



Endpoint Administrator

MD-102



Módulo 08: Implantar dispositivos usando o Windows Autopilot

Implantar dispositivos usando o Windows Autopilot

Introdução

Tradicionalmente, o processo de implantação de um novo dispositivo começa com a limpeza do dispositivo com qualquer sistema operacional pré-instalado e a implantação de uma das imagens da organização no dispositivo. No entanto, quando os administradores estão comprando um dispositivo de um OEM, o Windows 11 já é o sistema operacional no dispositivo. Embora simplesmente o uso da imagem do OEM não seja prático, o Windows 10 introduziu um novo processo chamado Windows Autopilot. O Autopilot foi projetado para obter o resultado desejado de implantar um novo hardware ou atualizar um hardware existente com a configuração desejada da organização, sem o processo de criar, gerenciar e enviar imagens grandes pela rede.

Usar o Autopilot para implantação moderna

Os métodos de implantação modernos adotam uma nova abordagem para provisionar dispositivos. Um dos principais benefícios do Windows 10 e posteriores é um recurso chamado Windows Autopilot. O Windows Autopilot é um método de implantação baseado em nuvem. Com o Autopilot, você pode configurar e pré-configurar dispositivos novos e existentes do Windows 10 ou posteriores. Os usuários em sua organização usam uma nova experiência pronta para uso do sistema operacional (OOBE) para configurar dispositivos sem precisar de uma imagem do Windows.

- O Autopilot oferece as seguintes vantagens em relação aos métodos de implantação locais:
- Você não precisa usar imagens.
- Você não precisa personalizar as implantações injetando drivers.
- Você não precisa implantar e manter uma infraestrutura de implantação.
- A configuração de implantações do Autopilot é relativamente simples em comparação com a criação e o gerenciamento de imagens tradicionais.
- Sem imagens para implantar, o consumo de largura de banda pesada não é mais uma preocupação.

Usar o Autopilot para implantação moderna (cont).

O Windows Autopilot é baseado em nuvem e baseado no Azure AD Premium e no Microsoft Intune. Usando o Windows Autopilot, você pode:

- Ingressar dispositivos no Azure AD automaticamente.
- Registre automaticamente dispositivos dos usuários em serviços de MDM.
- Restringir a criação da conta Administrador.
- Personalizar o conteúdo OOBÉ especificamente para sua organização.

Usar o Autopilot para implantação moderna (cont).

Comparando o Autopilot com métodos tradicionais:

	Implantação tradicional	Implantação moderna
Implanta imagens do Windows 11	Sim	Não
Pode ser usado com qualquer sistema operacional pré-instalado	Sim	Não
Requer uma instalação anterior do Windows 11	Não	Sim
Usa uma infraestrutura local	Sim	Não
Ferramentas para preparar a implantação	Windows ADK, Serviços de Implantação do Windows, Microsoft Deployment Toolkit (MDT) e Microsoft Configuration Manager	Designer de configuração do Windows e piloto automático do Windows

Usar o Autopilot para implantação moderna (cont).

Há certas circunstâncias em que os métodos de instalação tradicionais devem ser usados em vez do Autopilot. Esses cenários incluem:

- Implantações bare-metal.
- Quando o hardware de armazenamento em que o Windows 11 está instalado precisa ser substituído.
- No caso de uma instalação do Windows 11 corrompida.
- Quando uma organização exige solicitações de informações personalizadas do usuário além do que a configuração OOBÉ oferece (como personalizar a interface LTI com o MDT).

Examine os requisitos do Windows Autopilot

1

Os dispositivos devem ter o Windows 11 pré-instalado:

- Windows Pro, Enterprise ou Education

2

Os dispositivos devem ter conectividade com a Internet:

- O Windows Autopilot é um serviço em nuvem

3

Intune ou outro serviço de gerenciamento de dispositivos móveis (opcional):

- Para gerenciar dispositivos Windows 10 implantados e posteriores

4

Os dispositivos devem ser registrados na organização:

- Informações específicas do dispositivo enviadas para a nuvem

5

A organização deve usar o Azure AD (Entra ID):

- Ele também deve usar o Microsoft Store for Business ou o Intune

6

Acesso as URLs necessárias

- go.microsoft.com
- login.microsoftonline.com
- etc.

Preparar identidades do dispositivo para o Autopilot

- Processo de implantação do Windows Autopilot:
 - Obtenha IDs de hardware dos dispositivos que você deseja implantar.
 - Carregue os IDs de hardware.
 - Crie um perfil de implantação do Windows Autopilot.
 - Aplique o perfil de implantação do Windows Autopilot aos dispositivos ou grupos de dispositivos.
- Gerenciar o Windows Autopilot no Intune
 - Configure o registro automático de gerenciamento de dispositivos móveis de dispositivos membros do Azure AD (Entra ID).
- Preparar uma implantação do Microsoft Autopilot
 - Gerencie a implantação do Windows Autopilot usando o Intune ou a Microsoft Store para Empresas.
- Obtenha ou crie um arquivo CSV específico do dispositivo
 - Arquivo CSV necessário para implantar dispositivos usando o Windows Autopilot.
- Importe um hash de dispositivo diretamente para o Intune

Implemente o registro de dispositivos e a personalização pronta para uso

Passo 1

Crie um arquivo de implantação do Windows Autopilot

- Um perfil obrigatório que especifica as configurações a serem aplicadas aos dispositivos
- Você pode criar e usar vários perfis de implantação com o Windows Autopilot, mas só pode usar um único perfil para implantar cada dispositivo

Passo 2

Aplicar um perfil de implantação

- Até você aplicar o perfil de implantação, o Windows Autopilot não gerencia a fase de configuração do OOB no dispositivo
- O Windows Autopilot assume o controle da fase de configuração do OOB nos dispositivos aos quais você aplica o perfil

Comparar a experiência padrão e OOBÉ do Autopilot

Quando os funcionários ativam um computador que um fornecedor de hardware entregou, a fase de instalação do OOBÉ ocorre. Durante essa fase, o sistema operacional Windows solicita várias configurações, como:

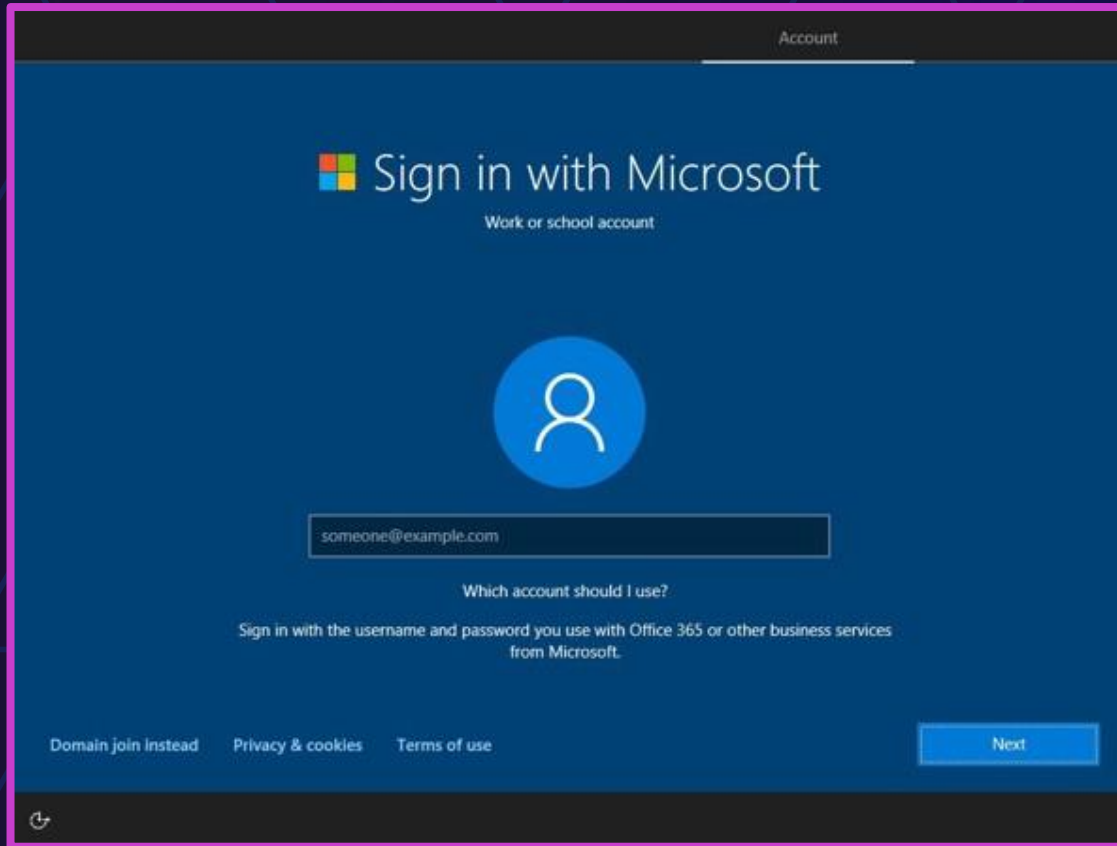
- Qual é o layout de teclado preferido?
- Aceita os Termos de Licença para Software Microsoft?
- O computador deve ingressar no AD DS ou Azure AD?
- Quais configurações de privacidade você deve usar?

