Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1643

(01/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'informatique en nuage – Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage

Exigences et lignes directrices relatives à la sécurité des conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage

Recommandation UIT-T X.1643

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués	X.1400–X.1429
Protocoles de sécurité (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
échange concernant les vulnérabilités/les états	X.1520–X.1539
échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	**X.1640–X.1659**
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Data protection	X.1770–X.1789
SÉCURITÉ DES RÉSEAUX IMT-2020	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1643

Exigences et lignes directrices relatives à la sécurité des conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage

Résumé

La Recommandation UIT-T X.1643 contient une analyse des menaces et des problèmes de sécurité concernant les conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage et décrit un cadre de référence assorti de lignes directrices relatives à la sécurité pour les conteneurs de virtualisation dans le nuage.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1643	2022-01-07	17	11.1002/1000/14804

Mots clés

Lignes directrices sur la sécurité, conteneurs de virtualisation, informatique en nuage.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télé¬com¬mu¬ni¬ca¬tions et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télé¬com¬mu¬ni¬ca¬tions à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1643

Exigences et lignes directrices relatives à la sécurité des conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage

1 Champ d'application

Cette Recommandation contient une analyse des menaces et des problèmes de sécurité concernant les conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage et décrit un cadre de référence assorti de lignes directrices relatives à la sécurité pour les conteneurs de virtualisation dans le nuage.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1162] Recommandation UIT-T X.1162 (2008), *Architecture de sécurité et opérations dans les réseaux entre homologues.*

[UIT-T X.1255] Recommandation UIT-T X.1255 (2013), *Cadre pour la découverte des informations relatives à la gestion d'identité.*

[UIT-T X.1279] Recommandation UIT-T X.1279 (2020), *Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité.*

[UIT-T X.1601] Recommandation UIT-T X.1601 (2015), *Cadre de sécurité applicable à l'informatique en nuage.*

[UIT-T X.1605] Recommandation UIT-T X.1605 (2020), *Exigences de sécurité pour les infrastructures en tant que service (IaaS) publiques dans l'informatique en nuage.*

[UIT-T Y.3508] Recommandation UIT-T Y.3508 (2019), *Informatique en nuage – Aperçu et exigences de haut niveau pour l'informatique en nuage répartie.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [b-UIT-T X.800]: précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

3.1.2 nuage des images [UIT-T Y.3508]: code exécutable présentant le statut d'information d'une machine virtuelle (voir paragraphe 3.1.10) ou conteneur (voir paragraphe 3.1.11).

3.1.3 environnement d'exécution [b-UIT-T Y.4500.1]: entité logique qui représente un environnement capable d'exécuter des modules logiciels.

3.1.4 passerelle [b-UIT-T H.350.4]: dispositif qui assure la conversion entre deux protocoles. Les passerelles assurent souvent la conversion entre le réseau IP et le réseau vocal public commuté en vue de permettre l'intégration des deux.

3.1.5 orchestration [b-UIT-T Y.3100]: dans le contexte d'IMT-2020, processus visant l'agencement, la coordination, l'instanciation et l'utilisation automatisés des fonctions et des ressources du réseau pour les infrastructures physiques et virtuelles sur la base de critères d'optimisation.

3.1.6 réseau superposé [b-UIT-T X.1162]: réseau virtuel qui s'exécute en parallèle d'un autre réseau. Comme tout autre réseau, le réseau superposé comprend une série de nœuds et des liens entre ces derniers. Étant donné que les liens sont des liens logiques, ils peuvent correspondre aux nombreux liens physiques du réseau sous-jacent.

3.1.7 registre [b-UIT-T X.1255]: mécanisme utilisé pour enregistrer les métadonnées relatives aux entités numériques et stocker les schémas de métadonnées, permettant de rechercher des identificateurs persistants grâce à l'utilisation des schémas de métadonnées.

3.1.8 usurpation d'identité [b-UIT-T X.1279]: prétention supposée par une entité d'être une entité différente, en présentant une image enregistrée ou un autre échantillon de données biométriques, ou une caractéristique biométrique artificiellement reproduite, afin d'usurper l'identité d'un individu.

3.1.9 sécurité dans la couche transport [b-UIT-R BT.1699]: protocole utilisé pour envoyer et recevoir des données codées via l'Internet. Ce protocole prend en charge une combinaison de technologies de sécurité diverses y compris le système de chiffrement par clé partagée, les certificats numériques, la fonction de hachage pour prévenir les écoutes illicites, la falsification de messages et l'usurpation d'identité.

3.1.10 machine virtuelle (VM) [b-UIT-T Q.1743]: programme logiciel qui simule l'unité centrale d'un ordinateur fictif. Les programmes exécutés par une machine virtuelle sont représentés sous la forme de codes d'octet, qui sont des opérations primitives pour cet ordinateur fictif.

