RSA Ready Implementation Guide for RSA SecurID

VMware vSphere Management Assistant 6.0

Daniel Pintal, RSA Partner Engineering
Last Modified: July 20th, 2016

RSA READY

Solution Summary

VMware vSphere Management Assistant (vMA) leverages the RSA Authentication Agent 7.0 for Pluggable Authentication Module (PAM) enabling RSA SecurID authentication using either standard or OpenSSH connection tools.

RSA Authentication Manager supported features	
vSphere Management Assistant 6.0	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the vSphere Management Assistant and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the vSphere Management Assistant and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.

Support for TCP and IPv6 is not available in RSA PAM.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the vSphere Management Assistant with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vSphere Management Assistant components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Installing the PAM Agent

Installing the PAM Agent involves setting up your environment and running an installation script.

Setting Up Your Environment

Before you perform the installation, verify that:

- You have root access for the vSphere Management Assistant server.
- You have uploaded the **PAM-Agent_v7.1.0.1.25_RHEL.tar** and **sdconf.rec** file to vSphere vMA.
- You have created an Agent Host record for the vMA Server in the RSA Authentication Manager database. For more information, see the RSA Authentication Manager documentation.
- You have created corresponding accounts on both the vMA and RSA Authentication Manager servers.

PAM Agent Installation:

1. Upload the **PAM-Agent_v7.1.0.1.25_RHEL.tar** and **sdconf.rec** file from your RSA AM to vSphere vMA 6 server.
2. Login as vi-admin.
3. Run the following command to enable root and set the password for the root account.

   ```
   sudo passwd root
   ```

4. Run the following command to enable vi-user and set the password for the vi-user account.

   ```
   sudo passwd vi-user
   ```

5. Run the following command to access root for the vMA server.

   ```
   sudo su
   ```

6. Run the following command to **access root** for the vMA server.

   ```
   md /var/ace
   ```

7. Place a copy of the **sdconf.rec** file in **/var/ace**.

8. Change the directory to the folder where you copied the RSA PAM Agent software and unzip the PAM-Agent_v7.1.0.1.25_RHEL.tar.gz file.

   ```
   gzip –d PAM-Agent_v7.1.0.1.25_RHEL.tar.gz
   ```

9. Extract the PAM-Agent_v7.1.0.1.25_RHEL.tar file.

   ```
   tar -xvf PAM-Agent_v7.1.0.1.25_RHEL.tar
   ```

10. Change the directory to the folder created when extracting the PAM Agent tar and run the install script from the folder created when extracting the PAM Agent.

    ```
    ./install_pam.sh
    ```

11. Follow the installation prompts, when prompted specify the directory in which you stored the **sdconf.rec** file. If the path is correct, press **ENTER**.
12. For each of the remaining prompt, press **ENTER** to accept the default value.
13. Modify the **/etc/hosts** file, removing the loopback entry replacing it with the primary network interface ip address, include the domain name for correct hosts file configuration.

Performing a Test Authentication

RSA recommends that you perform a simple test authentication to ensure that the PAM Agent is functioning properly. You must use a token with a PIN that is already registered in the RSA Authentication Manager database. Follow the New PIN procedure for proper registration. For additional information, contact your RSA Authentication Manager administrator.

To perform a test authentication:

1. Change your directory to **/opt/pam/bin/64bit** and type:

   ```
   ./acetest
   ```

2. Enter your user name and passcode.

> **Important: If you fail to authenticate, contact your RSA Authentication Manager administrator.**

Configuring the PAM Agent

Before you make any configuration changes, make backup copies of the original configuration files.

> **Important: Open a new SSH session using a standard user account to test SecurID authentication. Leave the first SSH connection open into the vMA server to prevent being locked out of the console.**

Multiple configuration files are located in the **/etc/pam.d** directory. Each file uses the name of the connection tool.

1. Change your directory to **/etc/pam.d**.
2. Edit the **sshd** file and modify the sshd configuration as follows:

```
#%PAM-1.0
auth       required     pam_securid.so
#auth      requisite    pam_nologin.so
#auth      include      common-auth
account    requisite    pam_nologin.so
account    include      common-account
password   include      common-password
session    required     pam_loginuid.so
session    include      common-session
```

Configuring OpenSSH

To display passcode authentication messages:

1. Edit the **sshd_config** file located in the **/etc/ssh** folder and make the following changes.
2. Locate and modify the setting below;

```
UsePAM yes
PasswordAuthentication no
```

> **Important: Setting the PasswordAuthentication parameter to no disables the OpenSSH password prompt so that the PAM Agent prompts for authentication. As a result, the user is prompted for an RSA SecurID passcode only.**

3. Locate and modify the setting below;

```
UsePrivilegeSeparation no
ChallengeResponseAuthentication yes
```

> **Important: Setting the ChallengeResponseAuthentication parameter to no causes authentication to fail. Make sure that this parameter is always set to yes.**

4. Restart the SSHD process.

```
/etc/init.d/sshd restart
```

RSA SecurID Login Screens

Login screen:

```
login as:
```

User-defined New PIN:

```
login as: d_pintal

Welcome to SUSE Linux Enterprise Server 11 SP3 for VMware  (x86_64) - Kernel \r
(\l).


Using keyboard-interactive authentication.
Enter PASSCODE:
Using keyboard-interactive authentication.
To continue you must enter a new PIN. Are you ready to enter a new PIN? (y/n) [n
]: y
Using keyboard-interactive authentication.
Enter a new PIN between 4 and 8 alphanumeric characters:
Using keyboard-interactive authentication.
Re-enter new PIN to confirm:
Using keyboard-interactive authentication.
New PIN accepted, press enter to continue.
```

