

Estudo de caso -

Visão geral -

ADatum Corporation é uma empresa de consultoria com sede em Montreal e filiais em Seattle e Nova York.

ADatum tem uma assinatura do Microsoft 365 E5.

Ambiente -

Ambiente de rede -

A rede contém um domínio local do Active Directory chamado adatum.com. O domínio contém os servidores mostrados na tabela a seguir.

| Name    | Operating system    | Role              |
|---------|---------------------|-------------------|
| DC1     | Windows Server 2019 | Domain controller |
| Server1 | Windows Server 2016 | Member server     |
| Server2 | Windows Server 2019 | Member server     |

ADatum tem um locatário híbrido do Azure AD chamado adatum.com.

Usuários e grupos -

O locatário adatum.com contém os usuários mostrados na tabela a seguir.

| Name  | Azure AD role                              | Member of      |
|-------|--|----------------|
| User1 | Cloud Device Administrator                 | GroupA         |
| User2 | Azure AD Joined Device Local Administrator | GroupB         |
| User3 | Global Reader                              | GroupA, GroupB |
| User4 | Global Administrator                       | Group1         |

Todos os usuários recebem uma licença do Microsoft Office 365 e uma licença Enterprise Mobility + Security E3.

O Enterprise State Roaming está habilitado para Grupo1 e GrupoA.

O Grupo1 e o Grupo2 têm um tipo de associação Atribuído.

Dispositivos -

ADatum possui os dispositivos Windows 10 mostrados na tabela a seguir.

| Name    | Type             | Member of      | Scope (Tags) |
|---------|------------------|----------------|--------------|
| Device1 | Corporate-owned  | Group1         | Default      |
| Device2 | Corporate-owned  | Group1, Group2 | Tag2         |
| Device3 | Personally-owned | Group1         | Tag1         |
| Device4 | Personally-owned | Group2         | Tag2         |
| Device5 | Corporate-owned  | Group3         | Default      |

Os dispositivos Windows 10 estão associados ao Azure AD e inscritos no Microsoft Intune.

Os dispositivos Windows 10 são configurados conforme mostrado na tabela a seguir.

| Name    | BitLocker Drive Encryption (BitLocker) | Secure Boot | VPN connection |
|---------|--|-------------|----------------|
| Device1 | Yes                                    | No          | VPN1           |
| Device2 | Yes                                    | Yes         | VPN1, VPN3     |
| Device3 | No                                     | No          | VPN3           |
| Device4 | No                                     | Yes         | None           |
| Device5 | Yes                                    | No          | None           |

Todos os dispositivos ingressados no Azure AD têm um arquivo executável chamado C:\AppA.exe e uma pasta chamada D:\Folder1.

Configuração do Microsoft Intune -

O Microsoft Intune tem as políticas de conformidade mostradas na tabela a seguir.

| Name    | Configuration                     | Assignment |
|---------|-----------------------------------|------------|
| Policy1 | Require BitLocker only            | Group1     |
| Policy2 | Require Secure Boot only          | Group1     |
| Policy3 | Require BitLocker and Secure Boot | Group2     |

**The Compliance policy settings are shown in the following exhibit.**

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ

Compliant

Not Compliant

Enhanced jailbreak detection ⓘ

Enabled

Disabled

Compliance status validity period (days) ⓘ

30

✓

As configurações de Inscrição Automática possuem as seguintes configurações:

- Escopo do usuário MDM: GrupoA
- Escopo do usuário MAM: GrupoB

Você tem um perfil de configuração do Endpoint Protection que possui as seguintes configurações de acesso controlado a pastas:

• Nome: Proteção1 •

Proteção de pasta: Ativar • Lista de aplicativos que têm acesso a pastas protegidas: C:\\*AppA.exe • Lista de pastas adicionais que precisam ser protegidas: D\Folder1 • Atribuições: - Grupos incluídos: Grupo2, GrupoB

Configuração do piloto automático do Windows -

ADatum tem um perfil de implantação do Windows Autopilot configurado conforme mostrado na exposição a seguir.

# Create profile

Windows PC

- ✓ Basics
- ✓ Out-of-box experience (OOBE)
- ✓ Assignments
- 4

Review + create

## Summary

### Basics

|   |            |
|---|------------|
| Name                                      | Profile1   |
| Description                               | --         |
| Convert all targeted devices to Autopilot | Yes        |
| Device type                               | Windows PC |

### Out-of-box experience (OOBE)

|                                      |                          |
|--------------------------------------|--------------------------|
| Deployment mode                      | User-Driven              |
| Join to Azure AD as                  | Azure AD joined          |
| Skip AD connectivity check (preview) | No                       |
| Language (Region)                    | Operating system default |
| Automatically configure keyboard     | Yes                      |
| Microsoft Software License Terms     | Hide                     |
| Privacy settings                     | Hide                     |
| Hide change account options          | Hide                     |
| User account type                    | Standard                 |
| Allow White Glove OOBE               | No                       |
| Apply device name template           | No                       |

### Assignments

|                 |        |
|-----------------|--------|
| Included groups | Group1 |
| Excluded groups | Group2 |

Atualmente, não há dispositivos implantados usando o Windows Autopilot.

O conector do Intune para Active Directory está instalado no Servidor1.

Requisitos -

Mudanças planejadas -

ADatum planeja implementar as seguintes mudanças:

- Adquirir um novo dispositivo Windows 10 chamado Device6 e inscreva-o no Intune.
- Novos computadores serão implantados usando o Windows Autopilot e serão ingressados no Azure AD híbrido.
- Implantação de um perfil de configuração de limite de rede que terá as seguintes configurações: - Nome: Boundary1 - Limite de rede: 192.168.1.0/24 - Tags de escopo: Tag1 - Atribuições: - Grupos incluídos: Grupo1, Grupo2
- Implantar dois perfis de configuração VPN chamados Connection1 e Conexão2 que terá as seguintes configurações: - Nome: Conexão1 - Nome da conexão: VPN1 - Tipo de conexão: L2TP - Atribuições: - Grupos incluídos: Grupo1, Grupo2, GrupoA - Grupos excluídos: -- - Nome: Conexão2 - Nome da conexão: VPN2 - Tipo de conexão: IKEv2 - Atribuições: - Grupos incluídos: GrupoA - Grupos excluídos: GrupoB

Requerimentos técnicos -

O ADatum deve atender aos seguintes requisitos técnicos: • Os usuários do Grupo A devem ser capazes de implantar novos computadores. • O esforço administrativo deve ser minimizado.

Você precisa garantir que os objetos do computador possam ser criados como parte da implantação do Windows Autopilot. A solução deve atender aos requisitos técnicos.

A quem você deve conceder o direito de criar os objetos de computador?

- A. Servidor1
- B. DC1
- C. GrupoA
- D. Servidor2