System Center
para Endpoint Protection para Linux

Microsoft Corporation

Data de publicação: 10/26/2015

Envie comentários ou sugestões sobre este documento para mpgfeed@microsoft.com. Informe o nome do guia do pacote de gerenciamento em seus comentários.

A equipe do Operations Manager incentiva os usuários a enviarem comentários sobre o pacote de monitoramento inserindo suas observações na página do pacote de gerenciamento no Catálogo de Pacotes de Gerenciamento (http://go.microsoft.com/fwlink/?LinkID=82105).

Índice

Guia do pacote de gerenciamento do SCEP

Este pacote de gerenciamento permite gerenciar o System Center Endpoint Protection (SCEP) a partir do System Center 2012 Operations Manager em um ambiente em rede, incluindo estações de trabalho e servidores, a partir de um local centralizado. Com o sistema de gerenciamento de tarefas do Operations Manager, você pode gerenciar o SCEP em computadores remotos, visualizar alertas e estados de integridade, bem como tomar providências diante de 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 operacional Linux instalado.

Este guia foi redigido com base na versão 4.5.10.1 do pacote de gerenciamento do SCEP.

Histórico do Guia

Versão	Data da Versão	Alterações
4.5.9.1	05/16/2012	Lançamento original deste guia.
4.5.10.1	11/06/2012	Novas distribuições do Linux suportadas. Melhor descrição para algumas ferramentas do pacote de gerenciamento.

Alterações na Versão 4.5.10.1

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

- Novas distribuições do 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

  Observação: Essas novas distribuições serão compatíveis somente com o uso do System Center 2012 Operations Manager Service Pack 1 e posteriores.
- Melhor descrição adicionada para:
  - Monitor Malware ativo
  - Alerta de Malware ativo (da Regra)

Configurações com suporte

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

Este pacote de gerenciamento requer o System Center 2012 Operations Manager 2007 R2 ou posterior. A tabela a seguir detalha os sistemas operacionais compatíveis com o pacote de gerenciamento:

Nome do sistema operacional	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 atendidos para a execução deste pacote de gerenciamento:

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

Os pacotes de gerenciamento do SCEP listados a seguir são integrados ao System Center 2012 Operations Manager 2007 R2 ou estão disponíveis para download a partir do catálogo on-line.

ID	Nome	Versão

Microsoft.Linux.Library	Biblioteca do sistema operacional 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 o monitoramento do produto Linux SCEP por meio do System Center 2012 Operations Manager no arquivo de configuração */etc/opt/microsoft/scep/scep.cfg* ou na interface da Web do SCEP para que ele funcione corretamente. Certifique-se de que o parâmetro 'scom_enabled' no arquivo de configuração mencionado acima esteja definido como *'scom_enabled = yes'* ou altere a configuração correspondente na interface da Web em **Configuração** > **Global** > **Opções de Daemon** > **SCOM ativado**.

Arquivos deste pacote de gerenciamento

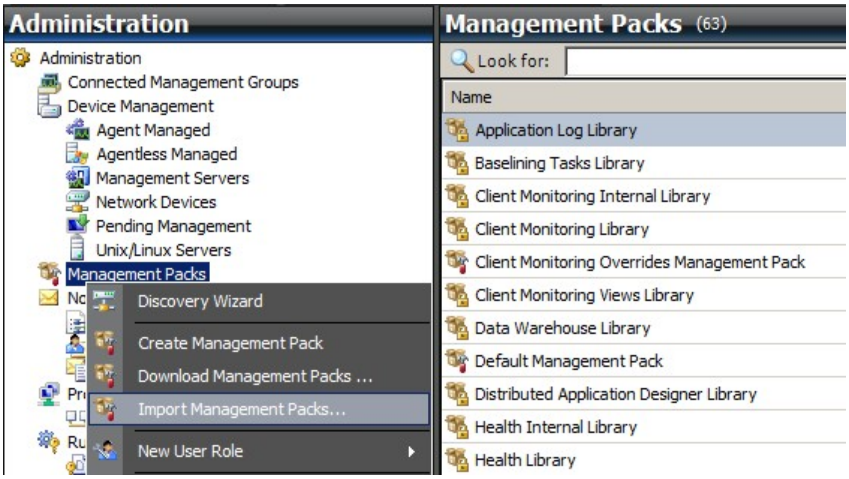
O pacote de gerenciamento do SCEP inclui os seguintes arquivos:

Nome do arquivo	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 o monitoramento, alertas, tarefas e exibições.

Início rápido

O pré-requisito para iniciar o monitoramento do SCEP é importar os pacotes de gerenciamento para o Operations Manager e identificar os computadores que serão monitorados (processo conhecido como "descoberta").

