Quantum

White Paper

Quantum StorageCare Guardian

April 2013

Quantum
BE CERTAIN

Notice

This White Paper contains proprietary information protected by copyright. Information in this White Paper is subject to change without notice and does not represent a commitment on the part of Quantum. Quantum assumes no liability for any inaccuracies that may be contained in this White Paper.

Quantum makes no commitment to update or keep current the information in this White Paper, and reserves the right to make changes to or discontinue this White Paper and/or products without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Quantum.

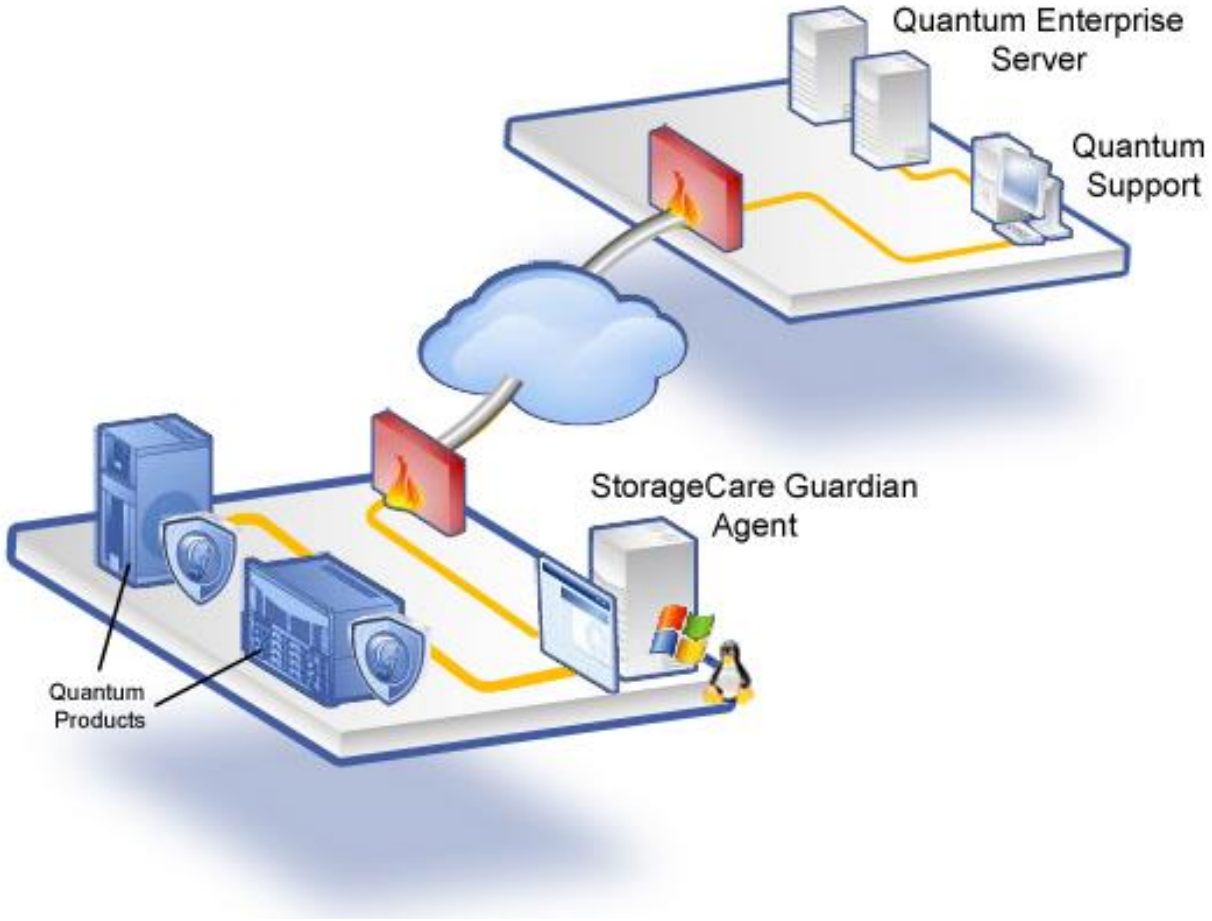
Contents

Introduction

This document describes the functions and operation of Quantum's StorageCare Guardian with the intention of explaining how StorageCare Guardian will operate within a datacenter. This document also addresses key questions such as a communication through firewalls, security, and other technical needs to achieve remote support.

