RSA NETWITNESS® SUITE

Versionshinweise

für Version 11.0.0.0

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme genannt werden sowie Produktdokumentation, 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.

Verbreitung

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.

Inhalt

Einleitung

In diesem Dokument sind Neuerungen und Änderungen in RSA NetWitness Suite 11.0.0.0 sowie Workarounds für bekannte Probleme aufgeführt. Lesen Sie dieses Dokument vor der Bereitstellung oder Aktualisierung von RSA NetWitness Suite 11.0.0.0.

RSA NetWitness Suite 11.0.0.0 beinhaltet einige der Hauptfunktionen der klassischen Security Analytics-Version sowie Tools für die Erkennung von Advanced Threats, mit denen Analysten auf Sicherheitsbedrohungen erkennen und darauf reagieren können.

Neuheiten

RSA NetWitness Suite 11.0.0.0 bietet deutliche Verbesserungen beim Analyst-Workflow sowie Funktionen, die die Bedrohungsbekämpfung für Analysten aller Erfahrungsniveaus einfacher macht. Administratoren profitieren von einer erweiterten Unterstützung und vereinfachten Wartungsfunktionen für Services und Hosts. NetWitness Suite 11.0.0.0 bietet die folgenden neuen Funktionen und Verbesserungen.

Benutzeroberfläche

Navigation auf Grundlage von Rollen. Die Benutzeroberfläche (UI) ist in fünf grundlegende Funktionsbereiche unterteilt: Reagieren, Untersuchen, Überwachung, Konfigurieren und Admin, was den typischen Security Operation Center-Rollen entspricht. Die Oberfläche wurde modernisiert und bietet einen verbesserten Workflow für Analysten und Threat Hunters. Weitere Informationen zur neuen Navigation und wichtige Tipps zum Kennenlernen von NetWitness Suite 11.0.0.0 finden Sie im Handbuch *Erste Schritte mit NetWitness Suite*.

Reagieren

- **Verbesserte Bedienung für Analysten**. NetWitness-Suite 11.0.0.0 bietet eine neue Möglichkeit zur Verwaltung von Incidents. „Reagieren“ ersetzt Incident Management ab Version 10.6. Weitere Informationen zu „Reagieren“ finden Sie im *NetWitness Reagieren – Benutzerhandbuch*.
- **Neue Ansicht „Reagieren“**. Über die Ansicht „Reagieren“ können Analysten und Incident-Experten den gesamten Umfang eines Incident verstehen und Incidents schnell und effizient selektieren und priorisieren.
- **Konsolidierte Warnmeldungen**. Analysten können alle Warnmeldungen zu Bedrohungen, die von der RSA NetWitness Suite 11.0.0.0 empfangen wurden, an einem zentralen Ort einsehen. Dies kann Warnmeldungen zu ESA-Korrelationsregeln, zu der automatisierten Bedrohungserkennung für ESA, zu Malware Analytics und zum Reporting beinhalten.
- **Liste mit priorisierten Incidents**. Die Incidents-Liste zeigt Analysten die Incidents-Warteschlange an, in der Incidents in der Reihenfolge ihres Schweregrads aufgeführt sind.
- **Hinzufügen verwandter Indikatoren nach Bedarf**. Analysten können hier verwandte Indikatoren suchen und diese einem Incident hinzufügen.

- **Nachverfolgen von Incident-Aufgaben bis zu ihrem Abschluss**. Analysten können Aufgaben innerhalb von Incidents erstellen und alle Aufgaben von einem zentralen Standort aus verwalten.
- **Zusammenarbeiten mit anderen Analysten**. Analysten können Hinweise veröffentlichen und den Verlauf der Aktivitäten zu einem Incident überprüfen.
- **Konsolidierter Incident-Ablauf**. Eine chronologische Liste der Indikatoren (Warnmeldungen) enthält die Ereignisse und Erweiterungen aus verschiedenen Datenquellen.
- **Interaktives Node-Diagramm mit Beziehungen zwischen den Einheiten**. Sie können Drill-downs zu Host- oder Benutzerdetails vornehmen und zur Ansicht „Untersuchen“ wechseln, um eine ausführliche Untersuchung vorzunehmen.
- **Kontextbezogene Informationen in der Ansicht „Reagieren“ nach Bedarf**. Analysten können mithilfe von kontextbezogenen Informationen aus Datenquellen wie Listen, RSA Archer, Active Directory, RSA NetWitness Endpoint, Warnmeldungen, Incidents und Live Connect den Zeitaufwand für die Erkennung und Reaktion reduzieren. Analysten können mit der Maus auf unterstrichene Elemente zeigen, um Kurzinformationen aufzurufen. Diese Kurzinformationen enthalten eine schnelle Übersicht über den Typ der verfügbaren kontextbezogenen Daten für die ausgewählte Einheit und liefern Links zu weiteren Untersuchungsaktionen. Sie können auch auf einen Bereich für Kontextabfragen zugreifen, der detaillierte Kontextinformationen für die ausgewählte Einheit liefert.

Investigate

- **Transparenz von Endpunktdaten**. Wenn NetWitness Suite zur Nutzung von Daten aus RSA NetWitness Endpoint konfiguriert ist, können Analysten die Endpunktdaten in Investigate sehen. Hierbei werden drei Typen von Ereignissen (Netzwerk, Protokoll und Endpunkt) in Investigate zur Verfügung gestellt und alle Ereignisse können auf die gleiche Weise untersucht werden. Weitere Informationen finden Sie im *Ermittlung und Malware-Analyse – Benutzerhandbuch*.
- **Ereignisanalyse**. Die Ereignisanalysefunktion bietet Analysten mehr Möglichkeiten zur Rekonstruktion eines Ereignisses als die Text-, Paket- oder Dateianalyse. Weitere Informationen finden Sie unter „Analysieren von Ereignissen in der Ansicht ‚Ereignisanalyse‘“ im *Ermittlung und Malware-Analyse – Benutzerhandbuch*.

- **Paketanalysefunktionen**.
  - Attribute in der Paketkopf- und -fußzeile im Hexadezimal- und ASCII-Format sind blau hervorgehoben. Wenn Sie den Mauszeiger auf einem hervorgehobenen Attribut platzieren, werden zusätzliche Informationen in einem Popup-Fenster angezeigt.
  - Übliche Dateisignaturen werden durch einen orangefarbenen Hintergrund hervorgehoben. Wenn Sie den Cursor über den hervorgehobenen Text bewegen, wird die Beschreibung des potenziellen Dateityps in einem Popup-Fenster angezeigt.
  - Es gibt vier Optionen für das Herunterladen: das Ereignis als PCAP, alle Nutzlasten, nur Anforderungsnutzlasten oder nur Antwortnutzlasten.
  - Schattierte Darstellung der hexadezimalen Zahlen in der Paketnutzlast, damit Analysten Muster besser erkennen können
  - Möglichkeit, sich nur die Nutzlasten anzeigen zu lassen, indem Paketkopf- und -fußzeilen aus der Ereignisdarstellung entfernt werden
- **Textanalysefunktionen**.
  - Möglichkeit, Protokollereignisse oder Endpunktereignisse in verschiedenen Formaten herunterzuladen
  - Anzeigen von URL- und Base64-Codierung und -Decodierung in einem Popup-Fenster, wenn der Text ausgewählt wird Sie können den ausgewählten Text auch kopieren.
  - Anzeigen von komprimiertem oder nicht komprimiertem Text für eine HTTP-Netzwerksitzung
  - Hervorheben der Metaschlüssel-/Metawert-Paare (ohne Unterscheidung von Groß- und Kleinschreibung) in der Textanalyse
- **Dateianalysefunktionen**. Wenn Sie Dateien herunterladen, werden die Dateien als passwortgeschütztes ZIP-Archiv exportiert. Das Standardpasswort lautet `netwitness`. Das Exportieren der Dateien in diesem Format sorgt dafür, dass sie nicht durch eine Virenschutzsoftware in die Quarantäne verschoben werden. Potenziell schädliche Dateien werden außerdem nicht automatisch von der Standardanwendung geöffnet und ausgeführt.

Reporting

- **Standarddatenquelle für Diagramme**. Die Diagramme werden für eine Standarddatenquelle ausgeführt, wenn keine Datenquelle angegeben ist. Standardmäßig

werden auch alle vorkonfigurierten Dashboards für die Standarddatenquelle ausgeführt, wenn keine Datenquelle angegeben ist.

- **Reporting zu RespondDB**. Sie können Berichte mit „Reagieren“-Daten erstellen und anzeigen, um eine bessere Transparenz während des Erkennungsvorgangs zu erzielen. Alle wichtigen Warnmeldungs- und Incident-Daten sind in der Ansicht „Reagieren“ für das Reporting verfügbar.
- **AutoKorrektur bei der NWDB-Regelsyntax**. Die NWDB-Core-Parser führen eine strenge Validierung der NWDB-Regelsyntax durch (die Abfragesyntax muss gültig sein). Für ein nahtloses Upgrade werden Regeln mit ungültiger Syntax während der ersten Ausführung nach einem Upgrade automatisch korrigiert. Weitere Informationen finden Sie im *Reporting-Benutzerhandbuch für Version 11.0*.

Dashboards

- **Neue vorkonfigurierte Dashboards (OOTB)**. Vorkonfigurierte Dashboards bieten unmittelbare Vorteile für SOC-Manager, Analysten und Systemadministratoren und stehen im Rahmen der NetWitness-Installation zur Verfügung. Die folgenden vorkonfigurierten Dashboards werden mit dieser Version eingeführt:
  - Investigation
  - Vorgänge – Dateianalyse
  - Vorgänge – Protokollanalyse
  - Bedrohung – Malwareindikatoren
- **Erweiterte Funktionalität für Dashboards**. Administratoren können Dashboards ganz einfach über die intuitive Benutzeroberfläche erstellen und verwalten:
  - Sie können die „Top-Werte“ von Investigation und Echtzeitdiagramm-Dashlets mit einem verwandten Dashboard verknüpfen, um detaillierte Informationen anzuzeigen. Eine „Mehr anzeigen“-Option ist im ausgewählten Dashlet verfügbar. Weitere Informationen finden Sie im Handbuch *Erste Schritte mit NetWitness Suite*.
  - Sie können ein Dashlet in Form eines Geomap-Diagramms für einen schnellen Überblick über den geografischen Standort hinzufügen. Der Netzwerkstatus und der Datenverkehr werden angezeigt. Zu den Funktionen von Geomap-Diagrammen zählt das Vergrößern, Verkleinern und Exportieren des Diagramms.
  - Passen Sie das Dashboards durch Hinzufügen, Löschen und Neuanordnen von Dashlets an.

- Aktivieren oder deaktivieren Sie einzelne Dashlets auf Grundlage Ihrer Anforderungen.
- Filtern Sie Diagrammwerte aus dem Dashboard für 24 Stunden oder dauerhaft, wenn Sie einige offensichtliche Werte ausblenden möchten, um sich auf die restlichen Werte zu konzentrieren.
- Konfigurieren Sie das Dashboard-Layout mithilfe der verfügbaren Dashlet-Breiten (1/2,1/3,2/3,1).
- Verwalten Sie Dashboards, indem Sie das gesamte Dashboard konfigurieren und die Einstellungen für „Vergangene Stunden“ und das Aktualisierungsintervall ändern.
- Sehen Sie sich die vergangenen Stunden und die zuletzt aktualisierten Informationen für das Reporting-Dashlet „Diagramme“ an.
- Exportieren oder importieren Sie Dashboards mit abhängigen Einheiten in ein ZIP-Format, um das separate Importieren oder Exportieren von abhängigen Elementen zu vermeiden.

Live

- **Unterstützung für TAXII-Server**. TAXII-Server werden für die Nutzung von STIX-formatierten Bedrohungsinformationen in NetWitness Suite eingesetzt. Die folgenden TAXII-Server sind für die NetWitness Suite geeignet:
  - Hail a TAXII
  - Anomali Limo
  - Soltra Edge
  - OpenTAXII
- **SSL-fähige Server**. Sie können SSL/TLS-Handshake für die TAXII- und Rest-Server aktivieren.
- **Automatische Bereinigung von TAXII-Daten**. Sie können einen Ablaufzeitraum im Feld „STIX-Daten entfernen, die älter sind als“ festlegen, damit die vom TAXII-Server abgerufenen STIX-Pakete, die älter als die angegebene Anzahl an Tagen sind, aus der MongoDB gelöscht werden. Dies begrenzt die Anzahl der veralteten Indikatoren in der NetWitness Suite.
- **Verbesserte Kategorieoberfläche**. Sie können durch die in Live verfügbaren Inhaltskategorien blättern, um herauszufinden, welche Inhalte je nach Anwendungsbeispiel verfügbar sind. Weitere Informationen finden Sie im *Handbuch zum Live-Services-Management*.

