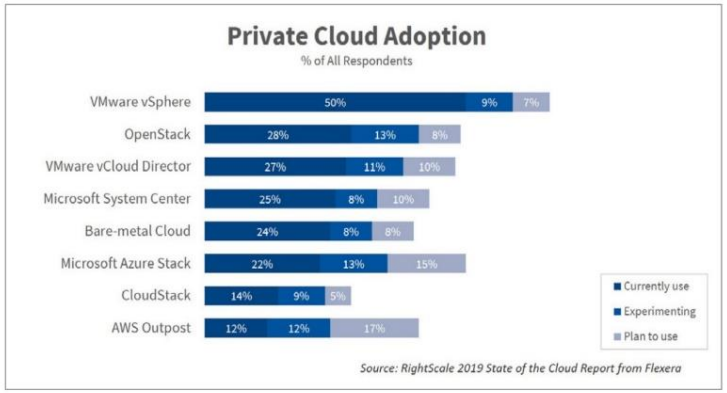
Durcissement openstack®

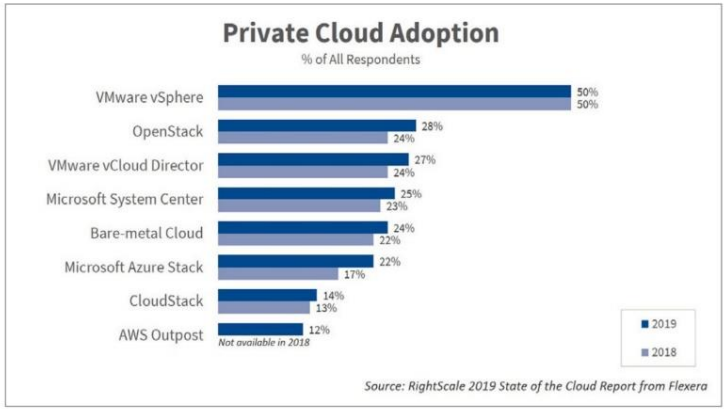
in good we trust.

metanext

Openstack - Contexte

Tendances Go To Cloud « On Premise »





Enjeux et Bénéfices

- Automatisation
- Scalabilité
- Amélioration TTM
- Fourniture d'instances de Cloud Computing
- Optimisation des coûts (invest., gestion DC, électricité, clim.)
- Qualité de service opérationnelle

openstack. en tant que solution IaaS à moindre coût (licence)

- Plateforme logicielle **IaaS Opensource** (licence Apache) utilisant du matériel standard
- Commande via **API, GUI ou CLI**
- **Foundation openstack** composée par Canonical, Red Hat, SUSE, eNovance, AT&T, Cisco, Dell, HP, IBM, Yahoo!, Oracle, Orange, Cloudwatt, EMC, VMware, Intel, NetApp.

metanext

Openstack - Les services proposés

Web Frontend

Tableau de bord (application web) de gestion des environnements cloud

Networking

Service réseau gère et manipule les réseaux et l'adressage IP.

Image

Service d'image permettant la découverte, l'envoi et la distribution d'image disque vers les instances.

Compute

Service de calcul (compute) gère des ressources de calcul des infrastructures.

Identity

Service d'identité fournit un annuaire central contenant la liste des services et la liste des utilisateurs.

Orchestration

Composant d'orchestration permettant de décrire une infrastructure sous forme de modèles et de le déployer.

Block Storage

Service de stockage en mode bloc gère les opérations de création, d'attachement et de détachement de ces périphériques sur les serveurs.

Object Storage

Service de stockage objet fournissant un système de stockage de données redondant et évolutif.

metanext

Openstack – Quelques exemples de menaces

Vulnérabilités	Menaces	Impacts	Remédiations
Mauvaise **gestion des droits**	Accès non autorisé	Modification des paramètres, suppression de machines, de données	Vérifier les accès définis dans le fichier policy.json
Utilisation d'une **version obsolète ou non patchée**	Exploitation d'une vulnérabilité	Indisponibilité du service	Mise en place d'un processus de veille et de gestion des vulnérabilités
Mauvaise **gestion des accès**	Utilisation du compte administrateur local par une personne non autorisée	Modification des paramètres ou suppression de machines, de données	Utiliser un annuaire centralisé pour gérer les authentifications et supprimer les comptes utilisateurs locaux
Aucune **supervision sécurité**	Exfiltration de données	Vol de données	Mettre en place une supervision des logs d'action et d'authentification (SIEM) et supervision sécurité réseau (IDS)
Pas de **chiffrement des disques**	Récupération d'informations sur un disque	Vol de données	Chiffrer les disques de stockage
Aucune **vérification des images** utilisées par Glance	Mise en place d'image malveillante	Indisponibilité du service ou modification d'intégrité des images	Signer les images avant stockage et vérifier la signature avant déploiement
Aucun **durcissement**	Exploitation de vulnérabilité	Indisponibilité du service ou récupération de données	Faire un durcissement des différentes couches (Hyperviseur, système d'exploitation, modules, logiciels) à l'aide des recommandations CIS, ANSSI,...
Pas de **quota d'utilisation des ressources**	Surexploitation des ressources matérielles	Indisponibilité du service	Définir des quotas (réseaux et matériels (RAM, espace disque,...)
Pas de **surveillance de charge réseau ou de la capacité des machines**	Interruption de service	Indisponibilité du service	Mettre en place une supervision réseau (NOC)

