SecurityIQ

Hardware and Architecture Sizing

and

Sample Deployment Configurations

Created: August, 2015

Last Updated: 2015-10-23

Last Updated By: Cathy Mallet

Table of Contents

Tables

Figures

Overview

SecurityIQ is designed to support enterprise implementations with thousands of applications, hundreds of thousands of users, and millions of events and/or permissions. The application is designed to scale in a linear, controlled fashion as new systems are added. Scalability can be achieved by both vertical and horizontal hardware scaling of the application server cluster.

A typical deployment consists of a central installation and remote gateways. In a majority of cases, the system/server being monitored does not require software or footprint on the server itself; the monitoring agents (software/footprint) are installed on SecurityIQ servers. In the case of NAS, certain vendors (eg NetApp) require the SecurityIQ server to be in the same physical site as the monitored system.

Further Information

Additional Information on hardware sizing can be found in:

- Server Installation Guide
- The relevant Agent Installation Guides
- Client Installation Guide

For information on the services that are run on the various servers, see the Server Installation Guide.

Sizing Considerations

There are many factors to consider when architecting your SecurityIQ solution. SailPoint professional services staff will work with you to appropriately size your environment. Some factors to consider include:

- How many applications/systems will be included?
- How many resources (e.g. number of folders on file servers) exist on each application/system?
- Will permission or entitlement analysis be carried out?
- Will Data Classification be carried out?
- How many data enrichment sources are there?
- How many AD domains are there?
    - Are they all in the same forest?
    - Are they all in trust relationships?
    - Is there a single domain that can reach all of them?
- How many data sources are there?
- Are the applications/systems geographically distributed?
- Are there "off hours" for batch processing, or is constant usage by end users anticipated?
- How many SecurityIQ administrators will be using the system?

- How many SecurityIQ end users (Business Users, Reviewers, etc) will be using the system?
- What is the size of the organization?
- Will you maintain periodic “snapshots” for historical history?
- Are there specific high availability/disaster recovery requirements?

Server Sizing Guide

The tables below provide guidance for a typical configuration. Each customer environment is unique, and it is strongly recommended that you discuss your sizing requirements with your SecurityIQ representative/consultant prior to purchasing the hardware.

Minimum Sizing Guides

The tables show the minimum server sizing for SecurityIQ.

Minimum Server Sizing

	CPU	Memory (GB)	Data Drive (D:) (GB)	Operating System	Roles / Features
Server(s)					
Event Handler(s)	4	8	20	Windows Server 2008 R2 64Bit	.Net3.5 SP1 .Net 4.5
General Services	4	8	20	Windows Server 2008 R2 64Bit	.Net3.5 SP1 .Net 4.5
User Interface (UI)	4	8	20	Windows Server 2008 R2 64Bit	.Net3.5 SP1 .Net 4.5
[1]Data Classification	4	8	80	Windows Server 2008 R2 64Bit	.Net3.5 SP1 .Net 4.5
Entitlement / Monitors / Collectors	4	8	40	Windows Server 2008 R2 64Bit	.Net3.5 SP1 .Net 4.5

Table 1: Minimum Server sizing guide

Minimum Elasticsearch Sizing

Component	Recommendation
CPU	4
Memory (GB)	8
Data (D:) Drive (GB)	20
[2]Data (DB) Storage	50GB
[4]TempDB (dedicated instance)	20GB
Log	20GB
Operating System	Windows Server 2008 R2 64Bit
Roles/Features	Net3.5 SP1 .Net 4.5

Table 2: Minimum Elasticsearch server sizing guide

Minimum SQL Server Database Sizing

Component	Recommendation
CPU	4
Memory (GB)	8
Data (D:) Drive (GB)	20
[3]Data (DB) Storage	50GB
[4]TempDB (dedicated instance)	20GB
Log	20GB
Operating System	Windows Server 2008 R2 64Bit
Roles/Features	SQL Server 2012 64Bit

Table 3: Minimum SQL Server sizing guide

Recommended Sizing Guides

The tables below depict the recommended server sizing for SecurityIQ.

