SUPPORT COURS

CONCEPTS DE VIRTUALISATION ET CLOUD COMPUTING

Dr Beman H. KAMAGATE

Maître -Assistant en Informatique

Ecole Supérieure Africaine des TIC

Bd. de Marseille face à Bernabe - Km 4. Treichville - 18 BP 1501 Abidjan 18.
Abidjan - Côte d'Ivoire. www.**esatic**.ci

Objectif du cours

L'objectif du cours de virtualisation et de cloud computing est de fournir aux étudiants une compréhension approfondie des concepts, des technologies et des applications liés à la virtualisation et au cloud computing. Voici quelques objectifs spécifiques que l'on peut attendre d'un tel cours :

Compréhension des concepts fondamentaux : Les étudiants devraient acquérir une connaissance approfondie des concepts fondamentaux de la virtualisation, y compris les différents types de virtualisation (matérielle, logicielle, etc.) et leur utilisation dans les environnements informatiques.

Maîtrise des technologies de virtualisation : Les étudiants devraient apprendre à utiliser des outils de virtualisation populaires tels que VMware, VirtualBox, et Hyper-V, en comprenant comment créer, gérer et optimiser des machines virtuelles et des conteneurs.

Compréhension du cloud computing : Les étudiants devraient acquérir une connaissance approfondie des concepts et des modèles de service du cloud computing, y compris les infrastructures en tant que service (IaaS), les plateformes en tant que service (PaaS) et les logiciels en tant que service (SaaS).

Familiarité avec les fournisseurs de services cloud : Les étudiants devraient apprendre à connaître les principaux fournisseurs de services cloud tels qu'Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform, ainsi que leurs offres de services et leurs différences.

Capacité à concevoir et à mettre en œuvre des solutions cloud : Les étudiants devraient être en mesure de concevoir et de mettre en œuvre des solutions cloud pour répondre aux besoins des entreprises, en utilisant les meilleures pratiques de sécurité, de performance et de gestion des coûts.

Développement de compétences pratiques : Les étudiants devraient acquérir des compétences pratiques en utilisant des outils et des technologies de virtualisation et de cloud computing dans des travaux pratiques, des études de cas et des projets de groupe.

Compréhension des défis et des meilleures pratiques : Les étudiants devraient être en mesure d'identifier les défis courants liés à la virtualisation et au cloud computing, ainsi que les meilleures pratiques pour les surmonter et pour assurer la sécurité, la fiabilité et la performance des solutions cloud.

Table des matières

1. Introduction à la Virtualisation

1.1. Définitions et concepts de base de la virtualisation

1.1.1. Définition

La virtualisation est une technologie qui permet de créer des versions virtuelles d'environnements informatiques, tels que des serveurs, des systèmes de stockage, des réseaux ou des systèmes d'exploitation. Cette abstraction des ressources physiques permet une utilisation plus efficace des infrastructures informatiques en les rendant plus flexibles, évolutives et rentables.

1.1.2. Les principaux concepts de la virtualisation incluent

Hyperviseur (ou VMM - Virtual Machine Monitor) : un logiciel qui crée et gère les machines virtuelles en isolant les ressources matérielles sous-jacentes.
Machine virtuelle (VM) : une instance logicielle autonome qui émule le comportement d'un système informatique complet, y compris le processeur, la mémoire, le stockage et les périphériques.
Hôte (ou serveur physique) : le matériel physique sur lequel l'hyperviseur s'exécute et sur lequel les machines virtuelles sont déployées.
Invité (ou VM) : une instance virtuelle exécutée sur un hôte, représentant un système d'exploitation et les applications associées.

1.2.Historique et évolution de la virtualisation

La virtualisation remonte aux années 1960 avec l'apparition des premiers systèmes informatiques multi-utilisateurs, mais elle a gagné en popularité dans les années 2000 avec l'avènement des technologies de virtualisation x86. Des entreprises telles que VMware, Microsoft et Xen ont développé des hyperviseurs commerciaux qui ont révolutionné la gestion des infrastructures informatiques en permettant la consolidation des serveurs et l'amélioration de l'efficacité opérationnelle.

Au fil des années, la virtualisation s'est étendue au-delà des serveurs pour inclure le stockage, les réseaux et même les applications. La montée en puissance des conteneurs, avec des technologies telles que Docker et Kubernetes, a également contribué à redéfinir

les approches de virtualisation en introduisant une isolation légère et une portabilité des applications.

