Deploying SecureCloud SaaS in a vCloud Environment

Securing Your Journey to the Cloud

Trend Micro™ SecureCloud

A Trend Micro & VMware White Paper

August 2011

DEPLOYING SECURECLOUD SAAS IN A VCLOUD ENVIRONMENT

I. EXECUTIVE SUMMARY

This is the second paper of a series of two and will focus on instructions for deploying Trend Micro™ SecureCloud™ in a VMware vCloud™ environment. It is intended for use in virtualized environments that have VMware vCloud Director to manage private cClouds; it is not intended to be used as an installation and administrative guide. For additional installation and administrative instructions, please refer to our online resources at the Trend Micro website. http://downloadcenter.trendmicro.com/

SecureCloud provides data protection and encryption key management for cloud environments. Data is encrypted on a virtual machine before being written to any SCSI, iSCSI, NFS, or IDE storage device and decrypted when read back. The symmetric keys for the encryption process are managed by the SecureCloud Key Manager—which is available as a hosted service from Trend Micro or can be installed within your own data center. SecureCloud's unique policy-based key management allows it to ensure encryption keys are released only into safe cloud environments via identity and integrity checks. This is achieved by applying numerous rules to key release decisions—such as checking what network services are running within the virtual machine—which help SecureCloud assess the cloud environment's identity and integrity.

II. TRIAL SIGN UP

A trial license is required to test SecureCloud. To obtain a trial license, complete the trial form available on the Trend Micro trial website for SecureCloud. When completing the trial form, be sure to choose SecureCloud Hosted Services.

SecureCloud Trial form: http://forms.trendmicro.com/index.php?dom=us&productID=125

You will receive an activation code once the trial form has been completed. This trial activation code is required later to allow the SecureCloud Management Server to generate encryption keys.

III. SECURECLOUD REGISTRATION

A SecureCloud account is required to download and install software. The SecureCloud registration page may be accessed directly from the SecureCloud Web Console Log On screen at: https://console.securecloud.com

From the SecureCloud Web Console Log On page, follow the *Click here* link to open the Registration page.

Enter a first and last name for the account, email address and password. A company name may also be entered if desired.

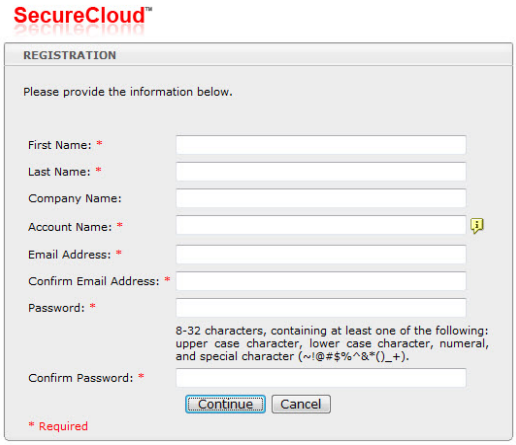


Figure 1: SecureCloud Registration Screen

After successfully completing the registration form, Trend Micro will send a Registration Verification email to the address provided. The email contains instructions for completing the SecureCloud registration.

IV. SECURECLOUD ACTIVATION

The SecureCloud account must be activivated the first time the SecureCloud Web console is opened. SecureCloud will not be able to issue encryption keys without a valid Activation Code.

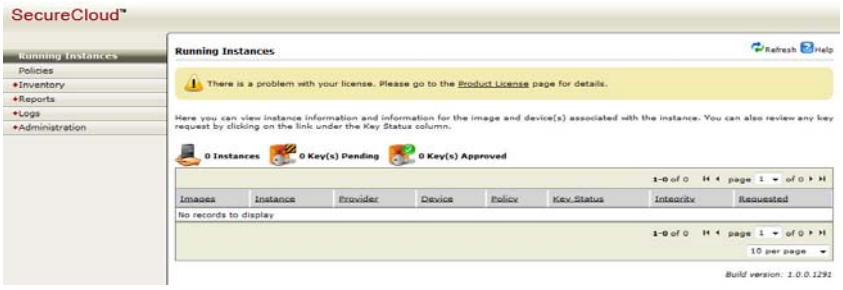


Figure 2: First SecureCloud Web Console Login

The first time the console opens, it will display a warning message at the top of the screen, stating “There is a problem with your license Please go to the Product License page for details.” This message simply indicates that the account Account ID created during the registration process has not been activated. Click the Product License link to open the Licenses screen.

Figure 3: Administration -> Licenses Screen

The Licenses screen contains information about the SecureCloud account. The status line will show a red icon with the status listed as the product has not been activated the first time Web Console is opened. . The necessary activation code will have been sent to the email address provided during trial registration. Find the email titled “Trend Micro SecureCloud Trial Confirmation”.

