IBM Security QRadar
Versão 7.2.5

# *Guia de Configuração de Avaliação de Vulnerabilidade*

**Nota**

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 99.

**Informações do produto**

Este documento se aplica ao IBM QRadar Security Intelligence Platform V7.2.4 e às liberações subsequentes, a menos que seja substituído por uma versão atualizada deste documento.

**© Copyright IBM Corporation 2007, 2015.**

# Índice



© Copyright IBM Corp. 2007, 2015

# Introdução às configurações de avaliação de vulnerabilidade do QRadar

A integração com scanners de avaliação de vulnerabilidade fornece aos administradores e profissionais de segurança informações para construir perfis de avaliação de vulnerabilidade para ativos de rede.

## Público-alvo

Os administradores devem ter acesso ao QRadar e um conhecimento das tecnologias de rede corporativa.

## Documentação técnica

Para obter informações sobre como acessar uma documentação mais técnica, notas técnicas e notas sobre a liberação, consulte Acessando a Nota Técnica de Documentação do IBM® Security (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

## Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte a Nota Técnica de Suporte e Download (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

## Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que envolverá necessariamente procedimentos operacionais adicionais e podem requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

© Copyright IBM Corp. 2007, 2015

# Capítulo 1. Visão geral do scanner avaliação da vulnerabilidade

Integrar os scanners de avaliação de vulnerabilidade com IBM Security QRadar para fornecer perfis de avaliação de vulnerabilidade para os recursos de rede.

As referências ao QRadar se aplicam a todos os produtos capazes de coletar informações de avaliação de vulnerabilidades.

Os perfis de ativos para os servidores e hosts em sua rede fornecem informações que podem ajudá-lo a resolver problemas de segurança. Usando perfis de ativos, é possível conectar ofensas que ocorrem em seu sistema aos ativos virtuais ou físicos como parte da investigação de segurança. Os dados de Ativos são úteis para identificar ameaças, identificar vulnerabilidades, serviços, portas e monitorar o uso de ativo em sua rede.

A guia **Ativos** fornece uma visualização unificada das informações conhecidas sobre os ativos. Conforme mais informações são fornecidas ao sistema por meio da avaliação de vulnerabilidade, o sistema atualiza o perfil do ativo. Os perfis de avaliação de vulnerabilidade usam dados de eventos correlacionados, atividade de rede e mudanças comportamentais para determinar o nível de ameaças e as vulnerabilidades presentes nos ativos de negócios críticos em sua rede. É possível planejar varreduras e assegurar que as informações de vulnerabilidade sejam relevantes para os ativos na rede.

## Instalando o Java Cryptography Extension irrestrito

O Java™ Cryptography Extension (JCE) é uma estrutura Java que é necessária para decriptografar algoritmos de criptografia avançados para traps AES de 192 bits ou SNMPv3 de 256 bits.

### Antes de Iniciar

Cada host gerenciado que recebe traps de alto nível SNMPv3 necessitam de JCE irrestrito. Se necessitar de algoritmos de criptografia avançados para comunicação SNMP, você deve atualizar a extensão de criptografia existente em seu host gerenciado com um JCE irrestrito.

### Procedimento

1. Utilizando o SSH, efetue login no QRadar Console.
2. Para verificar a versão do Java no Console, digite o comando a seguir: `java -version`.

   O arquivo JCE deve corresponder à versão do Java instalado no Console.
3. Faça download da versão mais recente do Java Cryptography Extension no website da IBM.

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk
4. Use o Secure Copy (SCP) para copiar os arquivos `local.policy.jar` e `US_export_policy.jar` para o seguinte diretório do Console: `/opt/ibm/java-[version]/jre/lib/security/`.

© Copyright IBM Corp. 2007, 2015

5. Opcional. Implementações distribuídas requerem que os administradores copiem os arquivos `local.policy.jar` e `US_export_policy.jar` do dispositivo do Console para o host gerenciado.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 2. Scanner AXIS

É possível importar dados de vulnerabilidade de qualquer scanner que emitir dados no formato Asset Export Information Source (AXIS). Axis é um formato de dados XML criado especificamente para compatibilidade de ativo e de vulnerabilidade com produtos IBM Security QRadar.

AXIS é um formato padrão para importações de resultado de varredura de dados de vulnerabilidade. Os dados de vulnerabilidade para scanners Axis devem estar em conformidade com o esquema de formato AXIS para que sejam importados com sucesso. Para integrar com sucesso um scanner AXIS ao QRadar, arquivos de resultados XML devem estar disponíveis em um *servidor remoto* ou em um scanner que suporte a comunicação SFTP ou SMB Share. Um servidor remoto é um sistema ou dispositivo de terceiro que pode hospedar os resultados da varredura XML.

## Incluindo uma varredura de vulnerabilidade AXIS

Inclua uma configuração do scanner AXIS para coletar relatórios específicos ou iniciar varreduras no scanner remoto.

### Sobre Esta Tarefa

A tabela a seguir descreve os parâmetros do scanner AXIS quando SFTP é selecionado como o método de importação:

*Tabela 1. Scanner AXIS - Propriedades de SFTP*

| Parâmetro | Descrição |
|---|---|
| Nome do Host Remoto | O endereço IP ou o nome do host do servidor que tem os arquivos de resultados da varredura. |
| Nome do usuário de login | O nome de usuário usado pelo QRadar para efetuar login no servidor. |
| Ativar autenticação de chave | Especifica que o QRadar é autenticado com um arquivo de autenticação baseada em chave. |
| Diretório remoto | A localização dos arquivos de resultados da varredura. |
| Arquivo de chave privado | O caminho completo para o arquivo que contém a chave privada. Se um arquivo-chave não existir, você deverá criar o arquivo `vis.ssh.key`. |
| Padrão de nome do arquivo | A expressão regular (regex) necessária para filtrar a lista de arquivos que estão no *Diretório remoto*. O padrão `.*\.xml` importa todos os arquivos XML do diretório remoto. |

A tabela a seguir descreve os parâmetros do scanner AXIS quando *SMB Share* é selecionado como o método de importação:

© Copyright IBM Corp. 2007, 2015

*Tabela 2. Scanner AXIS - Propriedades de SMB Share*

| Parâmetro | Descrição |
|---|---|
| Nome do host | O endereço IP ou o nome do host do SMB Share. |
| Nome do usuário de login | O nome de usuário usado pelo QRadar para efetuar login no SMB Share. |
| Domínio | O domínio usado para se conectar ao SMB Share. |
| Caminho de pasta do SMB | O caminho completo para o compartilhamento a partir da raiz do host SMB. Use barras, por exemplo, `/share/logs/`. |
| Padrão de nome do arquivo | A expressão regular (regex) necessária para filtrar a lista de arquivos no Diretório remoto. O padrão `.*\.xml` importa todos os arquivos xml no diretório remoto. |

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o scanner AXIS.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Axis Scanner**.
7. Na lista **Método de importação**, selecione **SFTP** ou **SMB Share**.
8. Configure os parâmetros.
9. Configure um intervalo do CIDR para o scanner.
10. Clique em **Salvar**.
11. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Para obter mais informações sobre como criar um planejamento de varredura, consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 3. Visão geral do scanner Beyond Security Automatic Vulnerability Detection System

A avaliação de vulnerabilidade é a avaliação dos ativos na rede para identificar e priorizar problemas de segurança em potencial. Os produtos do QRadar que suportam Avaliação de Vulnerabilidade podem importar dados de vulnerabilidade de produtos de scanner externos para identificar perfis de vulnerabilidades para ativos.

Os perfis de avaliação de vulnerabilidade usam dados de eventos correlacionados, atividade de rede e mudanças comportamentais para determinar o nível de ameaças e as vulnerabilidades presentes nos ativos de negócios críticos em sua rede. Conforme os scanners externos varrem os dados, o QRadar pode recuperar os dados de vulnerabilidade com um planejamento de varredura.

Para configurar o scanner Beyond Security AVDS, consulte “Incluindo um scanner de vulnerabilidade Beyond Security AVDS”.

## Incluindo um scanner de vulnerabilidade Beyond Security AVDS

Os dispositivos Beyond Security Automated Vulnerability Detection System (AVDS) criam dados de vulnerabilidade no formato Asset Export Information Source (AXIS). Arquivos no formato AXIS podem ser importados por arquivos XML que puderem ser importados.

### Sobre Esta Tarefa

Para integrar com êxito as vulnerabilidades do Beyond Security AVDS com o QRadar, você deve configurar o aplicativo de Beyond Security AVDS para publicar os dados de vulnerabilidade para um AXIS formatado pelo arquivo de resultados XML. Os dados de vulnerabilidade XML devem ser publicados em um servidor remoto que esteja acessível usando o Secure File Transfer Protocol (SFTP). O termo de servidor remoto refere-se a qualquer dispositivo, host de terceiros ou local de armazenamento de rede que possam hospedar os arquivos de resultados da varredura de XML publicados.

Os resultados de XML mais recentes que contêm as vulnerabilidades de Beyond Security AVDS são importados quando um planejamento de varredura é iniciado. Os planejamentos de varredura determinam a frequência com que os dados de vulnerabilidade criados pelo Beyond Security AVDS são importados. Após incluir seu dispositivo de Beyond Security AVDS para QRadar, crie um planejamento de varredura para importar os arquivos de resultado da varredura. As vulnerabilidades a partir do planejamento de varredura atualizam a guia **Ativos** após o planejamento da varredura ser concluído.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Beyond Security AVDS.

© Copyright IBM Corp. 2007, 2015

5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **Beyond Security AVDS**.
7. No campo **Nome do host remoto**, digite o endereço IP ou o nome do host do sistema que contém os resultados da varredura publicados a partir do seu scanner Beyond Security AVDS.
8. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
|---|---|
| **Nome do usuário de login** | Para autenticar com um nome de usuário e senha:<br>1. No campo **Nome de usuário de login**, digite um nome de usuário que possua acesso para recuperar os resultados da varredura do host remoto.<br>2. No campo **Senha de Login**, digite a senha que está associada ao nome de usuário. |
| **Ativar autorização de chave** | Para autenticar com um arquivo de autenticação baseado em chave:<br>1. Marque a caixa de seleção **Ativar autenticação de chave**.<br>2. No campo **Arquivo-chave privado**, digite o caminho do diretório para o arquivo-chave.<br>O diretório padrão para o arquivo-chave é `/opt/qradar/conf/vis.ssh.key`.<br>Se um arquivo-chave não existir, você deverá criar o arquivo vis.ssh.key. |

9. No campo **Diretório remoto**, digite o local do diretório dos arquivos de resultados da varredura.
10. No campo **Padrão de Nome do Arquivo**, digite uma expressão regular (regex) para filtrar a lista de arquivos especificados no Diretório Remoto. Todos os arquivos correspondentes são incluídos no processamento.

    O valor padrão é `.*\.xml`. O padrão `.*\.xml` importa todos os arquivos xml no diretório remoto.
11. No campo **Idade máxima dos relatórios (Dias)**, digite a idade máxima de arquivo para seu arquivo de resultados da varredura. Os arquivos que forem mais antigos do que a quantia de dias e o registro de data e hora especificados no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. O valor padrão é 7 dias.
12. Para configurar a opção **Ignorar duplicatas**:
    - Selecione essa caixa de seleção para controlar os arquivos que já foram processados por um planejamento de varredura. Esta opção evita que um arquivo de resultados de varredura seja processado uma segunda vez.
    - Desmarque essa caixa de seleção para importar os resultados de varredura de vulnerabilidade sempre que o planejamento de varredura for iniciado. Essa opção pode fazer com que diversas vulnerabilidades sejam associadas a um ativo.

Se um arquivo de resultado não for varrido dentro de 10 dias, o arquivo será removido da lista de rastreamento e será processado na próxima vez em que o planejamento de varredura for iniciado.

13. Para configurar um intervalo do CIDR para seu scanner:
    a. Digite a faixa de CIDR para a varredura ou clique em **Pesquisar** para selecionar uma faixa de CIDRna lista de redes.
    b. Clique em **Incluir**.
14. Clique em **Salvar**.
15. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 4. Scanners Digital Defense Inc AVS

É possível incluir um scanner Digital Defense Inc AVS em sua implementação do IBM Security QRadar.

## Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

## Sobre Esta Tarefa

Em intervalos em que são determinados por um planejamento de varredura, o QRadar importa os resultados XML mais recentes que contêm as vulnerabilidades do Digital Defense Inc AVS. Para ativar a comunicação com o scanner Digital Defense Inc AVS, o QRadar utiliza as credenciais que você especificar na configuração do scanner.

A lista a seguir fornece mais informações sobre os parâmetros do scanner Digital Defense Inc AVS:

**Nome do Host Remoto**
O nome do host do servidor remoto que hospeda o scanner Digital Defense Inc AVS.

**Porta Remota**
O número da porta do servidor remoto que hospeda o scanner Digital Defense Inc AVS.

**URL Remota**
A URL do servidor remoto que hospeda o scanner Digital Defense Inc AVS.

**ID do cliente**
O ID do cliente principal usado para se conectar ao scanner Digital Defense Inc AVS.

**Escopo do host**
Quando configurado como Interno, recupera a visualização ativa dos hosts internos do scanner Digital Defense Inc AVS. Quando configurado como Externo, recupera a visualização ativa externa do scanner Digital Defense Inc AVS.

**Recuperar Dados da Conta**
A opção **Padrão** indica que os dados são incluídos apenas do **ID do Cliente** especificado. Se desejar incluir dados do ID do Cliente e todas as suas subcontas, selecione **Todas as Subcontas**. Se desejar especificar um único ID do cliente alternativo, selecione **ID do Cliente Alternativo**.

© Copyright IBM Corp. 2007, 2015

**Método de Correlação**

Especifica o método pelo qual as vulnerabilidades são correlacionadas.

- A opção **Tudo Disponível** consulta o catálogo vulnerabilidade do Digital Defense Inc e tenta correlacionar as vulnerabilidades baseadas em todas as referências que forem retornadas para essa vulnerabilidade específica. As referências podem incluir CVE, Bugtraq, Microsoft Security Bulletin e OSVDB. Diversas referências geralmente são correlacionadas à mesma vulnerabilidade, porém retorna mais resultados e demora mais tempo para processar do que a opção **CVE**.
- A opção **CVE** correlaciona as vulnerabilidades que se basearem apenas no CVE-ID.

## Procedimento

1. Clique na guia **Administrador**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Clique no ícone **Scanners de VA**.
4. Clique em **Incluir**.
5. Na caixa de listagem **Tipo**, selecione **Digital Defense Inc AVS**.
6. Configure os parâmetros.
7. Para configurar os intervalos do CIDR que você deseja que o scanner considere, digite o intervalo do CIDR ou clique em **Procurar** para selecionar o intervalo do CIDR na lista de rede.
8. Clique em **Incluir**.
9. Clique em **Salvar**.
10. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Após incluir o scanner Digital Defense Inc AVS, será possível incluir um planejamento de varredura para recuperar as informações de vulnerabilidade.

# Capítulo 5. Visão geral do scanner eEye

O QRadar pode coletar dados de vulnerabilidade a partir dos scanners eEye REM Security Management Console ou eEye Retina CS.

As seguintes opções de protocolo estão disponíveis para coletar informações de vulnerabilidade a partir de scanners eEye:

- Inclua um scanner eEye do protocolo SNMP. Consulte "Incluindo uma varredura do eEye REM SNMP".
- Inclua um scanner eEye do protocolo JDBC. Consulte "Incluindo uma varredura eEye REM JDBC" na página 13

**Tarefas relacionadas**:

"Instalando o Java Cryptography Extension irrestrito" na página 1
O Java Cryptography Extension (JCE) é uma estrutura Java que é necessária para decriptografar algoritmos de criptografia avançados para traps AES de 192 bits ou SNMPv3 de 256 bits.

## Incluindo uma varredura do eEye REM SNMP

É possível incluir um scanner para coletar dados de vulnerabilidade por meio de SNMP dos scanners eEye REM ou CS Retina.

### Antes de Iniciar

Para utilizar os identificadores e descrições de CVE, você deverá copiar o arquivo `audits.xml` de seu scanner eEye REM para o host gerenciado responsável por receber os dados SNMP. Se o seu host gerenciado estiver em uma implementação distribuída, você deverá copiar o arquivo `audits.xml` primeiro para o Console e depois enviar o arquivo por meio do SSH para `/opt/qradar/conf/audits.xml` no host gerenciado. O local padrão do arquivo `audits.xml` no scanner eEye é `%ProgramFiles(x86)%\eEye Digital Security\Retina CS\Applications\RetinaManager\Database\audits.xml`.

Para receber as informações de CVE mais atualizadas, atualize periodicamente o QRadar com os arquivos de `audits.xml` mais recentes.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu servidor SecureScout.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **eEye REM Scanner**.
7. Na lista **Tipo de Importação**, selecione **SNMP**.
8. No campo **Diretório base**, digite um local para armazenar os arquivos temporários que contêm os dados de varredura do eEye REM. O diretório padrão é `/store/tmp/vis/eEye/`.

© Copyright IBM Corp. 2007, 2015

9. No campo **Tamanho do cache**, digite o número de transações que você deseja armazenar no cache antes que os dados SNMP sejam gravados no arquivo temporário. O padrão é 40. O valor padrão é de 40 transações.
10. No campo **Período de retenção**, digite o período de tempo, em dias, em que o sistema armazena as informações de varredura. Se um planejamento de varredura não importar dados antes que o período de retenção expire, as informações de varredura do cache serão excluídas.
11. Marque a caixa de seleção **Utilizar dados de vulnerabilidade** para correlacionar as vulnerabilidades do eEye com os identificadores Common Vulnerabilities and Exposures (CVE) e informações de descrição. .
12. No campo **Arquivos de dados de vulnerabilidade**, digite o caminho do diretório para o arquivo `audits.xml` eEye.
13. No campo **Porta de atendimento**, digite o número da porta que é utilizada para monitorar as informações de vulnerabilidade do SNMP recebidas a partir do seu scanner eEye REM. A porta padrão é 1162.
14. No campo **Host de origem**, digite o endereço IP do scanner eEye.
15. Na lista **Versão do SNMP**, selecione a versão de protocolo SNMP. O protocolo padrão é SNMPv2.
16. No campo **Sequência de Comunidades**, digite a sequência de comunidade SNMP para o protoloco SNMPv2, por exemplo,`Público`.
17. Na lista **Protocolos de autenticação**, selecione o algoritmo para autenticar os traps SNMPv3.
18. No campo **Senha de autenticação**, digite a senha que deseja usar para autenticar a comunicação SNMPv3. A senha deve incluir um mínimo de 8 caracteres.
19. Na lista **Protocolos de criptografia**, selecione o algoritmo de decriptografia SNMPv3.
20. No campo **Senha de Criptografia**, digite a senha para decriptografar os traps SNMPv3.
21. Para configurar um intervalo do CIDR para seu scanner:
    a. Digite a faixa de CIDR para a varredura ou clique em **Pesquisar** para selecionar uma faixa de CIDRna lista de redes.
    b. Clique em **Incluir**.
22. Clique em **Salvar**.
23. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Selecione uma das opções a seguir:

- Se você não utilizar o SNMPv3 ou utilizar uma criptografia SNMP de baixo nível, agora você estará pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.
- Se a sua configuração do SNMPv3 usar a criptografia AES192 ou AES256, você deverá instalar a extensão de criptografia Java irrestrita em cada Console ou host gerenciado que recebe os traps SNMPv3. Consulte “Instalando o Java Cryptography Extension irrestrito” na página 1.

