Dell Security Management Server

Aconselhamentos técnicos da versão 11.7

Março 2023
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: NOTA fornece informações importantes para ajudar você a usar melhor o computador.

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

Índice

1

Aconselhamentos técnicos do Dell Security Management Server

Entre em contato com o Dell ProSupport for Software

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone 24x7, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone de fora dos Estados Unidos, veja Números de telefone internacionais do Dell ProSupport for Software.

Novos recursos e funcionalidades da versão 11.7

Novos recursos e funcionalidades incluem:

- Upgrades
- Management Console
- Políticas de console de gerenciamento

Upgrades

- A versão Jetty em execução no Dell Security Management Server foi migrada para a versão 9.4.50.v20221201.

Management Console

- Agora, uma mensagem de erro lista todos os requisitos para a senha de superadministrador quando o administrador tenta atualizar a senha com um valor que não atenda a esses requisitos.

Políticas de console de gerenciamento

- Um problema na política *Vida útil do PIN do usuário* foi resolvido para que o administrador possa inserir *0* dias.

Aconselhamentos técnicos resolvidos da versão 11.7

Aconselhamentos de segurança resolvidos

- O Dell Security Management Server versão 11.7 inclui uma atualização de segurança que aborda uma vulnerabilidade OpenSSL (OpenSSL CVE-2022-3602).

Aconselhamentos técnicos resolvidos

- Foram feitas alterações para reduzir o tamanho do banco de dados.
- O processamento de inventários foi aprimorado.
- No console de gerenciamento do BitLocker Manager, em *Detalhes do Endpoint > Estados > Visto pela última vez no sistema*, um problema foi resolvido para que todos os registros de data e hora reflitam o fuso horário apropriado. [DDPSUS-3237]
- Um problema na política *Vida útil do PIN do usuário* foi resolvido para que o administrador possa inserir **0** dias. [DDPS-10857]

Aconselhamentos técnicos da versão 11.7

Management Console

- Em *Firewall do client* > *Configurações e regras*, o botão *OK* agora é ativado somente depois que o administrador faz atualizações válidas. Consulte *Populações* > *Empresa* > *Políticas de segurança* > *Prevenção de ameaças* > *Firewall do client (ativado)* > *Mostrar configurações avançadas* > *Firewall*. [DDPS-10788]

Novos recursos e funcionalidades da versão 11.6

Novos recursos e funcionalidades incluem:

- Management Console
- Políticas de console de gerenciamento

Management Console

- O servidor de recuperação agora permite chaves {} no campo ID de recuperação.

Políticas de console de gerenciamento

- Em *Criptografia avançada do Windows* > *Criptografia BitLocker* > *Configurações de volume do sistema operacional*, a política *Atraso do prompt de PIN* é nova. Essa política permite que os administradores definam o número de minutos para atrasar a exibição do *prompt de PIN do BitLocker* ao usuário.
- Em *Autenticação* > *Autenticação de pré-inicialização*:
  - A política *Tentativas permitidas de login do usuário com PIN armazenado em cache* possibilita que o administrador especifique o número de vezes que um usuário com PIN armazenado em cache pode tentar fazer login.
  - A política *Número de caracteres obrigatórios no PIN* permite que o administrador configure o comprimento mínimo do PIN para a autenticação PBA. As opções podem ter de 4 a 126 caracteres.
  - A política *Método de autenticação* agora tem um valor *Senha+PIN*. No entanto, para a versão 11.6, o valor Senha+PIN está sendo revisado, portanto, evite usá-lo até segunda ordem.

Aconselhamentos técnicos resolvidos da versão 11.6

Aconselhamentos de segurança resolvidos

Management Console

- Um problema foi resolvido salvando as *Configurações de firewall* em *Advanced Threat Prevention* > *Política de firewall do client*. [DDPS-10782, DDPSUS-3193, DDPSUS-3195]

Aconselhamentos técnicos resolvidos

- O Dell Security Management Server agora aceita caracteres curinga apropriados para o firewall do client. [DDPS-10400]
- Um problema foi resolvido para que o client de criptografia seja ativado ao usar o proxy do Security Server de front-end. [DDPS-10655, DDPS-10741]

Aconselhamentos técnicos da versão 11.6

- Não existem aconselhamentos técnicos.

Novos recursos e funcionalidades da versão 11.5

Novos recursos e funcionalidades incluem:

- Management Console
- Políticas de console de gerenciamento

- Dell Server

Management Console

- O administrador pode definir manualmente o PIN gerenciado pelo BitLocker em um dispositivo no nível *Empresa*, *Endpoint* ou *Grupo de endpoints* para garantir que o acesso a um dispositivo seja restrito apenas a indivíduos que conhecem o PIN. Posteriormente, o administrador pode atualizar o PIN com um novo valor ou redefini-lo sem valor algum. Quando o valor estiver vazio, nenhum PIN gerenciado pelo BitLocker será forçado ou enviado ao client.
- Para dispositivos protegidos com SED ou FDE, em *Grupos de endpoints > Detalhes e ação*, o administrador agora pode selecionar **Bloquear**, **Desbloquear** e **Remover usuários**. O *Tipo de grupo* pode ser *Definido por regra, Definido pelo administrador ou Active Directory*.
- Quando o administrador modifica o estado da Autenticação baseada em vários fatores (MFA) em *Usuários* ou *Grupos de usuários*, o administrador pode acessar **Gerenciamento > Log Analyzer** e selecionar **Ações de administrador** no campo *Categoria*. A coluna *Mensagem* exibe o que mudou, a função de administrador que realizou a ação e o Google Authenticator é redefinido. [DDPS-10438]
- Na seção *Estados > Status de proteção* da tela *Endpoints > Detalhes do Endpoint* de cada disco, uma coluna foi adicionada para o *Número de série do disco*. Esse número é voltado para os volumes protegidos de um dispositivo específico.

Políticas de console de gerenciamento

As políticas localizadas em *Criptografia avançada do Windows > Criptografia BitLocker > Configurações de volume do sistema operacional* foram alteradas:

- O valor da política *Vida útil do PIN do usuário* agora é mostrado em dias, e não em horas. A configuração padrão é definida como 90 dias.
- A política *Vida útil do PIN do usuário* agora permite que um valor 0 seja definido. Esse valor indica para o endpoint que um rodízio de PIN não é necessário no dispositivo.

Dell Server

- O arquivo `application.properties` agora contém as propriedades padrão de tempo de espera excedido e advertência para o console de gerenciamento. O administrador pode modificar esses valores para aumentar ou diminuir o tempo de advertência e o tempo de espera excedido. Os valores padrão são:
  - `idle.warn.seconds=1080`
  - `idle.timeout.seconds=1200`
- O Encryption Enterprise versão 11.5 contém atualizações para dependências de terceiros.
  - O Full Disk Encryption versão 11.5 ou posterior exige o Dell Security Management Server versão 11.5 ou posterior para manter a comunicação entre o client e o servidor.
  - O SED Manager versão 11.5 ou posterior exige o Dell Security Management Server versão 11.5 ou posterior para manter a comunicação entre o client e o servidor.
- O valor padrão de `ssos.domainadmin.verify` foi alterado para **false** a fim de permitir que o administrador registre corretamente o SSOS e reduza a solução de problemas.

Aconselhamentos técnicos resolvidos da versão 11.5

Aconselhamentos de segurança resolvidos

Para resolver problemas de segurança, os itens a seguir foram atualizados.

- A lista de codificações SSL e TLS foi atualizada.
- O Java foi atualizado para a versão 1.8.0.291.
- O Spring Framework foi atualizado.
- O JQuery usado para o console do Dell Security Management Server foi atualizado para a versão 3.5.0. [DDPS-10516]

Aconselhamentos técnicos da versão 11.5

Novos recursos e funcionalidades da versão 11.4

Management Console

- As unidades com criptografia automática e a criptografia completa de disco baseada em software da Dell agora são compatíveis com criptografia de vários discos, permitindo que os administradores protejam todos os discos fixos em endpoints, que contêm todos os drivers com criptografia automática ou todos os discos tradicionais. Essas políticas estão disponíveis nos níveis Empresa, Endpoint e Grupos de endpoints.

  No grupo de tecnologia *Criptografias avançadas do Windows*, as políticas de FDE são:
  - Criptografar todas as Unidades com criptografia automática (vários discos)
  - Criptografia de várias chaves (várias senhas)
  - Criptografar espaço usado primeiro (varredura múltipla)

  No grupo de tecnologia *Criptografias avançadas do Windows*, a política de SED é:
  - Criptografar todas as Unidades com criptografia automática (vários discos)

- A autenticação baseada em vários fatores agora está disponível em **Console de gerenciamento > Administrador de usuários** e **Administrador de grupos de usuários**. Essa opção é exibida somente para as funções de superadministrador e administrador de contas.
- Em **Gerenciamento > Gerenciamento de notificações**, a guia *Configurar SMTP* foi adicionada para permitir que o administrador defina e teste rapidamente as configurações de SMTP no console de gerenciamento.

Aconselhamentos técnicos resolvidos da versão 11.4

Management Console

- Em *Populações, domínios > guia Configurações > Autenticação sem senha*, a saída excessiva de logs foi resolvida. Essa saída excessiva ocorria em raras situações, quando a autenticação sem senha não estava configurada corretamente.
- Um problema foi resolvido em **Advanced Threat Prevention > Políticas de firewall do client** para permitir caracteres curinga na configuração *Bloqueio de DNS*. O administrador pode especificar todos os domínios superiores, por exemplo **.dell.com*, em vez de apenas o nome do domínio. [DDPS-10433]
- Em *Relatórios gerenciados*, um problema é resolvido para que os administradores possam modificar a propriedade csv.export.maxsize para o número de linhas. Além disso, o valor da propriedade não é mais ignorado. [DDPS-10441]
- Em *Relatórios gerenciados*, um problema foi resolvido para que os administradores possam modificar a propriedade email.export.maxsize para o número máximo de linhas a serem exportadas para relatórios agendados por e-mail. Além disso, agora a propriedade é consumida corretamente pelo servidor. [DDPS-10442]
- Um ID de política ausente foi resolvido para que uma nova instalação do servidor no Windows não registre mais erros nos modelos de política após uma confirmação. Isso está relacionado à política *Vida útil do PIN do usuário* em *Criptografias avançadas do Windows > Criptografia BitLocker > Configurações de volume do sistema operacional*. [DDPS-10451]
- Para autenticação baseada em vários fatores, as dicas de ferramenta esclarecem que o OTP deve ter no máximo seis caracteres nos campos *Dell Data Security* e *Configurar o Google Authenticator*. [DDPS-10458]
- Um problema na configuração padrão foi resolvido para que o Security Server agora seja iniciado. [DDPS-10571]

Aconselhamentos técnicos da versão 11.4

- Os campos de entrada para configuração de domínio foram restringidos para permitir que apenas um nome do host seja definido. As pesquisas diretas de nomes diferenciados foram removidas para evitar falhas de pesquisa de LDAP. [DDPS-10388]

Management Console

- Quando a autenticação baseada em vários fatores está configurada para enviar um e-mail, o atributo de e-mail deve ser definido para o usuário no Active Directory. [DDPS-10363]
- A política *Vida útil do PIN do usuário* em *Criptografias avançadas do Windows > Criptografia BitLocker > Configurações de volume do sistema operacional* atualmente não permite um valor desativado. [DDPS-10450]

Novos recursos e funcionalidades da versão 11.3

- Agora, o Dell Encryption em sistemas operacionais de servidor oferece suporte às edições Windows Server 2022 Standard e Datacenter.
- As bibliotecas log4j foram atualizadas para versões não afetadas pelas vulnerabilidades divulgadas recentemente, como CVE-2021-44228.
- O Compliance Reporter foi removido do Security Management Server. Agora, a opção "Gerenciar relatórios" lida com a funcionalidade que, antes, era realizada com o Compliance Reporter.

- Na ferramenta de configuração do servidor, quando o administrador importa um certificado, uma caixa de diálogo confirma que a importação do certificado foi feita com sucesso.
- O DiagnosticInfo coleta informações adicionais, inclusive:
  - Drivers de filtro de classe em uso
  - Versões do produto Dell Data Security
  - Números de série do hardware
  - Servidores instalados e o status de disponibilidade
  - Versões de compilação do Windows
  - Logs dos seguintes elementos:
    - Serviço Baseado em Componente
    - Aplicativos instalados
    - Gerenciamento e manutenção de imagens de implementação
    - Instalação do Security Management Server
    - Ferramenta de configuração do servidor e migração de servidores
    - Defesa contra ameaças
    - VMware Carbon Black
    - Atualizações do Windows

Management Console

- Na guia **Gerenciamento > Gerenciamento de serviços > Gerenciamento de eventos**, uma caixa de seleção permite que o administrador desative ou ative as guias *Ameaças avançadas* e *Eventos de ameaças avançadas*.
- Agora, o valor padrão da política, *Usar criptografia baseada em hardware para unidades de sistema operacional*, é desativado ou removido para novas instalações. A política está em *Criptografia avançada do Windows > Criptografia BitLocker — Configurações de volume do sistema operacional*.

Aconselhamentos técnicos resolvidos da versão 11.3

- O ícone "Política de controle de portas do Windows" é atualizado corretamente para corresponder ao valor principal do switch de políticas.
- Ao fazer log-in no Management Console, se um administrador especificar http:// em vez de https://, o sistema o redirecionará automaticamente. [DDPS-10071]

Aconselhamentos técnicos da versão 11.3

- Não existem aconselhamentos técnicos.

Novos recursos e funcionalidades da versão v11.2

- O Jetty foi atualizado para a versão 9.4.43.

Management Console

- Um nome de política foi alterado na *Criptografia avançada do Windows > Criptografia BitLocker*. Agora, a opção *Desativar o BitLocker em unidades com criptografia automática é Bloquear o BitLocker quando outras políticas do Dell Encryption estiverem presentes*.
- Em *Criptografia avançada do Windows > Criptografia BitLocker > Criptografia BitLocker > Configurações de volume de sistema operacional*, uma nova política força os usuários a redefinir o PIN caso o PIN tenha sido comprometido. A política de vida útil do PIN do usuário define a duração da vida útil do PIN do BitLocker antes de a recriação do PIN ser obrigatória. O valor é expresso em horas, e o valor padrão é 2160.
- Em *Gerenciar relatórios > Evento do EMS*, agora, o identificador plug-and-play por dispositivo (PNPDeviceID) está presente.

Aconselhamentos técnicos resolvidos da versão 11.2

- Foi resolvido um problema para que, se o ID de hardware do servidor contiver espaços em branco, o servidor não seja ativado. [DDPS-10277]

Management Console

- Foi resolvido um problema para que os administradores possam modificar políticas com menus suspensos e salvá-las. *Salvar* não resulta mais em uma caixa de diálogo *Erro ao validar a política*. [DDPS-10225]
- Foi resolvido um problema para que todas as colunas sejam exibidas na página *Gerenciar relatórios* > relatório *Detalhes do dispositivo*. [DDPS-10229]
- Foi resolvido um problema em *Populações* > *Usuários* > *Detalhes do usuário* > *Endpoints* para que, agora, o administrador possa selecionar o número de itens que serão exibidos por página. [DDPS-10258; DDPSUS-30249]
- Na página *Gerenciar relatórios* > Grupos de endpoints, agora, uma coluna permite que os administradores visualizem todos os grupos de endpoints nos quais um endpoint faz parte. É possível filtrar os registros com base no nome do grupo de endpoints. [DDPS-10261]
- Na ferramenta de configuração do servidor, a sintaxe do keytool é corrigida para que, agora, os administradores possam importar um certificado assinado internamente e para que nenhum erro seja exibido nos logs. [DDPS-10267]
- Em "Prevenção contra ameaças" > "Regras de firewall do client", foi resolvido um problema para que as portas personalizadas definidas para TCP ou UDP possam ser salvas ou confirmadas. [DDPS-10268; DDPSUS-3030]
- Na guia *Populações* > *Empresarial* > *Ameaça avançada*, agora, é possível fazer download dos arquivos de ameaça. [DDPS-10275]

Aconselhamentos técnicos da versão 11.2

- Não existem aconselhamentos técnicos.

Aconselhamentos técnicos resolvidos da versão 11.1.1

- Para empresas que usam a política Lista de permissões de dispositivos do EMS, essa versão de patch resolve um problema em que a modificação dessa política bloqueia todas as atualizações de política, especialmente se essas políticas adicionais tiverem um menu suspenso. Para identificar que esse é o problema, visualize a alteração da política adicional no Log Analyzer. O log da política adicional listará o conteúdo da política Lista de permissões de dispositivos do EMS em vez da configuração da política adicional. [DDPS-10225]

Novos recursos e funcionalidades da versão 11.1.0

- Nas páginas "Detalhes do endpoint" do Management Console, agora, o administrador pode pesquisar o ID do hardware.

Aconselhamentos técnicos da versão 11.1.0

- Atualmente, com o Dell Server, ocorre um cenário em que grandes políticas, como grandes conjuntos de regras SDE, Comuns ou PBE do usuário ou muitos itens da lista de permissões do EMS, não conseguem acessar os clients do Dell Encryption. [DDPSUS-2980, DDPC-12553]

Aconselhamentos técnicos resolvidos da versão 11.1.0

- No painel de indicadores do Management Console, agora, os eventos do Advanced Threat Protection estão sendo redirecionados corretamente para as páginas "Detalhes" adequadas. [DDPS-10135]
- Agora, as entradas da lista de permissão de dispositivos do EMS são convertidas em letras maiúsculas para que a exibição dos logs corresponda ao que deve ser aplicado. [DDPS-10169]
- Foi resolvido um problema durante a ativação do Encryption Client para que a verificação do ID de hardware seja validada devidamente. [DDPS-10174]

Aconselhamentos de segurança resolvidos da versão 11.1.0

- Agora, os cabeçalhos Strict-Transport-Security (HSTS) são apresentados a partir do Dell Server, o que impõe a comunicação HTTPS para todo o tráfego. [DDPS-10140]
- A versão do Jetty em execução no Dell Server foi migrada para a versão 9.4.39.v20210325. Essa versão impede a suscetibilidade a uma vulnerabilidade depois de receber um grande quadro TLS inválido. [DDPS-10147, DDPS-10150]

Novos recursos e funcionalidades da versão 11.0.1

- Para autenticação sem senha e informações sobre como configurar o Dell Encryption Enterprise para autenticação com o Windows Hello, consulte o artigo da KB 188216.

