RSA NETWITNESS® SUITE

AWS-Bereitstellungshandbuch

für Version 11.0

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.

Februar 2018

Inhalt

AWS-Bereitstellungsübersicht

Vor der Bereitstellung von RSA NetWitness® Suite in Amazon Web Services (AWS) müssen Sie folgende Voraussetzungen erfüllen:

- Sie kennen die Anforderungen Ihres Unternehmens.
- Sie kennen den Umfang einer NetWitness Suite-Bereitstellung.

Wenn Sie bereit sind, mit der Bereitstellung zu beginnen, führen Sie folgende Schritte aus:

- Stellen Sie sicher, dass Sie über eine „Throughput“-Lizenz für NetWitness Suite verfügen.
- Für die Paketerfassung in AWS können Sie eine der folgenden Lösungen von Drittanbietern erwerben. Wenn Sie sich für einen dieser Drittanbieter entscheiden, werden Ihnen ein Ansprechpartner und ein Professional Services-Techniker zugewiesen, die eng mit den RSA-Mitarbeitern zusammenarbeiten.
  - Gigamon® GigVUE 5.0
  - f5BIG-IP 12.1.0

Empfehlungen zur AWS-Umgebung

AWS-Instanzen haben dieselbe Funktionalität wie die NetWitness Suite-Hardwarehosts. RSA empfiehlt, die folgenden Aufgaben bei der Einrichtung Ihrer AWS-Umgebung durchzuführen.

- Gehen Sie je nach Ressourcenanforderungen der einzelnen Komponenten bei der Nutzung des Systems gemäß bewährten Vorgehensweisen vor und weisen Sie Elastic Block Store (EBS)-Volumes entsprechend zu.
- Vergewissern Sie sich, dass die Rechenkapazitäten eine Schreibgeschwindigkeit bieten, die um mindestens 10 % über der erforderlichen Erfassungs- und Verarbeitungsrate für die Bereitstellung liegt.
- Erstellen Sie das Concentrator-Verzeichnis für die Indexdatenbank auf der Provisioned IOPS-SSD.

Abkürzungen und andere in diesem Leitfaden verwendete Terminologie

Abkürzungen	Beschreibung
AMI	Amazon Machine Image
AWS	Amazon Web Services
BYOL	„Bring your own“-Lizenzierung
CPU	Zentrale Verarbeitungseinheit (Central Processing Unit)
Dedizierte Instanz	Dedizierte AWS-Instanzen werden in einer VPC auf Hardware ausgeführt, die einem einzigen Kunden zugewiesen ist. Dedizierte Instanzen sind auf Hosthardwareebene physisch von Instanzen isoliert, die zu anderen AWS-Konten gehören. Möglicherweise nutzen dedizierte Instanzen Hardware gemeinsam mit anderen Instanzen des gleichen AWS-Kontos, die keine dedizierten Instanzen sind. Weitere Informationen zu dedizierten Instanzen finden Sie in der AWS-Dokumentation „Amazon EC2 – Dedicated Instances“ (https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/).

Abkürzungen	Beschreibung
EBS-Optimierung	Eine für Amazon EBS optimierte Instanz verwendet einen optimierten Konfigurationsstapel und bietet zusätzliche, dedizierte Kapazität für Amazon EBS-I/Os. Diese Optimierung bietet für Ihre EBS-Volumes die beste Performance, da Konflikte zwischen Amazon EBS-I/Os und dem restlichen Datenverkehr von Ihrer Instanz minimiert werden. Weitere Informationen zu EBS-optimierten Instanzen finden Sie in der AWS-Dokumentation „Amazon EBS-optimierte Instances“ (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html).
EBS-Volume	Ein Elastic Block Store (EBS)-Volume ist ein hochverfügbarer und zuverlässiger Speichervolume, den Sie an alle laufenden Instanzen anhängen können, die sich in derselben Availability Zone befinden. Weitere Informationen zu EBS-Volumes finden Sie in der AWS-Dokumentation „Amazon EBS-Volumes“ (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html).
EC2-Instanz	Virtueller Server in der AWS Elastic Compute Cloud (EC2) für die Ausführung von Anwendungen in der AWS-Infrastruktur. Siehe auch **Instanz**.

Abkürzungen	Beschreibung
Optimierte Netzwerkfunktionen aktiviert	Die optimierten Netzwerkfunktionen bieten höhere Bandbreite, eine bessere PPS-Performance (Pakete pro Sekunde) sowie konsistent geringere Latenzen zwischen Instanzen. Wenn Ihre PPS-Rate die Obergrenze erreicht zu haben scheint, sollten Sie erwägen, auf die optimierten Netzwerkfunktionen umzusteigen, da Sie wahrscheinlich die oberen Schwellenwerte des Treibers der VM-Netzwerkschnittstelle (VIF) erreicht haben. Weitere Informationen zu optimierten Netzwerkfunktionen finden Sie in der AWS-Dokumentation „How do I enable and configure enhanced networking on my EC2 instances“ (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/).
EPS	Ereignisse pro Sekunde
GB	Gigabyte. 1 GB = 1.000.000.000 Byte
Gbit	Gigabit. 1 Gbit = 1.000.000.000 Bit.
Gbit/s	Gigabit pro Sekunde oder Milliarden Bit pro Sekunde. Maßeinheit für die Bandbreite eines digitalen Datenübertragungsmediums, z. B. Glasfaser.
GHz	Gigahertz. 1 GHz = 1.000.000.000 Hz
HDD	Festplattenlaufwerk
Instanz	Ein virtueller Host in AWS (d. h. eine virtuelle Maschine oder Server in der AWS-Infrastruktur, auf dem die Services oder Anwendungen ausgeführt werden). Siehe auch **EC2-Instanz**.
Instanztyp	Gibt die erforderlichen CPU- und RAM-Werte für eine Instanz an. Weitere Informationen zu den Instanztypen finden Sie in der AWS-Dokumentation „Amazon EC2-Instance-Typen“ (https://aws.amazon.com/ec2/instance-types/).

Abkürzungen	Beschreibung
IOPS	Eingabe-/Ausgabevorgänge pro Sekunde (Input/Output Operations per Second).
Mbit/s	Megabit pro Sekunde oder Millionen Bit pro Sekunde. Maßeinheit für die Bandbreite eines digitalen Datenübertragungsmediums, z. B. Glasfaser.
Lokal	Lokale Hosts werden vor Ort auf Computern installiert und ausgeführt (nicht in AWS), d. h. im Gebäude des Unternehmens, das die Hosts verwendet.
PPS	Pakete pro Sekunde
RAM	Random Access Memory (auch als Arbeitsspeicher bezeichnet)
Sicherheitsgruppe	Satz von Firewallregeln. Eine umfassende Liste der Ports, die Sie für alle NetWitness Suite-Komponenten einrichten müssen, finden Sie unter „Netzwerkarchitektur und Ports“ in RSA Link (https://community.rsa.com/docs/).
SSD	Solid-State-Laufwerk
Tag	Eine aussagekräftige Kennung für die AWS-Instanz.
Tap-Anbieter	Netzwerk-Tapping-Anbieter
vCPU	Virtual Central Processing Unit (auch als virtueller Prozessor bezeichnet)
VM	Virtuelle Maschine
VPC	Virtuelle Public Cloud
vRAM	Virtual Random Access Memory (auch als virtueller Arbeitsspeicher bezeichnet)

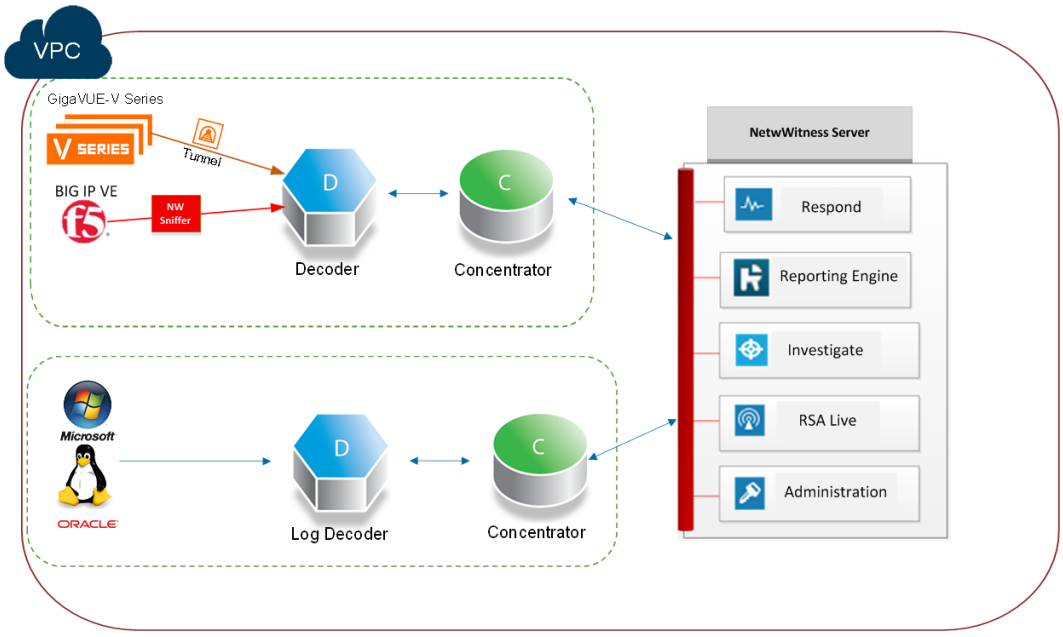
AWS-Bereitstellungsszenarien

Die folgenden Diagramme zeigen einige gängige Szenarien für die AWS-Bereitstellung. In den Diagrammen gilt Folgendes:

- **GigaVUE Series** (Gigamon®-Lösung) ist eine Agent-basierte Lösung, die **Tunneling** verwendet (implementiert vom NetWitness Suite-Administrator), um die Paketdatenerfassung in AWS zu erleichtern.
- **BIG-IP** (f5®-Lösung) ist eine Lösung zum Lastenausgleich, die einen Packet Decoder verwendet, der als Sniffer fungiert (angepasst vom NetWitness Suite-Administrator), um die Paketdatenerfassung in AWS zu erleichtern.
- **Decoder** erfasst Paketdaten. Der **Decoder** erfasst, analysiert und rekonstruiert sämtlichen Netzwerkdatenverkehr der Ebenen 2 bis 7.
- **Log Decoder** sammelt Protokolle. Der **Log Decoder** sammelt Protokollereignisse aus Hunderten Geräten und Ereignisquellen.
- Der **Concentrator** indiziert aus dem Netzwerk extrahierte Metadaten oder Protokolldaten und stellt sie für unternehmensweite Abfragen und Echtzeitanalysen zur Verfügung. Er erleichtert auch das Reporting und die Erzeugung von Warnmeldungen.
- NetWitness-Server hostet **Respond**, **Reporting**, **Investigate**, **Live Content Management**, **Administration** und andere Aspekte der Benutzeroberfläche.

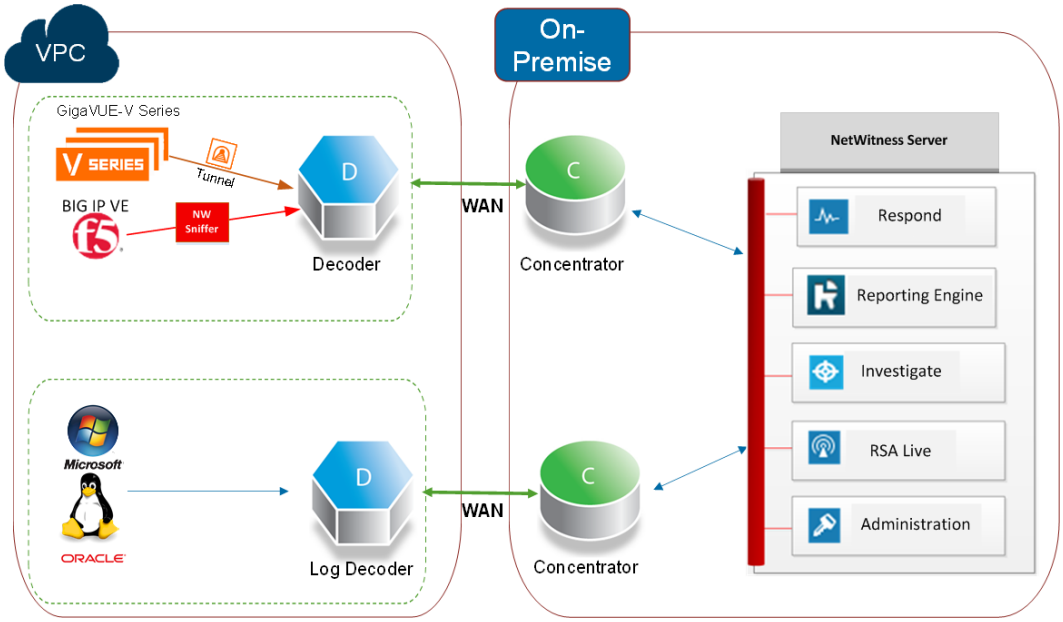
Full NetWitness Suite Stack-VPC-Transparenz (Paketlösung)

Dieses Diagramm zeigt alle NetWitness Suite-Komponenten (Full Stack), die in AWS bereitgestellt werden.


