RSA NETWITNESS® PLATFORM

Versionshinweise

Für Version 11.2.0.1

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

Versionshinweise

In diesem Dokument sind Korrekturen an NetWitness Platform 11.2.0.1 aufgeführt. Lesen Sie dieses Dokument vor der Bereitstellung von oder der Aktualisierung auf NetWitness Platform 11.2.0.1.

Behobene Probleme

In diesem Dokument werden die Probleme aufgeführt, die in der NetWitness-Plattform 11.2.0.1 behoben wurden.

Serverkorrekturen

Rückverfolgungsnummer	Beschreibung
ASOC-64089	Die Spracheinstellungen der Anwendung werden zurückgesetzt, wenn die Lokalisierung aktiviert ist. In NetWitness Platform 11.2.0.0 können Sie Französisch, Deutsch oder Japanisch nicht als Ihre Spracheinstellung festlegen.

Problembehebungen bei Malware Analysis

Rückverfolgungsnummer	Beschreibung
SACE-9874	Wenn Sie eine ältere Version des Hash-URL-Aufrufs verwenden, zeigt Malware Analysis nicht die Details des Anbieters von AntiVirus an.

Problembehebungen in Event Source Management

Rückverfolgungsnummer	Beschreibung
ASOC-62575	Bei Systemen mit einer großen Anzahl von aktiven Ereignisquellen kann der SMS-Dienst mit einem `java.lang.OutOfMemoryError: Java heap space`-Fehler abstürzen, wenn das System mit der Verarbeitung von Protokollstatistik-Nachrichten nicht Schritt halten kann.

Core-Korrekturen

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

Rückverfolgungsnummer	Beschreibung
SACE-10191	Der Log Decoder-Service wird wieder gestartet, wenn save.session.count auf „Auto“ gesetzt wird.
SACE-10283	Die MetaDB auf Log Decoder wird aufgrund falscher Parser-Verzeichnisstruktur wieder gestartet.
SACE-10336	Network Decoder stürzt aufgrund des 10G-Netzwerkkarten-Treibers ab.

Build-Nummern

In der folgenden Tabelle sind die Build-Nummern für die verschiedenen Komponenten von NetWitness Platform 11.2.0.1 aufgeführt.

Komponente	Versionsnummer
NetWitness Platform Decoder	11.2.0.1-9473.5
NetWitness Platform Concentrator	11.2.0.1-9473.5
NetWitness Platform Broker	11.2.0.1-9473.5
NetWitness Platform Log Decoder	11.2.0.1-9473.5
NetWitness Platform Archiver (Workbench)	11.2.0.1-9473.5
NetWitness Platform Event Stream Analysis-Server	11.2.0.1-448.5
NetWitness Platform Appliance	11.2.0.1-9473.5
NetWitness Platform Archiver	11.2.0.1-9473.5
NetWitness Platform-Konsole	11.2.0.1-9473.5
NetWitness Platform Legacy-Webserver	11.2.0.1-181010193532.5
NetWitness Platform Log Player	11.2.0.1-9473.5
NetWitness Platform-SDK	11.2.0.1-9473.5

Anweisungen zur Aktualisierung

Sie müssen die Informationen lesen und diese Verfahren für die Aktualisierung von NetWitness Platform Version 11.2.0.1 befolgen.

Die folgenden Aktualisierungspfade werden für NetWitness Platform 11.2.0.1 unterstützt:

- NetWitness Platform 11.2.0.0 auf 11.2.0.1
- NetWitness Platform 11.1.0.3 auf 11.2.0.1

Für 11.2.0.0 unterstützte Aktualisierungspfade finden Sie im *Leitfaden für die Aktualisierung von Version 11.0.x.x oder 11.1.x.x auf 11.2*.

Sie können den 11.2.0.1-Patch mit einer der folgenden Optionen aktualisieren:

- Wenn der NetWitness-Server über eine Internetverbindung zu Live-Services verfügt, kann die NetWitness Platform-Benutzeroberfläche verwendet werden, um den Patch anzuwenden.
- Wenn keine Internetverbindung vom NetWitness-Server zu Live-Services besteht, kann die Befehlszeilenoberfläche (CLI) verwendet werden, um den Patch anzuwenden.

