System Center Endpoint Protection

Manuale di installazione e Guida utente

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

Microsoft

Microsoft® System Center Endpoint Protection

Contenuti

Introduzione

Grazie per aver scelto System Center Endpoint Protection. Il motore di scansione d'avanguardia Microsoft è caratterizzato da una velocità di scansione e da percentuali di rilevamento senza pari combinati con un impatto estremamente ridotto che fanno di questo prodotto la soluzione ideale per qualsiasi server del sistema operativo Linux.

Funzionalità principale

Scansione su richiesta

La scansione su richiesta può essere avviata da un utente con privilegi (generalmente un amministratore di sistema) attraverso l'interfaccia della riga di comando o l'interfaccia web oppure dallo strumento di pianificazione automatica del sistema operativo (ad es.:cron). Il termine *su richiesta* si riferisce agli oggetti del file system sottoposti a scansione sulla base della richiesta dell'utente o del sistema.

Protezione in tempo reale

La protezione in tempo reale viene invocata in caso di tentativi di accesso agli oggetti del file system da parte di un utente e/o di un sistema operativo. Ciò consente anche di chiarire il termine *on-access*, in quanto una scansione viene avviata da un tentativo di accesso agli oggetti del file system.

Caratteristiche principali del sistema

Algoritmi avanzati del motore

Gli algoritmi del motore di scansione antivirus Microsoft offrono la percentuale di rilevamento più elevata e i tempi di scansione più rapidi in assoluto.

Multielaborazione

System Center Endpoint Protection è stato sviluppato per girare su unità con processore singolo o multiprocessore.

Euristica avanzata

System Center Endpoint Protection prevede un'euristica avanzata unica per worm Win32, infezioni backdoor e altre forme di malware.

Caratteristiche integrate

Archiviatori integrati consentono di decomprimere oggetti archiviati senza richiedere programmi esterni.

Velocità ed efficienza

Per aumentare la velocità e l'efficienza del sistema, l'architettura di System Center Endpoint Protection si basa sul daemon in esecuzione (programma residente) al quale vengono inviate tutte le richieste di scansione.

Sicurezza avanzata

Per una maggiore sicurezza, tutti i daemon esecutivi (ad eccezione di scep_dac) funzionano sotto un account utente senza privilegi.

Configurazione selettiva

Il sistema supporta una configurazione selettiva basata sull'utente o sul client/server.

Livelli di registrazione multipli

Possono essere configurati livelli di registrazione multipli per ottenere informazioni sull'attività e sulle infiltrazioni del sistema.

Interfaccia Web

La configurazione e l'amministrazione sono offerte tramite un'interfaccia web intuitiva e di facile utilizzo.

Assenza di librerie esterne

L'installazione di System Center Endpoint Protection non richiede librerie o programmi esterni ad eccezione di LIBC.

Notifica definita dall'utente

Il sistema può essere configurato in modo da informare utenti specifici in caso di rilevamento di infiltrazioni o di altri eventi importanti.

Bassi requisiti di sistema

Per un corretto funzionamento, System Center Endpoint Protection richiede appena 16MB di spazio libero su disco rigido e 32MB di RAM. L'applicazione funziona bene con le versioni del kernel 2.2.x, 2.4.x e 2.6.x del sistema operativo Linux.

Prestazioni e scalabilità

Da server meno potenti per uffici di piccole dimensioni a server ISP a livello aziendale caratterizzati da migliaia di utenti, System Center Endpoint Protection offre le prestazioni e la scalabilità che ci si aspetta da una soluzione UNIX, oltre alla sicurezza ineguagliabile dei prodotti di sicurezza Microsoft.

Terminologia e abbreviazioni

In questa sezione, analizzeremo i termini e le abbreviazioni utilizzati nel presente documento. Si noti che il font grassetto è riservato ai nomi dei componenti dei prodotti nonché ai termini e alle abbreviazioni definiti di recente. I termini e le abbreviazioni definiti in questo capitolo verranno spiegati in maggiori dettagli più avanti.

SCEP

SCEP è un acronimo standard per il prodotto di sicurezza sviluppato da Microsoft per i sistemi operativi Linux. È anche il nome del pacchetto software contenente i prodotti.

SCEP daemon

Controllo del sistema e daemon di scansione SCEP principali: *scep_daemon*.

Directory principale SCEP

Directory nella quale sono salvati i moduli SCEP caricabili contenenti il database delle firme antivirali. L'abbreviazione *@BASEDIR@* verrà utilizzata per riferimenti futuri a questa directory. Il valore *@BASEDIR@* (che dipende dal sistema operativo) è elencato di seguito:

```
Linux: /var/opt/microsoft/scep/lib
```

Directory di configurazione SCEP

Directory in cui sono salvati tutti i file relativi alla configurazione di System Center Endpoint Protection. L'abbreviazione *@ETCDIR@* verrà utilizzata per riferimenti futuri a questa directory. Il valore *@ETCDIR@* (che dipende dal sistema operativo) è elencato di seguito:

```
Linux: /etc/opt/microsoft/scep
```

File di configurazione SCEP

File di configurazione principale di System Center Endpoint Protection. Il percorso assoluto di questo file è il seguente:

@ETCDIR@/scep.cfg

Directory dei file binari SCEP

Directory in cui sono salvati i file binari System Center Endpoint Protection pertinenti. L'abbreviazione *@BINDIR@* verrà utilizzata per riferimenti futuri a questa directory. Il valore *@BINDIR@* (che dipende dal sistema operativo) è elencato di seguito:

```
Linux: /opt/microsoft/scep/bin
```

Directory dei file binari del sistema SCEP

Directory in cui sono salvati i file binari del sistema System Center Endpoint Protection pertinenti. L'abbreviazione *@SBINDIR@* verrà utilizzata per riferimenti futuri a questa directory. Il valore *@SBINDIR@* (che dipende dal sistema operativo) è elencato di seguito:

```
Linux: /opt/microsoft/scep/sbin
```

