Detalhes da versão do Sentinel 8.5

Agosto de 2021

O Sentinel 8.5 resolve vários problemas conhecidos e também adiciona alguns novos recursos.

Muitas destas melhorias foram feitas como resposta direta a sugestões de nossos consumidores. Agradecemos seu tempo e suas opiniões relevantes. Esperamos que você continue a nos ajudar para que nossos produtos atendam às suas necessidades. É possível publicar feedback no fórum do Sentinel, nossa comunidade online que também contém informações sobre produtos, blogs e links para recursos úteis. Também é possível compartilhar suas ideias para melhorar o produto no Portal de ideias.

A documentação deste produto está disponível nos formatos HTML e PDF em uma página que não requer login. Se você tiver sugestões para aprimoramentos da documentação, clique no ícone de comentário em qualquer página na versão HTML da documentação publicada na página Documentação do Sentinel. Para fazer o download deste produto, consulte o site de Download de Produtos.

Novidades

As seções a seguir descrevem os principais recursos fornecidos por esta versão, bem como os problemas resolvidos nela:

Integração do ArcSight Intelligence com o Sentinel

Com esta versão, o Sentinel fornece aos clientes uma forma de se integrar com incríveis tecnologias de análise do ArcSight Intelligence. Assim, os usuários do Sentinel podem obter pontuação de risco quase em tempo real e usá-la para a análise posterior na própria regra de correlação etc. Isso permite que o Sentinel obtenha muita experiência de busca por ameaças.

O ArcSight Intelligence é uma solução de análise comportamental de usuários e entidades que usa ciência de dados e análises avançadas para identificar as principais entidades e comportamentos de risco que ocorrem na sua organização. O Intelligence primeiro estabelece o comportamento normal para suas entidades organizacionais e depois usa análises avançadas para identificar os comportamentos anômalos de qualquer entidade e fornece uma pontuação de risco adequada para cada uma dessas entidades.

O Sentinel fornece uma maneira de integração com o ArcSight Intelligence 6.3. Essa integração facilita o envio dos dados dos usuários do Sentinel para o ArcSight Intelligence para análise e também fornece uma forma de receber detalhes de pontuação de risco das entidades do Intelligence. Isso faz com que o Sentinel detecte as entidades e os usuários mais arriscados na organização, que podem comprometer todo o sistema e criar uma possível ameaça.

MITRE ATT&CK

O MITRE ATT&CK ajuda as equipes de cibersegurança a avaliar a eficácia dos processos do SOC (Security Operations Center - Centro de Operações de Segurança) e das medidas defensivas para identificar áreas de aprimoramento. O MITRE ATT&CK é uma base de conhecimento acessível globalmente de táticas e técnicas adversárias de cibersegurança baseadas em observações do mundo real. A base de conhecimento do MITRE ATT&CK é usada como base para o desenvolvimento de modelos e metodologias específicas de ameaças no setor privado, no governo e na comunidade de produtos e serviços de cibersegurança.

Desta versão do Sentinel em diante, os administradores podem mapear regras de correlação com o ID do MITRE ATT&CK. MITRE ATT&CK significa MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). A metodologia do MITRE ATT&CK é uma linguagem comum do setor de táticas e técnicas de ator de ameaças baseada em observações do mundo real.

Os administradores do Sentinel agora podem mapear a própria regra de correlação pronta para uso ou personalizada diretamente com o ID do MITRE ATT&CK. Fornecendo assim uma série de análises de dados ao seu alcance e dando-lhes um poder de visualização de quais são as regras disparadas ou quais táticas e técnicas do MITRE estão sendo exploradas pelos clientes. O Sentinel está fornecendo a eles um certo grupo de conjuntos de ferramentas pelos quais eles podem obter imediatamente uma visão de sua rede e de quais são os ataques mais importantes que eles precisam evitar.