V. DEPLOYING SECURECLOUD WITH CENTOS 5.5

The SecureCloud Runtime Agent is the software module that is installed on a virtual machine image within a cloud service provider’s environment. The SecureCloud Runtime Agent provides identity and integrity check functionality of the virtual machine.

Before installing the SecureCloud Runtime Agent make sure of the following:

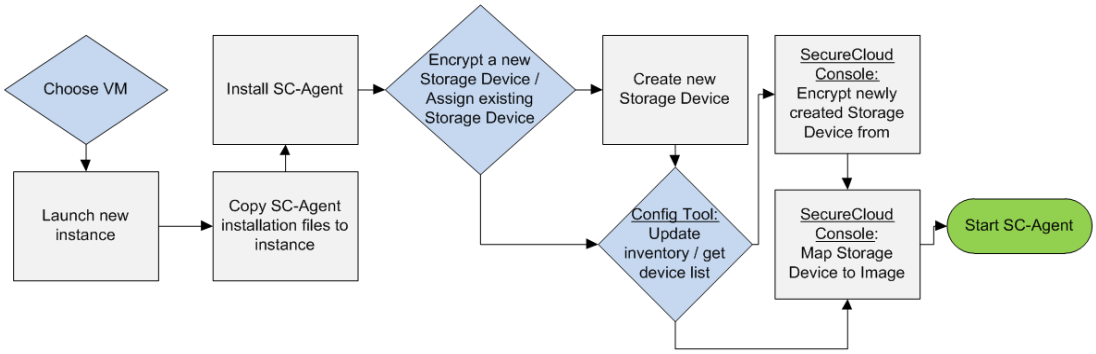
1. An additional disk has been added to the virtual machine.
2. The minimum version of cryptsetup is 1.0.07.

If required, upgrade the cryptsetup from 1.0.3 to 1.0.7 by following solution script:

```
yum -y install gcc automake autoconf libtool make e2fsprogs-devel
wget http://cryptsetup.googlecode.com/files/cryptsetup-1.0.7.tar.bz2
tar -jxvf cryptsetup-1.0.7.tar.bz2
cd cryptsetup-1.0.7
./configure
make
make install
mv /sbin/cryptsetup /sbin/cryptsetup_bak
cp /usr/sbin/cryptsetup /sbin/cryptsetup
```

DEPLOYING SECURECLOUD SAAS IN A VCLOUD ENVIRONMENT

The following workflow outlines the basic procedure to setup SecureCloud and provision a new storage device for encryption.



INSTALLING SECURECLOUD

1. Logon to the SecureCloud Management Console and gather the appropriate information needed during the installation procedure.

   - Note your SecureCloud "Account ID" number.
   - Note your user passphrase

2. SecureCloud Account ID and passphrase can be found in the SecureCloud Management Console, on the Administration -> Account Management screen.

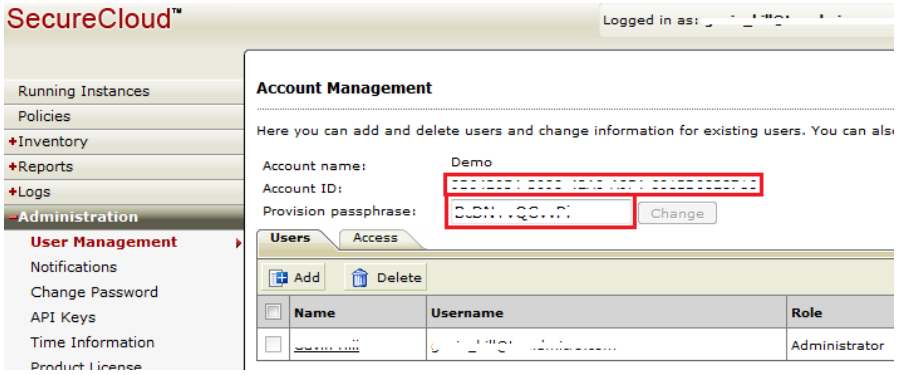


Figure 4: Administration -> Account Management Screen (SecureCloud Account ID)

3. Download the appropriate SecureCloud Agent from the Trend Micro Download Center to the virtual machine instance that the Runtime Agent will be installed on.

   http://downloadcenter.trendmicro.com/

4. Install the SecureCloud Runtime Agent by executing the command:

   rpm -ivh <scagnet-xxx.rpm>

   <scagent-xxx.rpm> is the name of the installation package you downloaded from the download center.