1.3.Types de virtualisation

Virtualisation matérielle : Cette approche implique l'utilisation d'un hyperviseur pour diviser les ressources physiques d'un serveur en plusieurs machines virtuelles distinctes. Chaque machine virtuelle fonctionne comme un système complet avec son propre système d'exploitation et ses applications.

Virtualisation logicielle : Cette méthode consiste à utiliser un logiciel pour émuler le comportement des composants matériels, permettant ainsi l'exécution de plusieurs systèmes d'exploitation sur un même matériel physique.
Virtualisation des applications : Également connue sous le nom de conteneurisation, cette forme de virtualisation encapsule des applications et leurs dépendances dans des conteneurs légers, offrant un environnement isolé et portable pour l'exécution des applications.
Avantages et inconvénients de la virtualisation

1.4. Avantages de la virtualisation

Consolidation des serveurs : permettant d'exécuter plusieurs machines virtuelles sur un seul serveur physique, ce qui réduit les coûts d'infrastructure et d'énergie.
Flexibilité et évolutivité : facilitant le déploiement et la gestion rapides de nouvelles instances virtuelles en fonction des besoins de charge de travail.
Isolation : assurant une séparation efficace entre les différentes machines virtuelles pour garantir la sécurité et la disponibilité des applications.
Test et développement simplifiés : permettant la création d'environnements de test et de développement isolés sans nécessiter de matériel dédié.

1.5. inconvénients de la virtualisation

Surcoûts liés à l'overhead de virtualisation et à la gestion des ressources.
Complexité accrue de la gestion des infrastructures virtualisées.
Risques de sécurité associés à la consolidation des charges de travail sur un même matériel physique.

Dépendance à l'égard des fournisseurs de virtualisation et des technologies propriétaires.

2. Technologies de Virtualisation

2.1. Hyperviseurs

Les hyperviseurs sont des logiciels qui permettent de créer et de gérer des machines virtuelles sur un matériel physique. Il existe deux types d'hyperviseurs :

Hyperviseurs de type 1 (ou bare-metal) : Ces hyperviseurs s'exécutent directement sur le matériel physique, sans système d'exploitation intermédiaire. Ils offrent généralement des performances optimales et une plus grande isolation entre les machines virtuelles.
Exemples : VMware vSphere/ESXi, Microsoft Hyper-V, KVM (Kernel-based Virtual Machine).
Hyperviseurs de type 2 (ou hosted) : Ces hyperviseurs s'exécutent sur un système d'exploitation hôte. Ils sont souvent utilisés pour des environnements de développement ou de test.
Exemples : VMware Workstation, Oracle VirtualBox.
Les fonctionnalités des hyperviseurs comprennent la gestion des ressources matérielles, la création et la gestion des machines virtuelles, la migration en direct (live migration), la haute disponibilité, la sécurité et la surveillance.

Une comparaison entre les principaux hyperviseurs peut être réalisée en examinant des critères tels que les performances, la fiabilité, la facilité de gestion, la compatibilité matérielle et logicielle, ainsi que les coûts.

2.2. Conteneurisation vs Virtualisation traditionnelle

La conteneurisation est une approche de virtualisation légère qui permet d'exécuter des applications et leurs dépendances dans des conteneurs isolés sur un système hôte. Contrairement à la virtualisation traditionnelle, qui utilise des machines virtuelles avec leur propre système d'exploitation, la conteneurisation partage le noyau de l'hôte entre les conteneurs, ce qui réduit l'overhead et améliore l'efficacité.
Les avantages de la conteneurisation incluent une plus grande portabilité des applications, des temps de démarrage plus rapides, une densité plus élevée des charges de travail et une utilisation plus efficace des ressources. Cependant, les conteneurs offrent une isolation

moins forte que les machines virtuelles et ne conviennent pas à toutes les charges de travail.

2.3.Gestion des machines virtuelles (VMs

La gestion des machines virtuelles comprend plusieurs aspects essentiels :

Provisionnement : création et configuration initiale des machines virtuelles, y compris l'attribution des ressources matérielles et la configuration réseau.

Migration : déplacement en temps réel des machines virtuelles entre différents hôtes physiques pour équilibrer la charge, maintenir la disponibilité ou effectuer des opérations de maintenance sans interruption de service.

Sauvegarde : création de copies de sauvegarde des machines virtuelles et de leurs données afin de garantir la récupération en cas de défaillance matérielle, de catastrophe ou de perte de données.

L'automatisation de ces processus est souvent réalisée à l'aide d'outils de gestion des infrastructures, tels que VMware vCenter, Microsoft System Center, ou des scripts personnalisés.