Recommended Server Sizing Guidance

	CPU	Memory (GB)	Data Drive (D:) (GB)	Operating System	Roles / Features
Server(s)					
Event Handler(s)	8	8	20	Windows Server 2012 R2 64Bit	.Net3.5 SP1 .Net 4.5
General Services	8	8	20	Windows Server 2012 R2 64Bit	.Net3.5 SP1 .Net 4.5
User Interface (UI)	8	8	20	Windows Server 2012 R2 64Bit	.Net3.5 SP1 .Net 4.5
[1]Data Classification	8	12	80	Windows Server 2012 R2 64Bit	.Net3.5 SP1 .Net 4.5
Entitlement / Monitors / Collectors	8	8	40	Windows Server 2012 R2 64Bit	.Net3.5 SP1 .Net 4.5

Table 4: Recommended Server sizing guide

Recommended Elasticsearch Sizing Guidance

Component	Recommendation
CPU	8
Memory (GB)	12
Data (D:) Drive (GB)	20
[2]Data (DB) Storage	150GB
[4]TempDB (dedicated instance)	30GB
Log	30GB
Operating System	Windows Server 2012 R2 64Bit
Roles/Features	Net3.5 SP1 .Net 4.5

Table 5: Recommended Elasticsearch sizing guide

Recommended SQL Server Sizing Guidance

Component	Recommendation
CPU	8
Memory (GB)	16
Data (D:) Drive (GB)	20
[3]Data (DB) Storage	150GB
[4]TempDB (dedicated instance)	30GB
Log	30GB
Operating System	Windows Server 2012 R2 64Bit
Roles/Features	SQL Server 2012 64Bit

Table 6: Recommended SQL Server sizing guide

[1] Data Classification is an optional service, and a Data Classification server is required if Data Classification is elected. Note: For each end point, a separate data classification service is started.

[2] The Elasticsearch server is memory and I/O intensive. As a guide for calculating database storage space for Elasticsearch, a key of 1GB per four (4) million events should be used.

[3] As a guide for calculating database storage space for the SQL Server, the following should be used: 50GB Base + 1GB per 1 million events

[4] SecurityIQ heavily utilizes Temp DB. For a dedicated instance, min 30GB is recommended. See Database Configuration for more detail.

SecurityIQ Architecture

SecurityIQ architecture requires a central installation with remote gateways where necessary (e.g., distributed environments).

SecurityIQ server services are centralized due to extensive database usage. Services are independent and do not require co-existence. Some of the services can be duplicated to provide better performance and high availability.
The only services that can be distributed are agent services (e.g., Monitor, Permission Analysis and Data Classification).

SecurityIQ is designed to work in a firewalled environment, and internal communication is based on WCF (SOAP-based) using designated (configurable) ports. The agents' communication with the central site is based on protocols defined by the vendors. For example:

- MSRPC
- SQLNet
- HTTP
- SMB

The diagram below provides a schematic view of the architecture:

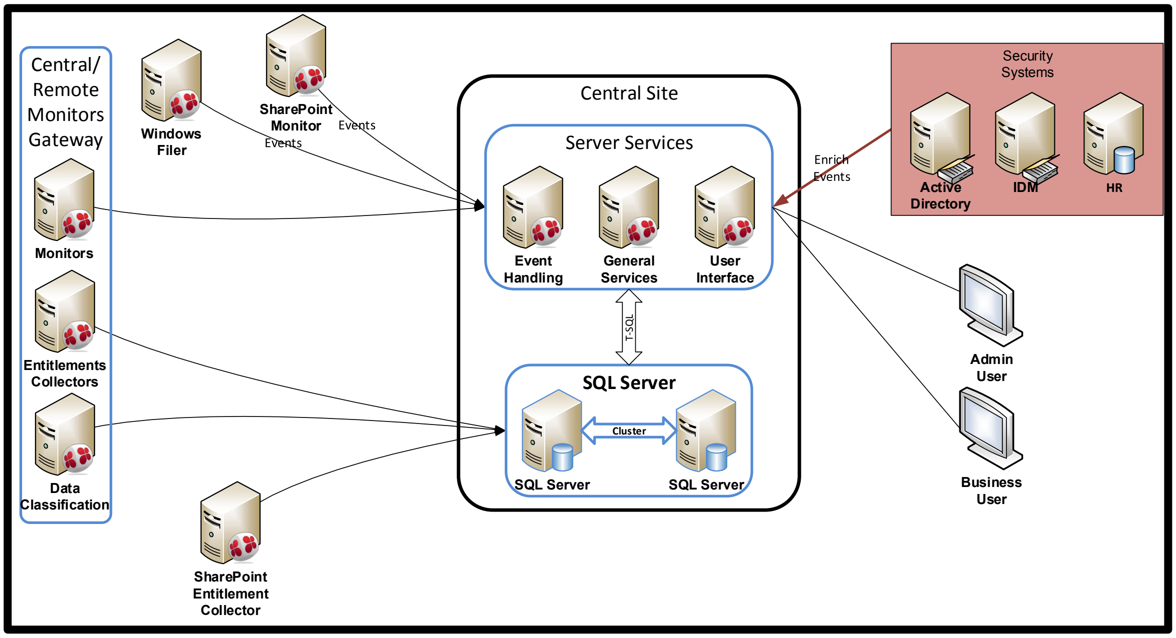

Figure 1: Architecture Schematic (sample configuration)

Scalability

Scalability can be achieved both vertically and horizontally through hardware scaling of the application server cluster. For example, Event Handlers and Entitlement Collectors can be added and/or the server (s) themselves can be upgraded (e.g. memory, CPU).

For complex environments/scenarios, it is recommended that you contact your SailPoint consultant to review your unique environment. This includes environments in which:

- Load balancing is required
- There are geographically-distributed nodes
- There is a large number of systems (applications) or bespoke systems
- There are constraints such as bandwidth, footprint, access restrictions and etc.

Anatomy Profiler and Elasticsearch

SecurityIQ supports basic searching of activities via the use of database indexes. Advanced searches, however, require application-level indexing. Anomaly Prolifer provides this functionality by performing application-level indexing on activities stored in the database.

New activities that appear in the SecurityIQ database are indexed by the Anomaly Profiler and handed over to Elasticsearch for further indexing. Elasticsearch is able to index every field inside an event, providing fast query and reporting of events.

Elasticsearch is a high-performance, highly scalable, full text indexing database, where the underlying indexing database is Lucene. Elasticsearch supports the creation and management of a full-mesh cluster above the Lucene layer.

The Anomaly Profiler and Elasticsearch need to be installed together.

Note: when Elasticsearch is scaled so that multiple Elasticsearch servers act as a cluster, a single instance of the Anomaly Profiler is maintained.

Given the functionality of the Anomaly Profiler and Elasticsearch, the service is memory and I/O intensive. The key hardware recommendations are:

- The service is installed on a dedicated server
- The minimum memory size is 12GB
- Dedicated disk drives, preferably Solid State Drives (SSD), for the Elasticsearch database. The disk size should be calculated with a key of 1GB per 4 million events. Using SSDs will provide a high performance boost.

The service can run in a VM environment, provided the storage is dedicated with a minimum memory size of 12GB.

Sample Deployment Configurations

Below are sample configurations that can be used as a guide for deploying SecurityIQ, or as a possible growth path.

The initial deployment may consist of Basic Deployment, and as additional applications (systems) are included, SecurityIQ can be scaled up vertically or horizontally or both.

Basic Deployment Sample

The minimum number of servers required to deploy SecurityIQ is two (2) - a database server and an application server. Figure 2 shows a basic sample deployment with two servers. This configuration is ideal for small environments.