Event Stream Analysis und ESA Analytics

- **Ein neuer ESA Analytics-Service (ESA Analytics Server) wurde hinzugefügt**. Es gibt jetzt zwei Services, die auf einem ESA-Host ausgeführt werden können:
  - Event Stream Analysis (ESA-Korrelationsregeln)
  - Event Stream Analytics Server (ESA Analytics) Der ESA Analytics-Service wird zur automatischen Bedrohungserkennung eingesetzt. Weitere Informationen zur automatischen Erkennung von Advanced Threats finden Sie im Handbuch *NetWitness Suite – Automatisierte Bedrohungserkennung* und im Abschnitt „Konfigurieren von ESA Analytics“ im *ESA-Konfigurationsleitfaden*.
- **Für vorkonfigurierte ESA Analytics-Module sind keine Kenntnisse von ESA-Regeln erforderlich**. Bei der automatisierten Bedrohungserkennung stehen derzeit zwei Module zur Verfügung: C2 (Command and Control, Befehl und Kontrolle) für Pakete und C2 für Protokolle.
- **Alle ESA Analytics-Module können an einem zentralen Ort (Admin > System) den Concentrator-Datenquellen zugeordnet werden**. ESA Analytics-Module sind auf Systemebene konfiguriert, damit Sie Bereitstellungen und Updates für Ihre Modulzuordnungen besser verwalten können.
- **Warnmeldungen befinden sich jetzt in der Ansicht „Reagieren“ (Reagieren > Warnmeldungen)**. In der Ansicht „Reagieren“ > „Warnmeldungen“ sind alle von NetWitness Suite empfangenen Bedrohungswarnmeldungen und Indikatoren enthalten. Sie können die Liste der Warnmeldungen nach dem Quelltyp „Event Stream Analysis“ filtern, um nur ESA-Warnmeldungen anzeigen zu lassen. Für Benutzer der Version 10.6 ist die Ansicht „Warnmeldungen“ > „Zusammenfassung“ nicht mehr verfügbar.
- **Eine neue Benutzeroberfläche zum Konfigurieren der Whois-Abfrage wurde hinzugefügt (Admin > System > Whois)**. Analysten sollten die Whois-Abfrage in der NetWitness Suite-Benutzeroberfläche und nicht in der Ansicht „Durchsuchen“ konfigurieren. Nachdem Whois konfiguriert wurde, ist es für alle ESA Analytics-Module verfügbar.
- **Externe ESA-Datenquellenverbindungen erfordern jetzt TLSv1.2**. Aus Sicherheitsgründen erfordern interne und externe Verbindungen in NetWitness Suite 11.0.0.0 jetzt TLSv1.2. Bei Verwendung einer externen Datenquelle wie z. B. MS SQL Server, MongoDB, MySQL und Postgres für Ihre Erweiterungsdaten (Konfigurieren >

ESA-Regeln > Einstellungen) müssen Sie sicherstellen, dass Ihr Datenquellenserver TLSv1.2-konform ist.

Core-Services

- **Neue Services**. Die folgenden Services werden mit NetWitness-Suite 11.0.0.0 eingeführt. Weitere Informationen finden Sie im *Leitfaden zu Hosts und Services*:
  - **Admin-Server**. Der NetWitness Administration Server ist der Back-end-Service für administrative Aufgaben in der NetWitness-Benutzeroberfläche (UI). Er abstrahiert die Authentifizierung, das Management von globalen Einstellungen und die Autorisierungsunterstützung für die Benutzeroberfläche.
  - **Configuration Server**. Der NetWitness Configuration Server übernimmt das Speichern und Bearbeiten von Konfigurationssammlungen. Eine Konfigurationssammlung ist eine logische Konfigurationsgruppierung, die selbstständig verwaltet werden kann.
  - **Orchestration Server**. Der NetWitness Orchestration Server ist verantwortlich für das Provisioning, Installieren und Konfigurieren aller Services, die eine NetWitness-Bereitstellung bilden. Er dient der Abstrahierung der Plattformbereitstellungslogik aus den NetWitness-Services selbst.
  - **Security Server**. Der NetWitness Security Server verwaltet die Sicherheitsinfrastruktur einer NetWitness-Bereitstellung. Er ist zuständig für alle sicherheitsbezogenen Aspekte, einschließlich:
    - Benutzer und Authentifizierungskonten
    - Rollenbasierte Zugriffskontrolle
    - Bereitstellung der PKI (Public Key Infrastructure)
  - **Investigate Server**. Der NetWitness Investigate Server ist verantwortlich für die Untersuchungen.
  - **Respond Server**. Der Respond Server ersetzt den Incident Management-Service.
- **Entschlüsselung der eingehenden Pakete bei einem Decoder**. Der Befehl `sslKeys` unterstützt das Hochladen privater Chiffrierschlüssel in einen Decoder, um eingehende Pakete vor dem Parsing-Schritt zu entschlüsseln, sodass aktivierte Parser die unverschlüsselte Paketnutzlast sehen und Metadaten entsprechend erstellen können.

Weitere Informationen finden Sie im *Konfigurationsleitfaden für Decoder und Log Decoder*.

- **Erweiterte Parseroptionen**: `decoder/parsers/config/parsers.option`. Dieser Konfigurations-Node besteht aus einer Reihe von Zeichenfolgeparametern, wobei dem Parser eine Optionsliste in Form von name = „Wert“-Paaren übergeben wird. Der neue Konfigurations-Node kann vom nativen Entropy Parser und den Lua-Parsern verwendet werden. Weitere Informationen finden Sie im *Tuningleitfaden für die Core-Datenbank*.
- **Parser, die ihren Zweck nicht mehr erfüllen, wurden aus den Decodern entfernt**. Die unten genannten älteren, integrierten Parser wurden aus den Decodern entfernt.
  - Diese nativen Parsern wurden aus den Decodern entfernt, da sie ihren Zweck nicht mehr erfüllen: LotusNotes, MSN, SAMETIME, YMSG, AIM, Net2Phone, YCHAT und WEBMAIL.
  - Die nativen AIM-Parser wurden entfernt, da jetzt AIM_Lua diese Funktion abdeckt.
  - Der WebMail-Parser wurde entfernt, da er nicht mehr relevant ist und WebMail verschlüsselt ist. Es gibt keinen Lua-Ersatz. Die Funktion des WebMail-Parsers bestand darin, den HTML-Code von Gmail, Yahoo und Hotmail zu analysieren und interessante Metadaten herauszuziehen. Die Anbieter dieser WebMail-Anwendungen ändern ihren HTML-Code aber so oft, dass der Parser seinen Zweck nicht mehr erfüllt.
- **Neuer nativer Entropy Parser**. Der Entropy Analyzer analysiert alle Netzwerksitzungen nativ auf dem Decoder, um Entropie-bezogene Werte zu berechnen. Das Ergebnis sind mehrere Zahlen, die Einblicke darin bieten, ob Datenverkehr verschlüsselt oder komprimiert ist oder einer erwarteten Byteverteilung entspricht. Entropie ist eine Messgröße für die Zufälligkeit von Daten. Ein hoher Entropiewert bei einer Anforderung oder Antwort deutet darauf hin, dass der Datenverkehr wahrscheinlich verschlüsselt oder komprimiert ist und dass eine Netzwerksitzung versucht, Informationen zu verbergen. Weitere Informationen finden Sie unter „Konfigurieren des nativen Entropy Parser“ im *Konfigurationsleitfaden für Decoder und Log Decoder***.**
- **Neuindexierung im Hintergrund, während der Core-Service online ist**. Im normalen Betrieb werden Änderungen an der Indexkonfiguration nur auf neue Daten angewendet, die zur Sammlung hinzukommen. Die Neuerstellung des Index für alle Daten in der Sammlung ist ein zeitaufwendiger Prozess, da der gesamte Metadatenbank-Speicher von der Festplatte gelesen werden muss. Ab Version 11.0.0.0 ist es möglich, den Index neu zu erstellen, während der Core-Service online ist. Version 11.0.0.0-Services erstellen immer dann Indizes im Hintergrund, wenn sie feststellen, dass ein Teil der Sitzungs- und

Metadatenbanken nicht indiziert ist. Weitere Informationen finden Sie im *Tuningleitfaden für die Core-Datenbank*.

- **Validierung der Service-Indexkonfigurationsdateien vor dem Speichern oder Neustart**. Eine strenge Prüfung der Indexdateien mit einer Validierung aller Elemente und Attribute erfolgt, wenn die Dateien gespeichert werden und der Service gestartet wird. Wenn Sie versuchen, eine Index-Konfigurationsdatei zu speichern, die nicht ordnungsgemäß formatiert ist, wird sie abgelehnt: Eine entsprechende Meldung wird in der Benutzeroberfläche angezeigt und die Datei wird nicht gespeichert. Eine strenge Überprüfung erfolgt ebenfalls, wenn ein Service gestartet wird. Zur Vermeidung von Problemen beim Upgrade von 10.x werden die Fehler jedoch als Warnungen ausgegeben. Wenn Sie versuchen, eine Indexdatei mit protokollierten Warnungen in der Benutzeroberfläche zu bearbeiten, ist das Speichern der Indexdatei erst dann möglich, wenn die Probleme behoben sind.
- **Neue inhaltsbezogene CPU-Auslastungsstatistiken.** Ab dieser Version bietet der Decoder CPU-Auslastungsstatistiken für alle installierten Inhalte. Die neue CPU-Auslastungsüberwachung zeigt, wie viel CPU-Zeit von Parsern, Feeds, Anwendungsregeln und lexikalischer Überprüfung verwendet wird. Die Statistiken werden als Stat-Nodes in der Servicestruktur der Ansicht „Explorer“ angezeigt, wenn `/decoder/parsers/config/detailed.stats` aktiviert ist und der Decoder Statistiken erfasst. Jedes Inhaltselement wird als einzelner Prozentwert (0-100) berücksichtigt, unabhängig von der Anzahl der ausgeführten Parse-Threads. Der Prozentsatz spiegelt die durchschnittliche CPU-Auslastung für den Inhalt über alle Threads hinweg wider.
- **Verbesserte RBAC-Funktion**. In RSA Security Analytics 10.6 war die Role-Based Access Control (RBAC, rollenbasierte Zugriffskontrolle) für den Befehl `/sdk packets` je nach Benutzer entweder aktiviert oder deaktiviert. Für Benutzer mit eingeschränkten Berechtigungen wurde der Zugriff in der Regel nicht zugelassen, sodass die pcap-Erstellung aus Investigation selbst in Sitzungen ohne Einschränkungen nicht möglich war. In RSA NetWitness Suite 11.0.0.0 funktioniert die RBAC nur noch paketbezogen. Sitzungen mit Einschränkungen werden während der pcap-Erstellung in Investigate einfach übersprungen. In Sitzungen, die zulässig sind, werden Pakete zurückgegeben. Weitere Informationen über die RBAC finden Sie im Handbuch *Systemsicherheit und Benutzerverwaltung*.
- **Neue Möglichkeit zur Analyse von komprimierten Websitzungen**. Decoder können zusätzliches Parsing von HTTP-Sitzungen mithilfe der Lua-Parsersprache durchführen.

Lua-Parser können die Dekomprimierung einzelner Komprimierungsinstanzen in einer HTTP-Sitzung anfordern. Dies ist eine ähnliche Funktionalität, wie sie die früheren Flex-Parser geboten haben.

- **Verbesserte Handhabung von Abfragetimeouts**. Für das Ablaufen von RESTful-Abfragen wurde das Standardverhalten auf „unbegrenzt“ geändert, sodass die normalen Prozesse zum Abbruch von Abfragen gelten. Da es keinen REST API-Sitzungsablauf mehr gibt, ist jetzt der Ablaufzeitpunkt der Einstellung `query.timeout` in der Benutzersitzung ausschlaggebend für Abfragetimeouts.
- **Decoder-Erfassung von VLANs auf mehreren Netzwerkschnittstellen mit „packet_mmap“**. Es ist jetzt möglich, eine beliebige Teilmenge von Erfassungsschnittstellen auszuwählen, indem Sie dem Konfigurationsparameter `/decoder/config/capture.device.params` eine entsprechende Konfiguration hinzufügen. Weitere Informationen finden Sie unter „Konfigurieren von Erfassungseinstellungen“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.
- **Paketerfassung von F5 BIG-IP VE in AWS**. Wenn Sie einen Decoder für die Clouderfassung bereitstellen möchten, kann der Administrator ihn so konfigurieren, dass er mithilfe der F5 BIG-IP Virtual Edition Netzwerkdaten aus der AWS-Cloudinfrastruktur aufnehmen kann.
- **Vergleich der Metaschlüssel in Anwendungsregeln**. In Anwendungsregeln in Decodern können die Werte für verschiedene Metaschlüssel in einer Sitzung verglichen werden. Metaschlüssel können nun auf der rechten Seite der binären Operatoren verwendet werden. Unterstützte Operatoren umfassen die relationalen Operatoren (`=, !=,<, <=, >, >=`) sowie `contains`, `begins`, `ends`, `count`, `ucount` und `length`. Weitere Informationen finden Sie unter „Regelerfassungssyntax“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.
- **Verbesserung der Regeln und Abfragesprache für relative Zeiträume**. Mit relativen Zeitpunkten kann eine `where`-Klausel auf einen Wert mit einem bestimmten Versatz von den frühesten oder spätesten Zeit-Metaelementen in der Sammlung verweisen. Weitere Informationen zur Abfragesyntax finden Sie im *Tuningleitfaden für die Core-Datenbank*.
- **Verbesserte Protokolltextindexierung**. Es wurde ein Basisniveau für das Protokollparsing definiert, damit der Text aller nicht analysierten Protokolle auf diese wichtigen Einheitenelemente gescannt wird, auch wenn kein Parser aktiviert ist: syslog-Zeitstempel, RFC 3339-Zeitstempel, IP-Adressen, E-Mail-Adressen, URL-Komponenten und Domainnamen. Jedes Element, das als ein solcher Datentyp identifiziert werden kann, wird automatisch mit dem entsprechenden Metaelement gekennzeichnet.
- **Möglichkeit, den Netzwerkstream aus mehreren Sitzungen rekonstruieren**.

Verbessert die Kombination geteilter Sitzungen. Der Decoder überwacht den Netzwerkstream, solange es die Arbeitsspeicherressourcen zulassen. Wenn in einem Netzwerkstream mehr Pakete eingehen, fügt der Decoder den nachfolgenden Sitzungen „split“-Metaelemente hinzu. Durch eine Kombination aus den „split“-Metaelementen und dem Streamschlüssel ist es möglich, den Netzwerkstream aus mehreren Sitzungen rekonstruieren.

