



Microsoft®

# System Center Operations Manager

## System Center Pacchetto di monitoraggio per Endpoint Protection per Linux

---

Microsoft Corporation

Pubblicato il: 10/26/2015

Inviare commenti o suggerimenti relativi al presente documento all'indirizzo [mpgfeed@microsoft.com](mailto:mpgfeed@microsoft.com). Si prega di indicare il nome della guida del pacchetto di gestione insieme al proprio commento.

Il team Operations Manager invita gli utenti a fornire il proprio commento sul pacchetto di monitoraggio pubblicando una recensione sulla pagina del pacchetto di gestione intitolata [Catalogo pacchetto di gestione](http://go.microsoft.com/fwlink/?LinkID=82105) (<http://go.microsoft.com/fwlink/?LinkID=82105>).

## Contenuti

<b>Guida pacchetto di gestione SCEP</b>	<b>3</b>
Storia della guida	3
Modifiche nella versione 4.5.10.1	3
Configurazioni supportate	3
Prerequisiti	3
File contenuti in questo pacchetto di gestione	4
Avvio rapido	4
Obiettivo del pacchetto di gestione	6
Visualizzazioni	6
Monitoraggi	7
Organizzazione gerarchica delle condizioni di	11
Proprietà degli oggetti	12
Avvisi	13
Attività	14
<b>Configurazione del pacchetto di gestione per SCEP</b>	<b>15</b>
Procedura consigliata: creazione di un pacchetto	15
Configurazione di sicurezza	15
Sincronizzazione delle regole delle soglie	16
Esclusioni	16
<b>Collegamenti</b>	<b>18</b>

# Guida pacchetto di gestione SCEP

Questo pacchetto di gestione consente all'utente di gestire System Center Endpoint Protection (SCEP) da System Center 2012 Operations Manager in un ambiente collegato che comprende workstation e server, a partire da una posizione centrale. Grazie al sistema di gestione delle attività Operations Manager, è possibile gestire SCEP su computer remoti, visualizzare avvisi e condizioni di sicurezza e rispondere prontamente ai nuovi problemi e alle nuove minacce.

System Center 2012 Operations Manager stesso non fornisce altre forme di protezione contro codici dannosi. System Center 2012 Operations Manager dipende dalla presenza di una soluzione SCEP sui computer su cui è installato il sistema operativo Linux.

La presente guida è stata scritta sulla base della versione 4.5.10.1 del pacchetto di gestione per SCEP.

## Storia della guida

Versione	Data di rilascio	Modifiche
4.5.9.1	05/16/2012	Rilascio originale di questa guida.
4.5.10.1	11/06/2012	Nuove distribuzioni Linux supportate. Migliore descrizione per alcuni strumenti del pacchetto di gestione.

## Modifiche nella versione 4.5.10.1

La versione 4.5.10.1 del pacchetto di gestione per System Center Endpoint Protection comprende le seguenti modifiche:

- Nuove distribuzioni Linux supportate:
  - 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**Nota:** queste distribuzioni saranno supportate solo se si utilizza System Center 2012 Operations Manager Service Pack 1 e versioni successive.
- È stata aggiunta una migliore descrizione per:
  - Monitoraggio malware attivo
  - Avviso malware attivo (da Regola)

## Configurazioni supportate

In generale, le configurazioni supportate sono descritte nel sito web [Configurazioni supportate di Operations Manager 2007 R2](http://go.microsoft.com/fwlink/?LinkId=90676) (<http://go.microsoft.com/fwlink/?LinkId=90676>).

Questo pacchetto di gestione richiede System Center 2012 Operations Manager 2007 R2 o una versione successiva. La seguente tabella contiene informazioni relative ai sistemi operativi supportati per questo pacchetto di gestione:

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

## Prerequisiti

Per eseguire questo pacchetto di gestione, è necessario conformarsi ai seguenti requisiti:

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

I pacchetti di gestione per SCEP elencati di seguito sono integrati in System Center 2012 Operations Manager 2007 R2 oppure possono essere scaricati dal catalogo on-line.

ID	Nome	Versione
----	------	----------

Microsoft.Linux.Library	Libreria sistema operativo Linux	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	Libreria gruppo istanze	6.1.7221.0
Microsoft.SystemCenter.Library	Libreria architettura System Center	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	Libreria gestione WS	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	Libreria magazzino dati	6.1.7221.0
Microsoft.Unix.Library	Libreria architettura Unix	6.1.7000.256
Microsoft.Unix.Service.Library	Libreria modelli servizio Unix	6.1.7221.0
Microsoft.Windows.Library	Libreria architettura Windows	6.1.7221.0
System.Health.Library	Libreria sicurezza	6.1.7221.0
System.Library	Libreria sistema	6.1.7221.0

**Importante:** Per un corretto funzionamento, il monitoraggio del prodotto Linux SCEP con System Center 2012 Operations Manager deve innanzitutto essere abilitato nel file di configurazione `/etc/opt/microsoft/scep/scep.cfg` oppure tramite l'interfaccia web SCEP. Assicurarsi che il parametro 'scom\_enabled' nel file di configurazione di cui sopra sia impostato come segue "scom\_attivato = sì" oppure modificare l'impostazione appropriata nell'interfaccia web sotto **Configurazione > Globale > Opzioni daemon > SCOM attivato**.

## File contenuti in questo pacchetto di gestione

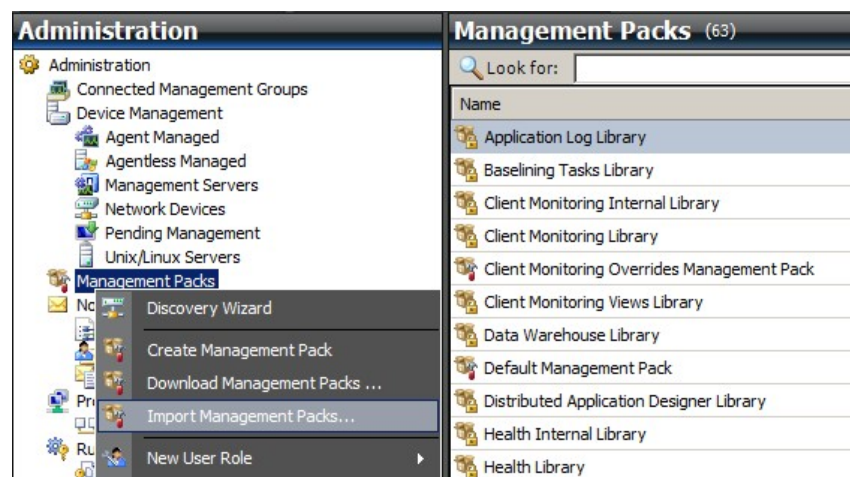
Il pacchetto di gestione per SCEP comprende i seguenti file:

Nomefile	Descrizione
Microsoft.SCEP.Linux.Library.mp	Contiene le definizioni delle classi e i relativi rapporti reciproci e monitora anche i tipi e le definizioni dei tipi di moduli.
Microsoft.SCEP.Linux.Application.mp	Implementa il monitoraggio e l'invio di avvisi, le attività e le visualizzazioni.

## Avvio rapido

Il prerequisito per l'avvio del monitoraggio SCEP consiste nell'importazione di pacchetti di gestione all'interno di Operations Manager e nell'identificazione di computer da monitorare (tale processo viene indicato con il nome di "rilevamento").