VPC
GigaVUE-V Series
V SERIES
Tunnel
BIG IP VE
NW Sniffer
D
Decoder
C
Concentrator
NetwWitness Server
Respond
Reporting Engine
Investigate
RSA Live
Administration
Microsoft
ORACLE
D
Log Decoder
C
Concentrator

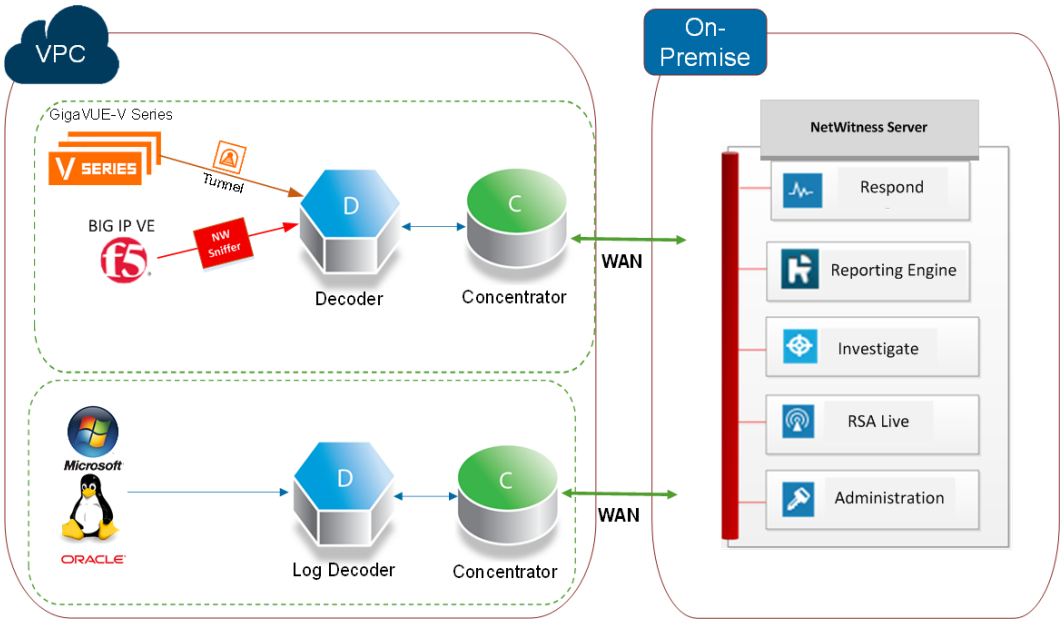
Hybrid-Bereitstellung – Decoder und Log Decoder (Paketlösung)

In diesem Diagramm sind der Decoder und Log Decoder dargestellt, die in AWS bereitgestellt sind, sowie alle anderen NetWitness Suite Komponenten, die an Ihrem Standort bereitgestellt werden.



Hybrid-Bereitstellung – Decoder, Log Decoder und Concentrator (Paketlösung)

In diesem Diagramm sind der Decoder, Log Decoder und Concentrator dargestellt, die in AWS bereitgestellt sind, sowie alle anderen NetWitness Suite Komponenten, die an Ihrem Standort bereitgestellt werden.



Voraussetzungen

Bevor Sie mit der Integration beginnen, benötigen Sie Folgendes:

- Zugriff auf AWS-Konsole
- Weiterleitungsfähiges Netzwerk (und korrekte AWS-Sicherheitsgruppen) für die Container, die Daten an den NetWitness Suite-Decoder übertragen.

Unterstützte Services

RSA bietet die folgenden NetWitness Suite-Services.

- NetWitness-Server
- Archiver
- Broker
- Concentrator

- Event Stream Analysis
- Log Decoder
- Decoder
- Remote Log Collector

AWS-Bereitstellung

Dieses Thema enthält die Regeln und allgemeinen Aufgaben, die Sie bei der Bereitstellung von RSA NetWitness® Suite-Komponenten in AWS befolgen müssen.

Regeln

Sie müssen die folgenden Regeln befolgen, wenn Sie NetWitness Suite in AWS bereitstellen.

- Stellen Sie mindestens einmal nach der Bereitstellung über SSH eine Verbindung mit der NetWitness Suite-Instanz her, um das System zu initialisieren.
- Legen Sie vor Aktivierung der vordefinierten Dashboards die Standarddatenquelle auf der Reporting Engine-Konfigurationsseite fest.
- Wenn Sie die Packet Decoder-Instanz neu starten, wird der Tunnel nicht beibehalten. Erstellen Sie den Tunnel im Packet Decoder erneut und starten Sie den Decoder-Service neu.
- Verwenden Sie immer private IP-Adressen, wenn Sie AWS-NetWitness Suite-Instanzen bereitstellen.

Hinweis: Wenn Sie dem Netwitness-Serverhost eine öffentliche IP-Adresse zuweisen, aktualisieren Sie die Konfigurationsdatei /etc/nginx/conf.d/nginx.conf wie folgt:

```
location /nwrpmrepo
{
alias /var/lib/netwitness/common/repo;
index index.html index.htm;
allow <Subnet-Gateway>/Subnet mask ;
#example
# allow 10.0.0.1/25;
deny all;
autoindex on;
}
```

Checkliste

Schritt	Beschreibung	√
1	Einrichten der AWS-Umgebung	
2	Suchen von NetWitness Suite-AMIs	

Schritt	Beschreibung	√
3	Starten einer Instanz und Konfigurieren eines Hosts	
4	Konfigurieren von Hosts (Instanzen) in NetWitness Suite	
5	Konfigurieren der Paketerfassung	

Einrichten der AWS-Umgebung

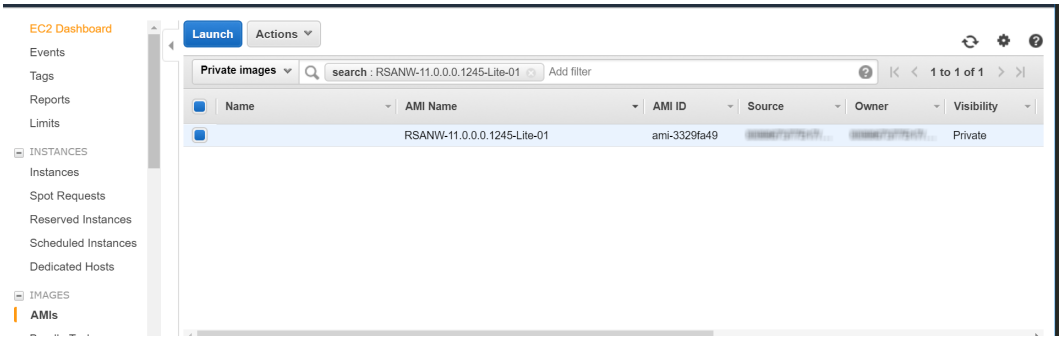
1. Stellen Sie sicher, dass Ihre AWS-Umgebung eine Kapazität aufweist, mit der Sie die Performancerichtlinien für NetWitness Suite erfüllen oder überschreiten, die in den Empfehlungen zur Konfiguration von AWS-Instanzen beschrieben sind.
2. Fahren Sie mit Suchen von NetWitness Suite-AMIs.

Suchen von NetWitness Suite-AMIs

Suchen Sie nach NW-AMI-Dateien innerhalb des Repositorys Öffentlich/Freigegeben/Community. Verwenden Sie „RSANW“ als Schlüsselwort, um nach AMI-Dateien zu suchen.

Hinweis: Weitere Anweisungen finden Sie in der AWS-Dokumentation **Suchen gemeinsamer AMIs** (https://docs.aws.amazon.com/de_de/AWSEC2/latest/UserGuide/usingsharedamis-finding.html).

1. Öffnen Sie die Amazon EC2-Konsole (Konto neue Abonnenten) unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie „AMIs“ im Navigationsbereich aus.
3. Wählen Sie im ersten Filter „Öffentliche Bilder“ aus.
4. Geben Sie in das Suchfeld „RSANW“ ein, um die NetWitness Suite-AMIs zu suchen.



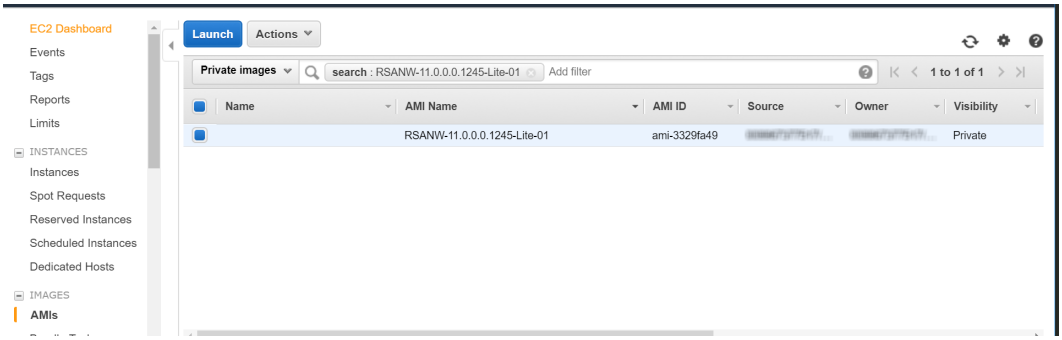
Hinweis: Wenden Sie sich an den RSA-Kundensupport (https://community.rsa.com/docs/DOC-1294), um Zugriff auf **RSANW-11.0.0.0.1245-Full-01** zu erhalten.

5. Fahren Sie mit Starten einer Instanz und Konfigurieren eines Hosts.

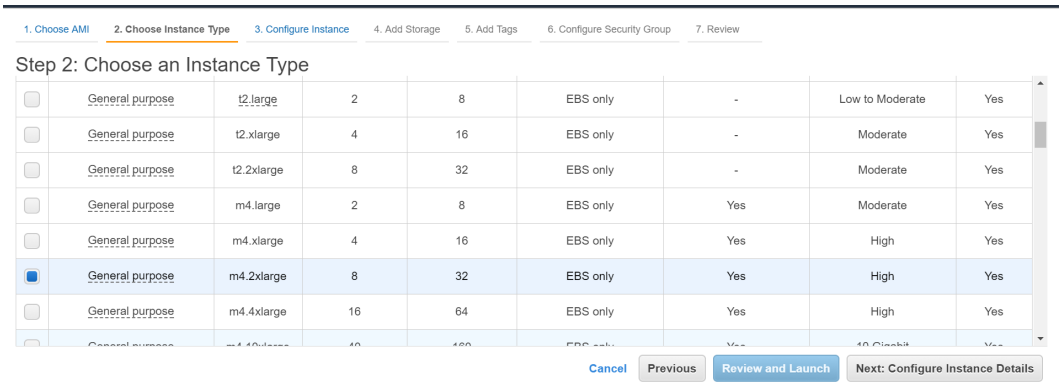
Starten einer Instanz und Konfigurieren eines Hosts

Hinweis: Weitere Anweisungen finden Sie in der AWS-Dokumentation „Starten einer Instance mit dem Startassistenten für Instances“ (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html).

1. Wählen Sie eine Instanz aus dem Raster aus (z. B. **RSA-NW-Concentrator-11.0.0.0-01**) und klicken Sie auf **Starten**.



2. Wählen Sie RAM und CPUs durch Auswahl des Instanztyps aus.
   In den Empfehlungen zur Konfiguration von AWS-Instanzen finden Sie Richtlinien zum Konfigurieren der EC2-Instanz basierend auf den Anforderungen der NetWitness Suite-Komponente (Service), für die Sie eine Instanz starten. Im folgenden Beispiel ist der Instanztyp **m4.2xlarge** mit **8** CPUs und **32** GB RAM ausgewählt.