Importando pacotes de gerenciamento

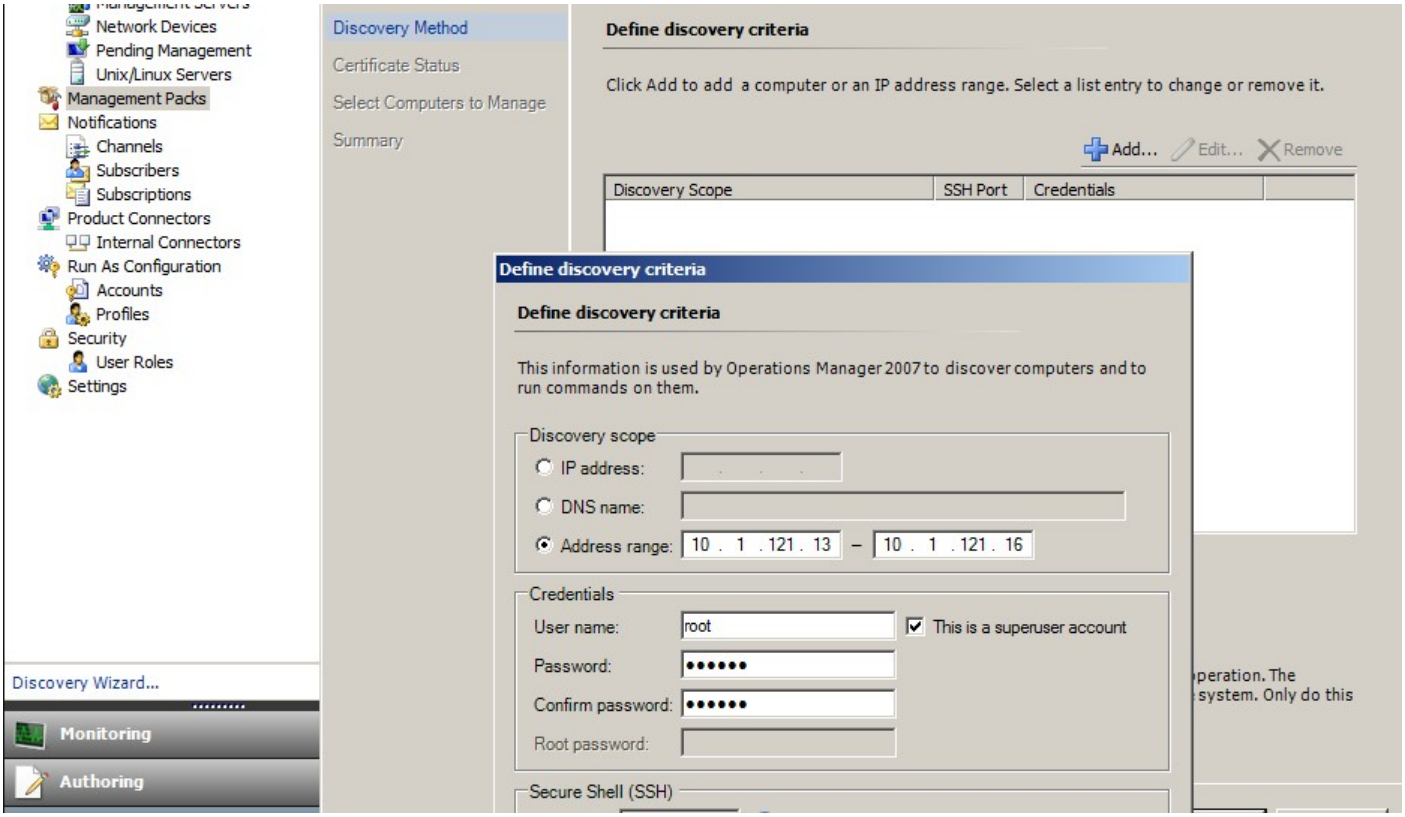


1. Clique no espaço de trabalho **Administration** no painel esquerdo da janela Console de Operações.
2. Clique com o botão direito em **Management Packs** e selecione **Import Management Packs...** no menu de contexto.
3. Na janela Pacotes de gerenciamento, clique no botão **Add** e selecione **Add from disk...** no menu suspenso.
4. Confirme que você deseja que o Operations Manager também pesquise e instale todas as dependências fora do disco local clicando em **Yes** na nova janela **Online Catalog Connection**.
5. Selecione os dois arquivos listados (Microsoft.SCEP.Linux.Application.mp, Microsoft.SCEP.Linux.Library.mp) e clique em **Install**.

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

Descoberta

Após a importação dos arquivos *.mp, será necessário realizar a descoberta do computador.



1. No espaço de trabalho **Administration** (no painel esquerdo da janela Console de Operações) clique no link **Discovery wizard...** (na parte inferior do painel esquerdo).
2. No Assistente para Gerenciamento de Computadores e Dispositivos, selecione a opção **Unix/Linux computers** e clique em **Next** para continuar.
3. Na seção Definir critérios de descoberta, clique no botão **Add**.
4. Defina um **Address range** IP a ser verificado e **Credentials** SSH aplicáveis aos computadores nos quais o System Center 2012 Operations Manager instalará seu agente.
5. Confirme o escopo e os critérios de credenciais clicando em **OK** e clique no botão **Discover** para iniciar o processo de descoberta.
6. Após a conclusão, será exibida uma lista que permite selecionar os sistemas para monitoramento/gerenciamento.

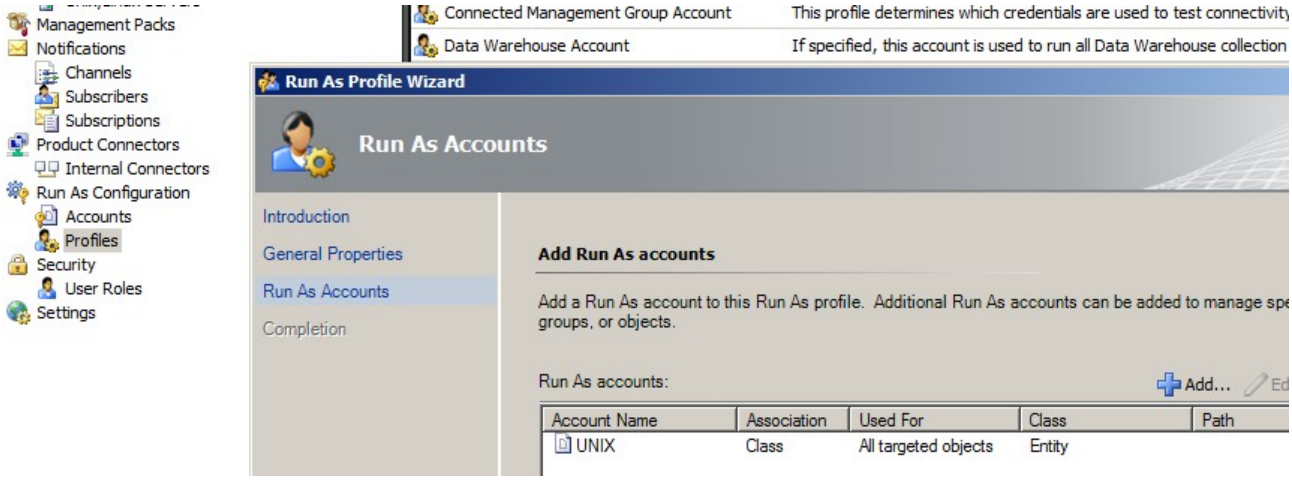
Observação: a instalação de um agente do Linux é compatível com as seguintes distribuições do Linux. Se não for possível instalar o agente do Linux através da descoberta, consulte as instruções de instalação manual no seguinte artigo da Microsoft: Instalando agentes entre plataformas manualmente (http://technet.microsoft.com/en-us/library/dd789016.aspx).

