System Center Endpoint Protection

Manual de Instalação e Guia do Utilizador

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

Índice

Introdução

Obrigado por utilizar o System Center Endpoint Protection. O mecanismo de análise de última geração da Microsoft possui velocidade de análise e taxas de deteção inigualáveis combinadas com um impacto mínimo que o torna na escolha ideal para qualquer servidor Linux.

Funcionalidade principal

Análise a pedido

A Análise a pedido pode ser iniciada por um utilizador privilegiado (geralmente um administrador do sistema) através da interface da linha de comandos, da interface Web ou da ferramenta de agendamento automático do sistema operativo (p.ex., cron). O termo *A pedido* refere-se a objetos do sistema de ficheiros que são analisados a pedido do utilizador ou do sistema.

Proteção em tempo real

A Proteção em tempo real é invocada sempre que um utilizador e/ou um sistema operativo tenta aceder a objetos do sistema de ficheiros. Isto também esclarece a utilização do termo *Em tempo real*, uma vez que uma análise é acionada por qualquer tentativa de acesso a objetos do sistema de ficheiros.

Principais recursos do sistema

Algoritmos avançados do mecanismo

Os algoritmos do mecanismo de análise antivírus da Microsoft fornecem as mais altas taxas de deteção e os tempos mais rápidos de análise.

Multiprocessamento

O System Center Endpoint Protection foi desenvolvido para funcionar em unidades de processador único, bem como de multiprocessadores.

Heurística Avançada

O System Center Endpoint Protection inclui uma heurística avançada exclusiva para worms do Win32, infeções de backdoor e outras formas de malware.

Recursos integrados

Os arquivadores integrados descompactam os objetos arquivados sem requerer nenhum programa externo.

Velocidade e eficiência

Para aumentar a velocidade e a eficiência do sistema, a arquitetura do System Center Endpoint Protection baseia-se no daemon em execução (programa residente) para onde todas as solicitações de análise são enviadas.

Segurança melhorada

Todos os daemons executivos (exceto scep_dac) são executados numa conta de utilizador sem privilégios para melhorar a segurança.

Configuração seletiva

O sistema suporta configuração seletiva com base no utilizador ou cliente/servidor.

Vários níveis de registo

Podem ser configurados vários níveis de registo para obter informações sobre atividades e infiltrações no sistema.

Interface Web

A configuração e a administração são disponibilizadas através de uma interface Web intuitiva e de fácil utilização.

Sem bibliotecas externas

A instalação do System Center Endpoint Protection não precisa de bibliotecas ou programas externos, exceto para o LIBC.

Notificação específica de utilizador

O sistema pode ser configurado para notificar utilizadores específicos no caso de uma infiltração detetada ou de outros eventos importantes.

Requisitos mínimos do sistema

Para ser executado com eficiência, o System Center Endpoint Protection requer apenas 16 MB de espaço no disco rígido e 32 MB de RAM. Funciona sem problemas com as versões de kernel do SO Linux 2.2.x, 2.4.x e 2.6.x.

Desempenho e escalabilidade

De servidores menos potentes de pequenos empresas a servidores ISP de classe empresarial com milhares de utilizadores, o System Center Endpoint Protection oferece o desempenho e a escalabilidade que espera de uma solução baseada em UNIX, além da segurança inigualável dos produtos de segurança da Microsoft.

Terminologia e abreviaturas

Nesta secção, iremos analisar os termos e abreviaturas utilizados no presente documento. Note que os tipos de letra em negrito aplicam-se aos nomes de componentes do produto e também aos termos e abreviaturas definidos recentemente. Os termos e abreviaturas definidos neste capítulo são explicados mais adiante no presente documento.

SCEP

SCEP é um acrónimo padrão para o produto de segurança desenvolvido pela Microsoft para sistemas operativos Linux. Também é o nome do pacote de software que contém os produtos.

SCEP daemon

O daemon principal de controlo do sistema e de análise do SCEP: *scep_daemon*.

Diretório base do SCEP

O diretório onde os módulos carregáveis do SCEP que contêm a base de dados de assinatura de vírus são armazenados. A abreviatura *@BASEDIR@* será utilizada para referências futuras a este diretório. O valor *@BASEDIR@* (dependendo do sistema operativo) é listado abaixo:

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

Diretório de configuração do SCEP

O diretório onde todos os ficheiros relacionados com a configuração do System Center Endpoint Protection são armazenados. A abreviatura *@ETCDIR@* será utilizada para referências futuras a este diretório. O valor *@ETCDIR@* (dependendo do sistema operativo) é listado abaixo:

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

Ficheiro de configuração do SCEP

Principal ficheiro de configuração do System Center Endpoint Protection. O caminho absoluto do ficheiro é o seguinte:

@ETCDIR@/scep.cfg

Diretório de ficheiros binários do SCEP

O diretório onde os ficheiros binários relevantes do System Center Endpoint Protection são armazenados. A abreviatura *@BINDIR@* será utilizada para referências futuras a este diretório. O valor *@BINDIR@* (dependendo do sistema operativo) é listado abaixo:

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

Diretório de ficheiros binários do sistema SCEP

O diretório onde os ficheiros binários relevantes do sistema System Center Endpoint Protection são armazenados. A abreviatura *@SBINDIR@* será utilizada para referências futuras a este diretório. O valor *@SBINDIR@* (dependendo do sistema operativo) é listado abaixo:

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

Diretório de ficheiros de objetos do SCEP

O diretório onde os ficheiros de objetos e bibliotecas relevantes do System Center Endpoint Protection são armazenados. A abreviatura *@LIBDIR@* será utilizada para referências futuras a este diretório. O valor *@LIBDIR@* (dependendo do sistema operativo) é listado abaixo:

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

Instalação

O System Center Endpoint Protection é distribuído como um ficheiro binário:

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

No ficheiro binário apresentado acima, *'ext'* é um sufixo dependente da distribuição do SO Linux, ou seja, 'deb' para Debian, 'rpm' para RedHat e SuSE, 'tgz' para outras distribuições do SO Linux.

Para instalar ou atualizar o produto, utilize o seguinte comando:

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

para visualizar o Contrato de Aceitação de Licença do Utilizador do produto. Depois de aceitar o Contrato de Aceitação, o pacote de instalação será colocado no diretório de trabalho atual, e as informações relevantes relacionadas com a instalação, desinstalação ou atualização do pacote serão apresentadas no ecrã.

