Reduxio Tech Note

StorSense Security

For more information, refer to Reduxio website at http://www.reduxio.com.
If you have comments about this documentation, submit your feedback to docs@reduxio.com.

Revisions:	Descriptions
June 5, 2016	Initial version.
June 20, 2016	Minor updates.

Reduxio Systems, Inc.
111 Pine Avenue
South San Francisco, CA, 94080
United States
www.reduxio.com

Contents

Overview

StorSense is a software-as-a-service (SaaS) support infrastructure for collecting and analyzing data reported from Reduxio systems. Once enabled, the StorSense agent running on the system will autonomously send configuration, alerts and statistics information to the Reduxio StorSense Cloud.

StorSense secures customer information using various security mechanisms. This tech note describes the information sent by StorSense, and how it is secured during transport to Reduxio and at-rest.

StorSense Components

The StorSense solution consists of the following components:

StorSense Agent	A built-in service running on each Reduxio system which communicates over a secured tunnel with the StorSense Cloud Service.
StorSense Cloud Service	A cloud service that monitors the Reduxio installed base and provides automated analysis and resolution of customer issues.
StorSense Remote Access	Optional remote access for Reduxio Support engineers using a customer-approved SSL tunnel.

Customer Benefits

StorSense provides an immediate value to storage customers:

- **Cloud-based** - no need to install agents or a separate management software.
- **Automated** - automatically predicts and detects customer issues.
- **No customer involvement** - no more "send me diagnostics".
- **Remote support** - allows faster identification and resolving of issues.
- **Long term statistics** – enables trend analysis.

Data Collection

The StorSense Agent running in the Reduxio system collects the following information:

System configuration	Hosts and volumes configuration, system settings.
System logs	Various system logs.
Performance statistics	System-wide and per-volume performance statistics.

Customer data itself is not collected in any way by the agent. Customer passwords are not collected or sent in any form..

Designed for Security

StorSense was designed from the ground up as a highly secure service, making no compromise on customer information of any kind.

Security Considerations

The following aspects were taken into consideration:

- **Authorization** – only authorized systems can communicate with StorSense.
- **Authentication** – systems must authenticate with StorSense prior to transfer of any information.
- **Risk isolation** – security risk should be isolated to a single system, i.e. a security break in a specific system should not affect any other system.
- **Complements existing security practices** – existing network security practices and policies do not change as a result of implementing StorSense.
- **Customer controls access** - Remote access from Reduxio support staff has to be enabled by the customer and is time limited to two hours. Customer can close this tunnel at any point.

Secure Transport

When StorSense is enabled, the system regularly communicates over the management ports with the Internet-based StorSense Cloud service. The communication is secured in various ways:

Strong Signing	The collected data is signed using a 1024-bit RSA private key. Generally speaking, 1024-bit keys are considered by the industry as highly secure, and unlikely to be compromised.
Unique Keys	Each system is configured during manufacturing with its own private key. This increases the level of authenticity of the communication of systems with the Reduxio Cloud Service, since even if a single key was ever to be compromised for a single system, no other system will be affected.
Secure Transport	The StorSense Agent communicates with the StorSense Cloud Service using a secure, encrypted HTTPS connection. This prevent eavesdropping confidential customer information over-the-wire.
No Firewall Changes	The StorSense communication only requires outbound ssh and https (TCP ports 22 and 443). This type of traffic is already allowed in most enterprise networks.

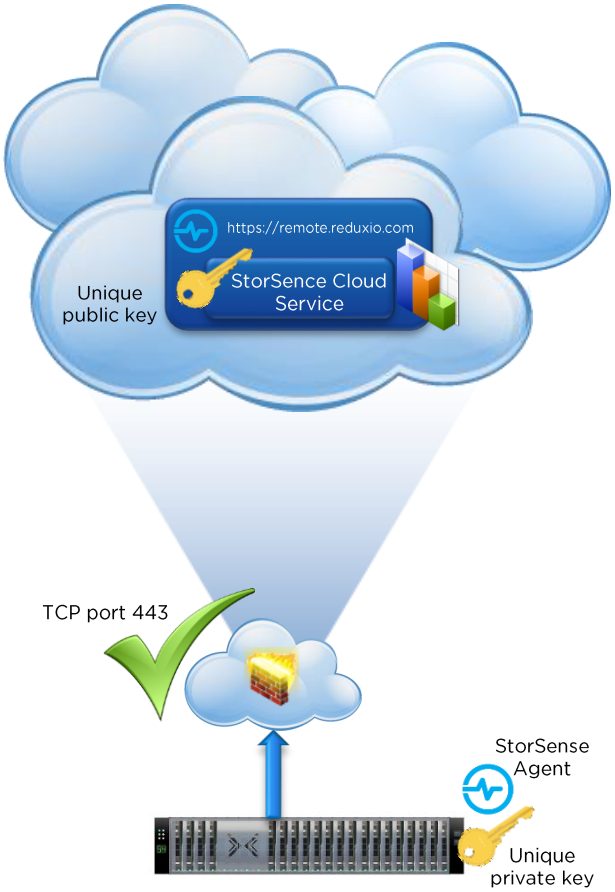

Figure 1. StorSense Architecture

Remote Access

StorSense also provides a capability that enables Reduxio Support to remotely connect to the system for advanced troubleshooting. This capability requires specific customer authorization and is time limited.

Requirements

The StorSense Agent communicates over secure transports with the StorSense Cloud Service. The StorSense communication requires outbound ssh and https (TCP ports 22 and 443) from the management ports/IPs to the StorSense cloud URL (https://remote.reduxio.com).

Table 1 lists the required TCP ports for this communication.

Table 1 - Open IP Ports

Service	TCP/IP Port	Direction
SSH (command-line management)	tcp/22	Inbound, Outbound
StorSense	tcp/443	Outbound

Conclusion

StorSense is a cloud-based support technology that provides highly secured transport from the Reduxio systems to the Reduxio Cloud Service. As a result, customers can benefit from automated support, reduced support overhead, all while their data, systems and network infrastructure are all kept highly secure.

References

Reduxio Documentation

- *Reduxio Administration Guide*