



Bit9 Security Platform 7.2.1

Operating Environment Requirements

Version 7.2.1.2102
Patch 14

13 May 2016

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: <http://www.carbonblack.com>

Copyright © 2004-2016 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Carbon Black is a trademark of Carbon Black, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

Contents

Overview	3
Bit9 Security Platform Server Requirements	3
Bit9 Security Platform Server: Supported Operating Systems	3
Bit9 Security Platform Database: Supported SQL Server Versions	3
Bit9 Security Platform Database: Supported AWS RDS MS SQL Server Versions	3
Bit9 Security Platform Web Server Platform: Support Server	4
Bit9 Platform Console: Supported Browsers	4
Bit9 Security Platform Server System Requirements	4
Bit9 Security Platform Server Architecture by Endpoint Count.....	5
Two-tier Deployment Architecture	5
Bit9 Security Platform Database: SQL Storage Requirements.....	7
Bit9 Security Platform Database: SQL Memory Configuration	7
Bit9 Security Platform Database: SQL Maintenance.....	7
Bit9 Security Platform Database: SQL Backups.....	8
Bit9 Security Platform Server: Virtualization	8
Bit9 Security Platform Server: Common Performance Pitfalls	8
Bit9 Security Platform Server: Communication Requirements	9
Bit9 Security Platform Agent Requirements	10
Bit9 Security Platform Agent Supported Operating Systems:	10
Bit9 Security Platform Agent: Hardware Recommendations	10
Bit9 Security Platform Agent Communication Ports.....	10
Bit9 Security Platform Agent: Certificates	10

Overview

This document describes the hardware, software and site requirements for implementing a Bit9 Security Platform Server installation. *It is a requirements summary only.* For a successful server installation, you must use the *Installing Bit9 Security Platform Server* manual for detailed descriptions of installation procedures. For successful agent installations, you must use the instructions in the “Managing Computers” chapter of *Using Bit9 Security Platform*. If there are any questions related to hardware and performance, please contact your Bit9 technical representative after reviewing this document.

Bit9 Security Platform Server Requirements

Bit9 Security Platform Server: Supported Operating Systems

Operating System	Architecture	Service Pack	Additional Notes/Requirements
Windows Server 2008 R2	x64	Use Latest	HVM Virtualization only
Windows Server 2012 R2	x64	Use Latest	HVM Virtualization only

Bit9 Security Platform Database: Supported SQL Server Versions

Database System	Architecture	Service Pack	Additional Notes/Requirements
SQL Server Express 2008 R2	x64	Use Latest	Limited to 1 CPU Socket (or 4 cores) Maximum memory utilized: 1Gb Maximum database size: 10Gb
SQL Server 2008 R2	x64	Use Latest	
SQL Server Express 2012	x64	Use Latest	Limited to 1 CPU Socket (or 4 cores) Maximum memory utilized: 1Gb Maximum database size: 10Gb
SQL Server 2012	x64	Use Latest	Standard edition for < 10K endpoints, Enterprise edition for larger deployments. See “Bit9 Security Platform Server Architecture by Endpoint Count” below for more details.
SQL Server 2014	x64	Use Latest	Same as SQL Server 2012.

Bit9 Security Platform Database: Supported AWS RDS MS SQL Server Versions

Database System	DB Engine Versions	Architecture	Additional Notes/Requirements
SQL Server Express	11.00.5058.0.v1 10.50.6000.34.v1	x64	Limited to 1 CPU Socket (or 4 cores) Maximum memory utilized: 1Gb Maximum database size: 10Gb
SQL Server Standard	12.00.4422.0.v1 11.00.5058.0.v1 10.50.6000.34.v1	x64	Standard edition for < 10K endpoints, Enterprise edition for larger deployments. See “Bit9 Security Platform Server Architecture by Endpoint Count” below for more details.
SQL Server Enterprise	12.00.4422.0.v1 11.00.5058.0.v1 10.50.6000.34.v1	x64	Standard edition for < 10K endpoints, Enterprise edition for larger deployments. See “Bit9 Security Platform Server Architecture by Endpoint Count” below for more details.