StorageCare Guardian Overview

StorageCare Guardian is agent software linking Quantum products back to Quantum support enabling remote service and administration. StorageCare Guardian employs web-architected interfaces for remote device administration, desktop sharing, diagnostics and data visualization, giving Quantum support personnel web-based information access from anywhere in the world. The StorageCare Guardian agent software monitors devices locally and manages Internet communications with the Quantum Enterprise server allowing communications and control.



Technology Overview

The StorageCare Guardian system is comprised of two major components: the StorageCare Guardian agent software running on either a Windows, Solaris, or Linux server at the customer site, and the Quantum Enterprise server applications that provide access to the information provided by the agents.

The StorageCare Guardian agent software at the customer site communicates with the Quantum devices at the customer site on a regular basis, checking the status of key data elements that provide a picture of the health of the devices. Additionally, the agent periodically communicates with the Quantum Enterprise server environment to update device status. The Enterprise server can also run a suite of applications allowing for:

- Viewing real-time device status
- Viewing system configuration
- Gathering diagnostic data (event logs, error logs)
- Connecting directly to the web management and/or telnet management interface of the device upon customer approval

StorageCare Guardian Agent

Key Security Features

StorageCare Guardian was designed to be completely secure, providing best-in-class support capability with no changes required to your existing network or security infrastructure. The following sections provide more detail on the following topics relating to information security:

- Network Security
- Data Security
- Access Control
- Best-in-Class Security
- Quantum Enterprise Server Security

Network Security

StorageCare Guardian leverages your existing network and security infrastructure. No changes are required in order for the StorageCare Guardian agent software to work. As long as the server designated to act as the Guardian agent can communicate with the Quantum devices and open an outbound connection to the Internet, StorageCare Guardian will provide the security necessary to protect your information assets.

The StorageCare Guardian agent server does not require a visible TCP/IP address. This is because Quantum will never initiate a connection to the StorageCare Guardian agent server at your site. The StorageCare Guardian agent initiates all communications with the Quantum back-end servers. The Guardian agent communicates with a single Quantum Enterprise server and two-way communication will only occur after the connection has been initiated.

Communications on the local area LAN use TCP port 80 or 443, depending on the settings of the Quantum device. Port 80 will be used by default, and if the device has SSL enabled, port 443 will be used. ALL communications between the agent and the Quantum Enterprise server are sent via secure HTTPS (port 443) and use 128-bit SSL encryption. In addition, trusted digital certificates (obtained through VeriSign)

protect both ends of the connection from unauthorized access. Messages sent from the agent to the Enterprise server are XML via HTTPS, while responses from the Quantum Enterprise server are SOAP (Simple Object Access Protocol) via HTTPS.

The StorageCare Guardian agent sends only changes to the Quantum Enterprise server. This minimizes the actual traffic between the customer site and Quantum. Once every 5 minutes, StorageCare Guardian connects to the Quantum device(s) via the web management interface and collects a snapshot of information. The new snapshot is compared to the previous and any changes are sent as updates to the Quantum Enterprise server.

On a separate schedule, once each minute, the agent also sends a small message to Quantum as a form of "heartbeat" to show the agent is active. These messages enable Quantum support personnel to queue a request to the agent software for up-to-date information, for instance an error log or event log. The next time the agent "checks in," the request is delivered, and depending on the Policy Manager settings for the agent, will either be granted or denied at the agent level. Policy Manager will be discussed in detail in the Access Control section of this document.

Data Security

One of the most common concerns customers raise regarding StorageCare Guardian is the security of the data stored on the Quantum device. StorageCare Guardian does not impact the backup process, data, or other IT processes in any way.

A key design element of StorageCare Guardian is that only the web management interface of the Quantum device is used to collect the device data. There is no in-band (i.e. SCSI, Fibre Channel or iSCSI) communication from the StorageCare Guardian agent software to the Quantum device.

This method has several key benefits in terms of data security – assuring customers StorageCare Guardian will never conflict with backup software in any way and not provide access to the data stored on the Quantum device. The StorageCare Guardian agent prohibits any actions that would enable customer data to be read or overwritten. By default, only programmatic (pre-scripted, software-controlled) access is possible to the device; no human access is available to Quantum support personnel without direct customer intervention protecting storage assets (i.e. Quantum cannot reboot or take devices off-line without your approval). Information needed by Quantum support personnel to determine device health is available within the Quantum side StorageCare back-end applications. These applications show a representation of the device, and allow support personnel to view status and configuration, review log files, etc. without the need to actually connect "live" to the device. Should the need arise for Quantum support personnel to gain real-time access to the device, the customer can, at their discretion, enable access by support personnel to the web and/or telnet management interfaces of the Quantum device. Access can be turned off as easily as it was enabled.