2.3. Automatisation et orchestration dans les environnements virtualisés

L'automatisation et l'orchestration jouent un rôle crucial dans la gestion des environnements virtualisés en permettant d'automatiser les tâches répétitives et de coordonner les opérations entre les différentes composantes de l'infrastructure.

Les outils d'automatisation et d'orchestration permettent de :

- Provisionner automatiquement des machines virtuelles et des ressources réseau.
- Gérer la configuration et les mises à jour logicielles.
- Surveiller les performances et les événements.
- Équilibrer la charge et optimiser l'utilisation des ressources.
- Mettre en œuvre des politiques de sécurité et de conformité.

Des outils populaires d'automatisation et d'orchestration incluent VMware vRealize Automation, **Microsoft Azure Automation, Kubernetes pour la conteneurisation, et des outils de gestion de la configuration tels que Puppet et Ansible**.

3. Cloud Computing

3.1. Définitions et concepts de base du cloud computing

Le cloud computing est un modèle de prestation de services informatiques qui permet d'accéder à des ressources informatiques, telles que des serveurs, des applications, des bases de données, des réseaux et des systèmes de stockage, via Internet. Les principaux concepts du cloud computing incluent :

Ressources à la demande : les utilisateurs peuvent accéder à des ressources informatiques à la demande et payer uniquement pour ce qu'ils utilisent, comme l'électricité ou l'eau.

Évolutivité : les ressources informatiques peuvent être rapidement adaptées pour répondre aux besoins fluctuants des utilisateurs, à la hausse ou à la baisse.

Partage des ressources : plusieurs utilisateurs peuvent partager des ressources informatiques physiques via la virtualisation, ce qui permet une utilisation plus efficace des ressources.

Accès via Internet : les services cloud sont généralement accessibles via Internet à partir de n'importe quel endroit et à tout moment, offrant une grande flexibilité d'accès.

3.2. Modèles de services : IaaS, PaaS, SaaS

Le cloud computing offre plusieurs modèles de services, chacun offrant un niveau différent d'abstraction et de contrôle pour les utilisateurs :

Infrastructure en tant que service (IaaS) : les fournisseurs de services cloud mettent à disposition des ressources informatiques virtuelles, telles que des serveurs, des machines virtuelles, des réseaux et du stockage, sur lesquelles les utilisateurs peuvent déployer et gérer leurs propres systèmes d'exploitation et applications. Exemples : Amazon Web Services (AWS) EC2, Microsoft Azure Virtual Machines.

Plateforme en tant que service (PaaS) : les fournisseurs de services cloud fournissent une plateforme de développement et d'exécution d'applications, comprenant généralement un ensemble d'outils et de services pour développer, tester, déployer et gérer des applications sans se soucier de l'infrastructure sous-jacente. Exemples : Google App Engine, Microsoft Azure App Service.

Logiciel en tant que service (SaaS) : les fournisseurs de services cloud fournissent des applications logicielles prêtes à l'emploi, accessibles via Internet et généralement facturées sur la base d'un abonnement. Les utilisateurs n'ont pas besoin de gérer ou de contrôler l'infrastructure sous-jacente, mais peuvent simplement utiliser l'application via un navigateur web ou une interface utilisateur. Exemples : Salesforce, Google Workspace, Microsoft Office 365.

3.3. Modèles de déploiement

Les modèles de déploiement décrivent où les services cloud sont déployés et comment ils sont gérés :

Cloud public : les ressources informatiques sont fournies par des fournisseurs de services cloud tiers et sont accessibles via Internet par le grand public. Les utilisateurs paient généralement un abonnement ou des frais d'utilisation en fonction de leur utilisation des ressources. Exemples : AWS, Microsoft Azure, Google Cloud Platform.

Cloud privé : les ressources informatiques sont dédiées à une organisation spécifique et sont gérées soit par l'organisation elle-même, soit par un tiers, mais elles ne sont pas partagées avec d'autres organisations. Le cloud privé peut être hébergé sur site ou dans un centre de données tiers.

Cloud hybride : une combinaison de cloud public et privé, permettant à une organisation de déplacer des charges de travail entre les deux environnements selon les besoins. Cette approche offre une plus grande flexibilité et peut aider à optimiser les coûts tout en répondant aux exigences de conformité et de sécurité.

