Microsoft Desktop Optimization Pack for Software Assurance

MBAM Scalability and High-Availability Guide

Technical White Paper

Published: September 2011

Garth Boyst, William Lees and Nathan Barnett

Microsoft

CONTENTS

Executive Summary **3**

Introduction **4**

MBAM Server Deployment **5**

MBAM Server Components 5

Steady State MBAM Server Behavior and Parameters 5

Examples of MBAM Server Deployments 6

MBAM Client Deployment **10**

MBAM Client Rollout 10

MBAM Client Policy Parameters 10

Conclusion **12**

For More Information **13**

Situation

How to prepare an MBAM deployment for robust scaling and high availability.

Solution

Understand the upper-limits supported by MBAM clients for specific hardware and network topologies. Also, understand what parameters affect system performance and how to use them to tune your environment.

Benefits

- Perform an MBAM deployment in the enterprise that has minimal impact on the performance of the infrastructure and resources.
- Reference for prescriptive guidance of resources and network topologies as determined by client load.

Products & Technologies

- Microsoft Windows Server 2008
- BitLocker Drive Encryption in Windows 7
- Microsoft BitLocker Administration and Monitoring
- Microsoft SQL Server 2008
- Microsoft Internet Information Services (IIS) 7.0

EXECUTIVE SUMMARY

The purpose of this whitepaper is to provide guidance to customers on how to create a scalable and robust Microsoft BitLocker Administration and Monitoring (MBAM) deployment. This document provides examples of network topologies and server hardware under various client loads, as well as the processes used for deployment.

This paper assumes that readers are familiar with BitLocker Drive Encryption, Microsoft Windows Server 2008 (and R2), Microsoft SQL Server 2008 (and R2), and Microsoft Internet Information Services (IIS) 7.0.

INTRODUCTION

BitLocker Drive Encryption (BDE) is a Windows security feature that is used by enterprise customers to secure the data on corporate assets - portable machines and removable drive devices in particular. BitLocker Drive Encryption allows you to encrypt the data stored on the Windows operating system volume and the configured data volumes (fixed and removable). It also ensures the integrity of early boot components by using Trusted Platform Module (TPM).

Microsoft BitLocker Administration and Monitoring (MBAM) provide features to manage the lifecycle of BitLocker encryption of computers in an enterprise. BitLocker creates recovery information at the time of encryption and MBAM stores that information in the recovery data store. This recovery information is required when BitLocker-protected drives need to be recovered in the event that the specified unlock method cannot be used such as if the TPM cannot validate the boot components, the personal identification number (PIN) is forgotten, or the password is forgotten. In these instances, the user must be able to provide the recovery PIN or password to unlock the encrypted data on the drive. Similarly, prior to enabling BitLocker on a computer with a TPM version 1.2, TPM must be initialized. The initialization process generates a TPM owner password, a password set on the TPM chip. The user must supply the TPM owner password to change the state of the TPM chip, such as when enabling or disabling the TPM or resetting the TPM lockout.

Microsoft BitLocker Administration and Monitoring (MBAM) has both a server and a client component. The MBAM servers can be deployed on one or more servers, each with different performance characteristics varying under different MBAM client loads. Understanding the roles of the server components will aid in deciding which topology best suits your environment. The initial deployment of MBAM clients degrade the performance of the enterprise's network infrastructure. Steps can be taken to ease the impact on performance. Included in this whitepaper are examples and best practices that administrators can use to tune their MBAM enterprise servers and infrastructure.

For more information about MBAM, see the product documentation on-line at http://onlinehelp.microsoft.com/mdop/gg703313.aspx. A downloadable version of the MBAM product documentation can be found at http://go.microsoft.com/fwlink/?LinkId=225356.

MBAM Server Deployment

This section provides guidance for deploying MBAM servers in a variety of configurations. The whitepaper describes the steady-state behavior of the MBAM servers and the environmental conditions and parameters that affect this behavior. It also provides examples of server configurations and the test data found under heavy client loads.

MBAM Server Components

MBAM server setup includes the following major components:

- MBAM web sites
- MBAM services
- MBAM databases

The MBAM IIS installation consists of the MBAM administration portal and three web services that are hosted on a single or a clustered instance of IIS 7.0 or 7.5. These components cannot be distributed. Additional information about deploying MBAM can be found at http://go.microsoft.com/fwlink/?LinkId=217220.

The Recovery Key, and Hardware database and the Compliance Status database can be hosted together or distributed between two separate servers. Each database can operate in a stand-alone fashion or in a mirrored configuration.

Steady-State MBAM Server Behavior and Parameters

When the MBAM client load increases, particularly during initial client deployment, the server system is stressed. The components that need more resources and tuning will become apparent. This section profiles the resource requirements for these components, outlines their behavior, and provides guidance to allow best performance.