Management Console

- Em *Populações* > *Grupos de usuários*, depois de clicar no nome de um grupo e selecionar a guia **Membros**, agora, o administrador pode clicar no botão **Exportar arquivo** para exportar a lista de membros de um grupo de usuários. Isso permite que o administrador faça uma comparação cruzada e, em seguida, utilize-a para criar uma lista de um grupo de usuários definido pelo administrador. Essa opção de exportação apresenta detalhes nas colunas *Usuário*, *Nome distinto* e *Nome comum*.
- Em *Populações* > *Grupos de endpoints*, depois de clicar no nome de um grupo e selecionar a guia **Membros**, agora, o administrador pode clicar no botão **Exportar arquivo** para exportar a lista de endpoints desse grupo de endpoints. Essa opção permite que o administrador faça a comparação cruzada com outros utilitários, crie grupos de usuários adicionais definidos pelo administrador e exporte listas de endpoints para um utilitário de gerenciamento de sistemas de terceiros, como o SCCM. A exportação apresentada dados nas colunas *Categoria (Tipo de SO)*, *Nome de host* e *SO/versão*.
- Na tela *Painel de indicadores* > *Status de proteção de endpoints*, para facilitar a identificação de lacunas de proteção, agora, o administrador pode selecionar uma opção e clicar no botão **Exportar arquivo**. Essa opção exporta a lista de endpoints presentes na lista de endpoints *Protegidos*, *Não protegidos* ou *Totais*. Os dados são exibidos nas colunas *Plataforma*, *ID do endpoint*, *Status de proteção (sim/não)*, *Inventário de proteção recebido*, *Inventário de proteção processado*, *Inventário de agentes recebido* e *Inventário de agentes processado*.

Aconselhamentos técnicos da versão 11.0.1

- Não existem aconselhamentos técnicos.

Aconselhamentos técnicos resolvidos da versão 11.0.1

- Não existem aconselhamentos técnicos resolvidos.

Aconselhamentos de segurança resolvidos da versão 11.0.1

- A versão do PostgreSQL foi atualizada para 11.12, resolvendo várias vulnerabilidades de segurança, inclusive CVE-2019-10164. [DDPS-10148]

Novos recursos e funcionalidades da versão v11.0.0

- Nova autenticação sem senha para os usuários que estão usando a autenticação do Windows Hello. No *Management Console* > *Domínios* > *Configurações de domínio*, os campos adicionais oferecem configuração para ADFS ou Microsoft Azure. [DDPS-9969, 10067]
- Migração de código do servidor para o Visual Studio 2019.

Aconselhamentos técnicos resolvidos da versão 11.0.0

- Foi resolvido um problema em que um método de opção HTTP não tinha sido definido corretamente e resultava em falsos positivos nos scanners de vulnerabilidade quando o servidor era examinado. [DDPSUS-2944]
- Agora, a documentação em português é exibida corretamente no menu Ajuda. [DDPS-9960]
- A linguagem foi modificada para mudar para uma sintaxe mais inclusiva. [DDPS-10031]
- Os direitos autorais do servidor foram atualizados corretamente para 2021. [DDPS-10060]
- Agora, as aprovações de endereço IPv6 são retidas corretamente para o filtro de negação de serviço. [DDPS-10133]
- **Management Console**:
  - A exportação do relatório "Detalhes do dispositivo" falhava devido aos limites de filtro de DoS. Esse problema foi resolvido. [DDPS-10050]
  - Várias melhorias de desempenho foram implementadas para pesquisas no Management Console. [DDPS-10065]

- Agora, as chaves do BitLocker estão sendo preenchidas corretamente por padrão. [DDPS-10085]
- Na guia *Gerenciamento de serviços* > *Gerenciamento de eventos*, uma caixa de seleção *Ativar eventos de ameaça* garante que a guia "Eventos de ameaça" seja exibida em *Populações* > *Empresarial* ou *Populações* > *Endpoints* > *guia Detalhes e ações* > *Detalhes do endpoint*. Na guia "Eventos de ameaça", as opções "Proteção da Web" e "Firewall do client" estão listadas no grupo "Prevenção contra ameaças". [DDPS-10095]
- Foi resolvido um problema para que, ao tentar carregar um domínio existente no Dell Security Management Server que executa a versão 11.0.0, o domínio existente não apresente mais falha ao carregar. [DDPS-10114]
- Agora, a página *Configurações de domínio* reflete corretamente a URL adequada de conexão LDAP quando o LDAP seguro (LDAPS) está em uso. [DDPS-10117]

Aconselhamentos de segurança resolvidos da versão 11.0.0

- Não existem aconselhamentos de segurança.

Aconselhamentos técnicos da versão 11.0.0

- Adicionado em 6/2021 — depois que a política é confirmada, um problema com alterações do Jetty no serviço Message Broker resulta em falhas na política de entrega dos serviços do Policy Proxy. Portanto, o Encryption Client pode não receber as políticas mais recentes. [DDPS-10171]

Novos recursos e funcionalidades da versão v10.2.14

- Com uma mudança global para a linguagem inclusiva, vários termos e expressões foram atualizados.
- As longas listas de políticas dos grupos de políticas foram reestruturadas para aprimorar a capacidade de leitura e o acesso. [DDPS-9667]
- No campo *ID de recuperação* da ferramenta Portal de recuperação de autoatendimento do Dell Data Security, uma caixa de diálogo será exibida com *ID de recuperação inválido* se um administrador digitar um espaço ou quaisquer caracteres especiais além de sublinhado ou hífen.

Aconselhamentos técnicos resolvidos da versão 10.2.14

- No Portal de recuperação, foi resolvido um problema em que o portal se desconecta automaticamente quando um administrador digita um espaço ou quaisquer caracteres especiais além de sublinhado ou hífen no campo "ID de recuperação" e, em seguida, clica em "Obter senha de recuperação". [DDPS-9968]
- **Management Console**:
  - Agora, os administradores podem inserir portas personalizadas com as políticas do firewall do client. [DDPS-9779]
  - A importação de dispositivos para um grupo de endpoints definido pelo administrador não mais diferencia maiúsculas de minúsculas. [DDPS-9967]
  - Agora, foi resolvido um problema de tela para que a notação do LDAPS atualize corretamente a URL do diretório na guia "Configurações de domínio" para exibir o LDAPS quando uma conexão de LDAP seguro é utilizada. [DDPS-9984]
  - Em "Relatórios gerenciados", os usuários não recebem mais e-mails duplicados de relatórios agendados quando vários destinatários são definidos. [DDPS-10015]
- **Portal de recuperação**
  - Agora, o Log Analyzer exibe log-ins por meio do Portal de recuperação, separadamente dos log-ins no Management Console. [DDPS-9941]

Aconselhamentos de segurança resolvidos da versão 10.2.14

- Não existem aconselhamentos de segurança.

Aconselhamentos técnicos da versão 10.2.14

- Ao fazer log-in no Portal de recuperação de autoatendimento com um nome de conta SAM (domínio\usuário), um erro será exibido. A solução temporária é fazer log-in com o UPN (user@domain.com). [DDPS-9974]
- Atualmente, quando uma recuperação do BitLocker é realizada no Management Console, os colchetes são definidos automaticamente no campo "ID de recuperação". Uma caixa de diálogo indica *ID de recuperação inválido*. A solução temporária é remover os colchetes do GUID no campo "ID de recuperação". [DDPS-10085]

Novos recursos e funcionalidades da versão 10.2.13

- Um portal baseado na Web, a ferramenta Dell Data Security - Self-Service Recovery Portal, hospedada pelo Dell Security Management Server, permite que os administradores com funções específicas recuperem dispositivos gerenciados pelo BitLocker. As funções incluem administradores de Recuperação com Autoatendimento, Sistema, Segurança e Suporte.

Aconselhamentos técnicos resolvidos da versão 10.2.13

- No Security Server, a ativação do SSOS não apresenta mais falha nas versões 10.2.11 e posteriores. [DDPS-9843]
- Foi resolvido um problema e, agora, a Server Configuration Tool atualiza os arquivos de configuração do serviço e os arquivos são devidamente assinados. [DDPS-9904]
- **Management Console**:
  - O manuseio de Exceções de Ponteiro Nulo resolveu um problema em que uma pesquisa em branco ou uma pesquisa por um dispositivo específico exibe NaN para o número de endpoints. Agora, as informações são exibidas. [DDPS-9769, DDPS-9910]
  - Foi resolvido um problema de um usuário em um Grupo de Usuários com a função de Administrador de Relatórios, Proprietário do Relatório e Usuário do Relatório. Agora, depois de fazer log-in, o usuário com essas funções pode visualizar o Painel de Indicadores. [DDPS-9773]
  - Em uma *página Detalhes do Endpoint > guia Usuários*, agora, é possível classificar as colunas *Usuário, Último Log-in com Sucesso* e *Último Log-in sem Sucesso*. [DDPS-9819]
  - Foi resolvido um problema na página *Recuperar Dados*, no campo *TPM > Nome do Host*. Se um administrador digitar apenas um espaço, os botões não serão ativados. [DDPS-9829]
  - Na configuração de e-mail, foi adicionado suporte à Autenticação Anônima e foi resolvido um problema relacionado à autenticação habilitada para TLS. Agora, o envio de e-mails, notificações e relatórios periódicos funciona como esperado. [DDPS-9832]
  - Em *Populações > Usuários*, a seta de classificação da coluna *Última Conciliação* agora é exibida. [DDPS-9833]
  - Foi resolvido um problema e, agora, as mensagens de e-mail de Resumo de Notificações são vinculadas ao Management Console. [DDPS-9908]
  - Foi resolvido um problema e, após um upgrade, a página Endpoints agora lista os endpoints. [DDPS-9910]
  - Na guia Configurações do Domínio, foi resolvido um problema e, se o administrador marcar a caixa de seleção LDAP Seguro e salvar as alterações nas configurações de domínio, nenhum erro interno será exibido. [DDPS-9911]
  - Foi resolvido um problema para que seja possível filtrar a página *Detalhes do Shield* em Gerenciar Relatórios e para que ela possa exibir dados. [DDPS-9915]
  - Foi resolvido um problema para que seja possível exportar o relatório *Detalhes do Dispositivo*. [DDPS-9983]

Aconselhamentos de segurança resolvidos da versão 10.2.13

- Não existem aconselhamentos de segurança.

Aconselhamentos técnicos da versão 10.2.13

- **Management Console**:
  - No momento, quando o administrador executa uma importação em massa para um Grupo de Endpoints definido pelo administrador e não há uma correspondência exata das letas maiúsculas e minúsculas, a importação apresenta falha. [DDPS-9967, DDPSUS-2891]
- **Recovery Portal**:
  - No momento, se um administrador copiar o URL conectado do Recovery Portal e o colar em outro navegador, o administrador não precisará fazer log-in novamente. [DDPS-9961]

- No momento, ao usar o mesmo navegador para fazer log-in como superadministrador no Management Console e, depois, em uma guia separada no Recovery Portal, será exibida uma caixa de diálogo Acesso Negado. A solução temporária é desconectar-se e, depois, fazer log-in em navegadores separados ou, primeiramente, fazer log-in no Recovery Portal. [DDPS-9965]

Novos recursos e funcionalidades da versão 10.2.12

- Agora, os certificados Cryptographic Next Generation são compatíveis.
- Para clientes que adquiriram o VMware Carbon Black e o Dell Encryption por dispositivo da Dell, agora, há suporte disponível para direitos padronizados.
- Essa funcionalidade se aplica ao Management Console:
  - O console de gerenciamento preexistente se tornou obsoleto. O URL de log-in preexistente e os URLs correspondentes não estão mais disponíveis.
  - O Microsoft Edge (Chromium) é compatível.
  - Para Security Management Servers recém-implementados, agora, a política *Sincronizar Usuários na Ativação do PBA* do grupo de políticas *Autenticação Pré-Inicialização* é ativada por padrão para sincronizar todas as contas de usuário ativas com o PBA durante a ativação. Isso ajuda a garantir que os usuários possam fazer log-in após a ativação do PBA e reduz as ocorrências em que os usuários devem realizar uma recuperação manual.
  - Em *Criptografia do Windows* > *Criptografia do BitLocker*, a política *Desativar o BitLocker em Unidades com Criptografia Automática* foi renomeada como *Bloquear o BitLocker Quando Outras Tecnologias Dell Encryption Estiverem Presentes* e o texto exibido ao passar o mouse foi simplificado.
  - O relatório Detalhes do Dispositivo em *Geração de Relatórios* > *Gerenciar Relatórios* > *Criar Novo Relatório* > *Detalhes do Dispositivo* contém uma nova coluna intitulada *Tecnologias Ativadas*.

Aconselhamentos técnicos da versão 10.2.12

- No momento, os dispositivos Server Encryption podem não ser ativados depois que um servidor recebe upgrade para a versão 10.2.11 ou posterior. Os dispositivos existentes permanecem criptografados. [DDPSUS-2839, DDPS-9843, DDPC-12115]

Aconselhamentos técnicos resolvidos da versão 10.2.12

- **Management Console**:
  - Na *página Detalhes do Endpoint* > *guia Detalhes e Ações,* a seção *Estados* exibe somente os discos presentes no último inventário que foi recebido do endpoint. Os dados históricos relacionados aos discos são retidos, mas não são mais exibidos. [DDPS-4239]
  -
  - Na *página Detalhes do Endpoint* > *guia Detalhes e Ações* > *seção Plug-ins e Agentes* > coluna *Plug-in do Endpoint,* foi adicionada uma descrição textual ao passar o ponteiro do mouse sobre cada valor da coluna *Plug-ins e Agentes*. [DDPS-5580]
  - Em *Detalhes do Endpoint* > *Detalhes e Ações* > *Plug-ins e Agentes*, são exibidos somente os plug-ins do último check-in no endpoint. Os plug-ins exibidos mudam quando o estado do plug-in é alterado de **qualquer estado (Ativo, Disponível)** para **Não presente** ou vice-versa. [DDPS-7421]
  - Em *Gerenciamento* > *Gerenciamento de Serviços* > *Gerenciamento de Eventos*, ao ativar a caixa de seleção *Exportar ao Arquivo Local* em *Exportar Eventos para um Sistema SIEM*, agora, o administrador deve digitar um caminho absoluto no campo *Localização do Arquivo* para salvar as preferências. [DDPS-9616]
  - Com a autenticação SQL, ao modificar as configurações do banco de dados na Server Configuration Tool, a senha do banco de dados agora é gravada em disco de forma criptografada, e não em texto simples. Anteriormente, a senha do banco de dados era criptografada assim que os serviços eram iniciados. [DDPS-9627]
  - Agora, o administrador de segurança tem acesso ao Log Analyzer. [DDPS-9701]
  - Foi resolvido um problema em que, após uma atualização, as mensagens de notificação por e-mail não eram enviadas corretamente se a opção **TUDO** fosse selecionada para TIPO e PRIORIDADE, resultando em um campo de filtro incorretamente NULO. Agora, esse campo é processado corretamente e a notificação é enviada. [DDPS-9725]
  - Foi resolvido um problema em que o relatório Detalhes da Proteção, de Gerenciar Relatório, excede o tempo de espera com muitos endpoints e ao obter dados durante o horário de pico. [DDPS-9727]
  - Foi resolvido um problema e, se um servidor for criptografado e uma varredura for concluída, o status Protegido e a Data serão exibidos no Management Console. [DDPS-9757]
  - Foi resolvido um problema em que os administradores de funções com acesso insuficiente para ver a página *Gerenciamento* > *Recuperar Endpoint* podiam clicar no link e, em seguida, desconectar-se. Agora, não poderão mais fazer isso. O link é exibido apenas para os administradores cujas funções incluem a recuperação de endpoints. [DDPS-9772]

- Na página *Detalhes do Endpoint > Detalhes e Ações*, agora, a classificação está funcionando na seção Controle de Dispositivos do Servidor dos endpoints aplicáveis. [DDPS-9800]
- Em *Populações > Grupos de Usuários > Editar Prioridade > Modificar Página de Prioridades dos Grupos de Usuários*, a classificação da coluna de prioridade agora está desativada, que é o comportamento anterior. [DDPS-9802]
- Foi resolvido um problema em que, em situações raras, as licenças do Threat Protection eram consumidas quando o Advanced Threat Prevention também estava instalado. [DDPS-9808, DDPSUS-2816, DDPSUS-2590]

Aconselhamentos de segurança resolvidos da versão 10.2.12

- Não existem aconselhamentos de segurança.

Novos recursos e funcionalidades da versão 10.2.11

- O SQL Server 2019 agora é compatível.
- Agora, o Microsoft Edge é compatível.
- O Security Management Server pode ter problemas com os elementos de IU do Internet Explorer 11. Devido à falta de suporte para os mecanismos modernos da Web, o Internet Explorer 11 não será mais compatível.
- O Security Management Server é compatível com o requisito da Microsoft de vinculação de canal LDAP e assinatura LDAP quando o Active Directory está em uso.

  Para ativar esse requisito no Security Management Server, você deve ter o certificado de emissão da raiz para os certificados do controlador de domínio importados no armazenamento de "Raiz Confiável" do Keystore de Certificados da Microsoft.
- Agora, as licenças adquiridas de forma padronizada podem ser inseridas em massa em um arquivo .csv. Para obter esse arquivo, entre em contato com o representante de vendas ou o suporte da Dell Security.
- Agora, o serviço Security Server adiciona automaticamente os endereços IP locais do servidor à ipWhitelist na inicialização do serviço.
- Management Console:
  - Em **Gerenciamento > Confirmar Políticas**, a ajuda integrada agora também inclui conteúdo para *Visualizar Confirmações Pendentes*.
  - Na página Endpoints, as colunas PBE e Gerenciador não são mais incluídas como parte das informações do endpoint. Agora, uma coluna *Tecnologias Ativadas* exibe todos os plug-ins ativados no endpoint.
  - O campo Lista de Permissões de Dispositivos EMS agora aceita um máximo de 150 caracteres por linha e 500 linhas.

