ZENworks 2020 Update 2

Referência O que Há de Novo

Agosto de 2021

Informações legais

Para saber mais sobre informações legais, marcas registradas, isenções de responsabilidade, garantias, exportação e outras restrições de uso, direitos restritos do Governo dos EUA, política de patente e conformidade com FIPS, consulte https://www.novell.com/company/legal/.

As garantias exclusivas para os produtos e serviços da Micro Focus e de suas afiliadas e licenciantes (“Micro Focus”) estão descritas nas declarações de garantia que acompanham esses produtos e serviços. Nenhuma informação nos termos deste documento deve ser interpretada como garantia adicional. A Micro Focus não será responsável por erros técnicos ou editoriais contidos neste documento. As informações constantes neste documento estão sujeitas à mudança sem aviso prévio.

Índice

Sobre este guia

Esta *Referência O Que Há de Novo do ZENworks* descreve os novos recursos na versão do ZENworks 2020 Update 2. O guia inclui as seguintes seções:

Público

Este guia destina-se aos administradores do ZENworks.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o recurso **comment on this topic** (comentar sobre este tópico) na parte inferior de cada página da documentação online.

Documentação adicional

O ZENworks é suportado por documentação adicional (nos formatos PDF e HTML), que pode ser utilizada para que você conheça e implemente o produto. Para acessar a documentação adicional, visite o site da Documentação do ZENworks na Web.

1 O que há de novo no ZENworks 2020 Update 2

As seções a seguir descrevem os novos recursos e aprimoramentos no ZENworks 2020 Update 2:

Suporte de plataforma

As seguintes plataformas novas são suportadas nesta versão:

- CentOS como Dispositivo Gerenciado
- macOS 11 (Big Sur) como Dispositivo Gerenciado
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (Servidor Principal)
  - SLES 15 SP2 (Dispositivo Gerenciado – Incluindo SLES para SAP)
  - SLED 15 SP2 (Dispositivo Gerenciado)
- Novas Plataformas Linux RHEL e Scientific
  - Scientific Linux 7.7 e 7.8
  - RHEL 7.8 e 8.2

Instalação e upgrade

Como o ZENworks pretende adotar uma arquitetura mais robusta e flexível e se alinhar aos padrões da Micro Focus, alguns aprimoramentos foram introduzidos no processo de Instalação e Upgrade na versão do ZENworks 2020 Update 2. Veja abaixo as mudanças introduzidas nessa versão:

Instalando o Docker e o Docker Compose

Antes de fazer upgrade ou instalar o ZENworks 2020 Update 2 em um Servidor Principal Linux, é necessário instalar o Docker e o Docker Compose no servidor. Para obter mais informações sobre Dockers, consulte https://docs.docker.com/.

Migrando dados do servidor para um novo caminho de arquivo

Após o upgrade para o ZENworks 2020 Update 2 em um Servidor Principal Windows, Linux ou da Aplicação, os dados do Servidor ZENworks, como MSIs, RPMs, registros e arquivos de configuração, que antes estavam no caminho de arquivo da Novell serão movidos para o novo caminho de arquivo da Micro Focus.

Por exemplo, em um servidor Linux, os arquivos de configuração que estavam em `/etc/opt/novell/zenworks` agora estarão disponíveis em `/etc/opt/microfocus/zenworks`. Da mesma forma, em um servidor Windows, os arquivos de configuração que estavam em `C:\Arquivos de Programas (x86)\Novell\ZENworks\conf` agora estarão disponíveis em `C:\Arquivos de Programas (x86)\Micro Focus\ZENworks\conf`.

Os arquivos e dados relacionados ao agente do ZENworks continuarão no local antigo da Novell.

Renomeando os serviços do servidor ZENworks

Após o upgrade para o ZENworks 2020 Update 2 em um Servidor Principal Windows, Linux ou da Aplicação, determinados serviços do servidor ZENworks, como ZENServer, ZENLoader e ZENJoinProxy, serão renomeados de Novell para Micro Focus. Por exemplo, em um servidor Linux, `novell-zenserver.service` será renomeado para `microfocus-zenserver.service`.