Observação: a descoberta de servidores Linux com uma instalação do SCEP é executada automaticamente em intervalos de oito horas em todos os computadores Linux gerenciados por meio do Operations Manager (ou seja, eles têm o pacote de gerenciamento 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 seções 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 gerenciamento e a próxima será executada em oito horas (em relação ao ciclo de descoberta). Se um produto SCEP for desinstalado, o respectivo 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. No espaço de trabalho **Administration** (painel esquerdo), navegue até **Run As Configuration** > **Accounts**.
2. Para criar uma nova conta, abra a seção **Actions** no painel **Ações** (painel direito) e clique em **Create Run As Account...**
3. Na janela Propriedades Gerais, selecione **Basic Authentication** no menu suspenso **Run As Account type**.
4. Depois de criar a nova conta, você precisará adicioná-la a um perfil para que a distribuição ocorra. Para isso, clique com o botão direito no perfil **Unix Privileged Account** em **Run As Configuration** > **Profiles**, selecione **Properties** e conclua o assistente para atribuir a conta recém-criada.



Observação: para obter mais informações sobre a criação de uma conta Executar como, consulte o tópico Configurando uma conta Executar como entre plataformas (http://go.microsoft.com/fwlink/?LinkId=160348) na biblioteca on-line do System Center 2012 Operations Manager 2007 R2.

Depois que as etapas acima forem concluídas, os servidores Linux recém-descobertos ficarão disponíveis em breve (em questão de minutos) em **Monitoring** > **Linux do System Center Endpoint Protection** > **Servers com SCEP**.

Instalação de um pacote de idioma para o SCEP

O formato do pacote de idioma é como se segue:
Microsoft.SCEP.Linux.Application.LNG.mp e Microsoft.SCEP.Linux.Library.LNG.mp

Use as mesmas etapas para instalar o pacote de idiomas que as descritas na seção **Importando pacotes de gerenciamento** acima. Para exibir o idioma instalado no System Center 2012 Operations Manager, siga as seguintes instruções:

1. Clique no ícone **Iniciar** do Windows e navegue até o **Painel de Controle**.
2. No Painel de Controle, clique nas **Opções Regionais e de Idioma**.
3. Altere a localidade do sistema para programas não Unicode na guia **Administrativo**. Na guia **Localização**, altere a localização atual conforme o pacote de idioma instalado.

Finalidade do pacote de gerenciamento

O pacote de gerenciamento do SCEP oferece as seguintes funcionalidades:

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

Exibições

administrador de servidor pode monitorar todos os computadores com o SCEP instalado a partir do console do Operations Manager. As seguintes exibições estão disponíveis para "Linux do System Center Endpoint Protection":

- **Alertas ativos** - Todos os alertas ativos do SCEP de todos os níveis de severidade. Não inclui alertas fechados.
- **Painel** - Exibe os espaços de trabalho Servidores com SCEP e Alertas ativos.
- **Servidores com SCEP** - Exibe todos os servidores Linux protegidos.
- **Servidores sem SCEP** - Exibe todos os servidores Linux desprotegidos.
- **Status da tarefa** - Lista todas as tarefas executadas.

Ao monitorar o estado do SCEP com o pacote de gerenciamento do System Center 2012 Operations Manager, você pode obter uma exibição instantânea da integridade do SCEP.

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

Ícone	Estado	Descrição
	Healthy	Um ícone verde indica êxito ou que há informações disponíveis que não exigem 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 coletados dados relacionados ao estado.

Uma exibição pode conter uma lista longa de objetos. Para encontrar um objeto específico ou um grupo de objetos, você pode usar os botões Escopo, Pesquisa e Localizar na barra de ferramentas do Operations Manager. Para obter mais informações, consulte o tópico Como gerenciar dados de monitoramento usando Escopo, Pesquisar e Localizar no Essentials (http://go.microsoft.com/fwlink/?LinkId=91983).