Aconselhamentos técnicos resolvidos da versão 10.2.11

- O arquivo de recuperação do Encryption baixado do Security Management Server não está mais envolvido em um arquivo executável e não requer a execução de um comando para extraí-lo. [DDPS-5054]
- As tabelas do banco de dados APNS (Apple Push Notification Server), que são usadas para suporte a dispositivos iOS, foram removidas. [DDPS-9453]
- As tabelas do banco de dados do MDM (suporte a dispositivos móveis) foram removidas. [DDPS-9454]
- Ao enviar um e-mail pelo JavaMail na página **Management Console > Gerenciamento de notificações**, o Console envia o e-mail como anônimo. A atualização para a versão mais recente do JavaMail resolveu o problema. [DDPS-9494]
- A senha usada ao fazer download de um pacote de recuperação de endpoint não é mais gravada em texto simples no arquivo output.log dos logs do Security Server ao usar o modo de depuração. [DDPS-9541]
- Na página **Management Console > Gerenciamento de notificações**, a caixa de diálogo *Enviar E-mail de Teste* agora exibe as informações corretas. [DDPS-9542]
- Devido à depreciação do produto, o arquivo `cloud-profile-updater. properties` foi removido de `'/opt/dell/server/security-server/conf'` e de `'/opt/dell/server/security-server/bin'`. [DDPS-9544]
- No **Management Console > Grupos de usuários**, quando um administrador tenta conceder a um grupo uma função de administrador mais alta que a designada à própria conta do administrador, é exibida uma mensagem *Acesso Negado* em vez de *Erro Interno*. [DDPS-9548]
- Ao atualizar o certificado de um Security Management Server usando a opção **Configuração avançada > Certificados do servidor > Criar e instalar certificado autoassinado**, o sistema atualiza a tabela *signingcertificate* como esperado.[DDPS-9549]
- Se o Management Console excede o tempo de espera e não consegue se conectar ao Security Management Server, é exibida uma caixa de diálogo *Conexão Recusada* mais descritiva. Clicar em **OK** redireciona o usuário à página de log-in. [DDPS-9557]
- No campo **Security Management Server > Suporte ao Servidor DMZ**, agora, o campo Nome do Host aceita qualquer FQDN ou nome do host válido, inclusive os que começam com um número. [DDPS-9561, DDPS-9561]

- Agora, é possível classificar os Eventos de Ameaças com base em um Endpoint individual. [DDPS-9568]
- Agora, selecionar a opção Ignorar para um Grupo de Endpoints exibe corretamente uma caixa de diálogo de confirmação. [DDPS-9596]
- Foi resolvido um problema em que a Política Vigente de um Endpoint ou Usuário não era atualizada corretamente. [DDPS-9621]
- Foi resolvido um problema em que a Exibição de Falhas de Criptografia não carregava no Security Management Server. [DDPS-9622]
- Os administradores com a função de Administrador de Segurança podem selecionar corretamente as opções Remover e Adicionar Endpoints a Grupos no Security Management Server. [DDPS-9626]
- O recurso Threat Protection do Painel de Indicadores agora exibe corretamente o indicador de cores conforme a Categoria da Ameaça. [DDPS-9634]
- Agora, o ID do Dispositivo é vinculado ao endpoint da guia *Eventos de Ameaças*. [DDPS-9640]
- Ao se conectar ao servidor Cylance na guia **Management Console > Ameaças Avançadas**, não é mais exibida uma mensagem de espera. [DDPS-9650]
- No **Management Console > Gerenciamento > Gerenciamento de Serviços > Gerenciamento de Eventos**, foi resolvido um problema em que os logs do Security Server exibiam eventos recentes, mas não exportavam eventos quando um evento inesperadamente mais antigo era detectado. [DDPS-9662]
- Os administradores com a função de Suporte não podem mais remover os endpoints apresentados na guia *Detalhes e Ações* de um endpoint. [DDPS-9698]
- Mais uma vez, os Eventos de Ameaças Avançadas podem pesquisar por nome do host ou hash SHA256. [DDPS-9710]

Aconselhamentos de segurança resolvidos da versão 10.2.11

- Foram resolvidas várias vulnerabilidades baseadas em Java. [DDPS-9101, DDPS-9332]

  Foram feitas atualizações nestas versões:
  - Versão Java: 1.8.0.241
  - Versão Jetty: 9.4.25
-

Aconselhamentos técnicos da versão 10.2.11

- No Management Console, se os endpoints forem exibidos sem o Número de Série, o administrador deverá definir as seguintes informações:
  - Entradas `UseBiosSerialNumber` no arquivo InventoryObjects.config (do Core Server para Encryption Enterprise; no Core Server e Inventory Server para Virtual Edition)
  - DeviceInventoryQueueProcessor
  - AgentInventoryQueueProcess

  Em seguida, o client e o agente devem ser atualizados para usar o campo *Etiqueta de inventário*, e não o campo *Serial* que é armazenado nas entradas `DeviceData:UseBiosSerialNumber`. [DDPS-9619]
- O Log Analyzer não tem a capacidade de filtrar usando uma hora de início e de término. [DDPS-9637]
- Os e-mails de relatório agendados por meio do recurso **Management Console > Geração de Relatórios > Gerenciar Relatórios** não localizam o assunto do e-mail devidamente para os idiomas japonês e coreano. [DDPS-9643]
- No momento, a notificação **Alterações das Políticas Não Confirmadas** é exibida para os administradores cujas funções não têm permissão para confirmar a política. Se eles tentarem confirmar as políticas pendentes, serão desconectados do Management Console. [DDPS-9702]
- No Management Console, os bancos de dados do MDM foram removidos. Portanto, a página Endpoints mostrará um erro: `Exception thrown in webservice controller java.lang.RuntimeException: NOT IMPLEMENTED: MDM_DEVICE`. No momento, esse problema não será corrigido. [DDPS-9729]

Novos recursos e funcionalidades da versão 10.2.10

- O Security Management Server foi aprimorado por meio de várias correções e aprimoramentos de segurança. Consulte Aconselhamentos de segurança resolvidos da versão 10.2.10 para obter mais informações.
- As respostas das consultas do LDAP são reforçadas no Security Management Server.
- Agora, o Security Management Server é assinado por um certificado de assinatura SHA256, pois o certificado de assinatura SHA1 está obsoleto

- A política Sincronizar Usuários na Ativação do PBA agora é ativada por padrão.
- O Security Management Server agora é integrado ao InstallShield 2019.
- O Security Management Server 10.2.10 agora oferece suporte ao VMware ESXi 6.7
- As colunas *Visto pela primeira vez no sistema* e *Visto pela última vez no sistema* foram adicionadas a **Populações > Endpoints > Detalhes e Ações** de cada disco do endpoint selecionado.
- Ao se comunicar com o Cylance SaaS, os atrasos na comunicação são apresentados com a seguinte mensagem:

  Tentando se conectar ao Cylance neste momento. Verifique novamente em instantes.

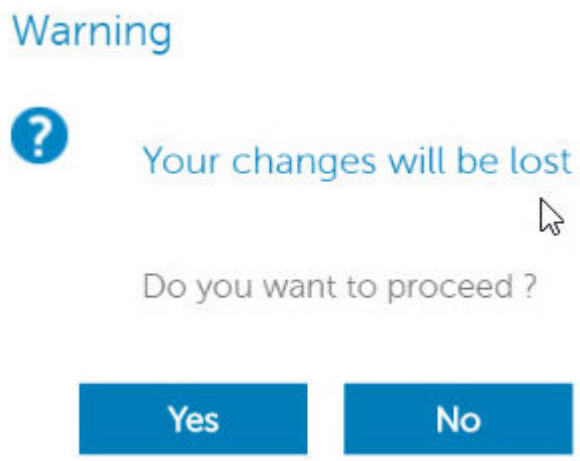
- No upgrade, todos os usuários são conciliados pelo Security Management Server para garantir que todos os grupos e usuários sejam refletidos com precisão no Management Console.
- Agora, o tenta limpar o banco de dados de auditoria por padrão e cumpre o limite de 80% do tamanho atribuído de 10 GB do banco de dados. Essa ação de limpeza impede a exibição de erros críticos no painel *Notificações do Painel de Indicadores*, que anteriormente detalhava que o Banco de Dados de Auditoria excedeu sua limitação de tamanho de 95%.

  Agora, a propriedade **auditdb.size.NotificationPercentage** é incluída em **Application.properties** do Security Server para gerenciar o tamanho do banco de dados de Auditoria do Advanced Threat Prevention.

  A propriedade **auditdb.size.percentage** é o limite de limpeza. Quando essa porcentagem do banco de dados for excedida, depois que **auditdb.clear.cron** for ativado, a porcentagem do espaço total será calculada. O valor padrão de **auditdb.clear.cron** é a cada duas horas.

  Se o valor de **auditdb.size.NotificationPercentage** for excedido, uma notificação da limpeza exibirá o Security Management Server, e a duração definida em **auditdb.cleanup.delete.hours** será usada para limpar os dados do banco de dados ddp_audit para que ele fique abaixo do limite **auditdb.size.percentage**.

- Depois de fazer upgrade do Security Management Server, os seguintes campos exibem a data atual, e não o valor Nulo:
  - Ativação do Shield
  - Autenticação de PBA
  - Log-in na IU Web
  - Criação de Usuário na IU Web
  - Sincronização do Policy Proxy
- Ao passar de uma página para a outra, o seguinte prompt será exibido se as alterações de política não forem salvas.



Aconselhamentos técnicos resolvidos da versão 10.2.10

- A página *Sobre* do Management Console agora exibe corretamente o *Modo Desconectado* quando o Modo Desconectado está em uso. [DDPS-9369]
- Os comandos do PBA Device Control agora funcionam como esperado. [DDPS-9373]
- Agora, o Management Console excede o tempo de esperada como esperado depois de 30 minutos de inatividade. [DDPS-9387]
- Agora, o Controle de Portas do Windows exibe corretamente um visto verde na guia Política de Segurança, quando ativada. [DDPS-9397]
- Os privilégios de usuário agora são avaliados corretamente depois de qualquer modificação na associação ao Active Directory. [DDPS-9401, DDPSUS-2689, DDPSUS-2702]

- A função de classificação de *Notificações do Painel de Indicadores* agora se comporta como esperado. [DDPS-9405]
- Agora, é possível descartar as notificações como esperado. [DDPS-9406]
- A remoção de um dispositivo de um Grupo de Endpoints não resulta mais em uma página da Web javascript:null. [DDPS-9421]
- Quando o serviço Dell PostgresSQL fica inacessível, a seguinte mensagem é exibida:

  Não é possível acessar o banco de dados. Verifique se o serviço PostgreSQL da Dell foi iniciado. [DDPS-9462]

- Agora, a página *Terceiros* exibe corretamente todas as informações de terceiros. [DDPS-9476]
- O Relatório de Detalhes do BitLocker Manager agora exibe corretamente as letras das unidades. [DDPS-9496, DDPSUS-2714]
- Agora, os Logs de Políticas da página *Confirmar* exibem informações válidas de data e hora no Log Analyzer ao usar um idioma diferente do inglês no navegador. [DDPS-9514]
- Os usuários com privilégios de Administrador agora podem criar Grupos de Endpoints e podem adicionar ou remover dispositivos do painel *Membros* do Management Console, como esperado. [DDPS-9515]
- O Security Management Server agora pode ser configurado para permitir ativações não relacionadas ao domínio. Se seu ambiente exigir esse fluxo de trabalho de ativação, consulte o artigo da base de conhecimento (KB) SLN306341. [DDPS-9531, DDPSUS-2578]
- Adicionado em 12/2020 — o Microsoft Edge é compatível. [DDPS-9814]

Aconselhamentos de segurança resolvidos da versão 10.2.10

- Foi resolvido um problema que permite a desserialização remota de dados por meio de uma interface RMI. Para obter mais informações, consulte o artigo da KB SLN320536. [DDPS-9446]
- Foi resolvido um problema que fazia com que os usuários com função de Administrador de Conta do Security Management Server elevassem suas permissões de forma inadequada. [DDPS-9516]
- Foi resolvido um problema em que cabeçalhos em branco eram exibidos incorretamente durante uma verificação de segurança. [DDPS-9519]

Aconselhamentos técnicos da versão 10.2.10

- Em raras circunstâncias, as políticas não aceitas não exibem um erro. Como solução temporária, verifique se há Valores Inválidos nos logs do Security Server. [DDPS-9501, DDPS-9534]
- Se o nome comum de um usuário for alterado no nível do Controlador de Domínio, o Management Console não refletirá o novo nome. [DDPS-9510]
- Se uma notificação de e-mail existente for modificada e salva, a próxima nova notificação de e-mail herdará as modificações da notificação anterior. [DDPS-9527]
- As ativações não relacionadas ao domínio que usarem o mesmo nome do host e o nome de usuário anteriormente ativados em um Security Management Server não serão ativadas e registrarão a falha abaixo no Compatibility Server. `Illegal activation attempt of non-domain User` [DDPS-9531, DDPSUS-2578]
- O botão **Atualizar** não está disponível no Management Console, nas seguintes páginas:
  - Domínios
  - Grupos de usuário
  - Usuário
  - Grupos de endpoint
  - Detalhes e Ações do Endpoint

  Como solução temporária, atualize o navegador. [DDPS-9532]

- Após a ativação inicial do Advanced Threat Prevention no Management Console, a página *Detalhes de Ameaças Avançadas* não é exibida corretamente. Como solução temporária, desconecte-se e faça log-in novamente no Management Console. [DDPS-9533]
- Ao recriar os certificados autoassinados do Security Management Server Virtual, o certificado de assinatura de políticas do Dell Manager não é recriado. Como solução temporária, importe um certificado com base em um certificado criado anteriormente (consulte o artigo da base de conhecimento (KB) SLN302996 para obter mais informações). Como alternativa, selecione **importar um certificado existente** e a opção **server.p12** para o Certificado e, em seguida, **server.key** para a chave privada. A senha padrão dessa chave é `changeit`. [DDPS-9549]
- No momento, não é possível classificar a guia Eventos de Ameaças do Enterprise e por Endpoint. [DDPS-9568]
- Ao modificar a lista de prioridades dos Grupos de Endpoints ou Grupos de Usuários, tentar classificar por Prioridade na fase de edição resultará em uma mensagem de erro interno e a classificação não será atualizada automaticamente. Cancele a operação ou atualize a página para retornar à página Grupo. Como solução temporária, não classifique ao editar a lista de prioridades. [DDPS-9567]
- O banner *Políticas Não Confirmadas* poderá persistir depois de confirmar as alterações de políticas existentes no Management Console ao usar o Internet Explorer 11 ou versões anteriores. [DDPS-9571]

Novos recursos e funcionalidades da versão 10.2.9

- Agora, é possível visualizar as alterações de políticas em Gerenciamento > Confirmar selecionando **Visualizar Logs**. A tela **Visualizar Logs** exibe uma visão geral das alterações de políticas associadas à confirmação selecionada.
- Agora, as novas instalações do Security Management Server monitoram o TLS 1.2 por padrão para todos os serviços baseados em Java, inclusive o Dell Security Server, o Dell Device Server e o Dell Compliance Reporter Server. Observe que o Dell Core Server não está configurado por padrão para usar o TLS 1.2 em novas instalações para evitar a introdução de problemas de compatibilidade com outros aplicativos que possam existir no mesmo servidor.

  O upgrade do Security Management Server não os altera por padrão para evitar problemas de compatibilidade com os dispositivos atualmente conectados. Para obter informações sobre como modificar os protocolos SSL/TLS aceitos para as instalações existentes do Security Management Server, e para obter informações sobre como proteger o Dell Core Server, um serviço baseado no Microsoft .NET, consulte o artigo da base de conhecimento (KB) SLN313386.

Aconselhamentos técnicos resolvidos da versão 10.2.9

- Agora, a remoção de prompts de substituição para as alterações pendentes de políticas exibe o número correto de alterações em Políticas Não Confirmadas. [DDPS-3974]
- A mensagem de erro correta agora é exibida ao adicionar um domínio com um número de porta inválido. [DDPS-6263]
- Em Gerenciamento de Licenças, a dica correta agora é exibida quando o pool de licenças é excedido. [DDPS-7176]
- Agora, todo o texto é exibido corretamente ao adicionar ou modificar Grupos de Endpoints ou Grupos de Usuários. [DDPS-7177]
- Agora, a página Gerenciamento de Eventos em alemão e francês é exibida corretamente. [DDPS-7249]
- Agora, editar funções de administrador no Management Console gera uma mensagem de aviso precisa. [DDPS-7300, DDPSUS-2311]
- Agora, as licenças do Threat Protection são consumidas devidamente quando os produtos são instalados e desativados. [DDPS-8925, DDPSUS-2590]
- Foi resolvido um problema que causa a não exibição de uma coluna em Grupos de Endpoints. [DDPS-8832]
- A validação da senha não apresentará mais um erro se a senha de um administrador contiver aspas duplas. [DDPS-8936]
- Ao instalar o Security Management Server no Windows, o serviço ACL será iniciado como esperado se a senha do administrador contiver uma barra invertida. [DDPS-8938]
- Foi resolvido um problema que resultava na falha das importações de certificados ao Security Server. [DDPS-8939]
- Foi resolvido um problema que resultava em bancos de dados truncados após a falha de um upgrade. [DDPS-8940]
- Agora, o Management Console exibe o número correto de endpoints protegidos na página Painel de Indicadores e na página Endpoints. [DDPS-8868]
- O instalador do Security Management Server agora calcula o espaço obrigatório para o banco de dados de Auditoria Postgres na unidade do sistema. [DDPS-9059]
- Foi resolvido um problema que fazia com que a raiz Digicert não fosse importada após o upgrade do Security Management Server. [DDPS-9246]
- Em Gerenciar Relatórios > Enviar Agendamentos de Relatório por E-mail, o título da página agora é exibido corretamente. [DDPS-9275]
- Foi resolvido um problema causado por um servidor syslog/SIEM definido incorretamente em Gerenciamento de Eventos do Management Console que causava um loop no trabalho de exportação de Eventos de Auditoria e o uso excessivo da CPU. [DDPS-9307]
- Foi resolvido um problema que fazia com que o comando *Ignorar Log-in* fosse definido incorretamente como o comando *Desbloquear* para dispositivos com um ambiente de Autenticação Pré-Inicialização. [DDPS-9308]
- Agora, a Tecnologia de Criptografia é exibida corretamente no painel Detalhes do Dispositivo quando um endpoint específico é selecionado. [DDPS-9310]
- As modificações na configuração do syslog em Gerenciamento de Serviços > Gerenciamento de Eventos agora são registradas nos logs do Security Server e nos logs de Ação do Administrador, como esperado. [DDPS-9329]
- Agora, os Dados de Eventos de Ameaças Avançadas são exportados no nível de Endpoint, como esperado. [DDPS-9327, DDPSUS-2658]

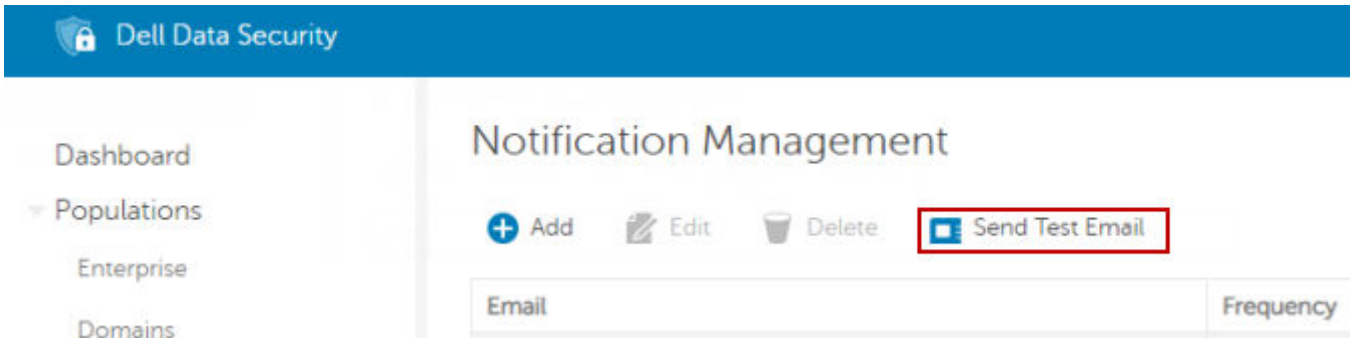
Aconselhamentos técnicos da versão 10.2.9

- Não existem aconselhamentos técnicos.