3.1.11 conteneurs de virtualisation [b-UIT-T L.1362]: subdivision d'un nœud de calcul qui fournit un environnement de calcul virtualisé isolé.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 panne de nœud: défaillance rendant un ou plusieurs nœuds de réseau inaccessibles dans un système d'orchestration.

3.2.2 attaque par reniflage des paquets: méthode de mise sur écoute de tout paquet traversant le réseau illégalement.

3.2.3 mode réseau pont pour conteneur de virtualisation: mode de réseau qui attribue un espace de noms et une adresse IP (protocole Internet) personnels à chaque conteneur de virtualisation et lui permet de communiquer directement avec le serveur.

3.2.4 attaque par évasion du conteneur de virtualisation: l'auteur d'une attaque prend illégalement l'autorité d'"exécution" du conteneur de virtualisation et utilise cette autorité pour obtenir une autorité supérieure de la machine virtuelle (VM) hôte du conteneur de virtualisation ou du serveur hôte physique.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACL	liste de contrôle d'accès (*access control list*)
API	interface de programmation d'applications (*application programming interface*)
CPU	unité centrale de traitement (*central processing unit*)
DDOS	déni de service réparti (*distributed denial of service*)
DOS	déni de service (*denial of service*)
DTLS	sécurité de la couche transport en mode datagramme (*datagram transport layer security*)
IaaS	infrastructure en tant que service (*infrastructure as a service*)
IP	protocole Internet (*Internet protocol*)
IPsec	protocole de sécurité IP (*IP security protocol*)
MITM	Intercepteur (*Man-in-the-Middle*)
OS	système d'exploitation (*operating system*)
TLS	sécurité de la couche transport (*transport layer security*)
VM	machine virtuelle (*virtual machine*)
VXLAN	réseau local extensible virtuel (*virtual extensible local area network*)

5 Conventions

Dans la présente Recommandation:

Le terme "**peut**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée.

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

6 Vue d'ensemble

La présente Recommandation précise le cadre de sécurité du conteneur de virtualisation présenté à la Figure 6-1 comprenant la sécurité de la couche utilisateur, la sécurité de la couche accès, la sécurité de la couche ressource, la sécurité de la couche service, la gestion de la sécurité et le service de sécurité.

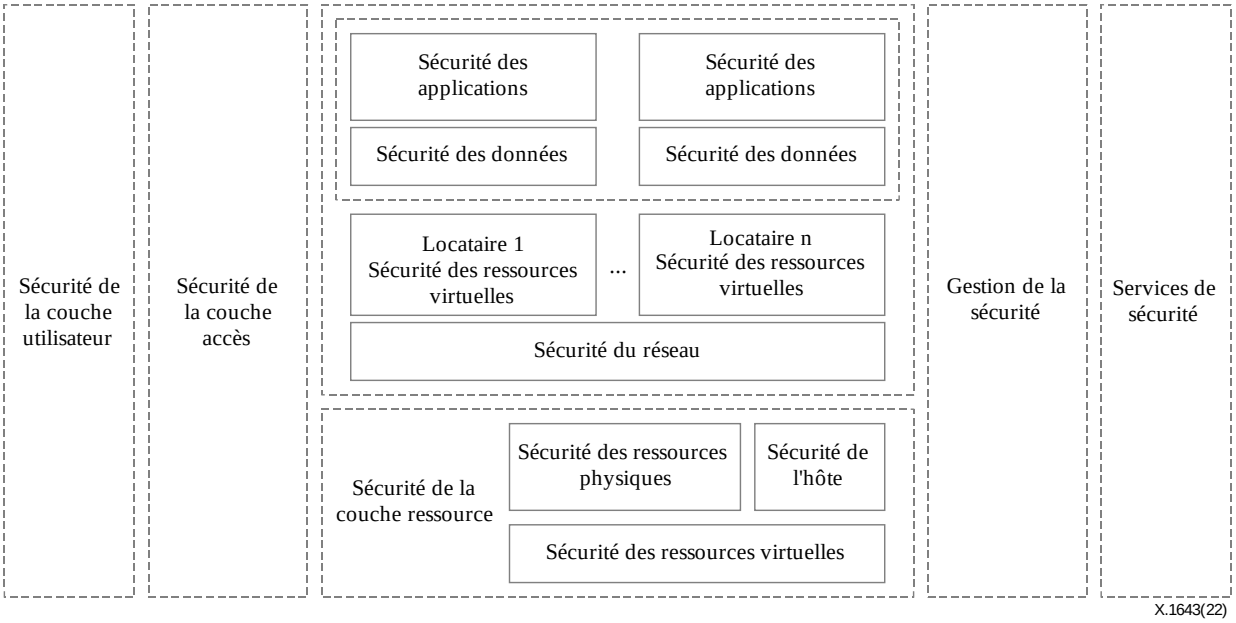

Figure 6-1 – Cadre de sécurité du conteneur de virtualisation

L'objectif d'utilisation du présent cadre consiste à:

– garantir la fiabilité et la stabilité du conteneur de virtualisation dans un environnement utilisant l'informatique en nuage;

– assurer la sécurité du conteneur de virtualisation en protégeant toutes ses composantes, soit la couche utilisateur, la couche accès, la couche ressource, etc.; et

– assurer la gestion de la sécurité et fournir des services de sécurité aux clients du service de conteneurs de virtualisation.