Sicherheit

- Zertifizierungsstellen für Zwischenzertifikate werden jetzt unterstützt.
- Verbessertes Sicherheitskonzept
- FIPS ist standardmäßig für alle Services aktiviert, mit Ausnahme von Log Collector und Log Decoder. FIPS kann für keinen Service deaktiviert werden, mit Ausnahme von Log Collector, Log Decoder und Decoder.
- Die FIPS 140-2-zertifizierten Verschlüsselungsmodule sind für alle Services aktiviert, die kryptografische Vorgänge ausführen. Für die folgenden Services wird die Verwendung von FIPS Cipher Suites nicht erzwungen, auch wenn das FIPS-Verschlüsselungsmodul genutzt wird:
  - NTP: UDP-Port 123
  - TCP: SSH-Port 22
  - TCP: Loopback-Port 8000 der Salt-API
  - CollectD
  - Log Collector
  - Log Decoder

  Hinweis: Standardmäßig ist bei Core-Geräten, bei denen in 10.6.4 der FIPS-Durchsetzungsmodus nicht aktiviert war, dieser auch nach einem Upgrade auf 11.0.0.0 nicht aktiviert. Dies wirkt sich auf die Log Decoder-, Log Collector- und Packet Decoder-Services aus.

Plattform

- **Einfachere 10G-Decoder-Konfiguration**. Sie können die Decoder- und pfring-RPMs getrennt und in beliebiger Reihenfolge installieren. Die Reihenfolge, in der die RPMs

installiert werden, spielt keine Rolle. Der Decoder kann den 10G-Adapter suchen und mit der Erfassung starten.

Administration

- **Optimierte Performance und Skalierbarkeit** der NetWitness Suite durch folgende Verbesserungen:
  - Schnelleres Host- und Service-Provisioning
  - Externe YUM-Repository-Funktion mit der Möglichkeit zur schnellen Installation der Software
  - Drittanbieter- und NW-Services wurden entkoppelt, um Scale-out-Optionen in zukünftigen Versionen bereitzustellen.
- **Vereinfachter Prozess für die Erstellung und Wartung von Services und Hosts**. Mehrere Hosts können über die Befehlszeile oder Benutzeroberfläche gleichzeitig bereitgestellt werden.
- **Zusätzliche Unterstützung für extern gemanagte YUM-Repositories**. Unterstützung für extern gemanagte YUM-Repositories.

Protokollanalyse

Ereignisquellenerkennung. Die Ereignisquellenerkennung verbessert die Protokollanalysegenauigkeit und bietet einen Workflow zum Finden und Korrigieren von Ereignisquellen, die nicht vollständig oder korrekt erkannt wurden, einschließlich:

- Zentrale Übersicht über alle Ereignisquellen
- Details zu jeder Ereignisquelle
  - Typen der erkannten Ereignisquellen
  - Wahrscheinlichkeit, dass der Ereignisquellentyp nicht richtig identifiziert wurde
  - Ermöglicht es Administratoren, problematische Ereignisquellen zu finden
- Details zu jeder Ereignisquelle und jedem Ereignisquellentyp
  - Protokolle für jeden Ereignisquellentyp
  - Importierte oder festgelegte Attribute
  - Ermöglicht Administratoren, festzustellen, ob die Ereignisquelle korrekt ist
- Möglichkeit zur Bestätigung oder Festlegung der richtigen Ereignisquellentypen

- Im Dialogfeld „Parser-Zuordnungen verwalten“ können Administratoren ausgewählten IP-Adressen die geeigneten Parser zuweisen.

Context Hub

- **Neue Datenquellen wurden hinzugefügt**
  - **RSA Archer**. Daten zur Asset-Bedeutung aus RSA Archer dienen zur Priorisierung von Sicherheitsereignissen basierend auf den geschäftlichen Auswirkungen und zur Abwehr der gefährlichsten Bedrohungen. Der Analyst kann anhand dieser Bewertung agieren. Weitere Informationen finden Sie im *Context Hub-Konfigurationsleitfaden*.
  - **Active Directory**. Identitätsinformationen aus Active Directory werden von Analysten verwendet, um die Erkennung und Reaktion in Bezug auf einen bestimmten Benutzer zu beschleunigen. Diese Informationen können für weitere benutzerbezogene Untersuchungen verwendet werden.
  - **Listen mit mehreren Spalten**. Analysten können kontextbezogene Informationen sehen, wenn eine Liste als Datenquelle konfiguriert ist. Wenn der Analyst z. B. über eine Blacklist mit IP-Adressen verfügt, kann er sie als Datenquelle mit einer oder mehreren Spalten konfigurieren. Danach können die kontextbezogenen Daten für die importierten Daten in den Ansichten „Reagieren“ und „Untersuchen“ abgerufen und angezeigt werden. Basierend darauf können weitere Aktionen durchgeführt werden können.
- **Inline-Kontextanzeige**. Eine schnelle Übersicht über Kontextdaten für Analysten, damit sie Metadaten für die weitere Untersuchung in der Node- und Ereignisansicht der Ansicht „Reagieren“ auswählen können. Diese Option ist verfügbar, wenn der Benutzer mit der Maus auf die entsprechenden Metadaten zeigt. Außerdem können Analysten hierüber zu Investigate und zu Endpoint wechseln und Elemente der Liste hinzufügen/aus ihr entfernen.
- **Bereich „Kontextabfrage“**. Kontextbezogene Informationen für die konfigurierten Datenquellen werden für die Analysten angezeigt, damit sie weitere Aktionen zur Untersuchung durchführen können.
- **Domain- und Datei-Hash-Abfrage**. Analysten können hier Abfragen durchführen, um neben den IP-Adressen Domains und Datei-Hashes im Context Hub zu suchen und erweiterten Kontext für verschiedene Indikatortypen während einer Untersuchung zu erhalten.
- **Risikoindikatortags**. Zusätzlich zur Live Connect-Suche können Analysten erweiterte Risikoinformationen (Risikobewertung und Risikogrund) abrufen. Dies umfasst das Risiko der Indikatoren und den Grund für die aktuelle Bewertung. Darüber hinaus sind neue Attribute für

die einzelnen Indikatortypen verfügbar:

- IP-Adresse
  - Identität (ASN, eingetragenes Land und Unternehmen)
  - Zugehörige Dateien und Domains
- Domain
  - Identität (WHOIS-Information: Name des Registrierten, Unternehmen, Adresse, E-Mail usw.)
  - Zugehörige IP-Adressen und Dateien
- Datei-Hash
  - Identität (Dateiname, Größe, Beschreibung, MD5, SHA1 und Datum/Uhrzeit der letzten Änderung)
  - Zertifikatsinformationen (Aussteller, Start- und Ablaufdatum, Signaturinformationen, Betreff usw.)
  - Zugehörige IP-Adressen und Domains

- **Feedback zur Live Connect-Risikobewertung**. Analysten können Feedback basierend auf ihrer Tier-Stufe, der Wahrscheinlichkeit und den Risikoindikatoren bereitstellen. Darüber hinaus können sie erweitertes Feedback zu einem Indikator in Live Connect angeben. Das Feedback besteht aus: Risikoindikatortags (Kontext dazu, wieso ein Indikator verdächtig ist), Wahrscheinlichkeit, Risikostatus und Analyst-Tier (Kontext dazu, wie ein Indikator erkannt oder selektiert wurde). Weitere Informationen finden Sie im Benutzerhandbuch zu NetWitness „Reagieren“.

Hinweise zum Upgrade

Die folgenden Upgradepfade werden für RSA NetWitness Suite 11.0.0.0 unterstützt:

- RSA NetWitness Suite 10.6.4.x auf 11.0.0.0

Weitere Informationen zum Upgrade auf 11.0.0.0 finden Sie in den Aktualisierungsanweisungen im Abschnitt Produktdokumentation.

Behobene Probleme

In diesem Abschnitt werden die Probleme aufgeführt, die seit der letzten -Hauptversion behoben wurden.

Serverkorrekturen

Rückverfolgungsnummer	Beschreibung
SATCE-1477/ASOC-24080	CEF-Parser-Umschaltflächeneinstellungen werden gelöscht, wenn die Parser-Einstellungen auf der Benutzeroberfläche geändert werden.
SACE-7121/ASOC-30636	Benutzerdefinierte Feeds mit CSV-Inhalt entsprechen nicht den Metawerten und Anführungszeichen werden nicht korrekt angezeigt.

Integritäts- und Zustandskorrekturen

Rückverfolgungsnummer	Beschreibung
ASOC-9225	Fehler „Seite kann nicht angezeigt werden“ bei der Anmeldung mit dem IE 10-Browser
SACE-6720	Auf der Seite „Monitoring“ werden alle Filter entfernt.

Problembehebungen beim Log Collector-Service

Rückverfolgungsnummer	Beschreibung
SAENG-2476	Wiederholte Fehlermeldungen werden angezeigt, falls der Domainname nicht auf dem LWCS-Computer aufgelöst werden kann.
ASOC-9586	Falsche Meldung für AWS-Sammlungsfehler erzeugt
ASOC-26826	Filterkonfiguration für Dateisammlung funktioniert nicht.

Problembehebungen bei Event Stream Analysis

Rückverfolgungsnummer	Beschreibung
ASOC-6633	Konfiguration der Testregeln: Out-of-Bound-Werte werden begrenzt.

Core-Korrekturen

Zu den Core-Services zählen Broker, Concentrator, Decoder und Log Decoder.

Rückverfolgungsnummer	Beschreibung
ASOC-18044	Metacallback-Feeds unterstützen keine Wertebereichindizes (IP-Bereich oder CIDR)

Nicht unterstützte Funktionen

Die folgenden Tabellen enthalten Informationen zu Funktionen, die in RSA NetWitness Suite 11.0.0.0 oder späteren Versionen nicht mehr unterstützt werden.

In 11.0.0.0 oder späteren Versionen nicht unterstützte Funktionen

Nr.	Funktion	Hinweise
1	Malware Colo	Malware-Colocation wird in 11.0.0.0 und späteren Versionen nicht unterstützt. Malware Analysis wird als eigenständige Malware Analysis-Instanz unterstützt.
2	All-in-One(AIO)-Bereitstellung	Die All-in-One-Bereitstellung wird nicht unterstützt. Die Neuinstallation von AIO wurde entfernt.
3	Eigenständigen Warehouse Connector auf Decoders	Warehouse Connector ist nicht standardmäßig auf Decoders und Log Decoders installiert. Warehouse Connector muss nach der Konfiguration des Decoder installiert und konfiguriert werden.
4	Verwaltungsfunktionen	1. Eigenes Passwort vergessen 2. E-Mail-Benachrichtigung an Benutzer, wenn das Passwort abläuft 3. Eine Änderung des Anmeldebanners wird nicht unterstützt. 4. AD-Benutzertest/-suche
5.	Pivotal	Pivotal wird nicht unterstützt. Unterstützung für HortonWorks wird bereitgestellt.

In zukünftigen Versionen verfügbare Funktionen

Die folgenden Funktionen sind nicht in 11.0.0.0 verfügbar und werden in zukünftigen Versionen zur Verfügung stehen.

Nr.	Funktion	Hinweise
1	IPDB-Reporting	Der IPDB Extractor-Service wird in 11.0.0.0 nicht unterstützt und in späteren Versionen verfügbar sein.
2	STIG	Wenn Sie über einen sicherheitsverstärkten STIG-Host verfügen, können kein Upgrade auf Version 11.0.0.0 durchführen, da die Backupskripte dies nicht unterstützen.
3	Unterstützung für mehrere Security Analytics-Server (NetWitness-Server)	Eine Bereitstellung mit mehreren Servern wird nicht unterstützt.
4	PKI-Authentifizierung	Die PKI-Authentifizierungsfunktion ist in Version 11.0.0.0 nicht verfügbar.
5	Warehouse Analytics	Warehouse Analytics wird für Version 11.0.0.0 nicht unterstützt, aber in späteren Versionen verfügbar sein.

Bekannte Probleme

In diesem Abschnitt werden Probleme beschrieben, die in dieser Version fortbestehen. Sofern ein Workaround oder eine Problembehebung verfügbar ist, werden ausführliche Anmerkungen bzw. Verweise eingefügt.

Bekannte Probleme während des Upgrades auf Version 11.0.0.0

Die folgenden bekannten Probleme treten während eines Upgrades von Version 10.6.x auf Version 11.0.0.0 auf:

Offlinelizenzen werden nach einem Upgrade von 10.6.4.x auf 11.0.0.0 nicht beibehalten.

Rückverfolgungsnummer: ASOC-41757

Problem: Selbst wenn Sie eine neue Antwort-BIN-Datei von Download Central hochgeladen haben, funktionieren Offlinelizenzen immer noch nicht. Obwohl alte Dateien `/var/lib/fneserver` wiederhergestellt sind, bleiben die Lizenzen weiterhin deaktiviert.

Workaround: Führen Sie zum Wiederherstellen der Lizenzen die folgenden Schritte aus:

1. Erzeugen Sie eine neue Antwort-BIN-Datei von Download Central.
2. Melden Sie sich bei NetWitness Server 11.0.0.0 (AdminServer) an.
3. Verschieben Sie RA*-Dateien (3 Dateien) aus `/var/lib/fneserver/`.
4. Melden Sie sich bei der RSA NetWitness 11.0.0.0-Benutzeroberfläche mit Administratorbenutzeranmeldedaten an und navigieren Sie zur Registerkarte „Admin > System > Lizenzierung > Übersicht“.
5. Klicken Sie unter „Lizenzierungsaktionen“ auf „Lizenzen aktualisieren“.
6. Laden Sie jetzt die Antwortdatei, die Sie von Download Central erhalten haben, unter „Admin > System > Lizenzierung > Registerkarte „Einstellungen“ > Antwort hochladen“ hoch.

Hinweis: Ein Upgrade mit dem Onlinemodus (RSA NetWitness Suite 11.0.0.0 mit Internetverbindung) funktioniert erfolgreich und alle Lizenzen werden nach dem Upgrade auf 11.0.0.0 wiederhergestellt.