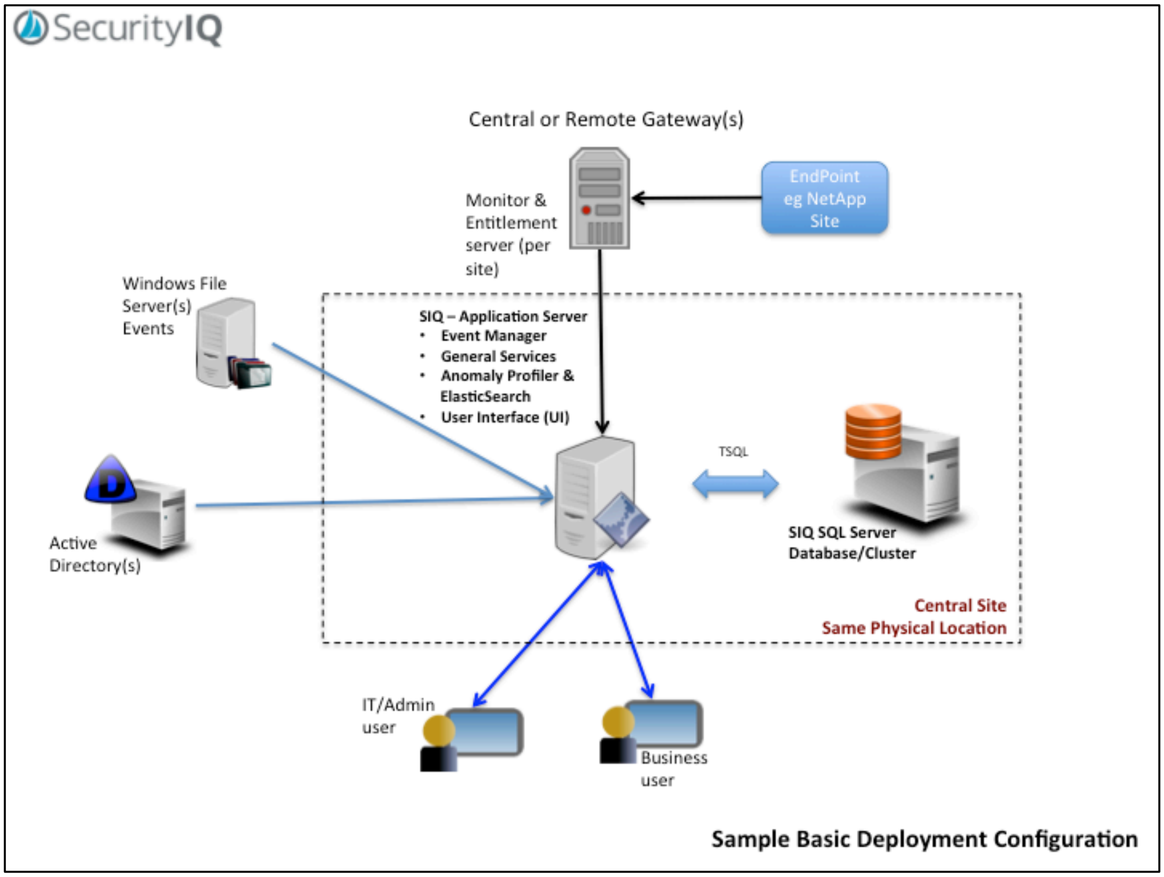
SecurityIQ
Central or Remote Gateway(s)
Monitor & Entitlement server (per site)
EndPoint eg NetApp Site
Windows File Server(s) Events
SIQ – Application Server
• Event Manager
• General Services
• Anomaly Profiler & ElasticSearch
• User Interface (UI)
TSQL
SIQ SQL Server Database/Cluster
Active Directory(s)
Central Site
Same Physical Location
IT/Admin user
Business user
Sample Basic Deployment Configuration

Figure 2: Sample Basic Deployment

Basic Deployment Example:

Application server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 40GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Monitor server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 20GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Database server

CPU = 8 core
Memory =16MB
Data (D:) Drive = 20GB
Data Storage = 150GB
TempDB = 30GB
Log = 30GB
Operating System = Windows 2012 R2 64Bit
Features = SQL Server 2012 64Bit

Intermediate Deployment Sample

The Intermediate Configuration offers a degree of high availability on the application server layer while still using the central database. In this configuration the User Interface and Elasticsearch are segregated from the application server. Additional scalability can be achieved by further segregating the application server into its components as shown in Advanced Deployment.

