



Azure-Bereitstellungsleitfaden

für Version 11.0.0.0



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.

März 2018

Inhalt

Azure-Bereitstellungsleitfaden	4
Empfehlungen zur Azure-Umgebung	4
Abkürzungen und andere in diesem Leitfaden verwendete Terminologie	4
Azure-Bereitstellungsszenarien	7
Azure-Sichtbarkeit des vollständigen NetWitness Suite-Stacks	7
Hybride Bereitstellung – Log Decoder	8
Unterstützte Services	8
VM-Konfigurationsempfehlungen für Azure	10
Azure-Bereitstellungsregeln und -Checkliste	12
Regeln	12
Checkliste	12
Schritt 1. Bereitstellung von NW-Server-Hosts in Azure	12
Aufgabe 1. - Hochladen von NW-Server-VHDs	12
Aufgabe 2. - Erstellen einer NW-Serverkopie	15
Aufgabe 3. Erstellen einer virtuellen Maschine (VM)	17
Schritt 2. Bereitstellen von Komponenten-Core-Services in Azure	26
Schritt 3. Konfiguration von Host-VMs in RSA NetWitness® Suite	31
Revisionsverlauf	33

Azure-Bereitstellungsleitfaden

Vor der Bereitstellung von RSA NetWitness® Suite in Azure 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.
- Verwenden Sie Chrome als Browser (Internet Explorer wird nicht unterstützt).

Empfehlungen zur Azure-Umgebung

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

- Gehen Sie je nach Ressourcenanforderungen der einzelnen Komponenten bei der Nutzung des Systems gemäß bewährten Vorgehensweisen vor und weisen Sie Speicherplatz entsprechend zu.
- Erstellen Sie das Concentrator-Verzeichnis für die Indexdatenbank auf der SSD.

Abkürzungen und andere in diesem Leitfaden verwendete

Terminologie

Abkürzungen	Beschreibung
Azure	Azure ist eine Public Cloud Computing-Plattform von Microsoft. Sie bietet eine Reihe von Cloud-Services an, z. B. für Datenverarbeitung, Analysen, Speicherung und Netzwerke. Sie können mit diesen Services neue Anwendungen entwickeln und skalieren oder vorhandene Anwendungen in der Public Cloud ausführen.
BYOL	„Bring your own“-Lizenzierung
CPU	Zentrale Verarbeitungseinheit (Central Processing Unit)

Abkürzungen	Beschreibung
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
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 auf Computern vor Ort installiert und ausgeführt (also nicht in Azure), d. h. im Gebäude des Unternehmens, das die Hosts verwendet.
RAM	Random Access Memory (auch als Arbeitsspeicher bezeichnet)
Sicherheit	Satz von Firewall-Regeln. Eine umfassende Liste der Ports, die Sie für alle NetWitness Suite-Komponenten einrichten müssen, finden Sie unter „Deployment: Network Architecture and Ports“ (https://community.rsa.com/docs/DOC-83050).
SSD	Solid-State-Laufwerk
vCPU	Virtual Central Processing Unit (auch als virtueller Prozessor bezeichnet)
VHD	Virtuelle Festplatte

Abkürzungen	Beschreibung
VM	Virtuelle Maschine
vRAM	Virtueller Random Access Memory. Dies ist der Arbeitsspeicher einer virtuellen Maschine.

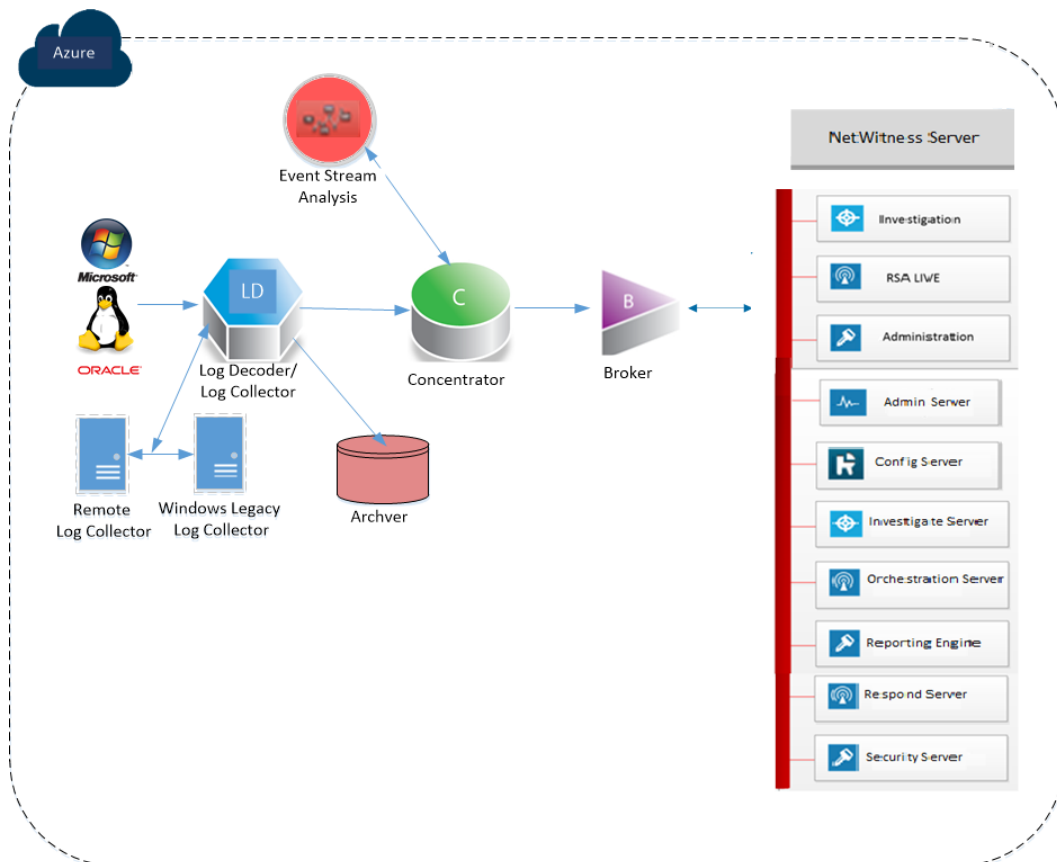
Azure-Bereitstellungsszenarien

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

- Der **Log Decoder** empfängt vom Log Collector gesammelte Protokolle. Der Log Collector 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 Engine, Investigate, RSA Live, Administration** und andere Aspekte der Benutzeroberfläche.

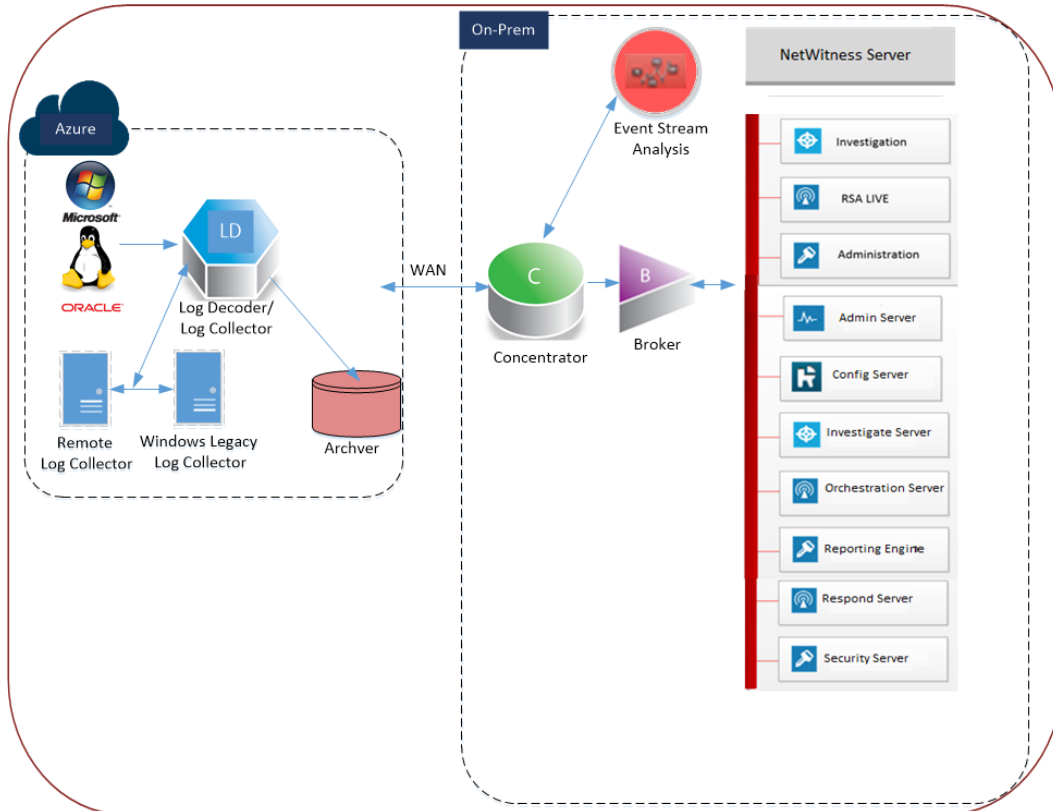
Azure-Sichtbarkeit des vollständigen NetWitness Suite-Stacks

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



Hybride Bereitstellung – Log Decoder

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



Unterstützte Services

RSA bietet die folgenden NetWitness Suite-Services.

