
# System Center
# para o Endpoint Protection para Linux

Microsoft Corporation

Data de publicação: 10/26/2015

Envie comentários ou sugestões sobre este documento para mpgfeed@microsoft.com. Inclua o nome do guia do pacote de monitorização com os seus comentários.

A equipa do Operations Manager incentiva os utilizadores a enviarem comentários sobre o pacote de monitorização, introduzindo as opiniões na página do pacote de gestão no Catálogo de Pacotes de Gestão (http://go.microsoft.com/fwlink/?LinkID=82105).

# Índice

# Guia do Pacote de Gestão do SCEP

Este pacote de gestão permite gerir o System Center Endpoint Protection (SCEP) a partir do System Center 2012 Operations Manager num ambiente em rede, incluindo estações de trabalho e servidores, a partir de um local centralizado. Com o sistema de gestão de tarefas do Operations Manager, pode gerir o SCEP em computadores remotos, ver alertas e estados de integridade, bem como resolver rapidamente novos problemas e ameaças.

O System Center 2012 Operations Manager por si só não fornece outra forma de proteção contra código malicioso. O System Center 2012 Operations Manager depende da existência da solução SCEP em computadores com o sistema operativo Linux instalado.

Este guia foi redigido com base na versão 4.5.10.1 do Pacote de Gestão do SCEP.

## Histórico do Guia

| Versão | Data da Versão | Alterações |
|---|---|---|
| 4.5.9.1 | 05/16/2012 | Edição original deste guia. |
| 4.5.10.1 | 11/06/2012 | Novas distribuições Linux suportadas.<br>Descrição melhorada para algumas ferramentas do pacote de gestão. |

## Alterações na Versão 4.5.10.1

A versão 4.5.10.1 do pacote de gestão para o System Center Endpoint Protection inclui as seguintes alterações:

- Novas distribuições Linux suportadas:
  - 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:** Estas distribuições novas serão apenas suportadas utilizando o System Center 2012 Operations Manager Service Pack 1 e versões superiores.
- Foi adicionada uma descrição melhorada para:
  - Monitor de Malware Ativo
  - Alerta de Malware ativo (da Regra)

## Configurações Suportadas

Em geral, as configurações suportadas estão descritas em Configurações do Operations Manager 2007 R2 Suportadas (http://go.microsoft.com/fwlink/?LinkId=90676).

Este pacote de gestão requer o System Center 2012 Operations Manager 2007 R2 ou posterior. A tabela a seguir detalha os sistemas operativos suportados para este pacote de gestão:

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

## Pré-requisitos

Os seguintes requisitos devem ser satisfeitos para executar este pacote de gestão:

- Atualização Cumulativa 5 do System Center Operations Manager 2007 R2 (http://support.microsoft.com/kb/2449679)

Os pacotes de gestão do SCEP listados a seguir estão integrados no System Center 2012 Operations Manager 2007 R2 ou estão disponíveis para transferência a partir do catálogo online.

| ID | Nome | Versão |
|---|---|---|

| | | |
|---|---|---|
| Microsoft.Linux.Library | Biblioteca do sistema operativo Linux | 6.1.7000.256 |
| Microsoft.SystemCenter.InstanceGroup.Library | Biblioteca de grupo de instâncias | 6.1.7221.0 |
| Microsoft.SystemCenter.Library | Biblioteca principal do System Center | 6.1.7221.0 |
| Microsoft.SystemCenter.WSManagement.Library | Biblioteca do WS-Management | 6.1.7221.0 |
| Microsoft.SystemCenter.DataWarehouse.Library | Biblioteca do Data Warehouse | 6.1.7221.0 |
| Microsoft.Unix.Library | Biblioteca principal do Unix | 6.1.7000.256 |
| Microsoft.Unix.Service.Library | Biblioteca de modelos de serviço do Unix | 6.1.7221.0 |
| Microsoft.Windows.Library | Biblioteca principal do Windows | 6.1.7221.0 |
| System.Health.Library | Biblioteca de integridade | 6.1.7221.0 |
| System.Library | Biblioteca de sistema | 6.1.7221.0 |

***Importante:*** Primeiro é necessário ativar a monitorização do produto Linux SCEP através do System Center 2012 Operations Manager no ficheiro de configuração */etc/opt/microsoft/scep/scep.cfg* 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 **Configuration** > **Global** > **Opções de Daemon** > **SCOM ativado**.

## Ficheiros deste Pacote de Gestão

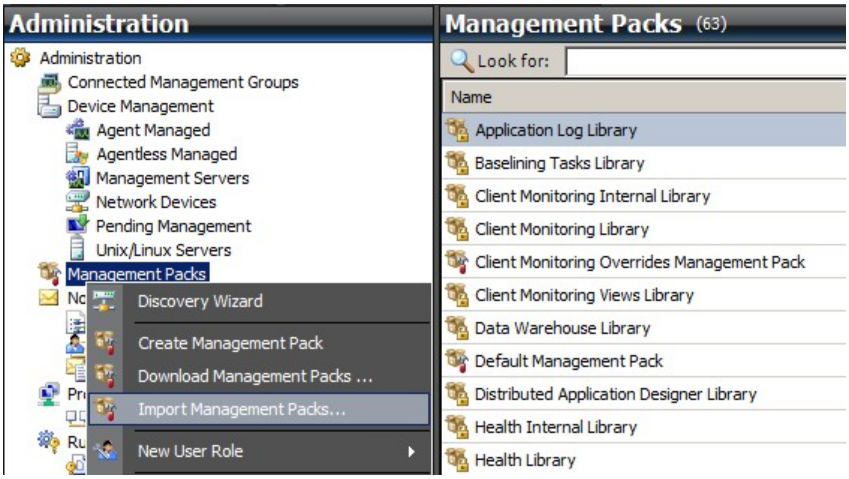
O Pacote de Gestão do SCEP inclui os seguintes ficheiros:

| Nome do ficheiro | Descrição |
|---|---|
| Microsoft.SCEP.Linux.Library.mp | Contém as definições de classe e suas relações mútuas, além das definições de tipos de monitor e tipos de módulo. |
| Microsoft.SCEP.Linux.Application.mp | Implementa a monitorização, alertas, tarefas e vistas. |

## Iniciação Rápida

O pré-requisito para iniciar a monitorização do SCEP é importar os pacotes de gestão para o Operations Manager e identificar os computadores que serão monitorizados (processo conhecido como “descoberta”).

