RSA NETWITNESS® SUITE

Leitfaden Datenschutzmanagement

für Version 11.0

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2018

Inhalt

Übersicht zum Datenschutz

In diesem Thema werden Überlegungen zum Konzept und zur Implementierung für einen Datenschutzbeauftragten oder Administrator behandelt, der den Umgang mit datenschutzrelevanten Daten in RSA NetWitness® Suite managt. Außerdem enthält es Informationen zu empfohlenen Anwendungsbeispielen.

Hinweis: Ein Datenschutzplan hat Auswirkungen auf fast alle Komponenten von NetWitness Suite. Die Person, die für die Konfiguration des Datenschutzes zuständig ist, muss die NetWitness Suite-Netzwerkkomponenten kennen, die Konfiguration von NetWitness Suite-Hosts und -Services verstehen, die im *Leitfaden für die ersten Schritte mit Hosts und Services* beschrieben sind, und wissen, welche Arten von Informationen geschützt werden müssen.

Behördliche Vorschriften in einigen Regionen, zum Beispiel in der Europäischen Union (EU), sehen vor, dass Informationssysteme über Einrichtungen zum Schutz von datenschutzrelevanten Daten verfügen müssen. Daten, aus denen sich direkt oder indirekt ableiten lässt, „wer was wann getan hat“, sind als datenschutzrelevante Daten zu betrachten. Dazu zählen beispielsweise auch Benutzernamen, E-Mail-Adressen und Hostnamen. NetWitness Suite bietet eine Reihe an Steuerungsmechanismen, die Kunden zum Schutz von datenschutzrelevanten Daten nutzen können. Diese Steuerungsmechanismen können in einer Vielzahl an Kombinationen zum Schutz der datenschutzrelevante Daten eingesetzt werden, ohne dass die Analysefunktionen signifikant beeinträchtigt werden.

Eine neue Benutzerrolle für den DPO (Data Privacy Officer, Datenschutzbeauftragter) wurde in NetWitness Suite 10.5 hinzugefügt, um das Management von datenschutzrelevanten Daten zu unterstützen. Der DPO kann NetWitness Suite durch eine Kombination verschiedener Techniken so konfigurieren, dass die Risikoexposition von Metadaten und Rohdateninhalten (Pakete und Protokolle) beschränkt wird. In NetWitness Suite werden folgende Methoden für den Schutz von Daten angewendet:

- Datenverschleierung
- Steuerung der Datenaufbewahrung
- Auditprotokollierung

Datenverschleierung

NetWitness Suite verfügt über konfigurierbare Optionen für die Datenverschleierung. Datenschutzbeauftragte und Administratoren können festlegen, welche Metaschlüssel in der Umgebung datenschutzrelevant sind, und einschränken, an welcher Stelle im NetWitness Suite-Netzwerk die Metawerte und Rohdaten für diese Schlüssel angezeigt werden. Statt der Originalwerte kann NetWitness Suite verschleierte Darstellungen zu Ermittlungs- und Analysezwecken bereitstellen. Darüber hinaus können DPOs und Administratoren die Persistenz datenschutzrelevanter Metawerte und Rohdatenprotokolle oder-pakete einschränken.

Zu Implementierung der Datenverschleierung wirken drei Methoden zusammen:

- Verschleierung von Metawerten zu datenschutzrelevanten Metaschlüsseln mit einem optionalen Salt. Als geschützt konfigurierte Metaschlüssel werden zum Zeitpunkt der Erstellung auf einem Decoder oder Log Decoder durch verschleierte Werte ersetzt. Die verschleierten Werte sind gehasht und werden als unlesbar eingestuft. Zur Implementierung müssen der Hashalgorithmus und Salt für Decoder und Log Decoder konfiguriert werden. Außerdem müssen datenschutzrelevante Sprachschlüssel auf allen Core-Services als geschützt eingerichtet werden.
- Rollenbasierte Zugriffskontrolle (Role-based Access Control, RBAC) für den Zugriff auf die Rohdatenprotokolle oder -pakete und datenschutzrelevante Metawerte. Der DPO kann Rollen mit fein abgestimmten Rechten zuordnen, die beschränken, welche Daten ein Analyst im Gegensatz zum Data Privacy Officer während der Konfiguration, Analyse und Untersuchung anzeigen kann. Das Handbuch *Systemsicherheit und Benutzerverwaltung* enthält eine detaillierte Darstellung der RBAC-Implementierung in NetWitness Suite. Zur Implementierung muss die Sichtbarkeit von Metawerten und Inhalten für jede Rolle auf den einzelnen Brokers, Concentrators, Decoder, Log Decoders und Archivers konfiguriert werden.
- Verhindern der Persistenz von datenschutzrelevanten Metawerten und Rohdatenprotokollen oder -paketen. Zur Implementierung müssen die Metaschlüssel auf Parsern für die einzelnen Decoders und Log Decoders als vorübergehend konfiguriert werden.

Steuerung der Datenaufbewahrung

NetWitness Suite ermöglicht es, Daten nur so lange aufzubewahren, wie dies erforderlich oder vorgegeben ist. Ein Administrator kann die Datenaufbewahrung mithilfe von Alters- und Zeitschwellenwerten auf Pro-Service-Basis konfigurieren. Auf jedem Service ausgeführte Planer löschen automatisch Daten, die diese Schwellenwerte erreichen. Einmal gelöscht, sind die Daten nicht länger in Benutzeroberflächen, Abfragen oder API-Aufrufen (Application Programming Interface) verfügbar. Einige Komponenten von NetWitness Suite unterstützen zudem das Löschen von Daten durch Überschreiben.

Der Administrator kann die Datenaufbewahrung auf verschiedene Weisen organisieren:

- Konfigurieren der Verweildauer von Daten im Speicher auf dem System.
- Für Core-Services: Konfigurieren einer automatischen Löschung von datenschutzrelevanten Daten eines bestimmten Alters, um eventuell gespeicherte sensible Daten strategisch zu entfernen.
- Konfigurieren von NetWitness Suite in einer Weise, dass Originaldaten nicht an andere Komponenten gesendet oder darauf gespeichert werden. Falls datenschutzrelevante Daten in andere Datenbanken auf den Reporting Engine-, Malware Analysis- und NetWitness-Servern übertragen werden, kann die Datenaufbewahrung dort ebenfalls gesteuert werden. Diese Konfiguration für Event Stream Analysis wird in der Ansicht „Services-Explorer“ gemanagt.

Hinweis: Wenn der DPO in einer bestimmten Situation, nachdem das System in Funktion ist, entscheidet, dass bereits gesammelte Daten datenschutzrelevant sind, kann der Administrator diese Daten manuell in den Datenbanken oder Dateien überschreiben, in denen diese Daten gespeichert sind.

Auditprotokollierung

Administratoren können die Auditprotokolle nutzen, die NetWitness Suite mithilfe der Funktion „Globale Auditprotokollierung“ erstellt. Die Funktion zur Auditprotokollierung erzeugt Auditprotokolleinträge zu vielen Aktivitäten. Im Folgenden finden Sie Beispiele für Protokolleinträge, die für den Datenschutz relevant sind:

- Änderungen an Berechtigungen und an den einer Rolle zugewiesenen Benutzern
- Fehlgeschlagene und erfolgreiche An- und Abmeldeversuche bei NetWitness Suite
- Datenlöschungen
- Exporte und Downloads von Daten

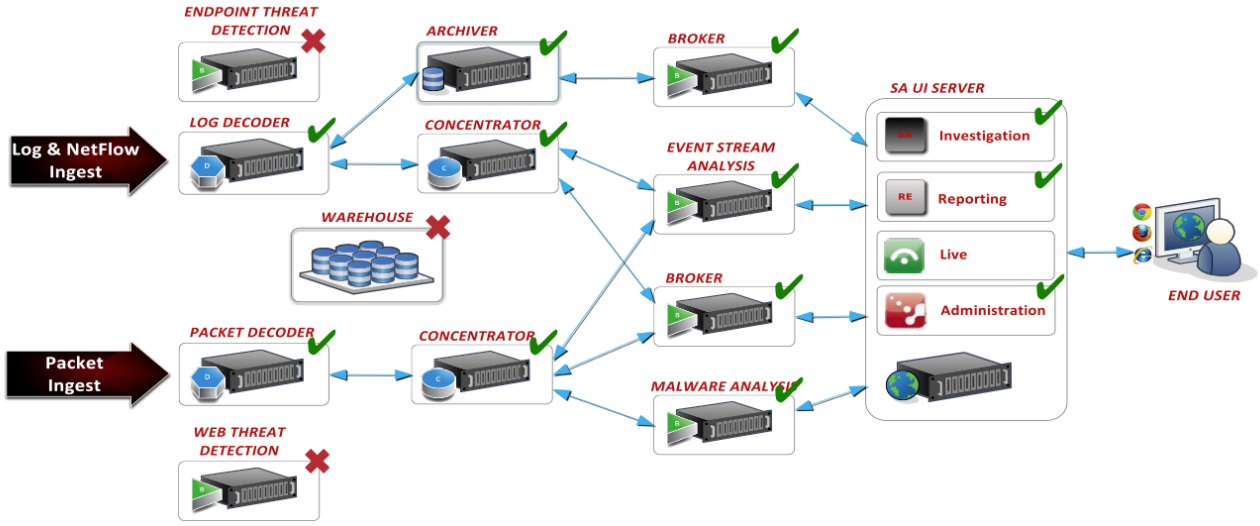
- Navigation von Benutzern zu Benutzeroberflächen und Abfragen, die die Benutzer durchgeführt haben
- Versuche (erfolgreich oder fehlgeschlagen) datenschutzrelevante Daten anzuzeigen oder zu ändern, einschließlich der Identifikation des Benutzers, der diesen Versuch unternommen hat

Alle Auditprotokolleinträge sind Bestandteil des standardmäßigen Überwachungspfads für NetWitness Suite. Die Administratoren können NetWitness Suite so konfigurieren, dass Auditprotokolle an ein festgelegtes Ziel weitergeleitet werden, z. B. auch an Drittanbietersysteme, die zusätzliche Filter- und Berichterstellungsfunktionen bieten. Weitere Informationen über die globale Auditprotokollierung erhalten Sie unter **Konfigurieren der globalen Auditprotokollierung** im Leitfaden *Systemkonfiguration*.

Durch die Datenschutzfunktion abgedeckte Komponenten

In der folgenden Abbildung sind die NetWitness Suite-Komponenten, die durch die Datenschutzfunktion der Version 10.5 oder höher abgedeckt werden, mit einem grünen Häkchen gekennzeichnet. Mit einem X markierte Komponenten werden von den Datenschutzfunktionen nicht unterstützt. Der *Leitfaden für die ersten Schritte mit NetWitness Suite* enthält eine funktionale Beschreibung der NetWitness Suite-Komponenten.

Hinweis: Die NetWitness Suite-Datenschutzfunktionen werden für Warehouse nicht unterstützt und geschützte Metadaten können über Warehouse Connector in Warehouse gelangen. Dies kann nur durch explizites Konfigurieren der Warehouse Connector-Metadatenfilter für das Herausfiltern dieser Daten verhindert werden. Wenn geschützte Metadaten in Warehouse gelangen, können Benutzer mit direkten Zugriff auf Warehouse diese Daten abfragen. Dies muss von den Datenschutzbeauftragten durch administrative, technische und verfahrensgestützte Kontrollen außerhalb von NetWitness Suite verhindert werden.



Implementierung der Datenschutzfunktionen nach Komponente

In der folgenden Tabelle ist für jede NetWitness Suite-Komponente angegeben, welche Datenschutzfunktionen unterstützt werden. Bei jeder Komponente wird durch ein Häkchen angegeben, ob diese Datenverschleierung, Steuerung der Datenaufbewahrung, Überschreiben von Daten sowie Auditprotokollierung unterstützt.

Komponente	Datenverschleierung	Steuerung der Datenaufbewahrung	Überschreiben von Daten	Auditprotokollierung
Datenaufnahme				
Decoder	√	√	√	√
Log Decoder	√	√	√	√
Metaaggregation				
Concentrator	√	√	√	√
Broker	-	√ (nur im DPO-Cache gespeichert)[1]		√
Echtzeitanalyse				
Investigation	√	√ (nur im DPO-Cache gespeichert)[2]		√
Event Stream Analysis	√			√
Malware Analysis	√	√		√

Komponente	Datenverschleierung	Steuerung der Datenaufbewahrung	Überschreiben von Daten	Auditprotokollierung
Reagieren	√	√		√
Reporting				
Reporting Engine	√	√		√
Langfristige Analysen				
Archiver	√	√	√ (unkomprimiert)[3]	√
Warehouse				

Hinweis:
1. Broker können Dateien zwischenspeichern. Hier muss eine Löschung durch Konfiguration eines individuellen Rollover und anderer Entfernungsmaßnahmen aus dem Cache erfolgen. Der Administrator kann den Cache-Rollover für einen Broker mithilfe des Planers auf der Registerkarte „Dateien“ in der Ansicht „Services-Konfiguration“ konfigurieren.
2. Investigation und der NetWitness-Server speichern Daten im Cache. Diese werden automatisch alle 24 Stunden gelöscht.
3. Der in Konfigurieren der Datenaufbewahrung beschriebene Vorgang des Überschreibens gilt für nicht komprimierte Daten.

Komponentenspezifische Konfigurations-Guidelines

DieNetWitness Suite-Komponenten und -Module, die Zugriff auf datenschutzrelevante Metadaten und deren verschleierte Gegenstücke haben, sind Investigation, Event Stream Analysis (ESA), Malware Analysis, Respond und Berichte. Sie erhalten Zugriff auf Daten basierend auf den der Rolle des Benutzers zugewiesenen Berechtigungen. Der Administrator oder Datenschutzbeauftragte konfiguriert jeden Decoder oder Log Decoder zur Identifizierung der Metaschlüssel, die zur Verschleierung markiert sind.

Für diese Komponenten existieren zusätzliche Guidelines, um zu erreichen, dass sie in Kombination mit einem Datenschutzschema wie erwartet funktionieren:

- **Event Stream Analysis**. Wenn ESA datenschutzrelevante Daten von NetWitness Suite Core empfängt, gibt ESA nur die verschleierte Version der Daten weiter. ESA speichert keine geschützten Daten noch zeigt es sie an. Es gibt einige zusätzliche Leitlinien für die Konfiguration erweiterter EPL-Regeln und Erweiterungsquellen (beschrieben im Thema **Sensible Daten** im Handbuch *Versenden von Warnmeldungen mit ESA*). Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.
- **Malware Analysis**. Malware Analysis referenziert während der Bewertung bestimmte Metaschlüssel, einschließlich `alias.host`, `client` und andere. Damit keine analytischen Funktionen verloren gehen, sollte Malware Analysis als vertrauenswürdiger Client so konfiguriert werden, dass die Verbindung zur Core-Infrastruktur der NetWitness Suite mit einem Konto hergestellt wird, das einem Benutzer mit DPO-Rolle entspricht. Andernfalls können manche Indikatoren für eine Infizierung (Indicators of Compromise, IOCs) unwirksam werden, wenn von Malware Analysis referenzierte Metaschlüssel zur Verschleierung markiert werden und Malware Analysis nicht darauf zugreifen kann.
- **Antwortserver-Dienst.** Antwortserver-Dienst verwendet eine Datenschutz-Zuordnungsdatei zur Anzeige verschleierter Daten in Warnmeldungen (siehe das Thema **Verschleiern von privaten Daten** im *Benutzerhandbuch zu Respond*) und bietet einen konfigurierbaren Datenaufbewahrungszeitraum für Warnmeldungen (siehe das Thema **Festlegen einer Aufbewahrungsfrist für Warnmeldungen und Incidents** im *Benutzerhandbuch zu Respond*). Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.
- **Reports.** In Reporting Engine wird jeder Core-Service mithilfe der beiden separaten Servicekonten als zwei separate Datenquellen hinzugefügt. Eine Datenquelle hat ein Servicekonto mit DPO-Rolle, die andere Datenquelle ein Servicekonto mit einer Nicht-DPO-Rolle. Das Thema **Konfigurieren des Datenschutzes für die Reporting Engine** im *Konfigurationsleitfaden Reporting Engine* enthält Verfahren zum Konfigurieren des Datenschutzes für die Reporting Engine. Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

Empfohlene Konfigurationen

In diesem Thema wird die empfohlene Datenschutzimplementierung für NetWitness Suite beschrieben und es werden mehrere zusätzliche Anwendungsbeispiele für den Umgang mit datenschutzrelevanten Daten in NetWitness Suite bereitgestellt. Administratoren können die NetWitness Suite-Hosts und -Services so einrichten, dass die Datenschutzanforderungen für ihre Umgebung erfüllt werden. RSA verfügt über empfohlene Konfigurationen für Datenschutz und Datenaufbewahrung.