Essas configurações podem ser confusas para os funcionários e, portanto, elas geralmente chamam o suporte técnico ou configuram incorretamente o Windows. Com a implantação de imagem personalizada tradicional, você pode pré-configurar essas configurações para que os funcionários não possam exibí-las ou configurá-las. No entanto, quando um fornecedor de hardware entrega um computador diretamente, a imagem padrão do Windows é usada e o funcionário precisa fornecer todas as configurações. Um funcionário que conclui o OOBÉ também se torna membro do grupo administradores local, o que pode causar muitos problemas.

Comparar a experiência padrão e OOBÉ do Autopilot (Cont).

O Windows Autopilot coloca os administradores no controle de toda a fase de instalação do OOBÉ para dispositivos Windows conhecidos. Depois que os administradores identificarem dispositivos por suas IDs de hardware, eles poderão criar e aplicar um perfil de implantação do Windows Autopilot a esses dispositivos. Quando os dispositivos começam e têm conectividade com a Internet, eles se conectam ao serviço de nuvem do Windows Autopilot, solicitam aos funcionários suas credenciais de empresa e aplicam as configurações do perfil do Windows Autopilot. Isso pré-configura e oculta muitas caixas de diálogo que, de outra forma, seriam exibidas durante o OOBÉ. Ele simplifica a experiência do usuário e permite que os funcionários obtenham dispositivos Windows configurados e produtivos em apenas algumas seleções. Com base nas credenciais dos funcionários, os dispositivos ingressam Azure AD e podem se registrar automaticamente no Intune ou em outra solução de gerenciamento de dispositivo móvel.

Comparar a experiência padrão e OOB E do Autopilot (Cont).



Fase de configuração OOB E padrão



Fase de configuração OOB E com Windows
Autopilot

Examinar os cenários do Autopilot

Modo orientado ao usuário:

O modo controlado pelo usuário do Windows Autopilot foi projetado para permitir que novos dispositivos Windows 10 ou posterior sejam transformados do estado inicial, diretamente da fábrica, em um estado pronto para uso sem exigir que a equipe de TI toque no dispositivo. O processo foi projetado para ser simples, de modo que qualquer pessoa possa realizá-lo, permitindo que os dispositivos sejam enviados ou distribuídos para o usuário final diretamente com instruções simples:

- Retire o dispositivo da caixa, conecte-o e ligue-o.
- Escolha um idioma, uma localidade e um teclado.
- Conecte-o a uma rede sem fio ou com fio com acesso à Internet.
- Especifique seu endereço de email e a senha da sua conta da organização.

Examinar os cenários do Autopilot (Cont).

Modo de autoimplantação:

O modo de autoimplantação do Windows Autopilot permite que um dispositivo seja implantado com pouca ou nenhuma interação do usuário, obtendo uma experiência ZTI com todos os prompts da OOBЕ configurados previamente. A página de status de registro será exibida enquanto o dispositivo estiver sendo configurado e, em seguida, o computador preencherá e exibirá a tela de entrada, pronta para as credenciais do Azure AD. Se o dispositivo estiver configurado como um dispositivo de quiosque, ele entrará automaticamente com uma conta configurada localmente.

Para executar uma implantação de modo de autoimplantação usando o Windows Autopilot:

Crie um perfil do Autopilot para o modo de autoimplantação com as configurações desejadas. No Microsoft Intune, esse modo é explicitamente escolhido quando o perfil é criado. Observe que esse modo não está disponível por meio do Microsoft Store para Empresas.

Verifique se o perfil foi atribuído ao dispositivo antes de tentar implantar esse dispositivo.

O modo de autoimplantação exige dispositivos com o TPM 2.0 e o Windows 10 versão 1903 ou posterior.

Examinar os cenários do Autopilot (Cont).

Autopilot para dispositivos existentes:

Conforme discutido anteriormente, o processo do Autopilot exige que o dispositivo tenha o Windows 10 ou o Windows 11 instalado. Esse recurso permite a recriação da imagem e o provisionamento de um dispositivo 8.1 para o modo controlado pelo usuário do Windows Autopilot com uma só sequência de tarefas nativa do Configuration Manager. Esse processo permite que um dispositivo tradicionalmente gerenciado com imagens faça a transição para o dispositivo usando métodos modernos.

Para facilitar isso, uma sequência de tarefas especial precisa ser usada para implantar a imagem no dispositivo Windows 8.1, o que inclui a entrega de um arquivo de configuração associado a um perfil do Intune. Os perfis precisam ser criados no Microsoft Intune antes da criação dos arquivos de configuração.

Examinar os cenários do Autopilot (Cont).

Windows Autopilot para implantação previamente provisionada

A partir do Windows 10 versão 1903, o Windows Autopilot também pode fornecer uma funcionalidade que permita que os parceiros ou a equipe de TI provisionem previamente um computador Windows, de modo que ele esteja totalmente configurado e pronto para os negócios. Do ponto de vista do usuário final, a experiência controlada pelo usuário do Windows Autopilot permanece inalterada, mas levar seu dispositivo a um estado totalmente provisionado é mais rápido.

Em vez de todo o processo de provisionamento ocorrer quando o usuário ligar o dispositivo, o processo de provisionamento será dividido. As partes demoradas, como instalações e políticas de aplicativo de dispositivo e usuário, são realizadas pela TI. As configurações e as políticas finais do usuário são aplicadas quando o usuário conecta e liga o dispositivo.

A implantação provisionada previamente exige o Windows 1903 ou posterior e uma assinatura do Intune. O dispositivo também precisa dar suporte ao TPM 2.0 e ao atestado de dispositivo, não havendo suporte para máquinas virtuais. O acesso ao domínio local não é necessário no processo de provisionamento prévio. A conectividade com a Internet (ou a conectividade com um controlador de domínio que esteja usando o ingresso no Azure AD híbrido) é necessária durante o processo final do usuário.

Examinar os cenários do Autopilot (Cont).

Redefinição do Windows Autopilot

Em muitos ambientes, você precisará regularmente redefinir os dispositivos para os estados iniciais depois que eles estiverem em uso por algum tempo. Por exemplo, uma organização pode fornecer dispositivos Windows aos funcionários temporários, que a organização precisa redefinir para cada novo usuário. As organizações também precisam redefinir os computadores nas salas de treinamento após cada aula. Com a implantação tradicional, você precisará reimplantar a imagem do Windows sempre que redefinir um dispositivo para o estado inicial. A Redefinição do Windows Autopilot permite que você atinja essa meta sem reimplantar uma imagem do Windows. Ela remove todos os arquivos pessoais, os aplicativos e as configurações e redefine um dispositivo Windows para o estado inicial na tela de bloqueio. Também pode implantar aplicativos e configurações organizacionais usando o Intune ou outra solução de MDM para que um dispositivo esteja pronto para uso após a Redefinição do Windows Autopilot.

A Redefinição do Windows Autopilot dá suporte a dois cenários:

- Redefinição local
- Redefinição remota

Examinar os cenários do Autopilot (Cont).