Quando o pacote estiver instalado, pode verificar se o principal serviço do SCEP está a funcionar utilizando o seguinte comando:

```
ps -C scep_daemon
```

Depois de premir ENTER, deverá ver a seguinte mensagem (ou semelhante):

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

Pelo menos dois processos do daemon do SCEP estão a ser executados em segundo plano. O primeiro PID representa o gestor de processos e ameaças do sistema. O outro representa o processo de análise do SCEP.

Instalação de um pacote de idioma

Para instalar o pacote de idioma pretendido para o System Center Endpoint Protection, utilize o seguinte comando:

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

em que *'lng'* necessita de ser substituído pelo código de idioma do ficheiro que pretende importar.

Depois de a notificação *Installation completed successfully* ser apresentada, atualize a variável de sistema LANG em conformidade e atualize o ambiente, se necessário. A instalação do pacote de idioma está concluída.

Cada pacote de idioma contém o seguinte:

- Interface Web localizada
- Saídas de consola localizadas de agentes e comandos do SCEP
- Documentação em PDF localizada

Visão geral da arquitetura

Quando o System Center Endpoint Protection estiver instalado com êxito, deve familiarizar-se com a sua arquitetura.

O sistema é composto pelos seguintes componentes:

UNIDADE CENTRAL

A unidade central do System Center Endpoint Protection é o SCEP daemon (scep_daemon). O daemon utiliza a biblioteca ibscep.so da API do SCEP e módulos de carregamento em00X_xx.dat do SCEP para fornecer tarefas do sistema base tais como análise, manutenção dos processos daemon do agente, manutenção do sistema de envio de amostras, registo, notificação, etc. Consulte a página *scep_daemon(8)* do manual para obter mais detalhes.

AGENTES

O objetivo dos módulos de agente do SCEP é integrar o SCEP com o ambiente de servidor do Linux.

UTILITÁRIOS

Os módulos de utilitários fornecem uma gestão simples e eficiente do sistema. Os mesmos são responsáveis por tarefas do sistema como gestão de quarentenas, configuração e atualização do sistema.

CONFIGURAÇÃO

A configuração adequada é o aspeto mais importante de um sistema de segurança; o resto deste capítulo explica todos os componentes relacionados. Recomenda-se vivamente o conhecimento aprofundado do ficheiro *scep.cfg*, uma vez este ficheiro contém informações essenciais para a configuração do System Center Endpoint Protection.

Após o produto ter sido instalado com êxito, todos os seus componentes de configuração são armazenados no diretório de configuração do SCEP. O diretório é composto pelos seguintes ficheiros:

@ETCDIR@/scep.cfg

Este é o ficheiro de configuração mais importante, pois controla todos os aspetos principais da funcionalidade do produto. O ficheiro scep.cfg é constituído por várias seções, tendo cada uma delas vários parâmetros. O ficheiro contém uma secção global e várias secções de "agente", com todos os nomes das secções entre parênteses retos. Os parâmetros da secção global são utilizados para definir as opções de configuração do daemon do SCEP, bem como valores predefinidos para a configuração do mecanismo de análise do SCEP. Os parâmetros das secções de agentes são utilizados para definir as opções de configuração dos módulos utilizados para intercetar vários tipos de fluxos de dados no computador e/ou na sua vizinhança, e prepará-lo para a análise. Note que além dos vários parâmetros utilizados para a configuração do sistema, também existem regras que regem a organização do ficheiro. Para obter informações detalhadas sobre a maneira mais eficiente de organizar esse ficheiro, consulte as páginas *scep.cfg(5)* e *scep_daemon(8)* do manual, bem como a página relevante do agente no manual.

@ETCDIR@/certs

Este diretório é utilizado para armazenar os certificados utilizados pela interface Web do SCEP para autenticação. Consulte a página *scep_wwwi(8)* do manual para mais detalhes.

@ETCDIR@/scripts/daemon_notification_script

Se ativado pelo parâmetro *'exec_script'* do ficheiro de configuração do SCEP, este script é executado em caso de uma infiltração detetada pelo sistema antivírus. É utilizado para enviar notificações por email sobre o evento para o administrador do sistema.

Integração com os serviços do Sistema de Ficheiros

Este capítulo descreve a configuração da Proteção em tempo real e A pedido, a qual fornecerá a proteção mais eficiente contra infecções do sistema de ficheiros por vírus e worms. O poder de análise do System Center Endpoint Protection é derivado do comando da Análise a pedido *'scep_scan'* e do comando da Análise em tempo real *'scep_dac'*. A versão Linux do System Center Endpoint Protection oferece uma técnica adicional de Análise em tempo real, a qual utiliza o módulo de biblioteca pré-carregada *libscep_pac.so*. Todos este comandos são descritos nas seções seguintes.

Análise a pedido

A análise a pedido pode ser iniciada por um utilizador privilegiado (geralmente um administrador do sistema) através da interface da linha de comandos, da interface Web ou da ferramenta de agendamento automático do sistema operativo (p.ex., cron). O termo *A pedido* refere-se a objetos do sistema de ficheiros que são analisados a pedido do utilizador ou do sistema.

A Análise a pedido não requer uma configuração especial para ser executada. Após o pacote do SCEP ter sido adequadamente instalado, a Análise a pedido pode ser executada imediatamente utilizando a interface da linha de comandos ou a ferramenta Agenda. Para executar a Análise a pedido a partir da linha de comandos, utilize a sintaxe seguinte:

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

em que FILES corresponde a uma lista de diretórios e/ou ficheiros a analisar.

Estão disponíveis várias opções da linha de comandos ao utilizar a Análise a pedido do SCEP. Para ver a lista completa de opções, consulte a página *scep_scan(8)* do manual.

Proteção em tempo real com tecnologia Dazuko

A Proteção em tempo real é invocada pelo acesso do(s) utilizador(es) e/ou pelo acesso do sistema operativo a objetos do sistema de ficheiros. Isto também explica o termo *Em tempo real*; a análise é acionada por qualquer tentativa de acesso a um objeto selecionado do sistema de ficheiros.