MBAM Web Sites and Services

MBAM web sites and services take few resources and can be hosted on servers with modest hardware. The total collection of these sites and services must be hosted together and cannot be sub-hosted at a smaller granularity. These IIS components are mainly business logic intermediaries and do not hold any local state themselves. The limiting factor that will inhibit web-role system performance is the maximum available number of IIS connections. This limit can be mitigated by increasing the number of IIS servers behind a load-balancing mechanism such as a network load-balancing server, and/or by increasing the maximum number of connections in IIS.

At around 70,000 clients, it is recommended that the aggregate number of connections on a single box or cluster be at least 200.

The memory footprint and disk space available to the web sites and service is negligible on modern systems growing linearly but slowly as the number of client connections increases.

MBAM Databases

The MBAM databases require the most resources and are the bottleneck for high client loads. In steady state using the MBAM client default timers defined in group policy, the Key and Hardware database is the component under the most strain.

Around 100,000 clients, the Key and Hardware database sustains approximately 150 transactions / second. The amount of disk I/O is also much higher on the Key and Hardware database than on the Compliance Status database.

Under the same conditions, the Compliance Status database sustains about 10% of the transaction load of the Key and Hardware database. The only exception is that every six hours there is an update from the Compliance Status database to the Reports database that produces a short spike of approximately 200 transactions / sec.

The communication intervals between the MBAM client and the servers are tunable and will affect performance. They are explained further in the MBAM Client deployment section of this whitepaper.

The memory requirement and disk space of these databases are negligible. The total database disk space in test laboratories is approximately 180 MB per 10,000 clients with the Compliance Status database consuming around 30% more disk space than the Key and Hardware database. The memory requirement for the computers hosting these databases was insignificant when MBAM was in steady state.

Examples of MBAM Server Deployments

The following are some variations on MBAM server topologies and steady-state data supporting the upper-bound client load for each.

All in One

The all-in-one MBAM deployment hosts all of the IIS and SQL components on one server. No load balancer is employed.

Reference Computer:

Two Dual Core XEON 2.40 GHz

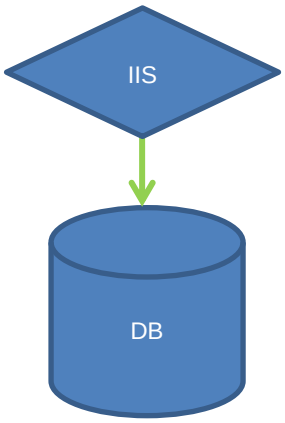
12 GB Ram

Summary:

Upper Limit Client Load - 21,000 clients

Two-Computer Installation

The two-computer installation includes two servers, one with the IIS components and one with the SQL databases. No load balancer is used.



Reference Computers:

IIS

Two Dual Core XEON 2.40 GHz

12 GB Ram

SQL

Two Dual Core XEON 2.40 GHz

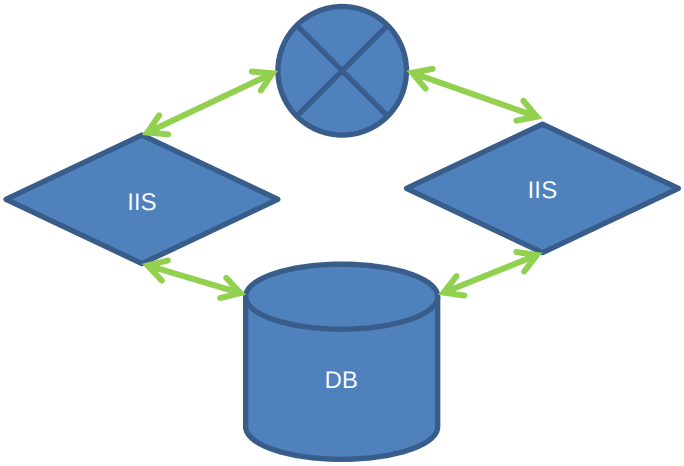
16 GB Ram

Summary:

Upper Limit Client Load - 55,000 clients

Two-Computer NLB Installation

The Two Computer NLB Installation contains a NLB cluster of two IIS servers and one SQL server containing both databases.