- NetWitness-Server
- Admin-Server
- Konfigurationsserver
- Investigate Server
- Orchestration Server
- Reporting Engine
- Antwortserver

- Security Server
- Archiver
- Broker
- Concentrator
- Event Stream Analysis
- Log Decoder
- Remote Log Collector

VM-Konfigurationsempfehlungen für Azure

Hinweis: Diese Empfehlungen waren für RSA Security Analytics 10.6.4 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 [Azure-Bereitstellungsleitfaden](#).

Dieses Thema enthält die minimalen Azure VM-Konfigurationseinstellungen, die für die virtuellen Stack-Komponenten von NetWitness Suite (NW) empfohlen werden.

- VM:
 - Die empfohlenen Einstellungen in den unten stehenden Tabellen mit den NetWitness Suite-Komponenten-VMs wurden unter den folgenden Umständen berechnet.
 - Es wurden Datenaufnahmeraten von 15.000 EPS verwendet.
 - Alle Komponenten wurden integriert.
 - Der Protokollstream umfasste einen Log Decoder, Concentrator und Archiver.
 - Incident-Management erhielt Warnmeldungen von der Reporting Engine und von Event Stream Analysis.
 - Die Hintergrundlast umfasste Berichte, Diagramme, Warnmeldungen, Untersuchungen und Incident-Management.
- VHD (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: Um die EPS-Raten zu erhöhen, muss der Concentrator-Index-Volume SSDs zugewiesen werden.

VM-Größenbestimmung			
Komponente	EPS	Berechnung	VM-Größe
Archiver	15.000	Anzahl der CPU: 16 Arbeitsspeicher: 112 GB	Standard D14 v2

VM-Größenbestimmung			
Komponente	EPS	Berechnung	VM-Größe
Broker	15.000	Anzahl der CPU: 4 Arbeitsspeicher: 14 GB	Standard DS3 v2
Concentrator	15.000	Anzahl der CPU: 16 Arbeitsspeicher: 112 GB	Standard DS14 v2
ESA und Context Hub	15.000	Anzahl der CPU: 20 Arbeitsspeicher: 140 GB	Standard D15 v2
Log Collector	15.000 NICHT-SSL	Anzahl der CPU: 8 Arbeitsspeicher: 16 GB	Standard F8
Log Decoder	15.000	Anzahl der CPU: 16 Arbeitsspeicher: 112 GB	Standard D14 v2
NW-Server*	15.000	Anzahl der CPU: 16 Arbeitsspeicher: 112 GB	Standard D14 v2

*Reporting Engine, Respond und Health & Wellness können nebeneinander auf dem NetWitness-Server-Host implementiert sein.

Azure-Bereitstellungsregeln und -Checkliste

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

Regeln

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

- Verwenden Sie immer private IP-Adressen, wenn Sie Azure NetWitness Suite-VMs bereitstellen.
- Legen Sie vor Aktivierung der vordefinierten Dashboards die Standarddatenquelle auf der Reporting Engine-Konfigurationsseite fest.

Checkliste

Schritt	Beschreibung	✓
1.	Schritt 1. Bereitstellung von NW-Server-Hosts in Azure	
2.	Schritt 2. Bereitstellen von Komponenten-Core-Services in Azure	
3.	Schritt 3. Konfiguration von Host-VMs in RSA NetWitness® Suite	

Schritt 1. Bereitstellung von NW-Server-Hosts in Azure

Führen Sie die folgenden Aufgaben zur Bereitstellung eines NetWitness-Server (NW-Server) auf einer virtuellen Maschine (VM) in der Azure Cloud-Umgebung aus.

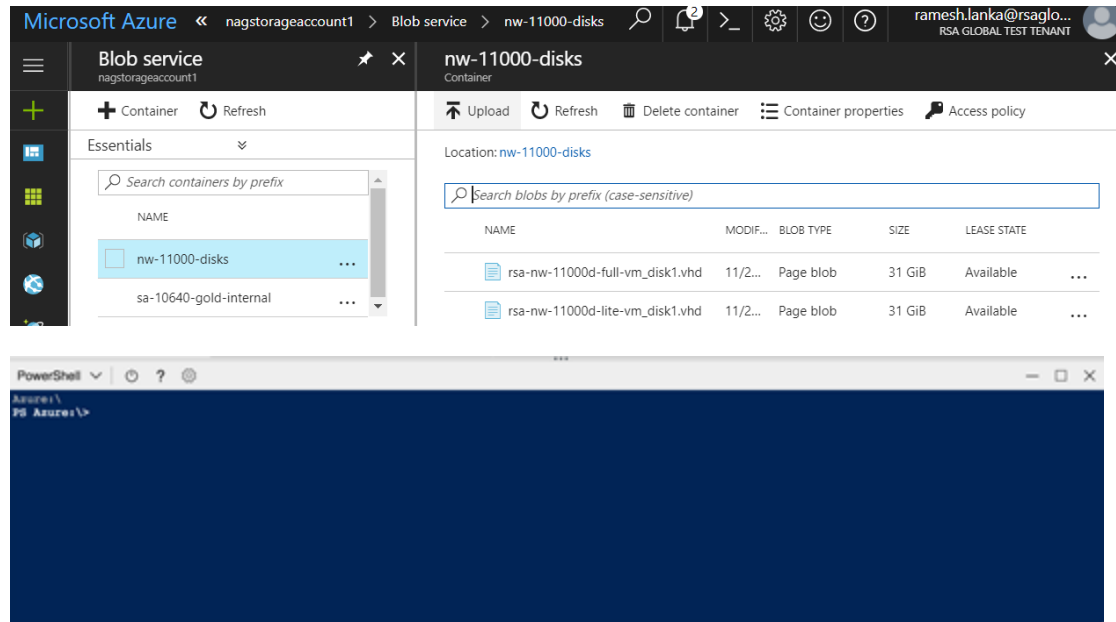
Hinweis: Es ist zur Bereitstellung von anderen Komponenten nicht zwingend erforderlich, den SA-Server in der Azure Cloud-Umgebung bereitzustellen (siehe [Azure-Bereitlungsszenarien](#)).

- [Aufgabe 1. - Hochladen von NW-Server VHDs](#)
- [Aufgabe 2. - Erstellen eines NW-Server-Image](#)
- [Aufgabe 3: - Erstellen einer virtuellen Maschine \(VM\)](#)

Aufgabe 1. - Hochladen von NW-Server-VHDs

Führen Sie die folgenden Schritte aus, um NW-Server-VHDs in Azure hochzuladen.

1. Wenden Sie sich an den RSA-Kundensupport (<https://community.rsa.com/docs/DOC-1294>), um eine Supportanfrage zu stellen, mit der Sie die NW-Server-VHDs anfordern. Eine gültige Durchsatzlizenz ist erforderlich.
2. Der Kundensupport aktualisiert den Fall mit VHD-URIs.
3. Öffnen Sie die Powershell-CLI über das Azure-Portal.



