System Center
(Linux Endpoint Protection)

SCEP

System Center 2012 Operations
Manager   SCEP(System Center Endpoint Protection)   . Operations Manager
                        SCEP   .
System Center 2012 Operations Manager   . System Center
2012 Operations Manager   Linux   SCEP
                     .

          SCEP   4.5.10.1   .

4.5.9.1	05/16/2012	.
4.5.10.1	11/06/2012	Linux .
		.

4.5.10.1

System Center Endpoint Protection   4.5.10.1   .

- Linux   :
  - Red Hat Enterprise Linux Server 5
  - SUSE Linux Enterprise 10
  - CentOS 5, 6
  - Debian Linux 5, 6
  - Ubuntu Linux 10.04, 12.04
  - Oracle Linux 5, 6
        :   System Center 2012 Operations Manager Service Pack 1   .
- :
  -
  -              (   )

                              [Operations Manager 2007 R2](http://technet.microsoft.com/ko-kr/library/bb309428.aspx) _____(http://technet.microsoft.com/ko-kr/library/
bb309428.aspx)   .

                              System Center 2012 Operations Manager 2007 R2   .
                     .

	x86	x64
Red Hat Enterprise Linux Server 5, 6		
SUSE Linux Enterprise 10, 11		
CentOS 5, 6		
Debian Linux 5, 6		
Ubuntu Linux 10.04, 12.04		
Oracle Linux 5, 6		

이 설명서에서 설명합니다.

- [System Center Operations Manager 2007 R2 _____ 5](http://support.microsoft.com/kb/2449679)
  (http://support.microsoft.com/kb/2449679)

  SCEP   System Center 2012 Operations Manager 2007 R2
  입니다.

ID		
Microsoft.Linux.Library	Linux	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library		6.1.7221.0
Microsoft.SystemCenter.Library	System Center	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS-Management	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library		6.1.7221.0
Microsoft.Unix.Library	Unix	6.1.7000.256
Microsoft.Unix.Service.Library	Unix	6.1.7221.0
Microsoft.Windows.Library	Windows	6.1.7221.0
System.Health.Library		6.1.7221.0
System.Library		6.1.7221.0

:   */etc/opt/microsoft/scep/scep.cfg*   SCEP   System
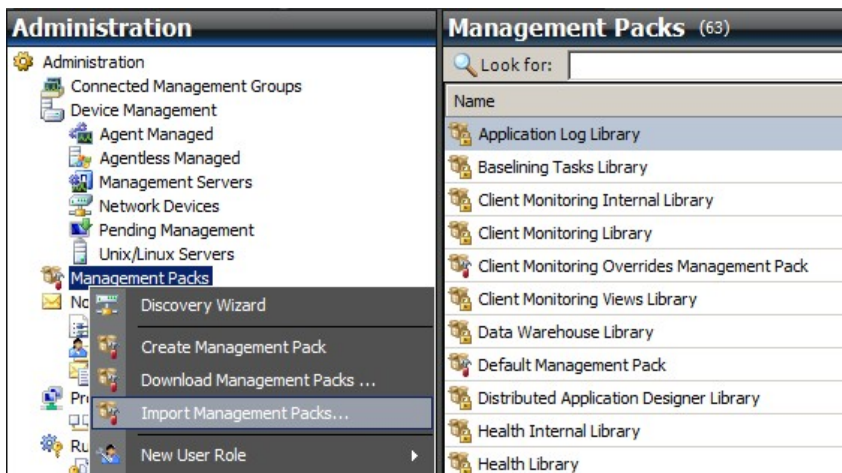Center 2012 Operations Manager   Linux SCEP   .
        'scom_enabled'   *'scom_enabled = yes'*   >   >
        > **SCOM**   .

SCEP   .

