

Reqo Maestro for ePO™ Enterprise Edition

December 14, 2003

Abstract

This white paper focuses on the architecture and features of Maestro for ePO™ Enterprise Edition and describes its terminology, concepts, design goals, and key components.

Contents

Introduction	3
Components	3
Maestro Data Warehouse.....	4
Maestro Web Application.....	6
Data Retention	7
Summary	8

Disclaimer

The information contained in this document represents the current view of Reqa Inc. on the issues discussed as of the date of publication. Because Reqa must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Reqa, and Reqa cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. REQA MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Reqa Inc.

Reqa may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document except as expressly provided in any written license agreement from Reqa, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Introduction

Reqo Maestro for ePO™ Enterprise Edition provides the following principal features beyond Maestro for ePO™ (Maestro) standard edition:

- Universal access to data on multiple ePO servers
- Minimization of data retrieval load from the ePO Production databases
- Improved data retrieval performance
- Increased reporting scalability
- Automated events retention policy for ePO source databases
- Automated events archival in Maestro data warehouse database

Maestro for ePO™ Enterprise Edition is installed on a dedicated server where it stores data which is retrieved periodically from a defined list of McAfee® ePolicy Orchestrator (ePO) databases throughout the enterprise.

Components

Maestro for ePO™ Enterprise data warehouse resides in a Microsoft® SQL Server 2000 database. The following are key components of the Maestro for ePO™ Enterprise Edition implementation:

- **ePO source databases** – a defined list of production ePO databases whose data will be aggregated into the Maestro Data Warehouse database.
- **Maestro Data Warehouse database** – central repository for all reporting data pulled from the defined list of ePO databases.
- **Maestro application database** – stores all Maestro for ePO™ related application data (i.e. usernames, queries, report settings, cache data, etc.).
- **Maestro data warehouse service** – is a Windows local service that runs on Maestro Data Warehouse SQL Server that pulls data from ePO source databases as per a defined schedule.
- **Maestro cache service** – is a Windows service responsible for reading data from the Maestro Data Warehouse database and caching report specific data in to the Maestro application database.
- **Maestro alerting service** – is a Windows service responsible for reading data from the Maestro Data Warehouse database, comparing event frequency against defined threshold alerting metrics, and sending alert notifications via email enabled mobile devices.
- **Maestro web application** – is a Web application that produces reports on the data in the Maestro application and Maestro Data Warehouse databases. This web based system allows for easy access to the critical data and reports to users throughout the enterprise network.

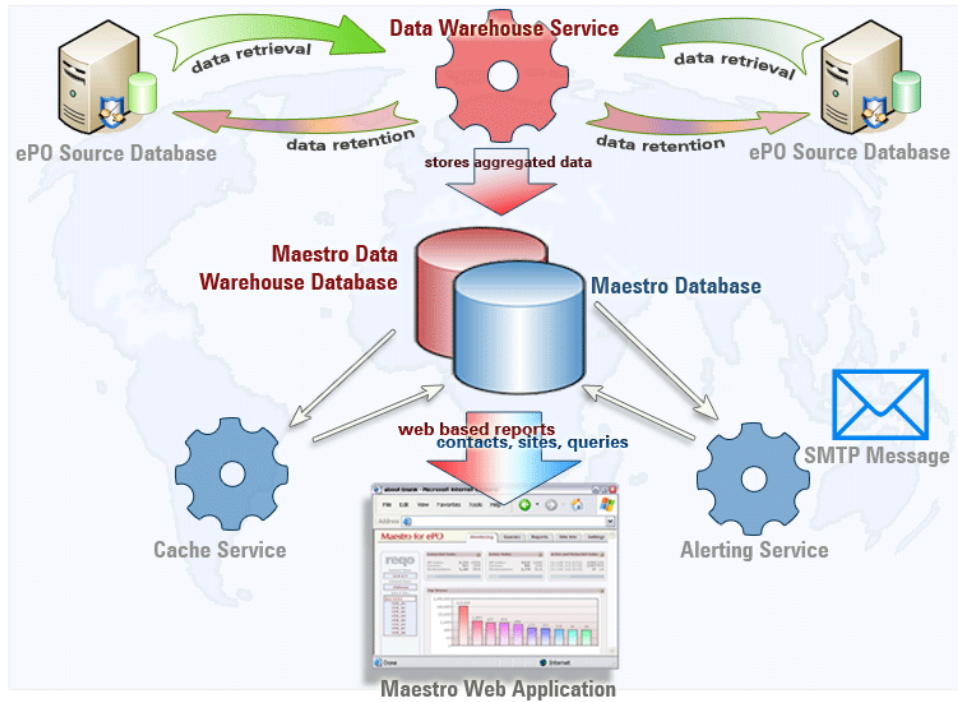


Figure 1 Components Integration Diagram

Maestro Data Warehouse

The Maestro Data Warehouse database contains the following SQL tables each with a defined data retrieval method as outlined below in Figure 2.