D'après la Figure 6-1:

a) **La sécurité de la couche utilisateur** gère les rôles d'utilisateur, les informations et les opérations d'identification afin de garantir le contrôle de l'accès utilisateur des conteneurs de virtualisation, d'authentifier les utilisateurs et de procéder à l'audit des opérations utilisateur.

b) **La sécurité de la couche accès** inclut les mécanismes de contrôle d'accès, tels que l'accès web ou l'accès de l'interface de programmation d'application (API).

c) **Sécurité de la couche ressource**: la sécurité de la couche ressource distingue la sécurité de la ressource physique, la sécurité du serveur et la sécurité de la ressource virtuelle.

   i) **La sécurité de la ressource physique** désigne la sécurité des ressources matérielles du conteneur de virtualisation, telle que la sécurité des ressources informatiques (l'unité centrale de traitement (CPU) ou la mémoire), les ressources réseau (routeur, commutateur), les ressources de stockage, etc.

   ii) **La sécurité de l'hôte** désigne le serveur hôte sur lequel le conteneur de virtualisation a été mis en œuvre, comme la sécurité du système d'exploitation (OS), de la machine virtuelle, etc.

   iii) **La sécurité de la ressource virtuelle** désigne la sécurité des composants virtuels de virtualisation, comme le calculateur virtuel, le réseau virtuel, le stockage virtuel, etc.

d) **La gestion de la sécurité** désigne les fonctions de gestion de la sécurité du conteneur de virtualisation dans un environnement utilisant l'informatique en nuage, y compris la gestion des identités, la gestion de l'authentification, la gestion des politiques de sécurité, la gestion des opérations de sécurité, la gestion de la maintenance, etc.

e) **Les services de sécurité** fournissent des fonctionnalités de sécurité du conteneur de virtualisation aux utilisateurs sous la forme de services.

7 Enjeux et menaces de sécurité pour le conteneur de virtualisation basé sur l'informatique en nuage

7.1 Enjeux et menaces de sécurité pour l'environnement d'exécution du conteneur de virtualisation

L'environnement d'exécution du conteneur de virtualisation est le premier endroit à protéger, car il est généralement le moins sûr et le plus vulnérable aux insertions de codes malveillants. En outre, d'autres menaces peuvent s'y présenter, telles que des modifications du code source malveillantes ou résultant d'une inadvertance, des altérations malveillantes ou erronées des contrôleurs de construction automatisés, des scripts de configuration chargés d'erreurs et l'ajout de bibliothèques non sécurisées ou de versions non sécurisées du code existant.

7.2 Enjeux et menaces de sécurité pour le conteneur de virtualisation au cours de la phase d'exécution

7.2.1 Enjeux et menaces de sécurité pour la surveillance de la phase d'exécution du conteneur de virtualisation

Les conteneurs de virtualisation sont éphémères. Or cette valeur fondamentale rend leur surveillance difficile. En outre, les outils de surveillance n'ont aucune visibilité ou aucune connaissance de l'intérieur du conteneur de virtualisation au niveau de l'API, ce qui rend la surveillance des comportements du conteneur de virtualisation plus difficile pendant sa phase d'exécution.

7.2.2 Enjeux et menaces de sécurité pour l'isolation de la phase d'exécution du conteneur de virtualisation

L'isolation est une valeur fondamentale du mécanisme de sécurité des conteneurs de virtualisation. En référence à la norme [UIT-T X.1605], l'évasion de machine virtuelle (VM), qui désigne les vulnérabilités des interfaces entre les machines virtuelles que les auteurs d'attaque peuvent exploiter pour contrôler la machine virtuelle ou le serveur de la machine virtuelle, constitue l'un des enjeux majeurs de sécurité de l'infrastructure en tant que service (IaaS) dans l'informatique en nuage. De même, avec une isolation non sécurisée, le moteur de conteneur de virtualisation pourrait souffrir d'une attaque par évasion du conteneur de virtualisation, c'est-à-dire que les auteurs d'attaque pourraient exploiter un conteneur de virtualisation compromis pour attaquer d'autres conteneurs de virtualisation qui partagent le même système d'exploitation hôte, puis attaquer le système d'exploitation hôte sous-jacent ou le serveur directement.

