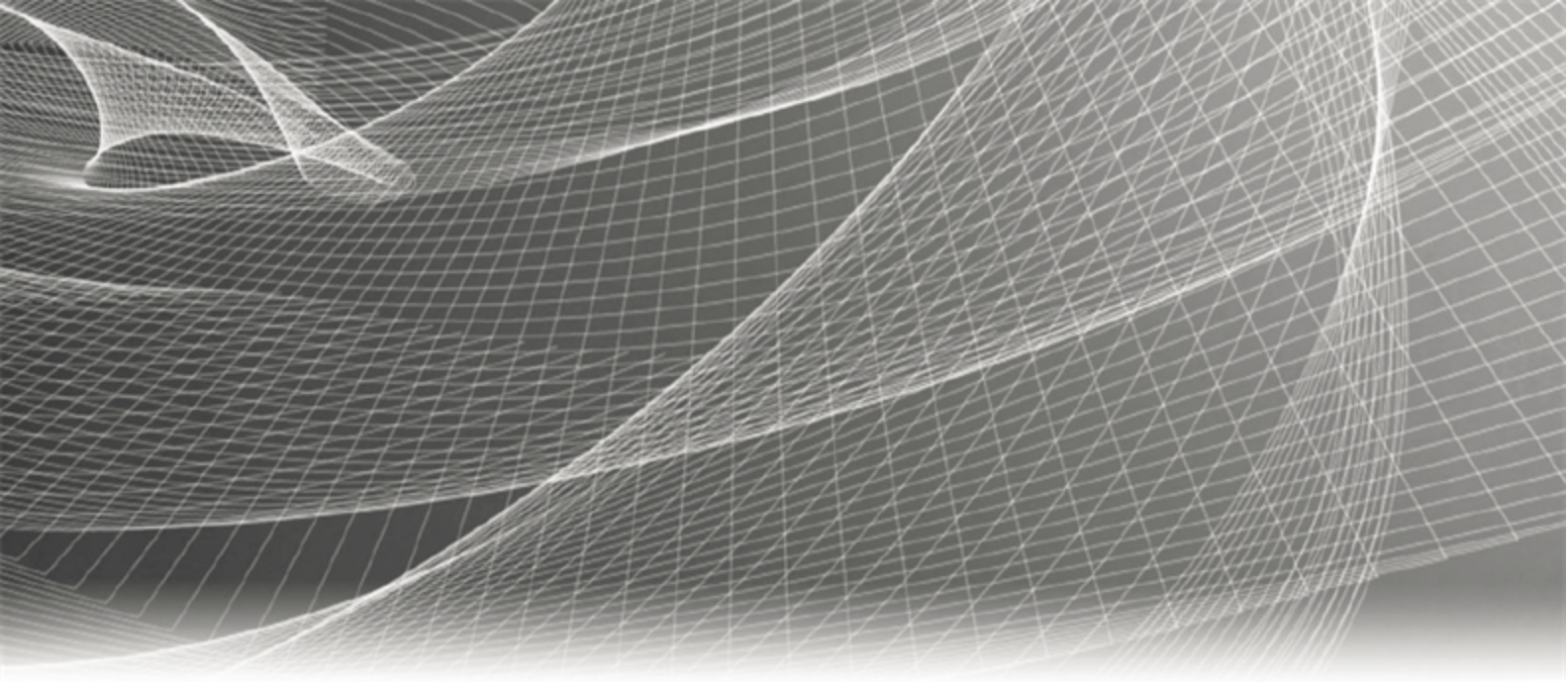


RSA SECURID® ACCESS

RSA® Authentication Manager 8.3

Performance & Scalability Guide

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell Inc. or its subsidiaries, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell Inc.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell Inc. believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

March 2018

Contents

Preface

About This Guide

The *Performance and Scalability Guide* describes the factors that affect the performance of an RSA® Authentication Manager deployment and provides suggestions for ensuring efficient and reliable authentication service.

This guide provides performance test data. Actual performance results in a production environment may be different.

This guide is intended for administrators and other trusted personnel.

RSA SecurID Access Support and Service

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Support for RSA Authentication Manager

Before you call Customer Support for help with the RSA Authentication Manager appliance, have the following information available:

- Access to the RSA Authentication Manager appliance.
- Your license serial number. To find this number, do one of the following:
  - Look at the order confirmation e-mail that you received when your ordered the product. This e-mail contains the license serial number.
  - Log on to the Security Console, and click **License Status**. Click **View Installed License**.
- The appliance software version. This information is located in the top, right corner of the Quick Setup, or you can log on to the Security Console and click **Software Version Information**.

Support for the Cloud Authentication Service and Identity Routers

If your company has deployed identity routers and uses the Cloud Authentication Service, RSA provides you with a unique identifier, called the Customer Support ID, which is required when you register with RSA Customer Support. To see your Customer Support ID, sign in to the Cloud Administration Console and click **My Account > Company Settings**.

RSA Ready Partner Program

The RSA Ready Partner Program website at www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Chapter 1: Performance Testing Results

RSA Authentication Manager Performance Testing Overview

The data in this chapter is derived from lab tests running RSA Authentication Manager 8.3. RSA SecurID authentication performance in a production environment can vary from the performance achieved in a lab environment. These test results provide general guidance.

Note: Many deployment, user, and administration factors can influence overall performance and test results may vary. For more information, see the chapters Performance Factors on page 13 and Performance Monitoring on page 27.

RSA recommends deploying a replica instance. In addition to enabling recovery of administrative functionality if the primary instance becomes unavailable, replica instances can improve authentication performance. Installing replica instances locally in a WAN mitigates the latency that occurs when authentication agents communicate over a long distance. For example, authentication agents in London can send authentication requests more quickly to a local replica instance than they can to a primary instance located in San Francisco.

