SYMANTEC CRITICAL PROTECTION SYSTEM

Linux Agent Installation in Prevention Mode

Version 1.0

19th December 2013

Central IT- ISG

COPYRIGHT INFORMATION

DOCUMENT CONTROL INFORMATION

Document Name	Linux Agent Installation in Prevention Mode
Document Version	1.0
Document Version Date	19th December 2013
Originator(s)	Maya Mishra
Peer reviewer(s)	Shivani Deshpande, Pulkit Maheshwari
Reviewer(s)	Shilpa Sawant, Sam Varughese
Approver(s)	Sh. Durga Dube
Last Review Date	19th December 2013
Next Review Date	December 2014
Document Maintainer(s)	Maya.mishra@ril.com

REVISION HISTORY

Please keep the latest version on top

Ver.	Change Description	Sections	Date	Author	Reviewer(s)	Approver(s)
1.0	Initial Document Creation		19th Dec 2013	Central IT - ISG	Shilpa Sawant, Sam Varughese	Sh. Durga Dube

REFERENCES

Reader should read this document in conjunction with the following documents

No	Document Name	Ver.	Location
1.		NA	
2.		NA	

ABOUT THIS DOCUMENT

This document describes the technical deployment aspects of implementing Symantec Critical System Protection (SCSP) system in the Reliance environment. These include the agent installation and configuration of linux agent in detection mode. This document is part of the base reference material regards the implementation of SCSP in Reliance

AUDIENCE

This document is intended for the HIPS administrators and information security staff, management and other personnel wants to obtain and understand the technical aspects of the HIPS deployment in Reliance.

DOCUMENT LOCATION

http://it.ril.com/isg/InfoSecurity Project Repository/HIPS_FIM/Implementation Documentation

CONFIDENTIALITY NOTE

This document is classified as confidential and should be accessed only by authorized personnel. The document contain detailed specification, actual configuration values and other aspects that are deemed confidential and critical for the secure operations of the HIPS system. Strictest form of action will be taken against users who are in violation of the confidentiality requirements of this document.

Definitions, Abbreviation and Acronyms

The terms in use in the document are explained below

Acronym		Description
SCSP	Symantec Critical Protection System	
HIPS	Host Intrusion Prevention System	
HA	High Availability	

