

Upgrade-Checkliste für virtuelle Hosts

für Version 10.6.6 auf 11.2

Aufgabe	Beschreibung	✓
Upgrade vorbereiten		
1.	Laden Sie RSANW-11.2-VirtUpgradeGde.pdf von RSA Link herunter und lesen Sie das Dokument. a. Beachten Sie die nicht unterstützten Komponenten und Services in 11.x. b. Lesen Sie die Abschnitte „Zu berücksichtigende Aspekte beim Upgrade von Event Stream Analysis (ESA)“ und „Investigate im gemischten Modus“ sorgfältig durch. c. Überprüfen Sie die neuen erforderlichen Ports.	
2.	Beachten Sie die Hardware, Bereitstellungen, Services und Funktionen, die in 11.1 nicht unterstützt werden.	
3.	Stellen Sie sicher, dass das Intervall für die Ausführung der Datenaufbewahrung ≥ 24 Stunden ist, damit der Respond-Service in 11.2 aktiviert wird.	
4.	Führen Sie die Aufgaben zur Vorbereitung des Upgrades für die Funktionen aus, die Sie verwenden. Achtung: Stellen Sie sicher, dass Sie die neuen Ports implementieren und testen, sodass das Upgrade nicht aufgrund von fehlenden Ports fehlschlägt.	
5.	Erstellen Sie einen externen CentOS 6-Host, um Backup-Tar-Dateien zu speichern.	
6.	Laden Sie die Datei <code>nw-backup-v4.0.zip</code> von RSA Link (https://community.rsa.com/docs/DOC-81514) auf den externen Host herunter.	
7.	Führen Sie die Skripte <code>get-all-systems.sh</code> und <code>ssh-propagate.sh</code> von dem externen Host aus aus.	
8.	Bewahren Sie eine Kopie der Datei <code>get-all-systems-master</code> zur späteren Referenz auf.	
9.	Führen Sie <code>nw-backup.sh</code> im TEST-Modus aus, um den Speicherplatzbedarf des externen Hosts zu evaluieren (z. B.: <code>nw-backup -t -l -D</code>).	
10.	Überprüfen Sie die Backupoptionen für <code>nw-backup.sh</code> , indem Sie das Hilfemenü anzeigen (<code>nw-backup.sh -h</code>).	

Aufgabe	Beschreibung	✓
Migrieren von Festplattenlaufwerken		
11.	Sichern Sie Daten in virtuellen 10.6.6.x-Maschinen (VMs).	
12.	Laden Sie 11.2 OVA von RSA Link herunter.	
13.	Stellen Sie den gleichen 10.6.6.x VM-Stack in 11.2 bereit.	
14.	Schalten Sie die 10.6.6.x- und die 11.2-VM aus.	
15.	Kopieren Sie die VMDK-Dateien aus 10.6.6.x und fügen Sie sie dem 11.2 OVA hinzu, der in Schritt 12 bereitgestellt wurde.	
16.	Behalten Sie die MAC-Adresse der aktualisierten SA-Server-VM bei.	
17.	Entfernen Sie die 10.6.6.x-VM aus dem Bestand (löschen Sie die VM nicht).	
18.	Schalten Sie die 11.2-VM ein.	
19.	Mounten Sie das Dateisystem von VMDK.	
20.	Stellen Sie die Backupdaten aus 10.6.6.x auf den 11.2-VMs wieder her.	
Phase 1: Einrichtung von SA-Server, Event Stream Analysis, Malware Analysis sowie Broker oder Concentrator-Hosts		
21.	Aktualisieren Sie den Inhalt von <code>all-systems</code> , sodass sie aus den Backupdaten von SA, ESA, MA und Broker/Concentrator bestehen.	
22.	Setzen Sie auf den ESA-Hosts das Administratorpasswort für die Mongo-Datenbank auf „netwitness“ zurück, wenn es Sonderzeichen enthält .	
23.	Führen Sie <code>nw-backup.sh</code> mit dem Flag <code>-u</code> für alle Hosts von Phase 1 aus und bestätigen Sie, dass es ohne Fehler abgeschlossen wurde.	
24.	Wenn Ihre Umgebung mehrere ESA-Appliances umfasst, bestimmen Sie einen primären ESA (auf dem der Context-Hub-Service ausgeführt wird) und kopieren Sie die Dateien <code>mongodb.tar.gz.*</code> von den sekundären ESAs auf den Standardbackuppfad des designierten primären ESA.	
25.	Vergewissern Sie sich, dass die Backup-Tar-Dateien lokal und remote gespeichert werden.	
26.	Richten Sie den 10.6.6.x SA-Serverhost auf dem 11.2 NW-Serverhost ein, indem Sie das Programm <code>nwsetup-tui</code> auf dem Host ausführen.	
27.	Installieren Sie die Services ESA, Malware Analysis und Broker oder Concentrator in der NetWitness 11.2-Benutzeroberfläche.	

Aufgabe	Beschreibung	✓
Phase 2: Upgrade für alle anderen Hosts durchführen		

Aufgabe	Beschreibung	✓
28.	Aktualisieren Sie die Inhalte von <code>all-systems</code> , sodass sie aus den Hostbackupdaten von Phase 2 bestehen.	
29.	Führen Sie <code>nw-backup.sh</code> im TEST-Modus aus, um den Speicherplatzbedarf des externen Hosts zu evaluieren (z. B.: <code>nw-backup -t -l -D</code>).	
30.	Führen Sie <code>nw-backup.sh</code> mit dem Flag <code>-u</code> für alle Hosts von Phase 2 aus und bestätigen Sie, dass es ohne Fehler abgeschlossen wurde.	
31.	Vergewissern Sie sich, dass die Backup-Tar-Dateien lokal und remote gespeichert werden.	
32.	Richten Sie alle anderen Hosts auf dem NW-Serverhost von 11.2 ein, indem Sie das Programm <code>nwsetup-tui</code> auf dem Host ausführen.	
33.	Installieren Sie den Hostservice in der NetWitness 11.2-Benutzeroberfläche:	
Durchführen von Anpassungen nach dem Upgrade		
34.	Führen Sie die Aufgaben nach dem Upgrade für die Funktionen aus, die Sie verwenden.	

Revisionsverlauf

Version	Datum	Beschreibung	Verfasser
1,0	11. September 2018	Allgemeine Verfügbarkeit (General Availability, GA)	IDD