



CASE STUDY

eSCOP Road to IT Security & Regulator Compliance

Social Services Agency Santa Clara County, California

The Social Services Agency (SSA) of Santa Clara County must respond to Federal and regional security and regulatory compliance requirements as part of its mandate to manage a wide variety of computing systems and very sensitive data. Collecting, auditing and reporting related IT events is a mission critical objective.

In the heart of Silicon Valley, the SSA had many technological choices but selected the security and platform expertise of Enterprise Certified Corporation (ECC). ECC professional services applied its eSCOP™ platform with the Microsoft System Center Operations Manager 2007's Audit Collection Services (ACS) to address extremely sensitive security requirements. In addition, with the enhanced features of eSCOP in support of Operations Manager 2007's Data Warehouse, ECC provides robust reporting, archiving and administrative functionality to manage system health and application event data.

Microsoft's System Center Operations Manager 2007 affords end-to-end system and security event monitoring. The new Enterprise Certified Corporation eSCOP™ application seamlessly integrates Operations Manager 2007 as an extensible and intuitive administrative console for the Audit Collection Services (ACS) and Data Warehouse databases. ECC eSCOP™ is designed to report, filter and archive extremely large, enterprise-wide data repositories at unmatched speeds.

SAA Enterprise Requirements and Challenges

The Social Services Agency mission requires the gathering and maintenance of extremely sensitive personal and institution data. SSA's organizational objectives include: (1) prevent child abuse, neglect and exploitation; (2) maintain and restore kinship relationships while nurturing the care of children and the elder; (3) maintain safe, healthy and productive lifestyles in a manner that respects personal liberty; and (4) assist residents in obtaining challenging, satisfying and economically rewarding employment.

On any given day, the SAA will generate over a gigabyte of IT security related events. For audit purposes, they maintain terabytes of related data. The SAA has taken a very proactive position in the protection of this private data. The ability to monitor and report on enterprise security and system health activity is a major focus.

Solution

The SAA selected Microsoft's System Center Operations Manager 2007 as a cornerstone of their security and system environment monitoring. In order to further enhance the County's ability to manage, report, and archive the very large data reservoirs, SAA employed ECC's professional services and its eSCOP platform.

Utilizing the event collection capability of System Center Operations Manager 2007, data is pulled from the target systems into one of two databases: (1) security events are sent to the Audit Collection Services database; and (2) system and application information is delivered to the Data Warehouse database. In turn, eSCOP parses the information into logical categorizations that map to regulatory compliance requirements and industry best practices. The SAA team is able to use the eSCOP advanced filtering functions to rapidly review the precise desired information and to create a wide variety of local and SQL Server based reports. This structure is also designed to provide immediate and rapid access to the most recent IT events while also supporting long term historic event analysis. In order to manage the large volumes of information, data partitions are created daily and retained as active or inactive at the discretion of the authorized system administrator. As "retired" historic data is required, eSCOP permits the retrieval of inactive database partitions and provides the same administrative, filtering and reporting functionality as is available for active database streams.

"The challenges associated with managing and insuring the secure integrity of over a gigabyte of IT event information on a daily basis can be daunting. We are charged with the responsibility for maintaining very sensitive information and we must be able to monitor, report, and archive this data to achieve internal objectives and regulatory compliance requirements. The ECC eSCOP product provides the very powerful filtering, reporting, data organizational management, and archiving features that make Microsoft System Center Operation Center 2007 a valuable component of our enterprise," stated Saini Dheeraj, SAA IT security director.

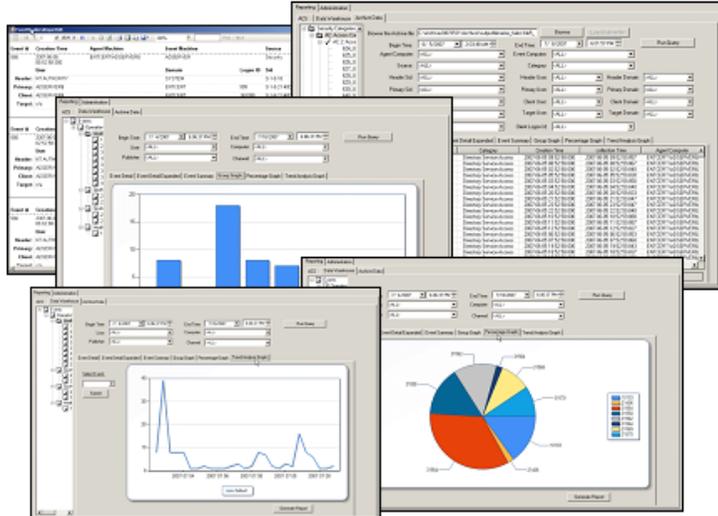
"In addition, ECC professional services provided the subject matter expertise to advance our security and compliance objectives. Under a relationship that can really be called a partnership, ECC has further mapped eSCOP and Operations Manager to our specific requirements," Dheeraj concluded.

Benefits

ECC eSCOP is an extensible and intuitive administrative console for System Center Operations Manager 2007's Audit Collection Services (ACS) and Data Warehouse databases. Among the benefits realized by SAA include:

ACS Security Event Data Organization and Categorization

- **Compliance/Security Best Practices:** Access Control, Audit and Accountability, Identification and Authentication, System and Communications Protection, System and Information Integrity, Contingency Planning
- **Audit Type:** Audit Account Logon Events, Audit Account Management, Audit Directory Services Access, Audit Logon Events, Audit Object Access, Audit Policy Change, Audit Privilege Use, Audit Process Tracking, Audit System Events
- **Event Series Grouping:** Events categorized by series event numbered groupings



Flexible Analysis of Operations Manager 2007 Data Warehouse Information Management

- **Operations Manager Collection:** Health Services Modules, Operations Manager Configuration, Operations Manager Connectors
- **Application Service Collection:** Tracking of targeted application events
- **System Services Collection:** Tracking targeted system events

Administration:

- **Integrated Console:** Intuitive interface to manage ACS and Data Warehouse databases
- **Filter Rules:** Event collection using rules and filter parameters
- **Current Data Collection:** Pre-selected and ad hoc values for filter parameters
- **Partition Management:** Partition setting, lifetime and growth management
- **Configurable Archiving:** Archive event data beyond the event lifetime window
- **Formatting and Storage:** File formats and offline storage management
- **Filter Display:** Filters view for peer review and audit health

Reporting:

- **IT Security Reporting:** Best practices based rapid, customizable reports
- **Data Warehouse Framework:** Collection based upon system health, collector and configuration
- **Very Large Database Reports:** Reliable output reports on millions of event records
- **Report Usability:** Wide variety of localized reports and output formats
- **Contact Scoping:** Targeted views and report with unique scoping

About Enterprise Certified Corporation

Enterprise Certified Corporation is a Microsoft Gold Certified Partner, having been awarded this status based upon strong customer reviews and VertiTest Laboratories independent testing. ECC is the only organization to have multiple principals named Microsoft Most Valuable Professions (MVP) in the field of security. ECC personnel have collectively decades of security and IT infrastructure consulting services and product development experience.

About Social Services Agency, Santa Clara County

The Social Services Agency of Santa Clara County, California is a culturally sensitive and socially responsible public agency providing high quality, professional, financial, and protective services. As such, the agency maintains and successfully manages very sensitive data information required by internal objectives and regulatory requirements.



Security Solutions
Networking Infrastructure Solutions
ISV/Software Solutions

Enterprise Certified Corporation

www.enterprisecertified.com info@enterprisecertified.com 800 701 2785 Sales Extension 4