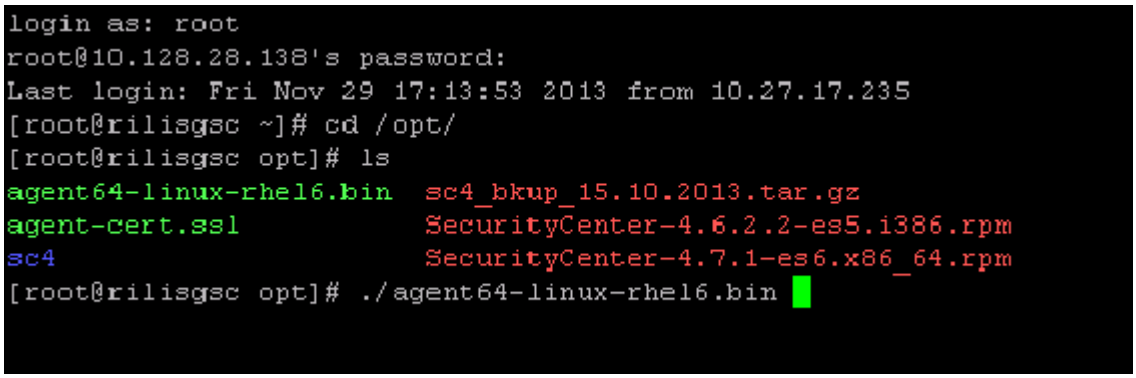
Table of Contents

Contents

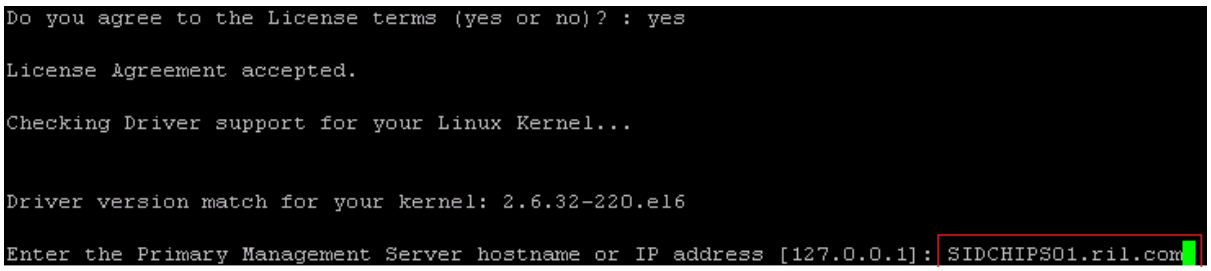
1 LINUX AGENT INSTALLATION IN PREVENTION MODE

Copy and keep two files agent64-linux-rhel6.bin and agent-cert.ssl files on the remote machine where agent is to be installed.
Ensure SELinux is set to Permissive mode.

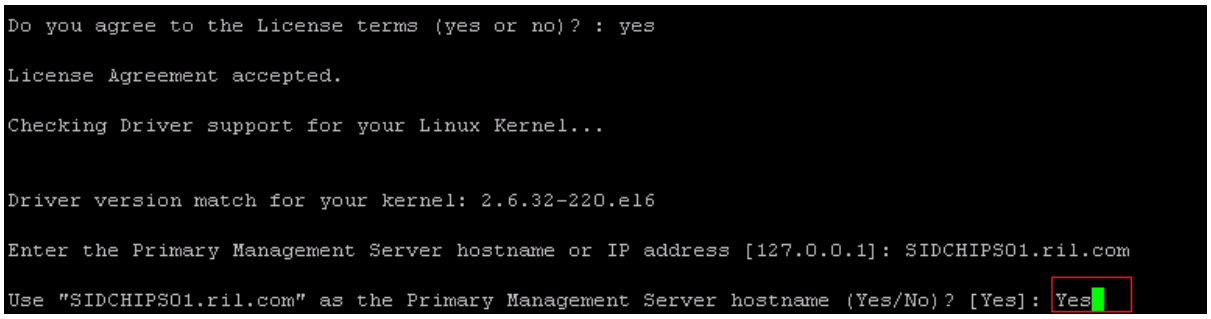
1. Install linux agent "agent64-linux-rhel6.bin"



2. Accept the license and enter hostname of the Primary Management Server



3. Enter Yes



4. Enter the path where "agent-cert.ssl" file is located.

```
Do you agree to the License terms (yes or no)? : yes

License Agreement accepted.

Checking Driver support for your Linux Kernel...


Driver version match for your kernel: 2.6.32-220.el6

Enter the Primary Management Server hostname or IP address [127.0.0.1]: SIDCHIPSO1.ril.com

Use "SIDCHIPSO1.ril.com" as the Primary Management Server hostname (Yes/No)? [Yes]: Yes


Enter Path to Management Server Certificate [/tmp/agent-cert.ssl]: /opt/agent-cert.ssl
```

5. Enter the Agent Name

```
Driver version match for your kernel: 2.6.32-220.el6

Enter the Primary Management Server hostname or IP address [127.0.0.1]: SIDCHIPSO1.ril.com

Use "SIDCHIPSO1.ril.com" as the Primary Management Server hostname (Yes/No)? [Yes]: Yes


Enter Path to Management Server Certificate [/tmp/agent-cert.ssl]: /opt/agent-cert.ssl

Certificate file /opt/agent-cert.ssl appears to be valid.


Enter Agent Name [rilisgsc]: 10.128.28.138
```

6. Enter the hostname of the Alternate Management Server.

```
****************** ALTERNATE SERVER ADDRESSES *******************
* A list of addresses of Management Servers to use in case      *
* a connection cannot be established with the Primary           *
* Management Server.  Each Alternate Management Server will     *
* be tried in the order in which it is specified in the list.   *
* ------------------------------------------------------------- *
* Use a comma to separate each hostname or IP address.          *
*****************************************************************


Current list of Alternate Management Server addresses:


Enter list of Alternate Management Server addresses
Use 'c' to clear current list, <ENTER> to keep current list [keep]: SIDCHIPSO2.ril.com
```