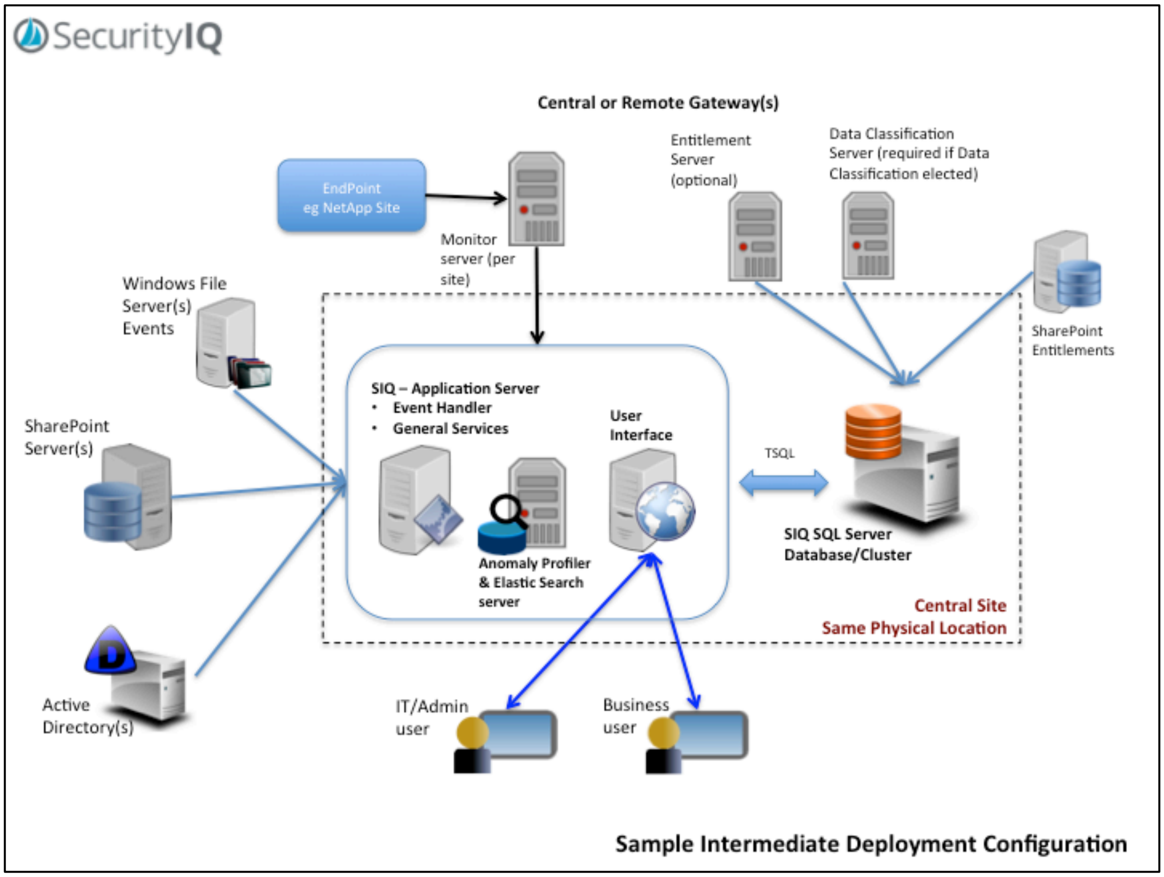
SecurityIQ
Central or Remote Gateway(s)
EndPoint eg NetApp Site
Monitor server (per site)
Entitlement Server (optional)
Data Classification Server (required if Data Classification elected)
SharePoint Entitlements
Windows File Server(s) Events
SharePoint Server(s)
Active Directory(s)
SIQ – Application Server
• Event Handler
• General Services
User Interface
Anomaly Profiler & Elastic Search server
TSQL
SIQ SQL Server Database/Cluster
Central Site
Same Physical Location
IT/Admin user
Business user
Sample Intermediate Deployment Configuration

