# Scanning database schemas

## Cloud Manager

Tom Onacki
September 16, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_scanning_databases.html on November 10, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

Scanning database schemas . . . 1
- Quick start . . . 1
- Reviewing prerequisites . . . 1
- Adding the database server . . . 2
- Enabling and disabling compliance scans on database schemas . . . 3
- Removing a database from Cloud Manager . . . 4

# Scanning database schemas

Complete a few steps to start scanning your database schemas with Cloud Compliance.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

**Review database prerequisites**

Ensure that your database is supported and that you have the information necessary to connect to the database.

**Deploy the Cloud Compliance instance**

Deploy Cloud Compliance in Cloud Manager if there isn't already an instance deployed.

**Add the database server**

Add the database server that you want to access.

**Select the schemas**

Select the schemas that you want to scan.

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

### Supported databases

Cloud Compliance can scan schemas from the following databases:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA

- SQL Server (MSSQL)

The statistics gathering feature **must be enabled** in the database.

### Database requirements

Any database with connectivity to the Cloud Compliance instance can be scanned, regardless of where it is hosted. You just need the following information to connect to the database:

- IP Address or host name
- Port
- Service name (only for accessing Oracle databases)
- Credentials that allow read access to the schemas

  When choosing a user name and password, it's important to choose one that has full read permissions to all the schemas and tables you want to scan. We recommend that you create a dedicated user for the Cloud Compliance system with all the required permissions.

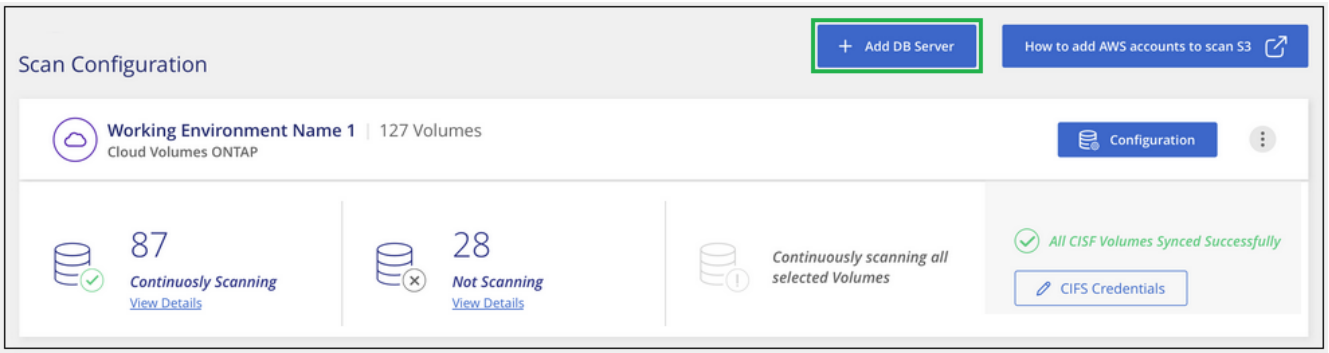
**Note:** For MongoDB, a read-only Admin role is required.

# Adding the database server

You must have deployed an instance of Cloud Compliance in Cloud Manager already.

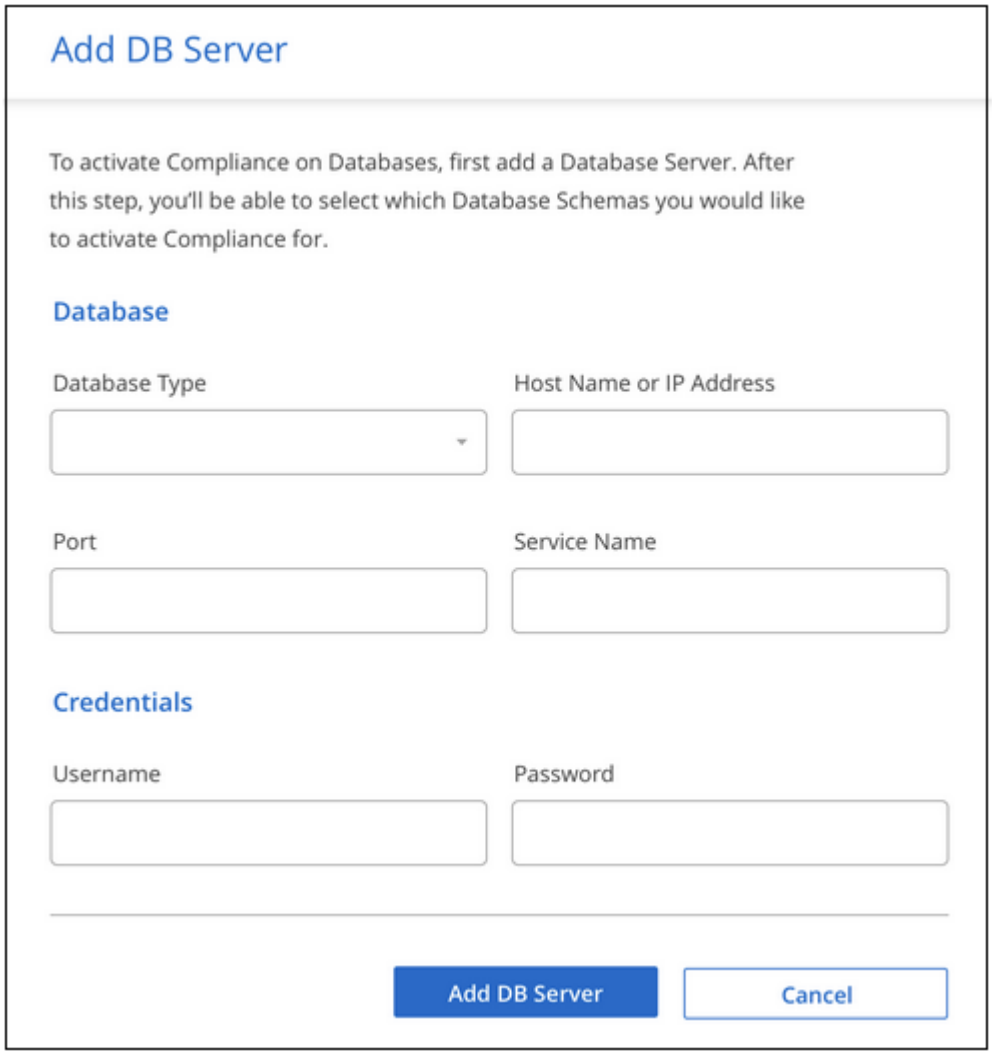
Add the database server where the schemas reside.