Des traitements inappropriés après l'exécution du conteneur de virtualisation peuvent également introduire d'autres menaces critiques pour la sécurité: 1) il pourrait y avoir une fuite d'informations résiduelles sensibles vers les auteurs d'attaque; 2) en cas d'impossibilité de libérer correctement les ressources informatiques ou réseau, d'autres conteneurs de virtualisation pourraient ne pas acquérir les ressources nécessaires.

7.3 Enjeux et menaces de sécurité pour le registre du conteneur de virtualisation

Comme défini dans [UIT-T X.1255], le registre est un mécanisme utilisé pour enregistrer les métadonnées relatives aux entités numériques et stocker les schémas de métadonnées, et qui permet de rechercher des identificateurs persistants grâce à l'utilisation des schémas de métadonnées. Par

ailleurs, le registre du conteneur de virtualisation contient des informations d'identification importantes pour l'autorisation. Par le biais de contrôles de sécurité mal configurés ou l'exploitation de vulnérabilités, les attaquants peuvent potentiellement accéder illégalement au registre du conteneur de virtualisation et modifier ou supprimer l'intégralité de son contenu. Les logiciels obsolètes peuvent présenter des vulnérabilités et le registre peut en souffrir, car les auteurs d'attaque pourraient exploiter leurs vulnérabilités en vue d'obtenir un accès via des attaques par porte dérobée. En outre, des configurations mal gérées pourraient également être exploitées par des auteurs d'attaque afin de détourner le registre du conteneur de virtualisation.

7.4 Enjeux et menaces de sécurité pour le nuage des images

Comme défini dans la Recommandation [UIT-T Y.3508], le nuage des images est un code exécutable avec le statut d'information de machines virtuelles ou de conteneurs de virtualisation, incluant des systèmes d'exploitation, des bibliothèques, des fichiers de données, des applications, etc. Étant donné que les conteneurs de virtualisation sont mis en œuvre sur le nuage des images, le nuage des images est une condition préalable de la sécurité du conteneur de virtualisation. Le nuage des images est confronté aux menaces majeures suivantes:

a) Les logiciels du nuage d'images peuvent contenir des vulnérabilités qui peuvent être exploitées par des auteurs d'attaques.

b) En cas de configuration incorrecte, la vérification de l'intégrité du nuage d'images peut échouer. En outre, la responsabilité relative à la validation de l'intégrité du nuage d'images dépend des scénarios d'application dans lesquels les fournisseurs de services en nuage sont responsables dès lors que les utilisateurs mettent en œuvre des conteneurs de virtualisation basés sur des nuages de service fournis par les fournisseurs de services en nuage; tandis que les utilisateurs sont responsables dès lors que les conteneurs de virtualisation mis en œuvre sont basés sur des nuages d'images provenant d'ailleurs, comme le téléchargement à partir d'un registre.

c) Les fichiers de nuages d'images peuvent être altérés de manière furtive. Par exemple, les auteurs d'attaque peuvent implanter une porte dérobée ou un logiciel malveillant dans les nuages d'images pendant le téléchargement en amont ou en aval.

7.5 Enjeux et menaces de sécurité pour le système d'exploitation (OS)

Dans l'environnement conteneurisé de virtualisation, tous les conteneurs de virtualisation "partagent" le noyau ainsi que d'autres ressources hôte avec le système hôte. Par conséquent, le système d'exploitation hôte sous-jacent représente la cible la plus vulnérable aux attaques. Si le système d'exploitation est compromis, tous les conteneurs de virtualisation le sont également. En outre, les contrôles et les politiques de sécurité basés sur le serveur peuvent être appliqués à chaque conteneur de virtualisation. De plus, les attaques par évasion des conteneurs de virtualisation qui se produisent via des bogues dans le code de l'application, qui peuvent contourner le moteur et accéder au système d'exploitation hôte et au noyau qui contrôle toutes les autres applications.

7.6 Enjeux et menaces de sécurité pour le système de gestion de l'orchestration du conteneur de virtualisation

Selon la définition donnée dans [b-UIT-T Y.3100], l'orchestration est un processus visant à automatiser l'agencement, la coordination, l'instanciation et l'utilisation des fonctions et des ressources du réseau pour les infrastructures à la fois physiques et virtuelles selon des critères d'optimisation, et c'est une technologie type utilisée dans les réseaux virtuels (tels que les environnements d'informatique en nuage). Dans un environnement de conteneurs de virtualisation en nuage, le système de gestion de l'orchestration permet de gérer des conteneurs de virtualisation à grande échelle qui sont mis en œuvre dans le nuage, et doit faire face aux multiples menaces et enjeux de sécurité suivants:

a) Abus de privilèges: si la politique de sécurité du système de gestion de l'orchestration ne suit pas le principe du moindre privilège, les utilisateurs pourraient en abuser et exploiter les conteneurs de virtualisation au-delà de leurs propres privilèges, ce qui entraîne des conséquences non négligeables en matière de sécurité.

