RSA NETWITNESS® PLATFORM

Versionshinweise

Für Version 11.2.1

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Inhalt

Einführung

In diesem Dokument sind Verbesserungen und Korrekturen in NetWitness Platform 11.2.1.0 aufgeführt. Lesen Sie dieses Dokument vor der Bereitstellung von oder der Aktualisierung auf NetWitness Platform 11.2.1.0.

Neuheiten

Die NetWitness Plattform Version 11.2.1.0 bietet folgende Verbesserungen.

NetWitness Analyse des Benutzer- und Entitätsverhaltens (UEBA)

Unterstützung für Remote Access Model. UEBA modelliert nun den Benutzerzugriff auf entfernte Computer mit dem Remote-Desktop-Protokoll. Dieses Modell definiert die häufig aufgerufenen entfernten Computer jedes Benutzers und zeigt jeden ungewöhnlichen Zugriff an. Weitere Informationen finden Sie im *Benutzerhandbuch zu RSA NetWitness UEBA*.

Behobene Probleme

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

Sicherheit

Rückverfolgungsnummer	Beschreibung
ASOC-61704	Yum-utils-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:2285
ASOC-61929	Kernelsicherheit Aktualisierung https://access.redhat.com/errata/RHSA-2018:2384
ASOC-60399	Openjdk-Sicherheitsupdate https://access.redhat.com/errata/RHSA-2018:2242
ASOC-59638	Gnupg2-Sicherheit Aktualisierung https://access.redhat.com/errata/RHSA-2018:2181

Rückverfolgungsnummer	Beschreibung
ASOC-62742	PostgreSQL Sicherheitsupdate https://access.redhat.com/errata/RHSA-2018:2557
ASOC-62744	BIND-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:2570
ASOC-59640	Python-Sicherheit Aktualisierung https://access.redhat.com/errata/RHSA-2018:2123

Server

Rückverfolgungsnummer	Beschreibung
SACE-10385/ SACE-10364	Die aktualisierten Seiten werden in der Ansicht „Integrität und Zustand“ nicht angezeigt.
SACE-9850	Bei der Sortierung in aufsteigender und absteigender Reihenfolge werden in der Ansicht „Diagramme“ keine Ergebnisse angezeigt.

Reporting

Rückverfolgungsnummer	Beschreibung
SACE-10456	Bei der Definition einer WHERE-Klausel wird in der Ansicht „Regeln“ nach jeder Bedingung automatisch eine zusätzliche Leerstelle hinzugefügt.

Untersuchen

Rückverfolgungsnummer	Beschreibung
SACE-10329	Wenn Sie eine Abfrage in der Ansicht „Ermittlungen“ durchführen, können Sie im Dialogfeld „Abfrage“ maximal sechs Zeichen eingeben.

Rückverfolgungsnummer	Beschreibung
SACE-10162	Die Ermittlungsabfrage mit Metagruppen unterstützt keine IP-Adressen im CIDR-Format.
SACE-10060	In Metaschlüsseln vom Typ „Ganzzahl“ werden im Drop-down-Feld „Intelli Sense“ keine Optionen für Operatoren angezeigt.

Integrität und Zustand

Rückverfolgungsnummer	Beschreibung
SACE-10237	Beim Export von Ereignisquellen wird eine ungültige CSV-Datei erstellt.

Event Stream Analysis

Rückverfolgungsnummer	Beschreibung
SACE-9793	Wenn der Whois-Service konfiguriert ist, tritt ein Fehler auf.

Core-Services

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

Rückverfolgungsnummer	Beschreibung
SACE-10222	Wenn der Concentrator neu gestartet wird, fehlt die Ausgabedatei.

Build-Nummern

In der folgenden Tabelle sind die Build-Nummern für die verschiedenen Komponenten von NetWitness Platform 11.2.1.0 aufgeführt.