Test Environment and Procedures

This section describes the environment and procedures used for performance testing.

Amazon Web Services (AWS) Amazon Machine Image (AMI) Test Environment

The RSA Authentication Manager Amazon Web Services (AWS) Amazon Machine Image (AMI) tests were performed on the AWS instance types of m4.large and m4.xlarge.

	m4.large	**m4.xlarge**
vCPU	2	4
Memory	8 GB	16 GB
Instance Storage	Amazon Elastic Block Storage (EBS) only	Amazon Elastic Block Storage (EBS) only
EBS-Optimized	Yes	Yes
Network Performance	Moderate	High
IPv6 Support	Yes	Yes

VMware Virtual Appliance Test Environment

The RSA Authentication Manager VMware virtual appliance tests were performed ion a mid-range machine.

Component	**Specification**
Model	Cisco UCS C200 M2 (High-Density Rack Mount Server)
CPU	Dual Quad Core CPU: Intel® Xeon® CPU E5620 @ 2.40GHz
Cache Size	12288 KB
Memory	8 GB
Disk	4 x 146 GB HDD Servers

Testing was done on a dedicated ESXi 6.0 (VMware vSphere Hypervisor 6.0) server running a single virtual appliance.

Hyper-V Virtual Appliance Test Environment

The RSA Authentication Manager Hyper-V virtual appliance tests were performed on hardware that is equivalent to the Dell-based RSA SecurID Appliance 250.

Component	Specification
Model	Dell PowerEdge R630
CPU	2 X Quad Core CPU: Intel Xeon E5-2609 v4 processor @ 1.70 GHz
Cache Size	20 MB
Memory	32 GB
Disk	2 X 600 GB SAS, RAID 1, HDD write cache enabled with write back
RAID Controller	PERC H730 with battery backup

Testing was done on a dedicated Hyper-V System Center 2012 R2 Virtual Machine Manager (VMM) server running a single virtual appliance. The virtual appliance was set-up with 8 vCPU and 8 GB RAM.

Hardware Appliance Test Environment

The RSA Authentication Manager 8.3 hardware appliance tests were performed in the following environment.

Component	Specification
RSA SecurID Appliance 130 (Dell)	
Model	Dell PowerEdge R230
CPU	1 X Dual Core CPU: Intel Xeon E3-1225 v5 processor @ 3.30 GHz
Cache Size	8 MB
Memory	16 GB
Disk	1 X 600 GB SAS, Non-RAID (HBA Mode), HDD write cache enabled with write back
RAID Controller	PERC H330 without battery backup
RSA SecurID Appliance 250 (Dell)	
Model	Dell PowerEdge R630
CPU	2 X Quad Core CPU: Intel Xeon E5-2609 v4 processor @ 1.70 GHz
Cache Size	20 MB
Memory	32 GB
Disk	2 X 600 GB SAS, RAID 1, HDD write cache enabled with write back
RAID Controller	PERC H730 with battery backup
RSA SecurID Appliance 130 (Intel)	
CPU	Quad Core CPU: Intel® Xeon® E3-1225 processor @ 3.10GHz
Cache Size	L1 64 KB / L2 256 KB / L3 6144 KB
Memory	8 GB
Disk	1TB 7.2K SATA
RSA SecurID Appliance 250 (Intel)	

Component	Specification
CPU	Two Quad Core CPUs: Intel® Xeon® E5-2600 processors @ 1.8GHz
Cache Size	10 GB
Memory	16 GB
Disk	2 x 600GB 10K SAS (RAID1)

Test Procedure

The methodology for performance tests is as follows:

- Tests obtain measurements in steady state.
- Test scripts and authentications are based on a "happy path" scenario that authenticates only valid users who are properly configured for authentication.
- Tests generate no intentional error conditions.
- Tests run with an increasing number of users making concurrent authentication requests until an upper range of 3,000 to 3,500 users is reached.
- Tests run under steady load for more than ten minutes.
- Tests run on servers with no other software installed.
- For the virtual appliance, the virtual machines are configured with 8 CPUs.

Note: For information on Risk-Based Authentication (RBA) testing for previous versions of Authentication Manager, see the *RSA Authentication Manager 8.2 SP1 Performance and Scalability Guide* on RSA Link: https://community.rsa.com/docs/DOC-80820. RSA SecurID Access, which includes Authentication Manager and the Cloud Authentication Service, provides the most current, advanced risk scoring and identity assurance capabilities .

RSA SecurID Authentication Test Results

The following tables show performance results of RSA SecurID authentication transactions for RSA Authentication Manager 8.3.

All tests were performed with a primary instance and one replica instance. Each test had a user load that simulated thousands of concurrent users. Performance and reliability is comparable to version 8.2 and version 8.2 SP1. Adding replica instances to authenticate additional users would improve performance

Amazon Web Services (AWS) Amazon Machine Image

Configuration	Average Response Time (sec)	Transactions Per Second (TPS)
Primary instance, replica instance, and authentication agents in AWS		
m4.large	2.92	576
m4.xlarge	2.39	1033
Primary instance on-premises, but replica instance and authentication agents in AWS		
m4.xlarge	2.50	657

The AWS performance test results are comparable to the test results for the Dell hardware appliance and the VMware and Hyper-V virtual appliance.

The m4.xlarge instance type has 4 virtual CPUs and 16 GB of memory, but achieves similar results to the Dell-

based RSA SecurID Appliance 250 with 8 cores (two Quad Core CPUs) and 32 GB of memory. The AMI appliance gains a performance advantage from Elastic Block Storage (EBS) and a higher processor clock speed.

