RSA NETWITNESS® PLATFORM

NetWitness UEBA – Quickstart-Handbuch

für RSA NetWitness® Platform 11.3

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

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 Nutzer 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 müssen beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

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

Juni 2019

Was ist NetWitness UEBA?

RSA NetWitness UEBA (Analyse des Nutzer- und Entitätsverhaltens) ist eine fortschrittliche Analyselösung zur Entdeckung, Untersuchung und Überwachung von riskanten Verhaltensweisen für alle Nutzer und Entitäten in Ihrer Netzwerkumgebung. NetWitness UEBA wird für folgende Zwecke verwendet:

- Erkennen von böswilligen Nutzern
- Erkennen von hochriskanten Verhaltensweisen
- Erkennen von Angriffen
- Untersuchen von aufkommenden Sicherheitsbedrohungen
- Identifizieren potenzieller Angreiferaktivitäten

Informationen zu diesem Handbuch

Dieses Handbuch enthält End-to-End-Anweisungen zur Konfiguration von NetWitness Platform UEBA und zur Verwendung von UEBA-Funktionen.

RSA NetWitness Platform 11.3 – Dokumentation in RSA Link

Die Produktdokumentation für NetWitness Platform ist nach funktionalen Gesichtspunkten aufgebaut. Wenn Sie nach einem bestimmten Benutzerhandbuch oder nach einer bestimmten Version suchen, gehen Sie zum Masterinhaltsverzeichnis der Version 11.x.

Verwenden Sie diese Links, um die Dokumentation der RSA NetWitness Platform 11.3 anzuzeigen. Beide Links stellen die gleiche Dokumentation in diesen beiden Formaten bereit:

- HTML-Benutzerhandbücher enthalten die neuesten Informationen zu derzeit unterstützten Versionen von 11.x: RSA NetWitness Platform 11.x Dokumentation.
- PDF-Benutzerhandbücher enthalten die Informationen für eine bestimmte Version: RSA NetWitness Platform 11.3 PDFs.

Verwenden Sie diese Links, um auf Dokumentationen zuzugreifen, die sich nicht auf eine bestimmte Version der Software beziehen:

- Benutzerhandbücher zur Hardwarekonfiguration: https://community.rsa.com/community/products/netwitness/hardware-setup-guides.
- Dokumentation für RSA-Inhalte wie Feeds, Parser, Anwendungsregeln und Berichte: https://community.rsa.com/community/products/netwitness/rsa-content.

Erste Schritte

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Anzeigen von Informationen zu Produktaktualisierungen, Verbesserungen und bekannten Problemen.	Versionshinweise
Verstehen von NetWitness UEBA.	*RSA NetWitness UEBA – Benutzerhandbuch*

Setup und Installation

Eigenständige Installation

Die folgenden Aufgaben müssen in der folgenden Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Überprüfen Sie die unterstützte Hardware.	Thema „Systemanforderungen“ im *Handbuch zur eigenständigen UEBA-Installation*
Überprüfen Sie die UEBA-Bereitstellung.	Thema „RSA NetWitness Eigenständige UEBA-Installation“ im *Handbuch zur eigenständigen UEBA-Installation*
Konfigurieren der Ports auf Ihrer Firewall.	Thema „RSA NetWitness Eigenständige UEBA-Installation“ im *Handbuch zur eigenständigen UEBA-Installation*
Installieren des NetWitness-Serverhosts.	Thema „Installationsaufgaben“ im *Handbuch zur eigenständigen UEBA-Installation*
Installieren des 11.3 Log Hybrid-Host.	Thema „Installationsaufgaben“ im *Handbuch zur eigenständigen UEBA-Installation*
Installieren und Konfigurieren von NetWitness UEBA.	Thema „Installationsaufgaben“ im *Handbuch zur eigenständigen UEBA-Installation*
Zuweisen der Rollen UEBA_Analysts und Analysts zu den UEBA-Nutzern.	„Rollenberechtigungen“ im Handbuch Systemsicherheit und Nutzerverwaltung