Benutzer- oder Rollenattribute zum Einschränken des Datenzugriffs durch ein Abfragepräfix werden nicht unterstützt.

Rückverfolgungsnummer: ASOC-42734

Problem: Wenn Sie Benutzer- oder Rollenattribute zum Einschränken des Zugriffs auf Daten über ein Abfragepräfix in 10.6.4.x konfiguriert haben und ein Upgrade auf 11.0 durchführen, funktioniert die Funktion nicht.

Workaround: Sie müssen den RSA NetWitness Suite-Patch 11.0.0.1 anwenden, um diese Konfiguration zu korrigieren.

Nach einem Upgrade auf 11.0 können sich mit Active Directory konfigurierte Benutzer nicht bei der NetWitness-Suite-Benutzeroberfläche anmelden.

Rückverfolgungsnummer: ASOC-42738

Problem: Wenn Sie Active Directory-Benutzer für externe Benutzeranmeldungen bei 10.6.4.1 oder früher konfiguriert haben und ein Upgrade auf 11.0 durchführen, können sich diese Benutzer nicht bei der NetWitness Suite-Benutzeroberfläche anmelden.

Workaround: Führen Sie einen der folgenden Schritte aus:

- Wenden Sie vor dem Upgrade auf 11.0.0.0 den Patch 10.6.4.2 an.
- Wenn der Patch 10.6.4.2 aus irgendeinem Grund nicht angewendet wurde, wenden Sie den Patch 11.0.0.1 an und führen Sie dann die externe Authentifizierungsmigration durch.

Fehlgeschlagene Benutzeranmeldung

Rückverfolgungsnummer: ASOC-43523

Problem: Benutzer können sich nach der Installation von 11.0.0.0 oder einem Upgrade auf 11.0.0.0 nicht bei der NetWitness Suite-Benutzeroberfläche anmelden. Der Grund ist, dass die Benutzeroberfläche keine Benutzerkontoinformationen von MongoDB abrufen kann.

Workaround: Wenden Sie den RSA NetWitness Suite-Patch 11.0.0.1 an.

Nach einem Upgrade auf 11.0.0.0 können in einer Bereitstellung mit gemischten Modi keine neue Ereignisquellen hinzugefügt werden.

Rückverfolgungsnummer: ASOC-41867

Problem: Nach einem Upgrade auf 11.0.0.0 und der Herstellung der Verbindung mit Log Collectors der Version 10.6.4 schlagen Testverbindungen auf der Benutzeroberfläche zum Bearbeiten fehl. Der Grund ist, dass die Benutzeroberfläche den Wert für das Startdatum der Sammlung (int) in das Zeichenfolgendatumsformat „1970-01-01 00:00:00“ konvertiert. Sie werden weiterhin Ereignisse aus der vorhandenen Ereignisquelle erfassen, können aber keine neue Ereignisquelle hinzufügen. Im Fall einer Massentestverbindung werden alle Werte jedoch direkt von der REST-Schnittstelle abgerufen und „Verbindung testen“ wird erfolgreich bestanden.

Workaround: Verwenden Sie die REST-Schnittstelle, um eine neue Ereignisquelle in einem gemischten Modus hinzuzufügen.

FIPS wird standardmäßig für den Log Collector-Service deaktiviert.

Rückverfolgungsnummer: ASOC-41841

Problem: FIPS wird standardmäßig für den Log Collector-Service deaktiviert, selbst wenn FIPS in 10.6.4 aktiviert war.

Hinweis: Selbst wenn FIPS in 10.6.4 aktiviert ist, wird es nach der Migration deaktiviert.

Workaround: Führen Sie zum Aktivieren von FIPS auf dem Log Collector-Service die folgenden Schritte aus:

1. Beenden Sie den Log Collector-Service.
2. Öffnen Sie die Datei `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`.
3. Ändern Sie den Wert der folgenden Variable zu **off**, wie hier beschrieben: zu

   `Environment="OWB_ALLOW_NON_FIPS=on"`

   in

   `Environment="OWB_ALLOW_NON_FIPS=off"`
4. Laden Sie den System-Daemon neu, indem Sie den Befehl `systemctl daemon-reload` ausführen.
5. Starten Sie den Log Collector-Service neu.
6. Legen Sie den FIPS-Modus für den Log Collector-Service in der Benutzeroberfläche fest:

   Hinweis: Dieser Schritt ist nicht erforderlich bei einem Upgrade, wenn FIPS in 10.6.4 aktiviert war.

   a. Navigieren Sie zu „ADMIN > Services“.

   b. Wählen Sie den Log Collector-Service aus und navigieren Sie zu „Ansicht > Konfigurieren.

   c. Aktivieren Sie im SSL FIPS-Modus das Kontrollkästchen im Bereich „Konfigurationswert“ und klicken Sie auf **Anwenden**.

   Hinweis: Legen Sie zum Aktivieren des Log Decoder und Packet Decoder in `/sys/config` die Option `ssl.fips` auf „ON“ fest und starten Sie den Service neu.

Die Investigation-Links sind für statische Diagramme deaktiviert.

Rückverfolgungsnummer: ASOC-42136

Problem: Der Investigation-Link ist für das statische Diagramm (das Ergebnis des Berichts weist das Diagrammformat auf) deaktiviert, in dem die Datenquelle als NetWitness Suite-Broker vorhanden ist (dieser Service ist standardmäßig verfügbar).

Workaround: Für dieses Problem gibt es zwei Workarounds:

- Die Regeln, die das Ergebnis als statisches Diagramm festlegen, können im tabellarischen Format angezeigt werden und Investigation funktioniert wie erwartet.

- Oder Sie können die folgenden Schritte durchführen, um das Problem zu beheben:
  1. Löschen Sie den NetWitness Suite-Broker und fügen Sie ihn mit demselben Namen erneut als Datenquelle zur Reporting Engine hinzu.
  2. Wenn die Berichte mit statischem Diagramm geplante Berichte sind, funktioniert der Investigation-Link bei der nächsten Ausführung wie erwartet.
  3. Wenn der Bericht ein Ad-hoc-Bericht ist, führen Sie den Bericht erneut aus, um die Investigation-Links abzurufen.

Installationsfehler auf Benutzeroberfläche nach Orchestrierung von Warehouse Connector oder Aktualisierung von 11.0 auf 11.0.0.1 für Instanz von Log Collector/Log Decoder

Problem: In einer Instanz von Log Collector/Log Decoder, wenn WC orchestriert oder

von 11.0 auf 11.0.0.1 aktualisiert wird, kann der Status in der Konsole als fehlgeschlagen angezeigt werden und ein Fehler wird

auf der Benutzeroberfläche angezeigt.

Workaround: Anweisungen zum Beheben dieses Problems finden Sie in diesem Wissensdatenbank-

Artikel: https://community.rsa.com/docs/DOC-84635.

Warehouse Connector ist auf Decoders nicht installiert.

Problem: Warehouse Connector ist standardmäßig nicht auf Decoders installiert.

Workaround: Wenn nach einem Upgrade die Notwendigkeit besteht, eine Warehouse-Verbindung erneut herzustellen, wird ein Dienstprogramm für die erneute Installation des Service bereitgestellt. Das Dienstprogramm wird während der Bootstrap-Phase bereitgestellt. Zum Installieren von Warehouse Connector müssen Sie den folgenden Befehl ausführen und den Host nach ID (--host-id), Name (--host-name) oder Adresse (--host-addr) angeben. Standardmäßig wird die neueste verfügbare Version installiert, es sei denn, eine bestimmte Version wird mit „--version“ angegeben. Führen Sie zum Installieren von Warehouse Connector auf einem Host den folgenden Befehl auf dem Admin-Server aus:

```
[root]warehouse-installer --host-id <uuid of the host>
Details about the command:
Location: /usr/bin
Utility Name: warehouse-installer
```

Nutzung:

```
[root@nw11pds5 bin]# warehouse-installer --help
Warehouse Connector Installer
warehouse-installer [options]
Install options:
--host-id <id> Specify host to install (by ID)
```

```
--host-name <name> Specify host to install (by name)
--host-addr <address> Specify host to install (by address)
--version <#.#.#.#> Install version (defaults to latest)
General options:
-v, --verbose Enable verbose output
```

Metaschlüssel für Investigation und Suche wurden zur Standard-Concentrator-Indexdatei hinzugefügt.

Rückverfolgungsnummer: ASOC-22338, ASOC-22895, ASOC-19406

Problem: Wenn Sie die folgenden Metaschlüssel als benutzerdefiniert zur Datei index-concentrator-custom.xml hinzugefügt haben, wurden diese nach dem Upgrade möglicherweise entfernt und es ist jetzt ein Standard-Metaschlüssel in der Datei index-concentrator.xml vorhanden. Es gibt folgende Metaschlüssel: direction, netname, ioc, eoc, boc, analysis.file, analysis.session, analysis.service, inv.category, inv.context.

Workaround: Entfernen Sie die aufgelisteten Schlüssel aus der Datei index-concentrator-custom.xml.

Duplizierte Dashboards für Bedrohungsindikatoren

Rückverfolgungsnummer: ASOC-41701

Problem: Das Dashboard „Bedrohung – Indikatoren“ wurde aktualisiert, um Berichte mit neuen Suchmetaschlüsseln bereitzustellen, und in „Bedrohung – Malwareindikatoren“ umbenannt. Nach dem Upgrade werden beide in der Benutzeroberfläche angezeigt, statt das alte zu ersetzen.

Workaround: Aktivieren Sie die Berichtsdiagramme und das Dashboard „Bedrohung – Malwareindikatoren“ und deaktivieren Sie das alte Dashboard „Bedrohung – Indikatoren“.

Nach dem Upgrade sind die benutzerdefinierten Integritäts- und Zustandsrichtlinien für den Context Hub-Server nicht verfügbar.

Rückverfolgungsnummer: ASOC-41826

Problem: Wenn Sie ein Upgrade auf NetWitness Suite 11.0.0.0 durchführen sind die für den Context Hub-Server konfigurierten benutzerdefinierten Integritäts- und Zustandsrichtlinien nicht verfügbar.

Workaround: Sie müssen diese benutzerdefinierten Richtlinien in 11.0.0.0 definieren.

Beim Upgrade auf 11.0 werden in Sammlungen, die auf einer Workbench in 10.4 erstellt wurden, leere Werte für Datumsbereich und Erstellungsdatum angezeigt.

Rückverfolgungsnummer: ASOC-9035

Problem: Alle Sammlungen, die von einer Workbench in Version 10.4 aus erstellt wurden, zeigen leere Werte für Datumsbereich und Erstellungsdatum an, nachdem ein Upgrade auf 11.0.0.0 durchgeführt wurde.

Workaround: Keiner.

Nach dem Upgrade kann das Geomap-Dashlet nicht mithilfe eines vorkonfigurierten Diagramms (OOTB) erstellt werden.

Rückverfolgungsnummer: ASOC-41896

Problem: Wenn Sie ein Upgrade auf NetWitness Suite 11.0.0.0 durchführen, kann das Geomap-Dashlet nicht mithilfe eines vorkonfigurierten Diagramms (OOTB) erstellt werden. Dies geschieht, wenn ein benutzerdefiniertes Dashboard ein Geomap-Dashlet verwendet, das mit einem vorkonfigurierten Diagramm (OOTB) erstellt wird.

Workaround: Die Datenquelle muss für dieses OOTB-Diagramm, das für die Verwendung im Dashlet mit Geomap erforderlich ist, manuell aktualisiert werden. Oder erstellen Sie ein neues Diagramm mit derselben vorkonfigurierten Regel (OOTB) und verwenden Sie das neue Diagramm im Geomap-Dashlet.

Der Warehouse Connector-Service zeigt SSL FIPS als deaktiviert an.

Rückverfolgungsnummer: ASOC-41930

Problem: Bei einem Upgrade von 10.6.x ohne FIPS-Einrichtung auf 11.0.0.0, wird auf der Benutzeroberfläche angezeigt, dass SSL FIPS deaktiviert ist, obwohl der Warehouse Connector-Service auf FIPS ausgeführt wird.

Workaround: Prüfen Sie SSL FIPS auf der Seite „Konfigurieren“ (Benutzeroberfläche) und starten Sie den Warehouse Connector-Service neu.

Context Hub

OutOfMemoryError im Context Hub-Service

Rückverfolgungsnummer: ASOC-41664

Problem: Im Context Hub-Service tritt ein OutOfMemoryError auf und der Service reagiert nicht mehr, wenn eine große Anzahl von TAXII-Feeds zum Abrufen von konfiguriert sind.

Workaround: Starten Sie den Context Hub-Service neu und stellen Sie sicher, dass der Zeitbereich, den Sie für das Abrufen von TAXII-Feeds vom TAXII-Server auswählen, nicht mehr als sechs Monate umfasst. Wenn das Problem selbst nach Aktualisieren des Zeitbereichs bestehen bleibt, finden Sie weitere Informationen im Thema „Troubleshooting“ im *Handbuch zum Management von Live Services*.

Die Option „Wechseln zu Investigate“ in der Ansicht „Reagieren“ führt nicht zum richtigen Link.

Rückverfolgungsnummer: ASOC-40944

Problem: Jedes Mal, wenn Sie den RabbitMQ-Server beenden und neu starten, ist die auf dem Bildschirm „Reagieren“ angezeigte Option „Wechseln zu Investigate“ nicht sichtbar. Der Bereich „Kontext“ für „Wechseln zu Investigate“ öffnet die gleiche Seite.

Workaround: Sie müssen den Jetty-Service auf dem NetWitness-Server neu starten. Melden Sie sich beim NetWitness-Serverhost an und geben Sie den Befehl zum Neustart des Jetty-Services ein.

Das Erhöhen der Begrenzungseinstellungen für Warnmeldungen und Incidents führt zu einem Abfragefehler.