Se uma regra de correlação mapeada com um ID do MITRE ATT&CK for acionada, os eventos acionados terão o ID do MITRE ATT&CK e o nome do MITRE ATT&CK. Esses eventos são analisados com um widget que está disponível em um painel de controle de saúde de segurança padrão. Os dez principais nomes do MITRE ATT&CK aparecem nesse painel de controle em uma Faixa de Tempo de um dia e com intervalo de exibição de uma hora.

Upgrade do JDK

Para evitar vulnerabilidades de segurança (CVE-2021-2161, CVE-2021-2163, CVE-2021-2341, CVE-2021-2432, CVE-2021-2369, CVE-2021-2388) e para usar os recursos de segurança dos novos padrões do JDK, faz-se o upgrade do JDK de 1.8.0_update242 para 1.8.0_update302

Armazenando eventos brutos do conector

O conector Syslog do Sentinel, da versão 2021.1r1 em diante, permitirá o armazenamento dos eventos brutos que vêm dos Conectores do ArcSight Intelligence. Esses são os eventos intocados e não processados que são gerados diretamente pelo dispositivo final. Essa configuração pode ser habilitada marcando a opção **Preserve Raw Event** (Preservar o Evento Bruto) no Conector Inteligente correspondente.

Suporte do TLS

O suporte do TLS 1.0 e do TLS 1.1 foi removido.

Versões do OS (sistema operacional)

Instalação tradicional: O Sentinel agora está certificado também na seguinte nova plataforma:

- RHEL (Red Hat Enterprise Linux) 8.3

OS descontinuado: Os seguintes sistemas operacionais agora estão descontinuados, pois o RHEL e o SLES removeram o suporte para estes SO:

- RHEL 7.6 e 7.7
- SLES 15 SP1

Correções de software

O Sentinel 8.5 inclui correções de software que resolvem os seguintes problemas:

- "A conversão em FIPS no servidor do Sentinel muda o protocolo de TLS 1.2 para TLS 1.1" na página 3
- "Chamadas REST do Sentinel falham após fazer upgrade do cliente Sentinel Java" na página 3
- "Erro ao gerar um novo relatório" na página 4

A conversão em FIPS no servidor do Sentinel muda o protocolo de TLS 1.2 para TLS 1.1

Problema: No servidor do Sentinel, ao fazer a conversão em FIPS, o protocolo muda de TLS 1.2 para TLS 1.1. Isso faz com que a conexão entre o SAM e o servidor do Sentinel seja terminada. No entanto, o cliente deverá usar o TLS 1.2

Correção: Agora, ao converter para FIPS, a versão do TLS não está sendo mudada de 1.2 para 1.1

Chamadas REST do Sentinel falham após fazer upgrade do cliente Sentinel Java

Problema: Depois de fazer upgrade do Sentinel Java Client de 8.1 para 8.2, as chamadas REST falham.

Correção: Agora, depois de fazer upgrade do Sentinel Java Client de 8.1 para 8.2, as chamadas REST não falham.

Erro ao gerar um novo relatório

Problema: Erro ao gerar um novo relatório. A principal causa do erro pode ser um keystore adulterado ou uma senha incorreta.

Correção: Não obter um erro ao gerar um novo relatório.

Requisitos do sistema

Para obter mais informações sobre requisitos de hardware, sistemas operacionais suportados e browsers, consulte os Sentinel System Requirements (Requisitos do sistema do Sentinel).

Informações sobre licença e compra

Para comprar uma licença corporativa ou fazer upgrade da sua licença existente, ligue para 1-800-529-3400, envie um e-mail para info@microfocus.com ou visite https://www.microfocus.com/en-us/products/netiq-sentinel/contact.

Instalando o Sentinel 8.5

Para obter informações sobre como instalar o Sentinel 8.5, consulte o *Sentinel Installation and Configuration Guide* (Guia de Instalação e Configuração do Sentinel).

Observação: Todos os hosts usados para o servidor Sentinel e seus componentes devem ser configurados em ambiente de resolução DNS de duas vias (nome de host para IP e IP para nome de host).

Fazendo upgrade para o Sentinel 8.5

Você pode fazer upgrade para o Sentinel 8.5 de qualquer versão anterior do Sentinel (do Sentinel 8.2 e posteriores).