b) Accès non autorisé aux API ouvertes: les API ouvertes et les autres ressources réseau accessibles au public, telles que les ports réseau sur l'Internet, exposent de nouvelles surfaces vulnérables aux attaques. Les auteurs d'attaques peuvent exploiter les vulnérabilités des API ouvertes, telles qu'une authentification, une autorisation ou un contrôle d'intégrité inappropriés, etc., et accéder à l'orchestration des conteneurs de virtualisation, puis exploiter ou modifier ses conteneurs de virtualisation.

c) Gestion des pannes de nœud: une panne de nœud désigne une défaillance rendant un ou plusieurs nœuds de réseau inaccessibles dans le système de gestion de l'orchestration. Une gestion inappropriée de la défaillance d'un nœud pourrait perturber les autres nœuds non affectés par la panne ainsi que la gestion de l'orchestration. Les auteurs d'attaques pourraient en faire un usage malveillant et réduire les performances des orchestrations.

d) Gestion de la configuration: un système de gestion de l'orchestration d'un conteneur de virtualisation introduit différentes configurations sur une quantité énorme d'installations et divers types de services, ce qui exige une politique de sécurité de haut niveau pour la gestion de la configuration. Une mauvaise configuration pourrait élargir les surfaces d'exposition aux attaques et entraîner des risques de sécurité importants. Par exemple, les auteurs d'attaque pourraient pénétrer dans le logiciel d'orchestration interne par le biais d'applications de conteneurs de virtualisation.

7.7 Enjeux et menaces de sécurité pour le réseau du conteneur de virtualisation

Un réseau de conteneurs de virtualisation peut fonctionner selon deux modes de réseau type, le mode de réseau de pont du conteneur de virtualisation et le mode de réseau superposé du conteneur de virtualisation, pour communiquer avec d'autres conteneurs de virtualisation sur le même serveur, sur différents serveurs ou au sein de conteneurs de virtualisation.

Le mode réseau pont de conteneur de virtualisation attribue un espace de noms et une adresse de protocole Internet (IP) individuels à chaque conteneur de virtualisation et permet au conteneur de virtualisation de communiquer directement avec le serveur.

Comme défini dans [UIT-T X.1162], un réseau superposé est un réseau virtuel qui fonctionne au-dessus d'un autre réseau. Comme tout autre réseau, le réseau superposé comprend une série de nœuds et des liens entre ces derniers. Étant donné que les liens sont des liens logiques, ils peuvent correspondre aux nombreux liens physiques du réseau sous-jacent. Dans un environnement de conteneurs de virtualisation en nuage, un réseau superposé de conteneur de virtualisation connecte des conteneurs de virtualisation distribués. Plus précisément, il construit un réseau virtuel superposé au-dessus du réseau sous-jacent de chaque serveur par la technique du réseau local virtuel extensible (VXLAN), afin de permettre l'interconnexion des conteneurs de virtualisation et de permettre aux conteneurs de virtualisation de communiquer entre les serveurs.

Les défis et les menaces de sécurité communs aux deux modes de réseau du conteneur de virtualisation comprennent:

– **Attaque par déni de service (DoS)/déni de service réparti (DDoS)**

  Un réseau de conteneurs de virtualisation est confronté à des menaces d'attaques DoS/DDoS provenant de réseaux internes et externes:

a) Menaces DoS/DDoS provenant des réseaux internes: un attaquant peut exploiter des conteneurs de virtualisation compromis pour lancer des attaques DoS/DDoS sur d'autres conteneurs de virtualisation sur le même réseau, afin de submerger les ressources informatiques des cibles telles que la bande passante, les unités centrales de traitement (CPU), etc.

b) Menaces DoS/DDoS provenant de réseaux externes: les conteneurs de virtualisation utilisant le même hébergeur partagent les mêmes adaptateurs de réseau physique. De plus, si un pirate lance des attaques DoS/DDoS sur un conteneur de virtualisation cible en envoyant un grand volume de paquets de données à partir de serveurs botnet, cela peut non seulement endommager le conteneur de virtualisation cible, mais aussi submerger la bande passante du réseau de la machine hôte, ce qui entraîne des attaques par déni de service DoS/ ou déni de service réparti DDoS sur le serveur et d'autres conteneurs de virtualisation.

– **Attaque par intercepteur**

Les conteneurs de virtualisation sous divers modes de réseau ne fournissent pas de mécanismes de chiffrement au départ, ce qui fait que les conteneurs de virtualisation sont en fait vulnérables à une attaque par intercepteur (MITM). Par exemple, la norme [UIT-T X.1279] définit l'usurpation d'identité comme la prétention supposée par une entité d'être une entité différente, en présentant une image enregistrée ou un autre échantillon de données biométriques, ou une caractéristique biométrique artificiellement reproduite, afin d'usurper l'identité d'un individu. Un auteur d'attaque pourrait exploiter un conteneur de virtualisation compromis et effectuer des attaques par usurpation d'identité vers un conteneur de virtualisation cible sur le même réseau virtuel. S'il y parvient, l'auteur des attaques peut détourner le trafic réseau normal du conteneur de virtualisation, puis réaliser une série d'attaques par intercepteur.