**Importar pacotes de gestão**

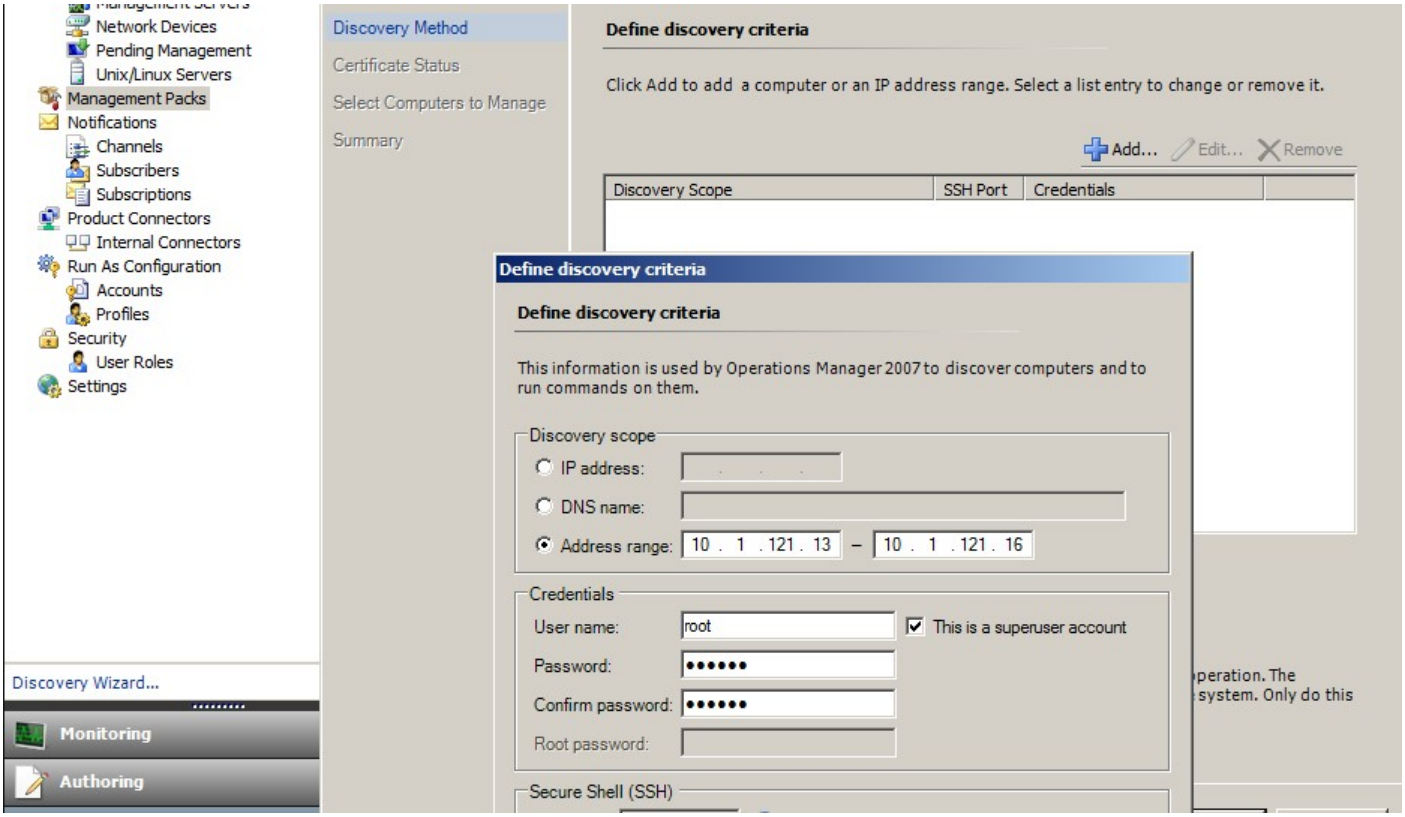



1. Clique na área de trabalho **Administration** o painel esquerdo da janela Consola de Operações.
2. Clique com o botão direito do rato em **Management Packs** e selecione **Import Management Packs...** no menu de contexto.
3. Na janela Pacotes de Gestão, clique no botão **Add** e selecione **Add from disk...** no menu pendente.
4. Confirme que pretende que o Operations Manager pesquise e instale todas as dependências fora do disco local clicando em **Yes** na janela **Online Catalog Connection**.
5. Certifique-se de que seleciona os dois ficheiros listados (Microsoft.SCEP.Linux.Application.mp, Microsoft.SCEP.Linux.Library.mp) e clique em **Install**.

**Nota:** para obter mais instruções sobre como importar um pacote de gestão, consulte Como Importar um Pacote de Gestão no Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkId=142351).

**Descoberta**

Após a importação bem sucedida dos ficheiros *.mp, será necessário realizar a descoberta do computador.




1. Na área de trabalho **Administration** (no painel esquerdo da janela Consola de Operações), clique na hiperligação **Discovery wizard...** (na parte inferior do painel esquerdo).
2. No Assistente para Gestão de Computadores e Dispositivos, selecione a opção **Unix/Linux computers** e clique em **Next** para continuar.
3. Na secção Definir critérios de descoberta, clique no botão **Add**.
4. Defina um **Address range** IP a ser analisado e **Credentials** SSH aplicáveis aos computadores nos quais o System Center 2012 Operations Manager irá instalar o respetivo agente.
5. Confirme o âmbito e os critérios de credenciais clicando em **OK** e clique no botão **Discover** para iniciar o processo de descoberta.
6. Após a conclusão, será apresentada uma lista que permite selecionar os sistemas para monitorização/gestão.

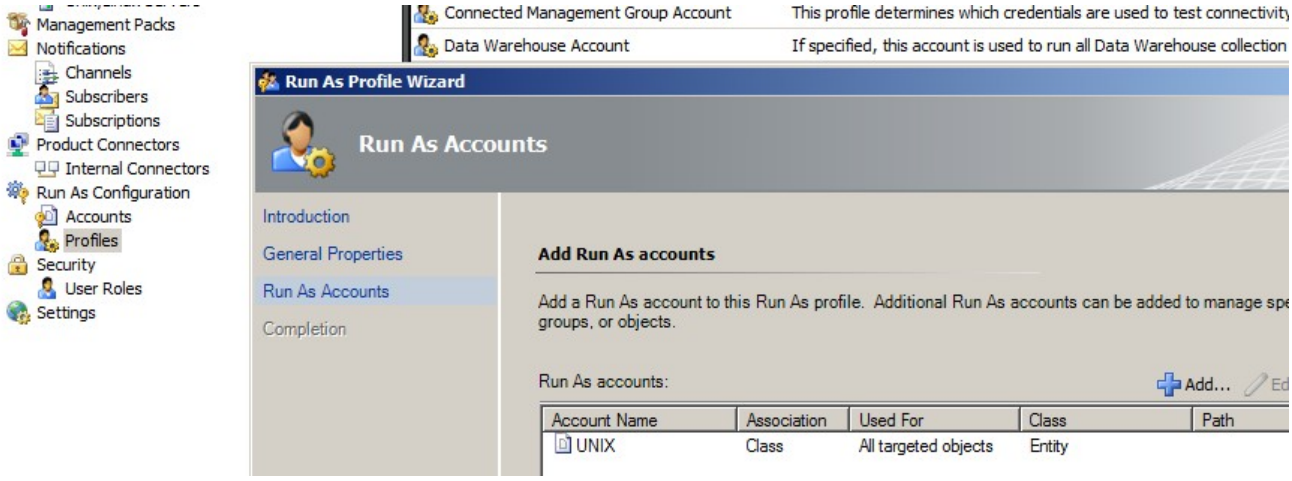
**Nota:** A instalação de um agente do Linux é suportada nas seguintes Distribuições do Linux. Se não for possível instalar o agente do Linux através da Descoberta, consulte as instruções de instalação manual no seguinte artigo da Microsoft: Instalar Agentes Entre Plataformas Manualmente (http://technet.microsoft.com/en-us/library/dd789016.aspx).

**Nota:** a descoberta de servidores Linux com uma instalação do SCEP é executada automaticamente em intervalos de 8 horas em todos os computadores Linux geridos através do Operations Manager (ou seja, têm o pacote de gestão do Linux adequado instalado para a distribuição do sistema). A descoberta cria todas as entidades de módulo de serviço: O Servidor Linux protegido e as entidades aninhadas ou o Servidor Linux desprotegido (podem ser encontrados nas secções adequadas). O SCEP pode ser considerado completamente instalado quando o serviço "scep_daemon" existe (interrompido ou em execução). Assim, a primeira descoberta ocorrerá durante a instalação de um pacote de gestão e a próxima será executada no prazo de 8 horas, em relação ao ciclo de descoberta. Se um produto SCEP for desinstalado, o respetivo servidor será automaticamente transferido para Desprotegido (Servidores sem SCEP) e vice-versa.