- Sie benötigen ein Speicherkonto, einen BLOB-Service und einen konfigurierten Container. Dies ist der Speicherort, an den die VHDs kopiert werden. Sobald diese vorhanden sind, können Sie den folgenden Befehl in der Powershell-CLI des Azure-Portals ausführen.

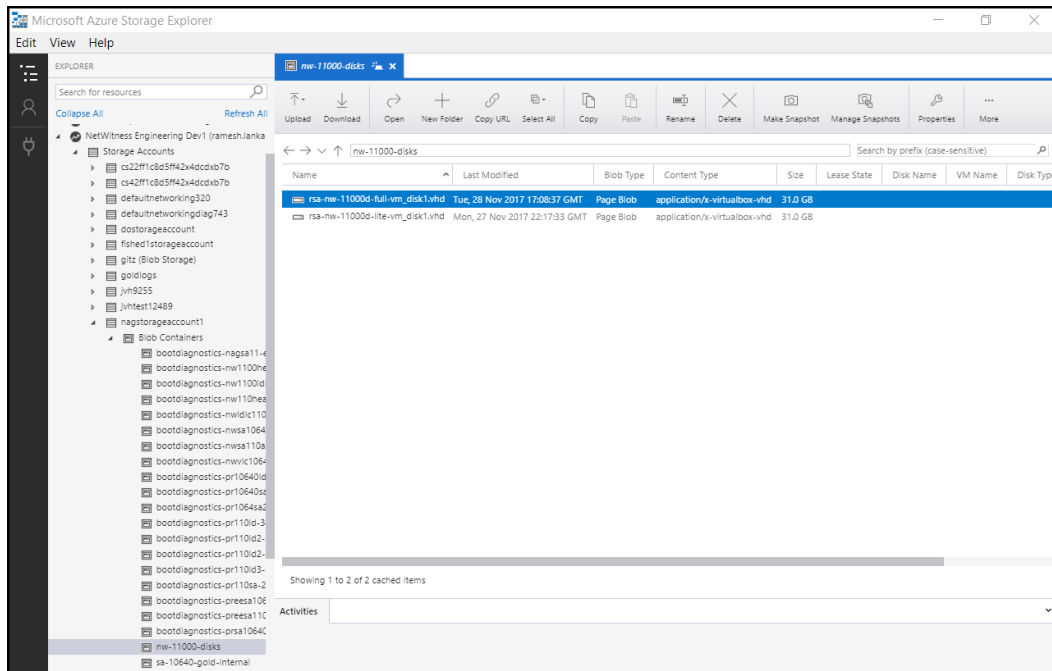
Beispiel:

```
az storage blob copy start --account-name customerstorageacct --
destination-container nwserver --destination-blob rsa-nw-11000d-
full-vm_disk1.vhd --source-uri
'https://netwitnessazure.blob.core.windows.net/nwvhdstore/rsa-nw-
11000d-full-vm_disk1.vhd?sv=2017-04-17&ss=b&srt=co&sp=rl&se=2017-
11-30T16:40:02Z&st=2017-11-
30T08:40:02Z&spr=https&sig=tBETVky%2BpTFNjAsgulzirXK99MVRt18GNRBSE
sx97k%3D' "
```

Die hervorgehobenen Flags im oben genannte Befehl müssen aktualisiert werden. Mit dem oben genannten Befehl wird die VHD kopiert. Da es zwei VHDs gibt, „Lite“ und „Full“, muss der Uploadvorgang zweimal durchgeführt werden.

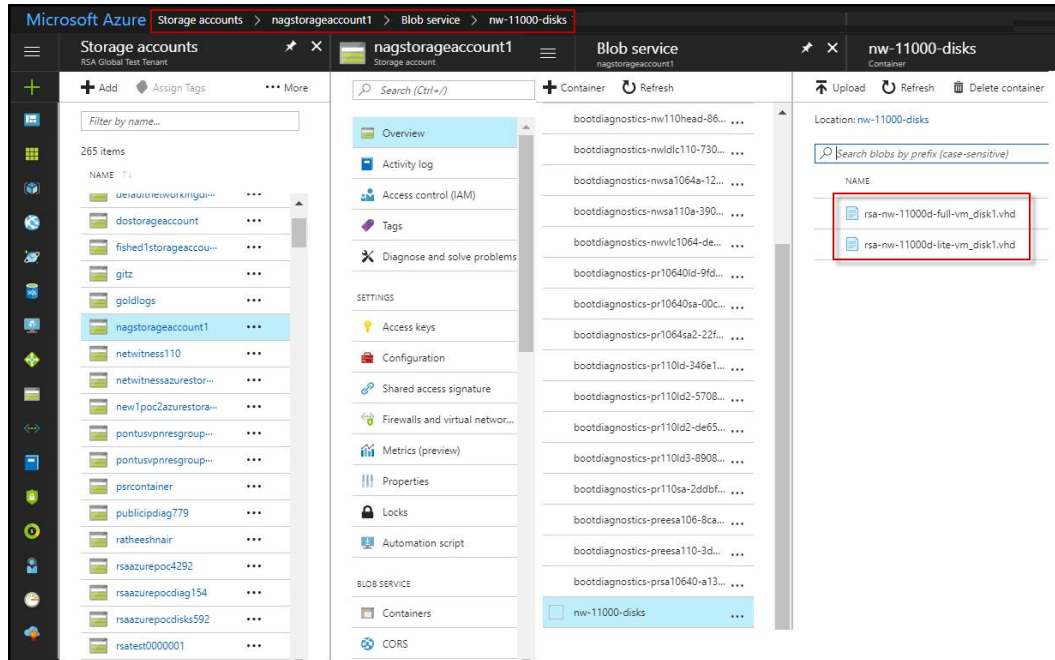
- account-name: Speicherkontoname.
 - --destination-container: der Containername.
 - --destination-blob: Name des Ziel-Blob oder der NW-Server-VHD. Ist dieser vorhanden, wird er überschrieben.
 - --source-uri: Ein SAS-Token-URI wird in der RSA-Kundensupportanfrage angegeben.
4. Sobald die VHDs erfolgreich kopiert wurden. Sie müssen ein Image und eine virtuelle Maschine erstellen.
 5. Stellen Sie sicher, dass alle NW-Server-VHDs in die Azure Cloud hochgeladen werden.

Hinweis: Alternativ können Sie das Windows-Dienstprogramm Microsoft Azure Storage Explorer (<http://storageexplorer.com/>) verwenden, um sicherzustellen, dass alle virtuellen Festplatten aus dem folgenden Speicherort-Abonnement vorhanden sind. Mit dieser Utility können Sie den Inhalt Ihres Speichers verwalten.



- a. Melden Sie sich beim Azure-Portal (<https://portal.azure.com>) an.

- b. Klicken Sie im rechten Bereich auf **Speicherkonten** > **netwitnessazurestorage1** > **Blob-Service** > **nwazurevhdstore**.

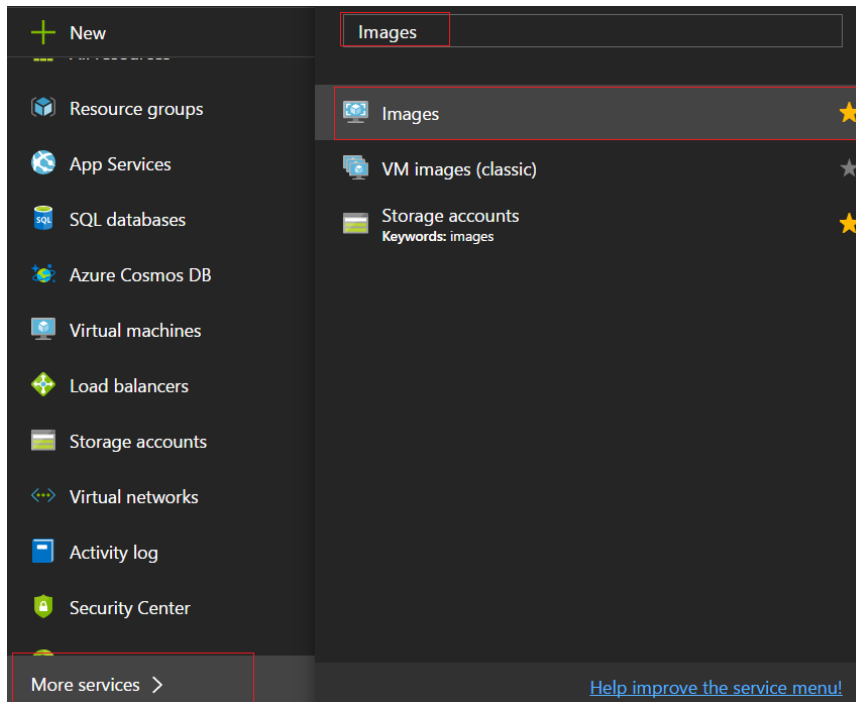


6. (Optional) Navigieren Sie im Azure-Explorer zur Gruppe **NetWitness** > **Speicherkonten** > **netwitnessazurestorage1** > **Blob-Container** > **nwazurevhdstore**). Der folgende Screenshot zeigt ein Beispiel für den Inhalt eines Speichercontainers.