A técnica utilizada pela Análise em tempo real do SCEP possui a tecnologia do módulo kernel Dazuko (da-tzu-ko) e baseia-se na interceção de solicitações do kernel. O projeto Dazuko é "open source", o que significa que o código fonte é gratuitamente distribuído. Isto permite aos utilizadores compilar o módulo kernel nos seus próprios kernels personalizados. Note que o módulo kernel Dazuko não é uma parte de qualquer produto do SCEP e não deve ser compilado e instalado no kernel antes de utilizar o comando Em tempo real *scep_dac*. A técnica Dazuko torna a Análise em tempo real independente do tipo de sistema de ficheiros utilizado. Também é adequada à análise de objetos do sistema de ficheiros através de Network File System (NFS), Nettalk e Samba.

Importante: Antes de fornecermos informações detalhadas relativas à configuração e utilização da Análise em tempo real, deve salientar-se que a análise foi primeiramente desenvolvida e testada para proteger sistemas de ficheiros montados externamente. Se existirem vários sistemas de ficheiros que não foram montados externamente, precisará de excluí-los do controlo de acesso aos ficheiros para evitar encerramentos do sistema. Um exemplo de um diretório típico a excluir é o diretório *'/dev'* e qualquer diretório utilizado pelo SCEP.

Princípio de funcionamento

A Proteção em tempo real do *scep_dac* (SCEP Dazuko-powered file Access Controller) é um programa residente que fornece monitorização e controlo contínuos do sistema de ficheiros. Cada objeto do sistema de ficheiros é analisado com base em tipos de eventos de acesso a ficheiros personalizáveis. A versão atual suporta os seguintes tipos de eventos:

Eventos abertos

Para ativar este tipo de acesso ao ficheiro, defina o valor do parâmetro *'event_mask'* para abrir na secção **[fac]** do ficheiro scep.cfg. Isto ativará o bit ON_OPEN da máscara de acesso do Dazuko.

Eventos fechados

Para ativar este tipo de acesso ao ficheiro, defina o valor do parâmetro *'event_mask'* para fechar na secção **[fac]** do ficheiro scep.cfg. Isto ativará o bit ON_OPEN da máscara de acesso do Dazuko. Isto ativará os bits ON_CLOSE e ON_CLOSE_MODIFIED da máscara de acesso do Dazuko.

Nota: Algumas versões de kernel do SO não suportam a interceção de eventos ON_CLOSE. Nestes casos, os eventos fechados não serão monitorizados pelo *scep_dac*.

Eventos de execução

Para ativar este tipo de acesso ao ficheiro, defina o valor do parâmetro *'event_mask'* para executar na secção **[fac]** do ficheiro scep.cfg. Isto ativará o bit ON_EXEC da máscara de acesso do Dazuko.

A Proteção em tempo real garante que todos os ficheiros abertos, fechados e executados sejam primeiro analisados pelo *scep_daemon* quanto a vírus. Dependendo dos resultados da análise, o acesso a ficheiros específicos é negado ou permitido.

Instalação e configuração

O módulo kernel Dazuko deve ser compilado e instalado no kernel em execução antes de inicializar o *scep_dac*. Para mais detalhes sobre como compilar e instalar o Dazuko, consulte:

http://www.dazuko.org

Quando o Dazuko estiver instalado, reveja e edite as secções **[global]** e **[fac]** do ficheiro de configuração do SCEP (scep.cfg). Note que o funcionamento adequado da Proteção em tempo real depende da configuração da opção *'agent_type'* na secção **[fac]** deste ficheiro. Além disso, deve definir os objetos do sistema do ficheiro (ou seja, diretórios e ficheiros) que deverão ser monitorizados pela Proteção em tempo real. Esta ação pode ser realizada através da definição dos parâmetros das opções *'ctl_incl'* e *'ctl_excl'*, que também se localizam na secção **[fac]**. Depois de fazer alterações ao ficheiro scep.cfg, pode forçar a releitura da configuração recém-criada, recarregando o daemon do SCEP.

Sugestões

Para garantir o carregamento do módulo Dazuko antes da inicialização do *scep_dac* daemon, siga estes passos:

Coloque uma cópia do módulo Dazuko em qualquer um dos seguintes diretórios reservados para módulos kernel:

```
/lib/modules
```

ou

```
/modules
```

Utilize os utilitários do kernel 'depmod' e 'modprobe' (Para o SO BSD, utilize 'kldconfig' e 'kldload') para lidar com as dependências e inicializar com êxito o módulo Dazuko recém-adicionado.

No script de inicialização scep_daemon '/etc/init.d/scep_daemon', introduza a seguinte linha antes da declaração de inicialização do daemon:

```
/sbin/modprobe dazuko
```

Para o SO BSD, a linha

```
/sbin/kldconfig dazuko
```

tem de ser inserida no script '/usr/local/etc/rc.d/scep_daemon.sh'.

Aviso! É extremamente importante que estes passos sejam executados pela ordem exata apresentada. Se o módulo kernel não estiver localizado no diretório de módulos kernel, este não será carregado corretamente, provocando o bloqueio do sistema.

Proteção em tempo real utilizando biblioteca LIBC pré-carregada

Nas secções anteriores, descrevemos a integração da Proteção em tempo real, com tecnologia Dazuko, com os serviços do sistema de ficheiros Linux/BSD. A utilização do Dazuko pode não ser viável em todas as situações, incluindo administradores de sistemas que mantêm sistemas críticos onde:

- o código fonte e/ou os ficheiros de configuração relacionados com o kernel em execução não estão disponíveis,
- o kernel é mais monolítico do que modular,
- o módulo Dazuko simplesmente não suporta o SO em questão.

Em nenhum destes casos, a técnica de Análise em tempo real baseada na biblioteca LIBC pré-carregada deve ser utilizada. Consulte os tópicos a seguir nesta secção para obter informações detalhadas. Note que esta secção é relevante apenas para utilizadores do SO Linux e contém informações relacionadas com o funcionamento, instalação e configuração da Análise em tempo real que utiliza a biblioteca *'libscep_pac.so'* pré-carregada.