### Importazione di pacchetti di gestione

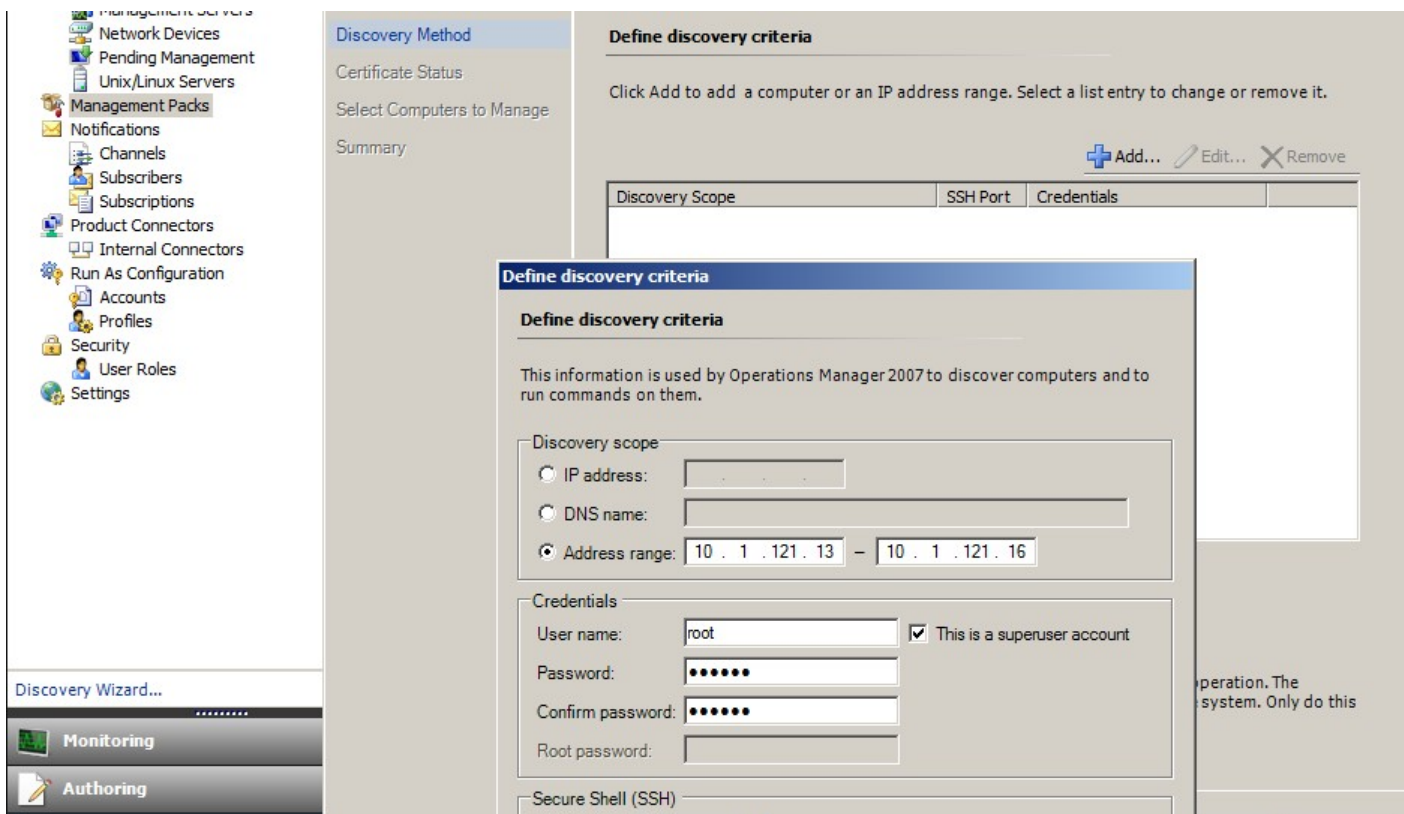


1. Fare clic sull'area di lavoro **Administration** nel pannello sulla sinistra della finestra Operations Console.
2. Fare clic con il tasto destro su **Management Packs** e selezionare **Import Management Packs...** dal menu contestuale.
3. Nella finestra Pacchetti di gestione fare clic sul pulsante **Add** e selezionare **Add from disk...** dal menu a discesa.
4. Confermare che si desidera che Operations Manager ricerchi e installi anche le dipendenze non sul disco locale, facendo clic su **Yes** nella finestra pop-up **Online Catalog Connection**.
5. Assicurarsi di selezionare entrambi i file elencati (Microsoft.SCEP.Linux.Application.mp, Microsoft.SCEP.Linux.Library.mp) e fare clic su **Install**.

**Nota:** Per ulteriori istruzioni relative all'importazione di un pacchetto di gestione, si rimanda alla pagina [Come importare un pacchetto di gestione in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=142351) (<http://go.microsoft.com/fwlink/?LinkId=142351>).

### Rilevamento

Dopo aver importato con successo i file \*.mp, sarà necessario eseguire il rilevamento del computer.



1. Nell'area di lavoro **Administration** (nel pannello sulla sinistra della finestra Operations Console), fare clic sul collegamento **Discovery wizard...** (nella parte inferiore del pannello sulla sinistra).
2. Nella procedura guidata di gestione del computer e del dispositivo, selezionare l'opzione **Unix/Linux computers** e fare clic su **Next** per continuare.
3. Nella sezione Definisci criteri di rilevamento, fare clic sul pulsante **Add**.
4. Impostare un **Address range** IP da controllare e le **Credentials** SSH applicabili ai computer, sui quali System Center 2012 Operations Manager installerà il suo agente.
5. Confermare i propri criteri relativi ad ambito e credenziali facendo clic su **OK** e sul pulsante **Discover** per avviare il processo di rilevamento.
6. Una volta terminata la procedura, verrà visualizzato un elenco che consentirà all'utente di selezionare i sistemi di monitoraggio/gestione.

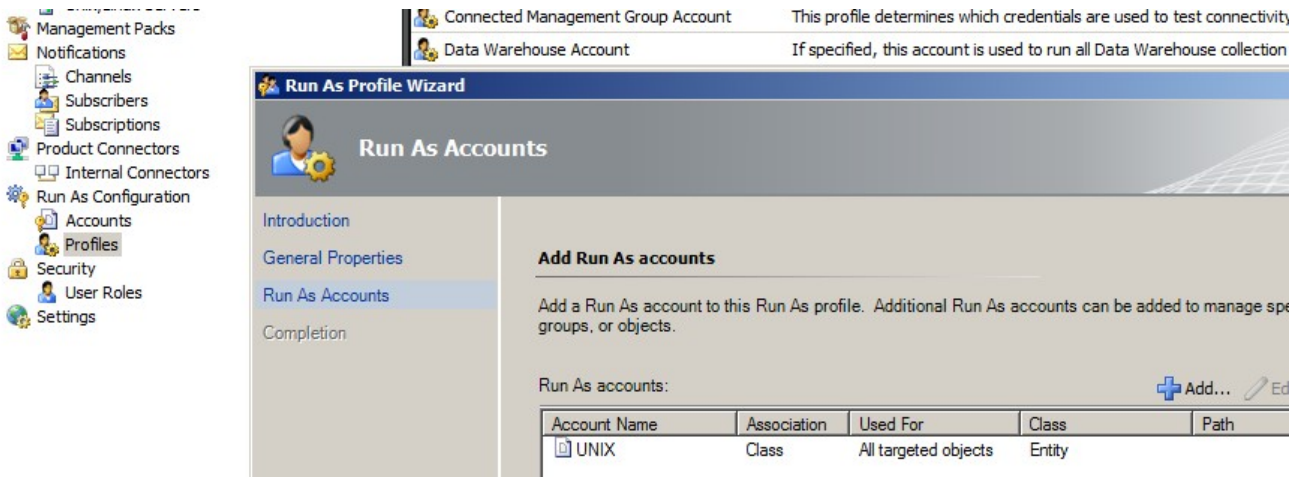
**Nota:** L'installazione di un agente Linux è supportata nelle seguenti [Distribuzioni Linux](#). Qualora non sia possibile installare l'agente Linux tramite il rilevamento, si prega di consultare le istruzioni di installazione contenute nel manuale nel seguente articolo Microsoft [Installazione manuale di agenti multiplatforma](http://technet.microsoft.com/en-us/library/dd789016.aspx) (<http://technet.microsoft.com/en-us/library/dd789016.aspx>).