The average response time shown in these tables is the authentication response time. If Authentication Manager is deployed in a mixed on-premises and cloud-based AWS deployment, the speed of your Internet connection can affect performance. Better bandwidth or a more reliable Internet connection can improve performance.

VMWare Virtual Appliance

Configuration	Average Response Time (seconds)	Transactions Per Second (TPS)
Primary and 1 Replica	2.48	1056

Hyper-V Virtual Appliance

Configuration	Average Response Time (seconds)	Transactions Per Second (TPS)
Primary and 1 Replica	2.28	1122

Dell Hardware Appliance

Configuration	Average Response Time (seconds)	Transactions Per Second (TPS)
RSA SecurID Appliance 130 (Dell PowerEdge R230) Primary and 1 Replica	2.77	820
RSA SecurID Appliance 250 (Dell PowerEdge R630) Primary and 1 Replica	2.28	1334

Intel Hardware Appliance

Configuration	Average Response Time (seconds)	Transactions Per Second (TPS)
RSA SecurID Appliance 130 (Intel)	3.59	652
RSA SecurID Appliance 250 (Intel)	3.11	740

Agent Reporting

RSA Authentication Manager 8.3 offers two new reports with information on the authentication agents in your deployment. Some newer authentication agents, such as the RSA SecurID Authentication Agent 8.0 for PAM, offer additional data, such as a unique Software Identifier for each installed agent.

RSA tested both reports:

- When you schedule reports, the Authentication Manager report scheduler collects the necessary data.
- The List All Authentication Agent Records report provides information on the authentication agents that have been added to Authentication Manager. For example, you can view the user groups and security

domains assigned to each agent, how many times each authentication agent is installed in your deployment, and whether each agent is enabled or disabled.

- The List All Installed Agents report provides details for all of the installed authentication agents in your deployment that have a corresponding record in Authentication Manager. For each installed authentication agent, this report displays the version number and platform, the hostname and IP address that was last used, the time and date of the last authentication, the security domain, and the name of the corresponding authentication agent record in Authentication Manager. Some newer authentication agents provide a unique Software Identifier for each installed agent. An agent might have one record in Authentication Manager, but the agent can be installed on multiple machines with a unique identifier for each installation.

To evaluate the report scheduler as it collects data and the List All Installed Agents Report as it runs, RSA created 16 authentication agents that use the REST protocol, and simulated 500,000 users with tokens and 500,000 unique authentications. The tests created 500,000 records in the audit log tables.

To evaluate the List All Authentication Agent Records report, unique authentications with 100,000 agents were not feasible, but 100,000 unique authentication agent records were created.

RSA tested reliability by running the report scheduler for 500,000 records while simultaneously testing 2,300,000 authentications with 250 users to the primary instance and 250 users to the replica instance.

The tests used a primary instance and a replica instance. Each had 8 CPUs and 8 GB of memory.

RSA Authentication Results

RSA obtained the following results from the scheduling and report running tests.

Test	Unique Records	Time	Average Authentication Manager CPU Usage
Report scheduler processing	500,000	20 minutes	9%
List All Installed Agents Report	500,000	9 minutes	9%
List All Authentication Agent Records	100,000	5 minutes	12%

RSA obtained the following results from the report scheduler reliability test, in which the report scheduler collected data while millions of authentications occurred.

Test	Unique Records Processed	Number of Authentications	Authentication Failure Rate	Time	Average Primary Instance CPU Usage	Average Primary Instance Memory Usage
Report scheduler reliablility	500,000	2,300,000	0.02%	22 minutes	58%	94%

Although there were no major authentication failures during testing, RSA recommends scheduling large reports to run during off-peak hours.

Chapter 2: Performance Factors

Performance Factor Overview

RSA Authentication Manager is configured by default to provide adequate authentication performance for most organizations. However, deployment, user, and administration factors can influence overall performance. The following sections provide a summary of the areas that affect the performance of an Authentication Manager deployment.

For examples of performance data from various tests performed using RSA Authentication Manager, see RSA Authentication Manager Performance Testing Overview on page 8.

Deployment Performance Factors Overview

Authentication efficiency is affected by several deployment factors. For more information, see Deployment Performance Factors on page 16.

For a virtual appliance, what VMware and Hyper-V factors affect authentication performance?	• Allocated disk space • Number of CPUs • Allocated RAM • Differing hardware and performance characteristics of hard drives and network infrastructure • Other resources available on the VMware or Hyper-V host machine
What identity source factors improve authentication performance?	• Network performance between the Authentication Manager instance and the identity source • Efficiency of the LDAP server • Active Directory Global Catalog
What network factors improve authentication performance?	• Installation on a packet-switched network • Reduction of network latency by providing a local replica instance
How does replication affect authentication performance?	Each replica instance added to the deployment decreases the authentication load on the primary instance. This can result in more transactions per second and a quicker response time.
How does automatic tuning for the virtual appliance affect authentication performance?	Automatic tuning optimizes authentication performance by making adjustments according to the memory size allocated for Authentication Manager. These settings can also be adjusted manually. The hardware appliance does not offer automatic tuning. The hardware appliance memory configuration cannot be changed.

User Performance Factors Overview

User location and work schedule can affect RSA SecurID authentication performance. For more information, see User Performance Factors on page 22.

How does user location affect authentication performance?	Authentication performance can suffer when all users must log on from geographically remote offices on a WAN. You can improve performance and reliability by locating replica instances physically closer to the users who authenticate to them.
How many concurrent	Authentication testing has been done simulating 5,000 concurrent agent

authentications can Authentication Manager accommodate?	authentications. Successful authentication by large numbers of users can be affected by the Agent Retry and Timeout settings.
What is the maximum number of users that Authentication Manager can support?	Authentication Manager has been tested with one million users.