Novos recursos e funcionalidades da versão 10.2.7

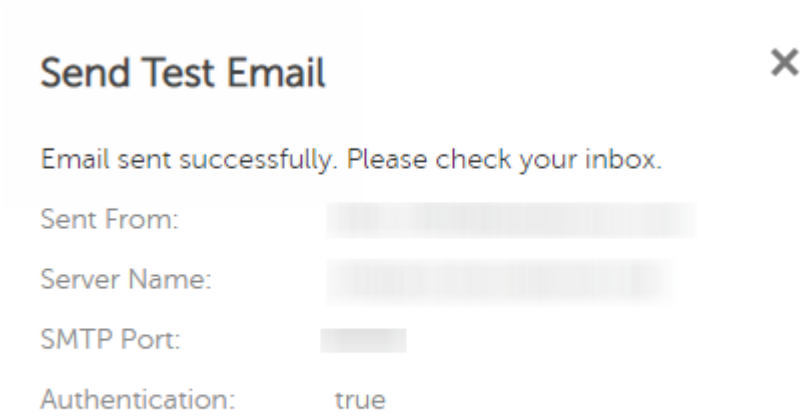
- Em Populações > Grupos de Endpoints, os grupos agora são exibidos por prioridade das políticas.
- Os grupos de endpoints têm uma nova opção para criar grupos com base em um TPM Presente ou em um TPM Ativo em um dispositivo com o Dell Encryption instalado.
- Agora, é possível enviar e-mails de teste no Management Console para validar os fluxos de trabalho de e-mail.

  Para testar o fluxo de trabalho de e-mail:
  1. Navegue até **Gerenciamento > Gerenciamento de Notificações**.
  2. Selecione **Enviar e-mail de teste**.

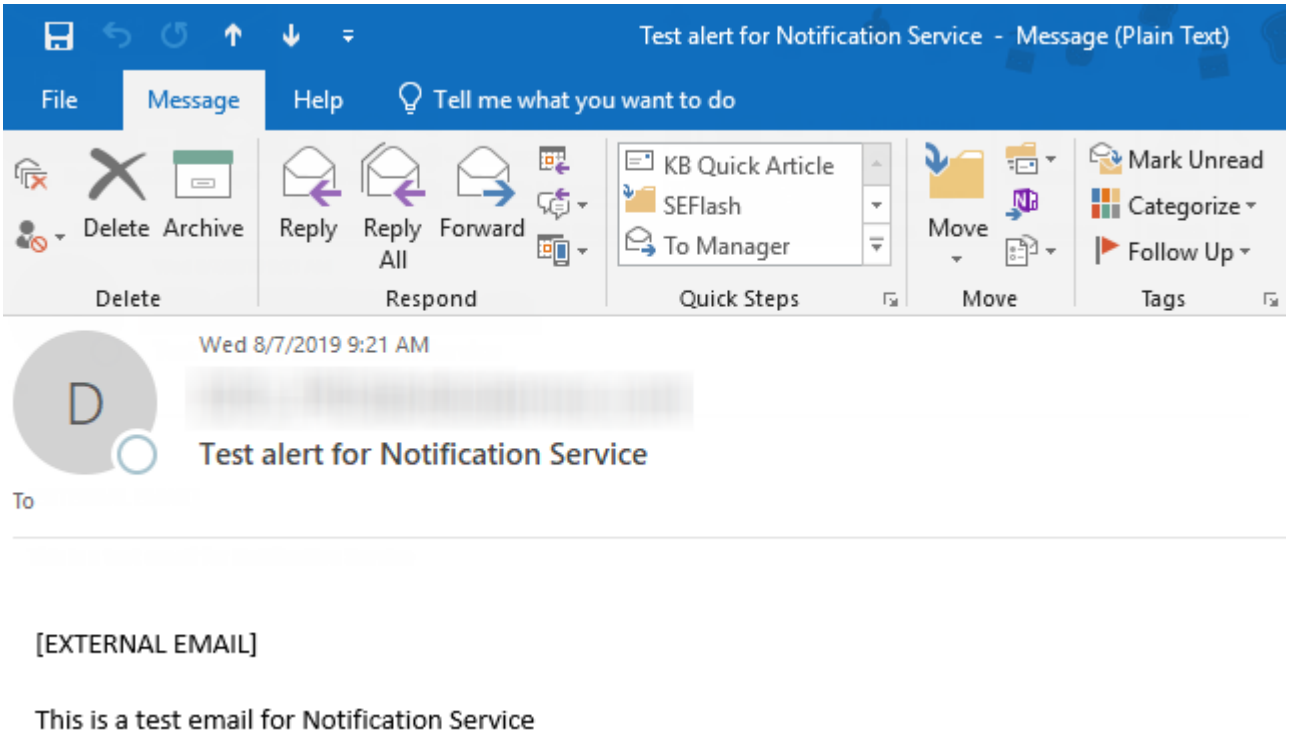


  3. Especifique o e-mail para testar e selecione **Enviar E-mail**.

  Se o e-mail passar pelo Dell Server com sucesso, a tela de resultados abaixo será exibida.



  Este é um exemplo de um e-mail de teste de sucesso.



Aconselhamentos técnicos resolvidos da versão 10.2.7

- Agora, a Server Configuration Tool atualiza todos os elementos obrigatórios ao importar certificados SSL e TLS. [DDPS-8450]
- Os processos de autenticação relacionados ao Message Broker do Dell Server foram aprimorados. [DDPS-8456]
- Os serviços foram reforçados para melhorar a postura de segurança. [DDPS-8487, DDPS-8689, DDPS-8740]
- Foi resolvido um problema que resultava na exibição de um número impreciso de substituições de políticas. [DDPS-8492]
- Ao alterar os valores de prioridade da Proteção Baseada em Conteúdo, todos os valores são preenchidos e permanecem como esperado. [DDPS-8531]
- É possível remover os dispositivos móveis selecionados de Populações > Endpoints como esperado. [DDPS-8853]
- Em Populações > Endpoints, a opção Exportar Arquivo como um Documento do Excel agora funciona como esperado. [DDPS-8857]
- As novas notificações por e-mail não herdam mais as modificações das notificações por e-mail existentes. [DDPS-8881]
- Agora, os e-mails agendados de geração de relatórios são enviados no horário agendado. [DDPS-8888]
- Agora, a opção Gerenciar Relatórios só aceita e-mails diferenciados por valores separados por vírgulas. [DDPS-8955]

Aconselhamentos técnicos da versão 10.2.7

- Agora, o banco de dados de Auditoria Postgres é instalado em C:/ProgramData. No momento, o instalador do Security Management Server não calcula o espaço obrigatório para o banco de dados de Auditoria Postgres na unidade do sistema. [DDPS-9059]

Novos recursos e funcionalidades da versão 10.2.6

- O serviço ACL da Dell foi renomeado como serviço Dell Access Group.

Aconselhamentos técnicos resolvidos da versão 10.2.6

- Agora, o arquivo de ajuda integrado do Security Management Server é traduzido automaticamente e corretamente para todos os idiomas compatíveis com base no local do navegador. [DDPS-8566]

- Agora, os aplicativos e arquivos de recursos do Security Management Server são assinados pelos certificados de assinatura de código SHA-1 e SHA-256 da Dell. [DDPS-8711, DDPS-8712, DDPS-8722, DDPS-8723]
- Os Grupos de Usuários e Grupos de Endpoints não aceitam mais caracteres especiais no campo Prioridade ao usar o Internet Explorer. [DDPS-8735]
- É possível pesquisar os campos como esperado em Relatórios Gerenciados. [DDPS-8737]
- Agora, os valores Tipo e Prioridade são retidos após a atualização do campo E-mail em Editar Notificações. [DDPS-8755]

Aconselhamentos técnicos da versão 10.2.6

- No momento, não é possível remover os dispositivos móveis selecionados de Populações > Endpoints. Como solução temporária, selecione o nome do host do dispositivo móvel e, em seguida, a opção **Remover** na página Detalhes do Endpoint. [DDPS-8853]
- Em Populações > Endpoints, a opção Exportar Arquivo como um Documento do Excel apresenta o erro 404. [DDPS-8857]
- Em Painel de Indicadores > Status da Proteção de Endpoints > Status da Proteção, a coluna Shield foi renomeada como PBE. [DDPS-8771]
- No momento, os comandos do Cloud Device Control não geram logs. [DDPS-8866]
- Se uma notificação de e-mail existente for modificada e salva, a próxima nova notificação de e-mail herdará as modificações da notificação anterior. [DDPS-8881]
- Os e-mails agendados de geração de relatórios são enviados 30 minutos depois do horário agendado. [DDPS-8888]
- Se a senha de um administrador contiver aspas duplas, a validação da senha apresentará falha e será exibida a seguinte mensagem:

  As credenciais são inválidas. Verifique o login e a senha. [DDPS-8936]

- Ao instalar o Security Management Server no Windows, se a senha do administrador contiver uma barra invertida, o serviço ACL não será iniciado, resultando em um tempo de espera excedido. [DDPS-8938]

Novos recursos e funcionalidades da versão 10.2.5

- Não existem novos recursos nem funcionalidades.

Aconselhamentos técnicos resolvidos da versão 10.2.5

- O desempenho da pesquisa por dados de Eventos de Ameaças Avançadas e Eventos de Auditoria foi aprimorado. [DDPS-8342, DDPS-8373]
- A versão padrão do PostgreSQL foi atualizada para resolver vulnerabilidades de terceiros. O serviço PostgreSQL utilizado pelo Security Management Server foi renomeado como Dell PostgreSQL 10.7. [DDPS-8480, DDPS-8985]
- Não é mais exibido um erro para um usuário externo ao tentar pré-compartilhar o acesso à chave com outro usuário externo. [DDPS-8664]

Aconselhamentos técnicos da versão 10.2.5

- Ao usar o Internet Explorer e editar a prioridade, os Grupos de Usuários e Grupos de Endpoints aceitam incorretamente caracteres especiais no campo Prioridade. [DDPS-8735]
- Os valores Tipo e Prioridade não são retidos após a atualização do campo E-mail em Editar Notificações. [DDPS-8755]

Novos recursos e funcionalidades da versão 10.2.4

- O Windows Server 2019 (Standard/Datacenter) agora é compatível.

Aconselhamentos técnicos resolvidos da versão 10.2.4

- Atualizado em 6/2019 — as funções Administrador de Relatórios, Proprietário do Relatório e Usuário do Relatório agora podem fazer log-in no Management Console, como esperado. [DDPS-6101, DDPS-8625]

- Foi resolvido um problema que resulta na persistência dos campos *Tipo* e *Prioridade* depois da criação de várias notificações no Management Console. [DDPS-6779]
- Foi resolvido um problema em que datas com formatação inválida geram eventos do SIEM/Syslog incorretamente na rede ou nos destinos locais. [DDPS-7570, DDPSUS-2325]
- Foi resolvido um problema que fazia com que os Relatórios Gerenciados não exibissem eventos do EMS. [DDPS-8561, DDPSUS- 2532]
- Foi resolvido um problema que fazia com que usuários com direitos adequados de arquivo não fossem exibidos na IU Pré-Compartilhamento. [DDPS-8567]
- Foi resolvido um problema em que o Core Server, o serviço ACL e o Key Server do Security Management Server não iniciavam após uma reinicialização. Para obter mais informações, consulte https://www.dell.com/support/article/us/en/04/sln316840. [DDPS-8522]

Aconselhamentos técnicos da versão 10.2.4

- Não existem aconselhamentos técnicos.

Aconselhamentos técnicos resolvidos da versão 10.2.3

- Foi resolvido um problema que fazia com que o banco de dados PostgreSQL não limpasse os dados corretamente durante os trabalhos padrão configurados de limpeza. Após a instalação, nos trabalhos de limpeza subsequentes, todos os trabalhos anteriores são conciliados. [DDPS-8397]
- Foi resolvido um problema com os dados exportados para um servidor Syslog ou SIEM por meio do Gerenciamento de Eventos do Management Console. [DDPS-8398]

Aconselhamentos técnicos da versão 10.2.3

- Em raras circunstâncias, o pré-compartilhamento de um documento protegido com um embargo definido pode não pré-compartilhar a chave em todos os casos. Para contornar esse problema, compartilhe a chave manualmente por meio do menu de clique com o botão direito de um usuário interno ou de um proprietário de arquivo interno. [DDPS-8567]

Novos recursos e funcionalidades da versão 10.2.2

- Não existem novos recursos nem funcionalidades.

Aconselhamentos técnicos resolvidos da versão 10.2.2

- Agora, o Security Management Server valida a versão 12.0.40660 do Microsoft Visual C++ 2013. Se essa versão não for encontrada, o instalador será encerrado. Confirme se essa versão está instalada antes de instalar o Security Management Server. [DDPS-8010, DDPSUS-2437]
- A consistência da tradução foi aprimorada. [DDPS-8064]
- Foi resolvido um problema que fazia com que os nomes das contas de serviço fossem rejeitados ao começar com um caractere de escape, como u e alguns caracteres especiais. [DDPS-8109]
- As instalações limpas do Security Management Server não resultam mais em mensagens de erro do serviço ACL. [DDPS-8149, DDPS-8270]
- A classificação por Caminho de Classificação, em Eventos de Auditoria, não resulta mais em um erro. [DDPS-8151]
- Foi resolvido um problema que resultava em erros internos ao fazer a transição entre telas do Management Console. [DDPS-8279]

Novos recursos e funcionalidades da versão 10.2.1

- Os dados de auditoria dos eventos bloqueados de captura de tela, dos eventos bloqueados de processos e dos eventos bloqueados de impressão agora são exibidos no Management Console.

Aconselhamentos técnicos resolvidos da versão 10.2.1

- A guia Eventos de Ameaças agora fica visível quando pelo menos uma licença do Threat Prevention ou do Advanced Threat Prevention é consumida. [DDPS-5728]
- A opção Gerenciar Relatórios funciona como esperado quando caracteres especiais são adicionados ao *Nome do Relatório*. [DDPS-6362]
- Agora, as exclusões de configurações padrão para codificações fracas são preservadas ao fazer upgrade da versão 9.10 para o Dell Security Management Server mais recente. [DDPS-7301]
- Os registros de data/hora usados para "Confirmar" as datas/horas são armazenados como UTC e serão convertidos no fuso horário atual com base na configuração de fuso horário do sistema que está visualizando a IU Web. [DDPS-7855]
- Foram resolvidas as informações díspares do *ID Exclusivo* dos endpoints nas páginas "Endpoint" e "Detalhes do Dispositivo". [DDPS-7928]
- Foi resolvido um problema de gerenciamento de dependências que resultava em falhas ao atualizar o Dell Security Management Server Virtual. [DDPS-7980]
- Foi resolvido um problema com mensagens de erro inofensivas do Dell Beacon Service, removendo dependências desnecessárias. [DDPS-7981]
- Foi resolvido um link simbólico incorreto que resultava em custos adicionais de armazenamento para registro em log. [DDPS-7991]
- Foi resolvido um problema em que o aplicativo Windows para Dell Security Management Server podia exceder o tempo de espera ou demorar muito tempo para fazer download dos dados principais. [DDPS-8121, DDPSUS-1796]

Novos recursos e funcionalidades da versão 10.1

- Uma página Downloads foi adicionada ao Management Console para fazer download do software de endpoint do Dell Data Security.
- Agora, há suporte à programação de e-mails de relatório. Um relatório deve ser criado em Geração de Relatórios > Gerenciar Relatórios no Management Console antes de a opção de programação estar disponível.
  - O campo *E-mail* é limitado a 1.024 caracteres.
  - O menu drop-down *Dia do Mês* oferece as opções 1 a 31 e Último para seleção.
  - *Hora* agendará o horário com base em sua localização atual.
  - A página Detalhes do Agendamento mostra a data de envio, o agendamento, o próximo envio etc.

Aconselhamentos técnicos resolvidos da versão 10.1

- O download de um pacote de chaves forenses usando o utilitário Administrative Download (CMGAd) é realizado com sucesso para endpoints com grandes conjuntos de chaves com base em um muitas ativações. [DDPS-6920, DDPSUS-2361]
- Foi resolvido um problema em que um cliente não conseguia executar relatórios do Advanced Threat Prevention ao usar o Compliance Reporter devido à pouca memória. [DDPS-7386, DDPSUS-2341]
- O Dell Enterprise Server 10.1 inclui uma atualização de segurança que aborda uma vulnerabilidade de desvio de segurança do Jetty (CVE-2017-7658). Os clientes e as equipes de campo devem aceitar a atualização 10.1 e todas as atualizações ou versões de manutenção do Dell Enterprise Server como uma prática recomendada. [DDPS-7387, DDPSUS-2344]
- Agora, as seleções feitas na página Eventos de Auditoria são salvas depois que um usuário sai da página. [DDPS-7445]
- Os servidores com muitos eventos do Advanced Threat Prevention podem apresentar alto uso de memória no Dell Security Management Server ou no Dell Security Management Server Virtual. Isso pode causar travamento de serviços no servidor. É possível aumentar o espaço máximo de heap e a memória física para contornar esse problema. [DDPS-7469]
- O Compliance Reporter fica oculto por padrão no Management Console. [DDPS-7717]

Aconselhamentos técnicos da versão 10.1

- Por padrão, os consoles do Dell Security Management Server e do Dell Security Center exportarão dados no formato UTF-8. Em alguns casos, esses dados não serão exibidos corretamente se o arquivo for aberto e exibido em Unicode, o que é feito por padrão para o Microsoft Excel. Para obter informações sobre como abrir arquivos com codificação UTF-8, consulte: https://support.office.com/en-us/article/choose-text-encoding-when-you-open-and-save-files-60d59c21-88b5-4006-831c-d536d42fd861?ocmsassetID=HA010121249&CorrelationId=050891fd-c54e-4e23-9e74-c8c75962d07f&ui=en-US&rs=en-US&ad=US. [DDPS-7613]
- Quando o Security Management Server é configurado em um ambiente IPv6 sem suporte a IPv4, o registro de notificações apresenta falha devido a um erro de comunicação. Para contornar esse problema, ative o suporte a IPv4 nesse ambiente. [DDPS-7655]

- Navegue até a guia *Enterprise* > *Eventos de Ameaças Avançadas*. Nela, selecionar o Nome do Host na lista resultará no direcionamento para Detalhes e Ações do Endpoint, e não à guia Eventos de Ameaças Avançadas. Para contornar esse problema, clique em **Eventos de Ameaças Avançadas** em *Detalhes e Ações*. [DDPS-7739]
- Quando um usuário recém-adicionado tenta fazer login na IU Web com um caractere especial "\" no nome de usuário, o log-in não é realizado com sucesso e resulta em uma mensagem de erro que exibe "O nome de usuário ou a senha usada é inválida". [DDPS-7768]

Novos recursos e funcionalidades da versão 10.0

- Agora, há suporte ao provisionamento do Advanced Threat Prevention em data centers geográficos do Government Cloud.
- Foram introduzidas tarefas adicionais de manutenção para reduzir o espaço em disco total utilizado.