**Nota:** Il rilevamento di server Linux con un'installazione SCEP si avvia automaticamente in base a intervalli di 8 ore su tutti i computer Linux gestiti tramite Operations Manager (ad es.: questi presentano il pacchetto di gestione Linux adeguato installato per la distribuzione del relativo sistema). Il rilevamento crea tutte le entità del modulo di servizio: il server Linux protetto e le entità nidificate o il server Linux non protetto (che è possibile trovare nelle relative sezioni). SCEP sarà considerato completamente installato se è presente il servizio "scep\_daemon" (interrotto o in esecuzione). Di conseguenza, il primo rilevamento avrà luogo durante l'installazione del pacchetto di gestione mentre il successivo verrà eseguito tra 8 ore, in base al ciclo di rilevamento. In caso di disinstallazione di un prodotto SCEP, il rispettivo server verrà automaticamente spostato su non protetto (server senza SCEP) e viceversa.

## Configurazione account Esegui come

Per creare un account Unix, utilizzare le seguenti istruzioni:

1. Nell'area di lavoro **Administration** (pannello sulla sinistra) accedere a **Run As Configuration > Accounts**.
2. Per creare un nuovo account, aprire la sezione **Actions** sul pannello (sulla destra) **Azioni** e fare clic su **Crea account esegui come...**
3. Nella finestra Proprietà generali, selezionare **Basic Authentication** dal menu a tendina **Run As Account type**.
4. Dopo aver creato un nuovo account, sarà necessario aggiungerlo a un profilo per far sì che possa verificarsi la distribuzione. Per eseguire tale operazione, fare clic con il tasto destro del mouse sul profilo **Unix Privileged Account** sotto **Run As Configuration > Profiles**, selezionare **Properties** e completare la procedura guidata per assegnare l'account appena creato.



**Nota:** Per ulteriori informazioni sulla creazione di un account Esegui come, consultare l'argomento [Configurazione di un account Esegui come multiplatforma](http://go.microsoft.com/fwlink/?LinkId=160348) (http://go.microsoft.com/fwlink/?LinkId=160348) nella libreria on-line System Center 2012 Operations Manager 2007 R2.

Dopo aver completato tutti i passi precedenti, i server Linux appena rilevati saranno presto (in pochi minuti) disponibili sotto **Monitoring > Linux System Center Endpoint Protection > Server con SCEP**.

## Installazione di un pacchetto lingue per SCEP

Il formato di un pacchetto lingue è il seguente:

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

Per l'installazione del pacchetto lingue, utilizzare la procedura descritta nella sezione di cui sopra **Importazione di pacchetti di gestione**. Per visualizzare la lingua installata in System Center 2012 Operations Manager, utilizzare le seguenti istruzioni:

1. Fare clic sull'icona Windows **Start** e accedere al **Pannello di controllo**.
2. Nel Pannello di controllo, fare clic su **Opzioni internazionali e della lingua**.
3. Modificare le opzioni internazionali di sistema per i programmi non Unicode nella scheda **Amministrativa**. Nella scheda **Posizione**, modificare la posizione corrente in base al pacchetto lingue installato.

## Obiettivo del pacchetto di gestione

Il pacchetto di gestione per SCEP presenta le seguenti funzionalità:

- Monitoraggio e avviso in tempo reale in merito a incidenti di sicurezza e allo stato delle condizioni di sicurezza.
- Consente agli amministratori del server di eseguire attività correlate alla sicurezza da remoto sui propri server. L'obiettivo principale di queste attività consiste nel porre rimedio ai problemi di disponibilità correlati alla sicurezza.

## Visualizzazioni

L'amministratore del server è in grado di monitorare, tramite la console Operations Manager, tutti i computer su cui è installato SCEP. Le seguenti visualizzazioni sono disponibili per "Linux System Center Endpoint Protection":

- **Avvisi attivi** - Tutti gli avvisi attivi SCEP di tutti i livelli di sicurezza. Non comprende gli avvisi chiusi.
- **Pannello di controllo** - Consente di visualizzare sia i server con SCEP sia le aree di lavoro degli avvisi attivi.
- **Server con SCEP** - Consente di visualizzare tutti i server Linux protetti.
- **Server senza SCEP** - Consente di visualizzare tutti i server Linux non protetti.
- **Stato attività** - Contiene un elenco di tutte le attività eseguite.

Durante il monitoraggio dello stato di SCEP con il pacchetto di gestione System Center 2012 Operations Manager, è possibile scaricare una visualizzazione istantanea della sicurezza SCEP.

Anziché attendere la comparsa di un avviso, è possibile visualizzare una sintesi dello stato per i componenti SCEP in qualsiasi momento facendo clic sul pannello **Monitoring > Linux System Center Endpoint Protection > Server con SCEP** della console di monitoraggio Operations Manager. Lo stato di un componente è indicato nel campo Stato con icone colorate:

Icona	Stato	Descrizione
	Healthy	Un'icona verde indica successo oppure la disponibilità di informazioni che non richiedono azioni.
	Warning	Un'icona gialla indica un errore o un allarme.
	Critical	Un'icona rossa indica un errore critico, un problema di sicurezza o la mancata disponibilità di un servizio.
	Not monitored	L'assenza di icone indica la mancata raccolta di dati che influiscono sullo stato.

Una visualizzazione può contenere un lungo elenco di oggetti. Per trovare un oggetto o un gruppo di oggetti specifici, è possibile utilizzare i pulsanti Ambito, Cerca e Trova sulla barra degli strumenti Operations Manager. Per ulteriori informazioni, consultare l'argomento [Come gestire i dati di monitoraggio utilizzando Ambito, Cerca e Trova](http://go.microsoft.com/fwlink/?LinkId=91983) (<http://go.microsoft.com/fwlink/?LinkId=91983>).

## Monitoraggi

In Operations Manager 2007, è possibile utilizzare i monitoraggi per la valutazione di varie condizioni che possono verificarsi negli oggetti monitorati.

Per SCEP sono disponibili in tutto 17 monitoraggi:

- 9 monitoraggi di unità - I componenti di monitoraggio fondamentali sono utilizzati per monitorare specifici contatori, eventi, script e servizi.
- 2 monitoraggi aggregati - Utilizzati per una visualizzazione aggregata che raggruppa vari monitoraggi in uno solo e utilizza quindi questo monitoraggio per impostare le condizioni di sicurezza e per generare un avviso.
- 6 monitoraggi delle dipendenze - Riferimenti contenenti i dati relativi allo stato dei monitoraggi esistenti.

**Nota:** Per ulteriori informazioni sui monitoraggi, consultare la Guida Operations Manager 2007 R2 (in System Center 2012 Operations Manager, premere il pulsante F1).

The screenshot shows the 'Monitoring' console for 'Server con SCEP'. The main table lists health monitors for 'zavadsky-rhel6-x64' with the following data:

State	Name	Motore antimalware	Attività antimalware	Definizioni antimalware
Warning	zavadsky-rhel6-x64	Healthy	Healthy	Healthy
Warning	zavadsky-sles11sp1-x86	Healthy	Healthy	Not monitored
Warning	zavadsky-rhel6-x86	Healthy	Healthy	Healthy

The 'Health Explorer' window shows a tree view of health monitors for 'zavadsky-rhel6-x64' (Entity), including: Availability, Configuration, Performance, Security, System Center Endpoint Protection per Linux, Età definizioni antimalware, Malware attivo, Monitoraggio motore antimalware, Monitoraggio servizio antimalware, Protezione in tempo reale, Riavvio in corso, and Ultima scansione.

The 'State Change Events' table shows the following event:

Time	From	To	Operational State
22/11/2011 6.02			Si

The 'Details' pane shows context information for the event, including Date and Time (22/11/2011 6.02.21), Property Name (1), Status (1), and OutData (event=pending\_restart, date=2011-11-11T09:40:10, status=no;event=pending\_restart, date=2011-11-11T09:40:12, status=yes).

