ESCOLA SUPERIOR DE TECNOLOGIA DA INFORMAÇÃO

Teste de Performance 7

TP6 (Capítulo 1) + TP7 (Capítulo 2)

Disciplina: Projeto de Bloco - Arquitetura e Infraestrutura de Aplicações

Aluno: Marcelo Carvalho

Professor: Fabio Campos Chaves

Data: 17/03/2020

Capítulo 1:

Faça upload de uma versão inicial do capítulo de Introdução de seu Projeto de Bloco. Você deve contemplar:

a. O tipo de negócio/processo/problema que pretende tratar a partir de uma aplicação distribuída rodando sobre uma infraestrutura com virtualização.
b. Uma justificativa de porque este problema é relevante.
c. Uma descrição da aplicação distribuída que você pretende implementar com detalhes de sua arquitetura, como o gerenciamento do código-fonte, do processo de desenvolvimento, pré-requisitos para instalação, servidores necessários, etc.
d. Uma proposta inicial de como organizar a infraestrutura de sua aplicação, de acordo com o sistema de virtualização em que você pretende implementá-la.

R:

[O tipo de negócio/processo/problema que pretende tratar a partir de uma aplicação distribuída rodando sobre uma infraestrutura com virtualização.]

Atualmente a empresa deseja implementar o conceito de BYOD, que significa *Traga o Seu Próprio Dispositivo*, do inglês Bring Your Own Device, para os usuários. Permitindo que utilizem os dispositivos de sua preferência. Assim os colaboradores ficam mais confortáveis com tudo em um só lugar, seja pessoal ou corporativo.

[Uma justificativa de porque este problema é relevante]

Daí surgem os desafios, pois ao permitir o tráfego e armazenamento de informações sensíveis e confidenciais aumenta o risco de vazamentos de informações ou misturar dados corporativos em aplicativos e ou plataformas inseguras. Portanto é necessária uma solução para permitir administração de políticas de segurança e gerenciamento sem interferir na privacidade ou causar transtornos para os usuários finais.

Fonte imagem:
The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits

https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating
Os números associados aos riscos de exposição dos dispositivos perdidos ou roubados por ano também são bastante alarmantes:'

Fonte imagem:
The Rise and Risk of BYOD
www.druva.com/blog/the-rise-and-risk-of-byod/