SQL Table Name	Data Retrieval Method
ActionDesc	Dump
BranchNode	Delta
ComputerProperties	Delta
DFW80_BlockedApps	Incremental
DFW80_IDSEvents	Incremental
Events	Incremental
IPSubnetMask	Delta
LeafNode	Delta
ProductProperties	Delta
ReportActionDesc	Dump
ServerInfo	Delta
Software	Delta
VirusType	Dump

Figure 2

The following data retrieval methods are used:

- **Delta** – this method of pulling data will scan every row in the ePO source database tables and compare with the stored timestamp in the Maestro Data Warehouse database. If the timestamp does not match, the corresponding data row will be updated in the Maestro Data Warehouse database.
- **Incremental** – this method of data retrieval keeps track of the last stored record and subsequently copies only newly inserted rows.
- **Dump** – this method of extracting data will overwrite the whole table in Maestro Data Warehouse database with the data from the ePO Source tables. This is used for reference tables that do not have a unique stable identifier.

Due to the fact that the majority of data is being pulled from the events table, approximately 95% of all retrieval traffic will be incremental and therefore will cause minimal utilization on the source ePO database servers and enterprise wide area network resources.

During data retrieval from the ePO source databases, all key fields are prepended by a three digit server identifier number used to reference the data source (ePO Server) within the Maestro web application.

The data warehouse service is able to support all ePO servers running versions 2.0 and higher. The number of source ePO databases are limited only by the hardware specifications of the Maestro Data Warehouse SQL server.

Scheduling of data retrieval from the defined ePO source databases can be custom defined per each source server in order to address early attack detection.

However, the default data retrieval schedule should work well in most current enterprise environments assuming that ePO databases are located in major network hubs throughout the enterprise.

The default data retrieval schedule is as follows:

- Events data pulled every five (5) minutes
- All other data pulled every fifteen (15) minutes

Below is the table of results with time statistics for a sample setup with three servers:

	ComputerProperties (Delta)	Events (Incremental)
ePO Source Databse 1	3,633	206,621
ePO Source Databse 2	806	3,549,214
ePO Source Databse 3	21,811	4,052,773
Total (rows)	26,250	7,808,608
Total Initial one-time insert (h:m:s)	0:00:05	1:12:51
Total Incremental refresh (insert, update, delete) (h:m:s)	0:03:41	0:02:42

In order for the Maestro data warehouse service to be able to read data from ePO source databases, linked servers will need to be configured on the Maestro Data Warehouse SQL server. Figure 3 depicts the linked servers in the SQL server.

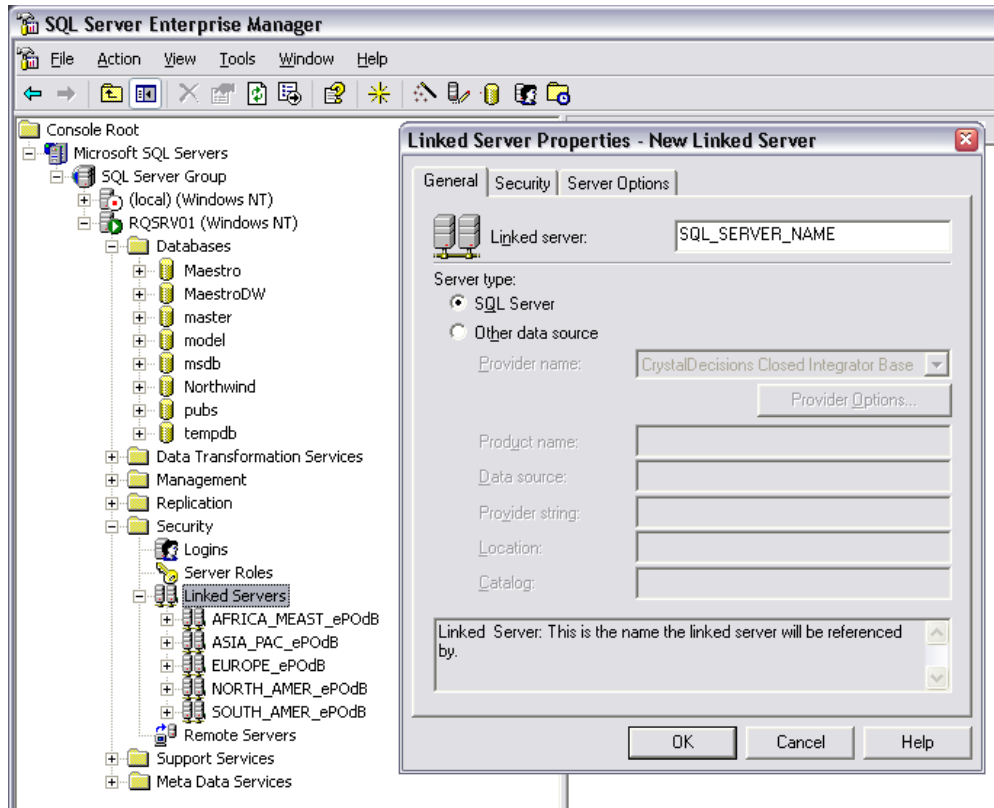


Figure 3

Maestro Web Application

The Maestro web application will only interact with the Maestro application and Maestro Data Warehouse databases. This architectural design allows a complete offload of data retrieval and caching utilization from the production ePO server.