Empfohlene Datenschutzkonfiguration

Die empfohlene Konfiguration zum Erzielen des besten analytischen Werts bei aktivierter Datenverschleierung ist die Definition datenschutzrelevanter Metadaten und die Aufbewahrung sowohl der ursprünglichen als auch der verschleierten (Hash-)Werte datenschutzrelevanter Daten auf der Festplatte für Decoders, Log Decoders, Concentrators und Brokers.

Es wird davon ausgegangen, dass nur eine Handvoll Metadaten (d. h. ungefähr 10 Metaschlüssel) als geschützt zu klassifizieren sind. Ein FIPS 140-kompatibler Hashalgorithmus in Kombination mit einem Salt erschwert das Reverse Engineering des Originalwerts. Die empfohlene Lösung ist SHA-256 mit einem mindesten 16 und maximal 60 Zeichen langen Salt.

Hinweis: Die Hashwerte werden standardmäßig im Binärformat gespeichert, da dies schnellere Antwortzeiten ermöglicht und weniger Speicherplatz in der Datenbank erfordert als das Speichern im Zeichenfolgenformat. Die empfohlene Speichermethode ist als Text/Zeichenfolge.

Brokers und Investigation können verschleierte und Originaldaten im Cache enthalten, wenn Datenschutzbeauftragte bei Ermittlungen Investigation verwenden, um den Originalwert zu überprüfen, auf den der verschleierte Wert verweist. Downstreamservices können auch die Verwendung der sensiblen Originalwerte für die Verarbeitung im Speicher beschränken, sodass Daten in diesen Downstreamsystemen nicht dauerhaft auf der Festplatte abgelegt werden. Dies gilt für ESA und Malware Analysis.

Die empfohlene Lösung zum Löschen der Daten, wenn diese nicht mehr benötigt werden, ist die integrierte und automatische Datenaufbewahrungssteuerung, die die Daten bei Erreichen eines bestimmten Schwellenwertes löscht. Sie können diese Methode für die folgenden Komponenten in NetWitness Suite 10.5 verwenden: Decoder, Log Decoder, Log Collector, Archiver, Malware Analysis, Incident Management und Reporting Engine. Sie können Event Stream Analysis manuell für die Unterstützung einer ähnlichen automatischen Datenaufbewahrungssteuerung konfigurieren.

Zum Managen des Cachespeichers löscht der NetWitness-Server den für die Ereignisermittlung verwendeten Cache alle 24 Stunden. Der Broker kann auch so konfiguriert werden, dass der lokal gespeicherte Cache regelmäßig gelöscht wird.

Optionen für die Konfiguration der Datenaufbewahrung

NetWitness Suite stellt alternative Steuerungsmöglichkeiten bereit, die der Administrator anwenden kann, um bei aktivierter Datenverschleierung stärkere Beschränkungen für die Speicherung datenschutzrelevanter Daten durchzusetzen.

Datenspeicher mit aktivierten Datenaufbewahrungsoptionen

In der folgenden Tabelle ist der Speicherort der Daten für die Standardkonfiguration ohne Datenschutz sowie für jede optionale Datenaufbewahrungsalternative aufgeführt. Ein Häkchen zeigt an, dass datenschutzrelevante Daten auf der Komponente gespeichert werden. Ein X bedeutet, dass keine datenschutzrelevanten Daten auf der Komponente gespeichert werden.

Komponente	Standardkonfiguration	Datenspeicheroptionen		
	Originaldaten gespeichert	Originaldaten und Hash gespeichert (empfohlen)	Nur Hash gespeichert	Keine Daten gespeichert (alle Metadaten sind vorübergehend)
Datenaufnahme				
Dekodieren	√	√	X	X
Log Decoder	√	√	X	X
Metaaggregation				

Komponente	Standardkonfiguration	Datenspeicheroptionen		
	Originaldaten gespeichert	Originaldaten und Hash gespeichert (empfohlen)	Nur Hash gespeichert	Keine Daten gespeichert (alle Metadaten sind vorübergehend)
Concentrator	√	√	X	X
Broker	√ (nur Cache)	√ (nur Cache)	X	X
Echtzeitanalyse				
Investigation	√	√ (nur Cache)	X	X
Event Stream Analysis	√	X	X	X
Malware Analysis	√	X	X	X
Antwortserver-Dienst	√	X	X	X
Reporting				
Reporting Engine	√	√ (Optional)	X	X

Komponente	Standardkonfiguration	Datenspeicheroptionen		
	Originaldaten gespeichert	Originaldaten und Hash gespeichert (empfohlen)	Nur Hash gespeichert	Keine Daten gespeichert (alle Metadaten sind vorübergehend)
Langfristige Analysen				
Archiver	√ (Optional)	√ (Optional)	X	X
Warehouse	√ (Optional)	√ (Optional)	X	X
Inhalt				
Live	-	-	-	-
Betrugsanalyse				
RSA Fraud and Risk Intelligence Suite	-	-	-	-
Endpunktschutz				
NetWitness Endpoint	-	-	-	-

Komponente	Standardkonfiguration	Datenspeicheroptionen		
	Originaldaten gespeichert	Originaldaten und Hash gespeichert (empfohlen)	Nur Hash gespeichert	Keine Daten gespeichert (alle Metadaten sind vorübergehend)

Hinweis:
„Nur Cache“ bedeutet, dass sensible Daten im Cache des Brokers oder des NetWitness-Server-Servers gespeichert werden. Einzelheiten zur automatisierten und manuellen Löschung des Caches finden Sie unter Konfigurieren der Datenaufbewahrung.

„Optional“ bedeutet, dass sensible Daten gespeichert werden, dies jedoch durch optionale Konfigurationen eingeschränkt werden kann. Beispiel: Um zu beschränken, wo sensible Daten gespeichert werden, aktivieren Sie nicht den DPO-Zugriff für Reporting und aggregieren Sie die geschützten Originaldaten nicht in den Archiver.

Option 1: Keine Originaldaten auf Datenträger gespeichert, nur Hash gespeichert

Administratoren können die dauerhafte Aufbewahrung sensibler Daten auf dem Datenträger eliminieren und nur verschleierte Daten speichern, wenn die Gefährdung zu groß ist. In diesem Szenario werden Metadaten, die während des Parsings auf den Decoders und Log Decoders erzeugt wurden, nur im Arbeitsspeicher verwendet und nicht auf die Festplatte geschrieben. Administratoren können einzelne Metaschlüssel auf einem Decoder oder Log Decoder als vorübergehend konfigurieren, um sicherzustellen, dass sensible Metadaten nicht auf die Festplatte geschrieben werden. Downstreamservices erkennen keine Originalwerte und müssen verschleierte Werte verwenden, um Ermittlungen und Analysen durchzuführen.

Zur Konfiguration dieses Datenschutzschemas muss Datenverschleierung mit konfigurierten Hash-Werten aktiviert sein. Sie können einzelne Metaschlüssel auf einem Decoder oder Log Decoder als vorübergehend konfigurieren, um sicherzustellen, dass Originalwerte nicht auf die Festplatte geschrieben werden.

- Die als sensibel identifizierten Originalwerte werden während des Parsings auf dem Decoder und Log Decoder aus den Rohdaten extrahiert und sind während des Parsings für das System zugänglich (Parser, Regeln, Feeds).
- Der Decoder speichert nicht die Originalwerte für Metaschlüssel, die als sensibel identifiziert wurden, sondern nur den Hash von Originalwerten zusammen mit anderen nicht sensiblen Metadaten, die mit dem Ereignis verknüpft sind.

Eine Nebenwirkung dieser Optionen ist ein gewisser Verlust an analytischen Fähigkeiten, aber Sie können diese so konfigurieren, dass sie den Anforderungen Ihrer Umgebung entsprechen.

- Indem Sie alle sensiblen Daten als vorübergehend konfigurieren, werden sensible Werte nicht dauerhaft auf dem Datenträger gespeichert und die analytischen Fähigkeiten bei Verwendung der Originalwerte sind nur zum Zeitpunkt des Parsings verfügbar (Parser, Regeln, Feeds).
- Event Stream Analysis (ESA)- und Malware Analysis-Systeme können sich nur auf die verschleierten Metawerte verlassen, wenn sie ihre Korrelation bzw. ihre Bewertung durchführen.
- Reporting Engine ist darauf beschränkt, Berichte mithilfe der nicht sensiblen und verschleierten Daten zu erstellen.
- Der Datenschutzbeauftragte kann den Originalwert nicht sehen, aber er kann den konfigurierten Hash und Salt verwenden, um festzulegen, ob ein verschleierter Wert einen bestimmten bekannten Originalwert repräsentiert.

Option 2: Keine Originalwerte oder verschleierten Werte gespeichert: nicht empfohlen

Administratoren können vollständig verhindern, dass der Originalwert dauerhaft auf dem Datenträger gespeichert wird, wenn die Gefährdung zu groß ist. Wie in Option 1 werden in diesem Szenario Metadaten, die während des Parsings auf den Decoders und Log Decoders erzeugt wurden, nur im Arbeitsspeicher verwendet und nicht auf die Festplatte geschrieben. Administratoren können einzelne Metaschlüssel auf einem Decoder oder Log Decoder als vorübergehend konfigurieren, um sicherzustellen, dass sensible Metadaten nicht auf die Festplatte geschrieben werden. Downstreamservices sehen keine Originalwerte und haben keine verschleierten Werte, um Ermittlungen und Analysen durchzuführen.

Konfigurieren Sie für dieses Datenschutzschema einzelne Metaschlüssel auf einem Decoder oder Log Decoder als vorübergehend, um sicherzustellen, dass Originalwerte nicht auf den Datenträger geschrieben werden.

- Die als sensibel identifizierten Originalwerte werden während des Parsings auf dem Decoder und Log Decoder aus den Rohdaten extrahiert und sind während des Parsings für das System zugänglich (Parser, Regeln, Feeds).
- Der Decoder speichert nicht die Originalwerte für Metaschlüssel, die als sensibel identifiziert wurden, sondern nur die nicht sensiblen Metadaten, die mit dem Ereignis verknüpft sind.

Eine Nebenwirkung dieser Optionen ist ein signifikanter Verlust an analytischen Fähigkeiten, aber Sie können diese so konfigurieren, dass sie den Anforderungen Ihrer Umgebung entsprechen.

- Indem Sie alle sensiblen Daten als vorübergehend konfigurieren, werden sensible Werte nicht dauerhaft auf dem Datenträger gespeichert und die analytischen Fähigkeiten bei Verwendung der Originalwerte sind nur zum Zeitpunkt des Parsings verfügbar (Parser, Regeln, Feeds). Siehe Konfigurieren der Datenaufbewahrung.
- Alle Downstreamkomponenten haben keine Einsicht in die Originalwerte, unabhängig davon, ob sie verschleiert sind oder nicht.
- Der Datenschutzbeauftragte hat keine Einsicht in den Originalwert, ob verschleiert oder nicht.

Optionale Optionen zum Überschreiben von Daten

Zum Überschreiben von Daten stehen verschiedene Optionen zur Verfügung. Sie sollten jede einzelne davon gründlich verstehen, bevor Sie das Überschreiben von Daten implementieren.

Option 1: Festplattenplatz für kontinuierliches Überschreiben älterer Daten beschränken

Wenn die gewünschte Frist zur Aufbewahrung der Daten und damit auch der für diese Daten erforderliche Speicherplatz bekannt sind, kann die Größe der zugrundeliegenden Hardware oder der Partition auf diese Größe beschränkt werden. Indem der Festplattenspeicher oder die Partitionsgröße reduziert wird, wird der verfügbare freie Speicherplatz, der gefüllt werden muss, bevor er durch neue Daten überschrieben wird, ebenfalls beschränkt. Die neu aufgenommenen Daten überschreiben kontinuierlich die älteren Daten. Jede der Lösungen muss zur Bereitstellungszeit erfolgen, um wirksam zu sein.

Nebenwirkungen dieser Option sind:

- Die Entnahme einiger Festplatten beschränkt die Anzahl der für die Verteilung der I/O verfügbaren Ressourcen, was zu Performanceeinbußen führt.
- Die kleinere Partitionsgröße kann zu Performanceeinbußen führen, würde aber die Auswirkungen auf die Performance durch die Entnahme von Festplatten mildern.

Option 2: Tiered Storage zum Überschreiben von Daten nach Plan verwenden

Wenn das Überschreiben von Daten automatisch nach Plan erforderlich ist, können Sie die Decoders und Concentrators konfigurieren, um Tiered Storage zu verwenden. Die Tiered-Storage-Konfiguration bietet einen Mechanismus für das Aufrufen eines Skripts, nachdem eine Datenbankdatei aus der Anwendung gelöscht wurde, aber bevor sie aus dem Dateisystem gelöscht wurde. Anstatt die Datei in den zweiten Tier, oder Cold-Speicher, zu verschieben, (die intendierte Funktion in einem Tiered-Storage-Anwendungsbeispiel), kann das Skript nötigenfalls ein Dienstprogramm wie `shred` von CentOS verwenden, um die Datei zu überschreiben. Dieses Tool ist weniger effektiv, wenn die Datenbank in einem Protokollierungsdateisystem wie XFS, in dem sich die Core-Datenbank befindet, und auf einem logischen RAID-Laufwerk gespeichert wird, mit dem z. B. die Core-Hosts eine Verbindung herstellen.

Die meisten anderen NetWitness Suite-Komponenten haben diese Option nicht. Ihre Daten werden in einer Datenbank gespeichert, die den Tiered-Storage-Mechanismus nicht unterstützt. Die einzige andere Komponente, die diese Überschreibungsmethode verwenden könnte, ist die Reporting Engine, da sie Berichte und Warnmeldungen als einzelne Dateien speichert. Allerdings werden die Reporting Engine-Diagramme in einer Datenbank gespeichert, daher wären sie gegenüber dieser Technik immun.

Option 3: Daten bereinigen mithilfe optionaler Bearbeitung von Zeichenfolgen und Mustern

Datenbereinigung bietet einen Mechanismus für das strategische Überschreiben einer bestimmten Teilmenge von Daten vom System, falls sensible Daten entweder absichtlich oder zufällig dauerhaft abgelegt wurden. Mit dem NetWitness Suite `wipe`-Dienstprogramm können die Daten in den Meta- und Paketdatenbanken für Core-Services, die RAW-Pakete oder Protokolle für bestehende Sitzungen enthalten können, basierend auf einer Sitzungskennung mit eindeutigen Mustern überschrieben werden. Alle Core-Komponenten haben die Möglichkeit, eine Teilmenge von Daten zu überschreiben, die mithilfe einer Abfragezeichenfolge, einschließlich regex-Mustern, gefunden wurde. Die Sitzungskennungen, die sich aus der Abfrage ergeben, werden in das NetWitness Suite-Dienstprogramm „wipe“ eingespeist.