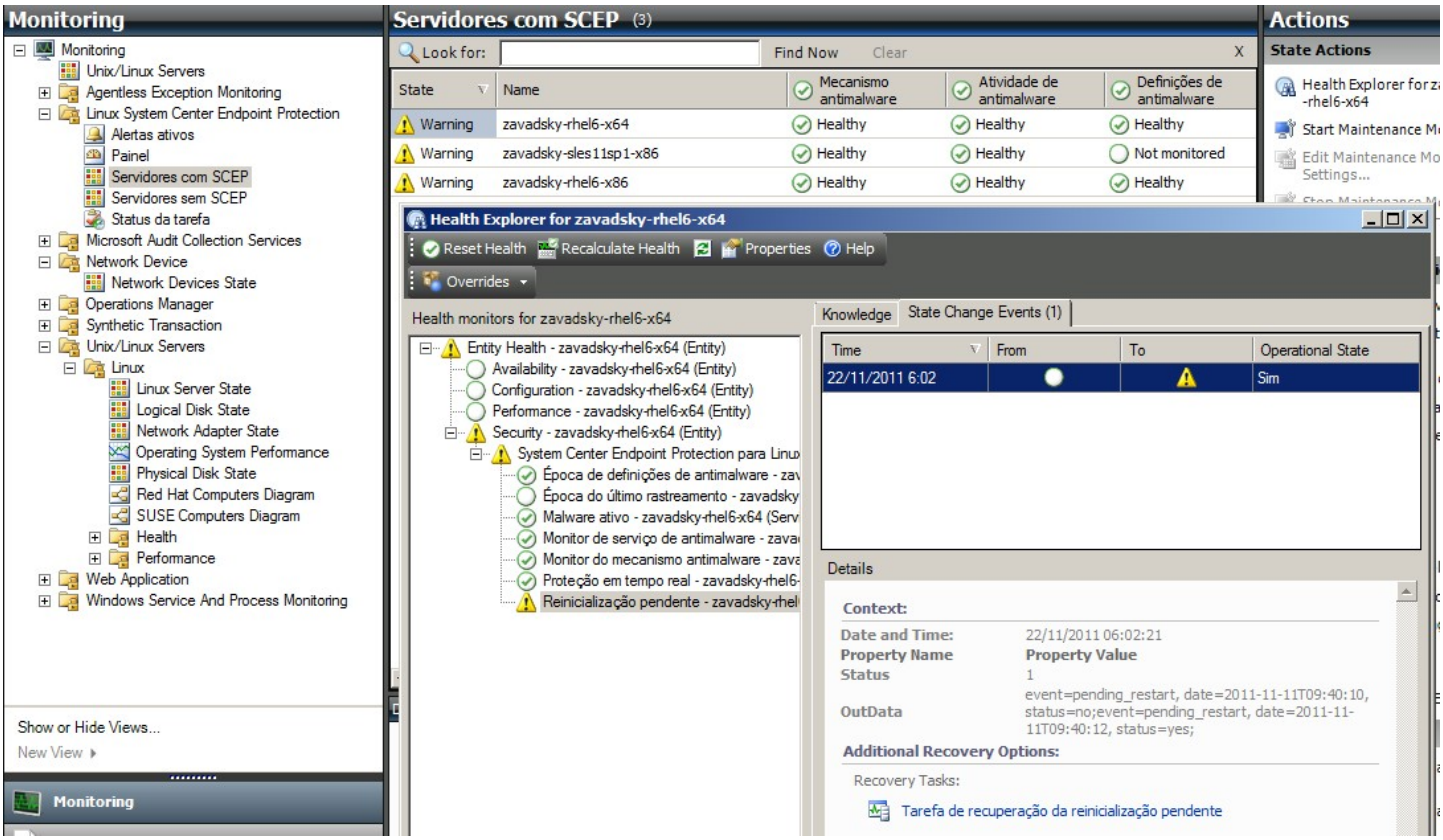
Monitores

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

Há um total de 17 monitores disponíveis para o SCEP:

- 9 monitores de unidades - Os componentes de monitoramento fundamentais são usados para monitorar contadores, eventos, scripts e serviços específicos.
- 2 monitores agregados - Usados com uma acumulação agregada para agrupar vários monitores em um único monitor e depois usá-lo para definir o estado de integridade e gerar um alerta.
- 6 monitores de dependência - Referências que contêm dados de status de monitores existentes.

Observação: Para obter mais informações sobre os monitores, consulte a Ajuda do Operations Manager 2007 R2 (pressione a tecla F1 no System Center 2012 Operations Manager).



Os monitores de integridade do SCEP têm a estrutura e as propriedades descritas a seguir.

Malware ativo

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Monitora o arquivo de log de texto: /var/log/scep/eventlog_scom.dat

Tipo de monitor	Monitor de unidade
Intervalo	Controlado por evento
Alerta	Sim. Sem resolução automática.
Redefinir comportamento	Volta ao status Saudável automaticamente após um período de oito horas. O alerta permanece ativo para reter as informações sobre a ameaça não tratada.
Observações	Este monitor alterará o estado para Crítico quando for detectado malware e isso não for eliminado. O estado retornará automaticamente para Íntegro depois de 8 horas (isso porque não é possível determinar com precisão se o malware foi limpo/excluído ou não). É necessário intervenção do administrador para considerar as circunstâncias e encerrar o tíquete manualmente.
Estado	Saudável - Sem malware Crítico - Malware ativo
Ativado	Verdadeiro
Tarefa de recuperação	Não

Este monitor rastreia operações de limpeza de malware malsucedidas. Ele comunicará um estado Crítico se o cliente informar que não foi possível remover o malware.

Época de definições de antimalware

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Comando utilizado para obter dados de monitoramento: /opt/microsoft/scep/sbin/scep_daemon --status
Intervalo	A cada oito horas
Alerta	Sim. Resolução automática
Estado	Saudável - época maior ou igual a três dias Aviso - época maior que três dias E menor ou igual a cinco dias Crítico - época maior que cinco dias
Ativado	Verdadeiro
Tarefa de recuperação	Sim, manualmente (sem recuperação automática)

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

Mecanismo antimalware

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Monitora o arquivo de log de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Controlado por evento
Alerta	Sim. Resolução automática
Estado	Saudável - Ativado Desativado - Aviso
Ativado	Verdadeiro
Tarefa de recuperação	Sim, manualmente (sem recuperação automática)

É recomendável que a proteção antimalware esteja sempre ativada.
Observação: Este monitor controla o status da proteção antivírus, que é diferente da proteção em tempo real. Com o mecanismo antimalware desativado, um rastreamento sob demanda pode ser iniciado.

Serviço de antimalware

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Monitora o status do processo: scep_daemon
Intervalo	A cada 10 minutos
Alerta	Sim. Resolução automática
Estado	Saudável - Em execução Crítico - Não está em execução
Ativado	Verdadeiro
Tarefa de recuperação	Sim, manualmente (sem recuperação automática)

O monitor comunica um estado Crítico quando o serviço de antimalware (scep_daemon) da máquina cliente não está em execução, não está respondendo ou quando o mecanismo antimalware não está funcionando corretamente.

Época do último rastreamento

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Comando utilizado para obter dados de monitoramento: /opt/microsoft/scep/sbin/scep_daemon --status
Intervalo	A cada oito horas
Alerta	Não
Estado	Saudável - época maior ou igual a sete Aviso - época maior que sete
Ativado	Verdadeiro
Tarefa de recuperação	Sim, manualmente (sem recuperação automática)

Este monitor controla o tempo desde o último rastreamento do computador (independentemente do tipo de rastreamento). Recomendamos agendar um rastreamento para execução semanalmente.

Reinicialização pendente

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Monitora o arquivo de log de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Controlado por evento
Alerta	Sim. Resolução automática
Estado	Não - Saudável Sim - Aviso
Ativado	Verdadeiro
Tarefa de recuperação	Sim, manualmente (sem recuperação automática)

Este monitor controla a necessidade de reiniciar o sistema para que alterações de configuração entrem em vigor (geralmente quando a proteção em tempo real é ativada/desativada). O monitor aplica a seguinte chamada para uma atualização sob demanda deste status: /opt/microsoft/scep/sbin/scep_daemon --status.