## Incluindo uma varredura eEye REM JDBC

É possível incluir um scanner para coletar dados de vulnerabilidade por meio de JDBC dos scanners eEye REM ou CS Retina.

### Antes de Iniciar

Antes de configurar o QRadar para pesquisar dados de vulnerabilidade, é recomendado criar uma conta e senha de usuário do banco de dados para o QRadar. Se você designar a permissão somente leitura da conta do usuário para o RetinaCSDatabase, será possível restringir o acesso ao banco de dados que contém as vulnerabilidades do eEye. O protocolo JDBC permite que o QRadar efetue login e pesquise eventos no banco de dados MSDE. Assegure-se de que nenhuma regra de firewall bloqueie a comunicação entre o scanner eEye e o Console ou host gerenciado responsável pela pesquisa com o protocolo JDBC. Se utilizar instâncias do banco de dados, você deverá verificar se a porta 1433 está disponível para o SQL Server Browser Service para resolver o nome da instância.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o scanner eEye.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir da implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **eEye REM Scanner**.
7. Na lista **Tipo de importação**, selecione **JDBC**.
8. No campo **Nome do host**, digite o endereço IP ou o nome do host do banco de dados eEye.
9. No campo **Porta**, digite 1433.
10. Opcional. No campo **Instância de banco de dados**, digite a instância de banco de dados para o banco de dados eEye.

    Se uma instância do banco de dados não for utilizada, deixe esse campo em branco.
11. No campo **Nome de usuário**, digite o nome de usuário necessário para consultar o banco de dados eEye.
12. No campo **Senha**, digite a senha necessária para consultar o banco de dados eEye.
13. No campo **Domínio**, digite o domínio obrigatório, se necessário, para se conectar ao banco de dados eEye.

    Se o banco de dados for configurado para Windows e estiver dentro de um domínio, o nome de domínio deverá ser especificado.
14. No campo **Nome do banco de dados**, digite `RetinaCSDatabase` como o nome do banco de dados.
15. Marque a caixa de seleção **Utilizar comunicação de canal nomeado**, se canais nomeados forem necessários para comunicação com o banco de dados eEye. Por padrão, essa caixa de seleção fica desmarcada.
16. Marque a caixa de seleção **Utilizar NTLMv2** se o scanner eEye utilizar NTLMv2 como um protocolo de autenticação. Por padrão, essa caixa de seleção fica desmarcada.

A caixa de seleção Usar NTLMv2 força as conexões MSDE a usarem o protocolo NTLMv2 ao se comunicar com servidores SQL que requerem autenticação NTLMv2. A caixa de seleção Usar NTLMv2 é selecionada e não tem nenhum efeito sobre as conexões MSDE com servidores SQL que não requererem autenticação NTLMv2.

17. Para configurar um intervalo do CIDR para o scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
18. Clique em **Salvar**.
19. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 6. Visão geral do scanner Foundstone FoundScan

O scanner Foundstone FoundScan consulta o FoundScan Engine para obter informações sobre o host e vulnerabilidade do FoundScan OpenAPI.

O QRadar suporta o Foundstone FoundScan versões 5.0 a 6.5.

O dispositivo FoundScan deve incluir uma configuração de varredura que é executada regularmente para manter os resultados do host e de vulnerabilidade atualizados. Para assegurar que o scanner FoundScan seja capaz de recuperar informações de varredura, assegure-se de que o sistema de FoundScan atenda aos requisitos a seguir:

- O aplicativo FoundScan deve estar ativo. Como a API fornece acesso ao aplicativo FoundScan, os administradores podem verificar se o aplicativo FoundScan é executado continuamente no servidor FoundScan.
- Os dados de varredura a serem importados devem ser completos e visíveis na interface com o usuário FoundScan para recuperar os resultados da varredura. Se a varredura for planejada para ser removida após a conclusão, os resultados deverão ser importados pelo planejamento de varredura antes de a varredura ser removida do FoundScan.
- Os privilégios de usuário apropriados devem ser configurados no aplicativo FoundScan para permitir comunicação entre o QRadar e o FoundScan. O FoundScan OpenAPI fornece informações do host e de vulnerabilidade. Todas as vulnerabilidades de um host designado são designadas para a porta 0.

Para se conectar ao FoundScan, o FoundScan Engine requer autenticação com certificados do lado do cliente. O FoundScan inclui uma autoridade de certificação padrão e os certificados de cliente que são os mesmos para todas as instalações do scanner. O plug-in do FoundScan também inclui certificados para utilização com o FoundScan 5.0. Se o FoundScan Server utilizar os certificados customizados, os administradores deverão importar os certificados e chaves apropriados. Instruções sobre como importar certificados são fornecidas nesta documentação de configuração.

Para incluir uma varredura de vulnerabilidade de API do FoundScan, consulte "Incluindo um scanner Foundstone FoundScan".

## Incluindo um scanner Foundstone FoundScan

Os administradores podem incluir um scanner Foundstone FoundScan para coletar informações de host e de vulnerabilidade por meio do OpenAPI FoundScan.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu servidor FoundScan.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner. Os

© Copyright IBM Corp. 2007, 2015

certificados para seu scanner FoundScan devem residir no host gerenciado selecionado na caixa de listagem Host gerenciado.

6. Na lista **Tipo**, selecione **FoundScan Scanner**.
7. No campo **URL do SOAP API**, digite o endereço IP ou o nome do host do Foundstone FoundScan que contém as vulnerabilidades que deseja recuperar com o SOAP API. Por exemplo, `https://foundstone IP address:SOAP port`. O valor padrão é `https://localhost:3800`.
8. No campo **Nome do cliente**, digite o nome do cliente que pertence ao nome do usuário.
9. No campo **Nome de usuário**, digite o nome de usuário necessário para acessar o servidor Foundstone FoundScan.
10. Opcional. No campo **Endereço IP do cliente**, digite o endereço IP do servidor que você deseja executar a varredura. Por padrão, esse valor não é utilizado; no entanto, ele será necessário quando os administradores validarem alguns ambientes de varredura.
11. Opcional. No campo **Senha**, digite a senha necessária para acessar o servidor Foundstone FoundScan.
12. No campo **Nome do portal**, digite o nome do portal. Este campo pode ser deixado em branco para o QRadar. Consulte o administrador do FoundScan para obter mais informações.
13. No campo **Nome da configuração**, digite o nome de configuração de varredura que existe no FoundScan e à qual o usuário tem acesso. Assegure-se de que essa configuração de varredura esteja ativa ou seja executada com frequência.
14. No campo **Armazenamento confiável da CA**, digite o caminho do diretório e o nome do arquivo para o arquivo de armazenamento confiável da CA. O caminho padrão é `/opt/qradar/conf/foundscan.keystore`.
15. No campo **Keystore da CA**, digite o caminho do diretório e o nome do arquivo para o keystore do cliente. O caminho padrão é `/opt/qradar/conf/foundscan.truststore`.
16. Para configurar um intervalo do CIDR para o scanner:
    a. No campo de texto, digite o intervalo do CIDR para o scanner considerar ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
17. Clique em **Salvar**.
18. Na guia **Administrador**, clique em **Implementar Mudanças**.

### O que Fazer Depois

Os administradores agora podem importar certificados de seu servidor FoundScan para ativar a comunicação. Consulte "Importando certificados do Foundstone FoundScan".

## Importando certificados do Foundstone FoundScan

Os administradores que utilizam os certificados customizados ou uma versão do Foundstone FoundScan inferior a V5.0 deverão importar os certificados apropriados no host gerenciado na configuração do scanner.

## Antes de Iniciar

O scanner deve ser incluído em um host gerenciado na configuração de varredura antes que os certificados sejam importados a partir do servidor FoundScan. Os certificados devem ser importados no host gerenciado correto para coletar dados de varredura de vulnerabilidade e do host.

## Procedimento

1. Obtenha os dois arquivos de certificado e a passphrase de seu administrador do FoundScan.
   - O arquivo `TrustedCA.pem` é o certificado de CA para o mecanismo do FoundScan.
   - O arquivo de certificado `Portal.pem` é a chave privada que inclui a cadeia de certificados para o cliente.
2. Utilizando o SSH, copie os dois arquivos pem para o host gerenciado designado em sua configuração do FoundScan. Se você tiver uma implementação distribuída, os arquivos deverão ser copiados para o Console e enviados por meio de SSH do dispositivo do Console para o host gerenciado.
3. Navegue para o local do diretório dos arquivos pem.
4. Para remover o certificado keystore anterior do host gerenciado, digite o seguinte comando: `rm -f /opt/qradar/conf/foundscan.keystore`
5. Para remover o certificado de armazenamento confiável anterior do host gerenciado, digite o seguinte comando: `rm -f /opt/qradar/conf/foundscan.truststore`
6. Para importar os arquivos pem em seu host gerenciado, digite o seguinte comando: `/opt/qradar/bin/foundstone-cert-import.sh [TrustedCA.pem] [Portal.pem]`
7. Repita a importação do certificado para quaisquer outros hosts gerenciados em sua implementação que se conectarem ao dispositivo Foundstone FoundScan.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 7. Visão geral do scanner IBM Security AppScan Enterprise

O QRadar recupera os relatórios do AppScan Enterprise com o serviço da web Representational State Transfer (REST) para importar dados de vulnerabilidade e gerar ofensas para sua equipe de segurança.

É possível importar resultados de varredura dos dados do relatório IBM Security AppScan Enterprise, fornecendo a você um ambiente de segurança centralizado para o escaneamento avançado do aplicativo e relatório de conformidade de segurança. É possível importar os resultados da varredura do IBM Security AppScan Enterprise para coletar informações de vulnerabilidade do ativo para malware, aplicativos da web e serviços da web em sua implementação.

Para integrar o AppScan Enterprise com QRadar, você deve executar as tarefas a seguir:

1. Gerar relatórios de varredura no IBM AppScan Enterprise.

   Informações de configuração de relatório podem ser localizadas em sua documentação do IBM Security AppScan Enterprise.
2. Configurar o AppScan Enterprise para conceder acesso do QRadar aos dados do relatório.
3. Configurar o scanner do AppScan Enterprise no QRadar.
4. Criar um planejamento no QRadar para importar resultados do AppScan Enterprise.

Para configurar o IBM AppScan Enterprise para conceder permissão para os dados do relatório, seu administrador do AppScan deverá determinar quais usuários têm permissões para publicar relatórios no QRadar. Após os usuários do AppScan Enterprise configurarem os relatórios, os relatórios que forem gerados pelo AppScan Enterprise poderão ser publicados no QRadar, tornando-os disponíveis para download.

Para configurar o AppScan Enterprise para conceder acesso aos dados do relatório de varredura, consulte o “Criando um tipo de usuário cliente para o IBM AppScan”.

## Criando um tipo de usuário cliente para o IBM AppScan

É possível criar tipos de usuário customizado para designar permissões para tarefas administrativas específicas e limitadas para administradores.

### Procedimento

1. Efetue login no dispositivo IBM AppScan Enterprise.
2. Clique na guia **Administração**.
3. Na página Tipos de Usuários, clique em **Criar**.
4. Selecione todas as seguintes permissões de usuário:
   - **Configurar integração do QRadar** – Marque essa caixa de seleção para permitir que os usuários acessem as opções de integração do QRadar para o AppScan Enterprise.

© Copyright IBM Corp. 2007, 2015

- **Publicar no QRadar** – Marque essa caixa de seleção para permitir que o QRadar acesse os dados do relatório de varredura publicados.
- **Conta de serviço do QRadar** – Marque essa caixa de seleção para incluir acesso à API REST para a conta do usuário. Essa permissão não fornece acesso à interface com o usuário.

5. Clique em **Salvar**.

### O que Fazer Depois

Agora você está pronto para ativar as permissões de integração. Consulte "Permitindo integração com o IBM Security AppScan Enterprise"

## Permitindo integração com o IBM Security AppScan Enterprise

O IBM Security AppScan Enterprise deve ser configurado para ativar a integração com o QRadar.

### Antes de Iniciar

Para concluir essas etapas, você deve ter feito login com um tipo de usuário customizado.

### Procedimento

1. Clique na guia **Administração**.
2. No menu de **Navegação**, selecione **Sistemas de Segurança de Rede**.
3. Na área de janela Configuração de integração do QRadar, clique em **Editar**.
4. Marque a caixa de seleção **Ativar integração do QRadar**. Quaisquer relatórios que são previamente publicados para o QRadar são exibidos. Se qualquer um dos relatórios exibidos não for mais necessário, é possível removê-lo da lista. Conforme você publica mais relatórios para o QRadar, os relatórios são exibidos nessa lista.

### O que Fazer Depois

Agora você está pronto para configurar o Mapeamento de Implementação do Aplicativo no AppScan Enterprise. Consulte "Criando um mapa de implementação do aplicativo no IBM Security AppScan Enterprise".

## Criando um mapa de implementação do aplicativo no IBM Security AppScan Enterprise

O Mapa de Implementação do Aplicativo permite que o AppScan Enterprise determine os locais que hospedam o aplicativo em seu ambiente de produção.

### Sobre Esta Tarefa

Conforme as vulnerabilidades são descobertas, o AppScan Enterprise conhece os locais dos hosts e os endereços IP afetados pela vulnerabilidade. Se um aplicativo for implementado em vários hosts, o AppScan Enterprise gerará uma vulnerabilidade para cada host nos resultados da varredura.

### Procedimento

1. Clique na guia **Administração**.
2. No menu de navegação, selecione **Sistemas de Segurança de Rede**.
3. Na área de janela Configuração de integração do QRadar, clique em **Editar**.
4. No campo **Local de teste de aplicativo (host ou padrão)**, digite o local de teste de seu aplicativo.
5. No campo **Local de produção do aplicativo (host)**, digite o endereço IP do seu ambiente de produção. Para incluir informações de vulnerabilidade no QRadar, o Mapeamento de Implementação do Aplicativo deverá incluir um endereço IP. Se o endereço IP não estiver disponível nos resultados da varredura do AppScan Enterprise, os dados de vulnerabilidade sem um endereço IP são excluídos do QRadar.
6. Clique em **Incluir**.
7. Repita este procedimento para mapear quaisquer ambientes de produção adicionais no AppScan Enterprise.
8. Clique em **Pronto**.

### O que Fazer Depois

Agora você está pronto para publicar relatórios concluídos. Consulte "Publicação de relatórios concluídos no IBM AppScan".

## Publicação de relatórios concluídos no IBM AppScan

Os relatórios de vulnerabilidade concluídos gerados pelo AppScan Enterprise devem ser acessíveis a QRadar por meio de publicação de relatório.

### Procedimento

1. Clique na guia **Tarefas e Relatórios**.
2. Navegue até o relatório de segurança que você deseja disponibilizar para o QRadar.
3. Na barra de menus de qualquer relatório de segurança, selecione **Publicar** > **Conceder** para fornecer acesso de relatório ao QRadar.
4. Clique em **Salvar**.

### O que Fazer Depois

Agora você está pronto para ativar as permissões de integração. Consulte "Incluindo um scanner de vulnerabilidade do IBM AppScan".

## Incluindo um scanner de vulnerabilidade do IBM AppScan

É possível incluir um scanner para definir quais relatórios de varredura no IBM Security AppScan serão coletados pelo QRadar.

### Antes de Iniciar

Se a instalação do AppScan estiver configurada para usar HTPS, será necessário um certificado do servidor. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.

- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

## Sobre Esta Tarefa

É possível incluir vários scanners do IBM AppScan para QRadar, cada um com uma configuração diferente. Diversas configurações permitem que o QRadar importe dados do AppScan para resultados específicos. O planejamento de varredura determina a frequência com a qual os resultados da varredura são importados do serviço da web REST no IBM AppScan Enterprise.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner IBM AppScan Enterprise.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **IBM AppScan Scanner**.
7. No campo **URL Base da Instância ASE**, digite a URL base completa da instância do AppScan Enterprise. O campo suporta os endereços HTTP e HTTPS, por exemplo, `http://myasehostname/ase/`.
8. Na lista **Tipo de Autenticação**, selecione uma das seguintes opções:
   - **Autenticação do Windows** – Selecione esta opção para usar a Autenticação do Windows com o serviço da web REST.
   - **Autenticação do Jazz** – Selecione esta opção para usar a Autenticação do Jazz™ com o serviço da web REST.
9. No campo **Nome de usuário**, digite o nome de usuário para recuperar os resultados da varredura do AppScan Enterprise.
10. No campo **Senha**, digite a senha para recuperar os resultados da varredura do AppScan Enterprise.
11. No campo **Padrão de nome do relatório**, digite uma expressão regular (regex) para filtrar a lista de relatórios de vulnerabilidade disponíveis do AppScan Enterprise. Por padrão, o campo **Padrão de Nome do Relatório** contém o `.*` como o padrão regex. O padrão `.*` importa todos os relatórios de varredura que forem publicados no QRadar. Todos os arquivos correspondentes a partir do padrão do arquivo são processados pelo QRadar. É possível especificar um grupo de relatórios de vulnerabilidade ou um relatório individual usando um padrão regex.
12. Para configurar um intervalo do CIDR para seu scanner:
    a. Digite a faixa de CIDR para o scanner ou clique em **Pesquisar** para selecionar uma faixa de CIDR na lista de rede.
    b. Clique em **Incluir**.
13. Clique em **Salvar**.
14. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura para o IBM Security AppScan Enterprise. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93

# Capítulo 8. Visão geral do scanner IBM Security Guardium

Os dispositivos IBM InfoSphere Guardium podem exportar informações de vulnerabilidade do banco de dados que podem ser fundamentais para proteger os dados do cliente.