Aufgabe 2. - Erstellen einer NW-Serverkopie

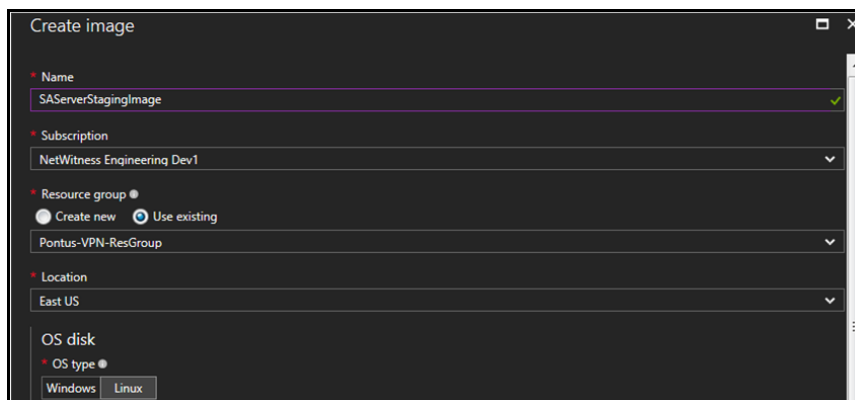
Führen Sie die folgenden Schritte aus, um in Azure aus hochgeladenen VHDs eine SA-Serverkopie zu erstellen.

1. Melden Sie sich bei <https://portal.azure.com> an.
2. Klicken Sie im linken Bereich auf **Weitere Services** und filtern Sie nach Images.

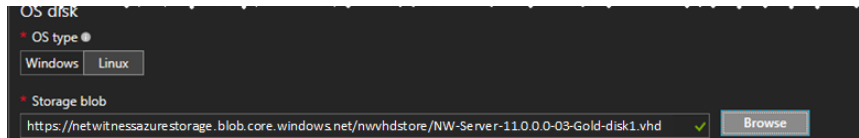
3. Klicken Sie auf **Images**.

4. Erstellen und konfigurieren Sie das Image.

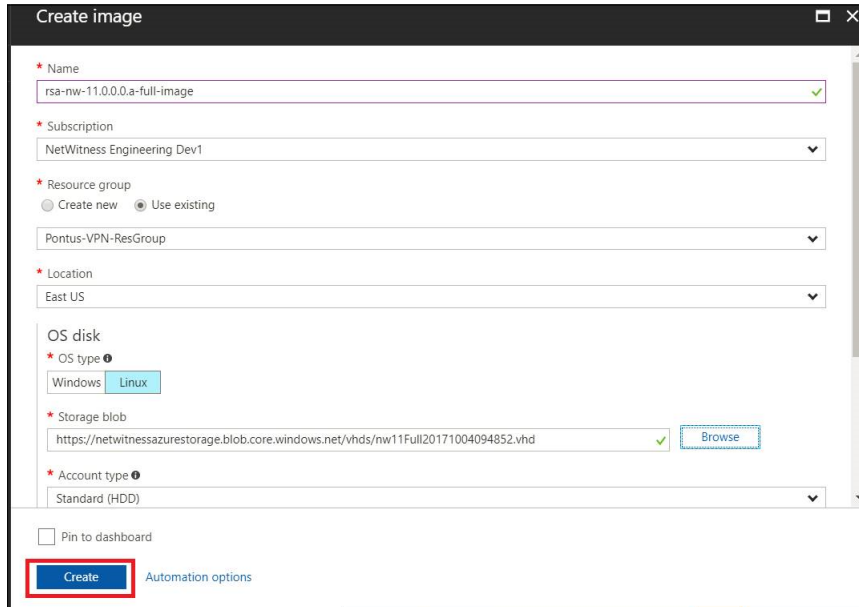
- a. Klicken Sie auf **Hinzufügen**.
- b. Geben Sie einen Image-Namen ein, wählen Sie die richtige Ressourcengruppe, wählen Sie einen gültigen Speicherort und legen Sie das Betriebssystemlaufwerk auf Linux fest. Navigieren Sie unter **Speicher-Blob** zu dem Speicherort, in den die VHDs hochgeladen werden.



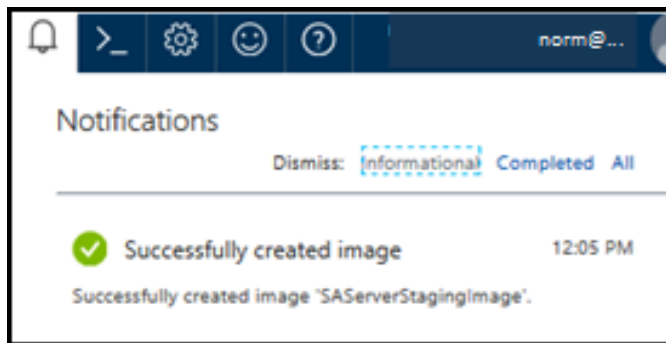
- c. Wählen Sie **https://netwitnessazurestorage.blob.core.windows.net/nwvhdstore/SA-Server-11.0.0.0-03-Gold-disk1.vhd** im Feld **BS-Laufwerk Speicher-Blob** aus.



- d. Stellen Sie sicher, dass **Standard (HDD)** für **Kontotyp** ausgewählt ist. Der folgende Screenshot zeigt eine vollständige Ansicht **Bild erstellen**.



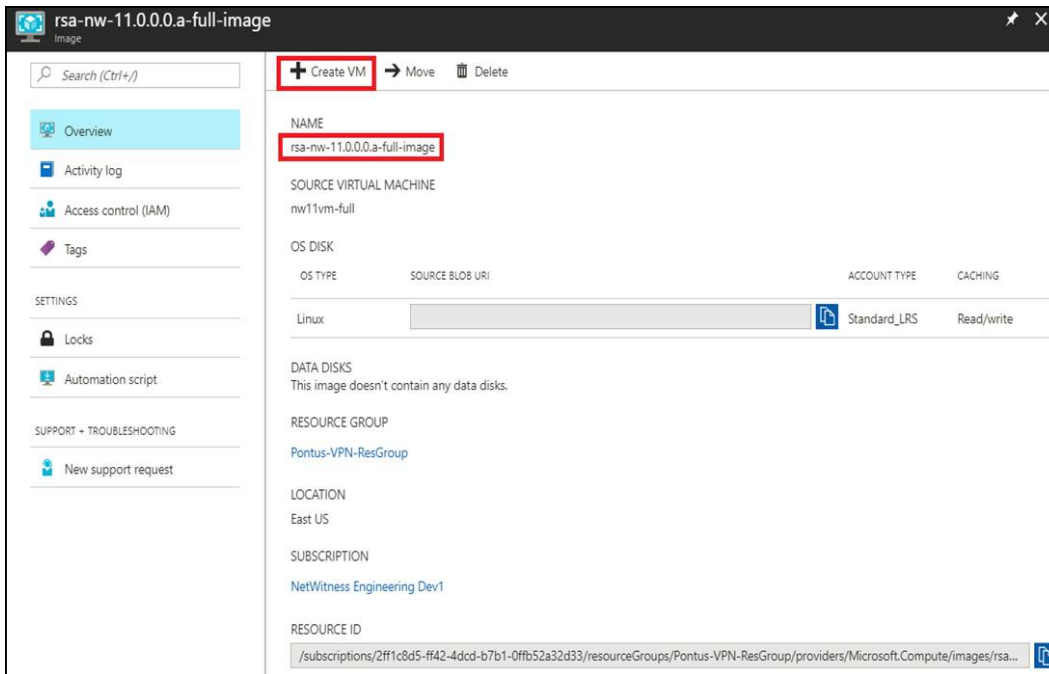
- e. Klicken Sie auf **Erstellen**, um das Image zu erstellen. Die folgende Bestätigung wird angezeigt, wenn das Image erstellt wird.