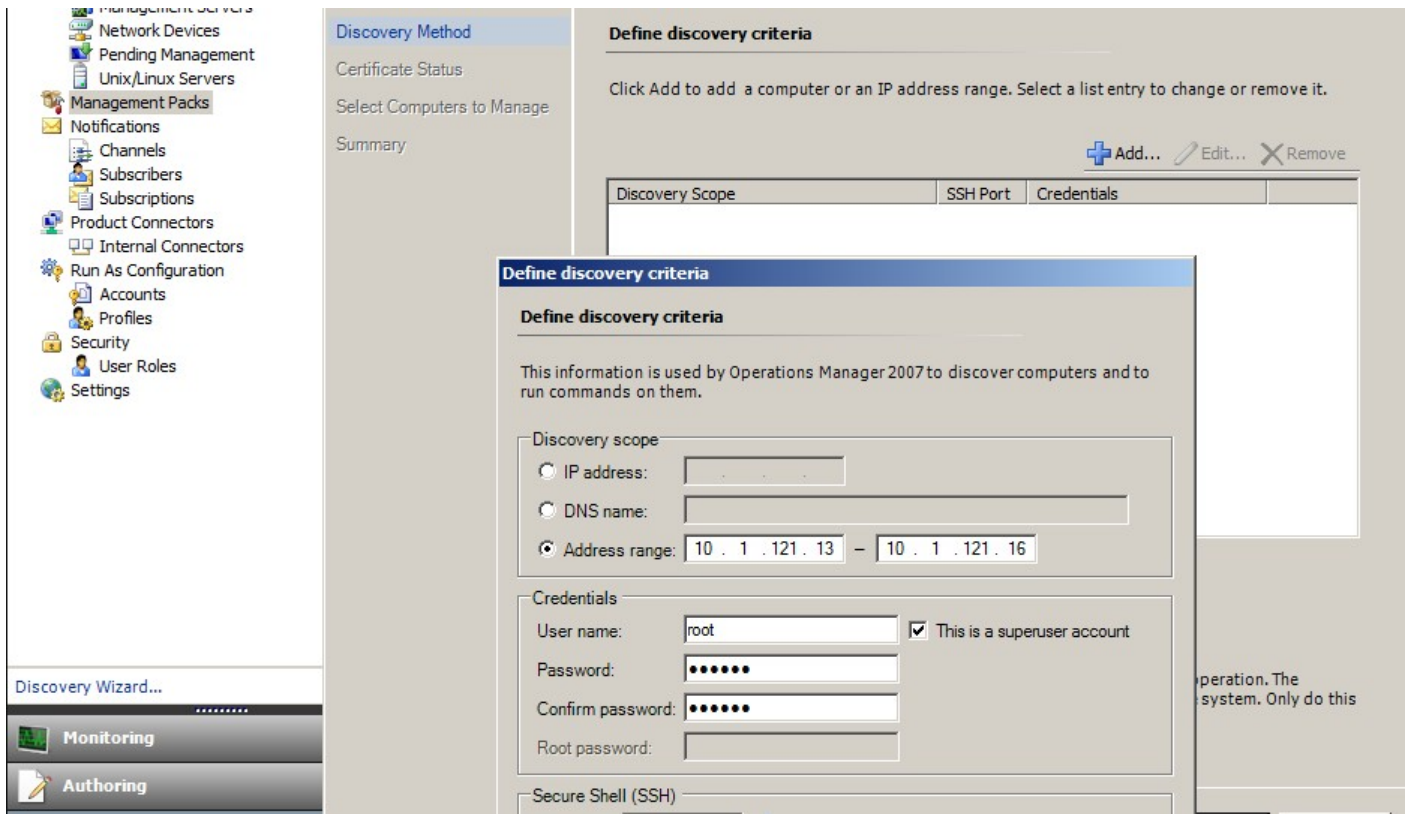|	
Microsoft.SCEP.Linux.Library.mp	, .
Microsoft.SCEP.Linux.Application.mp	, .

SCEP   Operations Manager   (
        " "   ).

1.   Administration   .
2. **Management Packs**   **Import Management Packs...**   .
3.   **Add**   **Add from disk...**   .
4. Operations Manager   (**Online Catalog Connection**   **Yes**   ).
5.   (Microsoft.SCEP.Linux.Application.mp   Microsoft.SCEP.Linux.Library.mp)   **Install**   .

      :   [Operations Manager 2007   ](http://go.microsoft.com/fwlink/?LinkId=142351)   .

*.mp   .