UPDATE INVENTORY TO SECURECLOUD MANAGEMENT SERVER

1. Run the configuration tool once the installation is successful. To do so, run the command:

   /var/lib/securecloud/scconfig.sh

2. Choose vCloud as the Cloud Service Provider that the instance is running on.
3. Input the Cloud Controller Address.
4. Input the Organization Name, user name and password.
5. Input the SecureCloud Management Server Web Service URL when prompted – This is not necessary since in this exercise you will be using the SecureCloud SaaS; this is a necessary step if installing the on-premise deployment model. Input the SecureCloud Management Server User Passphrase that was noted in step 1.
6. Enter "yes" to the prompt, "Do you want to update inventory?"
7. Enter "yes" to the prompt, "Do you want to wait for provisioning?"
8. Accept the default timeout setting for provisioning process.
9. Enter "yes" to the prompt, "Do you want to get mount device list?"

ENCRYPT THE DATA STORAGE DEVICE

1. Logon to the SecureCloud Management Console to configure the Data Storage. Click on the Device to be encrypted as shown in the Inventory -> Devices.

Figure 5: Inventory -> Devices – Not Configured

2. On the device page, in the "Device Information" area, change the following:
   - Platform/file system: linux ext3
   - Write access: Read/Write
   - Mount point: /encrypted
3. Save the configuration by clicking “Save”.
4. You will note that the target device status changes to “Configured”.
5. Select the checkbox for the device to be encrypted and click “Encrypt”.

Figure 6: Inventory -> Devices – Configured

6. Wait for the Configuration Tool to finish provisioning the device(s). When the provision process is complete, refresh the device list. The target device(s) will now have the "Encrypted" status.
7. Start the SecureCloud Agent service. To do so, run the command:

   Service scagentd start

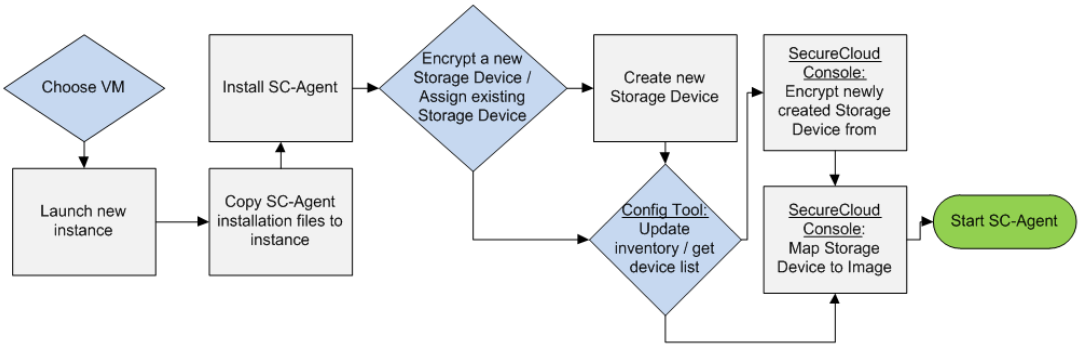
VI. DEPLOYING SECURECLOUD WITH WINDOWS 2008

The SecureCloud Runtime Agent is the software module that is installed on your virtual machine image within the cloud service provider’s environment. The SecureCloud Runtime Agent provides identity and integrity check functionality of the VM.

Before installing the SecureCloud Runtime Agent make sure an additional disk has been added to the virtual machine.

DEPLOYING SECURECLOUD SAAS IN A VCLOUD ENVIRONMENT

The following workflow outlines the basic procedure to setup SecureCloud and provision a new storage device for encryption.



INSTALLING SECURECLOUD

1. Logon to the SecureCloud Management Console and gather the appropriate information needed during the installation procedure.

    - Note the SecureCloud "Account ID" number.
    - Note the user passphrase

2. SecureCloud Account ID and passphrase can be found in the SecureCloud Management Console, on the Administration -> Account Management screen.

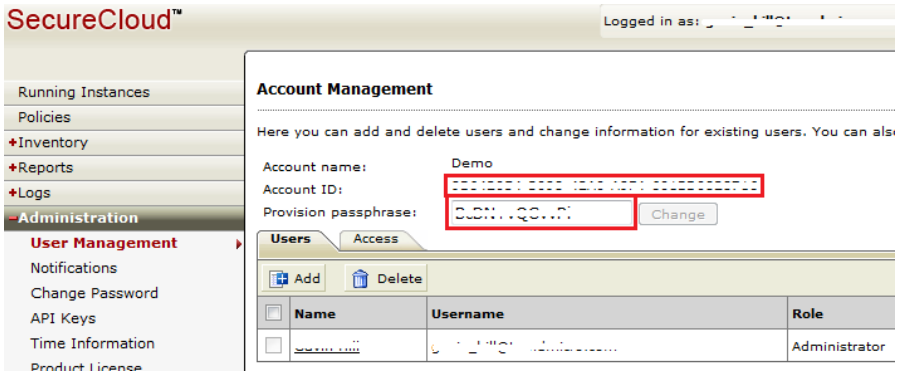


Figure 7: Administration -> Account Management Screen (SecureCloud Account ID)