Proteção em tempo real

Tipo de monitor	Monitor de unidade
Alvo	Servidor Linux protegido
Fonte de dados	Monitora o arquivo de log de texto: /var/log/scep/eventlog_scom.dat O monitor também pode usar a seguinte chamada para uma atualização de status sob demanda: /opt/microsoft/scep/sbin/scep_daemon --status.
Intervalo	controlado por evento
Alerta	Sim. Resolução automática
Estado	Ativado - Saudável Desativado - Aviso
Ativado	Verdadeiro
Tarefa de recuperação	Sim, manualmente (sem recuperação automática)

Monitora o status 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 a acumulação de integridade (pior estado) de todos os monitores de unidade de segurança Servidor Linux protegido do SCEP 7. Se o estado for "não inicializado", significa que o monitoramento não foi iniciado para este objeto ou que não há monitores de segurança definidos para ele.

Mecanismo antimalware

Tipo de monitor	Monitor de dependência

Alvo	Mecanismo antimalware
Alerta	Não
Ativado	Verdadeiro
Tarefa de recuperação	Não

Exibe o status do monitor de unidade Servidor Linux protegido/Mecanismo antimalware na lista de computadores monitorados.

Serviço de antimalware

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

Exibe o status do monitor de unidade Servidor Linux protegido/Serviço de antimalware na lista de computadores monitorados.

Definições de antimalware

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

Exibe o status do monitor de unidade Servidor Linux protegido/Época de definições de antimalware na lista de computadores monitorados.

Malware ativo

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

Exibe o status do monitor Servidor Linux protegido/Malware ativo no Gerenciador 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 Inacessível - Crítico
Ativado	Falso
Tarefa de recuperação	Não

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

Atividade de malware

Tipo de monitor	Monitor de unidade
Alvo	Atividade de antimalware
Fonte de dados	Monitora o arquivo de log de texto: /var/log/scep/eventlog_scom.dat
Intervalo	Controlado por evento
Alerta	Não
Estado	Sem malware - Saudável Atividade de malware detectada - Crítico
Ativado	Verdadeiro
Tarefa de recuperação	Não

Este monitor é alterado para o status Crítico cinco minutos após a detecção do malware (limpo ou não tratado) e permanece como Crítico durante os próximos 60 minutos. O status Crítico é atualizado a cada nova detecção positiva juntamente com a atualização

da duração do período de alerta. Em outras palavras, se nenhum malware for detectado no sistema durante um período de 60 minutos, o monitor retornará ao status 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 status para Crítico se não houver resposta do servidor dentro de 60 minutos após uma detecção de malware positiva (limpo ou não tratado). A alteração do status para Crítico também pode ser acionada se, após determinado período sem resposta do servidor, o malware for detectado logo após a renovação da conexão.

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

Exibe o status do monitor Atividade de antimalware/Aparecimento de malware de servidor.
Se mais de 5% de todos os computadores Linux (protegidos e não protegidos) registrarem uma detecção de malware ocorrida nos últimos 60 minutos, esse monitor será alterado para o status 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

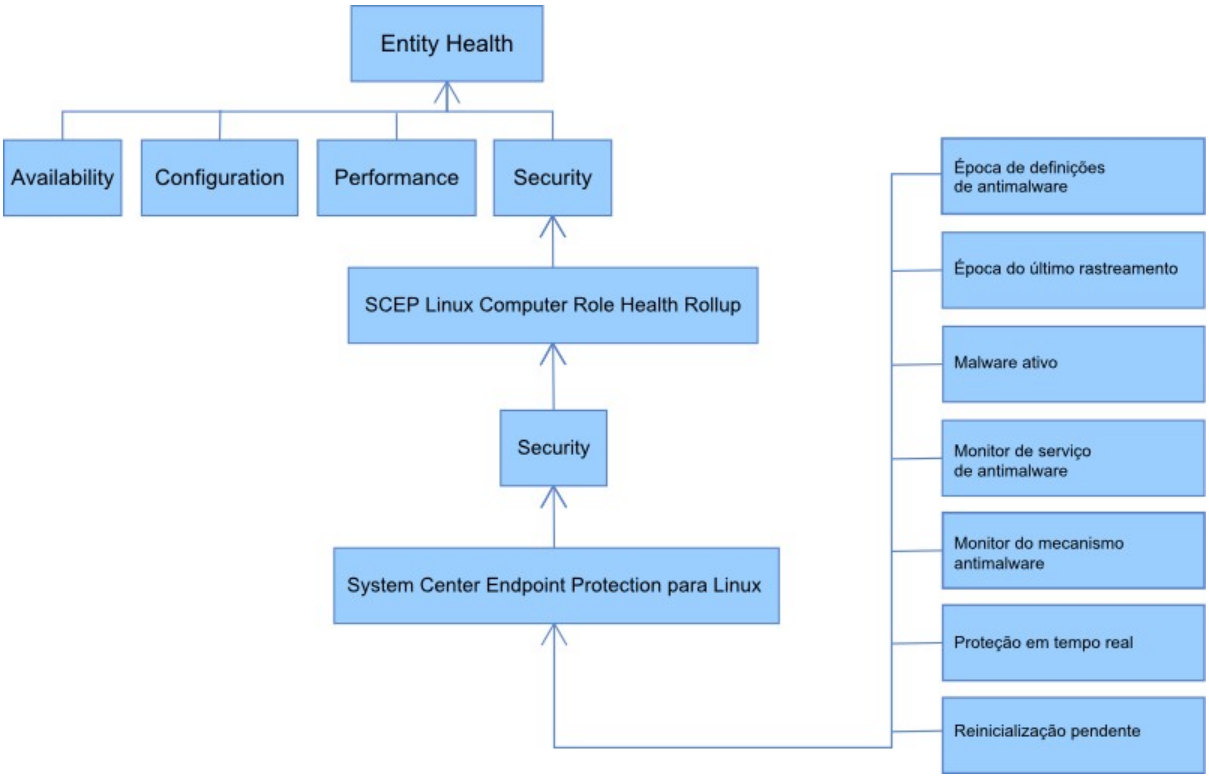
Propaga o status da entidade Computador Linux protegido para o monitor principal Computador Linux/Segurança.

Como a integridade é acumulada

Este pacote de gerenciamento expande o monitoramento do sistema operacional Linux como uma estrutura em camadas na qual cada camada depende da camada inferior para ser saudável. O topo dessa estrutura corresponde ao ambiente inteiro da Integridade da entidade, e o nível mais baixo dos ambientes de segurança são todos os monitores. Quando o status de uma das camadas é alterado, o status da camada acima também é alterado de maneira correspondente. Isso se chama acumulação de integridade.