Hinweis: Diese Option ist nicht verfügbar, wenn die Daten in der Core-Datenbank komprimiert wurden (wie es typischerweise in Archiver-Bereitstellungen geschieht).

In den meisten NetWitness Suite-Komponenten bietet die verwendete Datenbank keinen integrierten Redaktions- oder sicheren Löschmechanismus. Die Malware Analysis-Komponente kann das Datenobjekt in der Datenbank mit dem Wert `private` überschreiben, anstatt es während des Prozesses zum Management der Datenaufbewahrung zu löschen, aber dies gilt nicht als sicherer Löschmechanismus.

Achtung: Die Anwendung dieser Methode für eine große Anzahl von Sitzungen hat zwei Nachteile: Sie kann sehr viel Zeit kosten und sich auf die Performance auswirken.

Einschränkungen für das Überschreiben von Daten

Für die als Option 2 und 3 beschriebenen Überschreibungstechniken gelten gewisse Einschränkungen. Zum Überschreiben der Daten in den Festplattensektoren werden bei den obigen Optionen für das Überschreiben und dem als alternative Methode angegebenen Befehlszeilentool für das Überschreiben (`shred`, eine Funktion von CentOS) bestimmte Annahmen zum Festplattenlayout vorausgesetzt. NetWitness Suite-Hosts verwenden aus Gründen der Performance und Zuverlässigkeit SSD-Laufwerke und RAID-Konfigurationen und diese behindern die Funktion der Überschreibungstechniken. Wenn Überschreibungstechniken SSD-Laufwerke und RAID-Konfigurationen ändern, um die Sicherheit zu erhöhen, gehen damit unvermeidlicherweise Performanceeinbußen einher, die sich in den Aufnahmeraten, Abfragegeschwindigkeiten und möglicherweise auch anderen Bereichen bemerkbar machen. Es wird empfohlen, die für das Überschreiben verfügbaren Befehlszeilentools nur in speziellen Fällen zu verwenden, wenn es erforderlich ist, bestimmte Daten zu entfernen. Die Tools eignen sich wegen der potentiellen Performanceeinbußen nicht zur Verwendung in einer kontinuierlichen Echtzeitmethode.

Schnellstartverfahren

In diesem Abschnitt finden Sie eine umfassende Anleitung zur Vorbereitung auf die Konfiguration der Datenschutzfunktionen und zur anschließenden Durchführung der Konfiguration für die empfohlene Datenschutzlösung.

- Vorbereiten der Datenschutzkonfiguration
- Konfigurieren der empfohlenen Datenschutzlösung

Vorbereiten der Datenschutzkonfiguration

Dieses Thema enthält allgemeine Guidelines für die Planung und Konfiguration der Datenschutzrichtlinien im NetWitness Suite-Netzwerk. Bevor Sie mit der Konfiguration beginnen, müssen Sie wissen, welche Daten in Ihrem Netzwerk geschützt werden müssen, und eine Planung durchführen. Sie müssen folgendes tun:

1. Identifizieren Sie die Metaschlüssel, die datenschutzrelevante Daten enthalten und geschützt werden müssen. Diese Entscheidung basiert auf den spezifischen Anforderungen an Ihren Standort.
2. Entscheiden Sie, welche Benutzer Zugriff auf die datenschutzrelevanten Metadaten- und Rohdateninhalte haben sollen. Als Erstes ist zu entscheiden, ob die Rollen des Datenschutzbeauftragten und des Administrators für Ihren Standort voneinander getrennt werden sollen, indem eine benutzerdefinierte Systemrolle für Administratoren auf Decoders und Log Decoders konfiguriert und die Berechtigung `dpo.manage` entfernt wird. Standardmäßig haben Administratoren alle Berechtigungen einschließlich der Fähigkeit zum Konfigurieren der Umwandlung zu Hash mit Salt bei der Datenverschleierung. Bei einigen Standorte ist möglicherweise die Beschränkung dieses Zugriffs auf Data Privacy Officer gewünscht. Weitere Einzelheiten zu den genauen Berechtigungen jeder Rolle und dem Zweck dieser Berechtigungen finden Sie unter **Servicebenutzerrollen und -berechtigungen** im *Leitfaden für die ersten Schritte mit Hosts und Services*.
3. Planen Sie die zur Unterstützung eines angemessenen Datenschutzes in Ihrer NetWitness Suite-Bereitstellung erforderlichen Konfigurationsänderungen.
4. Bewerten Sie, welche Auswirkungen Ihre Konfiguration auf vordefinierte und angepasste Inhalte haben kann. Beispiel: Standardmäßig sind über Live verfügbare Inhalte für Reporting Engine nicht für verschleierte Metawerte ausgelegt.

In einer Bereitstellung müssen bestimmte Datenschutzkonfigurationen in den Core-Services identisch sein. In der folgenden Tabelle sind diese Einstellungen aufgeführt. Services, deren Einstellungen identisch sein müssen, sind mit einem Häkchen markiert.

	Identisch konfigurieren für:				
Datenschutzeinstellungen	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**
Hashalgorithmus und Salt für datenschutzrelevante Daten	√	√			
Datenschutzattribute von Sprachschlüsseln in der benutzerdefinierten Indexdatei (einschließlich Konfigurieren der Schlüssel als geschützt)	√	√	√	√	√
Vorübergehende Metaschlüssel (nicht persistent auf Festplatte) pro Service und Parser	√	√			
Sichtbarkeit von Metadaten- und Rohdateninhalten pro Systembenutzergruppe (Die Metaschlüssel müssen in der benutzerdefinierten Indexdatei vorhanden sein.)	√	√	√	√	√
Benutzer mit zugewiesener Servicebenutzerrolle `Aggregation` wird hinzugefügt.*	√	√	√		

	Identisch konfigurieren für:				
Datenschutzeinstellungen	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**

* Für den Zugriff auf Daten auf einem Aggregationsservice erfordert der Log Collector oder Broker eine Authentifizierung. Wenn Sie aufgefordert werden, den Benutzernamen und das Passwort einzugeben, müssen Sie sich als Benutzer mit zugewiesener Servicerolle `Aggregation` authentifizieren. Das Thema **Aggregationsrolle** im *Leitfaden für die ersten Schritte mit Hosts und Services*enthält detaillierte Informationen über diese Rolle. Befolgen Sie die Anweisungen im Thema **Hinzufügen, Replizieren oder Löschen eines Servicebenutzers** im *Leitfaden für die ersten Schritte mit Hosts und Services*, um einen Benutzer zu erstellen und dem neuen Benutzer die Servicebenutzerrolle „Aggregation“ zuzuweisen.

Konfigurieren der empfohlenen Datenschutzlösung

Dieses Thema erklärt Administratoren und Datenschutzbeauftragten, wie sie die empfohlene Datenschutzlösung in einem NetWitness Suite-Netzwerk konfigurieren können. Dies sind die grundlegenden Schritte, um das NetWitness Suite-System so zu konfigurieren, dass es sensible Daten erkennt, und um festzulegen, welche Person diese Daten einsehen kann. Die empfohlene Konfiguration erzeugt verschleierte Werte von bestimmten ursprünglichen Metaschlüsseln und bewahrt sowohl ursprüngliche als auch verschleierte Daten so auf, dass sie für Benutzer verfügbar sind, denen privilegierter Rollenzugriff zugewiesen wurde.

Diese Konfiguration hat mehrere Teile:

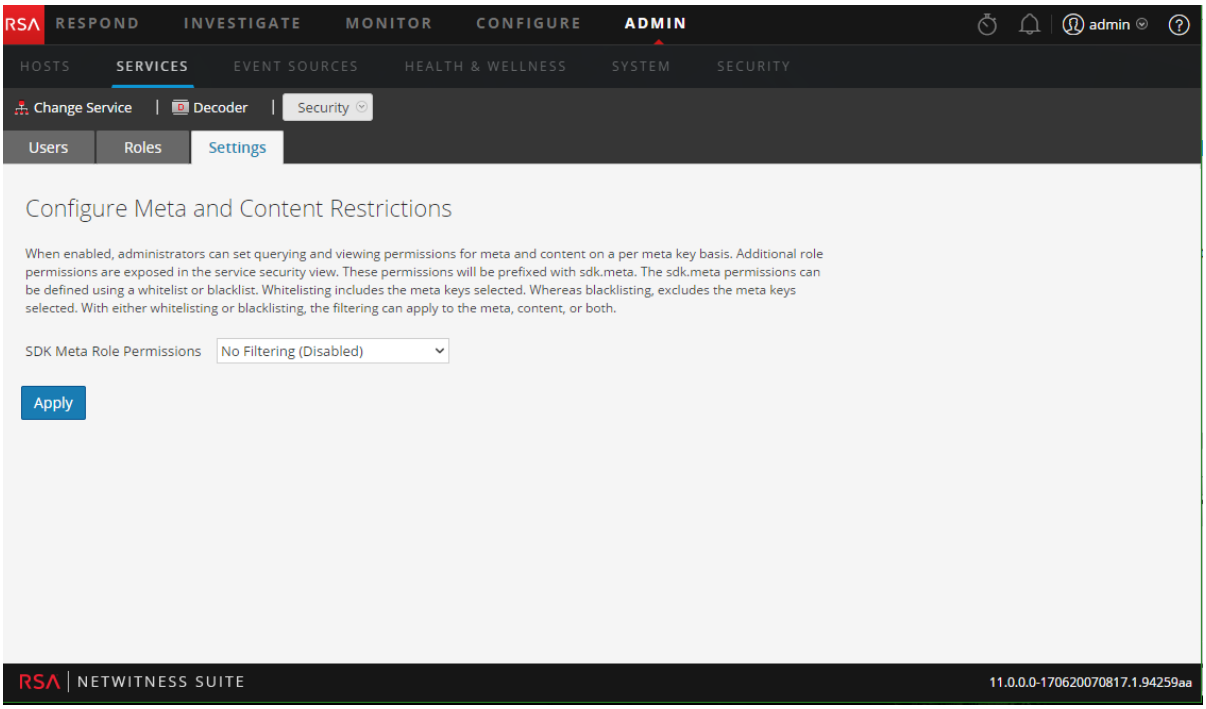
1. Erstellen Sie zunächst zwei Benutzer mit verschiedenen Berechtigungsniveaus. Ein Benutzer (der Datenschutzbeauftragte) kann alle Metadaten sehen und ein anderer Benutzer (ein Analyst) darf bestimmte Metadaten und Inhalte mit zugehörigen Metadaten nicht sehen.
2. Richten Sie mithilfe eines Salts und eines Hashs zwei Transformationen ein, um eine verborgene Version der ursprünglichen Metaschlüssel `username` und `ip.src` zu erstellen.
3. Konfigurieren von Datenaufbewahrung auf den Services Decoder und Concentrator

Hinweis: Die folgenden Bedingungen sind erforderlich, um dieses Verfahren abzuschließen:
- Concentrator und Decoder müssen dem NetWitness-Server-Server über vertrauenswürdige Verbindungen hinzugefügt werden.
- Es muss NW-Server Version 10.5 oder höher verwendet werden.
- Die Core-Services müssen Version 10.5 oder höher aufweisen.
- Die Aggregation muss auf allen Core-Services Aggregatorenkonten verwenden.

Konfigurieren von Metadaten- und Inhaltsbeschränkungen für Brokers, Concentrators und Decoders

Wenn Sie die Metadaten und Rohinhalte beschränken möchten, die Benutzer sehen können, müssen Sie SDK-Systemrollen aktivieren, um feiner abgestimmte Steuerungen zu erlauben, indem Sie Beschränkungen für Metadaten und Content auf jedem Service in der Ansicht „Services-Sicherheit“ konfigurieren.

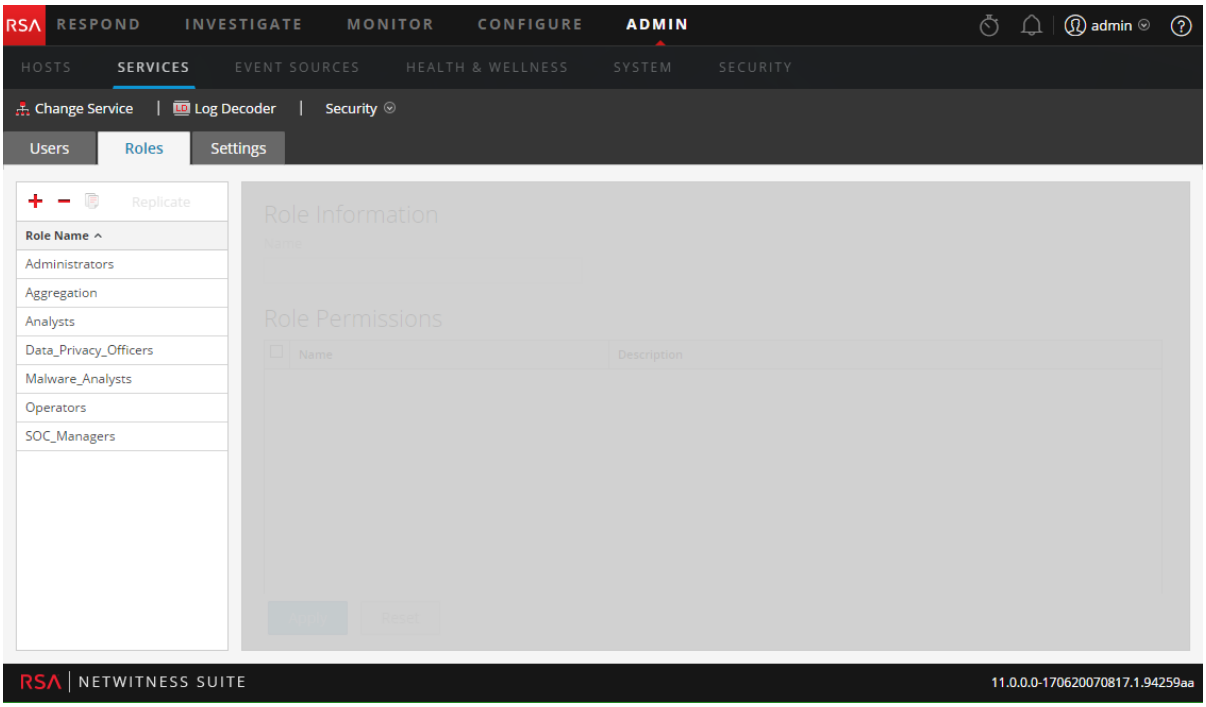
1. Wählen Sie in der Ansicht **Admin-Services** einen Service aus und klicken Sie dann auf  **> Ansicht > Sicherheit**.
2. Klicken Sie auf die Registerkarte **Einstellungen**.



3. Wählen Sie im Feld **SDK-Meta-Rollenberechtigungen** die Option **Metadaten und Content in der schwarzen Liste** aus. Klicken Sie auf **Anwenden**.

   Dies erlaubt es dem Administrator, individuelle Metaschlüssel einer schwarzen Liste hinzuzufügen, sodass nur der Datenschutzbeauftragte die Metaschlüssel und den Content sehen kann. Neue Rollen werden pro Metaschlüssel der Registerkarte Rollen hinzugefügt.

4. Klicken Sie auf die Registerkarte **Rollen**.



5. Auf der Registerkarte „Rollen“:

   a. Wählen Sie die Metaschlüssel aus, die sie vor Analysten verbergen möchten. Wählen Sie zum Beispiel `sdk.meta.username` und `sdk.meta.ip.src` aus.

      Dadurch können Analysten die datenschutzrelevanten Metaschlüssel `username` und `ip.src` nicht sehen, ebenso wenig wie jeglichen Content für jegliche Sitzung, in der diese Metaschlüssel enthalten sind.

   b. Heben Sie die Auswahl von `sdk.packet` auf. Dadurch können Analysten nicht länger Rohpakete und Protokolle massenweise exportieren.

   c. Klicken Sie auf **Anwenden**.