Information Collected

The StorageCare Guardian agent collects a predefined set of data elements for each device. Only information relating to the status and configuration of the device is transferred from the agent to Quantum. For instance, although the agent software must know the TCP/IP address for each of the Quantum device(s) in order to communicate with them, these addresses are not transferred to Quantum. Static information such as the configuration of the device, firmware revisions, log files etc. are collected weekly or on-demand.

Access Control

One of the key elements to guarding the security of your data is the Policy Manager function of StorageCare Guardian agent. While the Enterprise Server applications determine what is possible, the Policy Manager on your agent determines what will be allowed. By default, the Policy Manager is packaged as an integral part of the StorageCare Guardian agent, and is accessed via the Agent Configuration Utility. This utility

runs during the StorageCare Guardian software installation, when you add your Quantum devices into the agent configuration.

Policy Manager is one of the pages of the utility and accessed by clicking on the "Policy Manager" heading on the left side of the utility interface. Policy Manager focuses on ease of use and fits the needs of most Quantum customers. Policy Manager sets access permissions for a single agent. In the case of multiple agents at a customer site, for instance if the company has multiple sites around the world, an agent is typically installed at each site. By default, each agent has its own Policy Manager settings, and changes made to that agent's Policy Manager affect all devices monitored by that agent.

Policy Manager by default allows the access option "Diagnostic Data Collection" only. This is the programmatic (software controlled) collection of data from the Quantum device, but does not allow any access that could impact the operation of the device. Default settings allow a Quantum support personnel to log into the Guardian Console and view the device "dashboard" for the Quantum devices configured in that StorageCare Guardian agent instance showing the current status of the device, all Guardian generated alarms for the device, snapshots of the device configuration, access to event logs, error logs, and drive logs (product-dependent). None of these actions requires logging into the web or telnet management interface of the device; this is done purely through device dashboard in the StorageCare Guardian software. With customer permission Quantum support personnel may be granted access to the web or telnet management interface of the device. This is quickly enabled or disabled in the Agent Configuration Utility in Policy Manager. Changes take place immediately upon pressing "Deploy Changes to Agent". In addition to access control policies, there are number of other customer customizable policies with the exception of diagnostic data collection.

Best in Class Security

StorageCare Guardian utilizes an enterprise class technology originally developed in the medical devices field, helping the manufacturers of DNA sequencers, hospital prescription dispensing stations and many other medical devices to remotely communicate with and support their products in hospitals and university research labs. This same powerful, flexible technology is the basis of Quantum's StorageCare Guardian Solution. Since the technology used here has a strong heritage in the medical device industry, it has provided for best-in-class security features. For example, audit entries of all actions taken by users of the system with each entry showing the date, time, user, and device are recorded. The underlying secure transport technology used by StorageCare Guardian has been tested and validated repeatedly by industry-leading security firms such as @Stake (now part of Symantec Corporation) and VeriSign. Quantum is also VeriSign Security Certified™. StorageCare Guardian has undergone an extensive application security assessment by VeriSign Corporation based on open industry standards.

VeriSign Security Certification gives Quantum customers added assurance that information security best practices are being utilized when diagnostic data is transferred between installed systems and Quantum's Enterprise server. The certification document is available to Quantum customers on request.

Quantum Enterprise Server Security

The same emphasis on security used in developing the StorageCare Guardian agent is also evident in the design of the back-end application infrastructure that resides at Quantum. While the StorageCare Guardian console allows Quantum to provide better levels of service to our customers than ever before, it is important that these applications and the data they access is kept secure from unauthorized access.

One critical element of the security of StorageCare Guardian's Enterprise systems is the design of the network. StorageCare Guardian is a three-tier application, with one tier residing on the StorageCare Guardian agent at the customer site, a second tier on a web server on a protected DMZ, and a third tier (application and database servers) behind a second firewall. The use of two levels of firewall protection ensures that no unauthorized access to Quantum's StorageCare Guardian servers is possible.