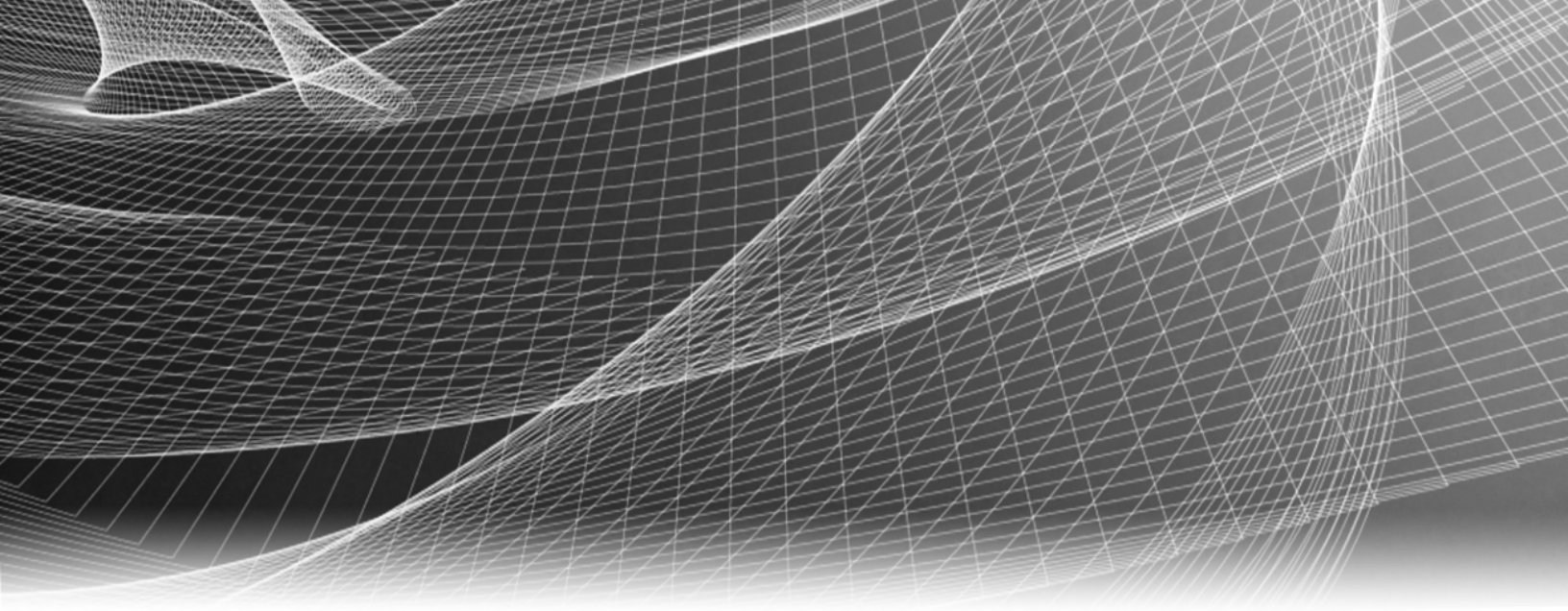


RSA Security Analytics

Serie 5 DAC mit 60 Laufwerken – Konfigurationshandbuch

RSA

EMC²

Trademarks

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the thirdpartylicenses.pdf file.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Serie 5 DAC mit 60 Laufwerken – Konfigurationshandbuch

- Serie 5 DAC mit 60 Laufwerken – Konfigurationshandbuch 4
  - DAC-Hardwarebeschreibung 5
  - Installieren des DAC 7

RSA

Serie 5 DAC mit 60 Laufwerken – Konfigurationshandbuch

Überblick

Dieses Dokument enthält Anweisungen zur Installation eines DAC mit 60 Laufwerken an Serie 5 Decoder-, Log Decoder- und Archiver-Appliances.

Kontext

Die Anweisungen zur Hardwarekonfiguration in diesem Dokument gelten nur für Hardware. Sie gelten nicht für eine spezifische Version der Security Analytics-Software. Dieses Dokument ist nur für neue Hardware gedacht. Es ist nicht für DACs mit bereits vorhandenen Daten vorgesehen.

⚠ **Caution:** Wenn Sie ein vorhandenes DAC zu einer neuen Appliance hinzufügen, befolgen Sie NICHT die Anweisungen in diesem Handbuch. Wenden Sie sich an RSA Customer Care.

Wenn Sie über ein DAC mit bereits vorhandenen Daten verfügen und versuchen, das Skript in diesen Anweisungen auszuführen, könnte das Skript fehlschlagen oder alle vorhandenen Daten auf dem DAC könnten gelöscht werden und alle erforderlichen virtuellen Laufwerke, logischen Volumes und die Verzeichnisstruktur könnten erstellt werden.