Administration Performance Factors Overview

The efficiency of the deployment is more affected by the tasks performed than by the number of administrators working concurrently. For more information, see Administration Performance Factors on page 25.

How do concurrent administration sessions affect authentication performance?	It is possible for an excessive number of concurrent administrator sessions to impact authentication rates because of the demands placed on the deployment. Normally this does not occur.
How does system maintenance affect authentication performance?	The following administrative tasks can slow down authentication performance: **Backup.** Although Authentication Manager continues to perform authentications during the backup process, authentication performance is slower. For this reason, backups should be done during non-peak hours. **Replica instance promotion.** You can promote a replica instance to the primary instance for disaster recovery, if the primary instance is unresponsive, or as a promotion for maintenance, if the primary instance is online and functioning. Promoting a replica instance in a deployment with a single replica instance suspends authentication until the promotion is complete. You can avoid suspending authentication by having at least two replica instances. **Reports.** Running a report can slow authentication performance if the report generates a large amount of data. You should run large reports during off-peak hours. **Batch Jobs.** Running daily batch jobs can also affect authentication performance. Batch jobs should be scheduled to limit impact on authentication.

Deployment Performance Factors

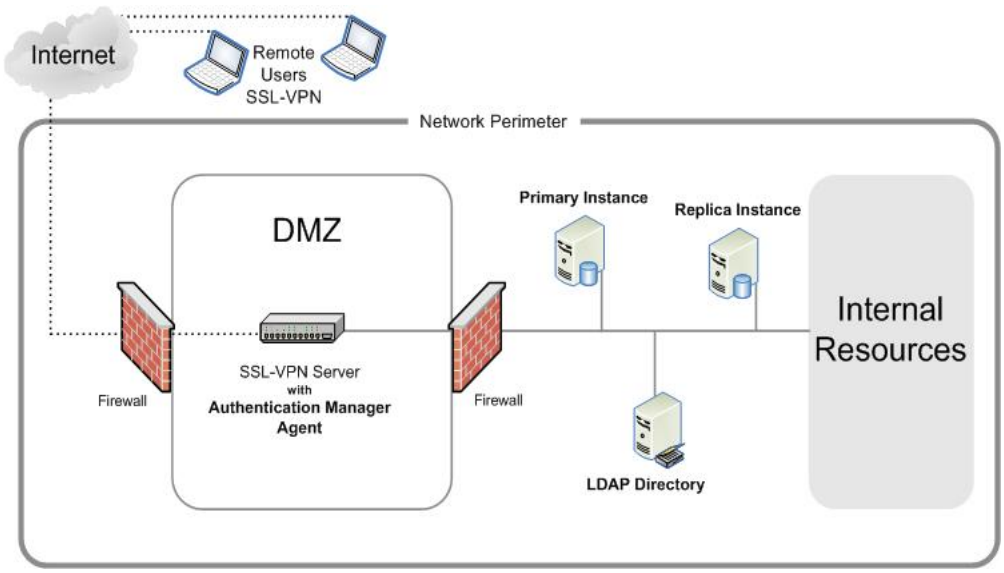
Authentication performance is affected by the way RSA Authentication Manageris deployed and maintained. Understanding the relationships among Authentication Manager components can help you organize your deployment for maximum efficiency and reliability.

Deployment Components

Because authentication protects critical resources, RSA Authentication Manager components should be deployed in a way that insures efficient, uninterrupted service and protection from unauthorized access.

For more information about Authentication Manager components, see the *Planning Guide.*

The following diagram shows a network protected by Authentication Manager.



The following table identifies each RSA Authentication Manager component and provides considerations for ensuring efficient authentication performance.

Component/Feature	Purpose	Performance Considerations
Primary instance	Authentication and administration	Authentication performance is affected by other installations running in the same environment as well as by the resources that are allocated for Authentication Manager.
(Optional but recommended) Replica instance	Authentication and redundancy The replica instance can be promoted to primary instance to recover administrative capacity if the primary instance becomes unavailable.	The Enterprise Edition license allows a maximum of 15 replicas to service a high volume of concurrent authentication requests. You can deploy replica instances in different geographic

Component/Feature	Purpose	Performance Considerations
		locations to provide authentication service that is physically close to users and authentication agents.
(Optional) Web tier	User provisioning and troubleshooting The web tier is the platform for Self-Service Console.	Although you can deploy a web tier on hardware that meets minimum requirements, RSA recommends that you adjust these requirements upwards based on expected usage. For more information, see the *Setup and Configuration Guide*.
(Optional) Self-Service Console	User provisioning and troubleshooting The Self-Service Console is a browser interface that enables users to update their profiles, change passwords for the Self-Service Console, configure life questions, clear devices enabled for risk-based authentication, change e-mail addresses or phone numbers for on-demand authentication, and manage on-demand authentication PINs. Users can also request, maintain, and troubleshoot tokens on the Self-Service Console.	Performance considerations provided for the web tier also apply to the Self-Service Console.
(Optional) Load balancer	Distribution of web tier traffic to the web tier servers	Perform periodic health checks to ensure efficient operation. For more information, see the *Setup and Configuration Guide*.
Authentication agent	Access control An authentication agent protects a resource by enabling authentication requests to Authentication Manager. Users must authenticate before they are allowed access to the protected resource.	After installation, maintain the agent by applying patches as they become available.
Cache	Quick access to recent data	Improve efficiency by managing the caching of system objects. For instructions, see the Security Console Help topic "Configure the Cache."
ClamAV	Virus detection ClamAV is an open source (GPL) antivirus engine for detecting Trojans, viruses, malware, and other threats. ClamAV is installed on each Authentication Manager instance.	Use ClamAV to scan an Authentication Manager instance for known malware. For instructions, see the *Administrator's Guide*.