Directory dei file degli oggetti SCEP

Directory in cui sono salvati i file e le librerie degli oggetti System Center Endpoint Protection pertinenti. L'abbreviazione *@LIBDIR@* verrà utilizzata per riferimenti futuri a questa directory. Il valore *@LIBDIR@* (che dipende dal sistema operativo) è elencato di seguito:

```
Linux: /opt/microsoft/scep/lib
```

Installazione

System Center Endpoint Protection viene distribuito come file binario:

```
scep.i386.ext.bin
```

Nel file binario visualizzato in alto, *'ext'* è un Linux suffisso che dipende dalla distribuzione del sistema operativo, ovvero, "deb" per Debian, "rpm" per RedHat e SuSE, "tgz" per altre distribuzioni del sistema operativo Linux.

Per installare il prodotto o passare a una versione successiva, utilizzare il seguente comando:

```
sh ./scep.i386.ext.bin
```

per visualizzare l'Accordo di accettazione della licenza per l'utente del prodotto. Dopo aver confermato l'Accordo di accettazione, il pacchetto di installazione verrà posizionato nella directory di lavoro corrente e verranno visualizzate sullo schermo le informazioni pertinenti relative all'installazione, alla disinstallazione o all'upgrade del pacchetto.

Dopo aver installato il pacchetto, è possibile verificare il funzionamento del servizio principale SCEP utilizzando il seguente comando:

```
ps -C scep_daemon
```

Dopo aver premuto INVIO, l'utente dovrebbe visualizzare il seguente messaggio (o un messaggio simile):

```
 PID TTY TIME CMD
2226 ? 00:00:00 scep_daemon
2229 ? 00:00:00 scep_daemon
```

Sono attivi almeno due processi daemon SCEP in background. Il primo PID rappresenta la gestione dei processi e delle minacce del sistema. L'altro rappresenta il processo di scansione SCEP.

Installazione di un pacchetto lingue

Per installare il pacchetto lingue richiesto per System Center Endpoint Protection, utilizzare il seguente comando:

```
sh ./scep-lang.lng.bin
```

dove *'lng'* deve essere sostituito dal codice della lingua del file che si desidera importare.

Dopo che verrà visualizzata la notifica *Installation completed successfully*, aggiornare la variabile di sistema LANG di conseguenza e aggiornare l'ambiente, se necessario. Tale operazione consente di terminare l'installazione del pacchetto lingue.

Ciascun pacchetto lingue contiene i seguenti elementi:

- Interfaccia web localizzata
- Risultati della console localizzata degli agenti e dei comandi SCEP.
- Documentazione localizzata in formato PDF

Panoramica architettura

Dopo aver installato correttamenteSystem Center Endpoint Protection, l'utente dovrà acquisire dimestichezza con l'architettura del prodotto.

Il sistema è composto dalle seguenti parti:

ARCHITETTURA

L'architettura di System Center Endpoint Protection è rappresentata dallo SCEP daemon (scep_daemon). Il daemon utilizza la libreria API SCEP libscep.so e i moduli di caricamento SCEP em00X_xx.dat per fornire attività di base del sistema tra cui scansione, manutenzione dei processi daemon degli agenti, manutenzione del sistema di invio dei campioni, registrazione, notifica, ecc. Per ulteriori informazioni, si prega di consultare la pagina dei manuali *scep_daemon(8)* .

AGENTI

L'obiettivo dei moduli degli agenti SCEP consiste nell'integrazione di SCEP con l'ambiente del server Linux.

UTILITY

I moduli delle utility offrono una gestione del sistema semplice ed efficace. Essi sono responsabili delle attività di sistema, tra cui la gestione della quarantena, la configurazione e l'aggiornamento del sistema.

CONFIGURAZIONE

Una corretta configurazione rappresenta l'aspetto più importante di un sistema di sicurezza. Il resto del presente capitolo è dedicato alla spiegazione di tutti i componenti correlati. Inoltre, si consiglia vivamente di comprendere a pieno il funzionamento del file *scep.cfg*, in quanto contiene informazioni essenziali per la configurazione di System Center Endpoint Protection.

Dopo aver installato correttamente il prodotto, tutti i componenti della configurazione verranno memorizzati nella directory di configurazione SCEP. La directory è composta dai seguenti file:

@ETCDIR@/scep.cfg

Si tratta del file di configurazione più importante, in quanto controlla tutti gli aspetti principali della funzionalità del prodotto. Il file scep.cfg è composto da varie sezioni, ciascuna delle quali contiene vari parametri. Il file contiene una sezione globale e varie sezioni "agenti", i cui nomi sono compresi tra parentesi quadre. I parametri nella sezione globale sono utilizzati per la definizione delle opzioni di configurazione per il daemon SCEP nonché dei valori predefiniti per la configurazione del motore di scansione SCEP. I parametri nelle sezioni degli agenti sono utilizzati per la definizione di opzioni di configurazione di moduli in grado di intercettare vari tipi di flussi dati nel computer e/o nei relativi dispositivi vicini e di prepararli per la scansione. Si noti che oltre ai vari parametri utilizzati per la configurazione del sistema, esistono anche regole che disciplinano l'organizzazione del file. Per ulteriori informazioni sul metodo più efficace di organizzazione di questo file, si prega di consultare*scep.cfg(5)* e le pagine dei manuali*scep_daemon(8)*, nonché la pagina dei manuali dei relativi agenti.

@ETCDIR@/certs

Questa directory viene utilizzata per l'archiviazione dei certificati utilizzati dall'interfaccia web SCEP ai fini dell'autenticazione. Per ulteriori informazioni, si prega di consultare la pagina dei manuali *scep_wwwi(8)*.