Bit9 Security Platform Web Server Platform: Support Server

Version	Part Of OS	Current Version	Supported Architecture	Supported Level	Additional Notes/Requirements
IIS 7.5	Windows 2008 R2 Server	7.5.7600.16385	x64	All	Required IIS Roles <ul style="list-style-type: none"> • Common HTTP Features: All • Application development: <ul style="list-style-type: none"> - ASP.NET (this will add ASP .NET 3.5) - .NET Extensibility - CGI - ISAPI Extensions - ISAPI Filters • Health & Diagnostics: <ul style="list-style-type: none"> - HTTP Logging - Logging Tools - Request Monitor - Tracing • Security: <ul style="list-style-type: none"> - Basic Authentication - Windows Authentication - URL Authorization - Request Filtering - IP and Domain Restrictions • Performance: None • Management Tools: <ul style="list-style-type: none"> - IIS Management Console - IIS Management Scripts and Tools - Management Service FTP Publishing Service: None
IIS 8.0	Windows 2012 Server R2 only				Same as IIS 7.5 Additional requirements: Private memory for IIS should be increased to 800 MB

Bit9 Platform Console: Supported Browsers

Browser	Version	Additional Notes/Requirements
Microsoft Internet Explorer	9.0 or higher	Windows only
Mozilla Firefox	Latest	Windows, Mac or Linux
Google Chrome	Latest	Windows, Mac or Linux
Safari	5.1.2 or higher	Mac

Bit9 Security Platform Server System Requirements

- Clean operating system installation, with the latest version/patch/service pack
- Microsoft IIS: Version corresponding to the Windows Server installed. Configured as described in the *Installing Bit9 Security Platform Server* guide
- Microsoft .Net:
 - Version 3.5 framework with latest patch level
 - Version 4.5 or 4.6 framework with latest patch level
- Microsoft Installer: Version 4.5 or newer
- Processor: Intel Xeon/i7 processor/multi-core running at least 2.5GHz. Although Intel processor is recommended, it is possible to use equivalent AMD processor
- Ethernet connection: 1 Gbps or faster connection required

Bit9 Security Platform Server Architecture by Endpoint Count

The Bit9 Security Platform Server should be deployed on a single computer that will house both the Bit9 Security Platform Server and SQL Server. The following table lists the requirements for this computer.

Endpoints	SQL Server Edition	Hardware		Required Database Storage	DAS (Locally attached)		PCIe Flash GB / 1K EPTS ²
		RAM (GB)	CPU Cores ¹		Disks	RAID	
Up to 100	Express	4	2	20 GB ³	2	1	n/a
101 – 250	Standard	12	2	55 GB	4	1+0	n/a
251 - 500		16	2	100 GB	4	1+0	n/a
501 – 1,000		16	4	175 GB	6	1+0	n/a
1,001 – 1,500		16	4	300 GB	6	1+0	n/a
1,501 – 2,000		16	4	500 GB	8	1+0	n/a
2,001 – 5,000		32	6	1 TB	8	1+0	n/a
5,001 - 10,000		48	8	1.2 TB	12	1+0	n/a
10,001 – 20,000		48	8	2 TB	24	1+0	50
20,001 - 40,000	Enterprise	64	12	2 TB	14	1+0	20
40,001 - 80,000		96	16	4 TB	14	1+0	20
80,001 - 160,000		96	16	8 TB	22	1+0	20

¹ CPU core requirements are based on physical, not hyper-threaded cores. Two CPUs might be necessary to reach required number of cores.

² PCIe sizing requirement is given in GB per 1K endpoints..

³ Database storage for SQL Express includes 10 GB for data file (maximum limit for SQL Express) and additional 10 GB for the log file.

Associated with the storage sizes listed above are the following caveats:

- By default, the Bit9 Platform Server saves no more than four weeks of events and no more than ten million events. Increasing these defaults will increase the size of the database. Under normal circumstances, the largest portion of the database will be taken up with storage of instances of files on endpoints.
- The Bit9 Platform Server carries out two scheduled database tasks described in the document *SQL Server Configuration for Bit9 Security Platform*. Stopping these tasks can cause the database to grow beyond the sizes listed above.
- The steps listed under “Database Growth” in the document *SQL Server Configuration for Bit9 Security Platform* are being followed.

Two-tier Deployment Architecture

Here are the requirements for a two-tier installation of the Bit9 Platform where the Bit9 Server and SQL Server reside on separate hardware.

1. For the SQL Server hardware, use the single-tier table above.
2. For the Bit9 Platform Server hardware, use the following table:

Endpoints	Hardware	
	RAM (GB)	CPU Cores ¹
Up to 1,000	4	2
1,001 - 80,000	8	4
Above 80,000	16	8

¹ CPU core requirements are based on physical, not hyper-threaded cores. Two CPUs might be necessary to reach required number of cores.