**Configuração de Contas Executar Como**

Para criar uma conta do Unix, siga estas instruções:

1. Na área de trabalho **Administration** (painel esquerdo), navegue até **Run As Configuration** > **Accounts**.
2. Para criar uma nova conta, abra a secção **Actions** no painel **Ações** (painel direito) e clique em **Criar Conta Executar Como...**
3. Na janela Propriedades Gerais, selecione **Basic Authentication** no menu pendente **Run As Account type**.
4. Depois de criar uma nova conta, é necessário adicioná-la a um perfil para que a distribuição ocorra. Para isso, clique com o botão direito do rato no perfil **Unix Privileged Account** em **Run As Configuration** > **Profiles**, selecione **Properties** e conclua o assistente para atribuir a conta recém-criada.




**Nota:** para obter mais informações sobre a criação de uma conta Executar Como, consulte o tópico Configurar uma Conta Executar Como Entre Plataformas (http://go.microsoft.com/fwlink/?LinkId=160348) na biblioteca online do System Center 2012 Operations Manager 2007 R2.

Depois de concluídos todos os passos acima, os servidores Linux recém-descobertos ficarão disponíveis em breve (em questão de minutos) em **Monitoring** > **Linux do System Center Endpoint Protection** > **Servidores com SCEP**.

**Instalação de um pacote de idioma para o SCEP**

O formato de um pacote de idioma é o seguinte:
Microsoft.SCEP.Linux.Application.LNG.mp e Microsoft.SCEP.Linux.Library.LNG.mp

Utilize os mesmos passos para instalar o pacote de idioma que os passos descritos na secção **Importar Pacotes de Gestão** acima. Para apresentar o idioma instalado no System Center 2012 Operations Manager, utilize as seguintes instruções:

1. Clique no ícone **Iniciar** do Windows e navegue até ao **Painel de Controlo**.
2. No Painel de Controlo, clique nas **Opções Regionais e de Idioma**.
3. Altere a região do sistema para programas não Unicode no separador **Administrativo**. No separador **Localização**, altere a Localização atual de acordo com o pacote de idioma instalado.

## Finalidade do Pacote de Gestão

O Pacote de Gestão do SCEP oferece as seguintes funcionalidades:

- Monitorização e alertas em tempo real para incidentes de segurança e o estado de integridade de segurança.
- Permite que os administradores de servidor executem tarefas relativas à segurança nos servidores remotamente. O principal objetivo destas tarefas é corrigir problemas de disponibilidade por questões de segurança.

## Vistas

O administrador de servidor pode monitorizar todos os computadores com o Operations Manager instalado a partir da consola do SCOM. Estão disponíveis as seguintes Vistas para o "Linux do System Center Endpoint Protection":

- **Alertas Ativos** – Todos os alertas ativos do SCEP de todos os níveis de gravidade. Não inclui alertas fechados.
- **Painel** – Apresenta as áreas de trabalho Servidores com SCEP e Alertas Ativos.
- **Servidores com SCEP** – Apresenta todos os Servidores Linux Protegidos.
- **Servidores sem SCEP** – Apresenta todos os Servidores Linux Desprotegidos.
- **Estado da tarefa** – Lista todas as tarefas executadas.

Ao monitorizar o estado do SCEP com o pacote de gestão do System Center 2012 Operations Manager, pode obter uma vista instantânea da integridade do SCEP.

Em vez de esperar que um alerta seja emitido, pode consultar o resumo do estado dos componentes do SCEP a qualquer momento clicando em **Monitoring** > **Linux do System Center Endpoint Protection** > painel **Servidores com SCEP** da consola de monitorização do Operations Manager. O estado de um componente é indicado no campo Estado com ícones coloridos:

| Ícone | Estado | Descrição |
|---|---|---|
| | Healthy | Um ícone verde indica êxito ou que existem informações disponíveis que não requerem ação. |
| | Warning | Um ícone amarelo indica um erro ou um aviso. |
| | Critical | Um ícone vermelho pode indicar um erro crítico, um problema de segurança ou que um serviço está indisponível. |
| | Not monitored | Nenhum ícone indica que não foram reunidos dados relativos ao estado. |

Uma vista pode conter uma longa lista de objetos. Para localizar um objeto específico ou um grupo de objetos, pode utilizar os botões Âmbito, Pesquisar e Localizar na barra de ferramentas do Operations Manager. Para obter mais informações, consulte o tópico Como Gerir Dados de Monitorização Utilizando Âmbito, Pesquisar e Localizar (http://go.microsoft.com/fwlink/?LinkId=91983).