Redefinição local do Windows Autopilot

A Redefinição local do Windows Autopilot usa a funcionalidade de redefinição do Windows. Você pode usar a Redefinição local do Windows Autopilot, independentemente de como você está gerenciando um dispositivo no momento. Ela preserva o nome do dispositivo, a associação ao Azure AD e o registro de MDM.

Por padrão, a Redefinição local do Windows Autopilot está desabilitada no Windows, o que ajuda a garantir que ela não seja iniciada acidentalmente. Para habilitar a Redefinição local do Windows Autopilot, defina a política `DisableAutomaticReDeploymentCredentials` como 0 (false).

Depois de habilitar a Redefinição local do Windows Autopilot, inicie-a pressionando CTRL + Tecla do logotipo do Windows + R quando estiver na tela de bloqueio do Windows. Somente os usuários com permissões administrativas podem iniciar a Redefinição local do Windows Autopilot.

Examinar os cenários do Autopilot (Cont).

Redefinição Remota do Windows Autopilot

Para iniciar uma redefinição remota do Windows Autopilot, você pode aproveitar um serviço de MDM, como Microsoft Intune. Esse método elimina a necessidade de a equipe de TI visitar fisicamente cada computador individual para iniciar o procedimento de redefinição. Seguindo estas etapas, você pode usar o Intune para iniciar o processo de redefinição remota do Windows Autopilot:

No centro de administração do Microsoft Intune, navegue até Dispositivos>Windows.

Selecione o dispositivo para o qual deseja iniciar uma Redefinição remota do Windows Autopilot.

Escolha Mais (as reticências) e selecione Redefinição do Autopilot para iniciar a redefinição.

Solucionar problemas do Windows Autopilot

Ao solucionar problemas do Windows Autopilot, é importante verificar os seguintes fatores-chave:

- **Configuração:** o Azure AD e o Microsoft Intune (ou um serviço de MDM equivalente) foi configurado conforme especificado nos requisitos de configuração do Windows Autopilot?
- **Conectividade de rede:** o dispositivo pode acessar os serviços descritos nos requisitos de rede do Windows Autopilot?
- **Comportamento da OOBÉ do Autopilot:** foram exibidas apenas as telas esperadas da configuração inicial pelo usuário? A página de credenciais do Azure AD foi personalizada com detalhes específicos da organização conforme o esperado?
- **Problemas de ingresso no Azure AD:** o dispositivo conseguiu ingressar no Azure AD?
- **Problemas de registro no MDM:** o dispositivo conseguiu se registrar no Microsoft Intune (ou em um serviço de MDM equivalente)?




Solucionar problemas do Windows Autopilot (Cont).

Diagnóstico do Windows Autopilot

O Windows Autopilot já pode agregar muitas das técnicas de solução de problemas listadas em um formato mais facilmente legível para isolar os problemas ocorridos. Essa função pode ser executada em um comando do PowerShell diretamente no dispositivo.

Abra o comando do PowerShell e insira o seguinte (Aceitar prompts de download)

PowerShell

 Copiar

```
Set-ExecutionPolicy Bypass  
Install-Script Get-AutoPilotDiagnostics -force  
Get-AutoPilotDiagnostics -Online
```

Solucionar problemas do Windows Autopilot (Cont).

Soluções de problemas de ingresso no Entra ID

O problema mais comum ao ingressar um dispositivo no Azure AD está relacionado às permissões do Azure AD. Verifique se a configuração correta está em vigor para permitir que os usuários ingressem dispositivos no Azure AD. Também poderão ocorrer erros se o usuário exceder o número de dispositivos que tem permissão para ingressar, conforme configurado no Azure AD.

Normalmente exibido em uma página de erro "Algo deu errado", o código de erro 801C0003 significa que a tentativa de ingressar no Azure AD não foi bem-sucedida.

Solucionar problemas do Windows Autopilot (Cont).

Soluções de problemas de registro do Intune

Entre os problemas comuns estão licenças incorretas ou ausentes atribuídas ao usuário ou excesso de dispositivos registrados para o usuário.

Ao encontrar o código de erro 80180018, ele é acompanhado por uma página de erro intitulada "Algo deu errado". Esse erro específico indica um processo de registro de MDM com falha.

Solucionar problemas do Windows Autopilot (Cont).

Soluções de problemas de importação de dispositivos

Se você enfrentar um cenário em que a importação de um arquivo CSV do dispositivo não resulta em nenhuma ação e um erro "400" aparecer no rastreamento de rede com o texto "Não é possível converter o literal "[DEVICEHASH]" para o tipo esperado "Edm.Binary", o hash do dispositivo dentro do arquivo está corrompido ou o hash pode não ser adicionado corretamente no arquivo. Para resolver esse problema, uma edição secundária no arquivo pode ser necessária para garantir que o hash do dispositivo esteja no formato correto.



TFTEC CLOUD



Obrigado

Implementar métodos de implantação dinâmica

Introdução

Mesmo com a capacidade de redefinir a imagem existente do Windows com o Autopilot, às vezes, até isso não é necessário, especialmente com novos dispositivos comprados de um OEM. Um novo dispositivo normalmente começa com uma nova instalação do Windows, e o que normalmente é necessário é a edição correta implantada (como o Windows Enterprise ou Education), a configuração e os aplicativos corretos. Quando esse é o caso, o provisionamento dinâmico pode simplificar ainda mais as implantações.

O provisionamento dinâmico usa várias transformações para atingir esse objetivo.

Nome	Descrição
Ativação da Assinatura do Windows	Com a Ativação da Assinatura do Windows, os usuários do Windows Pro podem atualizar para o Windows Enterprise sem precisar inserir uma chave do produto (Product Key) nem executar uma reinicialização.
Configuração de pacote de provisionamento	Usando o Designer de Configuração do Windows, você pode criar pacotes de configuração que podem ser implantados nos dispositivos dos usuários que podem ser usados para definir aplicativos e configurações nesses dispositivos.
Ingresso no Microsoft Entra com o registro automático de MDM	Ao usar o ingresso no Microsoft Entra com o registro automático de MDM, os usuários inserem os detalhes da conta corporativa ou de estudante, e o dispositivo é ingressado automaticamente no Microsoft Entra ID e registrado no MDM. Em seguida, o dispositivo do usuário é configurado de acordo com as políticas de MDM da organização.

Examinar a ativação da assinatura

A ativação de uma assinatura do Windows é necessária para atender aos requisitos de licenciamento. A ativação vincula a chave do produto (Product Key) do Windows a uma instalação específica do Windows em um dispositivo. Ela garante a integridade do software e fornece acesso ao suporte da Microsoft e a uma gama completa de atualizações. Há três métodos principais de ativação:

- Retail
- OEM
- Licenciamento por Volume da Microsoft (ativação por volume)

Os clientes do Licenciamento por Volume da Microsoft usam os Serviços de Ativação de Volume para ajudar com tarefas de ativação, que consistem na ativação baseada no Active Directory, no KMS (Serviço de Gerenciamento de Chaves) e nos modelos de MAK (chave de ativação múltipla).

Examinar a ativação da assinatura (Cont).

- Necessário para cumprir os requisitos de licenciamento
- Métodos atuais de ativação de volume
 - Serviço de gerenciamento de chaves (KMS).
 - Chave de ativação múltipla (MAK).
 - Ativação baseada no Active Directory.
- O Windows Pro pode ser atualizado para Enterprise sem reinstalar ou reiniciar
- Requisitos de ativação de assinatura
 - Windows Pro/Pro Education/Enterprise/Education instalado e ativado.
 - A instância do Azure AD (Entra ID) está disponível para gerenciamento de identidade.
 - Dispositivos ingressados no Azure AD ou híbridos no Azure AD.
- Ativação de assinatura VDA