Princípio de funcionamento

A Proteção em tempo real *libscep_pac.so* (SCEP Preload library based file Access Controller) é uma biblioteca de objetos partilhados que é ativada na inicialização do sistema. Esta biblioteca é utilizada para solicitações do LIBC por servidores de sistemas de ficheiros como o servidor FTP, servidor Samba, etc. Cada objeto do sistema de ficheiros é analisado com base em tipos de eventos de acesso a ficheiros personalizáveis. A versão atual suporta os seguintes tipos de eventos:

Eventos abertos

Este tipo de acesso a ficheiros é ativado se a palavra *'open'* estiver presente no parâmetro *'event_mask'* no ficheiro esest.cfg

(secção **[fac]**).

Eventos fechados

Este tipo de acesso a ficheiros é ativado se a palavra *'close'* estiver presente no parâmetro *'event_mask'* no ficheiro scep.cfg (secção **[fac]**). Neste caso, todas as funções do descritor de ficheiros e de encerramento do fluxo de FICHEIROS do LIBC são intercetadas.

Eventos de execução

Este tipo de acesso a ficheiros é ativado se a palavra *'exec'* estiver presente no parâmetro *'event_mask'* no scep.cfg (secção **[fac]**). Neste caso, todas as funções de execução do LIBC são intercetadas.

Todos os ficheiros abertos, fechados e executados são analisados pelo daemon do SCEP quanto a vírus. Com base nos resultados dessas análises, o acesso a determinados ficheiros é negado ou permitido.

Instalação e configuração

O módulo de biblioteca *libscep_pac.so* é instalado utilizando um mecanismo de instalação padrão das bibliotecas pré-carregadas. É necessário definir a variável de ambiente *'LD_PRELOAD'* com o caminho absoluto para a biblioteca *libscep_pac.so*. Para mais informações, consulte a página *ld.so(8)* do manual.

Nota: É importante que a variável de ambiente *'LD_PRELOAD'* seja definida apenas para os processos daemon do servidor de rede (ftp, Samba, etc.) que estará sob controlo da Proteção em tempo real. Geralmente, não é recomendado o pré-carregamento de solicitações LIBC para todos os processos do sistema operativo, pois pode reduzir drasticamente o desempenho do sistema, ou até mesmo, fazer com que o sistema bloqueie. Assim sendo, o ficheiro '/etc/ld.so.preload' não deve ser utilizado, e nem a variável de ambiente 'LD_PRELOAD' deve ser exportada a nível global. Ambos substituiriam todas as solicitações de LIBC relevantes, o que poderia levar a encerramentos do sistema durante a inicialização.

Para garantir que apenas as solicitações de acesso a ficheiros num determinado sistema de ficheiros são intercetadas, podem ser substituídas declarações executáveis utilizando a seguinte linha:

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

em que 'COMMAND COMMAND-ARGUMENTS' corresponde à declaração executável original.

Reveja e edite as secções **[global]** e **[fac]** do ficheiro de configuração do SCEP (scep.cfg). Para que a Análise em tempo real funcione corretamente, tem de definir os objetos do sistema de ficheiros (ou seja, diretórios e ficheiros) que precisam estar sob controlo da biblioteca pré-carregada. Tal pode ser conseguido através da definição dos parâmetros das opções *'ctl_incl'* e *'ctl_excl'* na secção **[fac]** do ficheiro de configuração do SCEP. Depois de fazer alterações ao ficheiro scep.cfg, pode forçar a releitura da configuração recém-criada, recarregando o daemon do SCEP.

Sugestões

Para ativar a Proteção em tempo real imediatamente após a inicialização do sistema, a variável de ambiente *'LD_PRELOAD'* deve estar definida no script de inicialização do servidor de ficheiros da rede adequado.

Exemplo: Vamos supor que pretendemos que a Análise em tempo real monitorize todos os eventos de acesso ao sistema de ficheiros imediatamente após o início do servidor Samba. No script de inicialização do daemon do Samba (/etc/init.d/smb), substituiríamos a declaração

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

pela seguinte linha:

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

Desta forma, os objetos do sistema de ficheiros selecionados controlados pelo Samba serão analisados na inicialização do sistema.

Mecanismos importantes do SCEP

Política de tratamento de objetos

O mecanismo da Política de tratamento de objectos fornece a filtragem de objetos analisados com base nos respetivos estados. Esta funcionalidade baseia-se nas seguintes opções de configuração:

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Para informações detalhadas sobre estas opções, consulte a página *scep.cfg(5)* do manual.

Cada objeto processado é primeiro tratado de acordo com a configuração da opção *'action_av'*. Se esta opção estiver definida para *'accept'* (ou *'defer'*, *'discard'*, *'reject'*) o objeto é aceite (ou adiado, ignorado, rejeitado). Se a opção estiver definida para *'scan'* o objeto é analisado quanto a infiltrações de vírus, e se a opção *'av_clean_mode'* estiver definida para *'yes'*, o objeto também é limpo. Além disso, as opções de configuração *'action_av_infected'*, *'action_av_notscanned'* e *'action_av_deleted'* são levadas em consideração para melhor avaliar o tratamento do objeto. Se uma ação *'accept'* foi tomada como resultado destas três opções de ação, o objeto é aceite. Caso contrário, o objeto é bloqueado.

Configuração específica de utilizador

A finalidade do mecanismo de Configuração específica de utilizador é fornecer um nível mais elevado de personalização e funcionalidade. Permite que o administrador do sistema defina os parâmetros da análise antivírus do SCEP com base no utilizador que está a aceder os objetos do sistema de ficheiros.

Pode encontrar uma descrição detalhada desta funcionalidade na página *scep.cfg(5)* do manual. Nesta secção, vamos dar apenas um pequeno exemplo de uma configuração específica de utilizador.

Neste exemplo, o objetivo é utilizar o módulo *scep_dac* para controlar os eventos de acesso ON_OPEN e ON_EXEC para um disco externo montado no diretório /home. O módulo pode ser configurado na secção **[fac]** do ficheiro de configuração do SCEP. Veja abaixo:

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

Para especificar definições de análise para um utilizador individual, o parâmetro *'user_config'* tem de especificar o nome do ficheiro de configuração especial onde as regras de análise individuais serão armazenadas. No exemplo mostrado, o ficheiro de configuração especial é denominado *'scep_dac_spec.cfg'* e localiza-se no diretório de configuração do SCEP (Este diretório baseia-se no seu sistema operativo. Consulte a página Terminologia e abreviaturas).