Rückverfolgungsnummer: ASOC-40246

Problem: Standardmäßig sind die Begrenzungseinstellungen für das Anzeigen der Anzahl von Warnmeldungen und Incidents auf 50 festgelegt. Wenn bei Erhöhung der Begrenzung ein Abfragefehler angezeigt wird, liegt das an einer großen Anzahl von Incidents und Warnmeldungen. Der tritt aufgrund einer Einschränkung der internen Datenbank auf.

Workaround: Begrenzen Sie die Anzeige von Warnmeldungen und Incidents auf 50.

Beim Hinzufügen zu einer Liste und Entfernen aus einer Liste werden über die Registerkarte „Datenquelle“ hinzugefügte Listen mit einer und mehreren Spalten nicht unterstützt.

Rückverfolgungsnummer: ASOC-37998

Problem: Wenn Sie in der Ansicht „Investigation“, „Ereignisse“ oder „Reagieren“ bestimmte Kontextmetadaten abfragen, werden die Listennamen angezeigt, die übereinstimmende Werte haben.

Wenn Sie mit der rechten Maustaste auf bestimmte Metadaten klicken und die Listenoption „Hinzufügen“ oder „Entfernen“ auswählen, werden die Namen von Listen mit einer und mehreren Spalten, die von der Registerkarte „Datenquelle“ hinzugefügt wurden, nicht angezeigt. Es werden nur über die Benutzeroberfläche mit der Registerkarte „Liste“ hinzugefügte Listen angezeigt.

Workaround: Sie müssen die Werte, die von der Registerkarte „Datenquelle“ hinzugefügt wurden, manuell zu der jeweiligen CSV-Datei hinzufügen. Damit sind die Werte aus der aktualisierten CSV-Datei bei der nächsten Ausführung des Scheduler in den jeweiligen Listen verfügbar.

Leere Liste importiert

Rückverfolgungsnummer: ASOC-34187

Problem: Wenn Sie eine Liste mit fehlenden Anführungszeichen importieren, z. B. "172.16.0.0, wird die Liste ohne Daten gespeichert. Der Grund ist, dass die CSV-Datei aufgrund eines Apache-Fehlers (CSV-141) mit einem falschen Format analysiert wird.

Workaround: Importieren Sie eine Liste mit den richtigen Anführungszeichen. Beispiel: “172.16.0.0”, “host.mycompany.com” usw.

Der SSL-Handshake mit einem RSA Archer-Zertifikat schlägt fehl, wenn Sie es als Datenquelle hinzufügen.

Rückverfolgungsnummer: ASOC-32654

Problem: Wenn Sie versuchen, RSA Archer als Datenquelle mit gültigen Anmeldeinformationen hinzuzufügen, schlägt die Testverbindung fehl (ARCHER-37085). Dazu kommt es, wenn die Option „Allen Zertifikaten vertrauen“ deaktiviert ist und Sie versuchen, ein vertrauenswürdiges RSA Archer-Zertifikat hochzuladen.

Workaround: Aktivieren Sie das Kontrollkästchen „Allen Zertifikaten vertrauen“ und laden Sie kein Zertifikat hoch.

Allgemeine Plattformprobleme

Die NetWitness Suite-Benutzeroberfläche reagiert möglicherweise nicht mehr.

Rückverfolgungsnummer: SACE-7751

Problem: Die NetWitness Suite-Benutzeroberfläche reagiert möglicherweise nicht mehr, wenn das System versucht, große Volumen von Live Connect-Protokollen zu lesen.

Workaround: Dieses Problem kann durch einen Neustart von jettysrv vorübergehend behoben werden.

Problem beim Exportieren von Metadaten

Rückverfolgungsnummer: SACE-8116

Problem: Obwohl der Export funktioniert, wird mit der aktuellen Funktion bei mehreren Metadatenwerten in einer Sitzung nur einer der Metadatenwerte exportiert. Wenn Sie beispielsweise eine Sitzung mit 100 alias.host-Metawerten haben, wird nur ein Wert exportiert.

Workaround: Keiner.

Der Benutzer wählt die Option zum Extrahieren von Metadaten aus, aber es werden keine Daten heruntergeladen.

Rückverfolgungsnummer: ASOC-35600

Problem: Wenn Sie den Export von Metadaten für ein Ereignis auswählen, wird die Exportdatei heruntergeladen und mit den angegebenen Dateinamen gespeichert, aber es sind keine Daten in der heruntergeladenen Datei enthalten.

Workaround: Keiner.

In der NW-Benutzeroberfläche wird ein leeres Pop-up-Dialogfeld für ungültige eine STIX-Datei zurückgegeben.

Rückverfolgungsnummer: ASOC-36138

Problem: Wenn Sie versuchen, eine ungültige STIX-Datei hochzuladen, sollte eine Fehlermeldung angezeigt werden, stattdessen wird jedoch ein leeres Pop-up-Dialogfeld zurückgegeben.

Workaround: Keiner.

Protokollexport wird immer im LOG-Format exportiert.

Rückverfolgungsnummer: ASOC-38270

Problem: Wenn Sie in der Investigation-Benutzeroberfläche die Option zum Extrahieren von Protokollen vom NetWitness-Server auswählen, wird das Protokoll immer im Format „LOG“ exportiert.

Workaround: Keiner.

Allgemeine Anwendungsprobleme

Klassische Seiten der NetWitness Suite-Benutzeroberfläche werden nicht geladen, wenn das System unter hoher Auslastung steht.

Rückverfolgungsnummer: ASOC-41999

Problem: Klassische Seiten der NetWitness Suite-Benutzeroberfläche werden nicht geladen, wenn das System unter hoher Auslastung steht, und der Fehler „`OutOfMemoryError: Metaspace`“ wird angezeigt.

Workaround: Ändern Sie „`-XX:MaxMetaspaceSize=256m`“ in „`-XX:MaxMetaspaceSize=512m`“ in der Datei `/etc/default/jetty` auf dem Admin-Node. Nachdem die Änderungen gespeichert wurden, starten Sie den jetty-Service neu (`systemctl restart jetty`).

Berechtigungen

Die messungsbasierte Lizenz kehrt nicht sofort zu „Gültig“ zurück, wenn keine Services mit der messungsbasierten Lizenz verbunden sind.

Rückverfolgungsnummer: ASOC-9078

Problem: Beispiel: Wenn eine messungsbasierte Lizenz für einen Log Decoder zur Verfügung steht und ein Log Decoder darunter aufgeführt wird, können die folgenden Bedingungen zutreffen:

- Sie haben die eingeräumte Nutzung überschritten und die Lizenz wurde als nicht mehr gültig markiert.
- Sie haben beschlossen, den Log Decoder in eine verfügbare servicebasierte Lizenz zu verschieben.
- Der Lizenz vom Typ Gemessen ist kein Service zugeordnet.
- Die messungsbasierte Lizenz kehrt nach sieben Tagen wieder in den Status „Gültig“ zurück.

Workaround: Keiner.

Ein Bericht zur aggregierten Nutzung wird erzeugt, wenn einer Lizenz ein Service zugeordnet ist und beim Exportieren von Nutzungsstatistiken „Alle“ ausgewählt wird.

Rückverfolgungsnummer: ASOC-10079

Problem: Für alle Lizenztypen (Alle/Gemessen/Servicebasiert) sollte die aggregierte PDF-/CSV-Datei nur erzeugt werden, wenn unter einem Lizenztyp mehr als ein Service aufgelistet ist.

Workaround: Keiner.

Reagieren

Beim Upgrade ist die Aggregationsregel für C2-Warnmeldungen der Bedingung „Gruppieren nach“ falsch.

Rückverfolgungsnummer: ASOC-41934

Problem: Beim Upgrade auf 11.0.0.0 hat die von der automatischen Bedrohungserkennung verwendete C2-Aggregationsregel einen anderen Wert für die Bedingung „Gruppieren nach“.

Workaround: Bearbeiten Sie nach dem Upgrade auf 11.0.0.0 die Aggregationsregel „Verdacht auf Befehl-und-Kontrolle-Kommunikation von Domain“ und ändern Sie die Bedingung „Gruppen nach“ in „Domain“. (Wechseln Sie dafür zu „KONFIGURIEREN > Incident-Regeln > Aggregationsregeln“ und doppelklicken Sie auf die Regel „Verdacht auf Befehl-und-Kontrolle-Kommunikation“, um diese zu bearbeiten.) Damit werden die Warnmeldungen und Incidents aggregiert, die für „Verdacht auf Befehl-und-Kontrolle-Kommunikation“ erstellt werden.

Ein Incident mit 1.000 Warnmeldungen kann nicht erstellt werden.

Rückverfolgungsnummer: ASOC-41855

Problem: Wenn Sie versuchen, manuell einen Incident mit mehr als 400 in der Ansicht „Warnmeldungsliste“ ausgewählten Warnmeldungen zu erstellen, können Probleme auftreten.

Workaround: Wählen Sie mehr als 400 Warnmeldungen aus, wenn Sie einen Incident erstellen.

Der Respond-Administrator kann im Dashboard keine Investigate-Dashlets abfragen oder Live-Dashlets anzeigen.

Rückverfolgungsnummer: ASOC-40749

Problem: Die Rolle „Respond_Administrator“ verfügt nicht über die Berechtigung zum Abfragen von Investigate. Dies ist notwendig, damit der Respond-Administrator zu Investigate wechseln oder Incidents aus Ereignissen erstellen kann. Die Rolle „Respond_Administrator“ verfügt außerdem nicht über die Berechtigung „Live: Auf Live-Modul zugreifen“, die erforderlich ist, um Live-Dashlets im Dashboard anzuzeigen.

Workaround:

1. Erstellen Sie die Rolle „Respond_Administrator“ manuell in den Core-Services. Wechseln Sie dafür zu „ADMIN > Services“, wählen Sie einen Core-Service aus und wählen Sie dann in der Drop-down-Liste „Aktionen“ unter „Ansicht > Sicherheit“ die Registerkarte „Rollen“ aus. Klicken Sie auf +, um die Rolle „Respond_Administrator“ hinzuzufügen. Fügen Sie die folgenden Berechtigungen zur Rolle „Respond_Administrator“ hinzu:

- sdk.content
- sdk.meta
- sdk.packets
- storedproc.execute

Replizieren Sie die Rolle „Respond_Administrator“ an andere Core-Services, die möglicherweise von den Benutzern verwendet werden.

2. Fügen Sie unter „ADMIN > Sicherheit“ auf der Registerkarte„ Rolle“ die Berechtigung „Live: Auf Live-Modul zugreifen“ zur Rolle „Respond_Administrator“ hinzu.

Wenn die messbasierte oder servicebasierte Lizenz zugeordnet ist, werden die lizenzierten Tage und das Startdatum falsch angezeigt.

Rückverfolgungsnummer: ASOC-26334

Problem: Wenn die messbasierte oder servicebasierte Lizenz zugeordnet ist, werden die lizenzierten Tage und das Startdatum auf der Benutzeroberfläche falsch angezeigt. Dies geschieht aufgrund eines Problems mit dem Lizenzierungssystem und wenn eine neue Lizenz zugeordnet wird. Die richtigen Daten (lizenzierte Tage und Startdatum) werden jedoch nach einigen Tagen in der Benutzeroberfläche korrekt dargestellt.

Workaround: Keiner.

Dateinamen für Malwareereignisse mit koreanischen Zeichen werden in der Ansicht „Reagieren“ nicht ordnungsgemäß angezeigt.

Rückverfolgungsnummer: ASOC-40159

Problem: Wenn koreanische Zeichen in einer Warnmeldung vorhanden sind, die von Malware Analysis empfangen wird, werden diese in der Ansicht „Reagieren“ nicht korrekt angezeigt.

Workaround: Keiner.

Die Domain kann in source/destination.device.geolocation nicht abgerufen werden.

Rückverfolgungsnummer: ASOC-39938

Problem: Ein geografischer Standort, der aus den ESA-Korrelationsregeln kommt, ist in der Ansicht „Incident-Details“ im Bereich „Verwandte Indikatoren“ nicht verfügbar. (Wechseln Sie zum Zugreifen auf den Bereich „Verwandte Indikatoren“ zu „REAGIEREN > Incidents“ und klicken in der Liste der Incidents auf den Link „ID“ oder „NAME“ für den Incident. Klicken Sie in der Symbolleiste der Ansicht „Incident-Details“ auf die Symbole für „Journal“, „Aufgaben“ und „Verwandt“. Das Journal wird auf der rechten Seite angezeigt. Klicken Sie auf die Registerkarte „VERWANDT“.)

Workaround: Keiner. Da dies eine neue Funktion ist, handelt es sich einfach um Daten, die nicht durchsuchbar sind.

Der Link für Security Analytics Incident Management in NetWitness SecOps Manager 1.3.1.2 ist in NetWitness Suite 11.0.0.0 nicht gültig.

Rückverfolgungsnummer: ASOC-41891

Problem: NetWitness Suite 11.0.0.0 kann nur mit NetWitness SecOps Manager 1.3.1.2 verwendet werden. Allerdings führt der Link für Security Analytics Incident Management in NetWitness SecOps Manager 1.3.1.2 zur veralteten Security Analytics Incident Management-Seite, die in NetWitness Suite 11.0.0.0 nicht gültig ist.

Workaround: Keiner.

Incidents und Aufgaben sind weiterhin verfügbar, wenn die RSA NetWitness SecOps Manager-Integration aktiviert ist.

Rückverfolgungsnummer: ASOC-39886

Problem: Nach der Aktivierung der NetWitness SecOps Manager-Integration im Respond-Serverservice werden alle Incidents in NetWitness SecOps Manager gemanagt. Wenn in früheren Versionen SecOps aktiviert war, waren Incidents und Korrekturaufgaben verborgen. In NetWitness Suite 11.0.0.0 können Benutzer weiterhin auf Incidents und Aufgaben in der Ansicht „Reagieren“ („REAGIEREN >Incidents“ und „REAGIEREN > Aufgaben“) zugreifen. Sie werden auch nicht daran gehindert, Incidents in NetWitness Suite zu erstellen. Wenn sie aus der Liste der Warnmeldungen in der Ansicht „Reagieren“ (REAGIEREN > Warnmeldungen) oder aus Investigate Incidents erstellen, werden diese Incidents nicht zu NetWitness SecOps Manager verschoben.