Introdução de uma nova variável de ambiente

Para um servidor Windows, foi introduzida uma nova variável de ambiente `%ZENSERVER_HOME%` que também aponta para o local de instalação do Servidor de um caminho não padrão (`C:\Arquivos de Programas (x86)\Micro Focus\ZENworks`).

Versão do TLS

Se você instalou recentemente o ZENworks 2020 Update 2, por padrão, o TLS1.2 está habilitado na zona e, quando você tentar registrar dispositivos com uma versão do Microsoft .NET anterior à 4.7, haverá falha no registro dos dispositivos. No entanto, o agente será instalado nos dispositivos.

Se você fizer upgrade de uma zona existente para o ZENworks 2020 Update 2, o TLS1.2 não estará habilitado por padrão. Se você habilitar o TLS1.2 na zona, alguns dos recursos talvez não funcionem conforme esperado, e certifique-se de instalar o Microsoft .NET 4.7 em todos os dispositivos na zona.

Se você habilitar o TLS1.2 na zona, o dispositivo deverá ser instalado com o Microsoft .NET 4.7 para ser registrado.

Substituindo servidores principais

Para obter mais detalhes sobre como substituir o primeiro Servidor Principal pelo segundo Servidor Principal ou substituir um Servidor Principal existente por um novo Servidor Principal, consulte *Replacing Primary Servers* (Substituindo servidores principais) na *ZENworks Disaster Recovery Reference* (Referência de Recuperação de Desastre do ZENworks).

Movendo um servidor principal para uma aplicação

Para obter mais detalhes sobre o procedimento para mover um Servidor Principal existente (Windows ou Linux) para um servidor da Aplicação, consulte *Moving from a Windows or Linux Primary Server to Appliance* (Movendo de um servidor principal Windows ou Linux para a aplicação) na *ZENworks Primary Server and Satellite Reference* (Referência de Servidor Principal e Satélite do ZENworks).

ZENworks Configuration Management

Gerenciamento de dispositivo do Windows 10

Na versão do ZENworks 2020 Update 2, novos recursos foram adicionados para permitir que você gerencie todo o ciclo de vida dos dispositivos Windows 10 usando o agente MDM incorporado nesses dispositivos. Para atender a casos de uso além dos recursos dos dispositivos Windows 10, você também pode implantar o agente do ZENworks em dispositivos que usam os agentes MDM do Windows 10.

Para obter mais informações sobre cada um dos recursos listados nesta seção, consulte a Windows MDM Reference (Referência do MDM do Windows).

Veja abaixo os novos recursos:

Recursos de configuração

Agora você pode configurar o Serviço de Notificação do Windows (WNS, Windows Notification Service) para enviar notificações por push a dispositivos Windows gerenciados pelo Windows Modern Management.

Recursos de registro

Os recursos de registro a seguir foram introduzidos.

Métodos de Registro: Os dispositivos Windows 10 podem ser registrados no ZENworks usando os métodos abaixo.

- Registro de pacote de aprovisionamento (PPKG)
- Ingresso no Azure Active Directory (Azure AD)
- Registro do Autopilot

Implantação do Agente do ZENworks: Agora é possível implantar o Agente do ZENworks em dispositivos Windows 10 que já foram registrados usando o modo de registro MDM.

Configuração dos Termos de Uso: Você pode atribuir a política de Termos de Uso a dispositivos para adicionar o conteúdo dos Termos de Uso que será exibido no agente durante o registro de dispositivos Windows 10, usando o registro de Ingresso no Azure AD ou do AutoPilot.

Recursos de gerenciamento

Os seguintes recursos de gerenciamento foram introduzidos:

Implantação de Bundles MDM do Windows 10: Agora é possível implantar os seguintes bundles em dispositivos MDM Windows 10:

Observação: O suporte a esses bundles está em fase experimental e deve ser usado apenas para fins de avaliação.

- O uso do bundle MDM Windows 10 – Instalar MSI implanta um pacote do Microsoft Installer (MSI) nos dispositivos MDM Windows 10.
- O uso do bundle CSP MDM Windows 10 distribui Provedores de Serviços de Configuração (CSPs, Configuration Service Providers) para implantar várias configurações disponíveis por meio dos CSPs nos dispositivos MDM Windows 10.