Aconselhamentos técnicos resolvidos da versão 10.0

- As chaves de recuperação do BitLocker agora são classificadas por data. [DDPS-6496]
- Os Eventos de Ameaças Avançadas não são preenchidos corretamente no Dell Compliance Reporter. [DDPS-6695]
- A configuração de alertas por e-mail do Advanced Threat Prevention é mantida corretamente. [DDPS-6710]
- Foi resolvido um problema que resultava em uma mensagem de erro "Ocorreu um erro de acesso aos dados" ao acessar a guia Revogação de Chaves da página Gerenciamento de Usuários Externos com texto na caixa de pesquisa. [DDPS-6716]
- Agora, os e-mails são enviados corretamente no horário agendado no Dell Compliance Reporter. [DDPS-6770]
- A comunicação intermitente dos domínios não resulta mais na remoção de usuários do Dell Security Management Server. [DDPS-6914]
- Foi resolvido um problema em que as atualizações não retinham corretamente o nome de usuário para conexões aos dados de eventos de auditoria. [DDPS-7036]
- Agora, a autenticação básica funciona novamente no Dell Security Management Server Virtual. [DDPS-7244]

Aconselhamentos técnicos da versão 10.0

- Os Eventos de Auditoria com números de PINs por objeto próximos a 500 fazem com que o Management Console pare de responder por um tempo. Para contornar esse problema, modifique o escopo da pesquisa para reduzir o número para menos de 500 eventos consolidados. [DDPS-7430]

Novos recursos e funcionalidades da versão 9.11

- Abaixo, são apresentados os requisitos para as permissões do SQL. O usuário atual que executa a instalação e os serviços deve ter direitos de administrador local.

Digite	Ação	Cenário	Privilégio SQL necessário
Back-end	Upgrade	Por definição, upgrades já têm DB e login/usuário estabelecidos	db_owner
Back-end	Restaurar e instalar	A restauração envolve o DB e login existentes.	db_owner
Back-end	Nova instalação	Usar o DB existente	db_owner
Back-end	Nova instalação	Criar um novo DB	dbcreator, db_owner
Back-end	Nova instalação	Usar o login existente	db_owner
Back-end	Nova instalação	Criar novo login	securityadmin
Back-end	Desinstalar o	NA	NA
Proxy front-end	Qualquer	NA	NA

Aconselhamentos técnicos resolvidos da versão 9.11

- Adicionado em 08/2018 — agora, a notificação de ameaças imediatas do Painel de Indicadores mostra "Advanced Threat Prevention". [DDPS-4995]
- O Dell Security Management Server Virtual 9.11 foi projetado com compatibilidade de hardware com o Workstation 10.x. [DDPS-5085]
- Agora, o cliente pode fazer upgrade com uma senha JKS não padrão ao tentar fazer uma recuperação do servidor. [DDPS-5854]
- A adição de dispositivos a um grupo de endpoints existente não exige mais uma alteração de política para o grupo de endpoints de destino [DDPS-6002]
- Agora, a tela Endpoints exibe o número de série com base no valor WMI do número de série do BIOS. [DDPS-6161]
- Agora, o recurso ATP é exibido por padrão para os Administradores que fazem log-in na IU Web antes do provisionamento do ATP. [DDPS-6268]
- Foi resolvido um problema em que, quando um usuário recusava o End User License Agreement quando ele estava configurado em inglês, a tela de idioma não era exibida após uma reinicialização da máquina. [DDPS-6365]

Aconselhamentos técnicos da versão 9.11

- Adicionado em 11/2018 — ao fazer upgrade da versão 9.10 para o Dell Security Management Server mais recente, as exclusões padrão de configurações para codificações fracas são perdidas. Para desativar as codificações fracas, consultehttps://www.dell.com/support/article/us/en/19/sln301519/how-to-disable-weak-ciphers-in-dell-security-management-server-and-virtual-server-dell-data-protection-enterprise-edition-and-virtual-edition?lang=en. [DDPS-7301]

Novos recursos e funcionalidades da versão 9.10

- Foi adicionada a opção para remover varreduras de usuário do cálculo de status protegido do servidor.

  Para ativá-la, o administrador deve modificar o arquivo InventoryObjects.config localizado em < C: \Arquivos de Programas\Dell\Enterprise Edition\Core Server\> por padrão.

  A seção que deve ser alterada é:

  <object name="DeviceInventoryQueueProcessor" singleton="false" type="Credant.Inventory.Processor.DeviceInventoryQueueProcessor, Credant.Inventory.Processor" >

  <property name="EvaluateLastLoggedInUserForProtection" value="true"/>

  </object>

  Alterar o valor "true" para "false" (não diferencia maiúsculas de minúsculas) exigirá uma reinicialização do serviço Core Server. Depois que o serviço for reiniciado, os valores de varredura de usuário não serão calculados no status protegido do dispositivo.

Aconselhamentos técnicos resolvidos da versão 9.10

- A caixa "Ativar Verificação de Assinatura Digital" na IU Web agora impede que o usuário adicione qualquer texto. [DDPS-5857]
- Foi resolvido um problema que resultava em uma mensagem de erro durante a instalação do Security Management Server com o TLS 1.0 e o TLS 1.1 desativados no SQL de destino. [DDPS-5982]
- Adicionado em 7/2019 — o Java foi atualizado para resolver uma vulnerabilidade de Execução Remota de Código na serialização RMI (CWE-502). [DDPS-6200, DDPSUS-2084]

Problemas resolvidos dos clientes

- O console do banco de dados não aceita caracteres inválidos, como " ' " ou " / " etc.[DDPS-6102]

Aconselhamentos técnicos da versão 9.10

- O Security Management Server Virtual pode travar ao obter um alto volume de chaves em um curto período. [DDPS-6193]

Novos recursos e funcionalidades da versão 9.9

- Agora, as políticas não confirmadas são exibidas em um ícone de crachá na parte superior do Remote Management Console.
- Agora, os Recursos estão disponíveis no Dell Server. No canto superior direito do Painel de Indicadores, é possível adicionar ou remover as seguintes opções com o menu Recursos:
  - Notificações
  - Status Protegido
  - Ameaça
  - Histórico de proteção
  - Histórico de inventário
  - Estatísticas de resumo
- Agora, a tecnologia de criptografia em uso é exibida na guia Status da Proteção da página Detalhes e Ações do Endpoint.
- O Dell Server agora oferece suporte a IPV6.
- Uma coluna Política foi adicionada a **Gerenciar Relatórios > Log Analyzer**, que exibe as ações do administrador relacionadas à Política.
- Agora, o Gerenciamento de Licenças usa as seguintes definições para o uso de licenças:
  - **Excedente** — acima do número máximo de licenças. A ativação de novos endpoints apresentará falha. A reativação de clients apresentará falha. Os clients existentes funcionarão normalmente.
  - **Aviso** — o número de licenças se aproxima do limite. A ativação de novos endpoints continuará até 105% do máximo. Considere adquirir licenças adicionais.
  - **OK** — não é necessário realizar qualquer ação. A ativação de novos endpoints continuará até 105% do máximo. [DDPS-2115]
- Uma nova política permite que o Advanced Threat Prevention detecte e resolva payloads mal-intencionadas com as seguintes opções:
  - Ignorar - nenhuma ação é realizada contra as violações de memória identificadas.
  - Alerta - Registrar a violação e relatar o incidente para o Dell Server.
  - Bloquear - Bloquear a chamada de processo se um aplicativo tentar chamar um processo de violação de memória. O aplicativo que fez a chamada tem autorização para continuar a executar.
  - Encerrar - Bloquear a chamada de processo se um aplicativo tentar chamar um processo de violação de memória e encerrar o aplicativo que fez a chamada.
- Agora, o Dell Server oferece suporte ao TLS 1.2.

Aconselhamentos técnicos resolvidos da versão 9.9

- As Exclusões de IP do campo Proteção da Web do Remote Management Console agora aceitam apenas formatos válidos. [DDPS-2206]
- Se os cookies do navegador não estiverem ativados, a mensagem "Os cookies devem estar ativados em seu navegador para usar este aplicativo" será exibida ao fazer log-in no Remote Management Console. [DDPS-2661]
- Agora, será exibida uma notificação de obtenção de boletim com sucesso para a primeira obtenção de boletim realizada com sucesso após uma falha de obtenção de boletim. [DDPS-4811]
- Agora, as alterações de precedência para Grupos de Endpoints e Grupos de Usuários são exibidas no Log Analyzer. [DDPS-5024]
- O ID do Dispositivo na guia Eventos de Ameaças em Nível Empresarial agora tem um hiperlink para a página Detalhes do Endpoint do Remote Management Console. [DDPS-5571]
- Agora, os logs exibem o nome de um Grupo de Usuários Definido pelo Administrador removido no Log Analyzer do Remote Management Console. Os logs são gerados quando um Grupo de Endpoints Definido pelo Administrador é modificado. [DDPS-5564, DDPS-5565]
- Ao executar Detalhes do Log no Compliance Reporter, agora, os logs mostram os detalhes do Nome de usuário como esperado. [DDPS-5584]
- Agora, os logs são gerados como esperado quando é emitida uma solicitação para Aprovar ou Negar Acesso ao Arquivo. [DDPS-5589]
- A mensagem de erro exibida durante a instalação no Server 2016 quando o pré-requisito .Net 3.5 ainda não está instalado corretamente mostra "Server 2016". [DDPS-5591]
- É possível exportar os endpoints como esperado no formato Excel ou CSV. [DDPS-5825, DDPS-5826]

Problemas resolvidos dos clientes

- Foi resolvido um problema que resultava na falha de carregamento da guia Ameaças Avançadas. [DDPS-5025]
- Agora, o Compliance Reporter mostra o nome do host dos endpoints ativados com parâmetros Aceitar. [DDPS-5527]
- Os relatórios Mídia Externa do Encryption agora mostram as informações do usuário. [DDPS-5576]
- Agora, as chaves de recuperação são baixadas como esperado para um nome do host que contém Unicode. [DDPS-5614]

- O número adequado de licenças é consumido quando o Endpoint Security Suite Enterprise é instalado com os recursos Firewall do Client e Proteção da Web. [DDPS-5673]
- Os arquivos exportados como CSV da guia Eventos de Ameaças Avançadas agora exibem o registro correto de data e hora. [DDPS-5732]
- Ao usar uma conexão SMTP não autenticada, a Server Configuration Tool não requer mais um nome de usuário ou uma senha. [DDPS-5785]
- Foi resolvido um problema que resultava em um erro interno ao digitar caracteres acentuados no campo de confirmação. [DDPS-5805]

Aconselhamentos técnicos da versão 9.9

- Adicionado em 02/2018 — os upgrades para o Dell Security Management Server 9.9.2 agora estão bloqueados para as versões de servidor anteriores ao Dell Data Protection | Encryption Enterprise Server 9.2. [DDPS-6254]
- Durante a instalação ou o upgrade do Security Management Server, um script ativo é executado no diretório %TEMP%, que pode ser bloqueado por antivírus. Para contornar isso, a Dell recomenda desativar todas as soluções antivírus antes de instalar ou fazer upgrade do Security Management Server. [DDPS-5832]
- Ao definir uma Regra de Firewall e definir um executável nessa regra, o valor da soma de verificação MD5 não valida a sintaxe. Certifique-se de que a entrada MD5 esteja definida corretamente antes de finalizar a adição de um executável. [DDPS-5858]

Novos recursos e funcionalidades da versão 9.8

- Os endpoints do Advanced Threat Prevention agora mostram o status Protegido na página Endpoints quando seus agentes informam o status dos plug-ins como Funcional. O Status do Plug-in é exibido na guia Provedores da página Detalhes e Ações do Endpoint.
- Agora, é possível exportar os eventos de auditoria do Advanced Threat Prevention para um servidor SIEM/syslog e para um arquivo local a partir de **Gerenciamento** > **Gerenciamento de Serviços** no modo conectado e desconectado.
- Os e-mails de notificação de evento de ameaça avançada agora incluem hiperlinks para detalhes adicionais sobre cada categoria de evento (Crítico, Alto, Médio, Baixo e Total).
- Uma nova política Proteção da Web permite que os administradores bloqueiem mais de 100 categorias específicas de informações.
- Agora, os administradores podem carregar e importar em massa uma lista CSV de Usuários para adicionar aos Grupos de Usuários Definidos pelo Administrador. Agora, é possível modificar a prioridade do Grupo de Usuários usando a funcionalidade de arrastar e soltar.
- A página Gerenciamento de Licenças agora é exibida nas Licenças Padronizadas Coletadas, com as Etiquetas de Serviço relevantes.
- As políticas de Autenticação Pré-Inicialização agora são exibidas no Grupo de Tecnologia de Autenticação, na guia Políticas de Segurança. Uma nova política permite que o administrador ative ou desative a capacidade dos usuários de selecionar a opção **Lembrar de mim** na tela de log-in do PBA.
- A partir da versão 9.8, não é mais possível usar o thick client vSphere do ESXi para implementação.
- O Hardware Crypto Accelerator e o Mobile Edition não são mais compatíveis. As políticas deles se tornaram obsoletas.
- O Enterprise Server foi renomeado como Security Management Server.

Aconselhamentos técnicos resolvidos da versão 9.8

- Agora, um erro é exibido ao digitar um endereço inválido de domínio para bloqueio de DNS nas configurações do Firewall do Client do Threat Prevention. [DDPS-3201]
- Agora, os tipos de conexão são validados. A tabela de executáveis exibe o valor digitado para Assinatura e o nome correto da coluna de Impressão Digital. É necessário informar um nome de rede para especificar o protocolo de rede ao adicionar uma regra personalizada do Firewall do Client do Threat Prevention. EtherType e valores EtherType personalizados (para protocolo de rede não relacionado a IP) e os valores do protocolo de transporte são exibidos depois que uma regra de Firewall é salva. Agora, é necessário salvar as regras duplicadas com nomes de regra exclusivos. [DDPS-3429, DDPS-3678, DDPS-3679, DDPS-3725, DDPS-3726, DDPS-3727, DDPS-5196]
- Agora, o prompt de confirmação de alteração da função de administrador mostra o nome de usuário correto depois da modificação das funções administrativas de um usuário. Além disso, o prompt exibe as alterações feitas na guia Admin de Detalhes do Usuário. [DDPS-4097, DDPS-4099]
- O erro exibido quando um nome do host inválido ou em branco é digitado durante a instalação mostra o rótulo do campo no instalador. [DDPS-4466]
- A ferramenta de diagnóstico, chamada de Data Collection Utility, é incluída no menu Iniciar com outros componentes do servidor. [DDPS-4918]

- Agora, os logs do Log Analyzer são gerados quando os endereços de e-mail de notificação são adicionados ou editados no Gerenciamento de Notificações. [DDPS-5063]
- As exportações de eventos de auditoria para o servidor SIEM/syslog agora são reenviadas quando ocorre um erro de transmissão durante a tentativa inicial de exportação. [DDPS-5132]
- Agora, os requisitos de formatação para as seguintes políticas do Advanced Threat Prevention estão incluídos nas dicas do Dell Server e no AdminHelp: Ações da Memória — Excluir Arquivos Executáveis, Controle de Scripts — Aprovar Scripts de Pastas (e Subpastas) e Configurações de Proteção — Excluir Pastas Específicas (inclui subpastas). O AdminHelp indica corretamente que as funções de Suporte e Administrador de Segurança podem fazer download de pacotes de chaves de recuperação. [DDPS-5184, DDPS-5287]
- Os hiperlinks das notificações do Advanced Threat Prevention funcionam corretamente quando um ou mais endpoints são ativados em um Dell Server com a propriedade de host definida como o host do servidor de front-end. [DDPS-5188]
- Agora, todos os arquivos são instalados nas localizações esperadas depois do upgrade em um Dell Server em execução no Modo Desconectado, quando os arquivos instalados anteriormente eram armazenados em uma localização não padrão. [DDPS-5190]
- O tipo de "Certificado" é preenchido na coluna Tipo de Notificação do Relatório de Todas as Notificações do Compliance Reporter. [DDPS-5217]
- O upgrade não apresenta mais falha quando a opção Executar como Conta de Serviço é alterada durante o upgrade. [DDPS-5226]
- É possível exportar os eventos de auditoria para um servidor SIEM/syslog com TLS/SSL via TCP, com as seguintes alterações de configuração:

  Para usar o TLS/SSL, o servidor syslog deve estar configurado para monitorar mensagens do TLS/SSL. O certificado raiz utilizado para configurar o servidor syslog deve ser adicionado ao repositório de chaves de Java do Servidor da Dell.

  O exemplo a seguir mostra as configurações necessárias para um servidor Splunk com certificações padrão. As configurações são específicas para ambientes individuais. Os valores de propriedade variam quando as certificações não são padrão.