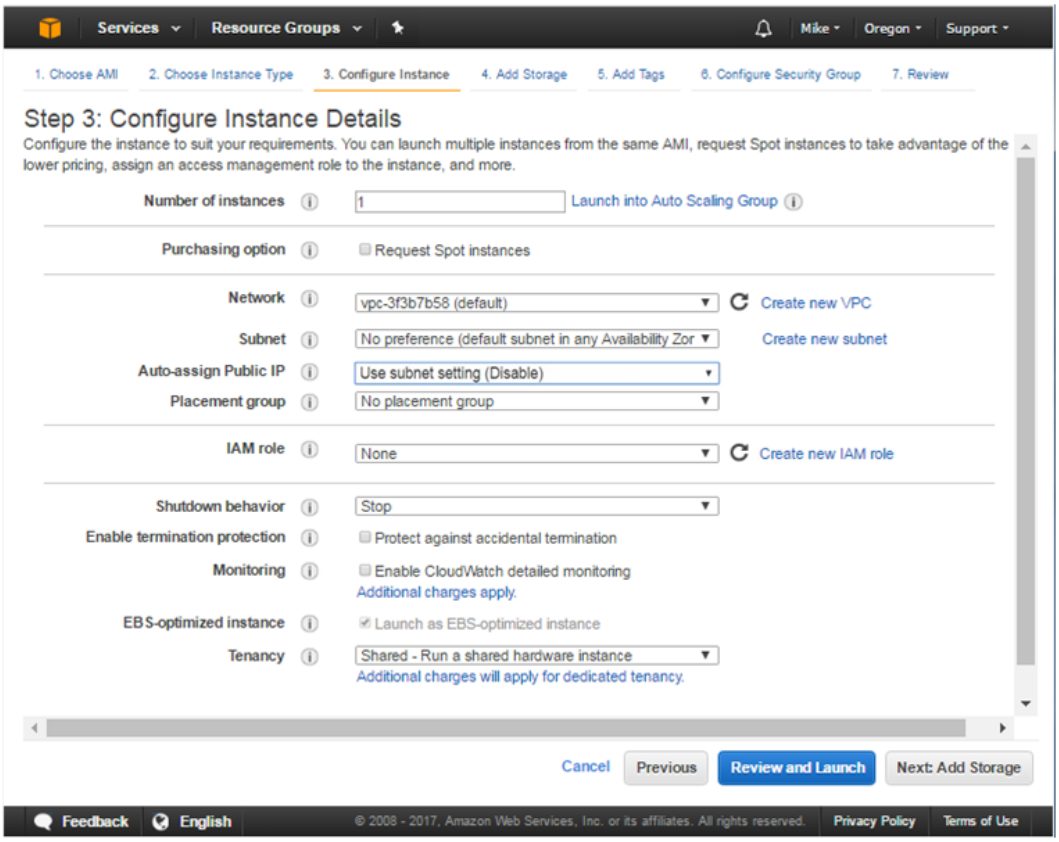


	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

3. Klicken Sie auf **Next: Konfigurieren der Instanzdetails** unten rechts auf der Seite **Schritt 2: Auswählen eines Instanztyps**.

   Die Seite **Schritt 3. Konfigurieren der Instanzdetails** wird angezeigt.

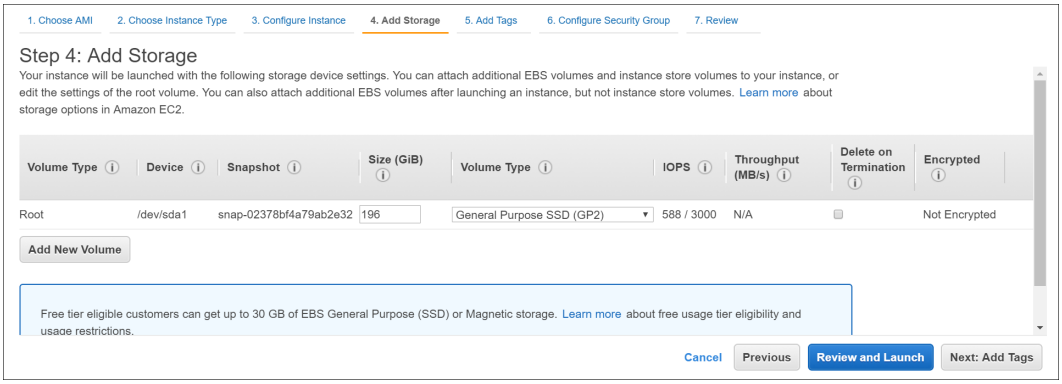
   Für NetWitness Suite werden standardmäßig für das Subnetz und den VPC die Werte im folgenden Beispiel eingetragen.



4. Klicken Sie auf **Next: Hinzufügen von Speicher** unten rechts auf der Seite **Schritt 3: Konfigurieren der Instanzdetails**.

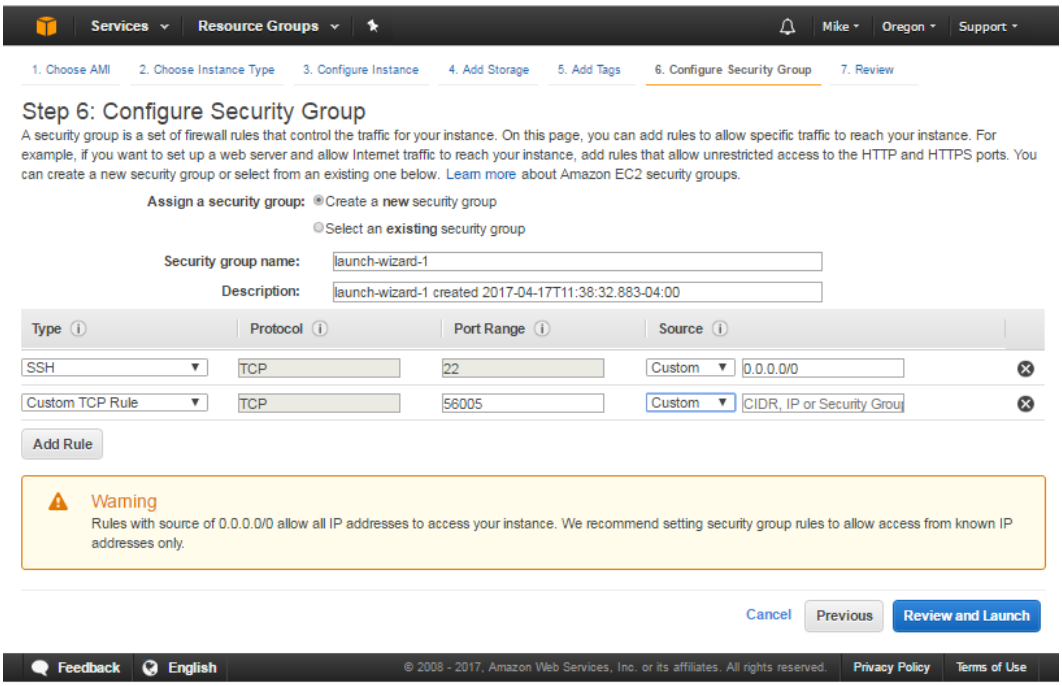
   Die Seite **Schritt 4. Hinzufügen von Speicher** wird angezeigt.

In den Empfehlungen zur Konfiguration von AWS-Instanzen finden Sie Richtlinien zum Konfigurieren des Speichers basierend auf den Anforderungen der NetWitness Suite-Komponente (Service), für die Sie eine Instanz starten.



5. Klicken Sie auf **Next: Hinzufügen von Tags** unten rechts auf der Seite **Schritt 4: Hinzufügen von Speicher**.
   Die Seite **Schritt 5. Hinzufügen von Tags** wird angezeigt. Geben Sie den Namen Ihrer Instanz ein.
6. Klicken Sie auf **Next: Konfigurieren der Sicherheitsgruppe** unten rechts auf der Seite **Schritt 5: Hinzufügen von Tags**.
   Die Seite **Schritt 6. Konfigurieren der Sicherheitsgruppe** wird angezeigt.
   a. Wählen Sie das Optionsfeld „Eine **neue** Sicherheitsgruppe erstellen“ aus.
   b. Erstellen Sie eine Regel, die die gesamte Firewall für die NetWitness Suite-Komponente öffnet.
      Sie müssen die Sicherheitsgruppe korrekt konfigurieren, um die Instanz (Host) von der NetWitness Suite-Benutzeroberfläche konfigurieren und eine SSH-Verbindung damit herstellen zu können.

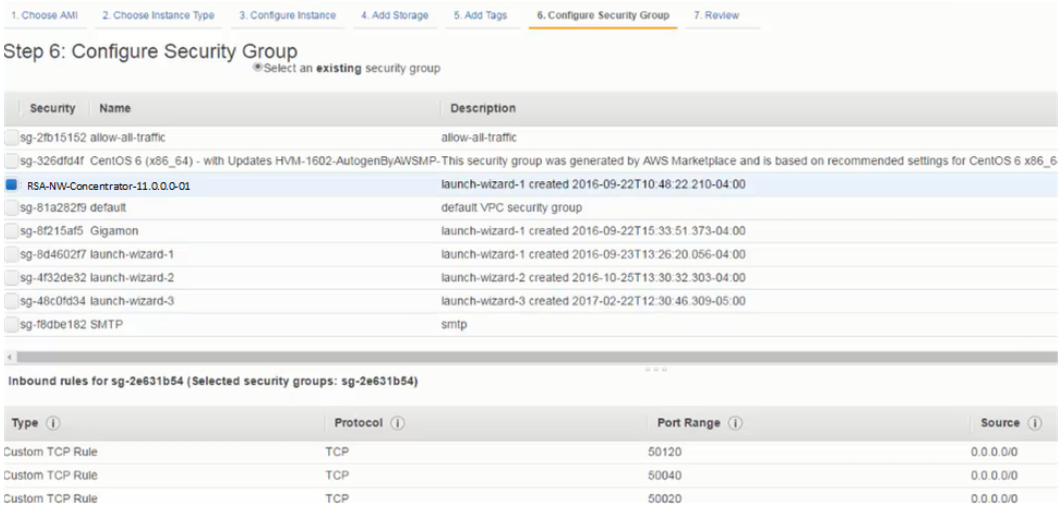
      Hinweis: Eine umfassende Liste der Ports, die Sie für alle NetWitness Suite-Komponenten einrichten müssen, finden Sie unter „Netzwerkarchitektur und Ports“ in RSA Link (https://community.rsa.com/docs/DOC-83050).



Hinweis: Nachdem Sie eine Sicherheitsgruppe konfiguriert haben, können Sie sie jederzeit ändern.

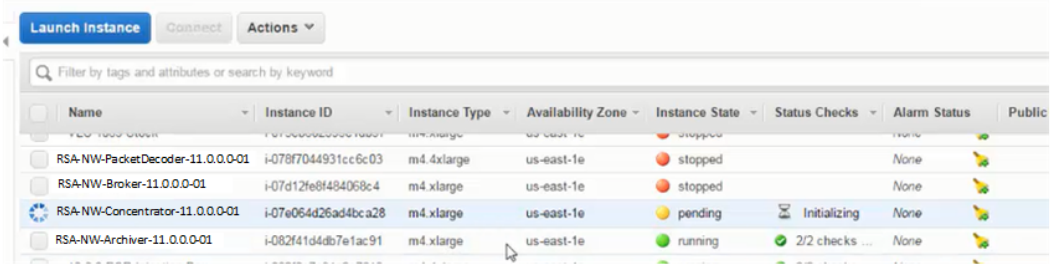
7. Klicken Sie auf **Prüfen und Starten** unten rechts auf der Seite **Schritt 6: Konfigurieren der Sicherheitsgruppe**.
   Die Seite **Schritt 7. Überprüfen des Instanzstarts** wird angezeigt.
8. Klicken Sie auf **Starten** unten rechts auf der Seite **Schritt 7. Überprüfen des Instanzstarts**.
   Das Dialogfeld **Vorhandenes Schlüsselpaar auswählen oder neues Schlüsselpaar erstellen** wird angezeigt.
9. Wählen Sie **Ohne Schlüsselpaar fortfahren** aus.

10. Klicken Sie auf **Instanz starten**.
    AWS zeigt die folgenden Informationen beim Erstellen der Instanz an.



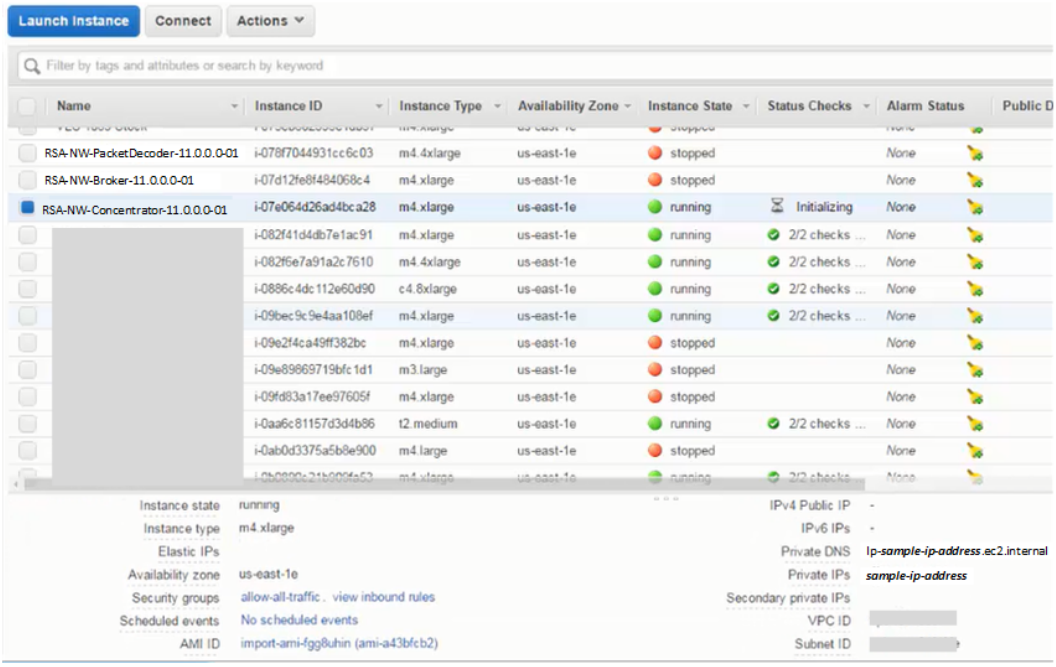
11. Klicken Sie auf **Instanzen anzeigen**.