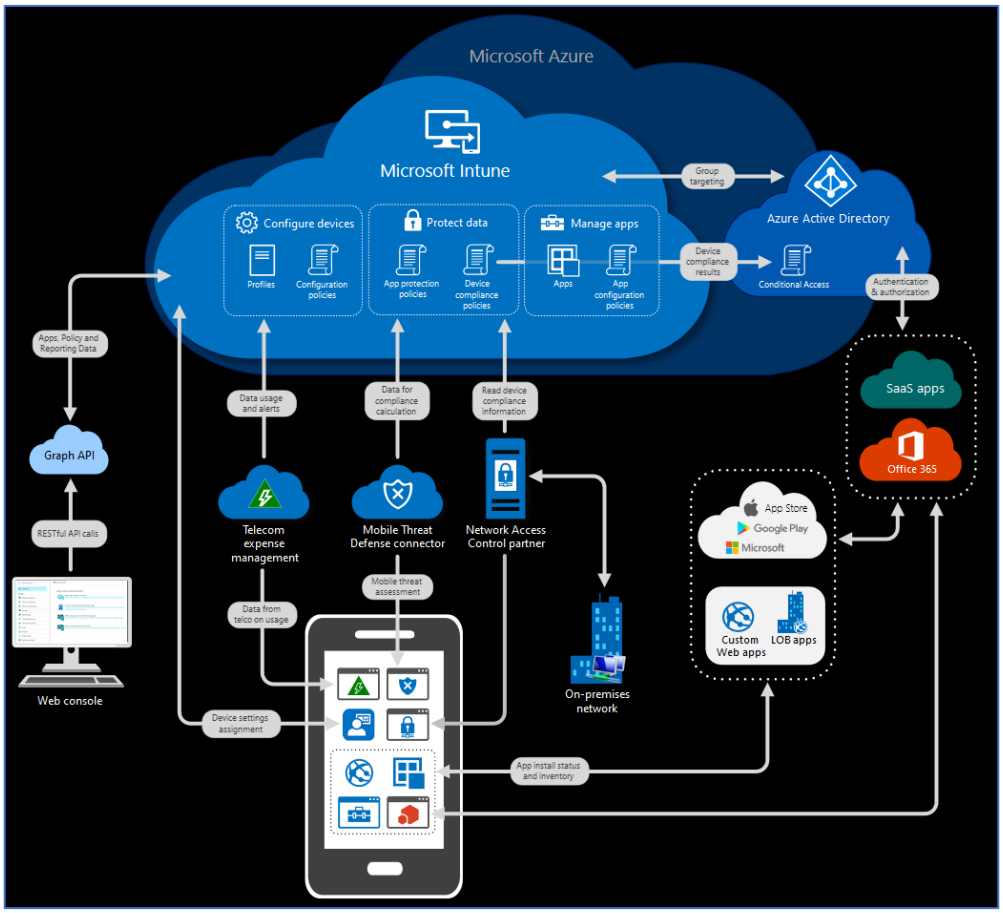
[**c. Uma descrição da aplicação distribuída que você pretende implementar com detalhes de sua arquitetura, como o gerenciamento do código-fonte, do processo de desenvolvimento, pré-requisitos para instalação, servidores necessários, etc.**]

O Microsoft Intune é uma solução de gerenciamento de dispositivos ou MDM – Mobile Device Management que permite um gerenciamento de mobilidade completo, a partir de uma única console de gerenciamento e desenvolvida para controlar dispositivos Windows, iOS, Android, MacOS. Através do Intune é possível configurar uma série de parâmetros de segurança, como criptografia, senha de acesso etc., restrições de rede, distribuir aplicativos de forma automatizada e outras funções.

O Microsoft Intune é uma solução em nuvem, baseada em SaaS – *Software As a Service, suportado pelo Microsoft Azure.* Possui licenciamento simplificado e oferece opções de integração com ferramentas internas de gerenciamento, como o *Microsoft System Center.*

Toda a adoção e configuração da solução exige esforço mínimo e ainda oferece a possibilidade de testar o produto até 90 dias sem custo e ou compromisso.

Abaixo um diagrama da arquitetura da solução:



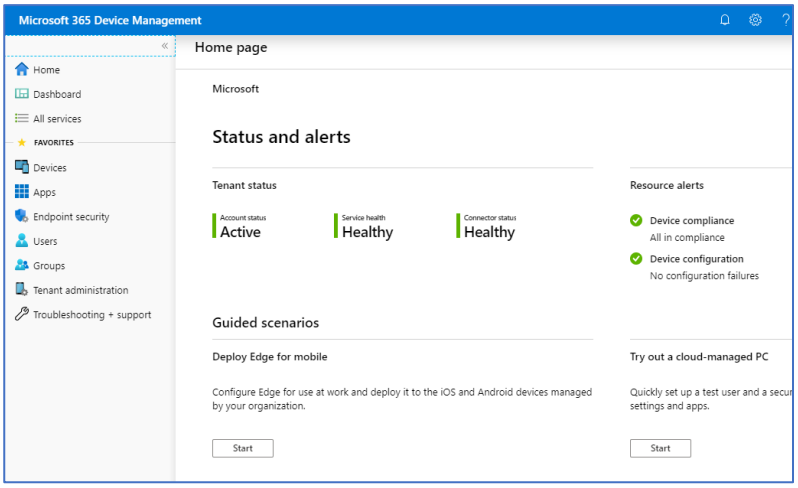
Detalhes técnicos sobre como o código-fonte da aplicação é gerenciado.