In addition, Maestro Data Warehouse database contains multiple indexes that are optimized for the Maestro web application and therefore significantly improve reporting performance.

To enable a user to report on the enterprise environment as well as on a hierarchical level of any ePO server directory, the Maestro web application interface contains a hierarchical navigational tree as shown in Figure 4.

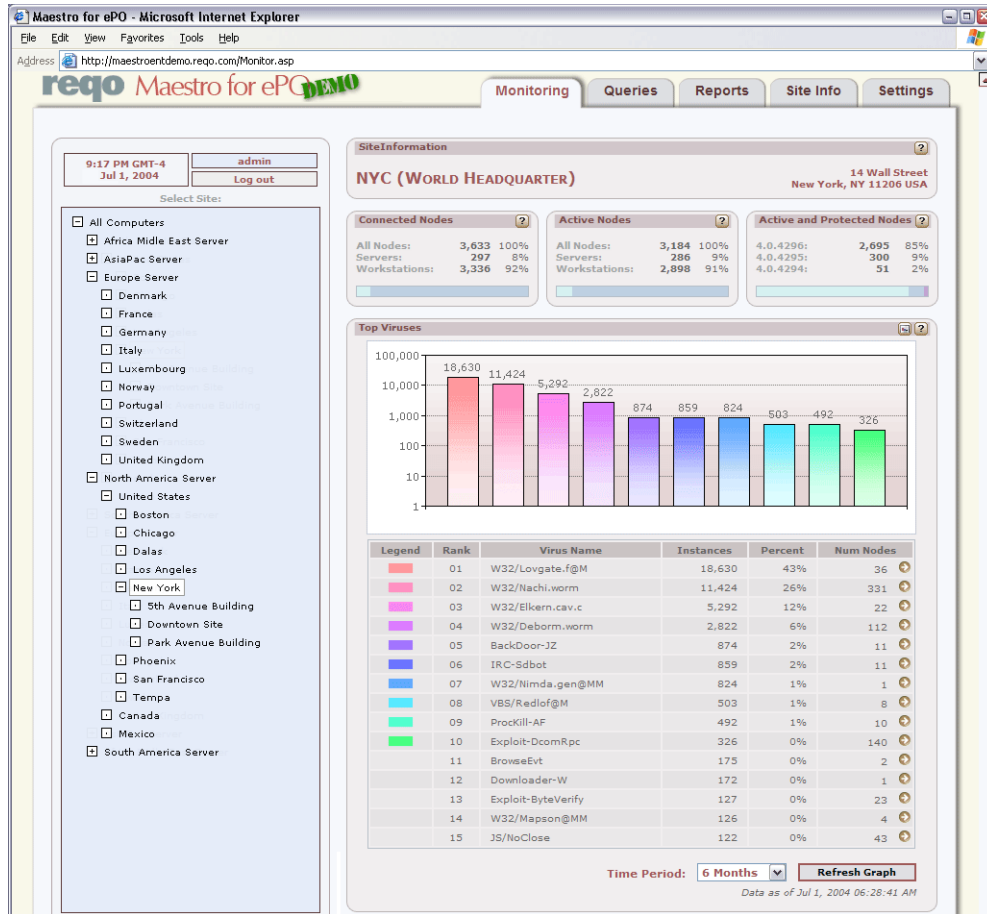


Figure 4

Data Retention

Because data is pulled from the ePO source servers to the central Maestro Data Warehouse database, it is no longer necessary to keep a large amount of historical data on each ePO source server. For this reason Maestro for ePO™ Enterprise Edition includes an automated data retention policy enforcement feature for ePO source databases. Data retention policy is completely customizable per ePO source server.

Default data retention policy for ePO source databases:

- Delete all virus events older than 30 days
- Delete all non-virus events older than 7 days
- Delete all orphaned events
- Delete events with specific TVD ID's

Default data retention policy for Maestro Data Warehouse database:

- Delete all virus events older than 12 months
- Delete all non-virus events older than 6 months
- Delete all orphaned events older than 6 months
- Delete events with specific TVD ID's older than 7 days

Due to the customizable data retention settings in Maestro Data Warehouse database, archival of older ePO data is an intrinsic feature Maestro for ePO™ Enterprise Edition.

Summary

Maestro for ePO™ Enterprise Edition was designed primarily for large global enterprise environments that will significantly benefit from the ability to monitor their entire security environment from a centralized location.

Rego Expert Services approaches each custom implementation project in a comprehensive and detailed manner. Our engineering team evaluates an enterprise environment from top to bottom including WAN topology, ePO infrastructure, hardware specifications, database optimization, and application integration..