Os processos de auditoria do IBM Guardium exportam os resultados de testes de Common Vulnerability and Exposures (CVE) com falha que foram gerados ao executar testes de avaliação de segurança no seu dispositivo IBM Guardium. Os dados de vulnerabilidades do IBM Guardium devem ser exportados para um servidor remoto ou servidor de temporariedade no formato Security Content Automation Protocol (SCAP). Em seguida, o QRadar poderá recuperar os resultados da varredura do servidor remoto que armazena a vulnerabilidade utilizando SFTP.

O IBM Guardium exporta apenas a vulnerabilidade de bancos de dados que contiverem os resultados de teste de CVE com falha. Se nenhum teste de CVE falhar, o IBM Guardium poderá não exportar um arquivo no término da avaliação de segurança. Para obter informações sobre como configurar os testes de avaliação de segurança e criar um processo de auditoria para exportar dados de vulnerabilidade no formato do SCAP, consulte a documentação do IBM InfoSphere Guardium.

Após configurar o dispositivo IBM Guardium, você estará pronto para configurar o QRadar para importar os resultados do servidor remoto que hospeda o dados de vulnerabilidade. Você deve incluir um scanner do IBM Guardium no QRadar e configurar o scanner para recuperar dados de seu servidor remoto. As vulnerabilidades mais recentes são importadas pelo QRadar ao criar um planejamento de varredura. Os planejamentos de varredura permitem determinar a frequência com que o QRadar solicita dados do servidor remoto que hospeda seus dados de vulnerabilidade do IBM Guardium.

Visão geral de integração para o IBM InfoSphere Guardium e o QRadar.

1. No seu dispositivo IBM InfoSphere Guardium, crie um arquivo SCAP com suas informações de vulnerabilidade. Consulte a documentação do IBM Security InfoSphere Guardium.
2. No seu QRadar Console, inclua um scanner do IBM Guardium. Consulte "Incluindo um scanner de vulnerabilidade IBM Security Guardium"
3. No seu QRadar Console, crie um planejamento de varredura para importar os dados do resultado da varredura. Consulte Capítulo 26, "Planejando uma varredura de vulnerabilidade", na página 93

## Incluindo um scanner de vulnerabilidade IBM Security Guardium

Incluir um scanner permite que o QRadar colete arquivos de vulnerabilidade SCAP do IBM InfoSphere Guardium.

### Sobre Esta Tarefa

Os administradores podem incluir diversos scanners IBM Guardium no QRadar, cada um com uma configuração diferente. Diversas configurações permitem que o QRadar importe dados de vulnerabilidade de resultados específicos. O

© Copyright IBM Corp. 2007, 2015

planejamento de varredura determina a frequência com a qual os resultados de varredura SCAP são importados do IBM InfoSphere Guardium.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner IBM Guardium.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **IBM Guardium SCAP Scanner**.
7. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
|---|---|
| **Nome do usuário de login** | Para autenticar com um nome de usuário e senha:<br>1. No campo **Nome de usuário de login**, digite um nome de usuário que possua acesso para recuperar os resultados da varredura do host remoto.<br>2. No campo **Senha de login**, digite a senha associada ao nome de usuário. |
| **Ativar autorização de chave** | Para autenticar com um arquivo de autenticação baseado em chave:<br>1. Marque a caixa de seleção **Ativar autenticação de chave**.<br>2. No campo **Arquivo-chave privado**, digite o caminho do diretório para o arquivo-chave.<br><br>O diretório padrão para o arquivo-chave é `/opt/qradar/conf/vis.ssh`. Se um arquivo-chave não existir, você deverá criar o arquivo-chave vis.ssh. |

8. No campo **Diretório remoto**, digite o local do diretório dos arquivos de resultados da varredura.
9. No campo **Padrão de nome de arquivo**, digite uma expressão regular (regex) necessária para filtrar a lista de arquivos de vulnerabilidades do SCAP especificados no campo **Diretório Remoto**. Todos os arquivos correspondentes são incluídos no processamento. Por padrão, o campo Padrão de nome de relatório contém `.*\.xml` como o padrão regex. O padrão `.*\.xml` importa todos os arquivos xml no diretório remoto.
10. No campo **Idade máxima dos relatórios (Dias)**, digite a idade máxima de arquivo para seu arquivo de resultados da varredura. Os arquivos que forem mais antigos do que a quantia de dias e o registro de data e hora especificados no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. O valor padrão é 7 dias.
11. Para configurar a opção **Ignorar duplicatas**:
    - Marque essa caixa de seleção para rastrear os arquivos que já foram processados por um planejamento de varredura. Esta opção evita que um arquivo de resultados de varredura seja processado uma segunda vez.

- Desmarque essa caixa de seleção para importar os resultados de varredura de vulnerabilidade sempre que o planejamento de varredura for iniciado. Esta opção pode fazer com que diversas vulnerabilidades sejam associadas a um ativo.

Se um arquivo de resultado não for varrido dentro de 10 dias, o arquivo será removido da lista de rastreamento e será processado na próxima vez em que o planejamento de varredura for iniciado.

12. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
13. Clique em **Salvar**.
14. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura para o IBM InfoSphere Guardium. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93

# Capítulo 9. Visão geral do scanner IBM Security SiteProtector

O módulo do scanner IBM SiteProtector para o QRadar acessa os dados de vulnerabilidade dos scanners IBM SiteProtector por meio de consultas Java Database Connectivity (JDBC).

O scanner IBM SiteProtector recupera dados de vulnerabilidade da tabela RealSecureDB e pesquisa novas vulnerabilidades sempre que um planejamento de varredura for iniciado. O campo **Comparar** permite que a consulta recupere quaisquer novas vulnerabilidades da tabela RealSecureDB para assegurar que vulnerabilidades duplicadas não sejam importadas. Quando o scanner IBM SiteProtector é configurado, o administrador poderá criar uma conta do usuário do SiteProtector especificamente para pesquisar dados de vulnerabilidade. Após a conta do usuário ser criada, o administrador poderá verificar se não há nenhum firewall rejeitando consultas na porta configurada para pesquisar o banco de dados.

Para configurar um scanner IBM Security SiteProtector, consulte “Incluindo um scanner de vulnerabilidade IBM SiteProtector”.

## Incluindo um scanner de vulnerabilidade IBM SiteProtector

O QRadar pode pesquisar os dispositivos IBM InfoSphere SiteProtector em busca de dados de vulnerabilidades com o JDBC.

### Sobre Esta Tarefa

Os administradores podem incluir diversos scanners IBM SiteProtector no QRadar, cada um com uma configuração diferente. Diversas configurações permitem que o QRadar consulte o SiteProtector e importe apenas os resultados de intervalos do CIDR específicos. O planejamento de varredura determina a frequência com que o banco de dados no scanner SiteProtector é consultado em busca de dados de vulnerabilidade.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o scanner IBM SiteProtector.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir da implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **IBM SiteProtector Scanner**.
7. No campo **Nome do host**, digite o endereço IP ou o nome do host do IBM SiteProtector que contém as vulnerabilidades a serem importadas.
8. No campo **Porta**, digite 1433 como a porta para o banco de dados do IBM SiteProtector.
9. No campo **Nome de usuário**, digite o nome de usuário necessário para consultar o banco de dados IBM SiteProtector.
10. No campo **Senha**, digite a senha necessária para consultar o banco de dados IBM SiteProtector.

© Copyright IBM Corp. 2007, 2015

11. No campo **Domínio**, digite o domínio obrigatório, se necessário, para se conectar ao banco de dados IBM SiteProtector.

    Se o banco de dados for configurado para Windows e estiver dentro de um domínio, o nome de domínio deverá ser especificado.
12. No campo **Nome do banco de dados**, digite `RealSecureDB` como o nome do banco de dados.
13. No campo **Instância de banco de dados**, digite a instância de banco de dados para o banco de dados IBM SiteProtectorIBM. Se você não estiver utilizando uma instância de banco de dados, este campo poderá ser deixado em branco.
14. Marque a caixa de seleção **Utilizar comunicação de canal nomeado** se canais nomeados forem necessários para comunicação com o banco de dados IBM SiteProtector. Por padrão, essa caixa de seleção fica desmarcada.
15. Marque a caixa de seleção **Utilizar NTLMv2** se o scanner IBM SiteProtector utilizar NTLMv2 como um protocolo de autenticação. Por padrão, essa caixa de seleção fica desmarcada.

    A caixa de seleção Usar NTLMv2 força as conexões MSDE a usarem o protocolo NTLMv2 ao se comunicar com servidores SQL que requerem autenticação NTLMv2. A caixa de seleção Usar NTLMv2 é selecionada e não tem nenhum efeito sobre as conexões MSDE com servidores SQL que não requererem autenticação NTLMv2.
16. Para configurar um intervalo do CIDR para o scanner:
    a. No campo de texto, digite o intervalo do CIDR para a varredura ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
17. Clique em **Salvar**.
18. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93

# Capítulo 10. Visão geral do scanner IBM Security Tivoli Endpoint Manager

O módulo do scanner IBM Tivoli Endpoint Manager acessa os dados de vulnerabilidade do IBM Tivoli Endpoint Manager utilizando o SOAP API instalado com o aplicativo Web Reports.

O aplicativo Web Reports para o Tivoli Endpoint Manager é necessário para recuperar dados de vulnerabilidade do Tivoli Endpoint Manager for QRadar. Os administradores podem criar um usuário no IBM Tivoli Endpoint Manager for QRadar para ser utilizado quando o sistema coletar as vulnerabilidades.

**Nota:** O QRadar é compatível com o IBM Tivoli Endpoint Manager versões 8.2.x. No entanto, os administradores podem usar a versão mais recente do IBM Tivoli Endpoint Manager disponível.

Para incluir um scanner IBM Tivoli Endpoint Manager, consulte "Incluindo um scanner de vulnerabilidade IBM Security Tivoli Endpoint Manager"

## Incluindo um scanner de vulnerabilidade IBM Security Tivoli Endpoint Manager

O QRadar acessa os dados de vulnerabilidade do IBM Tivoli Endpoint Manager usando a API SOAP instalada com o aplicativo Web Reports.

### Sobre Esta Tarefa

É possível incluir vários scanners do IBM Tivoli Endpoint Manager no QRadar. Cada scanner requer uma configuração diferente para determinar quais intervalos de CIDR você deseja que o scanner considere.

Use várias configurações para um único scanner do IBM Tivoli Endpoint Manager a fim de criar scanners individuais que coletem dados de resultado específicos a partir de locais específicos ou vulnerabilidades para tipos específicos de sistemas operacionais.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu IBM Tivoli Endpoint Manager.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **IBM Tivoli Endpoint Manager**.
7. No campo **Nome do host**, digite o endereço IP ou o nome do host do IBM Tivoli Endpoint Manager que contém as vulnerabilidades que você deseja recuperar com a API SOAP.
8. No campo **Porta**, digite o número da porta usada para se conectar ao IBM Tivoli Endpoint Manager usando a API SOAP. Por padrão, a porta 80 é o

© Copyright IBM Corp. 2007, 2015

número da porta para comunicação com o IBM Tivoli Endpoint Manager. Caso use o HTTPS, deve-se atualizar esse campo com o número da porta HTTPS. Para a maioria das configurações, use a porta 443.

9. Marque a caixa de seleção **Utilizar HTTPS** para se conectar de forma segura com o protocolo HTTPS.

   Se essa caixa de seleção for selecionada, o nome do host ou o endereço IP especificado usará o HTTPS para se conectar com o seu IBM Tivoli Endpoint Manager. Quando você usa o HTTPS, um certificado do servidor é necessário. Os certificados devem ser colocados na pasta `/opt/qradar/conf/trusted_certificates`. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. É possível usar SCP ou SFTP para copiar manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates`. Como alternativa, é possível fazer o download de uma cópia do certificado diretamente do host do QRadar. Para fazer isso, use o SSH para conectar o host e digite o comando a seguir: `/opt/qradar/bin/getcert.sh <IP or Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do IP ou do nome do host especificado e é colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.
10. No campo **Nome de usuário**, digite o nome de usuário para acessar o IBM Tivoli Endpoint Manager.
11. No campo **Senha**, digite a senha necessária para acessar o IBM Tivoli Endpoint Manager.
12. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo de CIDR que você deseja que esse scanner considere ou clique em **Pesquisar** para selecionar um intervalo de CIDR na lista de rede.
    b. Clique em **Incluir**.
13. Clique em **Salvar**.
14. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Você está pronto para criar um planejamento de varredura para o IBM Security Tivoli Endpoint Manager. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93

# Capítulo 11. Visão geral do scanner Juniper Profiler NSM

O QRadar pode coletar dados de vulnerabilidade a partir de um banco de dados PostgreSQL no scanner Juniper Profiler NSM ao pesquisar dados com o JDBC.

O console Juniper Networks Netscreen Security Manager (NSM) coleta passivamente informações de ativo valiosas de sua rede por meio de sensores Juniper Networks IDP implementados. O QRadar se conecta ao banco de dados Profiler armazenado no servidor NSM para recuperar esses registros. O servidor QRadar deve ter acesso ao banco de dados Profiler. O QRadar suporta o NSM versões 2007.1r2, 2007.2r2, 2008.1r2, 2009r1.1 e 2010.x. Para obter mais informações, consulte sua documentação do fornecedor. Para coletar dados do banco de dados PostgreSQL, o QRadar deverá ter acesso à porta do banco de dados Postgres por meio da porta TCP 5432. O acesso é fornecido no arquivo `pg_hba.conf`, que está localizado em `/var/netscreen/DevSvr/pgsql/data/pg_hba.conf` no sistema que hospeda o Juniper NSM Profiler.

Para incluir um scanner Juniper NSM Profiler, consulte “Incluindo um scanner Juniper NSM Profiler”.

## Incluindo um scanner Juniper NSM Profiler

Os administradores podem incluir um scanner Juniper NSM Profiler para pesquisar dados de vulnerabilidade com o JDBC.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu servidor FoundScan.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner. Os certificados para seu scanner FoundScan devem residir no host gerenciado selecionado na caixa de listagem Host gerenciado.
6. Na lista **Tipo**, selecione **Juniper NSM Profiler Scanner**.
7. No campo **URL do SOAP API**, digite o endereço IP ou o nome do host do Foundstone FoundScan que contém as vulnerabilidades que deseja recuperar com o SOAP API. Por exemplo, `https://foundstone IP address:SOAP port`. O valor padrão é `https://localhost:3800.`
8. No campo **Nome do cliente**, digite o nome do cliente que pertence ao nome do usuário.
9. No campo **Nome de usuário**, digite o nome de usuário necessário para acessar o servidor Foundstone FoundScan.
10. Opcional. No campo **Endereço IP do cliente**, digite o endereço IP do servidor que você deseja executar a varredura. Por padrão, esse valor não é utilizado; no entanto, ele será necessário quando os administradores validarem alguns ambientes de varredura.
11. Opcional. No campo **Senha**, digite a senha necessária para acessar o servidor Foundstone FoundScan.

© Copyright IBM Corp. 2007, 2015

12. No campo **Nome do portal**, digite o nome do portal. Este campo pode ser deixado em branco para o QRadar. Consulte o administrador do FoundScan para obter mais informações.
13. No campo **Nome da configuração**, digite o nome de configuração de varredura que existe no FoundScan e à qual o usuário tem acesso. Assegure-se de que essa configuração de varredura esteja ativa ou seja executada com frequência.
14. No campo **Armazenamento confiável da CA**, digite o caminho do diretório e o nome do arquivo para o arquivo de armazenamento confiável da CA. O caminho padrão é `/opt/qradar/conf/foundscan.keystore`.
15. No campo **Keystore da CA**, digite o caminho do diretório e o nome do arquivo para o keystore do cliente. O caminho padrão é `/opt/qradar/conf/foundscan.truststore`.
16. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR para o scanner ou clique em **Pesquisar** para selecionar um intervalo do CIDR a partir da lista de rede.
    b. Clique em **Incluir**.
17. Clique em **Salvar**.
18. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para importar certificados a partir do seu servidor FoundScan. Consulte "Importando certificados do Foundstone FoundScan" na página 16.

# Capítulo 12. Visão geral do scanner McAfee Vulnerability Manager

O scanner McAfee Vulnerability Manager permite que o QRadar importe as vulnerabilidades de um arquivo ou uma consulta XML para um arquivo de resultados da McAfee OpenAPI.

O QRadar pode coletar dados de vulnerabilidade de dispositivos McAfee Vulnerability Manager. As versões de software a seguir são suportadas

- v6.8 e v7.0 para a API SOAP do McAfee Vulnerability Manager
- v6.8, v7.0 e v7.5 para importações XML remotas

As opções de importação a seguir estão disponíveis para coletar informações de vulnerabilidade do McAfee Vulnerability Manager:

- Para incluir uma importação XML remota de dados de vulnerabilidade, consulte "Incluindo uma varredura de importação de XML remota".
- Para recuperar vulnerabilidades da API SOAP, consulte "Incluindo uma varredura da API SOAP do McAfee Vulnerability Manager" na página 36

## Incluindo uma varredura de importação de XML remota

Importações de XML remotas permitem que o QRadar se conecte a um servidor remoto e importe os dados de vulnerabilidade XML HostData criados pelo dispositivo McAfee Vulnerability Manager.

### Sobre Esta Tarefa

As importações de arquivo XML remotas permitem configurar o McAfee Vulnerability Manager para exportar os resultados da varredura para um servidor remoto. O QRadar se conecta ao repositório remoto por meio de SFTP e importa os relatórios de varredura XML concluída a partir de um diretório remoto. O método de coleção de importação do arquivo pode ser usado para importar relatórios da varredura concluída do McAfee Vulnerability Manager V7.0 e V7.5.

**Atenção:** A importação pode conter arquivos XML HostData e RiskData. Apenas os arquivos XML HostData são suportados, porque contêm as informações necessárias de host e de vulnerabilidade. Assegure-se de que apenas arquivos XML HostData sejam colocados no diretório remoto ou de que o padrão de nome do arquivo configurado corresponda apenas aos relatórios HostData.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o McAfee Vulnerability Manager.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **McAfee Vulnerability Manager**.
7. Na lista **Tipo de importação**, selecione **Importação XML remota**.

