

## **7) CESPE/CEBRASPE - CAU - Analista de Sistemas da Informação - 2024**

Na modalidade IaaS (infrastructure as a service), o sistema operacional e as aplicações instaladas podem ser controlados pelo próprio usuário.

## **7) CESPE/CEBRASPE - CAU - Analista de Sistemas da Informação - 2024**

Na modalidade IaaS (infrastructure as a service), o sistema operacional e as aplicações instaladas podem ser controlados pelo próprio usuário.

Certo

## **8) CESPE/CEBRASPE - CAU - Analista de Infraestrutura de Tecnologia da Informação - 2024**

O componente middleware é gerenciado pelo cliente no IaaS (Infraestrutura como Serviço) e no PaaS (Plataforma como Serviço), enquanto no SaaS (Programa como Serviço), esse componente é gerenciado pelo provedor de serviços de nuvem.

## **8) CESPE/CEBRASPE - CAU - Analista de Infraestrutura de Tecnologia da Informação - 2024**

O componente middleware é gerenciado pelo cliente no IaaS (Infraestrutura como Serviço) e no PaaS (Plataforma como Serviço), enquanto no SaaS (Programa como Serviço), esse componente é gerenciado pelo provedor de serviços de nuvem.

Errado. Embora o provedor de PaaS seja responsável por manter e gerenciar a infraestrutura subjacente e os serviços de middleware, o cliente ainda tem algum nível de controle sobre a configuração e a personalização desses serviços para atender às suas necessidades de aplicativos específicas. Isso permite um certo grau de flexibilidade e adaptabilidade no desenvolvimento e implantação de aplicativos na plataforma PaaS.

## 9) **CESPE/CEBRASPE - CAU - Assistente de Tecnologia da Informação - 2024**

No modelo de IaaS (Infrastructure as a Service), o usuário tem controle sobre sistemas operacionais, armazenamentos e aplicativos implantados, além do controle limitado de componentes de firewalls de host.

## 9) CESPE/CEBRASPE - CAU - Assistente de Tecnologia da Informação - 2024

No modelo de IaaS (Infrastructure as a Service), o usuário tem controle sobre sistemas operacionais, armazenamentos e aplicativos implantados, além do controle limitado de componentes de firewalls de host.

Certo. Host físico provedor.

## **10) CESPE/CEBRASPE - CAU - Analista de Sistemas da Informação - 2024**

A modalidade PaaS (platform as a software) é indicada para desenvolvedores de aplicações que operam na nuvem, pois oferece um ambiente de desenvolvimento de software.

## **10) CESPE/CEBRASPE - CAU - Analista de Sistemas da Informação - 2024**

A modalidade PaaS (platform as a software) é indicada para desenvolvedores de aplicações que operam na nuvem, pois oferece um ambiente de desenvolvimento de software.

Certo



## **11) CESPE/CEBRASPE - DATAPREV - Analista - Área: Processamento - 2023**

Em PaaS, o cliente não tem de se preocupar com a camada de infraestrutura, podendo concentrar-se somente nas aplicações que deseja disponibilizar.

## **11) CESPE/CEBRASPE - DATAPREV - Analista - Área: Processamento - 2023**

Em PaaS, o cliente não tem de se preocupar com a camada de infraestrutura, podendo concentrar-se somente nas aplicações que deseja disponibilizar.

Certo

## **12) CESPE/CEBRASPE - CAU - Analista de Infraestrutura de Tecnologia da Informação - 2024**

Entre os exemplos de uso da RPA (Robot Process Automation), estão reconhecimento de voz, conversão de voz em texto e gerenciamento remoto de infraestrutura.

## **12) CESPE/CEBRASPE - CAU - Analista de Infraestrutura de Tecnologia da Informação - 2024**

Entre os exemplos de uso da RPA (Robot Process Automation), estão reconhecimento de voz, conversão de voz em texto e gerenciamento remoto de infraestrutura.

Certo

## Serviços de Diretório

Lightweight Directory Access Protocol é um protocolo de acesso a diretórios usado para consultar e modificar informações armazenadas em um serviço de diretório. Ele é projetado para ser uma maneira eficiente e flexível de acessar e gerenciar informações de diretório em redes de computadores.

Estrutura de Dados Hierárquica: organiza os dados em uma estrutura hierárquica de árvore, semelhante à estrutura de um sistema de arquivos. Cada objeto no diretório é representado por uma entrada (ou entrada de diretório), que pode conter atributos que descrevem suas características.