@ETCDIR@/scripts/daemon_notification_script

Se abilitato dal parametro del file di configurazione SCEP *'exec_script'*, questo script verrà eseguito in caso di rilevamento di un'infiltrazione da parte del sistema antivirus. Lo script viene utilizzato per l'invio di e-mail di notifica sull'evento all'amministratore del sistema.

Integrazione con i servizi file system

Il presente capitolo contiene una descrizione della configurazione della protezione su richiesta e in tempo reale che offrirà la protezione antivirus e la protezione contro le infezioni del sistema dai file worm più efficaci. Le capacità di scansione di System Center Endpoint Protection derivano dal comando di scansione su richiesta *"scep_scan"* e dal comando di scansione on access *"scep_dac"*. La versione Linux di System Center Endpoint Protection offre una tecnica di scansione on-access aggiuntiva che utilizza il modulo della libreria precaricata *libscep_pac.so*. Tutti questi comandi sono descritti nelle sezioni successive.

Scansione su richiesta

La scansione su richiesta può essere avviata da un utente con privilegi (generalmente un amministratore di sistema) attraverso l'interfaccia della riga di comando o l'interfaccia web oppure dallo strumento di pianificazione automatica del sistema operativo (ad es.:cron). Il termine *su richiesta* si riferisce agli oggetti del file system sottoposti a scansione sulla base della richiesta dell'utente o del sistema.

La scansione su richiesta non richiede una configurazione speciale per funzionare. Dopo aver installato correttamente il pacchetto SCEP, è possibile eseguire immediatamente la scansione su richiesta utilizzando l'interfaccia della riga di comando o lo strumento della pianificazione attività. Per eseguire la scansione su richiesta dalla riga di comando, utilizzare la seguente sintassi:

```
@SBINDIR@/scep_scan [option(s)] FILES
```

dove FILE rappresenta un elenco di directory e/o di file da sottoporre a scansione.

Sono disponibili varie opzioni della riga di comando utilizzando la scansione su richiesta SCEP. Per visualizzare l'elenco completo delle opzioni, si prega di consultare la pagina dei manuali *scep_scan(8)*.

Protezione in tempo reale basata su tecnologia Dazuko

La protezione in tempo reale viene invocata dall'accesso degli utenti e/o del sistema operativo agli oggetti del file system. Ci consente di spiegare anche il termine *on-access*: la scansione viene avviata all'occasione di eventuali tentativi di accesso a un oggetto del file system selezionato.

La tecnica utilizzata dalla scansione on-access SCEP è attuata dal modulo del kernel Dazuko (da-tzu-ko) ed è basata sull'intercettazione di chiamate del kernel. Il progetto Dazuko è libero e ciò significa che il codice sorgente è distribuito gratuitamente. Ciò consente agli utenti di compilare il modulo del kernel per i propri kernel personalizzati. Si noti che il modulo del kernel Dazuko non fa parte dei prodotti SCEP e deve essere compilato e installato all'interno del kernel prima dell'utilizzo del comando on-access *scep_dac*. La tecnica Dazuko rende la scansione on-access indipendente dal tipo di file system utilizzato. Tale tecnica è anche adatta per la scansione di oggetti del file system attraverso Network File System (NFS), Nettalk e Samba.

Importante: Prima di fornire informazioni dettagliate relative alla configurazione e all'uso della scansione on-access, è importante notare che la scansione è stata principalmente sviluppata e testata allo scopo di proteggere file system installati esternamente. In caso di file system multipli non installati esternamente, sarà necessario escluderli dal controllo dell'accesso file allo scopo di impedire blocchi del sistema. Un esempio di directory tipica da escludere è rappresentato dalla directory *"/dev"* e da qualsiasi directory utilizzata da SCEP.

Principio di funzionamento

La protezione in tempo reale *scep_dac* (SCEP Dazuko-powered file Access Controller) è un programma residente in grado di offrire un monitoraggio e un controllo ininterrotti del file system. Ogni oggetto del file system viene sottoposto a scansione in base ai tipi di eventi di accesso file personalizzabili. Sono supportati dalla versione corrente i seguenti tipi di evento:

Eventi di apertura

Per attivare questo tipo di accesso file, impostare il valore di apertura del parametro *'event_mask'* nella sezione **[fac]** del file scep.cfg. Ciò attiverà la parte ON_OPEN della maschera di accesso Dazuko.

Eventi di chiusura

Per attivare questo tipo di accesso file, impostare il valore di chiusura del parametro *'event_mask'* nella sezione **[fac]** del file scep.cfg. Ciò attiverà la parte ON_OPEN della maschera di accesso Dazuko. Ciò attiverà la parte ON_CLOSE e ON_CLOSE_MODIFIED della maschera di accesso Dazuko.

Nota: talune versioni del kernel del sistema operativo non supportano l'intercettazione di eventi ON_CLOSE. In questi casi, gli eventi di chiusura non saranno monitorati da *scep_dac*.

Eventi di esecuzione

Per attivare questo tipo di accesso file, impostare il valore di esecuzione del parametro *'event_mask'* nella sezione **[fac]** del file scep.cfg. Ciò attiverà la parte ON_EXEC della maschera di accesso Dazuko.

La protezione in tempo reale garantisce un'immediata scansione di tutti i file aperti, chiusi ed eseguiti da parte di *scep_daemon* per la ricerca di eventuali virus. In base ai risultati della scansione, verrà negato o consentito l'accesso a file specifici.