1.   **Administration**   **Discovery wizard...**   .
2.   **Unix/Linux computers**   **Next**   .
3.   **Add**   .
4. IP **Address range**   System Center 2012 Operations Manager   SSH **Credentials**   .
5. **OK**   **Discover**   .
6.   /   .

      : Linux   [Linux   ](#)   .   Linux Microsoft   [   ](http://technet.microsoft.com/ko-kr/library/dd789016.aspx)   .

      : SCEP   Linux   Operations Manager   Linux   8   (Linux   ).   (Linux   Linux   (   )). "scep_daemon"   (   ) SCEP   .
8   . SCEP (SCEP   )   ,   .

Unix   .

1.   **Administration**   **Run As Configuration** > **Accounts**   .
2.   **Actions**   ...   .
3.   **Run As Account type**   **Basic Authentication**   .
4.   .   **Run As Configuration** >
   Profiles   **Unix Privileged Account**   **Properties**
                                        .
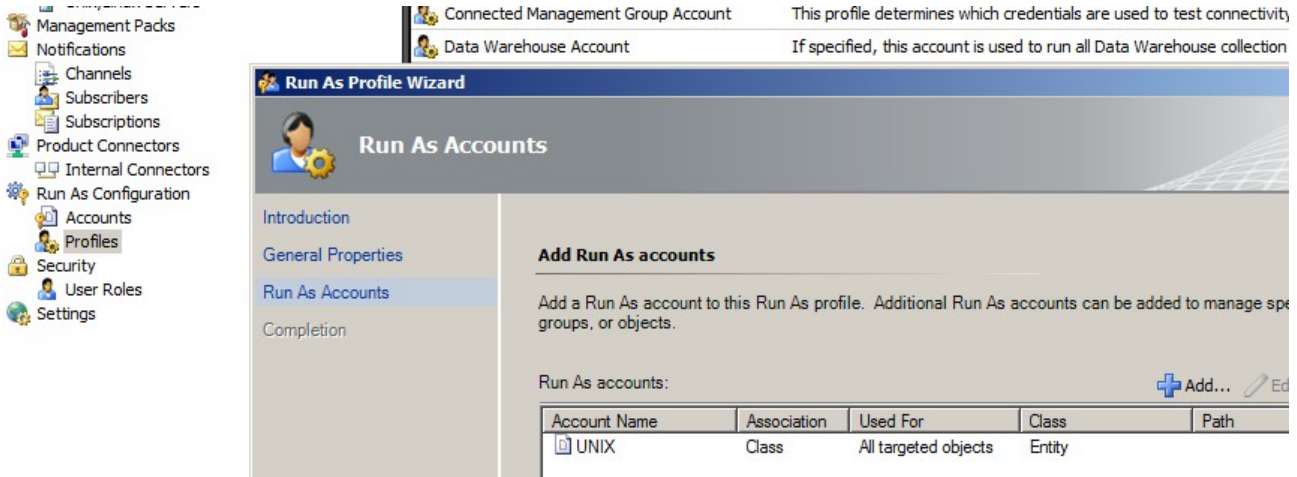
:   System Center 2012 Operations Manager 2007 R2
                    (http://technet.microsoft.com/ko-kr/library/dd788981.aspx)   .

                                Monitoring > **System Center Endpoint Protection Linux** > **SCEP**
                    Linux   .

SCEP

                    .
Microsoft.SCEP.Linux.Application.LNG.mp, Microsoft.SCEP.Linux.Library.LNG.mp

                                                        . System Center 2012
Operations Manager   .

1. Windows   .
2.   .
3.   .
            .

SCEP   .

-
-   .
                        .

Operations Manager   SCEP   . "System
Center Endpoint Protection Linux"   .

- ·   -   SCEP   ,   .
- ·   - SCEP   .
- **· SCEP**   -   Linux   .
- **· SCEP**   -   Linux   .
- ·   -   .

System Center 2012 Operations Manager   SCEP   SCEP   .

                                        Operations Manager   **Monitoring** > **System Center Endpoint**
Protection Linux > **SCEP**   SCEP   .
                                                                        .

⊘	Healthy	, .
⚠	Warning	.
✖	Critical	.
○	Not monitored	.