6. Vergewissern Sie sich, dass für die Rolle `Data_Privacy_Officers` auf der Registerkarte „Rollen“ der Wert „sdk.meta.values“ nicht ausgewählt ist. Klicken Sie auf **Anwenden**.

   Ein DPO kann alle Metadaten und alle Sitzungen anzeigen.

   Vergewissern Sie sich, dass für die Rolle `Aggregation` auf der Registerkarte „Rollen“ folgende Berechtigungen festgelegt sind: Wählen Sie `aggregate`, `sdk.content`, `sdk.meta` und `sdk.packets.` aus

Hinzufügen von Konten für Datenschutzbeauftragte und Analysten auf dem NetWitness-Server

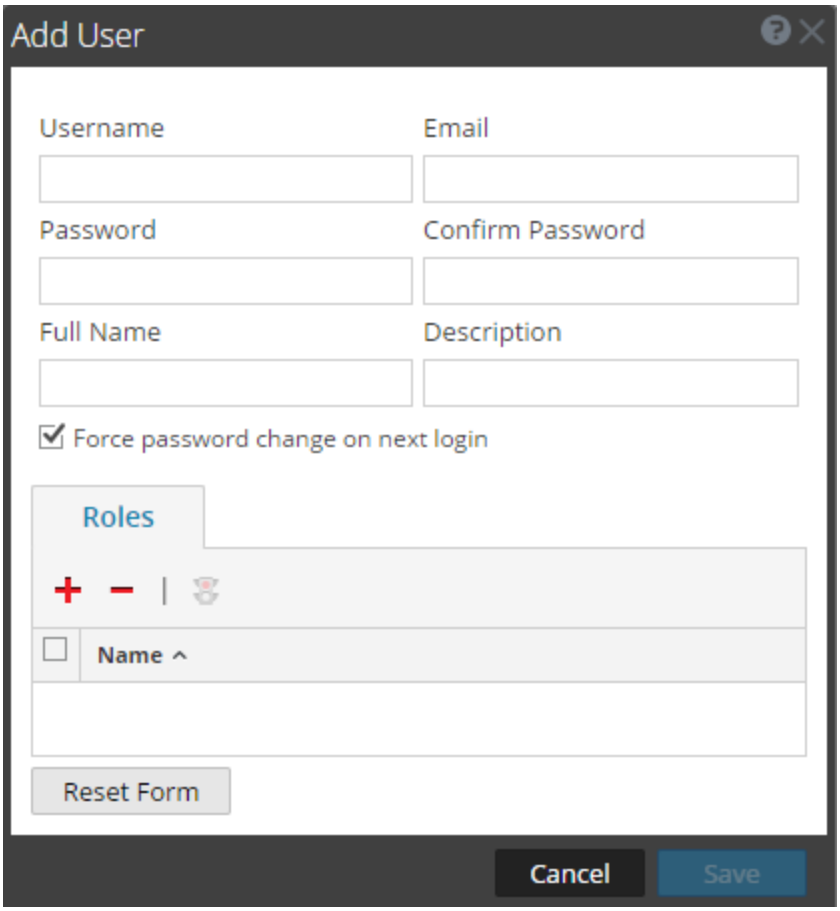
Sie müssen in NetWitness Suite zwei neue Benutzerkonten auf Systemebene hinzufügen, um einen berechtigten Datenschutzbeauftragten und einen typischen Analysten abzubilden. Wenn die Umgebung mit den vertrauenswürdigen Standardverbindungen konfiguriert wurde, müssen Sie in den Core-Services (Broker, Concentrator und Decoder) keine neuen Benutzerkonten erstellen. Wenn ein Benutzer auf dem NetWitness-Server-Server erstellt wird, kann sich dieser bei den Services anmelden.

Hinweis: Der Rollenname muss sowohl auf dem Server als auch auf den Services existieren und er muss in beiden Fällen identisch sein. Wenn Sie eine neue benutzerdefinierte Rolle auf dem NetWitness-Server erstellen, achten Sie darauf, dass Sie diese auch allen Core-Services hinzufügen.

1. Erstellen Sie für den Datenschutzbeauftragten ein neues Benutzerkonto:

   a. Wählen Sie in der Ansicht **Services-Sicherheit** die Registerkarte **Benutzer** aus. Klicken Sie auf der Symbolleiste der Registerkarte **Benutzer** auf +.

      Das Dialogfeld „Benutzer hinzufügen“ wird angezeigt.



b. Erstellen Sie das neue Konto mit den folgenden Anmeldeinformationen.

   Benutzername = <neuer Benutzername für die Anmeldung, zum Beispiel „DPOadmin“>
   E-Mail = <E-Mail-Adresse des neuen Benutzers, zum Beispiel „DPOadmin@rsa.com“>
   Passwort = <Passwort des neuen Benutzers, zum Beispiel „RSAprivacy1!@“>
   Vollständiger Name = <vollständiger Name des neuen Benutzers, zum Beispiel „DPO-Administrator“>

c. Klicken Sie auf die Registerkarte „Rollen“, + und wählen Sie für den neuen Benutzer die Rolle `Data_Privacy_Officers` aus.

d. Klicken Sie auf **Speichern**.

2. Erstellen Sie ein neues Benutzerkonto für den Analysten mit eingeschränkten Berechtigungen:

   a. Wählen Sie in der Ansicht **Services-Sicherheit** die Registerkarte **Benutzer** aus. Klicken Sie auf der Symbolleiste der Registerkarte **Benutzer** auf +.

      Das Dialogfeld „Benutzer hinzufügen“ wird angezeigt.

   b. Erstellen Sie das neue Konto mit den folgenden Anmeldeinformationen:

Benutzername = <neuer Benutzername für die Anmeldung, zum Beispiel „NichtprivAnalyst“>
E-Mail = <E-Mail-Adresse des neuen Benutzers, zum Beispiel „NichtprivAnalyst@rsa.com“>
Passwort = <Passwort des neuen Benutzers, zum Beispiel „RSAprivacy2!@“>
Vollständiger Name = <vollständiger Name des neuen Benutzers, zum Beispiel „Nicht privilegierter Analyst“>

c. Klicken Sie auf die Registerkarte „Rollen“, + und wählen Sie für den neuen Benutzer die Rolle `Analysts` aus.

d. Klicken Sie auf **Speichern**.

Konfigurieren von verborgenen Daten auf Decodern und Concentratorn

Dieses Verfahren erstellt die verborgenen Werte zur Bereitstellung für Benutzer, die keinen Zugriff auf die ursprünglichen Werte haben.

1. Konfigurieren Sie einen Salt, sodass der verborgene Wert einzigartig wird. Verschiedene Unternehmen beschäftigen eventuell Analysten mit demselben Vornamen und möglicherweise demselben Benutzernamen zur Anmeldung. Die Verwendung eines Salt schränkt die Möglichkeit ein, dass jemand von außerhalb Ihrer Organisation Ihren Mechanismus zur Verschleierung ermittelt. In diesem Beispiel verwenden Sie einen einfachen Salt und SHA-256, aber der Salt ist konfigurierbar und der Hashalgorithmus kann geändert werden. Weitere Informationen finden Sie unter Konfigurieren der Datenverschleierung.

   a. Um Salt und den Hash-Algorithmus zu definieren, wählen Sie die Ansicht **ADMIN > Services** aus.

   b. Wählen Sie einen **Decoder** in der Ansicht **Admin-Services** aus und klicken Sie auf  > **Ansicht > Konfiguration**.

   c. Klicken Sie auf die Registerkarte **Datenschutz** und wählen Sie den Hashalgorithmus (SHA-256) aus. Geben Sie im Feld „Salt“ einen Hash ein, zum Beispiel **rsasecurity**, und klicken Sie auf **Anwenden**.

2. Definieren Sie die Transformationen, inklusive Hash-Format, zwischen dem ursprünglichen Metaschlüssel und dem verschleierten Metaschlüssel auf dem Decoder. Das Standardformat für Hashes ist binär, die empfohlene Konfiguration nutzt jedoch das Format Text/Zeichenfolge.

   a. Klicken Sie auf die Registerkarte **Dateien** und wählen Sie aus dem Drop-down-Menü **index-decoder-custom.xml** aus. (Sie können diese Konfiguration genauso auf den Log Decoder in der Datei „index-logdecoder-custom.xml“ anwenden.)

b. Geben Sie die folgenden Zeilen in den verfügbaren Eingabebereich ein:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key name="username" description="Username" format="Text"
protected="true"><transform
destination="username.hash"/></key>
<key name="username.hash" description="Username Hash"
format="Text"/>
<key name="ip.src" description="Source IP Address"
format="IPv4" protected="true"><transform
destination="ip.src.hash"/></key>
<key name="ip.src.hash" description="Source IP Address
Hash" format="Text"/>
</language>
```

c. Wählen Sie zum Neustarten des Decoder-Services in der Symbolleiste im Drop-down-Menü **Ansicht** (gegenwärtig als „Konfiguration“ bezeichnet) die Option **System** aus. Wählen Sie in der Ansicht „Services“ > „System“ die Option **Service herunterfahren** aus. Der Service sollte automatisch neu starten.

3. Definieren Sie die Metaschlüssel auf dem Concentrator in der Datei „index-concentrator-custom.xml“:

a. Klicken Sie auf die Registerkarte **Dateien** und wählen Sie aus dem Drop-down-Menü **index-concentrator-custom.xml** aus.

b. Geben Sie die folgenden Zeilen in den verfügbaren Eingabebereich ein:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexValues" defaultAction="Auto">
<key name="username" description="Username" format="Text"
level="IndexValues" protected="true"/>
<key name="username.hash" description="Username Hash"
format="Text" level="IndexValues" token="true"/>
<key name="ip.src" description="Source IP Address"
format="IPv4" level="IndexValues" protected="true"/>
<key name="ip.src.hash" description="Source IP Address
Hash" format="Text" level="IndexValues" token="true"/>
</language>
```

c. Wählen Sie zum Neustarten des Concentrator-Services in der Symbolleiste im Drop-down-Menü **Ansicht** (gegenwärtig als „Konfiguration“ bezeichnet) die Option **System** aus. Wählen Sie in der Ansicht „Services“ > „System“ die Option **Service herunterfahren** aus. Der Service sollte automatisch neu starten.

Konfigurieren von Datenaufbewahrung auf Concentratorn und Decodern

Durch die Konfiguration der Datenaufbewahrung wird sichergestellt, dass die Daten auf den NetWitness Suite Core-Komponenten nach einer bestimmten Zeit gelöscht werden. Die Konfiguration der Datenaufbewahrung auf Concentratorn und Decodern ist nicht für alle Umgebungen erforderlich, aber möglicherweise müssen geltende Gesetze und Vorschriften eingehalten werden. Es ist wichtig, eine entsprechenden Aufbewahrungsfrist für Ihre Umgebung zu bewerten. Die von Ihnen festgelegten Einstellungen für den Datenaufbewahrungsplaner gelten für ALLE Daten auf einem Concentrator oder Decoder.

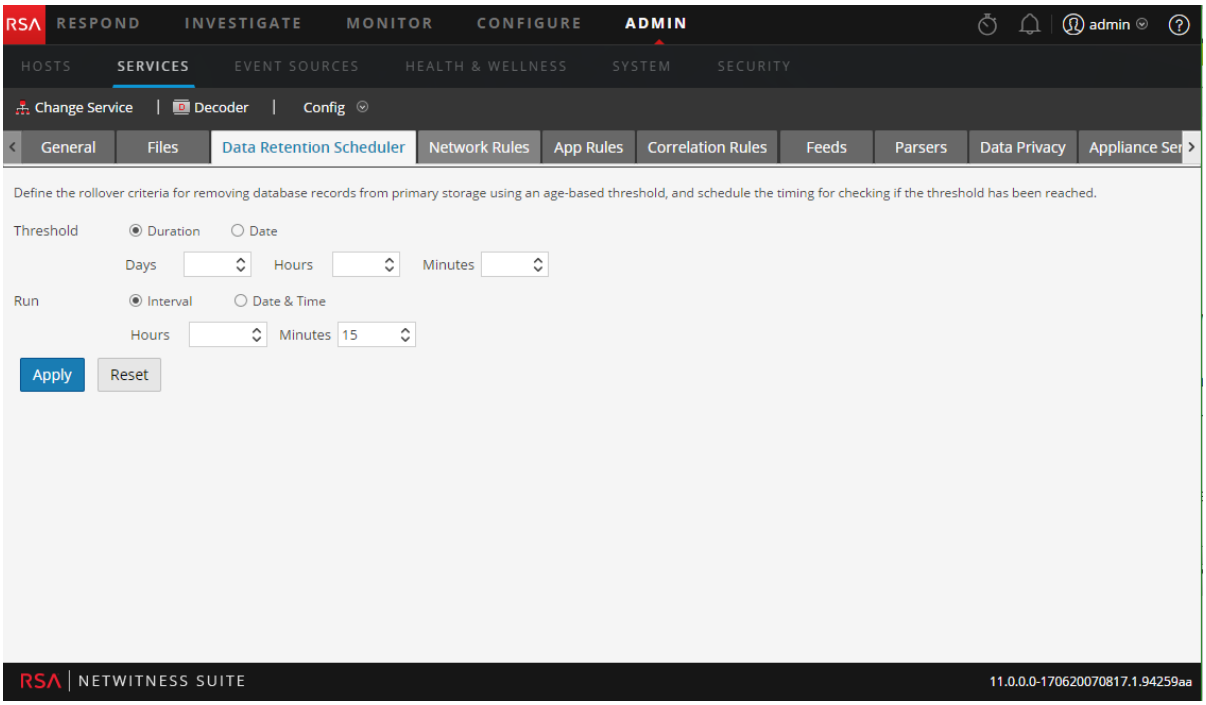
In diesem Beispiel ist NetWitness Suite so konfiguriert, dass alle 15 Minuten überprüft wird, ob der Schwellenwert für die Aufbewahrungsdauer erreicht wurde. Wenn der Schwellenwert erreicht wurde, löscht NetWitness Suite Daten, die älter als 90 Tage sind, aus den entsprechenden Datenbanken.

Achtung: Die Aufbewahrungsfrist von 90 Tagen ist nur ein Beispiel. Passen Sie Ihre Rollover-Kriterien abhängig vom Speicherort der Daten und den geltenden Gesetzen an. In einer Umgebung mit streng geregeltem Datenschutz wie z. B. in Europa, wo gesetzlich vorgeschrieben ist, dass persönlich identifizierbare Informationen (PII) nicht gespeichert werden dürfen oder häufig gelöscht werden müssen, müssen Sie möglicherweise die Aufbewahrungsfrist anpassen.

Dieses Verfahren ist optional. Wenn Sie kein Zeitlimit für die Aufbewahrungsfrist festlegen, löscht das System automatisch die ältesten Daten, wenn der Festplattenspeicher voll ist.

(Optional) Für jeden Concentrator und Decoder:

1. Navigieren Sie zur Registerkarte **Datenaufbewahrungsplaner** der Ansicht **Services-Konfiguration**.



2. Definieren Sie die Datenaufbewahrungsfrist. Legen Sie beispielsweise den **Schwellenwert** auf **Dauer** fest und geben Sie im Feld **Tage** den Wert **90** ein.
3. Definieren Sie, wie oft der Planer überprüfen soll, ob der Schwellenwert erreicht wurde. Stellen Sie zum Beispiel die Laufzeit auf **Intervall** ein und wählen Sie im Feld **Minuten** den Wert **15** aus.
4. Klicken Sie zum Speichern der Konfiguration auf **Anwenden**.

Datenschutz validieren

An diesem Punkt wurden Benutzern Rollen zugewiesen, die Berechtigungen in Bezug auf bestimmte Typen von Metadaten haben. Der nächste Schritt ist, sicherzustellen, dass der eingeschränkte Benutzer (der Analyst) nicht sehen kann, was der unbeschränkte Benutzer (der DPO) sehen kann. Sie müssen sich auch vergewissern, dass die Konfiguration der Datenaufbewahrung die Dauer beschränkt, die Daten auf den Systemen aufbewahrt werden.