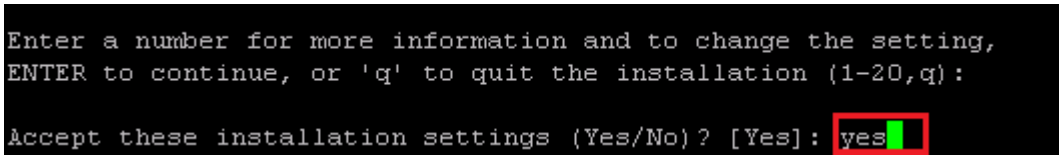
7. Enter Yes for Intrusion Prevention Mode.

```
**************** INTRUSION PREVENTION *********************
* If desired, you may disable the Intrusion Prevention    *
* Feature (IPS Driver) during install.                    *
***********************************************************

Enable IPS Feature (Yes/No)? [Yes]: Yes
```

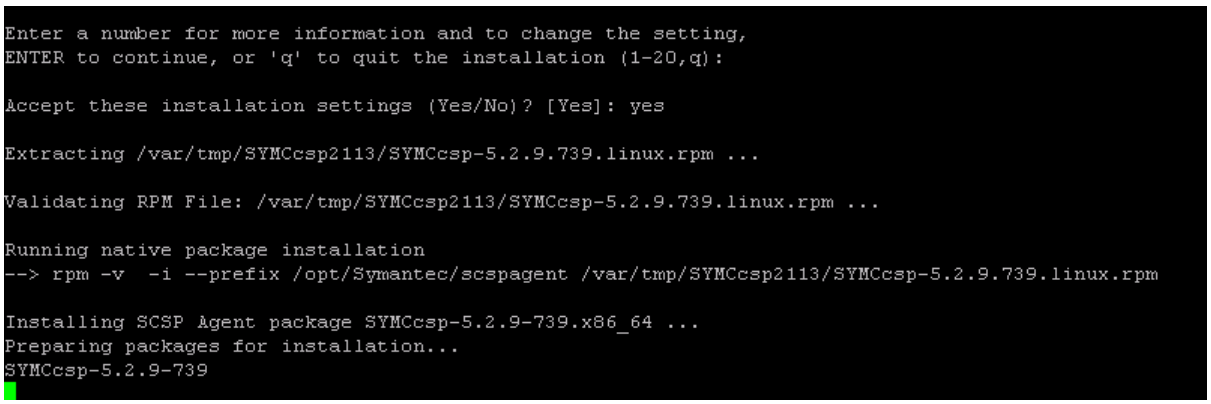
8. Press Enter.

```
*****************************************************************************
*     Symantec Critical System Protection Agent (Version 5.2.9.739)         *
*****************************************************************************
*            Name                    |         Setting                      *
* ------------------------------------------------------------------------- *
*  1) Installation Directory         |  /opt/Symantec/scspagent             *
*  2) Log Files Directory            |  /var/log/scsplog                    *
*  3) Primary Management Server      |  SIDCHIPSO1.ril.com                  *
*  4) Alternate Management Servers   |  SIDCHIPSO2.ril.com                  *
*  5) Management Server Certificate  |  /opt/agent-cert.ssl                 *
*  6) Agent Name                     |  10.128.28.138                       *
*  7) Agent Locale                   |  POSIX                               *
*  8) Agent Communication Port       |  443                                 *
*  9) Polling Interval               |  300 (seconds)                       *
* 10) Notifications Port             |  2222                                *
* 11) Agent Notifications            |  Enable                              *
* 12) Enable Intrusion Prevention    |  Enable                              *
* 13) Set Agent Protocol             |  https                               *
* 14) Common Config Group            |                                      *
* 15) Detection Config Group         |                                      *
* 16) Detection Policy Group(s)      |  Linux                               *
* 17) Prevention Config Group        |                                      *
* 18) Prevention Policy Group        |                                      *
* 19) Util Service Port              |  2323                                *
* 20) Enable Real-Time               |  Enable                              *
*     File Integrity Monitoring      |                                      *
*****************************************************************************

Enter a number for more information and to change the setting,
ENTER to continue, or 'q' to quit the installation (1-20,q):
```