Aufgaben bei der Aktualisierung

Aufgabe 1: Decoder-Services deaktivieren

Bevor Sie auf 11.2.0.1 aktualisieren, müssen Sie die Capture AutoStart auf Network Decoderund Network Hybrid-Services deaktivieren.

So deaktivieren Sie das Capture Autostart-Feld:

1. Navigieren Sie zu **ADMIN** > **Services**.
   Die Ansicht „Administration“ > „Services“ wird angezeigt.
2. Wählen Sie einen Network Decoder oder oder Network Hybrid-Dienst aus und wählen Sie  > Ansicht > Config
   .Die Ansicht „Services-Konfiguration“ für den ausgewählten Network Decoder oder Network Hybrid wird angezeigt.
3. Im Fenster Decoder **Konfiguration** wählen Sie das Feld **Capture Autostart** aus und klicken auf **Anwenden**.

Aufgabe 2: Aktualisieren des Patches

Sie können eine der folgenden Aktualisierungsmethoden basierend auf Ihrer Internetverbindung auswählen.

Onlinemethode (Verbindung mit Live-Services): Aktualisieren mithilfe der NetWitness-Benutzeroberfläche

Sie können diese Methode verwenden, wenn der NetWitness-Server mit Live-Services verbunden ist, und können das Paket abrufen.

Hinweis: Ein Update von 11.1.0.3 auf 11.2.0.1 mit der Onlinemethode ist verfügbar. Wenn Sie von 11.1.0.x auf 11.2.0.1 aktualisieren, müssen Sie zuerst ein Upgrade auf NetWitness Platform 11.2.0.0 durchführen und dann auf 11.2.0.1 aktualisieren.

Hinweis: Wenn der NetWitness-Server keinen Zugriff auf Live-Services hat, verwenden Sie die Offlinemethode (keine Verbindung mit Live-Services): Aktualisieren mithilfe der Befehlszeilenoberfläche .

Voraussetzungen

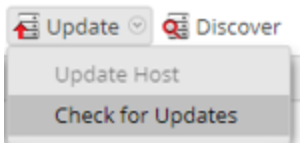
Achten Sie auf Folgendes:

1. Die Option „Informationen über neue Aktualisierungen täglich automatisch herunterladen“ ist aktiviert und wird in **ADMIN** > **System** > **Aktualisierungen** angewendet.
2. Navigieren Sie zu **ADMIN** > **Hosts** > **Aktualisierung** > **Nach Updates suchen**, um nach Updates zu suchen. Auf der Seite „Host“ wird der Status **Aktualisierung verfügbar** angezeigt.
3. 11.2.0.1 ist in der Spalte „Update-Version“ verfügbar.

Hinweis: Wenn Sie über benutzerdefinierte Zertifikate verfügen, verschieben Sie alle benutzerdefinierten Zertifikate aus dem Verzeichnis `/etc/pki/nw/trust/import/` in `/root/cert`. Um die Zertifikate zu verschieben, gehen Sie wie folgt vor:
1.) `mkdir /root/cert.`
2.) `mv /etc/pki/nw/trust/import/* /root/cert.`

Verfahren

1. Navigieren Sie zu **ADMIN** > **Hosts**.
2. Wählen Sie den NetWitness-Serverhost (nw-server) aus.
3. Überprüfen Sie die neuesten Aktualisierungen.



4. Aktualisierung verfügbar wird in der Spalte **Status** angezeigt, wenn für die ausgewählten Hosts im lokalen Update-Repository ein Versionsupdate vorhanden ist.