  1. Configure o servidor Splunk para usar o certificado do servidor Splunk e o certificado raiz para escutar as mensagens do TCP para TLS/SSL:

     $SPLUNK_HOME\etc\system\local\inputs.conf

     [tcp-ssl:<número da porta>]

     disabled = 0

     [SSL]

     serverCert = $SPLUNK_HOME\etc\auth\server.pem

     sslPassword = <senha>

     requireClientCert = false

     $SPLUNK_HOME\etc\system\local\server.conf

     [sslConfig]

     sslRootCAPath = $SPLUNK_HOME\etc\auth\cacert.pem

     sslPassword = <senha>

  2. Reinicie o servidor Splunk.

     Após o reinício, o **splunkd.log** terá entradas semelhantes às seguintes:

     07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig — a porta 5540 de IPv4 está reservada para entrada bruta (SSL)

     07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig — a porta 5540 de IPv4 negociará o novo protocolo de s2s

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig — a porta 5540 de IPv4 está reservada para entrada bruta (SSL)

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig — a porta 5540 de IPv4 negociará o novo protocolo de s2s

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig — a porta 9997 de IPv4 está reservada para splunk-to-splunk

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig — a porta 9997 de IPv4 negociará o novo protocolo de s2s

     07-10-2017 16:27:02.653 -0500 INFO TcpInputProc — criando aceitador bruto para a porta 5540 de IPv4 com SSL

     07-10-2017 16:27:02.653 -0500 INFO TcpInputProc — criando aceitador bruto para a porta 5541 de IPv4 com não SSL

     07-10-2017 16:27:02.654 -0500 INFO TcpInputProc — criando aceitador de dados de encaminhamento para a porta 9997 de IPv4 com não SSL

  3. Configure o Servidor da Dell para se comunicar com o servidor Splunk e exportar eventos de auditoria.

     Use o comando keytool para adicionar o certificado raiz do servidor Splunk (cacert.pem) ao repositório de chaves de Java do sistema operacional de servidor Dell. O certificado será adicionado ao repositório de chaves de Java do sistema operacional e não no repositório de chaves de Java do aplicativo do Servidor da Dell.

```
keytool -keystore <keystore_location> -alias <alias-name> -importcert -file
<certificate_file>
```

Para o Servidor de gerenciamento de segurança - adicione o certificado raiz do servidor Splunk (cacert.pem) ao repositório de chaves de Java, que no Windows geralmente está localizado neste caminho: `C:\Program Files\Dell\Java Runtime\jre1.8\lib\security\cacerts`

No Security Management Server Virtual — adicione o certificado raiz do servidor Splunk (cacert.pem) a `/etc/ssl/certs/java/cacerts` e reinicie o Dell Server.

4. Modifique o banco de dados do Dell Server para alterar o valor do SSL de **false** para **true**.

   No banco de dados, navegue até a tabela de informações, configuração de suporte específico do SIEM.

   Altere o valor "SSL":"false" para "SSL":"true"; por exemplo:

   ```
   {"eventsExport":{"exportToLocalFile":{"enabled":"false","fileLocation":"./logs/siem/audit-
   export.log"},"exportToSyslog":
   {"enabled":"true","protocol":"TCP","SSL":"true","host":"yourDellServer.yourdomain.com","por
   t":"5540"}}}
   ```

[DDPS-5234]

Problemas resolvidos dos clientes

- Foi resolvido um problema que resultava na falha de importação de uma licença com um erro no log do Security Server que informava que o sistema não consegue localizar a pasta `\AppData\Local\Temp\`. [DDPS-4240]
- Agora, a instalação prossegue como esperado quando a senha da Conta de Tempo de Execução do Serviço usada durante a instalação contém "**$_**" (cifrão seguido de sublinhado). [DDPS-4923]
- Foi resolvido um problema relacionado às alterações do perfil de validação da plataforma Microsoft que impediam o BitLocker Manager de começar a fazer a criptografia no Windows 10. [DDPS-5243]
- Agora, o Período de Locação do Dispositivo pode ser reduzido a um mínimo de 14 dias. [DDPS-5281]
- Foi resolvido um problema que resultava em um erro de violação de acesso no módulo "GKConsole.exe". [DDPS-5300]
- Agora, um seletor de páginas e uma lista drop-down permitem que o administrador navegue entre as páginas dos Grupos de Endpoints e selecione o número de grupos que serão exibidos por página. [DDPS-5349]
- Agora, os comentários de confirmação da política que começam com caracteres especiais são registrados no Histórico de Confirmação. [DDPS-5353]
- É possível importar com sucesso os certificados com senhas que incluem caracteres especiais. [DDPS-5396]
- Agora, o instalador aceita um ponto (".") no nome de usuário da conta de serviço SQL com o SQL Server 2008 R2 e o SQL Server 2016. [DDPS-5418]
- Não são mais exibidas entradas duplicadas no relatório de Detalhes do BitLocker Manager no Compliance Reporter depois do upgrade. [DDPS-5432]
- Foi resolvido um problema com as licenças do Threat Protection (TP) para Proteção da Web e Firewall e, agora, elas correspondem às licenças consumidas do Advanced Threat Prevention (ATP) com Proteção da Web e Firewall. [DDPS-5491]

Aconselhamentos técnicos da versão 9.8

- Adicionado em 01/2018 — os resultados do Eventos de Ameaças Avançadas são automaticamente limitados aos 10 mil primeiros resultados. Isso resolverá o problema em que os Eventos de Ameaças Avançadas não eram exibidos corretamente ao selecionar a guia no Dell Security Management Server
- Para bloquear todos os scripts do PowerShell com o Advanced Threat Prevention, as políticas PowerShell e Console do PowerShell devem ser definidas como **Bloquear**. Quando as duas políticas estiverem definidas como Bloquear, não será possível executar qualquer script, seja pelo console do PowerShell ou pelo console Cmd. As entradas de linha única do PowerShell são bloqueadas. Para permitir que os scripts aprovados sejam executados por meio do console Cmd, selecione a política Ativar Aprovação de Scripts das Pastas (e Subpastas) e adicione os scripts aprovados à política Aprovar Scripts das Pastas (e Subpastas). A política Console do PowerShell se aplica ao PowerShell 3 e versões posteriores. O Windows 7 inclui o PowerShell 2, por padrão. Para fazer upgrade para o PowerShell 3 no Windows 7, consulte www.microsoft.com/en-us/download/details.aspx?id=34595. [CYL-619]
- A partir da versão 9.8, não é mais possível usar o thick client vSphere do ESXi para implementação. Além disso, as instalações anteriores no ESXi 5.1 não foram impedidas, embora não sejam compatíveis. Agora, as instalações no ESXi 5.1 são impedidas. [DDPS-5086, DDPS-5269]
- Não é possível confirmar a política Logotipo Corporativo da Folha de Rosto dos Arquivos Protegidos do Office ao executar o Remote Management Console no Firefox. Para contornar esse problema, use o Internet Explorer ou o Google Chrome. [DDPS-5538]

- Adicionado em 08/2018 — o serviço Dell Policy Proxy pode enviar incorretamente duas solicitações ao servidor de back-end para solicitações SKID3. É possível ignorar esse comportamento com segurança. [DDPS-5585]

Novos recursos e funcionalidades da versão 9.7

- Agora, o Enterprise Server oferece suporte ao Advanced Threat Prevention com recursos opcionais de Firewall do Client e Proteção da Web. As políticas Firewall do Cliente e Proteção da Web foram reorganizadas para simplificar o gerenciamento desses recursos.
- Agora, o Enterprise Server oferece suporte ao Modo Desconectado, para ambientes fisicamente isolados.
- Adicionado em 7/2017 — agora, o Enterprise Server é compatível com o VMware ESXi 6.5.
- Agora, é possível especificar grupos e domínios do Active Directory ao adicionar ou modificar Grupos de Endpoints. O Enterprise Server coleta informações do Active Directory dos endpoints e disponibiliza esses dados para a especificação do Grupo de Endpoints.
- Agora, é possível modificar a Precedência do Grupo de Endpoints usando a funcionalidade de arrastar e soltar. Essa funcionalidade se aplica a Grupos de Endpoints do Active Directory, Definidos pelo Administrador e Definidos por Regras, mas não aos Definidos pelo Sistema. Esta é a precedência dos Grupos de Endpoints Definidos pelo Sistema para novas instalações e upgrades: a precedência mais alta é dada Grupo de Endpoints de VDI Não Persistente, seguido pelo de VDI Persistente. A precedência mais baixa é dada ao Grupo de Endpoints Padrão, seguido pelo de Aceitação.
- Adicionado em 7/2017 — agora, os administradores podem carregar e importar em massa uma lista CSV de Endpoints para adicionar aos Grupos de Endpoints Definidos pelo Administrador.
- Agora, é possível exportar os eventos do Advanced Threat Prevention a um servidor syslog ou a um arquivo local por meio de uma tela Gerenciamento de eventos simplificada.
- As novas políticas do Advanced Threat Prevention permitem exclusões de pastas do Controle de Aplicativos e a exclusão automática de arquivos em quarentena após um período configurável.
- Agora, é possível exportar os resultados do Log Analyzer para arquivos Excel ou CSV.

Aconselhamentos técnicos resolvidos da versão 9.7

- Na página Especificar Rede das Regras Personalizadas do Firewall do Client, no Remote Management Console, o campo Nome de Domínio Completo agora valida e rejeita formatos inválidos. Além disso, agora, o item **ICMP** da lista drop-down de Protocolo de Transporte e o tipo de Mensagem exibido são consistentes. [DDPS-2820, DDPS-2826, DDPS-2885]
- Os valores do Protocolo de Transporte são preenchidos na lista drop-down, nas Regras Personalizadas do Firewall do Client. [DDPS-3819].
- Agora, o AdminHelp pode ser movido para evitar obscurecer campos importantes do Remote Management Console. [DDPS-4258]
- Agora, as seguintes políticas de Controle de Portas Empresariais são exibidas com Classe: Armazenamento, a política principal: Armazenamento de Subclasse: Controle de Unidade Externa, Armazenamento de Subclasse: Controle de Unidade Óptica e Armazenamento de Subclasse: Controle de Unidade de Disquete. [DDPS-4682]
- Adicionado em 08/2018: os administradores podem fazer log-in nos endpoints com a política Autenticação de Acesso do Administrador definida como **Nenhum** e **Nenhum**. [DDPS-4739]
- A filtragem da guia Advanced Threat Protection do Remote Management Console está funcionando como esperado. [DDPS-4772]
- Agora, a caixa de diálogo Erro ao Validar Política que é exibida quando um valor atualizado de política falha na validação inclui o nome da política relacionada. [DDPS-4812]
- Agora, as Notificações do Painel de Indicadores de Eventos de Ameaças Avançadas são devidamente categorizadas por Tipo. [DDPS-4994]
- As localizações do Remote Management Console foram aprimoradas.

Problemas resolvidos dos clientes

- Agora, a recuperação de um dispositivo criptografado pelo EMS prossegue como esperado em um computador e um Dell Server diferentes do computador de criptografia original e do servidor que, originalmente, gerenciava a criptografia do dispositivo, quando os servidores pertencem à mesma federação. Para configurar a federação, siga estas etapas:

  1. Em um dos servidores que serão federados, edite `<installation folder>\Enterprise Edition\Security Server\conf\federatedservers.properties`:

     server.code — substitua "ENC(<código do servidor>)" por "CLR(<novo código; string que você selecionar>)". Esse será um código compartilhado entre os servidores federados.

     Server.uris — liste os servidores que serão federados, separados por vírgulas. Por exemplo: https://server1:8443,https://server2:8443

  2. Salve federatedservers.properties.
  3. Copie federatedservers.properties e salve-o fora do Security Server.

NOTA: O arquivo deve ser salvo fora do Security Server antes de reiniciar o servidor.

4. Reinicie o Security Server.

   Depois da reinicialização, "CLR(<novo código; string que você selecionar>)" é alterado para "ENC(<novo código compartilhado>)" e o novo código compartilhado do servidor é aplicado ao Security Server.

5. Copie o arquivo federatedservers.properties na pasta `\Security Server\conf` de cada servidor que será federado.

6. Reinicie cada Security Server depois de copiar o arquivo federatedservers.properties na pasta \conf.

[DDPS-2889]

- Foi resolvido um problema que causava um erro interno intermitente no Remote Management Console. [DDPS-4446]
- Agora, os protocolos SSL/TLS do Compliance Reporter podem ser configurados na propriedade eserver.ssl.protocols do arquivo `reporter/conf/eserver.properties` e são preservados durante as operações de backup/restauração. [DDPS-4547]
- Foi resolvido um problema no Remote Management Console em francês que causava um erro interno ao acessar o Painel de Indicadores. [DDPS-4675]
- Agora, é possível usar um só alias para mais de um domínio, permitindo a filtragem de usuários nos diferentes domínios. [DDPS-4683]
- A tradução em espanhol para a mensagem de sucesso da substituição de política foi corrigida. [DDPS-4718]
- Agora, a importação de um certificado durante a instalação prossegue como esperado quando há espaços no alias do certificado. [DDPS-4770]
- Foi aprimorado o manuseio de erros da Server Configuration Tool. [DDPS-4786]
- Agora, a importação do mesmo certificado do Server Encryption (SSOS) que é importado como o certificado SSL é bloqueada, com uma mensagem de erro que informa não ser possível importar o certificado duas vezes. [DDPS-4805]
- O campo Valor Pendente exibe o valor correto no relatório Detalhes de Políticas Pendentes do Compliance Reporter. [DDPS-4840]
- Agora, os registros de data e hora dos dados das SEDs são preservados quando os dados de recuperação são arquivados. [DDPS-4877]
- Uma consulta de Atualização do Perfil de Nuvem não resulta mais em políticas não confirmadas. [DDPS-4878]
- Foi resolvido um problema que causava um erro interno quando a opção **Geração de Relatórios** > **Eventos de Auditoria** era selecionada no Remote Management Console. [DDPS-4882]
- O valor do Intervalo de Consulta do Policy Proxy está correto no relatório Políticas Vigentes do Compliance Reporter. [DDPS-4927]
- Agora, a importação de um certificado válido com a Server Configuration Tool é realizada com sucesso depois de importar um certificado inválido. [DDPS-4928]

Aconselhamentos técnicos da versão 9.7

- Definir uma Ação de uma regra de Firewall do Client como Bloquear o Tráfego IPv4 impedirá a conectividade do client com o Dell Server. Não defina uma Ação dessa forma ao executar no Modo Conectado. [DDPC-5716]
- Os recursos Firewall do Client e Proteção da Web do Endpoint Security Suite Enterprise 1.4 exigem o Enterprise Server 9.7 ou versões posteriores. Antes de fazer upgrade dos clientes para usar esses recursos, o Enterprise Server 9.7 ou versões posteriores deve estar instalado, e a política Ação da Memória: Excluir Arquivos Executáveis deve ser ***aplicada*** nos clients anteriores à versão 1.4. Só inicie o upgrade do client quando a nova política estiver aplicada no client. [DDPS-5112]
- Alterado em 7/2017 — as configurações do SMTP não são retidas durante uma Instalação de Recuperação e devem ser reconfiguradas usando a Server Configuration Tool após a conclusão da recuperação. [DDPS-5239]
- Adicionado em 7/2017 — o Enterprise Server não oferece suporte aos domínios .local. [DDPS-5334]

Novos recursos e funcionalidades da versão 9.6

- Agora, o Dell Enterprise Server é compatível com os seguintes servidores:
  - Windows Server 2016
  - SQL Server 2016
- Agora, o Dell Enterprise Server oferece suporte ao Advanced Threat Prevention e ao Encryption em clients VMware e Citrix VDI persistentes e não persistentes.
- As novas políticas do Server Encryption permitem que o administrador configure o número máximo de tentativas e o intervalo de novas tentativas para a conexão com o Dell Server.
- Agora, está disponível o gerenciamento das contas de usuário locais pelo PBA remoto.
- As novas políticas e funcionalidades oferecem suporte à versão beta do Modo Desconectado.

Aconselhamentos técnicos resolvidos da versão 9.6

- Agora, a dica da política Armazenamento de Retenção de Clients do Controle de Auditoria indica que o armazenamento máximo é medido em megabytes. [DDPS-3682]
- Foi resolvido um problema que causava um erro ocasional de migração do banco de dados durante uma nova instalação. [DDPS-3792]
- Agora, a mensagem de erro do instalador que ocorre quando um nome do host inclui um sublinhado, que não é permitido, é mais específica. [DDPS-3902]
- Não ocorre mais um erro de acesso aos dados no Remote Management Console quando o idioma padrão de um perfil SQL não é inglês. [DDPS-4349]
- Um endpoint não relacionado ao domínio não será mais informado como desprotegido no Remote Management Console se o usuário tiver feito log-in mais recentemente que outros usuários em um endpoint e esse usuário tiver uma varredura de criptografia pendente ou incompleta. [DDPS-4470]
- A filtragem com o campo Removido do relatório Detalhes do BitLocker Manager - Reconhecimento de TMP do Compliance Reporter agora exibe resultados corretos. [DDPS-4608]
- A recuperação de chaves forenses agora prossegue como esperado quando uma ou mais instâncias key_id são inválidas. [DDPS-4689]

Problemas resolvidos dos clientes

- Agora, a habilitação de ativações não relacionadas ao domínio no arquivo server_config.xml é realizada com sucesso, como esperado, sem considerações à diferenciação de letras maiúsculas e minúsculas do valor digitado para a propriedade, accountType.nonActiveDirectory.enabled. Além disso, os logs do Compatibility Server indicam quando a habilitação da ativação não relacionada ao domínio apresenta falha devido a problemas de diferenciação entre maiúsculas e minúsculas no nome da propriedade em si. [DDPS-4068]
- Foi resolvido um problema que causava a falha da instância Java do Security Server com a seguinte mensagem de erro: EXCEPTION_ACCESS_VIOLATION. [DDPS-4245]
- Foi resolvido um problema que resultava em políticas não confirmadas que não foram iniciadas pelo administrador. [DDPS-4761]
- Adicionado em 05/2018 — o Dell Security Management Server seleciona políticas com base no grupo em que os endpoints não estão mais localizados, e não em políticas arbitradas. O grupo com o valor de precedência mais alto tem sucesso, e nenhum outro grupo é considerado. [DDPS-5377]

Aconselhamentos técnicos da versão 9.6

- Se a pasta ProgramData estiver aberta durante um upgrade, um erro será exibido: "C:/ProgramData/Del/Gatekeeper não está disponível..." Para contornar esse problema, feche a pasta ProgramData e clique em **OK** na caixa de diálogo de erro. [DDPS-4573]
- Ao executar o Compliance Reporter com o Google Chrome, o calendário de seleção de datas não será exibido na coluna Valor quando o campo **Criado** * for selecionado na área Filtrar Campos do Layout do Relatório. [DDPS-4691]
- Adicionado em 4/2017 — as categorias de Status do Threat Protection são diferentes entre as Notificações do Painel de Indicadores e os Resumos de Notificações por E-mail do Remote Management Console. As categorias de Notificações do Painel de Indicadores são Crítica, Importante, Secundária e Aviso. As categorias correspondentes das notificações por e-mail são Crítica, Alta, Média e Baixa. [DDPS-4802]

Novos recursos e funcionalidades da versão 9.5

- Adicionado em 8/28 — foi adicionada uma nova política que permite que os administradores forcem a Criptografia Baseada em Políticas quando uma SED é detectada.
- A partir da versão 9.4.1.6, o Dell Enterprise Server oferece suporte ao Advanced Threat Prevention em computadores Mac. O Advanced Threat Prevention oferece detecção de ameaças em tempo real, analisando possíveis execuções de arquivos para malware no sistema operacional e nas camadas de memória para impedir a entrega de payloads mal-intencionadas. O controle da execução no endpoint permite a detecção precisa e eficaz de ameaças mal-intencionadas, mesmo as que nunca foram vistas antes. O Advanced Threat Prevention usa técnicas de aprendizado de máquina que permitem a detecção de novos programas de malware, vírus, bots e variantes futuras desconhecidas, nos quais as assinaturas e as áreas de simulação apresentam falha. A proteção da memória fortalece os recursos básicos de proteção do sistema operacional, oferecendo uma camada adicional para detectar e negar determinados comportamentos geralmente usados por exploits.