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

Quando o parâmetro do ficheiro *'user_config'* estiver especificado na secção **[fac]**, o ficheiro *'scep_dac_spec.cfg'* tem de ser criado no diretório de configuração do SCEP. Por fim, adicione as regras de análise pretendidas.

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

Na parte superior da secção especial, introduza o nome de utilizador ao qual as regras individuais serão aplicadas. Esta configuração permitirá que todos os outros utilizadores que tentem aceder ao sistema de ficheiros sejam processados normalmente, ou seja, todos os objetos do sistema de ficheiros acedidos por outros utilizadores serão analisados quanto a infiltrações, exceto para o utilizador *"username"*, cujo acesso será rejeitado (bloqueado).

Agenda

A funcionalidade da Agenda inclui a execução de tarefas agendadas a uma hora específica ou num evento específico, a gestão e o início de tarefas com configuração e propriedades predefinidas e muito mais. A configuração e as propriedades das tarefas podem ser utilizadas para influenciar datas e horas de início, mas também para expandir a aplicação das tarefas introduzindo a utilização de perfis personalizados durante a execução das mesmas.

A opção *'scheduler_tasks'* é comentada por predefinição, fazendo com que a configuração padrão da agenda seja aplicada. No ficheiro de configuração do SCEP, todos os parâmetros e tarefas são separados por ponto e vírgula. Qualquer outro ponto e vírgula (e barra invertida) deve ser separado por barra invertida. Cada tarefa possui 6 parâmetros e a sintaxe como se segue:

- id - número exclusivo.
- name - descrição da tarefa.
- flags- os sinalizadores especiais para desativar a tarefa da agenda especificada podem ser definidos aqui.
- failstart - fornece instruções sobre o que fazer se não foi possível executar a tarefa na data agendada.
- datespec - uma especificação regular de data com 6 campos (crontab como estendidos por ano), datas recorrentes ou uma opção de nome de evento.
- command - pode ser um caminho absoluto para um comando seguido pelos respetivos argumentos ou por um nome de comando especial com o prefixo "@" (p. ex., atualização de antivírus: *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

Os seguintes nomes de eventos podem ser utilizados no lugar da opção datespec:

- start - inicialização do daemon.
- startonce - inicialização do daemon, mas no máximo uma vez ao dia.
- engine - atualização do mecanismo com êxito.
- login - inicialização do início de sessão na interface Web.
- threat - ameaça detetada.
- notscanned - ficheiro não analisado.

Para visualizar a configuração atual da agenda, utilize a Interface Web ou execute o seguinte comando:

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

Para uma descrição completa da Agenda e respetivos parâmetros, consulte a secção Agenda na página *scep_daemon(8)* do manual.

Interface Web

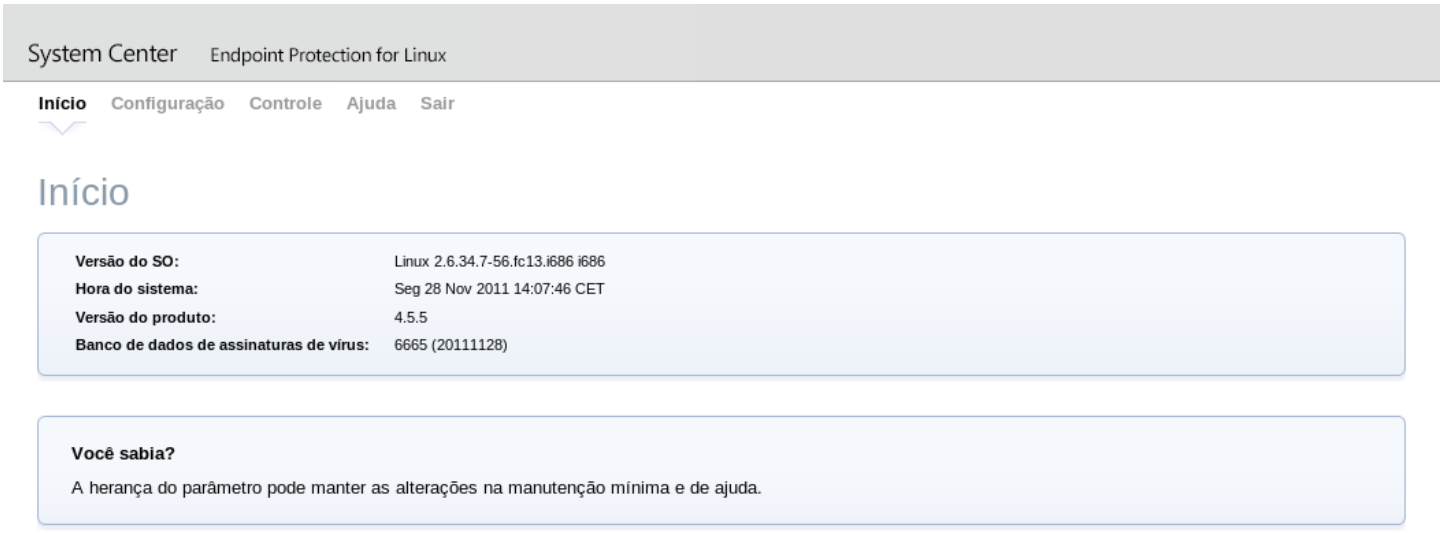
A interface Web permite a configuração e a administração fáceis dos sistemas de segurança do SCEP. Este módulo é um agente separado e deve ser explicitamente ativado. Para configurar a *Interface Web* rapidamente, defina as seguintes opções no ficheiro de configuração do SCEP e reinicie o daemon do SCEP:

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

Substitua o texto em itálico pelos seus próprios valores e direcione o seu navegador para *'https://address:port'* (observe o https). Inicie sessão com *'username/password'*. Pode encontrar as instruções básicas de utilização na página de ajuda e os detalhes técnicos sobre o *scep_wwwi* na página *scep_wwwi(1)* do manual.

A interface Web permite-lhe aceder remotamente ao daemon do SCEP e implementá-lo facilmente. Este poderoso utilitário facilita a leitura e a gravação de valores de configuração.