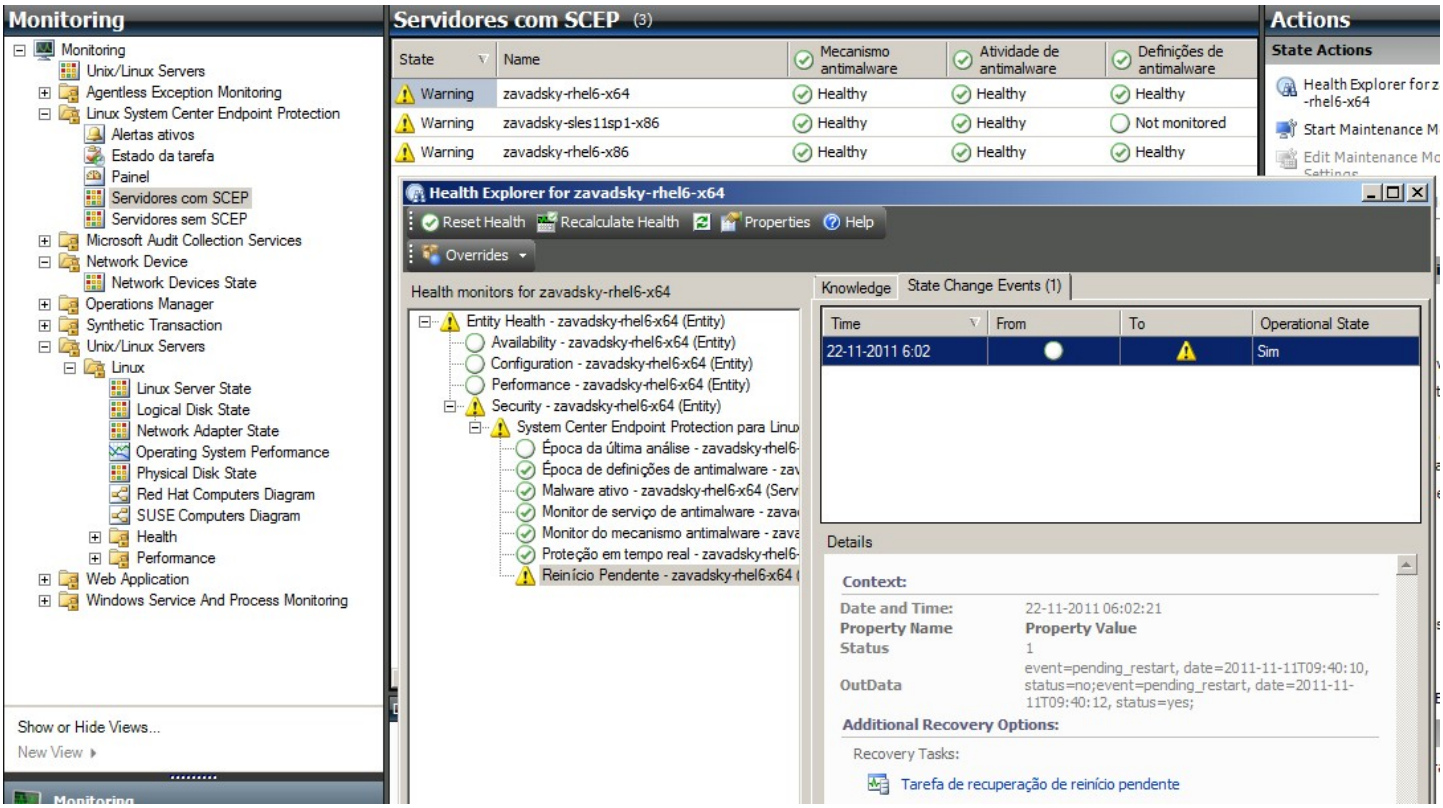
## Monitores

No Operations Manager 2007, os monitores podem ser utilizados para avaliar diversas condições que podem ocorrer em objetos monitorizados.

Existe um total de 17 monitores disponíveis para o SCEP:

- 9 Monitores de unidades – Os componentes de monitorização fundamentais são utilizados para monitorizar contadores, eventos, scripts e serviços específicos.
- 2 Monitores agregados – Utilizados para um pacote cumulativo agregado para agrupar vários monitores num único monitor e depois utilizá-lo para definir o estado de integridade e gerar um alerta.
- 6 Monitores de dependência - Referências que contêm dados sobre o estado de monitores existentes.

**Nota:** Para obter mais informações sobre os Monitores, consulte a Ajuda do Operations Manager 2007 R2 (prima a tecla F1 no System Center 2012 Operations Manager).




Os Monitores de integridade do SCEP possuem a estrutura e as propriedades descritas a seguir.

**Malware ativo**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Monitoriza o relatório de texto: /var/log/scep/eventlog_scom.dat |
| Intervalo | Controlado por evento |

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alerta | Sim. Sem resolução automática. |
| Redefinir comportamento | Volta ao estado Saudável automaticamente após um período de 8 horas. O alerta permanece ativo para reter as informações sobre o malware não tratado. |
| Notas | Este monitor mudará o estado para Crítico se for detetado malware que não tenha sido limpo. O estado reverte automaticamente para Saudável após 8 horas (isto porque não é possível determinar com precisão se o malware foi limpo/eliminado ou não). É necessária a intervenção do administrador para verificar as circunstâncias e fechar o bilhete manualmente. |
| Estado | Saudável – Sem malware<br>Crítico – Malware ativo |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Este monitor rastreia operações de limpeza de malwares mal sucedidas. Este monitor relata um estado Crítico se o cliente relatar que não conseguiu limpar o malware.

**Época de definições de antimalware**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Comando utilizado para obter dados de monitorização: /opt/microsoft/scep/sbin/scep_daemon --status |
| Intervalo | A cada 8 horas |
| Alerta | Sim. Resolução automática |
| Estado | Saudável – época <= 3 dias<br>Aviso – época > 3 E época <= 5 dias<br>Crítico – época > 5 dias |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Sim, manualmente (sem recuperação automática) |

As definições atualizadas ajudam a garantir que o computador está protegido contra as ameaças de malware mais recentes.

**Mecanismo antimalware**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Monitoriza o relatório de texto: /var/log/scep/eventlog_scom.dat |
| Intervalo | Controlado por evento |
| Alerta | Sim. Resolução automática |
| Estado | Saudável – Ativado<br>Desativado – Aviso |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Sim, manualmente (sem recuperação automática) |

Recomenda-se que a proteção antimalware esteja sempre ativada.
**Nota:** Este monitor controla o estado da Proteção antivírus, que é diferente da Proteção em tempo real. Com o Mecanismo antimalware desativado, não é possível iniciar uma Análise a pedido.

**Serviço de antimalware**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Monitoriza o estado do processo: scep_daemon |
| Intervalo | A cada 10 minutos |
| Alerta | Sim. Resolução automática |
| Estado | Saudável – Em execução<br>Crítico – Não está em execução |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Sim, manualmente (sem recuperação automática) |

O monitor relata um estado Crítico quando o serviço de antimalware (scep_daemon) na máquina cliente não está em execução ou não está a responder ou quando o mecanismo antimalware não está a funcionar corretamente.

**Época da última análise**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Comando utilizado para obter dados de monitorização: /opt/microsoft/scep/sbin/scep_daemon --status |
| Intervalo | A cada 8 horas |
| Alerta | Não |
| Estado | Saudável – época <= 7<br>Aviso – época > 7 |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Sim, manualmente (sem recuperação automática) |

Este monitor controla o tempo desde a última análise do computador (independentemente do tipo de análise). Recomendamos que agende uma análise para execução semanal.

**Reinício Pendente**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Monitoriza o relatório de texto: /var/log/scep/eventlog_scom.dat |
| Intervalo | Controlado por evento |
| Alerta | Sim. Resolução automática |
| Estado | Não – Saudável<br>Sim – Aviso |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Sim, manualmente (sem recuperação automática) |

Este monitor controla a necessidade de reiniciar o sistema para que as alterações à configuração sejam implementadas (geralmente quando a Proteção em tempo real é ativada/desativada). O monitor aplica a seguinte chamada para uma atualização a pedido deste estado: /opt/microsoft/scep/sbin/scep_daemon --status.

**Proteção em tempo real**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Servidor Linux protegido |
| Origem de dados | Monitoriza o relatório de texto: /var/log/scep/eventlog_scom.dat<br>O monitor também pode utilizar a seguinte chamada para uma atualização de estado a pedido: /opt/microsoft/scep/sbin/scep_daemon --status. |
| Intervalo | controlado por evento |
| Alerta | Sim. Resolução automática |
| Estado | Ativado – Saudável<br>Desativado – Aviso |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Sim, manualmente (sem recuperação automática) |

Monitoriza o estado da Proteção em tempo real. A proteção em tempo real alerta quando vírus, spyware ou outro software potencialmente indesejado tenta instalar-se no computador.

**System Center Endpoint Protection para Linux**

| | |
|---|---|
| Tipo de monitor | Monitor agregado |
| Alvo | Servidor Linux protegido |
| Condição | Pior de |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Este monitor é o pacote cumulativo de integridade (pior estado) de todos os monitores de unidade de segurança Servidor Linux protegido do SCEP 7. Se o estado não foi inicializado, a monitorização não começou para este objeto ou não há monitores de segurança definidos para este objeto.

**Mecanismo antimalware**

| | |
|---|---|
| Tipo de monitor | Monitor de dependência |

| | |
|---|---|
| Alvo | Mecanismo antimalware |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Apresenta o estado do monitor de unidade Servidor Linux protegido/Mecanismo antimalware na lista de computadores monitorizados.

**Serviço de antimalware**

| | |
|---|---|
| Tipo de monitor | Monitor de dependência |
| Alvo | Mecanismo antimalware |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Apresenta o estado do monitor de Unidade Servidor Linux protegido/Serviço de antimalware na lista de computadores monitorizados.

**Definições de antimalware**

| | |
|---|---|
| Tipo de monitor | Monitor de dependência |
| Alvo | Definições de antimalware |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Apresenta o estado do monitor de unidade Servidor Linux protegido/Época de definições de antimalware na lista de computadores monitorizados.