Identity Source

Identity sources contain user and user group data. Although the RSA Authentication Manager internal database stores user data, most deployments leverage the organization's existing LDAP directory, such as the Oracle Directory Server or Microsoft Active Directory.

Several factors can affect the performance of an external identity source, and in turn, the performance of Authentication Manager. The following table identifies the identity source factors and provides considerations for obtaining maximum performance.

Factor	Performance Considerations
Location. Authentication Manager instances installed in a different geographic location from the directory server suffer from network latency or outages that are increased by distance.	Locating the Authentication Manager deployment near the directory server mitigates network latency and outages.
Server hardware. The efficiency of user authentications depends on quick transactions between Authentication Manager and the LDAP directory. If the directory is hosted on a slow server or on a server that hosts other applications that compete for server resources, transactions will be slow.	Performance is maximized if the LDAP directory is hosted on a dedicated, high-performance machine.
Directory Access. Even access to a fast directory imposes limitations on the number of transactions that can be performed per second. In large organizations, Authentication Manager must be able to fulfill a high number of authentication requests in a short amount of time.	Using Active Directory Global Catalog allows the Authentication Manager deployment to access multiple instances of the directory, which increases the efficiency of directory transactions. For information about setting up a Global Catalog for Authentication Manager, see the *Administrator's Guide*.

Network

The network infrastructure can affect authentication efficiency. The following table identifies network factors and provides suggestions for obtaining efficient performance.

Factor	Performance Considerations
Data exchange. A slow network can have a substantial impact on authentication performance.	For efficient performance, RSA recommends that you install Authentication Manager on a packet-switched network. This provides the most efficient exchange of data between Authentication Manager components.
Network latency. The time required for a data packet to travel through the network to its destination and for a return packet to arrive.	An organization with a headquarters and multiple remote sites can reduce the latency that is imposed by distance by placing a replica instance at each remote site. Authentication performance improves because users at each site are authenticating to the nearest instance. Although placing replica instances locally increases latency for replication with the primary instance, the replication load is significantly less than the authentication load, and the replication process can be distributed over a longer period of time. Another advantage of having a local replica is that if one replica instance fails, users at that site can still authenticate to another replica instance in the deployment. If the network connection between sites fails, users can still authenticate to the local replica instance.

RSA Authentication Manager Trusted Realm

A realm is an organizational unit that includes all of the objects managed within a single deployment, such as users and user groups, tokens, password policies, and agents. Each RSA Authentication Manager deployment

has only one realm.

You can create a trust relationship with another Authentication Manager realm, which allows users from one deployment to authenticate on another deployment. The first time users authenticate from a trusted realm, they will experience some delay because the users must be verified as trusted users on their home realm. After the first authentication, however, the users will no longer experience a delay because the authentication data is stored locally.

Custom Applications

You can develop custom applications to meet the needs of your organization, but a custom application can have unintended effects on authentication and the efficiency of the RSA Authentication Manager deployment.

Guidance for developing custom applications is provided in the *Developer's Guide*. For information about resolving problems you might experience, see the *Developer's Guide*.

If you experience performance problems after installing a custom application, RSA recommends that you disable or tune the application, and then reassess the performance of your deployment. If disabling the custom application improves performance, remove the application until you can permanently correct the problem. If performance problems persist, you may need to make other changes to your Authentication Manager deployment.

Automatic Tuning for the Virtual Appliance

When you deploy a virtual machine for RSA Authentication Manager 8.3, several internal server settings are automatically configured according to the amount of memory you choose for the machine. This automatic tuning optimizes the deployment's efficiency. If necessary, you can make additional adjustments to server settings or disable automatic tuning. Automatic tuning only applies to the Authentication Manager virtual appliance. The Authentication Manager hardware appliance is already configured for optimal performance. The hardware appliance does not support automatic tuning or memory configuration changes.

When you deploy a virtual machine for Authentication Manager, the default value for memory size is 8 GB. If you change the default memory size, Authentication Manager automatically tunes several internal server settings based on the following memory values:

- 4 GB
- 8 GB
- 16 GB
- 32 GB

If you choose more than 32 GB of memory, the machine is tuned using the 32 GB settings. If you choose fewer than 4 GB of memory, the system fails to start unless automatic tuning is disabled. If you need to run with less than 4 GB of memory, see *Modifying Authentication Manager Automatic Tuning Values for the Virtual Appliance.*

When the operating system starts, the memory control service starts and runs **configureMemory.sh** to detect the current system memory and make the following adjustments:

- Update and set **kernel.shmmax** and **kernel.shmall**
- Update JVM wrapper files for admin, biztier, console, and radiusOC
- Update postgresql.conf tuning parameters

Automatic Tuning Default Values

The following tables show the Weblogic and Postgres values that are automatically set for 4 GB, 8 GB, and 16 GB

of memory. RADIUS is not automatically tuned. For information about RADIUS configuration settings, see the *RADIUS Reference Guide*.

Weblogic Servers

Server	Setting	4 GB	8 GB	16 GB	32 GB
Admin Console (OC)	-Xmx	512	512	512	1024
RADIUS OC	-Xmx	100	100	100	100
Biztier (Runtime)	-Xmx	250	1024	1024	2048
Console	-Xmx	300	1024	1024	2048

Note: -Xmx typically uses an additional 50-100% OS memory in addition to this value. For example, a setting of -Xmx512mb typically uses 1GB of memory in the OS.