Inicialização de Tarefas Rápidas: As seguintes tarefas rápidas são suportadas nos Dispositivos MDM Windows 10:

- Apagar Dispositivo
- Anular Registro do Dispositivo
- Descartar Dispositivo
- Anular Descarte do Dispositivo
- Dispositivo Perdido
- Cancelar Registro do Dispositivo

Outros recursos

Veja a seguir alguns dos outros recursos introduzidos para o recurso MDM do Windows 10:

- Os Dispositivos Windows 10 suportam reconciliação automática.
- O processo de Recriação da CA agora emite certificados para dispositivos MDM Windows 10.
- A configuração da API do MS Graph foi renomeada para Aplicativo MDM do Azure e precisa ser reconfigurada para aproveitar as vantagens dos novos aprimoramentos introduzidos nesta versão.

Introdução ao gerenciamento moderno

A página de Introdução do Gerenciamento Móvel foi reformulada para incluir também o registro e o gerenciamento dos dispositivos MDM Windows 10. Para obter mais informações, consulte a Modern Management Reference (Referência de Gerenciamento Moderno).

ZENworks Imaging

Restaurar Imagem usando o nome do bundle no WinPE: No ZENworks 2020 Update 1 e nas versões anteriores, a distro do WinPE suportava a restauração da imagem fornecendo o nome da imagem pelo comando IMG, e o comando não reconhecia se o bundle tinha sido especificado pelo comando. A partir do ZENworks 2020 Update 2, os comandos do bundle IMG são suportados na distro do WinPE. Para obter mais informações, consulte o guia sobre Preboot Services e Criação de Imagens.

Nova ferramenta para ler Informações sobre Imagens do ZENworks: A ferramenta zmginfo ajuda a reunir informações sobre uma imagem. Isso é útil principalmente quando você tem várias imagens no repositório de conteúdo ou no caminho compartilhado e precisa coletar informações sobre cada imagem para economizar tempo. Usando a ferramenta zmginfo, você pode reunir as informações básicas ou completas sobre a imagem. Usando o zmginfo, o administrador pode criar o xml do bundle, que pode ser importado como bundle e usado para converter todas as imagens de base do Linux em imagens de base do winpe.

Para obter mais informações, consulte o guia sobre Preboot Services e Criação de Imagens.

Gerenciamento remoto do ZENworks

Controle Remoto de um dispositivo com Sessão RDP ativa: Agora você poderá iniciar uma sessão remota em um dispositivo com uma sessão RDP ativa, da mesma forma que uma sessão de Gerenciamento Remoto normal. Para obter mais informações, consulte o guia da Remote Management Reference (Referência de Gerenciamento Remoto).

Gravação de uma Sessão de Gerenciamento Remoto (Suporte Experimental): Permite que os usuários no dispositivo gerenciado gravem a sessão de gerenciamento remoto. Para obter mais informações, consulte o guia da Remote Management Reference (Referência de Gerenciamento Remoto).

Gerenciamento móvel

Habilitação de atribuições de dispositivo para bundles Android: Os bundles Android criados para aplicativos da Play Store aprovados que antes eram restritos a atribuições de usuários agora também podem ser atribuídos a dispositivos. Para obter mais informações, consulte a Mobile Management Reference (Referência de Gerenciamento Móvel).

Aprovisionamento de Aplicativos do Sistema: Usando o recurso Bundles, você pode habilitar ou desabilitar os Aplicativos do Sistema em dispositivos Android. Os aplicativos do sistema são aplicativos internos pré-instalados no dispositivo. Para obter mais informações, consulte a Mobile Management Reference (Referência de Gerenciamento Móvel).

Introdução ao Gerenciamento Moderno: A página de Introdução do Gerenciamento Móvel foi reformulada para incluir também o registro e o gerenciamento dos dispositivos MDM Windows 10. Além disso, alguns recursos adicionais associados ao registro e ao gerenciamento de dispositivos Apple e Android foram incluídos nessa página. Para obter mais informações, consulte a Modern Management Reference (Referência de Gerenciamento Moderno).

Modificação do Local de Registro do Dispositivo Android: O local dos registros do Aplicativo do ZENworks nos dispositivos Android foi modificado para `Android/data/com.novell.zapp/files/Documents/zapp.log`. Para compartilhar esses registros, você precisa implantar o aplicativo Files nos dispositivos Android.