Aufgabe 3. Erstellen einer virtuellen Maschine (VM)

Führen Sie die folgenden Schritte aus, um mit dem SA-Server-Image eine VM in Azure zu erstellen.

1. Navigieren Sie zu **Images** und klicken Sie auf **VM erstellen**.



Der Abschnitt **1 Grundlagen – Grundeinstellungen konfigurieren** ist im Fokus.

2. Definieren Sie Werte für alle Felder.
 - a. Geben Sie im Feld **Name** einen benutzerdefinierten Namen (z. B. **NWServer1100**) ein.
 - b. Wählen Sie im Feld **VM-Festplattentyp** den Wert **HDD** aus der Drop-down-Liste.

Achtung: Der Benutzername und das Passwort, den bzw. das Sie definieren, wird verwendet, um sich beim System als Nicht-Administrator-Benutzer anzumelden. Verwenden Sie nicht den Root-Benutzer (die Anmeldung hat keine Superuser-Berechtigungen). Sie müssen das Root-Passwort ändern, wenn Sie sich zum ersten Mal bei der virtuellen Maschine anmelden. Dazu verwenden Sie den Befehl `su passwd root`. Dies ist ein wichtiger Schritt und sollte nicht übersprungen werden. Sie können nicht `root` für einen Benutzernamen verwenden (Azure-spezifisch).

- c. Geben Sie in das Feld **Benutzername** einen gültigen Benutzernamen ein.
- d. Klicken Sie im Feld **Authentifizierungstyp** auf **Passwort** und geben Sie ein sicheres Passwort ein, welches aus einer Kombination aus Kleinbuchstaben, Großbuchstaben, Ziffern und Symbolen besteht (z. B. **Netwitness@123**).
- e. Stellen Sie sicher, dass die in den Feldern **Abonnement**, **Ressourcengruppe** und **Speicherort** ausgewählten Werte korrekt sind.

f. Klicken Sie auf **OK**.

The screenshot shows the 'Create virtual machine' wizard in the Microsoft Azure portal. The 'Basics' tab is selected, and the 'Basics' step is highlighted in the left sidebar. The form fields are filled with the following values:

- Name: NW1100-LDNode
- VM disk type: SSD
- User name: nwadmin
- Authentication type: SSH public key
- Password: [masked]
- Confirm password: [masked]
- Subscription: NetWitness Engineering Dev1
- Resource group: Pontus-VPN-ResGroup
- Location: East US

The 'OK' button is visible at the bottom right.

Der Abschnitt **2 Größe – Größe der virtuellen Maschine auswählen** ist nun im Fokus.

- Klicken Sie auf **Erforderliche Größe basierend auf Kapazität** (z. B. **F8 Standard**) und klicken Sie dann auf **Auswählen**.

Hinweis: Die Dimensionierung hängt von den Kapazitätsanforderungen Ihres Unternehmens ab (in den [VM-Konfigurationsempfehlungen für Azure](#) finden Sie Empfehlungen von RSA zur VM-Größe basierend auf Protokollerfassungsraten). Die minimale Größe, die RSA für den SA-Server empfiehlt, ist **F8 Standard**.

F1 Standard	F2 Standard	F4 Standard
1 Core	2 Cores	4 Cores
2 GB	4 GB	8 GB
2 Data disks	4 Data disks	8 Data disks
2x500 Max IOPS	4x500 Max IOPS	8x500 Max IOPS
Load balancing	Load balancing	Load balancing
37.20 USD/MONTH (ESTIMATED)	74.40 USD/MONTH (ESTIMATED)	148.06 USD/MONTH (ESTIMATED)
F8 Standard	F16 Standard	A1_V2 Standard
8 Cores	16 Cores	1 Core
16 GB	32 GB	2 GB
16 Data disks	32 Data disks	2 Data disks
16x500 Max IOPS	32x500 Max IOPS	2x500 Max IOPS
Load balancing	Load balancing	Load balancing

Der Abschnitt **3 Einstellungen – Optionale Funktionen konfigurieren** ist nun im Fokus.

4. Klicken Sie auf und definieren Sie die Felder.
 - a. Stellen Sie im Feld **Speicher** sicher, dass **Verwaltete Festplatten verwenden** auf **Ja** festgelegt ist.
 - b. Wählen Sie im Feld **Netzwerk** Folgendes aus:
 - Ein gültiges **virtuelles Netzwerk** und **Subnetz**.



- **Keine** für **Öffentliche IP-Adresse**.

RSA empfiehlt die Auswahl von **Keine** für **Öffentliche IP-Adresse** (dies ist nicht obligatorisch). Sie können eine öffentliche IP-Adresse zuweisen, dies entspricht allerdings nicht den Best Practices zum Zuweisen einer öffentlichen IP-Adresse zu Elementen in der Azure Cloud.

- Eine gültige **Netzwerksicherheitsgruppe**.

Informationen zu Netzwerksicherheitsgruppen finden Sie in der Microsoft Azure-Dokumentation (<https://docs.microsoft.com/de-de/azure/virtual-network/virtual-networks-nsg>).

c. Wählen Sie im Feld „Monitoring“ Folgendes aus:

- **Aktiviert für Boot Diagnostics**
- **Aktiviert für Guest OS Diagnostics**
- ein gültiges **Diagnosespeicherkonto**

Der folgende Screenshot zeigt einen vollständigen Abschnitt „Einstellungen“.

Create virtual machine Settings

1 Basics Done ✓

2 Size Done ✓

3 Settings Configure optional features >

4 Summary SAServerStagingImage >

Storage

Use managed disks ☒ Yes

Network

* Virtual network >

* Subnet >

* Public IP address >

* Network security group (firewall) >

Extensions

Extensions >

High availability

* Availability set >

Monitoring

Boot diagnostics ☒ Enabled

Guest OS diagnostics ☐ Disabled ☐ Enabled

* Diagnostics storage account >

OK

d. Klicken Sie auf **OK**.

Der Abschnitt **4 Zusammenfassung – SA-Server-Staging-Image** ist nun im Fokus.

5. Überprüfen Sie, ob die Validierung erfolgreich war, und klicken Sie auf **OK**.

 Validation passed

Basics

Subscription	NetWitness Engineering Dev1
Resource group	Pontus-VPN-ResGroup
Location	East US