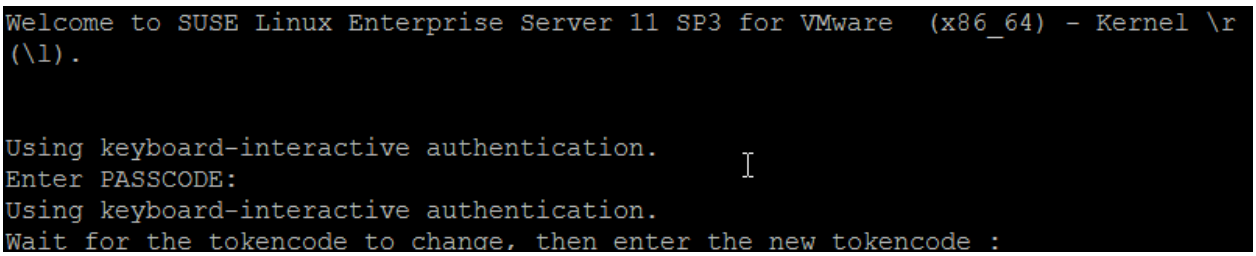
System-generated New PIN:

```
login as: d_pintal

Welcome to SUSE Linux Enterprise Server 11 SP3 for VMware  (x86_64) - Kernel \r
(\l).


Using keyboard-interactive authentication.
Enter PASSCODE:
Using keyboard-interactive authentication.
To continue, you must accept a new PIN generated by the system. Are you ready to
 have the system generate your PIN? (y/n) [n]: y
Using keyboard-interactive authentication.
Press enter and your screen will automatically clear in 10 seconds. Your new PIN
 is: eQTg
```

Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: July 20th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
RSA Authentication PAM Agent	7.1.0.1.25	SUSE Linux
VMware vSphere Management Assistant	6.0.0.1	SUSE Linux

RSA SecurID Authentication

Date Tested: July 20th, 2016

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	✓	N/A	N/A
System Generated PIN	✓	N/A	N/A
User Defined (4-8 Alphanumeric)	✓	N/A	N/A
User Defined (5-7 Numeric)	✓	N/A	N/A
Deny 4 and 8 Digit PIN	✓	N/A	N/A
Deny Alphanumeric PIN	✓	N/A	N/A
Deny PIN Reuse	✓	N/A	N/A
Passcode			
16 Digit Passcode	✓	N/A	N/A
4 Digit Fixed Passcode	✓	N/A	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	N/A	N/A
On-Demand Authentication			
On-Demand Authentication	✓	N/A	N/A
On-Demand New PIN	✓	N/A	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	N/A	N/A
No RSA Authentication Manager	✓	N/A	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	/var/ace
sdopts.rec	/var/ace
Node secret	/var/ace
sdstatus.12 / jastatus.12	/var/ace

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	8.1
RSA SecurID TCP API	NA
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Default Method
Display RSA Server Info	Yes
Perform Test Authentication	Yes
Agent Tracing	Yes

Node Secret:

Clearing the Node Secret is performed by logging in as ROOT and deleting the **/var/ace/securid** file.

sdconf.rec:

Clearing the SDCONF.REC file is performed by logging in as ROOT and deleting the **/var/ace/sdconf.rec** file.

sdopts.rec:

Clearing the SDOPTS.REC file is performed by logging in as ROOT and deleting the **/var/ace/sdopts.rec** file.

sdstatus.12:

Clearing the SDSTATUS.12 file is performed by logging in as ROOT and deleting the **/var/ace/sdstatus.12** file.

Agent Tracing:

Enable Debug Output

To enable debug output for the PAM agent, edit the configuration file by adding a debug argument as described below.

To enable debug output for the PAM agent

1. Change to **/etc/pam.d**
2. Edit the appropriate file by adding a debug argument for the pam_securid.so module.

```
auth required pam_securid.so debug
```

Enable SecurID Trace Logging

To enable the level of logging for the PAM agent and for the authentication utilities acetest and acestatus, set the following variable in the **/etc/sd_pam.conf** file.

```
RSATRACELEVEL=<value>
```

This variable enables detailed agent logging and sets the level of logging. The default value is 0.

Important: For combinations, add the corresponding values.

Value	Description
0	Disables logging
1	Logs regular messages
2	Logs function entry points
4	Logs function exit points
8	All logic flow controls use this (ifs)

Enable SecurID Trace Logging (cont.)

To enable output of the event logging for the PAM agent and for the authentication utilities acetest and acestatus, set the following variable in the /etc/sd_pam.conf file.

```
RSATRACEDEST=<filepath>
```

Specify the file path where the logs must be redirected. By default this is blank. If you do not set this variable in **/etc/sd_pam.conf,** the logs go to standard error for authentication utilities acetest and acestatus, and no logs are generated for authentication tools, even if the RSATRACELEVEL value has been specified.

Important: Default values refer to values when the agent is installed.