Workaround: Wenn Sie die SecOps Manager-Integration im Respond-Serverservice aktiviert haben, sollten Sie Folgendes in der Ansicht „Reagieren“ nicht verwenden: Ansicht „Incidents-Liste“, Ansicht „Incident-Details“ und Ansicht „Aufgabenliste“. Erstellen Sie Incidents außerdem nicht aus der Liste der Warnmeldungen in der Ansicht „Reagieren“ oder aus „Untersuchen“.

Für migrierte Incidents wird im Bereich „Übersicht“ für die Ereignisanzahl immer 0 angezeigt.

Rückverfolgungsnummer: ASOC-38026

Problem: Im Feld „Katalysatoren“ des Bereichs „Incident-Übersicht“ wird die Anzahl der Ereignisse für migrierte Incidents immer als 0 (null) angezeigt. Das ist in NetWitness Suite 11.0.0.0 erwartetes Verhalten. (Um auf den Bereich „Übersicht“ zuzugreifen, wechseln Sie „Reagieren > Incidents“. Wenn Sie auf einen Incident in der Liste der Incidents klicken, wird der Bereich „Übersicht“ auf der rechten Seite angezeigt. Wenn Sie auf einen Link im Feld „ID“ oder „NAME“ in der Liste der Incidents klicken, wird die Ansicht „Incident-Details“ mit dem Bereich „Übersicht“ auf der linken Seite geöffnet.)

Workaround: Keiner.

Wenn mehrere Werte vorhanden sind, kann mit allen Benutzernamen-, Dateinamen- und Domainwerten kein Wechsel zu Investigate durchgeführt werden.

Rückverfolgungsnummer: ASOC-37997

Problem: Wenn Benutzernamenfelder Kommas enthalten, die kein Trennzeichen zwischen Werte darstellen, können Sie möglicherweise bei bestimmten Metadaten nicht zu Investigate wechseln, wenn sich mehrere Werte im Feld befinden.

Workaround: Sie können andere Daten abfragen oder zu anderen Daten wechseln oder die Metadaten manuell untersuchen. Sie können immer noch über Investigate auf die Metadaten zugreifen.

In der Arbeitsspeichertabelle werden keine Erweiterungsinformationen für ESA-Warnmeldungen angezeigt.

Rückverfolgungsnummer: ASOC-37533

Problem: Sie können keine benutzerdefinierten Erweiterungen für ESA-Korrelationsregeln in den Warnmeldungen der Ansicht „Reagieren“ anzeigen.

Workaround: Keiner.

Metadaten für DOMAIN und HOST werden in der Ansicht „Reagieren“ nicht korrekt angezeigt.

Rückverfolgungsnummer: ASOC-37232

Problem: Domain und Hostmetadaten werden möglicherweise unter „Incident-Details“ in der Ansicht „Reagieren“ falsch gekennzeichnet, wenn „alias.host“ unterschiedliche Arten von Daten enthält. Das Verhalten des Felds „Domain“ ist inkonsistent und es wird möglicherweise mit Hostnamen gefüllt.

Workaround: Keiner. Im Feld „Domain“ sind weiterhin mehrere Arten von Informationen vorhanden.

Nach dem Upgrade können Incidents nicht über das Feld „Zuweisungsempfänger“ gefiltert werden.

Rückverfolgungsnummer: ASOC-36973

Problem: Nach dem Upgrade von Incidents von 10.6.x auf 11.0.0.0 können Analysten die migrierten nicht über das Feld „Zuweisungsempfänger“ filtern (Reagieren > Incidents > Bereich „Filter“).

Workaround: Keiner.

Reagieren – Erstellen von Incidents aus Warnmeldungen in der Warnmeldungsliste der Ansicht „Reagieren“

Rückverfolgungsnummer: ASOC-35811

Problem: Wenn Sie manuell einen Incident aus Warnmeldungen in der Warnmeldungsliste der Ansicht „Reagieren“ (REAGIEREN > Warnmeldungen) in 11.0.0.0 erstellen, stehen nur minimale Funktionen für die Erstellung eines Incident aus Warnmeldungen zur Verfügung. Sie können nur einen Namen für den Incident angeben und die Priorität wird standardmäßig auf „Niedrig“ festgelegt. Wenn Sie einen Incident manuell erstellen, stehen keine zusätzlichen Optionen wie das Hinzufügen einer Priorität, eines Zuweisungsempfängers oder einer Kategorie bereit.

Workaround: Sie können zusätzliche Felder aktualisieren, indem Sie den Incident nach der Erstellung manuell bearbeiten, z. B. die Priorität von „Niedrig“ in „Hoch“ ändern. Sie können einem Incident jedoch keine Kategorie hinzufügen.

Domains werden beim Schließen von Incidents als falsch positive Ergebnisse zur Whitelist hinzugefügt.

Rückverfolgungsnummer: ASOC-25135

Problem: Wenn in 10.6.x ein verdächtiger C&C-Incident als „Geschlossen – falsch positives Ergebnis“ gekennzeichnet wurde, wurde von Context Hub ein Eintrag zur Liste der Domains in der Whitelist hinzugefügt. Die Ansicht „Reagieren“ sollte über eine ähnliche Funktion verfügen.

Workaround: Analysten können Domains in der Ansicht „Reagieren“ manuell zu einer Whitelist hinzufügen. Entsprechende Verfahren finden Sie im *NetWitness Respond – Benutzerhandbuch*.

Integrationseinstellungen für SecOps Manager sollten in der Benutzeroberfläche zur Verfügung gestellt werden.

Rückverfolgungsnummer: ASOC-25127

Problem: Die Integrationseinstellungen für das Senden aller Incidents an RSA NetWitness SecOps Manager sollten in der Benutzeroberfläche zur Verfügung gestellt werden.

Workaround: Die Benutzeroberfläche für die partielle RSA NetWitness SecOps Manager-Integration wurde in 11.0.0.0 entfernt. Administratoren können die Integration in der Ansicht „Explorer“ des Respond-Serverservice abschließen.

Incidents werden nicht gekennzeichnet, wenn ein Benutzer Warnmeldungen manuell zu vorhandenen Incidents hinzufügt.

Rückverfolgungsnummer: ASOC-16640

Problem: Untersuchungswerte werden nicht hervorgehoben, wenn Warnmeldungen in „Reagieren“ manuell zu einem Incident hinzugefügt wurden. Warnmeldungen, die einem Incident dynamisch hinzugefügt werden, werden hervorgehoben.

Workaround: Keiner.

Log Collector

DPO-Rolle fehlt auf Log Collector.

Rückverfolgungsnummer: ASOC-7937

Problem: Die neue Rolle des Datenschutzbeauftragten (DPO) ist auf dem Log Collector nicht vorhanden.

Workaround: Keiner.

Kontrollpunktsammlung funktioniert nicht, Fehler „Sitzung von Peer beendet“ angezeigt

Rückverfolgungsnummer: ASOC-8351

Problem: Die Prüfpunktsammlung funktioniert nicht und die Protokolle zeigen die folgende Fehlermeldung an: **Sitzung von Peer beendet**

Workaround: Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Erstellen Sie eine Sicherungskopie und entfernen Sie dann die Kontrollpunktpositionsdatei (**/var/netwitness/logcollector/runtime/checkpoint/eventsources/checkpoint.CP_Security.xml**).
2. Starten Sie den Service neu, um die Datei erneut zu erzeugen.
3. (Optional) Wenn **Max. Abruf-Inaktivitätsdauer** auf 0 gesetzt ist, ändern Sie den Wert in 5.

Fehler beim Drosseln von Remote-Collector auf die Bandbreite von Local Collector

Rückverfolgungsnummer: ASOC-16717

Problem: Änderungen an der Konfiguration der Bandbreiteneinschränkung zur Kontrolle der Geschwindigkeit, mit der der Remote-Collector Ereignisdaten an einen Local Collector sendet, werden nach einem Neustart nicht beibehalten.

Das Skript `set-shoveltransfer-limit.sh` wird verwendet, um die Einschränkung der Bandbreite für Ereignisdaten festzulegen, die von einem Remote-Collector an einen Local Collector übertragen werden. Das Skript verwendet sowohl iptables-Regeln als auch Linux-Kernel-Filter zur Datenverkehrsformung, um die Upload-Bandbreite zu steuern, die vom RabbitMQ-Port auf Übertragungen zu einem Upstream Collector verwendet werden. Das Skript funktioniert korrekt, wenn es ausgeführt wird, behält aber die Filterwerte der Datenverkehrsformung nicht dauerhaft bei, sobald die Appliance neu gestartet wird.

Workaround: Fügen Sie auf dem Remote-Collector die Skriptausführung zu `/etc/rc.local` hinzu, wie im folgenden Beispiel gezeigt:
`"/opt/netwitness/bin/set-shovel-transfer-limit.sh -s -r 4096kbit"`

Investigation

Attribute für Benutzer und Rollen werden in den neuen Workflows der Ereignisanalyse in „Untersuchen“ nicht erzwungen.

Rückverfolgungsnummer: ASOC-42735

Problem: Attribute für Benutzer und Rollen werden in den neuen Workflows der Ereignisanalyse in „Untersuchen“ nicht von NetWitness Suite 11.0 erzwungen.

Workaround*:* Sie müssen den RSA NetWitness Suite-Patch 11.0.0.1 anwenden, um diese Konfiguration zu korrigieren.

In einer Umgebung mit gemischtem Modus kann ein Analyst mit unzureichenden Berechtigungen PCAPs und Protokolle von einem 10.6.x-Service, aber keine Dateien oder Nutzlasten in der Ansicht „Untersuchen > Ereignisanalyse“ herunterladen.

Rückverfolgungsnummer: ASOC-41697, ASOC-41698

Problem: Die rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC) wird auf dem 11.0.0.0-NW-Server nicht einheitlich für Downloads zugewiesen, wenn 10.6.x-Services untersucht werden. Wenn die sdk.packets-Einstellung nicht deaktiviert wurde, können Analysten mit Berechtigungen für SDK-Metadaten und -Rollen zur Beschränkung der Anzeige und der Rekonstruktion der Inhalte eines Ereignisses die PCAP und das Protokoll eines Ereignisses herunterladen, das über Inhaltsbeschränkungen verfügt. Andere Arten von Downloads scheinen zu funktionieren, dann wird aufgrund unzureichender Berechtigungen allerdings ein Fehler erzeugt. Die Daten bleiben geschützt.

Workaround: Deaktivieren Sie die sdk.packets-Einstellung für 10.6.x-Services, um das Herunterladen von PCAPs oder Protokollen durch Analysten während eines in Phasen durchgeführten Upgrades einzuschränken. Wenn das Upgrade aller Services abgeschlossen ist, ist die RBAC-Erfahrung in allen Services konsistent. Details finden Sie im Abschnitt „Upgradeaufgaben“ im *Upgradehandbuch für physische Hosts*.

In einer Umgebung mit gemischtem Modus wird in der Ansicht „Ereignisrekonstruktion > Datei“ das Wort „Beendet“ anstelle der Liste der Dateien angezeigt.

Rückverfolgungsnummer: ASOC-41703

Problem: Wenn ein Admin-Benutzer zum ersten Mal das Ereignis service=other und eine RAW-Datei rekonstruiert, wird in der Ansicht „Ereignisrekonstruktion“ möglicherweise das Wort „Beendet“ anstellt der RAW-Datei angezeigt.

Workaround: Wechseln Sie zu einem anderen Ereignis in der Ansicht „Ereignisse“ und kehren Sie zu diesem Ereignis zurück oder löschen Sie den Servicecache, um das richtige Ergebnis zu sehen. Alternativ kann der Admin-Benutzer die Datei in der Ansicht „Ereignisanalyse“ anzeigen. Da das Problem nur während eines Upgrades im gemischten Modus auftritt, besteht der beste Workaround darin, das Upgrade von verbundenen Services auf NW 11.0.0.0 abzuschließen. Details finden Sie im Abschnitt „Upgradeaufgaben“ im *Upgradehandbuch für physische Hosts*.

In einem Netzwerk mit gemischtem Modus und in einem reinen 11.0.0.0-Netzwerk scheint ein Analyst mit Inhaltseinschränkungen eingeschränkte Inhalte herunterladen zu können, kann aber das heruntergeladene Dateiarchiv nicht entpacken, das die ZIP-Datei nicht über den eingeschränkten Inhalt verfügt.

Rückverfolgungsnummer: ASOC-41698, ASOC-41696

Problem: Wenn ein Benutzer, der keine Berechtigungen für den Inhalt hat, Dateien herunterlädt, wird die mithilfe von RBAC angewendete Inhaltseinschränkung aufrechterhalten, aber die Benutzererfahrung ist nicht konsistent mit der Benutzererfahrung für andere Arten von Downloads mit unzureichenden Berechtigungen. Dies tritt in einer reinen 11.0.0.0-Umgebung und einer Umgebung mit gemischtem 11.0.0.0/10.6.x-Modus auf. Ein Analyst, dessen Berechtigungen das Anzeigen von Inhalten in der Ansicht „Ereignisrekonstruktion“ einschränken, kann eingeschränkte Inhalte in verbundenen 10.6.x-Services herunterladen. Der Analyst kann eingeschränkte Dateien als ZIP- oder GZIP-Datei exportieren und die Jobwarteschlange zeigt einen erfolgreichen Download an. Allerdings wird die Datei im ZIP- oder TAR-Format heruntergeladen und das Archiv kann nicht entpackt werden. Stattdessen wird eine Kopie als „CPGZ“ erstellt.