Settings

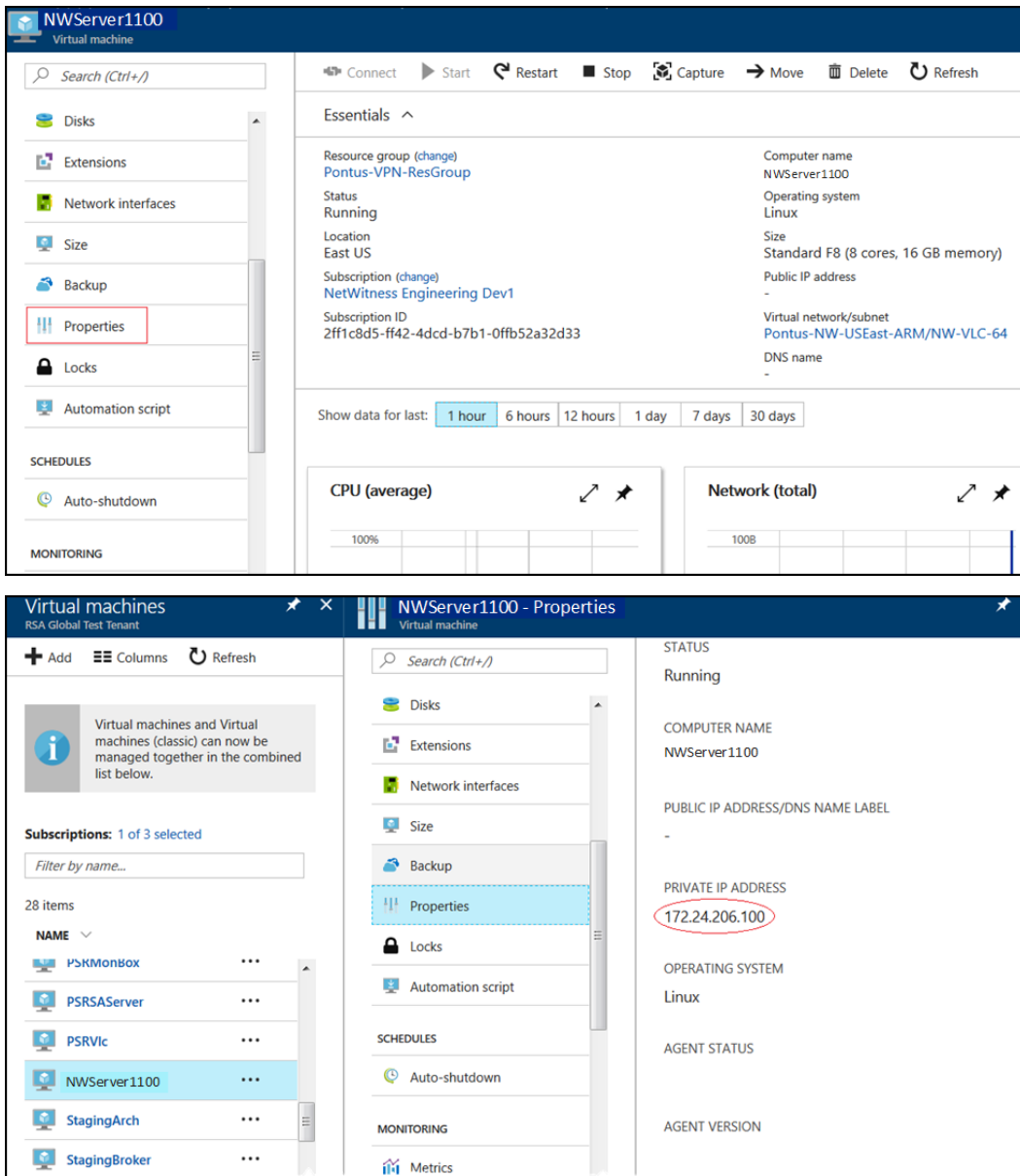
Computer name	NW1100-HeadNode
Disk type	SSD
User name	nwadmin
Size	Standard E4s v3
Managed	Yes
Private image	rsa-nw-11.0.0.0.a-full-image
Virtual network	Pontus-NW-USEast-ARM
Subnet	NW-VLC-64 (172.24.206.64/26)
Public IP address	None
Network security group (firewall)	None
Availability set	None
Guest OS diagnostics	Enabled
Boot diagnostics	Enabled
Diagnostics storage account	netwitness110
Auto-shutdown	Off

OK

Download template and parameters

Sie wissen, dass die NW-Server-VM-Bereitstellung erfolgreich war, wenn als VM-Status **Wird ausgeführt** angezeigt wird.

6. Klicken Sie auf **Eigenschaften**, um Details zur **IP-Adresse** anzuzeigen.



The top screenshot shows the 'NWServer1100' virtual machine page in the Azure portal. The 'Essentials' tab is active, displaying key information: Resource group (Pontus-VPN-ResGroup), Status (Running), Location (East US), Subscription (NetWitness Engineering Dev1), and Subscription ID (2ff1c8d5-ff42-4cd-b7b1-0ffb52a32d33). It also shows the Computer name (NWServer1100), Operating system (Linux), Size (Standard F8 (8 cores, 16 GB memory)), and Virtual network/subnet (Pontus-NW-USEast-ARM/NW-VLC-64). The 'Properties' tab is highlighted in the left-hand navigation pane.

The bottom screenshot shows the 'Virtual machines' overview page for the 'RSA Global Test Tenant'. A list of virtual machines is shown on the left, with 'NWServer1100' selected. The 'Properties' tab for this VM is active on the right. It displays the STATUS (Running), COMPUTER NAME (NWServer1100), PUBLIC IP ADDRESS/DNS NAME LABEL (-), and PRIVATE IP ADDRESS (172.24.206.100, which is circled in red). Other properties shown include OPERATING SYSTEM (Linux), AGENT STATUS, and AGENT VERSION.

7. Stellen Sie über SSH eine Verbindung mit der VM dar. Verwenden Sie den Benutzernamen, den Sie in Schritt 2d unter [Aufgabe 3](#) angegeben haben, und setzen Sie das Passwort **Root** zurück. Verwenden Sie die Befehlszeichenfolge `su passwd root`, um das Root-Passwort

zurückzusetzen, wie im folgenden Screenshot gezeigt.

```
login as: nwadmin
Using keyboard-interactive authentication.
Password:
[nwadmin@NW1100-HeadNode ~]$ sudo passwd root

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for nwadmin:
Changing password for user root.
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
passwd: all authentication tokens updated successfully.
[nwadmin@NW1100-HeadNode ~]$
```

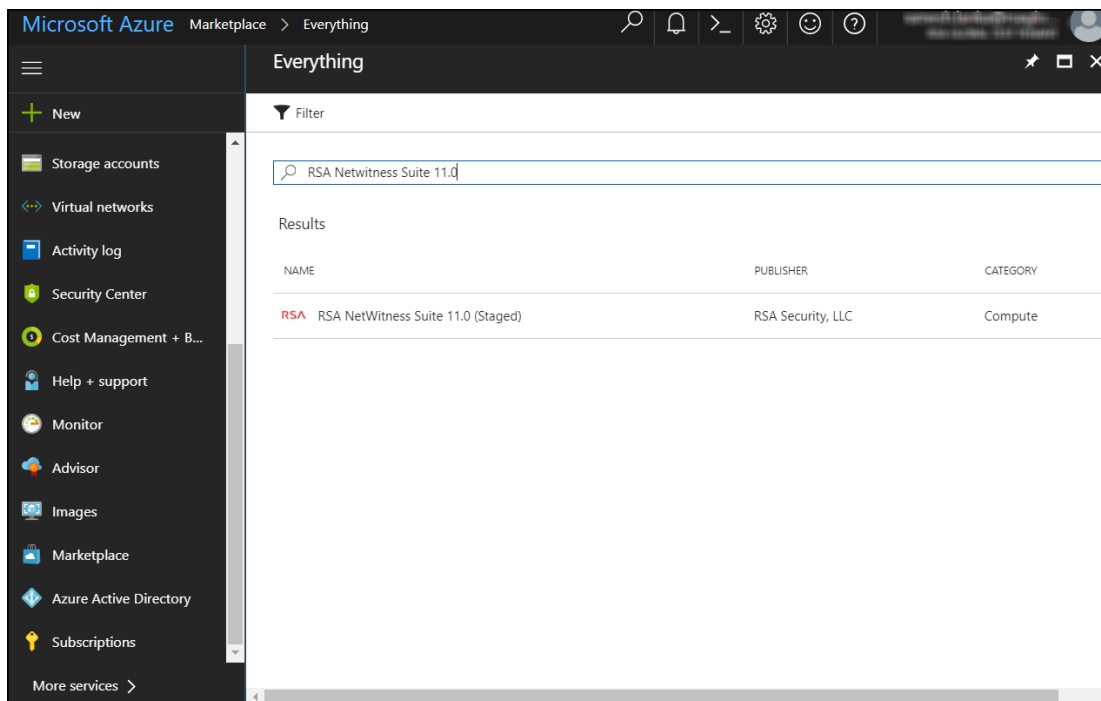
8. Schließen Sie die aktuelle SSH-Sitzung und öffnen Sie eine neue SSH-Sitzung mit **Root** als Benutzernamen und dem im vorherigen Schritt erstellten Passwort.

Hinweis: Schritt 8 ist ein kritischer, einmaliger Schritt für eine neue Bereitstellung. Wenn Sie diesen Schritt nicht abschließen, wird die Security Analytics-Benutzeroberfläche nicht geladen.