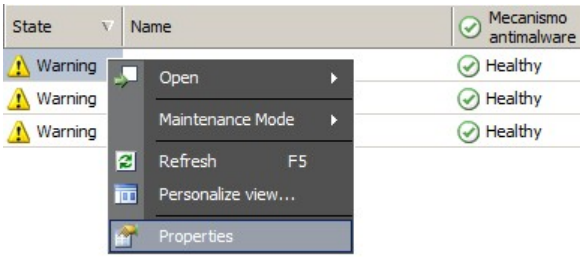
Por exemplo, se a proteção em tempo real retornar o status Aviso e todos os outros componentes tiverem o status Saudável, o status Aviso será transferido através da estrutura em árvore até chegar à raiz (Integridade da entidade), a qual também adquirirá o status Aviso.

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



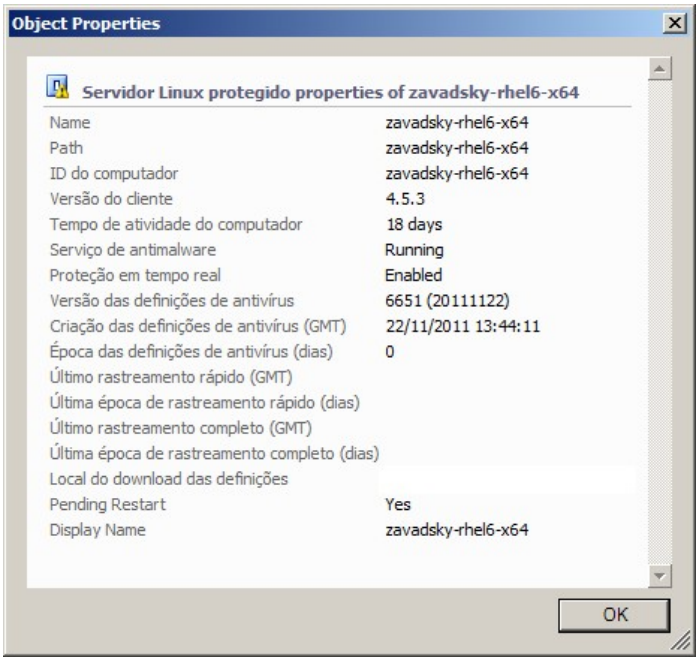
Propriedades do objeto

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



O objeto Servidor Linux protegido tem as seguintes propriedades:

- **ID do computador** - Identificador do servidor e nome do domínio.
- **Nome para exibição** - Nome do servidor e nome do domínio.
- **Versão do cliente** - Versão do produto SCEP instalada.
- **Tempo de atividade do computador** - O tempo de atividade do servidor (há quanto tempo uma máquina está ativa sem tempo de inatividade) não é um dado essencial para a devida operação de um pacote de gerenciamento, sua ausência, porém, indica um erro no pacote de gerenciamento.
- **Serviço de antimalware** - Status da proteção antimalware (Em execução/Não está em execução).
- **Proteção em tempo real** - Status da proteção em tempo real. Sua ausência sinaliza problemas no SCEP.
- **Definições de antivírus...** - Dados de status do banco de dados de vírus (versão, data de criação, época). A ausência de dados sinaliza problemas no SCEP.
- **Último rastreamento rápido/completo...** - Dados sobre o último rastreamento do computador. Se o rastreamento (Rápido/Completo) ainda não tiver sido executado, nenhum dado será exibido.
- **Local do download das definições** - Endereço/nome do servidor de atualização. As informações são exibidas após a primeira atualização bem-sucedida.
- **Reinicialização pendente** - Informações sobre a necessidade de reinicialização 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 severidade (gravidade) específica ocorreu em um objeto monitorado. Os alertas são definidos por regras. No console do Operations Manager, há uma exibição disponível em **Monitoring** > **Linux do System Center Endpoint Protection** > **Alertas ativos** que mostra os alertas que o usuário do console tem direito a ver para um objeto específico.

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

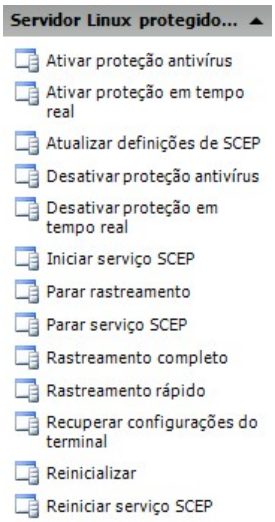
Alerta	Intervalo	Prioridade	Severidade	Descrição
Infecção por malware repetida	Controlado por evento	Alta	Crítico	O alerta é gerado em caso de detecções de malware repetidas (três ocorrências) em determinado intervalo de tempo (30 minutos). O alerta contém dados sobre o servidor e informações básicas sobre o malware.
Malware limpo	Controlado por evento	Baixa Média	Informações - Malware limpo com êxito Aviso - Interação do usuário necessária (por exemplo, reiniciar o servidor)	Alerta sobre um malware limpo com êxito. Contém todos os dados disponíveis sobre o malware específico. Cada malware detectado gera um alerta individual. O SCEP Linux atribui a prioridade e a severidade com base na eficiência do processos de limpeza, em que: Limpo = baixa + informações Limpo, mas uma ação é necessária (por exemplo, reinicialização) = média + aviso.
Malware Ativo (do Monitor)	Controlado por evento	Alta	Crítico	Alerta sobre um malware que não foi limpo. Contém todos os dados disponíveis sobre o malware específico.
Malware Ativo (da Regra)	Controlado por evento	Alto/Médio/ Baixo	Crítico/Médio/Baixo – baseado num tipo de Malware	O mesmo que acima. Usado para conectores para outros sistemas de monitorização/emissão de passagens. **Observação:** Essa regra (alerta) está desativada por padrão.
O serviço de antimalware do System Center Endpoint Protection não funciona	300 segundos	Média	Crítico	Alerta sobre indisponibilidade do SCEP do serviço de antimalware (scep_daemon). Inclui o respectivo 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 respectivo nome do servidor.
Proteção em tempo real desativada	Controlado por evento	Média	Aviso	Alerta sobre a desativação da proteção em tempo real. Inclui o respectivo nome do servidor.
Definições desatualizadas	A cada oito horas	Média	Aviso (época menor ou igual a cinco dias) E época maior que três dias) Crítico (época maior que cinco dias)	Alerta sobre o fato de que o banco de dados de assinatura de vírus não é atualizado há mais de três dias. Inclui o respectivo nome de servidor e a época do banco de dados de assinatura de vírus.
Aparecimento de malware	Controlado por evento	Alta	Crítico	O Forefront Endpoint Protection detectou mais de 5% de malware ativo nos computadores. É possível que o malware esteja se espalhando pelos computadores. É recomendável verificar se todos os servidores têm as definições mais atualizadas. Se for necessário alterar o número de ameaças ativas que geram esse alerta, substitua o parâmetro do monitor Aparecimento de malware (consulte o capítulo Substituições).