Installazione e configurazione

Il modulo del kernel Dazuko deve essere compilato e installato all'interno del kernel in esecuzione prima dell'inizializzazione di*scep_dac*. Per ulteriori informazioni sulle modalità di compilazione e di installazione di Dazuko, si prega di consultare:

http://www.dazuko.org

Dopo aver installato Dazuko, rivedere e modificare le sezioni **[globale]** e **[fac]** del file di configurazione SCEP (scep.cfg). Si noti che il corretto funzionamento della protezione in tempo reale dipende dalla configurazione dell'opzione*'agent_type'* all'interno della sezione **[fac]** di questo file. Inoltre, sarà necessario definire gli oggetti del file system (ad es.: le directory e i file) che devono essere monitorati dalla protezione in tempo reale. Tale operazione potrà essere eseguita attraverso la definizione dei parametri delle opzioni *"ctl_incl"* e *"ctl_excl"* che sono anche collocate all'interno della sezione **[fac]**. Dopo aver modificato il file scep.cfg, è possibile forzare la rilettura della nuova configurazione attraverso un ulteriore caricamento del daemon SCEP.

Suggerimenti

Per assicurarsi che il modulo Dazuko venga caricato prima dell'inizializzazione del daemon *scep_dac*, seguire la procedura sottostante:

Posizionare una copia del modulo Dazuko in una delle seguenti directory riservate ai moduli kernel:

```
/lib/modules
```

oppure

```
/modules
```

Utilizzare le utility del kernel 'depmod' e'modprobe' (Per il sistema operativo BSD, utilizzare'kldconfig' e 'kldload') per gestire le dipendenze e inizializzare correttamente il modulo Dazuko aggiunto di recente.

Nello script di inizializzazione scep_daemon '/etc/init.d/scep_daemon', inserire la seguente stringa prima dell'istruzione di inizializzazione del daemon:

```
/sbin/modprobe dazuko
```

Per il sistema operativo BSD, la stringa

```
/sbin/kldconfig dazuko
```

deve essere inserita nello script '/usr/local/etc/rc.d/scep_daemon.sh'.

Avvertenza È assolutamente importante seguire questa procedura nell'ordine corretto indicato. Se il modulo kernel non è posizionato all'interno della directory dei moduli kernel, questo non verrà caricato correttamente e ciò determinerà un blocco del sistema.

Protezione in tempo reale tramite l'utilizzo della libreria LIBC precaricata

Nelle sezioni precedenti, abbiamo descritto l'integrazione della protezione in tempo reale basata su tecnologia Dazuko con servizi di file system Linux/BSD. L'utilizzo di Dazuko potrebbe non essere possibile in tutte le situazioni, comprese quelle relative agli amministratori di sistema che gestiscono sistemi critici in cui:

- il codice sorgente e/o i file di configurazione correlati al kernel in esecuzione non sono disponibili,
- il kernel è più monolitico che modulare,
- il modulo Dazuko semplicemente non supporta il sistema operativo specifico.

In ognuno di questi casi, deve essere utilizzata la tecnica di scansione on-access basata sulla libreria LIBC precaricata. Per ulteriori informazioni, leggere gli argomenti che seguono nella presente sezione. Si noti che questa sezione riguarda esclusivamente gli utenti del sistema operativo Linux e contiene informazioni relative al funzionamento, all'installazione e alla configurazione della scansione on-access tramite l'utilizzo della libreria precaricata *'libscep_pac.so'*.

Principio di funzionamento

La protezione in tempo reale *libscep_pac.so* (SCEP Preload library based file Access Controller) rappresenta una libreria di oggetti condivisi attivata all'avvio del sistema. Questa libreria viene utilizzata per le chiamate della libreria LIBC da parte dei server del file system tra cui il server FTP, il server Samba, ecc.. Ogni oggetto del file system è sottoposto a scansione in base ai tipi di eventi di accesso file personalizzabili. Sono supportati dalla versione corrente i seguenti tipi di evento:

Eventi di apertura

Questo tipo di accesso file è attivato in caso di presenza della parola *'open'* nel parametro *'event_mask'* del file esest.cfg (**sezione [fac]**).

Eventi di chiusura

Questo tipo di accesso file è attivato in caso di presenza della parola *'close'* nel parametro *'event_mask'* del file scep.cfg (**sezione [fac]**). In questo caso, vengono intercettate tutte le funzioni di descrittore di file e di chiusura del flusso di FILE della libreria LIBC.

Eventi di esecuzione

Questo tipo di accesso file è attivato in caso di presenza della parola *'exec'* nel parametro *'event_mask'* del file scep.cfg (**sezione [fac]**). In questo caso, vengono intercettate tutte le funzioni di esecuzione della libreria LIBC.

Tutti i file aperti, chiusi ed eseguiti vengono sottoposti a scansione da parte del daemon SCEP per la ricerca di virus. In base al risultato di queste scansioni, verrà negato o consentito l'accesso a file specifici.

Installazione e configurazione

L'installazione del modulo della libreria *libscep_pac.so* avviene tramite l'utilizzo di un meccanismo di installazione standard delle librerie precaricate. È necessario definire la variabile d'ambiente *'LD_PRELOAD'* con il percorso assoluto alla libreria *libscep_pac.so*. Per ulteriori informazioni, si prega di consultare la pagina dei manuali *ld.so(8)*.

Nota: È importante che la variabile d'ambiente *"LD_PRELOAD"* venga definita esclusivamente per i processi del daemon del server di rete (ftp, Samba, ecc.) che saranno controllati dalla protezione in tempo reale. Generalmente, si sconsiglia il precaricamento delle chiamate della libreria LIBC per tutti i processi del sistema operativo, in quanto ciò potrebbe determinare un rallentamento significativo delle prestazioni del sistema o persino un blocco dello stesso. In questo senso, non dovrà né essere utilizzato il file '/etc/ld.so.preload' né esportata a livello globale la variabile d'ambiente "LD_PRELOAD". Entrambe le operazioni annullerebbero tutte le relative chiamate della LIBC e ciò potrebbe condurre a blocchi del sistema durante l'inizializzazione.

Per garantire l'intercettazione delle sole chiamate di accesso ai file rilevanti all'interno di un file system specifico, è possibile ignorare le istruzioni eseguibili utilizzando la seguente stringa:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

dove "COMMAND COMMAND-ARGUMENTS" rappresenta l'istruzione eseguibile originale.