A solução do Microsoft Intune é desenvolvida e suportada pela Microsoft e o acesso ao código fonte é vedado ao público. A solução é hospedada na nuvem de serviços da Microsoft, com ambiente altamente redundante e seguro. O fabricante segue normas rígidas, padrões internacionais e melhores práticas para desenvolvimento, homologação, controle e

[d. Uma proposta inicial de como organizar a infraestrutura de sua aplicação, de acordo com o sistema de virtualização em que você pretende implementá-la.]

A infraestrutura da solução já é provisionada na nuvem para funcionar de forma elástica, garantindo que consiga suprir as necessidades de acordo que com o número de usuários forem sendo adicionados a solução. Os pré-requisitos também são bastante simplificados, tanto para o lado de infraestrutura, baseado em SaaS quanto pelo lado de adoção por parte dos usuários finais. Os usuários possuem opções bastante simplificadas para realizar o processo de Enrollment (processo de aderir a solução a partir de seus dispositivos). Pode ser feita de instalando um agente específico chamado Portal da Empresa, disponível em qualquer Store online de forma gratuita, ou sem instalar nenhum componente adicional (MAM – Mobile Application Management), o administrador pode especificar políticas em nível de aplicação, como por exemplo para o email corporativo.

A solução possui uma console de gerenciamento web disponível em https://devicemanagement.microsoft.com/ e possui a aparência simplifica e fluida conforme abaixo:



Abaixo um planejamento macro da solução na empresa:

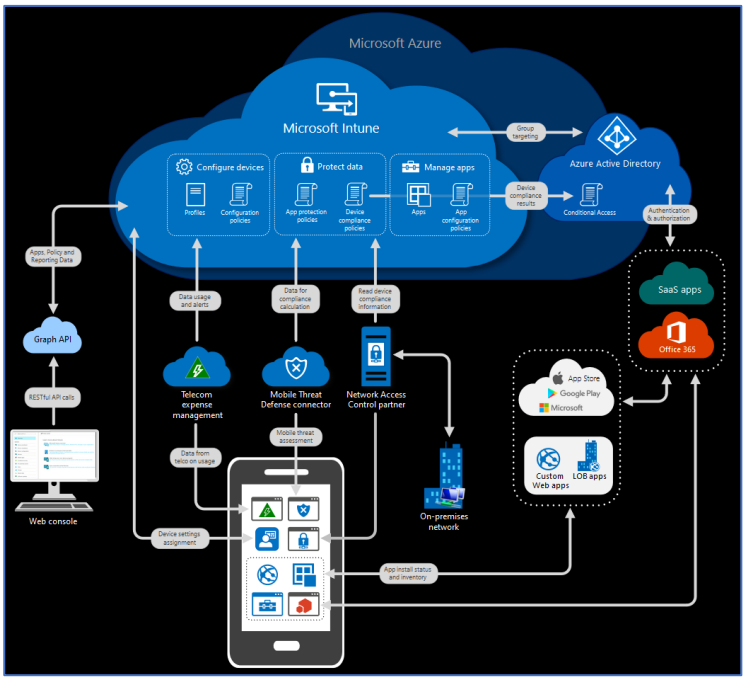
Capítulo 2:

Faça upload de uma versão inicial do capítulo 2/Proposta de Solução de seu Projeto de Bloco. Você deve contemplar:

- ***Uma pequena descrição textual teórica sobre a arquitetura da solução de virtualização que você pretende utilizar.***
- ***Comparações entre a forma como você pretende implantar seu ambiente e outras abordagens, usando outras ferramentas.***
- ***Um planejamento passo a passo (com descrições de cada etapa) de como será feita a implantação da aplicação distribuída virtualizada.***
- ***Um cronograma estimado com o prazo para execução de cada atividade.***

[A. Uma pequena descrição textual teórica sobre a arquitetura da solução de virtualização que você pretende utilizar.]