Figura 6-1. System Center Endpoint Protection - Ecrã Início.



A janela da interface Web do System Center Endpoint Protection está dividida em duas secções principais. A janela principal, na qual pode visualizar o conteúdo da opção de menu selecionada e o menu principal. Esta barra horizontal na parte superior permite-lhe navegar pelas seguintes opções principais:

- **Início** - fornece informações básicas do sistema do produto da Microsoft
- **Configuração** - pode alterar o sistema de configuração do System Center Endpoint Protection aqui
- **Controlo** - permite-lhe executar tarefas simples e visualizar as estatísticas globais sobre os objetos processados pelo scep_daemon
- **Ajuda** - fornece instruções detalhadas de utilização da interface Web do System Center Endpoint Protection
- **Terminar sessão** - utilize para encerrar a sessão atual

Importante: Certifique-se de que clica no botão **Guardar alterações** depois de fazer alguma alteração na secção **Configuração** da interface Web para guardar as suas novas definições. Para aplicar as suas definições, precisa de reiniciar o daemon do SCEP clicando em **Aplicar alterações** no painel esquerdo.

Exemplo de configuração da proteção em tempo real

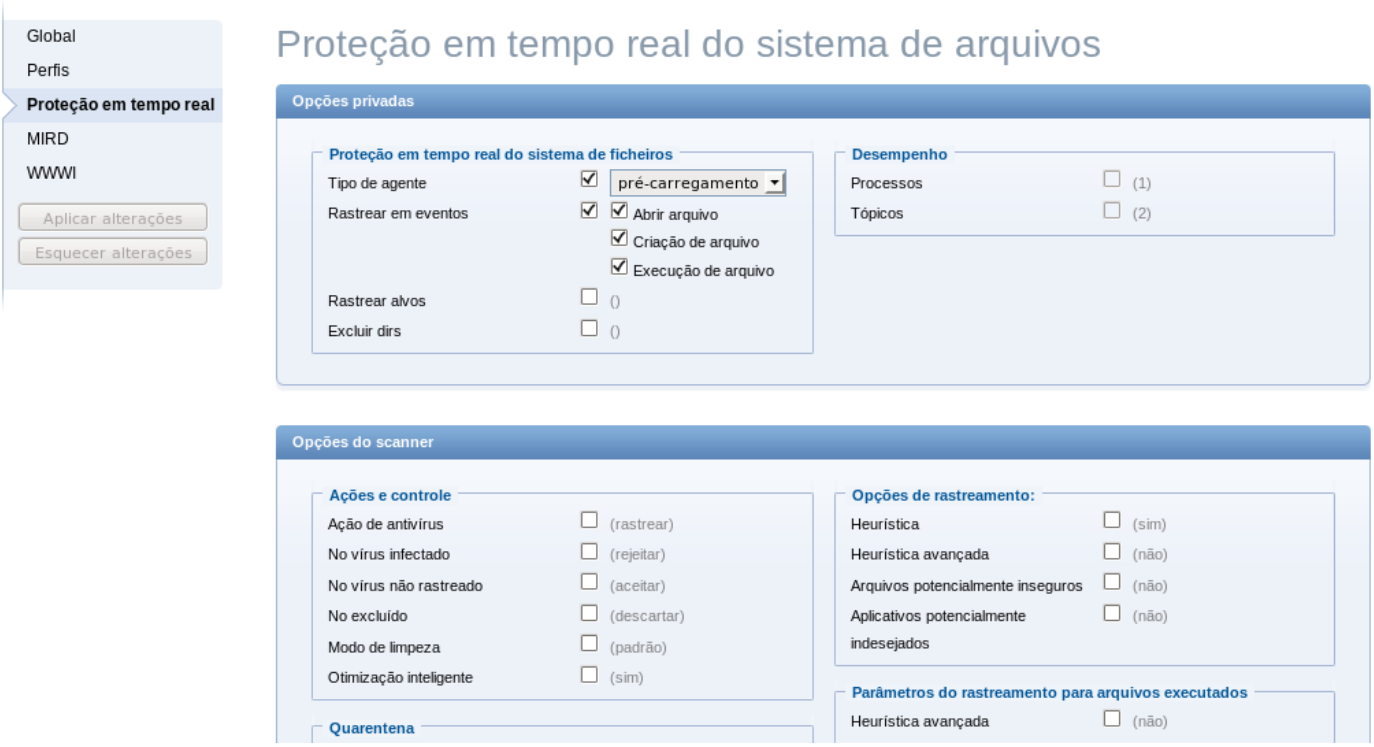
Há duas formas possíveis de se configurar o SCEP. No nosso exemplo, vamos demonstrar como utilizar ambas para configurar o módulo Access Controller, descrito no capítulo Proteção em tempo real utilizando biblioteca LIBC pré-carregada. Pode escolher a opção que melhor se adequa ao seu caso.

- Utilizando o ficheiro de configuração do SCEP:

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

- Utilizando a interface Web:

Figura 6-3. SCEP - Configuração > Análise em tempo real.