**Malware ativo**

| | |
|---|---|
| Tipo de monitor | Monitor de dependência |
| Alvo | Atividade de antimalware |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Apresenta o estado do monitor Servidor Linux protegido/Malware ativo no Gestor de integridade para Atividade de antimalware.

**Ping de máquina**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Atividade de antimalware |
| Intervalo | A cada 60 minutos |
| Alerta | Não |
| Estado | Acessível – Saudável<br>Inacessível – Crítico |
| Ativado | Falso |
| Tarefa de recuperação | Não |

Altera o estado para Crítico caso não haja resposta do servidor.

**Atividade de malware**

| | |
|---|---|
| Tipo de monitor | Monitor de unidade |
| Alvo | Atividade de antimalware |
| Origem de dados | Monitoriza o relatório de texto: /var/log/scep/eventlog_scom.dat |
| Intervalo | Controlado por evento |
| Alerta | Não |
| Estado | Sem malware – Saudável<br>Atividade de malware detetada – Crítico |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Este monitor é alterado para o estado Crítico 5 minutos após a deteção do malware (limpo ou não tratado) e permanece como Crítico durante os 60 minutos seguintes. O estado Crítico é atualizado a cada nova deteção positiva juntamente com a atualização da duração do período de alerta. Por outras palavras, se nenhum malware for detetado no sistema durante um período de 60 minutos, o monitor volta ao estado Saudável.

**Aparecimento de malware de servidor**

| | |
|---|---|
| Tipo de monitor | Monitor agregado |
| Alvo | Atividade de antimalware |
| Condição | Melhor de |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Monitores agregados: Atividade de malware, Ping de máquina.
Altera o estado para Crítico se não houver resposta do servidor dentro de 60 minutos após uma deteção de malware positiva (limpo ou não tratado). A alteração do estado para Crítico também pode ser acionada se, após determinado período sem resposta do servidor, o malware for detetado logo após a renovação da ligação.

**Aparecimento de malware**

| | |
|---|---|
| Tipo de monitor | Monitor de dependência |
| Alvo | Observador de servidores protegidos |
| Condição | Pior de 95% |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

Apresenta o estado do monitor Atividade de antimalware/Aparecimento de malware de servidor.
Se mais de 5% de todos os computadores Linux (protegidos e não protegidos) registarem uma deteção de malware ocorrida nos últimos 60 minutos, este monitor será alterado para o estado Crítico.

**Pacote cumulativo de integridade do papel do computador SCEP Linux**

| | |
|---|---|
| Tipo de monitor | Monitor de dependência |
| Alvo | Computador Linux |
| Alerta | Não |
| Ativado | Verdadeiro |
| Tarefa de recuperação | Não |

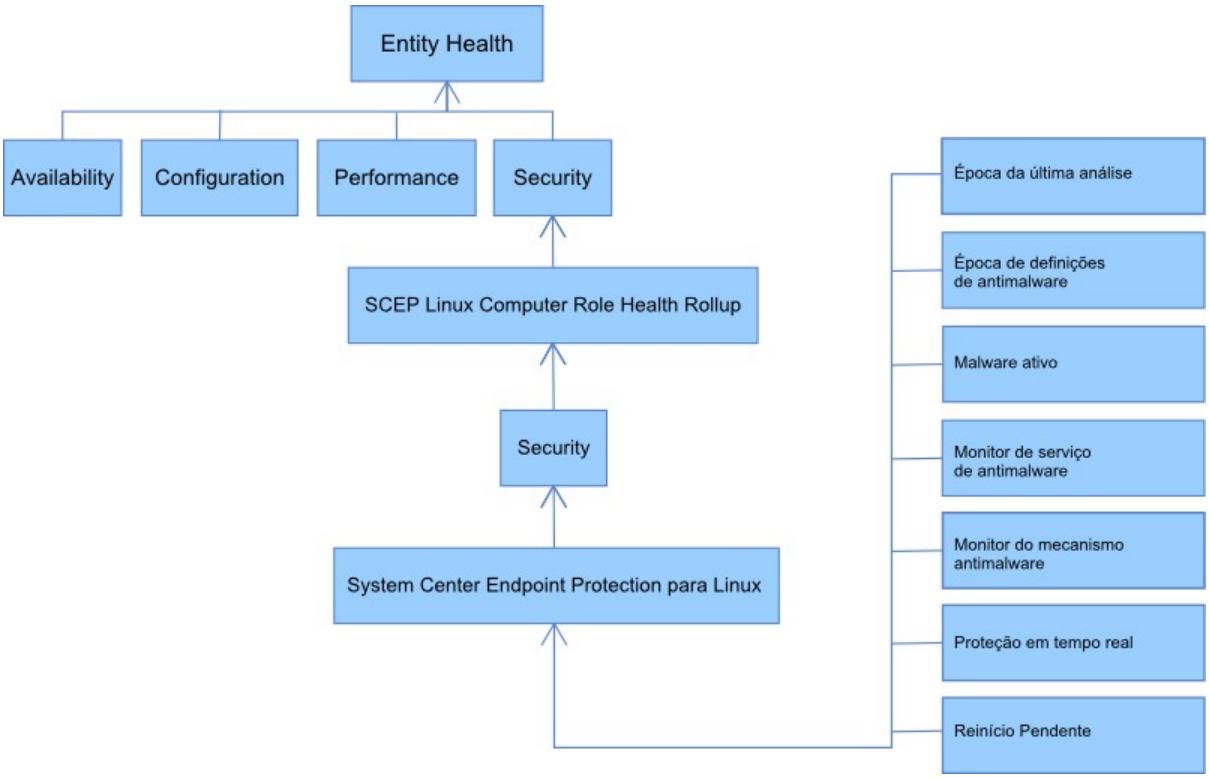
Propaga o estado da entidade Computador Linux protegido para o monitor principal Computador Linux/Segurança.

## Como Funciona o Pacote Cumulativo de Integridade

Este pacote de gestão expande a monitorização do sistema operativo Linux como uma estrutura em camadas na qual cada camada depende da camada inferior para ser saudável. O nível mais alto desta estrutura corresponde ao ambiente completo da Integridade da Entidade, e o nível mais baixo dos ambientes de Segurança corresponde a todos os monitores. Quando o estado de uma das camadas é alterado, o estado da camada acima também é alterado em conformidade. Esta ação é designada por integridade do pacote cumulativo.

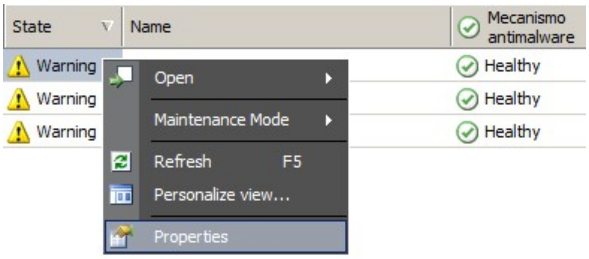
Por exemplo, se a Proteção em tempo real devolver o estado Aviso e todos os outros componentes tiverem o estado Saudável, o estado Aviso será transferido através da estrutura em árvore até chegar à raiz (Integridade da Entidade), a qual também adquirirá o estado Aviso.

O diagrama a seguir mostra como os estados de integridade dos objetos são acumulados neste pacote de gestão.