Conforme já mencionado anteriormente abaixo uma abordagem de como a infraestrutura da solução do Intune está organizada e como os componentes estão distribuídos:



A empresa tem a necessidade de melhorar a gestão dos dispositivos utilizados pelos usuários, bem como as informações corporativas, mantendo um foco em segurança da informação. A solução esta dividida em alguns pilares

1. Gerenciamento de dispositivos:
    - Gerenciar dispositivos de diferentes plataformas e sistemas operacionais, tais como iOS, MacOS, Linux, Windows.
    - Configurar políticas de gerenciamento com base nas políticas de segurança da informação. Bloquear dispositivos que tenham sido desbloqueados (Rooting ou Jailbreaking);
    - Permitir que os usuários utilizem dispositivos de sua escolha e ainda assim garantir que os padrões de segurança e facilidades de gerenciamento são mantidos com a mesma qualidade dos dispositivos fornecidos pela empresa;
    - Garantir relatórios completos e permitindo a visualização dos dispositivos que estão em conformidade com os padrões da empresa;
    - Distribuir configurações personalizadas para os dispositivos, tais como conexões VPN, certificados digitais, configurações e políticas (Exemplo: Bloqueio automático de tela a cada 3 minutos, habilitar criptografia do dispositivo e etc;
    - Permitir que o dispositivo seja apagado em caso de perda ou roubo, aumentando a segurança dos dados corporativos.

2. Conformidade e acesso condicional:
    - O Intune permite uma integração com o sistema de identidades (AzureAD) para permitir acesso a dados e aplicações corporativas com base em condições do dispositivo do usuário. Por exemplo, o usuário para sincronizar o email corporativo precisa que o dispositivo esteja em conformidade com os políticas definidas pela organização. Se a política determina que o dispositivo para estar em conformidade precisa estar com a criptografia de armazenamento

habilitada, somente dispositivos nessa condição conseguirão acessar o email corporativo.

3. Gerenciamento de aplicações:
   O intune possui um conceito de permitir um gerenciamento a nível de aplicações, permitindo proteger os dados corporativos sem misturar com os dados pessoais/privados dos usuários. As principais funcionalidades a serem adotadas:
   - Distribuir aplicações com base nas necessidades de negocio, baseado em grupos ou áreas de negocio;
   - Permitir a deleção seletiva dos dados, ou seja, em caso de perda, roubo ou desligamento da empresa somente os dados e aplicativos corporativos serão removidos;
   - Permitir a gestão das aplicações e dados corporativos sem a necessidade de instalar nenhum agente adicional;

[B. Comparações entre a forma como você pretende implantar seu ambiente e outras abordagens, usando outras ferramentas.]

O Microsoft Intune é uma solução em nuvem, baseada em SaaS – Software As a Service, suportado pela plataforma do Microsoft Azure.

Já foi realizado um processo de avaliação da solução pelo time responsável pelo gerenciamento de dispositivos, devidamente aprovado pela gestão. A avaliação foi realizada com base em 25 usuários que testaram e homologaram a solução de MDM.

Durante o processo de avaliação, foi avaliada outra solução de MDM, do fabricante VMWare – o AirWatch. Ambas as soluções são excelentes, líderes de mercado e atenderam todas as expectativas das necessidades de negócio da empresa. Abaixo um breve resumo do comparativo das soluções:

Microsoft Intune	**VMWare AirWatch MDM**
Distribuição de Apps e aplicações	Device Management
Device Management	Políticas de DLP (Data Loss Prevention)
Device Enrollment	Configuração simplificada
Device Compliance	Gerenciamento de políticas e segurança
Monitoramento de aplicações	Device Compliance
Configurações de Acesso Conditional	Gerenciamento de usuários e grupos
Gerenciamento de usuários e grupos	Gerenciamento via MAM (Mobile Application Management
Controles de usuários baseado em funções (roles)	Device Enrollment
Gerenciamento via MAM (Mobile Application Management	VMWare TrustPoint
Gerenciamento de políticas e segurança	Remote Commands
Integração com o Microsoft Configuration Manager (Co-Management)	Sistema de gerenciamento de eventos granular
Windows AutoPilot	Dynamic Watermark
Preço por usuário/mês: **$6 (USD)**	Preço por usuário/mês: **$10.90 (USD)**