12. Wählen Sie im linken Navigationsbereich **Instanzen** aus, um alle Instanzen zu überprüfen, die AWS initialisiert (z. B. **NW-Concentrator**).



Die IP-Adresse für den neuen Host **RSA-NW-Concentrator-11.0.0.0-01** lautet ***sample-ip-***

address.



13. Stellen Sie über SSH eine Verbindung mit der neu erstellten Instanz her. Verwenden Sie die standardmäßigen NetWitness Suite-Anmeldedaten.
14. Fahren Sie mit Konfigurieren von Hosts (Instanzen) in NetWitness Suite fort.

Installationsaufgaben

Aufgabe 1: Installieren von 11.0.0.0 auf dem NetWitness-Serverhost (NW-Server)

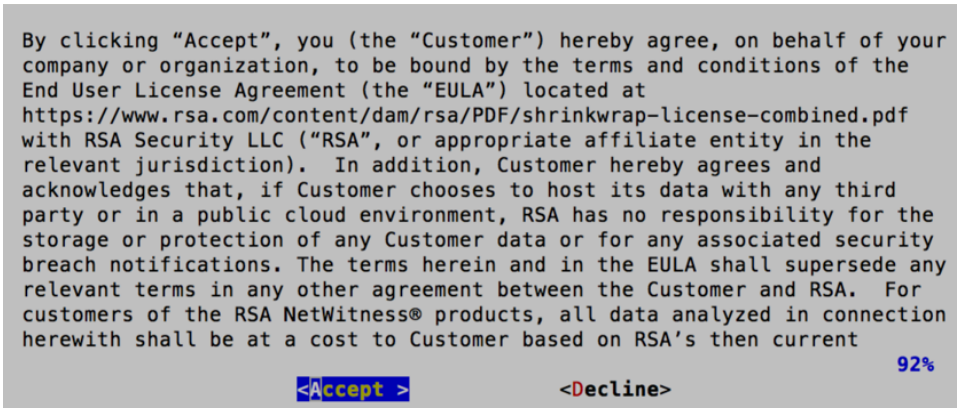
Hinweis: Sie können diese Aufgabe für die Instanz RSANW-11.0.0.0.1245-Full-01 durchführen.

1. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.

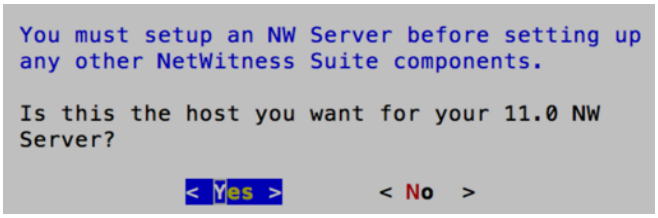
Dadurch wird das Setup-Programm gestartet und die EULA wird angezeigt.

Hinweis: 1.) Wenn Sie durch die Eingabeaufforderungen des Setup-Programms navigieren, verwenden Sie die Pfeile nach unten und oben, um zwischen den Feldern zu wechseln, die Tabulatortaste, um zwischen den Befehlen zu wechseln (z. B. **<Ja>**, **<Nein>**, **<OK>** und **<Abbrechen>**. Drücken Sie die **EINGABETASTE**, um Ihre Befehlsantwort zu registrieren und mit der nächsten Eingabeaufforderung fortzufahren.
2.) Das Setup-Programm übernimmt das Farbschema des Desktops oder der Konsole, den bzw. die Sie für den Zugriff auf den Host verwenden.
3.) Wenn Sie während des Setup-Programms (`nwsetup-tui`) die DNS-Server angeben, MÜSSEN diese gültig („gültig“ in diesem Zusammenhang bedeutet gültig während des Setups) und für `nwsetup-tui` zugänglich sein, damit Sie fortfahren können. Falsch konfigurierte DNS-Server führen dazu, dass die Konfiguration fehlschlägt. Wenn Sie nach dem Setup DNS-Server erreichen müssen, die während des Setups nicht erreichbar waren, (z. B. zur Verlagerung eines Hosts, der über andere DNS-Server verfügt) lesen Sie Aufgaben nach der Installation.
Wenn Sie während des Setups keinen DNS-Server angeben (`nwsetup-tui`), müssen Sie **1 Lokales Repository (auf dem NW-Server)** in der Eingabeaufforderung **NetWitness Suite Update-Repository** in Schritt 12 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repository zugreifen kann).

2. Gehen Sie zu **Akzeptieren** und drücken Sie die **EINGABETASTE**.



3. Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.

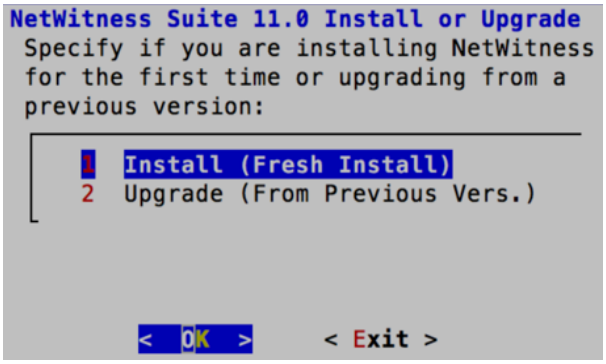


Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.

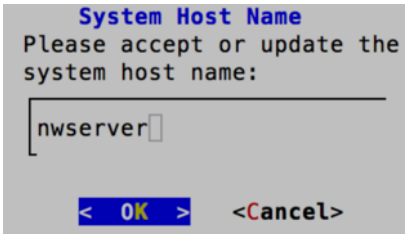
Wählen Sie **Nein**, wenn Sie 11.0.0.0 bereits auf dem NW-Server installiert haben.

Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und das Setup abschließen, müssen Sie das Setup-Programm (Schritt 2) neu starten und alle nachfolgenden Schritte ausführen, um diesen Fehler zu korrigieren.

4. Drücken Sie die **EINGABETASTE** (standardmäßig ist „Installation“ ausgewählt).
   Die Aufforderung „Installation“ oder „Upgrade“ wird angezeigt.



5. Die Aufforderung „Hostname“ wird angezeigt.

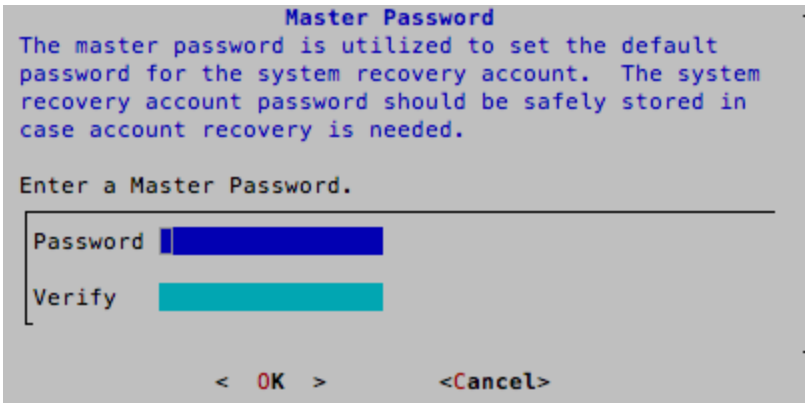


   Drücken Sie die **EINGABETASTE**, wenn dieser Name beibehalten werden soll. Wenn Sie den Hostnamen bearbeiten möchten, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um ihn zu ändern.
   Die Aufforderung „Masterpasswort“ wird angezeigt.

6. Für das Masterpasswort und Bereitstellungspasswort werden folgende Zeichen unterstützt:

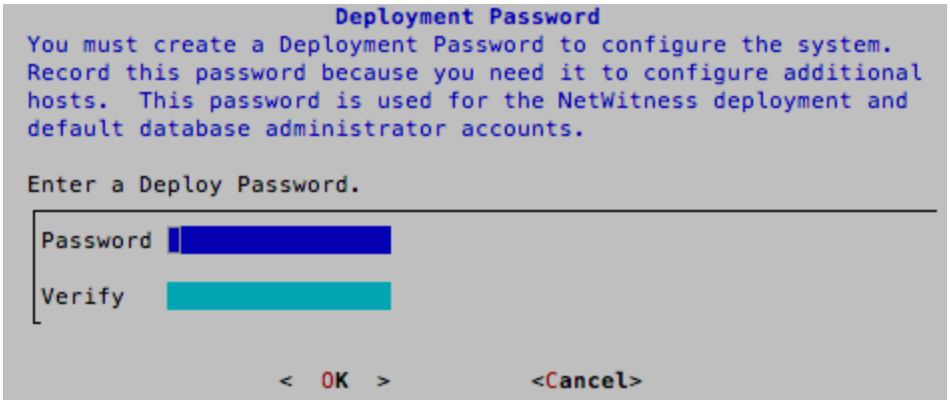
   - Symbole: ! @ # % ^ +
   - Zahlen: 0-9
   - Kleinbuchstaben: a-z
   - Großbuchstaben: A-Z

   Für das Masterpasswort und Bereitstellungspasswort werden keine nicht eindeutigen Zeichen unterstützt (z. B.: Leerzeichen { } [ ] ( ) / \ ' " ` ~ , ; : . < > -).



Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.

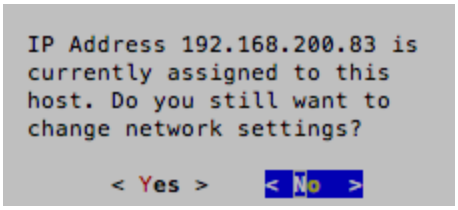
7. Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.



Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.

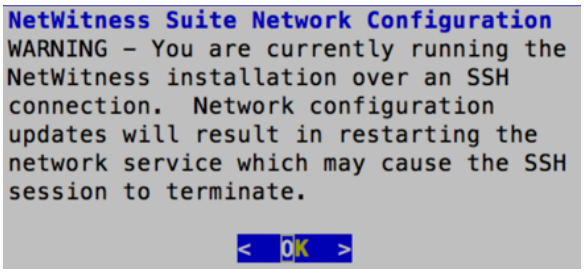
8. Beachten Sie:

- Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt.



  Drücken Sie die **EINGABETASTE**, wenn Sie diese IP verwenden und Ihre Netzwerkeinstellungen nicht ändern möchten. Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**, wenn Sie die auf dem Host gefundene IP-Konfiguration ändern möchten.

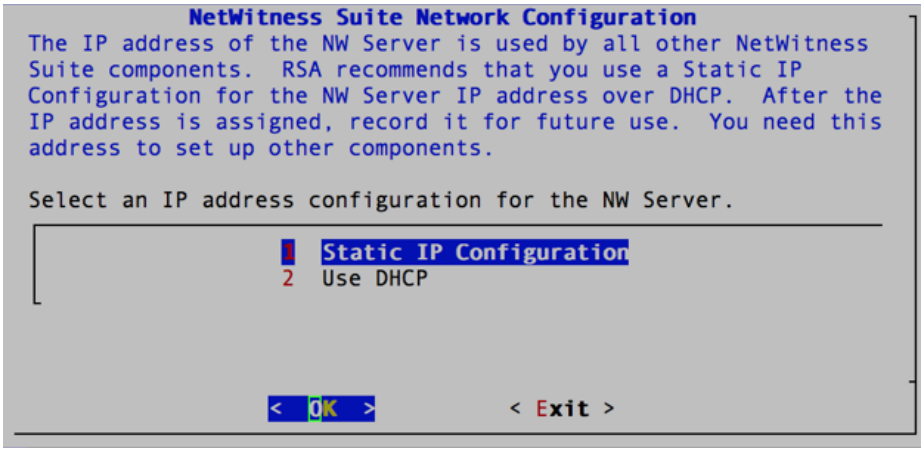
- Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt.



  Drücken Sie die **EINGABETASTE**, um die Warnung zu schließen.

- Wenn das Setup-Programm eine IP-Konfiguration gefunden hat und Sie sie ausgewählt haben, wird die Aufforderung „Update-Repository“ angezeigt. Fahren Sie mit Schritt 12 fort und schließen Sie die Installation ab.

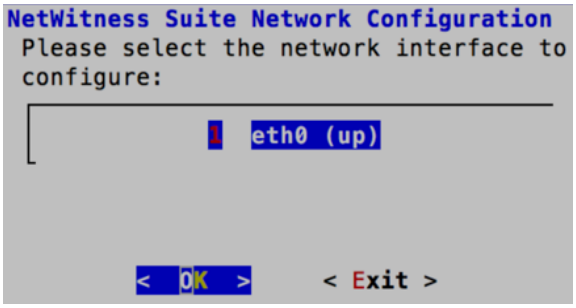
- Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung „Netzwerkkonfiguration“ angezeigt.



Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um **Statische IP-Adresse** zu verwenden.

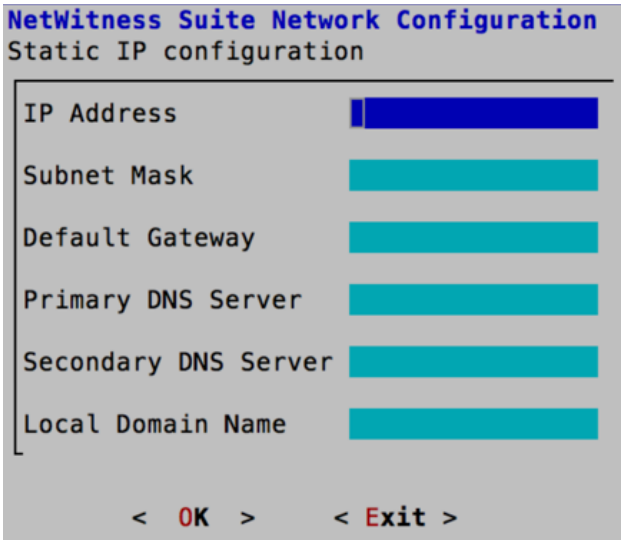
Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu „2 DHCP verwenden“ und drücken Sie die **EINGABETASTE**.

9. Die Eingabeaufforderung „Netzwerkkonfiguration“ wird angezeigt.



Gehen Sie mit dem Pfeil nach unten zur gewünschten Netzwerkschnittstelle. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**. Wenn Sie fortfahren möchten, gehen Sie zu **Beenden**.

10. Die Eingabeaufforderung „Konfiguration der statischen IP-Adresse“ wird angezeigt.



Geben Sie die Konfigurationswerte (mit dem Pfeil nach unten von Feld zu Feld gehend) ein.

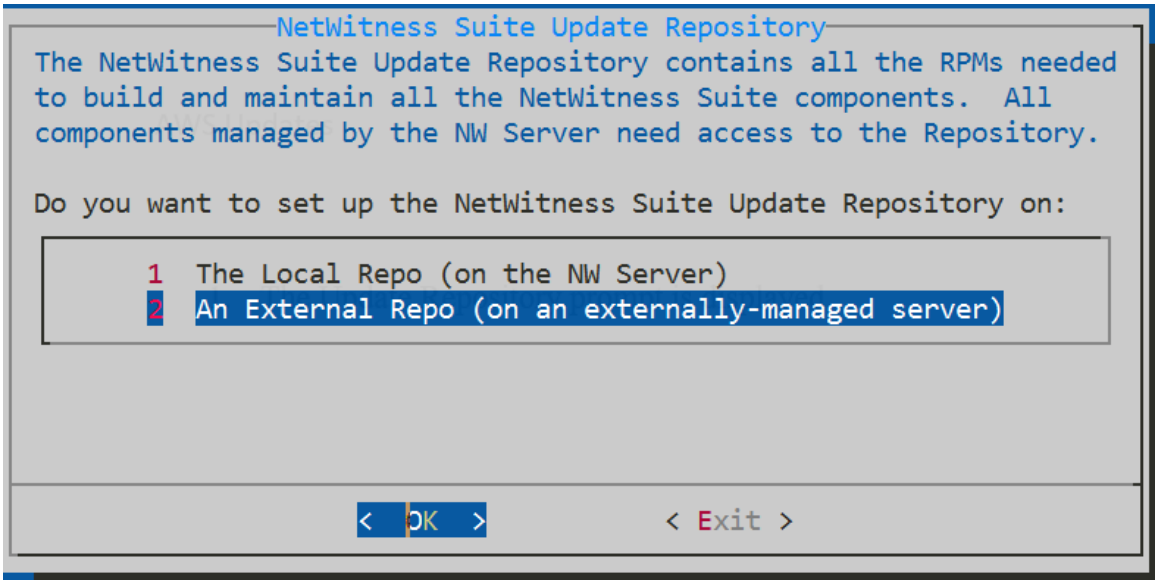
Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung Alle Felder sind Pflichtfelder angezeigt (die Felder **Primärer DNS-Server**, **Sekundärer DNS-Server** und **Lokaler Domainname** sind nicht erforderlich).

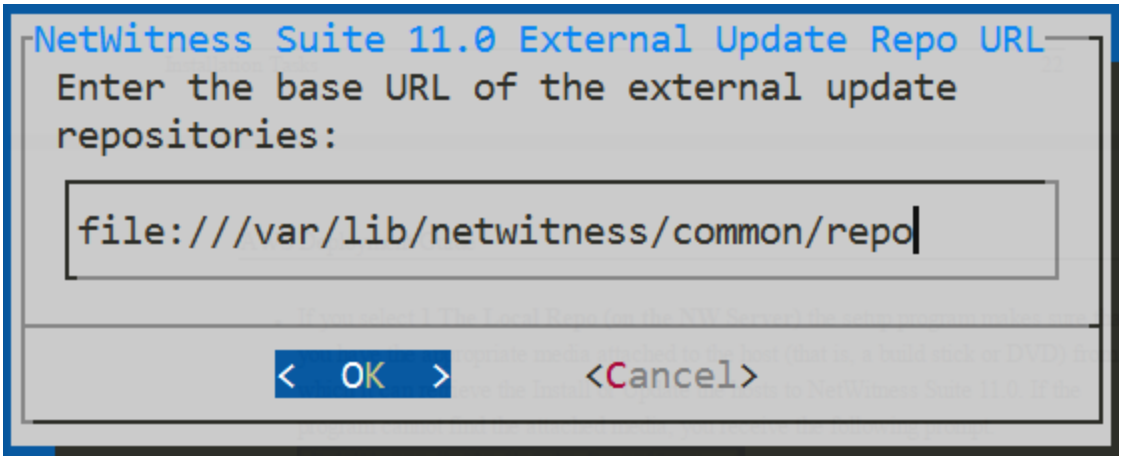
Bei Verwendung der falschen Syntax oder Zeichenlänge für eines der Felder wird die Fehlermeldung Ungültiger *Feldname* angezeigt.

Achtung: Wenn Sie den DNS-Server auswählen, stellen Sie sicher, dass der DNS-Server korrekt ist und der Host darauf zugreifen kann, bevor Sie mit der Installation fortfahren.

11. Die Eingabeaufforderung „Update-Repository“ wird angezeigt.



Bei Auswahl von **2 Externes Repository (auf einem extern gemanagten Server)** werden Sie zur Eingabe eines URL aufgefordert.

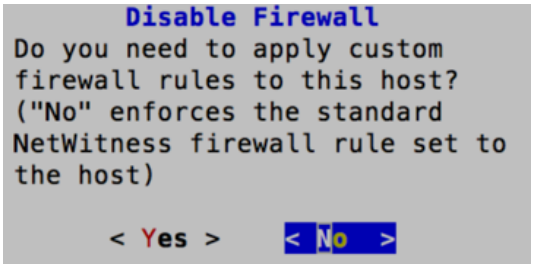


Verwenden Sie den Standard-URL des externen Repository der NetWitness Suite und klicken Sie auf **OK**.

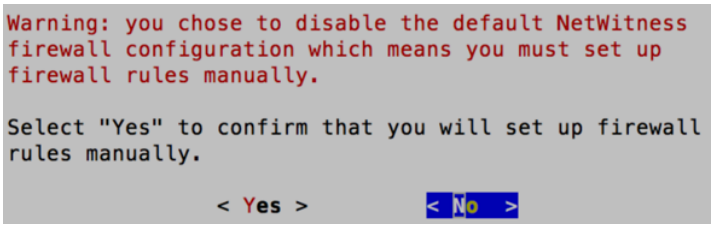
12. Um die Standardkonfiguration für Firewalls anzuwenden, drücken Sie die **EINGABETASTE**.

    - Um die Standardkonfiguration zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.

      Die Aufforderung „Firewall deaktivieren“ wird angezeigt.

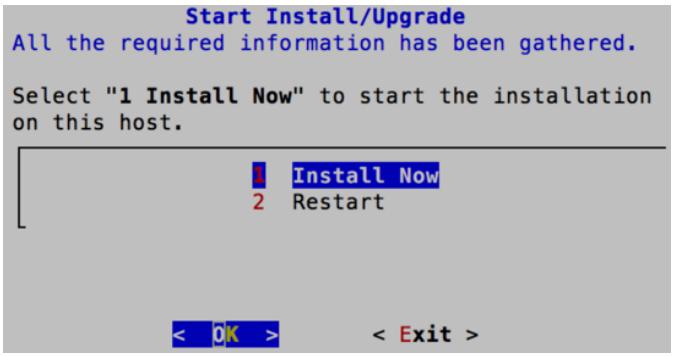
      

      Die Aufforderung zur Bestätigung der Deaktivierung der Firewallkonfiguration wird angezeigt.

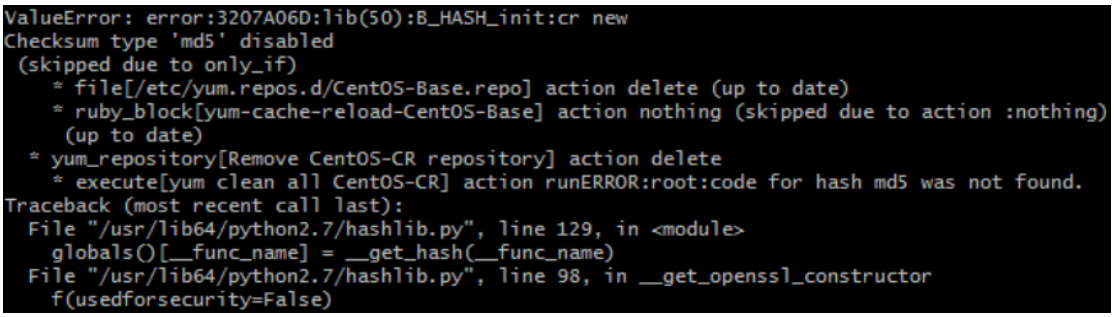
      Gehen Sie zu **Ja** und drücken Sie zur Bestätigung die **EINGABETASTE** (drücken Sie die **EINGABETASTE**, um die Standardkonfiguration für Firewalls zu verwenden).

13. Drücken Sie die **EINGABETASTE**, um 11.0.0.0 auf dem NW-Server zu installieren.
    Die Aufforderung „Installation starten“ wird angezeigt.



Wenn „Installation abgeschlossen“ angezeigt wird, haben Sie den 11.0.0.0 NW-Server auf diesem Host installiert.

Hinweis: Ignorieren Sie die Hashcodefehler ähnlich wie die Fehler in der folgenden Abbildung, die angezeigt werden, wenn Sie den Befehl `nwsetup-tui` initiieren. Yum verwendet kein MD5 für Sicherheitsabläufe, sodass sie sich nicht auf die Sicherheit des Systems auswirken.



Aufgabe 2: Installieren von 11.0.0.0 auf den Hosts anderer Komponenten

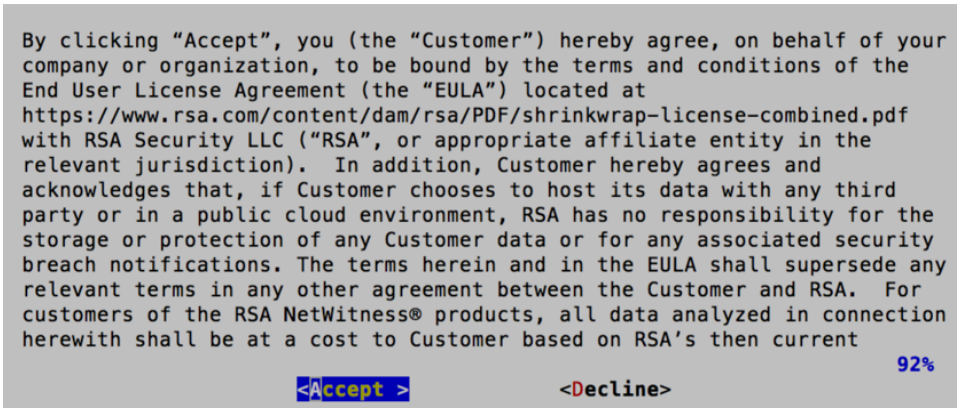
Hinweis: Sie können diese Aufgabe für die Instanz RSANW-11.0.0.0.1245-Lite-01 durchführen.

1. Führen Sie den Befehl `nwsetup-tui` aus, um den Host einzurichten.

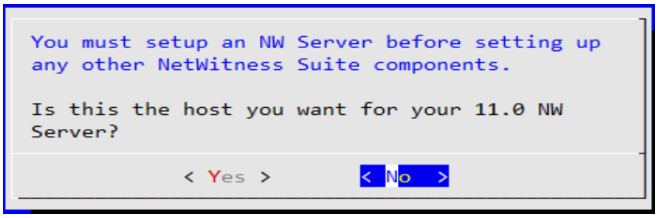
Dadurch wird das Setup-Programm gestartet und die EULA wird angezeigt.

