number Of Requests Received	2543
Number Of Enabled Charts	15	Number Of Requests Failed	0

The interface also shows a sidebar with 'HOST AND SERVICES' and a top navigation bar with 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN' tabs. The bottom status bar indicates 'RSA | NETWITNESS SUITE' and version '11.0.0.0-170709005430.1.9127d8d'.

注: 別の方法として、[ホストの詳細]ビューのオプションパネルに一覧表示されるサービスをクリックして、[サービスの詳細]ビューを表示することもできます。

各サービスの[詳細]ビューの詳細な説明については、「[\[監視\]ビュー](#)」を参照してください。

イベントソースの監視

NetWitness Suiteのイベントソースモニタリング機能には、次の機能があります。

- フェイルオーバーのサポート
- イベントソースおよび関連するCollectorとLog Decoderデバイスに関する統合されたビューを提供します。
- ルールに対するRegexのサポート
- 解除
- フィルタリング機能
- 履歴チャート

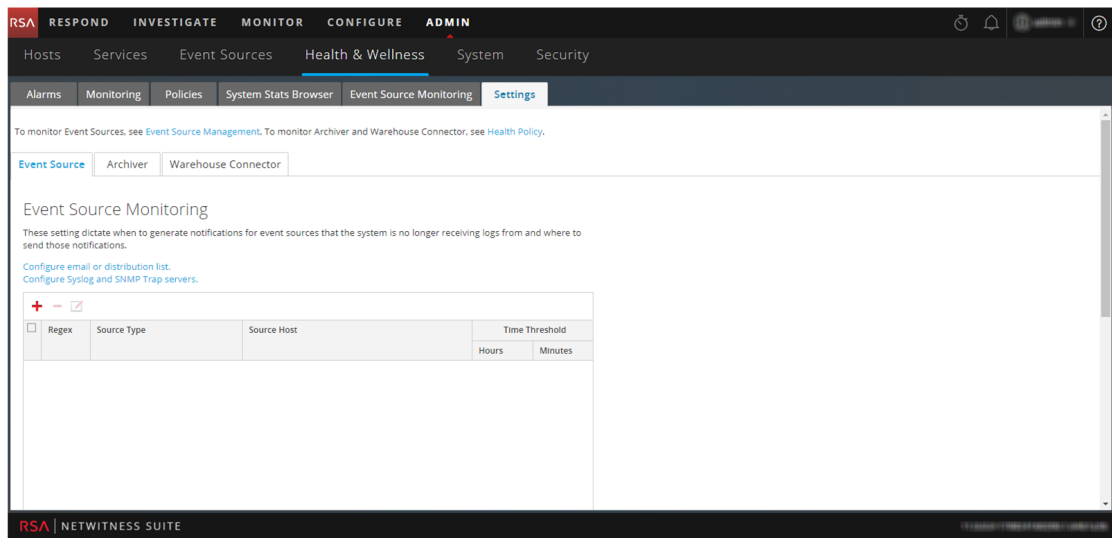
また、イベントソースの監視、ソースタイプから生成されたイベント数の確認、収集されたイベントの履歴チャートの表示を行うことができます。イベントソースを監視するためには、必要に応じて通知を生成して送信するようにイベントソースを構成する必要があります。

イベント ソース モニタリングの構成

イベント ソースを監視するためには、必要なときに通知を生成して送信するようにイベント ソースを構成する必要があります。関連する参照トピックについては、「[\[ヘルスマニタの設定\]ビュー: イベント ソース](#)」を参照してください。

NetWitness Suiteでイベント モニタリングを構成し、有効化するには、次の手順に従います。

1. **[管理]** > **[ヘルスマニタ]**に移動します。
2. **[設定]** > **[イベント ソース]**を選択します。
[イベント ソース]タブが表示されます。



3. **[イベント ソース モニタリング]**で、**+**をクリックします。
[監視対象ソースの追加/編集]ダイアログが表示されます。
4. NetWitness Suiteへのログ配信の停止を検出するために、監視対象となるイベント ソースについて、**[ソース タイプ]**、**[ソース ホスト]**、**[閾値]**を定義します。閾値を指定しなかった場合、NetWitness Suiteは、閾値が設定されるまでイベント ソースを監視し続けます。

注: [ソース タイプ]と[ソース ホスト]については、**[管理]** > **[サービス]** > **[Log Collectorサービス]** > **[表示]** > **[構成]**ビューの**[イベント ソース]**タブで、イベント ソースに対して構成した値を指定する必要があります。監視するイベント ソースを追加または変更します。イベント ソースを識別するパラメータは、ソース タイプとソース ホストの2つです。グローピング(パターン マッチングとワイルドカード文字)を使用して、イベント ソースの[ソース タイプ]と[ソース ホスト]を指定できます

The screenshot shows a dialog box titled "Add/Edit Source Monitor". It has a close button (X) in the top right corner. Inside the dialog, there is a checkbox labeled "Regex". Below it are two text input fields: "Source Type *" and "Source Host *". Underneath these is a "Time Threshold *" section with two spinners; the first is set to "0" and labeled "Hours", and the second is also set to "0" and labeled "Minutes". At the bottom right, there are two buttons: "Cancel" and "OK".

5. [OK]をクリックします。
イベントソースがパネルに表示されます。
6. 通知方法を構成するには、次のいずれかを実行します。
 - [メールサーバ設定を構成します。]を選択します。
[管理] > [システム] > [メールサーバ設定]パネルが表示され、通知の送信先を指定することができます。
 - [SyslogサーバおよびSNMPトラップサーバを構成します。]を選択します。
[管理] > [システム]の[監査の構成]パネルが表示され、通知の送信先となるSyslogとSNMPトラップを構成することができます。
7. [適用]をクリックします。
このイベントソースからのイベントの受信が停止し、時間の閾値が経過すると、NetWitness Suiteは通知の送信を開始します。

[イベントソースモニタリングの設定]ビューのパラメータの詳細については、「[\[イベントソースモニタリング\]ビュー](#)」を参照してください。

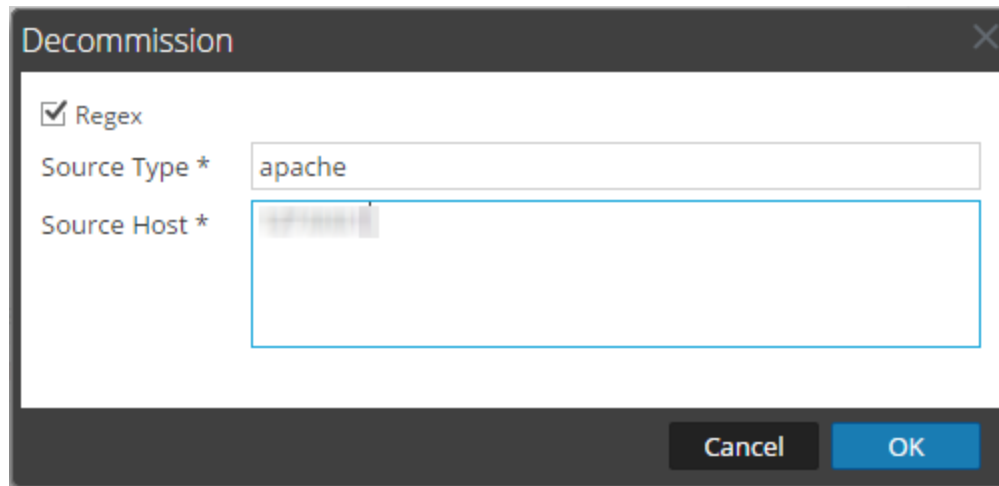
イベントソースモニタリングの解除

イベントソースモニタリングを設定したLog Collectorサービス(ローカルCollectorまたはリモートCollector)が運用できなくなった場合、NetWitness SuiteはCollectorが解除されるまで、イベントを受信していないことを通知します。

注意: リモートCollectorでフェイルオーバーローカルCollectorを構成し、ローカルCollectorがスタンバイLog Decoderにフェイルオーバーした場合、通知を止めるにはローカルCollectorを解除する必要があります。

イベントソースでのイベントソースモニタリングを解除する方法

1. [管理] > [ヘルスマニタ]に移動します。
2. [設定] > [イベント ソース]を選択します。
[イベント ソース]タブが表示されます。
3. [解除]で、**+**をクリックします。
[解除]ダイアログが表示されます。
4. イベント モニタリングの通知を解除するソースの[ソース タイプ]と[ソース ホスト]を定義します。



イベント ソースのフィルタ

フィルタを選択して、次のようなイベントを表示できます。

- 特定のイベント ソースに属しているイベント
- 特定のイベント ソース タイプに属しているイベント
- 特定のLog Collectorによって収集されたイベント
- イベント ソース タイプ、Log Collector、Log Decoder、最終収集時刻の順に並べ替えられたイベント リスト

イベント ソースのリストをフィルタするには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
2. [イベント ソース モニタリング]を選択します。
3. 次のいずれかの方法でリストをフィルタします。
 - 特定のイベント ソースによって生成されたイベントを表示するには、[イベント ソース]フィールドに目的のイベント ソースを入力します。[Regex]を選択してRegexフィルタを有効にし、

[適用]をクリックします。このフィルタを有効にすると、テキストの正規表現検索が実行され、一致するカテゴリがリストされます。さらに、このフィールドでは、グローピングパターンマッチングもサポートされます。

指定されたイベントソースによって生成されたすべてのイベントが表示されます。

- 特定のLog Collectorによって収集されたイベントを表示するには、ドロップダウンリストからLog Collectorを選択し、[適用]をクリックします。
指定されたLog Collectorによってさまざまなイベントソースから収集されたすべてのイベントのリストが表示されます。

注: 次のフィルタを選択することもできます。

特定のイベントソースタイプのイベントを表示するには、イベントソースタイプを選択し、[適用]をクリックします。


特定のタイムフレーム内で受信したイベントを表示するには、タイムフレームを選択し、[適用]をクリックします。クエリ結果をさらにフィルタして、検索されたログのうち特定の時間内に受信されたイベントソースのみが含まれるようにしたり、または特定の時間内にはログが受信されなかったイベントソースのみが含まれるようにしたりできます。

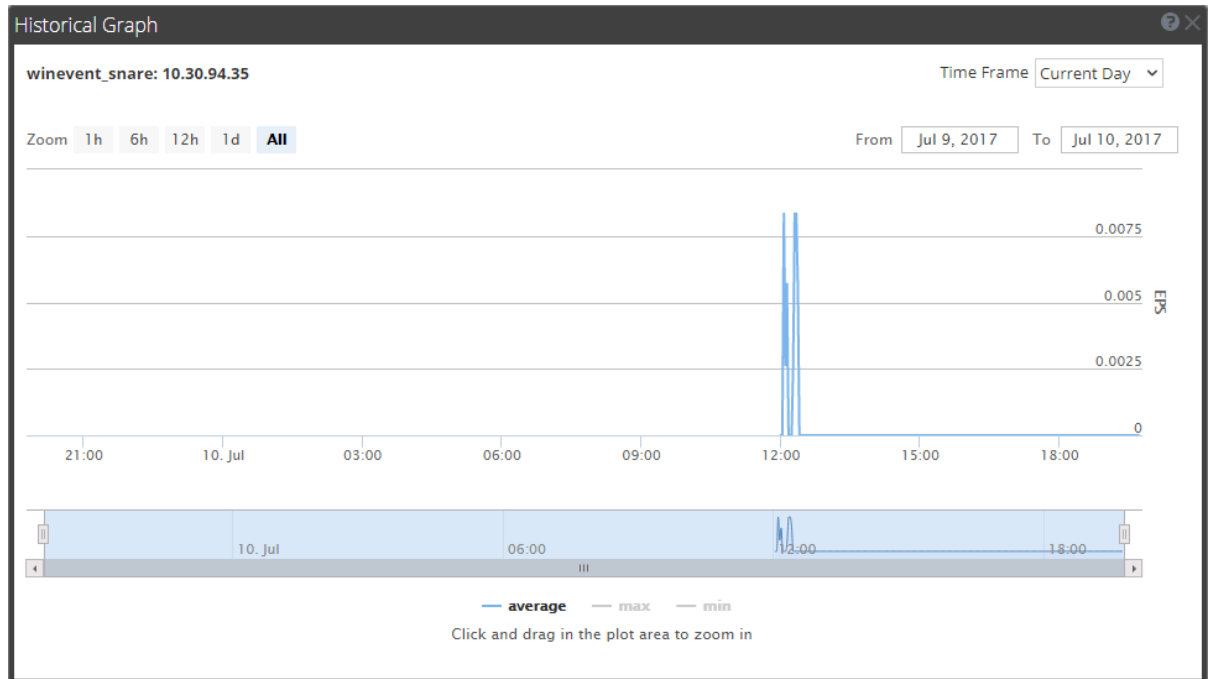
各種のパラメータとその説明の詳細については、「[\[イベントソースモニタリング\]ビュー](#)」を参照してください。

イベントソースでの収集イベントの履歴チャートの表示

イベントソースから収集されたイベントの履歴チャートは、選択した時間範囲にわたる収集の傾向に関する情報を提供します。

履歴チャートを表示するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [イベントソースモニタリング]をクリックします。
[イベントソースモニタリング]ビューが表示されます。
3. [履歴チャート]列で、を選択します。
選択されたイベントソースの履歴チャートが表示されます。
以下の図は、イベントソースタイプwinevent_snareの履歴チャートの例を示します。



デフォルトのチャート表示は、現在の日付に収集されたイベントを表示するためにカスタマイズされており、値は1時間の間隔(09.05~105.05時間)でズーム表示されています。チャートにポインタを合わせると、特定の時点での詳細が表示されます。たとえば、この図では時刻09.30における平均収集レートが表示されています。

注: [時間範囲]および[日付範囲]を選択することにより、チャート表示をカスタマイズできます。値のズームインや時間範囲を設定できるほか、プロット領域をクリックしてドラッグすることにより、チャートをズーム表示できます。表示をカスタマイズするためのパラメータやズームイン機能については、イベントソースから収集された「[\[ヘルスマニタ\]の\[履歴チャート\]](#)」を参照してください。

チャートにデータが表示されない場合は、次のいずれかの理由が考えられます。

- イベントソースが停止している。
- イベントソースが現在何も処理していない。

アラームの監視

ヘルスマニタ インタフェースでは、NetWitness Suite導入環境のホストとサービスに関するアラームを設定して監視できます。ポリシールールで定義された、ホストとサービスに関する統計閾値を超えると、「アクティブ」なアラームとして[アラーム]タブに表示されます。リカバリ閾値を超えると、アラームはグレー表示になり、「クリア済み」ステータスに変わります。

アラームのパラメータは[[ポリシーの管理](#)]で設定します。[ポリシーの管理](#)関連する参照トピックについては、「[\[ヘルスマニタ\]ビュー: \[アラーム\]ビュー](#)」を参照してください。

NetWitness Suiteでアラームを監視するには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。

[ヘルスマニタ]ビューが表示され、デフォルトで[アラーム]タブが開きます。

Time	State	Severity	Rule Name	Service	Hostname	IP Address	Stat	Value
2017-09-13 10:06:40 AM	Active	Critical	Concentrator Meta Rate Zero	Concentrator	nwappliance28765	10.31.125.172	Concentrator/Meta Rate (current)	0
2017-09-09 09:38:29 AM	Active	Critical	Log Decoder Capture Rate Zero	Log Decoder	nwappliance19848	10.31.125.173	Capture/Capture Packet Rate (current)	0
2017-09-09 09:34:36 AM	Active	Critical	ESA stopped aggregating	Event Stream Analysis	nwappliance7450	10.31.125.171	Workflow-NextGen/WorkUnitProcessingRate	0
2017-09-09 09:10:13 AM	Active	Critical	Broker Aggregation Stopped	Broker	nwappliance13731	10.31.125.170	Broker/Status	stopped
2017-09-09 09:10:13 AM	Active	High	Broker Session Rate Zero	Broker	nwappliance13731	10.31.125.170	Broker/Session Rate (current)	0
2017-09-26 07:00:57 AM	Cleared	Critical	ESA Service Stopped	Event Stream Analysis	nwappliance7450	10.31.125.171	ProcessInfo/Service Status	unknown
2017-09-19 08:31:25 PM	Cleared	Critical	Admin Server Stopped	Admin Server	nwappliance13731	10.31.125.170	ProcessInfo/Service Status	unknown
2017-09-19 02:53:49 AM	Cleared	Critical	Log Decoder Capture Not Started	Log Decoder	nwappliance19848	10.31.125.173	Capture/Capture Status	stopped
2017-09-14 09:30:14 AM	Cleared	Critical	Contexthub Service Stopped	Contexthub Server	nwappliance7450	10.31.125.171	ProcessInfo/Service Status	unknown
2017-09-09 09:38:29 AM	Cleared	Critical	Log Decoder Log Capture Pool Depleted	Log Decoder	nwappliance19848	10.31.125.173	Pool/Package Capture Queue	0
2017-09-09 09:34:32 AM	Cleared	Critical	Concentrator Aggregation Stopped	Concentrator	nwappliance28765	10.31.125.172	Concentrator/Status	stopped
2017-09-26 06:57:57 AM	Cleared	High	Custom Feeds Failure	NetWitness UI	nwappliance13731	10.31.125.170	Feeds/Custom Feeds Deployment Status	fail
2017-09-09 09:05:18 AM	Cleared	High	Admin Server in Unhealthy State	Admin Server	nwappliance13731	10.31.125.170	ProcessInfo/Overall Processing Status Indicator	PARTIALLY_WOR...

2. [詳細]パネルに詳細を表示するアラームをクリックします。
3. 選択したアラームの詳細を表示するには、< (展開)をクリックします。

Alarm Details	
Id	191-1037-0007
Time	2017-07-10 10:35:43 AM
State	ACTIVE
Severity	CRITICAL
Hostname	NWAPPLIANCE22655
Service	Concentrator
Policy	Concentrator Monitoring Policy
Rule Name	Concentrator Meta Rate Zero
Informational Text	<p>This Concentrator is not receiving meta from its upstream services, which is indicative of an aggregation problem or capture problem on an upstream service.</p> <p>Possible Remediation Action: Please check whether aggregation is started on the Concentrator, and whether all upstream Decoders from which it is aggregating are in a 'consuming' state. There should be additional corresponding alarms if this is not the case.</p> <p>To check the aggregation status of this</p>

SNMPアラートを使用したヘルスマニタの監視

NetWitnessサーバコンポーネントを監視し、SNMP(Simple Network Management Protocol)を使用して、閾値とシステム障害に基づくプロアクティブなアラートを発行することができます。

NetWitness Suiteコンポーネントの次の数値を監視することができます。

- 定義済みの閾値に到達したCPUの利用率
- 定義済みの閾値に到達したメモリ使用率
- 定義済みの閾値に到達したディスク使用率

SNMPの構成

SNMPv3閾値トラップおよび監視トラップを送信するように、NetWitnessサーバを構成することができます。閾値トラップはノードに構成した閾値と連動し、NetWitness Suiteコアアプリケーションから送信されます。監視トラップは、構成ファイルで指定された項目について、SNMPデーモンから送信されます。NetWitness SuiteからSNMPトラップを受信するには、ユーザ側で別のサービスにSNMPデーモンを設定する必要があります。NetWitness Suiteに対するSNMPの設定は、NetWitnessサーバの構成設定で行うことができます。詳細については、「*NetWitness Suite*ホストおよびサービススタートガイド」の「サービス構成設定」で、特定のホストに関する説明を参照してください。

閾値

閾値は、setLimitメッセージに対応する任意のサービス統計情報に対して設定することができます。現在の閾値は、getLimitメッセージを使用して取得できます。制限を設定するために、閾値の上限と下限を渡すことができます。

統計情報の値が下限または上限の閾値を超えたときに、SNMPトラップがトリガーされ、閾値が超過されたことが通知されます。このトラップは値が下限値を下回った後や上限値を上回った後はトリガーされませんが、値が通常の範囲(下限値よりも大きく、上限値よりも小さい)に戻ったときには別のトラップがトリガーされます。

サービスの閾値は、[サービス]の[エクスプローラ]ビューまたはREST APIを使用して設定する必要があります。

次に、CPU使用率を監視する閾値の例を示します(10%を下回った場合と90%を上回った場合の閾値)。

```
/sys/stats/cpu setLimit low=10 high=90
```

次に、REST APIを使用して閾値を設定する例を示します。

```
http://<log decoder>:50102/sys/stats/cpu?msg=setLimit&low=10&high=90
```

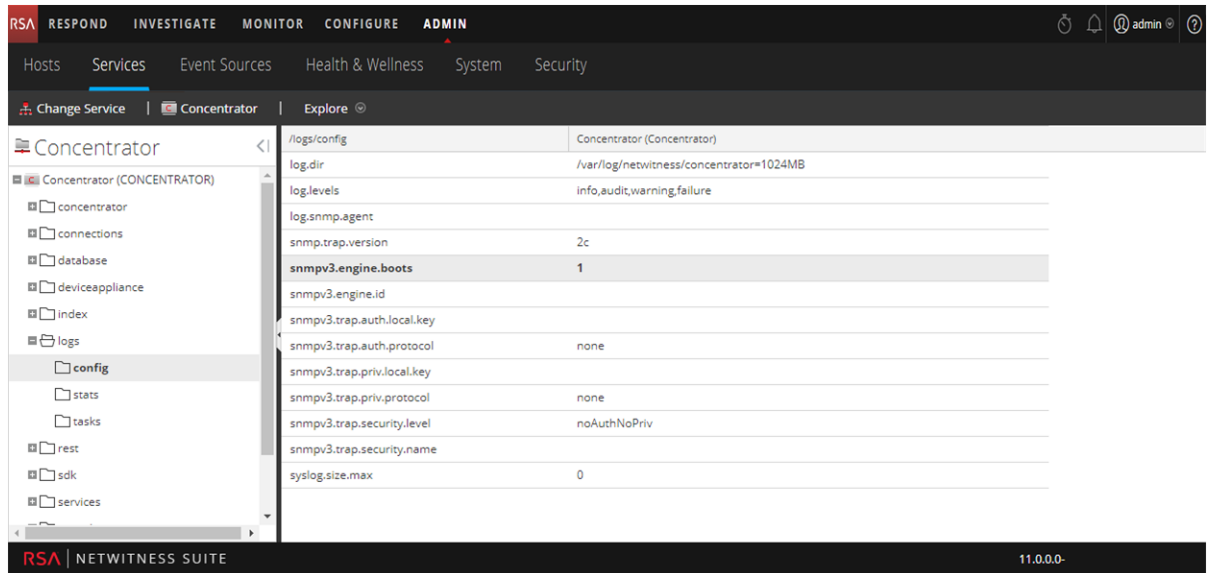
CPU使用率が90%を超えると、SNMPトラップが生成されます。

```
23435333 2013-Dec-16 11:08:35 Threshold warning path=/sys/stats/cpu  
old=77% new=91
```

ホストのSNMPv3の構成

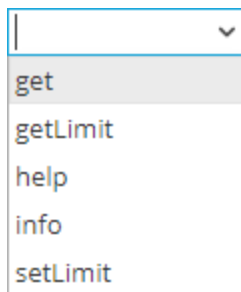
1. [管理]>[サービス]に移動します。
[サービス]ビューが表示されます。
2. サービスを選択します。
3. [アクション]列で、[表示]>[エクスプローラ]をクリックします。
4. ノードリストを展開し、configフォルダを選択します。たとえば、[logs]>[config]の順に選択します。

5. SNMPv3構成を設定します。



サービスの閾値の設定

1. [管理] > [サービス]に移動します。
[サービス]ビューが表示されます。
2. サービスを選択します。
3. [アクション]列で、[表示] > [エクスプローラ]をクリックします。
4. ノード リストを展開し、sysの下のstatsフォルダを選択します。
5. 統計情報を選択して(たとえば[cpu])、右クリックします。
6. ドロップダウンメニューの[プロパティ]を選択します。
[プロパティ]パネルが表示されます。[プロパティ]パネルのドロップダウン リストに、送信するメッセージが一覧表で表示されます。



7. setLimitを選択します。
8. 下限値と上限値を指定します。

ヘルスマニタのトラブルシューティング

すべてのホストおよびサービスに共通する問題

次の場合、ヘルスマニタ インタフェースに誤った統計情報が表示されることがあります。

- 一部またはすべてのホストとサービスが、正しくプロビジョニングおよび有効化されていない。
- 導入されているバージョンが混在している(つまり、ホストがさまざまなNetWitness Suiteバージョンに更新されている)。
- サポート サービスが実行されていない。

インタフェースまたはログ ファイルのメッセージから特定される問題

このセクションでは、NetWitness Suiteのヘルスマニタ インタフェースに表示されるか、またはヘルスマニタ ログ ファイルに記録されたメッセージによって特定される問題のトラブルシューティングについて説明します。

ユーザ インタフェース: システム管理サービスに接続できません

SMS(System Management Service) ログ:

```
Caught an exception during connection recovery!
```

```
java.io.IOException
```

```
at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:106)
```

```
at com.rabbitmq.client.impl.AMQChannel.wrap (AMQChannel.java:102)
```

```
at com.rabbitmq.client.impl.AMQConnection.start
```

メッ (AMQConnection.java:346)

セ at

ー com.rabbitmq.client.impl.recovery.RecoveryAwareAMQConnectionFactory.