Implantação por meio de pacotes de provisionamento

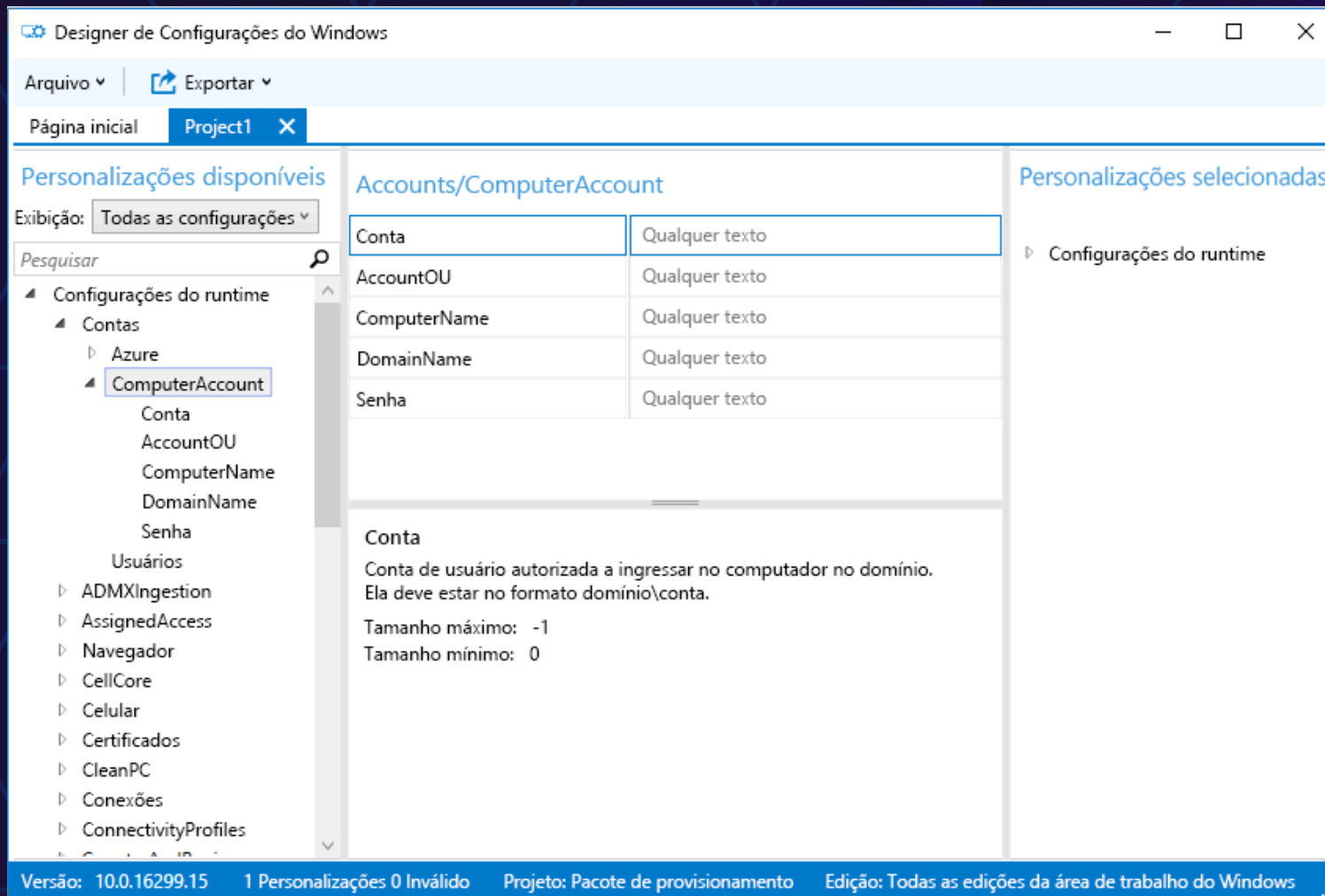
Um pacote de provisionamento é um método de aplicação de configurações a um dispositivo Windows 10 ou posterior usando mídia removível ou baixado diretamente no dispositivo. Eles são criados usando uma ferramenta gráfica chamada WCD (Designer de Configuração do Windows). Semelhante ao conceito de políticas de grupo, os administradores usam o WCD para selecionar opções para uma configuração específica. Em seguida, o WCD exporta um arquivo de pacote que contém as configurações que podem ser aplicadas a um dispositivo Windows 10 ou Windows 11.

Você pode usar um pacote de provisionamento para modificar uma instalação do Windows e definir muitas configurações de runtime sem precisar reinstalar o sistema operacional Windows. Por exemplo, você pode usar um pacote de provisionamento para:]

- Configurar a interface do usuário do Windows.
- Adicionar arquivos ou aplicativos adicionais.
- Ajustar configurações de conectividade.
- Atender aos requisitos de rede móvel.
- Gerenciar certificados.
- Cumprir as políticas de segurança.
- Remover software instalado.
- Redefinir a instalação do Windows para seu estado inicial.

Usar o Designer de Configurações do Windows

O Windows ADK (Kit de Avaliação e Implantação do Windows) inclui uma ferramenta chamada Designer de Configuração do Windows, que você pode usar para criar pacotes de provisionamento.



Ingresso no Microsoft Entra com o registro automático de MDM

O método de provisionamento dinâmico do Azure AD/MDM também é orientado por nuvem e também se baseia no Microsoft Entra ID P1 ou P2 e no Microsoft Intune. Após você registrar um dispositivo no MDM Intune, o MDM impõe a conformidade com suas políticas corporativas, adiciona ou remove aplicativos e muito mais. Além disso, o MDM pode relatar a conformidade de um dispositivo com o Microsoft Entra ID. Isso permite que o Microsoft Entra ID permita o acesso a recursos corporativos ou aplicativos protegidos somente pelo Microsoft Entra para dispositivos que estejam em conformidade com as políticas.

Usando Azure AD/MDM, você pode:

- Ingressar dispositivos no Microsoft Entra ID automaticamente
- Registrar automaticamente os dispositivos dos usuários em serviços de MDM
- Configurar os dispositivos ingressados usando políticas de MDM

Os requisitos para implementar o modelo de implantação Azure AD/MDM são:

- Windows 10/11 edição Pro ou Enterprise
- Uma instância do Microsoft Entra ID para gerenciamento de identidade
- Um MDM apropriado, como Microsoft Intune

Use a associação do Azure AD (Entra ID) com registro automático de MDM

- Conceito semelhante ao ingresso em um domínio AD DS local
- Simplifica cenários de provisionamento e suporte em vez de usar métodos locais
- Aplica-se a cenários BYOD/CYOD

Usando o Azure AD(Entra ID)/MDM, você pode:

- Ingressar dispositivos no Azure AD (Entra ID) automaticamente
- Registre automaticamente os dispositivos dos seus usuários em serviços MDM
- Configure os dispositivos associados usando políticas de MDM



Obrigado

Planeje uma transição
para o gerenciamento
moderno de endpoints

Introdução

À medida que as organizações continuam adotando a transformação digital, a necessidade de soluções de gerenciamento de dispositivos eficientes e seguras tornou-se cada vez mais importante. Com o advento do Windows Autopilot e o do cogerenciamento por meio do Configuration Manager e do Microsoft Intune, as organizações agora podem simplificar o provisionamento e o gerenciamento de dispositivos na era moderna. Este módulo introdutório orientará você pelos principais conceitos e considerações para fazer a transição para o gerenciamento de dispositivo moderno usando o Windows Autopilot e o cogerenciamento.

Neste módulo, você aprenderá sobre o Windows Autopilot, o cogerenciamento e os benefícios de combinar essas tecnologias. Você aprenderá sobre diferentes cenários de uso para ingresso no Microsoft Entra, cargas de trabalho que podem ser transferidas para o Intune e os pré-requisitos para cogerenciamento. Além disso, discutiremos as considerações e o planejamento de uma transição bem-sucedida para o gerenciamento moderno usando tecnologias existentes e novas.

Explore o uso do cogerenciamento para fazer a transição para o gerenciamento moderno



On-premises Active Directory or Microsoft Configuration Manager and Active Directory



Intune and Azure AD (Entra ID)

- A cogestão simplifica a transição para a gestão moderna.
- Dispositivos gerenciados usando o Active Directory local e o Azure Active Directory (Entra ID) e o Intune.
- Maximiza a produtividade por meio de logon único (SSO) em recursos locais e na nuvem.
- O Intune permite gerenciar políticas em dispositivos conectados à Internet sem usar a Política de Grupo que requer dispositivos ingressados no domínio local.