1. Sehen Sie rollenbasierte Verschleierung in Aktion:
   a. Melden Sie sich als unbeschränkter Benutzer an (DPOadmin) und vergewissern Sie sich, dass dieser Benutzer alle Daten einsehen kann, einschließlich der geschützten sensiblen Daten `username` und `ip.src`, sowie jede Sitzung, die diese Metadaten enthält.
   b. Melden Sie sich ab und melden Sie sich als DPO-Benutzer wieder an.

c. Importieren Sie für jeden Decoder und Log Decoder eine PCAP- oder Protokolldatei in die Ansicht „Services-System“. Laden Sie mithilfe der Option **Paketdatei hochladen** eine PCAP-Datei hoch, die die Metadaten `username` und `ip.src` enthält.

d. Wenn der Import abgeschlossen ist, sehen Sie sich die Metadaten in der Ansicht **Investigation > Navigieren** an. Wählen Sie dafür den Concentrator aus, der mit dem Decoder verbunden ist, auf den die Daten gerade importiert wurden.

e. Scrollen Sie herunter, um sich zu vergewissern, dass die Metaschlüssel `username` und `ip.src` und die entsprechenden Werte sichtbar sind.

f. Klicken Sie auf eine der grünen Nummern neben einem Wert `username` oder `ip.src` und überprüfen Sie, dass die Sitzung in der Ereignisansicht geladen wird.

g. Notieren Sie sich die Sitzungs-ID, um sie zu prüfen, wenn Sie sich als eingeschränkter Benutzer anmelden.

h. Melden Sie sich ab und melden Sie sich als eingeschränkter Benutzer (NonprivAnalyst) wieder an.

i. Wiederholen Sie die Schritte c bis f, um zu überprüfen, ob der Benutzer die Metaschlüssel `username` oder `ip.src` oder Sitzungen mit diesen Metaschlüsseln, einschließlich der vorhin erwähnten, nicht sehen kann.

j. Navigieren Sie zu der Ansicht **Investigation > Navigieren**, um zu einer bestimmten Sitzung zu springen. Wählen Sie im Menü **Aktionen** die Option **Zu Ereignis wechseln** und geben Sie die Sitzungs-ID ein.

2. Überprüfen Sie, ob die in der Datenbank aufbewahrten Daten innerhalb der Aufbewahrungszeit liegen, die im Datenaufbewahrungsplaner konfiguriert wurden.

a. Melden Sie sich ab und dann als unbeschränkter Benutzer (DPOadmin) wieder an.

b. Navigieren Sie auf dem Concentrator zur Ansicht **Services > Durchsuchen**.

c. Wählen Sie in der Node-Struktur den Node **database** und dann **stats** aus.

d. Beobachten Sie den Wert `meta.oldest.file.time` und überprüfen Sie, ob dieser nicht älter ist als der im Datenaufbewahrungsplaner eingesetzte Schwellenwert.

e. Ändern Sie den Service auf den Decoder und wiederholen Sie die Schritte b bis d, prüfen Sie auf `stats meta.oldest.file.time` und `packet.oldest.file.time`.

Detaillierte Verfahren

Dieses Thema enthält eine Sammlung von Verfahren, anhand derer ein Datenschutzbeauftragter einen Datenschutzplan für das NetWitness Suite-Netzwerk implementiert. Diese Verfahren sind Teil einer Gesamtkonfiguration und werden nach Bedarf zum Implementieren des Datenschutzplans und zum Managen des Informationsflusses im Netzwerk durchgeführt.

- Konfigurieren der Datenverschleierung
- Konfigurieren der Datenaufbewahrung
- Konfigurieren von Benutzerkonten für die Verwendung im Datenschutz

Konfigurieren der Datenverschleierung

In diesem Thema werden die Verfahren zur Konfiguration der Datenverschleierung in NetWitness Suite beschrieben. In einer einzelnen Bereitstellung müssen alle Core-Servicekonfigurationen für eine Datenschutzlösung identisch sein. Vergewissern Sie sich, dass Sie für alle Decoders und Log Decoders denselben Hash und Salt verwenden.

Hinweis: Damit die Datenverschleierung funktioniert, müssen Benutzerkonten wie in Konfigurieren von Benutzerkonten für die Verwendung im Datenschutz beschrieben konfiguriert werden.

Konfigurieren des Decoder-Hashalgorithmus und Salt-Werts

Abgeschlossenes Hashing von Werten als Teil der Datenschutzlösung geschieht zum Zeitpunkt der Erstellung von Metaschlüsseln auf Decoder und Log Decoder. Beide Services haben Standardeinstellungen für die Verwendung mit allen Metaschlüsseln, deren Werte ohne bestimmten Hashalgorithmustyp oder Salt-Wert umgewandelt werden. Die anfänglichen NetWitness Suite-Werte für Standardeinstellungen lauten: Hashalgorithmus (SHA-256) und Salt (keiner).

Hinweis: NetWitness Suite 10.4 und niedriger unterstützen für die Abwärtskompatibilität die Verwendung des Hash-Algorithmus SHA-1. RSA empfiehlt nicht die Verwendung des SHA-1-Algorithmus, da dieser in NetWitness Suite 10.5 nicht verfügbar ist.

Wenn Sie die Standardeinstellungen ändern möchten, können Sie sie auf der Registerkarte „Datenschutz“ in der Ansicht „Service-Konfiguration“ oder in den folgenden Nodes in der Ansicht „NetWitness Suite-Services-Explorer“ bearbeiten:

- `/decoder/parsers/transforms/default.type`

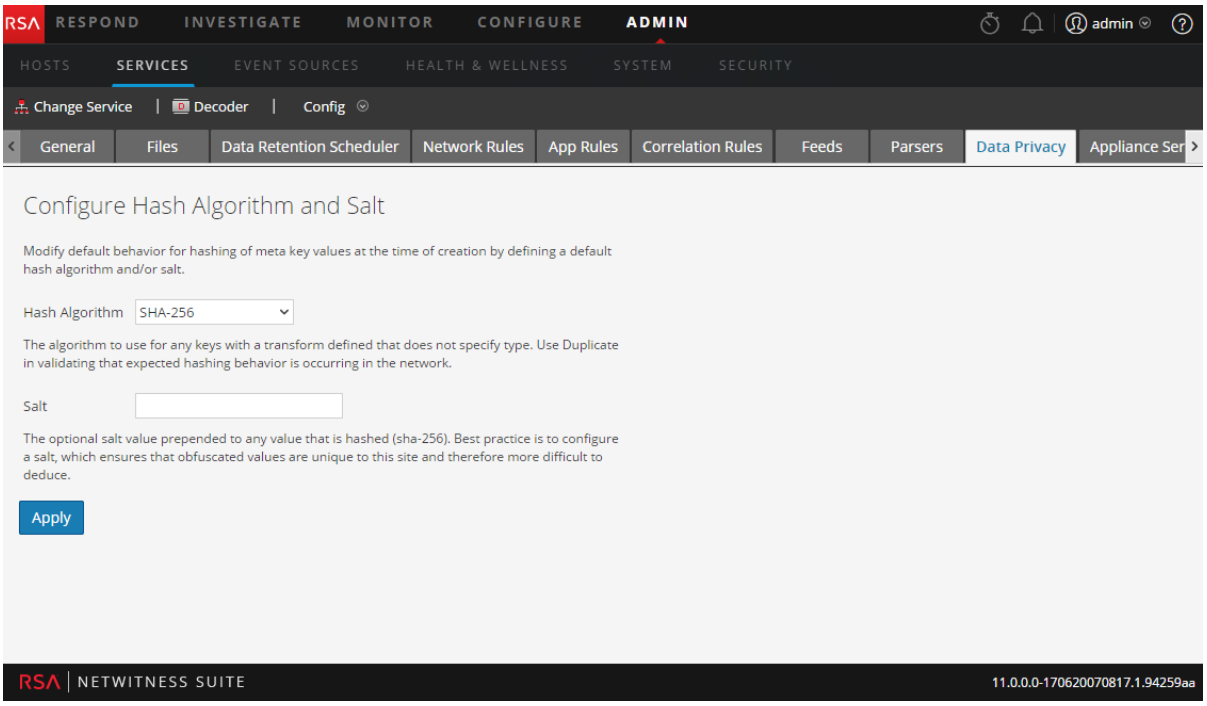
  Der zu verwendende Algorithmus für alle Schlüssel mit einer definierten Umwandlung, in der kein `type` angegeben wird. Die unterstützten Algorithmen sind: `duplicate` und `sha-256`.

- `/decoder/parsers/transforms/default.salt`

  Der Salt-Wert, der gehashten Werten (`sha-256`) vorangestellt wird. Dieser Wert ist optional, ein leerer Salt-Wert ist gültig und erzeugt einen Hashwert ohne Salt. Die Salt ist standardmäßig nicht definiert, damit Sie einen eindeutigen Salt für Ihre Umgebung erstellen können. Im Allgemeinen gilt: je länger und komplexer der Salt, desto besser die Sicherheit. Ein Salt-Wert von bis zu 60 Zeichen kann ohne größere Auswirkungen verwendet werden. Es wird ein Salt von mindestens 16 Zeichen empfohlen.

So bearbeiten Sie den standardmäßigen Hashalgorithmus und Salt:

1. Wählen Sie im Abschnitt **Admin** die Ansicht **Services** aus.
2. Wählen Sie im Raster **Services** einen Decoder- oder Log Decoder-Service aus und klicken Sie dann auf  > **Ansicht** > **Konfigurieren**. Wählen Sie die Registerkarte **Datenschutz** aus.



3. Wählen Sie im Abschnitt **Hash-Algorithmus und Salt konfigurieren** einen **Hashalgorithmus** für alle Metaschlüssel mit einer definierten Umwandlung aus, in der kein Typ angegeben wird: `sha-256`. (Für Administratoren ist ein zweiter Algorithmus, `duplicate`, verfügbar, mit dem sie überprüfen können, ob erwartetes Hashing-Verhalten im Netzwerk erfolgt.)
4. (Optional) Geben Sie in das Feld **Salt** einen Salt-Wert ein, der jedem gehashten Wert vorangestellt wird. Dieser Wert ist optional, ein leerer Salt-Wert ist gültig und erzeugt einen Hash ohne Salt. Der Salt ist standardmäßig nicht definiert, damit Sie einen eindeutigen Salt für Ihre Umgebung erstellen können. Im Allgemeinen gilt: je länger und komplexer der Salt, desto besser die Sicherheit. Bewährte Vorgehensweisen für Sicherheitszwecke geben einen Salt-Wert vor, der nicht kleiner als 100 Bits oder 16 Zeichen lang ist. Wenn ein eindeutiger Salt für jeden einzelnen Metaschlüssel erforderlich ist, muss dies in der Indexdatei konfiguriert werden, wie unten in Beispiel 3 gezeigt.
5. Klicken Sie auf **Anwenden**.

   Die neuen Einstellungen werden sofort wirksam.

Konfigurieren von Sprachschlüsseln

In NetWitness Suite 10.5 wurden der NetWitness Suite-Core-Sprache mehrere Sprachschlüsselattribute hinzugefügt, um Datenschutz zu ermöglichen. Sie können diese Attribute in der benutzerdefinierten Indexdatei für jeden Decoder oder Log Decoder bearbeiten. Die benutzerdefinierte Indexdatei (zum Beispiel „index-decoder-custom.xml“) kann auf der Registerkarte „Dateien“ in der Ansicht „Service-Konfiguration“ bearbeitet werden. Nachdem Sie an der Indexdatei Änderungen vorgenommen haben, wie die in den unten stehenden Beispielen, ist ein Neustart der Services in einer bestimmten Reihenfolge erforderlich.

Konfigurieren Sie basierend auf den Datenschutzanforderungen für Ihren Standort mithilfe der folgenden `key`-Attribute einzelne zu schützende Metaschlüssel:

- `protected`

  Dieses Attribut legt fest, dass NetWitness Suite die Werte als geschützt erachten und jede Veröffentlichung des Werts streng kontrollieren sollte. Wenn die geschützten Attribute verteilt werden, sorgt NetWitness Suite dafür, dass jedes vertrauenswürdige Downstreamsystem die Werte entsprechend behandelt. Fügen Sie dieses Attribut allen Services hinzu, die die geschützten Werte erstellen (d. h. Decoder oder Log Decoder) sowie allen Services, die sicheren Zugriff (SDK (Software Development Kit)-Abfrage/Werte, Aggregation) außerhalb von Core-Services bereitstellen. Davon ausgenommen ist ein Broker ohne angegebene Indexdatei, dem die Attribute nicht hinzugefügt werden müssen.

- `token`

  Dieses Attribut legt fest, dass Werte für diesen Schlüssel Platzhalter für andere Werte und visuell möglicherweise nicht interessant sind. Das Attribut `token` ist informationell und dient hauptsächlich dazu, dass Benutzeroberflächenelemente den Wert in einem nützlicheren oder einem visuell ansprechenderen Format anzeigen.

- `transform`

  Dieses untergeordnete Element zu `key` zeigt an, dass alle Werte für einen gegebenen Metaschlüssel umgewandelt und die sich ergebenden Werte dauerhaft einem anderen Metaschlüssel zugeordnet werden sollten. Das Element `transform` ist nur auf Decoders und Log Decoders erforderlich und hat informativen Charakter, wenn es auf anderen Core-Services angegeben ist. Das Element `transform` enthält die folgenden Attribute und untergeordneten Elemente:

Name	Typ	Beschreibung	Optional oder erforderlich
destination	Attribut	Gibt den Namen des Schlüssels an, dem der umgewandelte Wert dauerhaft zugeordnet wird.	Erforderlich
type	Attribut	Der anzuwendende Umwandlungsalgorithmus. Wenn kein Wert angegeben wird, wird der Wert von /decoder/parsers/transforms/default.type verwendet.	Optional
param	Untergeordnetes Element	Ein Name-Wert-Paar, bei dem jedes param-Element ein erforderliches name-Attribut hat und der untergeordnete Text der Wert ist. Das einzige unterstützte param-Element wird verwendet, um einen schlüsselspezifischen salt-Wert festzulegen. Wenn kein Wert angegeben wird, wird der Wert von /decoder/parsers/transforms/default.salt verwendet.	Optional

Beispiel 1

Markieren Sie auf einem Decoder oder Log Decoder username als geschützt und führen Sie das Hashing aller Werte zu username.hash mit dem standardmäßigen Algorithmus und Salt durch:

```
<key name="username" description="Username" format="Text"
protected="true"><transform destination="username.hash"/></key>
```

Beispiel 2

Markieren Sie auf einem Concentrator username als geschützt und username.hash als Token:

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key description="Username" format="Text" level="IndexValues"
name="username" protected="true"/>
<key description="Username Hash" format="Binary" level="IndexValues"
name="username.hash" token="true"/>
</language>
```

Beispiel 3

Markieren Sie auf einem Decoder oder Log Decoder `username` als geschützt und führen Sie das Hashing aller Werte zu `username.bin` mit dem angegebenen Algorithmus und Salt durch:

```
<key name="username" description="Username" format="Text"
protected="true">
<transform destination="username.bin" type="sha-256">
<param name="salt">0000</param>
</transform></key>
```

Konfigurieren von Metadaten- und Contentsichtbarkeit pro Benutzerrolle auf Core-Services

Bei einzelnen Broker-, Concentrator-, Decoder-, Log Decoder- und Archiver-Services, die in der Ansicht „Services-Sicherheit“ angezeigt werden, können Administratoren die Sichtbarkeit von Metadaten und Content konfigurieren, basierend auf der Benutzergruppe oder der Rolle, die einem Benutzer zugewiesen ist. Dies ist die Funktion „SDK-Metarollen“ und sie ist standardmäßig aktiviert.

Hinweis: Administratoren, die Metadaten- und Contentsichtbarkeit pro Benutzer konfigurieren möchten, dürfen die `sdk.content`-Berechtigung (auf der Registerkarte „Rollen“) nicht deaktivieren. Wenn die `sdk.content`-Berechtigung auf der Registerkarte „Rollen“ deaktiviert ist, sind Pakete und unverarbeitete Protokolle für `system.roles`-Node nicht sichtbar. Der `system.roles`-Node verarbeitet die Filterung mithilfe der Methode, die auf der Registerkarte „Einstellungen“ konfiguriert ist.

Wenn die Funktion `sdk.content` aktiviert ist, ist der nächste Schritt die Auswahl der Methode des Filterns von Metadaten und Content auf der Registerkarte „Einstellungen“. Die Auswahl einer Schwarze- oder Weiße-Listen-Option stellt zusätzliche Berechtigungen für bestimmte Metaschlüssel auf der Registerkarte „Rollen“ zur Verfügung. Das Ergebnis ist, dass Administratoren auf der Registerkarte „Rollen“ eine Benutzerrolle wählen können, z. B. Analyst, und bestimmte Metaschlüssel (und Inhalte) auswählen können, die für diese Benutzergruppe auf der schwarzen oder auf der weißen Liste stehen. Die Berechtigungen gelten für alle Benutzer in der Benutzergruppe.

In der folgenden Tabelle sind die Filteroptionen auf der Registerkarte „Einstellungen“ aufgeführt sowie die numerischen Werte, die zur Deaktivierung (0) und für andere Arten des Filterns verwendet werden (1 bis 6). Es ist nicht notwendig, die numerischen Werte zu kennen, es sei denn, Sie konfigurieren die Metadaten- und Contentsichtbarkeit im `system.roles`-Node manuell.

system.roles-Node-Wert	Option der Registerkarte Einstellungen	Ereignis-Metadaten	Ursprüngliches Ereignis
0	**Keine Filterung.** Systemrollen, die Berechtigungen auf Metaschlüsselbasis definieren, sind deaktiviert.	Sichtbar	Sichtbar
1	**Metadaten und Content in der weißen Liste.** Standardmäßig sind keine Metaschlüssel und Pakete sichtbar. Das Auswählen einzelner SDK-Metarollen pro Benutzergruppe ermöglicht Benutzern das Einsehen von Metadaten und Paketen für diese SDK-Metarolle.	Nicht sichtbar Zum Anzeigen auswählen	Nicht sichtbar Zum Anzeigen auswählen

system.roles-Node-Wert	Option der Registerkarte Einstellungen	Ereignis-Metadaten	Ursprüngliches Ereignis
2	**Nur Metadaten in der weißen Liste.** Standardmäßig sind Pakete sichtbar, jedoch keine Metadaten. Das Auswählen einzelner SDK-Metarollen pro Benutzergruppe ermöglicht Benutzern das Einsehen von Metadaten für diese Rolle.	Nicht sichtbar Zum Anzeigen auswählen	Sichtbar
3	**Nur Content in der weißen Liste.** Standardmäßig sind Metadaten sichtbar, jedoch keine Pakete. Das Auswählen einzelner SDK-Metarollen pro Benutzergruppe ermöglicht Benutzern das Einsehen von Paketen für diese Rolle.	Sichtbar	Nicht sichtbar Zum Anzeigen auswählen
4	**Metadaten und Content in der schwarzen Liste.** Standardmäßig sind alle Metadaten und Pakete sichtbar. Das Auswählen einzelner SDK-Metarollen pro Benutzergruppe verhindert, das Benutzer Metadaten und Pakete für diese Rolle einsehen.	Sichtbar Zum Ausblenden auswählen	Sichtbar Zum Ausblenden auswählen

system.roles-Node-Wert	Option der Registerkarte Einstellungen	Ereignis-Metadaten	Ursprüngliches Ereignis
5	**Nur Metadaten in der schwarzen Liste.** Standardmäßig sind alle Metadaten und Pakete sichtbar. Das Auswählen einzelner SDK-Metarollen pro Benutzergruppe verhindert, dass Benutzer Metadaten für diese Rolle einsehen.	Sichtbar Zum Ausblenden auswählen	Sichtbar
6	**Nur Content in der schwarzen Liste.** Standardmäßig sind alle Metadaten und Pakete sichtbar. Das Auswählen einzelner SDK-Metarollen pro Benutzergruppe verhindert, dass Benutzer Pakete für diese Rolle einsehen.	Sichtbar	Sichtbar Zum Ausblenden auswählen

Drei Faktoren bestimmen, was dem Benutzer angezeigt wird:

- Die Einstellung der SDK-Metarolle (schwarze oder weiße Liste).
- Die beschränkten Metaschlüssel, konfiguriert für die Gruppe, der der Benutzer angehört.
- Die Metaschlüssel in der analysierten Sitzung

Achtung: Beachten Sie, dass beim Hinzufügen zur schwarzen Liste das implizite Vertrauen für alle gewährt wird, außer für die konfigurierten Metadaten. Damit ein Decoder RBAC aktiviert hat und implizites Vertrauen verwendet, darf er nur eine Systemeinstellung für schwarze Listen verwenden; eine Einstellung für weiße Listen führt zu einigen Problemen mit Metaschlüsseln, die nicht explizit aktiviert und daher nicht sichtbar sind. Es ist unmöglich, implizites Vertrauen unter Whitelist-Regeln zu gewähren, da die Gesamtheit der Metaschlüssel nicht bekannt ist. Wenn Sie weiße Listen verwenden möchten, besteht ein Workaround darin, RBAC für den Decoder auszuschalten und für alle Benutzerkonten die Möglichkeit zu deaktivieren, sich direkt mit dem Decoder zu verbinden, wenn RBAC verwendet werden soll.

Im Folgenden finden Sie ein Beispiel dafür, wie sich die Konfiguration von SDK-Metarollen auf eine Gruppe mit beschränkten Metaschlüsseln auswirkt.

Konfiguration:

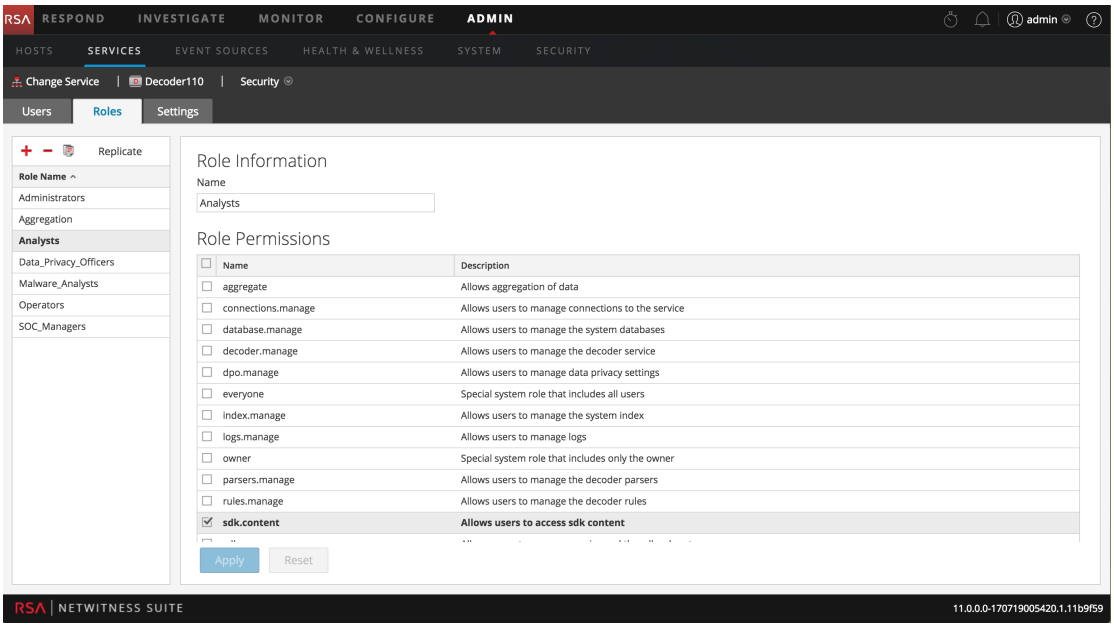
- Die SDK-Metarolleneinstellung ist **Metadaten und Content in der schwarzen Liste**. Wenn diese Option implementiert ist, sind standardmäßig alle Metadaten und Inhalte (Pakete und Protokolle) sichtbar.
- Der Administrator hat für die Gruppe „Analysten“ konfigurierte Metaschlüssel beschränkt, um zu verhindern, dass sensible Daten angezeigt werden (z. B. `username`).
- Die Pakete und Protokolle zu jeglichen Sitzungen, die den Metaschlüssel `username` enthalten, sind für einen Analysten nicht sichtbar.

Ergebnis: Jetzt führt ein Benutzer, der Mitglied der Gruppe Analysten ist, eine Ermittlung zu einer Sitzung durch. Abhängig vom Inhalt der Sitzung, fällt das Ergebnisse unterschiedlich aus:

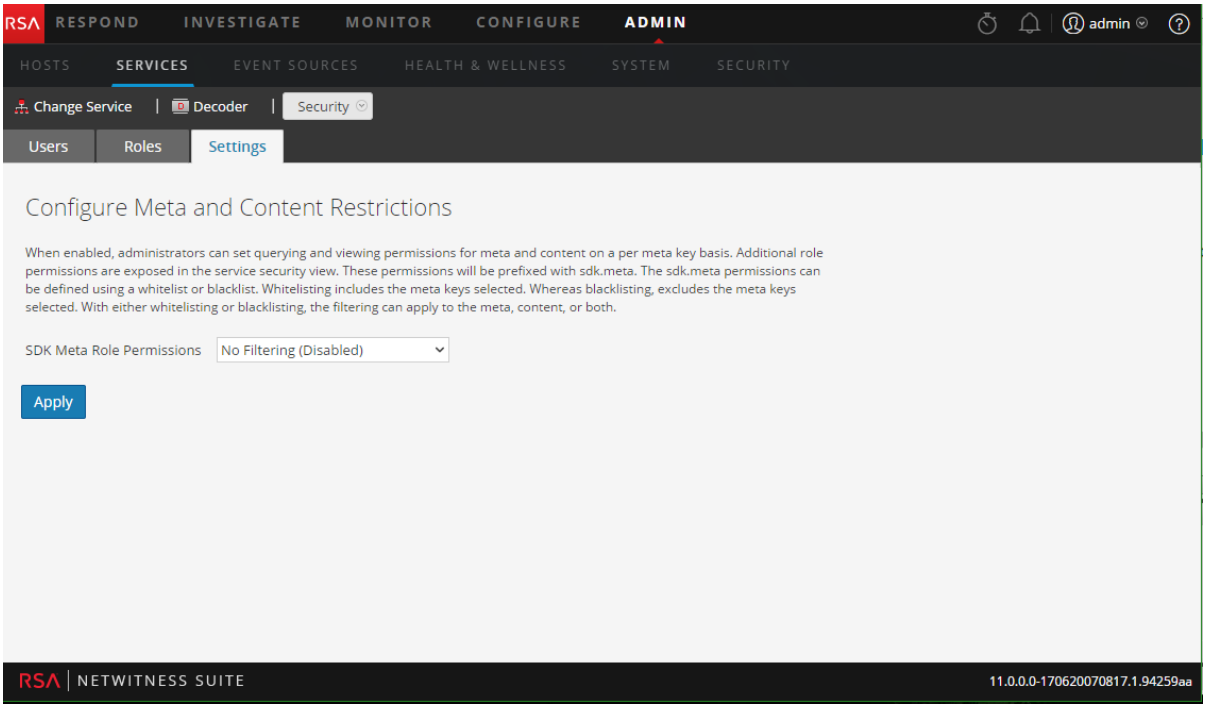
- Sitzung 1 enthält die folgenden Metaschlüssel: `ip`, `eth`, `host` und `file`. Die Sitzung enthält nicht `username`, daher werden alle Pakete und Protokolle in der Sitzung angezeigt.
- Sitzung 2 enthält die folgenden Metaschlüssel: `ip`, `time`, `size`, `file` und `username`. Da die Sitzung den Metaschlüssel `username` enthält, werden dem Analysten keine Pakete oder Protokolle der Sitzung angezeigt.

So konfigurieren Sie Beschränkungen für Metadaten und Inhalte für einen Decoder oder Log Decoder:

1. Wählen Sie in der Ansicht **Admin Services** aus.
2. Wählen Sie im Raster **Services** einen Broker-, Concentrator-, Decoder-, Log Decoder- oder Archiver-Service aus und klicken Sie auf  **> Ansicht > Sicherheit**. Klicken Sie auf die Registerkarte **Rollen**, wählen Sie eine Rolle aus und überprüfen Sie, ob die `sdk.content` Rolle aktiviert ist.



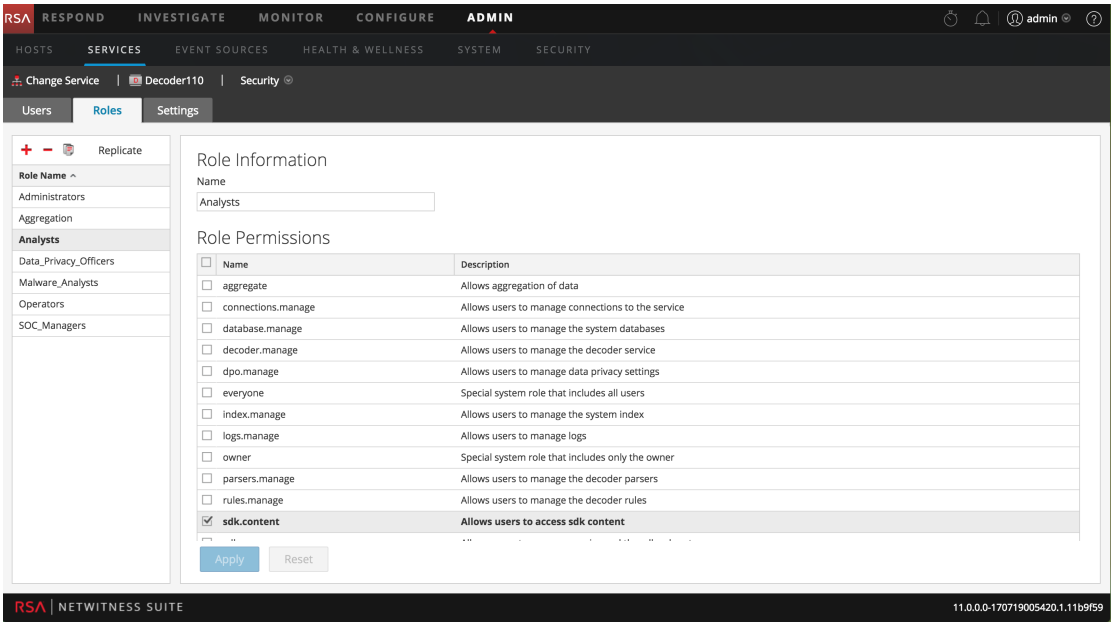
3. Klicken Sie auf die Registerkarte **Einstellungen**.



4. Wählen Sie eine der Filtermethoden (schwarze oder weiße Liste) und einen der Contenttypen (Metadaten und Content, Nur Metadaten oder Nur Content) aus und klicken Sie auf **Anwenden**.

5. Klicken Sie auf die Registerkarte **Rollen** und auf eine Rolle, für die Sie Content erlauben (weiße Liste) oder blockieren (schwarze Liste) möchten, wie in der Einstellung „SDK-Meta-Rollenberechtigungen“ angegeben.

Die Rollenberechtigungen für die ausgewählte Rolle werden angezeigt und die SDK-Metarollenberechtigungen sind zur Auswahl verfügbar, zum Beispiel `sdk.meta.action`. Wenn Sie eine der Optionen für die weiße Liste in der Einstellung „SDK-Rollenberechtigungen“ auswählen, müssen Sie jede SDK-Metarolle zuweisen, damit die ausgewählten Inhalte für Benutzer mit dieser zugewiesenen SDK-Metarolle sichtbar sind. Wenn Sie eine der Optionen für die schwarze Liste in der Einstellung „SDK-Rollenberechtigungen“ ausgewählt haben, wird ausgewählter Content vor Benutzern verborgen, denen die SDK-Metarolle zugewiesen ist.



6. Wählen Sie die SDK-Metarollenberechtigungen für Benutzer aus, denen diese Rolle zugewiesen ist. Klicken Sie auf **Anwenden**.