ジ ry.

```
newConnection (RecoveryAwareAMQConnectionFactory.java:36)
```

```
at com.rabbitmq.client.impl.recovery.AutorecoveringConnection.
```

```
recoverConnection (AutorecoveringConnection.java:388)
```

```
at com.rabbitmq.client.impl.recovery.AutorecoveringConnection.
```

```
beginAutomaticRecovery (AutorecoveringConnection.java:360)
```

```
at
```

```
com.rabbitmq.client.impl.recovery.AutorecoveringConnection.access
```



```
$000 (AutorecoveringConnection.java:48)
  at com.rabbitmq.client.impl.recovery.AutorecoveringConnection$1.
shutdownCompleted (AutorecoveringConnection.java:345)
  at
com.rabbitmq.client.impl.ShutdownNotifierComponent.notifyListene
rs (ShutdownNotifierComponent.java:75)
  at com.rabbitmq.client.impl.AMQConnection$MainLoop.run
(AMQConnection.java:572)
  at java.lang.Thread.run (Thread.java:745)
  Caused by: com.rabbitmq.client.ShutdownSignalException:
connection error
  at com.rabbitmq.utility.ValueOrException.getValue
(ValueOrException.java:67)
  at
com.rabbitmq.utility.BlockingValueOrException.uninterruptibleGetV
alue (BlockingValueOrException.java:33)
  at
com.rabbitmq.client.impl.AMQChannel$BlockingRpcContinuation.getRe
ply
(AMQChannel.java:343)
  at com.rabbitmq.client.impl.AMQConnection.start
(AMQConnection.java:292)
  ... 8 more
  Caused by: java.net.SocketException: Connection reset
  at java.net.SocketInputStream.read (SocketInputStream.java:189)
  at java.net.SocketInputStream.read (SocketInputStream.java:121)
  at java.io.BufferedInputStream.fill
(BufferedInputStream.java:246)
  at java.io.BufferedInputStream.read
(BufferedInputStream.java:265)
  at java.io.DataInputStream.readUnsignedByte
(DataInputStream.java:288)
  at com.rabbitmq.client.impl.Frame.readFrom (Frame.java:95)
  at com.rabbitmq.client.impl.SocketFrameHandler.readFrame
(SocketFrameHandler.java:139)
```

考えられる原因	<pre>at com.rabbitmq.client.impl.AMQConnection\$MainLoop.run (AMQConnection.java:532)</pre>
解決策	<p>RabbitMQサービスがNetWitnessサーバで実行されていません。</p> <p>次のコマンドを使用して、RabbitMQサービス、SMSサービス、NetWitness Suiteサービスを再開します。</p> <pre>systemctl restart rabbitmq-server systemctl restart rsa-sms systemctl restart jetty</pre>

メッセージ/問題	<p>ユーザインタフェース: システム管理サービスに接続できません</p>
原因	<p>システム管理サービス、RabbitMQ、Mongoのいずれかのサービスが実行されていません。</p>
解決策	<p>NetWitnessサーバで次のコマンドを実行して、これらのサービスすべてが実行されていることを確認します。</p> <pre>[root@nwserver ~]# systemctl status rsa-sms RSA NetWitness SMS :: Server is not running. [root@nwserver ~]# systemctl start rsa-sms Starting RSA NetWitness SMS :: Server... [root@nwserver ~]# systemctl status rsa-sms RSA NetWitness SMS :: Server is running (5687). [root@nwserver ~]# systemctl status mongod mongod (pid 2779) is running... systemctl status rabbitmq-server</pre>

```
Status of node nw@localhost ...
[{"pid,2501},
 {running_applications,
  [{"rabbitmq_federation_management,"RabbitMQ Federation
Management",
 "3.3.4"}],
```

メッセージ/問題	ユーザ インタフェース: システム管理 サービスに接続できません
考えられる原因	/var/lib/rabbitmq/パーティションの使用率が70%以上です。
解決策	カスタマ サポートにお問い合わせください。

メッセージ/問題	ユーザ インタフェース: ホスト移行失敗。
考えられる原因	1つ以上のNetWitness Suiteサービスが 停止状態 になっている可能性があります。
解決策	次のサービスが実行されていることを確認してから、NetWitnessサーバを再起動します。 Archiver、Broker、Concentrator、Decoder、Event Stream Analysis、Response Server、IPDB Extractor、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、Warehouse Connector、Workbench

メッセージ/	ユーザ インタフェース: サービスを利用できません。
---------------	----------------------------

問題	
考えられる原因	1つ以上のNetWitness Suiteサービスが 停止状態 になっている可能性があります。
解決策	次のサービスが 実行されていることを確認してから 、NetWitnessサーバを再起動します。Archiver、Broker、Concentrator、Decoder、Event Stream Analysis、Response Server、IPDB Extractor、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、Warehouse Connector、Workbench

メッセージ/問題	ユーザインタフェース: サービスを利用できません
考えられる原因	SMS(システム管理サービス)、RabbitMQ、Mongoのいずれかのサービスが実行されていません。
解決策1	<p>NetWitnessサーバで次のコマンドを実行して、これらのサービスすべてが実行されていることを確認します。</p> <pre>[root@nwserver ~]# systemctl status rsa-sms RSA NetWitness SMS :: Server is not running. [root@nwserver ~]# systemctl start rsa-sms Starting RSA NetWitness SMS :: Server... [root@nwserver ~]# systemctl status rsa-sms RSA NetWitness SMS :: Server is running (5687). [root@nwserver ~]# systemctl status mongod mongod (pid 2779) is running... systemctl status rabbitmq-server Status of node nw@localhost ... [{{pid,2501}, {running_applications, [{rabbitmq_federation_management,"RabbitMQ Federation</pre>

	Management", "3.3.4"},
解決策2	/var/lib/rabbitmqパーティションの使用率が75%未満であることを確認します
解決策3	エラーがないかNetWitnessサーバログファイル (var/lib/netwitness/uax/logs/nw.log)を確認します。

メッセージ/問題	ContextHubが停止し、データソースおよびリストを追加または編集できません。
考えられる原因	ストレージがいっぱい(95%以上)です。
解決策1	/etc/netwitness/contexthub-server/ contexthub-server.ymlにあるYMLファイルを更新することで、ストレージを増やします。 たとえば、ストレージを120 GBから150 GBを増やすには、関連するパラメータを編集して値を入力します(バイト単位)。 <code>rsa.contexthub.data.disk-size: 161061273600</code>
解決策2	不要または未使用の大規模なリストを削除します。
解決策3	STIXおよびTAXIデータを自動的に削除し、ストレージ領域をクリーンアップするように、リストのTTLインデックスを構成します。

メッセージ/問題	Context Hubが固定メモリ上で実行され、キャッシュ用に50%が予約されています。キャッシュが100%フルになると、キャッシュの応答が停止します。すべての新しい検索において、応答が低速になります。
考えら	キャッシュがいっぱい(50%以上)です。

れる原因	
解決策 1	デフォルトでは、Context Hubは30分ごとにキャッシュをクリーンアップします。データソースのキャッシュ有効期間を短縮します。
解決策 2	データソースのキャッシュを無効化します。
解決策 3	<p>/etc/netwitness/contexthub-server/contexthub-server.confファイルで利用可能な-Xmxオプションを編集することで、CH JavaプロセスのRAMを増やします。JAVA_OPTSで、-Xmxオプションを検索します。</p> <p>たとえば、次のようにエントリを編集します。</p> <pre>-Xmx8G</pre> <p>ここで、8Gは8 GBの領域を表します。その後、ContextHubサービスを再起動します。</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>注:メモリは、利用可能なシステムメモリよりも小さくします。ホスト上で他にも多くのサービスが実行されていることに注意してください。</p> </div>

メッセージ/問題	リスト データソースに正常でない統計情報やステータスが表示されます。
考えられる原因 1	<p>次のことを実行できません。</p> <ul style="list-style-type: none"> • データソースへのアクセス • CSVファイルの解析または読み取り • 一致しないCSVのスキーマ
考えられる原因 2	データソースにアクセスするときに認証できません。
解決策 1	csvファイルを正しい場所 (/var/lib/netwitness/contexthub-server/data/など)に保存し、必要な読み取り権限があることを確認します。
解決策 2	データソースの構成中に指定したcsvファイルのスキーマが一致していることを確認します。一致していない場合、新しいスキーマを使用して新しいデータ

解決策3	<p>ソースを作成するか、スキーマに一致するようにcsvファイルを編集します。たとえば、列1、列2、列3をもつスキーマを使用してリスト データ ソースを構成する場合があります。次にcsvファイルを更新する際に、列数が増減したり、列の順序が変更されます。このような場合、スキーマが一致しないため、構成済みのリスト データ ソースはヘルスマニタの統計情報に「異常」と表示されます。</p>
	<p>パスワードが正しいことを確認します。データソースの編集を確認するには、パスワードを入力し、[接続のテスト]をクリックします。</p>
	<p>前述の解決策に関連する詳細情報については、「<i>Context Hub</i>構成ガイド」のトピック「データソースとしてのリストの構成」を参照してください。</p>

ユーザ インタフェースまたはログから特定できない問題

このセクションでは、NetWitness Suiteのヘルスマニタ インタフェースに表示されたり、またはヘルスマニタ ログ ファイルに記録されたメッセージからは特定できない問題のトラブルシューティングについて説明します。たとえば、誤った統計情報がインタフェースに表示される場合があります。

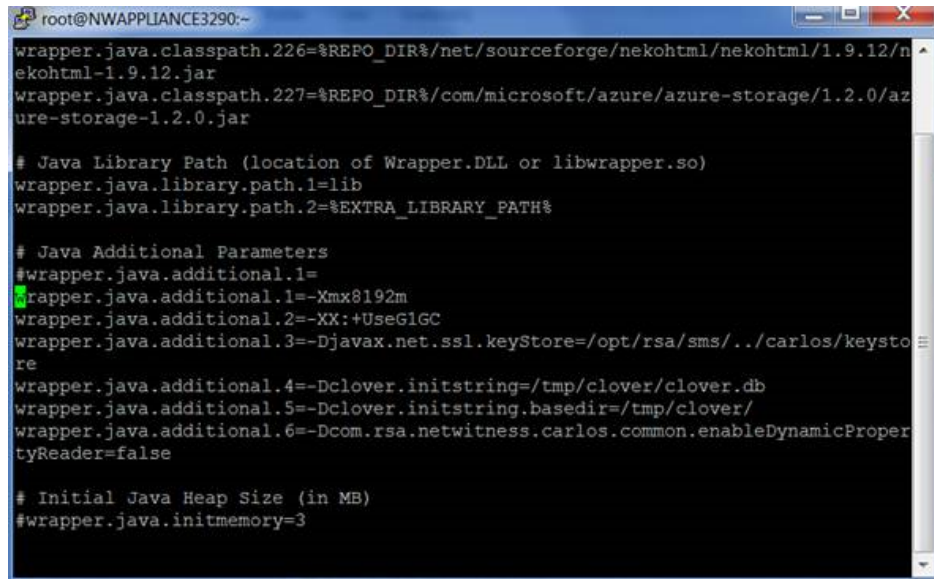
問題	ヘルスマニタ インタフェースに誤った統計情報が表示されます。
考えられる原因	SMSサービスが実行されていません。SMSサービスは、NetWitnessサーバで実行されている必要があります。
解決策	SMSサービスを再開します。

問題	jettysrv(jeTTYサーバ)を再起動するまで、アップグレード後のバージョンが
-----------	--

考えられる原因	NetWitness Suiteに表示されません。
	NetWitness Suiteは、30秒ごとにサービスをポーリングして、そのサービスがアクティブかどうかを確認します。その30秒の間にサービスが復帰した場合、そのサービスの新しいバージョンを取得しません。
解決策	<ol style="list-style-type: none"> 1. サービスを手動で停止します。 2. サービスがオフラインになるまで待ちます。 3. サービスを再開します。 NetWitness Suiteに正しいバージョンが表示されます。

問題	NetWitnessサーバに[サービスを利用できません]ページが表示されません。
考えられる原因	NetWitness Suiteをバージョン10.5にアップグレードした直後は、JDK 1.8がデフォルトのバージョンに設定されていないため、jettysrv(jeTTYサーバ)が起動できなくなります。jeTTYサーバがないと、NetWitness Suiteサーバは[サービスを利用できません]ページを表示できません。
解決策	jettysrvを再起動します。

問題	SMSサービスが停止し、ログファイルに次のエラーが表示されます。 java.lang.OutOfMemoryError: Java heap space
解決策	次の解決策を使用して、必要に応じてメモリを増やすことができます。 <ol style="list-style-type: none"> 1. /opt/rsa/sms/conf/wrapper.confを開きます。

A terminal window titled 'root@NWAPPLIANCE3290:~' showing configuration for wrapper.java.additional.1. The configuration includes classpath settings for nekohtml and azure-storage, library paths, and various Java additional parameters. The parameter wrapper.java.additional.1 is highlighted in green.

```
root@NWAPPLIANCE3290:~
wrapper.java.classpath.226=%REPO_DIR%/net/sourceforge/nekohtml/nekohtml/1.9.12/n
ekohtml-1.9.12.jar
wrapper.java.classpath.227=%REPO_DIR%/com/microsoft/azure/azure-storage/1.2.0/az
ure-storage-1.2.0.jar

# Java Library Path (location of Wrapper.DLL or libwrapper.so)
wrapper.java.library.path.1=lib
wrapper.java.library.path.2=%EXTRA_LIBRARY_PATH%

# Java Additional Parameters
#wrapper.java.additional.1=
wrapper.java.additional.1=-Xmx8192m
wrapper.java.additional.2=-XX:+UseG1GC
wrapper.java.additional.3=-Djavax.net.ssl.keyStore=/opt/rsa/sms/./carlos/keysto
re
wrapper.java.additional.4=-Dclover.initstring=/tmp/clover/clover.db
wrapper.java.additional.5=-Dclover.initstring.basedir=/tmp/clover/
wrapper.java.additional.6=-Dcom.rsa.netwitness.carlos.common.enableDynamicProp
ertyReader=false

# Initial Java Heap Size (in MB)
#wrapper.java.initmemory=3
```

2. wrapper.java.additional.1=-Xmx8192mを次で置換します。
wrapper.java.additional.1=-Xmx16g
3. SMSサービスを再開します。
systemctl start rsa-sms

NetWitness Suiteでの更新の管理

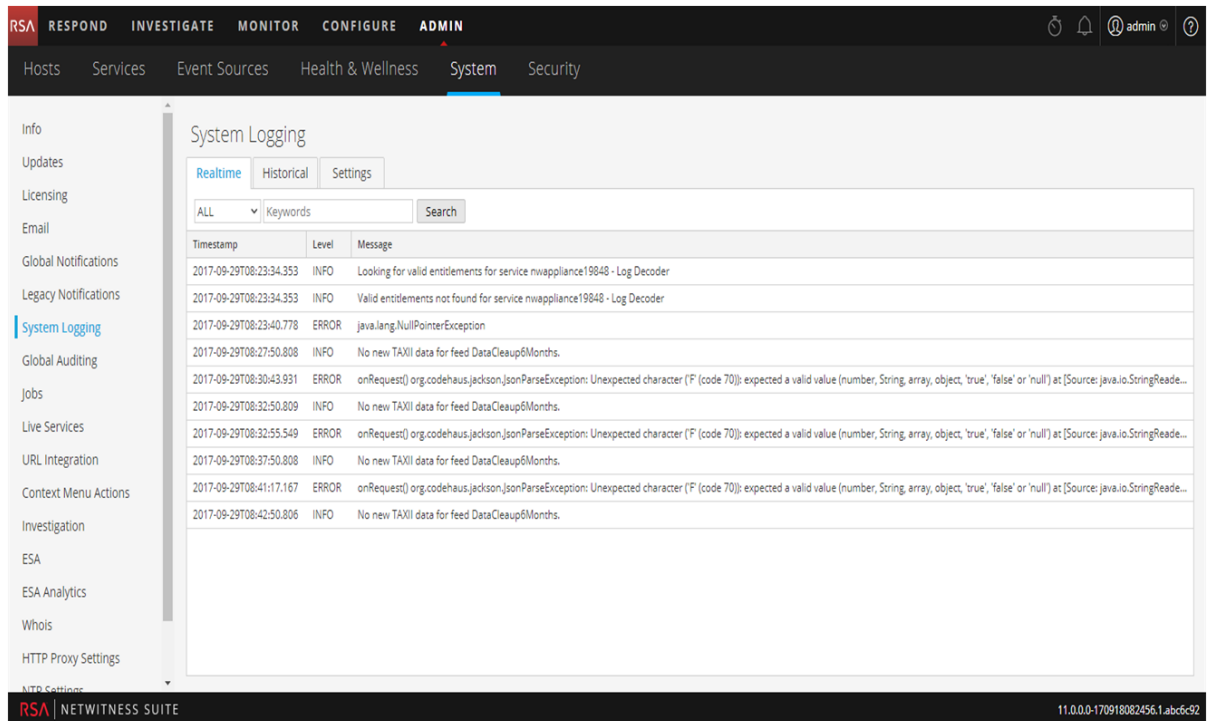
RSAは継続的な製品の改善に努めており、NetWitness Suiteソフトウェアバージョンの更新を定期的に発行します。ソフトウェアバージョンの更新は、リリース、サービスパック、パッチ(セキュリティパッチを含む)に加え、リリース、サービスパック、パッチが依存する補助的ソフトウェアで構成されます。ソフトウェアバージョンの更新のリリースごとにユーザガイドが提供され、更新をインストールするための詳細なステップが記載されています。リリースの更新ガイドをRSA Link (<https://community.rsa.com/community/products/netwitness>) からダウンロードして、記載されているステップに従うことが重要です。詳細情報については、「[ホストおよびサービス スタート ガイド](#)」のトピック「Update Existing Host to New Version」と、「[\[システム\]の\[更新\]パネル - \[設定\]タブ](#)」を参照してください。

システム ログとサービス ログの表示

NetWitness Suiteには、システム ログとサービス ログのビューが用意されています。サービス ログを表示して、サービスやホストに関するメッセージを選択することもできます。

システム ログの表示

1. [管理] > [システム]に移動します。
2. [オプション] パネルで、[システム ログ]を選択します。



Timestamp	Level	Message
2017-09-29T08:23:34.353	INFO	Looking for valid entitlements for service nwappliance19848 - Log Decoder
2017-09-29T08:23:34.353	INFO	Valid entitlements not found for service nwappliance19848 - Log Decoder
2017-09-29T08:23:40.778	ERROR	java.lang.NullPointerException
2017-09-29T08:27:50.808	INFO	No new TAXII data for feed DataCleanup6Months.
2017-09-29T08:30:43.931	ERROR	onRequest() org.codehaus.jackson.JsonParseException: Unexpected character ('F' (code 70)): expected a valid value (number, String, array, object, 'true', 'false' or 'null') at [Source: java.io.StringReade...
2017-09-29T08:32:50.809	INFO	No new TAXII data for feed DataCleanup6Months.
2017-09-29T08:32:55.549	ERROR	onRequest() org.codehaus.jackson.JsonParseException: Unexpected character ('F' (code 70)): expected a valid value (number, String, array, object, 'true', 'false' or 'null') at [Source: java.io.StringReade...
2017-09-29T08:37:50.808	INFO	No new TAXII data for feed DataCleanup6Months.
2017-09-29T08:41:17.167	ERROR	onRequest() org.codehaus.jackson.JsonParseException: Unexpected character ('F' (code 70)): expected a valid value (number, String, array, object, 'true', 'false' or 'null') at [Source: java.io.StringReade...
2017-09-29T08:42:50.806	INFO	No new TAXII data for feed DataCleanup6Months.

サービス ログの表示

NetWitness Suite サービス ログを表示するには、次の手順を実行します。

1. [管理] > [サービス]に移動します。
2. [サービス] グリッドでサービスを選択します。

3. [アクション] 列で、[表示] > [ログ] を選択します。

The screenshot shows the RSA NetWitness Suite interface. At the top, there is a navigation bar with tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. Below this, there is a sub-navigation bar with 'Change Service', 'nwappliance13731 - Broker', and 'Logs'. The main content area is titled 'System Logging' and has two tabs: 'Realtime' (selected) and 'Historical'. Below the tabs, there is a search area with a dropdown menu set to 'ALL', a 'Keywords' input field, a 'Broker' dropdown menu, and a 'Search' button. The main area contains a table of log entries with the following columns: Timestamp, Level, and Message.

Timestamp	Level	Message
2017-09-29T08:48:07.000	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 100000.
2017-09-29T08:48:07.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has logged in
2017-09-29T08:48:07.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has issued values (channel 30906) (thread 2311): fieldName=alert id1=0 id2=0 threshold=100000 size=20 flags=sessions,sort-total,order-descending,ignore-cache where="(device.ip=90.15...
2017-09-29T08:48:07.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has finished values (channel 30906, queued 00:00:00, execute 00:00:00): fieldName=alert id1=0 id2=0 threshold=100000 size=20 flags=sessions,sort-total,order-descending,ignore-cache w...
2017-09-29T08:48:46.000	AUDIT	User admin (session 30839, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30858, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30897, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30868, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30887, 10.31.125.170:46316) has logged out
2017-09-29T08:48:46.000	AUDIT	User admin (session 30829, 10.31.125.170:46316) has logged out

At the bottom of the interface, there is a footer with 'RSA | NETWITNESS SUITE' on the left and '11.0.0.0-170918082456.1.lab6c92' on the right.

ログ エントリーのフィルタ

[リアルタイム] タブで表示されている結果をフィルタするには、次の手順を実行します。

- (オプション) システム ログとサービス ログでは、[ログレベル] や [キーワード] を選択します。システム ログには、ログレベルが7種類あります。サービス ログには [トレース] レベルがないため、ログレベルは6種類です。デフォルトは、[すべて] になっています。
- (オプション) サービス ログの場合は、[サービス] でホストまたはサービスを選択します。
- [フィルタ] をクリックします。

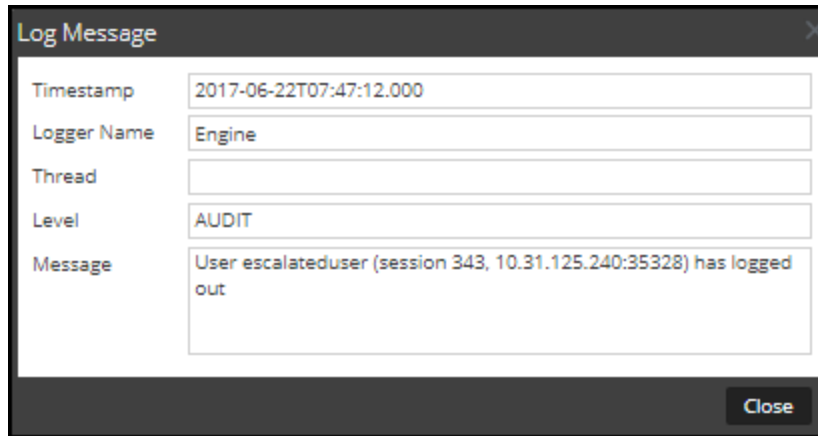
ビューが更新され、フィルタに一致する最新の10件のエントリーが表示されます。フィルタ条件に合致する新しいログ エントリーが記録されると、ビューが更新され、エントリーが表示されます。

ログ エントリーの詳細を表示

ログ グリッドの [リアルタイム] タブの各行に、ログ エントリーのサマリ情報が記載されています。詳細を表示するには、次の手順を実行します。

1. ログ エントリーをダブルクリックします。

[ログ メッセージ] ダイアログが表示され、[タイムスタンプ]、[ロガー名]、[スレッド]、[レベル]、[メッセージ]の各項目が表示されます。



2. 確認したら[閉じる]をクリックします。

Reporting Engineのログ ファイルへのアクセス

すべてのログ ファイル

Reporting Engineは次のログを`rsasoc/rsa/soc/reporting-engine/log`ディレクトリに格納しています。

- `reporting-engine.log`ファイルに最新のログが保存されます。
- `reporting-engine.log.*`ファイルに、以前のログのバックアップ コピーコピーが保存されます。
- 次の形式の名前が付いたファイルに、すべてのUNIXスクリプト ログを記録しています。
`reporting-engine.sh_timestamp.log`(たとえば、`reporting-engine.sh_20120921.log`)。

Reporting Engineは、ごくまれにコマンド ライン エラー メッセージを`rsasoc/nohup.out`ファイルに書き込むことがあります。

Upstartログ

Reporting Engineは、UpstartデーモンおよびReporting Engineの起動コマンドが書き込むログ メッセージと出力を`/var/log/secure`ディレクトリに追加します。

Upstartログ ファイルは、rootユーザのみが読み取り可能なシステム ログログ ファイルです。Reporting Engineは、ログ ファイルの生成、以前のログ ファイルのバックアップ コピーの保持、UNIXスクリプト ログ ファイルの格納、Upstartログ ファイルの別のディレクトリへの追加を行います。

履歴ログの検索とエクスポート

NetWitness Suiteでは、NetWitness Suiteログまたはサービス ログの表示と検索をページ形式で行うことができます。最初のロード時、グリッドには、システムまたはサービスのログ エントリーの最新情報のページが表示されます。履歴ログビューでは、ログをエクスポートできます。

システムログの履歴の表示

システムの履歴ログを表示するには、次の手順を実行します。

1. [管理] > [システム]に移動します。
2. [オプション]パネルで、[システム ログ]を選択します。
[システム ログ]パネルが開き、デフォルトで[リアルタイム]タブが表示されます。
3. [履歴]タブをクリックします。
システムの履歴 ログのリストが表示されます。

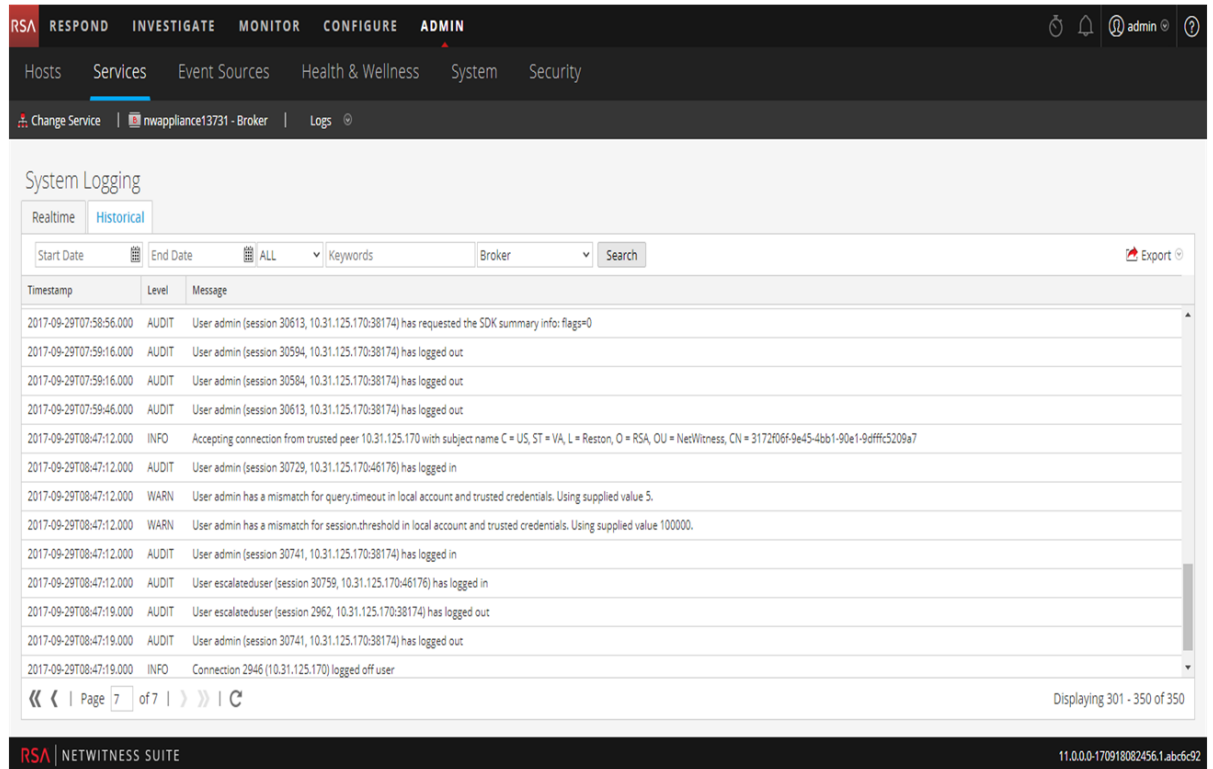
The screenshot shows the NetWitness Suite interface with the 'System Logging' section active. The 'Historical' tab is selected, and a table of log entries is displayed. The table has columns for Timestamp, Level, and Message. The entries show various system events, including looking for valid entitlements for services like Event Stream Analysis, Broker, Malware Analytics, and Concentrator, as well as starting Telemetry Rule Stat Collection for endpoints. One entry shows an error: 'java.lang.IllegalArgumentException: escalateduser'. The interface also includes search filters for Start Date, End Date, and Keywords, and an Export button.