5. Wählen Sie **11.2.0.1** aus der Spalte **Update-Version** aus.
   Gehen Sie in folgenden Fällen wie folgt vor:
   - Wenn Sie ein Dialogfeld mit den wichtigsten Funktionen der Aktualisierung sowie Informationen über die Aktualisierungen anzeigen möchten, klicken Sie auf das Informationssymbol ( ) rechts neben der Versionsnummer der Aktualisierung.
   - Wenn Sie die gewünschte Version nicht finden können, wählen Sie **Aktualisieren > Nach Updates suchen** aus, um das Repository auf alle verfügbaren Aktualisierungen zu prüfen. Wenn eine Aktualisierung verfügbar ist, wird die Meldung „Es sind neue Hostaktualisierungen verfügbar“ angezeigt und die Spalte **Status** wird automatisch aktualisiert und zeigt Aktualisierung verfügbar an. Standardmäßig werden nur die unterstützten Aktualisierungen für den ausgewählten Host angezeigt.
6. Klicken Sie in der Symbolleiste auf **Aktualisieren** > **Host ermitteln**.
7. Klicken Sie auf **Update beginnen**.
8. Klicken Sie auf **Host neu starten**.
9. Wiederholen Sie Schritte 6 bis 8 für andere Hosts.

Hinweis: Sie können erst mehrere Hosts zum gleichzeitigen Aktualisieren auswählen, nachdem Sie den NetWitness-Adminserver aktualisiert und neu gestartet haben. Alle ESA-, Endpoint Insights- und Malware Analysis-Hosts müssen auf dieselbe Version wie die des NW-Adminservers oder NetWitness-Adminservers aktualisiert werden.

Hinweis: Nicht alle Komponenten wurden für 11.2.0.1 geändert. Nachdem Sie die Aktualisierungsschritte durchgeführt haben, ist es deshalb normal, dass einige Komponenten mit verschiedenen Versionsnummern angezeigt werden. Eine Liste der Komponenten, die für diese Version aktualisiert wurden, finden Sie unter Build-Nummern.

Offlinemethode (keine Verbindung mit Live-Services): Aktualisieren mithilfe der Befehlszeilenoberfläche

Sie können diese Methode verwenden, wenn der NetWitness-Server nicht mit Live-Services verbunden ist.

Voraussetzungen

Achten Sie auf Folgendes:

- Sie haben die folgende Datei, die alle NetWitness Platform 11.2.0.1-Dateien enthält, über „RSA Link (https://community.rsa.com/) > NetWitness Platform > RSA NetWitness Logs and Network > Downloads > RSA Downloads“ in ein lokales Verzeichnis heruntergeladen:
  `netwitness-11.2.0.1.zip`

Verfahren

Sie müssen die Schritte zur Aktualisierung für NW-Adminserver und für Komponentenserver durchführen.

Hinweis: Wenn Sie von 11.1.0.3 auf 11.2.0.1 aktualisieren, müssen Sie NetWitness Platform 11.2.0.0-Dateien „netwitne-11.2.0.0.zip“ herunterladen und zusammen mit den 11.2.0.1-Dateien im Bereitstellungsordner einrichten. Wenn Sie von 11.1.0.x auf 11.2.0.1 aktualisieren, müssen Sie zuerst ein Upgrade auf NetWitness Platform 11.2.0.0 durchführen und dann auf 11.2.0.1 aktualisieren.

Hinweis: Wenn Sie die Befehle von der PDF in das Linux SSH-Terminal kopieren und einfügen, funktionieren die Zeichen nicht. Es wird empfohlen, die Befehle einzugeben.

1. Stellen Sie 11.2.0.1 bereit, indem Sie ein Verzeichnis auf dem NetWitness-Server unter `/tmp/upgrade/11.2.0.1` erstellen und das ZIP-Paket extrahieren.
   `unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1`

   Hinweis: Wenn Sie das ZIP-Paket in das erstellte Bereitstellungsverzeichnis kopiert haben, um es zu entpacken, stellen Sie sicher, dass Sie die anfängliche ZIP-Datei, die Sie in den Bereitstellungsspeicherort kopiert haben, löschen, nachdem Sie sie extrahiert haben.
2. Initialisieren Sie die Aktualisierung mit dem folgenden Befehl:
   `upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade`
3. Aktualisieren Sie den NetWitness-Server mit dem folgenden Befehl:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1`
4. Wenn die Aktualisierung des Komponentenhosts erfolgreich ist, starten Sie den Host von der NetWitness-Benutzeroberfläche neu.
5. Wiederholen Sie die Schritte 3 und 4 für jeden Komponentenhost und ändern Sie dabei die IP-Adresse auf die des Komponentenhosts, der aktualisiert wird.