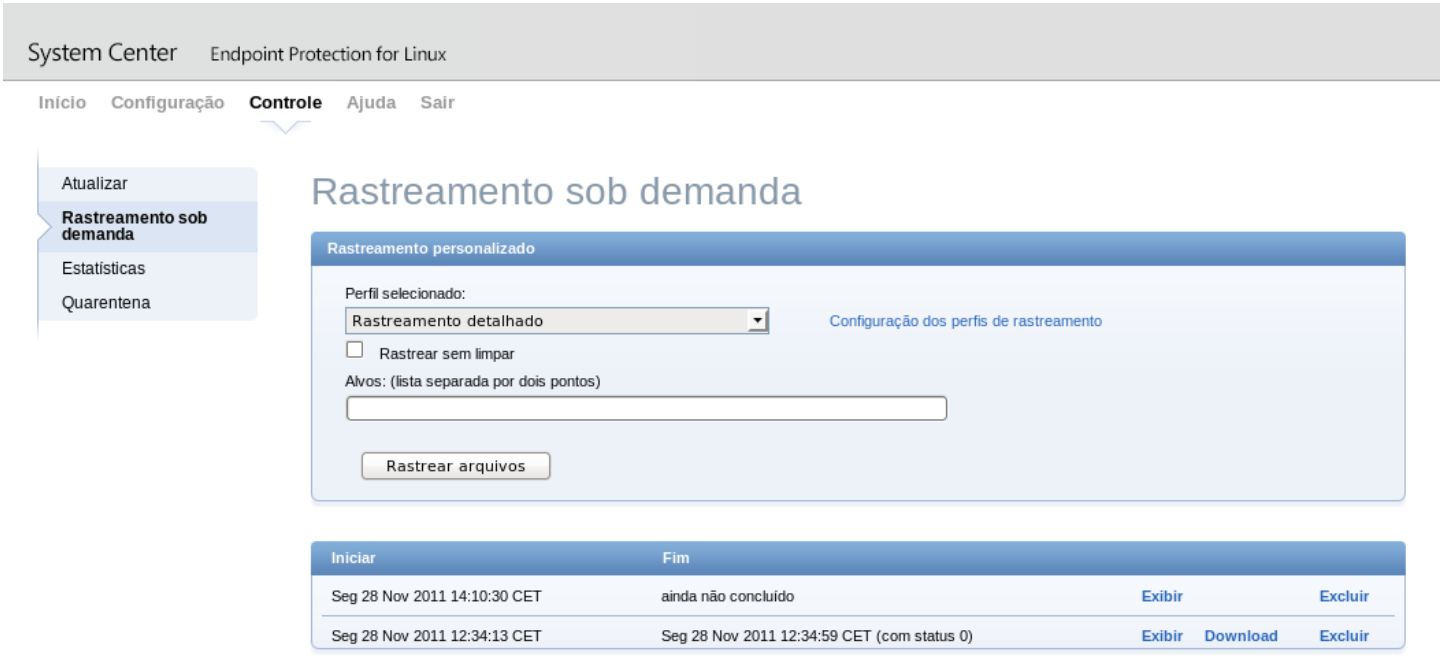
Quando alterar definições na interface Web, lembre-se sempre de guardar a sua configuração clicando em **Guardar alterações**. Para aplicar as novas alterações, clique no botão **Aplicar alterações** no painel da secção **Configuração**.

Análise a pedido

Esta secção inclui um exemplo de como executar a Análise a pedido para efetuar a análise quanto a vírus:

- Navegue até **Controlo > Análise a pedido**
- Introduza o caminho do diretório que pretende analisar
- Execute a análise através da linha de comando clicando no botão **Analisar ficheiros**

Figura 6-4. SCEP - Controlo > Análise a pedido.

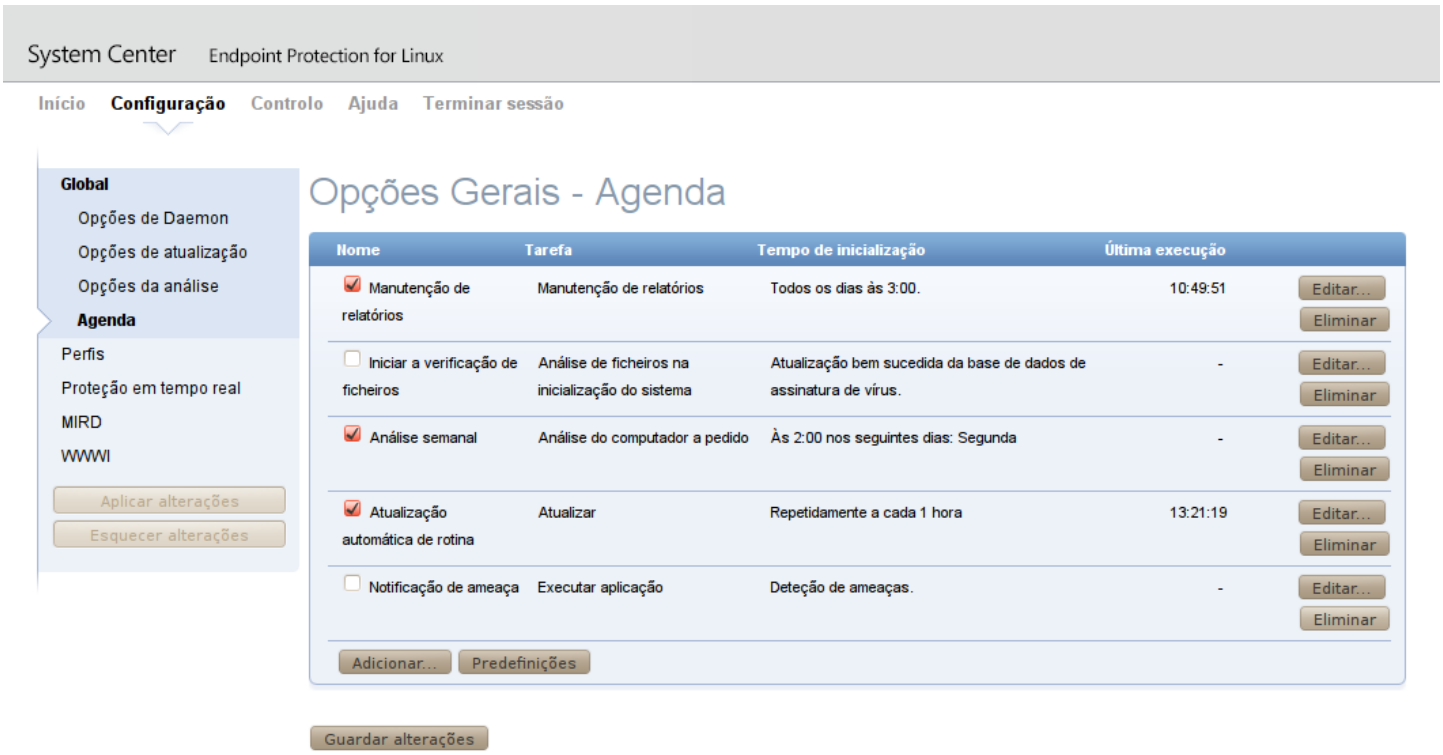


A Análise através da linha de comando da Microsoft será executada automaticamente em segundo plano. Para ver o progresso da análise, clique na hiperligação **Ver**. É aberta uma nova janela do navegador.