Rivedere e modificare le sezioni **[globale]** e **[fac]** del file di configurazione SCEP (scep.cfg). Per garantire un corretto funzionamento della scansione on-access, è necessario definire gli oggetti del file system (ad es:. directory e file) che devono essere controllati dalla libreria precaricata. È possibile raggiungere tale obiettivo definendo i parametri delle opzioni *"ctl_incl"* e *"ctl_excl"* nella sezione **[fac]** del file di configurazione SCEP. Dopo aver modificato il file scep.cfg, è possibile forzare la rilettura della nuova configurazione attraverso un ulteriore caricamento del daemon SCEP.

Suggerimenti

Per attivare la protezione in tempo reale subito dopo l'avvio del file system, è necessario definire la variabile d'ambiente*'LD_PRELOAD'* all'interno dello script di inizializzazione del server del file di rete appropriato.

Esempio: Supponiamo di voler eseguire una scansione on-access per monitorare tutti gli eventi di accesso al file system subito dopo l'avvio del server Samba. All'interno dello script di inizializzazione del daemon Samba (/etc/init.d/smb), sostituiremo l'istruzione

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

con la seguente stringa:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

In tal modo, saranno scansionati gli oggetti del file system selezionato controllati dal server Samba all'avvio del sistema.

Meccanismi SCEP importanti

Criteri di gestione degli oggetti

Il meccanismo dei criteri di gestione degli oggetti consente di filtrare gli oggetti sottoposti a scansione in base allo stato. Questa funzionalità si basa sulle seguenti opzioni di configurazione:

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Per ulteriori informazioni su queste opzioni, si prega di consultare la pagina dei manuali *scep.cfg(5)*.

Ogni oggetto sottoposto a scansione viene gestito dapprima in base alla configurazione dell'opzione *"action_av"*. Se questa opzione è impostata su *'accept'* (oppure *'defer'*, *'discard'*, *'reject'*) l'oggetto verrà accettato (oppure inoltrato, scartato o rifiutato). Se l'opzione è impostata su *"scansione"*, l'oggetto verrà sottoposto a scansione per la ricerca di infiltrazioni di virus e se l'opzione *"av_clean_mode"* è impostata su *"sì"*, l'oggetto verrà anche ripulito. Inoltre, verranno considerate le opzioni di configurazione *"action_av_infected"*, *"action_av_notscanned"* e *"action_av_deleted"* per un'ulteriore valutazione della gestione dell'oggetto. Se è stata intrapresa un'azione *'accept'* come risultato di queste tre opzioni di azione, l'oggetto verrà accettato. In caso contrario, l'oggetto verrà bloccato.

Configurazione specifica per l'utente

L'obiettivo del meccanismo di configurazione specifica per l'utente consiste nel fornire un maggior livello di personalizzazione e funzionalità. Tale strumento consente all'amministratore di sistema di definire i parametri di scansione antivirus SCEP basati sull'utente che accede agli oggetti del file system.

È possibile trovare una descrizione dettagliata di questa funzionalità nella pagina dei manuali *scep.cfg(5)* . In questa sezione forniremo solo un breve esempio di una configurazione specifica per l'utente.

In questo esempio, l'obiettivo consiste nell'uso del modulo *scep_dac* per il controllo degli eventi di accessoON_OPEN e ON_EXEC per un disco esterno installato in una directory/home. È possibile configurare il modulo nella sezione **[fac]** del file di configurazione SCEP. Vedere quanto segue:

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

Per specificare le impostazioni di scansione per un singolo utente, è necessario che il parametro*'user_config'* specifichi il nome del file della configurazione speciale in cui verranno salvate le singole regole di scansione. Nell'esempio visualizzato in questa sezione, il file di configurazione speciale è chiamato *'scep_dac_spec.cfg'* ed è posizionato all'interno della directory di configurazione SCEP (questa directory si basa sul sistema operativo dell'utente. Si prega di consultare la pagina Terminologia e abbreviazioni).

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

Dopo aver specificato il parametro del file *'user_config'* all'interno della sezione **[fac]**, è necessario creare il file *'scep_dac_spec.cfg'* nella directory di configurazione SCEP. Infine, aggiungere le regole di scansione desiderate.

```
[username]
action_av = "reject"
```

Nella parte superiore della sezione speciale, inserire il nome utente sul quale verranno applicate le singole regole. Questa configurazione consentirà ad altri utenti che tentano di accedere al file system di essere elaborati normalmente. Ad esempio, tutti gli oggetti dei file system nei confronti dei quali viene eseguito l'accesso da altri utenti saranno sottoposti a scansione per il rilevamento di infiltrazioni, ad eccezione per il *"nome utente"* dell'utente, il cui accesso verrà rifiutato (bloccato).

Pianificazione attività

La funzionalità della pianificazione attività comprende l'esecuzione di attività programmate a orari specifici o su eventi specifici, la gestione e il lancio di attività con configurazioni e proprietà predefinite e molto altro ancora. La configurazione e le proprietà delle attività possono essere utilizzate per influenzare le date e le ore dei lanci, ma anche per espandere l'applicazione di attività tramite l'introduzione dell'uso di profili personalizzati durante l'esecuzione delle attività stesse.