Note: Beachten Sie beim Lesen eines gedruckten Handbuchs, dass eventuell online unter **sadocs.emc.com/de-de** eine neuere Version erhältlich ist. Dieses Handbuch ist in der Security Analytics-Onlinehilfe unter "Hardware-Installationshandbücher" verfügbar.

Last Modified: September 14 2016, 12:09PM

RSA

DAC-Hardwarebeschreibung

Überblick

Dieses Thema bietet eine Übersicht über das Speichergerät RSA Direct-Attached Capacity (DAC) mit 60 Laufwerken.

Hardwarebeschreibung

Das DAC mit 60 Laufwerken ist ein leistungsstarkes Laufwerkarraygehäuse von EMC^2. Das DAC dient zur Erweiterung des nutzbaren Speichers auf einer Serie 5 Decoder-, Log Decoder- oder Archiver-Appliance.

Einführung

Die RSA Security Analytics-DAC-Appliance wird mit installierter DAC-Software geliefert. Die Erstkonfiguration eines DAC in Ihrem Netzwerk umfasst die folgenden Schritte:

1. Lesen Sie die Standortanforderungen und Sicherheitsinformationen.
2. Installieren Sie das DAC.

Lieferumfang

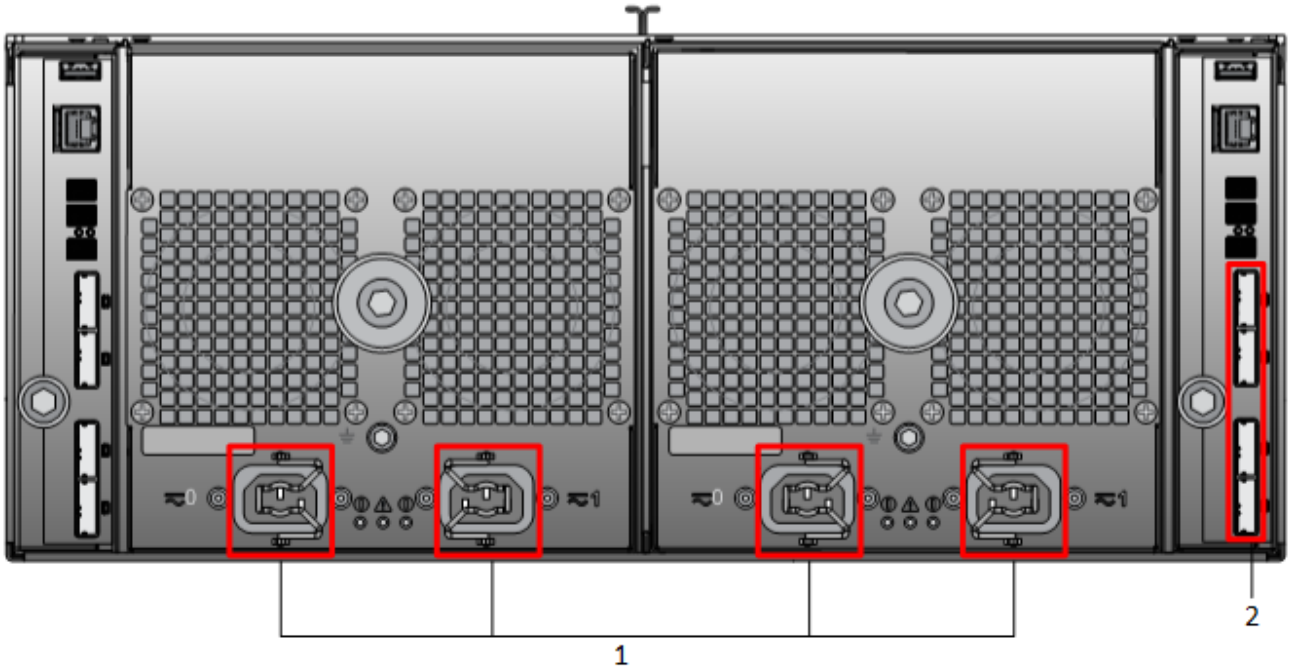
Lesen Sie hierzu die EMC^2 Dokumentation im Lieferumfang des DAC.

Materialien vom Kunden

Sie benötigen keine weiteren Materialien.

Last Modified: September 14 2016, 12:09PM

Rückansicht des DAC



Schlüssel	Beschreibung
1	Netzanschlussbuchsen
2	SAS-Ports Jede Portgruppe umfasst zwei primäre Ports und zwei Erweiterungsports. Die primären Ports befinden sich jeweils näher an der Oberseite des Gehäuses. **Note:** Verwenden Sie zum Anschluss des DAC mit 60 Laufwerken an die Appliance nur die markierten SAS-Ports.