Reference Computers:

IIS (2)

Two Dual Core XEON 2.40 GHz

48 GB Ram

SQL

Two Quad Core XEON 2.40 GHz

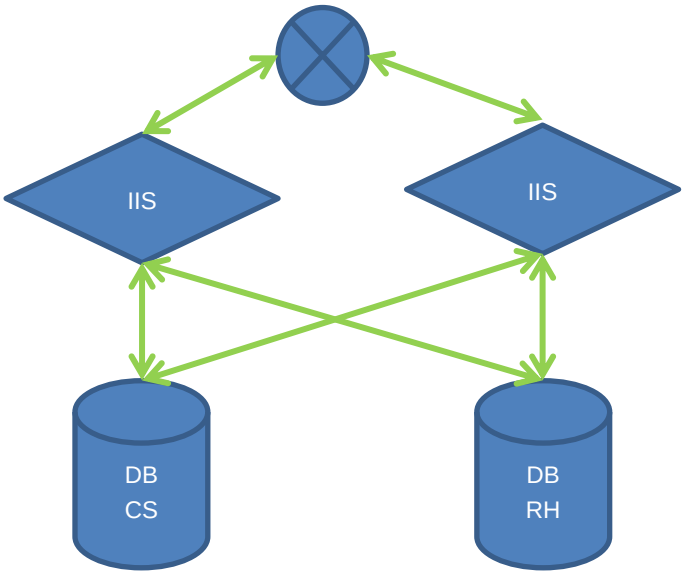
48 GB Ram

Summary:

Upper Limit Client Load - 110,000 clients

Four-Computer NLB Installation

The Four Box NLB Installation deployment contains an NLB cluster of two IIS servers and two SQL servers, one with the Recovery and Hardware database and the other with the Compliance Status database.



Reference Computers:

IIS (2)

Two Dual Core XEON 2.40 GHz

48 GB Ram

SQL Recovery and Hardware

Two Quad Core XEON 2.40 GHz

48 GB Ram

SQL Compliance Status

Two Quad Core XEON 2.40 GHz

48 GB Ram

Summary:

Upper Limit Client Load - 135,000 clients

MBAM Client Deployment

The MBAM client consists of two parts: the end-user client MBAM application and the agent process that runs as a service. The MBAM application communicates with the agent process. The agent process communicates through the web services to the databases providing information about compliance, hardware, and the recovery key. For more information about client deployment, see "Deploying the MBAM Client" (http://go.microsoft.com/fwlink/?LinkId=217226).

MBAM Client Rollout

Staging is an effective strategy when considering how to best rollout the MBAM client package in you enterprise.

There are two advantages to this approach:

1) It decreases the initial performance hit on the SQL databases.

2) The computers will be added to the databases more quickly due to a more even distribution of clients coming on line.

When the MBAM client first comes online, the agent communicates with the web service. The web service then inserts the data from each computer into the databases. By staging the client deployment in smaller batches with a delay between each batch, the number of timeouts and deadlocks decreases dramatically.

In the split database topology, the server under the greatest strain during rollout is the Compliance Status database.

Using default MBAM agent timers, the guidance is to deploy 5,000 clients every 2 hours.

MBAM Client Policy Parameters

Group policy can help tune certain parameters that can influence client performance for both deployment and steady state.

The policy setting NoStartupDelay toggles the initial delay between the start of the service and the communication between the client and the MBAM servers. This initial delay is set at a random interval between 0 and 17 minutes. This helps mitigate burst loads and long queues on the MBAM servers when a large number of clients are simultaneously deployed or brought back online such as after a power outage. This setting is particularly crucial during initial deployment. The default value for this setting NoStartupDelay is false, meaning that random interval startup is enabled.

There are two timers defined in policy, StatusReportingFrequency and ClientWakeupFrequency, which define how frequently the MBAM agent service performs periodic tasks. These settings are applied after the initial random delay is applied.

The ClientWakeupFrequency setting controls how often the agent will 'wake up' and perform tasks related to key recovery. This affects the load on the Key and Hardware database. The default value for this setting is 90 minutes. Typically the key recovery task does not communicate on initial first time run. The key recovery task does not communicate until a user runs an active user session because the encryption policy requires user input. The key recovery task uploads the existing recovery keys at most once per day. Finally, the key

recovery task does not allocate additional recovery keys until a new volume is detected on the computer.

The StatusReportingFrequency setting controls how often the agent reports computer status for reporting. This setting affects the load on the Compliance Status database. The default value for this setting is 270 minutes. This task causes communication traffic every time it runs, regardless of the "time" of the computer. This task will report if this is the initial run even if encryption is blocked waiting for user input or the computer is in a volume-steady-state situation.

CONCLUSION

MBAM is an enterprise, policy-driven, distributed system that is tunable using policy, server settings, and server configurations. Small changes in one parameter or configuration can have profound effects on the system as a whole. Careful planning and understanding of the MBAM configurations are the best ways to ensure successful deployment.

For More Information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

http://www.microsoft.com

http://www.microsoft.com/technet/itshowcase