I monitoraggi delle condizioni di sicurezza SCEP presentano la struttura e le proprietà descritte di seguito.

### Malware attivo

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Monitora il file di registro in formato testo: /var/log/scep/eventlog_scom.dat



Tipo di monitoraggio	Monitoraggio di unità
Intervallo	Basato su eventi
Avviso	Si. Nessuna risoluzione automatica
Reimposta comportamento	Il ritorno alla condizione di sicurezza è automatico dopo un periodo di 8 ore. L'avviso rimane attivo per conservare le informazioni relative al malware non trattato.
Note	Questo monitoraggio cambierà lo stato in critico in caso di individuazione di malware non pulito. Lo stato ritornerà automaticamente su Sicuro dopo 8 ore (poiché non è possibile determinare con precisione se il malware è stato pulito/eliminato o meno). È richiesto l'intervento dell'amministratore per valutare le circostanze e chiudere manualmente il ticket.
Stato	Sicuro - Nessun malware Critico - Malware attivo
Attivato	Vero
Attività di recupero	No

Questo monitoraggio consente di rilevare le operazioni di pulizia di malware non riuscite. Questo monitoraggio segnalerà uno stato critico in caso di segnalazione da parte del client della mancata pulizia del malware.

#### Età definizioni antim malware

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Comando utilizzato per ottenere i dati di monitoraggio: /opt/microsoft/scep/sbin/scep_daemon --status
Intervallo	Ogni 8 ore
Avviso	Si. Risoluzione automatica
Stato	Sicuro - età <= 3 giorni Avvertenza - età > 3 E età <= 5 giorni Critico - età > 5 giorni
Attivato	Vero
Attività di recupero	Si, manualmente (Nessuna risoluzione automatica)

Definizioni aggiornate garantiscono la protezione del computer contro le minacce malware più recenti.

#### Motore antim malware

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Monitora il file di registro in formato testo: /var/log/scep/eventlog_scom.dat
Intervallo	Basato su eventi
Avviso	Si. Risoluzione automatica
Stato	Sicuro - Attivato Disattivato - Allarme
Attivato	Vero
Attività di recupero	Si, manualmente (Nessuna risoluzione automatica)

Si consiglia di attivare sempre la protezione antim malware.

**Nota:** Questo monitoraggio consente di rilevare lo stato della protezione antivirus che non corrisponde alla protezione in tempo reale. Con il motore antim malware disattivato, non è possibile avviare una scansione su richiesta.

#### Servizio antim malware

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Monitora lo stato del processo: scep_daemon
Intervallo	Ogni 10 minuti
Avviso	Si. Risoluzione automatica
Stato	Sicuro - In esecuzione Critico - Non in esecuzione
Attivato	Vero
Attività di recupero	Si, manualmente (Nessuna risoluzione automatica)

Il monitoraggio consente di segnalare uno stato critico qualora il servizio antim malware (scep\_daemon) sulla macchina client non sia in esecuzione o non sia reattivo o qualora il motore antim malware non funzioni correttamente.



### Età ultima scansione

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Comando utilizzato per ottenere i dati di monitoraggio: /opt/microsoft/scep/sbin/scep_daemon --status
Intervallo	Ogni 8 ore
Avviso	No
Stato	Sicuro - età <= 7 Allarme - età > 7
Attivato	Vero
Attività di recupero	Sì, manualmente (Nessuna risoluzione automatica)

Questo monitoraggio consente di rilevare l'ora dell'ultima scansione del computer (indipendentemente dal tipo di scansione). Si consiglia di programmare l'esecuzione di una scansione ogni settimana.

### Riavvio in corso

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Monitora il file di registro in formato testo: /var/log/scep/eventlog_scom.dat
Intervallo	Basato su eventi
Avviso	Sì. Risoluzione automatica
Stato	No - Sicuro Sì - Allarme
Attivato	Vero
Attività di recupero	Sì, manualmente (Nessuna risoluzione automatica)

Questo monitoraggio consente di rilevare la necessità di riavviare il sistema per rendere attive le modifiche di configurazione (tipicamente quando si attiva/disattiva la protezione in tempo reale). Il monitoraggio applica la seguente chiamata per un aggiornamento su richiesta di questo stato: /opt/microsoft/scep/sbin/scep\_daemon --status.

### Protezione in tempo reale

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Server Linux protetto
Fonte dati	Monitora il file di registro in formato testo: /var/log/scep/eventlog_scom.dat Il monitoraggio può anche utilizzare la seguente chiamata per un aggiornamento dello stato su richiesta: /opt/microsoft/scep/sbin/scep_daemon --status.
Intervallo	basato su eventi
Avviso	Sì. Risoluzione automatica
Stato	Attivato - Sicuro Disattivato - Allarme
Attivato	Vero
Attività di recupero	Sì, manualmente (nessuna risoluzione automatica)

Monitora lo stato della protezione in tempo reale. La protezione in tempo reale invia avvisi in caso di tentativi di installazioni automatiche sul computer da parte di virus, spyware o altri software potenzialmente indesiderati.

### System Center Endpoint Protection per Linux

Tipo di monitoraggio	Monitoraggio aggregato
Destinazione	Server Linux protetto
Condizione	Peggior di
Avviso	No
Attivato	Vero
Attività di recupero	No

Questo monitoraggio consiste nella visualizzazione delle condizioni di sicurezza (stato peggiore) per tutti i monitoraggi delle unità di sicurezza del server Linux protetto SCEP 7. In caso di mancata inizializzazione dello stato, si verificano le seguenti condizioni: il monitoraggio non è stato avviato per questo oggetto oppure non sono stati definiti monitoraggi di sicurezza per questo oggetto.

### Motore antimalware

Tipo di monitoraggio	Monitoraggio delle dipendenze
----------------------	-------------------------------

Destinazione	Motore antimalware
Avviso	No
Attivato	Vero
Attività di recupero	No

Consente di visualizzare lo stato del monitoraggio delle unità del server Linux protetto/motore antimalware nell'elenco di computer monitorati.

#### Servizio antimalware

Tipo di monitoraggio	Monitoraggio delle dipendenze
Destinazione	Motore antimalware
Avviso	No
Attivato	Vero
Attività di recupero	No

Consente di visualizzare lo stato del monitoraggio delle unità del server Linux protetto/servizio antimalware nell'elenco di computer monitorati.

#### Definizioni antimalware

Tipo di monitoraggio	Monitoraggio delle dipendenze
Destinazione	Definizioni antimalware
Avviso	No
Attivato	Vero
Attività di recupero	No

Consente di visualizzare lo stato del monitoraggio del server Linux protetto/dell'età delle definizioni antimalware nell'elenco di computer monitorati.

#### Malware attivo

Tipo di monitoraggio	Monitoraggio delle dipendenze
Destinazione	Attività antimalware
Avviso	No
Attivato	Vero
Attività di recupero	No

Consente di visualizzare lo stato del monitoraggio del server Linux protetto/malware attivo nel sistema di esplorazione delle condizioni di sicurezza per l'attività antimalware.

#### Ping della macchina

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Attività antimalware
Intervallo	Ogni 60 minuti
Avviso	No
Stato	Raggiungibile - Sicuro Non raggiungibile - Critico
Attivato	Falso
Attività di recupero	No

Trasforma il relativo stato da Critico a Nessuna risposta dal server.

#### Attività malware

Tipo di monitoraggio	Monitoraggio di unità
Destinazione	Attività antimalware
Fonte dati	Monitora il file di registro in formato testo: /var/log/scep/eventlog_scom.dat
Intervallo	Basato su eventi
Avviso	No
Stato	Nessun malware - Sicuro Attività malware rilevata - Critico
Attivato	Vero
Attività di recupero	No

Questo monitoraggio passa allo stato critico entro 5 minuti dal rilevamento dei malware (puliti o non trattati) e rimane Critico per i successivi 60 minuti. Lo stato Critico si rinnova all'occorrenza di ogni nuovo rilevamento positivo e con esso anche la durata del periodo di allerta. In altre parole, in caso di mancato rilevamento di malware sul sistema durante un periodo di 60 minuti, il monitoraggio ritorna allo stato Sicuro.