© Copyright IBM Corp. 2007, 2015

8. No campo **Nome do host remoto**, digite o endereço IP ou o nome do host do servidor remoto que hospeda os dados XML do McAfee Vulnerability Manager.
9. No campo **Porta remota**, digite a porta para recuperar os dados de vulnerabilidade XML.
10. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
|---|---|
| **Nome do usuário de login** | É autenticado com um nome de usuário e uma senha. A senha não deve conter o caractere ! . Este caractere pode causar falhas de autenticação por meio de SFTP. |
| **Ativar autorização de chave** | Autenticar com um arquivo de autenticação baseado em chave. Se um arquivo-chave não existir, deve-se criar o arquivo vis.ssh.key e colocá-lo no diretório `/opt/qradar/conf/vis.ssh.key`. |

11. No campo **Diretório remoto**, digite o caminho do diretório para os dados de vulnerabilidade XML.
12. No campo **Padrão de Nome do Arquivo**, digite uma expressão regular (regex) para filtrar a lista de arquivos especificados no Diretório Remoto. Todos os arquivos correspondentes são incluídos no processamento. Assegure-se de que esse padrão corresponda apenas a relatórios XML HostData.
13. No campo **Idade máx. dos relatórios (dias)**, digite a idade máxima do arquivo de resultados da varredura.
14. Para configurar um intervalo do CIDR para o scanner:
    a. No campo de texto, digite o intervalo do CIDR para a varredura ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
15. Clique em **Salvar**.
16. Na guia **Administrador**, clique em **Implementar Mudanças**.

## Incluindo uma varredura da API SOAP do McAfee Vulnerability Manager

É possível incluir um scanner McAfee Vulnerability Manager para permitir que o QRadar colete informações do host e de vulnerabilidade por meio do McAfee OpenAPI.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o scanner.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner. Os certificados para o scanner devem estar no host gerenciado selecionado na lista **Host gerenciado**.
6. Na lista **Tipo**, selecione **McAfee Vulnerability Manager**.
7. No campo **URL do SOAP API**, digite o endereço IP ou o nome do host do McAfee Vulnerability Manager que contém as vulnerabilidades que deseja

recuperar com o SOAP API. Por exemplo, `https://foundstone IP address:SOAP port`. O valor padrão é `https://localhost:3800`.

8. No campo **Nome do cliente**, digite o nome do cliente que pertence ao nome do usuário.
9. No campo **Nome do usuário**, digite o nome do usuário para acessar o McAfee Vulnerability Manager.
10. Opcional: No campo **Endereço IP do cliente**, digite o endereço IP do servidor que você deseja executar a varredura.

    **Dica:** Em geral, esse campo não é usado, no entanto, pode ser necessário validar alguns ambientes de varredura.
11. No campo **Senha**, digite a senha para acessar o McAfee Vulnerability Manager.
12. No campo **Nome da configuração**, digite o nome de configuração de varredura que existe no McAfee Vulnerability Manager e para a qual o usuário tem acesso. Certifique-se de que essa configuração de varredura esteja ativa ou seja executada com frequência.
13. No campo **Armazenamento confiável da CA**, digite o caminho do diretório e o nome do arquivo para o arquivo de armazenamento confiável da CA.

    O caminho padrão é `/opt/qradar/conf/mvm.keystore`.
14. No campo **Keystore da CA**, digite o caminho do diretório e o nome do arquivo para o keystore do cliente.

    O caminho padrão é `/opt/qradar/conf/mvm.truststore`.
15. Na lista **Versões do McAfee Vulnerability Manager**, selecione a versão do software do seu McAfee Vulnerability Manager.
16. Para remover as vulnerabilidades detectadas anteriormente que não foram detectadas pela varredura mais recente, marque a caixa de seleção **Limpeza de vulnerabilidade**.
17. Para configurar um intervalo do CIDR para o scanner:
    a. Digite a faixa de CIDR para a varredura ou clique em **Pesquisar** para selecionar uma faixa de CIDRna lista de redes.

       O McAfee Vulnerability Manager aceita apenas intervalos de endereços do CIDR para uma sub-rede 0/0 que forem incluídos como 0.0.0.0/0.
    b. Clique em **Incluir**.
18. Clique em **Salvar**.
19. Na guia **Administrador**, clique em **Implementar Mudanças**.

### O que Fazer Depois

Agora você está pronto para criar certificados a partir do McAfee Vulnerability Manager. Consulte "Criando certificados do McAfee Vulnerability Manager".

## Criando certificados do McAfee Vulnerability Manager

Para se conectar por meio do Foundstone Open API, configure certificados de empresas terceirizadas com o McAfee Certificate Manager Tool.

### Antes de Iniciar

Se o Certificate Manager Tool não estiver instalado no servidor McAfee Foundstone Enterprise Manager, entre em contato com o Suporte Técnico da McAfee.

### Sobre Esta Tarefa

Os certificados de lado do cliente devem ser processados em arquivos keystore e de armazenamento confiável válidos do QRadar no servidor McAfee Foundstone Enterprise Manager.

O servidor McAfee Foundstone Enterprise Manager deve ser compatível com a versão do FIPS-Capable OpenSSL utilizada pelo Foundstone Certificate Manager para criar corretamente os certificados. Um Java Software Development Kit (Java SDK) deve estar presente neste servidor para esse processamento. Para obter o Java SDK mais recente, acesse o website a seguir:

http://java.sun.com.

### Procedimento

1. Efetue login no servidor McAfee Foundstone Enterprise Manager.
2. Execute o Foundstone Certificate Manager.
3. Clique na guia **Criar Certificados SSL**.
4. Digite o endereço do host do QRadar.

   O certificado deve ser criado com o endereço do host para o dispositivo QRadar que recupera os dados de vulnerabilidade do McAfee Vulnerability Manager.
5. Opcional: Clique em **Resolver**.

   Se ocorrer um erro quando o Foundstone Certificate Manager tentar resolver o host, digite o endereço IP no campo **Endereço do host**. Se o host não puder ser resolvido, consulte a Etapa 7.
6. Clique em **Criar certificado utilizando nome comum**.
7. Clique em **Criar certificado utilizando endereço do host**.
8. Salve o arquivo compactado que contém os arquivos de certificado em um diretório no McAfee Vulnerability Manager.
9. Copie a passphrase fornecida para um arquivo de texto.
10. Repita este processo para gerar quaisquer outros certificados para hosts gerenciados em sua implementação.

### O que Fazer Depois

Agora você está pronto para processar os certificados para criar os arquivos keystore e de armazenamento confiável necessários. Consulte “Processando certificados do McAfee Vulnerability Manager”.

## Processando certificados do McAfee Vulnerability Manager

Para criar os arquivos keystore e de armazenamento confiável necessários para o QRadar, processe os certificados criados pelo Foundstone Certificate Manager.

### Antes de Iniciar

Deve-se ter acesso ao portal de suporte para fazer o download dos arquivos necessários para criar os arquivos keystore e de armazenamento confiável. Os arquivos em lote requerem o caminho para o diretório inicial de Java no McAfee Vulnerability Manager.

### Procedimento

1. Efetue login no portal de suporte para fazer o download dos arquivos a seguir:
   - `VulnerabilityManager-Cert.bat.gz`
   - `q1labs_vis_mvm_cert.jar`
2. Extraia os arquivos compactados e copie os certificados e os arquivos transferidos por download para o mesmo diretório em seu McAfee Vulnerability Manager.
3. Abra a interface da linha de comandos no McAfee Vulnerability Manager.
4. Acesse o local do diretório dos arquivos.
5. Para executar o arquivo em lote, digite o seguinte comando: `VulnerabilityManager-Cert.bat "C:\Program Files\Java\jdk1.6.0_20"`.

   As aspas no comando especificam o diretório inicial de Java.
6. Repita este processo para criar arquivos keystore e de armazenamento confiável para qualquer outro host gerenciado em sua implementação.

### Resultados

Os arquivos keystore e de armazenamento confiável são criados. Se um erro for exibido, os administradores poderão verificar o caminho para o diretório inicial do Java.

### O que Fazer Depois

Agora você está pronto para importar os certificados nos seu dispositivo QRadar. Consulte “Importando certificados do McAfee Vulnerability Manager”

## Importando certificados do McAfee Vulnerability Manager

Os arquivos keystore e de armazenamento confiável devem ser importados no host gerenciado responsável pela varredura.

### Antes de Iniciar

O scanner deve ser incluído em um host gerenciado na configuração de varredura antes da importação dos certificados. Por motivos de segurança, um protocolo de transferência de arquivos seguro para copiar um arquivo de certificado.

### Procedimento

1. Para importar os certificados, use o Secure Copy para copiar os arquivos mvm.keystore e mvm.truststore para os seguintes diretórios no QRadar:
   - `/opt/qradar/conf/`
   - `/opt/qradar/conf/trusted_certificates/`

     **Nota:** Se o diretório `/opt/qradar/conf/trusted_certificates/` não existir, não crie o diretório. Se o diretório não existir, os administradores poderão ignorar a cópia do arquivo para o diretório ausente.

   Se você tiver uma implementação distribuída, os arquivos deverão ser copiados para o Console e enviados por meio de SSH do dispositivo do Console para o host gerenciado.
2. Efetue login no QRadar.
3. Clique na guia **Administrador**.

4. Na guia **Administrador**, selecione **Avançado** > **Implementar configuração completa**.

   **Nota:** Ao clicar em **Implementar configuração completa**, o QRadar reinicia todos os serviços. A reinicialização do serviço resulta em uma diferença na coleta de dados para eventos e fluxos até que o processo de implementação seja concluído.
5. Repita a importação do certificado para quaisquer outros hosts gerenciados em sua implementação que coletarem vulnerabilidades a partir do McAfee Vulnerability Manager.

# Capítulo 13. Visão geral do scanner do Microsoft SCCM

O IBM Security QRadar pode importar relatórios de varredura dos scanners do Microsoft System Center Configuration Manager (SCCM).

Para integrar um scanner do Microsoft SCCM, execute as etapas a seguir:

1. No seu scanner do Microsoft SCCM, configure a WMI. Consulte Capítulo 14, "Ativação da WMI no host do scanner", na página 43.
2. Se atualizações automáticas não estiverem ativadas no seu Console do QRadar, faça o download e instale o Microsoft SCCM RPM.
3. No seu Console do QRadar, inclua um scanner do Microsoft SCCM. Consulte Capítulo 15, "Incluindo um scanner do Microsoft SCCM", na página 45.
4. No seu QRadar Console, crie um planejamento de varredura para importar os dados do resultado da varredura. Consulte Capítulo 26, "Planejando uma varredura de vulnerabilidade", na página 93.

© Copyright IBM Corp. 2007, 2015

# Capítulo 14. Ativação da WMI no host do scanner

Antes de poder configurar um scanner do Microsoft SCCM, deve-se definir as configurações do seu sistema DCOM para cada host que deseja monitorar.

Assegure-se de que o host do scanner atenda às condições a seguir:

- Você é um membro do grupo Administradores nesse host.
- Um dos sistemas operacionais a seguir está instalado:
  - Windows 2000
  - Windows 2003
  - Windows 2008
  - XP
  - Software Vista
  - Windows 7

  **Nota:** Sistemas operacionais de 32 e de 64 bits são suportados.
- O DCOM é configurado e ativado.

  Se um firewall estiver instalado no host ou estiver localizado entre o host e o QRadar (como um hardware ou outro firewall intermediário), o firewall deverá ser configurado para permitir a comunicação do DCOM. Configure o firewall para permitir que a porta 135 seja acessível no host e permita portas DCOM (portas aleatórias acima de 1024). Dependendo da versão do Windows que você usa, também pode ser necessário configurar portas específicas para serem acessíveis ao DCOM. Para obter mais informações, consulte sua documentação do Windows.
- A Instrumentação de Gerenciamento do Windows (WMI) está ativada.
- O serviço de registro remoto está ativado.

Para obter instruções específicas sobre como configurar DCOM e WMI no Windows 2008 e no Windows 7, consulte os documentos no website de suporte IBM:

- Windows 2008 (http://www-01.ibm.com/support/docview.wss?uid=swg21681046)
- Windows 7 (http://www-01.ibm.com/support/docview.wss?uid=swg21678809)

© Copyright IBM Corp. 2007, 2015

# Capítulo 15. Incluindo um scanner do Microsoft SCCM

## Antes de Iniciar

Assegure-se de que a WMI esteja ativada no host do scanner.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. Configure os parâmetros do Microsoft SCCM a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do scanner** | O nome para identificar sua instância do scanner. |
| **Host gerenciado** | O host gerenciado da implementação do QRadar que gerencia a importação do scanner. |
| **Tipo** | Microsoft SCCM |
| **Nome do host** | O endereço IP ou o nome do host do servidor remoto que hospeda os arquivos de resultados da varredura. |
| **Domínio** | O domínio usado para se conectar ao servidor remoto. |

5. Configure os parâmetros restantes.
6. Para configurar um intervalo do CIDR para seu scanner:
   a. Digite o intervalo de CIDR que você deseja que este scanner considere ou clique em **Procurar** para selecionar um intervalo de CIDR na lista de rede.
   b. Clique em **Incluir**.
7. Clique em **Salvar**.

© Copyright IBM Corp. 2007, 2015

# Capítulo 16. Visão geral do scanner nCircle IP360

O QRadar pode importar relatórios de varredura XML2 de servidores SSH que contiverem informações de vulnerabilidade do nCircle IP360.

O QRadar não pode se conectar diretamente com dispositivos nCircle. É possível configurar um dispositivo de scanner nCircle IP360 para exportar resultados de varredura no formato XML2 para um servidor SSH remoto. Para importar os resultados de varredura mais recentes do servidor remoto para o QRadar, é possível planejar uma varredura ou pesquisar o servidor remoto em busca de atualizações para os resultados da varredura.

Os resultados da varredura contêm informações de identificação da configuração da varredura a partir das quais a varredura foi produzida. Os resultados de varredura mais recentes são usados quando o QRadar importa uma varredura. O QRadar suporta resultados de varredura exportados apenas do scanner IP360 no formato XML2.

Para integrar um scanner nCircle IP360, execute as etapas a seguir:

1. No seu scanner nCircle IP360, configure seu scanner nCircle para exportar relatórios de varredura. Consulte "Exportando resultados da varredura do nCircle IP360 em um servidor SSH".
2. No QRadar Console, inclua um scanner nCircle IP360. Consulte "Incluindo um scanner nCircle IP360" na página 48
3. No seu QRadar Console, crie um planejamento de varredura para importar os dados do resultado da varredura. Consulte Capítulo 26, "Planejando uma varredura de vulnerabilidade", na página 93

## Exportando resultados da varredura do nCircle IP360 em um servidor SSH

O QRadar usa uma função de exportação automatizada para publicar dados de varredura XML2 a partir de dispositivos nCircle IP360. O QRadar suporta o VnE Manager versão IP360-6.5.2 a 6.8.2.8.

### Antes de Iniciar

Assegure-se de que o servidor remoto seja um sistema UNIX com SSH ativado.

### Procedimento

1. Efetue login na interface com o usuário do IP360 VNE Manager.
2. No menu de navegação, selecione **Administrar** > **Sistema** > **VNE Manager** > **Exportação Automatizada**.
3. Clique na guia **Exportar para o Arquivo**.
4. Defina as configurações de exportação. A exportação deverá ser configurada para utilizar o formato XML2.
5. Registre as configurações de destino exibidas na interface com o usuário para a exportação de varredura. Essas definições são necessárias para configurar o QRadar para integrar-se com o seu dispositivo nCircle IP360.

© Copyright IBM Corp. 2007, 2015

# Incluindo um scanner nCircle IP360

O QRadar utiliza um shell seguro (SSH) para acessar um servidor remoto (servidor de exportação SSH) para recuperar e interpretar os dados de varredura de dispositivos nCircle IP360. O QRadar suporta o VnE Manager versão IP360-6.5.2 a 6.8.2.8.

## Antes de Iniciar

Esta configuração requer as configurações de destino registradas durante a exportação dos dados de varredura XML2 para o servidor remoto.

## Sobre Esta Tarefa

Se o scanner estiver configurado para usar uma senha, o servidor do scanner SSH ao qual o QRadar se conectar deverá suportar autenticação de senha. Se não suportar, a autenticação SSH para o scanner falhará. Certifique-se de que a linha a seguir seja exibida no arquivo `sshd_config`, localizada geralmente no diretório `/etc/ssh` no servidor SSH: `PasswordAuthentication yes`. Se o servidor do scanner não usar OpenSSH, a configuração poderá ser diferente. Para obter mais informações, consulte a documentação do fornecedor do scanner.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. Configure os parâmetros do nCircle IP360 a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do scanner** | O nome para identificar a instância do nCircle IP360. |
| **Host gerenciado** | O host gerenciado da implementação do QRadar que gerencia a importação do scanner. |
| **Tipo** | nCircle IP360 |
| **Nome do host do servidor SSH** | O endereço IP ou o nome do host do servidor remoto que hospeda os arquivos de resultados da varredura. |
| **Porta SSH** | O número da porta para conectar-se ao servidor remoto. |
| **Diretório remoto** | A localização dos arquivos de resultados da varredura. |
| **Padrão do arquivo** | A expressão regular (regex) para filtrar a lista de arquivos especificados no campo **Diretório remoto**. Para listar todos os arquivos de formato XML2 que terminam com XML, use a entrada a seguir: `XML2.*\.xml` |

5. Configure os parâmetros restantes.
6. Para configurar um intervalo do CIDR para seu scanner:
   a. Digite o intervalo de CIDR que você deseja que este scanner considere ou clique em **Procurar** para selecionar um intervalo de CIDR na lista de rede.

b. Clique em **Incluir**.
7. Clique em **Salvar**.
8. Na guia **Administrador**, clique em **Implementar Mudanças**.

# Capítulo 17. Visão geral do scanner Nessus

O QRadar pode usar um relacionamento de cliente e servidor Nessus para recuperar relatórios de varredura de vulnerabilidade. Também é possível usar a API XMLRPC Nessus ou a API JSON para acessar dados de varredura diretamente do Nessus.

Ao configurar o cliente Nessus, é necessário criar uma conta do usuário do Nessus para o sistema QRadar. Uma conta do usuário exclusiva assegura que o QRadar tenha as credenciais corretas para efetuar login e comunicar-se com o servidor Nessus. Após a criação da conta do usuário, um teste de conexão verifica as credenciais do usuário e o acesso remoto.

**Nota:** Não instale o software Nessus em um sistema crítico devido aos requisitos de CPU quando as varreduras estão ativas.

## Opções de coleta de dados

As opções a seguir estão disponíveis para coleta de dados de informações de vulnerabilidade a partir de scanners Nessus:

**Varredura ativa planejada**
As varreduras ativas permitem que varreduras predefinidas sejam iniciadas remotamente por meio de SSH no Nessus e os dados sejam importados durante a conclusão da varredura.

**Importação de resultados planejada**
Arquivos de resultados estáticos de varreduras concluídas são importados de um repositório sobre SSH que contém os resultados da varredura Nessus.

**Varredura ativa planejada - API XMLRPC**
XMLRPC permite que varreduras predefinidas sejam iniciadas remotamente e coletadas ativamente usando a API XMLRPC.

