Protection of User and Configuration Data on PS Series

Dell Engineering
October 2015

A Dell Technical White Paper

Revisions

Date	Description
October 2015	Initial release

Table of contents

1   Executive summary

Storage area networks store information critical to the success of many organizations. These systems contain information required to permit users to administer them as well as configuration information, both of which must be protected. This document outlines the storage of these types of information on the PS Series storage products from Dell.

2   Passwords

In order to administer the PS Series SAN, the user must log in to the PS Series Group. The Group may use an external source for usernames and passwords, such as RADIUS or Active Directory, but there is always at least one local user, grpadmin, that is the master administrator account. In order to assure that the grpadmin account password is secure, passwords are protected in standard UNIX fashion by a one way hash. As a result, disclosure of the stored password is not a concern provided that the user used a strong password. The hashed password is stored along with all the other system configuration parameters.

3   System Configuration Data

System configuration data is key to ensuring that the members of a PS Series Group are able to communicate with both each other and with the hosts supporting the applications. The system configuration parameters are stored in the Management Database, which is an internal data structure. It is stored on the storage maintained by the array, similar to any user-visible volume, but this internal volume is not accessible from the outside. All arrays have a copy of this database, and any changes are immediately replicated to all group members. The redundancy provided by the array RAID protects this configuration data exactly as it protects user data.

4   Replication of System Configuration Data within the Group

In order for all Members in a PS Series Group to have a copy of the system configuration data, the Management Database is replicated when changes are made to it. This replication uses the array Inter-Process Communication (IPC) mechanism, using a PS Series proprietary protocol. If IPSec is enabled in the Group, the IPC traffic is protected automatically by IPSec.

A special password, the group membership password, is used to allow additional PS Series arrays to join an existing group. The group membership password is stored in the Management Database with the configuration data, but unlike user passwords it not hashed for technical reasons. This password is not an administrative account password and cannot provide access to configuration data. The group membership password can be changed by an administrator and should be different than the grpadmin password. If it is changed, that change will result in a management database replication of that data, protected by IPSec if enabled as discussed above.

5 Changing System Configuration Data

Permission to change configuration data is tied to administrator accounts. There are several levels of accounts, including group, pool and volume administrators as well as a read-only role. Depending on the assigned role of the user account, a given admin may have authority to change all configuration settings, some, or none.

6 Monitoring the PS Series Group via SNMP

The PS Series group is optionally monitored using SNMP by SAN HeadQuarters (SAN HQ), a powerful monitoring tool dedicated to PS Series management. SNMP, if enabled, offers read-only access to the configuration data and any password data is omitted from the SNMP visible tables.

7 Monitoring the PS Series Group via SupportAssist

SupportAssist is a tool that periodically sends health and configuration data to Dell Support. While SupportAssist can see configuration data, all passwords are one-way hashed before they are sent to Dell. This means that any Dell support help based on this information is limited to "the passwords don't match" but not "your password is 'xyz'".

8 SED Unlock Keys

Some PS Series arrays contain Self Encrypting Drive (SED) technology. When SED drives are present, the PS Series array generates and maintains the keys required to unlock the drives. Without these keys, SED drives cannot be unlocked and the data on them cannot be accessed. These keys are handled separately from the rest of the system configuration data; SED unlock keys are NOT part of the configuration database. These are stored in a secure data spreading mechanism as described in the product documentation and the technical report *EqualLogic PS Series Architecture: Self Encrypting Drive Management with PS Series Arrays,* found on Dell Tech Center.

.

A   Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- *[EqualLogic PS Series Architecture: Self Encrypting Drive Management with PS Series Arrays](#)*

Many other PS Series papers are found on the Dell Tech Center EqualLogic Technical Content page at http://en.community.dell.com/techcenter/storage/w/wiki/2660.equallogic-technical-content.

Product documentation is available to customers with a Support Site login at:

https://eqlsupport.dell.com/secure/login.aspx