Postgres

postgresql.conf Settings	4 GB	8 GB	16 GB	32 GB
shared_buffers	960MB	1920MB	3840MB	7680MB
effective_cache_size	1GB	3GB	8GB	16GB
max_connections	200	200	200	200
work_mem	18MB	40MB	80MB	160MB
maintenance_work_mem	240MB	480MB	960MB	1920MB

Note: If you increase these values, you must also increase the corresponding **kernel.shmmax** and **kernel.shmall** in **/etc/sysctl.conf**.

SUSE OS

sysctl.conf Settings	4 GB	8 GB	16 GB	32 GB
kernel.shmmax	2077126656	4195561472	8431472640	17179869184
kernel.shmall	507111	1024307	2058465	4194304

Modifying Authentication Manager Automatic Tuning Values for the Virtual Appliance

You can disable or modify automatic configuration to meet the needs of your deployment. Automatic tuning only applies to the Authentication Manager virtual appliance. The Authentication Manager hardware appliance does not support automatic tuning or memory configuration changes.

Note: Making changes to automatic configuration can harm your deployment and should only be done by an administrator with expertise in database tuning. Be sure to make a copy of the original script before attempting any modifications.

Disable Automatic Configuration

You disable automatic configuration by modifying **memorycontrol** located at **/etc/init.d/memorycontrol**. This service cannot be disabled directly since it is part of the dependency chain, and other services will force it to start. To disable the auto configuration itself, you comment out the "config_memory" call in the script.

Before You Begin

This procedure should only be performed by an administrator with technical expertise. Make a copy of **memorycontrol** before you modify the file.

Procedure

1. Log on to the virtual machine operating system. For instructions, see the *Administrator's Guide*.
2. Change directories to **/etc/init.d/memorycontrol**.
3. Open **memorycontrol** in a text editor and comment out config_memory as shown in the following example:

```
case "$1" in
        start)
    #        config_memory
             mount_swap
             rc_status -v
             ;;
        stop)
             rc_status -v
             ;;
        *)
             echo "Usage: $0 {start|stop}"
             exit 1
             ;;
    esac
```

4. Save and close the **memorycontrol** file.

Permanently Change a Value

You can change the default settings by modifying the **configureMemory.sh** script located at **/opt/rsa/am/utils/bin/appliance/configureMemory.sh.**

Before you begin

This procedure should only be performed by an administrator with technical expertise. Make a copy of **configureMemory.sh** before you modify the script.

Procedure

1. Log on to the virtual machine operating system. For instructions, see the *Administrator's Guide*.
2. Change directories to **/opt/rsa/am/utils/bin/appliance/**.
3. Open **configureMemory.sh** in a text editor and enter your preferred values.
4. Save and close the **configureMemory.sh** file.

User Performance Factors

Authentication performance is affected by several user factors. Reviewing how and when users authenticate can help you organize your deployment for maximum efficiency and reliability.

User Location

Your RSA Authentication Manager deployment strategy should reflect the particular needs of your organization. For example, an organization whose members all work in the same building requires a different deployment strategy from an organization whose members are located in many different time zones.

The physical location of your primary and replica instances must balance performance with maintenance, security, and disaster recovery. For example, while it may be easier to upgrade or troubleshoot a complex deployment by having the primary instance and all the replica instances rack-mounted in the same room, authentication performance can suffer when all users must log on from geographically remote offices on a wide-area network (WAN).

You can improve performance and reliability by locating replica instances physically closer to the users who authenticate to them.

For example, in a corporation with multiple remote sites, the primary instance and one replica instance could be located in the corporate headquarters in New York, another replica instance could be located in the manufacturing facility in Mexico, and a third in a research laboratory in California.

Note: Because the deployment provides a critical service, the primary instance and all replica instances should be secured in a locked room that is accessible only by authorized personnel.

The following table presents three user location scenarios and the best type of deployment for each case.

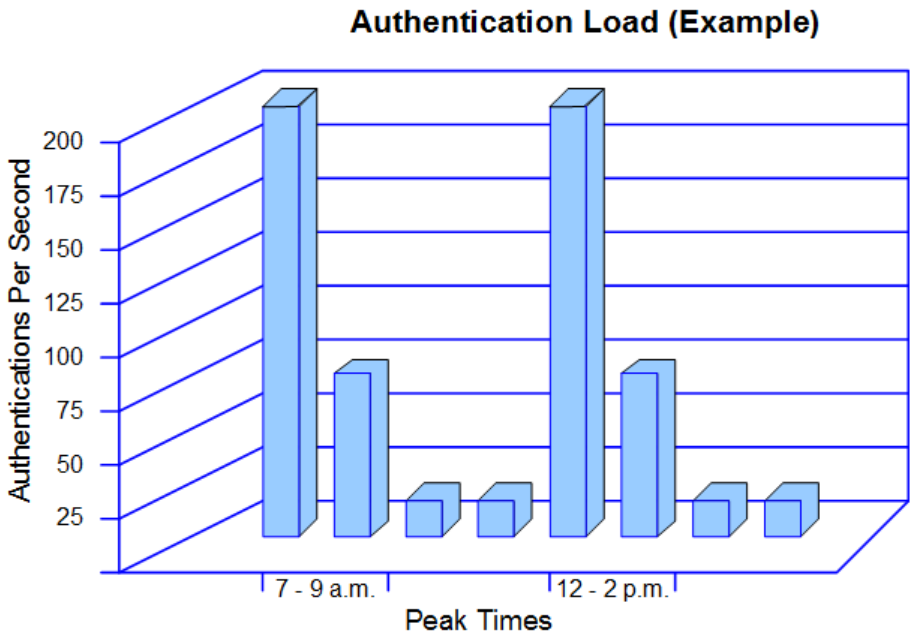
Location	Network	Suggested Deployment
Single location, for example, all users are in the same building or on a single campus.	Local-area network (LAN)	A primary instance and one replica instance that are physically separated, in order to maintain authentication service in the event of a physical disaster.
Multiple locations, for example, geographically separated buildings or campuses.	Two or more LANs connected by a WAN	A primary instance and remote replica instances. For example, the primary instance is deployed at the corporate headquarters and a replica instance is deployed at each remote office.
Multiple, widely-dispersed locations, for example, an internet service provider operating a web-based deployment.	WAN	A primary instance with multiple replica instances deployed at locations around the world.

