RSA NETWITNESS® PLATFORM

NetWitness Endpoint – 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

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell 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 Dell 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 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 Endpoint?

RSA NetWitness Endpoint ist ein Erkennungs- und Reaktionstool für Endpunkte, mit dem das Verhalten aller Endpunkte im Netzwerk kontinuierlich überwacht wird, um eine umfassende Transparenz und Analyse für alle ausführbaren Dateien und Prozesse bereitzustellen. Es hilft bei der Erkennung neuer, unbekannter und gezielter Angriffe, hebt verdächtige Aktivitäten zur Untersuchung hervor, deckt anomale Verhaltensweisen auf und bestimmt das Ausmaß der Infektion, damit Analysten schneller auf fortgeschrittene Bedrohungen reagieren können.

Informationen zu diesem Handbuch

Dieses Handbuch enthält End-to-End-Anweisungen zur Konfiguration von NetWitness Platform Endpoint und zur Verwendung von Endpoint-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, wie NetWitness Endpoint funktioniert.	„Erste Schritte mit NetWitness Platform“ und „Untersuchen“ im *Leitfaden für die ersten Schritte mit NetWitness Platform*

Setup und Installation

Neuinstallation

Die folgenden Aufgaben müssen in der angegebenen Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Erwerben einer Lizenz für Endpoint Log Hybrid.	Leitfaden zum Lizenzierungsmanagement
Überprüfen der unterstützten Hardware.	„Unterstützte Hardware“ im *Handbuch zur Installation physischer Hosts*
Überprüfen der Endpunktarchitektur; planen der Bereitstellung basierend auf der Anzahl der Endpunkte, der Verteilung und dem Standort dieser Endpunkte; und wählen einer der folgenden Bereitstellungen: • Server mit einzigem Endpunkt • Server mit mehreren Endpunkten	„NetWitness Endpoint-Architektur“ im *Bereitstellungshandbuch*
Konfigurieren der Ports auf Ihrer Firewall.	„Netzwerkarchitektur und Ports“ im *Bereitstellungshandbuch*

Beschreibung	Referenzen
Installieren von NetWitness Server und anderen Komponenten. Bei einer Bereitstellung mit einem Server mit einzigem Endpunkt müssen Sie NetWitness Server, EndPoint Log Hybrid und ESA installieren. Für einen Server mit mehreren Endpunkten müssen Sie zusätzlich zu den oben genannten Komponenten einen zusätzlichen Endpoint Log Hybrid, NetWitness Broker sowie einen darauf installierten Endpoint Broker installieren.	– *Installationshandbuch für physische Hosts* für Anweisungen zur Einrichtung physischer Hosts – *Installationshandbuch für virtuelle Hosts* für Anweisungen zur Einrichtung von virtuellen Hosts
Installieren von Endpoint Log Hybrid.	„RSA NetWitness Endpoint“ im *Installationshandbuch für physische Hosts*
Überprüfen der installierten Services.	*Leitfaden für die ersten Schritte mit Hosts und Services*
Hinweis: Überprüfen Sie die Standard-Policies und ändern Sie diese entsprechend.	Thema „Endpunktquellen“ im *Konfigurationsleitfaden für Endpoint* *NetWitness Endpoint Agent-Installationshandbuch*
Installieren von Endpoint Agent auf Hosts.	

Upgrade

Die folgenden Aufgaben müssen in der angegebenen Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Upgrade von 10.6.5 auf 11.3 – Nach dem NetWitness Platform 11.3-Upgrade, Installation des Endpoint Log Hybrid und anderer Endpoint-Komponenten.	– *Upgradehandbuch für physische Hosts* für Anweisungen zum Upgrade von physischen Hosts – *Upgradehandbuch für virtuelle Hosts* für Anweisungen zum Upgrade von virtuellen Hosts
Aktualisierung von 11.x auf 11.3 – Aktualisieren des Endpoint-Servers und der Agents.	*Leitfaden zur Aktualisierung*
Durchführen eines Upgrades der Endpoint-Agents von 11.1.x und 11.2.x auf 11.3.	„Upgrade für Agents“ in der *Installationsanleitung zu Endpoint Agent*
Migrieren von NetWitness Endpoint 4.4.0.x auf NetWitness Platform.	*Leitfaden zur Migration von NetWitness Endpoint 4.4.0.x auf RSA NetWitness Platform 11.3*