Last Modified: September 14 2016, 12:09PM

RSA

Installieren des DAC

Überblick

In diesem Thema wird erläutert, wie ein DAC mit 60 Laufwerken an folgenden Serie 5 Appliances installiert wird:

- Decoder
- Log Decoder
- Archiver

Voraussetzungen

Stellen Sie sicher, dass Sie über die folgende erforderliche Software verfügen:

- `rsa-sa-tools-10.5.1.0.82-1.el6.noarch.rpm` oder höher mit dem zur Konfiguration des Speichers erforderlichen Skript.

Diese RPM wird vierteljährlich aktualisiert. Bitte wenden Sie sich an RSA Customer Care, um die neueste Version zu erhalten.

⚠ **Caution:** Wenn Sie ein vorhandenes DAC zu einer neuen Appliance hinzufügen, befolgen Sie NICHT die Anweisungen in diesem Handbuch. Wenden Sie sich an RSA Customer Care.

Wenn Sie über ein DAC mit bereits vorhandenen Daten verfügen und versuchen, das Skript in diesen Anweisungen auszuführen, könnte das Skript fehlschlagen oder alle vorhandenen Daten auf dem DAC könnten gelöscht werden und alle erforderlichen virtuellen Laufwerke, logischen Volumes und die Verzeichnisstruktur könnten erstellt werden.

Last Modified: September 14 2016, 12:09PM

Übergeordnetes Verfahren

In der folgende Tabelle sind die Installationsanweisungen zusammengefasst.

Appliances	Aufgaben
Decoder, Log Decoder und Archiver	1. Verbinden Sie das DAC mit der Appliance, bevor Sie die Appliance einschalten, wie in Verbinden eines DAC mit 60 Laufwerken mit einer Appliance beschrieben. 2. Führen Sie das Skript `NwArrayConfig.py` aus, wie in Ausführen des DAC-Installationsskripts auf dem Decoder, Log Decoder oder Archiver beschrieben. 3. Starten Sie den Service neu, wie unter Neustarten des Services beschrieben. 4. Lizenzieren Sie die Appliance. Lesen Sie die Anweisungen zur Lizenzierung von Appliances im *Security Analytics-Lizenzierungsleitfaden*, auf den Sie über die Security Analytics-Option **Hilfe** sowie auf sadocs.emc.com/de-de zugreifen können.

Last Modified: September 14 2016, 12:09PM

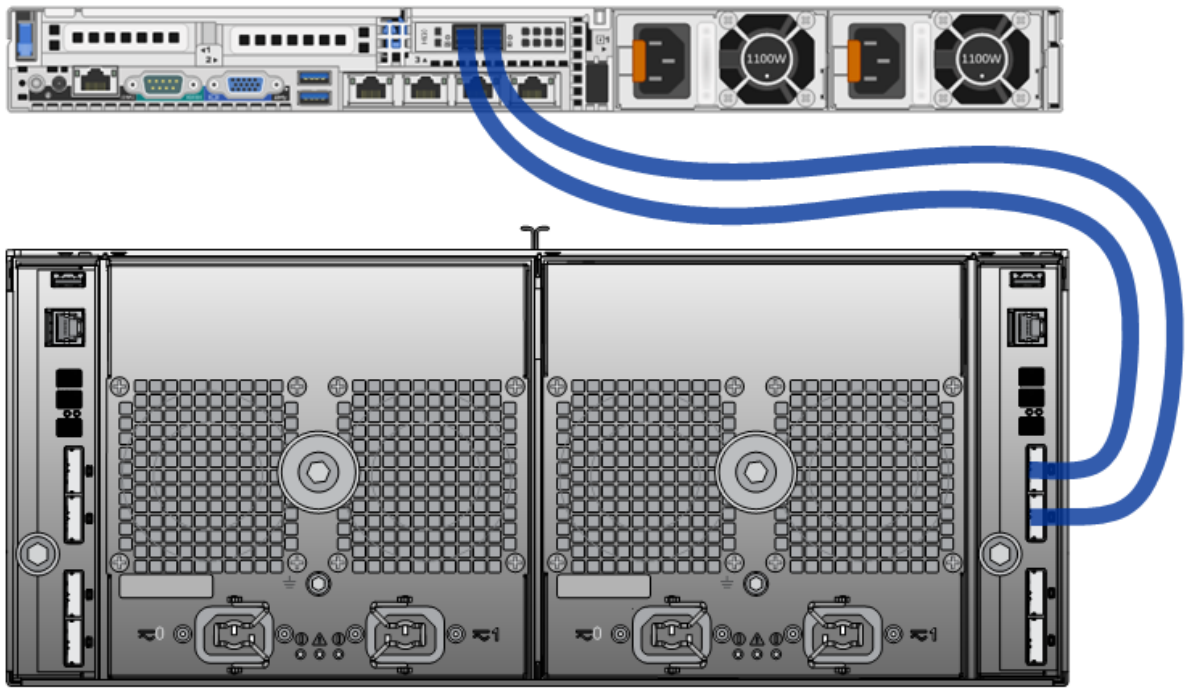
Verbinden eines DAC mit 60 Laufwerken mit einer Appliance

Die Verkabelungsanweisungen gelten für alle Serie 5 Decoder-, Log Decoder- und Archiver-Appliances.