A API Nessus XMLRPC está disponível apenas em servidores e clientes Nessus com o software V4.2 e superior.

**Varredura ativa planejada - API JSON**
Permite que varreduras predefinidas sejam iniciadas remotamente e coletadas ativamente usando a API JSON.

**Importação planejada de relatórios concluídos - API XMLRPC**
Permite que os relatórios concluídos sejam importados do servidor Nessus usando a API XMLRPC.

**Importação Planejada de Relatórios Concluídos - API JSON**
Permite que relatórios concluídos sejam importados do servidor Nessus.

## Certificados do servidor

Antes de incluir um scanner, é necessário um certificado do servidor para suportar conexões HTTPS. O QRadar suporta certificados com as seguintes extensões de arquivos: `.crt`, `.cert` ou `.der`. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

© Copyright IBM Corp. 2007, 2015

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando Secure Copy (SCP) ou Secure File Transfer Protocol (SFTP).
- Para fazer download automaticamente do certificado para o diretório `/opt/qradar/conf/trusted_certificates`, execute SSH no Console ou host gerenciado e digite o seguinte comando:

  `/opt/qradar/bin/getcert.sh <IP_or_Hostname> <optional_port_(443_default)>`.

## Incluindo uma varredura ativa planejada Nessus

Uma varredura em tempo real é executada no servidor Nessus e importa os dados de resultado de um diretório temporário no cliente Nessus que contém os dados de relatório de varredura.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Nessus.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Nessus Scanner**.
7. Na lista **Tipo de coleta**, selecione **Varredura ativa planejada**.
8. .
9. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome de Usuário do Servidor** | O nome de usuário para acessar o servidor Nessus. |
| **Senha do servidor** | Sua senha do servidor Nessus não deve conter o caractere de ponto de exclamação (!) ou poderão ocorrer falhas de autenticação sobre SSH. |
| **Dir. Temp. do cliente** | O caminho do diretório do cliente Nessus que o QRadar pode usar para armazenar arquivos temporários.<br><br>O QRadar usa o diretório temporário no cliente Nessus para fazer upload de destinos de varredura e ler resultados de varredura. Os arquivos temporários são removidos do diretório temporário quando a varredura é concluída e o relatório de varredura é transferido por download. |
| **Executável do Nessus** | O caminho do diretório para o arquivo executável no servidor Nessus. |
| **Arquivo de configuração do Nessus** | O caminho do diretório para o arquivo de configuração do Nessus no cliente Nessus. |
| **Nome do host do cliente** | O nome do host ou endereço IP do cliente Nessus. |

| Parâmetro | Descrição |
| --- | --- |
| **Porta SSH do cliente** | A porta SSH no servidor Nessus que pode ser usada para recuperar arquivos de resultado de varredura. |
| **Nome de usuário do cliente** | O nome de usuário para autenticar a conexão SSH. |
| **Senha do cliente** | Se o campo **Ativar autenticação de chave** estiver ativado, a senha será ignorada.<br><br>Se o scanner estiver configurado para usar uma senha, o servidor do scanner SSH que se conecta ao QRadar deverá suportar autenticação de senha. Se não suportar, a autenticação SSH para o scanner falhará. Assegure-se de que a seguinte linha seja exibida em seu arquivo `/etc/ssh/sshd_config`: `PasswordAuthentication yes`. Se o servidor do scanner não utilizar OpenSSH, consulte a documentação do fornecedor para obter as informações de configuração do scanner. |
| **Arquivo de chave privado** | O caminho do diretório para o arquivo-chave. Se um arquivo-chave não existir, você deverá criar o arquivo `vis.ssh.key`. |
| **Máscara CIDR** | O tamanho da sub-rede que você deseja varrer. O valor representa a maior parte da sub-rede que o scanner pode varrer de uma vez. A máscara segmenta a varredura para otimizar o desempenho da varredura. |

10. Para configurar um intervalo do CIDR para seu scanner:
    a. Digite o intervalo de CIDR que você deseja que este scanner considere ou clique em **Procurar** para selecionar um intervalo de CIDR na lista de rede.
    b. Clique em **Incluir**.
11. Clique em **Salvar**.
12. Na guia **Administrador**, clique em **Implementar Mudanças**.

## Incluindo uma importação de resultados planejada do Nessus

Uma importação de resultados planejada recupera os relatórios de varredura Nessus concluída de um local externo.

### Sobre Esta Tarefa

Um relatório de varredura concluído pode ser armazenado em um servidor Nessus ou em um repositório de arquivo. O QRadar se conecta ao servidor Nessus ou ao repositório de arquivo usando SSH e, em seguida, importa arquivos de relatórios de varredura concluídos. Os relatórios são filtrados por uma expressão regular definida ou uma idade máxima de relatório. O QRadar suporta importações de relatórios de varredura do Nessus no formato `.nessus` ou relatórios de varredura exportados para um formato de saída do Nessus, como XML2.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Nessus.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Nessus Scanner**.
7. Na lista **Tipo de coleção**, selecione **Importação de resultados planejada**.
8. No campo **Nome do host de resultados remotos**, digite o endereço IP ou o nome do host do servidor ou do cliente Nessus que hospeda seus arquivos de resultado de varredura do Nessus ou do XML2.
9. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
|---|---|
| **Nome do usuário de login** | Para autenticar com um nome de usuário e senha:<br>1. No campo **Nome de usuário do SSH**, digite o nome de usuário para acessar o scanner Nessus ou o repositório que hospeda os arquivos de resultado da varredura.<br>2. No campo **Senha de SSH**, digite a senha associada ao nome de usuário.<br><br>A senha não deve conter o caractere de ponto de exclamação (!) . Esse caractere pode causar falhas de autenticação pelo SSH. |
| **Ativar autorização de chave** | Para autenticar com um arquivo de autenticação baseado em chave:<br>1. Marque a caixa de seleção **Ativar autenticação de chave**.<br>2. No campo **Arquivo-chave privado**, digite o caminho do diretório para o arquivo-chave.<br><br>O diretório padrão para o arquivo-chave é `/opt/qradar/conf/vis.ssh.key`. Se um arquivo-chave não existir, você deverá criar o arquivo vis.ssh.key. |

10. No campo **Diretório de resultados remoto**, digite o local do diretório dos arquivos de resultados da varredura. O caminho do diretório padrão é `./`.
11. No campo **Padrão de Nome do Arquivo**, digite uma expressão regular (regex) para filtrar a lista de arquivos especificados no Diretório Remoto. Todos os arquivos correspondentes são incluídos no processamento. Por padrão, o campo **Padrão de nome de relatório** contém `.*\.nessus` como o padrão de expressão regular. O padrão `.*\.nessus` importa todos os arquivos de resultado formatados do Nessus no diretório remoto.
12. No campo **Idade máxima dos relatórios (Dias)**, digite a idade máxima de arquivo para seu arquivo de resultados da varredura. Arquivos que forem

mais antigos do que registro de data e hora especificado no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. O valor padrão é 7 dias.

13. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo de CIDR que você deseja que esse scanner considere ou clique em **Pesquisar** para selecionar um intervalo de CIDR na lista de rede.
    b. Clique em **Incluir**.
14. Clique em **Salvar**.

## Incluindo uma varredura em tempo real do Nessus com a API XMLRPC

O IBM Security QRadar pode usar a API XMLRPC para iniciar uma varredura pré-configurada que é baseada em um nome de varredura e em um nome de política opcional no servidor Nessus.

### Sobre Esta Tarefa

Para iniciar uma varredura ativa a partir do QRadar, você deverá especificar o nome da varredura e o nome da política para os dados de varredura ativa você deseja recuperar. Conforme a varredura ativa progride, é possível apontar o mouse sobre o scanner Nessus na janela Planejamento de varredura para visualizar a porcentagem da varredura ativa que está concluída. Após a varredura ativa atingir a conclusão, o QRadar usará a API XMLRPC para recuperar os dados de varredura e atualizar as informações vulnerabilidade de seus ativos.

A API Nessus XMLRPC está disponível apenas em servidores e clientes Nessus com o software V4.2 e superior.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Nessus.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Nessus Scanner**.
7. Na lista **Tipo de Coleta**, selecione **Varredura Ativa Planejada – API XMLRPC** .
8. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do host** | O endereço IP ou nome do host do servidor Nessus. |
| **Porta** | O número da porta do servidor Nessus. |
| **Nome de usuário** | O nome de usuário necessário para acessar o servidor Nessus |
| **Senha** | Sua senha do servidor Nessus não deve conter o caractere de ponto de exclamação (!) ou poderão ocorrer falhas de autenticação sobre SSH. |

| Parâmetro | Descrição |
| --- | --- |
| **Nome da varredura** | O nome da varredura que você deseja exibir quando a varredura ativa for executada no servidor Nessus.<br><br>Se esse campo estiver desmarcado, a API tentará iniciar uma varredura ativa para o QRadar Scan. Esse campo não suporta o uso do caractere e comercial (símbolo &) nesse campo. |
| **Nome da política** | O nome de uma política no servidor Nessus para iniciar uma varredura ativa.<br><br>A política deverá existir no servidor Nessus quando o sistema tentar iniciar a varredura. Se a política não existir, será exibido um erro na coluna **Status**. Os sistemas podem ter nomes de políticas customizadas, mas vários nomes de políticas padrão estão incluídos. `Varredura de rede externa`, `Varredura de rede interna`, `Testes de aplicativo da web`, `Preparar para auditorias PCI DSS` são nomes da política padrão. |

9. Para configurar um intervalo do CIDR para seu scanner:
   a. No campo de texto, digite o intervalo de CIDR que você deseja que esse scanner considere ou clique em **Pesquisar** para selecionar um intervalo de CIDR na lista de rede.
   b. Clique em **Incluir**.
10. Clique em **Salvar**.

## Incluindo uma importação de relatório concluído Nessus com a API XMLRPC

Uma importação de resultados planejada usando a API XMLRPC permite que os relatórios de vulnerabilidades concluídos sejam transferidos por download a partir do servidor Nessus.

### Sobre Esta Tarefa

O QRadar se conecta ao seu servidor Nessus e faz download dos dados a partir de quaisquer relatórios concluídos que corresponderem ao filtro de nome do relatório e idade máxima do relatório. O Nessus XMLRPC API está disponível em servidores e clientes Nessus que usam o software v4.2 e superior.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu servidor Nessus.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.

6. Na lista **Tipo**, selecione **Importação Planejada de Relatório Concluído – API XMLRPC**.
7. No campo **Nome de host**, digite o endereço IP ou o nome do host do IBM Tivoli Endpoint Manager que contém as vulnerabilidades deseja recuperar com a API SOAP.
8. No campo **Porta**, digite o número da porta do servidor Nessus. O valor de porta da API padrão é 8834 .
9. No campo **Nome de usuário**, digite o nome de usuário necessário para acessar o servidor Nessus.
10. No campo **Senha**, digite a senha necessária para acessar o servidor Nessus.
11. No campo **Padrão de nome de relatório**, digite uma expressão regular (regex) necessária para filtrar a lista de arquivos especificados no Diretório Remoto. Todos os arquivos correspondentes são incluídos no processamento. Por padrão, o campo Padrão de nome de relatório contém `.*` como o padrão regex. O padrão `.*` importa todos os arquivos de resultados no formato nessus no diretório remoto.
12. No campo **Idade máxima dos relatórios (Dias)**, digite a idade máxima de arquivo para seu arquivo de resultados da varredura. Os arquivos que forem mais antigos do que a quantia de dias e o registro de data e hora especificados no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. O valor padrão é 7 dias.
13. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
14. Clique em **Salvar**.

## Incluindo uma varredura ativa do Nessus com a API JSON

O IBM Security QRadar pode usar a API JSON para iniciar uma varredura pré-configurada que seja baseada em um nome de varredura e em um nome de política opcional no servidor Nessus.

### Sobre Esta Tarefa

Para iniciar uma varredura ativa a partir do QRadar, você deverá especificar o nome da varredura e o nome da política para os dados de varredura ativa você deseja recuperar. Conforme a varredura ativa progride, é possível apontar o mouse sobre o scanner Nessus na janela Planejamento de varredura para visualizar a porcentagem da varredura ativa que está concluída. Após a conclusão da varredura ativa, o QRadar usa a API JSON para recuperar os dados de varredura e atualizar as informações de vulnerabilidade para seus ativos.

A API JSON Nessus está disponível apenas em servidores e clientes Nessus com o software v6.0 e superior.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.

4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Nessus.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Nessus Scanner**.
7. Na lista **Tipo de coleta**, selecione **Varredura ativa planejada - API JSON**.
8. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do host** | O endereço IP ou nome do host do servidor Nessus. |
| **Porta** | O número da porta do servidor Nessus. |
| **Nome de usuário** | O nome de usuário necessário para acessar o servidor Nessus |
| **Senha** | Sua senha do servidor Nessus não deve conter o caractere de ponto de exclamação (!) ou poderão ocorrer falhas de autenticação. |
| **Nome da varredura** | O nome da varredura que você deseja exibir quando a varredura ativa for executada no servidor Nessus.<br><br>Se esse campo estiver desmarcado, a API tentará iniciar uma varredura ativa para o QRadar Scan. Esse campo não suporta o uso do caractere e comercial (símbolo &) nesse campo. |
| **Nome da política** | O nome de uma política no servidor Nessus para iniciar uma varredura ativa.<br><br>A política deverá existir no servidor Nessus quando o sistema tentar iniciar a varredura. Se a política não existir, será exibido um erro na coluna **Status**. Os sistemas podem ter nomes de políticas customizadas, mas vários nomes de políticas padrão estão incluídos. `Varredura de rede externa`, `Varredura de rede interna`, `Testes de aplicativo da web`, `Preparar para auditorias PCI DSS` são nomes da política padrão. |
| **Nome do scanner** | Se houver mais de um scanner Nessus em sua implementação, especifique o nome do scanner no qual deseja executar as varreduras. |

9. Para configurar um intervalo do CIDR para seu scanner:
   a. No campo de texto, digite o intervalo de CIDR que você deseja que esse scanner considere ou clique em **Pesquisar** para selecionar um intervalo de CIDR na lista de rede.
   b. Clique em **Incluir**.
10. Clique em **Salvar**.

# Incluindo uma importação de relatório concluído do Nessus com a API JSON

Uma importação de resultados planejada recupera relatórios de varredura concluídos do Nessus de um local externo usando a API JSON.

## Sobre Esta Tarefa

Um relatório de varredura concluído pode ser armazenado em um servidor Nessus ou em um repositório de arquivo. O IBM Security QRadar se conecta ao servidor Nessus ou ao repositório de arquivo usando a API JSON e, em seguida, importa arquivos de relatórios de varredura concluídos. Os relatórios são filtrados por uma expressão definida ou uma idade máxima de relatório.

A API JSON Nessus está disponível apenas em servidores e clientes Nessus com o software v6.0 e superior.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Nessus.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Nessus Scanner**.
7. Na lista **Tipo de coleta**, selecione **Importação planejada de relatórios concluídos - API JSON**.
8. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do host** | O endereço IP ou nome do host do servidor Nessus. |
| **Porta** | O número da porta do servidor Nessus. |
| **Nome de usuário** | O nome de usuário necessário para acessar o servidor Nessus |
| **Senha** | A senha do servidor Nessus. |
| **Filtro de nomes de relatórios** | Filtra a lista de arquivos especificados no Diretório remoto. Todos os arquivos correspondentes são incluídos no processamento. Por padrão, o campo Padrão de nome de relatório contém `.*` como o filtro. |
| **Idade máxima de relatório (dias)** | A idade máxima do arquivo para o arquivo de resultados de varredura. Arquivos que forem mais antigos do que registro de data e hora especificado no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. O valor padrão é 7 dias. |

9. Para configurar um intervalo do CIDR para seu scanner:
   a. No campo de texto, digite o intervalo de CIDR que você deseja que esse scanner considere ou clique em **Pesquisar** para selecionar um intervalo de CIDR na lista de rede.
   b. Clique em **Incluir**.
10. Clique em **Salvar**.

# Capítulo 18. Visão geral do scanner netVigilance SecureScout

O QRadar pode coletar dados de vulnerabilidade a partir de um banco de dados SQL no scanner SecureScout ao pesquisar dados com o JDBC.

O netVigilance SecureScout NX e o SecureScout SP armazenam os resultados da varredura em um banco de dados SQL. Este banco de dados pode ser um banco de dados do Microsoft MSDE ou SQL Server. Para coletar as vulnerabilidades, o QRadar se conecta ao banco de dados remoto para localizar os resultados da varredura mais recentes para um determinado endereço IP. Os dados retornados atualizam o perfil do ativo no QRadar com o endereço IP do ativo, serviços descobertos e vulnerabilidades. O QRadar suporta o software de scanner SecureScout versão 2.6.

É recomendado que os administradores criem um usuário especial em seu banco de dados SecureScout para o QRadar pesquisar dados de vulnerabilidade.

O usuário do banco de dados criado deve ter permissões de seleção para as seguintes tabelas:

- HOST
- JOB
- JOB_HOST
- SERVICE
- TCRESULT
- TESTCASE
- PROPERTY
- PROP_VALUE
- WKS
- IPSORT – O usuário do banco de dados deve ter permissão de execução para esta tabela.

Para incluir uma configuração do scanner, consulte “Incluindo uma varredura netVigilance SecureScout”.

## Incluindo uma varredura netVigilance SecureScout

Os administradores podem incluir um scanner SecureScout para consultar dados de vulnerabilidades com o JDBC.

### Antes de Iniciar

Para consultar dados de vulnerabilidade do QRadar, você deverá ter o acesso administrativo apropriado para pesquisar o scanner SecureScout com JDBC. Os administradores também devem assegurar que os firewalls, incluindo o firewall no host SecureScout, permitam uma conexão do host gerenciado responsável pela varredura com o scanner SecureScout.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.

© Copyright IBM Corp. 2007, 2015

3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu servidor SecureScout.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **SecureScout Scanner**.
7. No campo **Nome do banco de dados**, digite o endereço IP ou o nome do host do servidor de banco de SecureScout que contém o servidor SQL.
8. No campo **Nome de Login**, digite o nome de usuário necessário para acessar o banco de dados SQL do scanner SecureScout.
9. Opcional. No campo **Senha de login**, digite a senha necessária para acessar o banco de dados SQL do scanner SecureScout.
10. No campo **Nome do banco de dados**, digite `SCE`.
11. No campo **Porta do Banco de Dados**, digite a porta TCP que você deseja que o servidor SQL monitore as conexões. O valor padrão é 1433.
12. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
13. Clique em **Salvar**.
14. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 19. Visão geral do scanner Nmap

O QRadar utiliza o SSH para se comunicar com o servidor Nmap para iniciar varreduras do Nmap remoto ou fazer o download dos resultados de varredura do Nmap concluídos.