Les applications se trouvant dans les conteneurs de virtualisation peuvent choisir d'effectuer leur propre chiffrement en utilisant des protocoles tels que le protocole de sécurité de la couche transport (TLS) ou la sécurité dans la couche transport en mode datagramme (DTLS). Dans ces cas, un maître d'œuvre qui comprend les mouvements de trafic à l'intérieur du conteneur de virtualisation, ou entre les conteneurs de virtualisation, peut choisir de ne pas dupliquer la prestation de chiffrement. L'objectif de cette approche est de maximiser la protection du trafic entre les conteneurs de virtualisation tout en minimisant les surcoûts de calcul associés au chiffrement du même trafic plusieurs fois.

Les menaces de sécurité particulières auxquelles sont confrontés le mode réseau pont des conteneurs de virtualisation et le mode réseau superposé des conteneurs de virtualisation sont décrites aux paragraphes 7.7.1 et 7.7.2.

7.7.1 Mode réseau pont du conteneur de virtualisation

Dans le mode réseau pont du conteneur de virtualisation, un conteneur de virtualisation se connecte à un réseau virtuel par son interface réseau virtuelle, ce qui permet au conteneur de virtualisation de communiquer directement avec le serveur hôte et d'agir comme passerelle initiale. Les paquets réseau d'un conteneur de virtualisation seront d'abord envoyés à la passerelle initiale, puis acheminés vers d'autres conteneurs de virtualisation. Les conteneurs de virtualisation sous le même réseau virtuel sont interconnectés.

Sans une politique de sécurité de réseau pour le mode de réseau de pont de conteneur de virtualisation, il n'y a pas de contrôle d'accès au réseau entre les conteneurs de virtualisation. S'il n'y a pas de pare-feu ni d'autres mécanismes de défense du réseau, l'auteur d'une attaque se trouvant dans un conteneur de virtualisation peut facilement lancer diverses attaques vers d'autres conteneurs de virtualisation, par exemple par usurpation d'identité, attaque par reniflage de paquets, etc., ce qui entraîne de graves conséquences, comme la fuite d'informations sensibles, etc.

Par conséquent, il existe des risques pour la sécurité du réseau en mode réseau pont de conteneurs de virtualisation sans une politique de contrôle d'accès au réseau efficace entre les conteneurs de virtualisation sur le même hébergeur.

7.7.2 Mode réseau superposé du conteneur de virtualisation

Le mode réseau superposé des conteneurs de virtualisation ne dispose pas de politique de contrôle d'accès au réseau initial pour les conteneurs de virtualisation. De plus, comme le trafic réseau VXLAN n'est pas chiffré par défaut, il faut utiliser d'autres protocoles de tunnellisation, tels que le protocole de sécurité IP (IPsec), etc., pour crypter le trafic réseau VXLAN et garantir la sécurité du transfert des données.

8 Exigences et lignes directrices relatives à la sécurité des conteneurs de virtualisation dans un environnement utilisant l'informatique en nuage

Le présent paragraphe présente les exigences et lignes directrices correspondant aux enjeux et menaces de sécurité pour les conteneur de virtualisation tels que décrits au paragraphe 7.

8.1 Exigences et lignes directrices relatives à la sécurité de la phase d'exploitation des conteneurs de virtualisation

a) Lors de la mise à jour d'applications ou de services, les conteneurs de virtualisation en cours d'exécution doivent être arrêtés et remplacés par de nouveaux conteneurs de virtualisation.

b) Des outils doivent être utilisés pour rechercher les vulnérabilités courantes sur les durées de fonctionnement déployées. Toute instance à risque doit être mise à niveau.

c) Aucun utilisateur non autorisé ne doit avoir accès au démon de conteneur de virtualisation.

8.2 Exigences et lignes directrices relatives à la sécurité du registre des conteneurs de virtualisation

a) Le serveur qui héberge le registre doit être verrouillé afin d'atténuer le risque d'attaque à cet endroit.

b) Les outils de développement, le système de gestion de l'orchestration et les conteneurs de virtualisation doivent être configurés de façon à se connecter aux registres uniquement par le biais de canaux chiffrés.

c) Les registres doivent être débarrassés des images de services en nuage dangereuses et vulnérables qui ne doivent plus être utilisées.

d) Tout accès au registre doit nécessiter une authentification afin de garantir que seules les images de services en nuage provenant d'entités de confiance peuvent y être ajoutées.