Peak Authentication Times

Another user-related factor that can impact performance is the peak times at which users arrive at work, or return from lunch, and log on to the network.

For example, suppose most of your employees work in a single time zone and authenticate when they first arrive in the morning, and again after lunch. You would have a couple peak periods each work day during which users are authenticating to your network.

In a single shift, the peaks and valleys of the authentication load might look like the following graph.



When optimizing your deployment, it is important to consider the following questions:

- What are the peak periods during the day when most users are attempting to log on to the network?
- What is the maximum number of users that might log on during those peak periods?

Make sure your hardware can handle the expected peak authentication rates. For information about authentication throughput test results, see RSA Authentication Manager Performance Testing Overview on page 8.

Authentication Factors

Number of Users

When configuring your deployment for optimum performance, you must consider the size of your current user population and the anticipated size of your future user population.

For example, suppose your organization has 1,000 users, and you anticipate gradually adding another 100 users. A primary instance and one or two replica instances installed on hardware that meets the minimum system requirements is likely sufficient.

Suppose, however, that your organization has 75,000 users, and you expect to add another 15,000. In this case, you should consider a primary and multiple replica instances installed on hardware that meets or exceeds the minimum system requirements.

Make sure your hardware has enough excess capacity to handle the new users. You should also consider locating replica instances at remote sites where you have significant user populations to expedite the processing of authentication requests.

Authentication Frequency

If your user population authenticates frequently, make sure that you have enough storage space to accommodate Authentication Manager log files. A user population that authenticates frequently throughout the

day produces more log data than one that only authenticates at the beginning of the day. Establish a strategy for frequently archiving your log files. For more information, see Log Messages on page 29.

If an organization requires employees to begin their work day at a specific time, the authentication demand will be higher over a short period of time.

Remote Authentication

If a significant number of users access your network remotely, this may add noticeable overhead to network throughput.

Remote access typically requires a Remote Access Server (RAS) and associated software that is set up to service remote users. RAS configurations usually include or are associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

RAS devices are usually a component of a Virtual Private Network (VPN), which adds more overhead to your network. A VPN involves encrypting data before sending it through the public network, and decrypting the data at the receiving end. Some VPNs include an additional level of security by encrypting not only the data but also the originating and receiving network addresses, adding still more network overhead.

Note: If you have a Business Continuity license, remember that a large number of users may suddenly start authenticating remotely when the Business Continuity license is activated. Make sure that your hardware has enough excess capacity to support a sudden increase in the number of remote authentications.

Administration Performance Factors

RSA Authentication Managerprovides for delegated administration. You can create specific administrator roles to distribute administrative work. The following information identifies the performance impact of several administration activities and suggests ways to optimize authentication efficiency.

Administration Factors	Performance Considerations
Concurrent sessions. Because Authentication Manager provides for delegated administration, it is possible for many administrators to perform tasks at the same time.	It is possible for an excessive number of concurrent administrator sessions to cause a slowdown in authentication because of the demands placed on the deployment. Normally this does not occur.
User management. Administrative tasks that involve creating, reading, updating, and deleting users.	Mistakes made in the process of grooming the directory can deny access when users are unintentionally deleted or removed from a group. Great care must be exercised when directory changes are made so that users do not become unresolvable. For more information, see the *Administrator's Guide*.
Help Desk. An administrative role that helps users resolve authentication problems.	Users can lose their ability to authenticate for a variety of reasons. Access to a Help Desk administrator can be crucial in resolving access problems. If providing 24-hour coverage is not possible, you should consider installing a web tier in order to provide access to the Self-Service Console so that users can resolve authentication problems on their own.
Large Reports. Although small reports can be run during hours of normal authentication volume, large reports can challenge deployment resources and impact the efficiency of authentication.	Large reports should be run during off-peak hours. For example, a small report requesting a list of administrators who logged on between 8:00 a.m and 5:00 p.m. the previous day can safely be run during normal business hours. However, a report of all authentications or administration activity taking place during a month would likely be very large and should only be run during off-peak hours.
Backups. Regular backups are essential to recovering the deployment if something goes wrong, but the backup process competes for deployment resources and slows authentication performance.	Backups should only be scheduled during off-peak hours.
Disaster recovery. Restoring a primary instance or replacing a replica instance to recover from a loss of service can cause an authentication service outage.	Make sure your deployment has sufficient instances installed to provide authentication while repairs are made. If the deployment does not have a replica instance, no authentication can take place while the primary instance is repaired.

Chapter 3: Performance Monitoring

Performance Monitoring Overview

RSA Authentication Managerprovides several ways to monitor the performance of a deployment. The activity data from logs, reports, and SNMP statistics provide useful information that can help you troubleshoot performance problems. These are just a few examples of how performance data can help you locate and resolve deployment problems.