   Die Einstellungen werden sofort wirksam und gelten für neue Pakete und Protokolle, die von Decoder oder Log Decoder verarbeitet werden.

Konfigurieren von Metaschlüsseln, die auf einem Decoder nicht per Parser auf einen Datenträger geschrieben werden

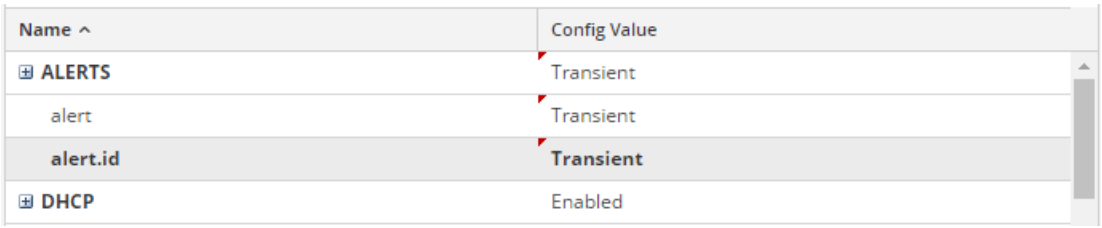
Auf einem Decoder und Log Decoder kann ein Datenschutzbeauftragter (DPO) einzelne Metaschlüssel konfigurieren, die nicht auf die Festplatte geschrieben werden. Dazu gibt der DPO die Metaschlüssel im Index und in der Parserkonfiguration als „vorübergehend“ an.

Hinweis: Dieselbe Fähigkeit war vorher auf Log Decodern verfügbar und wurde bei der Einrichtung der Parser durch Änderung der Datei „table-map.xml“ konfiguriert. Jetzt ist sie in der Ansicht „Service-Konfiguration“ integriert.

So konfigurieren Sie ausgewählte Metaschlüssel auf einzelnen Parsern, die nicht auf den Datenträger geschrieben werden:

1. Wählen Sie im Abschnitt **Admin Services** aus.
2. Wählen Sie im Raster **Services** einen Decoder- oder Log Decoder-Service und dann  **> Ansicht > Konfiguration** aus.
3. Wählen Sie im Abschnitt **Parserkonfiguration** auf der Registerkarte **Allgemein** einen Parser aus und wählen Sie dann **Vorübergehend** in der Drop-down-Liste **Konfigurationswert** aus. Greifen Sie auf die Liste zu, indem Sie auf den Konfigurationswert klicken („Aktiviert“, „Deaktiviert“ oder „Vorübergehend“).

   Die Konfigurationsänderung wird durch ein rotes Dreieck markiert.



4. Klicken Sie auf **Anwenden**.

   Die Änderung wird sofort wirksam. Der als „vorübergehend“ konfigurierte Parser speichert nicht länger Store-Metaschlüssel auf dem Datenträger.

Konfigurieren der Datenaufbewahrung

Ein NetWitness Suite-Benutzer mit Administratorrolle kann NetWitness Suite so konfigurieren, dass sensible Daten unabhängig von der Datenaufnahmerate des Systems nach einer bestimmten Aufbewahrungsfrist gelöscht werden. Beispiel: Als Richtlinie könnte festgelegt werden, dass Pakete (sowohl Roh- als auch Metadaten) nicht länger als 24 Stunden und einige Protokolle (sowohl Roh- als auch Metadaten) bis zu 7 Tage lang aufbewahrt werden. Falls sensible Daten in andere Datenbanken auf den Reporting Engine-, Malware Analysis-, Event Stream Analysis-Servern und NetWitness-Server gelangen, kann die Datenaufbewahrung dort ebenfalls verwaltet werden. Der Administrator muss jeden Service basierend auf Richtlinien und Datenschutzgesetzen einzeln für alle NetWitness Suite-Komponenten (außer Event Stream Analysis) einrichten.

Sensible Daten können sich auch im Cache befinden.

- Brokers können Dateien zwischenspeichern. Hier muss eine Löschung durch Konfiguration eines individuellen Rollover und anderer Entfernungsmaßnahmen aus dem Cache erfolgen. Der Administrator kann den Cache-Rollover für einen Broker mithilfe der Planerdatei in der Registerkarte „Dateien“ der Ansicht „Service-Konfiguration“ konfigurieren.
- Investigation und NetWitness-Server speichern Daten im Cache. Diese werden automatisch alle 24 Stunden gelöscht.
- Wenn der Datenschutzbeauftragte Daten exportiert, entspricht dies dem Speichern von Daten in der Jobwarteschlange auf dem NetWitness-Server. Zum Löschen dieser Daten muss der Administrator oder DPO die Jobwarteschlange regelmäßig löschen.

Datenaufbewahrung

Sie können einen wiederkehrenden Job für Decoder-, Log Decoder- und Concentrator-Services in NetWitness Suite planen, um zu überprüfen, ob die Daten bereit für die Löschung sind. Der Datenaufbewahrungsplaner bietet eine Möglichkeit zur Konfiguration der grundlegenden Planung (siehe unten). Die erweiterten Planereinstellungen stehen ebenfalls durch Bearbeitung der Planerdatei in der Registerkarte „Datei“ der Ansicht „Service-Konfiguration“ oder im Node in der Explorer-Ansicht zur Verfügung.

Der Archiver verfügt über flexible Optionen zur Datenspeicherung und -aufbewahrung. Sie können unterschiedliche Arten von Protokolldaten in einzelnen Sammlungen ablegen und diese individuell managen. Diese Sammlungen ermöglichen es Ihnen festzulegen, wie viel des gesamten Speicherplatzes verwendet werden soll und wie viele Tage die Protokolle in der Sammlung gespeichert werden sollen. Sie können außerdem bestimmen, ob die Protokolldaten gelöscht oder in den Cold-Offlinespeicher verschoben werden sollen, nachdem der für die Sammlung maximal festgelegte Speicherplatz erreicht wurde.

Beispielsweise können Sie sensible Daten in einer Sammlung ablegen und eine Beschränkung für die Speicherdauer konfigurieren, z. B. 30 Tage. Aktivieren Sie nicht den Warm- oder Cold-Speicher für diese Sammlung, um die Daten nach 30 Tagen zu löschen.

Vergleich zwischen Löschen und Aufbewahren von Protokolldaten

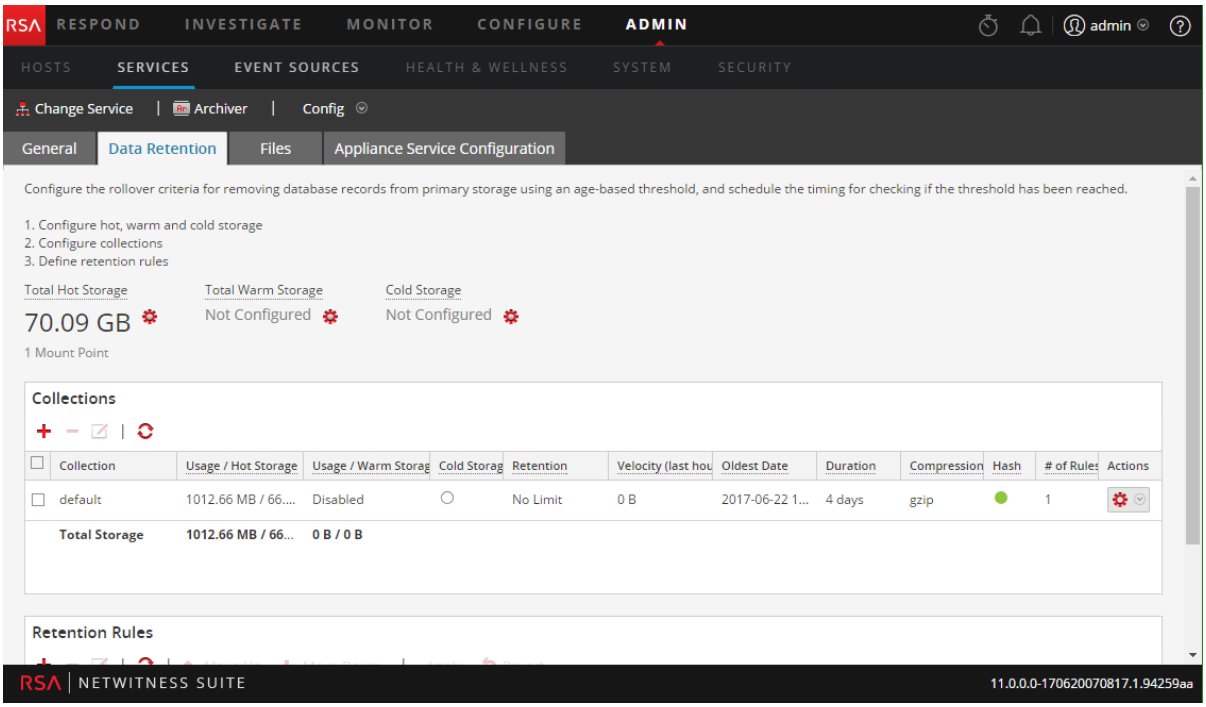
Administratoren können Hot-, Warm- und Cold-Tiered-Storage auf einem Archiver konfigurieren. Der Cold-Speicher enthält die ältesten Daten, die entweder für den Betrieb des Unternehmens benötigt werden oder für behördliche Auflagen erforderlich sind. Wenn eine Sammlung die Aufbewahrungsfristen für Hot- und Warm-Speicher erreicht hat, löscht NetWitness Suite die Protokolldaten aus diesen Speichern. Wenn ein Cold-Speicher konfiguriert wurde, wird eine Kopie darin abgelegt, bevor die Protokolle aus dem Hot- oder Warm-Speicher gelöscht werden. Sie können auswählen, ob der Cold-Speicher für jede Protokollspeichersammlung aktiviert werden soll. Cold-Speicher werden von NetWitness Suite nicht gemanagt.

Aktivieren oder Deaktivieren des Cold-Speichers in einer Protokollspeichersammlung

Wenn Protokolldaten in einer Sammlung die Aufbewahrungsfristen für Hot- und Warm-Speicher erreicht haben, können Sie sie löschen oder in den Offlinespeicher (Cold-Speicher) verschieben.

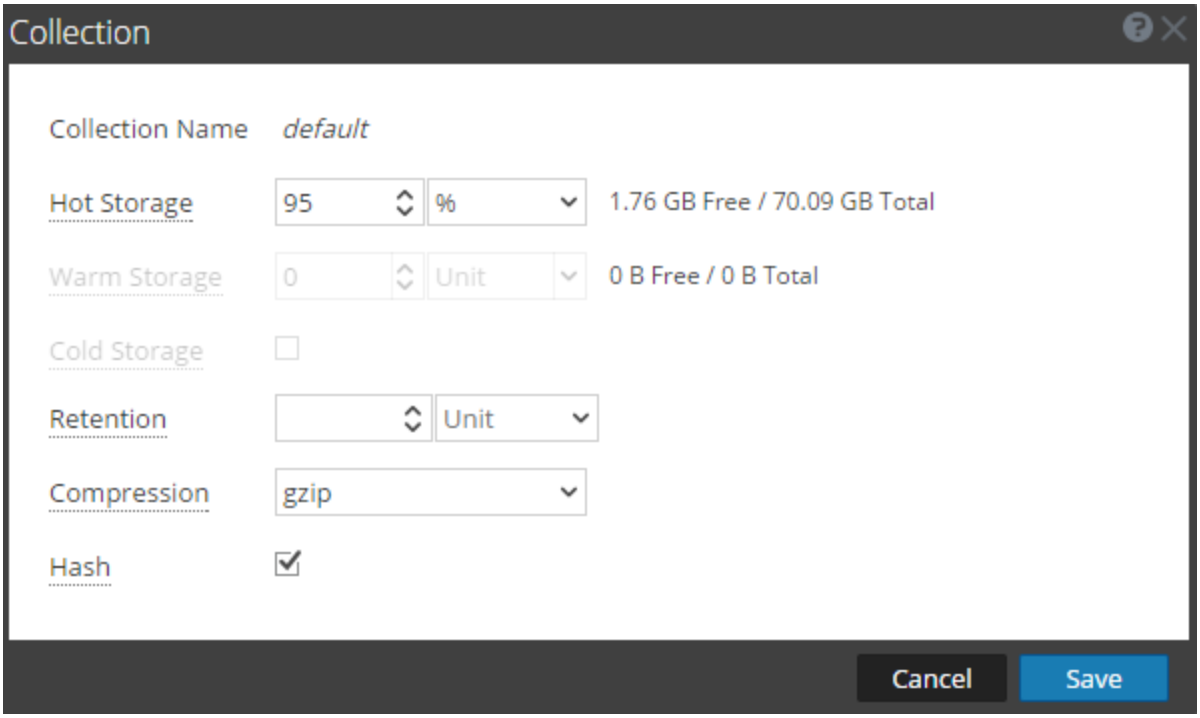
So aktivieren oder deaktivieren Sie den Cold-Speicher in einer Protokollspeichersammlung auf einem Archiver:

1. Wählen Sie im Abschnitt **Admin** die Ansicht **Services** aus.
2. Wählen Sie einen Archiver-Service und dann  **> Ansicht > Konfiguration** aus.
3. Klicken Sie auf die Registerkarte **Datenaufbewahrung**.



4. Wählen Sie im Abschnitt **Sammlungen** der Registerkarte „Datenaufbewahrung“ eine Sammlung aus und klicken Sie auf .

   Das Dialogfeld „Sammlung“ wird angezeigt.



Hinweis: Wenn die maximale Speichergröße der Sammlung keine komplette Datenaufbewahrung für die festgelegte Aufbewahrungsfrist zulässt, werden die Daten von NetWitness Suite gelöscht oder in den Warm- oder Cold-Speicher verschoben, sofern dies in der Sammlung angegeben ist.

5. Aktivieren oder deaktivieren Sie Cold-Speicher:
   - Deaktivieren Sie das Kontrollkästchen **Cold-Speicher**, um Protokolldaten zu löschen, wenn die Sammlung die festgelegten Aufbewahrungsfristen erreicht hat.
   - Aktivieren Sie das Kontrollkästchen **Cold-Speicher**, um Protokolldaten in einen Offlinespeicher zu verschieben, wenn die Sammlung die angegebenen Aufbewahrungsfristen erreicht hat.
6. Klicken Sie auf **Speichern**.

Konfigurieren der Protokollaufbewahrung und -speicherung auf einem Archiver

Weitere Informationen über die Protokollaufbewahrung und -speicherung auf einem Archiver finden Sie unter **Konfigurieren des Archiver-Speichers und der Protokollaufbewahrung** im *Konfigurationsleitfaden Archiver*.

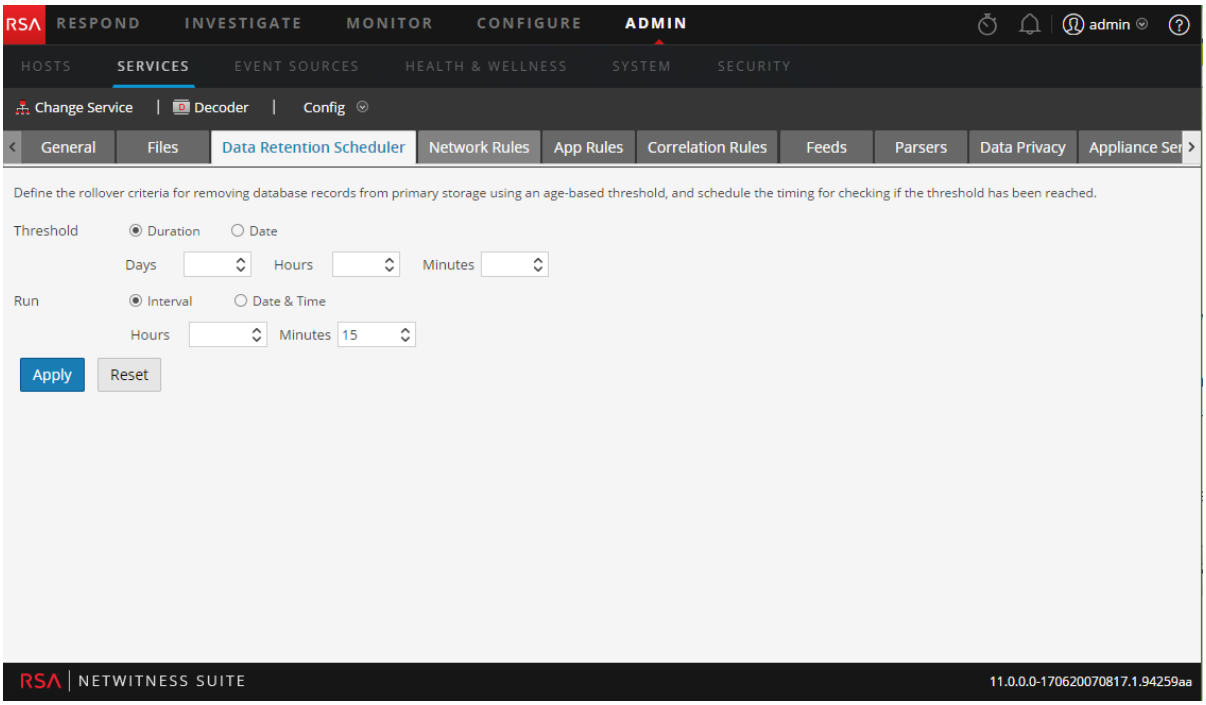
Planen eines wiederkehrenden Jobs zum Überprüfen der Datenaufbewahrungsfristen

Durch die Konfiguration des Datenaufbewahrungsplaners wird sichergestellt, dass die Daten, die sich auf den Komponenten Decoder, Log Decoder und Concentrator befinden, nach einer bestimmten Zeit gelöscht werden. Beispiel: Die Datenaufbewahrung auf einem Decoder kann so konfiguriert werden, dass alle 15 Minuten überprüft wird, ob der festgelegte Schwellenwert für die Aufbewahrungsdauer erreicht wurde. Wenn der Schwellenwert erreicht wurde, löscht NetWitness Suite Daten, die älter als 4 Stunden sind, aus den entsprechenden Datenbanken.

Achtung: Der Plan überschreibt alle vorherigen Pläne und wird sofort wirksam. Wenn die Aufbewahrungsfrist verringert wird, werden die Daten entfernt, die diese Aufbewahrungsfrist überschreiten.

Für einen Decoder, Log Decoder oder Concentrator:

1. Wählen Sie im Abschnitt **Admin** die Ansicht **Services** aus.
2. Wählen Sie im Raster **Services** einen Decoder-, Log Decoder- oder Concentrator-Service und dann  > **Ansicht** > **Konfiguration** aus.
3. Klicken Sie auf die Registerkarte **Datenaufbewahrungsplaner**.