Timestamp	Level	Message
2017-06-22T21:00:02.024	INFO	Looking for valid entitlements for service Event Stream Analysis
2017-06-22T21:00:02.024	INFO	Valid entitlements not found for service Event Stream Analysis
2017-06-22T21:00:02.026	INFO	Looking for valid entitlements for service Broker
2017-06-22T21:00:02.026	INFO	Valid entitlements not found for service Broker
2017-06-22T21:00:02.029	INFO	Looking for valid entitlements for service Malware Analytics
2017-06-22T21:00:02.029	INFO	Valid entitlements not found for service Malware Analytics
2017-06-22T21:00:02.032	INFO	Looking for valid entitlements for service Concentrator
2017-06-22T21:00:02.032	INFO	Valid entitlements not found for service Concentrator
2017-06-22T21:00:02.035	INFO	Looking for valid entitlements for service Log Decoder
2017-06-22T21:00:02.036	INFO	Valid entitlements not found for service Log Decoder
2017-06-22T21:05:02.200	ERROR	java.lang.IllegalArgumentException: escalateduser
2017-06-22T21:05:02.241	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.242	INFO	Starting Telemetry Parsers Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.287	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Concentrator]
2017-06-22T21:05:02.287	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Decoder]
2017-06-22T21:05:02.287	INFO	Starting Telemetry Parsers Stat Collection for Endpoint [Decoder]
2017-06-22T21:05:02.341	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.341	INFO	Starting Telemetry Parsers Stat Collection for Endpoint [Log Decoder]
2017-06-22T21:05:02.419	INFO	Starting Telemetry Rule Stat Collection for Endpoint [Concentrator]
2017-06-22T21:46:21.806	WARN	No Features Available in LLS

サービス ログの履歴の表示

サービスの履歴ログを表示するには、次の手順を実行します。

1. [管理] > [サービス] を選択します。
2. サービスを選択します。
3. [アクション] 列で、[表示] > [ログ] を選択します。
[サービス] の [ログ] ビューが表示され、[リアルタイム] タブが開きます。
4. [履歴] タブをクリックします。
選択したサービスの履歴 ログのリストが表示されます。



ログ エントリーの検索

[履歴] タブで表示される結果をフィルタするには、次の手順を実行します。

1. (オプション) [開始日] および [終了日] を選択します。オプションで [開始時刻] での時間、および [終了時刻] での時間を選択します。
2. (オプション) システム ログとサービス ログでは、[ログレベル] や [キーワード] を選択します。システム ログには、ログレベルが7種類あります。サービス ログには [トレース] レベルがないため、ログレベルは6種類です。デフォルトは、[すべて] になっています。
3. (オプション) サービス ログの場合は、[サービス] でホストまたはサービスを選択します。
4. [検索] をクリックします。
ビューが更新され、フィルタに一致する最新の10件のエントリーが表示されます。フィルタ条

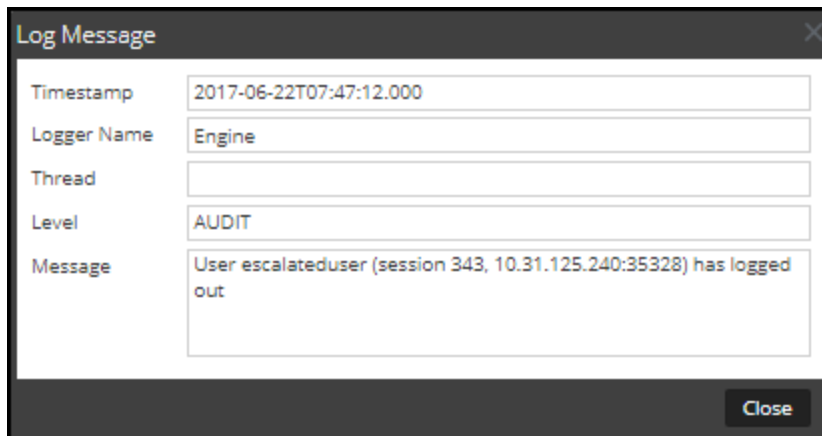
件に合致する新しいログエントリが記録されると、ビューが更新され、エントリが表示されます。

ログエントリの詳細を表示

ロググリッドの[履歴]タブの各行に、ログエントリのサマリ情報が記載されています。ログメッセージの詳細をすべて表示するには、次の手順を実行します。

1. ログエントリをダブルクリックします。

[ログメッセージ]ダイアログが表示され、[タイムスタンプ]、[ロガー名]、[スレッド]、[レベル]、[メッセージ]の各項目が表示されます。



2. 確認したら[閉じる]をクリックします。

ダイアログが閉じます。

ログエントリのページの操作

グリッドの下部にあるページ移動ツールを使用して、別のページに表示されているログエントリを表示できます。

- ナビゲーション ボタンの使用
- 表示したいページ番号を手動で入力し、Enterキーを押します。

ログファイルのエクスポート

現在のビューに表示されているログをエクスポートするには、次の手順を実行します。

[エクスポート]をクリックして、ドロップダウン オプション [CSV形式]または[タブ区切り]のいずれかを選択します。

ログタイプとフィールド区切り文字が識別可能なファイル名の付いたファイルがダウンロードされます。たとえば、CSV形式でエクスポートされたNetWitness Suiteシステム ログの名前は、UAP_log_export_CSV.txtとなり、タブ区切り形式でエクスポートされたホスト ログの名前は、APPLIANCE_log_export_TAB.txtとなります。

URL統合を使用したクエリのメンテナンス

URL統合機能では、[ナビゲート]ビューでサービスを調査するときに、ユーザが使用した階層リンクまたはクエリパスを管理します。これらのオブジェクトを頻繁に表示して編集する必要はありません。

URL統合では、Investigationでデータをドリルダウンするときに[ナビゲート]ビューのナビゲートリンクをクリックするたびに自動的に一意のIDが作成されます。ドリルダウンが完了すると、URLは現在のドリルダウンポイントのクエリIDを反映します。[表示名]は、[ナビゲート]ビューで階層リンクに表示されます。

[URL統合]パネルではドリルダウンで使用されたクエリのリストが保持され、適切な権限を持つユーザがこのクエリを編集したり、NetWitness Suiteの他のユーザのクエリパターンを解析することを可能にします。パネルでは、次のことを実行できます。

- リストの更新。
- クエリの編集。
- クエリの削除。
- リストのすべてのクエリのクリア。

注意: システムからクエリを削除すると、そのクエリIDは参照できなくなります。


クエリの編集

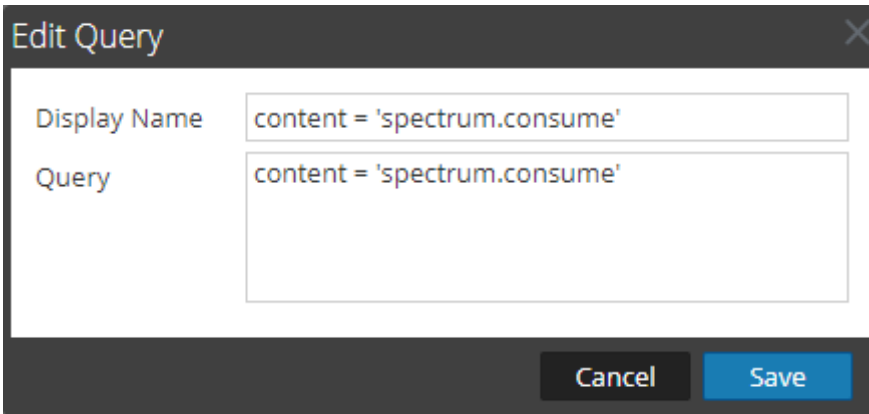
1. [管理] > [システム]に移動します。
2. オプション パネルで、[URL統合]を選択します。

URL Integration				
ID	Display Name	Query	Username	When Created ^
0	nwappliance11639	did = 'nwappliance11639'	admin	Tue Jul 11 2017 06:40:09 +00:00 (UTC)
1	threat.category = 'spe...	threat.category = 'spectrum'	admin	Tue Jul 11 2017 08:35:33 +00:00 (UTC)
2	content = 'spectrum.c...	content = 'spectrum.consume'	admin	Tue Jul 11 2017 08:41:33 +00:00 (UTC)
3	content = 'spectrum.a...	content = 'spectrum.analyze'	admin	Tue Jul 11 2017 08:46:09 +00:00 (UTC)
4	gwu.edu	domain.dst = 'gwu.edu'	admin	Tue Jul 11 2017 09:37:28 +00:00 (UTC)
5	10.100.33.1	ip.src = 10.100.33.1	admin	Wed Jul 12 2017 08:48:56 +00:00 (UTC)
6	ip.src = '127.0.0.1'	ip.src = 127.0.0.1	admin	Wed Jul 12 2017 09:35:24 +00:00 (UTC)
7	tcp.srcport = '54004'	tcp.srcport = 54004	admin	Wed Jul 12 2017 09:37:44 +00:00 (UTC)
8	nwappliance23912	did = 'nwappliance23912'	admin	Wed Jul 12 2017 11:09:05 +00:00 (UTC)
9	gwu.edu	domain.src = 'gwu.edu'	admin	Thu Jul 13 2017 13:58:52 +00:00 (UTC)
10	OTHER	service = 0	admin	Fri Jul 14 2017 04:56:50 +00:00 (UTC)
11	test dom	alert = 'test dom'	admin	Fri Jul 14 2017 09:59:43 +00:00 (UTC)

Page 1 of 1

Displaying 1 - 12 of 12

3. グリッドの列を選択し、列をダブルクリックするか、またはをクリックします。
[クエリの編集]ダイアログが表示されます。




4. [表示名]と[クエリ]を編集できます。どちらのフィールドも空白にはできません。
5. 変更を保存するには、[保存]をクリックします。

クエリの削除


注意: システムからクエリを削除すると、そのクエリIDは参照できなくなります。

NetWitness Suiteからクエリを完全に削除するには、次を行います。

1. [URL統合]パネルでクエリを選択します。
2. をクリックします。
クエリを削除するかどうかを確認するダイアログが表示されます。
3. はいをクリックします。

すべてのクエリのクリア

リストからすべてのクエリをクリアするには、次を行います。

-  Clear をクリックします。
リスト全体がクリアされます。

URIでのクエリの使用

URL統合は、NetWitness Suiteアーキテクチャに対する検索を可能にすることによって、サードパーティ製品との統合を容易に構成できるようにします。URIにクエリを記述することにより、カスタムリンクを作成可能なサードパーティ製品から、NetWitness Suiteの[調査]ビューの特定のドリルダウンポイントに直接アクセスできます。

URLエンコードクエリを使用してURIを入力するためのフォーマットは次のとおりです。

```
http://<nw host:port>/investigation/<serviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

各変数の意味は以下のとおりです

- **<nw host: port>**は、IPアドレスまたはDNS名で、必要に応じて、ポート(SSLの場合等)を指定します。ポート番号は、プロキシ使用時など非標準ポートでアクセスを構成する場合に必要です。
- **<serviceId>**はNetWitness Suiteインスタンスの内部サービスIDで、クエリの対象を指定します。サービスIDは、常に整数です。サービスIDは、NetWitness Suiteから[調査]ビューにアクセスする際にURLで確認できます。この値は、調査対象となるサービスによって変わります。
- **<encoded query>**は、URLエンコードされたNetWitness Suiteクエリです。クエリの長さはHTMLのURL制限で制限されています。
- **<start date>**および**<end date>**は、クエリの日付範囲を定義します。形式は<yyyy-mm-dd>T<hh:mm>です。start date(開始日)とend date(終了日)は指定が必要なパラメータです。相対日付範囲(たとえば、「直近1時間」など)はサポートされていません。すべての時間はUTCとして処理されます。

例:

```
http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00/2012-10-31T00:00
```

例

次のクエリの例では、NetWitnessサーバが192.168.1.10で、サービスIDが2に指定されています。

2013年3月12日の午前5:00から午前6:00までのすべてのアクティビティで、alias host(ホスト名)が存在するデータ

- カスタムピボット : alias.host exists
- https://192.168.1.10/investigation/2...13-03-12T06:00

2013年3月12日の午後5:00から午後5:10までのすべてのアクティビティで、IPアドレス10.10.10.3において送受信されるhttpトラフィック

- カスタムピボット : service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)
- ピボットのエンコード :
 - service=80 => service&3D80
 - ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
 - ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3
 - https://192.168.1.10/investigation/2...13-03-12T17:10

追加の注意事項

一部の値はエンコードする必要がない場合があります。たとえば、クエリにip.srcとip.dstを指定する場合、これらのパラメータはエンコードせずに参照することが可能です。

FIPSサポート

NetWitness Suite 11.0.0には、NetWitness Suite内のすべての暗号化操作をサポートするFIPS認定140-2暗号形式モジュールが付属しています。NetWitness Suiteは、レベル3設計保証をサポートする次の2つのモジュールを活用します。

- RSA BSAFEBSAFE Crypto-J
- OpenSSL with BSAFE(OWB)

どちらのモジュールも、標準NetWitness Suite構成と同等の運用環境で認定されています。

デフォルトでは、暗号形式モジュールは、可能な限りFIPS認定の暗号スイートを強制的に使用します。例外については、以下の情報およびリリースノートを参照してください。FIPSモジュールの詳細については、<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>を参照してください。

RSA BSAFEBSAFE Crtypo-J FIPS証明書の番号は2468で、OWB FIPS証明書は証明書番号2300でRSA BSAFEBSAFE Crypto-C Micro Editionに含まれています。

11.0.0.0では、FIPSはLog Collectorを除くすべてのサービスで有効です。これには、10.6.4.xでFIPSが有効であった場合のLog DecoderとDecoderが含まれます。Log Collector、Log DecoderおよびDecoderを除くどのサービスでもFIPSを無効にできません。

注: 11.0.0.0を新規にインストールする場合、デフォルトでは、Log CollectorとLog Decoderを除くすべてのコアサービスにFIPSが適用されます。Log Collector、Log DecoderおよびPacket Decoderを除くどのサービスでもFIPSを無効にできません。

注: 10.6.4.xから11.0.0.0にアップグレードする場合は、Log Collector、Log Decoder、およびDecoderサービスに次の条件が適用されます。

- Log Collectorは、10.6.4.xでFIPSが有効であった場合でも、11.0.0.0へのアップグレード後FIPSは有効になっていません。11.0.0.0にアップグレードした後にFIPSのサポートを有効にする必要があります。「[Log CollectorでのFIPSのサポート](#)」の手順を参照してください。
- 10.6.4.xでLog DecoderとPacket Decoderサービスに対してFIPSが有効であった場合は、11.0.0.0でもFIPSは有効です。ただし、Log DecoderとPacket Decoderが10.6.4.xでFIPSが有効になっていなかった場合、11.0.0.0でもFIPSは有効になりません。必要に応じて、これらのサービスに対してFIPSを手動で有効化する必要があります。「[Log DecodersおよびDecoderでのFIPSのサポート](#)」の手順を参照してください。

Log CollectorでのFIPSのサポート

Log CollectorでFIPSを有効にするには、次の手順を実行します。

1. Log Collectorサービスを停止します。
2. `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`ファイルを開きます。
3. ここで説明するように、次の変数の値をoffに設定します。
`Environment="OWB_ALLOW_NON_FIPS=on"`
から以下に変更します。
`Environment="OWB_ALLOW_NON_FIPS=off"`
4. 次のコマンドを実行して、システムデーモンを再ロードします。
`systemctl daemon-reload`
5. Log Collectorサービスを再開します。
6. UIで、Log CollectorサービスにFIPSモードを設定します。

注:このステップは、10.6.4から11.0.0.0にアップグレードし、FIPSが10.6.4で有効になっていた場合は不要です。

- a. [管理]>[サービス]に移動します。
- b. Log Collectorサービスを選択し、[表示]>[構成]に移動します。
- c. SSL FIPSモードで、[構成]の下のチェックボックスを選択し、[適用]をクリックします。

Log DecodersおよびDecoderでのFIPSのサポート

10.6.4.xでFIPSが有効になっていなかったLog DecoderおよびDecoderでFIPSを有効にするには、次の手順を実行します。

1. [管理]>[サービス]に移動し、Log DecoderまたはPacket Decoderサービスを選択します。
2. [表示]>[構成]を選択し、[システム構成]で[構成]列のチェックボックスを選択して[SSL FIPS Mode]を有効にします。
3. サービスを再起動します。
4. [適用]をクリックします。

NetWitness Suiteのトラブルシューティング

NetWitness Suiteのトラブルシューティングの詳細については、次の各トピックを参照してください。

- 「[デバッグ情報](#)」
- 「[エラー通知](#)」
- 「[その他のヒント](#)」
- 「[NwLogPlayer](#)」
- 「[Feedのトラブルシューティング](#)」

デバッグ情報

NetWitness Suiteログファイル

NetWitness Suiteのログ情報は次のファイルに記録されます。

コンポーネント	ファイル
rabbitmq	/var/log/rabbitmq/nw@localhost.log /var/log/rabbitmq/nw@localhost-sasl.log
collectd	/var/log/messages
nwlogcollector	/var/log/messages
nwlogdecoder	/var/log/messages
sms	/opt/rsa/sms/wrapper.log
sms	/opt/rsa/sms/logs/sms.log
sms	/opt/rsa/sms/logs/audit/audit.log
NetWitness Suite	/var/lib/netwitness/uax/logs/nw.log
NetWitness Suite	/var/lib/netwitness/uax/logs/ audit/audit.log
NetWitness Suite	/opt/rsa/jetty9/logs

関係するファイル

次のファイルは主要なNetWitness Suiteのコンポーネントで使用され、さまざまな問題を追求する際に役立ちます。

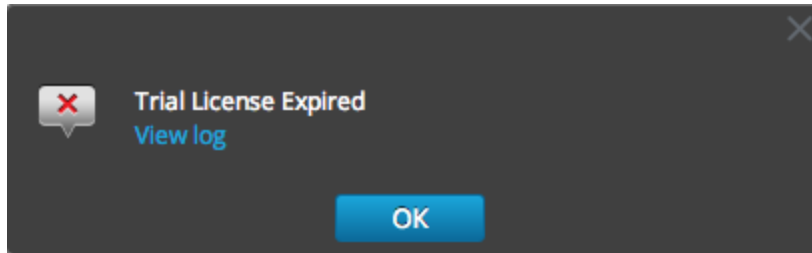
コンポーネント	ファイル	説明
rabbit	/etc/rabbitmq/rabbitmq.config	RabbitMQの構成ファイル。この構成ファイルによってRabbitMQの一部の動作、特にネットワークやSSLの設定に関する部分の動作が決まります。
rabbit	/etc/rabbitmq/rabbitmq-env.conf	RabbitMQの環境構成ファイル。このファイルではRabbitMQのノード名と有効なプラグインファイルの場所を指定します。
rabbit	/etc/rabbitmq/rsa_enabled_plugins	このファイルではRabbitMQの有効なプラグインをリストします。このファイルはRabbitMQサーバによって、rabbitmq-pluginsコマンドを使用して管理されます。Log Collectorを以前のバージョンからアップグレードする際の問題を回避するために、このファイルによって/etc/rabbitmq/enabled_pluginsが上書きされます。
rabbit	/etc/rabbitmq/ssl/truststore.pem	RabbitMQのトラストストア。このファイルには信頼できるCAのPEMエンコードされたX.509証明書が格納されます。RabbitMQに接続し、このリストに記載されたCAで署名された証明書を提示するクライアントは、信頼できるクライアントと見なされます。

コンポーネント	ファイル	説明
rabbit	/var/log/rabbitmq/mnesia/nw@localhost	<p>RabbitMQのMnesiaディレクトリ。MnesiaはErlang/OTPのデータベーステクノロジーであり、Erlangオブジェクトを永続的に格納するためのものです。RabbitMQでは、ポリシーの現在の設定、永続的な交換、クエリなどの情報を格納するために、このテクノロジーを使用しています。</p> <p>msg_store_persistentディレクトリとmsg_store_transientディレクトリは、RabbitMQがディスクにスプールするメッセージを格納する重要な場所です。たとえばメッセージが永続的なメッセージとして発行された場合や、メモリの制限によってディスクにページングされた場合などです。RabbitMQでメモリに関するアラームが発生した場合は、このディレクトリを確認してください。</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>注意: これらのファイルを手動で削除しないでください。キューをページまたは削除するにはRabbitMQツールを使用してください。これらのファイルを手動で変更すると、RabbitMQのインスタンスが動作しなくなることがあります。</p> </div>

エラー通知

NetWitness Suiteには、さまざまなコンポーネントおよび操作に関連する一連のエラーメッセージタイプがあります。NetWitness Suiteでは、シンプルなエラー通知およびログエントリーの形でフィードバックを表示できます。

エラー通知ダイアログが表示された場合、確認する方法が2種類あります。メッセージを確認するか、システムログを表示して詳細を確認します。



エラー通知が表示されたときに、システムログを表示して詳細を確認する場合は、[ログの表示]をクリックします。[管理]>[システム]ビューでログが開き、メッセージのリストが表示されます。タイムスタンプとメッセージレベルも表示されます。

Timestamp	Level	Message
2014-03-14T19:01:49.501	WARN	Failed setup yum service for device [REDACTED]
2014-03-14T19:02:53.907	ERROR	Unable to connect to endpoint vives:// [REDACTED]
2014-03-14T19:02:53.913	WARN	Failed setup yum service for device [REDACTED]
2014-03-14T19:03:23.925	ERROR	Timeout waiting for task. java.util.concurrent.TimeoutException: Timeout waiting for task. at c [REDACTED]
2014-03-14T19:03:23.926	WARN	Failed setup yum service for device [REDACTED]
2014-03-14T19:03:23.941	ERROR	Unable to connect to endpoint [REDACTED]
2014-03-14T19:03:23.942	WARN	Failed setup yum service for device [REDACTED]
2014-03-14T19:03:36.2	ERROR	Unable to connect to endpoint [REDACTED]
2014-03-14T19:03:36.11	WARN	Error occurred during applying system updates [REDACTED] YumSetupFail [REDACTED]
2014-03-14T19:05:44.120	ERROR	java.lang.Exception: Trial license does not match [REDACTED]

その他のヒント

管理者アカウントの保護

RSA LinkのNetWitness Suiteドキュメントで公開されているSTIG Hardening Guide (<https://community.rsa.com/docs/DOC-64211>)を参照してください。

監査ログログメッセージ

どのユーザアクションがどのログメッセージタイプの原因となったかを、`/var/log/messages`ファイルで確認できます。

Log Parserパッケージ(NetWitness Suite Parser v2.0.zip) に含まれているイベント カテゴリスプレッドシートには、イベント カテゴリとイベントのリストが示されており、レポート、アラート、クエリのビルドに役立てることができます。

NwConsoleによるチェック

RSAは、logParseというコマンド オプションをNwConsoleに追加しました。このコマンド オプションにより、ログをパースするために完全なシステムを用意しなくても、Log Parserを簡単にチェックすることができます。logParseコマンドの詳細については、コマンド ラインで「help logParse」と入力してください。

シッククライアント エラー: リモート コンテンツ デバイス エントリーが見つからない

エラー:「*The remote content device entry was not found*」が、Concentratorに適用した関連ルールで報告されます。

問題: Investigationで、Alertメタ キーのcorrelation-rule-nameメタ値をクリックしても、セッション情報は表示されません。

解決策 DecoderおよびConcentratorで関連ルールを使用する代わりに、ESAルールを使用します。ESAルールでは、ESAルールと一致する関連セッションを記録します。

サンプルParserの入手

FLEX ParserおよびLUA Parserは暗号化された状態でLiveから配布されるため、内容を表示できません。

ただし、暗号化されていないサンプルを、<https://community.emc.com/docs/DOC-41108>から入手できます。

WinRMイベント ソースの構成

このInside EMCの記事(<https://inside.emc.com/docs/DOC-122732>) には、Windows RM (Remote Management) コレクションの設定プロセスについて説明した動画が含まれています。

また、「Windowsイベント ソース構成ガイド」で説明する手順のショートカットである2つのスクリプトも含まれています。

NwLogPlayer

NwLogPlayerはSyslogトラフィックをシミュレートするユーティリティです。ホストされた環境において、NwLogPlayer.exeはRSA NetWitness® Suiteクライアント マシンのコマンド ライン ユーティリティとして次のディレクトリに配置されます。

```
C:\Program Files\NetWitness\NetWitness 9.8
```

また、NwLogPlayerはLog Decoderホストの/usr/binディレクトリにも配置されています。

使用方法

コマンドラインでnwlogplayer.exe -hと入力すると、次のように使用可能なオプションのリストが表示されます。

```
--priority arg      ログの優先度レベルの設定

-h [ --help ]      このメッセージを表示

-f [ --file ] arg   メッセージの入力元、デフォルトはstdin
(=stdin)

-d [dir ] arg      入力ディレクトリ

-s [ --server ]     リモート サーバを指定。デフォルトはlocalhost
arg (=localhost)

-p [ --port ] arg   リモート ポートを指定。デフォルトは514
(=514)

-r [ --raw ] arg    rawモードを指定します。
(=0)


- 0 =優先マークを追加(デフォルト)
- 1 =ファイル コンテンツがサーバに1行ずつコピーされる
- 3 =自動検出
- 4 =enVisionストリーム
- 5 =バイナリオブジェクト



-m [ --memory ]    スピード テスト モード。最大1メガバイトのメッセージをファイル コンテ
arg                ンツから読み取り、再生する。

--rate arg         1秒あたりのイベント数。プログラムが継続的に達成できるepsがrate
より小さい場合には、この引数には効果はありません。

--maxcnt arg       送信するメッセージの最大数

-c [ --
multiconn ]       複数の接続

-t [ --time ] arg  タイムスタンプの時刻のシミュレート。形式はyyyy-m-d-hh:mm:ss

-v [ --verbose ]   trueの場合、詳細な出力を行う
```

<code>--ip arg</code>	IPタグのシミュレート
<code>--ssl</code>	SSL接続を使用する
<code>--certdir arg</code>	OpenSSL認証局のディレクトリ
<code>--clientcert arg</code>	PEMエンコードされたSSLクライアント証明書を指定
<code>--udp</code>	UDPで送信

Feedのトラブルシューティング

概要

Feedジェネレーターの目的は、イベントソースを、それが属するグループのリストにマッピングすることです。

イベントソースからメッセージを収集しているのに、そのイベントソースが、正しいイベントソースグループに表示されない場合は、このトピックで説明する背景情報が問題の追跡に役立ちます。

詳細

ESM Feedでは複数のキーを1つの値にマッピングします。つまり、DeviceAddress、Forwarder、DeviceTypeの属性をgroupNameにマッピングします。

ESM Feedの目的は、Log Decoderで収集されるイベントソースのメタにgroupNameを追加することです。

仕組み

Feedジェネレーターは1分ごとに更新するようスケジュール設定されています。しかし、実際にトリガーされるのはイベントソースまたはグループに何らかの変更(作成、更新、削除)が行われた場合だけです。

Feedジェネレーターは、イベントソースとグループのマッピングを指定したFeedファイルを1つ作成し、同じFeedをNetWitness Suiteに接続するすべてのLog Decoderにプッシュします。

Log DecoderにFeedファイルがアップロードされると、新しく受信するイベントのメタデータにはgroupNameが追加され、このgroupNameがlogstatsに追加されます。

groupNameがlogstatsに追加されると、ESM Aggregatorによって情報がグループ化され、ESMに送信されます。この時点で、[イベントソースモニタリング]タブに[グループ名]列が表示されます。

上記のすべての処理が完了するにはある程度時間がかかります。そのため、新しいグループやイベントソースを追加した後は、そのグループ名が表示されるまでしばらく待たなければならない場合があります。

注: Feedの更新によりイベントソースタイプ属性が変更されると、NetWitness Suiteによって新しいlogstatsエントリーが追加されます。既存のエントリーが更新されることはありません。したがって、Log Decoderに2つの異なるlogstatsエントリーができることになります。それまでの既存のメッセージは元のタイプの下にリストされ、新しいメッセージはすべて、新しいイベントソースタイプとして記録されます。

Feedファイル

Feedファイルの形式は次のようになっています。

DeviceAddress, Forwarder, DeviceType, GroupName

DeviceAddressは、ipv4、ipv6とhostnameのいずれかです。これは、イベントソースがどのように定義されているかによって決まります。

Feedファイルの例を次に示します。