Note: Das DAC mit 60 Laufwerken wird mit 4 SAS-Kabeln geleifert. Sie verwenden 2 davon, um das DAC mit 60 Laufwerken mit einer Appliance zu verbinden, wie in der folgenden Abbildung gezeigt. **Serie 4 und Serie 5 Appliances erfordern unterschiedliche Kabel.** Verwenden Sie die Kabel mit den Mini-SAS-Ports, um eine Verbindung zu einer Serie 5 Appliance herzustellen. Die anderen Kabel ermöglichen das Verbinden mit einer Serie 4 Appliance.

So verbinden Sie ein DAC mit 60 Laufwerken mit einer Appliance:

1. Schließen Sie die SAS-Kabel mit dem einen Ende an die Ports des RAID-Controller an der Rückseite der Security Analytics S5 Archiver-, Decoder- oder Log Decoder-Appliance an.
   Wenn das Skript die zusätzlichen Laufwerke nicht erkennt, müssen Sie evtl. den anderen Port auf dem Raid-Controller verwenden.
2. Schließen Sie das andere Ende der SAS-Kabel an die DAC-Einheit mit 60 Laufwerken an.
   Achten Sie beim Verbinden des DAC mit 60 Laufwerken mit dem RAID-Controller darauf, die Kabel an die **primären SAS-Ports** des DAC für 60 Laufwerke anzuschließen, wie in der folgenden Abbildung gezeigt.



Last Modified: September 14 2016, 12:09PM

Ausführen der DAC-Installationsskripte auf dem Decoder, Log Decoder oder Archiver

1. Melden Sie sich als `root` an und überprüfen Sie, ob das **rsa-sa-tools**-Paket installiert ist, indem Sie den folgenden Befehl ausführen:
   `rpm -qa | grep sa-tools`
   Wenn das Paket nicht installiert ist, wenden Sie sich an den RSA-Support, um eine Kopie der RPM zu erhalten und zu installieren.
2. Ändern Sie das Verzeichnis in das rsa-sa-tools-RPM-Basisverzeichnis:
   `cd /opt/rsa/saTools`
3. Führen Sie den folgenden Befehl aus:
   `nwraidutil.pl | more`
4. Überprüfen Sie die Ergebnisse, um sicherzugehen, dass sich keine fremden Konfigurationen und keine Laufwerke mit dem Status `Unconfigured(bad)` unter den DAC-Laufwerken befinden. Wenn eines dieser Probleme auftritt, beheben Sie es, bevor Sie das Skript ausführen.
5. Führen Sie das Skript **NwArrayConfig.py** mithilfe der folgenden Befehlszeichenfolge aus:
   `./NwArrayConfig.py`
   Das Skript erstellt alle erforderlichen virtuellen Laufwerke, logischen Volumes und die Verzeichnisstruktur und schreibt die Debug-Meldungen
   in die Datei **arrayCfg.log**.
6. Überprüfen der Ergebnisse:
   a. Vergewissern Sie sich, dass das Skript keine Fehler erzeugt hat, indem Sie die Datei **arrayCfg.log** überprüfen.
   b. Führen Sie den folgenden Befehl aus, um die neuen Größen der Datenbanken zu überprüfen:
      `df -Ph|awk '/(decoder|logdecoder|archiver|Filesystem)/ {printf("%-64s  %4s\n",$6,$2)}'`
      Im Folgenden sehen Sie ein Beispiel für die Ergebnisse, die angezeigt werden:

```
Mounted                                  Size
/var/netwitness/decoder                   10G
/var/netwitness/decoder/index             30G
/var/netwitness/decoder/metadb           6.6T
/var/netwitness/decoder/sessiondb        746G
/var/netwitness/decoder/packetdb          95T
/var/netwitness/decoder/sessiondb0       746G
/var/netwitness/decoder/metadb0          6.6T
/var/netwitness/decoder/packetdb0         95T
```

7. Nachdem die Ausführung des Skripts erfolgreich abgeschlossen wurde, fügen Sie die Appliance mithilfe von Security Analytics Administration hinzu und lizenzieren Sie den Decoder-, Log Decoder- oder Archiver-Service.

Neustarten des Services

Der Decoder-, Log Decoder- oder Archiver-Service muss von neu gestartet werden, damit der neue Speicherplatz erkannt werden kann.

1. Starten Sie den Service neu.
2. Vergewissern Sie sich anschließend, dass er wieder online ist und mit der Erfassung beginnt.

Last Modified: September 14 2016, 12:09PM