Hinweis: 1.) Wenn Sie durch die Eingabeaufforderungen des Setup-Programms navigieren, verwenden Sie die Pfeile nach unten und oben, um zwischen den Feldern zu wechseln, die Tabulatortaste, um zwischen den Befehlen zu wechseln (z. B. **<Ja>**, **<Nein>**, **<OK>** und **<Abbrechen>**. Drücken Sie die **EINGABETASTE**, um Ihre Befehlsantwort zu registrieren und mit der nächsten Eingabeaufforderung fortzufahren.
2.) Das Setup-Programm übernimmt das Farbschema des Desktops oder der Konsole, den bzw. die Sie für den Zugriff auf den Host verwenden.
3.) Wenn Sie während des Setup-Programms (`nwsetup-tui`) die DNS-Server angeben, MÜSSEN diese gültig („gültig“ in diesem Zusammenhang bedeutet gültig während des Setups) und für `nwsetup-tui` zugänglich sein, damit Sie fortfahren können. Falsch konfigurierte DNS-Server führen dazu, dass die Konfiguration fehlschlägt. Wenn Sie nach dem Setup DNS-Server erreichen müssen, die während des Setups nicht erreichbar waren, (z. B. zur Verlagerung eines Hosts, der über andere DNS-Server verfügt) lesen Sie Aufgaben nach der Installation.
Wenn Sie während des Setups keinen DNS-Server angeben (`nwsetup-tui`), müssen Sie **1 Lokales Repository (auf dem NW-Server)** in der Eingabeaufforderung **NetWitness Suite Update-Repository** in Schritt 12 auswählen (die DNS-Server werden nicht definiert, sodass das System nicht auf das externe Repository zugreifen kann).

2. Gehen Sie zu **Akzeptieren** und drücken Sie die **EINGABETASTE**.



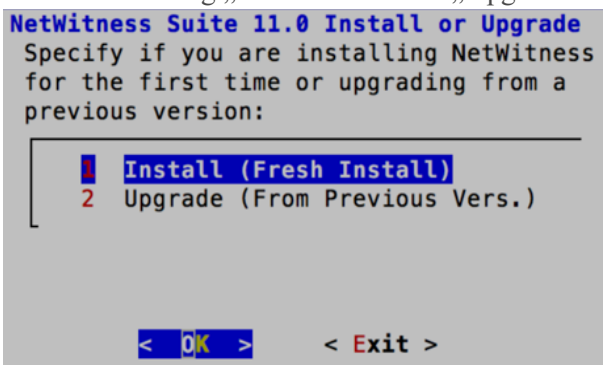
3. Die Eingabeaufforderung „Ist dies der NW-Server“ wird angezeigt.



Gehen Sie zu **Nein** und drücken Sie die **EINGABETASTE**.

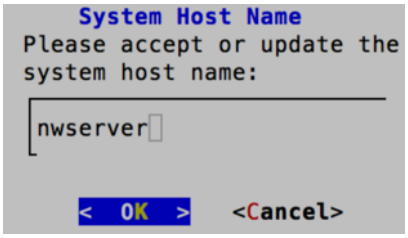
Achtung: Wenn Sie den falschen Host für den NW-Server auswählen und das Setup abschließen, müssen Sie das Setup-Programm (Schritt 2) neu starten und alle nachfolgenden Schritte ausführen, um diesen Fehler zu korrigieren.

4. Die Aufforderung „Installation“ oder „Upgrade“ wird angezeigt.



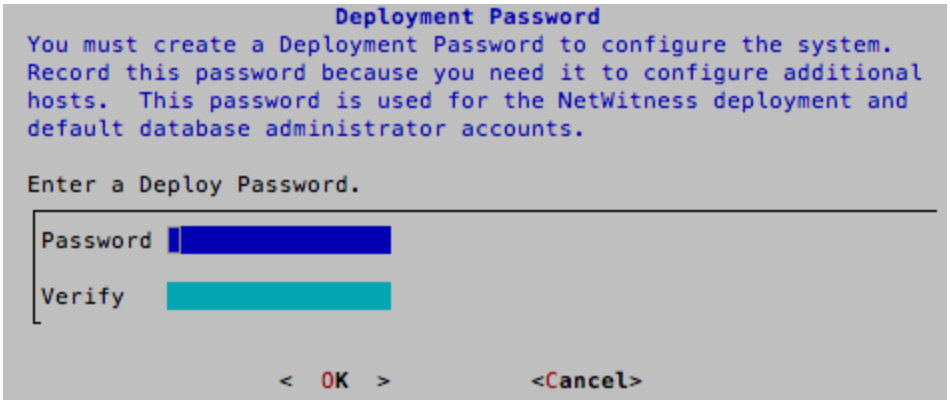
Drücken Sie die **EINGABETASTE** (standardmäßig ist „Installation“ ausgewählt).

5. Die Aufforderung „Hostname“ wird angezeigt.



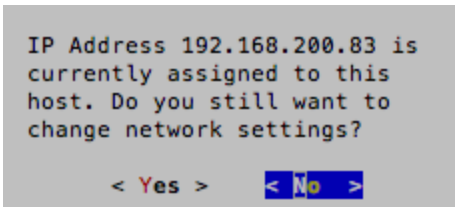
Drücken Sie die **EINGABETASTE**, wenn dieser Name beibehalten werden soll. Wenn Sie den Hostnamen bearbeiten möchten, gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um ihn zu ändern.

6. Die Aufforderung „Bereitstellungspasswort“ wird angezeigt.

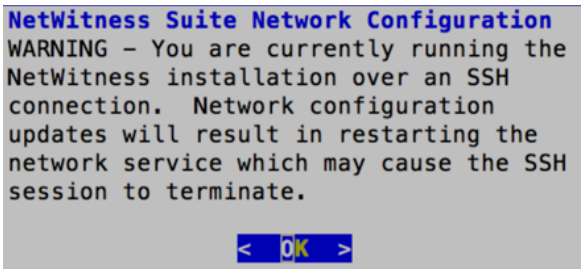


   Geben Sie das **Passwort** ein, gehen Sie mit dem Pfeil nach unten zu **Überprüfen**, geben Sie das Passwort erneut ein, gehen Sie zu **OK** und drücken Sie dann die **EINGABETASTE**.

7. Beachten Sie:
   Wenn das Setup-Programm eine gültige IP-Adresse für diesen Host findet, wird die folgende Eingabeaufforderung angezeigt.

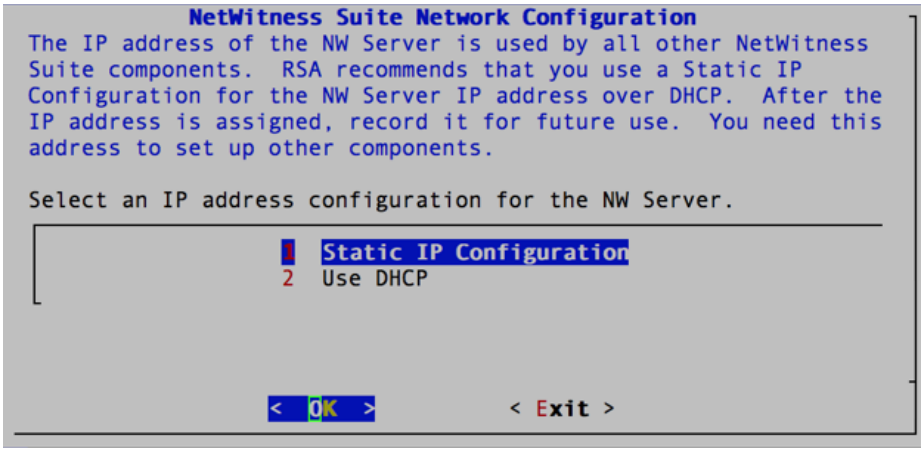


   Drücken Sie die **EINGABETASTE**, wenn Sie diese IP verwenden und Ihre Netzwerkeinstellungen nicht ändern möchten.
   Gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**, wenn Sie die auf dem Host gefundene IP-Konfiguration ändern möchten.
   Wenn Sie eine SSH-Verbindung verwenden, wird die folgende Warnung angezeigt.



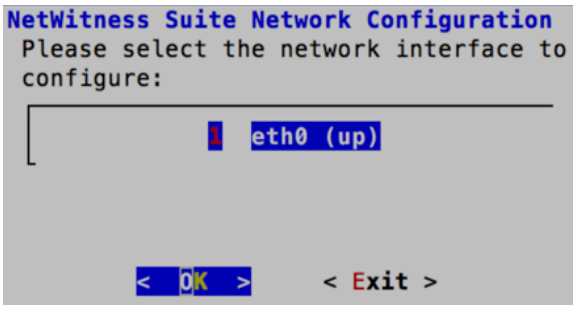
   Drücken Sie die **EINGABETASTE**, um die Warnung zu schließen. Wenn das Setup-Programm eine IP-Konfiguration gefunden hat und Sie sie ausgewählt haben, wird die Aufforderung „Update-Repository“ angezeigt. Fahren Sie mit Schritt 12 fort und schließen Sie die Installation ab.

Wenn das Setup-Programm keine IP-Konfiguration gefunden hat oder Sie beschlossen haben, die vorhandene IP-Konfiguration zu ändern, wird die Eingabeaufforderung „Netzwerkkonfiguration“ angezeigt.



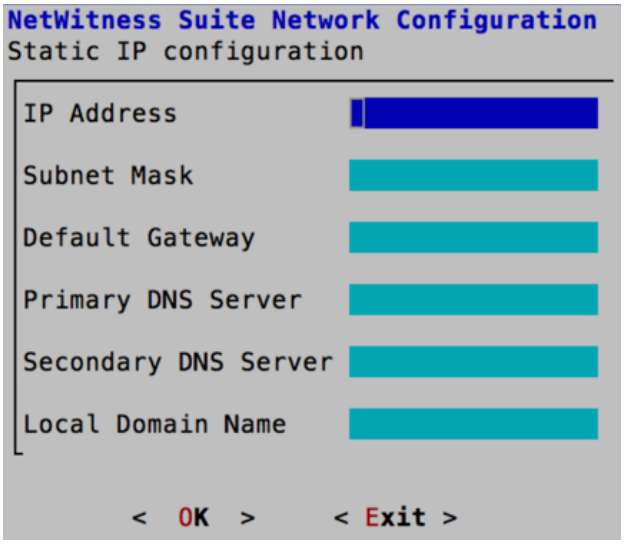
Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**, um **Statische IP-Adresse** zu verwenden.
Wenn Sie **DHCP** verwenden möchten, gehen Sie mit dem Pfeil nach unten zu „2 DHCP verwenden“ und drücken Sie die **EINGABETASTE**.

8. Die Eingabeaufforderung „Netzwerkkonfiguration“ wird angezeigt.



Gehen Sie mit dem Pfeil nach unten zur gewünschten Netzwerkschnittstelle. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**. Wenn Sie fortfahren möchten, gehen Sie zu **Beenden**.

9. Die Eingabeaufforderung „Konfiguration der statischen IP-Adresse“ wird angezeigt.

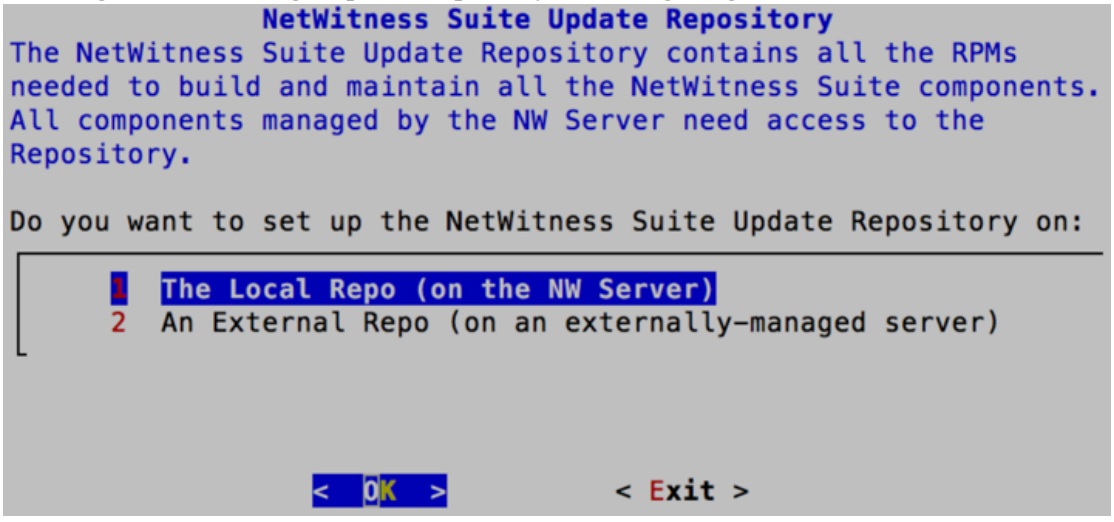


Geben Sie die Konfigurationswerte (mit dem Pfeil nach unten von Feld zu Feld gehend) ein. Gehen Sie zu **OK** und drücken Sie die **EINGABETASTE**.