3. Download the appropriate SecureCloud Agent from the Trend Micro Download Center to the virtual machine instance that you will be installing the Runtime Agent on.

    http://downloadcenter.trendmicro.com/

4. Extract the installation package and run "InstallationWizard.exe" and then follow the on-screen instructions.

UPDATE INVENTORY TO SECURECLOUD MANAGEMENT SERVER

1. Run the configuration tool once the installation is successful, Start Menu under "All Programs > Trend Micro SecureCloud Agent > Configuration Tool"
2. Choose vCloud as the Cloud Service Provider that the instance is running on.
3. Input the Cloud Controller Address.
4. Input the Organization Name, user name and password.
5. Input the SecureCloud Management Server Web Service URL when prompted – This is not necessary since in this exercise you will be using the SecureCloud SaaS; this is a necessary step if installing the on-premise deployment model. Input the SecureCloud Management Server User Passphrase that was noted in step 1.
6. nter "yes" to the prompt, "Do you want to update inventory?"
7. Enter "yes" to the prompt, "Do you want to wait for provisioning?"
8. Accept the default timeout setting for provisioning process.
9. Enter "yes" to the prompt, "Do you want to get mount device list?"

ENCRYPT THE DATA STORAGE DEVICE

1. Logon to the SecureCloud Management Console to configure the Data Storage. Click on the Device to be encrypted as shown in the Inventory -> Devices.

Figure 8: Inventory -> Devices – Not Configured

2. On the device page, in the "Device Information" area, change the following:
   - Platform/file system: Windows NTFS
   - Write access: Read/Write
   - Mount point: G
3. Save the configuration by clicking “Save”.
4. You will note the target device status changes to “Configured”.
5. Select the checkbox for the device to be encrypted and click “Encrypt”.

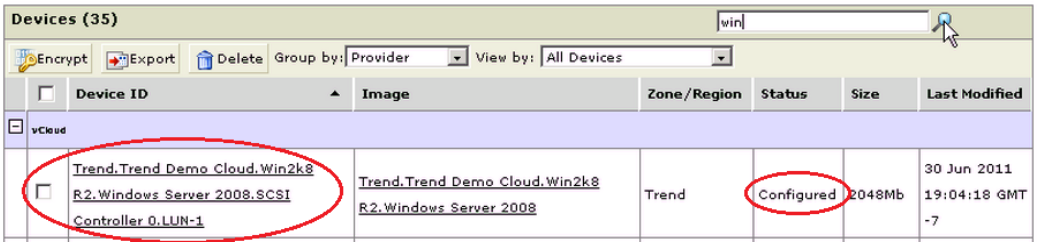


Figure 9: Inventory -> Devices – Configured

6. Wait for the Configuration Tool to finish provisioning the device(s). When the provision process is complete, refresh the device list. The target device(s) will now have the "Encrypted" status.

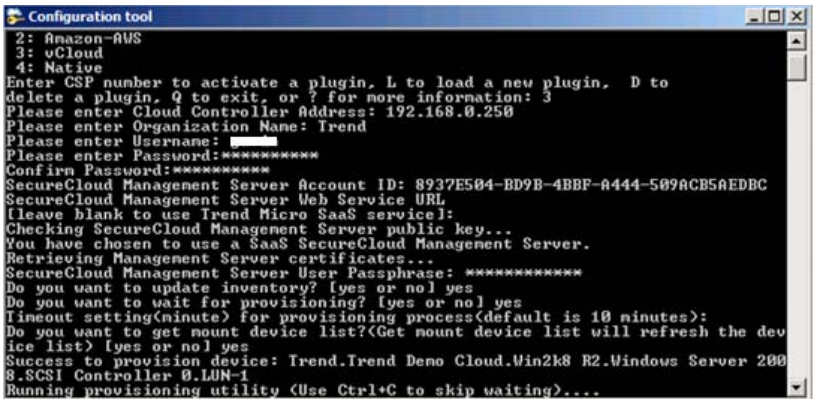


Figure 11: Configuration Tool

7. Start the SecureCloud Agent service from the service panel.

VII. CONCLUSION

The steps described in this document have been provided to outline to perform the basic setup of SecureCloud SaaS. Please refer to the SecureCloud Administrators Guide for complete details on all SecureCloud functionality, which is available at http://downloadcenter.trendmicro.com/.

©2011 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WP01_CloudSecurity_110812US]