```
"12.12.12.12", "d6", "NETFLOW", "grp1"
"12.12.12.12", "ld4", "netflow", "grp1"
"12.12.12.12", "d6", "netfow", "grp1"
"0:E:507:E6:D4DB:E:59C:A", "10.25.50.243", "apache", "Apachegrp"
"1.2.3.4", "LCC", "apache", "Apachegrp"
"10.100.33.234", "LC1", "apache", "Apachegrp"
"10.25.50.248", "10.25.50.242", "apache", "Apachegrp"
"10.25.50.251", "10.25.50.241", "apache", "Apachegrp"
"10.25.50.252", "10.25.50.255", "apache", "Apachegrp"
"10.25.50.253", "10.25.50.251", "apache", "Apachegrp"
"10.25.50.254", "10.25.50.230", "apache", "Apachegrp"
"10.25.50.255", "10.25.50.254", "apache", "Apachegrp"
"13.13.13.13", "LC1", "apache", "Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7", "apache", "Apachegrp"
"Appliance1234", "apache", "Apachegrp"

"CB:F255:9:8:6C88:EEC:44CE:7", "10.25.50.253", "apache", "Apachegrp"
```

トラブルシューティング

問題が発生している場所を絞り込むには、次の項目を確認してください。

Feedファイルの有無

FeedのZIPアーカイブが次の場所にあることを確認してください。

/opt/rsa/sms/esmfeed.zip

このファイルは変更しないでください。

Log Decoderが使用するグループ メタ

グループ メタがLog Decoderに読み込まれていることを確認します。Log DecoderのRESTにアクセスし、logstatsを確認します。

```
http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain
```

これはグループの情報が含まれるlogstatsファイルのサンプルです。

```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4 count=338
lastSeenTime=2015-Feb-04 22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group , apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304 source=5.6.7.8
count=1301 lastSeenTime=2015-Feb-04 22:30:19 lastUpdatedTime=2015-Feb-
04 22:30:19 groups=AllOtherGroup , ApacheTomcatGroup
```

グループ情報が太字で表示されています。

Concentratorでのデバイス グループ メタの確認

Device GroupメタがConcentratorに存在し、イベントにdevice.groupフィールドの値が表示されることを確認します。

Device Group (8 values) 
[testgroup \(28,878\)](#) - [localgroup \(3,347\)](#) - [squid \(3,346\)](#) - [allothergroup \(780\)](#) - [apachetomcatgroup \(561\)](#) - [ip1234group \(457\)](#) - [cacheflowelff \(219\)](#) - [apachegroup \(91\)](#)

```
sessionid      = 22133
time           = 2015-02-05T14:35:03.0
size          = 91
lc.cid         = "NWAPPLIANCE10304"
forward.ip     = 127.0.0.1
device.ip      = 20.20.20.20
medium        = 32
device.type    = "unknown"
device.group  = "TestGroup"
kig_thread    = "0"
```

SMSのログ ファイル

次の場所にあるSMSのログ ファイルをチェックして、情報メッセージやエラー メッセージを確認します。/opt/rsa/sms/logs/sms.log

次に情報メッセージの例を示します。

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDecoder : <logdecoder IP>
```

次にエラーメッセージの例を示します。

```
Error creating CSV File : <reason>Unable to push the ESM Feed: Unable to
create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> : Error: <error>
Unable to push the ESM Feed: CSV file is empty, make sure you have al-
least on group with al-least one eventsources.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file on LogDecoder-
<logdecoderIP>Unable to push the ESM Feed:
admin@<logdecoderIP>:50002/decoder/parsers received error: The zip
archive "/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could not be
opened
Unable to push the ESM Feed: <reason>
```

ESMReaderおよびESMAggregatorによるLogstatsデータの読み取りおよび公開を確認

logstatsがcollectdによって収集され、イベントソース管理モジュールに対して公開されていることを確認します。

ESMReader

1. LogDecoderでdebug "true"フラグを/etc/collectd.d/NwLogDecoder_ESM.confに追加します。

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">        port        "56002"
        ssl            "yes"
        keypath        "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
```



```

4838-a2f7- ba7e9a165aae.pem"
    certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7- ba7e9a165aae.pem"
    interval  "600"
    query     "all"
    <stats>      </stats>    </Module>    <Module
"NgEsmReader" "update">      port      "56002"
    ssl         "yes"
    keypath     "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7- ba7e9a165aae.pem"
    certpath   "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7- ba7e9a165aae.pem"
    interval   "60"
    query      "update"
    <stats>      </stats>    </Module></Plugin>

```

2. collectd service restart
コマンドを実行します。

3. 次のコマンドを実行します。

```
tail -f /var/log/messages | grep collectd
```

ESMReaderがlogstatsを読み込んでおり、エラーが発生していないことを確認します。読み取りの問題が発生している、次のようなエラーが表示されます。

```
Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
all: error getting ESM data for field "groups" from logstat
device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
<reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
NgEsmReader_update: error getting ESM data for field "forwarder" from
logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
```

ESMAggregator

1. NetWitness Suiteで、`/etc/collectd.d/ESMAggregator.conf`の中のverboseフラグのコメントを解除します。

```

# ESMAggregator module collectd.conf configuration file
#
# Copyright (c) 2014 RSA The Security Divsion of EMC
#

```

```

<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"

<Module "ESMAggregator">
    verbose 1
    interval "60"
    cache_save_interval "600"
    persistence_dir "/var/lib/netwitness/collectd"
</Module>    </Plugin>

```

2. 次を実行します。

collectd service restart。

3. 次のコマンドを実行します。

```
run "tail -f /var/log/messages | grep ESMA"
```

ESMAggregatorのデータを検索し、logstatエントリがログの中に含まれているかどうかを確認します。

サンプル出力：

```

Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:

```

```
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

JMX Feedジェネレーター ジョブのインターバルの構成

Feedジェネレーター ジョブはデフォルトでは1分ごとに実行されるようスケジュールされています。必要に応じてjconsoleを使用してこれを変更できます。

Feedジェネレーター ジョブのインターバルを変更するには、次の手順を実行します。

1. SMSサービス用のjconsoleを開きます。
2. [MBeans]タブで、[com.rsa.netwitness.sms] > [API] > [esmConfiguration] > [Attributes]に移動します。
3. FeedGeneratorJobIntervalInMinutesプロパティの値を変更します。
4. 同じナビゲーション ツリーの下にある[Operations]で[commit()]をクリックします。この操作により、/opt/rsa/sms/confにある対応するjsonファイルに新しい値が永続的に設定され、SMS再起動時にはこの値が使用されます。

新しい値を設定すると、新しいインターバルでFeedジェネレータージョブが再スケジュールされます。

参考情報

このセクションでは、システムメンテナンスタスクを実行できるNetWitness Suiteユーザインタフェースビューについて説明します。このインタフェースを使用して、次の操作を実行します。

- サービスを監視および維持します(設定、統計、コマンドとメッセージの構文、REST API、RSAコンソールユーティリティ、NetWitness Suiteがサポートするプロトコルを含みます)。
- 現在のNetWitness Suiteバージョンとライセンスのステータスを表示します。
- ホストに適用するソフトウェアバージョン更新を保存するローカル更新リポジトリを管理します。

次の各トピックでは、各インタフェースについて詳しく説明しています。

- [\[ヘルス モニタ\]ビュー](#)
- [\[システム\]ビュー: \[システム\]の\[情報\]パネル](#)

[ヘルス モニタ]ビュー

ヘルスマニタの設定を使用すると、アラームの設定と表示、イベントの監視、ポリシーとシステム統計情報の表示を行うことができます。それぞれの詳細については、次のトピックを参照してください。

- [\[ヘルス モニタ\]ビュー: \[アラーム\]ビュー](#)
- [\[イベント ソース モニタリング\]ビュー](#)
- [\[ヘルスマニタ\]の\[履歴チャート\]](#)
- [\[ヘルスマニタの設定\]ビュー: Archiver](#)
- [\[ヘルスマニタの設定\]ビュー: イベント ソース](#)
- [\[ヘルスマニタの設定\]ビュー: Warehouse Connector](#)
- [\[監視\]ビュー](#)
- [\[ポリシー\]ビュー](#)
- [\[システム統計ブラウザ\]ビュー](#)

[ヘルス モニタ]ビュー: [アラーム]ビュー

ホストとサービスを監視し、すべてのアクティブなアラームを表示してユーザ定義の制限に達したときに判断できます。アラームは、[ポリシー]タブでホストまたはサービスに対して定義および割り当てたポリシー ルールによってトリガーされます。次のことが可能です。

- すべてのシステムおよびサービスで現在アクティブなすべてのアラームを表示する
- アラームを選択して詳細を表示する

実行したいことは何ですか？

ロール	実行したいこと	手順
管理者	NetWitnessサーバとサービスのアラームステータスの表示。	アラームの監視
管理者	特定のアラームに関する詳細な情報の表示。	アラームの監視

関連トピック

[ポリシーの管理](#)

簡単な説明

このビューへのアクセスに必要な権限は、[サービスの管理]です。[アラーム]ビューにアクセスするには、[Admin] > [ヘルスマニタ]に移動します。[ヘルスマニタ]ビューが開き、[アラーム]タブが表示されます。[アラーム]タブには、アラームリストと[アラームの詳細]パネルが含まれています。

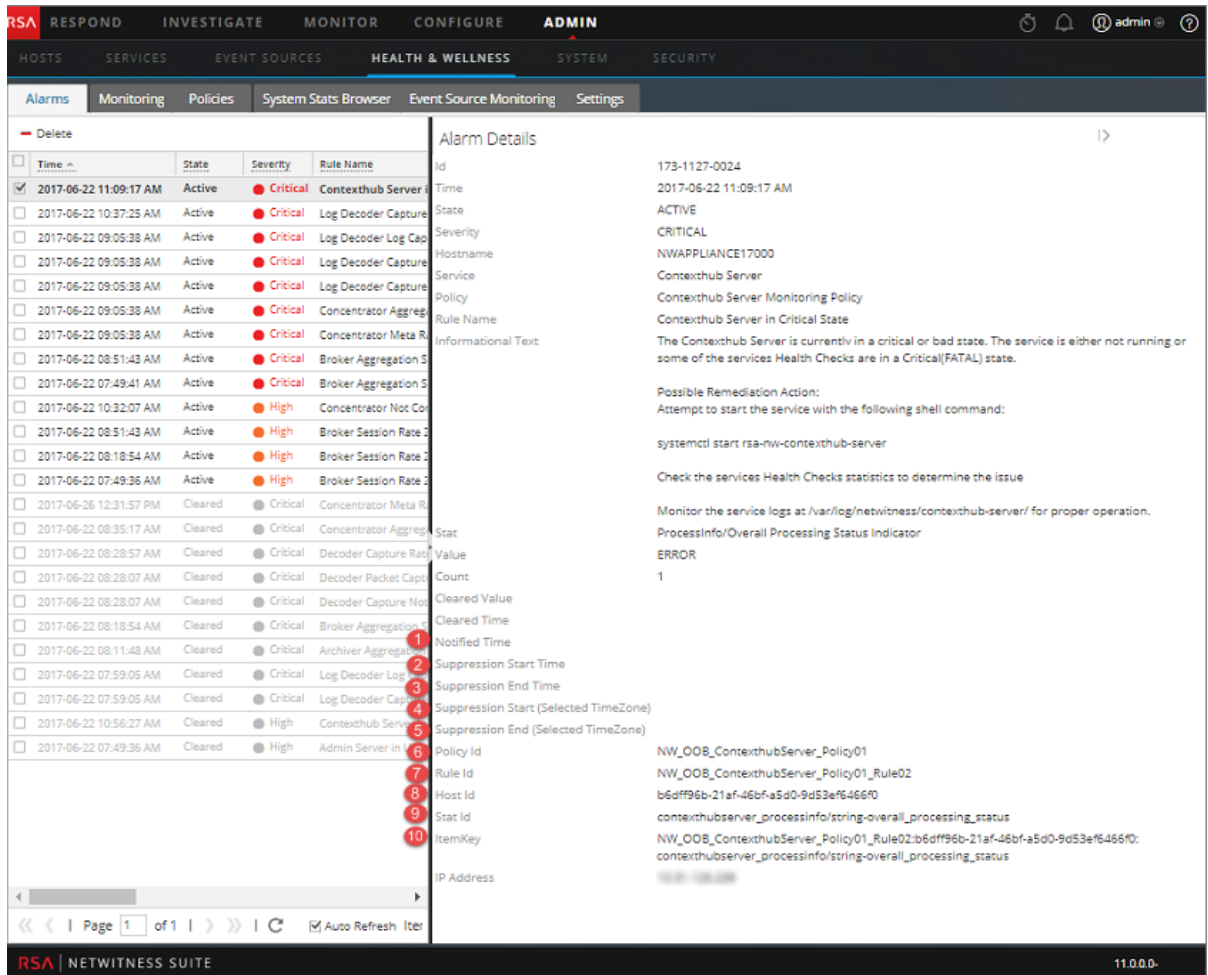
The screenshot shows the RSA NetWitness Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN' (selected). Below this is a sub-navigation bar with 'HOSTS', 'SERVICES', 'EVENT SOURCES', 'HEALTH & WELLNESS' (selected), 'SYSTEM', and 'SECURITY'. The main content area is titled 'Alarms' and contains a table with columns: Time, State, Severity, Rule Name, Service, Hostname, IP Address, Status, Value, and Id. Red circles 1 through 9 are placed above the following columns: 1 (Time), 2 (State), 3 (Severity), 4 (Rule Name), 5 (Service), 6 (Hostname), 7 (IP Address), 8 (Value), and 9 (Id). The table lists various alarms with their respective details, such as 'ContextHub Server in Critical State' and 'Log Decoder Capture Rate Zero'.

1 アラームが発生した時刻。

- 2 アラームのステータス:
 - **アクティブ** = 統計的閾値を超えたため、アラームがトリガーされました。
 - **クリア済み** = リカバリ閾値を超えたため、アラームがアクティブではなくなりました。
- 3 アラームに割り当てられた重大度:
 - **クリティカル**
 - **高**
 - **中**
 - **低**
- 4 アラームをトリガーしたルールの名前。
- 5 ルールで定義されているサービス。
- 6 アラームがトリガーされたホスト。
- 7 アラームをトリガーしたルールで使用されている統計情報。
- 8 アラームをトリガーした統計情報の値。
- 9 アラームのID番号。

注: NetWitness Suiteは、時間順にアラームをソートします。関連パラメータは昇順または降順にソートできます。

次の図は、[アラームの詳細]パネルを展開した状態の[アラーム]タブを示しています。



[アラームの詳細]パネル

[アラームの詳細]パネルには、アラームリストで選択されたアラームの情報が表示されます。アラームリストのすべての情報のほかに、次のフィールドも含まれます。

- 1 アラームの通知時刻
- 2 抑制開始時刻
- 3 抑制終了時刻
- 4 抑制開始(選択済みタイムゾーン)
- 5 抑制終了(選択済みタイムゾーン)
- 6 ポリシーID
- 7 ルールID
- 8 ホストID
- 9 統計情報ID

10 アイテム キー

[イベント ソース モニタリング]ビュー

注: イベント ソースの管理については、「*NetWitness Suite* イベント ソース管理ガイド」の「イベント ソース管理の概要」を参照してください。

NetWitness Suiteは、ユーザ インタフェースでさまざまなイベント ソースの統計を監視する方法を提供します。Log Decoderから取得された履歴の情報が表示されます。ユーザ インタフェースはさまざまなパラメータでフィルタ表示できます。

[イベント ソース モニタリング]ビューにアクセスするには、次の手順を実行します。

1. [管理]>[ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [イベント ソース モニタリング]をクリックします。

実行したいことは何ですか？

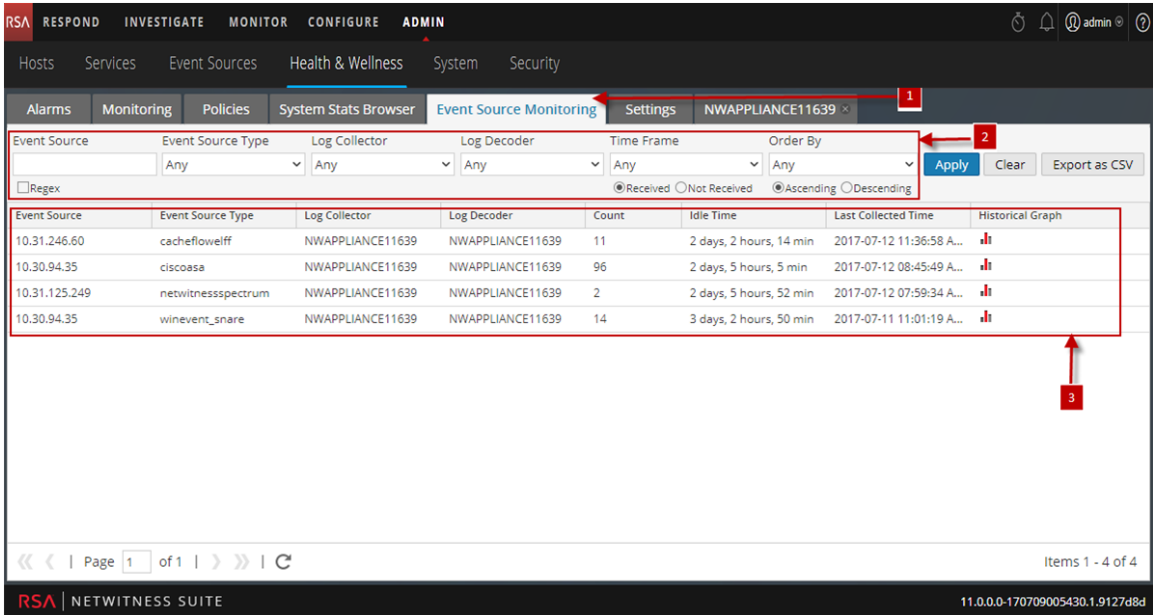
ロー ル	実行したいこと	手順
管理 者	イベント ソースから収集されたイベントの表示	イベント ソースから収集されたイベントの[履歴チャート]ビュー

関連トピック

- [イベント ソースの監視](#)
- [イベント ソースのフィルタ](#)
- [イベント ソースでの収集イベントの履歴チャートの表示](#)

簡単な説明

[イベント ソース モニタリング]ビューが表示されます。



- 1 [イベント ソース モニタリング] タブが表示されます。
- 2 [イベント ソース モニタリング] タブをフィルタおよびカスタマイズするために使用されるツールバー。
- 3 [イベント ソース統計] パネルが表示されます。

フィルタ


次の表に、[イベント ソース モニタリング] ビューのフィルタおよびカスタマイズに使用できるさまざまなパラメータを示します。

パラメータ	説明
イベント ソース	監視対象のイベント ソースの名前を入力します。 Regexフィルタを有効化するには、[Regex]を選択します。このフィルタを有効にすると、テキストに対して正規表現検索が実行され、一致するカテゴリがリストされます。[Regex]を選択していない場合は、グロビングパターンマッチングがサポートされます。
イベント ソース タイプ	選択したイベント ソースのイベント ソースタイプを選択します。

パラメータ	説明
Log Collector	指定したLog Collectorによって収集されたデータを表示するには、[Log Collector]を選択します。
Log Decoder	指定したLog Decoderによって収集されたデータを表示するには、[Log Decoder]を選択します。
タイムフレーム	対象の統計の時間範囲を選択します。 選択した時間範囲内でログの受信元のイベントソースのみを含むクエリ結果が必要な場合は[受信]を選択します。 または 選択した時間範囲内でログの受信元でないイベントソースのみを含むクエリ結果が必要な場合は[受信していない]を選択します。
Order By	リストを表示する際のソート順を選択します。 昇順でソートするには[昇順]を選択します。
適用	クリックすると、選択したフィルタが適用され、設定した条件でリストが表示されます。
クリア	クリックすると、選択したフィルタが解除されます。
CSVでエクスポート	クリックすると、情報がCSV形式でエクスポートされます。

[イベントソース統計]ビューの表示

パラメータ	説明
イベントソース	イベントソースの名前を表示します。
イベントソースタイプ	イベントソースタイプを表示します。
Log Collector	イベントが最初に収集されたLog Collectorを表示します。

パラメータ	説明
Log Decoder	イベントが処理されたLog Decoderを表示します。
件数	カウント値が最後にリセットされてからLog Decoderが受信したイベントの数を表示します。
アイドル時間	最後の統計収集から経過した時間を表示します。
最終収集時刻	Log Decoderがイベントソースのイベントを最後に処理した日時を表示します。
履歴チャート	イベントソースについて収集された統計の履歴チャートを表示するには、  をクリックします。

[ヘルスマニタ]の[履歴チャート]


Archiverのモニタリングを構成すると、Archiverでの集計やストレージの利用状況が重大な閾値に達したときに自動的に通知を生成できます。[履歴チャート]ビューでは、履歴データがビジュアル化されます。

詳細については、次のトピックを参照してください。

- [イベントソースから収集されたイベントの\[履歴チャート\]ビュー](#)
- [システム統計の履歴チャート](#)

イベントソースから収集されたイベントの[履歴チャート]ビュー

イベントソースから収集されたイベントの[履歴チャート]ビューでは、履歴データがビジュアル化されます。このビューにアクセスするには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[監視]タブが開きます。
2. [イベントソースモニタリング]をクリックします。
[イベントソースモニタリング]ビューが表示されます。
3. [履歴チャート]列で、を選択します。
ポップアップウィンドウに選択したイベントソースタイプの履歴チャートが表示されます。

この図は、イベントソースタイプwinevent_snareから収集されたイベントを示しています。



必要に応じてチャートをカスタマイズできます。次の表に、履歴チャートをカスタマイズするためのさまざまなパラメータを示します。

パラメータ	説明
タイムフレーム	履歴データのタイムフレームを選択します。利用可能なオプションは次のとおりです。今日、今週、今月。
<date>~<date>	特定の日付で履歴データの時間範囲を選択します。

履歴チャートのデータの詳細ビューをズームイン表示できます。

ズームイン機能1および2

いずれかの値を選択すると、選択した値の範囲の履歴データを表示できます。次の図は、ズームインの時間範囲として6hを選択した例です。右下隅にあるスライドバーも6hのウィンドウに変更されます。


また、右隅のバーをスライドさせて、任意の範囲にズームインできます。

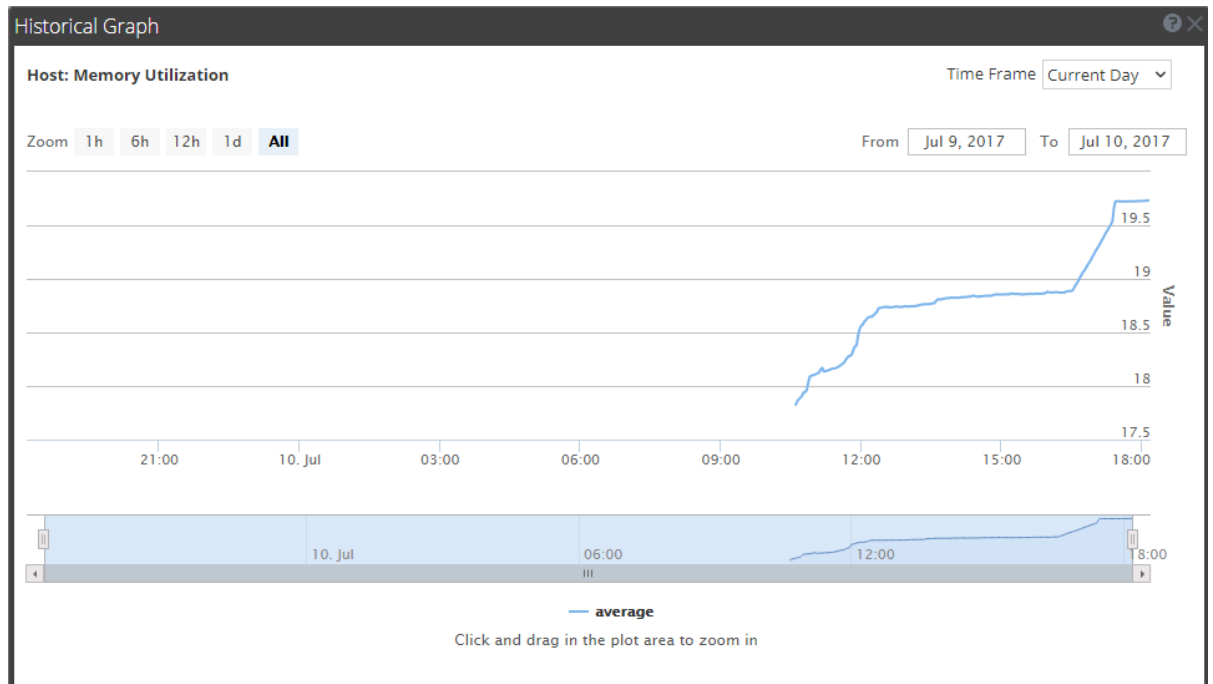
ズームイン機能3

プロット領域をクリックしてドラッグすると、必要な時間範囲にズームインできます。

システム統計の履歴チャート

システム統計の履歴チャートにアクセスするには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [システム統計ブラウザ]タブをクリックします。
[システム統計ブラウザ]タブが表示されます。
3. [履歴チャート]列で、を選択します。
選択したホストの統計が、履歴チャートに表示されます。
この図は、メモリ使用率統計のシステム統計ビューを示しています。



パラメータ

必要に応じてチャートビューをカスタマイズできます。次の表に、[履歴チャート]ビューをカスタマイズするためのさまざまなパラメータを示します。

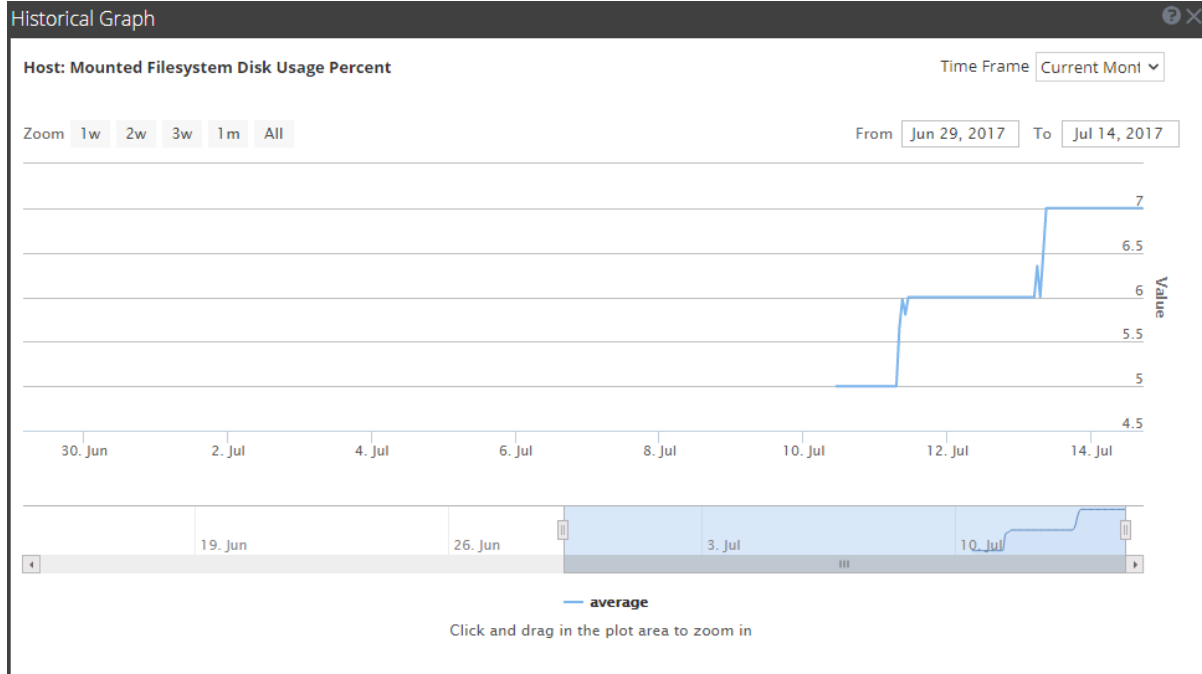
パラメータ	説明
タイムフレーム	履歴データの時間範囲を選択します。 利用可能なオプションは次のとおりです。今日、今週、今月、今年。
<date>~<date>	特定の日付で履歴データの時間範囲を選択します。