**Restrição:** Embora exista um binário NMap em cada host do QRadar, ele é reservado apenas para uso interno do QRadar. A configuração do scanner de vulnerabilidade do NMap para usar um host gerenciado de QRadar Console ou QRadar como o scanner NMap remoto não é suportada e pode causar instabilidades.

Quando os administradores configuram uma varredura do Nmap, uma conta do usuário Nmap específica pode ser criada para o sistema do QRadar. Uma conta de usuário exclusiva assegura que o QRadar possui as credenciais necessárias para efetuar login e estabelecer comunicação com o servidor Nmap. Após a criação da conta do usuário ser concluída, os administradores poderão testar a conexão do QRadar para o cliente Nmap com SSH para verificar as credenciais do usuário. Este teste assegura que cada sistema é capaz se comunicar antes da tentativa do sistema de fazer o download de dados de varredura de vulnerabilidade ou iniciar uma varredura em tempo real.

As opções a seguir estão disponíveis para coleta de dados de informações de vulnerabilidade a partir de scanners Nmap:

- Varredura ativa remota. As varreduras em tempo real utilizam o arquivo binário de Nmap para iniciar remotamente as varreduras. Após a varredura ativa ser concluída, os dados serão importados por meio do SSH. Consulte “Incluindo uma varredura remota em tempo real de Nmap” na página 65.
- Importação dos resultados remotos. Os dados do resultado de uma varredura concluída anteriormente são importados por meio do SSH. Consulte “Incluindo uma importação de resultados remotos de Nmap”

## Incluindo uma importação de resultados remotos de Nmap

Uma importação de resultados remotos recupera relatórios de varreduras Nmap concluídas por meio de SSH.

### Sobre Esta Tarefa

As varreduras devem ser geradas no formato XML utilizando a opção `-oX` em seu scanner Nmap. Após incluir seu scanner Nmap, você deverá designar um planejamento de varredura para especificar a frequência com que os dados de vulnerabilidade são importados do scanner.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do Scanner**, digite um nome para identificar seu scanner de Nmap.

© Copyright IBM Corp. 2007, 2015

5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Nessus Scanner**.
7. Na lista **Tipo de coleção**, selecione **Importação de resultados remota**.
8. No campo **Nome do host do servidor**, digite o nome do host ou o endereço IP do sistema remoto que hospeda o cliente Nmap. Sugerimos que os administradores hospedem o Nmap em um sistema baseado em UNIX com SSH ativado.
9. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
|---|---|
| **Nome do usuário de login** | Para autenticar com um nome de usuário e senha:<br>1. No campo **Nome de usuário do servidor**, digite o nome de usuário necessário para acessar o sistema remoto que hospeda o cliente NMap.<br>2. No campo **Senha de login**, digite a senha associada ao nome de usuário.<br><br>A senha não deve conter o caractere ! . Este caractere pode causar falhas de autenticação por meio de SSH.<br><br>Se o scanner estiver configurado para utilizar uma senha, o servidor do scanner SSH que se conecta ao QRadar deverá suportar autenticação de senha.<br><br>Se não suportar, a autenticação SSH para o scanner falhará. Assegure-se de que a seguinte linha seja exibida em seu arquivo `/etc/ssh/sshd_config`: `PasswordAuthentication yes`.<br><br>Se o servidor do scanner não utilizar OpenSSH, consulte a documentação do fornecedor para obter as informações de configuração do scanner. |
| **Ativar autorização de chave** | Para autenticar com um arquivo de autenticação baseado em chave:<br>1. Marque a caixa de seleção **Ativar autenticação de chave**.<br>2. No campo **Arquivo-chave privado**, digite o caminho do diretório para o arquivo-chave.<br><br>O diretório padrão para o arquivo-chave é `/opt/qradar/conf/vis.ssh.key`. Se um arquivo-chave não existir, você deverá criar o arquivo vis.ssh.key. |

10. No campo **Pasta remota**, digite o local do diretório dos arquivos de resultados de varredura.
11. No campo **Padrão de arquivo remoto**, digite uma expressão regular (regex) necessária para filtrar a lista de arquivos especificados na pasta remota. Todos os arquivos correspondentes são incluídos no processamento. O padrão regex

para recuperar resultados do Nmap é `.*\.xml`. O padrão `.*\.xml` importa todos os arquivos de resultados xml na pasta remota. Os relatórios de varredura importados e processados não são excluídos da pasta remota. É recomendado planejar uma tarefa cron para excluir relatórios de varredura processados anteriormente.

12. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
13. Clique em **Salvar**.
14. Na guia **Administrador**, clique em **Implementar Mudanças**.

### O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93

## Incluindo uma varredura remota em tempo real de Nmap

O QRadar monitora o status da varredura em tempo real em andamento e espera o servidor Nmap concluir a varredura. Após a varredura ser concluída, os resultados de vulnerabilidade serão transferidos por download por meio de SSH.

### Sobre Esta Tarefa

Vários tipos de varredura de porta de Nmap necessitam que o Nmap seja executado como um usuário raiz. Portanto, o QRadar deverá ter acesso raiz ou a caixa de seleção **Detecção de S.O.** deverá ser desmarcada. Para executar varreduras de Nmap com a Detecção de SO ativada, você deve fornecer credenciais de acesso raiz para QRadar ao incluir o scanner. Como alternativa, é possível que seu administrador configure o Nmap binário com raiz setuid. Consulte seu administrador de Nmap para obter mais informações.

**Restrição:** Embora exista um binário NMap em cada host do QRadar, ele é reservado apenas para uso interno do QRadar. A configuração do scanner de vulnerabilidade do NMap para usar um host gerenciado de QRadar Console ou QRadar como o scanner NMap remoto não é suportada e pode causar instabilidades.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do Scanner**, digite um nome para identificar seu scanner de Nmap.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Scanner de Nmap**.
7. Na lista **Tipo de varredura**, selecione **Varredura ativa remota**.
8. No campo **Nome do Host do Servidor**, digite o endereço IP ou nome do host do servidor Nmap.

9. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
| --- | --- |
| **Nome de Usuário do Servidor** | Para autenticar com um nome de usuário e senha:<br>1. No campo **Nome de Usuário do Servidor**, digite o nome de usuário necessário para acessar o sistema remoto que hospeda o cliente Nmap usando SSH.<br>2. No campo **Senha de login**, digite a senha associada ao nome de usuário.<br><br>Se a caixa de seleção **Detecção de S.O.** estiver marcada, o nome de usuário deverá ter privilégios de administrador. |
| **Ativar autorização de chave** | Para autenticar com um arquivo de autenticação baseado em chave:<br>1. Marque a caixa de seleção **Ativar autenticação de chave**.<br>2. No campo **Arquivo-chave privado**, digite o caminho do diretório para o arquivo-chave.<br><br>O diretório padrão para o arquivo-chave é `/opt/qradar/conf/vis.ssh.key`. Se um arquivo-chave não existir, você deverá criar o arquivo vis.ssh.key.<br><br>Se o scanner estiver configurado para utilizar uma senha, o servidor do scanner SSH que se conecta ao QRadar deverá suportar autenticação de senha.<br><br>Se não suportar, a autenticação SSH para o scanner falhará. Assegure-se de que a seguinte linha seja exibida em seu arquivo `/etc/ssh/sshd_config`: `PasswordAuthentication yes`.<br><br>Se o servidor do scanner não utilizar OpenSSH, consulte a documentação do fornecedor para obter as informações de configuração do scanner. |

10. No campo **Nmap Executável**, digite o caminho do diretório completo e nome do arquivo do arquivo binário Nmap. O caminho do diretório padrão para o arquivo binário é `/usr/bin/Nmap`.
11. Marque uma opção para a caixa de seleção **Desativar Ping**. Em algumas redes, o protocolo ICMP é parcialmente ou completamente desativado. Nas situações em que o ICMP não estiver ativado, será possível marcar essa caixa de seleção para ativar os pings do ICMP para aprimorar a precisão da varredura. Por padrão, a caixa de seleção é desmarcada.
12. Selecione uma opção para a caixa de seleção **Detecção de S.O.**:
    - Selecione essa caixa de seleção para ativar a detecção do sistema operacional no Nmap. Privilégios de administrador deverão ser fornecidos para o scanner para utilizar essa opção.

- Limpe essa caixa de seleção para receber resultados de Nmap sem a detecção do sistema operacional.

13. Na lista **Tempo limite máx. de RTT**, selecione um valor de tempo limite. O valor de tempo limite determina se uma varredura deve ser interrompida ou emitida novamente devido à latência entre o scanner e o destino de varredura. O valor padrão é 300 milissegundos (ms). Se você especificar um período de tempo limite de 50 milissegundos, será recomendado que os dispositivos que serão varridos estejam na rede local. Os dispositivos nas redes remotas podem utilizar um valor de tempo limite de 1 segundo.
14. Selecione uma opção na lista **Modelo sincronização**. As opções incluem:
    - Paranoid – Essa opção produz uma avaliação lenta não invasiva.
    - Sneaky – Essa opção produz uma avaliação lenta não invasiva, porém aguarda 15 segundos entre as varreduras.
    - Polite - Esta opção é mais lenta que o normal e é destinada a diminuir a carga na rede.
    - Normal - Esta opção é o comportamento padrão da varredura.
    - Aggressive – Esta opção é mais rápida do que uma varredura normal e consome mais recursos.
    - Insane – Esta opção não é tão precisa quanto varreduras lentas e é adequada apenas para redes muito rápidas.
    -
15. No campo **Máscara CIDR**, digite o tamanho da sub-rede varrida. O valor especificado para a máscara representa a maior parte da sub-rede que o scanner pode varrer de uma vez. A máscara segmenta a varredura para otimizar o desempenho da varredura.
16. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
17. Clique em **Salvar**.
18. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93

# Capítulo 20. Visão geral do Outpost24 Vulnerability Scanner

O IBM Security QRadar usa HTTPS para se comunicar com a API do Outpost24 Vulnerability Scanner, para fazer o download de ativos e de dados de vulnerabilidade a partir de varreduras concluídas anteriormente.

A tabela a seguir lista as especificações para o Outpost24 Vulnerability Scanner:

*Tabela 3. Especificações do Outpost24 Vulnerability Scanner*

| Especificação | Valor |
|---|---|
| Nome do scanner | Outpost24 Vulnerability Scanner |
| Versões suportadas | HIAB V4.1<br><br>OutScan V4.1 |
| Tipo de conexão | HTTPS |
| Mais informações | Website do Outpost24 (http://www.outpost24.com/) |

## Certificados do servidor

Antes de incluir um scanner, é necessário um certificado do servidor para suportar conexões HTTPS. O QRadar suporta certificados com as seguintes extensões de arquivos: `.crt`, `.cert` ou `.der`. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando Secure Copy (SCP) ou Secure File Transfer Protocol (SFTP).
- Para fazer download automaticamente do certificado para o diretório `/opt/qradar/conf/trusted_certificates`, execute SSH no Console ou host gerenciado e digite o seguinte comando:

  `/opt/qradar/bin/getcert.sh <IP_or_Hostname> <optional_port_(443_default)>`.

## Instalar o Java Cryptography Extension irrestrito

Os certificados padrão que são usados por OUTSCAN e HIAB usam chaves de 2048 bits. Como resultado disso, é necessário modificar a criptografia de Java quando os certificados forem usados. Para obter informações adicionais, consulte "Instalando o Java Cryptography Extension irrestrito" na página 1.

## Etapas de configuração

Para configurar o QRadar para fazer o download de ativos e de dados de vulnerabilidade a partir do Outpost24 Vulnerability Scanner, conclua as etapas a seguir:

1. Se as atualizações automáticas não forem ativadas, faça o download e instale a versão mais recente de RPM do Outpost24 Vulnerability Scanner em seu sistema QRadar.
2. No Outpost24 Vulnerability Scanner, crie um token do aplicativo para QRadar.

© Copyright IBM Corp. 2007, 2015

3. No QRadar Console, inclua o Outpost24 Vulnerability Scanner. Configure todos os parâmetros necessários e use a tabela a seguir para identificar os valores específicos do Outpost24:

*Tabela 4. Parâmetros do Outpost24 Vulnerability Scanner*

| Parâmetro | Valor |
|---|---|
| Tipo | Outpost24 Vulnerability Scanner |
| Nome do Host do Servidor | O nome do host ou o endereço IP do dispositivo Outpost24 Vulnerability Scanner. |
| Porta | 443 |
| Token da API | Deve-se usar o token da API criado no dispositivo Outpost24 Vulnerability Scanner. |

4. Planeje uma varredura.

**Tarefas relacionadas**:

"Criando um token de autenticação da API do Outpost24 para QRadar"
Para ativar o IBM Security QRadar para usar a API do Outpost24 para fazer o download de ativos e de dados de vulnerabilidade, crie um Token de Acesso ao Aplicativo no Outpost24 Vulnerability Scanner.

Capítulo 26, "Planejando uma varredura de vulnerabilidade", na página 93
Os planejamentos de varredura são intervalos designados para os scanners que determinam quando os dados de avaliação de vulnerabilidades são importados de dispositivos de varredura externos em sua rede. Os planejamentos de varredura também podem definir intervalos ou sub-redes do CIDR que são incluídos na importação de dados quando a importação de dados de vulnerabilidade ocorre.

## Criando um token de autenticação da API do Outpost24 para QRadar

Para ativar o IBM Security QRadar para usar a API do Outpost24 para fazer o download de ativos e de dados de vulnerabilidade, crie um Token de Acesso ao Aplicativo no Outpost24 Vulnerability Scanner.

### Procedimento

1. Efetue login no Outpost24 Vulnerability Scanner.
2. Selecione **Configurações > Conta**.
3. Clique na guia **Política de Segurança**.
4. Na área de janela Tokens de Acesso ao Aplicativo, clique em **Novo**.
5. Na janela Mantendo o Token de Acesso ao Aplicativo, assegure-se de que a caixa de seleção **Ativo** esteja marcada.
6. Digite um nome para o aplicativo, por exemplo, QRadar.
7. Configure as restrições de IP e os direitos de acesso de usuário.
8. Clique em **Salvar**.
9. Copie o token de autenticação de 64 caracteres em um arquivo.

### O que Fazer Depois

No sistema QRadar, inclua o Outpost24 Vulnerability Scanner.

# Capítulo 21. Positive Technologies MaxPatrol

É possível incluir um scanner Positive Technologies MaxPatrol na implementação do IBM Security QRadar.

Em intervalos determinados por um planejamento de varredura, o QRadar importa resultados do arquivo XML que contêm as vulnerabilidades do MaxPatrol. O scanner MaxPatrol importa arquivos de um servidor remoto que contém os dados de varredura exportados.

A tabela a seguir fornece detalhes do scanner Positive Technologies MaxPatrol:

*Tabela 5. Detalhes do scanner Positive Technologies MaxPatrol*

| | |
|---|---|
| Fornecedor | Positive Technologies |
| Nome do scanner | MaxPatrol |
| Versões suportadas | V8.24.4 e mais recente |

Use os procedimentos a seguir para integrar o Positive Technologies MaxPatrol ao QRadar

1. Configure o scanner Positive Technologies MaxPatrol para exportar relatórios de varredura. Ative as exportações de vulnerabilidade do arquivo XML compatíveis com o QRadar. Para obter os arquivos e os procedimentos de configuração necessários, entre em contato com o Suporte ao cliente da Positive Technologies.
2. No QRadar Console, inclua um scanner Positive Technologies MaxPatrol.
3. No seu QRadar Console, crie um planejamento de varredura para importar os dados do resultado da varredura.

## Integrando o Positive Technologies MaxPatrol ao QRadar

Procedimentos necessários para integrar o Positive Technologies MaxPatrol ao QRadar.

### Procedimento

1. Configure o scanner Positive Technologies MaxPatrol para exportar relatórios de varredura. Ative as exportações de vulnerabilidade do arquivo XML compatíveis com o QRadar. Para obter os arquivos e os procedimentos de configuração necessários, entre em contato com o Suporte ao cliente da Positive Technologies.
2. No QRadar Console, inclua um scanner Positive Technologies MaxPatrol.
3. No seu QRadar Console, crie um planejamento de varredura para importar os dados do resultado da varredura.

## Incluindo um scanner Positive Technologies MaxPatrol

Inclua um scanner Positive Technologies MaxPatrol na implementação do IBM Security QRadar.

© Copyright IBM Corp. 2007, 2015

## Antes de Iniciar

Assegure-se de que os pré-requisitos a seguir sejam atendidos:

- O sistema Positive Technologies MaxPatrol está configurado para exportar relatórios de vulnerabilidade XML compatíveis com o QRadar.
- Um SFTP ou SMB share está configurado e contém os relatórios de vulnerabilidade XML exportados.

## Sobre Esta Tarefa

A tabela a seguir descreve os parâmetros do scanner Positive Technologies MaxPatrol quando SFTP é selecionado como o método de importação:

*Tabela 6. Propriedades de SFTP do scanner Positive Technologies MaxPatrol*

| Parâmetro | Descrição |
|---|---|
| Nome do Host Remoto | O endereço IP ou o nome do host do servidor que tem o arquivo de resultados da varredura. |
| Nome do usuário de login | O nome de usuário usado pelo QRadar para efetuar login no servidor. |
| Ativar autenticação de chave | Especifica que o QRadar é autenticado com um arquivo de autenticação baseada em chave. |
| Diretório remoto | A localização dos arquivos de resultados da varredura. |
| Arquivo de chave privado | O caminho completo para o arquivo que contém a chave privada. Se um arquivo-chave não existir, você deverá criar o arquivo `vis.ssh.key`. |
| Padrão de nome do arquivo | A expressão regular (regex) necessária para filtrar a lista de arquivos no Diretório remoto. O padrão `.*\.xml` importa todos os arquivos XML no diretório remoto. |

A tabela a seguir descreve os parâmetros do scanner Positive Technologies MaxPatrol quando SMB Share é selecionado como o método de importação:

*Tabela 7. Propriedades de SMB Share do scanner Positive Technologies MaxPatrol*

| Parâmetro | Descrição |
|---|---|
| Nome do host | O endereço IP ou o nome do host do SMB Share. |
| Nome do usuário de login | O nome de usuário usado pelo QRadar para efetuar login no SMB Share. |
| Domínio | O domínio usado para se conectar ao SMB Share. |
| Caminho de pasta do SMB | O caminho completo para o compartilhamento a partir da raiz do host SMB. Use barras, por exemplo, `/share/logs/`. |

*Tabela 7. Propriedades de SMB Share do scanner Positive Technologies MaxPatrol (continuação)*

| Parâmetro | Descrição |
|---|---|
| Padrão de nome do arquivo | A expressão regular (regex) necessária para filtrar a lista de arquivos no Diretório remoto. O padrão `.*\.xml` importa todos os arquivos xml no diretório remoto. |

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o scanner Positive Technologies MaxPatrol.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Scanner Positive Technologies MaxPatrol**.
7. Configure os parâmetros.
8. Configure um intervalo do CIDR para o scanner.
9. Clique em **Salvar**.
10. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Para obter mais informações sobre como criar um planejamento de varredura, consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 22. Visão geral do scanner Qualys

O QRadar pode recuperar informações de vulnerabilidade do QualysGuard Host Detection List API ou fazer o download de relatórios de varredura diretamente de um dispositivo QualysGuard. O QRadar suporta integração com dispositivos QualysGuard que usam software da versão 4.7 à 7.10.