Tarefas

O pacote de gerenciamento do SCEP implementa 13 tarefas. A execução dessas tarefas é imediata. As saídas são exibidas imediatamente após a execução das tarefas ou podem ser visualizadas posteriormente, na janela Status 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 do Console de Operações.



- **Desativar proteção antivírus** - Desativa todos os componentes da proteção antivírus e desativa o rastreamento sob demanda.
- **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.
- **Rastreamento completo** - Atualiza o banco de dados de assinatura de vírus e executa um rastreamento completo do computador.
- **Rastreamento rápido** - Atualiza o banco de dados de assinatura de vírus e executa um rastreamento rápido do computador.
- **Parar rastreamento** - Interrompe todos os rastreamentos do computador em execução.
- **Recuperar configurações do servidor** - Exibe o status atual do produto SCEP. A lista de parâmetros exibida é idêntica às propriedades da entidade Servidor Linux protegido. Os dados exibidos não são transferidos para Servidor Linux protegido.
- **Reiniciar serviço Antimalware** - Reinicia o serviço de antimalware do SCEP (scep_daemon).
- **Parar serviço Antimalware** - Interrompe 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 do banco de dados de assinatura de vírus.
- **Reinicializar** - Reinicia o computador Linux.

Configurando o pacote de gerenciamento do SCEP

Prática recomendada: criar um pacote de gerenciamento para personalizações

Por padrão, o Operations Manager salva todas as personalizações (por exemplo, substituições) no pacote de gerenciamento padrão. Como prática recomendada, em vez disso, você deve criar um pacote de gerenciamento separado para cada pacote de gerenciamento lacrado que deseja personalizar.

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

A criação de um novo pacote de gerenciamento para armazenar personalizações de cada pacote de gerenciamento lacrado facilita a exportação de personalizações de um ambiente de teste para um ambiente de produção. Além disso, facilita também a exclusão de um pacote de gerenciamento, pois é necessário excluir todas as dependências para que seja possível excluir o pacote em si. Se as personalizações de todos os pacotes de gerenciamento forem salvas no pacote de gerenciamento padrão e for necessário excluir um único pacote de gerenciamento, primeiro será necessário excluir o pacote de gerenciamento padrão, o que também excluirá personalizações de outros pacotes.

Configuração de segurança

O computador deve executar o serviço SSHD, e a porta SSH (valor padrão 22) deve estar aberta. O System Center 2012 Operations Manager conecta-se através da porta aos computadores Linux remotos usando o tipo Run As Account apropriado (localizado no painel **Administration** > **Run As Configuration** do console de monitoramento do Operations Manager) com o tipo **Basic Authentication**.

Nome do perfil Executar como	Observações
Unix Privileged Account	Usada para monitoramento remoto do servidor Unix, bem como para reiniciar processos quando direitos privilegiados são necessários.

Este pacote de gerenciamento não usa a Unix Action Account.

Aviso: Monitorar os computadores usando a conta raiz gera um possível risco de segurança, por exemplo, se a senha for descoberta.