履歴チャートのデータの詳細ビューをズームイン表示できます。

ズームイン機能1および2:

いずれかの値を選択すると、選択した値の範囲の履歴データを表示できます。次の図は、ズームインの時間範囲として6hを選択した例です。右下隅にあるスライドバーも6hのウィンドウに変更されます。

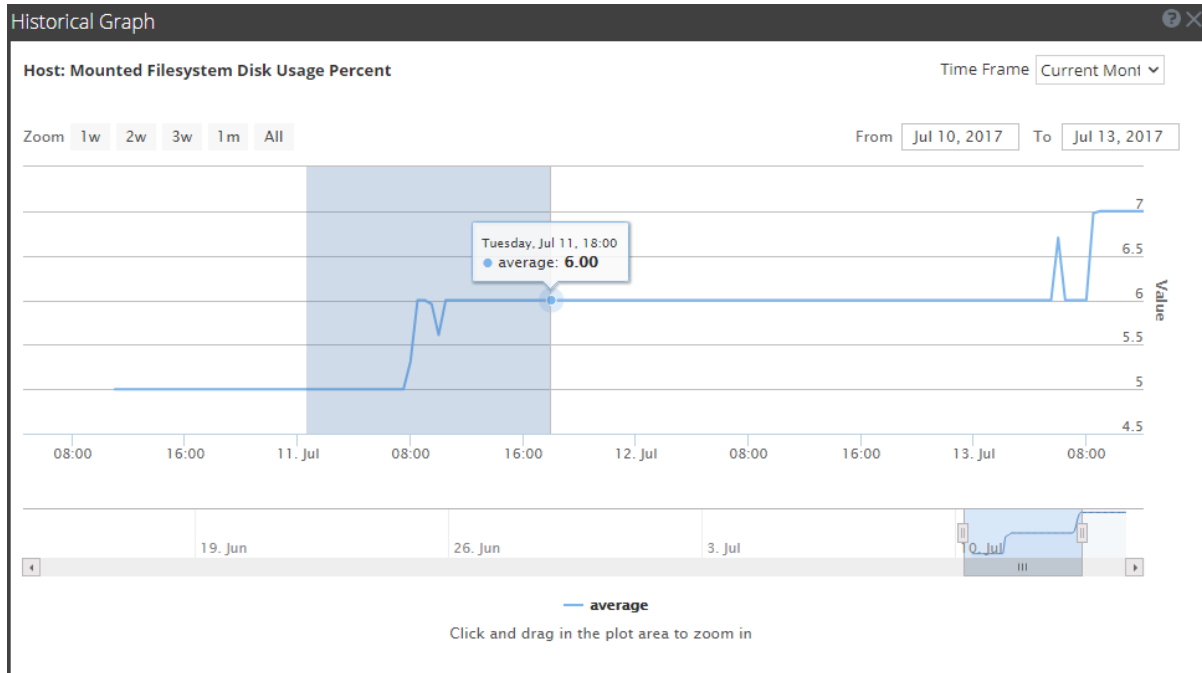
また、右隅のバーをスライドさせて、任意の範囲にズームインできます。



ズームイン機能3:

プロット領域をクリックしてドラッグすると、必要な時間範囲にズームインできます。

下の図は、クリックしてドラッグしたときのグラフの表示例を示しています。



[ヘルスマニタの設定]ビュー: Archiver

注: ArchiverとWarehouse Connectorを監視するには、「稼働状態ポリシー」を参照してください。

Archiverモニタリングビューにアクセスするには、次の手順を実行します。

1. [管理] > [ヘルスマニタ]に移動します。
2. [設定] > [Archiver]を選択します。

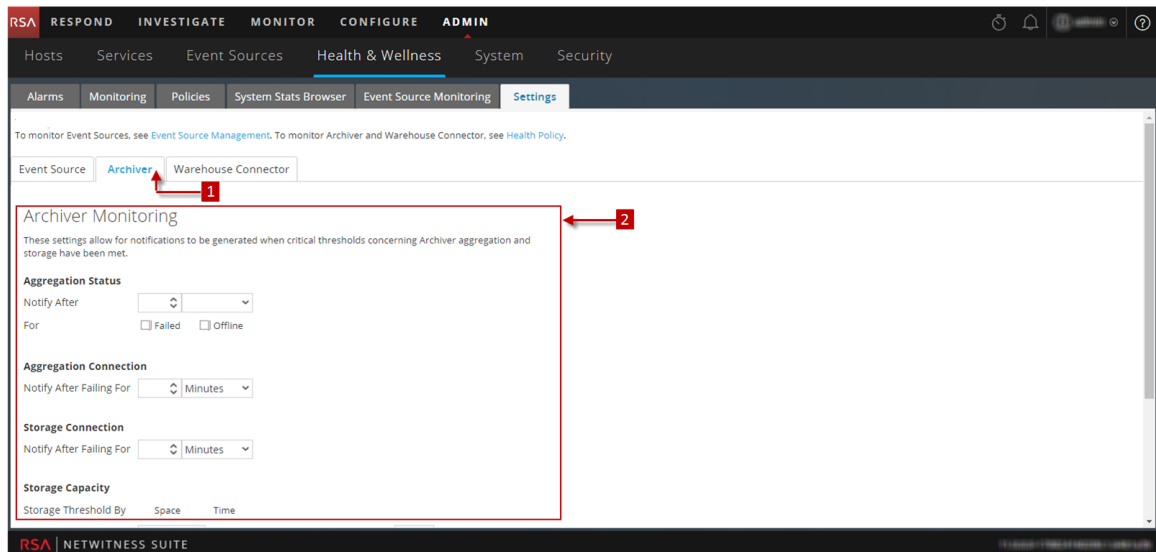
実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	Archiverのサービスの詳細の監視	サービスの詳細の監視

関連トピック

[サービスの詳細の監視](#)

簡単な説明



1 [Archiverモニタリング]パネルが表示されます

2 通知を自動的に受信するように[Archiverモニタリング]パネルを構成します

機能

次の表は、重大な閾値に達したときに自動で通知が生成されるようArchiverを構成するために必要なパラメータをリストしています。

パラメータ	値	説明
集計ステータス	次の時間経過したら通知 対象	集計ステータスが通知されるまでの時間(分または時間) 失敗 - 有効化されている場合、指定した期間(分または時間)、Archiverの集計ステータスが「失敗」であったときに通知します オフライン - 有効化されている場合、指定した期間(分または時間)、Archiverの集計ステータスが「オフライン」であったときに通知します
集計接続	次の時間失敗したら通知	Archiverの集計接続失敗後、指定した期間(分または時間)の経過後に通知します。
ストレージ接続	次の時間失敗したら通知	Archiverのストレージ接続が失敗後、指定した期間(分または時間)の経過後に通知します。

パラメータ	値	説明
ストレージ容量	ストレージ閾値	容量ベースの閾値を指定する場合には、[スペース]を選択し、[ストレージ使用率]フィールドを指定します。Archiverのストレージ容量がここで指定した割合を超えたときに通知します。 時間ベースの閾値を指定する場合には、[時間]を選択し、[最も古いファイル日数]フィールドを指定します。Archiverストレージに格納されているファイルの日数がここで指定した日数を超えたときに通知します。
	ストレージ使用率	使用するストレージ サイズが全体の何パーセントになったら通知するかを入力します。
	Warmストレージサイズ	使用するWarmストレージ サイズが全体の何パーセントになったら通知するかを入力します。
通知のタイプ	メールサーバを構成します。	クリックして、NetWitness Suiteの通知を受信できるようにメールを構成します。
	SyslogサーバおよびSNMPTラップサーバを構成します。	クリックして、監査ログを構成します。
	NWコンソール、メール、Syslog通知、SNMPTラップ通知	NetWitness Suiteユーザ インタフェースの通知ツールバーで通知を受信するには、NWコンソールを有効化します。 メールを通知を受信するには、メールを有効化します。 Syslogイベントを生成するには、Syslog通知を有効化します。 監査イベントをSNMPTラップとして受信するには、SNMPTラップ通知を有効化します。

[ヘルスマニタの設定]ビュー: イベント ソース

注: イベント ソースの管理については、「RSA NetWitness Suite イベント ソース管理ガイド」の「イベント ソース管理の概要」を参照してください。

[イベントソースモニタリング]ビューは、[イベントソース]パネル、[監視対象ソースの追加/編集]ダイアログ、[解除]パネル、[解除]ダイアログで構成されています。このビューを使用して次の項目を構成します。

- イベントソースからLog Collectorへのログ配信が停止した場合に通知を生成するタイミング。
- 通知の送信先。
- リモートCollectorおよびローカルCollectorがスタンバイLog DecoderにフェイルオーバーしたときにLog Collectorを解除するタイミング。

このビューへのアクセスに必要なロールは、[NW監査の管理]です。このビューにアクセスするには、次の手順を実行します。

1. [管理]>[ヘルスマニタ]に移動します。
2. [設定]>[イベントソース]を選択します。

実行したいことは何ですか？

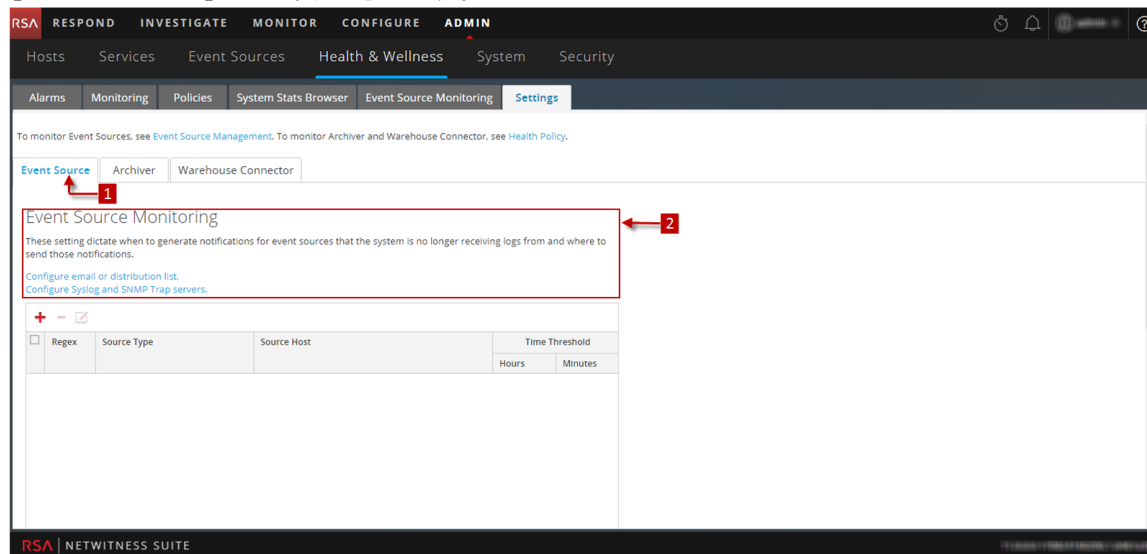
ロール	実行したいこと	手順
管理者	イベントソースモニタリング機能の表示	イベントソースの監視

関連トピック

[イベントソースモニタリングの構成](#)


簡単な説明

[イベントソース]タブが表示されます。






- 1 [イベント ソース モニタリング]パネルが表示されます
- 2 通知を受信するように[イベント ソース モニタリング]パネルを構成します

[イベント ソース モニタリング]パネル

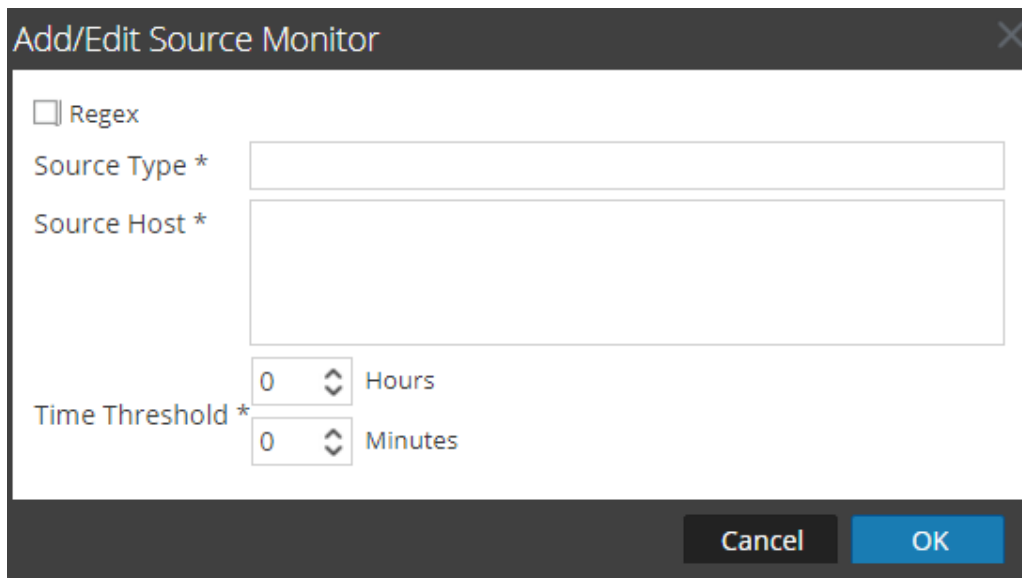
機能	説明
メールサーバを構成します。	[管理]>[システム]>[メール]ビューが開き、必要に応じて、イベント ソース モニタリング出力のメール配信を調整できます。
SyslogサーバおよびSNMPトラップサーバを構成します。	[管理]>[システム]>[監査]ビューが開き、必要に応じて、イベント ソース モニタリング出力のSyslogおよびSNMPトラップ配信を調整できます。
	監視するイベント ソースを追加または変更する[監視対象ソースの追加/編集]ダイアログを表示します。
	選択したイベント ソースを監視対象から削除します。
	イベント ソースを選択します。
ソースタイプ	イベント ソースのソースタイプを表示します。
ソースホスト	イベント ソースのソースホストを表示します。
閾値	NetWitness Suiteが通知の送信を停止するまでの時間を表示します(時間の閾値)。
適用	追加、削除、変更を適用し、直ちに有効にします。
キャンセル	追加、削除、変更をキャンセルします。

[解除]パネル

機能	説明
	監視を解除するイベント ソースを追加または変更する[解除]ダイアログを表示します。

機能	説明
	選択したイベントソースを解除対象から削除します。
	イベントソースを選択します。
Regex	正規表現を使用するかどうかを示します。
ソースタイプ	解除したイベントソースのソースタイプを表示します。
ソースホスト	解除したイベントソースのソースホストを表示します。
適用	追加、削除、変更を適用し、直ちに有効にします。
キャンセル	追加、削除、変更をキャンセルします。

[監視対象ソースの追加/編集]ダイアログ



The dialog box titled "Add/Edit Source Monitor" includes the following elements:

- Regex
- Source Type * (text input field)
- Source Host * (text input field)
- Time Threshold * (0) [spinner] Hours
- Time Threshold * (0) [spinner] Minutes
- Buttons: Cancel, OK

[監視対象ソースの追加/編集]ダイアログでは、監視するイベントソースを追加または変更します。イベントソースを識別するパラメータは、ソースタイプとソースホストの2つです。グロブリング(パターンマッチングおよびワイルドカード文字)を使用して、次の例に示すように、イベントソースのソースタイプとソースホストを指定できます。

ソースタイプ	ソースホスト
ciscopix	1.1.1.1

ソースタイプ	ソースホスト
*	1.1.1.1
*	*
*	1.1.1.1 1.1.1.2
*	1.1.1.[1 2]
*	1.1.1.[123]
*	1.1.1.[0-9]
*	1.1.1.11[0-5]
*	1.1.1.1,1.1.1.2
*	1.1.1.[0-9] 1.1.1.11[0-5]
*	1.1.1.[0-9] 1.1.1.11[0-5],10.31.204.20
*	1.1.1.*
*	1.1.1.[0-9]{1,3}

機能

機能	説明
Regex	正規表現を使用する場合は、チェックボックスをオンにします。
ソースタイプ	イベントソースのソースタイプ。[管理]>[サービス]>[Log Collectorサービス]>[表示]>[構成]ビューの[イベントソース]タブで、イベントソースに対して構成した値を使用する必要があります。
ソースホスト	イベントソースのホスト名またはIPアドレス。[管理]>[サービス]>[Log Collectorデバイス]>[表示]>[構成]ビューの[イベントソース]タブで、イベントソースに対して構成した値を使用する必要があります。
閾値	NetWitness Suiteが通知の送信を停止するまでの時間。

機能	説明
キャンセル	イベントソース、またはイベントソースの変更を[イベントソースモニタリング]パネルに追加せずに、ダイアログを閉じます。
OK	イベントソースを[イベントソースモニタリング]パネルに追加します。

[解除]ダイアログ

機能	説明
ソースタイプ	イベントソースのソースタイプ。[管理] > [サービス] > [Log Collectorデバイス] > [表示] > [構成]ビューの[イベントソース]タブで、イベントソースに対して構成した値を使用する必要があります。
ソースホスト	イベントソースのホスト名またはIPアドレス。[管理] > [サービス] > [Log Collectorサービス] > [表示] > [構成]ビューの[イベントソース]タブで、イベントソースに対して構成した値を使用する必要があります。
キャンセル	イベントソースの追加、削除、変更を[解除]パネルに適用せずに、ダイアログを閉じます。
OK	イベントソースの追加、削除、変更を[解除]パネルに適用します。

[ヘルスマニタの設定]ビュー: Warehouse Connector

注: ArchiverとWarehouse Connectorを監視するには、「稼働状態ポリシー」を参照してください。

Warehouse Connectorモニタリングを構成することで、Warehouse Connectorとそのストレージに関する重要な閾値を超える条件が発生した場合に、自動的に通知を生成できます。

[Warehouse Connectorモニタリング]ビューへのアクセス

1. [Admin] > [ヘルスマニタ]に移動します。
2. [設定] > [Warehouse Connector]を選択します。

実行したいことは何ですか？

ロール	実行したいこと	手順
管理者	Warehouse Connectorの詳細の表示	[Warehouse Connectorの詳細]ビュー

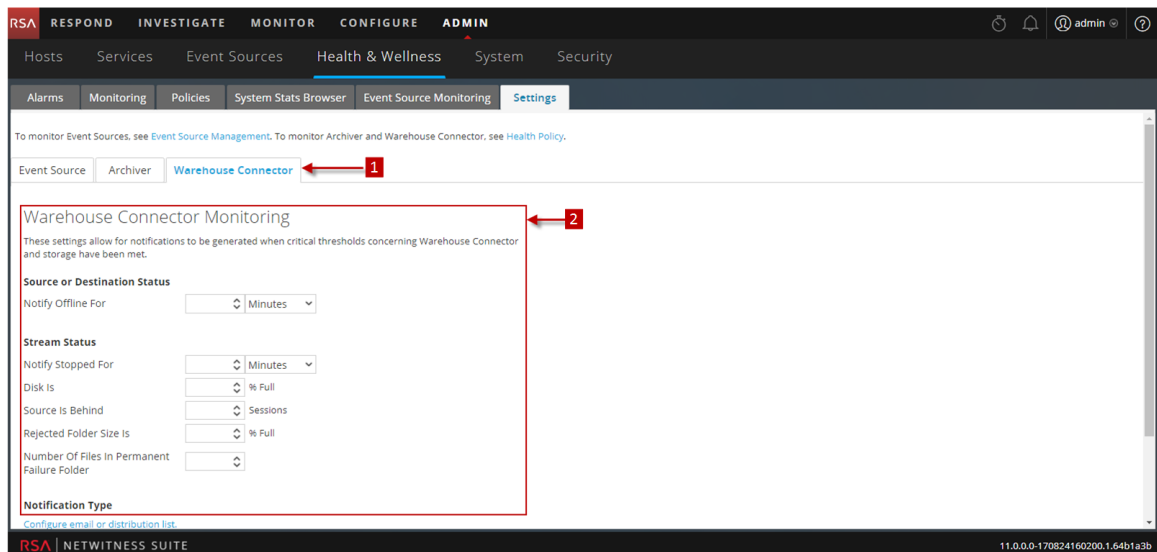
関連トピック

[\[Warehouse Connectorの詳細\]ビュー](#)

[サービスの詳細の監視](#)

簡単な説明

[Warehouse Connectorモニタリング]ビューが表示されます。



1 [Warehouse Connectorモニタリング]ビュー パネルが表示されます

2 Warehouse Connectorモニタリング パラメータを構成 できます

Warehouse Connectorモニタリングパラメータ

次の表に、重要な閾値を超えた場合に自動的に通知を生成するようWarehouse Connectorモニタリングを構成するパラメータを示します。

パラメータ	値	説明
ソースまたは宛先のステータス	次の時間オフラインの場合に通知	ソースまたは宛先の接続がオフラインになってから通知が送信されるまでの時間および時間の単位(分または時間)。
ストリームステータス	次の時間停止している場合に通知	ストリームがオフラインになってから通知が送信されるまでの時間および時間の単位(分または時間)。
	ストレージ	超過した場合に通知が送信されるディスク使用量(%)の制限。
	ソース遅延	ソースが未処理となった場合に通知が発生するまでのセッション数。
	拒否フォルダサイズ	超過した場合に通知が送信されるフォルダ使用量(%)の制限。
	永続的な失敗フォルダ内ファイル数	超過した場合に通知が送信されるパーマネントのFailureフォルダのファイル数の制限。
通知のタイプ	メールサーバを構成します。	クリックして、NetWitness Suiteの通知を受信できるようにメールを構成します。
	SyslogサーバおよびSNMPトラップサーバを構成します。	クリックして、監査ログを構成します。

パラメータ	値	説明
	NWコンソール、 メール、 Syslog通知、SNMPト ラップ通知	NetWitness Suiteユーザ インタフェースの通知ツール バーで通知を受信するには、NWコンソールを有効 化します。 メール通知を受信するには、メールを有効化しま す。 Syslogイベントを生成するには、Syslog通知を有効 化します。 監査イベントをSNMPトラップとして受信するには、 SNMPトラップ通知を有効化します。

[監視]ビュー

NetWitness Suiteでは、ホストや個々のNetWitness Suiteサービスの詳細な統計や他の情報を [詳細]ビューで確認できます。[監視]ビューでは、全ホストの稼働状態、ホストで実行中のサービス、さまざまな角度から見たホストの状態、ホストの詳細、サービスの詳細を表示できます。

このビューにアクセスするには、次の手順を実行します。

1. [管理]>[ヘルスマニタ]に移動します。
2. [監視]タブをクリックします。

実行したいことは何ですか？

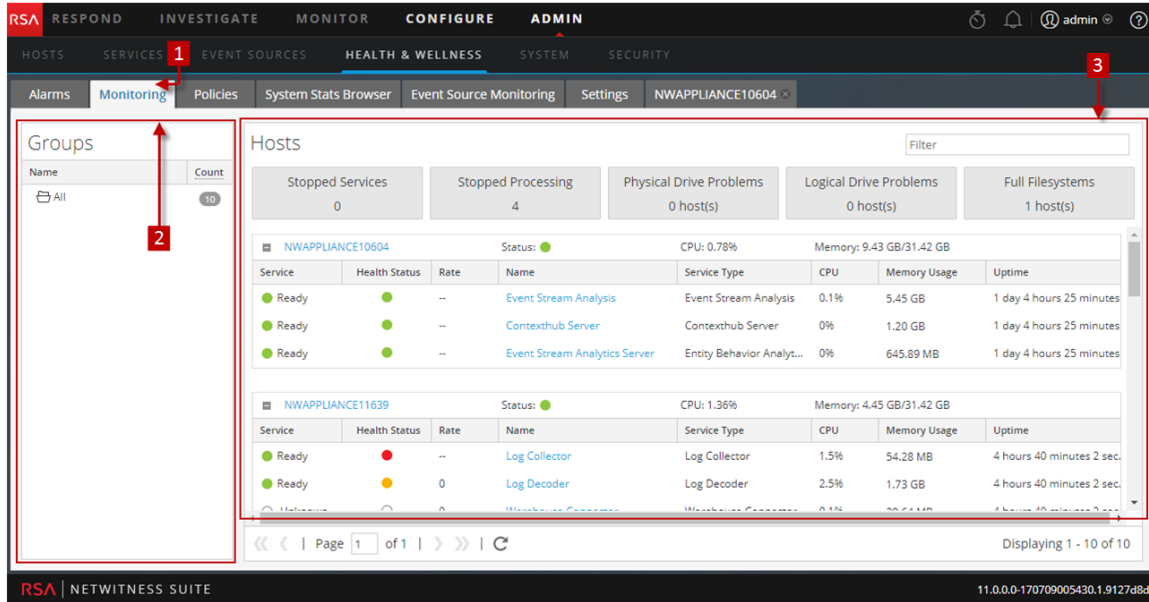
ロール	実行したいこと	手順
管理者	処理手順の表示および実行	ホストとサービスの監視

関連トピック

- [ホストとサービスの監視](#)

簡単な説明

[
モニタリング]ビューが表示されます。



- 1 [モニタリング]タブが表示されます。
- 2 グループを選択する[グループ]パネル。
- 3 [ホスト]パネルには、運用の統計情報が表示されます。

[グループ]パネル

[グループ]パネルには、使用可能なホストのグループがリストされます。グループを選択すると、グループ内のホストが[ホスト]パネルに表示されます。

注：[グループ]パネルの[件数]に表示される合計ホスト数が、[ホスト]パネルに表示されている実際のホスト数より少ない場合は、「[ヘルスマニタのトラブルシューティング](#)」トピックを参照して、この問題の考えられる原因および推奨ソリューションを確認してください。

[ホスト]パネル

[ホスト]パネルには、ホストの状態に関する統計情報および各ホストで実行中のサービスが表示されます。



パラメータ	説明
Filter	[フィルタ]フィールドにホスト名またはサービス名を入力すると、一致するホストとサービスが[ホスト]パネルに表示されます。
サービス停止中	[サービス停止中]をクリックすると、停止中のサービスがすべて一覧表示されます。停止中のサービスがインストールされているホストも表示されます。


パラメータ	説明
処理停止中	[処理停止中]をクリックすると、処理を停止しているサービスと、そのサービスがインストールされているホストがすべて一覧表示されます。
物理ドライブ障害 <#>ホスト	このオプションをクリックすると、物理ドライブに問題のあるホストが表示されます。
論理ドライブ障害 <#>ホスト	このオプションをクリックすると、論理ドライブに問題のあるホストが表示されます。
ファイルシステムフル <#>ホスト	このオプションをクリックすると、ファイルシステムがフルになっているホストが表示されます。

注: ボックスの上部にあるサマリ情報は、NetWitness Suiteに構成されているすべてのホストのシステム統計を表示します。グループを選択してホストをフィルタしても、表示内容は変更されません。

上部のボタンの下には、ホスト、ホストにインストールされているサービス、ホストとサービスに関する情報のリストが表示されます。

パラメータ	説明
ホスト名	<p>ホスト名を表示します。</p> <p>ホストにサービスがインストールされている場合、ホスト名の先頭に■記号が表示されます。</p> <p>■記号をクリックすると、そのホストにインストールされているサービスがすべて表示されます。</p>

パラメータ	説明
ステータス	ホストのステータスを表示します。  - ホストがアクティブで実行中であることを示します。  - ホストが停止中か、または処理が開始されていないことを示します。
CPU	ホストの現在のCPU使用率を表示します。
メモリ	ホストで使用されているメモリを表示します。

ホスト名の先頭にある記号をクリックすると、そのホストにインストールされているサービスがすべて一覧表示されます。次の表に、サービスで表示される各種パラメータとその説明を示します。

パラメータ	説明
サービス	サービスのステータスを表示します。  利用可能 - サービスがアクティブで実行中であることを示します。  停止 - サービスが停止中か、または処理が開始されていないことを示します。
稼働状態ステータス	サービスの処理のステータスを表示します。  - 処理が実行中で、データがゼロより大きいレートで処理されていることを示します。  - 処理が停止されたことを示します。  - 処理は有効ですが、データが処理されていないことを示します。
レート	データが処理されるレートを示します。
名前	サービスの名前。
サービスタイプ	サービスのタイプ名。
CPU	サービスの現在のCPU使用率を表示します。
メモリ使用量	サービスに使用されるメモリを表示します。
アップタイム	サービスの実行時間を表示します。

[Archiverの詳細]ビュー

[Archiverの詳細]ビューには、Archiverの情報が表示されます。次の図は、[Archiverの詳細]を示したものです。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, with sub-tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Health & Wellness' tab is selected, and the 'System Stats Browser' sub-tab is active. The main content area shows 'Archiver Details' for the host 'NWAPLIANCE25988'. The details are organized into two sections: 'Service' and 'Details'.