8.3 Exigences et lignes directrices relatives à la sécurité du nuage des images des conteneurs de virtualisation

a) L'objectif des images de services en nuage est de créer un conteneur de virtualisation d'application ou de service. Les images de services en nuage ne doivent pas être utilisées pour d'autres tâches.

b) Les signatures des images de services en nuage doivent être validées avant l'exécution des images de services en nuage pour garantir que les images de services en nuage proviennent de sources fiables et n'ont pas été altérées.

c) Une surveillance et une maintenance continues des registres doivent être mises en œuvre pour garantir que les images de services en nuage qui s'y trouvent sont maintenues et mises à jour à mesure que les vulnérabilités et les exigences de configuration changent.

d) L'accès aux images de services en nuage doit utiliser des noms inaltérables permettant de distinguer les différentes versions des images de services en nuage.

8.4 Exigences et lignes directrices relatives à la sécurité pour le système d'exploitation hôte des conteneurs de virtualisation

a) Les vecteurs d'attaque doivent être réduits au minimum en supprimant de l'environnement du serveur tout ce qui ne lui est pas essentiel.

b) Les charges de travail virtualisées et conteneurisées ne doivent pas être mélangées sur la même instance hôte.

c) La version du système d'exploitation hôte doit être validée par la mise en œuvre de pratiques et d'outils de gestion.

d) Toute authentification au sein du système d'exploitation doit être auditée.

e) Les conteneurs de virtualisation doivent fonctionner avec l'ensemble minimal de permissions requises pour le système de fichiers. Tout changement de fichier dans le système d'exploitation hôte du conteneur de virtualisation ne doit être effectué que dans le respect des politiques d'autorisation.

8.5 Exigences et lignes directrices relatives à la sécurité pour le système de gestion de l'orchestration des conteneurs de virtualisation

a) Un système de gestion de l'orchestration doit être installé à partir d'une source officielle, fiable et à jour.

b) Le système de gestion de l'orchestration doit être configuré pour assurer une haute disponibilité et un basculement automatique dans la mesure du possible.

c) Le système de gestion de l'orchestration doit utiliser un modèle d'accès au moindre privilège, dans lequel l'utilisateur ne se voit accorder que la capacité d'effectuer les actions spécifiques sur l'hôte, le conteneur de virtualisation et l'image du service en nuage spécifiques.

d) Des méthodes d'authentification forte, telles que l'authentification multifactorielle au lieu d'un simple mot de passe, doivent être utilisées pour les comptes administratifs du système de gestion de l'orchestration.

e) Le système de gestion de l'orchestration doit être configuré pour séparer le trafic réseau en réseaux virtuels distincts par niveau de sensibilité.

f) Le système de gestion de l'orchestration doit être configuré pour isoler les déploiements dans des ensembles spécifiques d'hôtes par niveau de sensibilité.

8.6 Exigences et lignes directrices relatives à la sécurité des conteneurs de virtualisation sous différents modes de réseau

8.6.1 Restriction de trafic entre conteneurs de virtualisation en mode réseau pont pour conteneur de virtualisation

En mode réseau pont, la configuration de sécurité initiale par défaut du conteneur de virtualisation ne permet pas de contrôler ni de restreindre l'accès au réseau. Afin de prévenir les menaces de déni de service ou de déni de service réparti (DoS/DDoS) potentielles, il devrait y avoir des politiques de contrôle d'accès au réseau selon les exigences réelles, notamment:

a) La communication entre conteneurs de virtualisation doit être complètement interdite si possible. Dans des scénarios d'application spécifiques, si tous les conteneurs de virtualisation du serveur n'ont pas besoin de communication réseau entre eux, la communication entre conteneurs de virtualisation peut être interdite en modifiant la configuration de sécurité par défaut.

b) Des politiques de contrôle d'accès entre conteneurs de virtualisation doivent être mises en œuvre: dans l'environnement en nuage du conteneur de virtualisation où la multi-location existe, il peut arriver dans une certaine situation qu'un seul conteneur de virtualisation occupe plusieurs serveurs afin de submerger la bande passante des autres conteneurs de

virtualisation. Afin d'assurer une communication régulière entre les conteneurs de virtualisation et d'éviter les trafics anormaux causés par les attaques DoS/DDoS, des mécanismes de restriction du trafic de communication entre les conteneurs de virtualisation doivent être mis en œuvre.

c) Des mécanismes et des politiques de cryptage doivent être mis en place, par exemple, l'utilisation du protocole IPsec pour crypter le trafic et assurer la confidentialité de la communication entre les conteneurs de virtualisation, afin de l'empêcher de renifler le réseau ou de subir une attaque par intercepteur

8.6.2 Contrôle d'accès entre conteneurs de virtualisation

a) Contrôle d'accès pour le mode réseau pont des conteneurs de virtualisation

En mode réseau pont, la configuration de sécurité initiale par défaut des conteneurs de virtualisation permet aux conteneurs de virtualisation de se connecter au même réseau virtuel et de communiquer directement entre eux. Par conséquent, afin d'empêcher les accès anormaux, les mécanismes et les politiques de contrôle d'accès doivent être configurés à la demande. Notamment:

1) Des réseaux virtuels différents pour les conteneurs de virtualisation doivent être configurés pour cloisonner le réseau entre les différents conteneurs de virtualisation. Cela permettra de bloquer le trafic de communication avec d'autres réseaux et d'atteindre l'objectif d'isolement entre les réseaux des conteneurs de virtualisation.