Workaround: Keiner. Wenn das Upgrade aller Services abgeschlossen ist, ist die RBAC-Erfahrung in allen Services konsistent. Details finden Sie im Abschnitt „Upgradeaufgaben“ im Upgradehandbuch für physische Hosts.

Bei einem Klick mit der rechten Maustaste in der Protokollansicht wird die Ereignisrekonstruktion oder die Ereignisanalyse nicht gestartet, wenn Sie auf eine Protokollspalte klicken, die in mehrere Zeilen umbrochen ist.

Rückverfolgungsnummer: ASOC-37989

Problem: In der Protokollansicht eines Ereignisses ist die Aktion des Klickens mit der rechten Maustaste zum Starten der Ereignisrekonstruktion oder Ereignisanalyse nicht verfügbar, wenn die Spalte „Protokolle“ in der Protokollansicht in mehrere Zeilen umbrochen ist.

Workaround: Analysten können in derselben Ereigniszeile mit der rechten Maustaste auf eine andere Spalte klicken, in der kein Zeilenumbruch vorhanden ist.

In der Ereignisanalyse wird die Meldung zu gerenderten Paketen für Ereignisse mit einer kleinen Nutzlast aber großen Anzahl von Paketen nicht angezeigt.

Rückverfolgungsnummer: ASOC-37348

Problem: Wenn ein Ereignis über mehr als 2.500 Pakete verfügt, sollte im unteren Bereich der Ergebnisse eine Meldung mit der Anzahl der gerenderten Pakete angezeigt werden. Diese Meldung wird für Ereignisse mit 2.500 oder mehr Paketen und einer sehr kleinen Nutzlast nicht angezeigt, da die gesamte Nutzlast in der Ansicht angezeigt werden kann.

Workaround: Keiner.

Probleme bei PCAP- und Nutzlastdownloads in der Ansicht „Ereignisanalyse“ in einer Umgebung mit gemischtem Modus

Rückverfolgungsnummer: ASOC-37309

Problem: Für den Ereignisanalyseworkflow müssen alle Services 11.0.0.0 ausführen. Wenn auf dem NW-Server, -Broker und -Concentrator 11.0.0.0 ausgeführt wird und auf dem Decoder 10.6.x, kann der Admin-Benutzer keine Dateien, Protokolle, PCAPs und Nutzlasten herunterladen.

Workaround: Laden Sie Dateien über die Ereignisrekonstruktion herunter.

Beim Anzeigen eines Dateiarchivs im Bereich „Dateianalyse“ der Ereignisanalyse werden die einzelnen Dateinamen im Archiv nicht angezeigt.

Rückverfolgungsnummer: ASOC-35607

Problem: Sie können das Archiv, aber nicht die im Archiv enthaltenen Dateinamen sehen.

Workaround: Zeigen Sie das Ereignis in der Ansicht „Untersuchen > Ereignisrekonstruktion“ an, um die einzelnen Dateinamen zu sehen.

Parallelkoordinatenvisualisierung zeigt Sonderzeichen nicht korrekt an

Rückverfolgungsnummer: ASOC-9346

Problem: Wenn Sie den Metaschlüssel content type als eine Art der Metadaten für die Achse konfigurieren und der Metawert Sonderzeichen enthält, dann werden die Werte nicht korrekt angezeigt.

Workaround: Keiner.

Workbench

Rückverfolgungsnummer: ASOC-6859

Problem: In der Registerkarte „Sammlungen“ wird eine leere Sammlung angezeigt, wenn der Workbench-Service während des Wiederherstellungsprozesses angehalten oder neu gestartet wurde.

Workaround: Keiner.

Datumsbereich wird für Sammlung nicht angezeigt, wenn Workbench-Service oder Jettysrv während der Wiederherstellung neu gestartet wird.

Rückverfolgungsnummer: ASOC-6822

Problem: Der Datumsbereich wird für eine Sammlung nicht angezeigt, wenn der Workbench-Service oder Jettysrv während der Wiederherstellung neu gestartet wird.

Workaround: Keiner.

Live

Der Status der Fortschrittsleiste des STIX-Feeds ist unvollständig.

Rückverfolgungsnummer: ASOC-40642

Problem: Manchmal ist der Status der Fortschrittsleiste für einige der STIX-Feeds unvollständig, selbst wenn die Feeds erfolgreich an die Decoder übertragen werden.

Workaround: Keiner.

Malware Analysis

Benutzer mit Analystenrolle können den Schadsoftwarescan nicht nach Bedarf ausführen.

Rückverfolgungsnummer: ASOC-5425

Problem: Ein Benutzer, der die Analystenrolle erfüllt, hat Zugriff auf die Module Investigation und Malware Analysis. Wenn ein solcher Benutzer jedoch versucht, den Malware Analysis-Scan nach Bedarf über den Bildschirm „Investigation“ auszuführen, wird die Fehlermeldung „Ungültiger Benutzername“ angezeigt. Der Job wird übermittelt, schlägt jedoch aufgrund der Anmeldedaten fehl.

Workaround: Keiner.

Wenn auf dem Core-Gerät keine IP-Adresse konfiguriert wurde, ist die Option „Netzwerksitzung anzeigen“ für Malware Analysis-Ereignisse deaktiviert.

Rückverfolgungsnummer: ASOC-5571

Problem: Aufgrund der neuen Service-ID und ASG-Änderungen wird in Malware Analysis in der Schadsoftware-Ereigniszusammenfassung nicht die Option Netzwerksitzung anzeigen angezeigt. Die Geräte-ID wird scheinbar als null angezeigt.

Workaround: Keiner.

Event Stream Analysis

Bereitstellung (bis 10.4 Synchronisation genannt) schlägt fehl, wenn Sie die folgende Regel von RSA Live bereitstellen: Kein Protokollverkehr von Gerät in vorgegebenem Zeitraum erkannt

Rückverfolgungsnummer: SAENG-5888

Problem: Die Bereitstellung, früher Synchronisation genannt, schlägt fehl für die von Live bereitgestellte Regel „Kein Protokollverkehr von Gerät in vorgegebenem Zeitraum“. Dieses Problem wird nicht beobachtet, wenn Sie die Regeln von Live auf einer 10.4.-Konfiguration bereitstellen und die Synchronisation durchführen. Das Problem tritt auf, wenn Sie eine Aktualisierung Ihres Systems von einer Version vor 10.4 durchführen, in der die Regeln von Live mit falschen Modul-IDs bereitgestellt werden.

Workaround: Löschen Sie die Regeln mit falschen Modul-IDs und stellen Sie sie erneut von Live bereit.

Zwischen Klein- und Großschreibung unterscheidende Sortierung im ESA-Raster „Alle Regeln“ funktioniert nicht ordnungsgemäß.

Rückverfolgungsnummer: SAENG-3605

Problem: Wenn Regelnamen sowohl mit Groß- als auch Kleinbuchstaben anfangen, funktioniert die Sortierung in der Spalte „Name der Regel“ im ESA-Raster „Alle Regeln“ nicht ordnungsgemäß. Beispielsweise folgt bei der Sortierung nach Namen auf „Regel 1“ nicht „regel 2“.

Workaround: Keiner.

Die ESA-Komprimierungsstufe kann nicht wie in anderen Appliances festgelegt werden.

Rückverfolgungsnummer: ASOC-26481

Problem: Administratoren können die Komprimierungsstufe in ESA nicht wie mit anderen Appliances festlegen, auch nicht bei Verwendung der Ansicht „Explorer“.

Workaround: Löschen Sie die Concentrator-Quelle aus ESA und fügen Sie sie erneut hinzu, damit die Änderungen der Komprimierungsstufe dargestellt werden:

1. Entfernen Sie die Concentrator-Datenquelle aus ESA. (Wechseln Sie zu „ADMIN > Services“, wählen Sie den Event Stream Analysis-Service aus und wählen Sie dann aus dem

Menü „Aktionen“ die Optionen „Ansicht > Konfigurieren“ aus. Entfernen Sie auf der Registerkarte „Datenquellen“ der Ansicht „Konfigurieren“ die Concentrator-Datenquelle.)

2. Legen Sie die Komprimierungsstufe in ESA fest. (Wechseln Sie zur Ansicht „Durchsuchen“, navigieren Sie in der Node-Liste zu „Workflow/Source/nextgenAggregationSource“ und legen Sie „CompressionLevel“ fest.)
3. Fügen Sie die Concentrator-Datenquelle wieder zu ESA hinzu. (Kehren Sie zur Registerkarte „Datenquellen“ der Ansicht „Konfigurieren“ zurück und fügen Sie die Concentrator-Datenquelle hinzu.)

Event Stream Analysis-Service reagiert nicht mehr bei Verwendung der abfragebasierten Aggregation für die automatisierte Bedrohungserkennung für Protokolle.

Rückverfolgungsnummer: ASOC-25174

Problem: Event Stream Analysis reagiert möglicherweise nicht aufgrund von hohem Ressourcenverbrauch und die Konfiguration des Wrapper muss angepasst werden.

Workaround: Sie müssen möglicherweise die Einstellungen der Ping-Zeit in der Datei `wrapper.conf` ändern. Führen Sie folgende Schritte durch:

1. Wechseln Sie zu **Administration > Services > Event Stream Analysis> Explorer** und navigieren Sie zum Ordner `/opt/rsa/esa/conf/ .`
2. Ändern Sie die Einstellungen in die folgenden Werte:
   `wrapper.ping.timeout=300`
3. Fügen Sie die folgenden Zeilen am Ende der Datei hinzu:
   `wrapper.restart.delay=40`
   `wrapper.ping.timeout.action=RESTART`
4. Starten Sie den Event Stream Analysis-Service neu.

ESA zeigt Warnung für Array-Operatoren an

Rückverfolgungsnummer: ASOC-14157

Problem: Beim Schreiben einer erweiterten Regel schlagen Array-Operatoren wie AnyOf fehl. Beispiel:

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

führt zu einem Fehler ähnlich dem folgenden:

```
Logger name:
com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
```

```
Level : WARN

Message : Expected array-type input from property 'alias_host' but
received class java.util.Vector
```

Workaround: Um einen unscharfen Vergleich zu erhalten, müssen Sie zunächst das Array in eine Zeichenfolge konvertieren. Beispiel:

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

Hinweis: Wenn Sie Array-Operatoren in EPL in den Versionen 10.5, 10.5.0.1 und 10.6 verwendet haben, müssen Sie EPL mithilfe des oben genannten Workarounds ändern.

Keine Aktualisierung des Namens der Weiterleitungsregel bei Änderung des Namens einer erweiterten Regel

Rückverfolgungsnummer: ASOC-9585

Problem: Bei einer siteübergreifenden Bereitstellung wird bei Änderung des Namens einer erweiterten Regel der Name der Weiterleitungsregel nicht zusammen mit dem Namen der erweiterten Regel geändert. Das kann zu einer verwaisten Regel führen, die weiterhin Ereignisse weiterleiten kann.

Workaround: Erstellen Sie zur Umbenennung einer siteübergreifenden erweiterten Regel eine neue Regel und löschen Sie die alte.

Bereitstellung schlägt fehl, wenn der Server ausfällt, auf dem eine externe Datenbank gehostet wird.

Rückverfolgungsnummer: ASOC-9011

Problem: Sie können eine Datenbankverbindung so konfigurieren, dass die Datenbank als eine Erweiterungsquelle für eine Regel verwendet wird. Ein Verweis auf die Datenbank wird in allen ESA bereitgestellt, auch wenn die ESA keine Regeln bereitstellt, die von der Datenbank verwendet werden. Wenn der Server, der die Datenbank hostet, ausfällt, wird jede neue Bereitstellung fehlschlagen.

Workaround: Starten Sie den Server, der die Datenbank hostet, neu.

Konfiguration der Testregeln: Out-of-Bound-Werte werden begrenzt.

Rückverfolgungsnummer: ASOC-6633

Problem: Wenn Sie Parameter für Testregeln konfigurieren, können Sie die folgenden Werte konfigurieren:

- **MemoryCheckPeriod**: Definiert das Abrufintervall zur Prüfung der Auslastung des ESA-Speichers.
- **MemoryThresholdForTrialRules**: Definiert den Schwellenwert. Wenn er erreicht wird, werden alle Testregeln deaktiviert.
  Wenn Sie diese Parameter mit Out-of-Bound Werten konfigurieren, werden die Werte des

Systems für die minimalen oder maximalen Werte statt der für die Parameter definierten Werte begrenzt.

Workaround: Keiner.

Reporting Engine

Einige Complianceberichte können nicht von Live bereitgestellt werden.

Rückverfolgungsnummer: SAENG-1334

Problem: Wenn die Abhängigkeiten bestimmter Complianceberichte in Live nicht vor den Berichten selbst bereitgestellt werden, wird deren Bereitstellung fehlschlagen.

Workaround: Versuchen Sie erneut, die Bereitstellung durchzuführen. Wenn das Problem weiterhin besteht, versuchen Sie, zuerst die abhängigen Regeln/Listen und dann die Berichte bereitzustellen.

Einige Reportingwarnmeldungen können fehlschlagen oder werden verzögert, wenn die RabbitMQ-Verbindung blockiert ist.

Rückverfolgungsnummer: SAENG-5329

Problem: Wenn die Option **Warnmeldungen weiterleiten an Reagieren** aktiviert ist und RabbitMQ-Verbindungen zum Respond-Server blockiert sind, können einige Reporting Engine-Threads blockiert werden.

Workaround: Deaktivieren Sie die Option **Warnmeldungen weiterleiten an Reagieren**, bis der RabbitMQ-Broker von Reagieren im NetWitness Suite-Server gestartet wurde und die Verbindungen annehmen kann.

Aktualisierungen der Verbindungsparameter auf der Seite „Service“ werden unter „Reportingdatenquellen“ widergespiegelt.