- If user authentication is slow, you can use the Real-Time Activity Monitors to view authentication activity log messages in real time to see the problem as it is happening.
- If user authentication is slow, you might also use Authentication Manager logs to help you determine whether the delay is due to a slow response from the LDAP directory or a processor-intensive process that Authentication Manager is performing that might be better performed during off-peak hours.
- To view specific log data, set up and run a report to collect activity data for a given time frame. For example, the report might include all authentications that took place during a specified time frame and which instances performed the authentications, to see whether the authentication work is distributed evenly.
- If you have a third-party Network Management System (NMS), you can keep track of activity that occurs in your production environment. This allows you to respond to problems as they happen.

Note: For more information about viewing deployment activity, see the RSA Authentication Manager Help. The Help is available in the Security Console, the Operations Console, and on RSA Link.

Activity Monitors

Activity Monitors help you locate performance problems in the deployment. Activity Monitors let you view RSA Authentication Managerlog activity in real time. To access the Activity Monitors on the Security Console, click **Reporting > Real-time Activity Monitors**.

RSA Authentication Managerprovides four Activity Monitors. Each Activity Monitor opens in a separate browser window and displays a different type of information.

Monitor	Information Displayed
Authentication Activity	• Which user is authenticating • Source of the authentication request • Server used for authentication
System Activity	• Time of an activity • Description of activity • Whether the activity succeeded • Server where the activity took place
Administration Activity	• Changes to user data, such as when users are added or deleted.
Runtime Activity Monitor in the User Dashboard	• Log entries for real-time authentication activity over the past seven days for one user • Time of activity, result of activity, and description of activity

Note: A large number of administrators running real-time Activity Monitors can use significant system resources and slow performance. To avoid slowdowns, RSA recommends that you limit the number of Activity Monitors that are active at the same time.

Log Messages

RSA Authentication Manager generates log messages for all events. These messages are stored in log and database files according to the origin of the message. You can use these log files to monitor deployment activity and produce a record of events such as user logon requests or administrative operations.

Most log settings are instance-based, unless you choose to replicate logging configuration changes. The exception is log rotation settings, which are configured in the Operations Console on each instance.

The system does not log most successful read actions.

Log Types

Authentication Manager maintains the following types of logs:

- **Trace.** Log messages that you can use to debug your system.
- **Administrative Audit.** Log messages that record administrative actions, such as adding and editing users. This category does not include system level failures of administrative actions. Those messages are captured in the system log.
- **Runtime Audit**. Log messages that record any runtime activity, such as authentication and authorization of users.
- **System**. System level messages, such as "Server started" and "Connection Manager lost db connection." This category includes system level failures of administrative actions.

Trace log messages are written locally to the appliance file system. The Administrative Audit, Runtime Audit, and System Audit log messages for each appliance are recorded in the Authentication Manager internal database and consolidated on the primary instance.

Logging Levels

For each type of log, you can use the Security Console to configure the level of detail written to the log files. For example, you might choose to record only fatal errors in the Administrative Audit log, while recording all messages in the System log.

If you change the logging levels and want to return to the default values, select the values listed in the following table.

Log	Default Setting
Trace Log	Fatal
Administrative Audit Log	Success
Runtime Audit Log	Success
System Log	Warning

Reports

Reports provide access to logged information, and current information about the users, administrators, and system activity in a deployment. You create a report using one of the supplied templates. Each template allows you to choose the types of information being reported and the parameters to apply in order to refine that information.

After you have created and saved a report, an administrator can run the report manually at any time. You can also schedule the report to run automatically on a given day and time. You can view the report output in the Security Console, or download the report as a CSV, XML, or HTML file.

Reports provide information about the performance of your deployment. For example, you might create a report that shows all of the administrative activity occurring during peak working hours. You can design a report so that it includes relevant information such as date and time, description, instance name, identity source, and security domain. You can then analyze the report to make sure there are no CPU or memory-intensive operations being performed during peak hours.

You might also create a report that shows all the authentications during a 24-hour period of time. You can use the report to determine when your peak authentication time is, as well as the number of authentications that took place at that peak. You can also use the report to determine which instances are processing each authentication. This helps you determine if your deployment is load balanced properly.

Note: Be aware that running reports uses significant system resources and can slow the performance of your deployment. RSA recommends that you schedule reports to run during off-peak hours. For test data, see Agent Reporting on page 11.

SNMP Overview

RSA Authentication Manager supports a third-party network management system (NMS) using Simple Network Management Protocol (SNMP). An NMS reveals how Authentication Manager is functioning in a production environment, making it easier to configure the deployment for optimal performance.

You can define the information that you want an NMS to provide by specifying GETS and traps. The NMS requests information using GETS and receives messages that are triggered by traps. The NMS obtains network information from the Management Information Base (MIB).

GETS and traps differ in two ways:

- A GET requests information, whereas a trap automatically sends information.
- A GET is composed of aggregate data, but a trap is an individual piece of data.

For example, assume that Authentication Manager is configured to send a notification each time a successful authentication occurs. If there are 100 successful authentications, 100 trap messages are sent. If you were to do a GET for successful authentications, you would receive one message showing a value of 100.

You can configure the NMS to receive Authentication Manager error, warning, or success notifications. Notifications can be intercepted and filtered based on the data sent in the trap message (message ID, for example).

You can also set traps to monitor disk usage, memory usage, and the CPU system load. You can select an interval at which to check the instance and send a notification to the NMS if too many resources are being used.

SNMP settings are instance-based. Changes that you make to one instance do not affect the other instances.

In Authentication Manager, SNMP obtains values only from the internal database, not from external identity sources. For example, suppose you have 2000 users in an external identity source but only 1000 users in the Authentication Manager internal database. If you have a GET for the total number of users, the value returned is 1000.