Aconselhamentos técnicos resolvidos da versão 9.5

- Ao importar um certificado existente durante o upgrade, o instalador não exibirá mais um erro se a senha padrão do certificado tiver sido alterada. [DDPS-2644]
- Pesquisar endpoints no Remote Management Console usando o ID de Recuperação do Shield agora exibe os resultados esperados. [DDPS-4017]
- Foi resolvido um problema que fazia com que as Estatísticas Resumidas no Painel de Indicadores do Remote Management Console não fossem atualizadas como esperado. [DDPS-4082]
- Uma segunda notificação ou notificação subsequente adicionada ao Gerenciamento de Notificações do Remote Management Console não retém mais os valores de Tipo e Prioridade da notificação adicionada anteriormente. [DDPS-4178]
- Após o upgrade, os relatórios Detalhes da Política de Método de Autenticação SED e Status das Varreduras e Falhas de Criptografia do Windows do Compliance Reporter estão disponíveis, como esperado. [DDPS-4183]
- Depois que o usuário pesquisa pelo nome de usuário da opção Executar como Conta de Serviço, as credenciais agora são preenchidas na caixa de diálogo Informações da Conta de Tempo de Execução do Serviço no instalador. [DDPS-4234]
- A categoria Advanced Threat Prevention agora é preenchida no Log Analyzer, no Remote Management Console. [DDPS-4241]
- Foi resolvido um problema que resultava em falha na inscrição da Atualização Automática do Agente do Advanced Threat Prevention. [DDPS-4244]
- As opções Adicionar Usuário e Adicionar Grupo foram removidas de Detalhes do Domínio dos Membros de Usuários Não Relacionados ao Domínio, no Remote Management Console. Essas opções não são aplicáveis aos usuários que não são relacionados ao domínio. [DDPS-4255]

Problemas resolvidos dos clientes

- O campo Especificação da página Adicionar Grupo de Endpoints do Remote Management Console agora tem o comprimento validado e exibirá um erro se mais de 4 mil caracteres forem digitados. [DDPS-2953, DDPS-4260]
- O campo TPM Ativado do relatório Detalhes do BitLocker Manager do Compliance Reporter agora está preciso. [DDPS-3394]
- Durante a instalação do novo banco de dados, o instalador agora cria o banco de dados na pasta definida em Configurações do Banco de Dados de Propriedades do Servidor, e não na pasta do banco de dados principal especificada em Arquivos de Propriedades do Banco de Dados. [DDPS-4221]

Aconselhamentos técnicos da versão 9.5

- Alterado em 7/2017 — o botão **Log-in** do Remote Management Console pode ser desativado no Google Chrome ou no Internet Explorer do Server 2012. Para contornar esse problema, limpe o cache do navegador e tente fazer log-in ou use o Mozilla Firefox 41.x ou versões posteriores. [DDPS-4558]
- As políticas do Advanced Threat Prevention não serão validadas corretamente se seus valores não estiverem entre aspas duplas (") e contiverem caracteres curingas ou especiais, como vírgulas (,), colchetes ([ ]) e til (~). Para forçar a validação, coloque as strings entre aspas duplas ("). Não use caracteres curinga e especiais, que não são permitidos. [DDPS-4589]
- Adicionado em 2/2017 — a validação de políticas iniciada na versão 9.5 poderá resultar em uma mensagem "Erro ao validar a política" no Remote Management Console ao tentar visualizar a política quando o valor dela estiver formatado incorretamente. Para contornar esse problema, corrija a formatação dos valores das políticas afetadas. Para identificar as políticas afetadas, siga estas etapas:

  1. Abra o <diretório de instalação do Core Server> **PolicyService.config**.

     Enterprise Server — Arquivos de Programas\Dell\Enterprise Edition\Core Server

     VE — /opt/dell/server/core-server

  2. Altere o valor da propriedade StrictValidation de **true** para **false**: `<property name="StrictValidation" value="false"/>`
  3. Reinicie os serviços.
  4. No Remote Management Console, navegue para visualizar a política no nível em que ocorreu o "Erro ao validar a política" e anote o nome da política identificado no erro.
  5. Corrija a formatação do valor da política e clique em **Salvar**.
  6. No painel esquerdo, clique em **Gerenciamento** > **Confirmar**, digite a descrição da alteração da política e clique em **Confirmar Políticas**.
  7. Se quiser, altere o valor da propriedade StrictValidation de **false** para **true** para reativar a validação de políticas.

  [DDPS-4779]

Novos recursos e funcionalidades da versão 9.4.1.6

- Agora, o Dell Enterprise Server oferece suporte ao Advanced Threat Prevention em computadores Mac. O Advanced Threat Prevention oferece detecção de ameaças em tempo real, analisando possíveis execuções de arquivos para malware no sistema operacional e nas camadas de memória para impedir a entrega de payloads mal-intencionadas. O controle da execução no endpoint permite a detecção precisa e eficaz de ameaças mal-intencionadas, mesmo as que nunca foram vistas antes. O Advanced Threat Prevention usa técnicas de aprendizado de máquina que permitem a detecção de novos programas de malware, vírus, bots e variantes futuras desconhecidas, nos quais as assinaturas e as áreas de simulação apresentam falha. A proteção da memória fortalece os recursos básicos de proteção do sistema operacional, oferecendo uma camada adicional para detectar e negar determinados comportamentos geralmente usados por exploits.

Novos recursos e funcionalidades da versão 9.4.1

- Um novo recurso de Atualização Automática de Agentes do Advanced Threat Prevention está disponível e pode ser ativado a partir do Gerenciamento de Serviços, no painel esquerdo do Remote Management Console. Ativar a Atualização Automática de Agentes permite que os clientes façam download e apliquem atualizações automaticamente a partir do servidor do Advanced Threat Prevention. As atualizações são liberadas mensalmente.
- As novas políticas do Advanced Threat Prevention permitem que o administrador configure o manuseio automático após a detecção de uma payload mal-intencionada e defina configurações estendidas do Controle de Scripts para Scripts Ativos, PowerShell e macros do Office.
- O Relatório de Eventos de Ameaças Avançadas agora pode ser exportado como um arquivo Excel ou .csv a partir da guia Eventos de Ameaças Avançadas do Remote Management Console.
- Uma nova política permite que o administrador oculte os ícones de criptografia do Explorador de Arquivos para usuários gerenciados.

Aconselhamentos técnicos resolvidos da versão 9.4.1

- A Dell continuará oferecendo suporte às versões atuais do Dell Enterprise Server em plataformas de software de terceiro, desde que isso seja tecnicamente e comercialmente razoável para a Dell, quando não houver dependência externa. Devido à dependência externa, o VMware ESXi 5.1 não é mais compatíveis a partir da versão 9.4.1. Para obter mais informações, consulte http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf.
- Não ocorre mais um erro durante o download do pacote de chaves forenses do Dell Enterprise Server. [DDPS-3244]
- O campo Inventário Recebido na página Detalhes do Endpoint do Remote Management Console agora é preenchido após a ativação de um endpoint. [DDPS-3982]
- Agora, os e-mails de notificação são enviados como esperado quando a opção Todos os Tipos de Notificação é selecionada ao configurar Gerenciamento de Notificações no Remote Management Console. [DDPS-4003, DDPS-4038]
- Foi resolvido um problema que resultava em um erro interno ao clicar em Chaves de Recuperação do Dispositivo na página Detalhes do Endpoint do Remote Management Console. [DDPS-4222]

Novos recursos e funcionalidades da versão 9.4

- Agora, o Remote Management Console apresenta opções aprimoradas e configuráveis de Painel de Indicadores e Notificações por E-mail para atualizar os administradores sobre eventos de ameaças, expirações de certificados, disponibilidade de licenças, alterações de configurações, atualizações de produtos e artigos da base de conhecimento.
- Os clientes do Advanced Threat Prevention agora podem aproveitar estes recursos, disponíveis no Remote Management Console:
- Agora, é possível importar e adicionar certificados à Lista Segura.
- É possível integrar o software de Gerenciamento e Correlação de Eventos de Segurança (SIEM) para capturar eventos de Ameaças Avançadas.
- Agora, estão disponíveis dados aprimorados sobre ameaças e os dispositivos nos quais elas são identificadas.
- A categoria da política Criptografia de Pastas de Arquivos do Remote Management Console foi renomeada como Criptografia Baseada em Política.
- O item de menu Gerenciamento de Alertas do Remote Management Console foi renomeado como Gerenciamento de Notificações.
- As instalações do Dell Enterprise Server não são mais compatíveis com os sistemas operacionais de 32 bits.

Aconselhamentos técnicos resolvidos da versão 9.4

- O instalador não aceita mais sublinhados nos nomes de host. Um caractere de sublinhado ("_") no nome do host do Compatibility Server ou do Security Server causa a falha da conexão com esse servidor. Um nome do host não pode conter um caractere de sublinhado ("_") devido a um problema da plataforma Java, JDK-6587184. Para obter mais informações, consulte http://bugs.java.com/view_bug.do?bug_id=6587184. [DDPMTR-1345, DDPS-3570]
- Os valores de política do relatório Política do BitLocker Manager agora são preenchidos corretamente, e os dispositivos gerenciados não são mais exibidos em linhas duplicadas. [DDPS-2810, DDPS-3427]
- O Dell Enterprise Server agora oferece suporte a vários direitos associados a uma só etiqueta de serviço. [DDPS-2949]
- Adicionado em 7/2017 — o tópico Funções do Administrador no AdminHelp não indica mais que o administrador do sistema pode confirmar políticas, recuperar dados e recuperar endpoints e que o administrador de segurança pode delegar direitos de administrador, embora esses administradores não tenham essas permissões. Agora, o tópico indica corretamente que os administradores de contas podem delegar direitos de administrador. [DDPS-3004, DDPS-3005, DDPS-3006]
- Agora, o formato válido de chave é baixado do Enterprise Server nos arquivos de recuperação do Enterprise Edition for Mac, e foi resolvido um problema que fazia com que o servidor entregasse chaves de recuperação em branco do FileVault. [DDPS-3139, DDPS-3873]
- Os domínios com nomes que incluem espaços ou caracteres especiais agora podem ser adicionados ao Remote Management Console. [DDPS-3329]
- Agora, os Nomes de Alias de Domínio são resolvidos como esperado no Remote Management Console, e o log-in com um Alias de Domínio inválido não é mais realizado com sucesso. [DDPS-3330, DDPSUS-767]
- O relatório Eventos do Advanced Threat Prevention do Compliance Reporter agora inclui o campo Tipo, que exibe o tipo de ameaça. [DDPS-3331]
- Agora, os administradores poderão atualizar as Configurações de Domínio do Remote Management Console depois que suas credenciais do usuário forem alteradas no Active Directory e quando o servidor ou serviço Active Directory estiver indisponível. A mensagem "Falha ao recuperar domínio" ou "'código:10180" não é mais exibida. [DDPS-3336, DDPS-3337, DDPS-3338]
- Agora, digitar qualquer combinação de caracteres maiúsculos e minúsculos nas configurações do Compliance Reporter exibe os resultados esperados. [DDPS-3369]
- Foi resolvido um problema que causava tempos de espera excedidos do Remote Management Console ao pesquisar por endpoints. [DDPS-3400]
- Foi resolvido um problema que causava um erro durante a instalação em servidores com processadores sobrecarregados. [DDPS-3444]
- Agora, os administradores com UPNs com mais de 32 caracteres podem enviar comandos SED com eficiência para os dispositivos. [DDPS-3432]
- Foi resolvido um problema que causava um erro interno no Remote Management Console. [DDPS-3454]
- O provisionamento do serviço Advanced Threat Prevention prossegue como esperado quando usado com um servidor proxy. [DDPS-3475]
- Agora, a pasta de backup é preservada após uma reversão de instalação durante o upgrade. [DDPS-3527]
- As configurações de modelo de políticas que incluem o valor Rijndael agora migram corretamente durante o upgrade. [DDPS-3531]
- Foram aprimorados os logs para o erro que ocorre quando um usuário com UPNs duplicados no banco de dados do Dell Data Protection tenta fazer log-in no Remote Management Console. [DDPS-3578]
- Foram aprimorados os logs para o erro que ocorre ao pesquisar por um usuário cujo nome de grupo inclui um caractere especial. [DDPS-3587]
- Agora, a política Pastas Criptografadas Comuns é aplicada corretamente a %ENV:USERPROFILE%\Downloads. [DDPS-3752]
- Agora, os endpoints que foram removidos anteriormente podem ser adicionados de volta ao inventário de forma consistente e receber novas políticas, como esperado. [DDPS-3772]
- A página Detalhes e Ações do Domínio do Remote Management Console não ficará mais ilegível se a conta do serviço de domínio usada para adicionar o domínio incluir aspas (") na senha. [DDPS-3813]
- A opção Salvar estará disponível quando a senha de Autenticação SQL for atualizada na Server Configuration Tool. [DDPS-3817]
- Foi resolvido um problema que causava a alta carga da CPU do Compatibility Server na reinicialização quando a perícia forense era ativada no Security Server. [DDPS-3833]
- Foi resolvido um erro que causava travamentos ocasionais do serviço Core Server quando vários inventários eram executados. [DDPS-3877]
- Um erro interno não é mais exibido na página Políticas Vigentes de um Endpoint ou Usuário após o upgrade de um Enterprise Server anterior à versão 9.2. [DDPS-4000]

Aconselhamentos técnicos da versão 9.4

- Após a instalação do Dell Enterprise Server e do DDP Enterprise Server - Virtual Edition, o Remote Management Console exibe "Uma substituição não confirmada", indicando uma confirmação de política pendente. A política representa uma configuração interna. Para contornar esse problema, confirme as políticas após a instalação. No painel esquerdo, clique em **Gerenciamento** > **Confirmar**, digite a descrição, "Confirmação inicial" e clique em **Confirmar Políticas**. [DDPS-3163]
- Se o banco de dados ou a instância SQL estiverem configurados com um agrupamento que seja diferente do padrão, a instalação apresentará falha. Um agrupamento diferente do padrão não deve diferenciar entre letras maiúsculas e minúsculas. Para obter uma lista de agrupamentos e diferenciação de maiúsculas e minúsculas, consulte https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx. [DDPS-3355]
- Para que os clients Dell Data Protection SED e HCA 8.5.1 e os clients anteriores se comuniquem com o Dell Enterprise Server e o Virtual Edition 9.4, as seguintes configurações devem ser definidas no servidor:

1. No Security Server, acesse <pasta de instalação>\Enterprise Edition\Security Server\conf\spring-jetty.xml e transforme a propriedade excludeProtocols em comentário:

   <!--

   <property name="excludeProtocols" value="SSL,SSLv2,SSLv3" />

   -->

2. No arquivo ..\Dell\Java Runtime\jre1.8\lib\security\java.security, remova "SSLv3" da seguinte linha:

   jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768

   [DDPS-3371]

- Os grupos de segurança universais não são compatíveis devido à forma como são criados no Active Directory. [DDPS-3765]

Novos recursos e funcionalidades da versão 9.2

- Agora, o Dell Enterprise Server oferece suporte ao Advanced Threat Prevention. O Advanced Threat Prevention oferece detecção de ameaças em tempo real, analisando possíveis execuções de arquivos para malware no sistema operacional e nas camadas de memória para impedir a entrega de payloads mal-intencionadas. O controle da execução no endpoint permite a detecção precisa e eficaz de ameaças mal-intencionadas, mesmo as que nunca foram vistas antes. O Advanced Threat Prevention usa técnicas de aprendizado de máquina que permitem a detecção de novos programas de malware, vírus, bots e variantes futuras desconhecidas, nos quais as assinaturas e as áreas de simulação apresentam falha. A proteção da memória fortalece os recursos básicos de proteção do sistema operacional, oferecendo uma camada adicional para detectar e negar determinados comportamentos geralmente usados por exploits.
- O Remote Management Console tem uma nova aparência, com um design HTML 5 responsivo que pode ser visualizado em praticamente qualquer tamanho de tela. Ele não requer mais instalação e, agora, é acessado neste URL:

  https://server.domain.com:8443/webui/

- Agora, o Remote Management Console oferece os seguintes novos recursos e funções:
  - É possível definir notificações de alerta por e-mail para eventos do Threat Protection e do Advanced Threat Prevention.
  - Quando os dados são recuperados em um computador com mais de uma unidade com criptografia automática, é possível selecionar cada unidade individualmente para recuperação.