Figure 3: Sample Intermediate Deployment

Intermediate Deployment Example:

Application server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 40GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

User Interface server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 20GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Monitor server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 40GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Anomaly Profiler & Elasticsearch Server

CPU = 8 core
Memory = 12MB
Data (D:) Drive = 20GB
[1]Data Storage = 50GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

[1] Disk space calculation is based on 1GB per 4 million events

Database server

CPU = 8 core
Memory =16MB
Data (D:) Drive = 20GB
Data Storage = 200GB[2]
TempDB = 30GB
Log = 30GB
Operating System = Windows 2012 R2 64Bit
Features = SQL Server 2012 64Bit

[2] Disk space calculation is based on 50GB base + 1GB per 1 million events

Advanced Deployment Sample

The Advanced Deployment Configuration offers flexibility, scalability and performance. The application server is fully segregated into its components – Event Handler, General Services, Elasticsearch, and User Interface. This scenario also segregates the Entitlement Collector from the Monitors and includes a Data Classification server.

Data Classification is an optional feature/service, and if elected, a Data Classification server will be required.

As the application load increases, adding additional Monitor servers, Event Handlers, Elasticsearch and Entitlement servers can offset the increased load.

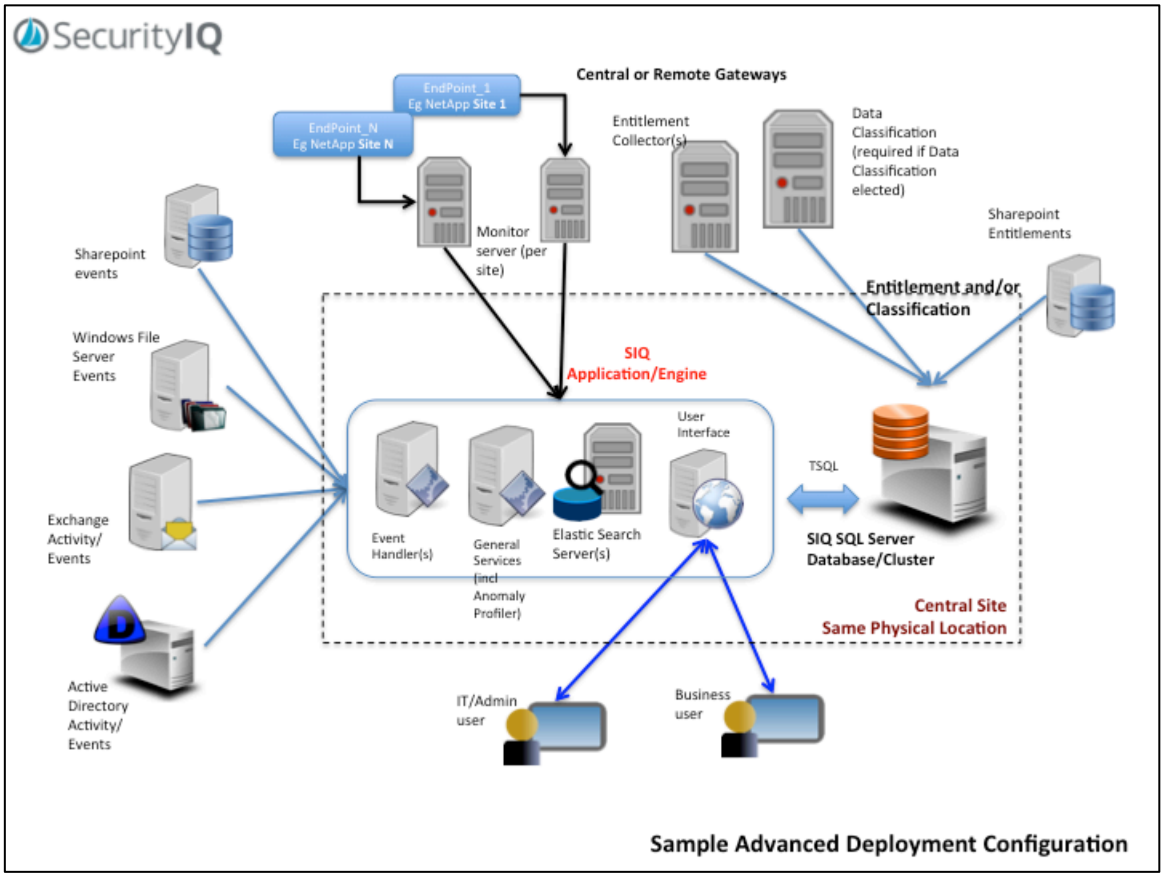

Figure 4: Sample Advanced Deployment

Advanced Deployment Example:

Event Handler

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 20GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

User Interface server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 20GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

General Services server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 20GB
Operating System = Windows 2012 R2 64Bit

Features = .Net 3.5 SP1 and

Monitor server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 40GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Entitlement Collector server

CPU = 8 core
Memory = 8MB