10. Wenn Sie nicht alle Pflichtfelder ausfüllen, wird die Fehlermeldung Alle Felder sind Pflichtfelder angezeigt (die Felder **Primärer DNS-Server**, **Sekundärer DNS-Server** und **Lokaler Domainname** sind nicht erforderlich).
Bei Verwendung der falschen Syntax oder Zeichenlänge für eines der Felder wird die Fehlermeldung Ungültiger *Feldname* angezeigt.

Achtung: Wenn Sie den DNS-Server auswählen, stellen Sie sicher, dass der DNS-Server korrekt ist und der Host darauf zugreifen kann, bevor Sie mit der Installation fortfahren.

11. Die Eingabeaufforderung „Update-Repository“ wird angezeigt.



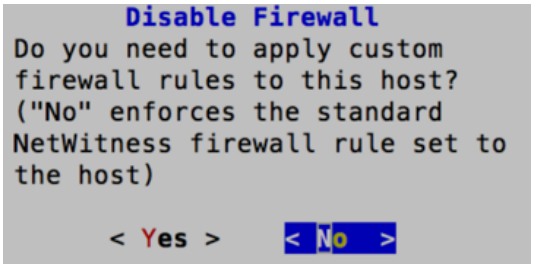
Drücken Sie die **EINGABETASTE**, um das **lokale Repository** auf dem NW-Server

auszuwählen.

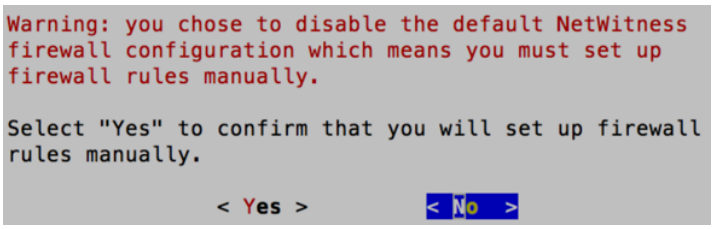
12. Gehen Sie wie folgt vor:

    - Um die Standardkonfiguration für Firewalls anzuwenden, drücken Sie die **EINGABETASTE**.
    - Um die Standardkonfiguration zu deaktivieren, gehen Sie zu **Ja** und drücken Sie die **EINGABETASTE**.

      Die Aufforderung „Firewall deaktivieren“ wird angezeigt.

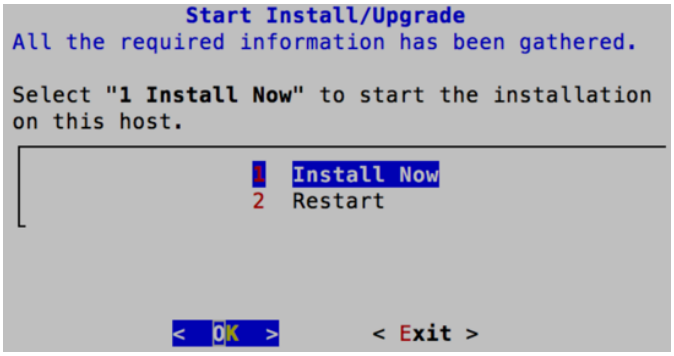
      

      Die Aufforderung zur Bestätigung der Deaktivierung der Firewallkonfiguration wird angezeigt.

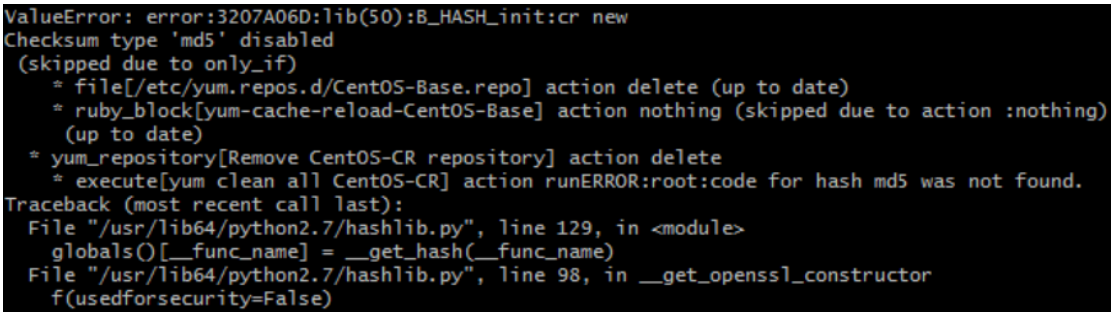
      Gehen Sie zu **Ja** und drücken Sie zur Bestätigung die **EINGABETASTE** (drücken Sie die **EINGABETASTE**, um die Standardkonfiguration für Firewalls zu verwenden).

13. Die Aufforderung „Installation starten“ wird angezeigt.

    Drücken Sie die **EINGABETASTE**, um 11.0 auf dem NW-Server zu installieren.
    Wenn „Installation abgeschlossen“ angezeigt wird, haben Sie den 11.0.0.0 NW-Server auf diesem Host installiert.

Hinweis: Ignorieren Sie die Hashcodefehler ähnlich wie die Fehler in der folgenden Abbildung, die angezeigt werden, wenn Sie den Befehl `nwsetup-tui` initiieren. Yum verwendet kein MD5 für Sicherheitsabläufe, sodass sie sich nicht auf die Sicherheit des Systems auswirken.



Konfigurieren von Hosts (Instanzen) in NetWitness Suite

Konfigurieren Sie einzelne Hosts und Services, wie im RSA NetWitness® Suite *Leitfaden zur Host- und Servicekonfiguration* beschrieben. In diesem Leitfaden finden Sie auch Verfahren zur Anwendung von Updates und zur Vorbereitung auf Versionsupgrades.

Hinweis: Nachdem Sie erfolgreich eine Instanz starten, weist AWS einen Standard-Hostnamen zu. Anweisungen zum Ändern eines Hostnamens finden Sie in der Dokumentation „Ändern des Namens und Hostnamens eines Hosts“ in RSA Link (https://community.rsa.com).

Konfigurieren der Paketerfassung

Sie können eine der folgenden Lösungen von Drittanbietern im Packet Decoder integrieren, um Pakete in der AWS-Cloud zu erfassen:

- Gigamon® GigaVUE
- f5® BIG-IP

Integrieren von Gigamon GigaVUE im Packet Decoder

Es gibt zwei Hauptaufgaben zur Konfiguration der Gigamon®-Tap-Drittanbieterlösung zur Paketerfassung:

Aufgabe 1. Integrieren der Gigamon®-Lösung

Aufgabe 2. Konfigurieren eines Tunnels auf dem Packet Decoder

Aufgabe 1. Integrieren der Gigamon-Lösung

Gigamon® Visibility Platform on AWS steht über den AWS Marketplace zur Verfügung und wird mit einer BYOL-Lizenz aktiviert. Eine kostenlose 30-Tage-Testversion ist ebenfalls verfügbar.

Weitere Informationen zur Gigamon®-Lösung finden Sie im „Gigamon® Visibility Platform for AWS Data Sheet“ (https://www.gigamon.com/sites/default/files/resources/datasheet/ds-gigamon-visibility-platform-for-aws-4095.pdf).

Details zur Bereitstellung finden Sie im „Gigamon® Visibility Platform for AWS Getting Started Guide“ (https://www.gigamon.com/sites/default/files/resources/deployment-guide/dg-visibility-platform-for-aws-getting-started-guide-4111.pdf).

Nach Bereitstellung der „Monitoring-Sitzung“ innerhalb der Gigamon GigaVUE-FM können Sie den Packet Decoder-Tunnel konfigurieren.

Aufgabe 2. Konfigurieren des Tunnels auf dem Packet Decoder

1. Stellen Sie über SSH eine Verbindung mit dem Decoder her.
2. Senden Sie die folgenden Befehlszeichenfolgen:

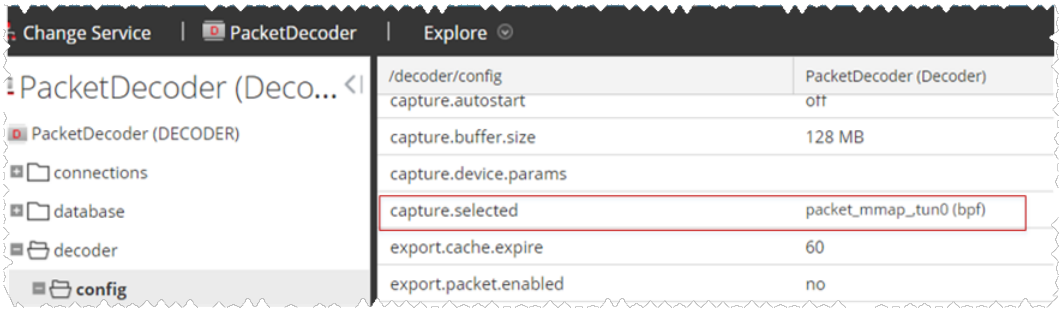
```
$ sudo ip link add tun0 type gretap local any remote <ip_address_of_
VSERIES_NODE_TUNNEL_INTERFACE> ttl 255

$ sudo ip link set tun0 up mtu <MTU-SIZE>

$ sudo ifconfig (to verify if the tunnel tun0 is being listed in the
list of interfaces)

$ sudo lsmod | grep gre ( to make sure if the below kernel modules
are running:

ip_gre 18245 0

ip_tunnel 25216 1)

If they are not running then execute the below commands to enable the
modules

$ sudo modprobe act_mirred

$ sudo modprobe ip_gre
```

3. Erstellen Sie eine Firewallregel im Packet Decoder, um Datenverkehr über den Tunnel zuzulassen.
   a. Öffnen Sie die Datei `iptables`.
      `vi /etc/sysconfig/iptables`
   b. Hängen Sie die Zeile `-A INPUT -p gre -j ACCEPT` vor der Anweisung `commit` an.
   c. Starten Sie `iptables` neu, indem Sie die folgenden Befehle ausführen.
      `service iptables restart`

4. Legen Sie die Schnittstelle im Packet Decoder fest.

   a. Melden Sie sich bei NetWitness Suite an und wählen Sie den Node `decoder/config` in der Explorer-Ansicht für den Packet Decoder-Service aus.

   b. Definieren Sie `capture.selected = packet_mmap_,tun0`.

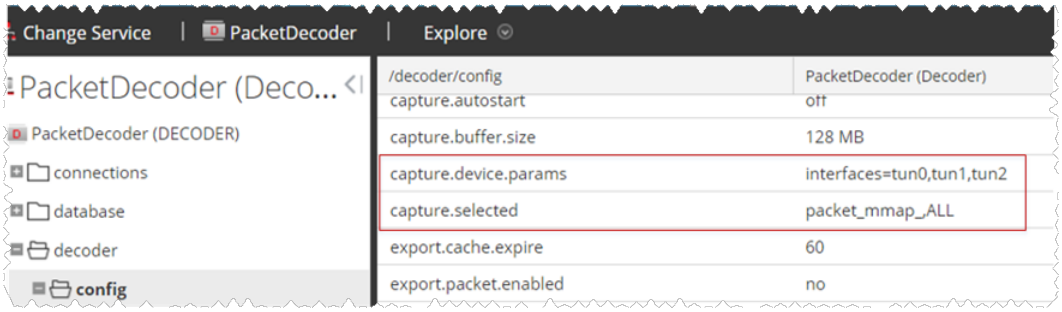


5. (Bedingungsabhängig) – Wenn Sie über mehrere Tunnel auf dem Packet Decoder verfügen.

   a. Starten Sie den Decoder-Service nach der Erstellung des Tunnels im Packet Decoder neu.

   b. Melden Sie sich bei NetWitness Suite an und wählen Sie den Node `decoder/config` in der Explorer-Ansicht für den Packet Decoder-Service aus. Definieren Sie die folgenden Parameter.

   ```
   capture.device.params = interfaces=tun0,tun1,tun2
   capture.selected = packet_mmap_,All
   ```



6. Starten Sie den Decoder-Service neu.

   ```
   $ sudo restart nwdecoder
   ```

   Der Benutzer sollte so eingerichtet sein, dass der Netzwerkdatenverkehr im Decoder erfasst wird.

Führen Sie die folgenden Schritte aus, um ein neues Projekt zu erstellen und Ihren Projektschlüssel zu erhalten.

Integrieren von f5® BIG-IP im Packet Decoder

BIG-IP Virtual Edition (VE) ist eine Inline-Technologie für virtuelle Server/Load Balancer. Ein typischer Anwendungsfall ist, dass das F5®-Gerät als virtueller Webserver mit einer einzigen IP-Adresse/einem einzigen Hostnamen fungiert, der Anforderungen an einen Pool von Webservern in der Cloud managt.

Der gesamte Datenverkehr zu RSA NetWitness® Suite geht über den virtuellen f5® BIG-IP-VE-Server.