Openstack – Sécurisation de la plateforme

Metanext et sa practice GRC SSI & Cloud Security s'appuie sur plus de 15 années d'expertise et conseil dans la Virtualisation et le Cloud Computing délivrés au quotidien pour vous accompagner dans la sécurisation des données, du Système d'Information et ses environnements.

Système d'exploitation et hyperviseur

Durcir les configurations de l'hyperviseur (KVM, VMware ESXi) et du système d'exploitation (RED HAT, SUSE,...).

Gestion de l'authentification

Fédération de la gestion d'identité, désactivation des comptes locaux, revue des comptes pour l'ensemble des modules.

Fichiers de configuration

Gestion des accès aux fichiers de configuration, revue périodique des paramètres, contrôle de conformité avec la politique de sécurité (suppression des protocoles obsolètes, services non utilisées).

Gestion des autorisations

Revue périodique des droits d'accès définis dans le fichier « policy.json » de chaque module.

Réseaux

Chiffrement des flux, supervision des machines et de la disponibilité des services, cloisonnement de la communication entre machines à l'aide de la micro-segmentation.

Cycle de développement logiciel

Veille sur les nouvelles attaques ou l'obsolescence des librairies utilisées. Pentests des composants, portail web Horizon et sur les développements complémentaires.

Cycle de vie du produit

Gestion de l'obsolescence des versions d'Openstack, mise à disposition des patchs de sécurité.

Gestion des vulnérabilités

Gestion des vulnérabilités de l'environnement Openstack (hyperviseurs, systèmes d'exploitation, modules Openstack) et logiciels associés.

Filtrage

Restreindre les accès (filtrage de port) au niveau du pare-feu et du système ouverts et de vérifier que les flux utilisés sont chiffrés.

Supervision sécurité

Paramétrer des scenarios de sécurité sur le SIEM pour détecter des comportements anormaux à l'aide des logs d'authentifications et d'action (commande utilisée).

metanext

Openstack – Pour aller plus loin …

Metanext accompagne ses clients dans le comparatif, choix et paramétrage d'outils de sécurisation de plateformes Cloud et sur l'ensemble des composantes du SI.

Ansible-hardening utilise des guides de durcissement (**STIG, DISA**) de sécurité standard pour sécuriser les hôtes Linux.

OpenVAS, (**Open source Vulnerability Assessment Scanner**), permet de tester la présence dans les systèmes de failles de sécurité.

Permet d'automatiser les tests de sécurité, en veillant à la conformité aux normes dans chaque environnement et à chaque étape du développement.

Un Guide d'implémentation technique de sécurité (**STIG**) est une méthodologie de cybersécurité pour normaliser les protocoles de sécurité dans les réseaux, les serveurs, les postes de travail afin d'améliorer la sécurité globale

Guide de sécurité Openstack	Guide de sécurité Red Hat - Openstack	Ouvrages Génériques
Openstack security guide (lien) Automated security hardening for Linux hosts with Ansible (lien) Messaging security (lien) Security Checklist (lien) The policy.json file (lien) Security compliance and PCI-DSS (lien) OpenStack Security Notes, and how they help you the Operator (lien) keystone.conf.security_compliance (lien) Openstack security (lien) Vulnerability Management Process (lien) OpenStack Releases (lien)	Security and Hardening Guide (lien) Configuration Reference (lien) Federate with Identity Service (lien) Integrate with Identity Service (lien) Deploy Fernet on the Overcloud (lien) Logging, Monitoring and Troubleshooting (lien) Firewall Rules for Red Hat OpenStack Platform (lien) Manage Secrets with OpenStack Key Manager (lien) Red Hat OpenStack Platform Life Cycle (lien)	OpenStack Cloud Security (lien) Cloud Security Automation: Get to grips with automating your cloud security on AWS and OpenStack (lien) OpenStack for Architects: Design production-ready private cloud infrastructure, 2nd Edition (lien) Identity, Authentication, and Access Management in Openstack: Implementing and Deploying Keystone, OpenStack's Identity Service (lien)