Examinar os pré-requisitos para cogerenciamento

Para habilitar o cogerenciamento para dispositivos locais do Active Directory:

- Os dispositivos devem ser associados ao Azure AD híbrido (Entra ID)
- Conexão mais recente do Azure AD (Entra ID) instalada e configurada para sincronizar contas de computador com o Azure AD
- O Intune MDM deve ser instalado e configurado para registro automático
- Os dispositivos ingressados no Active Directory usam o Windows 10 versão 1709 ou posterior
- Registro automático do Azure AD (Entra ID) habilitado

Cargas de trabalho de transição para o Microsoft Intune:

- Políticas de acesso a recursos
- Políticas do Windows Update
- Proteção de endpoint
- Configuração do dispositivo

Avalie as considerações sobre o gerenciamento moderno

- Remove o processo de imagem sempre que possível
- Transforma o sistema operacional existente com pouca ou nenhuma interação do usuário e sem implantar uma nova imagem
- Implantação mais rápida, eficiente e com menor utilização da rede
- Requer Windows 11 ou posterior no dispositivo de destino
 - A atualização local é recomendada para dispositivos que ainda executam o Windows 7 ou 8.1
- A implantação moderna pode alterar um sistema operacional Windows 11 instalado de várias maneiras
 - Removendo software pré-instalado
 - Atualizando uma edição do Windows 11
 - Ingressar um dispositivo Windows 11 no AD DS ou Azure AD

Avalie as considerações sobre o gerenciamento moderno (Cont).

	MDT	Microsoft Configuration Manager	Windows Autopilot
Exigir a criação de golden images	Sim	Sim	Não
Capacidade de reconstruir ou redefinir o dispositivo	Sim	Sim	Sim
Capacidade de realizar uma build bare-metal	Sim	Sim	Não
Pode ser usado com qualquer sistema operacional pré-instalado	Não	Não	Somente Windows 11
Instalação de aplicativos quando o dispositivo está sendo construído	Sim	Sim	Sim
Implantação de aplicativos pós build	Não	Sim	Sim
Migração de dados do usuário (USMT)	Sim	Sim	Sim – OneDrive/Enterprise State Roaming (ESR)
Execute uma atualização no local	Sim	Sim	Sim (em combinação com o Microsoft Configuration Manager)

Avalie as considerações sobre o gerenciamento moderno (Cont).

- Cenários a considerar usando imagens com gerenciamento moderno:
 - Um dispositivo apresenta uma Tela Azul da Morte (BSOD) e não consegue inicializar o Windows, resultando na necessidade de uma construção bare-metal
 - Quando você entrega uma série de aplicativos complexos e dependências em um dispositivo, que é então cogerenciado
 - Há uma falha de hardware de um dispositivo que requer conectividade de rede para instalar aplicativos ou ingressar em um domínio corporativo do Active Directory
- Situações como substituições de unidades de armazenamento de clientes, implantações bare-metal e dispositivos que não suportam um caminho de atualização para o sistema operacional desejado.

Avalie as atualizações e migrações na transição moderna

- Cenários para migração de dados e configuração do usuário:
 - Substituição de dispositivo
 - O dispositivo está sendo atualizado de um sistema operacional mais antigo para o Windows 11 e uma atualização local não é possível (como um caminho de atualização não compatível)
 - É necessária uma instalação limpa
- Dois cenários de migração
 - Lado a lado: os computadores de origem e de destino são diferentes
 - Limpar e carregar (migração de atualização): os computadores de origem e de destino são iguais
- A migração move arquivos e configurações para uma instalação limpa do sistema operacional Windows

Avalie as atualizações e migrações na transição moderna (cont).

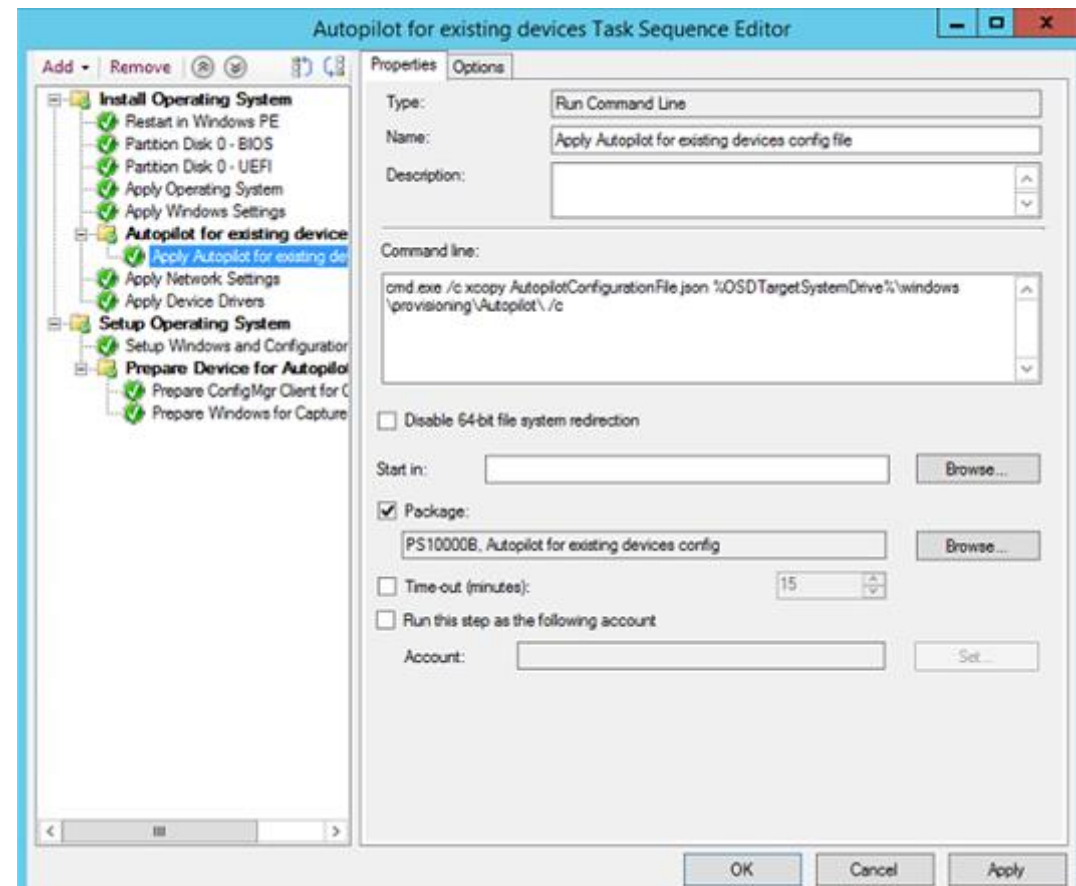
Atualização no local	Migração
Preserve o ambiente	Fornece um ambiente padronizado
Não precisa reinstalar aplicativos ou transferir dados	Você pode controlar o que migra
A atualização pode ser revertida se necessário	Limpa o ambiente
Apenas alguns caminhos de atualização são possíveis	Você deve reinstalar os aplicativos
Você deve usar a imagem padrão do Windows	Você pode usar uma imagem personalizada do Windows

Avalie as atualizações e migrações na transição moderna (cont).

Atualizações no local

Adapte a implantação moderna de desktops com o Windows Autopilot para um dispositivo legado existente

Transforme um ponto de extremidade tradicional associado a um domínio em um dispositivo gerenciado pelo Azure AD e execute uma reconstrução, tudo dentro da mesma peça de automação



Migrar dados durante a transição moderna

Migrar dados durante a transição modernaAo migrar um usuário para um novo dispositivo ou realizar uma migração local, considere quais configurações de usuário e aplicativo devem ser mantidas e qual método usar para garantir que essas informações sejam retidas

Sincronizando o estado do usuário

- Quando o Enterprise State Roaming (ESR) está ativado, o usuário só precisa fazer login no novo dispositivo, e o dispositivo manterá todas as configurações suportadas pelo ESR
- Migre todas as configurações e dados que os usuários precisam (sem dados desnecessários ou obsoletos), mas considere o esforço necessário para migrar determinados tipos de dados
- Não ignore configurações simples que têm impacto significativo

Migrando o estado do usuário

- Use a ferramenta de migração de estado do usuário (USMT) para migrar arquivos ou configurações durante atualizações e migrações
- Fase 1: capturar configurações e dados do computador de origem e armazená-los em um armazenamento de migração
- Fase 2: Restaurar configurações e dados capturados no computador de destino (após instalar o sistema operacional)

Migrar dados durante a transição moderna (cont).