#### Attacco di malware al server

Tipo di monitoraggio	Monitoraggio aggregato
Destinazione	Attività antimalware
Condizione	Migliore di
Avviso	No
Attivato	Vero
Attività di recupero	No

Monitoraggi aggregati: Attività malware, Ping della macchina.

Trasforma lo stato in Critico in caso di mancata risposta dal server entro 60 minuti da un rilevamento positivo di malware (pulito o non trattato). Il passaggio dello stato a Critico può essere anche attivato se, dopo un periodo di mancanza di risposte dal server, viene rilevato un malware subito dopo il rinnovo della connessione.

#### Attacco di malware

Tipo di monitoraggio	Monitoraggio delle dipendenze
Destinazione	Sistema di supervisione server protetti
Condizione	Peggior del 95%
Avviso	No
Attivato	Vero
Attività di recupero	No

Consente di visualizzare lo stato del monitoraggio dell'attività antimalware/dell'attacco di malware al server.

Se più del 5% di tutti i computer Linux (protetti e non) registra un rilevamento di malware negli ultimi 60 minuti, questo monitoraggio passa allo stato Critico.

#### Visualizzazione delle condizioni di sicurezza del ruolo del computer SCEP Linux

Tipo di monitoraggio	Monitoraggio delle dipendenze
Destinazione	Computer Linux
Avviso	No
Attivato	Vero
Attività di recupero	No

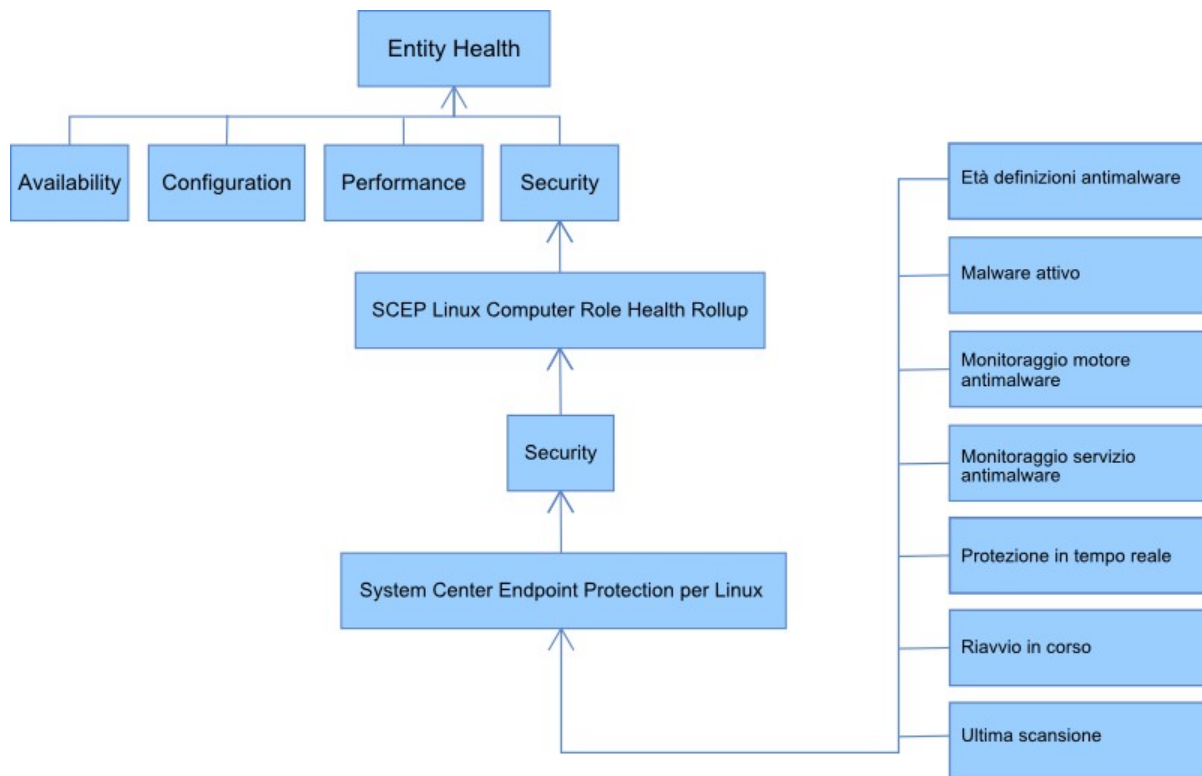
Propaga lo stato dell'entità del computer Linux protetto sul monitoraggio principale Computer Linux/sicurezza.

### Organizzazione gerarchica delle condizioni di sicurezza

Questo pacchetto di sicurezza espande il monitoraggio del sistema operativo Linux come struttura stratificata in cui, per ricevere protezione, ciascun livello dipende dal livello inferiore. Il livello massimo di questa struttura è rappresentato dall'intero ambiente di sicurezza dell'entità, mentre il livello minimo degli ambienti di sicurezza è rappresentato da tutti i monitoraggi. Per garantire le corrispondenze, se lo stato di uno dei livelli cambia, cambierà anche lo stato del livello superiore. Questa azione prende il nome di organizzazione gerarchica delle condizioni di sicurezza.

Ad esempio, se la protezione in tempo reale restituisce lo stato di Allarme e tutti gli altri componenti sono rappresentati da Sicurezza, lo stato di Allarme verrà trasferito attraverso la struttura ad albero sulla root (Sicurezza dell'entità), che acquisirà anch'essa lo stato Allarme.

Il diagramma che segue illustra l'organizzazione gerarchica delle condizioni di sicurezza degli oggetti in questo pacchetto di gestione.



## Proprietà degli oggetti

Per visualizzare le proprietà di un oggetto, fare clic con il tasto destro del mouse sull'oggetto e selezionare **Properties**.

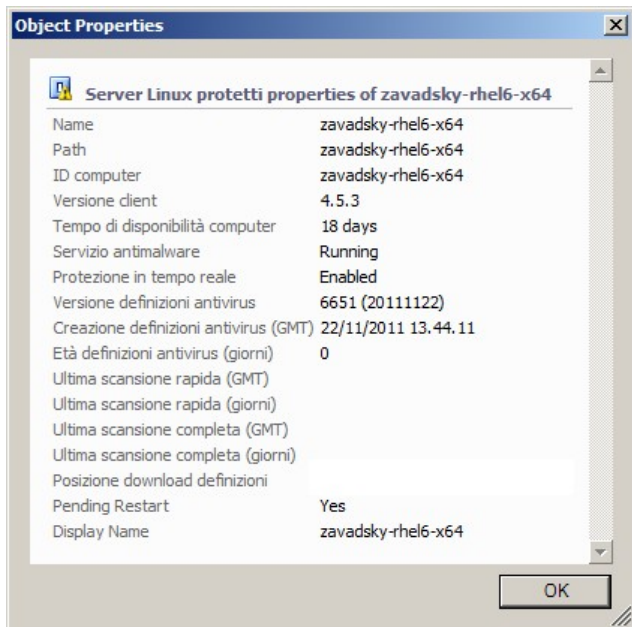
State	Name	Health
Warning	...	Healthy
Warning	...	Healthy
Warning	...	Healthy

State	Name	Health
Warning	...	Healthy
Warning	...	Healthy
Warning	...	Healthy

L'oggetto del server Linux protetto presenta le seguenti proprietà:

- **ID computer** - Identificatore del server, nome del dominio.
- **Nome visualizzato** - Nome del server, nome del dominio.
- **Versione client** - Versione del prodotto SCEP installato.
- **Tempo di disponibilità computer** - Il tempo di disponibilità del server (misura del tempo di funzionamento di una macchina senza tempi di inattività) è rappresentato dai dati vitali per il corretto funzionamento di un pacchetto di gestione. Pertanto, la sua assenza potrebbe indicare un errore nel pacchetto di gestione.
- **Servizio antimalware** - Stato di protezione antimalware (in esecuzione/non in esecuzione).
- **Protezione in tempo reale** - Stato di protezione in tempo reale, la cui assenza è indice di problemi SCEP.
- **Definizioni antivirus...** - Dati relativi allo stato del database delle firme antivirali (versione, data di creazione, età), la cui assenza è indice di problemi SCEP.
- **Ultima scansione rapida/completa...** - Dati relativi all'ultima scansione del computer. Se la scansione (Scansione rapida/Scansione completa) non è ancora stata eseguita, non comparirà alcun dato.
- **Posizione download definizioni** - Indirizzo/nome del server di aggiornamento. Le informazioni verranno visualizzate dopo il primo aggiornamento avvenuto con successo.
- **Riavvio in corso** - Informazioni relative alla necessità di riavviare il sistema per applicare le modifiche, dovuta a una nuova installazione o a modifiche apportate nella configurazione SCEP.



