DR Appliance

Contents

Overview

This document outlines the use and options of the PINsafe appliance. The PINsafe DR appliance acts as a MySQL slave against which authentications may be made. It is designed for use in Disaster Recovery sites where in standard operations there are no authentications, and when the DR site is invoked, will handle authentications.

Note: When an account is locked on the DR server, the account lock is not replicated back to the PINsafe Master appliances.

Prerequisites

PINsafe DR appliance version 2

Restoring Data from a DR server

Note: Ensure backups are taken before following these steps.

DR servers can act as a source of data if the PINsafe Master servers cannot be read. A MySQL dump can be made from the DR appliance and copied to the PINsafe Primary Master.

```
mysql
stop slave;
exit;
mysqldump --single-transaction --flush-logs pinsafe_rep > /tmp/master_dump.sql
```

The data can then be copied to the remaining PINsafe appliances, see MySQL Appliance Database Synchronisation

How to promote a DR to Synchronise with data sources in the event of a disaster

DR servers will authenticate users in the event of a disaster. If the disaster is prolonged perhaps with the permanent loss of the PINsafe Master servers, new users may be required to be added to the DR appliance. PINsafe DR servers in the event of a Disaster Recovery Scenario can be configured to read data sources to add users for authentication.

Note: This assumes that the PINsafe Master servers are no longer accessible and should only be carried out in a Disaster Recovery scenario. Ensure that a backup has been made of the DR appliance.

DR Preparation

Configuring the DR server with the required settings in advance will save time in a disaster scenario and ensure the data is known. The steps below for Data Repositories, Add Groups, Configure transports can be pre-configured and should match those of the Master appliances, incorrect data may result in PIN numbers being resent or users being deleted/added.

Set Mode to Synchronised

On the PINsafe DR appliance Administration Console select Mode/General then set the Mode to Synchronised then Apply. This should only be done when the DR is to be used to write data to the MySQL database. In standard DR operation it should be left in Slave Mode.

Add Data Repositories

On the PINsafe Administration console select Repository Server, then add the required repository. Synchronisation schedule should not be set unless data is to be imported as in a disaster scenario. A DR data source should be specified as the repository.

Add Groups

PINsafe groups can be created and should match those on the PINsafe Master servers.

Configure Transports

PINsafe Transports can be created and should match those on the PINsafe Master servers.

Post Disaster (Returning back to standard DR)

When the main site is back in operation, the MySQL database replication would need to be established again, with the Master PINsafe servers. If the data on the DR site is to be used, it would need to be copied to the PINsafe Primary Master server. The changes to make a DR would need to be reversed so that it once again runs in slave mode.

If the DR site is to become the main site, then Primary/Standby Masters servers should be deployed.

Testing

Known Issues

Troubleshooting