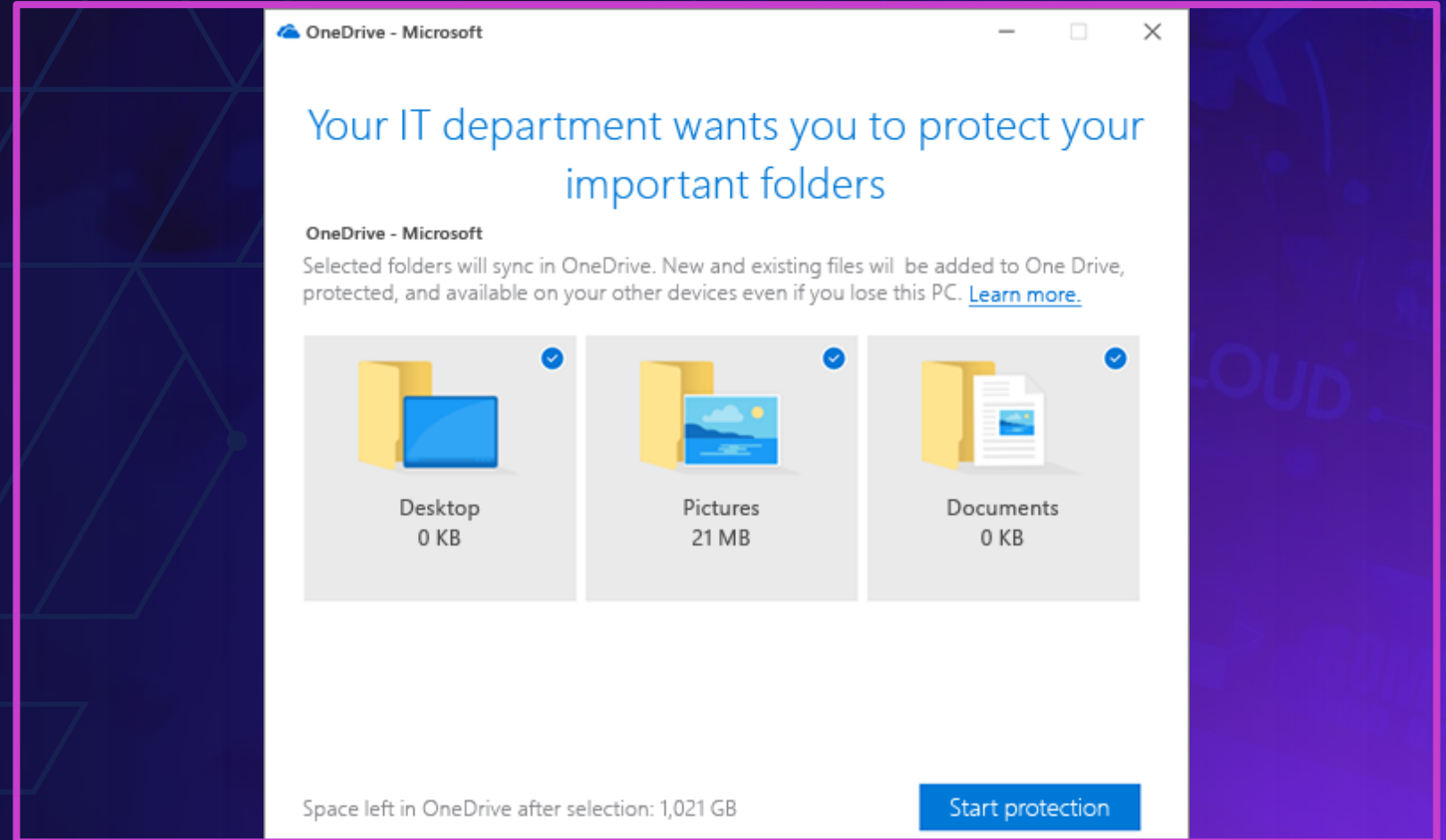
Migração de estado do usuário no cenário de substituição e atualização de computador

- No cenário de substituição, os computadores de origem e de destino são diferentes
 - Ao implantar o Windows em novos computadores, você pode capturar o estado do usuário dos computadores de origem antes ou depois de implantar o Windows nos computadores de destino
 - Depois que o Windows for implantado nos computadores de destino, você poderá restaurar os estados do usuário nesses computadores
- No cenário de atualização, os computadores de origem e de destino são os mesmos
 - Ao atualizar para o sistema operacional Windows 10 ou posterior em computadores que possuem sistemas operacionais existentes, você pode capturar o estado do usuário, armazená-lo em armazenamento temporário, executar uma instalação limpa do Windows e, em seguida, restaurar o estado do usuário nos computadores atualizados
- Pasta Windows.old

Migrar dados durante a transição moderna (cont).

Movimentação de pasta conhecido

- Migre automaticamente os arquivos do usuário para o OneDrive
- Operação imediata ou silenciosa
- Esteja atento à largura de banda ao implementar
- Não é possível usar a movimentação de pasta conhecida (KFM) se estiver usando o redirecionamento de pasta ou tipos de arquivo não suportados



Migrar dados durante a transição moderna (cont).

Usando o USMT com o Microsoft Configuration Manager

Crie um pacote USMT no Microsoft Configuration Manager

Crie um pacote USMT personalizado ou use o pacote padrão

Configurar um ponto de migração de estado (função do sistema de site do Microsoft Configuration Manager)

Atua como um compartilhamento de arquivos para armazenar dados

Armazena um hash exclusivo:

- Dispositivo que permite a captura de dados
- Dispositivo atualizado
- Dados relevantes a serem restaurados

Sequência de Tarefas

Pode incluir USMT

Ocorre na sequência de tarefas quando:

- Capturando configurações
- Restabelecendo as configurações de um usuário dependendo das opções selecionadas

Use modelos USMT para migração

modelos xml que controlam os dados coletados no perfil de um usuário:

- MigApp.xml
- MigDocs.xml
- MigUser.xml
- ConfigMgr.xml

Migrar cargas de trabalho durante a transição moderna

- Migrar o gerenciamento de clientes para o Intune
 - Considere o gerenciamento baseado em nuvem de dispositivos clientes quando versões de sistemas operacionais legados forem removidas
 - Reduzir o uso do Microsoft Configuration Manager pode reduzir ou eliminar uma camada de complexidade
 - Revise outras considerações para migrar para um gerenciamento 100% baseado em nuvem
- Escolhendo cargas de trabalho no Intune
 - Organizações maiores podem querer continuar usando o Microsoft Configuration Manager e aproveitar o cogerenciamento no Intune
 - Mantém o investimento de tempo no Microsoft Configuration Manager
 - Valor na migração de algumas cargas de trabalho (implantação de SO, alguns aplicativos)



Obrigado

Gerenciar o Windows 365

Introdução

Este módulo ensinará você a gerenciar o Windows 365, a solução de gerenciamento de computadores baseada em nuvem da Microsoft. O Windows 365 permite que você forneça aos usuários uma experiência personalizada e segura do Windows 11 de qualquer lugar, em qualquer dispositivo. Neste módulo, você aprenderá sobre os principais recursos do Windows 365, como configurar e gerenciar o serviço e como configurar e proteger computadores do Windows 365 para seus usuários. Seja você novato ou experiente no Windows 365, este módulo fornecerá conhecimentos e habilidades para gerenciar e otimizar efetivamente seu ambiente do Windows 365. Então vamos começar.

Explorar o Windows 365

O Windows 365 é um serviço baseado em nuvem de ponta que simplifica a forma como você cria e gerencia máquinas virtuais. Ele gera automaticamente para seus usuários finais um novo tipo de máquina virtual do Windows chamado de PC na nuvem. Com o Windows 365, cada PC na nuvem é atribuído a um usuário individual, fornecendo a cada um deles um dispositivo Windows dedicado. Usando o Windows 365, você pode experimentar os benefícios do Microsoft 365, que incluem maior produtividade, segurança aprimorada e colaboração ininterrupta. Com esses recursos, o Windows 365 oferece uma solução flexível e escalonável para dar suporte às necessidades de crescimento e mudança da sua organização.