### Qualys Detection Scanners

Inclua um Qualys Detection Scanner se desejar usar o QualysGuard Host Detection List API para consultar diversos relatórios de varredura para coletar dados de vulnerabilidade para ativos. Os dados retornados pela consulta contêm as vulnerabilidades como números de identificação, que o QRadar compara com o Qualys Vulnerability Knowledge Base mais recente. O Qualys Detection Scanner não suporta varreduras ativas, mas consegue recuperar informações de vulnerabilidade agregadas em diversos relatórios de varredura. O QRadar suporta parâmetros de procura chave para filtrar as informações que você deseja coletar. Também é possível configurar a frequência com que o QRadar irá recuperar e armazenar em cache o Qualys Vulnerability Knowledge Base.

### Scanners Qualys

Inclua um scanner Qualys se desejar importar relatórios específicos em tempo real ou importados que incluam dados de varredura ou de ativos. Ao incluir um scanner Qualys, é possível escolher entre os tipos de coleção a seguir:

- Planejada em tempo real - Relatório de varredura
- Importação planejada - Relatório de dados de ativo
- Importação planejada - Relatório de varredura

## Incluindo um scanner Qualys Detection

Inclua um scanner Qualys detection para usar uma API para consultar diversos relatórios de varredura e coletar dados de vulnerabilidade para ativos. O scanner Qualys detection usa o QualysGuard Host Detection List API.

### Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. Faça o download do certificado a partir da URL do Qualys para sua região.

**Exemplos:**

- Site americano da API de Qualys (http://qualysapi.qualys.com)
- Site Europeu de Qualys (http://qualysapi.qualys.eu)

O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.

© Copyright IBM Corp. 2007, 2015

- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Qualys detection.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Qualys Detection Scanner**.
7. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do host do servidor Qualys** | O nome completo do domínio (FQDN) ou o endereço IP do console de gerenciamento QualysGuard. Se você digitar o nome completo do domínio (FQDN), use o nome do host e não a URL, por exemplo, digite `qualysapi.qualys.com` ou `qualysapi.qualys.eu`. |
| **Nome de usuário do Qualys** | O nome de usuário especificado deve ter acesso para fazer o download da Base de Conhecimento do Qualys Vulnerability. Para obter mais informações sobre como atualizar contas do usuário do Qualys, consulte a documentação do Qualys. |
| **Filtro do sistema operacional** | A expressão regular (regex) para filtrar os dados de varredura pelo sistema operacional. |
| **Nomes do grupo de recursos** | Uma lista separada por vírgula para consultar os endereços IP pelo nome do grupo de recursos. |
| **Filtro de tempo de varredura do host (dias)** | Os tempos de varredura do host que forem mais antigos que o número de dias especificado serão excluídos dos resultados retornados pelo Qualys. |
| **Período de retenção de vulnerabilidade do Qualys (dias)** | O número de dias que você deseja que o QRadar armazene o Qualys Vulnerability Knowledge Base. Se uma varredura estiver planejada e o período de retenção tiver expirado, o sistema fará o download de uma atualização.<br><br>**Atenção:** Depois de criar esse scanner pela primeira vez, as atualizações subsequentes nesse período de retenção podem não entrar em vigor. Para que essa mudança entre em vigor após a criação inicial, você pode precisar excluir ou limpar o cache. |

| Parâmetro | Descrição |
| --- | --- |
| **Forçar a atualização de vulnerabilidade do Qualys** | Força o sistema a atualizar para o Qualys Vulnerability Knowledge Base em cada varredura planejada. |

8. Opcional: Para configurar um proxy, marque a caixa de seleção **Usar proxy** e configure as credenciais do servidor proxy.
9. Opcional: Para configurar um certificado de cliente, marque a caixa de seleção **Usar certificado do cliente** e configure os campos **Caminho do arquivo de certificado** e **Senha do certificado**.
10. Opcional: Para configurar um intervalo do CIDR para seu scanner, configure os parâmetros de intervalo do CIDR e clique em **Incluir**.

    **Restrição:** A API QualysGuard Host Detection List aceita apenas os intervalos de CIDR para um máximo de classe A ou /8 única e não aceita o endereço IP do host local (127.0.0.1).
11. Clique em **Salvar**.
12. Na guia **Administrador**, clique em **Implementar Mudanças**. Mudanças na configuração do proxy requerem uma **Configuração de implementação completa**.

# Incluindo uma varredura ativa planejada Qualys

Inclua uma varredura planejada em tempo real para iniciar varreduras pré-configuradas no Scanner Qualys e, em seguida, colete os resultados da varredura concluída.

## Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Qualys.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Qualys Scanner**.
7. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
| --- | --- |
| **Nome do host do servidor Qualys** | O nome completo do domínio (FQDN) ou o endereço IP do console de gerenciamento QualysGuard. Se você digitar o nome completo do domínio (FQDN), use o nome do host e não a URL, por exemplo, digite `qualysapi.qualys.com` ou `qualysapi.qualys.eu`. |
| **Nome de usuário do Qualys** | O nome de usuário especificado deve ter acesso para fazer o download da Base de Conhecimento do Qualys Vulnerability. Para obter mais informações sobre como atualizar contas do usuário do Qualys, consulte a documentação do Qualys. |

8. Opcional: Para configurar um proxy, marque a caixa de seleção **Usar proxy** e configure as credenciais do servidor proxy.
9. Opcional: Para configurar um certificado de cliente, marque a caixa de seleção **Usar certificado do cliente** e configure os campos **Caminho do arquivo de certificado** e **Senha do certificado**.
10. Na lista **Tipo de coleção**, selecione **Ativa Planejada - Relatório de Varredura**.
11. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
| --- | --- |
| **Nome do scanner** | Para obter o nome do scanner, entre em contato com o administrador da rede. O dispositivo de varredura pública deve limpar o nome deste campo. |
| **Perfis de opção** | O nome do perfil de opção que determina qual varredura em tempo real será iniciada. As varreduras em tempo real suportam apenas um nome de perfil de opção por configuração de scanner. |

12. Opcional: Para configurar um intervalo do CIDR para seu scanner, configure os parâmetros de intervalo do CIDR e clique em **Incluir**.
13. Clique em **Salvar**.
14. Na guia **Administrador**, clique em **Implementar Mudanças**. Mudanças na configuração do proxy requerem uma **Configuração de implementação completa**.

## Incluindo um relatório de dados de ativo de importação planejada do Qualys

Inclua uma importação de dados do relatório de ativos para planejar o QRadar para recuperar um único relatório de ativos do scanner Qualys.

### Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório /opt/qradar/conf/trusted_certificates usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: /opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório /opt/qradar/conf/trusted_certificates no formato apropriado.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Qualys.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Qualys Scanner**.
7. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do host do servidor Qualys** | O nome completo do domínio (FQDN) ou o endereço IP do console de gerenciamento QualysGuard. Se você digitar o nome completo do domínio (FQDN), use o nome do host e não a URL, por exemplo, digite qualysapi.qualys.com ou qualysapi.qualys.eu. |
| **Nome de usuário do Qualys** | O nome de usuário especificado deve ter acesso para fazer o download da Base de Conhecimento do Qualys Vulnerability. Para obter mais informações sobre como atualizar contas do usuário do Qualys, consulte a documentação do Qualys. |

8. Opcional: Para configurar um proxy, marque a caixa de seleção **Usar proxy** e configure as credenciais do servidor proxy.
9. Opcional: Para configurar um certificado de cliente, marque a caixa de seleção **Usar certificado do cliente** e configure os campos **Caminho do arquivo de certificado** e **Senha do certificado**.
10. Na lista **Tipo de coleção**, selecione **Importação Planejada - Relatório de Dados de Ativo**.
11. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Título do modelo de relatório** | O título do modelo de relatório para substituir o título do relatório de dados de ativo padrão. |
| **Idade máx. dos relatórios (dias)** | Arquivos que forem mais antigos do que registro de data e hora especificado no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. |

| Parâmetro | Descrição |
| --- | --- |
| **Arquivo de importação** | O caminho do diretório para fazer o download e importar um único relatório de ativos do Qualys. Se você especificar um local de arquivo de importação, o QRadar fará o download do conteúdo do relatório de ativos do Qualys para um diretório local e importará o arquivo. Se esse campo ficar em branco ou se o arquivo ou o diretório não puder ser localizado, o scanner Qualys usará a API para recuperar o relatório de ativos usando o valor no campo **Título do modelo de relatório**. |

12. Opcional: Para configurar um intervalo do CIDR para seu scanner, configure os parâmetros de intervalo do CIDR e clique em **Incluir**.
13. Opcional: Para que o QRadar possa criar vulnerabilidades customizadas a partir dos dados de varredura em tempo real, marque a caixa de seleção **Ativar criação de vulnerabilidade customizada** e selecione as opções que deseja incluir.
14. Clique em **Salvar**.
15. Na guia **Administrador**, clique em **Implementar Mudanças**. Mudanças na configuração do proxy requerem uma **Configuração de implementação completa**.

## Incluindo um relatório de varredura de importação planejada do Qualys

Inclua uma importação de dados do relatório de varredura para planejar o QRadar para recuperar relatórios de varredura a partir do scanner Qualys.

### Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Qualys.
5. Na lista **Host gerenciado**, selecione o host gerenciado que gerencia a importação do scanner.

6. Na lista **Tipo**, selecione **Qualys Scanner**.
7. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Nome do host do servidor Qualys** | O nome completo do domínio (FQDN) ou o endereço IP do console de gerenciamento QualysGuard. Se você digitar o nome completo do domínio (FQDN), use o nome do host e não a URL, por exemplo, digite `qualysapi.qualys.com` ou `qualysapi.qualys.eu`. |
| **Nome de usuário do Qualys** | O nome de usuário especificado deve ter acesso para fazer o download da Base de Conhecimento do Qualys Vulnerability. Para obter mais informações sobre como atualizar contas do usuário do Qualys, consulte a documentação do Qualys. |

8. Opcional: Para configurar um proxy, marque a caixa de seleção **Usar proxy** e configure as credenciais do servidor proxy.
9. Opcional: Para configurar um certificado de cliente, marque a caixa de seleção **Usar certificado do cliente** e configure os campos **Caminho do arquivo de certificado** e **Senha do certificado**.
10. Na lista **Tipo de coleção**, selecione **Importação Planejada - Relatório de Varredura**.
11. Configure os parâmetros a seguir:

| Parâmetro | Descrição |
|---|---|
| **Perfis de opção** | O nome do perfil de opção para determinar qual varredura iniciar. O QRadar recupera os dados completos da varredura ativa após a varredura ativa ser concluída. As varreduras em tempo real suportam apenas um nome de perfil de opção por configuração de scanner. |
| **Padrão de nome do relatório de varredura** | A expressão regular (regex) para filtrar a lista de relatórios de varredura. |
| **Idade máx. dos relatórios (dias)** | Arquivos que forem mais antigos do que registro de data e hora especificado no arquivo de relatório serão excluídos quando a varredura de planejamento for iniciada. |
| **Arquivo de importação** | O caminho do diretório para fazer o download e importar um único relatório de varredura do Qualys, por exemplo, `/qualys_logs/test_report.xml`. Se você especificar um local de arquivo de importação, o QRadar fará o download do conteúdo do relatório de varredura do Qualys para um diretório local e importará o arquivo. Se esse campo ficar em branco ou se o arquivo ou o diretório não puder ser localizado, o scanner Qualys usará a API para recuperar o relatório de varredura usando o valor no campo **Perfil de opções**. |

12. Opcional: Para configurar um intervalo do CIDR para seu scanner, configure os parâmetros de intervalo do CIDR e clique em **Incluir**.
13. Opcional: Para que o QRadar possa criar vulnerabilidades customizadas a partir dos dados de varredura em tempo real, marque a caixa de seleção **Ativar criação de vulnerabilidade customizada** e selecione as opções que deseja incluir.
14. Clique em **Salvar**.
15. Na guia **Administrador**, clique em **Implementar Mudanças**. Quaisquer mudanças na configuração requererem clicar em **Implementar configuração completa**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 23. Visão geral de scanners Rapid7 NeXpose

Os scanners NeXpose Rapid7 podem fornecer relatórios de dados do site para o QRadar para importar as vulnerabilidades conhecidas sobre sua rede.

As seguintes opções estão disponíveis para coletar informações de vulnerabilidade a partir de scanners Rapid7 NeXpose:

- Site de importação de relatórios ad hoc por meio da API Rapid7. Consulte "Incluindo uma importação de site da API do scanner Rapid7 NeXpose".
- Site de importação de um arquivo local. Consulte "Incluindo uma importação de arquivo local do scanner Rapid7 NeXpose" na página 84

## Incluindo uma importação de site da API do scanner Rapid7 NeXpose

As importações da API permitem que o QRadar importe os dados do relatório ad hoc de vulnerabilidades em seus sites a partir de scanners Rapid7 NeXpose. Os dados do site importados pelo planejamento de varredura dependem do nome do site.

### Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Rapid7 NeXpose.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **Rapid7 Nexpose Scanner**.
7. Na lista **Tipo de Importação**, selecione **Dados do Site de Importação - Relatório Adhoc por meio da API**.
8. No campo **Nome do host remoto**, digite o endereço IP ou o nome do host do scanner Rapid7 NeXpose.
9. No campo **Nome do usuário de login**, digite o nome do usuário para acessar o scanner Rapid7 NeXpose. O login deve ser um usuário válido. O nome de usuário pode ser obtido a partir da interface com o usuário Rapid7 NeXpose ou do administrador Rapid7 NeXpose.

© Copyright IBM Corp. 2007, 2015

10. No campo **Senha de login**, digite a senha para acessar o scanner Rapid7 NeXpose.
11. No campo **Porta**, digite a porta usada para conectar ao Rapid7 NeXpose Security Console. O número da porta é a mesma porta para se conectar à interface com o usuário do Rapid7 NeXpose.
12. No campo **Padrão de nome de site**, digite a expressão regular (regex) para determinar quais sites Rapid7 NeXpose serão incluídos na varredura. Todos os sites que corresponderem ao padrão serão incluídos quando o planejamento de varredura for iniciado. A expressão regular de valor padrão é `.*` para importar todos os nomes de site.
13. No campo **Porta**, digite a porta usada para conectar ao Rapid7 NeXpose Security Console.
14. No campo **Tempo limite de cache (minutos)**, digite o período de tempo em que os dados do último relatório de varredura gerado são armazenados no cache. Se o tempo limite de cache expirar, os novos dados de vulnerabilidade serão solicitados da API quando a varredura planejada for iniciada.
15. Para configurar um intervalo do CIDR para o scanner:
    a. No campo de texto, digite o intervalo do CIDR para a varredura ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
16. Clique em **Salvar**.
17. Na guia **Administrador**, clique em **Implementar Mudanças**.

### O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

## Incluindo uma importação de arquivo local do scanner Rapid7 NeXpose

Importar dados de vulnerabilidade de site utilizando os arquivos locais permite que o QRadar importe varreduras de vulnerabilidade concluídas com base nos relatórios de varredura concluída copiados do seu scanner Rapid7 NeXpose para o QRadar.

### Antes de Iniciar

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

## Sobre Esta Tarefa

As importações de arquivo local coletam vulnerabilidades de um site a partir de um arquivo local que é transferido por download. O arquivo XML do Rapid7 NeXpose que contém as informações de site e de vulnerabilidade deve ser copiado de seu dispositivo Rapid7 NeXpose para o Console ou host gerenciado que você especifica quando o scanner é incluído no QRadar. O diretório no host gerenciado deverá existir antes que o sistema possa copiar os relatórios do site para o host gerenciado. Os administradores podem usar Secure Copy (SCP) ou Secure File Transfer Protocol (SFTP) para copiar os arquivos de site para o host gerenciado.

**Nota:** Os arquivos do site que são importados não são excluídos da pasta de importação, mas são renomeados para `.processed0`. Os administradores podem criar uma tarefa cron para excluir arquivos do site processados anteriormente, se necessário.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner Rapid7 NeXpose.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione o **Rapid7 Nexpose Scanner**.
7. Na lista **Tipo de Importação**, selecione **Dados do Site de Importação - Arquivo Local**.
8. No campo **Diretório de importação**, digite o caminho do diretório para os dados de vulnerabilidade XML. Se você especificar uma pasta de importação, os dados de vulnerabilidade deverão ser movidos do scanner Rapid7 NeXpose para o QRadar.
9. No campo **Padrão de nome de importação**, digite uma expressão regular (regex) padrão para determinar quais arquivos XML Rapid7 NeXpose serão incluídos no relatório de varredura. Todos os nomes de arquivo que corresponderem ao padrão regex serão incluídos ao importar o relatório de varredura vulnerabilidade. Você deve utilizar um padrão regex válido neste campo. O valor padrão `.*\.xml` importa todos os arquivos da pasta de importação.
10. Para configurar um intervalo do CIDR para seu scanner:
    a. No campo de texto, digite o intervalo do CIDR que você deseja que este scanner considere ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
11. Clique em **Salvar**.
12. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 24. Visão geral do scanner SAINT

Os administradores podem integrar seus scanners vulnerabilidade Security Administrator's Integrated Network Tool (SAINT) com o QRadar para dispositivos SAINT com o software V7.4.x .

Os administradores podem incluir scanners SAINT no QRadar para coletar dados de vulnerabilidade SAINT para hosts, incluindo informações de endereços MAC, portas e serviços. O scanner SAINT identifica vulnerabilidades com base no nível de varredura especificado e utiliza o SAINTwriter para gerar relatórios customizados. Portanto, seu sistema SAINT deve incluir um modelo de relatório e varreduras SAINTwriter customizados que são executados regularmente para assegurar que os resultados sejam atuais.