L'opzione *'scheduler_tasks'* è commentata per impostazione predefinita e ciò causa l'applicazione della configurazione della pianificazione attività predefinita. Nel file di configurazione SCEP, tutti i parametri e le attività sono separati da punti e virgola. Altri eventuali punti e virgola (e barre inverse) non devono essere accompagnati da barre inverse. Ciascuna attività contiene 6 parametri e la sintassi è la seguente:

- id- numero unico.
- nome - descrizione dell'attività.
- flag - i flag speciali per la disattivazione della specifica attività di pianificazione possono essere impostati qui.
- failstart - istruzione che indica le operazioni da compiere in caso di impossibilità di esecuzione dell'attività all'orario programmato.
- datespec - Specifica di data regolare con 6 (crontab simile all'anno esteso) campi, la data ricorrente o l'opzione del nome di un evento.
- comando - può rappresentare un percorso assoluto a un comando seguito dai relativi argomenti o il nome di un comando speciale con il prefisso "@" (ad es.: aggiornamento antivirus: *@update*).

```
#scheduler_tasks = "id;nome;flag;failstart;datespec;comando;id2;nome2;...";
```

È possibile utilizzare i seguenti nomi di eventi al posto dell'opzione datespec:

- avvio - avvio del daemon.
- startonce - avvio del daemon ma almeno una volta al giorno.
- motore - aggiornamento del motore efficace.
- accesso - avvio dell'accesso all'interfaccia web.
- minaccia - minaccia rilevata.
- notscanned - File non scansionato.

Per visualizzare la configurazione della pianificazione attività corrente, utilizzare l'Interfaccia web o eseguire il seguente comando:

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

Per una descrizione completa della pianificazione attività e dei relativi parametri, consultare la sezione Pianificazione attività della pagina dei manuali*scep_daemon(8)*.

Interfaccia web

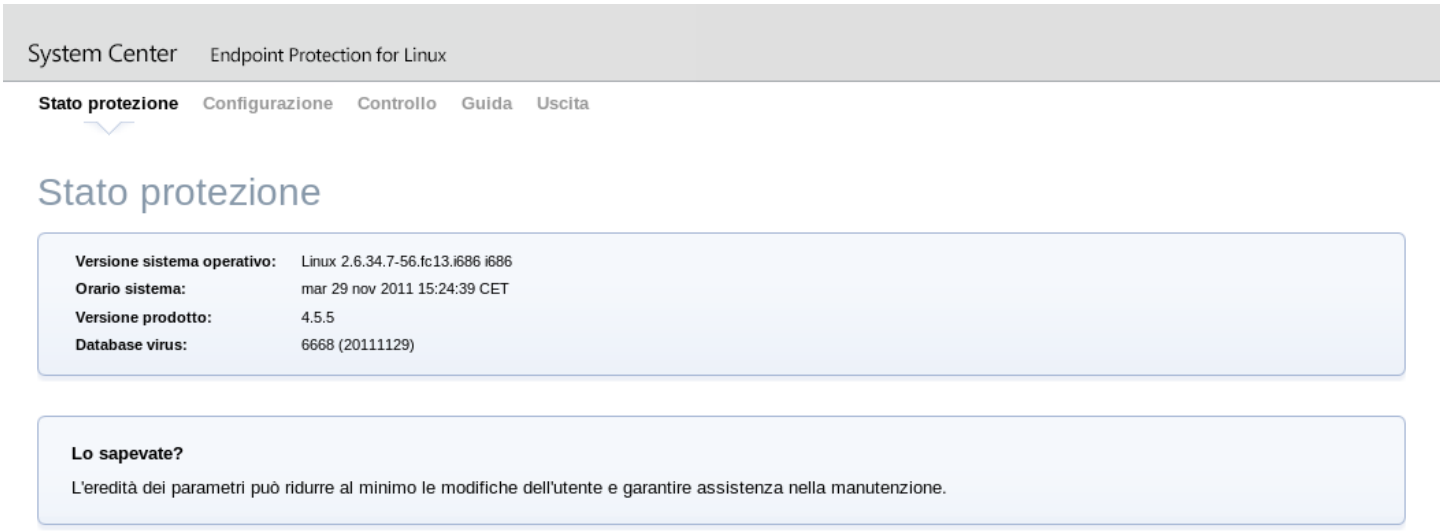
L'interfaccia web consente di eseguire una configurazione e un'amministrazione di facile utilizzo dei sistemi di sicurezza SCEP. Questo modulo rappresenta un agente separato che deve essere attivato in modo esplicito. Per una configurazione rapida dell'*Interfaccia web*, impostare le seguenti opzioni nel file di configurazione SCEP e riavviare il daemon SCEP:

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Sostituire il testo in corsivo con i propri valori e indirizzare il browser su *'https://indirizzo:porta"* (notare l'https). Effettuare l'accesso con *"nome utente/password"*. Le istruzioni relative all'uso di base sono disponibili nella pagina della guida, mentre i dettagli tecnici relativi a*scep_wwwi* sono disponibili nella pagina dei manuali *scep_wwwi(1)*.

L'interfaccia web consente agli utenti di effettuare l'accesso da remoto al daemon SCEP e di utilizzarlo facilmente. Questa potente utility facilita la lettura e la scrittura dei valori di configurazione.

Figura 6-1. System Center Endpoint Protection - Schermata iniziale.



La finestra dell'interfaccia web di System Center Endpoint Protection è suddivisa in due sezioni principali. La finestra principale, che serve per visualizzare i contenuti dell'opzione del menu selezionato e del menu principale. La barra orizzontale nella parte superiore consente all'utente di selezionare le seguenti opzioni principali:

- **Stato protezione** - fornisce le informazioni principali del sistema e dei prodotti Microsoft
- **Configurazione** - è possibile modificare la configurazione di sistema System Center Endpoint Protection qui
- **Controllo** - consente all'utente di eseguire semplici attività e visualizzare le statistiche globali sugli oggetti elaborati da scep_daemon
- **Guida** - fornisce istruzioni d'uso dettagliate per l'interfaccia web System Center Endpoint Protection
- **Uscita** - utilizzare per uscire dalla sessione corrente

Importante: Assicurarsi di fare clic sul pulsante **Salva modifiche** dopo aver apportato eventuali modifiche nella sezione **Configurazione** dell'interfaccia web per salvare le nuove impostazioni. Per applicare le impostazioni sarà necessario riavviare il daemon SCEP facendo clic su **Applica modifiche** nel pannello sulla sinistra.