Importante: Devido ao último upgrade do JDK, para configurar LDAPS e SDK, o usuário precisará usar o nome de host em vez do endereço IP, e ele também deverá ser solucionável.

Importante: Há uma mudança no procedimento de upgrade da instalação tradicional e da aplicação. Consulte Settings in Elasticsearch for Secure Cluster Communication (Configurações no Elasticsearch para a comunicação segura em cluster) e siga as etapas. Isso só será aplicável se você estiver fazendo upgrade do Sentinel para as versões mais recentes de 8.3.1 e anteriores.

Importante: Você pode executar uma atualização offline fazendo download do Patch ISO offline para cada aplicação. Para obter mais informações, consulte Performing Offline Updates (Executando atualizações offline).

Aviso: Se você fizer upgrade das versões anteriores para o Sentinel 8.3, deverá atribuir manualmente a permissão **Enviar eventos e anexos** a usuários não administradores que enviam eventos ou anexos ao Sentinel. A menos que você atribua essa permissão, o Sentinel não receberá mais eventos e anexos do Guardião de Mudanças ou do Gerente de Configuração Segura.

Para instalação tradicional, consulte Upgrading the Operating System (Fazendo upgrade do sistema operacional) no *Sentinel Installation and Configuration Guide* (Guia de Instalação e Configuração do Sentinel).

Problemas conhecidos

A Micro Focus se esforça para garantir que nossos produtos forneçam soluções de qualidade para suas necessidades de software empresarial. Os problemas conhecidos a seguir estão sendo atualmente pesquisados. Se você precisar de assistência adicional com qualquer problema, entre em contato com o Suporte técnico.

A atualização do Java 8 incluída no Sentinel pode impactar os seguintes plug-ins:

- Conector Cisco SDEE
- Conector SAP (XAL)
- Integrador do Remedy

Caso haja problemas com esses plug-ins, priorizaremos e corrigiremos os problemas de acordo com as políticas de gerenciamento de defeitos padrão. Para obter mais informações sobre as políticas de suporte, consulte Políticas de suporte.

Não é possível exibir o gráfico de previsão de capacidade de armazenamento

Problema: Em **Sentinel Principal** > **Armazenamento** > **Integridade**, o gráfico **Previsão de Capacidade de Armazenamento** não está disponível. Isso ocorre porque o Zulu OpenJDK não inclui as fontes necessárias.

Solução temporária: Use os seguintes comandos para instalar as fontes:

- yum install fontconfig
- yum install dejavu

Erro ao iniciar um painel do Kibana após fazer upgrade do Sentinel

Problema: Iniciar um painel do Kibana exibe a seguinte mensagem: `Nenhum padrão de índice padrão. Você deve selecionar ou criar um para continuar.`

Solução temporária: Para definir um padrão de índice Kibana como o padrão de índice padrão:

1. Selecione um dos seguintes:
   - alerts.alerts
   - security.events.normalized_*
2. Clique em **Definir como Padrão**.

Não é possível copiar os links de alerta de todos os alertas em uma tela de alerta no Mozilla Firefox e Microsoft Edge

Problema: A opção **Selecionar todos *<número de alertas>* Alertas** > **Copiar link de alerta** não funciona no Firefox nem no Edge.

Solução temporária: Execute estas etapas:

1. Selecione manualmente todos os alertas em cada página da tela de alerta usando a caixa de seleção que permite selecionar todos os alertas.

2. Clique em **Copiar Link de Alerta**.
3. Cole-o no aplicativo desejado.

A instalação do Sentinel, do Collector Manager e do Correlation Engine como uma imagem da aplicação OVF não exibe a tela de login

Problema: O instalador é interrompido na tela de instalação em andamento e não exibe a tela de login, mesmo que a instalação esteja concluída.

Solução temporária: Reinicialize a máquina virtual e inicie o Sentinel, o Gerenciador de Coletor ou o Mecanismo de Correlação.