Die virtuellen Serverfunktionen von BIG-IP klonen den gesamten Datenverkehr zu einem bestimmten Computer, indem MAC-Adressen umgeschrieben und in ein Subnetz geladen werden, das auch vom Ziel-Sniffer verwendet wird. In diesem Handbuch wird beschrieben, wie Sie den Decoder als Sniffer einrichten.

Informationen zur f5® BIG-IP VE-Bereitstellung

f5® BIG-IP VE on AWS steht über den AWS Marketplace zur Verfügung und wird mit einer BYOL-Lizenz aktiviert. Eine kostenlose 30-Tage-Testversion ist ebenfalls verfügbar.

Weitere Informationen zu dieser Lösung finden Sie im f5® BIG-IP DNS Data Sheet (https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf).

Aufgabe 1: Einrichten einer virtuellen Serverinstanz von BIG-IP VE

Richten Sie eine virtuelle BIG-IP VE-Serverinstanz gemäß den Anweisungen im Handbuch „BIG-IP Virtual Edition 12.1.0 and Amazon Web Services: Multi-NIC Manual“ (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-multi-nic-setup-amazon-ec2-12-1-0.html) ein. Führen Sie alle Schritte bis zum letzten Schritt „Erstellen eines virtuellen Servers“ aus.

Auf diesem virtuellen Server wird die Paketerfassung durchgeführt. Je nach Ihrem Volume müssen Sie möglicherweise mehrere virtuelle Server erstellen.

Im Rahmen der Erstellung des virtuellen Servers benötigen Sie mindestens einen Server in Ihrer NetWitness Suite-Domain, um den Datenverkehr zu verarbeiten, der vom virtuellen Server weitergeleitet wird (z. B. können Sie eine andere Instanz in AWS erstellen, um den internen Server zu hosten).

Aufgabe 2: Erstellen eines Clone-Pools

1. Stellen Sie sicher, dass die Decoder-Instanz über eine Netzwerkschnittstelle im selben Subnetz verfügt wie eine der Netzwerkschnittstellen in der BIG-IP VE-Instanz.
   Der Clone-Pool übernimmt das Senden von Paketen an den Decoder durch Umschreiben von MAC-Adressen und Senden an eine Netzwerkschnittstelle. Das Umschreiben von MAC-Adressen kann zur Paketweiterleitung in ein anderes Subnetz verwendet werden.
2. Richten Sie den Clone-Pool im virtuellen BIG-IP VE-Server gemäß den Anweisungen im Artikel „K13392: Configuring the BIG-IP system to send traffic to an intrusion detection

system (11.x - 13.x)“ (https://support.f5.com/kb/en-us/solutions/public/13000/300/sol13392.html) ein.
In diesem Dokument wird erläutert, wie Sie den Clone-Pool erstellen und wie Sie einen vorhandenen virtuellen Server so einrichten, dass er den Datenverkehr in diesen Clone-Pool kopiert. In diesem Fall platzieren wir die Decoder-Instanz in den Clone-Pool.

Richtlinien

Die folgenden Richtlinien helfen Ihnen dabei, die Paketerfassung mit BIG-IP-VE korrekt zu konfigurieren.

- Die IP-Adresse der Decoder-Instanz muss sich in einem der Subnetze befinden, in dem sich auch BIG-IP VE befindet. BIG-IP verwendet diese IP-Adresse, um den Decoder als Teil des Clone-Pools zu identifizieren.
- Wenn Sie die Decoder-Instanz dem Clone-Pool hinzufügen, fragt BIG-IP nach der Portnummer und der IP-Adresse. Die Portnummer spielt für den geklonten Datenverkehr keine Rolle. Der Decoder empfängt den gesamten geklonten Datenverkehr, unabhängig davon, welche Portnummer hier verwendet wurde.
- Standardmäßig ist es im AWS-Subnetz, das vom Decoder und von BIG-IP VE genutzt wird, nicht zulässig, dass der geklonte Datenverkehr von der BIG-IP VE-Schnittstelle zur Decoder-Schnittstelle verläuft. Sie müssen **`source/dest. check`** sowohl in der Decoder- als auch in der BIG-IP VE-Netzwerkschnittstelle in AWS deaktivieren.
- Die Decoder-Instanz kann standardmäßig nur eine Netzwerkschnittstelle (eth0) haben. Der Decoder erfasst den Datenverkehr an dieser Schnittstelle, er kann aber auch administrativen Datenverkehr an dieser Schnittstelle empfangen. RSA empfiehlt die Verwendung von Netzwerkregeln zum Herausfiltern von ssh- und nwdecoder-Datenverkehr aus dem Erfassungsstream. Dies sind die Ports 22 (ssh) und 50004/56004 (nwdecoder).

Troubleshooting und Tipps

Es können Bereiche geprüft werden, wenn Pakete nicht vom Decoder akzeptiert werden.

- Stellen Sie sicher, dass BIG-IP VE die Pakete von der richtigen Schnittstelle sendet.
  Die BIG-IP VE-Instanz enthält „tcpdump“. Verwenden Sie es, um sicherzustellen, dass die geklonten Pakete von der erwarteten Schnittstelle gesendet werden. Ist dies nicht der Fall, ist der Clone-Pool oder der virtuelle Server nicht richtig eingerichtet.
- Stellen Sie sicher, dass der Decoder Pakete empfängt.
  Auf dem Decoder ist `tcpdump` installiert. Verwenden Sie es, um sicherzustellen, dass der Decoder Pakete empfängt. Wenn der Decoder Pakete nicht erfasst, stellen Sie Folgendes

sicher:

- **`source/dest. check`** von AWS ist deaktiviert.
- Der Decoder befindet sich im selben Subnetz wie die Schnittstelle, die BIG-IP-VE zum Klonen von Paketen verwendet.

Empfehlungen zur Konfiguration von AWS-Instanzen

Hinweis: Diese Empfehlungen waren für RSA Security Analytics Version 10.6.3 qualifiziert. Diese Empfehlungen können als Basis für 11.0.0.0 verwendet und bei Bedarf angepasst werden.

Hinweis: Eine Beschreibung der in diesem Thema verwendeten Begriffe und Abkürzungen finden Sie unter Abkürzungen und andere in diesem Leitfaden verwendete Terminologie.

Dieses Thema enthält die minimalen Konfigurationseinstellungen für AWS-Instanzen, die für die virtuellen Stack-Komponenten von RSA NetWitness® Suite empfohlen werden.

- EC2-Instanz:
  - Minimaler Instanztyp: **m4-2xlarge** ist der minimale Instanztyp, der für alle NetWitness Suite-Komponenten-AMIs erforderlich ist, damit sie funktionieren kann.
  - Anpassungen des Instanztyps: Sie müssen die Instanztypen entsprechend Ihrer Datenaufnahmerate, Inhalte und Parser, Dashboard-Berichte, geplanten Berichte, Ermittlungen und aktiven Benutzer anpassen.
  - Empfohlene Einstellungen: Die empfohlenen Einstellungen in den unten stehenden Tabellen mit SA-Komponenten-Instanzen wurden unter den folgenden Umständen berechnet.
    - Es wurden Datenaufnahmeraten von 15.000 EPS und 1,5 Gbit/s verwendet.
    - Alle Komponenten wurden integriert.
    - Der Protokollstream umfasste einen Log Decoder, Concentrator und Archiver.
    - Der Paketstream umfasste einen Packet Decoder und Concentrator.
    - Respond erhielt Warnmeldungen von der Reporting Engine und von Event Stream Analysis.
    - Die Hintergrundlast umfasste Berichte, Diagramme, Warnmeldungen, Ermittlungen und Respond.
- EBS-Volumes (Speicher)

  Wenden Sie sich an den RSA-Kundensupport (https://community.rsa.com/docs/DOC-1294), um Unterstützung bei der Erhöhung der Volumes basierend auf Ihren Speicheranforderungen mit dem RSA Sizing & Scoping Calculator zu erhalten.

Hinweis: Der Concentrator-Index-Volume muss auf Provisioned IOPS-SSDs zugewiesen werden.

- Index
- Meta
- Sitzung
- Paket

Archiver

EC2-Instanz			
EPS	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
5.000	m4.xlarge Anzahl der CPU: 4 Arbeitsspeicher: 16 GB	Nein	Ja
10.000	m4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 32 GB	Nein	Ja
15.000	m4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 64 GB	Nein	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
archiver	/dev/sdg	Durchsatzoptimierte HDD	240 MB/s
Workbench aus	/dev/sdh	Durchsatzoptimierte HDD	–

Broker

EC2-Instanz		
Instanztyp	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
m4.xlarge Anzahl der CPU: 4 Arbeitsspeicher: 16 GB	Nein	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
broker	/dev/sdg	SSD für allgemeine Zwecke	–

Concentrator – Protokollstream

EC2-Instanz			
EPS	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
5.000	m4.xlarge Anzahl der CPU: 4 Arbeitsspeicher: 16 GB	Nein	Ja
10.000	m4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 32 GB	Nein	Ja
15.000	m4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 64 GB	Nein	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
index,session	/dev/sdg	Provisioned IOPS	10.000
metadb	/dev/sdh	Durchsatzoptimierte HDD	240 MB/s

Paketstream-Lösungen

Concentrator – Gigamon-Lösung

EC2-Instanz			
Mbit/s/Gbit/s	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
500 Mbit/s	c4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 30 GB	Nein	Ja
1.000 MBit/s	c4.8xlarge Anzahl der CPU: 36 Arbeitsspeicher: 60 GB	Nein	Ja
1,5 Gbit/s	m4.10xlarge Anzahl der CPU: 40 Arbeitsspeicher: 160 GB	Nein	Ja

Concentrator – f5 BIG-IP-Lösung

Muss aktualisiert werden, wenn f5 BIG-IP-Performancetests abgeschlossen sind.

EC2-Instanz			
Mbit/s/Gbit/s	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
230 MBit/s	m4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 64 GB	Nein	Nein

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
index,session	/dev/sdg	Provisioned IOPS	15.000
metadb	/dev/sdh	Durchsatzoptimierte HDD	240 MB/s

Decoder – Gigamon-Lösung

EC2-Instanz			
Mbit/s/Gbit/s	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
500 Mbit/s	c4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 15 GB	Ja	Ja
1.000 Mbit/s	c4.2xlarge Anzahl der CPU: 16 Arbeitsspeicher: 30 GB	Ja	Ja
1,5 Gbit/s	c4.8xlarge Anzahl der CPU: 36 Arbeitsspeicher: 60 GB	Ja	Ja

Decoder – f5 BIG-IP-Lösung

Muss aktualisiert werden, wenn f5 BIG-IP-Performancetests abgeschlossen sind.

EC2-Instanz			
Mbit/s/Gbit/s	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
230 MBit/s	m4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 64 GB	Nein	Nein

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
index,session,meta	/dev/sdg	Durchsatzoptimierte HDD	240 MB/s
Paket	/dev/sdh	Durchsatzoptimierte HDD	240 MB/s

ESA und Context Hub auf Mongo-Datenbank

	EC2-Instanz		
EPS	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
9.000	m4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 32 GB	Nein	Ja
18.000	r4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 61 GB	Nein	Ja
30.000 Aggregationsrat	r4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 122 GB	Nein	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
apps (/opt/rsa)	/dev/sdg	SSD für allgemeine Zwecke	–

Log Collector (Syslog-, Netflow- und Dateisammlungsprotokolle)

EC2-Instanz			
EPS	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
30.000 NICHT-SSL	c4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 15 GB	Nein	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
log Collector	/dev/sdg	SSD für allgemeine Zwecke	–

Log Decoder

EC2-Instanz			
EPS	**Instanztyp**	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
5.000	c4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 15 GB	Ja	Ja
10.000	c4.2xlarge Anzahl der CPU: 16 Arbeitsspeicher :30 GB	Ja	Ja
15.000	c4.8xlarge Anzahl der CPU: 36 Arbeitsspeicher: 60 GB	Ja	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
index,session,meta	/dev/sdg	Durchsatzoptimierte HDD	240 MB/s

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
Paket	/dev/sdh	Durchsatzoptimierte HDD	240 MB/s

NetWitness-Server, Reporting Engine, Respond und Health & Wellness

EC2-Instanz		
Instanztyp	**Optimierte Netzwerkfunktionen aktiviert**	**Typ der Mehrmandantenfähigkeit – dediziert – Ausführen einer dedizierten Instanz**
m4.2xlarge Anzahl der CPU: 8 Arbeitsspeicher: 32 GB	Nein	Ja
m4.4xlarge Anzahl der CPU: 16 Arbeitsspeicher: 64 GB	Nein	Ja

EBS-Volumes (Speicher)			
Volumes	**Device**	**Volume Type**	**IOPS/Baseline Durchsatz**
/ (root)	/dev/sda1	SSD für allgemeine Zwecke	–
usr,var,opt,home,tmp	/dev/sdf	SSD für allgemeine Zwecke	–
uax,ipdb	/dev/sdg	SSD für allgemeine Zwecke	–
redb,rehome	/dev/sdh	SSD für allgemeine Zwecke	–