Hinweis: Sie können die Versionen aller Hosts mit dem Befehl `upgrade-cli-client --list` auf dem NetWitness-Server überprüfen. Wenn Sie den Hilfeinhalt von `upgrade-cli-client` anzeigen möchten, verwenden Sie den Befehl `upgrade-cli-client --help`.

Hinweis: Wenn während des Aktualisierungsprozesses der folgende Fehler angezeigt wird:
`2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671] o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error; protocol method: #method<connection.close>(reply-code=320, reply-text=CONNECTION_FORCED - broker forced connection closure with reason 'shutdown', class-id=0, method-id=0)`
, wird der Patch ordnungsgemäß installiert. Es ist keine Aktion erforderlich. Wenn beim Aktualisieren eines Hosts auf eine neue Version weitere Fehler auftreten, wenden Sie sich an den Kundensupport (Kundenbetreuung kontaktieren).

Anweisungen für Aktualisierung des externen Repository über die CLI

Hinweis: Das einzurichtende externe Repository sollte ein 11.2.0.1-Repository sein, das unter demselben Verzeichnis wie in 11.2.0.0 festgelegt ist.

1. Stellen Sie 11.2.0.1 bereit, indem Sie ein Verzeichnis auf dem NetWitness-Server unter `/tmp/upgrade/11.2.0.1` erstellen und das ZIP-Paket extrahieren.
   `unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1`

   Hinweis: Wenn Sie das ZIP-Paket in das erstellte Bereitstellungsverzeichnis kopiert haben, um es zu entpacken, stellen Sie sicher, dass Sie die anfängliche ZIP-Datei, die Sie in den Bereitstellungsspeicherort kopiert haben, löschen, nachdem Sie sie extrahiert haben.

2. Initialisieren Sie die Aktualisierung mit dem folgenden Befehl:
   `upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade`
3. Aktualisieren Sie den NetWitness-Server mit dem folgenden Befehl:
   `upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1`
4. Wenn die Aktualisierung des Komponentenhosts erfolgreich ist, starten Sie den Host von der NetWitness-Benutzeroberfläche neu.
5. Wiederholen Sie die Schritte 3 und 4 für jeden Komponentenhost und ändern Sie dabei die IP-Adresse auf die des Komponentenhosts, der aktualisiert wird.

Hinweis: Sie können die Versionen aller Hosts mit dem Befehl `upgrade-cli-client --list` auf dem NetWitness-Server überprüfen. Wenn Sie den Hilfeinhalt von `upgrade-cli-client` anzeigen möchten, verwenden Sie den Befehl `upgrade-cli-client --help`.

Hinweis: Wenn während des Aktualisierungsprozesses der folgende Fehler angezeigt wird:
`2017-11-02 20:13:26.580 ERROR 7994 — [ 127.0.0.1:5671] o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error; protocol method: #method<connection.close>(reply-code=320, reply-text=CONNECTION_FORCED - broker forced connection closure with reason 'shutdown', class-id=0, method-id=0)`
, wird der Patch ordnungsgemäß installiert. Es ist keine Aktion erforderlich. Wenn beim Aktualisieren eines Hosts auf eine neue Version weitere Fehler auftreten, wenden Sie sich an den Kundensupport (Kundenbetreuung kontaktieren).

Aufgaben nach der Aktualisierung

Aufgabe 1 (optional): Verschieben der benutzerdefinierten Zertifikate

Verschieben Sie die benutzerdefinierten Zertifikate aus dem externen Verzeichnis in das Verzeichnis `/etc/pki/nw/trust/import`.

Aufgabe 2 (bedingungsabhängig): Neukonfigurieren der PAM-Radius-Authentifizierung

Wenn Sie die PAM-Radius-Authentifizierung in 11.2.x.x mit dem `pam_radius`-Paket konfiguriert haben, müssen Sie sie in 11.2.0.1 mit dem `pam_radius_auth`-Paket neu konfigurieren.

Sie müssen die unten stehenden Befehle auf dem NW-Server ausführen, auf dem sich der Admin-Server befindet.

Hinweis: Wenn Sie `pam_radius` in 11.x.x.x konfiguriert haben, führen Sie die unten stehenden Schritte aus, um die vorhandene Version zu deinstallieren, oder fahren Sie mit Schritt 2 fort.