Os seguintes tipos de coleta de dados são suportados para as configurações do scanner SAINT:

- Varredura Ativa – Inicia varreduras remotas no scanner SAINT. Uma varredura ativa gera um relatório de vulnerabilidade com base no nome da sessão, que é importado após a varredura ser concluída.
- Somente relatório - Importe relatórios concluídos a partir do scanner SAINT com base no nome da sessão.

Para configurar um modelo para seu relatório, consulte “Configurando um modelo SAINTwriter”.

## Configurando um modelo SAINTwriter

Antes que os administradores possam incluir e importar as vulnerabilidades a partir de um scanner SAINT, um modelo deverá ser configurado no SAINTwriter.

### Procedimento

1. Efetue login na interface do usuário SAINT.
2. No menu de navegação, selecione **Dados** > **SAINTwriter**.
3. Clique em **Tipo de Relatório**.
4. Na lista **Tipo**, selecione **Customizado**.
5. No campo **Nome do arquivo**, digite um nome do arquivo de configuração.

   O nome do arquivo de configuração que é criado e deverá ser utilizado quando incluir o scanner SAINT no QRadar.
6. Na lista **Tipo de modelo**, selecione **Detalhes Técnicos**.
7. Clique em **Continuar**.
8. Selecione **Lista**.
9. Na lista **Colunas a serem incluídas no host**, altere uma coluna Nenhum para **Endereço MAC**.
10. Na lista **Colunas a serem incluídas na vulnerabilidade**, altere o nome da coluna Nenhum para **Porta**.
11. Na lista **Colunas a serem incluídas na vulnerabilidade**, altere a coluna Nenhum para **Serviço**.
12. Clique em **Salvar**.

© Copyright IBM Corp. 2007, 2015

### O que Fazer Depois

Agora você está pronto para incluir uma configuração de varredura no QRadar para o scanner SAINT. Consulte "Incluindo uma varredura de vulnerabilidade SAINT".

## Incluindo uma varredura de vulnerabilidade SAINT

Os administradores podem incluir uma configuração do scanner SAINT para coletar relatórios específicos ou iniciar varreduras no scanner remoto.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar seu scanner SAINT.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **SAINT Scanner**.
7. No campo **Nome do host remoto**, digite o endereço IP ou o nome do host do scanner SAINT.
8. Escolha uma das seguintes opções de autenticação:

| Opção | Descrição |
|---|---|
| **Nome do usuário de login** | Para autenticar com um nome de usuário e senha:<br>1. No campo **Nome de usuário de login**, digite um nome de usuário que possua acesso ao host remoto.<br>2. No campo **Senha de login**, digite a senha associada ao nome de usuário. |
| **Ativar autorização de chave** | Para autenticar com um arquivo de autenticação baseado em chave:<br>1. Marque a caixa de seleção **Ativar autenticação de chave**.<br>2. No campo **Arquivo-chave privado**, digite o caminho do diretório para o arquivo-chave.<br>O diretório padrão para o arquivo-chave é `/opt/qradar/conf/vis.ssh.key`.<br>Se um arquivo-chave não existir, você deverá criar o arquivo vis.ssh.key. |

9. No campo **Diretório base do SAINT**, digite o caminho para o diretório de instalação do scanner SAINT.
10. Na lista **Tipo de varredura**, selecione uma das seguintes opções:
    - Varredura Ativa – Inicia uma varredura de vulnerabilidade para gerar dados de relatório com base no nome da sessão.
    - Somente Relatório – Gera um relatório de varredura com base no nome da sessão.

11. Para as configurações de **Varredura Ativa**, selecione uma opção para a caixa de seleção **Ignorar dados existentes**.
    - Marque essa caixa de seleção para forçar a varredura ativa a reunir novos dados de vulnerabilidade a partir da rede. Esta opção remove todos os dados da pasta da sessão antes de a varredura ativa iniciar.
    - Desmarque essa caixa de seleção para permitir que a varredura ativa utilize os dados existentes na pasta da sessão.
12. Na lista **Nível de varredura**, selecione um nível de varredura. As opções incluem:
    - Varredura de vulnerabilidade – Varre todas as vulnerabilidades.
    - Varredura de porta - Varre serviços TCP ou UDP que atendem na rede.
    - Varredura de conformidade de PCI - Varre portas e serviços com ênfase na conformidade de PCI DSS.
    - Principais 20 varreduras SANS - Varre as 20 vulnerabilidades de segurança mais críticas.
    - Varredura FISMA – Varrer todas as vulnerabilidades, incluindo todas as varreduras e níveis de PCI customizados.
13. No campo **Nome da sessão**, digite o nome da sessão para a configuração do scanner SAINT.
14. No campo **Configuração do SAINT Writer**, digite o nome do arquivo de configuração SAINTwriter.
15. Para configurar um intervalo do CIDR para o scanner:
    a. No campo de texto, digite o intervalo do CIDR para a varredura ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
    b. Clique em **Incluir**.
16. Clique em **Salvar**.
17. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 25. Visão geral do scanner Tenable SecurityCenter

Um scanner Tenable SecurityCenter pode ser utilizado para planejar e recuperar quaisquer registros de relatório de varredura de vulnerabilidade abertos a partir dos scanners de vulnerabilidade Nessus em sua rede. .

Para configurar o scanner Tenable SecurityCenter, consulte “Incluindo uma varredura Tenable SecurityCenter”.

## Incluindo uma varredura Tenable SecurityCenter

É possível incluir um scanner Tenable SecurityCenter Manager para permitir que o QRadar colete informações do host e de vulnerabilidade por meio da API Tenable.

### Antes de Iniciar

Verifique a localização do arquivo `request.php` no Tenable SecurityCenter antes de um scanner ser incluído no QRadar.

Antes de você incluir este scanner, um certificado do servidor é necessário para suportar conexões HTTPS. O QRadar suporta certificados com as extensões do arquivo a seguir: .crt, .cert ou .der. Para copiar um certificado no diretório `/opt/qradar/conf/trusted_certificates`, escolha uma das opções a seguir:

- Copie manualmente o certificado para o diretório `/opt/qradar/conf/trusted_certificates` usando SCP ou SFTP.
- O SSH no Console ou o host gerenciado e recupere o certificado usando o comando a seguir: `/opt/qradar/bin/getcert.sh <IP ou Hostname> <optional port - 443 default>`. Em seguida, um certificado é transferido por download do nome do host ou IP especificado e colocado no diretório `/opt/qradar/conf/trusted_certificates` no formato apropriado.

### Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Scanners de VA**.
3. Clique em **Incluir**.
4. No campo **Nome do scanner**, digite um nome para identificar o scanner.
5. Na lista **Hosts Gerenciados**, selecione o host gerenciado a partir de sua implementação do QRadar que gerencia a importação do scanner.
6. Na lista **Tipo**, selecione **Tenable SecurityCenter**.
7. No campo **Endereço do servidor**, digite o endereço IP do Tenable SecurityCenter.
8. No campo **Local da API**, digite o caminho para o arquivo `request.php` no Tenable SecurityCenter.

   O caminho padrão para o arquivo da API é `sc4/request.php`.
9. No campo **Nome do usuário**, digite o nome do usuário para acessar a API Tenable SecurityCenter.
10. No campo **Senha**, digite a senha para acessar a API Tenable SecurityCenter.
11. Para configurar um intervalo do CIDR para o scanner:

© Copyright IBM Corp. 2007, 2015

a. No campo de texto, digite o intervalo do CIDR para a varredura ou clique em **Pesquisar** para selecionar um intervalo do CIDR na lista de rede.
b. Clique em **Incluir**.

12. Clique em **Salvar**.
13. Na guia **Administrador**, clique em **Implementar Mudanças**.

## O que Fazer Depois

Agora você está pronto para criar um planejamento de varredura. Consulte Capítulo 26, “Planejando uma varredura de vulnerabilidade”, na página 93.

# Capítulo 26. Planejando uma varredura de vulnerabilidade

Os planejamentos de varredura são intervalos designados para os scanners que determinam quando os dados de avaliação de vulnerabilidades são importados de dispositivos de varredura externos em sua rede. Os planejamentos de varredura também podem definir intervalos ou sub-redes do CIDR que são incluídos na importação de dados quando a importação de dados de vulnerabilidade ocorre.

## Sobre Esta Tarefa

Os planejamentos de varredura são criados para cada produto de scanner em sua rede e são utilizados para recuperar dados de vulnerabilidades. Não há nenhum limite para o número de planejamentos de varredura que podem ser criados. Geralmente é útil criar em sua rede diversas varreduras em busca de vulnerabilidades. Grandes importações de vulnerabilidade podem demorar muito tempo para serem concluídas e geralmente consomem muitos recursos do sistema. Uma varredura não pode ser planejada enquanto o scanner não tiver sido incluído.

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Planejar Scanners de VA**.
3. Clique em **Incluir**.
4. Na lista **Scanners de VA**, selecione o scanner que requer um planejamento de varredura.
5. Escolha uma das opções a seguir:

| Opção | Descrição |
|---|---|
| **CIDR de Rede** | Selecione essa opção para definir um intervalo do CIDR para a importação de dados.<br><br>Se um scanner incluir diversas configurações do CIDR, o intervalo do CIDR poderá ser selecionado na lista. |
| **Sub-rede/CIDR** | Selecione esta opção para definir um intervalo de sub-rede ou do CIDR para a importação de dados.<br><br>O valor de sub-rede/CIDR que é definido pelo administrador deve ser um CIDR de Rede que esteja disponível para o scanner. |

6. Na lista **Prioridade**, selecione o nível de prioridade a ser designado para a varredura.

| Opção | Descrição |
|---|---|
| **Baixa** | Indica que a varredura é de prioridade normal. Baixa prioridade é o valor padrão da varredura. |

© Copyright IBM Corp. 2007, 2015

| Opção | Descrição |
| --- | --- |
| **Alto** | Indica que a varredura é de alta prioridade.<br><br>As varreduras de alta prioridade são sempre colocadas acima das varreduras de baixa prioridade na fila de varredura. |

7. No campo **Portas**, digite as portas que são incluídas no planejamento de varredura. Quaisquer portas que não estiverem no planejamento não são importadas a partir dos dados de vulnerabilidade. Os administradores podem especificar quaisquer valores de porta de 1 a 65536. Valores de porta individuais podem ser incluídos como valores separados por vírgulas, junto com os intervalos de portas. Por exemplo, 21,443, 445, 1024-2048.
8. Selecione o horário de início do planejamento.
9. No campo **Intervalo**, digite um intervalo de tempo para indicar a frequência com que deseja repetir essa varredura. Os planejamentos de varredura podem conter intervalos por hora, dia, semana ou mês.
10. Clique em **Salvar**.

# Capítulo 27. Visualizando o status de uma varredura de vulnerabilidade

A janela Planejamento de varredura fornece aos administradores uma visualização de status de quando cada scanner está planejado para coletar dados de avaliação de vulnerabilidades para o ativo na rede.

## Sobre Esta Tarefa

O nome de cada varredura é exibido, juntamente com o intervalo do CIDR, porta ou intervalo de portas, prioridade, status e o próximo tempo de execução.

*Tabela 8. Status do planejamento da varredura*

| Nome da coluna | Descrição |
|---|---|
| Scanner de VA | Exibe o nome do planejamento de varredura. |
| CIDR | Exibe os intervalos do endereço do CIDR que são incluídos na importação de dados de vulnerabilidade quando o planejamento de varredura é iniciado. |
| Portas | Exibe os intervalos de portas que são incluídos na importação de dados de vulnerabilidade quando o planejamento de varredura é iniciado.<br><br>Os planejamentos de varredura são capazes de iniciar uma varredura remota em um dispositivo de vulnerabilidade remoto de fornecedores específicos. Por exemplo, NMap ou Nessus, ou Nessus Scan Results Importer; as portas listadas na coluna Portas são as portas contidas na varredura.<br><br>Para a maioria dos scanners, o intervalo de portas não é considerado ao solicitar informações de ativos a partir de um scanner.<br><br>Por exemplo, os scanners nCircle IP360 e Qualys relatam vulnerabilidades em todas as portas, mas requerem que você especifique quais informações de porta devem ser obtidas do relatório completo para exibição na interface com o usuário. |
| Prioridade | Exibe a prioridade da varredura.<br><br>Os planejamentos de varredura de alta prioridade são enfileirados acima da prioridade e executados antes das varreduras de baixa prioridade. |
| Status | Exibe o status atual da varredura. Cada campo de status contém informações exclusivas sobre o status da varredura.<br>• As novas varreduras podem ser editadas até que o estado seja alterado.<br>• As varreduras pendentes devem aguardar outra varredura ser concluída.<br>• As varreduras em andamento fornecem uma porcentagem completa com informações de dicas de ferramentas sobre a importação de dados.<br>• As varreduras concluídas fornecem um resumo das vulnerabilidades importadas ou de quaisquer importações de dados parciais que ocorreram.<br>• As varreduras com falha fornecem uma mensagem de erro sobre o porquê as vulnerabilidades falharam a serem importadas. |

© Copyright IBM Corp. 2007, 2015

*Tabela 8. Status do planejamento da varredura (continuação)*

| Nome da coluna | Descrição |
|---|---|
| Hora da Última Conclusão | Exibe a última vez em que a varredura importou com sucesso registros de vulnerabilidade para o planejamento. |
| Próximo Tempo de Execução | Exibe a próxima vez em que a varredura está planejada para importar dados de vulnerabilidade. Os planejamentos de varredura que exibem *Never* na interface com o usuário são varreduras únicas. |

## Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Planejar Scanners de VA**.
3. Revise a coluna Status para determinar o status de suas origens de log.

   A coluna de status de cada scanner fornece uma mensagem de status sobre cada importação de vulnerabilidade com sucesso ou com falha.

# Capítulo 28. Scanners de vulnerabilidade suportados

Os dados de vulnerabilidade podem ser coletados de vários fabricantes e fornecedores de produtos de segurança. Se o scanner implementado em sua rede não estiver listado neste documento, será possível entrar em contato com seu representante de vendas para revisar o suporte para o seu dispositivo.

*Tabela 9. Scanners de vulnerabilidade suportados*

| Fornecedor | Nome do scanner | Versões suportadas | Nome da configuração | Tipo de conexão |
|---|---|---|---|---|
| Beyond Security | Automated Vulnerability Detection System (AVDS) | AVDS Management V12 (versão secundária 129) e superior | Beyond Security AVDS Scanner | Importação do arquivo de dados de vulnerabilidade com SFTP |
| eEye Digital Security | eEye REM | REM V3.5.6 | eEye REM Scanner | Listener de trap SNMP |
| | eEye Retina CS | Retina CS V3.0 - V4.0 | | Consultas de banco de dados sobre JDBC |
| Genérico | Axis | N/A | Scanner Axis | Importação do arquivo de dados de vulnerabilidade com SFTP |
| IBM | InfoSphere Guardium | v9.0 e superior | IBM Guardium SCAP Scanner | Importação do arquivo de dados de vulnerabilidade com SFTP |
| IBM | IBM Security AppScan Enterprise | V8.6 | IBM AppScan Scanner | Serviço da web IBM REST com HTTP ou HTTPS |
| IBM | InfoSphere SiteProtector | V2.9.x | IBM SiteProtector Scanner | Consultas de banco de dados sobre JDBC |
| IBM | Tivoli Endpoint Manager | V8.2.x | IBM Tivoli Endpoint Manager | API baseada em SOAP com HTTP ou HTTPS |
| Juniper Networks | NetScreen Security Manager (NSM) Profiler | 2007.1r2 | Juniper NSM Profiler Scanner | Consultas de banco de dados sobre JDBC |
| | | 2007.2r2 | | |
| | | 2008.1r2 | | |
| | | 2009r1.1 | | |
| | | 2010.x | | |
| McAfee | Foundstone | V5.0 - V6.5 | Foundscan Scanner | API baseada em SOAP com HTTPS |
| McAfee | Vulnerability Manager | V6.8 | McAfee Vulnerability Manager | API baseada em SOAP com HTTPS |
| | | V7.0 | | Importação do arquivo XML |
| | | V7.5 | | |
| nCircle | ip360 | VnE Manager V6.5.2 - V6.8.28 | nCircle ip360 Scanner | Importação do arquivo de dados de vulnerabilidade com SFTP |
| Nessus | Nessus | Linux V4.0.2 - V4.4.x | Nessus Scanner | Importação de arquivo sobre SFTP com a execução do comando SSH |
| | | Microsoft Windows V4.2 - V4.4.x | | |
| Nessus | Nessus | Linux V4.2 - V5.x | Nessus Scanner | Nessus XMLRPC API sobre HTTPS |
| | | Microsoft Windows V4.2 - V5.x | | |
| netVigilance | SecureScout | V2.6 | Scanner SecureScout | Consultas de banco de dados sobre JDBC |
| Open source | NMap | V3.7 - V6.0 | NMap Scanner | Importação de arquivo de dados de vulnerabilidade sobre SFTP com a execução do comando SSH |
| Qualys | QualysGuard | V4.7 -V7.10 | Qualys Scanner | APIv2 sobre HTTPS |
| Qualys | QualysGuard | V4.7 -V7.10 | Qualys Detection Scanner | API Host Detection List sobre HTTPS |
| Rapid7 | NeXpose | V4.x - V5.5 | Scanner Rapid7 NeXpose | Chamada de Procedimento Remoto (RPC) sobre HTTPS |
| | | | | Importação de arquivo local do arquivo XML sobre SCP ou SFTP para um diretório local |
| Saint Corporation | SAINT | V7.4.x | Scanner Saint | Importação de arquivo de dados de vulnerabilidade sobre SFTP com a execução do comando SSH |
| Tenable | SecurityCenter | V4.6.0 | Tenable SecurityCenter | Solicitação JSON sobre HTTPS |

© Copyright IBM Corp. 2007, 2015

# Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

**O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:**

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

© Copyright IBM Corp. 2007, 2015

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a mudanças ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

## Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Os termos a seguir são marcas comerciais ou marcas registradas de outras empresas:

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

## Considerações sobre política de privacidade

Os produtos de Software IBM, incluindo soluções software como um serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto para ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar na coleta de informações de identificação pessoal. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, esta Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de gerenciamento e autenticação de sessão. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade ativada.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para aviso e consentimento.

Para obter informações adicionais sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte o IBM Privacy Policy em http://www.ibm.com/privacy e o IBM Online Privacy Statement em http://www.ibm.com/privacy/details, a seção “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” em http://www.ibm.com/software/info/product-privacy.

# Índice Remissivo



© Copyright IBM Corp. 2007, 2015