Protocolo de Acesso: é um protocolo de acesso baseado em texto que define operações para pesquisar, adicionar, modificar e excluir informações no diretório.

Modelo Cliente-Servidor: O LDAP segue um modelo cliente-servidor, onde os clientes LDAP enviam solicitações de operações de diretório para servidores LDAP, que respondem com os resultados correspondentes. Isso permite que os clientes consultem e atualizem informações no diretório de forma eficiente.

Padrão Aberto: O LDAP é um padrão aberto, definido pela RFC 4510 e RFCs relacionadas, o que significa que é amplamente suportado por uma variedade de sistemas e aplicativos. Isso inclui sistemas operacionais, servidores de diretório, aplicativos de email, sistemas de autenticação e muito mais.

Serviços de Diretório: O LDAP é comumente usado em conjunto com serviços de diretório, como o Active Directory da Microsoft, OpenLDAP, Apache Directory Server e muitos outros. Esses serviços de diretório fornecem um armazenamento centralizado e organizado de informações sobre usuários, grupos, recursos de rede e outros objetos.

Segurança: O LDAP oferece recursos de segurança, como autenticação e controle de acesso, para proteger os dados armazenados no diretório. Isso inclui suporte a autenticação baseada em senha, criptografia de dados e mecanismos de autorização baseados em políticas de acesso.

Aplicações: O LDAP é amplamente utilizado em uma variedade de aplicações e ambientes, incluindo autenticação de usuários em redes corporativas, diretórios de endereços de email, armazenamento de informações de configuração em sistemas de rede e muito mais.

# Serviços de Diretório

O Active Directory (AD) é um serviço de diretório desenvolvido pela Microsoft para gerenciar recursos em uma rede de computadores baseada no Windows. Ele desempenha um papel central na administração de identidades, autenticação e autorização dentro de um ambiente empresarial.

**Serviço de Diretório:** O Active Directory funciona como um serviço de diretório, o que significa que armazena informações sobre recursos da rede, como usuários, computadores, impressoras, grupos, políticas de segurança e outros objetos.

**Hierarquia Lógica:** O AD é organizado em uma estrutura hierárquica lógica chamada de domínio. Um domínio é uma unidade de gerenciamento de segurança e política, e pode conter usuários, grupos e computadores. Vários domínios podem ser agrupados em uma floresta.

**Floresta:** Uma floresta é uma coleção de um ou mais domínios do Active Directory que compartilham uma relação de confiança comum e um esquema de diretório comum. A floresta é a unidade de maior escopo no AD.

**Controladores de Domínio:** Os controladores de domínio são servidores que executam o serviço de diretório do Active Directory. Eles mantêm uma cópia do banco de dados do AD e fornecem serviços de autenticação e autorização para os usuários e computadores da rede.

**Política de Grupo:** O Active Directory permite a aplicação de políticas de grupo, que são configurações de segurança e configurações do sistema que podem ser aplicadas em nível de domínio, unidade organizacional ou local de computador para controlar o ambiente de segurança e configuração dos computadores e usuários.

**Autenticação Única:** Uma das principais vantagens do Active Directory é a capacidade de fornecer autenticação única para os usuários em toda a rede. Isso significa que os usuários podem usar as mesmas credenciais (nome de usuário e senha) para acessar recursos em diferentes partes da rede.

**Integração com outros serviços Microsoft:** O AD é integrado a muitos outros serviços da Microsoft, como o Microsoft Exchange Server (para e-mail), Microsoft SharePoint (para colaboração), Microsoft Azure (para computação em nuvem) e outros, fornecendo uma base sólida para a infraestrutura de TI corporativa.

**Segurança:** O Active Directory oferece recursos avançados de segurança, incluindo controle de acesso baseado em função, auditoria de eventos e políticas de segurança granulares, ajudando as organizações a proteger seus recursos de rede contra ameaças internas e externas.

Active Directory é uma solução de gerenciamento de identidade e acesso da Microsoft, comumente usada em ambientes Windows e Linux. Embora o Active Directory não seja nativamente projetado para armazenar chaves SSH (Secure Shell), que é uma forma de acessar e gerenciar sistemas remotos, geralmente usada em sistemas Unix/Linux, embora existam implementações para Windows também. Não é uma prática padrão para o Active Directory ou para sistemas Unix/Linux descartar informações de usuários que não estão atualmente logados. Os sistemas operacionais geralmente mantêm registros de todos os usuários, suas configurações e informações relevantes, mesmo que não estejam ativamente logados no momento.