Gerenciamento de bundles

Uma nova opção **Continuar em caso de falha** foi incluída no workflow Copiar Relacionamentos. Ao copiar relacionamentos de um dispositivo para outro conjunto de objetos, se houver um erro, a operação continuará para o restante dos objetos. Os detalhes dos erros serão exibidos no final da operação, junto com uma opção para exportar os detalhes da operação para referência e ação futuras. Para obter mais informações, consulte a Software Distribution Reference (Referência de Distribuição de Software).

Diversos

Habilitar clientes a usar a versão mais recente do pacote puppet-agent: Antes, o ZENworks incluía o pacote puppet-agent como parte do build, o que permitia que os usuários usassem a política Puppet. No entanto, com as atualizações contínuas da versão do puppet-agent, após o lançamento do ZENworks, os usuários não podiam usar a versão mais recente do pacote puppet-agent. A partir desta versão, para que a política Puppet seja eficaz no ZENworks 2020 Update 2 e versões mais recentes nos dispositivos gerenciados pelo Linux, você precisa garantir que o pacote puppet-agent seja instalado nos dispositivos. Para obter mais informações, consulte a Configuration Policies Reference (Referência de Políticas de Configuração).

Aprimoramentos de segurança no ZENworks

Os aprimoramentos de segurança introduzidos nesta versão permitem registrar e comunicar-se com os dispositivos de forma segura, mesmo em um ambiente DMZ.

- Se você instalou recentemente o ZENworks 2020 Update 2, por padrão, as configurações de Segurança estão habilitadas em todos os Servidores Principais.
- Se você fizer upgrade dos Servidores Principais, por padrão, as configurações de Segurança estarão desabilitadas.
- Se você adicionar um novo Servidor Principal à zona, por padrão, as Configurações de Segurança estarão habilitadas após o upgrade para o ZENworks 2020 Update 2.

Você precisa executar o seguinte comando zman para habilitar as configurações:

- `zman ssassc` (Security-Set-Agent-Server-Secure-Communication) foi introduzido para habilitar ou desabilitar a autenticação para comunicação entre o Agente do ZENworks e os servidores ZENworks.

Para obter mais informações sobre os Aprimoramentos de Segurança apresentados nesta versão, consulte a ZENworks Securing Devices Reference (Referência de Proteção de Dispositivos do ZENworks).

Registro do dispositivo

Pré-aprovando o registro do dispositivo

Os dispositivos pré-aprovados são aqueles aprovados pelos administradores para fazer parte da zona. Isso é útil principalmente quando você precisa pré-aprovar dispositivos durante o registro em massa de um conjunto conhecido de dispositivos. É possível usá-lo também para permitir a reconciliação de dispositivos conhecidos, se necessário.

Usando a chave de autorização

Uma chave de Autorização pode ser usada pelo agente do ZENworks para autorizar o próprio registro na zona e para qualquer comunicação com o servidor durante a instalação.

Protegendo o dispositivo gerenciado e o registro do dispositivo iOA

Para registrar os agentes iOA mais recentes ou os Dispositivos Gerenciados na zona, você precisa especificar uma chave de Autorização durante o registro do dispositivo ou garantir que o dispositivo faça parte da lista de dispositivos pré-aprovados.

Comunicação do dispositivo

Usando o OSP para comunicação do dispositivo, incluindo o login no ZCC

Para a maioria dos recursos, o ZENworks passou a usar o protocolo O-Auth para estabelecer a identidade do usuário. Portanto, um novo serviço chamado OSP foi introduzido e é usado para efetuar login no ZCC e para comunicação entre serviços e entre o dispositivo e os servidores.

Protegendo o conteúdo e a coleta entre dispositivos, servidores principais e servidores satélites

Com a introdução desse novo recurso de segurança, a coleta de ponta a ponta e a transferência de conteúdo entre dispositivos gerenciados, Servidores Principais e Servidores Satélites são feitas por SSL. Para isso, basta especificar a configuração no ZCC ou usar os comandos zman recém-incluídos.

Protegendo a comunicação de serviço Web entre o dispositivo e o servidor principal ou satélite

Para reforçar a segurança da comunicação de serviço Web entre o Agente do ZENworks e os servidores Principal e Satélite do ZENworks, foram feitas melhorias de segurança nas chamadas de serviço Web nesta versão.