3.4.Principaux fournisseurs de services cloud

Les principaux fournisseurs de services cloud offrent une gamme étendue de services et de solutions cloud pour répondre aux besoins variés des entreprises et des organisations :

Amazon Web Services (AWS) : le leader du marché du cloud computing, offrant une large gamme de services, notamment le calcul, le stockage, les bases de données, l'analyse, l'IA, l'IoT, la sécurité et bien d'autres.

Microsoft Azure : la plateforme cloud de Microsoft, offrant une intégration étroite avec les technologies Microsoft existantes, ainsi qu'une gamme de services cloud pour le calcul, le stockage, les bases de données, l'analyse, l'IoT, l'IA et bien d'autres.

Google Cloud Platform (GCP) : la plateforme cloud de Google, offrant des services cloud évolutifs et performants, ainsi que des solutions d'IA, d'analyse de données, d'apprentissage automatique, de développement d'applications et bien plus encore.
Ces fournisseurs de services cloud sont largement reconnus pour leur fiabilité, leur évolutivité, leur sécurité et leur vaste écosystème de partenaires et de développeurs.

4. Architecture et Services Cloud

4.1. Composants et architecture d'une plate-forme cloud

Une architecture cloud typique comprend plusieurs composants qui interagissent pour fournir des services informatiques à travers Internet. Les principaux composants incluent :

Infrastructure physique : les centres de données comprennent des serveurs, des dispositifs de stockage, des équipements réseau et des systèmes de refroidissement.
Virtualisation : l'abstraction des ressources physiques permet la création de machines virtuelles et de conteneurs, fournissant une flexibilité et une isolation accrues.
Orchestration : les outils d'orchestration automatisent le déploiement, la configuration et la gestion des ressources cloud, assurant une utilisation efficace des ressources.
Services cloud : une gamme étendue de services, tels que le stockage, le calcul, les bases de données, les réseaux, la sécurité, l'analyse, l'IA, l'IoT, etc.
L'architecture cloud peut être mise en œuvre selon différents modèles, tels que le modèle en couches (layers), le modèle de microservices, ou le modèle de service-oriented architecture (SOA).

4.2. Services cloud courants

Les services cloud offrent une variété de fonctionnalités pour répondre aux besoins informatiques des utilisateurs. Voici quelques services courants :
Stockage : les services de stockage cloud offrent un espace de stockage flexible et évolutif pour stocker des données, des fichiers, des médias, des sauvegardes, etc.
Exemples : Amazon S3, Google Cloud Storage, Azure Blob Storage.
Calcul : les services de calcul cloud fournissent des ressources de calcul virtuelles pour exécuter des applications, des charges de travail, des algorithmes, etc.
Exemples : Amazon EC2, Google Compute Engine, Azure Virtual Machines.

Bases de données : les services de base de données cloud offrent des solutions de stockage, de gestion et d'analyse de données, avec des options relationnelles et non relationnelles.

Exemples : Amazon RDS, Google Cloud SQL, Azure Cosmos DB.

Réseaux : les services de réseau cloud permettent de gérer et de sécuriser les communications entre les différentes ressources cloud, ainsi que l'accès aux utilisateurs.

Exemples : Amazon VPC, Google Virtual Private Cloud (VPC), Azure Virtual Network.

4.3. Évolutivité et élasticité dans le cloud

L'évolutivité et l'élasticité sont des caractéristiques clés du cloud computing, permettant aux utilisateurs de faire face aux fluctuations de la demande de manière efficace :

Évolutivité : la capacité à augmenter ou à réduire dynamiquement les ressources informatiques en fonction des besoins de charge de travail, afin de maintenir les performances et la disponibilité.

Élasticité : la capacité à ajouter ou à supprimer automatiquement des ressources en réponse aux variations de la demande, de manière transparente et sans intervention humaine.

Ces caractéristiques sont essentielles pour répondre aux exigences de performances, de disponibilité et de coût dans les environnements cloud.

4.4.Analyse des coûts et modèles de tarification

L'analyse des coûts et la gestion financière sont des aspects importants de l'utilisation des services cloud. Les fournisseurs de services cloud offrent divers modèles de tarification, tels que :

Tarification à l'utilisation : les utilisateurs paient uniquement pour les ressources qu'ils consomment, selon une tarification à la demande ou basée sur l'utilisation.

Tarification à l'abonnement : les utilisateurs paient un montant fixe sur une base régulière (mensuelle ou annuelle) pour un accès illimité à certaines ressources ou services.

Tarification basée sur les ressources : les coûts sont calculés en fonction des ressources allouées, telles que le nombre de machines virtuelles, la capacité de stockage, les heures d'utilisation, etc.