3. Make sure that the network latency between the Bit9 Platform Server and SQL Server is 0.7 ms or lower. The freeware utility hrPing or similar can be used to validate the latency.
4. The SQL server instance and underlying database storage has to be dedicated to the Bit9 Platform Server

Bit9 Security Platform Database: SQL Storage Requirements

The SQL database should meet the following requirements:

- The OS and paging file must be on a separate physical partition from the SQL database. Use of two additional disk drives configured as a RAID-1 partition (mirror) is recommended.
- Any AV software must be configured to exclude SQL data directories.
- Direct attached storage (DAS) is required, using a 6 GB/s SAS (Serial Attached SCSI) adapter or better.
- All hard drives must be 2.5" in size, and have rotational speed of 15K RPM. Note that for deployments larger than 40,000 endpoints, 10K RPM drives can be used if the total required disk size requirement cannot be met with available 15K RPM drives.
- RAID-10 should be used with DAS drives
Stripe element size: 64 KB.
Controller cache-write policy: "Write Back"
- Performance of SQL storage should be validated with the Bit9SQLIO tool prior to deployment of Bit9 Security Platform Server.
- When PCIe Flash storage is not used, the entire database (data + log + indexes + temp) should be on the single large DAS partition. Total disk space shown in the table above includes both hard drive and flash drive space.
- The table shows that Enterprise SQL server requires less storage per endpoint. The reason is that this edition of SQL server supports compression, which reduces storage requirements for more than 50%.

Special considerations for PCIe (PCI-express) flash storage:

- Use of a PCIe card is required when noted in the sizing table.
- Recommended Flash card: Virident FlashMax II.
- When PCIe Flash storage is used, the database should be partitioned so that indexes go to the flash storage partition, and all other files (data + log + temp) go to the single large DAS partition. Check table above for PCIe card space requirements for every 1K endpoints.
- Even though it is not required, in order to further improve product performance, the entire database except for the log file (data + indexes + temp) can be moved to flash storage. Security teams who require extremely fast search response times may opt for such an option. This will require 100 GB of flash storage for every 1K endpoints for SQL Standard edition, or 50GB per 1K endpoints for SQL Enterprise edition.
- When PCIe flash storage is used, card airflow requirements have to be met by the hardware box.
- Note that transaction logs should remain on SAS disks or other storage optimized for sequential writes.

Bit9 Security Platform Database: SQL Memory Configuration

Since the Bit9 Security Platform Server database is relatively large, SQL Server will take all the RAM it has at its disposal, potentially leading to system memory starvation. For that reason, a SQL Server memory cap should always be set on SQL Server. On systems with 16GB RAM, set the memory cap to 12GB. For systems with more RAM, make sure that the SQL maximum server memory is set to at least 5 GB less than the total RAM installed in the system for SQL Server Standard, and 10 GB for SQL Server Enterprise edition.

Note: In a small configuration with SQL Server Express, there is no need to set a SQL memory cap because SQL Server Express already limits memory use to 1 GB.

Bit9 Security Platform Database: SQL Maintenance

Bit9 Security Platform Server does its own scheduled SQL DB Maintenance tasks on daily and weekly basis. This functionality is important in order to maintain database performance and limit growth. The maintenance tasks include:

- Deleting obsolete data
- Defragmenting indexes
- Rebuilding statistics

Note: Use of any other, custom maintenance tasks would be counter-productive and should be avoided.

Bit9 Security Platform Database: SQL Backups

The Bit9 Security Platform database uses the “Simple” recovery model. The “Full” recovery model should not be used to avoid a performance penalty and excessive database log growth.

Bit9 Security Platform Server supports automated database backups, but only for deployments up to 100 endpoints. In all other cases, full database backups should be done using best SQL server practices. Also, a database consistency check should be done prior to backup to ensure that the database is not corrupt.

Recommended backup frequency is 2-3 full backups per week. More frequent backups might negatively impact server performance.

Database backup can run anywhere from minutes to hours, depending on database size, network speed (when backups are sent over the network) and performance backup storage. Backups impact server performance should be avoided during busy times (e.g. when many users rely on console performance), or during internal Bit9 Security Platform Server maintenance times (see table below).

Maintenance Task	Times
Daily Cleanup Task	Every day at 12 AM (midnight), Bit9 Security Platform Server local time. Task can run anywhere from 1 to 4 hours.
Database Index Maintenance	Every Saturday starting at 4 AM. Task can run anywhere from 2 to 6 hours.

Bit9 Security Platform Server: Virtualization

Bit9 Security Platform supports the use of virtualized environments for its deployment if the environment is smaller than 5,000 endpoints. Virtual environments must meet the minimum hardware configurations listed in the tables above, and also must meet the following requirements:

- VMware ESX Server 4.01+; recommend patching to current level
- SQL and Bit9 Security Platform Server must be installed on the same virtual machine
- Memory must be allocated as “reserved”
- For virtualized servers, the underlying disk architecture must still meet aforementioned minimum requirements. Note that physical DAS storage, solely dedicated to the Bit9 VM, must be used.

Bit9 Security Platform Server: Common Performance Pitfalls

There are several pitfalls when purchasing and configuring hardware for the Bit Platform Server. This section lists most common mistakes.