Rückverfolgungsnummer: ASOC-8149

Problem: Wenn auf der Serviceseite Änderungen oder Aktualisierungen an Servicenamen, Ports oder Parametern vorgenommen werden, werden sie nicht an die entsprechenden Datenquellen, die zur Reporting Engine hinzugefügt werden, weitergeleitet.

Workaround: Fügen Sie Datenquellen mit geändertem Service hinzu und nutzen Sie diese. Wenn die Namen der vorhandenen Services geändert wurden, müssen die entsprechenden Planungen in Reporting aktualisiert werden.

Aus NWDB-Berichten kann nicht zu „Ermittlung“ navigiert werden, wenn die Verbindungsparameter auf der Seite „Service“ aktualisiert werden.

Rückverfolgungsnummer: ASOC-8575

Problem: Der Link Investigation für die Metawerte der ausgeführten Berichte wird auf der NWDB-Ergebnisseite nicht angezeigt.

Workaround: Keiner. Wird in einer zukünftigen Version behoben.

Aktualisierungen der Verbindungsparameter auf der Seite „Service“ werden unter „Reportingdatenquellen“ widergespiegelt.

Rückverfolgungsnummer: ASOC-8149

Problem: Wenn auf der Serviceseite Änderungen oder Aktualisierungen an Servicenamen, Ports oder Parametern vorgenommen werden, werden sie nicht an die entsprechenden Datenquellen, die zur Reporting Engine hinzugefügt werden, weitergeleitet.

Workaround: Fügen Sie Datenquellen mit geändertem Service hinzu und nutzen Sie diese. Wenn die Namen der vorhandenen Services geändert wurden, müssen die entsprechenden Planungen in Reporting aktualisiert werden.

Reporting

Kategoriemetadaten für die Incident-Sammlung werden nicht unterstützt.

Rückverfolgungsnummer: ASOC-40851

Problem: Wenn Sie die Kategoriemetadaten für die Incident-Sammlung verwenden, werden die Ergebnisse in einem falschen Format wiedergegeben. Daher werden diese Metadaten nicht unterstützt und Sie können keine Kategorienmetadaten in der select- oder der where-Klausel verwenden. Darüber hinaus stehen sie auch nicht in der Liste der Metadaten auf der Seite „Regelerstellung“ zur Auswahl.

Workaround: Keiner.

Beim Abfragen der Respond-Datenbank werden leere Zeilen angezeigt.

Rückverfolgungsnummer: ASOC-37846

Problem: Wenn beim Abfragen der Respond-Datenbank Daten für die angeforderten Spalten nicht verfügbar sind, werden leere Zeilen auf der Benutzeroberfläche angezeigt.

Workaround: Keiner.

Im Diagramm mit Summen werden falsche Daten angezeigt.

Rückverfolgungsnummer: ASOC-37958

Problem: Im Diagramm mit Summen werden falsche Daten angezeigt, wenn die Gesamtzahl der Werte höher als die Diagrammbegrenzung ist. Wenn beispielsweise 16 Zahlenwerte abgerufen werden, werden im Diagramm möglicherweise nur die ersten 10 angezeigt.

Workaround: Keiner.

Die Optionen „Ausblenden“ und „Untersuchen“ werden in den Browsern Google Chrome und Mozilla Firefox im Windows 10-Betriebssystem nicht unterstützt.

Rückverfolgungsnummer: ASOC-37590

Problem: Wenn Sie den Browser Chrome oder Firefox in einem Windows 10-Betriebssystem verwenden und auf einen Diagrammdatenpunkt klicken, werden die Optionen „Ausblenden“ und „Untersuchen“ nicht angezeigt. Diese Optionen sind bei Verwendung des Internet Explorer-Browsers jedoch verfügbar.

Workaround: Deaktivieren Sie die Touchfunktion in Chrome und Firefox. Wenden Sie zum Deaktivieren dieser Option in Chrome das folgende Verfahren an:

1. Navigieren Sie in Chrome oder Firefox zu chrome://flags/.
2. Wählen Sie die Option „Deaktivieren“ für das Flag „Touch Events API“ aus.
3. Starten Sie den Browser neu.

Wenden Sie zum Deaktivieren dieser Option in Firefox das folgende Verfahren an:

1. Navigieren Sie zu „about:config“.
2. Klicken Sie auf „Ich bin mir der Gefahren bewusst“.
3. Suchen Sie nach dem Einstellungsnamen „dom.w3c_touch_events.enabled“.
4. Aktualisieren Sie die Spalte „Wert“ auf 0.
5. Starten Sie den Browser neu.

Die Ergebnisse des Regeltests werden bei einer großen Datenmenge nicht in Internet Explorer 10 angezeigt.

Rückverfolgungsnummer: SAENG-3926

Problem: Wenn Sie mehrfach schnell hintereinander auf **Regeltest** klicken, werden die Ergebnisse einer großen Eingabedatenmenge möglicherweise nicht in Internet Explorer 10 angezeigt.

Workaround: Falls dieses Problem auftritt, versuchen Sie, einen der folgenden Schritte auszuführen:

- Schließen Sie das Fenster „Regeltest“ in Internet Explorer 10 und führen Sie den Test erneut aus.
- Prüfen Sie die Regelausführung in einem anderen Browser, wie Chrome oder Mozilla Firefox.

Dynamische Listen können nicht hinzugefügt werden, wenn ein Berichtplan über die Seite „Alle Pläne anzeigen“ bearbeitet wird.

Rückverfolgungsnummer: SAENG-5837

Problem: Sie können eine dynamische Liste nicht mit der Option Bearbeiten auf der Seite „Alle Pläne anzeigen“ zu einem vorhandenen Plan hinzufügen.

Workaround: Bearbeiten Sie den Plan auf der Seite Berichtplan, um eine dynamische Liste hinzuzufügen.

Administration

In einem von NetWitness Suite erfassten Konfigurationsauditereignis fehlt der Kontext, welcher Service geändert wurde.

Rückverfolgungsnummer: ASOC-8889

Problem: Der NetWitness Suite-Server erfasst nicht den anwendbaren Zielservice für Konfigurationsänderungen in Auditereignissen.

Workaround: Keiner.

Übermäßige Auditprotokolle werden beim Zugriff auf NetWitness Suite-Benutzeroberflächenseiten/Importieren/Exportieren/Anmelden/Abmelden protokolliert.

Rückverfolgungsnummer: ASOC-8916

Problem: NetWitness Suite erstellt eine übermäßige Menge Auditprotokolle, wenn sich NetWitness-Benutzer anmelden, abmelden, importieren, exportieren und über die NetWitness Suite-Benutzeroberfläche auf Seiten zugreifen.

Workaround: Keiner.

Auditprotokolle: SA_SERVER erfasst nicht den Wert für queryString.

Rückverfolgungsnummer: ASOC-8994

Problem: Wenn Dateiinhalte eines NetWitness Suite-Service geändert werden, zeigen die Auditprotokolle des NetWitness Suite-Servers nicht an, welche Datei der Benutzer geändert hat.

Workaround: Keiner.

In der E-Mail, die auf das Ablaufen des Passworts hinweist, fehlen Quelleninformationen.

Rückverfolgungsnummer: ASOC-9187

Problem: In der vom NetWitness Suite-Server gesendeten E-Mail, die auf das Ablaufen des Passworts hinweist, wird weder der Name noch die URL des sendenden NetWitness Suite-Servers genannt. Wenn mehrere NetWitness Suite-Server vorhanden sind, wissen Sie möglicherweise nicht, wo Sie Ihr Passwort aktualisieren können.

Workaround: Keiner.

In Auditprotokollen wird nicht die Seite (Name) angegeben, auf die zugegriffen wurde, wenn der Benutzer versucht, auf NetWitness Suite-Seiten zuzugreifen, für die der Benutzer keine Berechtigung hat.

Rückverfolgungsnummer: ASOC-9323

Problem: Wenn der Benutzer auf Seiten der NetWitness Suite-Benutzeroberfläche zuzugreifen versucht, ohne über die erforderlichen Berechtigungen zu verfügen, werden die Namen der Seiten, auf die der Benutzer zugegriffen hat, nicht von der Auditprotokollen erfasst.

Workaround: Keiner.

Ereignisquellenmanagement

Die Umbenennung des Log Collector- oder Log Decoder-Hostnamens wird nicht in der Ansicht „Ereignisquellenmanagement“ widergespiegelt.

Rückverfolgungsnummer: ASOC-9235

Problem: Wenn Sie unter **Administration > Seite „Host“** den „Namen“ der Log Collector- oder Log Decoder-Appliance bearbeiten, wird diese Änderung nicht in **Administration > Ereignisquellen > Seite „Verwalten“** in die Spalten „Log Collector“ oder „Log Decoder“ übertragen.

Workaround: Nachdem Sie einen Namen auf der Seite „Host“ aktualisiert haben, führen Sie die folgenden Schritte aus:

1. Führen Sie SSH auf der NetWitness Suite-Appliance durch.
2. Starten Sie den SMS-Service durch Ausführen des folgenden Befehls neu: service rsa-sms restart.
3. Warten Sie darauf, dass die Seite **Ereignisquellenverwaltung** wieder auf der NetWitness Suite-Benutzeroberfläche angezeigt wird und löschen Sie dann die Ereignisquellen mit den alten Log Collector- oder Log Decoder-Namen.

Wenn Sie Ereignisse von gelöschten Ereignisquellen sammeln, werden sie automatisch mit dem neuen Log Collector- oder Log Decoder-Namen wieder der Seite der Ereignisquellenverwaltung hinzugefügt.

Core-Services

Das Kontrollkästchen „SSL FIPS-Modus“ in der Ansicht „Services > Konfigurieren“ sollte für Brokers, Concentrators und Archivers deaktiviert werden, da eine Änderung des Wertes für das Kontrollkästchen die FIPS-Durchsetzung für den Service nicht deaktiviert.

Rückverfolgungsnummer: ASOC-41902

Problem: In 11.0.0.0 wird für den Broker, Concentrator und Archiver immer FIPS durchgesetzt und der Administrator hat nicht die Option, zwischen FIPS und Nicht-FIPS zu wechseln. Der Administrator kann das Kontrollkästchen „SSL FIPS-Modus“ verwenden, um den FIPS-Modus auf einem Log Decoder, Packet Decoder oder Log Collector ein- und auszuschalten.

Workaround: Keiner.

Broker-Systemrollen zeigen nicht die in Concentrator festgelegten angepassten Metaschlüssel an.

Rückverfolgungsnummer: ASOC-6749

Problem: Wenn benutzerdefinierte Metaschlüssel festgelegt wurden, sollten dieselben Metaschlüssel auch im Broker angezeigt werden. In den Broker-Systemrollen werden jedoch nicht die benutzerdefinierten Metaschlüssel angezeigt.

Workaround: Sie können die Concentrator-Sprachdatei und die benutzerdefinierte Indexdatei (sofern vorhanden) in den Broker kopieren, um die SDK-Metaschlüsselrollen zu den Systemrollen hinzuzufügen.

Fehler aufgrund einer ungültigen XML-Datei für mehrere MetaCallback bei der Option „Erweitert“ der benutzerdefinierte Feedkonfiguration

Rückverfolgungsnummer: ASOC-40867

Problem: NetWitness Suite bietet keine Unterstützung für das Hochladen von Feeds für die XML-Dateien, in denen mehrere Callbacks vorhanden sind.

Workaround: Der Ad-hoc-Feed kann über NwConsole oder direkt über die REST-URL des Decoder hochgeladen werden. Das gilt nicht für den wiederkehrenden Feed.

Möglichkeit zur Erstellung von Quell- und Ziel-IP-basierten Feeds mithilfe von CIDR oder Bereich

Rückverfolgungsnummer: SATCE-628

Problem: Bei der Erstellung eines quell- und zielbasierten Feeds auf einem Log Decoder wird nur der Quellmetaschlüssel ausgefüllt. Sie können keinen bereichsbasierten oder CIDR-Feed verwenden. Sie müssen jede einzelne IP-Adresse auflisten.

Workaround: Erstellen Sie zwei verschiedene Feeds mithilfe von IP-Adressen, dann können Sie CIDR in diesen Feeds verwenden.

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokument	Link
RSA NetWitness Suite 11.0 – Onlinedokumentation	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0 – Upgradeanweisungen	https://community.rsa.com/community/products/netwitness/110
RSA NetWitness Suite 11.0 – Upgradecheckliste	https://community.rsa.com/community/products/netwitness/110
Leitfaden zur Hardwarekonfiguration von RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA-Inhalte für RSA NetWitness Suite	https://community.rsa.com/community/products/netwitness/rsa-content

Kontaktieren des Kundendienstes

Verwenden Sie die folgenden Kontaktinformationen, wenn Sie Fragen haben oder Unterstützung benötigen.

RSA SecurCare	https://knowledge.rsasecurity.com
Tel.	1-800-995-5095, Option 3
Internationale Kontakte	https://germany.emc.com/support/rsa/contact/phone-numbers.htm
E-Mail	nwsupport@rsa.com
Community	https://community.rsa.com/community/rsa-customer-support
Basis-Support	Der technische Support für Ihre technischen Probleme ist von montags bis freitags von 08:00 bis 17:00 Uhr Ortszeit erreichbar.
Enhanced Support	Nur für Fehler des Schweregrads 1 und 2 ist der technische Support telefonisch an 365 Tagen im Jahr rund um die Uhr verfügbar.

Vorbereitung zum Kontaktieren des Kundendienstes

Wenn Sie sich mit dem Kundendienst in Verbindung setzen, sollten Sie sich an Ihrem Computer befinden. Halten Sie die folgenden Informationen bereit:

- Die Versionsnummer des verwendeten RSA NetWitness Suite-Produkts oder der Appliance
- Typ der verwendeten Hardware

Revisionsverlauf

Version	Datum	Beschreibung
1,0	24. Oktober 2017	GA