Aconselhamentos técnicos resolvidos da versão 9.2

- Pesquisas adicionais sobre problemas de direitos geraram melhorias nos testes, resultando na resolução de alguns problemas abertos e não resolvidos. [DDPMTR-1768, DDPS-1571, DDPS-1716/DDPSUS-235]
- Foram traduzidos alguns itens das telas do Remote Management Console que, antes, não eram traduzidos. [DDPS-846, DDPS-1519, DDPS-1525, DDPS-1722, DDPS-1928]
- O relatório Políticas Vigentes do Compliance Reporter agora exibe as conexões ao Gatekeeper e o tipo correto de valor para a política Intervalo de Consulta do Policy Proxy. [DDPS-1233]
- Quando um computador não integrante do domínio ingressa no domínio, não são mais exibidas entradas duplicadas de endpoint no Remote Management Console e o endpoint recebe políticas corretamente. [DDPS-1304]
- O relatório Lista de Administradores do Compliance Reporter agora inclui o campo Nome do Grupo. [DDPS-1720]
- No Remote Management Console, ao adicionar ou editar as regras de Firewall do Client, o campo executável Assinado Por é validado. [DDPS-1794/DDPSTE-445]

- Ao resgatar a senha de recuperação do BitLocker Manager no Remote Management Console para mais de um volume, agora, a primeira senha de recuperação é excluída antes de selecionar o segundo volume e os volumes subsequentes do BitLocker. [DDPS-1808]
- A desinstalação com o setup.exe não requer mais reinicialização. [DDPS-1839]
- Ao final da instalação do servidor, agora, a caixa de seleção ao lado de Mostrar Log do Instalador do Windows fica visível. [DDPS-1840]
- Agora, as permissões herdadas de um grupo são removidas dos administradores do Remote Management Console quando o grupo é removido. [DDPS-1853]
- O relatório Políticas Locais do Compliance Reporter agora inclui as alterações de políticas baseadas em dispositivos feitas nos níveis de Endpoint e Grupo de Endpoints. [DDPS-1859]
- A mensagem de erro exibida quando o Core Server está em execução durante a inicialização da Server Configuration Tool não indica mais que é necessário interromper o Compatibility Server. A Server Configuration Tool funciona corretamente quando o Compatibility Server está em execução. [DDPS-1863]
- Agora, o novo nome de um computador renomeado substitui o nome anterior, em vez de ser exibido como um segundo endpoint no Remote Management Console quando as chaves são depositadas antes de o novo nome do computador ser processado no inventário. [DDPS-1895]
- A política Mensagem do OneDrive do Cloud Storage não se aplica mais e foi removida do Remote Management Console. [DDPS-1917]
- Agora, um upgrade é realizado como esperado após o cancelamento de um upgrade anterior. [DDPS-2065]
- O arquivo de Ajuda padrão do Cloud Encryption entregue aos endpoints por meio da política Conteúdo do Arquivo de Ajuda agora é renderizado corretamente nos endpoints. [DDPS-2071]
- O pacote de recuperação Mac agora inclui o nome do host e a extensão na caixa de diálogo Salvar exibida no endpoint. [DDPS-2090]
- Uma Exceção Desconhecida não ocorre mais durante o upgrade depois que os usuários são removidos manualmente do Active Directory. [DDPS-2330]
- As consultas de inventário dos clients gerenciados foram reduzidas de doze para duas horas para refletir com mais precisão as alterações de status. [DDPS-2371]
- Foi resolvido um problema que causava algumas falhas de inicialização de serviços, recuperação de direitos padronizados e inicialização do Compliance Reporter após a instalação ou o upgrade, quando eram feitas alterações de configuração por meio da Server Configuration Tool. [DDPS-2755]
- Quando um endpoint é movido de um Grupo de Endpoints para outro Grupo de Endpoints não padrão, agora, as políticas do Grupo de Endpoints são aplicadas de forma consistente com base nas configurações de Precedência. [DDPS-2881]
- Foi resolvida uma política padrão de Regras de Criptografia SDE que causava problemas com as atualizações do Windows. O problema resultava da criptografia dos arquivos executáveis \System32. A política padrão foi alterada para os EE e VE Servers 9.2 e versões posteriores. [DDPS-2952, DDPC-1207]

Aconselhamentos técnicos da versão 9.2

- É possível excluir um layout de relatório do Compliance Reporter sem uma mensagem de erro, embora haja relatórios subordinados anexados a ele. [DDPS-1094]
- O campo Exclusões de IP para Proteção da Web do Remote Management Console aceita formatos inválidos. [DDPS-2206]
- A descrição de uma regra personalizada do Firewall do Client no Remote Management Console não inclui o tipo de rede local ou remota. [DDPS-2278]
- Se os cookies do navegador não estiverem ativados, a mensagem "Ocorreu um erro interno" será exibida ao fazer log-in no Remote Management Console, em vez de uma mensagem que solicita que o usuário ative os cookies. [DDPS-2661]
- O relatório Política de Dispositivos Móveis do Compliance Reporter não é preenchido. [DDPS-2675]
- Na Programação de Exibição de Relatórios do Compliance Reporter, a dica do campo Destinatários do E-mail informa que é possível separar os endereços de e-mail por vírgulas ou colocá-los em linhas separadas. Os endereços de e-mail não podem ser colocados em linhas separadas, mas devem ser separados por vírgulas. [DDPS-2678]
- Durante a reinicialização dos serviços, navegar para as páginas de População Empresarial do Remote Management Console resultará em uma mensagem Acesso Negado, em vez de retornar à página de log-in. [DDPS-2815]
- Depois que o serviço Advanced Threat Prevention for provisionado, os Eventos de Ameaça Avançada só começarão a ser exibidos quando o administrador se desconectar e, depois, fizer log-in novamente no Remote Management Console. [DDPS-2816]
- A guia Políticas de Segurança de Endpoints do Remote Management Console mostra os valores da política Informações de Recuperação do BitLocker a Serem Armazenadas no AD DS como *Senhas de Recuperação e Pacotes de Chaves* e *Somente Senhas de Recuperação*. Em Políticas Vigentes de Endpoint, os valores da mesma política são *Senhas e Chaves* e *Somente Senhas*. [DDPS-2821]
- A regra personalizada de Firewall do Client permite que o administrador digite endereços de sub-rede, embora não seja possível criar sub-redes para redes locais ou remotas. [DDPS-2838]
- Algumas dicas e áreas de algumas páginas não são localizadas no Remote Management Console. [DDPS-2842, DDPS-2844, DDPS-2989, DDPS-2994, DDPS-2996, DDPS-2997, DDPS-2999]

- A opção "Substituir Número" está truncada na guia Políticas de Segurança de Endpoints no Remote Management Console em espanhol, italiano, francês, português e português brasileiro. [DDPS-2843]
- O ícone AdminHelp não está disponível na tela de log-in do Remote Management Console. [DDPS-2858]
- A guia Detalhes do Usuário do Remote Management Console exibe o ícone Políticas Vigentes para dispositivos móveis, embora as políticas vigentes não se apliquem aos dispositivos móveis. [DDPS-2880]
- Há um atraso entre a conclusão da consulta do servidor com base no Intervalo de Consulta do Servidor configurado e a exibição de eventos do Threat Protection no Remote Management Console. [DDPS-2896]
- O botão de atualização não funciona na página Gerenciamento de Alertas do Remote Management Console. [DDPS-2923]
- A página Adicionar Domínio do Remote Management Console não tem barra de rolagem vertical; portanto, em telas pequenas ou com baixa resolução, o botão Adicionar Domínio não é visível. [DDPS-2945]
- Digitar uma senha inválida do LDAP ao adicionar um domínio no Remote Management Console resulta em um prompt para verificar os logs, em vez de uma mensagem que informa que a senha é inválida. [DDPS-2954]
- O Remote Management Console não funcionará se o TLS 1.0 estiver desativado. [DDPS-2955]
- Ao adicionar um usuário no Remote Management Console, as pesquisas por usuários que pertencem a muitos grupos do Active Directory podem demorar mais que o esperado. Se isso ocorrer, clicar no botão Pesquisar mais de uma vez na caixa de diálogo Adicionar Usuários por Domínio pode causar travamento do Security Server. Não clique no botão Pesquisar mais de uma vez na caixa de diálogo Adicionar Usuários por Domínio. [DDPS-3010]
- Ao digitar um nome do host inválido durante a instalação do serviço Advanced Threat Prevention, ocorrerá um tempo de espera excedido. Para contornar esse problema, clique em OK na caixa de diálogo Tempo de Espera Excedido para retornar à página Gerenciamento de Serviços. Verifique o nome do host e reinicie a instalação do serviço Advanced Threat Prevention. [DDPS-3019]
- Os alertas por e-mail dos eventos do Advanced Threat Prevention não estão sendo enviados. [DDPS-3031]

Aconselhamentos técnicos resolvidos da versão 9.1.5

- No Compliance Reporter, agora, o relatório Políticas Móveis inclui resultados de todos os dispositivos móveis ativados. [DDPMTR-838]
- Agora, durante um upgrade feito enquanto o banco de dados SQL está indisponível, o upgrade continua sem atraso. A Server Configuration Tool poderá ser usada para migrar o banco de dados quando ele estiver disponível. [DDPMTR-1226]
- Quando a opção Reutilizar Certificado SSL para SSOS for selecionada durante uma nova instalação, o certificado SSL será reutilizado como esperado. [DDPMTR-1243]
- Agora, o campo Destinatários de E-mail do Compliance Reporter aceita apenas uma vírgula (",") como separador, em vez de aceitar caracteres especiais. [DDPMTR-1257]
- O campo de configuração Excluir Processos da política do Threat Protection não aceita mais valores inválidos no Remote Management Console. [DDPMTR-1346]
- O Dell Enterprise Server 9.1.5 inclui uma atualização de segurança que aborda uma vulnerabilidade do OpenSSL (CVE-2015-4000 do OpenSSL). Os clientes e as equipes de campo devem aceitar a atualização 9.1.5 e todas as atualizações ou versões de manutenção do Dell Enterprise Server como uma prática recomendada. [DDPMTR-1507]
- Foi aprimorado o desempenho para ativações de client com base no acesso simplificado do Active Directory. [DDPMTR-1538]
- A importação de certificados com espaços nos nomes dos alias foi aprimorada. [DDPMTR-1611]

Aconselhamentos técnicos da versão 9.1.5

- A migração para uma versão posterior à 9.0 apresenta falha ao usar um banco de dados do Microsoft SQL 2005. [DDPMTR-1633]
- Adicionado em 02/2016 — após a migração para a versão 9.1.5, o grupo Usuários do Domínio do Remote Management Console não exibe todos os usuários do grupo. [DDPS-1937]
- Adicionado em 02/2016 — o Remote Management Console exibe o status desprotegido para unidades USB criptografadas pelo EMS. [DDPS-2835]

Novos recursos e funcionalidades da versão 9.1

- Os direitos de Administrador Forense para um Grupo de Usuários agora podem ser delegados pelo Superadministrador ou pelo Administrador de Segurança a um membro do Grupo de Usuários.
- Agora, o Server Encryption é compatível, apresentando controle de portas e criptografia de armazenamento removível, além de suporte à programação de manutenção, que permite o controle sobre a aplicação de políticas que exigem reinicialização.
- Agora, a Ativação Diferida do Client é compatível, permitindo que uma empresa estenda as políticas de criptografia gerenciadas centralmente aos dispositivos dos usuários em um ambiente de BYOD.

- As novas políticas permitem que os administradores suprimam ou filtrem as notificações pop-up do Endpoint Security Suite nos computadores client. Essa atualização é compatível com o Endpoint Security Suite 1.1.1 e os clients posteriores.
- Agora, o suporte ao feedback de usuários para a Dell está disponível por meio da política para a maioria dos clients do Dell Data Protection.

Aconselhamentos técnicos resolvidos da versão 9.1

- Ao adicionar ou editar as regras do Firewall do Client no Remote Management Console, agora, o EtherType Personalizado aceita apenas quatro caracteres, e os valores digitados no campo Nome do Domínio são validados. [DDPMTR-528, DDPMTR-732]
- No Remote Management Console, ao adicionar ou editar as regras do Sistema de Rede Principal, o campo Tipos de Conexão é bloqueado como esperado e não pode ser editado. [DDPMTR-562]
- No Remote Management Console, agora, é possível recuperar um endpoint que foi removido anteriormente. [DDPMTR-640]
- No Remote Management Console, quando é feita uma tentativa de importar uma licença inválida ou duplicada, a mensagem de erro genérica anterior foi substituída por uma mensagem que descreve o erro mais claramente. [DDPMTR-764]
- Agora, a política Credenciais Seguras do Windows é agrupada corretamente com as Políticas de Armazenamento Fixo, e não com as políticas de Configurações Gerais. A política Criptografia SDE Ativada deve ser definida como Verdadeiro para que as Credenciais Seguras do Windows sejam aplicadas. [DDPMTR-786, DDPSTE-638]
- No relatório Dispositivo Móvel do Compliance Reporter, agora, os registros de data e hora dos comandos enviados aos dispositivos móveis estão corretos. [DDPMTR-839]
- No Remote Management Console, Log Analyzer — Ações do Administrador agora exibe dados precisos para alterações de políticas de endpoint, e Logs do Sistema exibe entradas de log-in dos usuários de subdomínios. [DDPMTR-911, DDPMTR-991]
- Após a desinstalação, os logs do wrapper são removidos como esperado. [DDPMTR-913]
- Agora, a política Segurança do Threat Protection desativa todas as políticas e recursos do Threat Protection. [DDPMTR-1011]
- O campo Nome do Host agora é selecionado para inclusão por padrão e os nomes de host exibidos no Resultado do Relatório estão corretos no relatório Detalhes do Threat Protection do Compliance Reporter. [DDPMTR-1014]
- A conciliação do Active Directory não apresenta mais falha quando um dos vários domínios fica off-line ou inacessível na rede. [DDPMTR-1153]
- Foi resolvido o erro de upgrade em que era registrado um erro em relação à tabela UserEntity, coluna EID. [DDPMTR-1237]
- Agora, a política Segurança do Threat Protection desativa todas as políticas e recursos do Threat Protection. As três políticas Proteção contra Malware, Firewall do Client e Proteção da Web não precisam mais ser definidas individualmente como Falso. [DDPSTE-451, DDPMTR-1011]

Aconselhamentos técnicos da versão 9.1

- No Remote Management Console, os campos das políticas com valores numéricos aceitam um caractere "+" ou "-" imediatamente anterior ao valor da política. Para contornar esse problema, certifique-se de não incluir esses caracteres nos valores das políticas antes de confirmá-las. [DDPMTR-765]
- Se os relatórios padrão do Compliance Reporter forem personalizados antes do upgrade, a versão anterior dos relatórios personalizados deverá ser restaurada para continuar a usá-los. No entanto, após a restauração da versão anterior, os novos relatórios incluídos no upgrade não estarão disponíveis. [DDPMTR-870]
- Quando um certificado autoassinado for criado na instalação, ele será válido a partir de um período aproximadamente seis horas posterior ao horário de instalação, em vez de ser imediatamente válido. Para contornar esse problema, na guia Configurações da Server Configuration Tool, selecione a opção Desativar Verificação da Cadeia de Confiança. [DDPMTR-1195]
- Adicionado em 09/2015 — o formato CIDR deve ser usado para especificar uma sub-rede em Configurações do Firewall no Remote Management Console. [DDPMTR-1253]
- No Remote Management Console, ao adicionar ou editar as regras de Firewall do Client e ao selecionar o Protocolo de Transporte ICMP no menu drop-down Transporte, o Tipo de Mensagem exibe o tipo de mensagem padrão como "Resposta-Eco" em vez de "Todos", como esperado. [DDPMTR-1254]
- Ao usar a Autenticação do Windows para executar uma nova instalação ou um upgrade, se as credenciais do usuário conectado forem diferentes das credenciais da conta de serviços de domínio e for usado um certificado de uma autoridade de assinatura, o certificado deverá ser armazenado em uma pasta acessível durante a instalação tanto para a conta de serviços de domínio quanto para o usuário conectado. Se as credenciais do usuário conectado forem diferentes das credenciais da conta de serviços de domínio e for usado um certificado autoassinado, antes de iniciar a instalação ou o upgrade, você deverá fazer log-in com as credenciais da conta de serviços de domínio. [DDPSUS-406]

Novos recursos e funcionalidades da versão 9.0

- Agora, o Dell Enterprise Server oferece suporte ao Endpoint Security Suite com um amplo conjunto de novas políticas e opções de geração de relatórios do Compliance Reporter. O Endpoint Security Suite inclui os seguintes recursos:
- Proteção contra malware
- Client Firewall
- Proteção na web
- DDP|E Encryption
- Gerenciamento de SED
- Advanced Authentication
- BitLocker Manager

Aconselhamentos técnicos resolvidos da versão 9.0

- Agora, o AdminHelp informa corretamente que é possível definir o valor OneTimePassword, em vez de Senha de Uso Único, para as políticas de autenticação de log-in e autenticação na sessão. [DDPS-1594]
- Nas versões localizadas do instalador do Remote Management Console, o banner da caixa de diálogo Host agora é dimensionado corretamente. [DDPSTE-275]
- Quando o Enterprise Server é desinstalado, o arquivo LSARecovery.log agora é removido, como esperado. [DDPSTE-308]
- Agora, o AdminHelp informa corretamente o Intervalo de Consulta padrão do servidor para as Configurações do Sistema SED e TPM como 720 minutos. Além disso, o Intervalo de Consulta do Cloud Storage Server é especificado como 1-1.440 minutos. [DDPSTE-486, DDPSTE-586, DDPSTE-591]
- Agora, estão localizadas algumas áreas das telas do Remote Management Console que, antes, não eram localizadas. [DDPSTE-501, DDPSTE-502, DDPSTE-503]

Aconselhamentos técnicos da versão 9.0

- Nas páginas Resultados do Relatório de Detalhes do Dispositivo Móvel e Eventos do EMS do Compliance Reporter, algumas colunas e as barras de rolagem inferiores não ficam visíveis. [DDPMTR-969]
- No Remote Management Console, quando houver entradas duplicadas de um endpoint do Mobile Edition, selecionar a opção Resolver Usuário exibirá um erro e não resolverá as entradas duplicadas. [DDPSTE-371]
- No Remote Management Console, ao adicionar ou editar as regras do Firewall do Client, os campos Endereço IP e Tipo de Rede não são validados; é possível mover e redimensionar os cabeçalhos das colunas até que os títulos fiquem ilegíveis; é possível selecionar várias linhas, o que impede que elas sejam editadas; o botão Cancelar não responde nas caixas de diálogo Adicionar e Editar; e um executável adicionado só é exibido quando a regra é fechada e, depois, reaberta. [DDPSTE-414, DDPSTE-415, DDPSTE-421, DDPSTE-426, DDPSTE-430, DDPSTE-431, DDPSTE-437, DDPSTE-443]
- No Remote Management Console, ao adicionar regras do Firewall do Client, a caixa de diálogo Adicionar congela ocasionalmente quando são digitados valores formatados incorretamente. Para contornar esse problema, clique no botão Fechar no canto superior direito da caixa de diálogo e, em seguida, clique no botão Adicionar em Especificar Redes para reabrir a caixa de diálogo. [DDPSTE-432]
- Ao realizar uma Limpeza Remota em um dispositivo iOS gerenciado por meio de EAS, embora a Limpeza Remota seja realizada com sucesso e um registro de data e hora Confirmado seja exibido no Enterprise Server, um erro é registrado nos logs do servidor EAS e do Policy Proxy. [DDPSTE-529]
- Uma licença do Mobile Edition só é consumida quando um client móvel é ativado. [DDPSTE-549]
- O arquivo de log do Key Server, log.txt, é armazenado em `C:\<installpath>\Dell\Enterprise Edition\Key Server rather than in C:\`<caminho de instalação>\Dell\Enterprise Edition\Key Server\logs, como esperado. [DDPSTE-637]
- Se um valor personalizado for usado para a Porta TCP do Message Broker, após uma nova instalação ou o upgrade a partir de um Enterprise Server anterior à versão 8.5, o valor deverá ser configurado manualmente. Para uma nova instalação, abra o <diretório de instalação do Compatibility Server>\conf\server_config.xml e altere o valor broker.port para o número de porta correto. Para um upgrade a partir de um Enterprise Server anterior à versão 8.5, altere o valor broker.port do arquivo server_config.xml e o valor activemq.port.tcp de Message Broker\conf\application.properties para o número de porta correto. [DDPSTE-654]