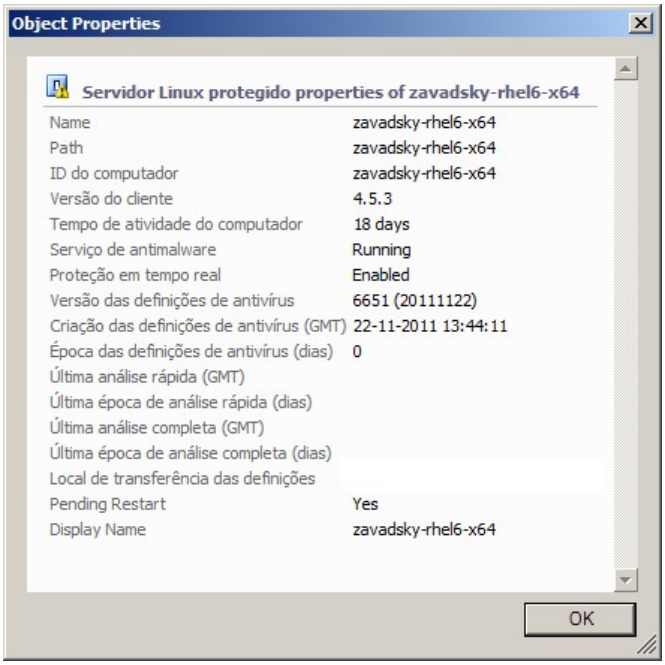

## Propriedades de Objetos

Para ver as propriedades de um objeto, clique com o botão direito do rato e selecione **Properties**.




O objeto Servidor Linux protegido tem as seguintes propriedades:

- **ID do Computador** – Identificador do servidor e nome do domínio.
- **Nome de Visualização** – Nome do servidor e nome do domínio.
- **Versão do Cliente** – Versão do produto SCEP instalada.
- **Tempo de Atividade do Computador** – Tempo de atividade do servidor (quanto tempo uma máquina está ativa sem tempo de inatividade) não é um dado essencial para o funcionamento adequado de um pacote de gestão, porém, a sua ausência pode indicar um erro no pacote de gestão.
- **Serviço de Antimalware** – Estado da proteção antimalware (Em execução/Não está em execução).
- **Proteção Em Tempo Real** – Estado da Proteção em tempo real. A sua ausência assinala problemas no SCEP.
- **Definições de Antivírus...** – Dados sobre o estado da base de dados de vírus (versão, data de criação, época). A ausência de dados assinala problemas no SCEP.
- **Última Análise Rápida/Completa...** – Dados sobre a última análise do computador. Se a análise (Análise Rápido/Completa) ainda não tiver sido executada, não serão apresentados quaisquer dados.
- **Local de Transferência das Definições** – Endereço/nome do servidor de atualização. As informações são apresentadas após a primeira atualização bem sucedida.
- **Reinício Pendente** – Informações sobre a necessidade de reinício para que as alterações sejam aplicadas devido a uma nova instalação ou a alterações na configuração do SCEP.




## Alertas

Um alerta é um item que indica que uma situação predefinida com uma gravidade específica ocorreu num objeto monitorizado. Os alertas são definidos por regras. Na consola Operations Manager, existe uma vista disponível em **Monitoring** > **Linux do System Center Endpoint Protection** > **Alertas Ativos** que mostra os alertas que o utilizador da consola tem direito a ver para um objeto específico.

**Nota:** se forem gerados mais alertas do mesmo tipo várias vezes (por exemplo, Malware ativo) no mesmo servidor, apenas o primeiro será apresentado (os alertas redundantes serão ignorados).

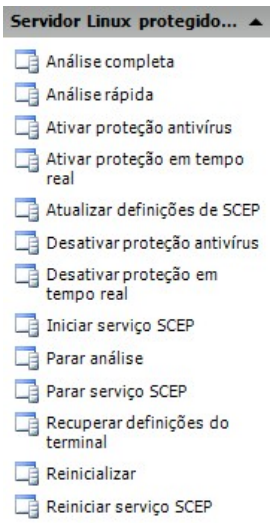
| Alerta | Intervalo | Prioridade | Gravidade | Descrição |
|---|---|---|---|---|
| Infeção por malware repetida | Controlado por evento | Alta | Crítica | O alerta é gerado em caso de deteções de malware repetidas (3 ocorrências) num determinado intervalo de tempo (30 minutos). O alerta contém dados sobre o servidor e informações básicas sobre o malware. |
| Malware limpo | Controlado por evento | Baixa<br>Média | Informações – Malware limpo com êxito<br>Aviso – Interação do utilizador necessária (por exemplo, reiniciar o servidor) | Alerta sobre um malware limpo com êxito. Contém todos os dados disponíveis sobre o malware específico. Cada malware detetado gera um alerta individual. O SCEP Linux atribui a prioridade e a gravidade com base na eficiência do processo de limpeza, em que:<br>Limpo = baixa + informações<br>Limpo, mas uma ação é necessária (por exemplo, reinício = média + aviso. |
| Malware ativo (do Monitor) | Controlado por evento | Alta | Crítica | Alerta sobre um malware que não foi limpo. Contém todos os dados disponíveis sobre o malware específico. |
| Malware ativo (da Regra) | Controlado por evento | Alta/Média/ Baixa | Crítica/Média/Baixa – baseada num tipo de Malware | O mesmo que acima. Utilizado para conectores para outros sistemas de monitorização/bilhetes.<br>**Nota:** Esta regra (alerta) é desativada por predefinição. |
| O serviço de antimalware do System Center Endpoint Protection não funciona | 300 segundos | Média | Crítica | Alerta sobre indisponibilidade do SCEP do serviço de antimalware (scep_daemon). Inclui o respetivo nome de servidor e a versão do SCEP. |
| Proteção antimalware desativada | Controlado por evento | Média | Aviso | Alerta sobre a desativação da Proteção antimalware. Inclui o respetivo nome de servidor. |

| | | | | |
|---|---|---|---|---|
| Proteção em tempo real desativada | Controlado por evento | Média | Aviso | Alerta sobre a desativação da Proteção em tempo real. Inclui o respetivo nome de servidor. |
| Definições desatualizadas | A cada 8 horas | Média | Aviso (época <= 5 dias E época > 3 dias)<br>Crítica (época > 5 dias) | Alerta sobre o facto de a base de dados de assinatura de vírus não ser atualizada há mais de 3 dias. Inclui o respetivo nome de servidor e a época da base de dados de assinatura de vírus. |
| Aparecimento de malware | Controlado por evento | Alta | Crítica | O Forefront Endpoint Protection detetou mais de 5% de malware ativo nos computadores. É possível que o malware esteja a propagar nos computadores. Sugere-se que verifique se todos os servidores utilizam as definições mais atualizadas. Se for necessário alterar o número de ameaças ativas que geram este alerta, substitua o parâmetro do monitor Aparecimento de malware (consulte o capítuloSubstituições). |

## Tarefas

O Pacote de Gestão do SCEP implementa 13 tarefas. A execução destas tarefas é imediata. As saídas são apresentadas imediatamente após a execução das tarefas ou podem ser visualizadas posteriormente na janela Estado da tarefa. O tempo máximo necessário para a execução da tarefa é de 180 segundos. A substituição não está disponível. Todas as tarefas são comandos BASH executados através de SSH.

As tarefas podem ser invocadas em **Monitoring** > **Linux do System Center Endpoint Protection** > **Servidores com SCEP** no painel direito da janela Consola de Operações.