Esempio di configurazione della protezione in tempo reale

È possibile configurare SCEP in due modi. Nel nostro esempio, illustreremo le modalità di utilizzo di entrambi i metodi di configurazione del modulo Controllo accessi, descritti nel capitoloProtezione in tempo reale tramite l'utilizzo della libreria LIBC precaricata. È possibile scegliere l'opzione più adatta alle proprie esigenze.

- Utilizzo del file di configurazione SCEP:

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- Utilizzo dell'interfaccia web:

Figura 6-3. SCEP - Configurazione > Scansione on-access.

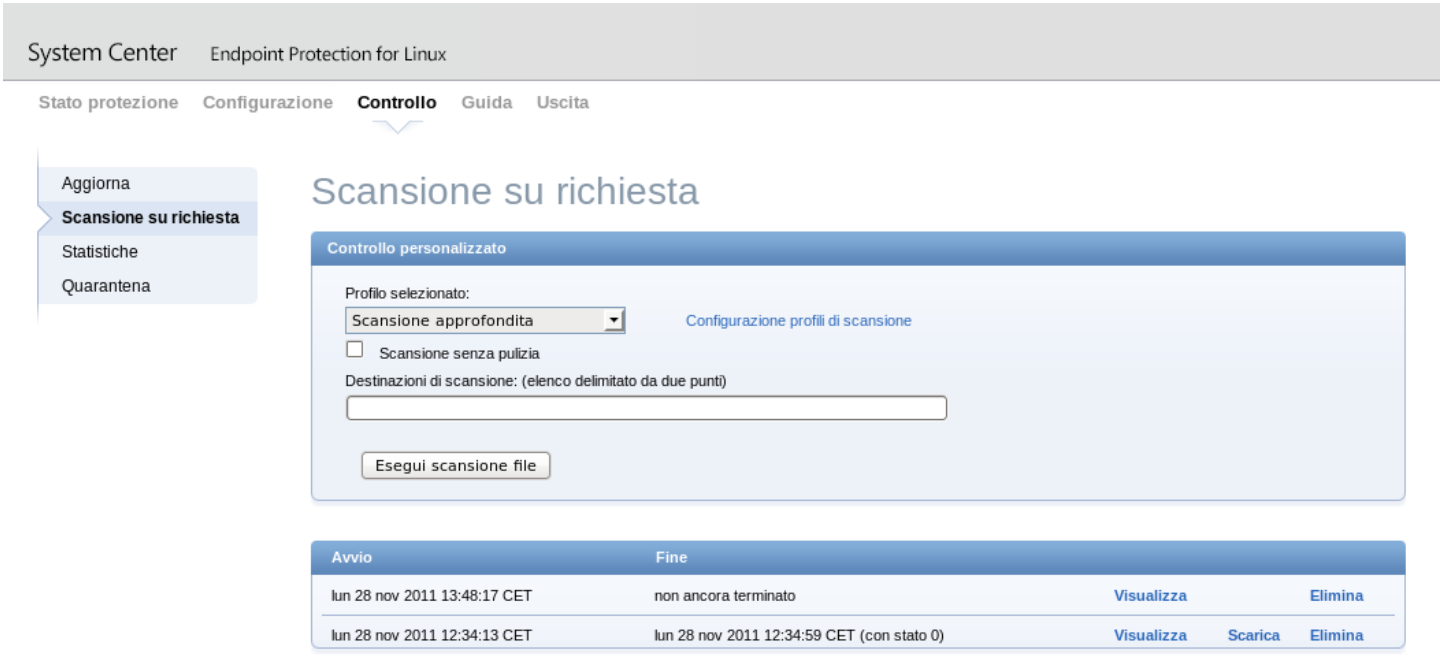
Se si modificano le impostazioni nell'interfaccia web, ricordare sempre di salvare la propria configurazione facendo clic su **Salva modifiche**. Per applicare le nuove modifiche, fare clic sul pulsante **Applica modifiche** nel pannello delle sezioni **Configurazione**.

Scansione su richiesta

Questa sezione comprende un esempio relativo alle modalità di esecuzione della scansione su richiesta per la ricerca di virus:

- Accedere a **Controllo > Scansione su richiesta**
- Inserire il percorso alla directory che si desidera sottoporre a scansione
- Eseguire la scansione della riga di comando facendo clic sul pulsante **Scansione file**

Figura 6-4. SCEP - Controllo > Scansione su richiesta.



La scansione della riga di comando Microsoft sarà eseguito automaticamente in background. Per visualizzare il progresso di scansione, fare clic sul collegamento **Visualizza**. Si aprirà una nuova finestra del browser.

Pianificazione attività

È possibile gestire le attività di pianificazione attraverso il file di configurazione SCEP (vedere capitolo Pianificazione attività) o l'utilizzo dell'interfaccia web.

Figura 6-5. SCEP - Globale > Pianificazione attività.

Fare clic sulla casella di controllo per attivare/disattivare un'attività pianificata. Per impostazione predefinita, vengono visualizzare le seguenti attività pianificate:

- **Manutenzione registro** - Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido. La pianificazione attività avvierà i registri di deframmentazione. Tutte le voci vuote del registro saranno rimosse durante questo processo. Ciò consentirà di lavorare in modo più rapido con i registri. Tale miglioramento potrà essere più evidente se i registri conterranno un numero elevato di elementi.
- **Controllo file di avvio** - Esegue una scansione della memoria e dei servizi di esecuzione in seguito a un aggiornamento avvenuto con successo del database delle firme antivirali.
- **Controllo settimanale** - Esegue una scansione dell'intero sistema ogni settimana (per impostazione predefinita il lunedì alle 2:00). Questa attività può essere personalizzata dall'utente.
- **Aggiornamento automatico regolare** - L'aggiornamento regolare System Center Endpoint Protection rappresenta il miglior metodo per ottenere il livello massimo di protezione del computer. Per ulteriori informazioni, consultare la sezione Utility di aggiornamento SCEP.
- **Notifica delle minacce** - Per impostazione predefinita, ciascuna minaccia verrà registrata nel syslog. Inoltre, è possibile configurare SCEP per l'esecuzione di uno script esterno (notifica) finalizzata all'invio di una notifica a un amministratore di sistema via e-mail sul rilevamento della minaccia.