1. From the *Scan Configuration* page, click the **Add DB Server** button.




2. Enter the required information to identify the database server.
   a. Select the database type.
   b. Enter the port and the host name or IP address to connect to the database.
   c. For Oracle databases, enter the Service name.
   d. Enter the credentials so that Cloud Compliance can access the server.

e. Click **Add DB Server**.



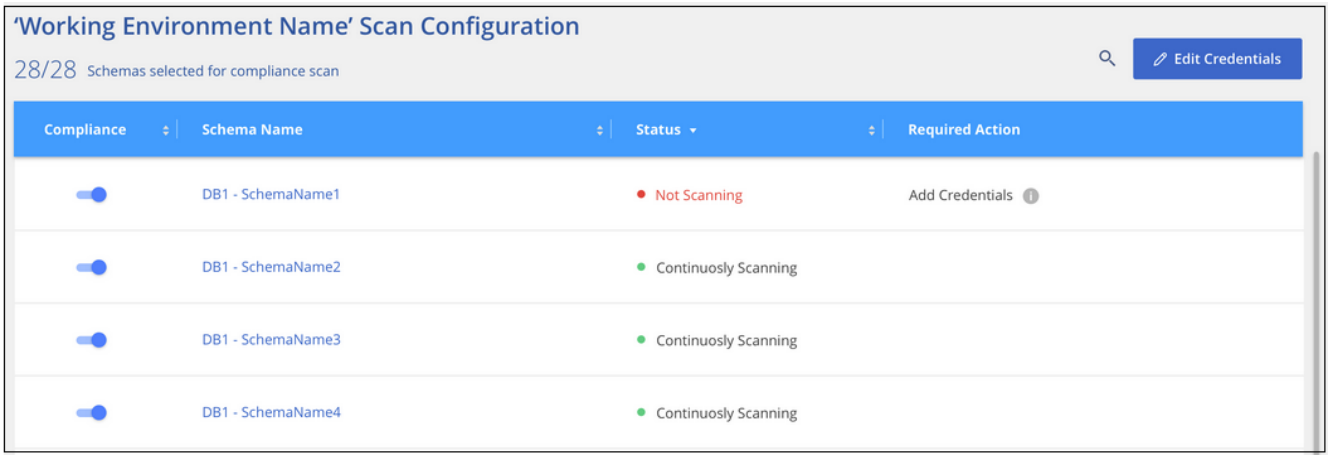

The database is added to the list of working directories.

# Enabling and disabling compliance scans on database schemas

You can stop or start scanning schemas at any time.

1. From the *Scan Configuration* page, click the **Configuration** button for the database you want to configure.

2. Select the schemas that you want to scan by moving the slider to the right.



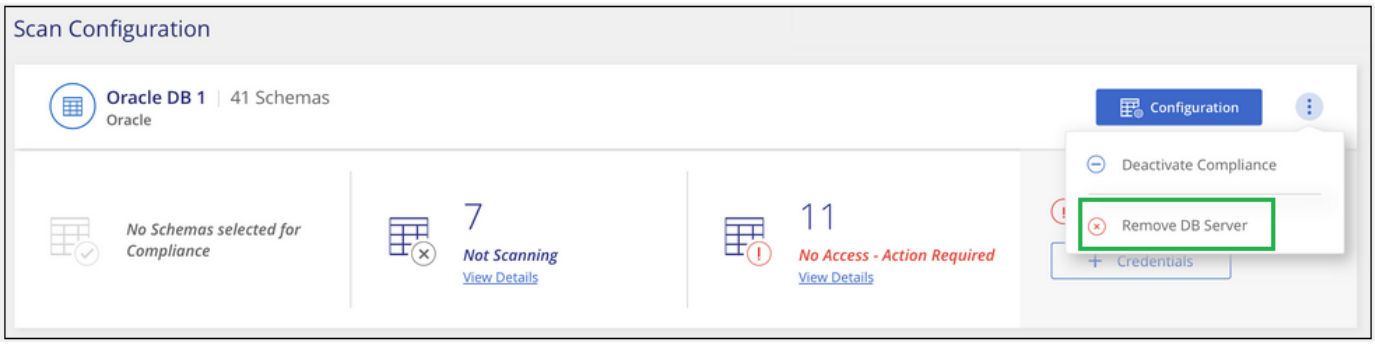

*Result*

Cloud Compliance starts scanning the database schemas that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

# Removing a database from Cloud Manager

If you no longer want to scan a certain database, you can delete it from the Cloud Manager interface and stop all scans.

From the *Scan Configuration* page, click the ⋮ button in the row for the database, and then click **Remove DB Server**.



**Copyright Information**

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

**Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.