## Avvisi

Un avviso è un elemento che indica che si è verificata una situazione predefinita di una determinata gravità (rilevanza) su un oggetto monitorato. Gli avvisi sono definiti tramite regole. Nella console Operations Manager, in **Monitoring > System Center Endpoint Protection Linux > Avvisi attivi**, è disponibile una schermata che consente di visualizzare gli avvisi che l'utente della console ha diritto a visionare per un oggetto specifico.

**Nota:** Se più avvisi dello stesso tipo (ad es.: Malware attivo) vengono generati dallo stesso server, verrà visualizzato solo il primo (gli avvisi ridondanti vengono ignorati).

Avviso	Intervallo	Priorità	Gravità	Descrizione
Infezione da malware ripetuta	Basato su eventi	Elevata	Critica	L'avviso viene generato in caso di rilevazioni di infezioni da malware ripetute (3 occorrenze) in un intervallo temporale specifico (30 minuti). L'avviso contiene dati relativi al server e alle informazioni di base sul malware.
Malware pulito	Basato su eventi	Bassa Media	Informazioni - Pulizia di malware riuscita Allarme - È necessaria l'interazione dell'utente, ad es.: riavvio del server	Avvisa che l'operazione di pulizia di malware è riuscita. Contiene tutti i dati disponibili relativi al malware specifico. Ciascun malware rilevato genera un singolo evento. SCEP Linux assegna priorità e livello di gravità in base all'efficienza del processo di pulizia dove: Pulito = bassa + informazioni Pulito ma è necessaria un'azione (ad es.: riavvio) = media + allarme.
Malware attivo (da Monitoraggio)	Basato su eventi	Elevata	Critica	Avvisa che il malware non è stato pulito. Contiene tutti i dati disponibili relativi al malware specifico.
Malware attivo (da Regola)	Basato su eventi	Elevata/Media/ Bassa	Critica/Media/Bassa - basata su un tipo di Malware	Come sopra. Utilizzato per i connettori ad altri sistemi di monitoraggio/ biglietteria. <b>Nota:</b> questa regola (avviso) è disattivata per impostazione predefinita.
Il servizio antimalware di System Center Endpoint Protection non è attivo	300 secondi	Media	Critica	Avvisi relativi alla mancata disponibilità del servizio antimalware SCEP (scep_daemon). Comprende il rispettivo nome del server e la rispettiva versione SCEP.













Protezione antim malware disattivata	Basato su eventi	Media	Allarme	Avvisi relativi alla protezione antim malware disattivata. Comprende il rispettivo nome del server.
Protezione in tempo reale disattivata	Basato su eventi	Media	Allarme	Avvisi relativi alla protezione in tempo reale disattivata. Comprende il rispettivo nome del server.
Definizioni non aggiornate	Ogni 8 ore	Media	Avvertenza (età <= 5 giorni E età > 3 giorni) Critico (età > 5 giorni)	Avvisi relativi al database delle firme antivirali non aggiornato per più di 3 giorni. Comprende il rispettivo nome del server e la rispettiva età del database delle firme antivirali.
Attacco di malware	Basato su eventi	Elevata	Critica	Forefront Endpoint Protection ha rilevato più del 5% di malware attivi sui computer degli utenti. Potrebbe verificarsi una propagazione di malware sui computer degli utenti. Assicurarsi che tutti i server utilizzino le definizioni più aggiornate. Se si desidera modificare il numero di minacce attive che causano questo avviso, ignorare il parametro del monitoraggio Attacco di malware (vedere capitolo <a href="#">Esclusioni</a> ).

## Attività

Il pacchetto di gestione per SCEP implementa 13 attività. L'esecuzione di questa attività è immediata. I risultati vengono visualizzati subito dopo l'esecuzione delle attività oppure successivamente nella finestra Stato attività. Il tempo massimo richiesto per l'esecuzione delle attività è di 180 secondi. L'opzione di esclusione non è disponibile. Tutte le attività corrispondono a comandi BASH eseguiti tramite SSH.

È possibile invocare le attività sotto **Monitoring > Linux System Center Endpoint Protection > Server con SCEP** nel pannello sulla destra della finestra Operations Console.

### Server Linux protetti Tasks ▲

-  Aggiorna definizioni SCEP
-  Attiva protezione antivirus
-  Attiva protezione in tempo reale
-  Avvia servizio SCEP
-  Disattiva protezione antivirus
-  Disattiva protezione in tempo reale
-  Interrompi scansione
-  Interrompi servizio SCEP
-  Recupera impostazioni dell'endpoint
-  Riavvia servizio SCEP
-  Riavvio
-  Scansione completa
-  Scansione rapida

- **Disattiva protezione antivirus** - Disattiva tutti i componenti della protezione antivirus, disattiva la scansione su richiesta.
- **Attiva protezione antivirus** - Attiva tutti i componenti della protezione antivirus.
- **Disattiva protezione in tempo reale** - Disattiva la protezione in tempo reale.
- **Attiva protezione in tempo reale** - Attiva la protezione in tempo reale.
- **Scansione completa** - Aggiorna il database delle firme antivirali ed esegue una scansione del computer completa.
- **Rapida completa** - Aggiorna il database delle firme antivirali ed esegue una scansione del computer rapida.
- **Interrompi scansione** - Interrompe tutte le scansioni del computer in esecuzione.
- **Recupera impostazioni del server** - Consente di visualizzare lo stato attuale dei prodotti SCEP. L'elenco dei parametri visualizzati è identico alle proprietà dell'entità del server Linux protetto. I dati visualizzati non vengono trasferiti al server Linux protetto.
- **Riavvia servizio antimalware** - Riavvia il servizio antimalware SCEP (scep\_daemon).
- **Interrompi servizio antimalware** - Interrompe il servizio antimalware SCEP (scep\_daemon).
- **Avvia servizio antimalware** - Avvia il servizio antimalware SCEP (scep\_daemon).
- **Aggiorna definizioni antimalware** - Avvia l'aggiornamento del database delle firme antivirali.
- **Riavvio** - Riavvia il computer Linux.

## Configurazione del pacchetto di gestione per SCEP

### Procedura consigliata: creazione di un pacchetto di gestione per le personalizzazioni

Per impostazione predefinita, Operations Manager salva tutte le personalizzazioni, tra cui le esclusioni relative al pacchetto di gestione predefinito. Una procedura consigliata consiste invece nel creare un pacchetto di gestione separato per ciascun pacchetto di gestione bloccato che si desidera personalizzare.

Quando si crea un pacchetto di gestione per memorizzare le impostazioni personalizzate per un pacchetto di gestione bloccato, è utile basare il nome del nuovo pacchetto di gestione sul nome del pacchetto di gestione personalizzato, come ad esempio "Personalizzazioni SCEP 2012".