Konfiguration

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Verstehen von NetWitness Endpoint und allgemeiner Aufgaben, die für die Konfiguration erforderlich sind.	„Übersicht über NetWitness Endpoint und Konfiguration von Endpoint Server“ im *Konfigurationsleitfaden für Endpoint*
Überprüfen von Gruppen und Policies für Agents.	Thema „Endpunktquellen“ im *Konfigurationsleitfaden für Endpoint*
Einrichten des RSA Live-Kontos und Überprüfen, ob die ESA-Inhalte und Anwendungsregeln für Endpunkte verfügbar sind. **Hinweis:** Der File Reputation Service wird in RSA Live automatisch aktiviert.	*Handbuch zum Live-Services-Management*
Erstellen einer rollenbasierten Zugriffskontrolle (Role-Based Access Control, RBAC).	„Rollenberechtigungen“ im Handbuch Systemsicherheit und Nutzerverwaltung
Konfigurieren der Datenaufbewahrungs-Policy.	„Konfigurieren der Datenaufbewahrung“ im *Konfigurationsleitfaden für Endpoint*
Managen von inaktiven Agents.	„Managen inaktiver Agents“ im *Konfigurationsleitfaden für Endpoint*

Investigation

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Verstehen, wie Ermittlungen funktionieren.	„So funktioniert NetWitness Investigate“ im *NetWitness Investigate – Benutzerhandbuch*.

Beschreibung	Referenzen
Konfigurieren von Ermittlungsansichten.	„Konfigurieren von NetWitness Investigate-Ansichten und Voreinstellungen“ im *NetWitness Investigate – Benutzerhandbuch*
Starten einer Ermittlung in verschiedenen Investigate-Ansichten.	„Starten einer Ermittlung“ im *NetWitness Investigate – Benutzerhandbuch*
Überprüfen der Best Practices für Dateien und Hosts und Einrichten der Ansicht „Untersuchen“ für Ermittlungen.	„Best Practices“ unter „Untersuchen von Dateien“ und „Untersuchen von Hosts“ im *NetWitness Endpoint – Benutzerhandbuch*
Untersuchen von Dateien.	„Untersuchen von Dateien“ im *NetWitness Endpoint – Benutzerhandbuch*
Untersuchen von Hosts.	„Untersuchen von Hosts“ im *NetWitness Endpoint – Benutzerhandbuch*
Untersuchen eines Prozesses.	„Untersuchen von Hosts“ im *NetWitness Endpoint – Benutzerhandbuch*
Analysieren von heruntergeladenen Dateien.	„Analysieren heruntergeladener Dateien“ im *NetWitness Endpoint – Benutzerhandbuch*
Ändern des Dateistatus und Korrektur.	„Ändern des Dateistatus oder Korrektur“ im *NetWitness Endpoint – Benutzerhandbuch*
Analysieren von Ereignissen.	„Analysieren von Ereignissen“ im *NetWitness Endpoint – Benutzerhandbuch* „Analysieren von Rohdaten und Metadaten in der Ansicht „Ereignisanalyse““, „Untersuchen von Metadaten in der Ansicht „Navigation““ und „Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse““ im *NetWitness Investigate – Benutzerhandbuch*

Antwort und Reporting

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Reagieren auf Endpunkt-Incidents.	*NetWitness Respond – Benutzerhandbuch*
Anzeigen von Berichten in Bezug auf Endpunktdaten.	*Benutzerhandbuch Reporting*

Wartung

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Überwachen von Integrität und Zustand.	Leitfaden Systemwartung

Integration (für Legacy NetWitness Endpoint)

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

Beschreibung	Referenzen
	
Konfigurieren von NetWitness Endpoint 4.4.x-Metadaten mit NetWitness Platform.	„Integrieren von NetWitness Endpoint 4.4.0.2 oder höher mit NetWitness Platform“ im *Konfigurationsleitfaden für Endpoint*
Konfigurieren des integrierten Betriebs von NetWitness Endpoint 4.4.x mit NetWitness Platform.	*RSA NetWitness Endpoint-Integrationsleitfaden*