Explorar o Windows 365 (cont)

O Windows 365 está disponível em duas edições:

Windows 365 Business

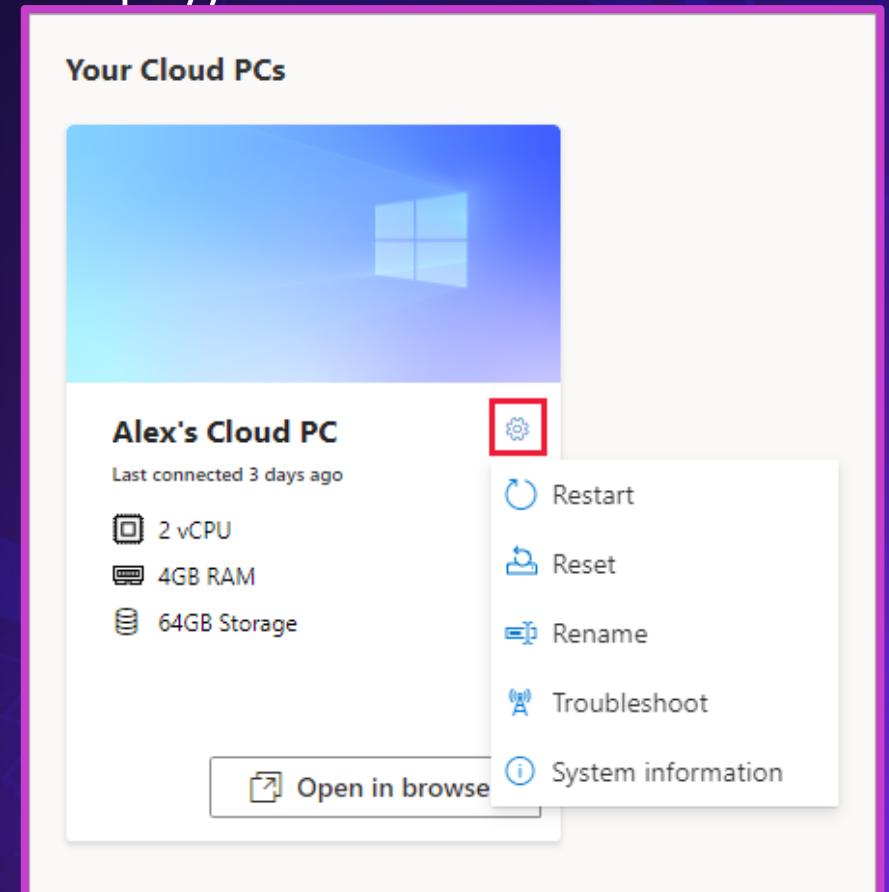
- Para empresas menores (até 300 licenças) que desejam PCs em nuvem prontos para uso com opções de gerenciamento simples.
- Sem pré-requisitos de licenciamento.
- Sem dependências do Azure ou do Active Directory.

Windows 365 Enterprise

- Para empresas maiores que desejam assentos ilimitados para a criação de Cloud PCs.
- Inclui opções para criar Cloud PCs personalizados com base em imagens de dispositivos personalizadas.
- Mais opções de gerenciamento e integração total com o Microsoft Intune.

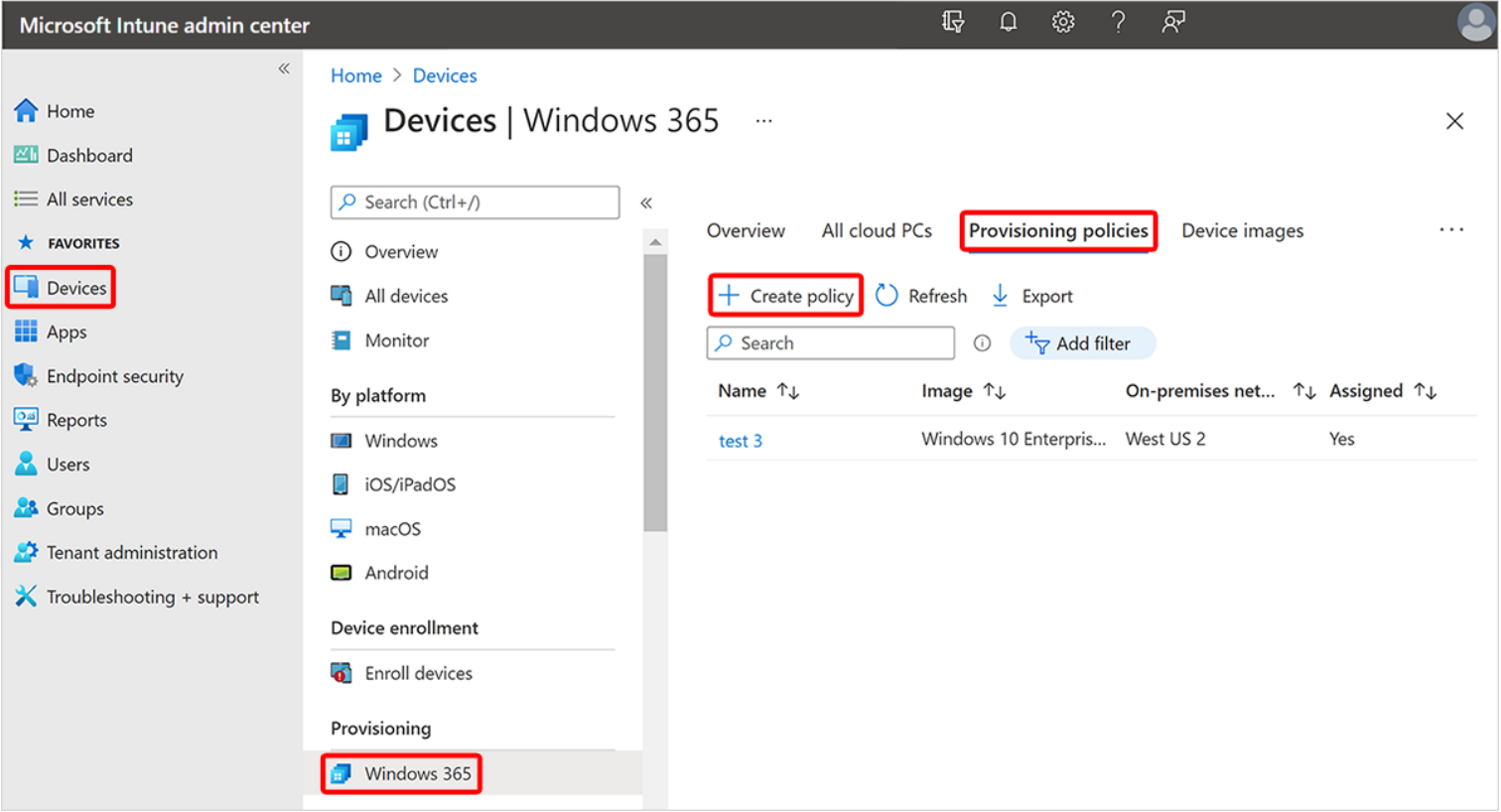
Acesse PCs na nuvem

<https://windows365.microsoft.com>



Configurar o Windows 365

- Atribuir licenças aos usuários
- Crie uma conexão de rede do Azure
- Configurar imagem personalizada (opcional)
- Crie políticas de provisionamento
- Configurar e aplicar perfis de dispositivos/aplicativos