A aplicação Sentinel 8.2 no Microsoft Hyper-V Server 2016 não é iniciada ao reinicializar

Problema: No Hyper-V Server 2016, a aplicação Sentinel não é iniciada quando você a reinicializa e exibe a seguinte mensagem:

```
A start job is running for dev-disk-by\..
```

Esse problema ocorre porque o sistema operacional modifica o UUID do disco durante a instalação. Logo, ele não consegue localizar o disco durante a reinicialização.

Solução temporária: Modifique o UUID do disco manualmente. Para obter mais informações, consulte o Artigo 7023143 da Base de Conhecimento.

Erro ao fazer upgrade da aplicação de HA do Sentinel 8.2

Problema: Quando você faz upgrade para a aplicação de HA do Sentinel 8.2, o Sentinel exibe o seguinte erro:

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited
with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

Solução temporária: Antes de responder ao prompt acima, faça o seguinte:

1. Inicie outra sessão usando PuTTY ou software similar para o host em que você está executando o upgrade.
2. Adicione a seguinte entrada ao arquivo `/etc/csync2/csync2.cfg`:

   `/etc/opt/novell/sentinel/config/configuration.properties`
3. Remova a pasta `sentinel` de `/var/opt/novell`:

   `rm -rf /var/opt/novell/sentinel`
4. Retorne para a sessão em que você iniciou o upgrade e digite `r` para continuar com o upgrade.

A instalação da aplicação Collector Manager e Correlation Engine falha em idiomas que não sejam o inglês no modo MFA

Problema: A instalação da aplicação do Gerenciador de Coletor e do Mecanismo de Correlação falha no modo MFA se o idioma do sistema operacional é diferente do inglês.

Solução temporária: Instale as aplicações Collector Manager e Correlation Engine em inglês. Após concluir a instalação, mude o idioma conforme desejado.

Problemas de utilização nas telas de instalação da aplicação

Problema: Os botões **Próximo** e **Anterior** nas telas de instalação da aplicação não aparecem ou estão desabilitados em alguns casos, como os seguintes:

- Quando você clica em **Anterior** na tela de pré-verificação do Sentinel para editar ou revisar as informações na tela de Configurações de rede da aplicação do servidor do Sentinel, não aparece o botão **Próximo** para continuar a instalação. O botão **Configurar** permite que você edite apenas as informações especificadas.
- Se você especificou configurações de rede incorretas, a tela de Pré-verificação do Sentinel indicará que você não pode continuar com a instalação por causa de informações de rede incorretas. Não é exibido o botão **Anterior** para voltar à tela anterior para modificar as configurações de rede.

Solução temporária: Reinicie a instalação da aplicação.

O Gerenciador de Coletor fica sem memória se a sincronização de horário está habilitada em open-vm-tools

Problema: Se você instalar e habilitar manualmente a sincronização de horário nas open-vm-tools, elas sincronizarão periodicamente o horário entre a aplicação Sentinel (convidado) e o servidor VMware ESX (host). Essas sincronizações de horário podem resultar na mudança do relógio do convidado para antes ou depois do horário do servidor ESX. Até que o horário seja sincronizado entre a aplicação Sentinel (convidado) e o servidor ESX (host), o Sentinel não processará eventos. Como resultado, um grande número de eventos é enfileirado no Collector Manager, o que pode acabar eliminando eventos quando atingir seu limite. Para evitar esse problema, o Sentinel desabilita a sincronização de horário por padrão na versão de open-vm-tools disponível no Sentinel.

Solução temporária: Desabilitar a sincronização de horário. Para obter mais informações sobre a desabilitação da sincronização de horário, consulte Disabling Time Synchronization (Desabilitando a sincronização de horário).

O Gerente de agente exige autenticação SQL quando o modo FIPS 140-2 é ativado

Problema: Quando o modo FIPS 140-2 for habilitado no Sentinel, o uso da autenticação do Windows para o Agent Manager causará falha na sincronização com o banco de dados do Agent Manager.