Service			
CPU	0.2%	Used Memory	32.98 MB
Running Since	2017-Jul-10 10:30:25	Max Process Memory	31.42 GB
Build Date	2017-Jul-09 07:24:34	Version Information	11.0.0.0

Details			
Aggregation State	stopped	Time Begin	
Session Free Pages	0	Time End	
Meta Free Pages	0	Session Rate Max	0
Database Status		Session Rate	0
Database Session Rate		Database Session Free Space	
Database Session Rate Max		Database Session Volume Bytes	

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、サービスの現在の全般的な統計が表示されます。

統計情報	説明
集計状態	データ集計の状態。
最初の日時	インデックスにトラッキングされた最初のセッションの時刻 (UTC)。
セッション空きページ	集計に利用可能なセッション ページ。
最新の日時	インデックスにトラッキングされている最新のセッションの時刻 (UTC)。
メタ空きページ	集計に利用可能なページ。
最大セッションレート	1秒あたりの最大セッション。

統計情報	説明
データベース ステータス	<p>データベースのステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • closed - QUERY およびUPDATEでは使用できません(データベースが初期化されます)。通常、この値は表示されません。 • opened - QUERY およびUPDATEで使用できます。 • failure - openに失敗しました。この値が表示される理由はさまざまです。収集が開始できなかつたり、クエリからデータが返されなかつた場合に確認できます。通常は、データベースの破損が原因です。
セッション レート	1秒あたりのセッション。
データベース セッション レート	サービスがセッションをデータベースに書き込む1秒あたりのレート。
データベース セッション空き 領域	集計に利用可能なセッション空き領域
最大データ ベース セッショ ンレート	サービスがセッションをデータベースに書き込む1秒あたりの最大レート
データベース セッション ボ リューム バイ ト	データベース内のセッションのバイト数。

[Brokerの詳細]ビュー

[Brokerの詳細]ビューには、Brokerの情報が表示されます。次の図は、[Brokerの詳細]を示したものです。

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、サービスの現在の全般的な統計が表示されます。

統計情報	説明
集計状態	データ集計の状態。
メタレート	1秒あたりのメタデータ オブジェクト。
セッションレート	1秒あたりのセッション。
最大メタレート	1秒あたりの最大メタデータ オブジェクト。
最大セッションレート	1秒あたりの最大セッション。

[Concentratorの詳細]ビュー

[Concentratorの詳細]ビューには、Concentratorの情報が表示されます。次の図は、[Concentratorの詳細]を示したものです。

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、サービスの現在の全般的な統計が表示されます。

統計情報	説明
集計状態	データ集計の状態。
最初の日時	インデックスにトラッキングされた最初のセッションの時刻 (UTC)。
メタレート	1秒あたりのメタデータ オブジェクト。
最新の日時	インデックスにトラッキングされている最新のセッションの時刻 (UTC)。
最大メタレート	1秒あたりの最大メタデータ オブジェクト。
セッションレート	1秒あたりのセッション。
最大セッションレート	1秒あたりの最大セッション。

[Decoderの詳細]ビュー

[Decoderの詳細]ビューには、Decoderの情報が表示されます。次の図は、[Decoderの詳細]を示したものです。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The main content area is titled 'Decoder Details' and is divided into two sections: 'HOST AND SERVICES' and 'Details'.

HOST AND SERVICES

Host	CPU	2.6%	Used Memory	271.64 MB
Decoder	Running Since	2017-Jul-12 19:24:52	Max Process Memory	31.42 GB
Warehouse Connector	Build Date	2017-Jul-11 07:20:38	Version Information	11.0.0.0

Details

Capture Status	started	Meta Bytes	565.67 MB
Capture Kept	4.83 MB	Meta Total	28302488
Capture Dropped	0	Packet Bytes	15.68 GB
Capture Dropped Percent	0%	Packet Total	40851335
Capture Rate	0	Session Bytes	4.00 KB
Capture Rate Max	0	Session Total	2712
Time Begin	2016-Sep-20 16:31:56	Pool Packet Write	0
Time End	2017-Jul-14 12:35:43	Pool Packet Assembler	0
Assembler Packet Pages	37	Pool Packet Capture	49962

At the bottom of the interface, the text 'RSA | NETWITNESS SUITE' and the version number '11.0.0.0-170709005430.1.9127d8d' are visible.

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、サービスの現在の全般的な統計が表示されます。

統計情報	説明
収集ステータス	データ収集のステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> • starting: データ収集を開始しています(データはまだ収集されていません)。 • started: データを収集しています。 • stopping: データ収集を停止しています(データ収集の停止リクエストを受け取りましたが、データの収集はまだ停止していません)。 • stopped: データを収集していません。 • disabled: Decoderサービスとして構成されていません。
メタバイト	データベース内のメタのバイト数。

統計情報	説明
保持された収集	収集中に保持されたパケット数。
メタ合計	データベース内のメタデータの数。
ドロップされた収集	ネットワークカードでドロップされたと報告されたパケットの数。サービスがデータの収集を停止した後で、レートはゼロにリセットされます。
パケットバイト	データベース内のパケットのバイト数。
ドロップされた収集の割合	ネットワークカードでドロップされたと報告されたパケットの割合。
パケット合計	パケット データベースに保持されているパケット オブジェクトの数。サイズ制限のためにデータベースによってファイルがロール オフされると、この値は減少します。サービスがデータの収集を停止した後でも、値はリセットされません。
収集レート	サービスがデータを収集する速度を1秒あたりのメガビット数で表したものの。レートは、短時間(10秒)の移動平均です。サービスがデータの収集を停止した後で、レートはゼロにリセットされます。
セッションバイト	データベース内のセッションのバイト数。
最大収集レート	サービスがデータを収集する速度を1秒あたりの最大メガビット数で表したものの。レートは、短時間(10秒)の移動平均です。サービスがデータの収集を停止した後で、データ収集中の最大レートが表示されます。

統計情報	説明
セッション合計	セッション データベースに含まれるセッション数。サイズ制限のためにデータベースによってファイルがロール オフされると、この値は減少します。サービスがデータの収集を停止した後でも、値はリセットされません。
最初の日時	最初のパケットが収集された日時(最初のパケットがパケット データベースに格納された日時)。パケットがパケット データベースからロールアウトされると、この時刻は増加します。
プールパケット書き込み	現在PCSパイプライン内にあり、データベースに書き込む必要があるパケット ページ数。
最新の日時	最後のパケットが収集された日時(パケットがデータベースに書き込まれた日時)。新しいパケットが収集されるとこの時刻が増えます。
プールパケットアセンブラ	アセンブルを待機しているパケット ページ数。
アセンブラパケットページ	アセンブルを待機しているパケット ページ数。
プールパケット収集	収集に使用できるパケット ページ数。

[ESA(Event Steam Analysis)の詳細]ビュー

[Event Stream Analysisの詳細]ビューには、ESAの情報が表示されます。次の図は、[Event Stream Analysisの詳細]を示しています。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The main menu has 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Health & Wellness' section is active, showing 'Alarms', 'Monitoring', 'Policies', 'System Stats Browser', 'Event Source Monitoring', and 'Settings'. The 'System Stats Browser' is selected, displaying 'ESA Details' for host 'NWAPPLIANCE10604'.

Service Details:

Service	CPU	Used Memory
0.2%	1.14 GB	
Running Since	2017-Jul-11 10:37:31	Max Process Memory
31.42 GB		
Build Date	2017-Jul-09 03:33:32	Version Information
11.0.0.0		

Details

Rules | Monitor | JVM

Deployed Rule Memory Utilization [Enable & Disable Rules](#)

Name	Event Stream Engine	Average Estimated Memory (last hr)
dynamicAlert	Local ESA (Default)	-
dynamicAlert: meta_value_length	Local ESA (Default)	-
Module_Engine_LOCAL_596367dbe4b0ef1bdfb8c5ed	Local ESA (Default)	-
NullRule	Local ESA (Default)	-
test_rule	Local ESA (Default)	-

Footer: RSA | NETWITNESS SUITE 11.0.0.0-170709005430.1.9127d8d

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、サービスの現在の全般的な統計とルール情報が表示されます。[ルール]タブ、[監視]タブ、[Java仮想マシン(JVM)]タブで構成され、Event Stream Analysisルールとその他の統計が表示されます。

[監視]タブ

Event Stream Analysisサービスについて、次の全般的な統計情報を表示します。

- イベントメッセージフィールドあたりの平均受信バイト数
- イベントメッセージあたりの平均受信バイト数
- 総受信バイト数
- 受信フィールドの合計数
- ESAサービスで導入されているルールの数 有効化されたルールと無効化されたルールの合計が導入されたルールの数と等しくなります。
- ESAサービスのすべてのルールに一致したイベントの合計数
- サービスの前の起動時以降にESAサービスによって分析されたイベントの合計数
- ESAサービスのすべてのルールによりトリガーされたアラートの合計数
- 遅延ドロップ合計
- 時間ごとのフィード合計

- 早期終了合計
- フィード間の秒数
- ウィンドウの期間
- ウィンドウのイベント合計
- 処理されたウィンドウの割合
- ソース作業ユニット合計
- ペイロードでドロップされたバス合計
- バスドロップ イベント合計
- フィールドでドロップされたバス合計
- メッセージ バスに送信されたアラートの数
- バス イベント合計
- バス作業ユニット合計
- 検出されたエンドポイント合計
- 消失したエンドポイント合計
- 失敗したクライアント合計
- 成功したクライアント合計
- 成功したサーバ合計
- 前回の成功からの時間(分)
- 成功したプロキシ リクエスト合計
- 成功したリクエスト合計
- 失敗したプロキシ リクエスト合計
- 失敗したリクエスト合計

[ESA Analyticsの詳細]ビュー

[ESA Analyticsの詳細]ビューには、選択したESA Analyticsサービスの稼働状態ステータス情報が表示されます。ESA Analyticsサービスは、自動脅威検出のためにデータを処理します。緑色(正常)以外のステータスを示すチェック済みの項目に対処して、データ処理が中断されず、クリティカルなイベントが見逃されないようにすることが重要です。

次の図は、[ESA Analyticsの詳細]ビューを示しています。

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

ESA Analyticsの詳細

このセクションには、選択したESA Analyticsサービスの現在の全般的な統計が表示されます。

稼働状態ステータス

[稼働状態ステータス]セクションには、選択したESA Analyticsサービスの次の項目の正常性が表示されます。

- Mongo
- JVM(Java仮想マシン)
- ディスク領域
- 不審なドメイン モジュール
- ユーザ動作分析モジュール

次の表に、各稼働状態ステータスの意味を示します。

稼働状態ステータス	説明
緑	Healthy
黄	非健全
赤	重大で、早急に注意を払う必要があります。

稼働状態ステータス	説明
--	該当なし

[ホストの詳細]ビュー

[ホストの詳細]ビューには、ホストの情報が表示されます。次の図は、[ホストの詳細]を示しています。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, there are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Hosts' tab is active, and the 'System Stats Browser' sub-tab is selected. The main content area is titled 'Host Details' and shows information for host 'NWAPLIANCE9'. The 'System Info' section includes: Host (NWAPLIANCE9), CPU (3.01%), Running Since (2017-Jul-10 09:44:02), Current Time (2017-Jul-11 16:43:42), Uptime (1 day 6 hours 59 minutes 40 seconds), and System Info (Linux 3.10.0-514.26.2.el7.x86_64 x86_64). The 'Physical Drive' section shows details for the drive, including State, Enclosure, Slot, Failure Count, Raw Size, and Inquiry Data. The left sidebar lists various services: Host, Broker, Reporting Engine, Orchestration Server, Security Server, Admin Server, Config Server, Investigate Server, and Respond Server.

左側のオプションパネルには、ホストおよびホストにインストールされているサービスが表示されます。ホストまたはいずれかのサービスをクリックすると、それに関連する統計と情報が表示されます。

[ホストの詳細]パネルには、ホストに固有の情報が表示され、ホストのハードウェアに関する情報も表示されます。

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、ホストの現在のパフォーマンス、容量、履歴統計が表示されます。

パラメータ	説明
ホスト	ホスト名。
CPU	ホストの現在のCPU使用率。
起動日時	ホストを起動した時刻。

パラメータ	説明
現在日時	ホスト上の現在の時刻。
アップタイム	ホストがアクティブな期間。
システム情報	ホストにインストールされているOSバージョン。
メモリ使用率	ホストが使用しているメモリの割合。
使用メモリ	メモリ使用量 (GB)。
総メモリ	システムにインストールされているメモリの容量。
キャッシュメモリ	GB単位のディスクにキャッシュされたメモリ。
スワップ使用率	使用中のシステムスワップの割合。
使用済みスワップ	GB単位の使用済みスワップ。
スワップ合計	システムにインストールされているスワップの容量。

システム情報の下のセクションでは、次の表示で説明するタブに、ホストの全般的な統計が表示されます。

タブ	説明
物理ドライブ	ホスト上の物理ドライブのタイプ、使用量、補足情報。
論理ドライブ	ホスト上の論理ドライブ
ファイルシステム	ホストのファイルシステム情報、サイズ、使用済みの容量、使用可能な容量。
アダプタ	ホスト上で使用されているアダプター

タブ	説明
メッセージバス	<p>[公開レート] - 受信メッセージがメッセージバスキューに公開されるレート。</p> <p>[キューイングされたメッセージの合計] - メッセージキューのメッセージ数。</p> <p>[メモリ使用量] - メッセージバスが使用しているメモリの量(バイト単位)。</p> <p>[ディスクの空き容量] - メッセージバスが利用できるディスクの空き容量(バイト単位)。</p> <p>[メモリ制限] - システムメモリの上限。メモリ使用量がこの値を超えた場合、[メモリアラーム]が発行され、Security Analyticsがメッセージの受信を停止します。</p> <p>[ディスクの空き容量制限] - メッセージバスのディスクの空き容量制限。利用可能なディスクの空き容量がこの値を下回ると、[ディスクの空き容量アラーム]が発行され、Security Analyticsがメッセージの受信を停止します。</p> <p>[利用可能なメモリ制限] - [メモリ使用量アラーム]を発行する前に、このメッセージブローカーで利用可能なメモリの量(バイト単位)。</p> <p>[利用可能なディスク制限] - [ディスクの空き容量制限]アラームを発行する前に、このメッセージブローカーで利用可能なディスクの容量(バイト単位)。</p> <p>[ディスクの空き容量アラーム] - [True または[False]。[True]は、利用可能なディスクの空き容量が[ディスクの空き容量制限]で設定された値を下回っており、Security Analyticsがメッセージの受信を停止していることを示します。</p> <p>[メモリアラーム] - [True]または[False]。[True]は、利用可能なメモリ量が[メモリ制限]で設定された値を下回っており、Security Analyticsがメッセージの受信を停止していることを示します。</p>

[Log Collectorの詳細]ビュー

[Log Collectorの詳細]ビューには、Log Collectorの情報が表示されます。次の図は、[Log Collectorの詳細]を示しています。

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

下のセクションには、サービスの全般的な統計を表示する[収集]タブと[イベント処理]タブがあります。

[収集]タブ

NetWitness Suiteで実装している各 Log Collection プロトコルのイベントの収集統計が表示されます(「[ログ収集ガイド](#)」の「[ログ収集のスタートガイド](#)」を参照してください)。

[イベント処理]タブ

ログ収集時の NetWitness Suite 内部のイベント処理プロトコル (=Log Decoder) の統計を表示します。

パラメータ	説明
転送プロトコル	ログの収集に使用される NetWitness Suite プロトコル(すなわち Log Decoder) です。

パラメータ	説明
ステータス	Log Decoderのステータスです。有効な値は次のとおりです。 <ul style="list-style-type: none">• starting: データ収集を開始しています(データはまだ収集されていません)。• started: データを収集しています。• stopping: データ収集を停止しています(データ収集の停止リクエストを受け取りましたが、データの収集はまだ停止していません)。• stopped: データを収集していません。• disabled: Decoderサービスとして構成されていません。
EPS	このLog DecoderがLog Collectorからのイベントを処理するレート(1秒あたりのイベント数) です。
イベント合計	Log Decoderが処理したイベント数の合計です。
エラー	発生したエラーの数です。
警告	発生した警告の数です。
バイトレート	現在のスループット(1秒あたりのバイト数) です。

[Log Decoderの詳細]ビュー

[Log Decoderの詳細]ビューには、Log Decoderの情報が表示されます。次の図は、[Log Decoderの詳細]を示したものです。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, there are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Health & Wellness' tab is active, and the 'System Stats Browser' sub-tab is selected. The main content area displays 'Log Decoder Details' for a host named 'NWAPLIANCE11639'. The 'Service' table shows CPU usage at 2.3%, Used Memory at 1.73 GB, Running Since at 2017-Jul-12 10:23:15, Max Process Memory at 31.42 GB, and Build Date at 2017-Jul-09 07:20:33. The 'Details' table shows Capture Status as 'started', Packet Rate Max as 1, Events Per Second as 0, Pool Packet Capture as 50000, Meta Rate as 0, Pool Packet Assembler as 0, Meta Rate Max as 65, Assembler Packet Pages as 0, Capture Dropped as 0, Pool Packet Write as 0, Capture Dropped Percent as 0%, Time Begin as 2017-Jul-10 11:58:52, and Time End as 2017-Jul-12 11:36:58.

関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

このセクションには、サービスの現在の全般的な統計が表示されます。

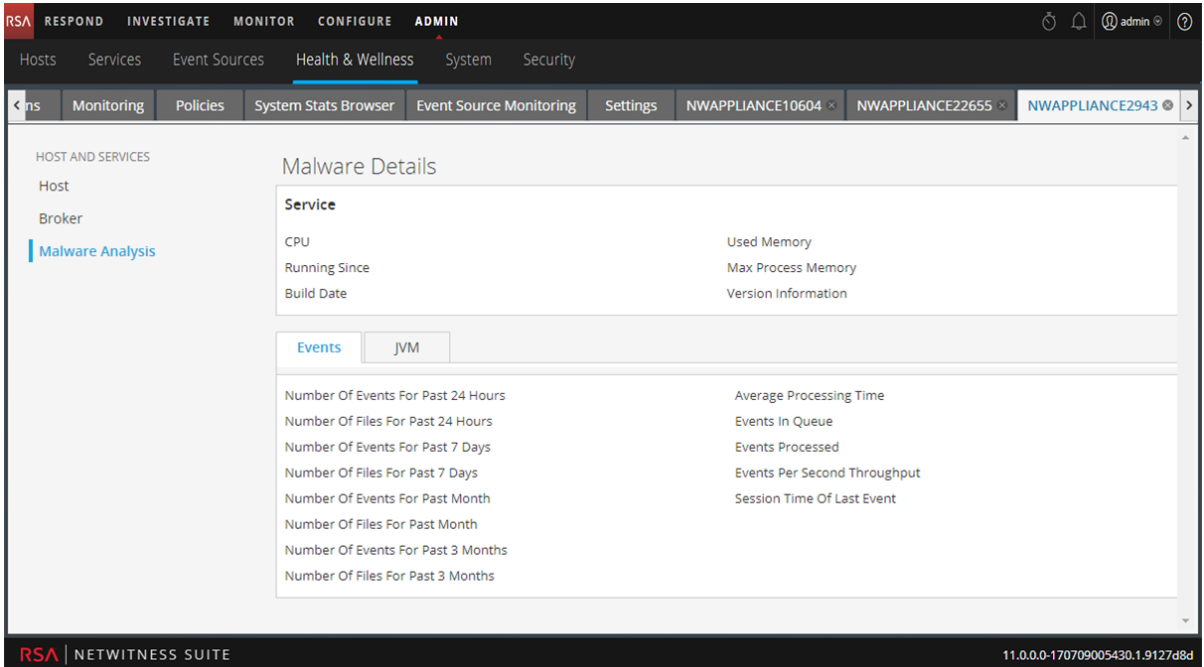
統計情報	説明
収集ステータス	データ収集のステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> • starting: データ収集を開始しています(データはまだ収集されていません)。 • started: データを収集しています。 • stopping: データ収集を停止しています(データ収集の停止リクエストを受け取りましたが、データの収集はまだ停止していません)。 • stopped: データを収集していません。 • disabled: Log Decoderサービスとして構成されていません。
最大パケットレート	サービスが1パケットをデータベースに書き込む1秒あたりの最大レート。レートは、短時間(10秒)の移動平均です。サービスがデータの収集を停止した後で、データ収集中の最大レートが表示されます。

統計情報	説明
秒あたり のイベン トの数	Log Decoder がLog Collectorからのイベントを処理するレート(秒あたりのイベントの数)。
プール パケット 収集	収集に使用できるパケット ページ数。
メタレー ト	サービスがメタデータ オブジェクトをデータベースに書き込む1秒あたりのレート。レートは、短時間(10秒)の移動平均です。サービスがデータの収集を停止した後で、レートはゼロにリセットされます。
プール パケット アセンブ ラ	アセンブルを待機しているパケット ページ数。
最大メ タレート	サービスがメタデータ オブジェクトをデータベースに書き込む1秒あたりの最大レート。レートは、短時間(10秒)の移動平均です。サービスがデータの収集を停止した後に、データ収集中に到達した最大レートが表示されます。
アセンブ ラパケッ トペー ジ	アセンブルを待機しているパケット ページ数。
ドロップ された 収集	ネットワークカードでドロップされたと報告されたパケットの数。サービスがデータの収集を停止した後で、レートはゼロにリセットされます。

統計 情報	説明
プール パケット 書き込 み	PCSパイプライン内にあり、データベースに書き込む必要があるパケット ページの 数。
ドロップ された 収集の 割合	ネットワークカードでドロップされたと報告されたパケットの割合。
最初の 日時	最初のパケットが収集された日時(最初のパケットがパケット データベースに格納さ れた日時)。パケットがパケット データベースからロールアウトされると、この時刻は 増加します。
最新の 日時	最後のパケットが収集された日時(パケットがデータベースに書き込まれた日時)。 新しいパケットが収集されるとこの時刻が増えます。

[マルウェアの詳細]ビュー

[マルウェアの詳細]ビューには、Malware Analysisの情報が表示されます。次の図は、[マルウェアの詳細]を示したものです。



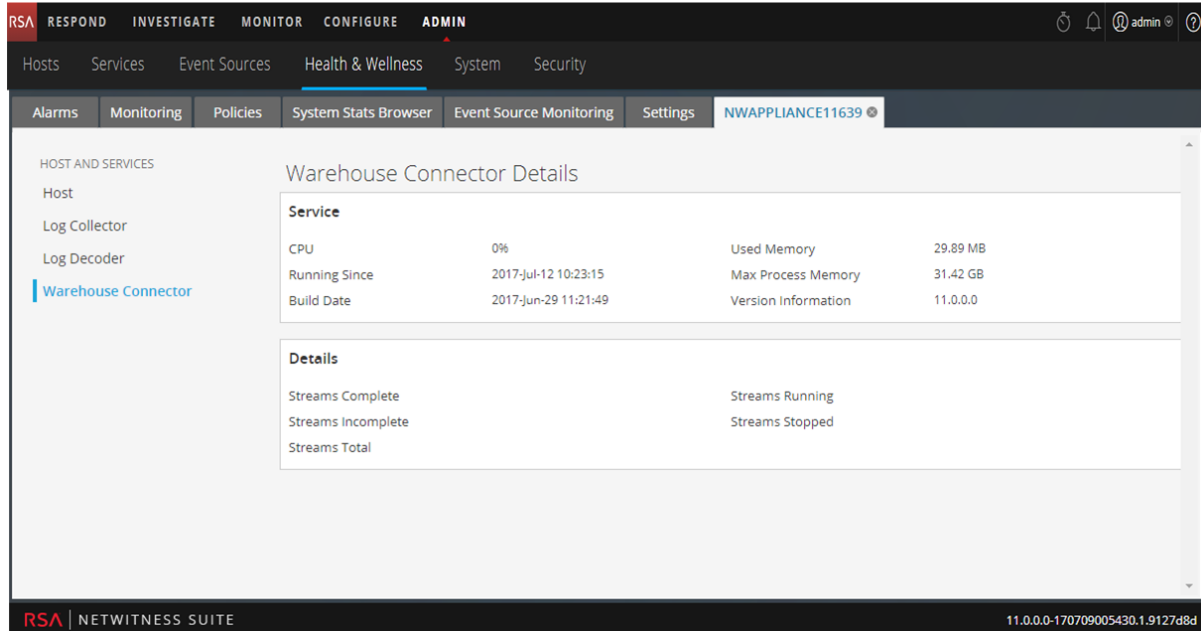
関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

Malware Analysisサービスの次のイベント関連統計情報を表示します。

- 過去24時間のイベントの数
- 平均処理時間
- 過去24時間のファイルの数
- キューのイベント
- 過去7日間のイベントの数
- 処理されたイベント
- 過去7日間のイベントの数
- 1秒あたりのイベント数スループット
- 過去1か月のイベントの数
- 前回のイベントのセッション時間
- 過去1か月のファイルの数
- 過去3か月のイベントの数
- 過去3か月のファイルの数