                                                                    .   Operations Manager
                    ,   .   [   ](http://technet.microsoft.com/ko-kr/library/bb437275.aspx)
                    (http://technet.microsoft.com/ko-kr/library/bb437275.aspx)   .

Operations Manager 2007
                    .

SCEP   17   .

- · 9   -   ,   ,
                    .

- · 2   -
                                        .

- · 6   -   .

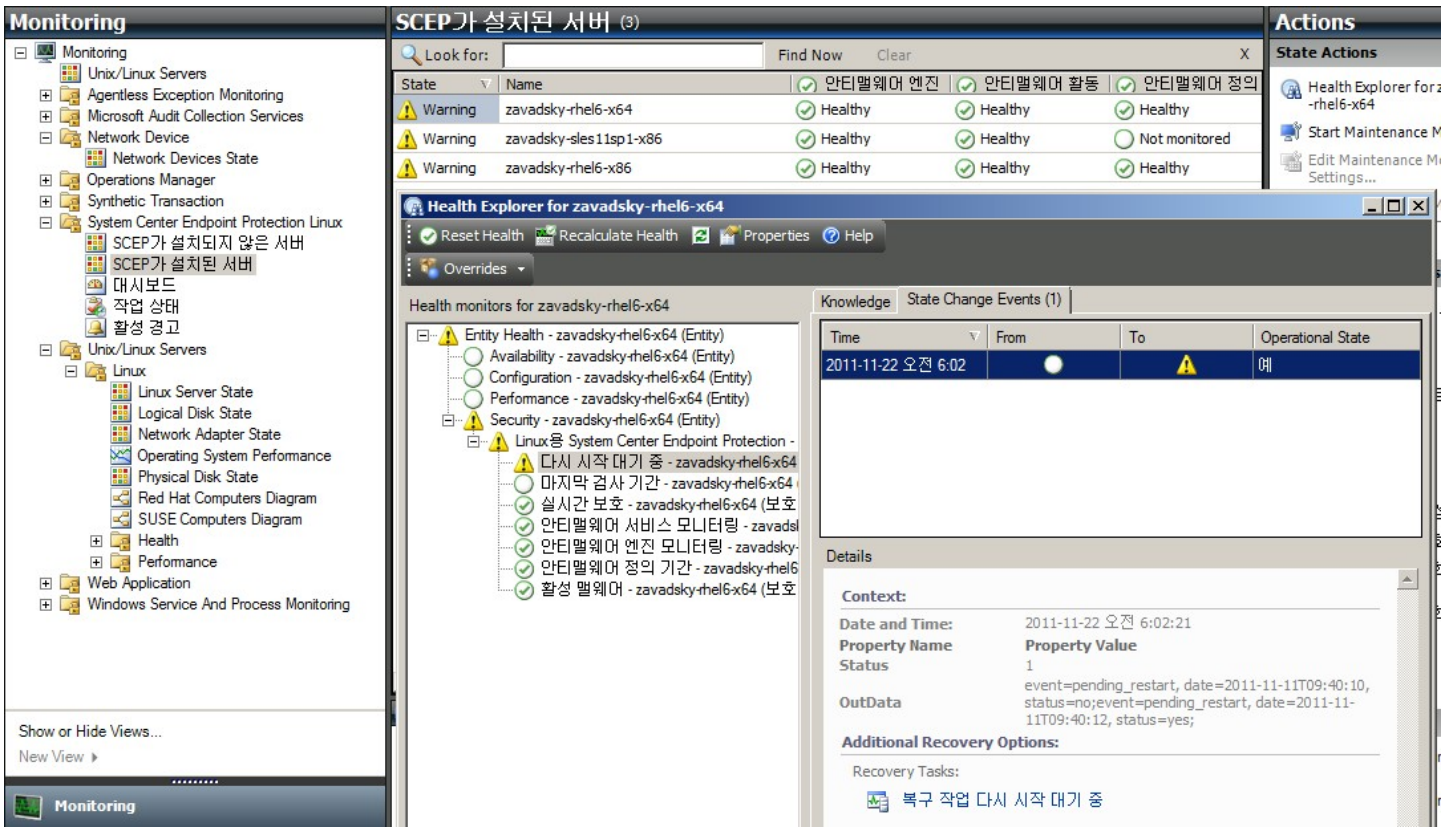   :   Operations Manager 2007 R2   (System Center 2012 Operations
Manager   F1   ).