Caso não pretenda usar a conta raiz para monitorar e gerir, você pode usar uma conta de usuário padrão, mas esta conta necessita ter direitos para executar os comandos *sudo*. Por isso, a seguinte configuração tem de estar presente no arquivo /etc/sudoers em cada estação de trabalho monitorada SCEP Linux para autorizar a elevação sudo para a conta de usuário selecionada. Isso é um exemplo de configuração para o nome de usuário 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
#--------------------------------------------------------------------------------
```

Ajustando as regras de limite de desempenho

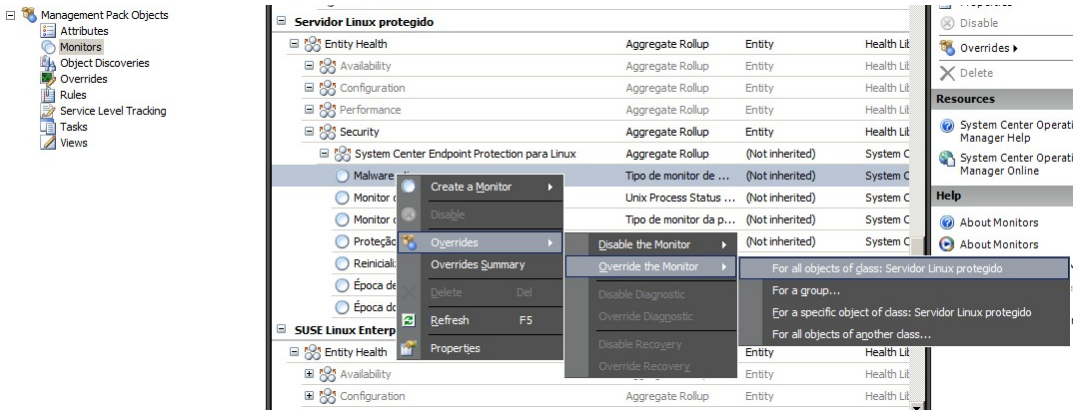
A tabela a seguir lista as regras de limite de desempenho que apresentam limites padrão que podem exigir ajuste adicional para atender às necessidades de seu ambiente. Avalie essas regras para determinar se os limites padrão são adequados para seu ambiente. Se um limite padrão não for adequado para o ambiente, você pode ajustá-lo aplicando uma substituição a ele.

Nome da regra	Parâmetro de substituição	Limite padrão	Limitações de ajuste
Regra da infecção por malware repetida	Limite de contagem de infecção repetida	3 ocorrências	Configurar um valor menor que 2 torna a regra obsoleta.
Regra da infecção por malware repetida	Janela de tempo de infecção repetida	30 minutos	Não é recomendável definir um valor inferior à duração de um rastreamento sob demanda, pois uma sobreposição pode impedir que um alerta seja gerado.
Regra de Alerta de Malware Ativo	Ativado	Falso	Caso use conectores para outros sistemas de monitorização/emissão de passagens, pode ativar este alerta.

Substituições

As substituições podem ser usadas para refinar as configurações de um objeto de monitoramento no System Center 2012 Operations Manager. Isso inclui monitores, regras, descobertas de objetos e atributos provenientes de pacotes de gerenciamento importados.

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



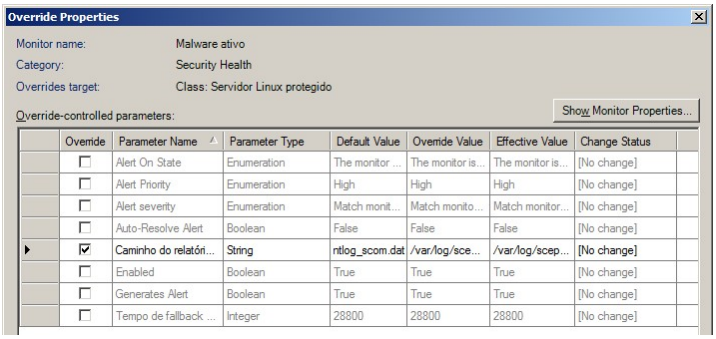
Use a janela Substituições para criar ou modificar uma substituição para uma ocorrência de qualquer um dos seguintes parâmetros:

- **Tempo de fallback de monitor de malware ativo** (relacionado somente ao monitor Malware ativo)
- **Época de definições de antimalware** (relacionado somente ao monitor Época de definições de antimalware)
- **Intervalo de detecção** (relacionado somente ao monitor Época do último rastreamento)
- **Estado de Alerta Ativo**
- **Prioridade do Alerta**
- **Severidade 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 padrão não for adequada para seu ambiente, você pode ajustar os limites aplicando uma substituição a eles:

Parâmetro de substituição	Nome do monitor	Valor padrão	Observações de ajuste

Intervalo ping	Ping de máquina	3600 segundos	Intervalo para verificar a disponibilidade do Servidor Linux protegido. Uma duração menor aciona um status 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 monitorado 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 status 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. Se, durante o intervalo da Janela de tempo do aparecimento de malware, um número de computadores maior que o valor percentual definido para Aparecimento de malware (consulte Aparecimento de malware) registrar atividade de malware, um alerta Aparecimento de malware será gerado. Observação: 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 detecção 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 arquivo em que os eventos do System Center 2012 Operations Manager são gravados. Só altere esse parâmetro em caso de problemas.
Época crítica de definições de antimalware	Época de definições de antimalware	5 dias	Após este intervalo, é gerado um alerta Erro notificando 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 elas são 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 das 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 em operação.
Intervalo de detecção	Época do último rastreamento	28800 segundos	Intervalo de verificação do último rastreamento executado.
Época máxima do rastreamento	Época do último rastreamento	7 dias	Deve ser configurado de acordo com as configurações do produto SCEP. Se um rastreamento estiver agendado para cada sete dias, defina este valor para sete dias.
Caminho do relatório	Reinicialização pendente	/var/log/scep/ eventlog_scom.log	Caminho para o arquivo em que os eventos do System Center 2012 Operations Manager são gravados. Só altere esse parâmetro em caso de problemas.
Caminho do relatório SCEP	Proteção em tempo real	/var/log/scep/ eventlog_scom.log	Caminho para o arquivo em que os eventos do System Center 2012 Operations Manager são gravados. Só altere esse parâmetro em caso de problemas.
Porcentagem	Aparecimento de malware	95%	Porcentagem dos Servidores Linux (protegidos e não protegidos) necessária para que o status Saudável seja retornado e o grupo monitorado inteiro seja considerado Saudável. Se for detectado malware em 5% ou mais do total, um Aparecimento de malware será gerado.



Observação: Para obter mais informações sobre Substituições, consulte o tópico Como monitorar utilizando substituições (http://go.microsoft.com/fwlink/?LinkID=117777).

Links

Os seguintes links trazem informações sobre tarefas comuns associadas a este pacote de gerenciamento:

- Administrando o ciclo de vida do pacote de gerenciamento (http://go.microsoft.com/fwlink/?LinkId=211463)
- Como importar um Pacote de Gerenciamento no Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=142351)
- Como monitorar 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)
- Configurando 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 de Pacotes de Gerenciamento (http://go.microsoft.com/fwlink/?LinkId=209940)
- Como remover um pacote de gerenciamento (http://go.microsoft.com/fwlink/?LinkId=209941)
- Como gerenciar dados de monitoramento usando Escopo, Pesquisar e Localizar no Essentials (http://go.microsoft.com/fwlink/?LinkId=91983)
- Monitorando o Linux usando o SCOM 2007 R2 (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Instalando agentes entre plataformas manualmente (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- Configurando Elevação sudo para UNIX e Monitorando Linux com 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 gerenciamento, consulte o fórum da comunidade do System Center Operations Manager (http://go.microsoft.com/fwlink/?LinkID=179635).
Um recurso útil é o blog System Center Operations Manager Unleashed (http://opsmgrunleashed.wordpress.com/), que contém postagens com exemplos sobre pacotes de monitoramento específicos.

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

- Blog da equipe do Operations Manager (http://blogs.technet.com/momteam/default.aspx)
- Blog de Kevin Holman sobre o Operations Manager (http://blogs.technet.com/kevinholman/default.aspx)
- Blog Thoughts on OpsMgr (http://thoughtsonopsmgr.blogspot.com/)
- Blog de Raphael Burri (http://rburri.wordpress.com/)
- Blog de BWren sobre gerenciamento de espaço (http://blogs.technet.com/brianwren/default.aspx)
- Blog da equipe de suporte do System Center Operations Manager (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++ (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Observações sobre o System Center Operations Manager

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

Para obter solução de problemas, visite estes segmentos do fórum:

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