Embora a solução da VMWare seja superior, o critério adotado foi influenciado pelo preço entre as soluções e integração com soluções já implementadas na empresa, como o Microsoft Configuration Manager e o Office 365.

Fonte de informações:
Microsoft Intune Features
https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/microsoft-intune

Workspace ONE Powered by AirWatch
https://www.air-watch.com/pricing/

A implementação é feita por meio de assinatura e com base em licenças por número de usuários. Serão adquiridas 800 licenças da solução para atender o cenário da empresa.

[C. Um planejamento passo a passo (com descrições de cada etapa) de como será feita a implantação da aplicação distribuída virtualizada..]

A implantação será realizada em fases.

Fonte imagem: Intune migration guide
https://docs.microsoft.com/en-us/mem/intune/fundamentals/migration-guide

1. Fase 1: Setup básico: Nesta etapa as configurações básicas utilizadas na avaliação e homologação da solução serão revisadas;
2. Fase 2: Serão definidas as configurações e políticas de gerenciamento de dispositivos, levando em consideração dispositivos da empresa e dispositivos pessoais (CYOD e BYOD). Também serão definidos os perfis de usuários e respectivas configurações com base nas necessidades de negócio;
3. Fase 3: Configurações de aplicativos: Serão definidas as políticas de uso de aplicativos e informações corporativas nos dispositivos. As configurações para dispositivos no modelo BYOD serão mais restritivas para garantir um nível elevado de segurança em dispositivos que não são gerenciados pela empresa;
4. Fase 4: Plano de comunicação: Os usuários começaram a receber os comunicados com base no plano de comunicação que envolve divulgação da tecnologia, política de uso, suporte do Service Desk, perguntas frequentes, guias, dicas e tutoriais.
5. Fase 5: Fase de adoção: Os usuários começaram a adotar a solução de MDM, com base no dispositivo e perfil de usuário definido na Fase 2;

[D. Um cronograma estimado com o prazo para execução de cada atividade.

- Cronograma de atividades e o prazo estimado para conclusão da implementação da solução SaaS é de 35 dias:

Projeto Bloco - TP7	**35 days**
Fase 1:	**16 days**
Revisão de políticas	8 hrs
Revisão da infraestrutura básica (Rede, internet, usuár	16 hrs
Adquirir e atribuir licenças	8 hrs
Fase 2:	**13 days**
Definir número de dispositivos que cada usuário reg	8 hrs
Gerenciar configurações de dispositivos (criptografi	8 hrs
Entregar aplicativos, perfis de email, perfis de VPN	24 hrs
Avaliação de critérios no nível do dispositivo para as	24 hrs
Publicar e implantar aplicativos	40 hrs
Fase 3	**15 days**
Configurar políticas de MAM	16 hrs
Preparar configurações de privacidade e segurança	8 hrs
Configurar políticas de segurança de dispositivo	8 hrs
Testes finais de poíticas de MAM	16 hrs
Fase 4	**1 day**
Plano de comunicação para usuários VIP	3 hrs
Plano de comunicação para usuários Marketing	1 hr
Plano de comunicação para usuários Finanças	1 hr
Plano de comunicação para usuários Administração	1 hr
Plano de comunicação para usuários Vendas	1 hr
Fase 5	**5 days**
Iniciar campanhas de adoção da solução	2 hrs
Prover workshops periódicos de utilização	16 hrs
Iniciar campanhas de Home Office	24 hrs