# Mini-Spec for Secured Password for non-secured XDCR

*Amadeus*

**Creator(s):** David Maier
**Reviewers(s) :** Don Pinto, Perry Krug
**Creation Date:** Jan the 11th
**Update Date:** Jan the 18th
**Version:** 0.1
**Status:** Draft

Couchbase

# TOC

# Overview

Amadeus requested this security feature in the context of their Figaro project. The feature request is about securing the XDCR password on the wire when using non-secure XDCR.

Here some context:

- Couchbase already comes with a ‘secure XDCR’ option which means that the password for setting up the XDCR link from the source to the target can already be secured by using SSL encryption (via HTTPS)
- If using secure XDCR all data transfer from the source to the target is encrypted, too
- However, if using non-secure XDCR, the password is currently transferred in plain-text from the source to the target

Because Amadeus uses anyway a VPN connection between the source and the target cluster, they would like not to send the data itself encrypted again BUT their is the security policy that passwords must not be sent in clear text over the wire, even within the VPN. So this feature is about securing the password transfer if using non-secure XDCR.

The feature is needed for the Spock release. The request has highest priority because of the Go-Live plans of Figaro.

The purpose of this document is to get a common understanding and to exchange ideas how this security feature could be implemented.

# Requirements

This section helps to make sure that the customer requirements are aligned with our understanding of what's requested.

The following high level requirements or user stories are describing the feature best:

| ***Id*** | ***Subject*** | ***Comment*** |
|---|---|---|
| 0 | Password not in clear text for administrative XDCR access | In the context of XDCR, the admin password which is used for setting up the XDCR link should not be transferred in clear text from the source cluster to the target cluster and vice versa. |
| 1 | Password not in clear text for XDCR data access | When accessing the target bucket, then the bucket password should not be transferred in clear-text, too. |
| 2 | No data encryption | In this particular case, the data should not be encrypted in order to avoid any encryption overhead. |

Couchbase

# Implementation Plan

The implementation will consist two parts:

1. Use an HTTPS connection for connecting to ‘ns_server’ on the target cluster. XDCR needs to connect to the target ‘ns_server’ for a number of reasons:

- Validate the remote cluster reference
- Get the vBucket-Map of the target cluster in order to retrieve the target cluster’s topology information
- Perform frequent checkpointing

The connection to ‘ns_server’ will be HTTPS instead of HTTP. This means that part 1 requires the certificate for the target cluster. The current thinking, is to leverage ssl type remote cluster reference, which already has the certificate as a required parameter. As of now there are two types of remote cluster references:

- Secured XDCR: HTTPS and SSL for secure admin and data transfer
- Non-Secure XDCR: HTTP and plain TCP connection