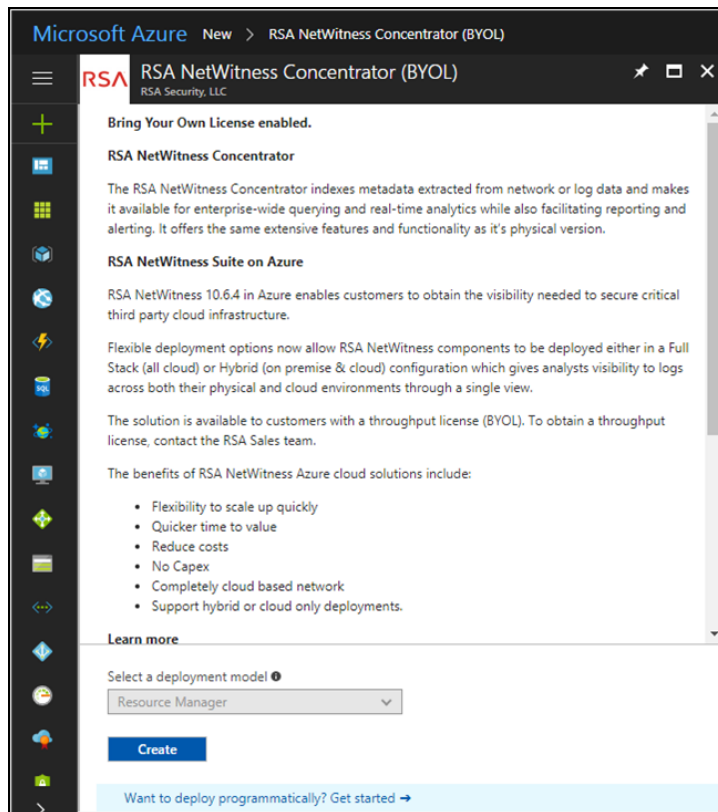
Schritt 2. Bereitstellen von Komponenten-Core-Services in Azure

Führen Sie das folgende Verfahren aus, um Core-RSA NetWitness® Suite-Komponentenservices auf virtuellen Maschinen (VMs) in der Azure-Cloud-Umgebung zu konfigurieren.

1. Navigieren Sie zu azuremarketplace.microsoft.com und melden Sie sich mit Ihren Anmeldedaten an.
2. Suchen Sie nach RSA.



3. Klicken Sie auf RSA NetWitness® Suite-Core-Service (z. B. **RSA NetWitness Concentrator**) und klicken Sie dann auf **Erstellen**.



Der Assistent **Erstellen einer virtuellen Maschine** wird angezeigt. Der Abschnitt **1 Grundlagen** ist im Fokus.

4. Führen Sie die grundlegenden Einstellungen durch.
 - a. Geben Sie unter **Name** einen Namen für eine virtuelle Maschine an (z. B. **Concentrator**).
 - b. Wählen Sie **SSD** als **VM-Festplattentyp** des Concentrator aus. Wählen Sie „HDD“ für alle anderen Komponenten aus.
 SSD (Solid State Disk) hat eine bessere Performance als eine HDD.
 - c. Wählen Sie **Passwort** als **Authentifizierungstyp** aus.
 - d. Geben Sie Ihre Anmeldedaten ein (d. h. **Benutzername** und **Passwort**) und bestätigen Sie das Passwort unter **Passwort bestätigen**.
 - e. Klicken Sie auf **OK**.

The screenshot shows the 'Create virtual machine' wizard in the Microsoft Azure portal, specifically the 'Basics' step. The left sidebar shows the progress: 1 Basics (selected), 2 Size, 3 Settings, and 4 Summary. The main area contains the following fields:

- Name:** NW1100-LDNode (with a green checkmark)
- VM disk type:** SSD (dropdown menu)
- User name:** nwadmin (with a green checkmark)
- Authentication type:** SSH public key (selected) and Password (button)
- Password:** (masked with dots, with a green checkmark)
- Confirm password:** (masked with dots, with a green checkmark)
- Subscription:** NetWitness Engineering Dev1 (dropdown menu)
- Resource group:** Create new (radio button) and Use existing (radio button, selected). The dropdown shows 'Pontus-VPN-ResGroup'.
- Location:** East US (dropdown menu)

An 'OK' button is at the bottom right.

Azure überprüft Ihre Grundeinstellungen. Der Abschnitt **2 Größe** ist nun im Fokus.

5. Klicken Sie auf die geeignete VM-Größe (z. B. **Standard DS14 v2** für den Concentrator) für den Service und klicken Sie auf **Auswählen** für die **Größe** einer virtuellen Maschine.

Unter [VM-Konfigurationsempfehlungen für Azure](#) finden Sie Empfehlungen von RSA zu den VM-Größen für jeden Service.

The screenshot shows the 'Create virtual machine' wizard in the Microsoft Azure portal, specifically the 'Choose a size' step. The left sidebar shows the progress: 1 Basics (Done), 2 Size (selected), 3 Settings, and 4 Purchase. The main area displays a table of available VM sizes with their features and estimated costs.

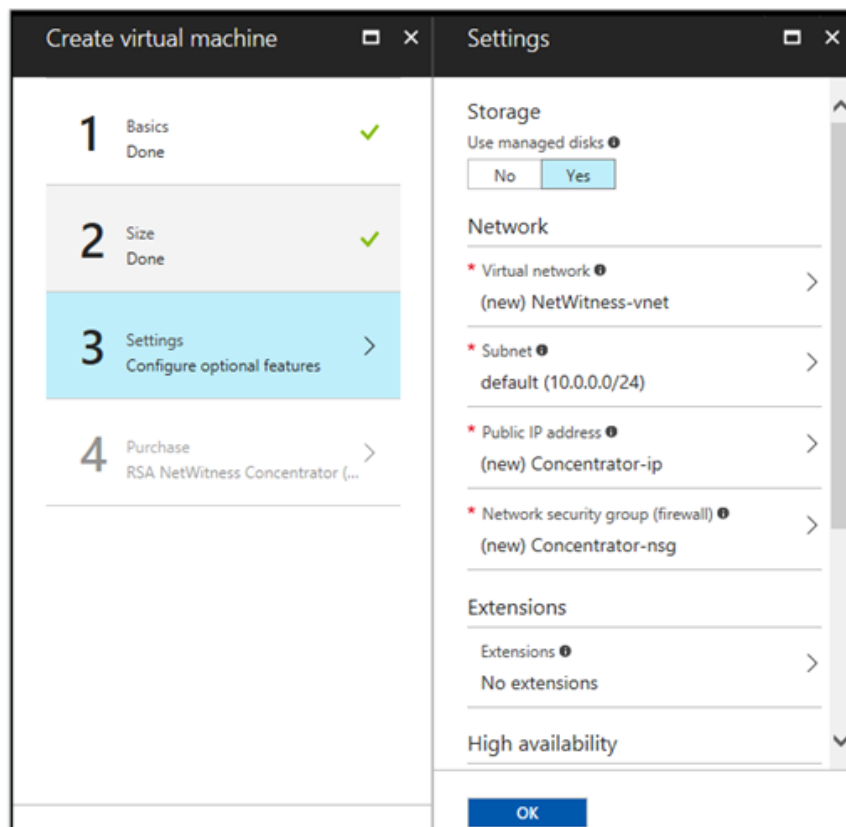
DS14_V2 Standard		DS15_V2 Standard		D2_V3 Standard	
USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)	
16	Cores	20	Cores	2	Core
112	GB	140	GB	8	GB
32	Data disks	40	Data disks	2	Data disks
50000	Max IOPS	62500	Max IOPS	2x500	Max IOPS
224 GB	Local SSD	280 GB	Local SSD	50 GB	Local SSD
Load balancing		Load balancing			
Premium disk support		Premium disk support			

A 'Select' button is at the bottom center.

Azure überprüft Ihre Angaben für die **Größe**. Der Abschnitt **3 Einstellungen** ist nun im Fokus.