SCEP   .

	Linux
	/var/log/scep/eventlog_scom.dat .
	.
	8 . .

	.
	8 .
	                             .
	                   .

	- -
	True

                    ,
      .

	Linux
	: /opt/microsoft/scep/sbin/scep_daemon -- status .
	8
	.

	- <= 3
	- > 3 , <= 5
	- > 5
	True
	, ( )

.

	Linux
	/var/log/scep/eventlog_scom.dat
	.
	-
	-
	True
	, ( )

.

: .

.

	Linux
	scep_daemon .
10	
	.
	-
	-
	True
	, ( )

(scep_daemon) ,
.

	Linux
	: /opt/microsoft/scep/sbin/scep_daemon -- status .
8	
	- <= 7
	- > 7
	True
	, ( )

.

.

	Linux
	/var/log/scep/eventlog_scom.dat
	.
	- -
	True
	, ( )

(
). /opt/microsoft/scep/sbin/

scep_daemon --status .

	Linux
	/var/log/scep/eventlog_scom.dat /opt/microsoft/scep/sbin/scep_daemon --status .
	.
	- -
	True
	, ( )

. ,
.

Linux   System Center Endpoint Protection

	Linux
	True

SCEP 7 Linux ( ) .
.

	True

Linux / .

	True

Linux   /   .

	True

Linux   /   .

	True

Linux   /   .

Ping

	60
	- -
	False

.

	/var/log/scep/eventlog_scom.dat
	- -
	True

5   (   )   60
.   .   60

.

	True

: , Ping

60 ( ).

.

	95%
	True

/ .

Linux ( ) 5% 60

.

SCEP Linux

	Linux
	True

Linux Linux / .

Linux , .
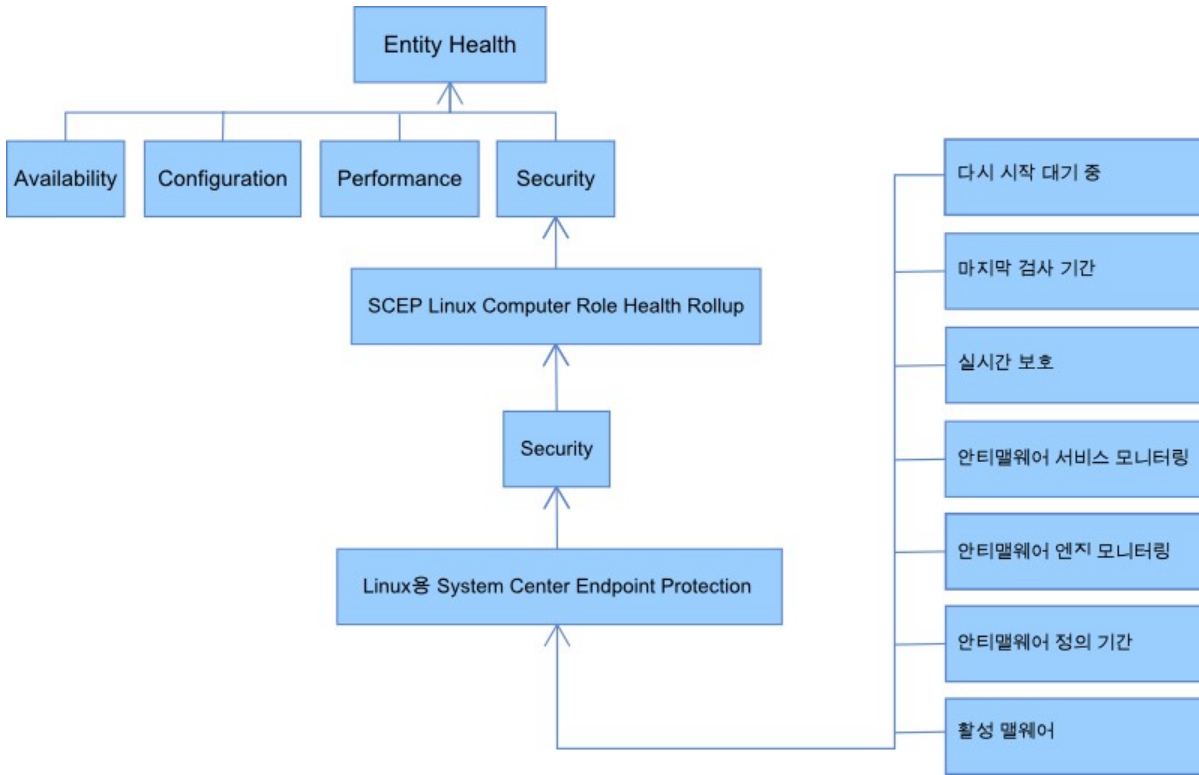
. .