Statistiche

È possibile visualizzare le statistiche di tutti gli agenti SCEP attivi in questa sezione. Il riepilogo **Statistiche** si aggiorna ogni 10 secondi.

Figura 6-6. SCEP - Controllo > Statistiche.

Registrazione

SCEP offre la registrazione del daemon del sistema attraverso syslog. *Syslog* rappresenta uno standard per i messaggi del programma di registrazione e può essere utilizzato per la registrazione di eventi di sistema tra cui eventi di rete e di sicurezza.

I messaggi fanno riferimento a una funzione:

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

Ai messaggi viene assegnata una priorità o un livello da parte del relativo mittente:

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

Questa sezione contiene una descrizione delle modalità di configurazione e di lettura dell'output di registrazione di syslog. L'opzione *'syslog_facility'* (valore predefinito *'daemon'*) definisce la funzione syslog utilizzata per la registrazione. Per modificare le impostazioni del syslog, modificare il file di configurazione SCEP o utilizzare l'Interfaccia web. Modificare il valore del parametro *'syslog_class'* per modificare la classe di registrazione. Raccomandiamo di modificare queste impostazioni solo se si ha dimestichezza con il syslog. Per un esempio di configurazione del syslog, si rimanda al paragrafo sottostante:

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

Il nome e la collocazione del file di registro dipendono dall'installazione e dalla configurazione del syslog (ad es.:rsyslog, syslog-ng, ecc.). Tra i nomi di file standard per i file di output del syslog vi sono, ad esempio, *'syslog'*, *'daemon.log'*, ecc.. Per seguire l'attività del syslog, eseguire uno dei seguenti comandi dalla console:

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

Importante: Per un corretto funzionamento, il monitoraggio del prodotto Linux SCEP con System Center Operations Manager deve innanzitutto essere abilitato nel file di configurazione SCEP oppure tramite l'interfaccia web SCEP. Assicurarsi che il parametro *'scom_enabled'* nel file di configurazione di cui sopra sia impostato come segue *'scom_enabled = yes'* oppure modificare l'impostazione appropriata nell'interfaccia web sotto **Configurazione** > **Globale** > **Opzioni daemon** > **SCOM attivato**.

Aggiornamento del sistema di sicurezza SCEP

Utility di aggiornamento SCEP

Per preservare il corretto funzionamento di System Center Endpoint Protection, è necessario aggiornare il database delle firme antivirali. L'utility *scep_update* è stata sviluppata in modo specifico a tale scopo. Per ulteriori informazioni, consultare la pagina dei manuali *scep_update(8)* Nel caso in cui il server acceda a Internet tramite il proxy HTTP, sarà necessario definire le opzioni di configurazione aggiuntive *'proxy_addr'*, *'proxy_port'*. Nel caso in cui l'accesso al proxy HTTP richieda un nome utente e una password, sarà necessario definire anche le opzioni *'proxy_username'* e *'proxy_password'* in questa sezione. Per avviare un aggiornamento, inserire il seguente comando:

@SBINDIR@/scep_update

Allo scopo di garantire all'utente finale un livello di sicurezza massimo, il team Microsoft si occupa continuamente della raccolta di definizioni virus in tutto il mondo. In brevissimi intervalli di tempo, vengono aggiunti nuovi modelli al database delle firme antivirali. Per tale motivo, raccomandiamo l'esecuzione regolare degli aggiornamenti. Per poter specificare la frequenza degli aggiornamenti, sarà necessario configurare l'attività *'@update'* nell'opzione *'scheduler_tasks'* nella sezione **[globale]** del file di configurazione SCEP. Per impostare la frequenza degli aggiornamenti, è anche possibile utilizzare la Pianificazione attività. Per un aggiornamento corretto del database delle firme antivirali, è necessario che il daemon SCEP sia attivo e funzionante.

Descrizione del processo di aggiornamento SCEP

Il processo di aggiornamento si compone di due fasi: Innanzitutto, i moduli di aggiornamento precompilati vengono scaricati dal server Microsoft.

La seconda fase del processo di aggiornamento consiste nella compilazione di moduli caricabili dallo scanner System Center Endpoint Protection da quelli archiviati nel mirror locale. Tipicamente, verranno creati i seguenti moduli di caricamento SCEP: modulo di caricamento (em000.dat), modulo scanner (em001.dat), modulo database firme antivirali (em002.dat), modulo supporto archivi (em003.dat), modulo euristica avanzata (em004.dat), ecc.. I moduli verranno creati nella seguente directory:

@BASEDIR@

I vostri commenti

Ci auguriamo che questa guida rappresenti un valido supporto per una comprensione profonda dei requisiti di installazione, configurazione e manutenzione di System Center Endpoint Protection. Tuttavia, il nostro obiettivo consiste nel miglioramento continuo della qualità e dell'efficacia della nostra documentazione. Qualora riteniate che questa Guida presenti punti poco chiari o incompleti, vi preghiamo di comunicarcelo contattando l'Assistenza clienti.

support.microsoft.com

Siamo a vostra disposizione per offrirvi il massimo supporto e saremo lieti di fornirvi la nostra assistenza in caso di problemi relativi al prodotto.

Appendice A. Licenza PHP

The PHP License, version 3.01 Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.