Schritt 1: Überprüfen der vorhandenen Seite und Deinstallieren der vorhandenen `pam_radius`

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

Schritt 2: Führen Sie für die Installation des `pam_radius_auth` -Pakets den folgenden Befehl aus:

```
yum install pam_radius_auth
```

Schritt 3: Bearbeiten Sie die RADIUS-Konfigurationsdatei `/etc/raddb/server` wie folgt und fügen Sie die Konfigurationen für dem Radius-Server hinzu:

```
# server[:port] shared_secret timeout (s)
server secret 3
```

Beispiel: 111.222.33.44 secret 1

Schritt 4: Bearbeiten Sie die NetWitness-Server-PAM-Konfigurationsdatei `/etc/pam.d/securityanalytics`, um die folgende Zeile hinzuzufügen. Wenn die Datei nicht vorhanden ist, erstellen Sie sie und fügen Sie die folgende Zeile hinzu:

```
auth sufficient pam_radius_auth.so
```

Schritt 5: Stellen Sie die Schreibberechtigung für `/etc/raddb/server`-Dateien mit dem folgenden Befehl bereit.

```
chown netwitness:netwitness /etc/raddb/server
```

Schritt 6: Führen Sie zum Kopieren der `pam_radius_auth`-Bibliothek den folgenden Befehl aus:

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

Schritt 7: Führen den folgenden Befehl aus, um den Jetty-Server nach Vornehmen von Änderungen an `pam_radius_auth`-Konfigurationen neu zu starten.

```
systemctl restart jetty
```

Aufgabe 3: Neustart des Respond-Servers

Starten Sie den Respond-Server neu:

```
systemctl restart rsa-nw-respond-server
```

Aufgabe 4: Aktualisieren des Standorts des 10G-Treibers

Sie müssen den 10G-Treiber an der richtigen Stelle im aktuellen Kernel aktualisieren.

Schritt 1: Wenn Sie 10G-Decoder verwenden, führen Sie die folgenden Befehle nach dem 11.2.0.1-Upgrade aus und starten Sie die Decoder-Appliance erneut. Klicken Sie auf **Y**, wenn Sie zum Überschreiben aufgefordert werden.

- cp /var/lib/dkms/ixgbe-zc/5.3.7.14/$(uname -r)/x86_64/module/ixgbe_zc.ko.xz /lib/modules/$(uname -r)/extra/
- cp /var/lib/dkms/i40e-zc/2.4.6.14/$(uname -r)/x86_64/module/i40e_zc.ko.xz /lib/modules/$(uname -r)/extra/
- `cp /var/lib/dkms/pfring/6.5.0.14/$(uname -r)/x86_64/module/pf_ring.ko.xz /lib/modules/$(uname -r)/extra/`

Schritt 2: Wenn Sie das Capture **Autostart-Feld** deaktiviert haben, wie in Aufgabe 1: Decoder-Services deaktivieren. Sie müssen den **Capture AutoStart** auf den Network Decoder und Network Hybrid-Diensten neu aktivieren.

So aktivieren Sie das Capture Autostart-Feld:

1. Navigieren Sie zu **ADMIN** > **Services**.
   Die Ansicht „Administration“ > „Services“ wird angezeigt.
2. Wählen Sie einen Network Decoder oder Network Hybrid-Service aus und wählen Sie  > **Ansicht** > **Config**.
   Die Ansicht „Services-Konfiguration“ für den ausgewählten Network Decoder oder Network Hybrid wird angezeigt.
3. Aktivieren Sie im Bereich **Decoder Konfiguration** das Feld **Capture AutoStart** und klicken Sie auf **Anwenden**.

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokument	Standort
RSA NetWitness Platform 11.2.0.0 Onlinedokumentation	https://community.rsa.com/community/products/netwitness/112

Feedback zur Produktdokumentation

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

Kontaktieren des Kundendienstes

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

RSA Link	https://community.rsa.com/
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/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	Der technische Support ist nur für Fehler des Schweregrads 1 und 2 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 Platform-Produkts oder der Appliance
- Typ der verwendeten Hardware

Revisionsverlauf

Version	Datum	Beschreibung
0,1	25. Oktober	Letzter Entwurf