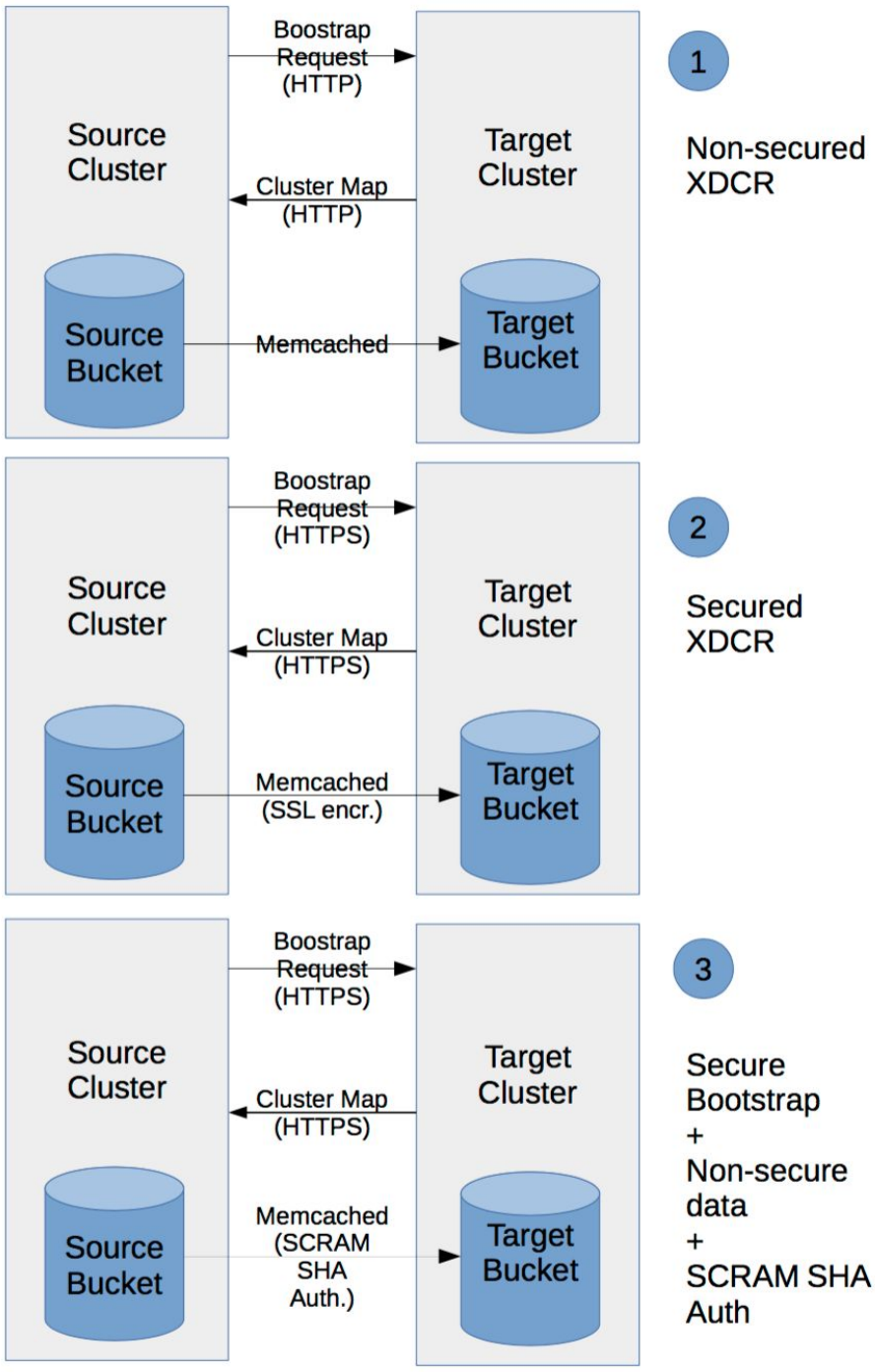
We could add a configurable parameter, e.g., a checkbox, to ssl type, hence making two subtypes of SSL:

- Default ssl type, which has the same behavior as before
- “Half” ssl type, where we adopt the fix for this feature request

2. Use SCRAM-SHA authentication to connect to the target ‘memcached’

- As for now non-secure XDCR uses plain authentication to connect to the ‘memcached’ service on the target cluster. The plan is tu use SCRAM-SHA authentication instead in order to hash the password.
- If the target ‘memcached’ supports it, then the strongest SCRAM-SHA mechanism will be used (in order: SCRAM-SHA512, SCRAM-SHA256, SCRAM-SHA1)
- If the target ‘memcached’ service does not support SRAM-SHA, hen XDCR will throw an authentication error

The following diagram describes the targeted scenario as mode #3:



## Summary

The feature is needed in order to fulfill one of Amadeus' security policies that passwords should not be transferred in clear text over the wire when using XDCR. The feature request will be addressed by securing the administrative communication via HTTPS and by making sure that the bucket access via XDCR is using a SCRAM-SHA based hashing for authentication purposes. The delivery is expected in the Spock release.

## References

- Jira: https://issues.couchbase.com/browse/MB-20750