4. Legen Sie den Schwellenwert basierend auf der Dauer, die die Daten gespeichert sind, oder dem Datum, an dem die Daten gespeichert wurden, fest. Führen Sie einen der folgenden Schritte aus:

   a. Wählen Sie zum Definieren des Zeitraums, den Daten vor einer Löschung gespeichert werden können, **Dauer** aus, und geben Sie die Anzahl der Tage (maximal 365), Stunden (maximal 24) und Minuten (maximal 60) ein, die seit dem Zeitstempel der Datei vergangen sind.

   b. Wählen Sie **Datum** aus und geben Sie in den Feldern „Kalender“ und „Zeit“ den Kalendertag bzw. die Uhrzeit an, um die Löschung der Daten basierend auf dem Datum des Zeitstempels zu definieren.

5. Führen Sie einen der folgenden Schritte aus, um den **Plan für das Überprüfen der Rollover-Kriterien** zu konfigurieren:

   a. Wenn Sie ein regelmäßiges Intervall festlegen möchten, in dem die geplante Datenbanküberprüfung erfolgt, wählen Sie **Intervall** aus und geben Sie die **Stunden** und **Minuten** zwischen den geplanten Überprüfungen ein.

   b. Wenn Sie ein regelmäßiges Datum und eine Uhrzeit festlegen möchten, zu der die geplante Datenbanküberprüfung erfolgt, wählen Sie **Datum und Zeit** aus und geben Sie die Systemuhrzeit für den Rollover im Format `hh:mm:ss` an.

      - Wählen Sie zum Festlegen des Tags **Jeden Tag**, **Wochentage** oder **Wochenenden** aus. Die Standardeinstellung des Planers lautet **Jeden Tag**.
      - Wählen Sie zum Festlegen eines anderen Satzes Wochentage **Benutzerdefiniert** aus

und klicken Sie auf alle Tage, an denen die Datenbanküberprüfung erfolgen soll.

Achtung: Der Plan überschreibt alle vorherigen Pläne und wird sofort wirksam. Wenn die Aufbewahrungsfrist verringert wird, werden die Daten entfernt, die diese Aufbewahrungsfrist überschreiten.

6. Klicken Sie auf **Anwenden**, um die Konfiguration abzuschließen.

Konfigurieren von Benutzerkonten für die Verwendung im Datenschutz

In diesem Thema werden die Verfahren zur Konfiguration von Benutzerkonten in NetWitness Suite beschrieben, die mit verschleierten Daten arbeiten. Damit die Datenverschleierung funktioniert, müssen Konten und Berechtigungen für verschiedenen Benutzertypen konfiguriert werden.

- Passen Sie die standardmäßige Systemrolle `Administrators` in NetWitness Suite an, um die Berechtigungen zu entfernen, die nur für den Datenschutzbeauftragten verfügbar sein sollen.
- Fügen Sie auf Systemebene zwei neue Benutzerkonten hinzu, um einen Data Privacy Officer und einen typischen Analysten abzubilden.
- Fügen Sie auf Serviceebene ein Benutzerkonto mit der Aggregationsrolle hinzu, sodass Decoders und Log Decoders Daten auf einen Concentrator oder Broker aggregieren können.
- Konfigurieren Sie auf der Reporting Engine zwei separate Servicekonten: Ein Servicekonto für das allgemeine Reporting, das keine sensiblen Daten umfasst, und ein weiteres Konto für Benutzer mit den nötigen Berechtigungen für den Zugriff auf alle Daten, einschließlich sensibler Daten. Dieses Verfahren ist im *Konfigurationsleitfaden Reporting Engine* unter **Konfigurieren von Datenquellenberechtigungen** beschrieben.

Anpassen der standardmäßigen Benutzerrolle Administratoren auf Serviceebene

Um die Funktionen für Datenschutzbeauftragte und Administratoren auf jedem Decoder und Log Decoder zu trennen, müssen Sie die Berechtigung `dpo.manage` von einem Klon der Administratorrolle entfernen.

1. Wählen Sie in der Ansicht **Administration > Services** einen Decoder oder Log Decoder aus. Klicken Sie auf  **> Ansicht > Sicherheit**.
2. Klicken Sie in der Ansicht **Services > Sicherheit** auf die Registerkarte **Rollen**, wählen Sie **Administratoren** aus und klicken Sie auf  .

   Geben Sie im Dialogfeld **Neuen Rollennamen eingeben** einen neuen Rollennamen wie „Nicht_DPO_Administratoren“ ein und klicken Sie auf **Speichern**.
3. Wählen Sie die neue Rolle aus.

   Die Rolleninformationen werden zur Bearbeitung angezeigt.

4. Klicken Sie auf das Kästchen neben **dpo.manage**, um es zu deaktivieren, und klicken Sie auf **Anwenden**.

   Die Berechtigung zum Managen der Datenschutzkonfiguration wird aus der neuen Rolle entfernt.

5. Wählen Sie in der Registerkarte **Benutzer** jeden Benutzer mit der Rolle **Administratoren** aus und ändern Sie die Rolle zu der geklonten Rolle.

6. Überprüfen Sie, ob sich die Benutzer mit der geänderten Rolle Administratoren sich mit Administratorberechtigungen anmelden können.

7. Vergewissern Sie sich, dass die Benutzer mit der geänderten Administratorrolle die Metadaten- und Inhaltsbeschränkungen in der Registerkarte Einstellungen nicht ändern können.

Hinzufügen eines Benutzerkontos mit der Benutzerrolle „Aggregation“ auf Serviceebene

So stellen Sie sicher, dass Decoders und Log Decoders die Daten auf einen Concentrator oder Broker aggregieren können:

1. Wählen Sie in der Ansicht **Administration > Services** einen Decoder oder Log Decoder aus. Klicken Sie auf  **> Ansicht > Sicherheit**.

2. Fügen Sie in der Registerkarte **Benutzer** einen Benutzer mit der Rolle `Aggregation` hinzu und klicken Sie auf **Anwenden**.

   Hinweis: Das Thema **Aggregationsrolle** im *Leitfaden für die ersten Schritte mit Hosts und Services* enthält detaillierte Informationen über die Anwendung dieser Benutzerrolle.

Hinzufügen von Konten für Datenschutzbeauftragte und Analysten auf dem NetWitness-Server

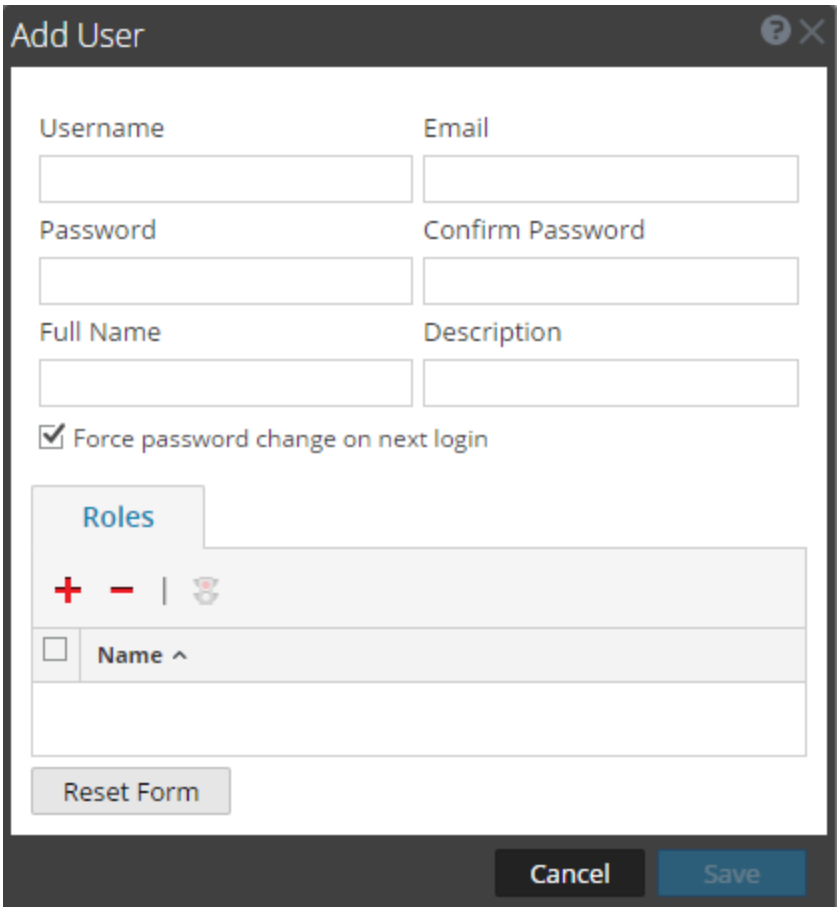
Sie müssen in NetWitness Suite zwei neue Benutzerkonten auf Systemebene hinzufügen, um einen berechtigten Datenschutzbeauftragten und einen typischen Analysten abzubilden. Wenn die Umgebung mit den vertrauenswürdigen Standardverbindungen konfiguriert wurde, müssen Sie in den Core-Services (Broker, Concentrator und Decoder) keine neuen Benutzerkonten erstellen. Wenn ein Benutzer auf dem NetWitness-Server-Server erstellt wird, kann sich dieser bei den Services anmelden.

Hinweis: Der Rollenname muss sowohl auf dem Server als auch auf den Services existieren, und er muss in beiden Fällen identisch sein. Wenn Sie eine neue benutzerdefinierte Rolle auf dem NetWitness-Server erstellen, achten Sie darauf, dass Sie diese auch allen Core-Services hinzufügen.

1. Erstellen Sie für den Datenschutzbeauftragten ein neues Benutzerkonto:

   a. Wählen Sie in der Ansicht **Sicherheit** die Registerkarte **Benutzer** aus und klicken Sie auf +.

   Das Dialogfeld „Benutzer hinzufügen“ wird angezeigt.



   b. Erstellen Sie das neue Konto mit den folgenden Anmeldeinformationen.

   Benutzername = <neuer Benutzername für die Anmeldung, zum Beispiel „DPOadmin“>
   E-Mail = <E-Mail-Adresse des neuen Benutzers, zum Beispiel „DPOadmin@rsa.com“>
   Passwort = <Passwort des neuen Benutzers, zum Beispiel „RSAprivacy!@“>
   Vollständiger Name = <vollständiger Name des neuen Benutzers, zum Beispiel „DPO-Administrator“>

c. Klicken Sie im Abschnitt **Rollen und Attribute** auf die Registerkarte **Rollen**, + und wählen Sie die Rolle `Data_Privacy_Officers` für den neuen Benutzer aus.

d. Klicken Sie auf **Speichern**.

2. Erstellen Sie ein neues Benutzerkonto für den Analysten mit eingeschränkten Berechtigungen:

a. Klicken Sie in der Ansicht **Administration > Sicherheit** auf die Registerkarte **Benutzer**. Klicken Sie auf der Symbolleiste der Registerkarte **Benutzer** auf +.

Das Dialogfeld „Benutzer hinzufügen“ wird angezeigt.

b. Erstellen Sie das neue Konto mit den folgenden Anmeldeinformationen:

Benutzername = <neuer Benutzername für die Anmeldung, zum Beispiel „NichtprivAnalyst“>
E-Mail = <E-Mail-Adresse des neuen Benutzers, zum Beispiel „NichtprivAnalyst@rsa.com“>
Passwort = <Passwort des neuen Benutzers, zum Beispiel „RSAprivacy!@“>
Vollständiger Name = <vollständiger Name des neuen Benutzers, zum Beispiel „Nicht privilegierter Analyst“>

c. Klicken Sie im Abschnitt **Rollen und Attribute** auf die Registerkarte **Rollen**, + und wählen Sie die Rolle `Analysts` für den neuen Benutzer aus.

d. Klicken Sie auf **Speichern**.

Referenzen zum Datenschutz

Die folgenden Referenzmaterialien sind für das Management des Datenschutzes und der Datenaufbewahrung verfügbar. Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

- Thema **Registerkarte „Datenschutz“** im *Konfigurationsleitfaden für Decoder und Log Decoder*
- Thema **Registerkarte „Datenaufbewahrung“ – Archiver** im *Konfigurationsleitfaden Archiver*
- Thema **Registerkarte „Datenaufbewahrungsplaner“** im *Leitfaden für die ersten Schritte mit Hosts und Services*