Exclusões de unidade da política de criptografia de dados da Microsoft

As unidades de dados removíveis agora podem ser excluídas da criptografia por tipo de unidade na Política de Criptografia de Dados da Microsoft quando o uso obrigatório da política é assegurado nos dispositivos gerenciados.

Antimalware

O Antimalware do ZENworks é um novo componente do ZENworks Endpoint Security Management no agrupamento Segurança do ZENworks Control Center. O Antimalware é uma solução compacta que protege os dispositivos gerenciados contra todas as ameaças de malware mais recentes. Quando implantado nos dispositivos em sua zona, o Agente de Antimalware recebe continuamente as atualizações dos arquivos de autenticação de malware do Serviço de Nuvem do Antimalware para detectar infecções por malware por meio das verificações tanto no momento do acesso quanto sob demanda. Os arquivos infectados são colocados em quarentena até serem desinfetados.

Para obter mais informações sobre os tópicos desta seção, consulte o seguinte:

- ZENworks Endpoint Security Antimalware Reference (Referência do Antimalware do ZENworks Endpoint Security)

Página Protegendo Contra Malware – Introdução

A página de Introdução de Segurança inclui uma página adicional com guias chamada “Protegendo Contra Malware”. É possível usá-la como um ponto único de acesso para configurar, implantar e personalizar todos os recursos que o Antimalware do ZENworks oferece.

Direitos de atualização de Antimalware

Os Direitos de Atualização de Antimalware são necessários para implantar políticas Antimalware nos dispositivos. Os direitos são habilitados automaticamente para o período de avaliação ao ativar o Gerenciamento de Segurança de Endpoint no modo de Avaliação.

Políticas de segurança de endpoint do Windows

Quatro novas políticas são usadas para gerenciar a implantação, a personalização e a continuidade do Antimalware:

Política de Imposição de Antimalware: Essa é a política de base que instala o Agente de Antimalware nos dispositivos gerenciados. Essa política deve ser implantada para usar qualquer uma das outras políticas Antimalware. Ela inclui configurações para todos os tipos de verificações de malware, incluindo no momento do acesso, completas, rápidas, de dispositivo externo e contextuais sob demanda. Também há configurações para comportamento de quarentena e definição de conteúdo para ser excluído das verificações.

Se as configurações padrão dos direitos e das notificações do usuário final forem mantidas quando a política for implantada, os usuários finais terão acesso ao Console de Status do Agente em seus endpoints, o que permite iniciar as próprias verificações, ver o status de atualização da verificação e do agente e receber notificações da atividade do agente controlada pela política.

Política de Exclusões da Verificação de Antimalware: O Antimalware oferece exclusões da verificação tanto internas quanto personalizadas que você pode adicionar a qualquer uma das políticas Antimalware. A política de Exclusões da Verificação é empregada pela atribuição de dispositivo quando outras políticas Antimalware também são atribuídas aos mesmos dispositivos, o que simplifica a propagação das exclusões da verificação na zona. É possível habilitar ou desabilitar as exclusões para tipos de verificação específicos.

Política de Verificação Personalizada de Antimalware: A Política de Verificação Personalizada é usada em uma abordagem mais direcionada para verificar unidades locais em dispositivos gerenciados quando há suspeita de uma ameaça específica ou para direcionar as verificações para determinados locais nesses dispositivos. Ela inclui uma programação própria, em vez de usar a programação da zona configurada para a Política de Imposição Antimalware.

Política de Verificação de Rede de Antimalware: A Política de Verificação de Rede também é usada em uma abordagem mais direcionada, porém, explicitamente para verificar pastas e arquivos em unidades de Rede. Ela também tem uma programação própria e inclui uma configuração adicional para autenticação em locais de rede.

Dashlets de segurança do Antimalware

Quatro novos dashlets que assumem como padrão o Painel de Segurança são oferecidos para monitorar ameaças de malware, verificações de malware e atualizações de autenticação de malware.

Status de malware do dispositivo: Esse dashlet exibe o status do malware para dispositivos individuais na zona referente a um período de detecção selecionado.

Última verificação de malware do dispositivo: Esse dashlet exibe a saúde dos dispositivos na zona contra ameaças de malware. Por padrão, ele exibe informações sobre qualquer tipo de verificação executada nos dispositivos para um período especificado.