[Warehouse Connectorの詳細]ビュー

[Warehouse Connectorの詳細]タブには、ビルドされた日付、CPU、バージョン情報など、Warehouse Connectorの情報が表示されます。次の図に、[Warehouse Connectorの詳細]を示します。



関連する手順については、「[サービスの詳細の監視](#)」を参照してください。

[ポリシー]ビュー

このビューへのアクセスに必要な権限は、[サービスの管理]です。

実行したいことは何ですか？

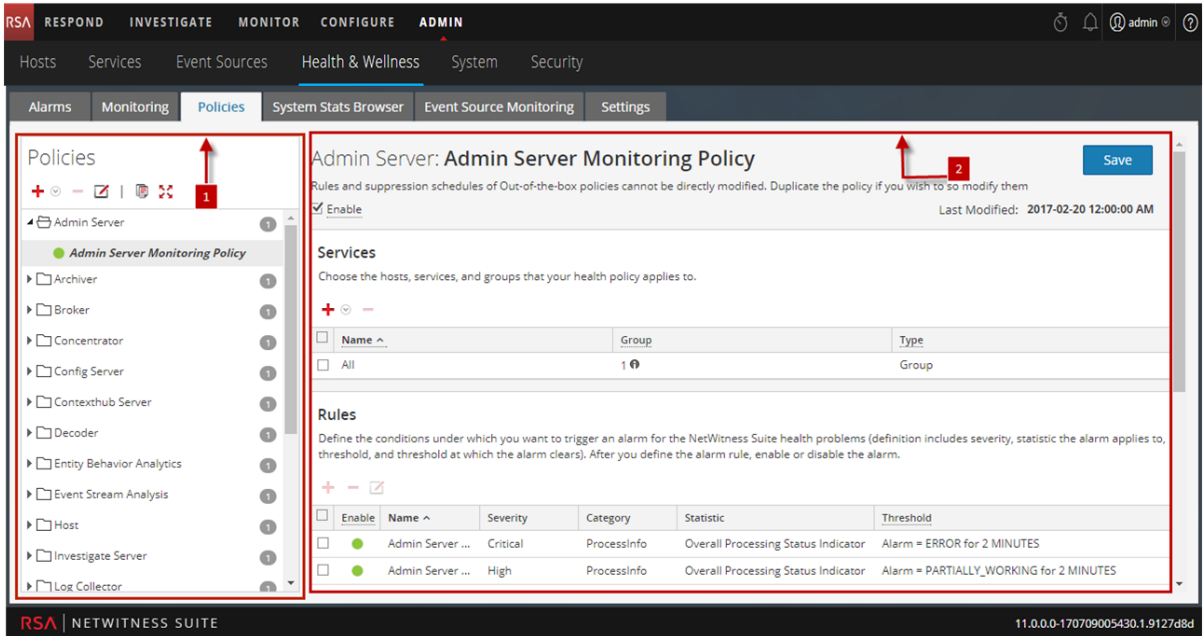
ロール	実行したいこと	手順
管理者	NetWitnessサーバおよびサービスのポリシーの表示	ポリシーの管理
管理者	ポリシーの追加、編集、複製、削除	ポリシーの管理

関連トピック

[ポリシーの管理](#)

簡単な説明

次の図は[ポリシー]ビューを示しています。



1 [ポリシー]パネル





2 [ポリシー詳細]パネル

1. [管理]>[ヘルスマニタ]に移動します。
2. [ポリシー]タブをクリックします。

[ポリシー]パネル

[ポリシー]パネルでは、このパネルに表示されているホストとサービスのポリシーを追加または削除できます。








機能	説明
	新しいポリシーの対象として選択可能なサービスタイプが表示されます。ポリシーを定義するサービスタイプを選択します。
	選択されたポリシーを[ポリシー]パネルから削除します。一度に削除できるポリシーは1つだけです。
	ポリシー名を変更できます。

機能	説明
	選択されたポリシーのコピーを作成します。たとえば、[第1ポリシー]を選択して  をクリックすると、NetWitness Suiteによってこのポリシーのコピーが作成され、第1ポリシー(1)という名前が付けられます。
	[ポリシー]パネルで、サービスとホストを展開しポリシーのリストを表示します。
	[ポリシー]パネルで、サービスとホストを閉じ、ポリシーのリストを非表示にします。
	リストの内容： <ul style="list-style-type: none"> 定義したポリシーの対象となるサービスとホスト。 ホストとサービスに適用できるRSA標準ポリシー

[ポリシー詳細]パネル

[ポリシー詳細]パネルには、[ポリシー]パネルから選択したポリシーが表示されます。

機能	説明
保存	このパネルで行った変更を保存します。
ポリシーのタイプ	選択されたポリシーのタイプを表示します。
最終更新日	このポリシーが前回修正された日付を表示します。
<input type="checkbox"/> 有効化	ポリシーを有効化または無効化するには、このチェックボックスをオンまたはオフにします。
サービス	

機能	説明
	<p>次のものを選択するメニューが表示されます。</p> <ul style="list-style-type: none"> • [グループ]: このポリシーに追加するサービスグループを選択するための[グループ]ダイアログを表示する場合。 • [サービス/ホスト]: このポリシーに追加するサービスまたはホストを選択するための[サービス/ホスト]ダイアログを表示する場合。ポリシーのタイプが[ホスト]の場合、メニューには[サービス]ではなく[ホスト]が表示されます。ポリシーのタイプに応じて、サービスまたはホストを選択できます。
	<p>選択されたサービスまたはグループをこのポリシーから削除します。</p>
<h3>ルール</h3>	
	<p>[ルールの追加]ダイアログが表示され、このポリシーのルールを定義できます。</p>
	<p>選択されたルールをこのポリシーから削除します。</p>
	<p>選択されたルールの[ルールの編集]ダイアログを表示します。</p>
<h3>ポリシーの抑制</h3>	
	<p>ポリシーを抑制する時間帯を追加します。</p>
	<p>選択されたポリシー抑制時間帯を削除します。</p>
<p>タイムゾーン</p>	<p>ドロップダウンリストからポリシーのタイムゾーンを選択します。このタイムゾーンは、ポリシー抑制とルール抑制の両方に適用されます。</p>
<input type="checkbox"/>	<p>ポリシー抑制時間帯を選択するには、チェックボックスをオンにします。</p>

機能	説明
日	指定した時間帯にポリシーを抑制する曜日。ポリシーを抑制する曜日をクリックします。曜日の任意の組み合わせ(すべての曜日を含む)を選択できます。
時間範囲	選択した曜日にポリシーが抑制される時間範囲。
通知	
+	メール通知行を追加します。
-	選択されたポリシー抑制時間帯を削除します。
通知の設定	[グローバル通知]ビューが開き、メール通知設定を定義できるようになります。
<input type="checkbox"/>	ポリシー抑制時間帯を選択するには、チェックボックスをオンにします。
出力	[グローバル通知]ページで定義された通知のタイプ。メール、SNMP、Syslog、スクリプトがあります。
受信者	通知の受信者の名前。
通知サーバ	メール通知サーバを選択します。このドロップダウンリストに表示される値のソースについては、「システム構成ガイド」の「通知サーバの構成」を参照してください。
テンプレート	このメール通知のテンプレートを選択します。RSAでは、Health & Wellness Default SMTP TemplateとAlarms Templateを提供しています。このドロップダウンリストに表示される他の値のソースについては、「システム構成ガイド」の「通知テンプレートの構成」を参照してください。
<div style="border: 1px solid green; padding: 5px;"> <p>注: 指定した受信者へのヘルスマニタメール通知に、ヘルスマニタテンプレートのデフォルトのメール件名を追加する場合は、「デフォルトのメール件名を含める」を参照してください。</p> </div>	

[グループ]ダイアログ

機能	説明
----	----

[グループ]パネル

名前	定義されたサービスグループを表示します。次のオプションを選択できます。 <ul style="list-style-type: none"> • [すべて]: [サービス]パネルにすべてのサービスが表示されます。 • 個々のグループ: [サービス]パネルにそのグループに属するサービスが表示されます。
----	--

[サービス]パネル

名前	サービスの名前を表示します。
ホスト	サービスが実行されているホストを表示します。
タイプ	サービスのタイプを表示します。

[ルール]ダイアログ

機能	説明
----	----

<input type="checkbox"/> 有効化	このポリシーのルールを有効化または無効化するには、このチェックボックスをオンまたはオフにします。
名前	ルールの名前を入力します。
説明	ルールの説明を入力します。RSAでは、次の情報をこのフィールドに含めることを推奨しています。 <ul style="list-style-type: none"> • 情報: ルールの目的と監視対象の問題。 • 改善策: このルールのアラームをトリガーする状況を解決するためのステップ。
重大度	ルールの重大度を選択します。有効な値は次のとおりです。 <ul style="list-style-type: none"> • クリティカル • 高 • 中 • 低

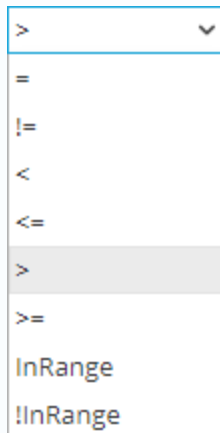
機能	説明
統計情報	<p>このルールでチェックする統計を選択します。次のオプションを選択できます。</p> <ul style="list-style-type: none"> 左ドロップダウン リストから統計のカテゴリを1つ選択します。 右ドロップダウン リストから統計を1つ選択します。 <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>注: PKI(公開鍵基盤)ポリシーの場合は、カテゴリで[公開鍵基盤]を選択して、次のいずれかの統計を選択します。</p> <ul style="list-style-type: none"> - NetWitnessサーバ公開鍵基盤証明書の有効期限: 証明書が期限切れになるまでの残り時間を表示します。 - NetWitnessサーバ公開鍵基盤CRLの有効期限: CRL(証明書失効リスト)が期限切れになるまでの残り時間を表示します。 - NetWitnessサーバ公開鍵基盤CRLのステータス: 現在のCRLのステータスを表示します。 </div> <p>ルールでチェックできる統計の例については、「[システム統計ブラウザ]ビュー」を参照してください。</p>
アラーム閾値	<p>ポリシーアラームをトリガーするルールの閾値を定義します。</p> <ul style="list-style-type: none"> amount <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>注: CRLの有効期限でサポートされている形式は、ddddhhmmです。たとえば、次のようになります。</p> <ul style="list-style-type: none"> - 10000は1日 - 2359は23時間59分 - 10023は1日と23分 - 3650100は365日と1時間 </div> <ul style="list-style-type: none"> 期間(分)
リカバリ	<p>ルールをクリアする閾値とタイミングを定義します。</p> <ul style="list-style-type: none"> 演算子: <ul style="list-style-type: none"> NetWitness Suite 10.5の場合: =、!=、<、<=、>、>= NetWitness Suite 10.5.0.1以降の場合: 以下の「閾値演算子」を参照してください amount 期間(分)
<h3>ルールの抑制</h3>	

機能	説明
+	このオプションを選択すると、ルール抑制時間帯を追加できます。
-	このオプションを選択すると、選択したルール抑制時間帯を削除できます。
<input type="checkbox"/>	チェックボックスをオンにすると、ルール抑制時間帯を選択できます。
タイムゾーン: <i>time-zone</i>	ポリシーのタイムゾーンを表示します。ポリシーのタイムゾーンは[ポリシーの抑制]パネルで選択します。
日	指定した時間帯にルールを抑制する曜日。ルールを抑制する曜日をクリックします。曜日の任意の組み合わせ(すべての曜日を含む)を選択できます。
時間範囲	選択した曜日にルールが抑制される時間帯。

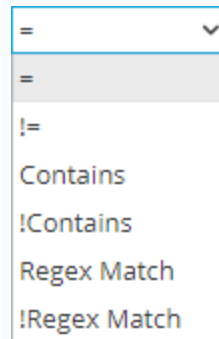
閾値演算子

[ルール]ダイアログの[アラーム閾値]フィールドと[リカバリ閾値]フィールドでは、指定した統計条件に基づいて数値演算子または文字列演算子のいずれかを入力するよう求められます。

数値演算子のドロップダウンメニュー:



文字列演算子のドロップダウンメニュー:



RSAヘルスマニタのメール テンプレート

注: 指定した受信者へのヘルスマニタメール通知に、ヘルスマニタテンプレートのデフォルトのメール件名を追加する場合は、「[デフォルトのメール件名を含める](#)」を参照してください。

ヘルスマニタ デフォルトSMTPテンプレート

RSA NetWitness Suite

Health Alarm Notification

File Collection Service is off on HOST1000

State

Active

Severity

High

Host

HOST1000

Service

Log Collector

AlarmId

103-2248-0001

Policy

Check Point

Rule

File Collection Service is off

Statistic

Collection State

Value

stopped

Time

April 13, 2015 10:48:13 PM UTC

アラーム テンプレート

RSA NetWitness Suite Health Alarm Notification

File Collection Service is off on HOST1000

State
Cleared

Severity
High

Host
HOST1000

Service
Log Collector

AlarmId
103-2248-0001

Policy
BootCamp Notification

Rule
Check Point Collection is off

Statistic
Collection State

Value
Policy-Disabled

Time
April 14, 2015 2:31:21 AM UTC

NetWitness Suiteの事前定義ポリシー

次の表は、NetWitness Suiteの事前定義ポリシーと、各ポリシーに定義されたルールの一覧を示しています。

これらのポリシーに対して次のタスクを実行できます。

- サービス/グループの割り当ての変更。
- ポリシーの有効化/無効化。

これらのポリシーに対して次のタスクを実行することはできません。

- ポリシーの削除。
- ポリシー名の編集。

注: 事前定義ポリシーに関する追加情報については、
[ヘルスマニタ]の[ポリシー]下のユーザ インタフェースを参照してください。

ポリシー名	ルール名	アラームのトリガー
	Communication Failure Between Master Security Analytics Host and a Remote Host	10分以上にわたって、ホストがダウンしている、 ネットワークがダウンしている、メッセージブロー カーがダウンしている、セキュリティ証明書が無 効または見つからない。

ポリシー名	ルール名	アラームのトリガー
NetWitness サーバ Monitoring Policy	Critical Usage on Rabbitmq Message Broker Filesystem	var/lib/rabbitmqで、マウントされたファイルシステム全体のディスク使用率が75%を超える。
	Filesystem is Full	マウントされたファイルシステム全体のディスク使用率が100%に達する。
	High Filesystem Usage	マウントされたファイルシステムのディスク使用率が95%を超える。
	High System Swap Utilization	スワップの使用率が5%を超える状態が5分以上継続する。
	High Usage on Rabbitmq Message Broker Filesystem	マウントされたファイルシステム全体のディスク使用率が60%を超える。
	Host Unreachable	ホストがダウンしている。
	LogCollector Event Processor Exchange Bindings Status	10分以上にわたってログ収集メッセージブローカーキューに問題がある。
	LogCollector Event Processor Queue with No Bindings	10分以上にわたってログ収集メッセージブローカーキューに問題がある。
	LogCollector Event Processor Queue with No Consumers	10分以上にわたってログ収集メッセージブローカーキューに問題がある。
	Power Supply Failure	ホストの電源がない。
RAID Logical Drive Degraded	RAID論理ドライブのステータスが「Degraded」または「Partially Degraded」である。	

ポリシー名	ルール名	アラームのトリガー
	RAID Logical Drive Failed	RAID論理ドライブのステータスが「Offline」、 「Failed」、「Unknown」である。
	RAID Logical Drive Rebuilding	RAID論理ドライブのステータスが「Rebuild」である。
	RAID Physical Drive Failed	RAID物理ドライブのステータスが、「Online」、 「Online Spun Up」、「Hotspare」のいずれでもない。
	RAID Physical Drive Failure Predicted	RAID物理ドライブの予測障害数が1より大きい。
	RAID Physical Drive Rebuilding	RAID物理ドライブのステータスが「Rebuild」である。
	RAID Physical Drive Unconfigured	RAID物理ドライブのステータスが「Unconfigured (good)」である。
	SD Card Failure	SDカードのステータスがOKでない。
NetWitness Suite Archiver Monitoring Policy	Archiver Aggregation Stopped	Archiverのステータスが「開始」でない。
	Archiver Database(s) Not Open	データベースのステータスが「オープン」でない。
	Archiver Not Consuming From Service	デバイスのステータスが「consuming」でない。
	Archiver Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	Archiver Service Stopped	サービスのステータスが「開始」でない。

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite Broker Monitoring Policy	Broker >5 Pending Queries	保留クエリが5個以上ある状態が10分以上継続している。
	Broker Aggregation Stopped	Brokerのステータスが「開始」でない。
	Broker Not Consuming From Service	デバイスのステータスが「consuming」でない。
	Broker Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	Broker Service Stopped	サービスのステータスが「開始」でない。
	Broker Session Rate Zero	セッションレート(現在)が0の状態が2分以上継続している。

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite	Concentrator >5 Pending Queries	保留クエリが5個以上ある状態が10分以上継続している。
Concentrator Monitoring Policy	Concentrator Aggregation Behind >100K Sessions	未処理デバイスセッションが100,000以上の状態が1分以上継続している。
	Concentrator Aggregation Behind >1M Sessions	未処理デバイスセッションが1,000,000以上の状態が1分以上継続している。
	Concentrator Aggregation Behind >50M Sessions	未処理デバイスセッションが50,000,000以上の状態が1分以上継続している。
	Concentrator Aggregation Stopped	Brokerのステータスが「開始」でない。
	Concentrator Database(s) Not Open	データベースのステータスが「オープン」でない。
	Concentrator Meta Rate Zero	Concentratorメタレート(現在)が0の状態が2分以上継続している。
	Concentrator Not Consuming From Service	デバイスのステータスが「consuming」でない。
	Concentrator Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	Concentrator Service Stopped	サービスのステータスが「開始」でない。

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite Decoder Monitoring Policy	Decoder Capture Not Started	収集ステータスが「開始」でない。
	Decoder Capture Rate Zero	収集レート(現在)が0の状態が2分以上継続している。
	Decoder Database Not Open	データベースのステータスが「オープン」でない。
	Decoder Dropping >1% of Packets	収集の/パケットドロップレート(現在)が1%以上である。
	Decoder Dropping >10% of Packets	収集の/パケットドロップレート(現在)が10%以上である。
	Decoder Dropping >5% of Packets	収集の/パケットドロップレート(現在)が5%以上である。
	Decoder Packet Capture Pool Depleted	パケット収集キューが0の状態が2分以上継続している。
	Decoder Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	Decoder Service Stopped	サービスのステータスが「開始」でない。

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite Event Steam Analysis Monitoring Policy	ESA Overall Memory Utilization > 85%	ESAの総メモリ使用率が85%以上である。
	ESA Overall Memory Utilization > 95%	ESAの総メモリ使用率が95%以上である。
	ESA Service Stopped	サービスのステータスが「開始」でない。
	ESA Trial Rules Disabled	評価版ルールのステータスが有効でない。
NetWitness Suite IPDB Extractor Monitoring Policy	IPDB Extractor Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	IPDB Extractor Service Stopped	サービスのステータスが「開始」でない。
NetWitness Suite Incident Management Monitoring Policy	Incident Management Service Stopped	サービスのステータスが「開始」でない。

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite Log Collector Monitoring Policy	Log Collector Service Stopped	サービスのステータスが「開始」でない。
	Log Decoder Event Queue > 50% Full	現在のキューのイベント数がキューの50%以上を使用している。
	Log Decoder Event Queue > 80% Full	現在のキューのイベント数がキューの80%以上を使用している。
	Log Collector Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
NetWitness Suite Log Decoder Monitoring Policy	Decoder Dropping > 10% of Packets	収集のパケットドロップレート(現在)が10%以上である。
	Log Capture Not Started	収集ステータスが「開始」でない。
	Log Decoder Capture Rate Zero	収集レート(現在)が0の状態が2分以上継続している。
	Log Decoder Database Not Open	データベースのステータスが「オープン」でない。
	Log Decoder Dropping > 1% of Logs	収集のパケットドロップレート(現在)が1%以上である。
	Log Decoder Dropping > 5% of Logs	収集のパケットドロップレート(現在)が5%以上である。
	Log Decoder Packet Capture Pool Depleted	パケット収集キューが0の状態が2分以上継続している。
	Log Decoder Service Stopped	サービスのステータスが「開始」でない。
Log Decoder Service in Bad State	サービスのステータスが「開始」または「Ready」でない。	

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite Malware Analysis Monitoring Policy	Malware Analysis Service Stopped	サービスのステータスが「開始」でない。
NetWitness Suite Reporting Engine Monitoring Policy	Reporting Engine Alerts Critical Utilization	アラート使用率が10%以上の状態が5分以上継続している。
	Reporting Engine Available Disk <10%	使用可能ディスク領域が10%未満である。
	Reporting Engine Available Disk <5%	使用可能ディスク領域が5%未満である。
	Reporting Engine Charts Critical Utilization	チャート使用率が10%以上の状態が5分以上継続している。
	Reporting Engine Rules Critical Utilization	ルール使用率が10%以上の状態が5分以上継続している。
	Reporting Engine Schedule Task Pool Critical Utilization	スケジュールタスクプール使用率が10%以上の状態が15分以上継続している。
	Reporting Engine Service Stopped	サービスのステータスが「開始」でない。
	Reporting Engine Shared Task Critical Utilization	共有タスクプール使用率が10%以上の状態が5分以上継続している。

ポリシー名	ルール名	アラームのトリガー
NetWitness Suite Warehouse Connector Monitoring Policy	Warehouse Connector Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	Warehouse Connector Service Stopped	サービスのステータスが「開始」でない。
	Warehouse Connector Stream Behind	未処理のストリームが2,000,000以上である。
	Warehouse Connector Stream Disk Utilization > 75%	ストリーム ディスク使用率(宛先ロード待ち)が75%以上である。
	Warehouse Connector Stream in Bad State	ストリームのステータスが、「consuming」または「Online」でない状態が10分以上継続している。
	Warehouse Connector Stream Permanently Rejected Files > 300	永続的に拒否したファイルの数が300以上である。
	Warehouse Connector Stream Permanently Rejected Folder > 75% Full	拒否フォルダの使用率が75%以上である。
NetWitness Suite Workbench Monitoring Policy	Workbench Service in Bad State	サービスのステータスが「開始」または「Ready」でない。
	Workbench Service Stopped	サービスのステータスが「開始」でない。

[システム統計ブラウザ]ビュー

NetWitness Suiteには、ホストとサービスのステータスやオペレーションを監視する方法が用意されています。[システム統計ブラウザ]タブには、収集状況、ホストまたはサービスのシステム情報が表示されます。

選択したパラメータに基づいて統計ビューをカスタマイズして、データをフィルタ表示することができます。

[システム統計ブラウザ]ビューにアクセスするには、次の手順を実行します。

1. [管理]>[ヘルスマニタ]に移動します。
[ヘルスマニタ]ビューが表示され、[アラーム]タブが開きます。
2. [システム統計ブラウザ]タブをクリックします。

実行したいことは何ですか？

ロール	実行したいこと	手順
管理者	システム統計の履歴チャートの表示	システム統計の履歴チャート

関連トピック

[サービス統計情報の監視](#)

[システム統計のフィルタ](#)

[システム統計の履歴チャートの表示](#)

簡単な説明

[システム統計ブラウザ]ビューが表示されます。

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
localhost.localdomain	Host	FileSystem	Error Status		0	2017-05-17 05:32:38 PM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/run/user/0	3.14 GB size 0 bytes used 3.14 GB available	2017-05-17 04:07:38 AM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/dev	15.70 GB size 0 bytes used 15.70 GB available	2017-05-17 05:32:38 PM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/sys/fs/cgroup	15.71 GB size 0 bytes used 15.71 GB available	2017-05-17 05:32:38 PM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/run	15.71 GB size 8.43 MB used 15.70 GB available	2017-05-17 05:32:38 PM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/	70.09 GB size 2.82 GB used 67.27 GB available	2017-05-17 05:32:38 PM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/dev/shm	15.71 GB size 12.00 KB used 15.71 GB available	2017-05-17 05:32:38 PM	📊
localhost.localdomain	Host	FileSystem	Mounted Filesystem Disk Usage	/home	3.99 GB size 32.16 MB used 3.96 GB available	2017-05-17 05:32:38 PM	📊

1 [システム統計ブラウザ]ビューが表示されます

2 [システム統計ブラウザ]ビューのフィルタとカスタマイズに使用されるツールバー

フィルタ

この表は、システム統計ビューのフィルタとカスタマイズに使用できるさまざまなパラメータを示しています。

パラメータ	説明
ホスト	統計情報を表示するホストをドロップダウンメニューから選択します。 使用可能なすべてのホストをリストするには、[任意]を選択します。
コンポーネント	統計を表示するコンポーネントをドロップダウンメニューから選択します。 選択したホスト上のすべてのコンポーネントをリストするには、[任意]を選択します。
カテゴリ	統計を表示する必要があるカテゴリを入力します。 Regexフィルタを有効化するには、[Regex]を選択します。このフィルタを有効にすると、テキストに対して正規表現検索が実行され、一致するカテゴリがリストされます。 [Regex]を選択していない場合は、グロービングパターンマッチングがサポートされません。
統計情報	すべてのホストまたはコンポーネントに関して表示する必要がある統計情報を入力します。 Regexフィルタを有効化するには、[Regex]を選択します。このフィルタを有効にすると、テキストに対して正規表現検索が実行され、一致するカテゴリがリストされます。 [Regex]を選択していない場合は、グロービングパターンマッチングがサポートされません。
Order By	リストを表示する際のソート順を選択します。 リストを昇順でフィルタ表示するには、[昇順]を選択します。

コマンド

コマンド	アクション
適用	クリックすると、選択したフィルタが適用され、設定した条件でリストが表示されます。
クリア	クリックすると、選択したフィルタが解除されます。

システム統計ビューの表示

統計情報、サービスまたはホストのシステム情報が表示されます。

統計の詳細へのアクセス

いずれかの統計情報を選択して、パネルの右側にある[統計の詳細]をクリックします。

[統計の詳細]パネルが開き、選択した統計情報の詳細が表示されます。

Stat Details	
Host	14e55a22-12ba-4af2-a376-80a2ebe49993
Hostname	NWAPPLIANCE10604
Component ID	appliance
Component	Host
Name	Mounted Filesystem Disk Usage
Subitem	/dev/shm
Path	
Plugin	appliance_df
Plugin Instance	dev_shm
Type	fs_usage
Type Instance	
Description	Disk usage information for mounted filesystem /dev/shm
Category	FileSystem
Last Updated Time	2017-07-14 03:11:18 PM
Value	15.71 GB size, 12.00 KB used, 15.71 GB available
Raw Value	1.686945792E10 bytes size, 12288.0 bytes used, 1.6869445632E10 bytes available
Graph Data Key	14e55a22-12ba-4af2-a376- 80a2ebe49993/appliance_df-dev_shm/fs_usage
Stat Key	14e55a22-12ba-4af2-a376- 80a2ebe49993/appliance_df-dev_shm/fs_usage
stat_collector_version	11.0.0.0
Filesystem	tmpfs

[システム]ビュー: [システム]の[情報]パネル

このトピックでは、システムのバージョンやライセンス ステータスなどの情報を表示する[システム]の[情報]パネルについて説明します。

このビューへのアクセスに必要な権限は、[システム設定の管理]です。

このビューにアクセスするには、次のいずれかを実行します。

- [管理] > [システム]に移動します。
デフォルトでは、[システム]の[情報]パネルが表示されます。
- [通知]トレイにNetWitness Suiteの更新が使用可能という通知が表示されている場合は、[表示]をクリックします。