Modèles de tarification spécifiques : les fournisseurs de services cloud proposent souvent des options de tarification spécifiques pour des services particuliers, tels que les bases de données, l'analyse, l'IA, etc.

Une analyse des coûts permet aux organisations de comprendre et de contrôler leurs dépenses cloud, en optimisant l'utilisation des ressources et en choisissant les modèles de tarification les plus adaptés à leurs besoins.

5. Sécurité et Gouvernance dans le Cloud

5.1.Défis de sécurité dans le cloud

Bien que le cloud computing offre de nombreux avantages, il présente également des défis uniques en matière de sécurité, notamment :

Perte de contrôle direct sur l'infrastructure : les données et les charges de travail sont hébergées sur des infrastructures appartenant à des tiers, ce qui peut rendre la surveillance et la protection plus complexes.

Menaces de sécurité partagées : les utilisateurs partagent les ressources et l'infrastructure avec d'autres clients du cloud, ce qui signifie que les actions d'un utilisateur peuvent potentiellement affecter la sécurité d'autres utilisateurs.

Menaces persistantes avancées (APT) : les attaquants peuvent exploiter les failles de sécurité dans les environnements cloud pour accéder à des données sensibles ou perturber les opérations.

Conformité et réglementations : les entreprises doivent se conformer à diverses réglementations et normes de sécurité, ce qui peut être plus complexe dans un environnement cloud.

5.2. Modèles de responsabilité partagée

Dans le cadre du cloud computing, la responsabilité de la sécurité est partagée entre le fournisseur de services cloud et l'utilisateur. Les modèles de responsabilité partagée varient en fonction des types de services cloud utilisés :

Infrastructure en tant que service (IaaS) : le fournisseur de services cloud est responsable de la sécurité de l'infrastructure sous-jacente, tandis que l'utilisateur est responsable de la sécurité des systèmes d'exploitation, des applications et des données.

Plateforme en tant que service (PaaS) : le fournisseur de services cloud est responsable de la sécurité de la plateforme, y compris les systèmes d'exploitation et les middleware, tandis que l'utilisateur est responsable de la sécurité des applications et des données.

Logiciel en tant que service (SaaS) : le fournisseur de services cloud est responsable de la sécurité de l'ensemble du service, y compris l'infrastructure, la plateforme et les applications, tandis que l'utilisateur est responsable de la sécurité des données et de l'accès au service.

5.3. Mécanismes de sécurité

Pour renforcer la sécurité dans le cloud, plusieurs mécanismes de sécurité peuvent être mis en œuvre :

Chiffrement des données : le chiffrement des données permet de protéger les informations sensibles en les rendant illisibles pour toute personne non autorisée qui tenterait d'y accéder.

Pare-feu : les pare-feu permettent de contrôler et de filtrer le trafic réseau entrant et sortant, en bloquant les connexions non autorisées et en détectant les activités suspectes.

Gestion des identités et des accès (IAM) : la gestion des identités et des accès permet de contrôler et de gérer les droits d'accès des utilisateurs aux ressources cloud, en s'assurant que seules les personnes autorisées ont accès aux données et aux services.

Surveillance et détection des menaces : la surveillance continue et la détection des menaces permettent d'identifier et de répondre rapidement aux activités malveillantes ou aux incidents de sécurité dans le cloud.

5.4. Conformité réglementaire et gouvernance dans le cloud

La conformité réglementaire et la gouvernance sont essentielles pour garantir que les entreprises respectent les lois, les réglementations et les normes applicables dans leurs opérations cloud. Cela comprend :

Conformité aux réglementations sectorielles : les entreprises doivent se conformer à des réglementations spécifiques à leur secteur, telles que le RGPD pour la protection des données personnelles en Europe, ou la norme PCI DSS pour la sécurité des données de carte de crédit.

Gouvernance des données : la gouvernance des données implique la gestion et le contrôle des données sensibles pour garantir leur intégrité, leur confidentialité et leur disponibilité tout au long de leur cycle de vie.

Audit et surveillance : l'audit et la surveillance des activités dans le cloud permettent de vérifier la conformité aux politiques de sécurité, d'identifier les problèmes de conformité et de prendre des mesures correctives.

En mettant en œuvre des pratiques de sécurité robustes et une gouvernance efficace, les entreprises peuvent réduire les risques de sécurité dans le cloud et assurer la protection de leurs données et de leurs systèmes.