Komponente	Versionsnummer

NetWitness Platform-Webserver	11.2.1-x
NetWitness Platform Decoder	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform Broker	11.2.1-x
NetWitness Platform Log Decoder	11.2.1-x
NetWitness Platform Archiver (Workbench)	11.2.1-x
NetWitness Platform Event Stream Analysis Server	11.2.1-x
NetWitness Platform Appliance	11.2.1-x
NetWitness Platform Archiver	11.2.1-x
NetWitness Platform-Cloud-Gateway-Server	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform-Konsole	11.2.1-x
NetWitness Platform Endpoint-Server	11.2.1-x
NetWitness Platform Investigate-Server	11.2.1-x
NetWitness Platform Legacy-Webserver	11.2.1-x
NetWitness Platform Log Player	11.2.1-x
NetWitness Platform Respond-Server	11.2.1-x
NetWitness Platform-SDK	11.2.1-x

Upgradeanweisungen

Die folgenden Upgradepfade werden für NetWitness Platform 11.2.1.0 unterstützt:

- RSA NetWitness® Platform 11.1.0.0 auf 11.2.1.0
- RSA NetWitness® Platform 11.1.0.1 auf 11.2.1.0
- RSA NetWitness® Platform 11.1.0.2 auf 11.2.1.0

- RSA NetWitness® Platform 11.1.0.3 auf 11.2.1.0
- RSA NetWitness® Platform 11.2.0.0 auf 11.2.1.0
- RSA NetWitness® Platform 11.2.0.1 auf 11.2.1.0

Weitere Informationen zum Upgrade auf 11.2.1.0 finden Sie in den Upgradeanweisungen im Abschnitt Installation und Upgrade.

Bekannte Probleme

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

Hinweis: Die bekannten Probleme der früheren Versionen von 11.2.1.0 sind möglicherweise in den Service Packs behoben. Weitere Informationen finden Sie im entsprechenden Patch oder den Patchversionshinweisen, die auf RSA Link verfügbar sind: https://community.rsa.com/.

UEBA

Doppelte Statistiken sind in den UEBA-Richtlinien aufgeführt.

Rückverfolgungsnummer: ASOC-70119

Problem: Wenn Sie eine Regel unter der UEBA-Richtlinie erstellt haben, werden unter „Statistik“ doppelte Werte angezeigt.

Workaround:

1. Melden Sie sich mit folgendem Befehl bei MongoDB an:
   ```
   mongo admin -u deploy_admin -p {Geben Sie das Passwort ein.}
   ```
2. Führen Sie in MongoDB den folgenden Befehl aus
   ```
   use sms;
   db.getCollection('sms_statdefinition').find({componentId
   :"presidioairflow"})
   db.getCollection('sms_statdefinition').deleteMany({componentId
   :"presidioairflow"})
   ```

Der UEBA-Dienst zeigt eine fehlerhafte Version an.

Rückverfolgungsnummer: ASOC-69605

Problem: Wenn Sie NetWitness Platform auf 11.2.1 aktualisiert haben, wird in der Ansicht **ADMIN > Hosts** eine fehlerhafte UEBA-Version angezeigt.

Workaround: Sie müssen den UEBA-Dienst aktualisieren.

1. Navigieren Sie zu **ADMIN > Hosts**.
2. UEBA-Host wählen
3. Klicken Sie in der Symbolleiste auf **Aktualisieren** > **Host ermitteln**.
4. Klicken Sie auf **Update beginnen**.

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokumentation	Standort-URL
RSA NetWitness Platform 11.2 Onlinedokumentation	https://community.rsa.com/community/products/netwitness/112
RSA NetWitness Platform 11.2 Anweisungen für das Upgrade	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D

Feedback zur Produktdokumentation

Sie können eine E-Mail an sahelpfeedback@emc.com senden, um Feedback zu den Dokumentation der RSA NetWitness Platform zu geben.

Kontaktieren der Kundenbetreuung

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 Platform-Produkts oder der Appliance.
- Typ der verwendeten Hardware

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

RSA Link	https://community.rsa.com Im Hauptmenü klicken Sie auf **Meine Fälle**.
Tel.	1-800-995-5095, Option 3
Internationale Kontakte	http://germany.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/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	Der technische Support ist nur für Fehler des Schweregrads 1 und 2 telefonisch an 365 Tagen im Jahr rund um die Uhr verfügbar.

Revisionsverlauf

Version	Datum	Beschreibung
1,0	17. Dezember 2018	Zweiter Entwurf