Data (D:) Drive = 40GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Data Classification server

CPU = 8 core
Memory = 12MB
Data (D:) Drive = 80GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

Elasticsearch Server

CPU = 8 core
Memory = 12MB
Data (D:) Drive = 20GB
[1]Data Storage = 150GB
Operating System = Windows 2012 R2 64Bit
Features = .Net 3.5 SP1 and

[1] Database storage calculation is based on 1GB per 4 million events

Database server

CPU = 8 core
Memory =16MB
Data (D:) Drive = 20GB
[2]Data Storage = 300GB+
TempDB = 40GB
Log = 40GB
Operating System = Windows 2012 R2 64Bit
Features = SQL Server 2012 64Bit

[2] Database storage calculation is based on 50GB base + 1GB per 1 million events

Supported Operating Systems and Platforms

The tables below depict the supported platforms and versions.

Supported Server Information

System	Supported Versions
SecurityIQ Server	Windows 2008R2/2012/2012R2 64Bit
Workstations	Windows 7+
Browsers	HTML5 supported browsers
Database	MS SQL Server 2008R2/2012 64Bit

Table 7: Supported Platforms

Supported Endpoint Information

File Servers/Services

System	Supported Versions
Windows File Server	Windows 2003/2003R2/2008/2008R2/2012/2012R2, 32/64 bit
NetApp	ONTAP (7mode) version 7.3 and above – support for CIFS & NFS 8.2 and greater CDot
EMC Celerra	Celerra 6 and greater – support for CIFS
EMC Isilon	OneFS 7.1 and greater– support for CIFS
HDS	11 and greater – support for CIFS

Table 8: Supported File Servers

Microsoft Infrastructure

System	Supported Versions
Active Directory	Domain Controllers 2008+
Exchange	Exchange 2010 SP1+

Table 9: Supported Active Directory and Exchange Platforms

Content Management

System	Supported Versions
Sharepoint	2007 SP1+

Table 10: Supported Content Management Platforms

Cloud Services

Supported Services
Exchange Online (Office 365 Mail)
Dropbox.com (enterprise)
Google Drive (enterprise)
Box.com (enterprise)

Table 11: Supported Cloud Platforms

Database Configuration

The database is the heart of SecurityIQ.

The database engine of MS SQL Server 2012 64 bit has built-in (native) high availability and encryption features. SecurityIQ takes advantage of these features to ensure high availability and encryption.

Both dedicated and shared database configurations are supported.