2) Le contrôle d'accès basé sur la politique de liste blanche doit être mis en œuvre pour assurer la sécurité du réseau entre les conteneurs de virtualisation, la communication entre les conteneurs de virtualisation doit être interdite par défaut, puis configurer les règles de contrôle d'accès à la demande. Le contrôle d'accès basé sur la politique de liste blanche réduit la surface d'attaque par une stratégie de minimisation.

b) Contrôle d'accès pour le mode réseau superposé des conteneurs de virtualisation

En mode réseau superposé de conteneurs de virtualisation, différents conteneurs de virtualisation peuvent accéder directement les uns aux autres sur le même sous-réseau et le même hébergeur. La liste de contrôle d'accès (ACL) doit être ajoutée manuellement aux politiques de contrôle d'accès du serveur, ou un pare-feu doit être mis en œuvre sur le serveur, afin de contrôler l'accès des hôtes externes aux applications internes des conteneurs de virtualisation.

Dans un vaste environnement en nuage de conteneurs de virtualisation, il n'est pas toujours pratique de mettre à jour les règles de pare-feu manuellement en raison des fréquentes mises à jour dynamiques des microservices [b-UIT-T J.1301]. Il est recommandé d'utiliser certains outils pour gérer le processus automatiquement, comme la micro-segmentation des conteneurs de virtualisation qui est une technique de pare-feu destinée aux conteneurs de virtualisation fournissant des mécanismes d'isolement de segmentation de réseau à grain fin et permet de cloisonner en segments un seul conteneur de virtualisation, des conteneurs de virtualisation dans un même sous-ensemble de réseau, ou des applications de conteneurs de virtualisation, et d'appliquer des politiques de contrôle d'accès au réseau en conséquence.

Bibliographie

[b-UIT-T H.350.4] Recommandation UIT-T H.350.4 (2011), *Architecture des services d'annuaire pour les systèmes à protocole SIP*.

[b-UIT-T J.1301] Recommandation UIT-T J.1301 (2021), *Spécification d'un service média convergent fondé sur le nuage pour prendre en charge la télévision par câble utilisant le protocole Internet et la radiodiffusion – Exigences.*

[b-UIT-T L.1362] Recommandation UIT-T L.1362 (2019), *Interface pour la gestion d'énergie dans les environnements de virtualisation des fonctions de réseau – Couche d'abstraction verte version 2.*

[b-UIT-T Q.1743] Recommandation UIT-T Q.1743 (2016), *Références IMT évoluées à la version 11 du réseau central évolué en mode paquet LTE-advanced.*

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre de sécurité pour les systèmes ouverts: Présentation générale.*

[b-UIT-T X.1162] Recommandation UIT-T X.1162 (2008), *Architecture de sécurité et opérations dans les réseaux entre homologues.*

[b-UIT-T X.1251] Recommandation UIT-T X.1251 (2019), *Cadre de contrôle de l'identité numérique par l'utilisateur.*

[b-UIT-T X.1255] Recommandation UIT-T X.1255 (2013), *Cadre pour la découverte des informations relatives à la gestion d'identité.*

[b-UIT-T X.1279] Recommandation UIT-T X.1279 (2020), *Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité.*

[b-UIT-T X.1604] Recommandation UIT-T X.1604 (2020), *Exigences de sécurité relatives au réseau en tant que service (NaaS) dans l'informatique en nuage.*

[b-UIT-T Y.3100] Recommandation UIT-T Y.3100 (2017), *Réseaux IMT-2020: termes et définitions.*

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014), *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire*.

[b-UIT-T Y.3502] Recommandation UIT-T Y.3502 (2014), *Technologies de l'information – Informatique en nuage – architecture de référence.*

[b-UIT-T Y.4500.1] Recommandation UIT-T Y.4500.1 (2018), *oneM2M – Architecture fonctionnelle.*

[b-UIT-R BT.1699] Recommandation UIT-R BT.1699 (2013), *Harmonisation des formats des applications déclaratives pour la télévision interactive.*

[b-ISO/CEI 19944] ISO/CEI 19944:2016, *Technologies de l'information – Services et dispositifs en nuage: s: débits, catégories et utilisation des données.*

[b-ISO/CEI 27000] ISO/CEI 27000:2016, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

[b-ISO/CEI 27729] ISO/CEI 27729:2012, *Information et documentation – Code international normalisé des noms (ISNI)*.

[b-ISO/CEI 29100] ISO/CEI 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre privé*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022