- **Desativar Proteção Antivírus** – Desativa todos os componentes da proteção antivírus e desativa a Análise a pedido.
- **Ativar Proteção Antivírus** – Ativa todos os componentes da proteção antivírus.
- **Desativar Proteção em Tempo Real** – Desativa a Proteção em tempo real.
- **Ativar Proteção em Tempo Real** – Ativa a Proteção em tempo real.
- **Análise Completa** – Atualiza a base de dados de assinatura de vírus e executa uma análise completa do computador.
- **Análise Completa** – Atualiza a base de dados de assinatura de vírus e executa uma análise completa do computador.
- **Parar Análise** – Para todas as análises do computador em execução.
- **Recuperar Definições do Servidor** – Apresenta o estado atual do produto SCEP. A lista de parâmetros apresentada é idêntica às propriedades da entidade Servidor Linux protegido. Os dados apresentados não são transferidos para o Servidor Linux protegido.
- **Reiniciar Serviço Antimalware** – Reinicia o serviço de antimalware do SCEP (scep_daemon).
- **Parar Serviço Antimalware** – Para o serviço de antimalware do SCEP (scep_daemon).
- **Iniciar Serviço Antimalware** – Inicia o serviço de Antimalware do SCEP (scep_daemon).
- **Atualizar Definições de Antimalware** – Inicia a atualização da base de dados de assinatura de vírus.
- **Reinicializar** – Reinicia o computador Linux.

## Configurar o Pacote de Gestão do SCEP

### Prática Recomendada: Criar um Pacote de Gestão para Personalizações

Por predefinição, o Operations Manager guarda todas as personalizações (por exemplo, substituições) no Pacote de Gestão Padrão. Como prática recomendada, deve criar, em alternativa, um pacote de gestão separado para cada pacote de gestão lacrado que pretende personalizar.

Quando cria um pacote de gestão com a finalidade de armazenar definições personalizadas de um pacote de gestão lacrado, é útil basear o nome do novo pacote no nome do pacote que o mesmo personalizará (por exemplo, "Personalizações do SCEP 2012").

A criação de um novo pacote de gestão para armazenar personalizações de cada pacote de gestão lacrado facilita a exportação de personalizações de um ambiente de teste para um ambiente de produção. Além disso, facilita também a eliminação de um pacote de gestão, pois é necessário eliminar todas as dependências para que seja possível eliminar o pacote de gestão em si. Se as personalizações de todos os pacotes de gestão forem guardadas no Pacote de Gestão Padrão e for necessário eliminar um único pacote de gestão, primeiro será necessário eliminar o Pacote de Gestão Padrão, o que também eliminará personalizações de outros pacotes de gestão.

### Configuração da Segurança

O computador deve executar o serviço SSHD e a porta SSH (valor predefinido 22) deve estar aberta. O System Center 2012 Operations Manager estabelece ligação através da porta aos computadores Linux remotos utilizando o tipo Run As Account adequado (localizado no painel **Administration** > **Run As Configuration** da Consola de monitorização do Operations Manager) com o tipo **Basic Authentication**.

| Nome do Perfil Executar Como | Notas |
|---|---|
| Unix Privileged Account | Utilizada para monitorizar remotamente o servidor Unix, bem como para reiniciar processos quando são necessários direitos privilegiados. |

Este pacote de gestão não utiliza a Unix Action Account.

***Aviso:*** A monitorização de computadores utilizando a conta raiz gera um possível risco de segurança, caso a palavra-passe tenha sido descoberta.

Caso não pretenda utilizar a conta raiz para monitorizar e gerir, pode utilizar uma conta de utilizador padrão, porém esta conta necessita de ter direitos que permitam executar comandos *sudo*. Por esta motivo, a seguinte configuração deve existir no ficheiro /etc/sudoers em todas as estações de trabalho monitorizadas pelo SCEP Linux, para autorizar a elevação sudo para a conta de utilizador selecionada. Este é um exemplo da configuração para o nome de utilizador user1:

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

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

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

### Ajustar as Regras de Limite de Desempenho

A tabela a seguir lista as regras de limite de desempenho que apresentam limites predefinidos que podem requerer ajuste adicional para satisfazer as necessidades do seu ambiente. Avalie estas regras para determinar se os limites predefinidos são adequados para o seu ambiente. Se um limite predefinido não for adequado para o seu ambiente, pode ajustar os limites aplicando uma substituição aos mesmos.

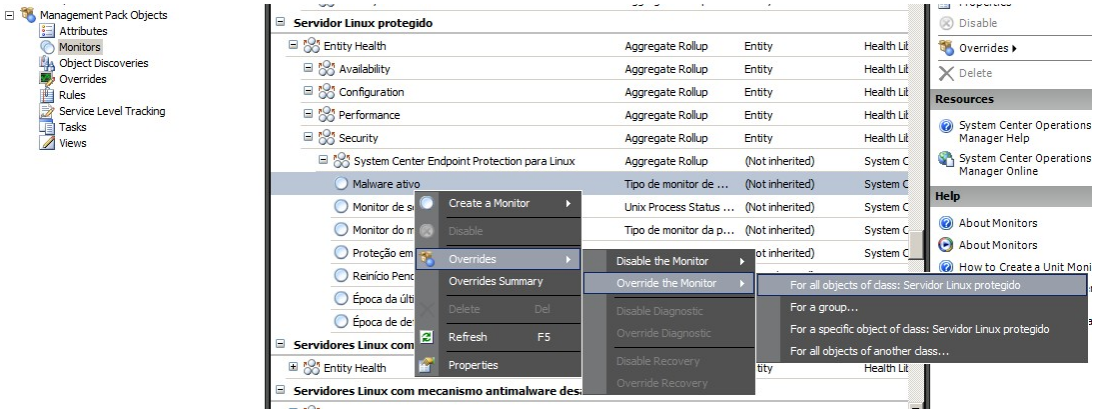
| Nome da regra | Parâmetro de substituição | Limite predefinido | Limitações de ajuste |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Regra da infeção por malware repetida | Limite de contagem de infeção repetida | 3 ocorrências | A definição de um valor inferior a 2 torna a regra obsoleta. |
| Regra da infeção por malware repetida | Janela de tempo de infeção repetida | 30 minutos | Não é recomendável que defina um valor inferior à duração de uma Análise a pedido, uma vez que uma sobreposição pode impedir a geração de um alerta. |
| Regra de Alerta de Malware Ativo | Ativado | Falso | Se utilizar conectores para outros sistemas de monitorização/bilhetes, pode ativar este alerta. |

## Substituições

As substituições podem ser utilizadas para otimizar as configurações de um objeto de monitorização no System Center 2012 Operations Manager. Isto inclui monitores, regras, descobertas de objetos e atributos provenientes de pacotes de gestão importados.

Para substituir um monitor, na Consola de Operações, clique no botão **Authoring** e expanda **Management Pack Objects** > **Monitors**. No painel Monitores, localize e expanda completamente o tipo de objeto. Em seguida, clique num monitor e depois em **Overrides**.