Agenda

Pode gerir as tarefas da agenda através do ficheiro de configuração da Microsoft (consulte o capítulo Agenda) ou utilizando a interface Web.

Figura 6-5. SCEP - Global > Agenda.



Clique na caixa de verificação para ativar/desativar uma tarefa agendada. Por predefinição, são apresentadas as seguintes tarefas agendadas:

- **Manutenção de relatórios** - O programa elimina automaticamente os relatórios mais antigos para poupar espaço no disco rígido. A Agenda iniciará a desfragmentação de relatórios. Todas as entradas de relatórios vazios serão removidas durante este processo. Desta forma, a velocidade será melhorada quando trabalhar com relatórios. A melhoria será mais evidente se os relatórios tiverem um grande número de entradas.
- **Análise de ficheiros na inicialização** - Analisa a memória e os serviços em execução após uma atualização bem sucedida da base de dados de assinatura de vírus.
- **Análise semanal** - Analise todo o sistema de ficheiros semanalmente (por predefinição à segunda-feira às 02:00 h). Esta tarefa pode ser personalizada pelo utilizador.
- **Atualização automática de rotina** - Atualizar periodicamente o System Center Endpoint Protection é o melhor método para se manter o nível máximo de segurança no computador. Consulte o Utilitário de atualização do SCEP para mais informações.
- **Notificação de ameaça** - Por predefinição, todas as ameaças serão registadas no syslog. Além disso, o SCEP pode ser configurado para executar um script externo (notificação) para notificar um administrador do sistema através de um email sobre a deteção de ameaça.

Estatísticas

Pode visualizar as estatísticas de todos os agentes ativos do SCEP aqui. O resumo das **Estatísticas** é atualizado de 10 em 10 segundos.

Figura 6-6. SCEP - Controlo > Estatísticas.

Registo

O SCEP fornece o registo no daemon do sistema através do syslog. O *Syslog* é uma norma para mensagens de programas de registo e pode ser utilizado para registar eventos do sistema como eventos da rede e de segurança.

As mensagens referem-se a um recurso:

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

As mensagens têm uma prioridade/nível atribuído pelo remetente da mensagem:

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

Esta secção descreve como configurar e ler os resultados do registo do syslog. A opção *'syslog_facility'* (valor predefinido *'daemon'*) define o recurso do syslog utilizado para o registo. Para modificar as configurações do syslog, edite o ficheiro de configuração do SCEP ou utilize a Interface Web. Modifique o valor do parâmetro *'syslog_class'* para alterar a classe do registo. Recomenda-se a modificação destas definições apenas se estiver familiarizado com o syslog. Para ver um exemplo de configuração do syslog, consulte abaixo:

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

O nome e a localização do relatório dependem da sua instalação e configuração do syslog (p.ex., rsyslog, syslog-ng, etc.). Nomes de ficheiros padrão para os ficheiros de saída do syslog são por exemplo *'syslog'*, *'daemon.log'*, etc. Para seguir a atividade do syslog, execute um dos seguintes comandos na consola:

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

Importante: Primeiro é necessário ativar a monitorização do produto Linux SCEP, utilizando o System Center Operations Manager no ficheiro de configuração do SCEP ou na interface Web do SCEP para que funcione corretamente. Certifique-se de que o parâmetro *'scom_enabled'* no ficheiro de configuração mencionado acima está definido como *'scom_enabled = yes'* ou altere a configuração correspondente na interface Web em **Configuração** > **Global** > **Opções de Daemon** > **SCOM ativado**.

Atualização do sistema de segurança do SCEP

Utilitário de atualização do SCEP

Para manter a eficácia do System Center Endpoint Protection, é necessário manter a base de dados de assinatura de vírus atualizada. O utilitário *scep_update* foi desenvolvido especificamente para esta finalidade. Consulte a a página *scep_update(8)* do manual para mais detalhes. No caso do seu servidor aceder à Internet através do proxy HTTP, as opções de configuração adicionais *'proxy_addr'*, *'proxy_port'* devem ser definidas. Se o acesso ao proxy HTTP requerer um nome de utilizador e palavra-passe, as opções *'proxy_username'* e *'proxy_password'* também devem ser definidas nesta secção. Para iniciar uma atualização, introduza o seguinte comando:

@SBINDIR@/scep_update

Para fornecer a maior segurança possível ao utilizador final, a equipa da Microsoft recolhe continuamente definições de vírus do mundo inteiro - novos padrões são adicionados à base de dados de assinatura de vírus em intervalos muito curtos. Por este motivo, recomendamos que as atualizações sejam iniciadas regularmente. Para poder especificar a frequência das atualizações, necessita de configurar a tarefa *'@update'* na opção *'scheduler_tasks'* na secção **[global]** do ficheiro de configuração do SCEP. Também pode utilizar a Agenda para definir a frequência da atualização. O daemon do SCEP deve estar instalado e em execução para atualizar com êxito a base de dados de assinatura de vírus.

Descrição do processo de atualização do SCEP

O processo de atualização consiste em duas etapas: Primeiro, os módulos de atualização pré-compilados são transferidos do servidor da Microsoft.

A segunda etapa do processo de atualização é a compilação de módulos carregáveis pela análise do System Center Endpoint Protection a partir daqueles armazenados na imagem local. Normalmente, são criados os seguintes módulos de carregamento do SCEP: módulo do carregador (em000.dat), módulo de análise (em001.dat), módulo da base de dados de assinatura de vírus (em002.dat), módulo de suporte de ficheiros (em003.dat), módulo de heurística avançada (em004.dat), etc. Os módulos são criados no seguinte diretório:

@BASEDIR@

Informe-nos

Esperamos que este guia lhe tenha fornecido conhecimentos profundos sobre os requisitos para a instalação, configuração e manutenção do System Center Endpoint Protection. No entanto, o nosso objetivo é melhorar continuamente a qualidade e a eficiência da nossa documentação. Se achar que alguma secção neste Guia é pouco clara ou está incompleta, informe-nos entrando em contato com o Suporte ao cliente:

support.microsoft.com

Estamos empenhados em fornecer o mais alto nível de suporte, e esperamos ajudá-lo caso tenha algum problema relacionado com este produto.

Anexo A. Licença PHP

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.