Category	Problem Explanation	Possible Mitigations
Slow SQL Storage	Misconfigured or slow storage used for SQL database files can significantly impact the ability of the server to process agent events and file changes and can cause a backlog of server tasks and slow console response.	<ol style="list-style-type: none"> 1. Use direct-attached storage with correctly sized disks and RAID architecture 2. Avoid using SAN storage due to high latency 3. For larger deployments, use fast SSD/Flash storage, as documented
Slow Network	A slow network connection between the Bit9 Platform Server and SQL Server can significantly impact the ability of the server to process agent events and files. This can cause a backlog of messages and loss of visibility into the agent inventory and operation.	<ol style="list-style-type: none"> 1. Deploy Bit9 Platform in a 1-tier model, with both the Bit9 server and SQL Server on the single machine 2. Reduce network latency between Bit9 and SQL server by using fewer, faster switches, or a direct cable connection
Resource Sharing	Shared SQL server or SQL storage layer can impact overall server performance because the server cannot utilize hardware resources as needed. Also, sharing introduces a varying load which makes it impossible to predict future server performance.	<ol style="list-style-type: none"> 1. Provide a dedicated SQL server instance to the Bit9 Platform 2. Provide dedicated storage to Bit9 SQL storage files, not used by either other databases or other applications

Category	Problem Explanation	Possible Mitigations
Hardware Virtualization	Improperly virtualized server hardware or virtualizing the server for a large number of endpoints can impact the overall server performance. The impact can be on either the network, CPU, memory or storage layer. As a reminder, virtualization is supported only below 5,000 endpoints.	<ol style="list-style-type: none"> 1. Move product to physical hardware 2. Move product to 1-tier virtual hardware 3. Ensure that the virtual machine satisfies OER requirements (CPU, Memory), uses physical storage, and that there is very low latency between the Bit9 and SQL servers in case of 2-tier deployment

Bit9 Security Platform Server: Communication Requirements

Requirement	Details	Additional Notes
Port 443 access	Outbound SSL From Bit9 Security Platform Server to Bit9 Security Platform Knowledge	Allow connection to services.bit9.com (proxy connections are supported)
	Inbound HTTPS from Bit9 Console users and Bit9 Agents (for software upgrades)	
Inbound Port 41002 access	Inbound SSL from Bit9 Agents	Port is configurable
Outbound Port 514 access	Outbound UDP for Syslog/SIEM connections	Optional, if Syslog/SIEM integrations are enabled. Port is configurable
Ethernet connection	1 GB/s connection required for connection to Bit9 Security Platform Agents	
Static IP address only	(no DHCP) with an assigned FQDN or alias; IPv4 and/or IPv6 supported	
AD Integration	Server must be a member of a domain if AD integration is utilized	
Bandwidth	For every 1000 agents, you can expect server bandwidth to average about: <ul style="list-style-type: none"> • Inbound: 200kb/s • Outbound: 50kb/s 	

Bit9 Security Platform Agent Requirements

Bit9 Security Platform Agent Supported Operating Systems:

Please refer to “Bit9 Supported Operating Systems v7.2.1” documents.

Bit9 Security Platform Agent: Hardware Recommendations

Agent systems should be in compliance with all hardware requirements for the OS you are running. Consider all processes that run on the agent systems when determining hardware configuration.

It is important to note that only industry standard desktop, laptop or notebook computers as well as server hardware platforms are supported. Mobile, tablet, embedded or fixed-function devices require additional qualifications. Please contact Bit9 Support for additional information.

Requirement	Details	Additional Notes
Memory	The Agent typically uses 50-100MB of virtual memory	
	Systems running WePOS, POSReady, XP Embedded or Embedded 7 should have at least 512MB of physical memory	
	Other supported operating systems should have at least 1GB of physical memory	
Disk Space	The Agent requires at least 200MB of free disk space on the system volume; 500MB is recommended.	Actual storage requirements depend on factors such as the number of files on the computer and the Bit9 Security Platform Server configuration.
	If Bit9 Security Platform is installed to a location other than the system volume, 100MB of free space must be available on the installation volume.	

Bit9 Security Platform Agent Communication Ports

Requirement	Details	Additional Notes
Port 41002	From Bit9 Security Platform Agent inbound to Bit9 Security Platform Server on TCP port 41002 (configurable)	
Port 443	From Bit9 Security Platform Agent inbound to Bit9 Security Platform Server on TCP port 443 for Bit9 Security Platform Agent upgrade	(Optional) Can be configured to use a Windows file server instead

Bit9 Security Platform Agent: Certificates

Make sure your root certificates are up to date and not expired. Additionally, it is important to have your CRL (Certificate Revocation List) up to date.