Principais ameaças de malware: Esse dashlet exibe a lista das principais ameaças de malware na zona. Por padrão, as principais ameaças de malware são exibidas com base no número de dispositivos infectados.

Versão de autenticação de malware do dispositivo: Esse dashlet exibe a lista de versões de Autenticação de Malware e as versões do Agente de Antimalware que estão instaladas nos dispositivos da zona.

Página Antimalware do dispositivo

Essa página é uma nova guia acessada quando um dispositivo é selecionado. Ela mostra o status de instantâneo das ameaças de malware, a programação da verificação e as informações sobre o arquivo em quarentena referentes ao dispositivo selecionado. Você também pode executar ações específicas nos arquivos, iniciar verificações e atualizar as versões do Agente de Antimalware e de Autenticação de Malware no dispositivo.

Página de detalhes da ameaça de malware

Para acessar essa página, clique em um link de ameaça de malware na seção Ameaças de Malware da página Antimalware de um dispositivo. Ela mostra informações detalhadas sobre a ameaça selecionada e detalhes dos dispositivos que foram infectados com a ameaça.

Tarefas rápidas do Antimalware

Quando um ou mais dispositivos com o Agente de Antimalware instalado são selecionados no agrupamento Dispositivos do ZENworks Control Center, cinco novas tarefas rápidas ficam disponíveis para execução nos dispositivos selecionados. Veja abaixo as tarefas rápidas incluídas:

- Iniciar Verificação de Malware
- Atualizar Autenticação de Malware
- Atualizar Agente de Antimalware
- Restaurar Arquivo da Quarentena de Malware
- Apagar Arquivo da Quarentena de Malware

Comandos zac do Antimalware

O Antimalware inclui vários comandos zac novos específicos desse componente. Os comandos incluídos são: iniciar verificações de malware nos dispositivos, verificar o status do malware do Agente de Antimalware, instalar, atualizar ou remover o agente e apagar arquivos da quarentena, entre outros.

Páginas Configuração da Zona do Antimalware

Agora há três novas páginas de configuração da zona incluídas no agrupamento Segurança da página principal de configuração do ZENworks. Cada uma dessas páginas inclui configurações padrão que você pode personalizar. As páginas são as seguintes:

Programações do agente de Antimalware: Define as programações para verificações de malware e atualizações de assinaturas de malware. Você pode anular essa programação no nível da pasta de dispositivo ou do dispositivo.

Notificações do agente de Antimalware: Configura os alertas e as notificações que são exibidos pelo agente de Antimalware nos dispositivos gerenciados. Você pode anular essas configurações no nível da pasta de dispositivo ou do dispositivo.

Configuração do Antimalware: Define o Servidor Principal do ZENworks que será usado como servidor Antimalware, que deve ser configurado manualmente para implantar o componente Antimalware. Ela também define a programação de manutenção do Agente de Antimalware.

Página de configuração de conteúdo sob demanda

Essa nova página de configuração da zona agora faz parte do agrupamento Bundle, Política e Conteúdo da página principal de configuração do ZENworks. Ela gerencia a taxa de download e o tamanho do cache de conteúdo para distribuição do conteúdo na zona, que atualmente inclui arquivos de autenticação do Antimalware e atualizações do Agente de Antimalware.

Status do serviço Antimalware

O status do Serviço Antimalware agora pode ser acessado na página Diagnósticos do ZCC.

Banco de dados Antimalware

O Banco de Dados Antimalware é novo no ZENworks 2020 Update 2. Sua finalidade é fornecer dados para os recursos de monitoramento do Antimalware pela página Antimalware e pelos dashlets de segurança do Antimalware. Quando configurado, esse banco de dados é sincronizado com o Banco de Dados do ZENworks e, portanto, deve ser do mesmo tipo. Por exemplo: PostgreSQL, Microsoft SQL Server ou Oracle.

O Banco de Dados Antimalware é configurado na página Protegendo Contra Malware – Introdução em Segurança no ZENworks Control Center. Se o Banco de Dados Antimalware for configurado usando um banco de dados externo que ainda não existe, será possível criar um por meio de um comando da CLI usando o arquivo `setup.exe`.