Solução temporária: Use a autenticação do SQL para o Gerente de Agente.

A instalação de alta disponibilidade do Sentinel em modo não FIPS 140-2 exibe um erro

Problema: A instalação do Sentinel de Alta Disponibilidade no modo não FIPS 140-2 é concluída com sucesso, mas exibe o seguinte erro duas vezes:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

Solução temporária: O erro é esperado e você pode ignorá-lo com segurança. Embora o instalador exiba o erro, a configuração de alta disponibilidade do Sentinel funciona com sucesso em modo não FIPS 140-2.

O comando Keytool exibe um aviso

Problema: Ao usar o comando Keytool, este aviso será exibido:

```
The JKS keystore uses a proprietary format. It is recommended to migrate to
PKCS12which is an
industry standard format using "keytool -importkeystore -srckeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -destkeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -deststoretype pkcs12".
```

Solução temporária: O aviso é esperado e você pode ignorá-lo com segurança. Embora o aviso seja exibido, o comando Keytool funciona conforme o esperado.

O Sentinel não processa feeds de inteligência de ameaças no modo FIPS

Problema: No modo FIPS, ao processar feeds de inteligência de ameaça prontos para uso em URLs, o Sentinel exibe o seguinte erro:`Alerta fatal recebido: protocol_version`. Esse problema ocorre porque os feeds de ameaças out-of-the-box agora suportam apenas o TLS 1.2, que não funciona no modo FIPS.

Solução temporária: Realize o seguinte:

1. Clique em **Sentinel Principal** > **Integração** > **Fontes de Inteligência de Ameaças**.
2. Edite cada URL para mudar o protocolo de `http` para `https`.

Efetuar logout do Sentinel Principal não efetua logout dos painéis de controle e vice-versa no modo de autenticação multifatorial

Problema: No modo de autenticação multifatorial, se você efetuar logout do **Sentinel Principal**, não efetuará logout dos painéis de controle do Sentinel e vice-versa. Isso ocorre devido a um problema na Metodologia do Advanced Authentication.

Solução temporária: Até que uma correção esteja disponível no Advanced Authentication Framework, atualize a tela para exibir a tela de login.

O painel de controle personalizado do Kibana não é exibido após fazer upgrade para o Sentinel 8.3.1

Problema: O painel de controle personalizado do Kibana não é exibido quando você faz upgrade do Sentinel 8.3 ou anterior para o Sentinel 8.3.1.

Solução temporária: Recrie o painel de controle personalizado após fazer upgrade do Sentinel.

Quando você inicia o Kibana, a mensagem de erro de conflito é exibida

Problema: Depois de instalar ou fazer upgrade do Sentinel e ao iniciar o Kibana pela primeira vez, a mensagem de erro de conflito é exibida.

Solução temporária: Ignore a mensagem de erro de conflito, pois ela não afeta a funcionalidade.

Quando você reinicializa o OS Red Hat 8.1 e 8.2, o Sentinel não é iniciado automaticamente

Problema: Depois de instalar o Sentinel no SO Red Hat 8.1 e 8.2, o Sentinel (Server, RCM ou RCE) não é iniciado automaticamente após a reinicialização.

Solução temporária: Mude o valor SELINUX para **SELINUX=desabilitado** no arquivo `/etc/selinux/config`.

Quando você abre o console de gerenciamento da aplicação do Sentinel, uma mensagem de erro é exibida

Problema: Depois de fazer upgrade para o Sentinel 8.3, quando você tentar abrir o Console de Gerenciamento da Aplicação do Sentinel do CE (Correlation Engine - Mecanismo de Correlação) ou do CM (Collector Manager - Gerenciador de Coletor) dos servidores HA (High Availability - Alta Disponibilidade), uma mensagem de erro `404 Não encontrado` será exibida.

Solução temporária: Para obter mais informações, consulte o documento da Base de Conhecimento da Micro Focus.