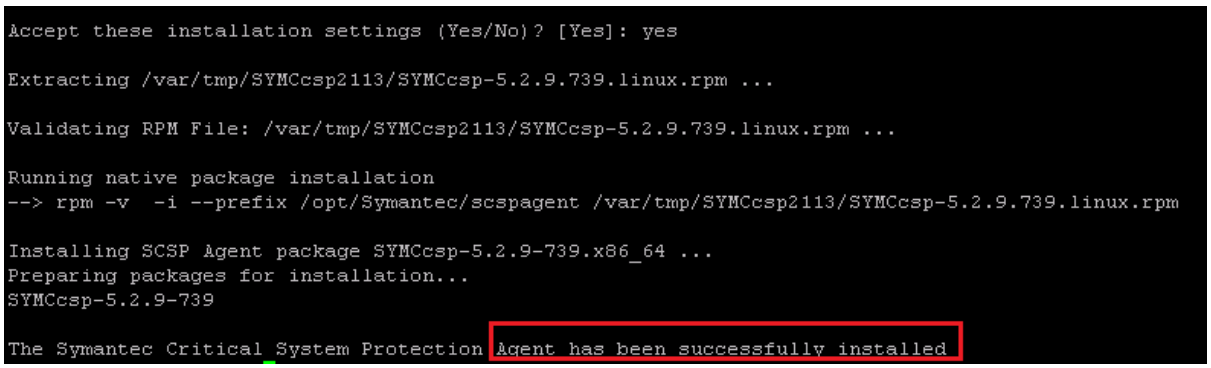
9. Enter Yes



10. The Agent Installation begins.



11. Agent Installation is successfully completed.



12. Check the SCSP services. Turn on all the runlevels for sidsagent, sisips.nfsd, sisipsagent, sisipsutil by entering the following command:
chkconfig --level 0123456 servicename on

```
[root@rilisgsc opt]# chkconfig --list
SecurityCenter  0:off   1:off   2:on    3:on    4:on    5:on    6:off
abrt-ccpp       0:off   1:off   2:off   3:on    4:off   5:on    6:off
abrt-oops       0:off   1:off   2:off   3:on    4:off   5:on    6:off
abrtd           0:off   1:off   2:off   3:on    4:off   5:on    6:off
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
cpuspeed        0:off   1:on    2:on    3:on    4:on    5:on    6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
ip6tables       0:off   1:off   2:off   3:off   4:off   5:off   6:off
iptables        0:off   1:off   2:off   3:off   4:off   5:off   6:off
irqbalance      0:off   1:off   2:off   3:on    4:on    5:on    6:off
kdump           0:off   1:off   2:off   3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mdmonitor       0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:on    3:on    4:on    5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
ntpd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
ntpdate         0:off   1:off   2:off   3:off   4:off   5:off   6:off
postfix         0:off   1:off   2:on    3:on    4:on    5:on    6:off
psacct          0:off   1:off   2:off   3:off   4:off   5:off   6:off
quota_nld       0:off   1:off   2:off   3:off   4:off   5:off   6:off
rdisc           0:off   1:off   2:off   3:off   4:off   5:off   6:off
restorecond     0:off   1:off   2:off   3:off   4:off   5:off   6:off
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
saslauthd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
sisidsagent     0:off   1:off   2:on    3:on    4:off   5:on    6:off
sisips.nfsd     0:on    1:on    2:on    3:on    4:on    5:on    6:on
sisipsagent     0:off   1:off   2:on    3:on    4:off   5:on    6:off
sisipsutil      0:off   1:off   2:on    3:on    4:off   5:on    6:off
smartd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
```