6. Gestion des Performances et des Ressources

6.1. Surveillance et gestion des performances dans le cloud

La surveillance des performances dans le cloud consiste à collecter, à analyser et à interpréter les données sur les ressources informatiques pour garantir que les services cloud fonctionnent de manière optimale. Cela inclut la surveillance des indicateurs de performance clés (KPI) tels que la disponibilité, la latence, le débit, l'utilisation des ressources, etc. Les outils de surveillance et de gestion des performances fournissent des tableaux de bord et des alertes pour aider les administrateurs à identifier les problèmes potentiels et à prendre des mesures correctives.

6.2. Optimisation des ressources et des coûts

L'optimisation des ressources et des coûts dans le cloud vise à maximiser l'efficacité opérationnelle et à minimiser les dépenses inutiles. Cela comprend l'identification et la suppression des ressources inutilisées, l'ajustement de la taille des instances en fonction des besoins, l'utilisation de modèles de tarification économiques, la mise en œuvre de politiques d'achat réservé, et l'utilisation d'outils d'analyse des coûts pour comprendre et optimiser les dépenses cloud.

6.3. Planification de la capacité et équilibrage de charge

La planification de la capacité dans le cloud implique d'estimer les besoins futurs en ressources informatiques pour garantir des performances optimales et éviter les temps d'arrêt imprévus. Cela comprend l'analyse des tendances de charge de travail, la prévision de la croissance, la sélection d'instances adaptées aux besoins, la mise en place de stratégies de redimensionnement automatique, et l'utilisation d'outils de gestion de la capacité pour surveiller et ajuster les ressources en temps réel. L'équilibrage de charge assure une distribution équitable du trafic entre les différentes instances pour éviter les goulets d'étranglement et garantir une utilisation efficace des ressources.

6.4.Dépannage et résolution des problèmes dans les environnements cloud

Le dépannage et la résolution des problèmes dans le cloud impliquent l'identification, l'analyse et la résolution des incidents de manière efficace pour minimiser l'impact sur les opérations.

Cela comprend l'utilisation de techniques de dépannage telles que l'analyse des journaux, la surveillance des métriques, le suivi des modifications, le recours à des experts techniques, et la mise en place de plans d'intervention d'urgence pour répondre rapidement aux problèmes critiques.

7.Travaux pratiques

TP1 : Création et gestion de machines virtuelles avec VirtualBox

Objectifs :

Comprendre les concepts de base de la virtualisation.

Apprendre à utiliser VirtualBox pour créer et gérer des machines virtuelles.

Configurer différents paramètres de virtualisation tels que le stockage, la mémoire et les réseaux.

Installer un système d'exploitation invité sur une machine virtuelle.

Explorer les fonctionnalités avancées telles que les snapshots et le partage de fichiers.

Matériel requis :

Un ordinateur avec VirtualBox installé (téléchargeable gratuitement sur virtualbox.org).

Un système d'exploitation hôte compatible (Windows, macOS, Linux).

Des fichiers d'installation d'un système d'exploitation invité (par exemple, une image ISO de Linux).

Instructions :

Installation de VirtualBox :

Téléchargez et installez VirtualBox sur votre ordinateur en suivant les instructions du site officiel.

Lancez VirtualBox pour vous familiariser avec son interface.

Création d'une machine virtuelle :

Créez une nouvelle machine virtuelle en utilisant l'assistant de création de VirtualBox.

Configurez les paramètres de base tels que le nom de la machine, le type et la version du système d'exploitation invité, ainsi que la quantité de mémoire RAM à allouer.

Configuration du stockage :

Créez et configurez un disque dur virtuel pour votre machine virtuelle.

Choisissez entre un disque dur dynamiquement alloué ou fixe en fonction de vos besoins.

Installation du système d'exploitation invité :

Montez le fichier d'installation de votre système d'exploitation invité sur la machine virtuelle.

Démarrez la machine virtuelle et suivez les instructions pour installer le système d'exploitation.

Configuration avancée :

Explorez les fonctionnalités avancées de VirtualBox telles que les snapshots pour sauvegarder l'état de la machine virtuelle à un moment donné.

Configurez le partage de fichiers entre l'hôte et l'invité pour faciliter le transfert de données.

Exercices pratiques :

Clonez une machine virtuelle existante pour créer une copie identique.

Ajoutez et configurez des périphériques virtuels supplémentaires tels que des cartes réseau ou des contrôleurs USB.

Expérimentez avec les paramètres de performance pour optimiser les ressources allouées à la machine virtuelle.