La creazione di un nuovo pacchetto di gestione per la memorizzazione delle personalizzazioni di ciascun pacchetto di gestione bloccato facilita l'esportazione delle personalizzazioni da un ambiente di test a un ambiente di produzione. Ciò rende anche più semplice eliminare un pacchetto di gestione, poiché, prima di poterlo eliminare, è necessario eliminare eventuali dipendenze. Se le personalizzazioni per tutti i pacchetti di gestione vengono salvate nel pacchetto di gestione predefinito e si desidera eliminare un solo pacchetto di gestione, è necessario prima eliminare il pacchetto di gestione predefinito; in questo modo, tuttavia, vengono eliminate anche le personalizzazioni effettuate agli altri pacchetti di gestione.

### Configurazione di sicurezza

Il computer deve eseguire il servizio SSHD ed è necessario aprire la porta SSH (valore predefinito 22). System Center 2012 Operations Manager effettua la connessione attraverso la porta ai computer remoti Linux utilizzando il Run As Account appropriato (collocato nel pannello **Administration > Run As Configuration** della console di monitoraggio Operations Manager) con il tipo **Basic Authentication**.

Nome profilo Esegui come	Note
Unix Privileged Account	Utilizzato per il monitoraggio da remoto del server Unix, nonché per il riavvio di processi che richiedono diritti privilegiati.

Questo pacchetto di gestione non utilizza Unix Action Account.

**Attenzione:** Il monitoraggio di computer attraverso l'account root presenta un rischio di sicurezza potenziale, ad es. in caso di rottura della password.

Se non si desidera utilizzare l'account root per il monitoraggio e la gestione, è possibile ricorrere ad un account utente standard che, a tal fine, dovrà essere in possesso dei diritti di esecuzione dei comandi *sudo*. Di conseguenza, per autorizzare l'elevazione sudo dell'account utente selezionato, nel file */etc/sudoers* di ciascuna workstation monitorata da Linux SCEP dovrà essere presente la seguente configurazione. Esempio di configurazione per il nome utente user1:

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

user1 ALL=(root) NOPASSWD: /opt/microsoft/scx/bin/scxlogfileviewer -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
#-----

```

## Sincronizzazione delle regole delle soglie prestazionali

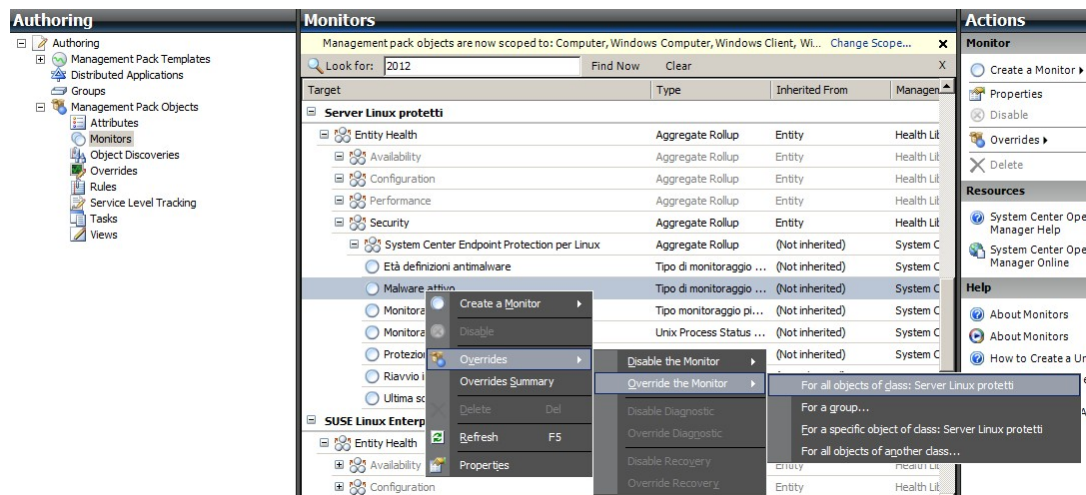
La seguente tabella contiene un elenco delle regole delle soglie prestazionali che presentano soglie predefinite che potrebbero richiedere un'ulteriore sincronizzazione per adattarsi all'ambiente specifico. Valutare queste regole per stabilire se le soglie predefinite sono appropriate per il proprio ambiente. Nel caso in cui una soglia predefinita non sia appropriata per l'ambiente specifico, sarà necessario modificare le soglie applicando un'esclusione:

Nome regola	Parametro esclusione	Soglia predefinita	Limitazioni sincronizzazione
Regola di infezione da malware ripetuta	Soglia conteggio infezioni ripetute	3 occorrenze	L'impostazione di un valore inferiore a 2 rende la regola obsoleta.
Regola di infezione da malware ripetuta	Finestra temporale infezioni ripetute	30 minuti	È sconsigliata l'impostazione del valore inferiore alla durata di una scansione su richiesta, poiché una sovrapposizione potrebbe impedire la generazione di un avviso.
Regola avviso Malware attivo	Attivato	Falso	È possibile attivare questo avviso in caso di utilizzo di connettori ad altri sistemi di monitoraggio/biglietteria.

## Esclusioni

È possibile utilizzare le esclusioni per rifinire le impostazioni di un oggetto di monitoraggio in System Center 2012 Operations Manager. Sono compresi monitoraggi, regole, rilevamenti di oggetti e attributi provenienti da pacchetti di gestione importati.

Per escludere un monitoraggio, in Operations Console fare clic sul pulsante **Authoring** ed espandere **Management Pack Objects > Monitors**. Nel pannello Monitoraggio, ricercare ed espandere completamente un tipo di oggetto, quindi fare clic su un monitoraggio e su **Overrides**.



Utilizzare la finestra Esclusioni per creare o modificare un'esclusione per un'occorrenza di uno dei seguenti parametri:

- **Tempo di fallback del monitoraggio di malware attivi** (correlato esclusivamente al monitoraggio Malware attivo)
- **Età definizioni antimalware** (correlato esclusivamente al monitoraggio Età definizioni antimalware)
- **Intervallo di rilevamento** (correlato esclusivamente al monitoraggio Età ultima scansione)
- **Avviso sullo stato**
- **Priorità avvisi**
- **Gravità avviso**
- **Avviso con risoluzione automatica**
- **Attivato** - Stabilire se il monitoraggio selezionato è attivo o inattivo.
- **Genera avvisi**
- **Percorso file di registro SCEP**

Nel caso in cui un'esclusione predefinita non sia appropriata per l'ambiente specifico, sarà necessario modificare le soglie applicando un'esclusione:

Parametro esclusione	Nome monitoraggio	Valore predefinito	Note ottimizzazione
Intervallo ping	Ping della macchina	3600 secondi	Intervallo che consente di verificare la disponibilità del server Linux protetto. Una durata più breve attiva più velocemente uno stato di Errore sul monitoraggio dell'Attacco di malware al server, qualora il funzionamento della macchina si arresti a causa di un attacco. Di conseguenza, il carico sulla rete, sul computer monitorato e sul server System Center 2012 Operations Manager aumenta.
Finestra temporale attacco malware	Attività malware	3600 secondi	Intervallo necessario al monitoraggio per rispedire lo stato Sicuro dopo l'attività di un malware. Per garantire un corretto funzionamento della combinazione, il valore del monitoraggio della finestra temporale dovrà essere superiore rispetto al Ping della macchina/Intervallo del ping. Qualora, durante l'intervallo della finestra temporale dell'attacco malware, un certo numero di computer che superano il valore percentuale dell'attacco malware impostato (vedere il paragrafo Attacco malware) registri un'attività malware, verrà generato un avviso di attacco malware.  Nota: Ciò è diverso dall'attacco di malware al server, che invece non genera un avviso.
Tempo di fallback del monitoraggio di malware attivi	Malware attivo	28800 secondi	Intervallo temporale a partire dal rilevamento del malware, dopo il quale il malware viene considerato pulito.
Percorso file di registro SCEP	Malware attivo	/var/log/scep/eventlog_scom.log	Percorso al file in cui sono registrati gli eventi System Center 2012 Operations Manager. Non modificare questo parametro a meno che non compaiano dei problemi.
Età critica definizioni antimalware	Età definizioni antimalware	5 giorni	Dopo questo intervallo, verrà generato un avviso di Errore in cui si segnala un prodotto SCEP non aggiornato.
Età condizioni di sicurezza definizioni antimalware	Età definizioni antimalware	3 giorni	Età massima consentita delle definizioni antimalware, durante la quale queste possono essere considerate aggiornate. Questo valore dovrà sempre essere inferiore al valore dell'Età critica delle definizioni antimalware.
Intervallo	Età definizioni antimalware	28800 secondi	Intervallo per la verifica dell'età delle definizioni antimalware.
Intervallo	Servizio antimalware	300 secondi	Intervallo per la verifica della disponibilità del servizio antimalware.
Nome del processo	Servizio antimalware	scep_daemon	Nome del servizio antimalware. Non modificare questo valore nel caso in cui sia attivo il monitoraggio.
Intervallo di rilevamento	Età ultima scansione	28800 secondi	Intervallo per la verifica dell'esecuzione dell'ultima scansione.
Età massima scansione	Età ultima scansione	7 giorni	Da configurare conformemente alle impostazioni dei prodotti SCEP. In caso di programmazione di una scansione ogni 7 giorni, impostare questo valore su 7 giorni.
Percorso file di registro	Riavvio in corso	/var/log/scep/eventlog_scom.log	Percorso al file in cui sono registrati gli eventi System Center 2012 Operations Manager. Non modificare questo parametro a meno che non compaiano dei problemi.
Percorso file di registro SCEP	Protezione in tempo reale	/var/log/scep/eventlog_scom.log	Percorso al file in cui sono registrati gli eventi System Center 2012 Operations Manager. Non modificare questo parametro a meno che non compaiano dei problemi.

Percentuale	Attacco di malware	95%	Percentuale di server dai Server Linux (protetti + non protetti) necessaria per ritornare lo stato Sicuro, per far sì che l'intero gruppo monitorato possa essere considerato Sicuro. In caso di rilevamento di malware su almeno il 5% del totale, sarà generato un attacco di malware.
-------------	--------------------	-----	--

Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
<input type="checkbox"/>	Alert On State	Enumeration	The monitor ...	The monitor is...	The monitor is...	[No change]
<input type="checkbox"/>	Alert Priority	Enumeration	High	High	High	[No change]
<input type="checkbox"/>	Alert severity	Enumeration	Match monit...	Match monito...	Match monitor...	[No change]
<input type="checkbox"/>	Auto-Resolve Alert	Boolean	False	False	False	[No change]
<input type="checkbox"/>	Enabled	Boolean	True	True	True	[No change]
<input type="checkbox"/>	Generates Alert	Boolean	True	True	True	[No change]
<input checked="" type="checkbox"/>	Percorso file di rapporto SCEP	String	/var/log/sc...	entlog_scom.dat	/var/log/scep...	[Added]
<input type="checkbox"/>	Tempo di fallback del monito...	Integer	28800	28800	28800	[No change]

**Nota:** Per ulteriori informazioni sulle Esclusioni, consultare [Come monitorare utilizzando le esclusioni](http://go.microsoft.com/fwlink/?LinkID=117777) (<http://go.microsoft.com/fwlink/?LinkID=117777>).

## Collegamenti

I collegamenti che seguono consentono all'utente di accedere alle informazioni relative alle attività comuni associate a questo pacchetto di gestione:

- [Gestione del ciclo di vita dei pacchetti di gestione](http://go.microsoft.com/fwlink/?LinkID=211463) (<http://go.microsoft.com/fwlink/?LinkID=211463>)
- [Come importare un pacchetto di gestione in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkID=142351) (<http://go.microsoft.com/fwlink/?LinkID=142351>)
- [Come monitorare utilizzando le esclusioni](http://go.microsoft.com/fwlink/?LinkID=117777) (<http://go.microsoft.com/fwlink/?LinkID=117777>)
- [Come creare un account Esegui come in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkID=165410) (<http://go.microsoft.com/fwlink/?LinkID=165410>)
- [Configurazione di un account Esegui come multipiattaforma](http://go.microsoft.com/fwlink/?LinkID=160348) (<http://go.microsoft.com/fwlink/?LinkID=160348>)
- [Come modificare un profilo Esegui come esistente](http://go.microsoft.com/fwlink/?LinkID=165412) (<http://go.microsoft.com/fwlink/?LinkID=165412>)
- [Come esportare le personalizzazioni dei pacchetti di gestione](http://go.microsoft.com/fwlink/?LinkID=209940) (<http://go.microsoft.com/fwlink/?LinkID=209940>)
- [Come eliminare un pacchetto di gestione](http://go.microsoft.com/fwlink/?LinkID=209941) (<http://go.microsoft.com/fwlink/?LinkID=209941>)
- [Come gestire i dati di monitoraggio utilizzando Ambito, Cerca e Trova](http://go.microsoft.com/fwlink/?LinkID=91983) (<http://go.microsoft.com/fwlink/?LinkID=91983>)
- [Monitoraggio di Linux con SCOM 2007 R2](http://blogs.technet.com/b/birojitrn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx) (<http://blogs.technet.com/b/birojitrn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx>)
- [Installazione manuale di agenti multipiattaforma](http://technet.microsoft.com/en-us/library/dd789016.aspx) (<http://technet.microsoft.com/en-us/library/dd789016.aspx>)
- [Configurazione dell'elevazione sudo per UNIX e del monitoraggio di Linux con System Center 2012 - 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) (<http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx>)

Per domande relative a Operations Manager e ai pacchetti di monitoraggio, consultare la pagina [Forum System Center Operations Manager](http://go.microsoft.com/fwlink/?LinkID=179635) (<http://go.microsoft.com/fwlink/?LinkID=179635>).

Una risorsa utile è rappresentata dal collegamento [Unleashed blog System Center Operations Manager](http://opsmgrunleashed.wordpress.com/) (<http://opsmgrunleashed.wordpress.com/>), contenente post ordinati "Per esempi" per specifici pacchetti di monitoraggio.

Per ulteriori informazioni relative a Operations Manager, si rimanda ai seguenti blog:

- [Blog team Operations Manager](http://blogs.technet.com/momteam/default.aspx)  
(<http://blogs.technet.com/momteam/default.aspx>)
- [Blog OpsMgr di Kevin Holman](http://blogs.technet.com/kevinholman/default.aspx)  
(<http://blogs.technet.com/kevinholman/default.aspx>)
- [Opinioni su OpsMgr](http://thoughtsonopsmgr.blogspot.com/)  
(<http://thoughtsonopsmgr.blogspot.com/>)
- [Blog di Raphael Burri](http://rburri.wordpress.com/)  
(<http://rburri.wordpress.com/>)
- [Spazio gestione di BWren](http://blogs.technet.com/brianwren/default.aspx)  
(<http://blogs.technet.com/brianwren/default.aspx>)
- [Blog team di assistenza System Center Operations Manager](http://blogs.technet.com/operationsmgr/)  
(<http://blogs.technet.com/operationsmgr/>)
- [Ops Mgr ++](http://blogs.msdn.com/boris_yanushpolsky/default.aspx)  
([http://blogs.msdn.com/boris\\_yanushpolsky/default.aspx](http://blogs.msdn.com/boris_yanushpolsky/default.aspx))
- [Note su System Center Operations Manager](http://blogs.msdn.com/mariussutara/default.aspx)  
(<http://blogs.msdn.com/mariussutara/default.aspx>)

Per la risoluzione dei problemi, consultare i thread dei seguenti forum:

- [Microsoft.Unix.Library mancante](http://social.technet.microsoft.com/Forums/en-US/operationsmanagemgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)  
(<http://social.technet.microsoft.com/Forums/en-US/operationsmanagemgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/>)