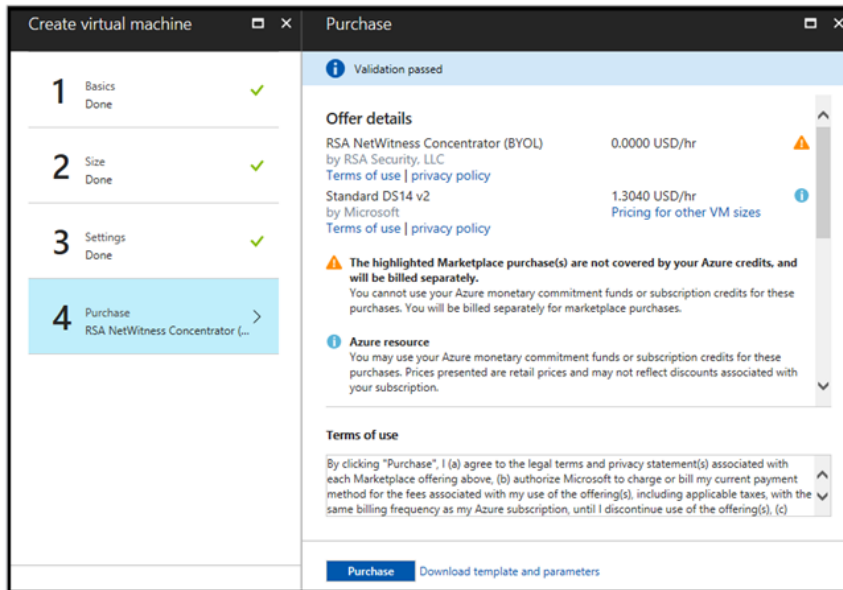
6. Nehmen Sie die **Einstellungen** vor.
 - a. Stellen Sie im Feld **Speicher** sicher, dass **Verwaltete Festplatten verwenden** auf **Ja** festgelegt ist.
 - b. Gehen Sie unter **Netzwerk** wie folgt vor:
 - Passen Sie die Angaben unter **Virtuelles Netzwerk**, **Subnetz** und **Öffentliche IP-Adresse** an die Anforderungen Ihres Netzwerks an.
 - Geben Sie eine gültige **Netzwerksicherheitsgruppe** an.

Informationen zu Netzwerksicherheitsgruppen finden Sie in der Microsoft Azure-Dokumentation (<https://docs.microsoft.com/de-de/azure/virtual-network/virtual-networks-nsg>). Eine umfassende Liste der Ports, die Sie für alle RSA NetWitness® Suite-Komponenten einrichten müssen, finden Sie unter „Deployment: Network Architecture and Ports“ (<https://community.rsa.com/docs/DOC-83050>).



- c. Klicken Sie auf **OK**.

Azure überprüft Ihre VMs. Der Abschnitt **4 Kauf** ist nun im Fokus.



7. Klicken Sie auf **Kauf**, um die Core-Service-VM für die RSA Security Analytics-Komponente (z. B. **Concentrator**) in Azure zu erstellen.
8. Konfigurieren Sie den VM-Host in RSA NetWitness® Suite 11.0.0.
Siehe [Schritt 3. Konfiguration von Host-VMs in RSA NetWitness® Suite](#).
9. Wiederholen Sie die Schritte 1 bis 8 für die restlichen Komponenten-Core-Services von RSA Security Analytics.

Schritt 3. Konfiguration von Host-VMs in RSA 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 eine virtuelle Maschine erfolgreich erstellt haben, weist Azure dieser einen Standardhostnamen zu. Anweisungen zum Ändern eines Hostnamens finden Sie in „Ändern des Namens und Hostnamens eines Hosts“ unter *Bearbeiten eines Hosts* (<https://community.rsa.com/docs/DOC-41716>) in der RSA NetWitness® Suite-Hilfe.

1. Stellen Sie über SSH eine Verbindung mit dem Host her. Verwenden Sie die Anmeldedaten, die Sie im Abschnitt **1 Grundlagen** des Assistenten zur **VM-Erstellung** bei der Erstellung der VM in Azure angegeben haben (siehe Punkt 4d von [Schritt 2. Bereitstellen von Komponenten-Core-Services in Azure](#)).
2. Setzen Sie das Passwort für **root** zurück.

```
login as: nwadmin
Using keyboard-interactive authentication.
Password:
[nwadmin@NW1100-HeadNode ~]$ sudo passwd root

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

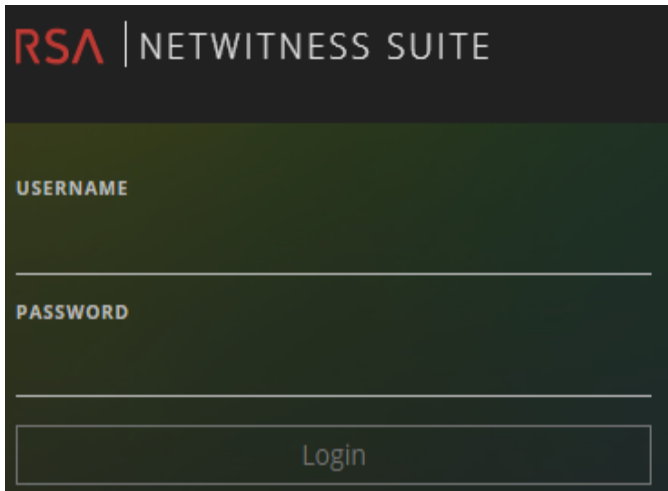
[sudo] password for nwadmin:
Changing password for user root.
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
passwd: all authentication tokens updated successfully.
[nwadmin@NW1100-HeadNode ~]$
```

3. Stellen Sie über SSH eine Verbindung zum Host her. Verwenden Sie **root** als Benutzername und das im vorherigen Schritt erstellte Passwort und stellen Sie für NetWitness Suite eine IP-Adresse für das Provisioning bereit.

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Mon Nov  6 08:29:23 2017 from 172.24.193.230
[root@NW1100-HeadNode ~]# nwsetup-tui
```

Informationen finden Sie im Abschnitt „Aufgaben für die Installation“ und im Abschnitt „Konfigurieren von Hosts (Instanzen)“ im *AWS-Bereitstellungshandbuch für RSA NetWitness 11.0.0.0*.

4. Melden Sie sich bei RSA NetWitness Suite an.



The image shows the RSA NetWitness Suite login interface. It features a dark background with the RSA logo and 'NETWITNESS SUITE' text at the top. Below this, there are two input fields labeled 'USERNAME' and 'PASSWORD'. At the bottom, there is a 'Login' button.

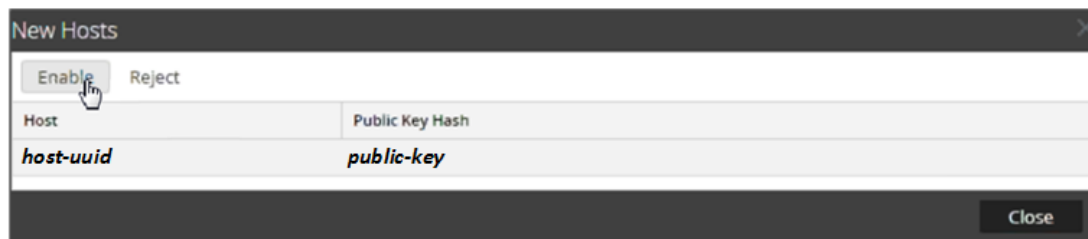
5. Navigieren Sie zu **Administration > Hosts**.

Das Dialogfeld **Neue Hosts** wird mit den Host-VMs angezeigt, die Sie in Azure erstellt haben.

6. Wählen Sie die Hosts aus, die Sie aktivieren möchten.



Die Menüoption **Aktivieren** wird aktiv.

7. Klicken Sie auf **Aktivieren**.



The image shows the 'New Hosts' dialog box. It has a title bar with 'New Hosts' and a close button. Inside, there are two buttons: 'Enable' (which is highlighted with a mouse cursor) and 'Reject'. Below these buttons is a table with two columns: 'Host' and 'Public Key Hash'. The table contains one row with the values 'host-uuid' and 'public-key'. At the bottom right, there is a 'Close' button.

8. Wählen Sie den Host aus, den Sie aktiviert haben.

9. Klicken Sie auf  **Install**  und wählen Sie die Komponente aus, die Sie in Azure bereitgestellt haben (z. B. Event Stream Analysis). Weitere Informationen erhalten Sie im *Leitfaden für die ersten Schritte mit Hosts und Services für Version 11.0.0.0*.

Revisionsverlauf

Version	Datum	Beschreibung
1,0	21-Jan	Erste Version