. . .

(

) , .

Entity Health
- Availability
- Configuration
- Performance
- Security
  - SCEP Linux Computer Role Health Rollup
    - Security
      - Linux용 System Center Endpoint Protection

- 다시 시작 대기 중
- 마지막 검사 기간
- 실시간 보호
- 안티맬웨어 서비스 모니터링
- 안티맬웨어 엔진 모니터링
- 안티맬웨어 정의 기간
- 활성 맬웨어

Properties

Linux

- **ID** -
- -
- - SCEP
- - ( )
- - (/).
- - , SCEP
- ... - DB (, ,) , SCEP
- / ... - , (/)
- - / ,
- - SCEP

13

. Operations Manager

Monitoring > **System Center Endpoint Protection Linux** >   .

  :   (:   )
(   ).

				(30) (3) . .
			- - (:)	, . . SCEP Linux . = + (:) = +
( )				, .
( )		/ /	/ / -	. / . : ( ) .
System Center Endpoint Protection .	300			SCEP(scep_daemon) , SCEP .

14

				, .
				, .
	8		(<= 5 , > 3) (> 5)	3 DB , DB .
				Forefront Endpoint Protection 5% . . . ( ).

SCEP 13 , .
. 180 .
. SSH V|BASH .

Monitoring > System Center Endpoint Protection Linux > SCEP
.

- • - .
- • - .
- • - .
- • - .
- • - DB .
- • - DB .
- • - .
- • - SCEP , Linux
 . Linux .
- • - SCEP (scep_daemon) .
- • - SCEP (scep_daemon) .
- • - SCEP (scep_daemon) .
- • - DB .
- • - Linux .

SCEP

:

Operations Manager

.

(: "SCEP 2012 Customizations").

.   .

.   .

SSHD   , SSH   (22)   .   System
Center 2012 Operations Manager   Run As Account(Operations Manager   **Administration** > **Run
As Configuration**   ) **Basic Authentication**   Linux   .

Unix Privileged Account	Unix .

Unix Action Account   .

 :

.

.

sudo   .   sudo
Linux SCEP   /etc/sudoers   .
user1   .

```
#----------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)   NOPASSWD:      /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)   NOPASSWD:      /bin/sh -c /sbin/reboot
user1  ALL=(root)   NOPASSWD:      /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)   NOPASSWD:      /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)   NOPASSWD:      /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)   NOPASSWD:      /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)   NOPASSWD:      /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)   NOPASSWD:      /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)   NOPASSWD:      /bin/sh -c pkill scep_sci
user1  ALL=(root)   NOPASSWD:      /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#----------------------------------------------------------------------------
```
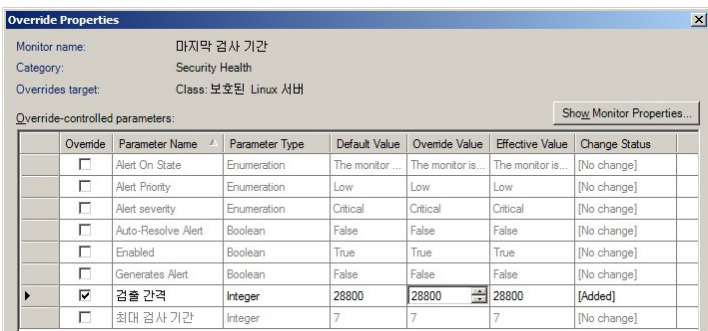
.