Neuinstallation

Die folgenden Aufgaben müssen in der folgenden Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Überprüfen Sie die unterstützte Hardware.	„Unterstützte Hardware“ im *Handbuch zur Installation physischer Hosts*
Überprüfen der UEBA-Architektur.	Thema „NetWitness Platform-Netzwerkarchitekturdiagramm“ im *Bereitstellungshandbuch*
Konfigurieren der Ports auf Ihrer Firewall.	„Netzwerkarchitektur und Ports“ im *Bereitstellungshandbuch*
Installieren von NetWitness Server-Host und anderen Komponenten.	„Aufgabe 1: Installieren von 11.3 auf dem NetWitness Server-Host (NW-Server)“ und „Aufgabe 2: Installieren von 11.3 auf anderen Komponentenhosts“ im *Handbuch zur Installation physischer Hosts* „Installieren des virtuellen NetWitness Platform-Host in virtueller Umgebung“ im *Handbuch zur Installation virtueller Hosts*
Installieren von UEBA.	„RSA NetWitness® UEBA“ im *Handbuch zur Installation physischer Hosts*
Zuweisen der Rollen UEBA_Analysts und Analysts zu den UEBA-Nutzern.	„Rollenberechtigungen“ im *Handbuch Systemsicherheit und Nutzerverwaltung*

Aktualisierung

Die folgenden Aufgaben müssen in der folgenden Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Stellen Sie das Endpoint Pack von RSA Live bereit, das die Dateikategorie Lua-Parser für die UEBA-Integration mit Endpoint enthält.	Während der Bereitstellung müssen Sie den Service Endpoint Log Hybrid Log Decoder angeben. Wählen Sie im Falle mehrerer Endpoint-Server alle Endpoint Log Hybrid Log Decoder-Services aus.
Aktivieren von Endpoint-Datenquellen wie Prozess und Registrierung, um Warnmeldungen in UEBA zu erzeugen.	„Aktivieren von Endpoint-Datenquellen“ in den *Anweisungen zur Aktualisierung*

Beschreibung	Referenzen
Aktivieren der UEBA-Indikator-Weiterleitung zur Übertragung der UEBA-Indikatoren zum NetWitness Respond-Server und zum Korrelationsserver zum Erstellen von Incidents.	„Aktivieren der UEBA-Indikator-Weiterleitung“ in den *Anweisungen zur Aktualisierung*
Nach dem Aktualisieren auf NetWitness Platform 11.3 ändert sich die Broker- oder Concentrator-UUID. Sie müssen die Core-Services von NetWitness Platform aktualisieren und die Broker- oder Concentrator-UUID aktualisieren.	„Aktualisieren der Broker- oder Concentrator-UUID“ in den *Anweisungen zur Aktualisierung*
Aktualisieren der Airflow-Konfiguration.	„Aktualisieren der Airflow-Konfiguration“ in den *Anweisungen zur Aktualisierung*
Neustart des Airflow-Planungsservice, nachdem die presidio_upgrade-DAG erfolgreich war.	„Neustart des Airflow-Planungsservice“ in den *Anweisungen zur Aktualisierung*

Investigation

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Untersuchen von Nutzern mit hohem Risiko	Thema „Untersuchen von Nutzern mit hohem Risiko“ im *RSA NetWitness UEBA – Benutzerhandbuch*
Untersuchen von Top-Warnmeldungen.	Thema „Untersuchen von Top-Warnmeldungen“ im *RSA NetWitness UEBA – Benutzerhandbuch*

Monitoring

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	

Beschreibung	Referenzen
Überprüfen von NetWitness UEBA-Metriken zu Integrität und Zustand.	Thema „Anzeigen von NetWitness UEBA-Metriken zu Integrität und Zustand“ im RSA NetWitness UEBA – Benutzerhandbuch
Überwachen von Integrität und Zustand von UEBA.	Thema „Überwachen von Integrität und Zustand von UEBA“ im RSA NetWitness UEBA – Benutzerhandbuch