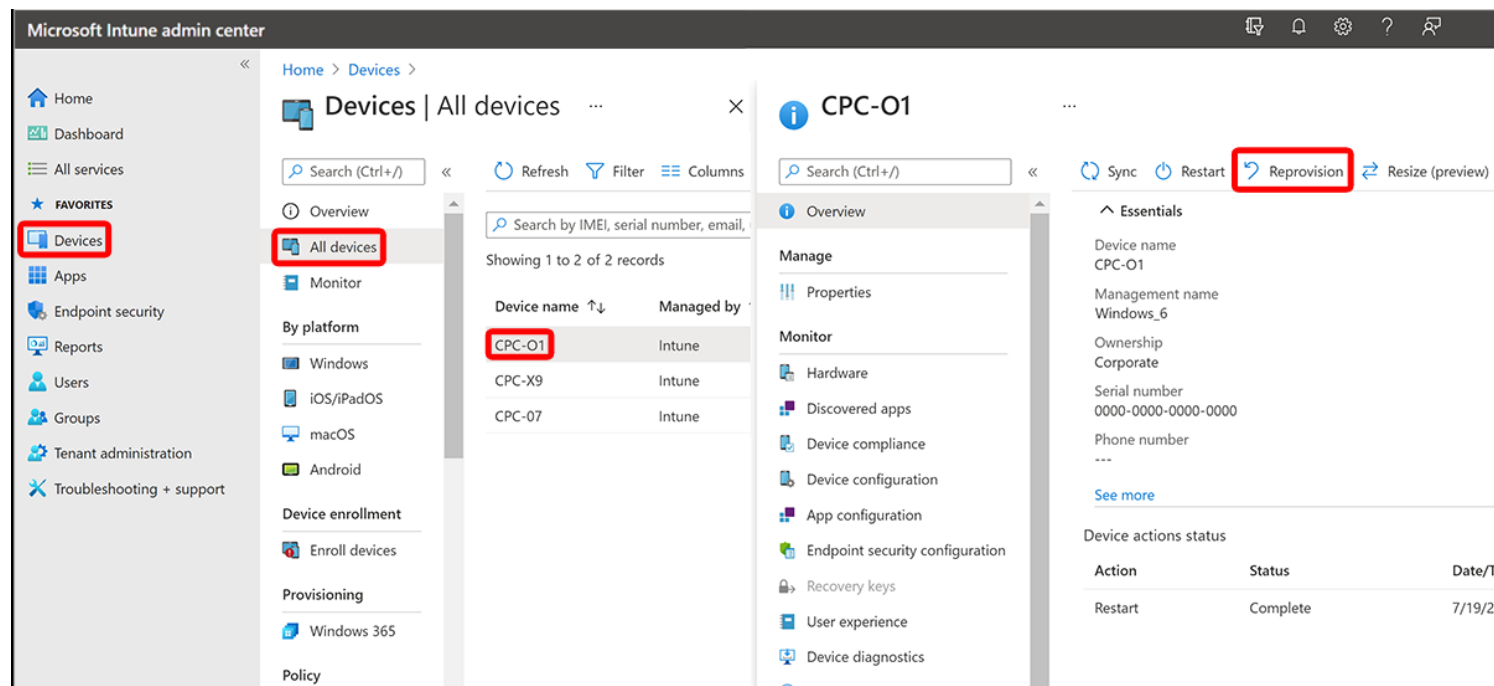
The screenshot displays the Microsoft Intune admin center interface. The left sidebar shows the navigation menu with 'Devices' highlighted. The main content area is titled 'Devices | Windows 365' and shows the 'Provisioning policies' tab. A table lists the policies, with one policy named 'test 3' visible. The 'test 3' policy is associated with the 'Windows 10 Enterpris...' image and the 'West US 2' region. The 'Assigned' column shows 'Yes'.

Name ↑↓	Image ↑↓	On-premises net... ↑↓	Assigned ↑↓
test 3	Windows 10 Enterpris...	West US 2	Yes

Administrar o Windows 365

O gerenciamento do Cloud PC é igual ao gerenciamento de dispositivos físicos

- A maioria das ações remotas são iguais às dos dispositivos físicos:
 - Restart
 - Sync
 - Rename
 - Quick Scan
 - Full Scan
 - Update Windows Defender
- Ações exclusivas do Cloud PC:
 - Reprovisioning
 - Resizing
 - Collect diagnostics





Obrigado

Gerenciar a Área de Trabalho Virtual do Azure

Introdução

Este módulo ensinará você a gerenciar a Área de Trabalho Virtual do Azure, a solução de VDI (infraestrutura de área de trabalho virtual) baseada em nuvem da Microsoft. A Área de Trabalho Virtual do Azure permite que você forneça aos usuários uma experiência personalizada e segura do Windows 10 em qualquer lugar, em qualquer dispositivo. Neste módulo, você aprenderá sobre os principais recursos da Área de Trabalho Virtual do Azure, como configurar e gerenciar o serviço e como configurar e proteger computadores da Área de Trabalho Virtual do Azure para seus usuários. Seja você novato na Área de Trabalho Virtual do Azure ou experiente com o serviço, este módulo fornecerá conhecimentos e habilidades para gerenciar e otimizar efetivamente seu ambiente da Área de Trabalho Virtual do Azure.

Examinar a Área de Trabalho Virtual do Azure

- Serviço de virtualização de desktops e aplicativos baseado em nuvem no Azure
- Conecte-se por meio de dispositivos Windows, Mac, iOS, Android e Linux com acesso à Internet usando um aplicativo nativo ou o cliente Web da Área de Trabalho Virtual do Azure
- Benefícios da Área de Trabalho Virtual do Azure
 - Gerenciamento centralizado de segurança para desktops de usuários com Azure AD (Entra)
 - Gestão Simplificada
 - Gestão de Desempenho
 - Implantação do Windows 10 em várias sessões
 - Opções de licenciamento
 - Economia de custos computacionais

Explore a Área de Trabalho Virtual do Azure

- Com o Azure Virtual Desktop em execução no Azure, você pode:
 - Estabeleça uma experiência Windows 10 ou 11 multisessão do Windows.
 - Implante aplicativos do Microsoft 365 e otimize-os para cenários virtuais multiusuários.
 - Migre desktops e aplicativos RDS e Windows Server existentes para qualquer dispositivo.
 - Virtualize ambientes de desktop e aplicativos individuais.
 - Administre desktops e aplicativos por meio de uma plataforma de gerenciamento unificada.
- Principais capacidades:
 - Ambiente abrangente de virtualização de desktop na sua assinatura do Azure.
 - Publique pools de hosts conforme necessário para dar suporte a diversas cargas de trabalho.
 - Use sua própria imagem para cargas de trabalho de produção ou teste na Galeria do Azure.
 - Economize custos com recursos agrupados e multissessões.
 - Ofereça propriedade individual com desktops pessoais (persistentes).
 - Dimensionamento automático para ajustar automaticamente a capacidade com base no dia/hora ou na demanda flutuante.
- Implantar/gerenciar e atribuir/conectar usuários a desktops virtuais

Configurar a Área de Trabalho Virtual do Azure

- Crie e conecte-se a uma área de trabalho do Windows 11 com a Área de Trabalho Virtual do Azure:
 - Crie um pool de hosts pessoal.
 - Crie uma máquina virtual (VM) de host de sessão associada ao seu locatário do Azure Active Directory (Entra ID) com o Windows 11 Enterprise e adicione-a ao pool de hosts.
 - Crie um espaço de trabalho e um grupo de aplicativos que publique uma área de trabalho na VM do host da sessão.
 - Atribua usuários ao grupo de aplicativos.
 - Conecte-se à área de trabalho.
- Pré-requisitos:
 - Uma conta do Azure com uma assinatura ativa.
 - A conta deve receber as funções RBAC integradas de Proprietário ou Colaborador.
 - Uma rede virtual na mesma região do Azure na qual você deseja implantar seus hosts de sessão.
 - Uma conta de usuário no Azure Active Directory que você pode usar para se conectar à área de trabalho.
 - Um cliente de Área de Trabalho Remota instalado em seu dispositivo para conectar-se à área de trabalho.

Administrar a Área de Trabalho Virtual do Azure

- Utilize a CLI do Azure e o Azure PowerShell
 - Utilize a extensão CLI do Azure e um módulo Azure PowerShell para o Azure Virtual Desktop para criar, atualizar, eliminar e interagir com objetos de serviço do Azure Virtual Desktop em vez de utilizar o portal do Azure.
- Extensão CLI do Azure e módulo Azure PowerShell:
 - Azure CLI: az desktopvirtualization
 - Azure PowerShell: Az.DesktopVirtualization
- A extensão CLI do Azure não possui comandos para aplicativos
 - Utilize o módulo Azure PowerShell.



Obrigado

Laboratórios



TFTEC CLOUD

Lab 01

TASK01:

- Implantando o Windows 11 com Autopilot
- Criar e configurar o Windows 365
- Criar e configurar a Área de Trabalho Virtual do Azure