.

.

		3	2
			.
		30	
			.
		False	/
			.

System Center 2012 Operations Manager   ,
                        ,   ,   .

Authoring   **Management Pack Objects** > **Monitors**
.   , **Overrides**   .

.

- (   )
- (   )
- (   )
-
-
-
-
- -   .
-
- SCEP

                                                                          .

Ping	Ping	3600	Linux
			,
			. ,
			System Center 2012
			Operations Manager .

		3600	Ping/Ping ( ) : ,
		28800	.
SCEP		/var/log/scep/ eventlog_scom.log	System Center 2012 Operations Manager . .
		5	SCEP .
		3	, . .
		28800	.
		300	.
		scep_daemon	. .
		28800	.
		7	SCEP . 7 7 .
		/var/log/scep/ eventlog_scom.log	System Center 2012 Operations Manager . .
SCEP		/var/log/scep/ eventlog_scom.log	System Center 2012 Operations Manager . .
%		95%	Linux (+) % . 5% .

Override Properties							
Monitor name:	마지막 검사 기간						
Category:	Security Health						
Overrides target:	Class: 보호된 Linux 서버						

Override-controlled parameters: Show Monitor Properties...

	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
	☐	Alert On State	Enumeration	The monitor ...	The monitor is...	The monitor is...	[No change]
	☐	Alert Priority	Enumeration	Low	Low	Low	[No change]
	☐	Alert severity	Enumeration	Critical	Critical	Critical	[No change]
	☐	Auto-Resolve Alert	Boolean	False	False	False	[No change]
	☐	Enabled	Boolean	True	True	True	[No change]
	☐	Generates Alert	Boolean	False	False	False	[No change]
▶	☑	검출 간격	Integer	28800	28800	28800	[Added]
	☐	최대 검사 기간	Integer	7	7	7	[No change]

: (http://go.microsoft.com/fwlink/?LinkID=117777)

.

.

- _____
  (http://technet.microsoft.com/ko-kr/library/cc974486.aspx)
- Operations Manager 2007 _____
  (http://technet.microsoft.com/ko-kr/library/cc974494.aspx)
- _____
  (http://go.microsoft.com/fwlink/?LinkID=117777)
- Operations Manager 2007 _____
  (http://technet.microsoft.com/ko-kr/library/bb309445.aspx)
- _____
  (http://technet.microsoft.com/ko-kr/library/dd788981.aspx)
- _____
  (http://technet.microsoft.com/ko-kr/library/dd891202.aspx)
- _____
  (http://technet.microsoft.com/ko-kr/library/cc974487.aspx)
- _____
  (http://technet.microsoft.com/ko-kr/library/cc974489.aspx)
- ___,_____
  (http://technet.microsoft.com/ko-kr/library/bb437275.aspx)
- SCOM 2007 R2 _____ Linux _____
  (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- _____
  (http://technet.microsoft.com/ko-kr/library/dd789016.aspx)
- System Center 2012 UNIX Linux _____ sudo _____ - Operations Manager
  (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

Operations Manager   System Center Operations Manager _____(http://
social.technet.microsoft.com/Forums/ko-kr/category/systemcenteroperationsmanager)   .
System Center Operations Manager Unleashed _____(http://opsmgrunleashed.wordpress.com/)
            ,   "   "   .

Operations Manager   .

- Operations Manager _____
  (http://blogs.technet.com/momteam/default.aspx)
- Kevin Holman OpsMgr _____
  (http://blogs.technet.com/kevinholman/default.aspx)
- OpsMgr _____
  (http://thoughtsonopsmgr.blogspot.com/)
- Raphael Burri _____
  (http://rburri.wordpress.com/)
- BWren _____
  (http://blogs.technet.com/brianwren/default.aspx)
- System Center Operations Manager _____
  (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++
  (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- System Center Operations Manager _____
  (http://blogs.msdn.com/mariussutara/default.aspx)

                                          .

- Microsoft.Unix.Library ____
  (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-

49ab62126b74/)