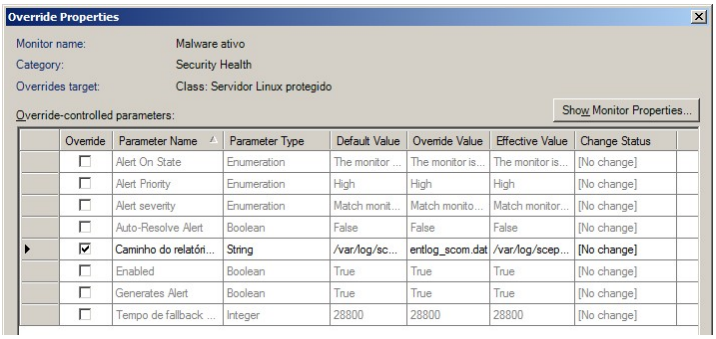

Utilize a janela Substituições para criar ou modificar uma substituição para uma ocorrência de qualquer um dos seguintes parâmetros:

- **Tempo de Fallback de Monitor de Malware Ativo** (relacionado apenas com o monitor Malware ativo)
- **Época de Definições de Antimalware** (relacionado apenas com o monitor Época de Definições de Antimalware)
- **Intervalo de Deteção** (relacionado apenas com o monitor Época da Última Análise)
- **Estado de alerta ativo**
- **Prioridade do alerta**
- **Gravidade do alerta**
- **Alerta de resolução automática**
- **Ativado** – Determina se o monitor selecionado está ativado ou desativado.
- **Gera alerta**
- **Caminho do relatório SCEP**

Se uma substituição predefinida não for adequada para o seu ambiente, pode ajustar os limites aplicando uma substituição aos mesmos:

| Parâmetro de substituição | Nome do monitor | Valor predefinido | Notas de ajuste |
|---|---|---|---|
| Intervalo ping | Ping de máquina | 3600 segundos | Intervalo para verificar a disponibilidade do Servidor Linux protegido. Uma duração mais curta aciona um estado de Erro no monitor Aparecimento de malware de servidor mais rápido, caso a máquina pare de responder devido a um ataque. Consequentemente, a carga na rede, no computador monitorizado e no servidor do System Center 2012 Operations Manager aumenta. |

| | | | |
|---|---|---|---|
| Janela de tempo do aparecimento de malware | Atividade de malware | 3600 segundos | Intervalo necessário para o monitor voltar ao estado Saudável após uma atividade de malware. Para que a combinação funcione corretamente, o valor do monitor Janela de tempo deve ser maior que o Ping de máquina/Intervalo ping.<br>Se, durante o intervalo da Janela de tempo do aparecimento de malware, um número de computadores superior ao valor percentual definido para Aparecimento de malware (consulte Aparecimento de malware) registar atividade de malware, será gerado um alerta Aparecimento de malware.<br><br>Nota: É diferente do Aparecimento de malware de servidor, que não gera um alerta. |
| Tempo de fallback de monitor de malware ativo | Malware ativo | 28800 segundos | Intervalo de tempo, desde a deteção de malware, após o qual o malware é considerado limpo. |
| Caminho do relatório SCEP | Malware ativo | /var/log/scep/ eventlog_scom.log | Caminho para o ficheiro em que os eventos do System Center 2012 Operations Manager são gravados. Não altere este parâmetro, a não ser que ocorram problemas. |
| Época crítica de definições de antimalware | Época de definições de antimalware | 5 dias | Após este intervalo, é gerado um alerta de Erro a notificar sobre um produto SCEP desatualizado. |
| Época saudável de definições de antimalware | Época de definições de antimalware | 3 dias | Época máxima permitida para definições de antimalware durante a qual podem ser consideradas atualizadas. Este valor deve ser sempre inferior ao valor da Época crítica de definições de antimalware. |
| Intervalo | Época de definições de antimalware | 28800 segundos | Intervalo de verificação da época de definições de antimalware. |
| Intervalo | Serviço de antimalware | 300 segundos | Intervalo de verificação da disponibilidade do Serviço de antimalware. |
| Nome do processo | Serviço de antimalware | scep_daemon | Nome do serviço de antimalware. Não altere este valor se o monitor estiver operacional. |
| Intervalo de deteção | Época da última análise | 28800 segundos | Intervalo de verificação da última análise executada. |
| Época máxima da análise | Época da última análise | 7 dias | Deve ser configurada de acordo com as definições do produto SCEP. Se uma análise estiver agendada para cada 7 dias, defina este valor para 7 dias. |
| Caminho do relatório | Reinício Pendente | /var/log/scep/ eventlog_scom.log | Caminho para o ficheiro em que os eventos do System Center 2012 Operations Manager são gravados. Não altere este parâmetro, a não ser que ocorram problemas. |
| Caminho do relatório SCEP | Proteção em tempo real | /var/log/scep/ eventlog_scom.log | Caminho para o ficheiro em que os eventos do System Center 2012 Operations Manager são gravados. Não altere este parâmetro, a não ser que ocorram problemas. |
| Percentagem | Aparecimento de malware | 95% | Percentagem dos Servidores Linux (protegidos e não protegidos) necessária para que o estado Saudável seja devolvido e o grupo monitorizado completo seja considerado Saudável. Se for detetado malware em 5% ou mais do total, será gerado um Aparecimento de malware. |




**Nota:** Para obter mais informações sobre Substituições, consulte Como Monitorizar Utilizando Substituições (http://go.microsoft.com/fwlink/?LinkID=117777).

## Hiperligações

As seguintes hiperligações permitem ligá-lo a informações sobre tarefas comuns associadas a este pacote de Gestão:

- Administrar o Ciclo de Vida do Pacote de gestão (http://go.microsoft.com/fwlink/?LinkId=211463)
- Como importar um Pacote de Gestão no Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=142351)
- Como Monitorizar Utilizando Substituições (http://go.microsoft.com/fwlink/?LinkID=117777)
- Como Criar uma Conta Executar Como no Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=165410)
- Configurar uma Conta Executar Como Entre Plataformas (http://go.microsoft.com/fwlink/?LinkId=160348)
- Como Modificar um Perfil Executar Como Existente (http://go.microsoft.com/fwlink/?LinkID=165412)
- Como Exportar Personalizações do Pacote de Gestão (http://go.microsoft.com/fwlink/?LinkId=209940)
- Como Remover um Pacote de Gestão (http://go.microsoft.com/fwlink/?LinkId=209941)
- Como Gerir Dados de Monitorização Utilizando Âmbito, Pesquisar e Localizar (http://go.microsoft.com/fwlink/?LinkId=91983)
- Monitorizar o Linux Utilizando o SCOM 2007 R2 (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Instalar Agentes Entre Plataformas Manualmente (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- Configurar Elevação sudo para o UNIX e Monitorizar o Linux com o 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)

Para obter respostas a perguntas sobre o Operations Manager e pacotes de monitorização, consulte o fórum da comunidade do System Center Operations Manager (http://go.microsoft.com/fwlink/?LinkID=179635).
Um recurso útil é o blogue System Center Operations Manager Unleashed (http://opsmgrunleashed.wordpress.com/), que contém publicações com exemplos sobre pacotes de monitorização específicos.

Para obter mais informações sobre o Operations Manager, consulte os seguintes blogues:

- Blogue da Equipa do Operations Manager (http://blogs.technet.com/momteam/default.aspx)
- Blogue de Kevin Holman sobre o Operations Manager (http://blogs.technet.com/kevinholman/default.aspx)
- Blogue Thoughts on OpsMgr (http://thoughtsonopsmgr.blogspot.com/)
- Blogue de Raphael Burri (http://rburri.wordpress.com/)
- Blogue de BWren sobre Gestão de Espaço (http://blogs.technet.com/brianwren/default.aspx)
- Blogue da Equipa de Suporte do System Center Operations Manager (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++ (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Notas sobre o System Center Operations Manager

(http://blogs.msdn.com/mariussutara/default.aspx)

Para obter informações sobre a resolução de problemas, visite estes tópicos do fórum:

- O Microsoft.Unix.Library está em falta (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)