SailPoint recommends a dedicated instance for performance reasons. However, SailPoint does understand this is not always possible in customer environments and will fully support a shared database configuration provide the following metrics are met:

Metric	Requirement
Disk I/O Throughput (IOPS)	12K IOPS
Disk I/O Throughput Rate	10500 MB/S
Throughput in Transactions/Sec	6000 TPS
Disk I/O latencies for Read	< 8ms
Disk I/O latencies for Write	< 1ms

Table 12: Database Performance Metrics

With shared database configurations, the following are also recommended:

- Separate disks are used for SecurityIQ due to high I/O rate
- TempDB access is on fast drives – for example, Solid State Drives can be used (fault tolerance is not necessary).
- Disk space is monitored by administrators to ensure availability of disk space
- Access to the database via SQL Management Studio so that monitoring and maintenance can be performed on the database.
- If the DB is on a physical machine, turn off hyper-threading

Database Interaction

nHibernate (standard, open source and object-relational mapper) is used for a majority of the database interactions, and all the server services communicate directly with the database.

End users communicate via designated services using a browser (rich) client.

TempDB

With the high number of events being monitored, SecurityIQ performs a high level of inserts and utilizes TempDB extensively. For large installations, use of Solid State Drives (SSD) for TempDB is encouraged

When allocating dedicated storage for TempDB ensure the following for optimum performance of TempDB:

- Storage is on a separate drive
- The drive is real and formatted to 64K allocation unit
- One TempDB file is allocated per real core on the system
- TempDB and Logs are managed so they don't outgrow the available disk space

Additional Database Settings

The database is central to SecurityIQ and its performance is critical for a successful implementation of SecurityIQ. In order to ensure optimum database performance, the following database settings are aslo recommended:

- Backup/Recovery - **SIMPLE** mode for recovery plan is mandatory; otherwise performance issues will be experienced due to constant database activity resulting from real-time auditing.
- Database Storage
  - If the database server running as a Virtual Machine (VM), ensure the database storage are REAL disks dedicated to the VM
  - Data and Logs must be on separate drives
  - Drives must be formatted to 64K allocation unit
- Instance Level Settings
  - FileStream – "Full Access Enabled" for saving of reports and files
  - CLR – Enabled (running .Net code in DB - Safe Mode). For example, calculation of permission path
  - SQL Mixed Authentication

Capacity Review

It is recommended that SecurityIQ capacity be reviewed on a regular basis to ensure optimum performance. The initial review should be undertaken after 3 months of deployment since by this stage, SecurityIQ usage trends, disk space growth, and system utilisation trends will be evident. Following the initial review, a yearly capacity review is recommended for growth management.

The capacity review should take into consideration:

- The number of events/activities captured
- The database growth rate
- CPU and Memory utilization
- Addition of new features – eg Data Classification
- Historical Data Archiving

Based on the capacity review findings, the SecurityIQ architecture can be scaled vertically or horizontally. For example, you may find it necessary to:

- Segregate the services such as the User Interface, Reporting or Elasticsearch
- Segregate Entitlement Collection from the Monitor Server
- Add Elasticsearch nodes or increase memory
- Increase the number of Event Handlers due to an increase in systems being monitored
- Increase server or database disk space

Virtualization Architecture

Systems virtualization is becoming an efficient way of consolidating and managing enterprise infrastructures. In deploying SecurityIQ in a virtualized environment, SailPoint recommends that the **database server** layer not be virtualized. This is primarily for I/O performance and to avoid scalability issues that could arise in a virtualized environment.

SailPoint understands that it may not be possible to have a non-virtualized environment. In such cases, provided the database performance metrics are met (see Table 12: Database Performance Metrics), SailPoint will fully endorse the configuration.

SailPoint also fully endorses virtualization of the **application server** layer, as long as adequate dedicated memory and resource allocation configurations are taken into consideration.

Another consideration is that Virtual Machines (VMs) often run in a shared host. Because of this shared host environment, adequate resource allocation and management is needed to maintain a stable virtual environment. These resources can be everything from network access, to disk space, to memory, to CPU cycles. Providing a stable environment with adequate resources will enable SecurityIQ to run without conflict.