Version Information	
Current Version	11.0.0.0-170917005424.1.daecdd2
Current Build	170917005424
License Server ID	0050560145B5
License Status	Enabled <input type="button" value="Disable"/>

[バージョン情報]セクションには、現在インストールされているNetWitness Suiteのバージョン情報が表示されます。次の表に、[バージョン情報]セクションの機能とその説明を示します。

名前	説明
現在 のバー ジョン	<p>現在実行しているSecurity Analyticsのバージョンが表示されます。バージョンの形式は、<i>major-release.minor-release.stability-id.build-number</i>です。<i>stability-id</i>の値は次のようになります。</p> <ul style="list-style-type: none"> • 1: 開発中 • 2: アルファ • 3: ベータ • 4: RC • 5: ゴールド
現在 のビル ド	<p>現在のビルド番号を表します。主にトラブルシューティングの際に使用されます。</p>
ライセ ンス サーバ ID	<p>各クライアントホストは、ホストのライセンスを管理するために、LLS(Local Licensing Server)がインストールされた状態で出荷されます。このフィールドは、このSecurity AnalyticsのインスタンスにLLSがインストールされているかどうかを表します。</p> <ul style="list-style-type: none"> • LLSがインストールされている場合は、ライセンスサーバIDが表示されます。 • [Unknown](不明)と表示されている場合、LLSがインストールされていないことを表します。
ライセ ンスス テータ ス	<p>ライセンスが有効かどうかを示します。ライセンスの状態に応じて、次のようになります。</p> <ul style="list-style-type: none"> • 有効な場合: このフィールドに「有効」と表示されます。右側の[無効化]ボタンをクリックしてライセンスを無効化できます。 • 無効な場合: このフィールドに「無効」と表示されます。右側の[有効化]ボタンをクリックしてライセンスを有効化できます。

[システム]の[更新]パネル - [設定]タブ

「[システム更新の設定]タブ」では、Live更新リポジトリへの接続をセットアップする場合に使用するインタフェースについて説明します。これらの設定によって、NetWitness SuiteはLive更新リポジトリにアクセスし、ローカル更新リポジトリを同期することができるようになります。

このビューへのアクセスに必要な権限は、[システム更新の適用]です。

このビューにアクセスするには、次の手順を実行します。

1. [管理]>[システム]に移動します。
2. [更新]を選択します。

実行したいことは何ですか？

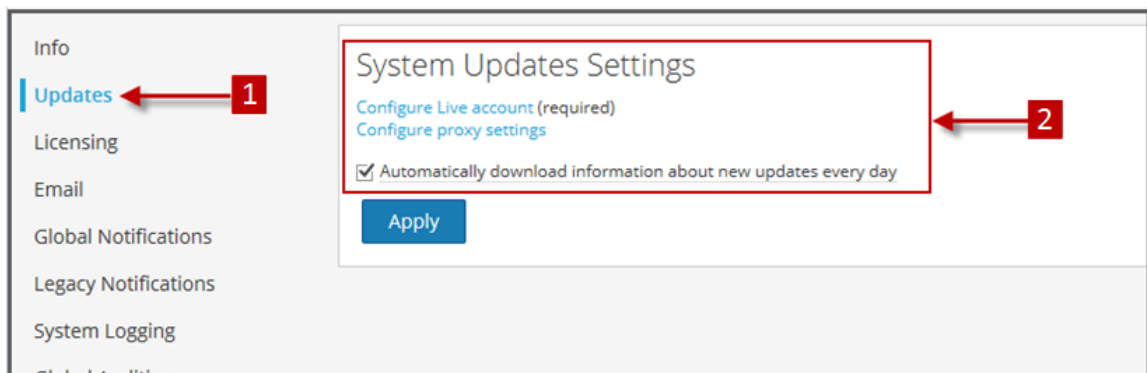
ロール	実行したいこと	手順
管理者	更新の自動ダウンロード	RSA更新リポジトリとの自動同期を有効化します。

関連トピック

[NetWitness Suiteでの更新の管理](#)

簡単な説明

[システム更新の設定]パネルが表示されます。



1 [システム更新の設定]タブが表示されます

2 自動更新用のアカウントと設定を構成します

機能

この表は、[システム更新の設定]パネルの機能について説明しています。

機能	説明
Liveアカウントの構成	[ADMIN] > [システム] > [Liveサービス] パネルを表示します。Liveアカウント認証情報を構成していない場合は、このパネルで構成できます。
プロキシ設定の構成	[ADMIN] > [システム] > [HTTPプロキシ設定] パネルを表示します。HTTPプロキシ設定を構成していない場合は、ここで構成できます。
新しい更新に関する情報を毎日自動的にダウンロード	選択すると、RSA更新リポジトリとの自動同期が有効になります。使用可能な新しい更新がある場合に、[ADMIN] > [ホスト] パネルに情報が自動的に表示されます。
適用	このタブの設定を適用します。

[システム ログ]: [設定] ビュー

RSA NetWitness Suiteの[システム ログ] パネルにある[設定] ビューでは、ログファイルのサイズ、保持するバックアップログファイルの数、NetWitness Suite内のパッケージに対するデフォルトのログレベルを構成します。詳細な手順については、「システム構成ガイド」の「ログファイル設定の構成」を参照してください。

[設定] タブにアクセスするには、次の手順を実行します。

1. [管理] > [システム] に移動します。
2. [オプション] パネルで[システム ログ] を選択します。
[システム ログ] パネルが開き、デフォルトで[リアルタイム] タブが表示されます。
3. [設定] タブをクリックします。

実行したいことは何ですか？

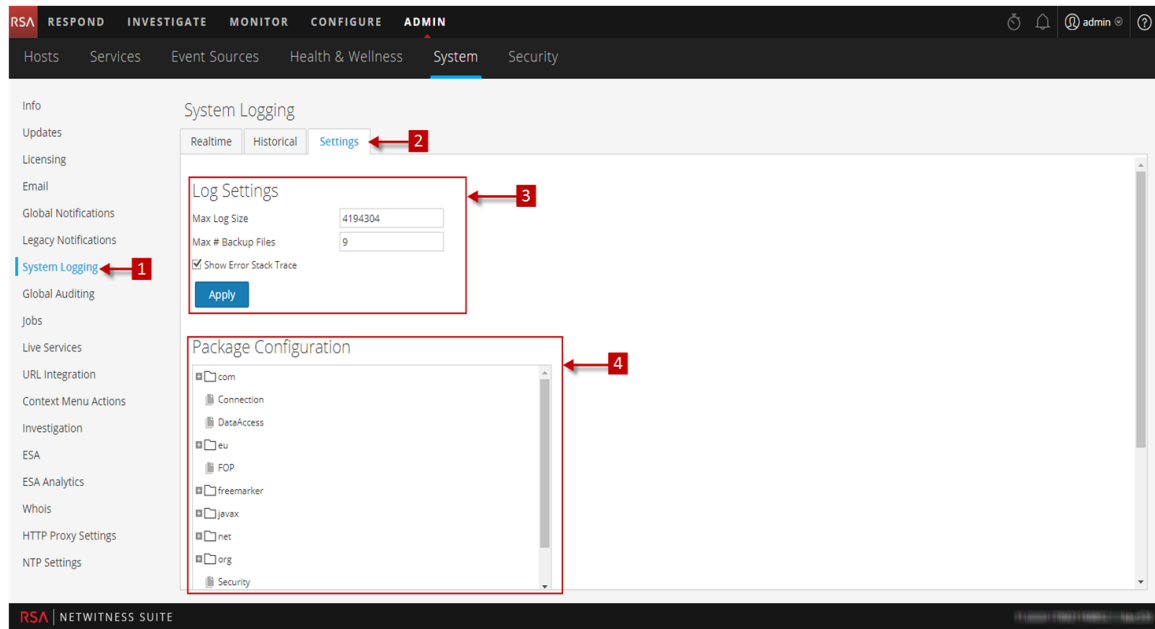
ロール	実行したいこと	手順
管理者	ログファイルのサイズの構成	[ログの設定] ツールバーのセットアップ

関連トピック

[\[システム ログ\] : \[履歴\] タブ](#)

[\[システム ログ\] : \[リアルタイム\] タブ](#)

簡単な説明



- 1 [システム ログ] パネルが表示されます
- 2 [設定] タブが表示されます
- 3 このセクションでは、ユーザがログの設定を構成できます
- 4 このセクションでは、ユーザがパッケージを構成できます

機能

[設定] タブには、[ログの設定] と [パッケージ構成] の2つのセクションがあります。

ログの設定

[ログの設定] セクションでは、NetWitness Suiteのログ ファイルのサイズと、NetWitness Suiteで保持するバックアップ ログの数を構成します。

機能	説明
最大ログ サイズ	各ログ ファイルの最大サイズをバイトで指定します。この設定の最小値は4,096です。

機能	説明
最大バックアップファイル数	保持するバックアップログファイルの数を指定します。この設定の最小値は0です。ログファイルの最大数に到達し、新しいバックアップファイルが作成されると、最も古いバックアップが破棄されます。
エラースタックトレースの表示	チェックボックスを選択すると、エラー、スタック、トレースのログメッセージが表示されます。
適用	以降のすべてのログに対して、設定をただちに有効にします。

パッケージ構成

[パッケージ構成]セクションのツリー構造にNetWitness Suiteのパッケージが表示されます。

機能	説明
パッケージツリー	ツリーにはNetWitness Suite内で使用されるすべてのパッケージが含まれています。ツリーをドリルダウンすることで、各パッケージのログレベルを表示できます。 rootログレベルは、明示的には設定されないすべてのパッケージに対するデフォルトのログレベルを表します。rootレベルはINFOに設定されています。
[パッケージ]フィールド	このフィールドには、 パッケージ ツリーでパッケージを選択したときに、そのパッケージの名前が表示されます。
ログレベル	選択したパッケージにログレベルが明示的に設定されている場合は、その値が [ログレベル] フィールドに表示されます。
再帰的にリセット	チェックボックスを選択すると、ログが再帰的にリセットされます。
適用	以降のすべてのログに対して、設定をただちに有効にします。
リセット	選択したパッケージをrootのログレベルにリセットします。

[システム ログ]: [リアルタイム] タブ

このトピックでは、[システム] の [ログ] > [リアルタイム] タブと、[サービス] の [ログ] ビュー > [リアルタイム] タブの機能について説明します。

[リアルタイム] タブは、NetWitness Suite のログまたはサービス ログをリアルタイムに表示するビューです。このタブをロードすると、ビューには最新のログ エントリーが10個表示されます。新しいログ エントリーが記録されると、ビューが更新され、そのエントリーが表示されます。

[リアルタイム] タブにアクセスするには:

1. [管理] > [システム] に移動します。
2. [オプション] パネルで [システム ログ] を選択します。
[システム ログ] パネルが開き、デフォルトで [リアルタイム] タブが表示されます。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	ログ エントリーの詳細の表示	システム ログとサービス ログの表示

関連トピック

[\[システム ログ\]: \[設定\] ビュー](#)

[\[システム ログ\]: \[履歴\] タブ](#)

簡単な説明

次の図は[システム ログ]パネルに表示される[リアルタイム]タブの例です。

The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'System' tab is active. On the left, the 'System Logging' menu item is highlighted with a red callout '1'. The main content area shows the 'System Logging' panel with the 'Realtime' tab selected, indicated by a red callout '2'. The panel includes a search bar and a table of log entries.

Timestamp	Level	Message
2017-09-27T11:06:53.371	WARN	Host has not received update, resetting Concentrator-New
2017-09-27T11:06:58.035	INFO	No new TAXII data for feed Haila.
2017-09-27T11:08:56.039	INFO	No new TAXII data for feed TAXIIProxy.
2017-09-27T11:10:20.037	INFO	No new TAXII data for feed Anomall.
2017-09-27T11:11:53.369	WARN	Service has not received update, resetting LogDecoder-New - Log Collector
2017-09-27T11:11:53.370	WARN	Service has not received update, resetting LogDecoder-New - Log Decoder
2017-09-27T11:11:53.371	WARN	Host has not received update, resetting LogDecoder-New
2017-09-27T11:11:53.371	WARN	Service has not received update, resetting Concentrator-New - Concentrator
2017-09-27T11:11:53.372	WARN	Host has not received update, resetting Concentrator-New
2017-09-27T11:11:58.039	INFO	No new TAXII data for feed Haila.
2017-09-27T11:13:56.046	INFO	No new TAXII data for feed TAXIIProxy.
2017-09-27T11:15:20.038	INFO	No new TAXII data for feed Anomall.

1 [システム ログ]パネルが表示されます

2 [リアルタイム]タブが表示されます

次の図は[サービス]の[ログ]ビューにある[リアルタイム]タブの例です。これらのタブには類似した項目が表示されます。


The screenshot shows the RSA NetWitness Suite interface. The top navigation bar includes 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Services' tab is active. On the left, the 'Logs' menu item is highlighted with a red callout '1'. The main content area shows the 'System Logging' panel with the 'Realtime' tab selected, indicated by a red callout '2'. The panel includes a search bar and a table of log entries.

Timestamp	Level	Message
2017-09-27T11:18:07.000	INFO	Broker returned 0 from session call because of dead range 11,458,239, 11,458,238
2017-09-27T11:18:07.000	AUDIT	User admin (session 1471833, 10.31.204.145:47332) has requested the SDK session info: id1=11458239 id2=11458238
2017-09-27T11:18:07.000	INFO	Broker returned 0 from session call because of dead range 11,458,239, 11,458,238
2017-09-27T11:18:40.000	AUDIT	User admin (session 1471745, 10.31.204.145:47288) has logged out
2017-09-27T11:18:42.000	INFO	Accepting connection from trusted peer 10.31.204.145 with subject name C = US, ST = VA, L = Reston, O = RSA, OU = NetWitness, CN = a4c8b5e6-bbc9-44ed-b6b0-9a971516e6c1
2017-09-27T11:18:42.000	AUDIT	User admin (session 1471882, 10.31.204.145:37796) has logged in
2017-09-27T11:18:42.000	WARN	User admin has a mismatch for query.simeout in local account and trusted credentials. Using supplied value 5.
2017-09-27T11:18:42.000	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 10000.
2017-09-27T11:18:42.000	AUDIT	User admin (session 1471899, 10.31.204.145:36104) has logged in
2017-09-27T11:18:43.000	AUDIT	User escalateduser (session 1471916, 10.31.204.145:37796) has logged in

機能

[リアルタイム]タブにはツールバーがあり、エントリーをフィルタできる入力フィールドが表示されます。またツールバーの下にはログエントリーを表示するグリッドがあります。

ツールバー

機能	説明
ログレベルドロップダウン 	グリッドに表示するエントリーのログレベルを選択します。[ログレベル]ドロップダウンには、システムまたはサービスで使用可能なログレベルが表示されます。 <ul style="list-style-type: none"> システムログには、ログレベルが7種類あります。 サービスログには[トレース]レベルがないため、ログレベルは6種類です。 デフォルトは、[すべて]になっています。
[キーワード]フィールド	エントリーをフィルタリングする際に使用するキーワードを指定します。このフィールドは、システムおよびサービスのログフィルタリングで共通です。
[サービス]フィールド(サービスログのみ)	サービスログでログを表示するサービスタイプを指定できます。指定可能な値は、ホストまたはサービスです。
[検索]ボタン	クリックすると、ログレベル、キーワード、サービスの選択内容に基づいてフィルタが実行されます。

ロググリッドの列

列	説明
タイムスタンプ	エントリーのタイムスタンプです。
レベル	メッセージのログレベルです。
メッセージ	ログエントリーのテキストです。

[システム ログ]:[履歴]タブ

[履歴]タブでは、NetWitness Suiteのログまたはサービスのログの履歴をページ形式で表示および検索できます。最初のロード時、グリッドには、システムまたはサービスの最新のログエントリのページが表示されます。

[履歴]タブにアクセスするには、次の手順を実行します。

1. [管理]>[システム]に移動します。
2. [オプション]パネルで[システム ログ]を選択します。
[システム ログ]パネルが開き、デフォルトで[リアルタイム]タブが表示されます。
3. [履歴]タブをクリックします。

実行したいことは何ですか?

ロール	実行したいこと	手順
管理者	履歴チャートの表示	システム統計の履歴チャート

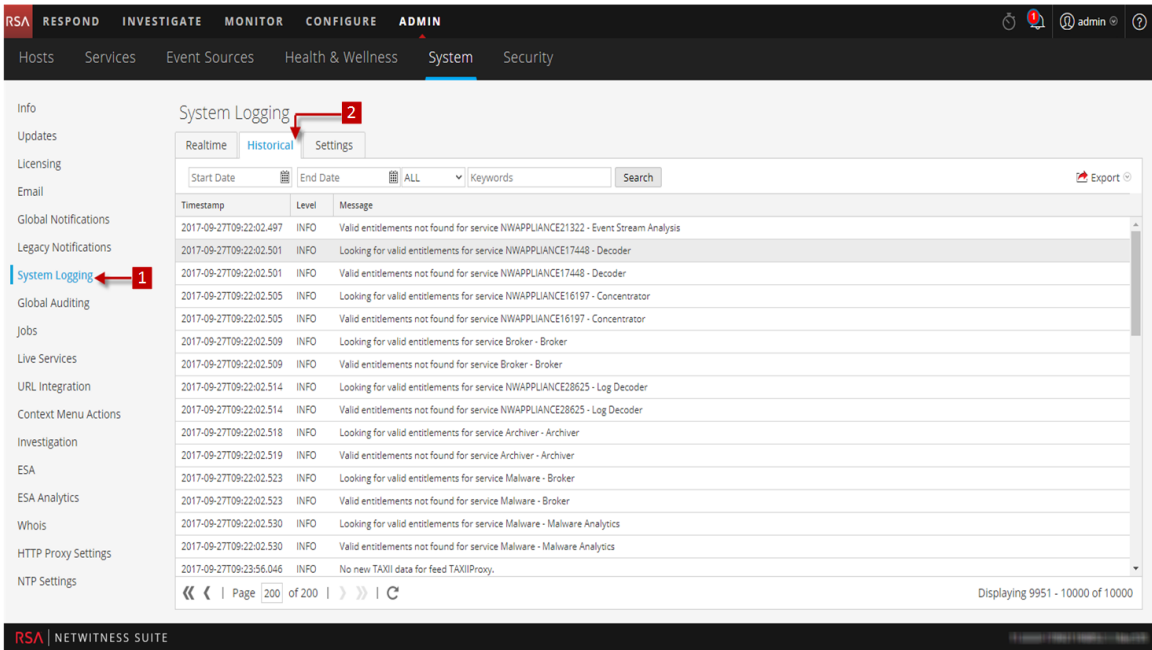
関連トピック

[\[システム ログ\]:\[リアルタイム\]タブ](#)

[\[システム ログ\]:\[設定\]ビュー](#)

簡単な説明

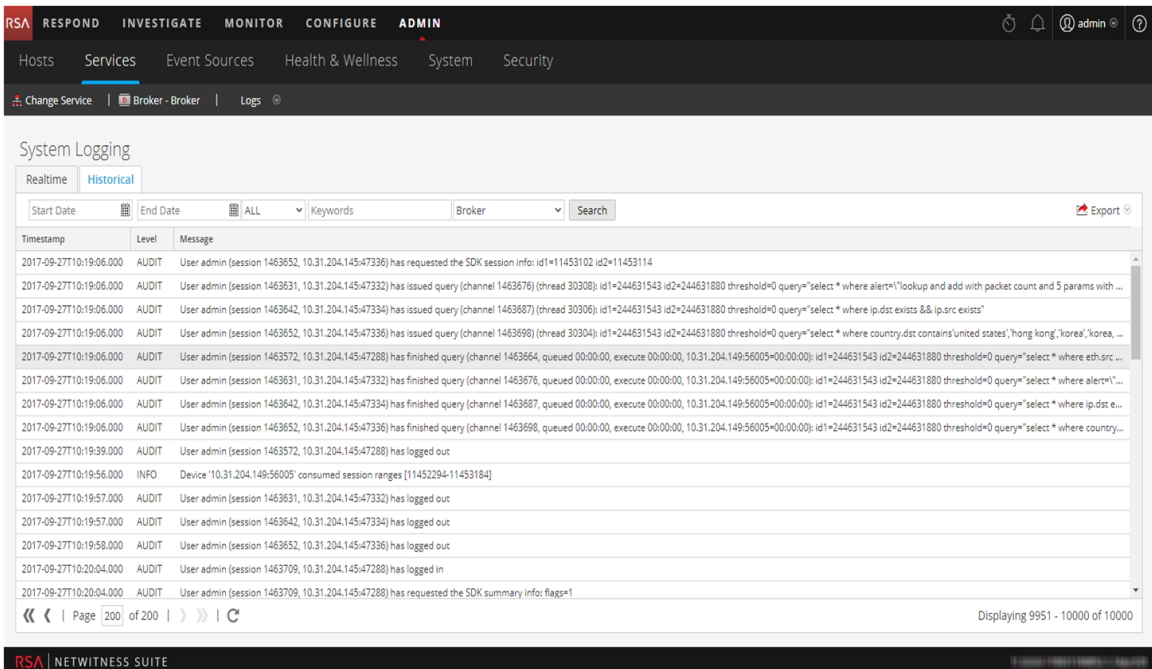
次の図は、[システム ログ] パネルにある[履歴]タブの例です。NetWitness Suiteのログを示しています。



1 [システム ログ] タブの表示

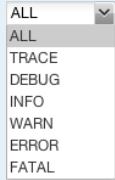
2 [履歴] タブの表示

次の図は、[サービス]の[ログ]ビューにある[履歴]タブの例です。この例では、サービスのログが表示されています。



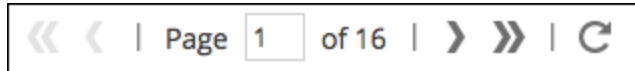
機能

[履歴]タブにはツールバーがあり、エントリーをフィルタできる入力フィールドが表示されます。またログエントリーが表示されるグリッドと、ページを操作するツールも表示されます。

機能	説明
[開始日]および[終了日]	[開始日]と[終了日]の検索範囲オプションは、ログエントリーの表示範囲を一定の範囲に限定します。これらを使用する際には、開始日と終了日の両方を指定する必要があります。時刻の設定はオプションです。終了日は、開始日より前には設定できません。
ログレベルドロップダウン	グリッドに表示するエントリーのログレベルを選択します。[ログレベル]ドロップダウンには、システムまたはサービスで使用可能なログレベルが表示されます。 <ul style="list-style-type: none"> システムログには、ログレベルが7種類あります。 サービスログには[トレース]レベルがないため、ログレベルは6種類です。 デフォルトは、[すべて]になっています。 
[キーワード]フィールド	エントリーをフィルタリングする際に使用するキーワードを指定します。このフィールドは、システムおよびサービスのログフィルタリングで共通です。
[サービス]フィールド (サービスログのみ)	サービスログでログを表示するサービスタイプを指定できます。指定可能な値は、ホストまたはサービスです。
[検索]ボタン	クリックすると、開始日と終了日、ログレベル、キーワード、サービスの選択内容に基づいてログエントリーが絞り込まれます。
エクスポート	クリックすると、現在表示されているグリッドエントリーがテキストファイルにエクスポートされます。ファイル形式は、カンマ区切りまたはタブ区切りを選択できます。

列	説明
タイムスタンプ	エントリーのタイムスタンプです。
レベル	メッセージのログレベルです。
メッセージ	ログエントリーのテキストです。

グリッドの下にあるページ移動ツールを使用して、ログエントリーのページを移動できます。



ログエントリーの検索

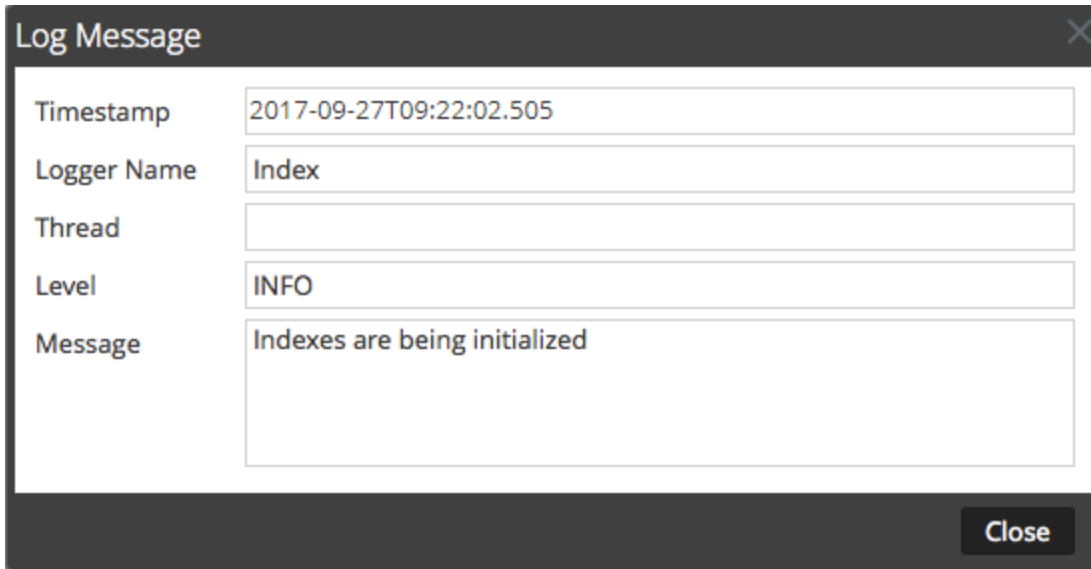
[履歴]タブで表示される結果をフィルタするには、次の手順を実行します。

1. (オプション) [開始日]および[終了日]を選択します。オプションで[開始時刻]での時間、および[終了時刻]での時間を選択します。
2. (オプション) システムログとサービスログでは、[ログレベル]や[キーワード]を選択します。
3. (オプション) サービスログの場合は、[サービス]でホストまたはサービスを選択します。
4. [検索]をクリックします。
ビューが更新され、フィルタに一致する最新の10件のエントリーが表示されます。フィルタ条件に合致する新しいログエントリーが記録されると、ビューが更新され、エントリーが表示されます。

ログエントリーの詳細を表示

ロググリッドの[履歴]タブの各行に、ログエントリーのサマリ情報が記載されています。詳細を表示するには、次の手順を実行します。

1. ログエントリーをダブルクリックします。
[ログメッセージ]ダイアログが表示され、[タイムスタンプ]、[ロガー名]、[スレッド]、[レベル]、[メッセージ]の各項目が表示されます。



2. ダイアログを閉じるには、[閉じる]をクリックします。

ログ エントリーのページの移動

グリッドの別のページを表示するには、グリッドの下部にあるページ移動ツールを使用します。

- ナビゲーション ボタンの使用
- 表示したいページを手動で入力し、Enterキーを押します。

エクスポート

現在のビューに表示されているログをエクスポートするには、次の手順を実行します。

[エクスポート]をクリックして、ドロップダウン オプション([CSV形式]または[タブ区切り]のいずれか)を選択します。

ログタイプとフィールド区切り文字が識別可能なファイル名の付いたファイルがダウンロードされます。たとえば、CSVでエクスポートされたNetWitness Suiteシステム ログの名前は、UAP_log_export_CSV.txtとなり、タブ区切り値でエクスポートされたアプライアンス ログの名前は、APPLIANCE_log_export_TAB.txtとなります。