Usuários com permissão de visualização de ocultação do gerenciamento ainda podem ver a guia de gerenciamento na página do Kibana

Problema: Depois de fazer upgrade para o Sentinel 8.4, os usuários com permissão de visualização de ocultação do gerenciamento ainda podem ver a guia Gerenciamento na página do Kibana, mas não podem acessar os recursos da guia Gerenciamento.

Quando o administrador muda a função de alertas do usuário, as mudanças não são atualizadas imediatamente na página do Kibana

Problema: Os usuários existentes não podem ver nenhum alerta na página do Kibana imediatamente, embora o administrador tenha atualizado a permissão para ver os alertas.

Solução temporária: Quando a permissão do usuário é atualizada, você precisa efetuar logout e login novamente.

Quando você inicia o painel de controle de visualização como um usuário locatário, uma mensagem de erro é exibida

Problema: Quando um usuário locatário não padrão inicia o painel de controle de visualização, é exibida uma mensagem de erro **Proibido**. Esta mensagem de erro é exibida sempre que o painel de controle é iniciado pelo usuário locatário não padrão que tem permissão **View-only** (Apenas Visualização) para a opção **Gerenciamento** e não há nenhum usuário com permissão **Editar** para a opção **Gerenciamento** nesse locatário.

Solução temporária: Ignore a mensagem de erro, pois ela não afeta a funcionalidade.

No RHEL, o RCM e o RCE não estão se conectando com o servidor quando o CRL está habilitado

Problema: O RCM (Remote Collector Manager - Gerenciador de Coletor Remoto) e o RCE (Remote Correlation Engine - Mecanismo de Correlação Remoto) não conseguem se conectar com o servidor quando o CRL está habilitado no RHEL.

Solução temporária: Faça upgrade da **versão de cURL** na máquina para 7.60 ou acima.

O RCM não está encaminhando os eventos para o servidor Sentinel quando visualização do evento, FIPS e CRL estão habilitados

Problema: Na nova instalação da configuração distribuída, após habilitar a Visualização de Eventos, os serviços FIPS e CRL, o RCM (Collector Manager Remoto) não está encaminhando os eventos para o servidor Sentinel.

Solução temporária: Se a Visualização de Eventos e o FIPS ou a Visualização de Eventos e CRL estiverem habilitados, o RCM encaminhará os eventos para o servidor Sentinel.

Há falhas com exceções nos relatórios de incidentes depois de fazer upgrade do OS de qualquer versão mais antiga para a versão mais recente

Problema: Quando você está fazendo upgrade do sistema operacional de uma versão mais antiga para a versão mais recente, há falhas com exceções nos relatórios de incidentes.

Uma exceção é registrada ao tentar reindexar pela primeira vez

Problema: Uma exceção está sendo registrada quando a operação de reindexação é executada pela primeira vez.

Erro ao executar `convert_to_fips.sh` no build da aplicação RCM/RCE do Sentinel 8.5

Problema: Quando o administrador do sistema executa `convert_to_fips.sh` no build da aplicação RCM/RCE do Sentinel 8.5, depois de fornecer credenciais corretas dos usuários em um loop contínuo, a seguinte mensagem de erro é exibida:

```
ERROR: Failed to connect to <Sentinel server IP>:
Failed to retrieve token for communication channel.
```

Solução temporária: Execute estas etapas:

1. Saia da execução do script.
2. Acesse `<Instalação do RCM/RCE do Sentinel>/etc/opt/novell/sentinel/config/configuration.properties`
3. Defina o valor de `rest.endpoint.port` para a porta do servidor web correspondente.

   Por exemplo, `rest.endpoint.port=8443`
4. Execute novamente `convert_to_fips.sh`

Contatando a Micro Focus

Para problemas específicos do produto, entre em contato com o Suporte da Micro Focus em https://www.microfocus.com/support-and-services/.

Informações ou conselhos técnicos adicionais estão disponíveis em várias fontes:

- Documentação do produto, artigos da Base de Dados de Conhecimento e vídeos: https://www.microfocus.com/support-and-services/
- Páginas da Comunidade Micro Focus: https://www.microfocus.com/communities/

Informações legais